Upgrade

17 JUL 2018
VMware Validated Design 4.3
VMware Validated Design for Software-Defined Data Center 4.3

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

About VMware Validated Design Upgrade

The *VMware Validated Design Upgrade* document provides step-by-step instructions for upgrading VMware software in a Software-Defined Data Center (SDDC) that are deployed according to the VMware Validated Design for Software-Defined Data Center.

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

Intended Audience

The *VMware Validated Design Upgrade* document 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.

Required VMware Software

VMware Validated Design Upgrade is compliant and validated with certain product versions. For more information about supported product versions, see *VMware Validated Design Release Notes* and VMware Software Versions in the Upgrade.

SDDC Upgrade Overview

1

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 a successful SDDC upgrade.

This chapter includes the following topics:

Upgrade Policy

VMware Validated Design provides prescriptive guidance to update and upgrade the SDDC management products according to an upgrade validation policy.

Updates That Are Validated by VMware Validated Design

VMware Validated Design follows a set of lifecycle management principles for the SDDC.

Upgrade	Might impact 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 a VMware Validated Design provides a prescriptive path between each release where, unless specific express patches or hot fixes are required for an environment, a deviation is not supported.

Updates That Are Not Validated by VMware Validated Design

Scalability and functionally tests for individual patches, express patches or hot fixes are not typically performed against VMware Validated Design. If a patch must be applies to your environment, follow the VMware published practices and VMware Knowledge Base articles for the specific patch. If an issue occurs during or after the process of applying a patch, contact VMware Technical Support.

Upgrade Paths and Application Upgrade Sequence

You must follow the SDDC upgrade path and sequences specified for this VMware Validated Design.

Upgrade Paths

You must run version 4.2 of this VMware Validated Design before you upgrades to version 4.3.

Currently Installed Version	Upgrade Path
2.0	1 3.0 2 3.0.2 3 4.0.x
3.0	1 3.0.2 2 4.0.x
3.0.2	1 4.0.x 2 4.1
4.0.x	4.1
4.1	4.2
4.2	4.3

Upgrade Sequence

The upgrade process of this VMware Validated Design follows a prescriptive path that isolates the VMware components in functional layers. By following this path, you can incrementally upgrade from one version to another while minimizing context switching between products and user interfaces and minimizing the number of product champions required during maintenance windows. In addition, the upgrade sequence reduces the overall upgrade window and the impact in the event of a failed upgrade. Follow this sequence also for interoperability with the broader components in the SDDC. In this way, the upgrade sequence provides progressive, granular upgrade over the course of time.

Table 1-1. Upgrade Sequence of This VMware Validated Design

Order	Upgraded or Updated	Component	Sub-Component (in Order)	Layer
1	Yes	vRealize Automation	vRealize Automation Appliances	Cloud Management
			vRealize Orchestrator (Embedded)	
			vRealize Automation IaaS Components	
2	Yes	vRealize Business for Cloud	vRealize Business Appliance	
			vRealize Business Data Collectors	
3	Yes	vRealize Operations Manager	-	Operations Management
4	Yes	vRealize Log Insight	vRealize Log Insight Appliances	
			vRealize Log Insight Agents	
5†	Determined by Organization	vSphere Storage APIs for Data Protection-based Backup Solution	-	Business Continuity - Backup and Restore
6	No	NSX for vSphere	NSX Manager Instances	Virtual Infrastructure - Networking
			NSX Controller Instances	
			NSX Networking Fabric	
			NSX Edges	
7	Yes	Platform Services Controller	-	Virtual Infrastructure - Management
		vCenter Server	-	
		vSphere Replication	-	Business Continuity - Disaster Recovery
		Site Recovery Manager	-	
		vSphere Update Manager Download Service	-	Virtual Infrastructure - Management
		ESXi	-	
		VMware Tools	-	
		vSAN	-	
8	Yes	vCenter Server	-	Virtual Infrastructure - Shared Edge and Compute
			-	
		ESXi	-	

Note vSphere Data Protection is deprecated. VMware Validated Designs do not provide guidance for its usage and lifecycle management during the upgrade process.

VMware Validated Design requires a compatible and supported backup solution. Refere to ....If the backup solution is not compatible, upgrade the backup solution before you proceed with upgrading the rest of the components of this VMware Validated Design.

Introducing vRealize Suite Lifecycle Manager and Third vRealize Automation Appliance

VMware Validated Design 4.3 extends the product stack with vRealize Suite Lifecycle Manager for automated deployment, lifecycle, and configuration drift management of the vRealize Suite products, and adds a third node to the vRealize Automation appliance cluster for automatic database failover. Add these components to your environment as a part of the post-upgrade process for the operations management and cloud management layers, respectively.

vRealize Suite Lifecycle Manager

VMware Validated Design 4.3 uses vRealize Suite Lifecycle Manager for automated deployment of the vRealize products in the SDDC stack.

The vRealize Suite Lifecycle Manager solution supports the deployment and upgrade of following vRealize Suite products:

- vRealize Operations Manager
- vRealize Log Insight
- vRealize Automation (with embedded vRealize Orchestrator)
- vRealize Business for Cloud

vRealize Suite Lifecycle Manager provides the following features for management of multi-product environments:

- Manage a vRealize Suite product repository (installation and upgrade).
- Create environments.
- Deployment and management of VMware Marketplace content
- Support existing vRealize Suite-based environments.
- Analyze the configuration drift in environments.
- Scale environments out.
- Upgrade environments.

You add it to the product stack as a part of the post-upgrade process for the operations management layer. See Deploy and Configure vRealize Suite Lifecycle Manager Post-Upgrade and Import the vRealize Product Configurations in vRealize Suite Lifecycle Manager.

Three-Node Cluster of vRealize Automation Appliances

VMware Validated Design 4.3, the Cloud Management Platform contains three vRealize Automation appliances for automatic failover of the PostgreSQL database. You deploy the third appliance as a part of the post-upgrade process for the cloud management layer. See Expand vRealize Automation to a Three-Node Appliance Architecture Post-Upgrade.

VMware Software Versions in the Upgrade

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

Table 1-2. Upgrade from VMware Validated Design for Software-Defined Data Center 4.2 to VMware Validated Design for Software-Defined Data Center 4.3

SDDC Layer	Product Name	Product Version in VMware Validated Design 4.2	Product Version in VMware Validated Design 4.3	Operation Type
Cloud Management	vRealize Automation with Embedded vRealize Orchestrator	7.3	7.4	Upgrade
	vRealize Business for Cloud	7.3.1	7.4	Upgrade
Operations Management	vRealize Operations Manager	6.6.1	6.7	Upgrade
	vRealize Log Insight	4.5.1	4.6	Upgrade
	vRealize Log Insight Agent	4.5.1	4.6	Upgrade
Virtual Infrastructure	NSX for vSphere	6.4.0	6.4.1	Update
	vCenter Server	6.5 Update 1	6.5 Update 2	Update
	Platform Services Controller	6.5 Update 1	6.5 Update 2	Update
	vSphere Update Manager Download Service	6.5 Update 1	6.5 Update 2	Update
	ESXi	6.5 Update 1	6.5 Update 2	Update
	vSAN	6.6.1	6.6.1 Update 2	Update
Business Continuity and Disaster Recovery	Site Recovery Manager	6.5.1	6.5.1.1	Patch
	vSphere Replication	6.5.1	6.5.1.3	Patch
	Backup solution based on VMware vSphere Storage APIs for Data Protection	Compatible Version	Compatible Version	Not applicable

For information about all components included in the VMware Validated Design 4.2 and VMware Validated Design 4.3 software bill of materials, see *the VMware Validated Design Release Notes*.

General Prerequisites for the SDDC Upgrade

Before you upgrade the functional layers of the SDDC, verify that your existing VMware Validated Design environment meets certain general prerequisites.

- Verify that your environment implementation follows exactly the software bill of materials for the previous release.
- Examine the release notes for each product version included in the updated software bill of materials for the design.
- Examine the *VMware Validated Design Planning and Preparation* documentation and the individual prerequisites for each layer of upgrade. Address any hardware or software requirements that might impact the upgrade.
- Verify that your server hardware has been certified with vSphere 6.5 Update 2. For more information, see the VMware Compatibility Guide.
- Verify that your *VMware vSphere Storage APIs for Data Protection*-based backup solution has been certified with vSphere 6.5 Update 2. For more information, contact your backup solution vendor.

Note VMware vSphere Data Protection has reached End of Availability. The design no longer provides guidance for its usage and lifecycle management.

- Review all custom integrations developed and deployed externally from the VMware Validated Design framework to ensure compatibility with product versions in the updated software bill of materials.
- Review all third-party product integrations in your environment to ensure compatibility with the product versions in the updated software bill of materials.

Best Practices in SDDC Upgrades

Prepare for an upgrade and perform post-upgrade activities to verify the operational state of the SDDC.

Planning for the SDDC Upgrade

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

  You organize upgrade sequences to allocate a single maintenance window to the upgrade of each layer.
- Allocate time in your maintenance window to run operational verification tests. For example, critical business functions, integration validations, and system performance. Add time to respond to incidents or errors without exceeding your maintenance window.
- Plan for any potential impact to tenant workloads during an upgrade. If capacity allows, use vSphere vMotion to temporarily migrate tenant workloads to other compute clusters during an upgrade.

- Communicate the upgrade to your organization and tenant stakeholders.
- Communicate the upgrade to your VMware Technical Account Manager and Global Support Service representative, as applicable.
- Perform and verify the backups and snapshots for the SDDC management components.
- Ensure the management virtual machines or appliances are not running on snapshot before you perform the upgrade of the respective layer. Guidance for each layer discusses the use of snapshots.

Considerations for an Upgrade Failure

- Collect the product support bundles for the failed product upgrade and contact VMware Technical Support.
- Rollback the component upgrade.

  In the event of a component upgrade failure, the order of operations ensures that backward compatibility and interoperability are maintained between the layers. You can roll back to a previous version of the components in a layer.

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

Post-Upgrade Operations

After you complete an upgrade, consider the following practices.

- Verify business functionality, integration, and system performance. For more information, see the *VMware Validated Design Operational Verification* documentation.
- Conduct an upgrade retrospective discussion. Document the areas for process improvement and incorporate them in the next upgrade.

Upgrade the Cloud Management Layer

2

You start the upgrade of the VMware Validated Design from the previous version by upgrading the product versions and then implementing the design changes of the cloud management layer.

Procedure

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

You begin upgrading VMware Validated Design from the previous version by upgrading the cloud management layer. In the context of the cloud management layer, you start with by upgrading vRealize Automation because it connects to the rest of the cloud management layer components.

2 Upgrade vRealize Business Virtual Appliances

After you complete the upgrade of vRealize Automation, upgrade vRealize Business to complete the upgrade of the cloud management layer to VMware Validated Design 4.3.

3 Post-Upgrade Configuration of the Cloud Management Layer

After you complete the upgrade of the Cloud Management Layer, perform the post-upgrade configuration changes to the environment according to the design objectives and deployment guidance to ensure your environment remains aligned to this VMware Validated Design.

4 Expand vRealize Automation to a Three-Node Appliance Architecture Post-Upgrade

Perform the post-upgrade operation of expanding your vRealize Automation cluster to include a third appliance so that your environment remains aligned to this VMware Validated Design.

Table 2-1. Upgrade Sequence for the Cloud Management Layer

Order	Components	Sub-Component
1	vRealize Automation	vRealize Automation Appliances with Embedded vRealize Orchestrator
		vRealize Automation IaaS Components
2	vRealize Business for Cloud	vRealize Business Server
		vRealize Business Data Collector
3	Post-Upgrade Configuration Changes	-
4	Post-Upgrade Expansion of vRealize Automation	-

Upgrade vRealize Automation Virtual Appliances and the Infrastructure-as-a-Service Components

You begin upgrading VMware Validated Design from the previous version by upgrading the cloud management layer. In the context of the cloud management layer, you start with by upgrading vRealize Automation because it connects to the rest of the cloud management layer components.

You first upgrade the vRealize Automation virtual appliances in Region A. You then perform an automated upgrade of the vRealize Automation Infrastructure-as-a-Service (IaaS) components in Region A and Region B.

Table 2-5. 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.locall
	vRealize Automation Server Appliance	192.168.11.51	vra01svr01a.rainpole.local
		192.168.11.52	vra01svr01b.rainpole.local
	vRealize Automation for IaaS Web 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 IaaS Model Manager VIP	192.168.11.59	vra01ims01.rainpole.local
	vRealize Automation IaaS Model Manager Server	192.168.11.57	vra01ims01a.rainpole.local
		192.168.11.58	vra01ims01b.rainpole.local
	vRealize Automation IaaS DEM Worker	192.168.11.60	vra01dem01a.rainpole.local
		192.168.11.61	vra01dem01b.rainpole.local
	vRealize Automation IaaS Proxy Agent	192.168.31.52	sfo01ias01a.sfo01.rainpole.local
		192.168.31.53	sfo01ias01b.sfo01.rainpole.local
	Microsoft SQL Server for vRealize Automation	192.168.11.62	vra01mssql01.rainpole.local
Region B	vRealize Automation IaaS Proxy Agent	192.168.32.52	lax01ias01a.lax01.rainpole.local
		192.168.31.53	lax01ias01b.lax01.rainpole.local

Prerequisites

Verify that all vRealize Automation components have the required compute and storage resources to perform the upgrade, including space for temporary objects created during the process.

Table 2-2. Hardware Requirements for Upgrading vRealize Automation

Node	Hardware Requirement for Each Node	Description
vRealize Automation Appliances	Available disk space	■ Disk1 with 50 GB ■ Disk3 with 25 GB ■ Disk4 with 50 GB ■ At least 4.5 GB of free disk space on the root partition to download and run the upgrade. ■ At least 4.5 GB of free space on the `/storage/db` ■ `/storage/log` subfolder cleaned of older archived ZIP files to free up disk space.
	Memory	18 GB
	vCPU	4
vRealize Automation IaaS Windows virtual machines and Microsoft SQL Server database	Available disk space	5 GB

Verify that third-party software components required for the upgrade are available on the vRealize Automation nodes.

Table 2-3. Software Requirements for Upgrading vRealize Automation

Node	Software Requirement	Description
Primary vRealize Autonation IaaS Model Manager Server: vra01iws01a.rainpole.local	Java	■ Java SE Runtime Environment 8 64-bit Update 161 or later installed. Remove versions prior to Update 161. ■ After you install Java, set the `JAVA_HOME` environment variable to the directory path of the new version.

Download the required software for the upgrade is available on the vRealize Automation nodes and verify the current condition of vRealize Automation .

Table 2-4. Configuration Prerequisites for Upgrading vRealize Automation

Prerequisite Category	Description
Compatibility	Verify all third-party integrations that might have been configured for use with vRealize Automation are compatible with vRealize Automation version 7.4. Contact the third-party integration vendor or developer to ensure compatibility.
Backup	■ Verify that current backups of the vRealize Automation virtual appliances and the Infrastructure-as-a-Service (IaaS) virtual machines exist. ■ Verify that a current backup of the external vRealize Automation database exists. The default name of the Microsoft SQL Server database is `VRADB-01`.
Downloads	Download the vRealize Automation `VMware-vR-Appliance-7.4.0.xxx-xxxxxxx-updaterepo.iso` upgrade file to a shared datastore. If you have space on an NFS datastore, upload the upgrade file to the NFS datastore to save space on your vSAN datastore. You can then mount the `.iso` file to the vRealize Automation virtual appliances from the vSphere Web Client.

Table 2-4. Configuration Prerequisites for Upgrading vRealize Automation (Continued)

Prerequisite Category	Description

Cluster Integrity and Health	■ Examine the health of vRealize Automation by using the vRealize Production Test Tool to ensure that it is in good health. Remediate any issues prior to beginning the upgrade. See the product download page version 1.7.1.
	■ Open a Web browser and log in to the VAMI management interfaces by navigating to **`https://vra01svr01a.rainpole.local:5480`**. Select **vRA Settings > Cluster** and verify that all vRealize Automation IaaS Windows Server nodes meet the following requirements:
	  ■ Have a `Last Connected` status of less than 30 seconds.
	  ■ Have a `Time Offset` status of less than 1 second.
	■ Open a web browser and log in to both VAMI management interfaces by navigating to **`https://vra01svr01a.rainpole.local:5480`** and **`https://vra01svr01b.rainpole.local:5480`**. Select **vRA Settings > Cluster** and verify that both vRealize Automation virtual appliances meet the following requirements:
	  ■ Have a `Last Connected` status of less than 10 minutes.
	  ■ The PostgreSQL database is connected and reporting a `Status` state of `Up`, indicating that the master and replica nodes are running.
	  ■ The PostgreSQL database is connected and reporting a `Valid` state of `Yes`, indicating synchronization between the master and replica nodes.
	■ Open a Web browser and log in to both VAMI management interfaces by navigating to **`https://vra01svr01a.rainpole.local:5480`** and **`https://vra01svr01b.rainpole.local:5480`**. Select **Services** and verify that all Services are reporting a status of `REGISTERED`.

Preparing the vRealize Automation Environment	■ Make the vRealize Automation environment unavailable to end users and any automated integrations during the upgrade maintenance window. ■ Verify that the vRealize Automation environment has been quiesced for all activities, including but not limited to, users ordering new virtual machines and third-party integrations that may automate the ordering of new virtual machines. Without quiescing the environment, rollback operations may be disruptive, generating orphaned objects after snapshots have been created. Remediating such situation might require extending the maintenance window. ■ Verify that you have access to all databases and load balancers that are impacted by, or participate in, the vRealize Automation upgrade.

Procedure

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

Before you upgrade the vRealize Automation virtual appliances and the vRealize Automation IaaS nodes, direct all traffic to the primary node and disable the health check on the NSX load balancer for the management applications.

2 Take Snapshots of the vRealize Automation Virtual Machines

Before you perform the upgrade of vRealize Automation, take a snapshot for each virtual machine in the environment. If you must perform a rollback of vRealize Automation to the previous state, these snapshots accelerate the rollback operation.

3 Unregister vRealize Automation from vRealize Business

Before you perform the upgrade of vRealize Automation, unregister the vRealize Automation default tenant from vRealize Business.

4 Configure the Authentication Provider of vRealize Orchestrator with the Default Tenant

Before you perform the upgrade of vRealize Automation, you reconfigure the vRealize Orchestrator authentication provider to the default tenant and admin group to ensure the vRealize Orchestrator services come online post-upgrade.

5 Upgrade the vRealize Automation Appliances and IaaS Components

When you upgrade the vRealize Automation in the cloud management layer, start the procedure from the primary vRealize Automation virtual appliance using the upgrade `.iso` file. The upgrade process supports automatic upgrade of both the vRealize Automation virtual appliance and the vRealize Automation IaaS components.

6 Restore the Configuration of the vRealize Orchestrator Authentication Provider

7 Register vRealize Business Back with vRealize Automation

After you complete the upgrade of vRealize Automation, re-register the vRealize Automation default tenant vsphere.local with vRealize Business.

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

After you complete upgrade of vRealize Automation, restore traffic distribution and health checks on the NSX load balancer, across the primary and secondary components of vRealize Automation platform.

9 Delete the Snapshots of the vRealize Automation Virtual Machines

After you complete the upgrade of vRealize Automation and verify operations and functionality, delete the virtual machine snapshots.

What to do next

- Verify that vRealize Automation is operational after the upgrade.

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

Before you upgrade the vRealize Automation virtual appliances and the vRealize Automation IaaS nodes, direct all traffic to the primary node and disable the health check on the NSX load balancer for the management applications.

The configuration change disables the second pool member for the five vRealize Automation VIPs. During an upgrade, the services inside the second node might not be upgraded or initialized because of installation or power cycle operations. If the load balancer passes a request to the second node, the request will fail. If the second pool member remains enabled, you might experience failures during vRealize Automation upgrade, and service initialization or registration failures during a vRealize Automation appliance power cycle operations.

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

Load Balancer Pools on sfo01m01lb01	Secondary Member to Disable
vra-svr-443	According to which node is labeled as REPLICA: ■ vra01svr01a ■ vra01svr01b
vra-svr-8444	According to which node is labeled as REPLICA ■ vra01svr01a ■ vra01svr01b
vra-iws-443	vra01iws01b
vra-ims-443	vra01ims01b
vra-vro-8283	According to which node is labeled as REPLICA: ■ vra01svr01a ■ vra01svr01b

Procedure

1 Log in to the first vRealize Automation appliance.

   a Open a Web browser and go to **`https://vra01svr01a.rainpole.local:5480`**

   b Log in using the following credentials.

Settings	Value
User name	root
Password	*vra_appA_root_password*

2 On **vRA Settings** tab, click the **Database** tab and check which node has the REPLICA label. The REPLICA label indicates which vRealize Appliance is the secondary.

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

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

   b Log in using the following credentials.

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

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

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

6 From the **NSX Manager** drop-down menu, select **172.16.11.65** and double-click the **sfo01m01lb01** NSX Edge to open its network settings.

7 On the **Manage** tab, click the **Load Balancer** tab and click **Pools**.

8 Select the **vra-svr-443** pool that contains the vRealize Automation appliances and click **Edit**.

9 In the **Edit Pool** dialog box, select the secondary node, click **Edit**, select **Disable** from the **State** drop-down menu, and click **OK**.

10 In the **Edit Pool** dialog box, select **NONE** from the **Monitors** drop-down menu and click **OK**.

11 Repeat the procedure on the remaining load balancer pools.

12 To verify that the load balancer redirects the traffic to the primary node of the vRealize Automation virtual appliance, open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac`** to verify that the login page of the vRealize Automation administration portal appears.

Take Snapshots of the vRealize Automation Virtual Machines

Before you perform the upgrade of vRealize Automation, take a snapshot for each virtual machine in the environment. If you must perform a rollback of vRealize Automation to the previous state, these snapshots accelerate the rollback operation.

Table 2-6. vRealize Automation Virtual Machines

Region	Folder	Role	Virtual Machine Name
Regoin A	sfo01-m01fd-vra	vRealize Automation Appliances	vra01svr01a
	sfo01-m01fd-vra		vra01svr01b
	sfo01-m01fd-vra	vRealize Automation IaaS Web Servers	vra01iws01a
	sfo01-m01fd-vra		vra01iws01b
	sfo01-m01fd-vra	vRealize Automation IaaS Model Manager Servers	vra01ims01a
	sfo01-m01fd-vra		vra01ims01b
	sfo01-m01fd-vra	vRealize Automation IaaS DEM Workers	vra01dem01a
	sfo01-m01fd-vra		vra01dem01b
	sfo01-m01fd-vraias	vRealize Automation IaaS Proxy Agents	sfo01ias01a
	sfo01-m01fd-vraias		sfo01ias01b
Region B	lax01-m01fd-vraias	vRealize Automation IaaS Proxy Agents	lax01ias01a
	lax01-m01fd-vraias		lax01ias01b

Note If you are using the designated Microsoft SQL Server vra01mssql01.rainpole.local covered within the VMware Validated Design include this in the snapshot take for vRealize Automation. If you are using a shared instance of Microsoft SQL Server to host the vRealize Automation IaaS database along with other databases, ensure that you have a recent backup per the vRealize Automation Upgrade Prerequisites.

Procedure

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

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

   b Log in using the following credentials.

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

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

3 Shut down the vRealize Automation virtual machines in the environment according to Shutdown Order of the Management Virtual Machines.

   a In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra** tree .

   b Right-click the **vra01dem01a** virtual machine, select **Power > Shut Down Guest OS** and click **Yes** in the confirmation dialog box that appears.

   c Repeat the steps on the remaning vRealize Automation virtual machines in the environment.

4 Take a snapshot of the vRealize Automation virtual machines in the environment.

   a In the **Navigator**, right-click the **vra01svr01a.rainpole.local** 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	VMware Validated Design Cloud Management Layer Upgrade
Description	-
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

   c Repeat these steps for the remaining vRealize Automation virtual machines in the environment.

5 Power on the vRealize Automation virtual machines in the environment according to Startup Order of the Management Virtual Machines.

   a In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra** tree .

   b Right-click the **vra01mssql01** virtual machine, select **Power > Power On** and click **Yes** in the confirmation dialog box that appears.

   c Repeat the steps on the remaining vRealize Automation virtual machines in the environment.

Unregister vRealize Automation from vRealize Business

Before you perform the upgrade of vRealize Automation, unregister the vRealize Automation default tenant from vRealize Business.

Procedure

1 Log in to the vRealize Business Server appliance management console.

   a Open a Web browser and go to **`https://vrb01svr01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

2 Unregister vRealize Business from the default tenant, vsphere.local, in vRealize Automation.

   a On the **Registration** tab, click the **vRA** tab.

   b Enter the following values and click **Unregister**.

Setting	Value
Hostname	vra01svr01.rainpole.local
SSO Default Tenant	vsphere.local
SSO Admin User	**`administrator`**
SSO Admin Password	***`vra_administrator_password`***

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

Configure the Authentication Provider of vRealize Orchestrator with the Default Tenant

Before you perform the upgrade of vRealize Automation, you reconfigure the vRealize Orchestrator authentication provider to the default tenant and admin group to ensure the vRealize Orchestrator services come online post-upgrade.

Procedure

1 Log in to vRealize Orchestrator Control Center

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local:8283/vco-controlcenter/`**.

   b Log in using the following credentials

Setting	Value
User Name	vra-admin-rainpole@rainpole.local
Password	*vra-admin-rainpole_password*

2 Under the **Manage** group of settings, click **Configure Authentication Provider**.

3 On the **Configure Autenthication Provider** page, click **Change** next to **Default tenant**, enter **`vsphere.local`**, and click **Apply**.

4 Click **Change** next to **Admin group**, enter **`vsphere.local`**, select the `vcoadmins` group, and click **Apply**.

5 Click **Save Changes**.

Upgrade the vRealize Automation Appliances and IaaS Components

When you upgrade the vRealize Automation in the cloud management layer, start the procedure from the primary vRealize Automation virtual appliance using the upgrade `.iso` file. The upgrade process supports automatic upgrade of both the vRealize Automation virtual appliance and the vRealize Automation IaaS components.

Table 2-7. vRealize Automation Nodes in the SDDC

Region	Role	Fully Qualified Domain Name
Region A	vRealize Automation Appliances	vra01svr01a.rainpole.local
		vra01svr01b.rainpole.local
	vRealize Automation IaaS Web Servers	vra01iws01a.rainpole.local
		vra01iws01b.rainpole.local
	vRealize Automation IaaS Model Manager Servers	vra01ims01a.rainpole.local
		vra01ims01b.rainpole.local

Table 2-7. vRealize Automation Nodes in the SDDC (Continued)

Region	Role	Fully Qualified Domain Name
	vRealize Automation IaaS DEM Workers	vra01dem01a.rainpole.local
		vra01dem01b.rainpole.local
	vRealize Automation Iaas Proxy Agents	sfo01ias01a.sfo01.rainpole.local
		sfo01ias01b.sfo01.rainpole.local
Region B	vRealize Automation IaaS Proxy Agents	lax01ias01a.lax01.rainpole.local
		lax01ias01b.lax01.rainpole.local

Prerequisites

- Verify that current backups of the vRealize Automation virtual appliances and the vRealize Automation IaaS virtual machines exist.
- Verify that a current backup of the external vRealize Automation database exists. The default name of the Microsoft SQL Server database is `VRADB01`.
- Verify that the primary IaaS Web Server virtual machine vra01iws01a satisfies the following requirements:
  - Java SE Runtime Environment 8 64-bit update 161 or later is installed.
  - `JAVA_HOME` environment variable is set to the Java directory path.
- Mount the upgrade `.iso`file, `VMware-vR-Appliance-7.4.0.`*`xxx-build_number`*`-updaterepo.iso`, on the primary vRealize Automation virtual appliance vra01iws01a.

Procedure

1 Log in to the first vRealize Automation appliance.

   a Open a Web browser and go to **`https://vra01svr01a.rainpole.local:5480`**

   b Log in using the following credentials.

Settings	Value
User name	root
Password	*vra_appA_root_password*

2 Click the **Update** tab and click the **Settings** button.

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

4 Click the **Status** tab and click **Check Updates** to load the update from the upgrade `.iso` file.

5 Verify that the update listed in **Available Updates** matches the version in this VMware Validated Design, click **Install Updates** and click **OK** in the **Install Updates** dialog box.

Note You can also follow the upgrade process within the logs on the vRealize Automation virtual appliance.

- `/opt/vmware/var/log/vami/vami.log` - Logs the initial unpacking and staging of the upgrade bundle to the primary vRealize Automation virtual appliance.

Once completed, additional logging is available in the `updatecli.log`

- `/opt/vmware/var/log/vami/updatecli.log` - Logs the additional vRealize Automation upgrade processes, such as, the upgrade script execution.

6 On the **Status** page, monitor the **Update Status**.

After the upgrade completes, the `System reboot is required to complete the update` message appears on the **Status** page.

7 On the **System** tab, click **Reboot** and click **Reboot** in the confirmation dialog box to restart the primary vRealize Automation appliance.

The secondary vRealize Automation virtual appliance restarts automatically.

8 Log in to the first vRealize Automation appliance.

a Open a Web browser and go to **`https://vra01svr01a.rainpole.local:5480`**

b Log in using the following credentials.

Settings	Value
User name	root
Password	*vra_appA_root_password*

9 On the **Update** tab, click the **Status** button, and monitor the vRealize Automation IaaS upgrade for each Windows Server-based component.

10 After the upgrade completes for the vRealize Automation IaaS components, use the **vRA Settings > Cluster** tab to verify that each vRealize Automation IaaS nodes and components are version 7.4.0.*xxxxx*.

11 On the **vRA Settings > Licensing** tab, verify that the vRealize Automation product license information remains and a valid license is still available.

12 If the upgrade process has removed the license, re-enter the license key.

a Enter the license key in the **New License Key** text box and click **Submit Key**.

b Verify that the license has been applied.

c Repeat this step on the vra01svr01b.rainpole.local virtual appliance.

Restore the Configuration of the vRealize Orchestrator Authentication Provider

After you perform the upgrade of vRealize Automation, you configure the default tenant and admin group of the vRealize Orchestrator authentication provider with the configuration before the upgrade, that is, with the Rainpole tenant.

Procedure

1 Log in to the vRealize Automation appliance by using Secure Shell (SSH) client to configure the embedded vRealize Orchestrator.

   a Open an SSH connection to **`vra01svr01a.rainpole.local`**

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vra_appA_root_password*

2 Verify that the vRealize Orchestrator user interface service is running.

   a Run the following command to verify that the service is set to automatically start.

```
chkconfig vco-configurator
```

   b If the service reports `Off`, run the following command to enable an automatic restart of the Orchestrator user interface service upon subsequent reboots of the vRealize Automation appliance.

```
chkconfig vco-configurator on
```

   c Verify the status of Orchestrator User Interface by running the following command .

```
service vco-configurator status
```

   d Repeat the procedure to configure vRealize Orchestrator for the other host.

3 Log in to vRealize Orchestrator Control Center to change the default tenant and admin group for the authentication provider.

   a Open an SSH connection to vra01svr01a.rainpole.local using the following credentials.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local:8283/vco-controlcenter/`** .

   b Log in using the following credentials

Setting	Value
User Name	root
Password	*vra_appA_root_password*

4 Associate the default tenant and admin group for the vRealize Orchestrator authentication provider with the Rainpole tenant.

   a Under the **Manage** group of settings, select **Configure Authentication Provider**

   b On the **Configure Autenthication Provider** page, click **Change** next to **Default tenant**, enter **`rainpole`**, and click **Apply**.

   c Click **Change** next to **Admin group**, enter **`ug-vRO`**, and click **Search**.

   d From the drop-down menu, select the **rainpole.local\ug-vROAdmins** group and click **Apply**.

   e Click **Save Changes**.

Register vRealize Business Back with vRealize Automation

After you complete the upgrade of vRealize Automation, re-register the vRealize Automation default tenant vsphere.local with vRealize Business.

Procedure

1 Log in to the vRealize Business Server appliance management console.

   a Open a Web browser and go to **`https://vrb01svr01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

2 Click **Registration > vRA**, enter the following credentials to register with the vRealize Automation server, and click **Register**.

Setting	Value
Hostname	vra01svr01.rainpole.local
SSO Default Tenant	vsphere.local

Setting	Value
SSO Admin User	administrator
SSO Admin Password	*vra_administrator_password*
Accept "vRealize Automation" certificate	Selected

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

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

After you complete upgrade of vRealize Automation, restore traffic distribution and health checks on the NSX load balancer, across the primary and secondary components of vRealize Automation platform.

On the NSX load balancer, you re-enable the secondary vRealize Automation nodes and select the monitor for the associated traffic in the pools.

Table 2-8. vRealize Automation Pool Members to Re-Enable on the NSX Load Balancer

Server Pool on the sfo01m01lb01 Load Balancer	Secondary Member to Re-Enable	Service Monitor to Re-Associate
vra-svr-443	According to which one is the primary node: ■ vra01svr01a ■ vra01svr01b	vra-svr-443-monitor
vra-svr-8444	According to which one is the primary node: ■ vra01svr01a ■ vra01svr01b	vra-svr-443-monitor
vra-iws-443	vra01iws01b	vra-iws-443-monitor
vra-vro-8283	vra01svr01b	vra-vro-8283-monitor

Procedure

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

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

b Log in using the following credentials.

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

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

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

4 From the **NSX Manager** drop-down menu, select **172.16.11.65** and double-click on the **sfo01m01lb01** NSX Edge to open its network settings.

5 On the **Load Balancer** tab, click **Pools**.

6 Select the **vra-svr-443** pool that is associated with the traffic to the vRealize Automation portal and click **Edit**.

7 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**.

8 In the **Edit Pool** dialog box, select **vra-svr-443-monitor** from the **Monitors** drop-down menu and click **OK**.

9 Repeat the procedure on the remaining load balancer pools.

Delete the Snapshots of the vRealize Automation Virtual Machines

After you complete the upgrade of vRealize Automation and verify operations and functionality, delete the virtual machine snapshots.

Table 2-9. vRealize Automation Virtual Machines

Region	Folder	Role	Virtual Machine Name
Regoin A	sfo01-m01fd-vra	vRealize Automation Appliances	vra01svr01a
	sfo01-m01fd-vra		vra01svr01b
	sfo01-m01fd-vra	vRealize Automation IaaS Web Servers	vra01iws01a
	sfo01-m01fd-vra		vra01iws01b
	sfo01-m01fd-vra	vRealize Automation IaaS Model Manager Servers	vra01ims01a
	sfo01-m01fd-vra		vra01ims01b
	sfo01-m01fd-vra	vRealize Automation IaaS DEM Workers	vra01dem01a
	sfo01-m01fd-vra		vra01dem01b
	sfo01-m01fd-vraias	vRealize Automation IaaS Proxy Agents	sfo01ias01a
	sfo01-m01fd-vraias		sfo01ias01b
Region B	lax01-m01fd-vraias	vRealize Automation IaaS Proxy Agents	lax01ias01a
	lax01-m01fd-vraias		lax01ias01b

Note If you are using the designated Microsoft SQL Server vra01mssql01.rainpole.local covered within the VMware Validated Design clean up the snapshot taken for the vRealize Automation upgrade task.

Procedure

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

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

   b Log in using the following credentials.

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

2 In the **Navigator**, click **VMs and Templates** and navigate to the vra01svr01a virtual machine.

3 Right-click the **vra01svr01a** virtual machine and select **Snapshots > Manage Snapshots**.

4 In the **Snapshot Manager**, click the snapshot that you created before the vRealize Automation upgrade and select **Delete**.

5 Click **Yes** in the confirmation dialog and click **Close** in **Snapshot Manager**.

6 Repeat the procedure for the remaining vRealize Automation virtual machines.

Upgrade vRealize Business Virtual Appliances

After you complete the upgrade of vRealize Automation, upgrade vRealize Business to complete the upgrade of the cloud management layer to VMware Validated Design 4.3.

Table 2-10. vRealize Business Nodes in the SDDC

Region	Role	IP Address	Fully Qualified Domain Name
Region A	vRealize Business Server	192.168.11.66	vrb01svr01.rainpole.local
	vRealize Business Data Collector	192.168.31.54	sfo01vrbc01.sfo01.rainpole.local
Region B	vRealize Business Data Collector	192.168.32.54	lax01vrbc01.lax01.rainpole.local

Prerequisites

- Download the vRealize Business `vRealize-Business-for-Cloud-7.4.0.xxxx-build_number-updaterepo.iso` upgrade file to a shared datastore.

  If you have space on an NFS datastore, upload the upgrade file to the NFS datastore to save space on your vSAN datastore. You can then mount the `.iso` upgrade file to the vRealize Business for Cloud virtual appliances from the vSphere Web Client.

- Verify that current backups of the vRealize Business virtual appliances exist.

Procedure

1 Take Snapshots of the vRealize Business Virtual Machines

Before you perform the upgrade of vRealize Business, take a snapshot for each virtual machine in the environment. If you must perform a rollback of vRealize Business to the previous state, these snapshots accelerate the rollback operation.

2 Upgrade the vRealize Business Server Virtual Appliance

When you upgrade vRealize Business in the cloud management layer, start the procedure from the vRealize Business server virtual appliance using the upgrade `.iso` file.

3 Upgrade the vRealize Business Data Collector Virtual Appliances

After you complete the upgrade of the vRealize Business for Cloud server virtual appliance, upgrade the region-specific vRealize Business data collector virtual appliances by using the appliance management interface.

4 Delete the Snapshots of the vRealize Business Virtual Machines

After you complete the upgrade of vRealize Business and verify operations and functionality, delete the virtual machine snapshots.

What to do next

- Verify that vRealize Business for Cloud functions are operational.

Take Snapshots of the vRealize Business Virtual Machines

Before you perform the upgrade of vRealize Business, take a snapshot for each virtual machine in the environment. If you must perform a rollback of vRealize Business to the previous state, these snapshots accelerate the rollback operation.

Table 2-11. vRealize Business Virtual Machines

Region	Folder	Role	Virtual Machine Name
Region A	sfo01-m01fd-vra	vRealize Business for Cloud Server	vrb01svr01
	sfo01-m01fd-vraias	vRealize Business for Cloud Data Collector	sfo01vrbc01
Region B	lax01-m01fd-vraias	vRealize Business for Cloud Data Collector	lax01vrbc01

Procedure

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

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

b Log in using the following credentials.

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

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

3 Shut down the vRealize Business nodes in the environment according to Shutdown Order of the Management Virtual Machines.

   a In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra** tree .

   b Right-click the **sfo01vrbc01** virtual machine, select **Power > Shut Down Guest OS** and click **Yes** in the confirmation dialog box that appears.

   c Repeat the steps on the remaining vRealize Business virtual machines in the environment.

4 Take a snapshot of the vRealize Business virtual machines in the environment.

   a In the **Navigator**, click **VMs and Templates** and expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra** tree.

   b Right-click the **vrb01svr01** 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	VMware Validated Design 4.3 Cloud Management Layer Upgrade
Description	-
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

   d Repeat these steps for the remaining virtual machines in the environment.

5 Power on the vRealize Business virtual machines in the environment according to Startup Order of the Management Virtual Machines.

   a In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra** tree .

   b Right-click the **vrb01svr01** virtual machine, select **Power > Power On** and click **Yes** in the confirmation dialog box that appears.

   c Repeat the steps on the remaining vRealize Business virtual machines in the environment.

Upgrade the vRealize Business Server Virtual Appliance

When you upgrade vRealize Business in the cloud management layer, start the procedure from the vRealize Business server virtual appliance using the upgrade `.iso` file.

Prerequisites

- Mount the upgrade `iso` file, `vRealize-Business-for-Cloud-7.4.x.xxx-`*`build_number`*`-updaterepo.iso`, to the vRealize Business server virtual appliance vrb01svr01.

Procedure

1 Log in to the vRealize Business Server appliance management console.

   a Open a Web browser and go to **`https://vrb01svr01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

2 Unregister vRealize Business from the default tenant in vRealize Automation vsphere.local.

   a On the **Registration** tab, click the **vRA** tab.

   b Enter the following values and click **Unregister**.

Setting	Value
Hostname	vra01svr01.rainpole.local
SSO Default Tenant	vsphere.local
SSO Admin User	administrator
SSO Admin Password	*vra_administrator_password*

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

3 Start the upgrade of the vRealize Business server virtual 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 **Status** and click **Check Updates** to load the update from the upgrade `.iso` file.

   d Verify that the update listed in **Available Updates** matches the version in this VMware Validated Design and click **Install Updates**.

4 Log in to the vRealize Business Server appliance management console.

   a Open a Web browser and go to **`https://vrb01svr01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

5 Re-register vRealize Business with the default tenant in vRealize Automation, vsphere.local.

a Click **Registration > vRA** and enter the following credentials to register with the vRealize Automation server.

Setting	Value
Hostname	vra01svr01.rainpole.local
SSO Default Tenant	vsphere.local
SSO Admin User	administrator
SSO Admin Password	*vra_administrator_password*
Accept "vRealize Automation" certificate	Selected

b Click **Register**.

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

Upgrade the vRealize Business Data Collector Virtual Appliances

After you complete the upgrade of the vRealize Business for Cloud server virtual appliance, upgrade the region-specific vRealize Business data collector virtual appliances by using the appliance management interface.

Table 2-12. vRealize Business Data Collectors in the SDDC

Region	URL
Region A	**`https://sfo01vrbc01.sfo01.rainpole.local:5480`**
Region B	**`https://lax01vrbc01.lax01.rainpole.local:5480`**

You can update the two vRealize Business data collectors in Region A and Region B sequentially or in parallel.

Prerequisites

- Mount the upgrade`.iso` file, `vRealize-Business-for-Cloud-7.4.x.`*`xxx-build_number`*`-updaterepo.iso`, on both the sfo01vrbc01 and lax01vrbc01 virtual appliances.

Procedure

1 Log in to the appliance management interface of the vRealize Business for Cloud data collector virtual appliance.

a Open a browser and go **`https://sfo01vrbc01.sfo01.rainpole.local:5480`**.

b Log in using the following credentials.

Setting	Value
User Name	root
Password	*vrb_collector_root_password*

2 Click the **Update** tab and click **Settings**.

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

4 Click **Status** and click **Check Updates** to load the update from the upgrade `.iso` file.

5 Verify that the update listed in **Available Updates** matches the version in this VMware Validated Design and click **Install Updates**.

   After a successful upgrade, the appliance automatically restarts.

6 Repeat this step on the other vRealize Business data collector virtual appliance.

What to do next

Post-upgrade, verify that vRealize Business data collectors are operational.

Delete the Snapshots of the vRealize Business Virtual Machines

After you complete the upgrade of vRealize Business and verify operations and functionality, delete the virtual machine snapshots.

Table 2-13. vRealize Business Virtual Machines

Region	Folder	Role	Virtual Machine Name
Region A	sfo01-m01fd-vra	vRealize Business for Cloud Server	vrb01svr01
	sfo01-m01fd-vraias	vRealize Business for Cloud Data Collector	sfo01vrbc01
Region B	lax01-m01fd-vraias	vRealize Business for Cloud Data Collector	lax01vrbc01

Procedure

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

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

   b Log in using the following credentials.

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

2 In the **Navigator**, click **VMs and Templates** and expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra** tree.

3 Right-click the **vrb01svr01** virtual machine and select **Manage Snapshots**.

4 In the **Snapshot Manager**, click the snapshot that you created before the vRealize Business upgrade and select **Delete**.

5 Click **Yes** in the confirmation dialog box and click **Close** in **Snapshot Manager**.

6 Repeat the procedure for the other vRealize Business data collector virtual machines.

Post-Upgrade Configuration of the Cloud Management Layer

After you complete the upgrade of the Cloud Management Layer, perform the post-upgrade configuration changes to the environment according to the design objectives and deployment guidance to ensure your environment remains aligned to this VMware Validated Design.

Procedure

1 Increase the Memory for the vRealize Automation IaaS Server Virtual Machines

After you complete the upgrade of Cloud Management Layer, increase the memory allocated to the vRealize Automation IaaS Windows Server-based virtual machines to ensure alignment with the VMware Validated Design.

2 Re-Configure the vRealize Log Insight Agent on vRealize Business

After you upgrade vRealize Business, deploy a new version of the vRealize Log Insight agent on and update the agent configuration to the appliances. You must reconfigure the vRealize Log Insight agent on each node to continue log forwarding and stay aligned with VMware Validated Design.

3 Update the Content Pack for vRealize Automation

In this version of VMware Validated Design, install a new vRealize Log Insight content pack for vRealize Automation so that the dashboards in vRealize Log Insight user interface provide details according to the architecture changes and capabilities of the vRealize Automation version in this design. Before you install the content pack, you must clean up the setup for the earlier pack to avoid conflicts or duplicate log information in vRealize Log Insight.

Increase the Memory for the vRealize Automation IaaS Server Virtual Machines

After you complete the upgrade of Cloud Management Layer, increase the memory allocated to the vRealize Automation IaaS Windows Server-based virtual machines to ensure alignment with the VMware Validated Design.

Increase the Memory for the vRealize Automation IaaS Server Virtual Machines in Region A

After you complete the upgrade of Cloud Management Layer, increase the memory on the vRealize Automation IaaS virtual machines to align with the updated architecture and design.

Repeat this procedure using the order and virtual machines information in the following table to increase the memory.

Order	Virtual Machine	vCenter Folder	Memory Size (MB)
1	vra01iws01b	sfo01-m01fd-vra	8192 MB
2	vra01ims01b	sfo01-m01fd-vra	8192 MB
3	vra01dem01b	sfo01-m01fd-vra	8192 MB
4	sfo01ias01b	sfo01-m01fd-vraias	8192 MB
5	vra01iws01a	sfo01-m01fd-vra	8192 MB
6	vra01ims01a	sfo01-m01fd-vra	8192 MB
7	vra01dem01a	sfo01-m01fd-vra	8192 MB
8	sfo01ias01a	sfo01-m01fd-vraias	8192 MB

Procedure

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

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

   b Log in using the following credentials.

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

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

3 Shut down the vRealize Automation virtual machine according to the predefined order.

   a In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra** tree .

   b Right-click the vra01iws01b virtual machine, select **Power > Shut Down Guest OS** and click **Yes** in the confirmation dialog box that appears.

   c Verify that the vra01iws01b virtual machine shuts down gracefully.

4 Increase the virtual memory of the vRealize Automation virtual machine.

   a Right-click the vra01iws01b virtual machine and select **Edit Settings**.

   b In the **Edit Settings** dialog box, click the **Virtual Hardware** tab and set the **Memory** settings to **`8192 MB`**.

   c Click **OK**.

5 Right-click the vra01iws01b virtual machine and select **Power > Power on**.

6 From the virtual machine console, verify that vra01iws01b boots, and uses the configuration settings specified.

7 Wait several minutes for the operating system and services to start on the virtual machine.

8 Log in to the vRealize Automation appliance management console and verify the status each vRealize Automation IaaS node.

   a Open a Web browser and go to **`https://vra01svr01a.rainpole.local:5480`**

   b Log in using the following credentials.

Settings	Value
User name	root
Password	*vra_appA_root_password*

   c Click **vRA Settings > Cluster** and verify that **vra01iws01a** has a Last Connected status of less than 30 seconds and a Time Offset status of less than 1 second.

9 Repeat this procedure to increase the memory on the remaining vRealize Automation IaaS virtual machines in Region A.

Increase the Memory for the vRealize Automation IaaS Server Virtual Machines in Region B

After you upgrade the cloud management layer, increase the memory on the vRealize Automation IaaS virtual machines to align with this version of VMware Validated Design.

Repeat this procedure using the following order and virtual machines information to increase the memory.

Order	Virtual Machine	vCenter Folder	Memory Size (MB)
1	lax01ias01b	lax01-m01fd-vraias	8192 MB
2	lax01ias01a	lax01-m01fd-vraias	8192 MB

Procedure

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

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

   b Log in using the following credentials.

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

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

3 Shut down the vRealize Automation virtual machines in the environment according to the defined order.

   a In the **Navigator**, expand the **lax01m01vc01.lax01.rainpole.local > lax01-m01dc > lax01-m01fd-vraias** tree .

   b Right-click the vra01iws01b virtual machine, select **Power > Shut Down Guest OS** and click **Yes** in the confirmation dialog box that appears.

   c Verify that the vra01iws01b virtual machine shuts down gracefully.

4 Increase the memory of the IaaS virtual machine.

   a Right-click the vra01iws01b virtual machine and select **Edit Settings**.

   b In the **Edit Settings** dialog box, click the **Virtual Hardware** tab and set **Memory** to **`8192 MB`**.

   c Click **OK**.

5 Right-click the vra01iws01b virtual machine and select **Power > Power on**.

6 From the vVirtual machine console, verify that vra01iws01a boots, and uses the configuration settings specified.

7 Wait several minutes for the operating system and services to start on the virtual machine.

8 Log in to the vRealize Automation appliance management console and verify the status each vRealize Automation IaaS node.

   a Open a Web browser and go to **`https://vra01svr01a.rainpole.local:5480`**

   b Log in using the following credentials.

Settings	Value
User name	root
Password	*vra_appA_root_password*

   c Click **vRA Settings > Cluster** and verify that **vra01iws01a** has a Last Connected status of less than 30 seconds and a Time Offset status of less than 1 second.

9 Repeat this procedure to increase the memory on the remaining vRealize Automation IaaS virtual machines in Region B.

Re-Configure the vRealize Log Insight Agent on vRealize Business

After you upgrade vRealize Business, deploy a new version of the vRealize Log Insight agent on and update the agent configuration to the appliances. You must reconfigure the vRealize Log Insight agent on each node to continue log forwarding and stay aligned with VMware Validated Design.

Configure the vRealize Log Insight Linux Agents on vRealize Business in Region A

vRealize Log Insight Agent comes pre-installed on the vRealize Business virtual appliances.

After you upgrade vRealize Business, reapply the configuration for connecting to vRealize Log Insight to the server and data collector in Region A.

Procedure

1 Enable Secure Shell (SSH) on the vRealize Business appliances.

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

vRealize Business Node	Virtual Appliance Management Interface URL
vRealize Business Server Appliance	https://vrb01svr01.rainpole.local:5480
vRealzie Business Data Collector	https://sfo01vrbc01.sfo01.rainpole.local:5480

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_root_password*

The appliance management interface of the appliance opens.

c Click the **Administration** tab and click **Administration**.

d Under the **Actions** section, verify that the **SSH service status** is `Enabled`.

e Repeat the step for the second vRealize Business appliance.

2 Configure the vRealize Log Insight agent in the vRealize Business appliance.

a Open an SSH connection to the vRealize Business appliance using the following settings.

Setting	Value
Hostname	■ vrb01svr01.rainpole.local ■ sfo01vrbc01.sfo01.rainpole.local
User name	root
Password	*vrb_root_password*

b Edit the `liagent.ini` file in a text editor.

For example, run the following command:

```
vi /var/lib/loginsight-agent/liagent.ini
```

c Modify the `[server]` section to look like the following.

```
[server]
hostname= sfo01vrli01.sfo01.rainpole.local
proto = cfapi
port = 9000
ssl = no
```

d Replace all instances of the `FQDN_localhost_need_update` parameter located after `agent_name` with **`vrb01svr01.rainpole.local`**, by using the following commands in the `vi` editor.

vRealize Business Node	vi command
vRealize Business Server Appliance	`:%s/FQDN_localhost_need_update/vrb01svr01.rainpole.local/g`
vRealize Business Data Collector	`:%s/FQDN_localhost_need_update/sfo01vrbc01.sfo01.rainpole.local/g`

e Press Escape and type `:wq!` to save the file.

f Start the Log Insight agent.

```
/etc/init.d/liagentd start
```

g Verify that the Log Insight agent is running.

```
/etc/init.d/liagentd status
```

h Turn on autorun by default for the Log Insight agent.

```
chkconfig liagentd on
```

i Repeat this step to configure the vRealize Business Data Collector at sfo01vrbc01.sfo01.rainpole.local.

Configure the vRealize Log Insight Linux Agent on vRealize Business in Region B

vRealize Log Insight Agent comes pre-installed on the vRealize Business virtual appliances.

After you upgrade vRealize Business, reapply the configuration for connecting to vRealize Log Insight to the data collector in Region A.

Procedure

1 Enable Secure Shell (SSH) on the vRealize Business data collector appliance.

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

vRealize Business node	Virtual Appliance Management Interface URL
vRealzie Business Data Collector	`https://lax01vrbc01.lax01.rainpole.local:5480`

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_root_password*

The appliance management interface of the appliance opens.

c Click the **Administration** tab and click **Administration**.

d Under the **Actions** section, click **Toggle SSH setting**.

e Verify that the **SSH service status** reports **`Enabled`**.

2 Configure the Log Insight agent on the vRealize Business appliance.

a Open an SSH connection to the vRealize Business appliance using the following settings.

Setting	Value
Hostname	lax01vrbc01.lax01.rainpole.local
User name	root
Password	*vrb_root_password*

b Edit the `liagent.ini` file in a text editor.

For example, enter

```
vi /var/lib/loginsight-agent/liagent.ini
```

c Add the following information under `[server]` section.

```
[server]
hostname=lax01vrli01.lax01.rainpole.local
proto = cfapi
port = 9000
ssl = no
```

d Replace all instances of `FQDN_localhost_need_update` parameter located after `agent_name` with **`lax01vrbc01.lax01.rainpole.local`**, by using the following commands in the `vi` editor.

vRealize Business Node	vi command
vRealize Business Data Collector	`:%s/FQDN_localhost_need_update/lax01vrbc01.lax01.rainpole.local/g`

e Press Esc and enter `:wq!` to save the file.

f Start the Log Insight agent.

```
/etc/init.d/liagentd start
```

g Verify that the Log Insight agent is running.

```
/etc/init.d/liagentd status
```

h Turn on auto-run by default for the Log Insight agent.

```
chkconfig liagentd on
```

Update the Content Pack for vRealize Automation

In this version of VMware Validated Design, install a new vRealize Log Insight content pack for vRealize Automation so that the dashboards in vRealize Log Insight user interface provide details according to the architecture changes and capabilities of the vRealize Automation version in this design. Before you install the content pack, you must clean up the setup for the earlier pack to avoid conflicts or duplicate log information in vRealize Log Insight.

Clean up the old agent group and content pack from vRealize Log Insight. Then proceed with installing the latest content pack and apply the latest vRealize Log Insight agent configuration on the vRealize Automation cluster.

Clean Up the Old Agent Group and Content Pack for vRealize Automation

Clean up the old agent group and content packs in vRealize Log Insight in preparation to apply the new vRealize Automation solution.

Procedure

1 Log in to the vRealize Log Insight user interface.

a Open a Web browser and go to **`https://sfo01vrli01.sfo01.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 From the drop-down menu at the top, point to **vRA - Appliance Agent Group** from the **Active Groups** section and click the delete icon.

5 In the **Delete Agent Group** dialog box, click **Delete** to confirm.

6 Repeat this procedure on **vRA - Windows Agent Group**.

7 In the vRealize Log Insight user interface, click the configuration drop-down menu icon and select **Content Packs**.

8 In the **Installed Content Packs** area on the left, click **VMware - vRA 7**.

9 In the central pane, click the gear icon, and from the drop-down menu, select **Uninstall**.

10 In the **Uninstall Content Pack** dialog box, click **Uninstall**.

11 After the uninstallation is complete, repeat this operation on vRealize Log Insight in Region B, lax01vrli01.lax01.rainpole.local.

Install the Latest vRealize Log Insight Content Packs for the Cloud Management Platform in Region A and Region B

After cleaning up the old vRealize Automation 7 content pack, install the new vRealize Automation 7.3+ content pack to support the later versions of vRealize Automation and to stay in alignment with the VMware Validated Design.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://sfo01vrli01.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 In the **Content Pack Marketplace** area on the left, click **Marketplace**.

4 In the list of content packs, locate the **VMware - vRA 7.3** content pack and click its icon.

5 In the **Install Content Pack** dialog box, select the **Licensing Agreement** and click **Install**.

6 After the installation is complete, repeat this operation on vRealize Log Insight in Region B, lax01vrli01.lax01.rainpole.local.

After the installation, the **VMware - vRA 7.3** content pack appears under the **Installed Content Pack** area on the left.

Configure vRealize Log Insight Linux Agents in the vRealize Automation Appliances in Region A

Log in to the VAMI console interface of the primary vRealize Automation appliance and configure the Log Insight agent. This setting propagates to the other vRealize Automation appliances in the cluster.

Agent configuration for the vRealize Automation appliances includes the following tasks:

- In the management interface of the vRealize Automation appliances, enable log forwarding to vRealize Log Insight.
- Create an agent group for configuring log forwarding from the vRealize Automation modules on the appliances.
- Create an agent group for configuring log forwarding from the operating system of the appliances.

Procedure

1. Log in to the vRealize Log Insight user interface.
   a. Open a Web browser and go to **`https://sfo01vrli01.sfo01.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. Create the agent group for vRealize Automation appliances on vRealize Log Insight.
   a. From the drop-down menu on the top, select **vRealize Automation 7 - Linux** from the **Available Templates** section.
   b. Click **Copy Template** at the bottom of the page.
   c. In the **Copy Agent Group** dialog box, enter **`vRA – Appliance Agent Group`** in the name text box and click **Copy**.
   d. In the agent filter text boxes, enter the following values pressing Enter after each host name.

Filter	Operator	Values
Hostname	Matches	■ vra01svr01a.rainpole.local ■ vra01svr01b.rainpole.local ■ vra01svr01c.rainpole.local

e Click **Refresh Data** and verify that all the hosts in the filter appear in the **Agents** list.

f Click **Save New Group** at the bottom of the page.

5 To verify the configuration, click the **Dashboards** tab, under the **VMware - vRA 7.3** category click **General - Overview**.

The dashboard shows log data from the components of the vRealize Automation Appliances.

Create Log Insight Agent Groups for vRealize Automation Windows Agents in Region A

Create agent groups for the vRealize Automation IaaS components and for Microsoft SQL Server. By using the agent groups, you can configure Log Insight Windows Agents centrally from the vRealize Log Insight user interface.

Procedure

1 Log in to the vRealize Log Insight user interface.

a Open a Web browser and go to **`https://sfo01vrli01.sfo01.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 Create an agent group for the IaaS components of vRealize Automation.

a From the drop-down menu at the top, select **vRealize Automation 7 - Windows** from the **Available Templates** section.

b Click **Copy Template**.

c In the **Copy Agent Group** dialog box, enter **`vRA – Windows Agent Group`** in the name text box and click **Copy**.

d In the agent filter text boxes, use the following selections.

Press Enter to separate the host name values.

Filter	Operator	Values
Hostname	Matches	■ vra01iws01a.rainpole.local ■ vra01iws01b.rainpole.local ■ vra01ims01a.rainpole.local ■ vra01ims01b.rainpole.local ■ vra01dem01a.rainpole.local ■ vra01dem01b.rainpole.local ■ sfo01ias01a.sfo01.rainpole.local ■ sfo01ias01b.sfo01.rainpole.local

e Under **Agent Configuration**, click **Edit**.

f Under `[filelog|vra-agent-proxy-agent-vsphere]`, locate `directory=C:\Program Files (x86)\VMware\vCAC\Agents\proxy-agent-vsphere\logs\` and change it to `directory=C:\Program Files (x86)\VMware\vCAC\Agents\VSPHERE-AGENT-01\logs` .

g Click **Refresh Data** and verify that all the agents that are listed in the filter appear in the Agents list.

h Click **Save New Group** at the bottom of the page.

Create Log Insight Agent Groups for vRealize Automation Windows Agents in Region B

Create agent groups for the vRealize Automation IaaS components and for Microsoft SQL Server. By using the agent groups, you can configure Log Insight Windows Agents centrally from the vRealize Log Insight user interface.

Procedure

1 Log in to the vRealize Log Insight user interface.

a Open a Web browser and go to **`https://lax01vrli01.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 Create an agent group for the IaaS components of vRealize Automation.

a From the drop-down menu at the top, select **vRealize Automation 7 - Windows** from the **Available Templates** section.

b Click **Copy Template**.

c In the **Copy Agent Group** dialog box, enter **`vRA – Windows Agent Group`** in the name text box and click **Copy**.

d In the agent filter text boxes, use the following selections.

Use Enter to separate the host name values.

Filter	Operator	Values
Hostname	matches	■ lax01ias01a.lax01.rainpole.local ■ lax01ias01b.lax01.rainpole.local

e Under **Agent Configuration**, click **Edit**

f In the `[filelog|vra-agent-proxy-agent-vsphere]` section, locate `directory=C:\Program Files (x86)\VMware\vCAC\Agents\proxy-agent-vsphere\logs\` and change it to **`directory=C:\Program Files (x86)\VMware\vCAC\Agents\VSPHERE-AGENT-51\logs`**

g Click **Refresh** and verify that all the agents that are listed in the filter appear in the Agents list.

h Click **Save New Group** at the bottom of the page.

Expand vRealize Automation to a Three-Node Appliance Architecture Post-Upgrade

Perform the post-upgrade operation of expanding your vRealize Automation cluster to include a third appliance so that your environment remains aligned to this VMware Validated Design.

By adding a node to the vRealize Automation cluster and operating with the synchronous replication mode enabled, the embedded PostgreSQL database can automatically failover between nodes. Failover support improves resilience of the CMP stack to failures and reduces the number of manual failover procedures.

Prerequisites

Table 2-14. System Requirements for the Third vRealize Automation Appliance

Requirement	Value
IP Address	192.168.11.50
FQDN	vra01svr01c.rainpole.local
Required storage	■ Virtual disk provisioning ■ Thin ■ Required storage: 140 GB

Table 2-14. System Requirements for the Third vRealize Automation Appliance (Continued)

Requirement	Value
Application virtual network	xRegion01-VXLAN
Certificate authority	Root Active Directory domain controller as a certificate authority for the environment.

Procedure

1 Update the Distributed Firewall Policies for the Third vRealize Automation Virtual Appliance

Before you add a third vRealize Automation virtual appliance to the environment, update the NSX distributed firewall policies for vRealize Automation.

2 Replace the vRealize Automation Certificate

Before you expand the vRealize Automation cluste with a third vRealize Automation virtual appliance, on the vRealize Automation virtual appliances and vRealize Automation IaaS components, you must install a certificate that includes the host name of the third appliance.

3 Add a Third vRealize Automation Appliance to the Cluster

4 Configure the Environment for the Third vRealize Automation Appliance

After you complete the expansion of vRealize Automation, update the anti-affinity and startup rules in the environment.

5 Configure Log Forwarding for the Third vRealize Automation Appliance in Region A

Log in to the primary management console interface of the newly added vRealize Automation appliance and update the Log Insight Agent configuration.

6 Enable Disaster Recovery for the Third vRealize Automation Appliance

After you complete the expansion of vRealize Automation cluster in Region A for the cloud management layer, update the NSX load balancer with, and enable replication for, the new vRealize Automation virtual appliance to Region B. Next, you update the protection group and recovery plan for the cloud management layer in Site Recovery Manager, as well as, the anti-affinity and VM Group rules. Once completed, the addition of the new vRealize Automation virtual appliance will be be fully integrated into the VMware Validated Design.

Update the Distributed Firewall Policies for the Third vRealize Automation Virtual Appliance

Before you add a third vRealize Automation virtual appliance to the environment, update the NSX distributed firewall policies for vRealize Automation.

Update the distributed firewall policies, which allow communication between vRealize Automation and the SDDC components, to include the third vRealize Automation Virtual Appliance.

Add the Third Appliance to the IP Set for vRealize Automation Appliances in the Distributed Firewall

Update the existing IP Set for the vRealize Automation virtual appliances with the IP address of the third appliance.

Procedure

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

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

   b Log in using the following credentials.

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

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

3 In the **Navigator**, click **Groups and Tags** and click the **Grouping Objects** tab.

4 From the **NSX Manager** drop-down menu, select **172.16.11.65**.

5 Click **IP Sets**.

6 Select the **vRealize Automation Appliances** IP set and click the **Edit IP Set** icon.

7 In the **Edit IP Set** dialog box, click **Add New Row** icon to add the IP address of the third vRealize Automation virtual appliance to the IP Set and click **OK**.

   Verify that the **Universal Synchronization** check box remains selected.

Setting	Value
IP Set Name	vRealize Automation Appliances
Additional IP Address	192.168.11.50

Replace the vRealize Automation Certificate

Before you expand the vRealize Automation cluste with a third vRealize Automation virtual appliance, on the vRealize Automation virtual appliances and vRealize Automation IaaS components, you must install a certificate that includes the host name of the third appliance.

You add the third vRealize Automation virtual appliance as an additional subject alternative name (SAN) in the certificate. You must also update the trusted vRealize Automation certificate on the vRealize Business for Cloud and vRealize Operations Manager deployments in the environment.

Procedure

1 Re-Generate the vRealize Automation Certificate to Cover the Third Appliance

Before you extend the CMP with a third vRealize Automation appliance, generate a new certificate for the vRealize Automation components that includes the new appliance node. The certificate must contain the host name and FQDN of the new node in advance so that the new appliance can participate in the communication between the vRealize Automation components and to the connected management solutions such as vRealize Business and vRealize Operations Manager right after you add the appliance to the CMP.

2 Replace the vRealize Automation Certificate in Region A

Replace the existing certificate for all vRealize Automation services from the vRealize Automation Management Console. You replace the certificate on the vRealize Automation Appliance, IaaS Web server, and IaaS Manager server to maintain a trusted communication between the vRealize Automation nodes.

3 Update the vRealize Automation Certificate on vRealize Orchestrator and vRealize Business in Region A

After you update the vRealize Automation certificate, reconnect vRealize Orchestrator and vRealize Business to vRealize Automation to install the new certificate.

4 Update the vRealize Automation Certificate on vRealize Operations Manager in Region A

After you change the certificate of the vRealize Automation Appliance and IaaS components, update the certificate on vRealize Operations Manager to keep the communication trusted by reconnecting the vRealize Automation Adapter.

Re-Generate the vRealize Automation Certificate to Cover the Third Appliance

Before you extend the CMP with a third vRealize Automation appliance, generate a new certificate for the vRealize Automation components that includes the new appliance node. The certificate must contain the host name and FQDN of the new node in advance so that the new appliance can participate in the communication between the vRealize Automation components and to the connected management solutions such as vRealize Business and vRealize Operations Manager right after you add the appliance to the CMP.

Prerequisites

- Provide a Window Server 2012 host that is part of the sfo01.rainpole.local domain.
- Install a Certificate Authority server on the rainpole.local domain.

Procedure

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

2 On the Windows host where you connect to the data center, from VMware Knowledge Base article 2146215, download the `CertGenVVD-`*`version`*`.zip` file of the Certificate Generation Utility that is compatible with this version of VMware Validated Design and extract the ZIP file to the `C:` drive.

3 Verify that the `vra.txt` file in the `C:\CertGenVVD-version\ConfigFiles` folder contains the host name and FQDN of the third vRealize Automation appliance.

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=default
ST=default
CC=default
CN=vra01svr01.rainpole.local
keysize=default
[SAN]
vra01svr01a
vra01svr01b
vra01svr01c
vra01svr01
vra01iws01a
vra01iws01b
vra01iws01
vra01ims01a
vra01ims01b
vra01ims01
vra01dem01
vra01dem02
vra01svr01a.rainpole.local
vra01svr01b.rainpole.local
vra01svr01c.rainpole.local
vra01svr01.rainpole.local
vra01iws01a.rainpole.local
vra01iws01b.rainpole.local
vra01iws01.rainpole.local
vra01ims01a.rainpole.local
vra01ims01b.rainpole.local
vra01ims01.rainpole.local
vra01dem01.rainpole.local
vra01dem02.rainpole.local
#vRA-cluster-ip
192.168.11.53
```

4 Generate the CA-signed certificates for the management components in the SDDC.

Repeat Use the Certificate Generation Utility to Generate CA-Signed Certificates for the SDDC Management Components from the *VMware Validated Design Planning and Preparation* documentation.

Replace the vRealize Automation Certificate in Region A

Replace the existing certificate for all vRealize Automation services from the vRealize Automation Management Console. You replace the certificate on the vRealize Automation Appliance, IaaS Web server, and IaaS Manager server to maintain a trusted communication between the vRealize Automation nodes.

Procedure

1 Log in to the first vRealize Automation appliance.

   a Open a Web browser and go to **`https://vra01svr01a.rainpole.local:5480`**

   b Log in using the following credentials.

Settings	Value
User name	root
Password	*vra_appA_root_password*

2 On the **vRA Settings** tab, click the **Database** subtab and check which node has the `MASTER` label.

   If the `MASTER` node listed is not vra01svr01a.rainpole.local, log in to the management console of the `MASTER` appliance using the previous instruction.

3 On the **vRA Settings** tab, click the **Certificates** subtab.

4 Under **vRA Certificate**, select **Import** next to **Certificate Action**.

5 From a text editor on the Windows host where you run the `CertGenVVD` utility, copy the content of the following certificate files and paste it in to the following text boxes in the user interface, and click **Save Settings**.

Source Content	Target Text Box
vra.key	RSA Private Key
vra.3.pem	Certificate Chain
Passphrase that you optionally entered at generation	Passphrase

6 Scroll down on the page and verify that all cluster nodes have been successfully updated.

   You might wait several minutes for the operation to finish.

7 Click the **Certificates** tab and repeat the procedure to configure the IaaS Web server and IaaS Manager Service with the new certificate details.

IaaS Component	Component Type	Certificate Action
IaaS Web server	IaaS Web	Import Certificate
IaaS Manager Service	Manager Service	Import Certificate

Update the vRealize Automation Certificate on vRealize Orchestrator and vRealize Business in Region A

After you update the vRealize Automation certificate, reconnect vRealize Orchestrator and vRealize Business to vRealize Automation to install the new certificate.

Procedure

1 Log in to the first vRealize Automation appliance by using a Secure Shell (SSH) client.

   a Open an SSH connection to the primary vRealize Automation virtual appliance **`vra01svr01a.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vro_appA_root_password*

2 Stop the Orchestrator server and the Control Center services of the embedded vRealize Orchestrator server.

```
service vco-server stop && service vco-configurator stop
```

3 Update the vRealize Automation certificate in the component registration with vRealize Automation for embedded vRealize Orchestrator.

   a Verify the trusted certificate in the embedded vRealize Orchestrator trust store `vco.cafe.component-registry.ssl.certificate` using the command-line interface.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

   The SHA1 thumbprint must match that of vRealize Automation's certificate.

   b Run the following commands to update the trust store with the new vRealize Automation certificate.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --uri
https://vra01svr01.rainpole.local/
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --registry-certificate --uri
https://vra01svr01.rainpole.local
```

   When prompted, press Y to accept the new certificate.

   c After both operations have completed, verify that the trusted certificate in the embedded vRealize Orchestrator trust store has been updated.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

   The SHA1 thumbprint must match that of vRealize Automation's certificate.

   An alias store, `Alias: Imported<hash>`, is created for all certificates in the chain presented from vRealize Automation.

4 Start the Orchestrator server and the Control Center services of the built-in vRealize Orchestrator server on the vRealize Automation appliance, and verify their status.

```
service vco-configurator start && service vco-server start
service vco-configurator status && service vco-server status
```

5 Repeat this process on the secondary vRealize Orchestrator node.

6 Log in to the vRealize Business Server appliance management console.

a Open a Web browser and go to **`https://vrb01svr01.rainpole.local:5480`**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

7 On the **Registration** tab, click the **vRA** tab, enter the following credentials to register with the vRealize Automation server and initiate an update of a vRealize Automation certificate.

Setting	Value
Hostname	vra01svr01.rainpole.local
SSO Default Tenant	rainpole
SSO Admin User	administrator
SSO Admin Password	*vra_administrator_password*
Accept "vRealize Automation" certificate	Deselected

8 Click **Register** to connect to vRealize Automation and get its certificate.

A failure message appears at the top of the page.

9 Wait until the SSO Status changes to `The certificate of "vRealize Automation" is not trusted. Please view and accept to register.`

10 Click the **View "vRealize Automation" certificate** link to download the vRealize Automation certificate.

11 Select the **Accept "vRealize Automation" certificate** check box and click **Register**.

SSO Status changes to `Connected to vRealize Automation`.

Update the vRealize Automation Certificate on vRealize Operations Manager in Region A

After you change the certificate of the vRealize Automation Appliance and IaaS components, update the certificate on vRealize Operations Manager to keep the communication trusted by reconnecting the vRealize Automation Adapter.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

3 In the left pane of vRealize Operations Manager, under **Management** click **Certificates**.

4 Select the row that contains `CN=vra01svr01.rainpole.local` and click the **Delete** icon.

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

6 Select the **vRealize Automation Management Pack** solution and click **Configure**.

7 In the **Manage Solutions** dialog box, select **vRealize Automation Adapter**, click **Test Connection**, accept the new certificate, and click **Save Settings**.

Add a Third vRealize Automation Appliance to the Cluster

Prerequisites

Procedure

1 Take Snapshots of the vRealize Automation Virtual Machines

   Before you perform the upgrade of vRealize Automation, take a snapshot for each virtual machine in the environment. If you must perform a rollback of vRealize Automation to the previous state, these snapshots accelerate the rollback operation.

2 Take Snapshots of the vRealize Business Virtual Machines

   Before you perform the upgrade of vRealize Business, take a snapshot for each virtual machine in the environment. If you must perform a rollback of vRealize Business to the previous state, these snapshots accelerate the rollback operation.

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

   Before you upgrade the vRealize Automation virtual appliances and the vRealize Automation IaaS nodes, direct all traffic to the primary node and disable the health check on the NSX load balancer for the management applications.

4 Add the Third vRealize Automation Appliance as a Disabled Member to the Load Balancer in Region A

Before you expand the vRealize Automation cluster, add the host name and IP address of the third vRealize Automation virtual appliance as a disabled member of the server pools on the load balancer.

5 Deploy the Third vRealize Automation Virtual Appliance

Deploy a third vRealize Automation virtual appliance to the management cluster in Region A using the downloaded `.ova` file. Then, you can expand the vRealize Automation cluster.

6 Join the Third vRealize Automation Appliances to the Cluster

After you deploy the third vRealize Automation appliance, join it to the vRealize Automation cluster. After you join the appliance, the vRealize Automation services start, and the appliance inherits the settings from the cluster, such as, certificate and licensing.

7 Enable Synchronous Mode for vRealize Automation Database Replication

After you expand vRealize Automation to include the third vRealize Automation virtual appliance, change the replication method of the PostgreSQL database to synchronous mode. Synchronous mode for automatic failover with improved data loss protection.

8 Enable the State and Health Monitoring for the New vRealize Automation Appliance on the Load Balancer in Region A

After you complete expansion of the vRealize Automation cluster, update traffic distribution and health checks on the NSX load balancer in Region A to cover the new configuration of primary and secondary components of vRealize Automation platform.

9 Delete the Snapshots of the vRealize Automation and vRealize Business Virtual Machines

After you expand the vRealize Automation cluster and verify operations and functionality, delete the virtual machine snapshots.

Procedure

◆

Example:

What to do next

Take Snapshots of the vRealize Automation Virtual Machines

Before you perform the upgrade of vRealize Automation, take a snapshot for each virtual machine in the environment. If you must perform a rollback of vRealize Automation to the previous state, these snapshots accelerate the rollback operation.

Table 2-15. vRealize Automation Virtual Machines

Region	Folder	Role	Virtual Machine Name
Regoin A	sfo01-m01fd-vra	vRealize Automation Appliances	vra01svr01a
	sfo01-m01fd-vra		vra01svr01b
	sfo01-m01fd-vra	vRealize Automation IaaS Web Servers	vra01iws01a
	sfo01-m01fd-vra		vra01iws01b
	sfo01-m01fd-vra	vRealize Automation IaaS Model Manager Servers	vra01ims01a
	sfo01-m01fd-vra		vra01ims01b
	sfo01-m01fd-vra	vRealize Automation IaaS DEM Workers	vra01dem01a
	sfo01-m01fd-vra		vra01dem01b
	sfo01-m01fd-vraias	vRealize Automation IaaS Proxy Agents	sfo01ias01a
	sfo01-m01fd-vraias		sfo01ias01b
Region B	lax01-m01fd-vraias	vRealize Automation IaaS Proxy Agents	lax01ias01a
	lax01-m01fd-vraias		lax01ias01b

Note If you are using the designated Microsoft SQL Server vra01mssql01.rainpole.local covered within the VMware Validated Design include this in the snapshot take for vRealize Automation. If you are using a shared instance of Microsoft SQL Server to host the vRealize Automation IaaS database along with other databases, ensure that you have a recent backup per the vRealize Automation Upgrade Prerequisites.

Procedure

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

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

   b Log in using the following credentials.

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

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

3 Shut down the vRealize Automation virtual machines in the environment according to Shutdown Order of the Management Virtual Machines.

   a In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra** tree .

   b Right-click the **vra01dem01a** virtual machine, select **Power > Shut Down Guest OS** and click **Yes** in the confirmation dialog box that appears.

   c Repeat the steps on the remaning vRealize Automation virtual machines in the environment.

4 Take a snapshot of the vRealize Automation virtual machines in the environment.

a In the **Navigator**, right-click the **vra01svr01a.rainpole.local** 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	VMware Validated Design Cloud Management Layer Upgrade
Description	-
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

c Repeat these steps for the remaining vRealize Automation virtual machines in the environment.

5 Power on the vRealize Automation virtual machines in the environment according to Startup Order of the Management Virtual Machines.

a In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra** tree .

b Right-click the **vra01mssql01** virtual machine, select **Power > Power On** and click **Yes** in the confirmation dialog box that appears.

c Repeat the steps on the remaining vRealize Automation virtual machines in the environment.

Take Snapshots of the vRealize Business Virtual Machines

Before you perform the upgrade of vRealize Business, take a snapshot for each virtual machine in the environment. If you must perform a rollback of vRealize Business to the previous state, these snapshots accelerate the rollback operation.

Table 2-16. vRealize Business Virtual Machines

Region	Folder	Role	Virtual Machine Name
Region A	sfo01-m01fd-vra	vRealize Business for Cloud Server	vrb01svr01
	sfo01-m01fd-vraias	vRealize Business for Cloud Data Collector	sfo01vrbc01
Region B	lax01-m01fd-vraias	vRealize Business for Cloud Data Collector	lax01vrbc01

Procedure

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

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

   b Log in using the following credentials.

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

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

3 Shut down the vRealize Business nodes in the environment according to Shutdown Order of the Management Virtual Machines.

   a In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra** tree .

   b Right-click the **sfo01vrbc01** virtual machine, select **Power > Shut Down Guest OS** and click **Yes** in the confirmation dialog box that appears.

   c Repeat the steps on the remaining vRealize Business virtual machines in the environment.

4 Take a snapshot of the vRealize Business virtual machines in the environment.

   a In the **Navigator**, click **VMs and Templates** and expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra** tree.

   b Right-click the **vrb01svr01** 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	VMware Validated Design 4.3 Cloud Management Layer Upgrade
Description	-
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

   d Repeat these steps for the remaining virtual machines in the environment.

5 Power on the vRealize Business virtual machines in the environment according to Startup Order of the Management Virtual Machines.

   a In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra** tree .

   b Right-click the **vrb01svr01** virtual machine, select **Power > Power On** and click **Yes** in the confirmation dialog box that appears.

   c Repeat the steps on the remaining vRealize Business virtual machines in the environment.

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

Before you upgrade the vRealize Automation virtual appliances and the vRealize Automation IaaS nodes, direct all traffic to the primary node and disable the health check on the NSX load balancer for the management applications.

The configuration change disables the second pool member for the five vRealize Automation VIPs. During an upgrade, the services inside the second node might not be upgraded or initialized because of installation or power cycle operations. If the load balancer passes a request to the second node, the request will fail. If the second pool member remains enabled, you might experience failures during vRealize Automation upgrade, and service initialization or registration failures during a vRealize Automation appliance power cycle operations.

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

Load Balancer Pools on sfo01m01lb01	Secondary Member to Disable
vra-svr-443	According to which node is labeled as `REPLICA`: ■ vra01svr01a ■ vra01svr01b
vra-svr-8444	According to which node is labeled as `REPLICA` ■ vra01svr01a ■ vra01svr01b
vra-iws-443	vra01iws01b
vra-ims-443	vra01ims01b
vra-vro-8283	According to which node is labeled as `REPLICA`: ■ vra01svr01a ■ vra01svr01b

Procedure

1 Log in to the first vRealize Automation appliance.

   a Open a Web browser and go to **`https://vra01svr01a.rainpole.local:5480`**

   b Log in using the following credentials.

Settings	Value
User name	root
Password	*vra_appA_root_password*

2 On **vRA Settings** tab, click the **Database** tab and check which node has the `REPLICA` label. The `REPLICA` label indicates which vRealize Appliance is the secondary.

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

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

   b Log in using the following credentials.

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

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

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

6 From the **NSX Manager** drop-down menu, select **172.16.11.65** and double-click the **sfo01m01lb01** NSX Edge to open its network settings.

7 On the **Manage** tab, click the **Load Balancer** tab and click **Pools**.

8 Select the **vra-svr-443** pool that contains the vRealize Automation appliances and click **Edit**.

9 In the **Edit Pool** dialog box, select the secondary node, click **Edit**, select **Disable** from the **State** drop-down menu, and click **OK**.

10 In the **Edit Pool** dialog box, select **NONE** from the **Monitors** drop-down menu and click **OK**.

11 Repeat the procedure on the remaining load balancer pools.

12 To verify that the load balancer redirects the traffic to the primary node of the vRealize Automation virtual appliance, open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac`** to verify that the login page of the vRealize Automation administration portal appears.

Add the Third vRealize Automation Appliance as a Disabled Member to the Load Balancer in Region A

Before you expand the vRealize Automation cluster, add the host name and IP address of the third vRealize Automation virtual appliance as a disabled member of the server pools on the load balancer.

On the load balancer for application virtual network, perform the procedure three times to update the server pools related to the traffic to the vRealize Automation appliance with the settings for the third vRealize Automation virtual appliance.

Table 2-17. Load Balancer Pool Updates for vRealize Automation in Region A

Pool Name	Algorithm	Monitors	New Member	IP Address	State	Port	Monitor Port
vra-svr-443	ROUND-ROBIN	NONE	vra01svr01c	192.168.11.50	Disabled	443	443
vra-svr-8444	ROUND-ROBIN	NONE	vra01svr01c	192.168.11.50	Disabled	8444	443
vra-vro-8283	ROUND-ROBIN	NONE	vra01svr01c	192.168.11.50	Disabled	8283	8283

Procedure

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

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

   b Log in using the following credentials.

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

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

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

4 From the **NSX Manager** drop-down menu, select **172.16.11.65** and double-click the **sfo01m01lb01** NSX Edge to open its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Pools**.

6 Select the pool named **vra-svr-443** and click the **Edit** icon.

7 Under **Members**, click the **Add** icon to add a third pool member.

8 In the **New Member** dialog box, enter the following values, and click **OK**.

Setting	Value
Name	vra01svr01c
IP Address/VC Container	192.168.11.50
State	Disabled
Port	443
Monitor Port	443
Weight	1

9 Repeat the procedure to update the remaining server pools with the details about the third vRealize Automation virtual appliance in a disabled state.

Deploy the Third vRealize Automation Virtual Appliance

Deploy a third vRealize Automation virtual appliance to the management cluster in Region A using the downloaded `.ova` file. Then, you can expand the vRealize Automation cluster.

Prerequisites

Download the `.ova` file, `VMware-vRA-Appliance-7.4.0.xxx-build_number.ova`, for vRealize Automation 7.4 to the system from which you are performing the upgrade.

Procedure

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

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

b Log in using the following credentials.

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

2 In the vSphere Web Client, select **Home > Hosts and Clusters**.

3 Right-click the **sfo01m01vc01.sfo01.rainpole.local** vCenter Server object and select **Deploy OVF Template**.

4 On the **Select template** page, select **Local file**, browse to the location of the `.ova` file on your file system and click **Next**.

5 On the **Select name and folder** page, enter the following information, and click **Next**.

Setting	Value
Name	Selected
Select a folder or datacenter	sfo01-m01fd-vra

6 On the **Review details** page, examine the virtual appliance details, such as product, version, download and disk size, and click **Next.**

7 On the **Accept license agreements** page, accept the end user license agreements and click **Next**.

8 On the **Select storage** page, set the following datastore configuration and click **Next**.

Setting	Value
Select virtual disk format	Thin Provision
VM storage policy	vSAN Default Storage Policy
Datastore	sfo01-m01-vsan01

9 On the **Setup Networks** page, select the distributed port group that ends with `Mgmt-xRegion01-VXLAN` from the **Destination Network** drop-down menu and click **Next**.

10 On the **Customize template** page, configure the following values, and click **Next**.

Option	Description
Enable SSH service in the appliance	Selected
Hostname	vra01svr01c.rainpole.local
Initial Root Password	*vra_appC_root_password*
Default Gateway	192.168.11.1
Domain Name	rainpole.local
Domain Names Servers	172.16.11.4,172.17.11.4
Domain Search Path	rainpole.local,sfo01.rainpole.local,lax01.rainpole.local
Network 1 IP Address	192.168.11.50
Network 1 Netmask	255.255.255.0

11 On the **Ready to complete** page, review the configuration settings you have specified and click **Finish**.

12 In the **Navigator** pane, click **sfo01m01vc01.sfo01.rainpole.local**, click the **VMs** tab and type **`vra01svr01`** in the search text box.

13 Select virtual machine **vra01svr01c** and click the **Power On** icon and wait until the power-on procedure is completed.

14 In the virtual machine console, verify that **vra01svr01c** uses the configuration settings you specified.

a In the vSphere Web Client, right-click the appliance and select **Open Console** to open the remote console to the appliance.

b Examine the welcome screen of the appliance console.

c Close the virtual appliance console.

Join the Third vRealize Automation Appliances to the Cluster

After you deploy the third vRealize Automation appliance, join it to the vRealize Automation cluster. After you join the appliance, the vRealize Automation services start, and the appliance inherits the settings from the cluster, such as, certificate and licensing.

Procedure

1 Log in to the first vRealize Automation appliance.

   a Open a Web browser and go to **`https://vra01svr01a.rainpole.local:5480`**

   b Log in using the following credentials.

Settings	Value
User name	root
Password	*vra_appA_root_password*

2 On the **vRA Settings** tab, click the **Database** subtab and check which node has the `MASTER` label.

   If the `MASTER` node listed is not vra01svr01a.rainpole.local, log in to the management console of the `MASTER` appliance using the previous instruction.

3 Log in to the management console of the newly deployed vRealize Automation appliance.

   a Open a Web Browser and go to **`https://vra01svr01c.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vra_appC_root_password*

4 If the **Installation Wizard** appears, click **Cancel** to go directly to the management interface.

5 On the **Admin** tab, click **Time Settings** and verify that the time source is the same as on the `MASTER`.

6 On **vRA Settings** tab, click the **Cluster** tab.

7 Enter the following settings on the **Cluster** page and click **Join Cluster**.

Setting	Value
Leading Cluster Node	*FQDN of the master vRealize Automation appliance*
Admin User	root
Password	*vra_appMaster_root_password*

8 If certificate warnings are displayed, ignore them.

9 Monitor the status of the services as they are restarted on vra01svr01c.rainpole.local.

   a Click the **Services** tab and click the **Refresh** button to monitor the progress of services startup.

10 Start the embedded vRealize Orchestrator services on vra01svr01c.rainpole.local.

   a On the **vRA Settings > Orchestrator** tab, select **Orchestrator user interface**.

   b If the service is stopped, in the **Actions** area, click **Start**.

   c Repeat this step for **Orchestrator Server**.

11 Configure the Orchestrator user interface service to start automatically after upgrade.

a Open an SSH connection to vra01svr01c.rainpole.local.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vra_appC_root_password*

c Run the following command to verify that the service is set to automatically start.

```
chkconfig vco-configurator
```

d If the service reports `Off`, run the following command to enable an automatic restart of the Orchestrator user interface service upon subsequent reboots of the vRealize Automation appliance.

```
chkconfig vco-configurator on
```

e Verify the status of Orchestrator User Interface by running the following command .

```
service vco-configurator status
```

Enable Synchronous Mode for vRealize Automation Database Replication

After you expand vRealize Automation to include the third vRealize Automation virtual appliance, change the replication method of the PostgreSQL database to synchronous mode. Synchronous mode for automatic failover with improved data loss protection.

Procedure

1 Log in to the first vRealize Automation appliance.

a Open a Web browser and go to **`https://vra01svr01a.rainpole.local:5480`**

b Log in using the following credentials.

Settings	Value
User name	root
Password	*vra_appA_root_password*

2 On the **vRA Settings** tab, click the **Database** button to review the current **Replication Mode**.

3 Verify the following database settings.

Setting	Expected Value
Replication Mode	Database is in Asynchronous Mode
Connection Status	Connected

4 Verify that the following hosts appear in the list of database nodes.

Database Node Host	Status
vra01svr01a.rainpole.local	Up
vra01svr01b.rainpole.local	Up
vra01svr01c.rainpole.local	Up

5 Verify that each of the two replica hosts has the following configuration.

Setting	Expected Value
Sync State	Async
Valid	Yes

6 Click the **Sync Mode** button to enable the synchronous replication mode of the PostgreSQL database.

Wait until the **Replication Mode** updates.

7 Verify the following database settings.

Setting	Expected Value
Replication Mode	Database is in Synchronous Mode. Automatic failover is now turned on!
Connection Status	Connected

8 Verify that you see the hosts in Step 4.

9 Verify that each of the two replica hosts has the following configuration.

Setting	Expected Value
Sync State	Sync
Valid	Yes

Enable the State and Health Monitoring for the New vRealize Automation Appliance on the Load Balancer in Region A

After you complete expansion of the vRealize Automation cluster, update traffic distribution and health checks on the NSX load balancer in Region A to cover the new configuration of primary and secondary components of vRealize Automation platform.

Load Balancer Pool on the sfo01m01lb01	New Member to Enable	Monitors
vra-svr-443	vra01svr01c	vra-svr-443-monitor
vra-svr-8444	vra01svr01c	vra-svr-443-monitor
vra-vro-8283	vra01svr01c	vra-vro-8283-monitor

Procedure

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

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

   b Log in using the following credentials.

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

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

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

4 From the **NSX Manager** drop-down menu, select **172.16.11.65** and double-click the **sfo01m01lb01** NSX Edge to open its network settings.

5 On the **Manage** tab, click the **Load Balancer** tab, click **Pools**.

6 Select the **vra-svr-443** pool that is associated with the traffic to the vRealize Automation portal and click **Edit**.

7 In the **Edit Pool** dialog box, select the new vRealize Automation appliance, click **Edit**, select **Enable** from the **State** drop-down menu, and click **OK**.

8 In the **Edit Pool** dialog box, select **vra-svr-443-monitor** from the **Monitors** drop-down menu and click **OK**.

9 Repeat the procedure on the remaining load balancer pools.

Delete the Snapshots of the vRealize Automation and vRealize Business Virtual Machines

After you expand the vRealize Automation cluster and verify operations and functionality, delete the virtual machine snapshots.

Table 2-18. vRealize Automation Virtual Machines

Region	Folder	Role	Virtual Machine Name
Regoin A	sfo01-m01fd-vra	vRealize Automation Appliances	vra01svr01a
	sfo01-m01fd-vra		vra01svr01b
	sfo01-m01fd-vra		vra01svr01c
	sfo01-m01fd-vra	vRealize Automation IaaS Web Servers	vra01iws01a
	sfo01-m01fd-vra		vra01iws01b
	sfo01-m01fd-vra	vRealize Automation IaaS Model Manager Servers	vra01ims01a
	sfo01-m01fd-vra		vra01ims01b
	sfo01-m01fd-vra	vRealize Automation IaaS DEM Workers	vra01dem01a

Table 2-18. vRealize Automation Virtual Machines (Continued)

Region	Folder	Role	Virtual Machine Name
	sfo01-m01fd-vra		vra01dem01b
	sfo01-m01fd-vraias	vRealize Automation IaaS Proxy Agents	sfo01ias01a
	sfo01-m01fd-vraias		sfo01ias01b
Region B	lax01-m01fd-vraias	vRealize Automation IaaS Proxy Agents	lax01ias01a
	lax01-m01fd-vraias		lax01ias01b

Table 2-19. vRealize Business Virtual Machines

Region	Folder	Role	Virtual Machine Name
Region A	sfo01-m01fd-vra	vRealize Business for Cloud Server	vrb01svr01
	sfo01-m01fd-vraias	vRealize Business for Cloud Data Collector	sfo01vrbc01
Region B	lax01-m01fd-vraias	vRealize Business for Cloud Data Collector	lax01vrbc01

Procedure

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

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

   b Log in using the following credentials.

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

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

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

   b Log in using the following credentials.

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

3 In the **Navigator**, click **VMs and Templates** and navigate to the vra01svr01a virtual machine.

4 Right-click the **vra01svr01a** virtual machine and select **Snapshots > Manage Snapshots**.

5 In the **Snapshot Manager**, click the snapshot that you created before the vRealize Automation upgrade and select **Delete**.

6 Click **Yes** in the confirmation dialog and click **Close** in **Snapshot Manager**.

7 Repeat the procedure for the remaining vRealize Automation and vRealize Business virtual machines.

Configure the Environment for the Third vRealize Automation Appliance

After you complete the expansion of vRealize Automation, update the anti-affinity and startup rules in the environment.

Procedure

1 Update the Anti-Affinity Rules for vRealize Automation Virtual Machines in Region A

After you complete the expansion of the vRealize Automation cluster, update the VM/Host anti-affinity to ensure that each of the vRealize Automation virtual appliances are maintained on different hosts.

2 Update the VM Group for the vRealize Automation Virtual Appliances in Region A

After you expand the vRealize Automation cluster, update the VM Group for the vRealize Automation appliances so that vSphere HA handles the new vRealize Automation appliance when powering on the CMP virtual machines.

Update the Anti-Affinity Rules for vRealize Automation Virtual Machines in Region A

After you complete the expansion of the vRealize Automation cluster, update the VM/Host anti-affinity to ensure that each of the vRealize Automation virtual appliances are maintained on different hosts.

Table 2-20. Anti-Affinity Rules for the vRealize Automation Virtual Appliances

Name	Type	Members
anti-affinity-rule-vra-svr	Separate Virtual Machines	vra01svr01a
		vra01svr01b
		vra01svr01c

Procedure

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

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

b Log in using the following credentials.

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

2 From the **Home** page, click **Hosts and Clusters**.

3 Under **sfo01m01vc01.sfo01.rainpole.local**, expand **sfo01-m01dc**, and click **sfo01-m01-mgmt01**.

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

5 Under **VM/Host Rules**, select the existing **anti-affinity-rule-vra-svr** rule and click **Edit**.

6 In the **Edit VM/Host Rule** dialog box, click **Add**, select the vra01svr01c, click **OK**.

The rule includes the virtual machines of the three vRealize Automation appliances.

Update the VM Group for the vRealize Automation Virtual Appliances in Region A

After you expand the vRealize Automation cluster, update the VM Group for the vRealize Automation appliances so that vSphere HA handles the new vRealize Automation appliance when powering on the CMP virtual machines.

Procedure

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

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

b Log in using the following credentials.

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

2 In the **Navigator**, select **Host and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local** tree.

3 Update the VM Group for the vRealize Automation appliances.

a Select the **sfo01-m01-mgmt01** cluster and click the **Configure** tab.

b On the **Configure** page, click **VM/Host Groups**.

c On the **VM/Host Groups** page, select the **vRealize Automation Virtual Appliances** VM/Host Group and click the **Edit** button.

d In the **Edit VM/Host Group** dialog box, click the **Add** button.

e In the **Add VM/Host Group Member** dialog box, select **vra01svr01c** and click **OK**.

The VM Group contains vra01svr01a, vra01svr01b**,** and vra01svr01c.

f Click **OK** to save the update to the VM Group.

Configure Log Forwarding for the Third vRealize Automation Appliance in Region A

Log in to the primary management console interface of the newly added vRealize Automation appliance and update the Log Insight Agent configuration.

Agent configuration for the vRealize Automation virtual appliances includes the following tasks:

- Verify that the log forwarding configuration has been inherited and configured on the new vRealize Automation virtual appliance to send logs to the vRealize Log Insight cluster.
- Update the agent group for configuring log forwarding from the vRealize Automation modules to include the new vRealize Automation virtual appliance.
- Update the agent group for configuring log forwarding from the operating system to include the new vRealize Automation virtual appliance.

Procedure

1 Log in to the third vRealize Automation appliance.

   a Open a Web browser and go to **`https://vra01svr01c.rainpole.local:5480`**

   b Log in using the following credentials.

Settings	Value
User name	root
Password	*vra_appC_root_password*

2 Configure log forwarding to vRealize Log Insight.

   a On the **vRA Settings** tab, click the **Logs** tab.

   b Scroll down to the **Log Insight Agent Configuration** section.

c Verify that the following values are replicated from vra01svr01a.rainpole.local to vra01svr01c.rainpole.local, and click **Save Settings**.

Setting	Value
Host	sfo01vrli01.sfo01.rainpole.local
Port	9000
Protocol	CFAPI
SSL Enabled	Deselected

d Scroll down to the **Agent Behavior Configuration** section.

Setting	Value
Reconnect	30
Max Buffer Size	2000
Debug Level	No Debug Messages

3 Log in to the vRealize Log Insight user interface.

a Open a Web browser and go to **`https://sfo01vrli01.sfo01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

4 Click the configuration drop-down menu icon and select **Administration**.

5 Under **Management**, click **Agents**.

6 Add the new appliance to the agent group for the vRealize Automation appliances.

You use this agent group to configure centrally the collection of logs that appear in the vRealize Automation dashboards.

a From the **All Agents** drop-down menu, select **vRA7 - Appliance Agent Group**.

b In the agent filter text boxes, add the host name of the new vRealize Automation appliance and press Enter.

Filter	Operator	Values
Hostname	Matches	▪ **`vra01svr01c.rainpole.local`**

c Click **Refresh** and verify that all the agents in the filter appear in the **Agents** list.

d Click **Save Agent Group** at the bottom of the page.

7 Repeat the steps to add the new vRealize Automation appliance to the **VA - Linux Agent Group** that stores central configuration for the agents on the management virtual appliances.

Filter	Operator	Values
Hostname	Matches	▪ `vra01svr01c.rainpole.local`

8 To verify the configuration, click **Dashboards** on the main navigation bar, and under the **VMware - vRA 7** category click **General - Overview**.

The dashboard shows log data from the components of the third vRealize Automation appliances.

Enable Disaster Recovery for the Third vRealize Automation Appliance

After you complete the expansion of vRealize Automation cluster in Region A for the cloud management layer, update the NSX load balancer with, and enable replication for, the new vRealize Automation virtual appliance to Region B. Next, you update the protection group and recovery plan for the cloud management layer in Site Recovery Manager, as well as, the anti-affinity and VM Group rules. Once completed, the addition of the new vRealize Automation virtual appliance will be be fully integrated into the VMware Validated Design.

Procedure

1 Add the Third vRealize Automation as an Enabled Member to the Load Balancer in Region B

Before you update the vRealize Automation disaster recovery configuration, add the name and IP address of the third vRealize Automation virtual appliance as an enabled member of the server pools on the load balancer.

2 Replicate the Third vRealize Automation Appliance in Region A

After you expand the vRealize Automation cluster, support the failover to Region B by enabling replication of the third vRealize Automation virtual appliance. After you configure the replication, you update the protection group to protect the newly replicated vRealize Automation virtual appliance.

3 Add the Third vRealize Automation Appliance to the Protection Group for the Cloud Management Layer

After you configure the replication of the third vRealize Automation appliance, update the protection group to protect the appliance. You use the protection group to protect the cloud management layer virtual machines by using Site Recovery Manager.

4 Update the Recovery Plan for the Cloud Management Layer

After you update the protection group for the Cloud Management Layer, update the existing recovery plan. You use the recovery plan to configure dependencies between the virtual machines.

5 Update the Anti-Affinity Rules for vRealize Automation Virtual Machines in Region B

Update the VM/Host anti-affinity rule to ensure that each of the vRealize Automation virtual appliances are maintained on different hosts after a failover.

6 Update the VM Group for the vRealize Automation Virtual Appliances in Region B

Update the VM Group for vRealize Automation virtual appliances with the new vRealize Automation appliance so that vSphere HA handles the new vRealize Automation appliance when powering on the CMP virtual machines after failover.

Add the Third vRealize Automation as an Enabled Member to the Load Balancer in Region B

Before you update the vRealize Automation disaster recovery configuration, add the name and IP address of the third vRealize Automation virtual appliance as an enabled member of the server pools on the load balancer.

Table 2-21. Load Balancer Pool Updates for vRealize Automation in Region B

Pool Name	Algorithm	Monitors	New Member Name	IP Address	State	Port	Monitor Port
vra-svr-443	ROUND-ROBIN	vra-svr-443-monitor	vra01svr01c	192.168.11.50	Enabled	443	443
vra-svr-8444	ROUND-ROBIN	vra-svr-8444-monitor	vra01svr01c	192.168.11.50	Enabled	8444	443
vra-vro-8283	ROUND-ROBIN	vra-vro-8283-monitor	vra01svr01c	192.168.11.50	Enabled	8283	8283

Procedure

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

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

b Log in using the following credentials.

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

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

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

4 From the **NSX Manager** drop-down menu, select **172.17.11.65** and double-click the **lax01m01lb01** NSX Edge to open its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Pools**.

6 Select the **vra-svr-443** pool and click the **Edit** icon.

7 In the **Edit Pool** dialog box, click the **Add** icon under **Members**.

8 In the **New Member** dialog box, enter the following values, and click **OK**.

Setting	Value
Name	vra01svr01c
IP Address/VC Container	192.168.11.50
State	Enabled
Port	443
Monitor Port	443
Weight	1

9 Repeat the procedure to update remaining load balancer pools with the third vRealize Automation virtual appliance in an enabled state.

Replicate the Third vRealize Automation Appliance in Region A

After you expand the vRealize Automation cluster, support the failover to Region B by enabling replication of the third vRealize Automation virtual appliance. After you configure the replication, you update the protection group to protect the newly replicated vRealize Automation virtual appliance.

Procedure

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

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

b Log in using the following credentials.

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

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

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

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

4 Select the new vRealize Automation virtual appliance

New vRealize Automation Component	Virtual Machine Name
vRealize Automation Appliance	vra01svr01c

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

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

7 On the **Target site** page, select the **lax01m01vc01.lax01.rainpole.local** vCenter Server in Region B and click **Next**.

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

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

   a Click the **Edit** link.

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

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

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

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

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

Important

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

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

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

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

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

13 (Optional) Monitor the replication progress.

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

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

   c On the **Monitor** tab, click the **vSphere Replication** tab, and select **Outgoing Replications** to see details for the replication of the virtual machines of the cloud management layer from this site.

Add the Third vRealize Automation Appliance to the Protection Group for the Cloud Management Layer

After you configure the replication of the third vRealize Automation appliance, update the protection group to protect the appliance. You use the protection group to protect the cloud management layer virtual machines by using Site Recovery Manager.

Procedure

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

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

   b Log in using the following credentials.

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

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

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

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

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

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

6 Select the **SDDC Cloud Management PG** Protection Group and click the **Edit Protection Group** icon.

   The **Edit Protection Group** wizard appears.

7 On the **Name and location** page, click **Next**.

8 On the **Protection group type** page, click **Next**.

9 On the **Virtual machines** page, select vra01svr01c under **Replicated Virtual Machines** and click **Next**.

10 On the **Ready to complete** page, review the protection group settings and click **Next**.

11 On the **Apply changes** page, monitor the updates.

   - **Reconfigure protection group** updates to a checked status.
   - **Protect virtual machines** updates to a checked status.

12 Click **Finish**

13 Verify that vra01svr01c has been added to the Site Recovery Manager protection group.

a Click the **SDDC Cloud Management PG** protection group.

a Click the **Related Objects** tab, and click the **Virtual Machines** option.

b Verify that vra01svr01c is listed with a **Protection Status** of OK.

Update the Recovery Plan for the Cloud Management Layer

After you update the protection group for the Cloud Management Layer, update the existing recovery plan. You use the recovery plan to configure dependencies between the virtual machines.

Procedure

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

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

b Log in using the following credentials.

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

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

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

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

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

6 Change the priority of the vra01svr01c virtual machine.

a On the **Virtual Machines** tab, right-click **vra01svr01c** and select **All Priority Actions > 2 (High)**.

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

7 Configure dependencies between the virtual machines that have the vRealize Automation Server role.

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

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

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

d Click **OK**.

Update the Anti-Affinity Rules for vRealize Automation Virtual Machines in Region B

Update the VM/Host anti-affinity rule to ensure that each of the vRealize Automation virtual appliances are maintained on different hosts after a failover.

Table 2-22. Anti-Affinity Rules for the vRealize Automation Virtual Appliances

Name	Type	Members
anti-affinity-rule-vra-svr	Separate Virtual Machines	vra01svr01a
		vra01svr01b
		vra01svr01c

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** page, click **Hosts and Clusters**.

3 Under **lax01m01vc01.lax01.rainpole.local**, click **lax01-m01dc**, and click **lax01-m01-mgmt01**.

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

5 Under **VM/Host Rules**, select the existing **anti-affinity-rule-vra-svr** rule.

6 Click **Edit** to edit the existing virtual machine anti-affinity rule.

7 In the **Edit VM/Host Rule** dialog box, click **Add**, select the vra01svr01cand click **OK**.

   The rule includes the virtual machines of the three vRealize Automation appliances.

Update the VM Group for the vRealize Automation Virtual Appliances in Region B

Update the VM Group for vRealize Automation virtual appliances with the new vRealize Automation appliance so that vSphere HA handles the new vRealize Automation appliance when powering on the CMP virtual machines after failover.

Procedure

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

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

   b Log in using the following credentials.

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

2 In the **Navigator**, select **Host and Clusters** and expand the **lax01m01vc01.lax01.rainpole.local** tree.

3 Update the VM Group for the vRealize Automation Virtual Appliances.

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

   b On the **Configure** page, click **VM/Host Groups**.

   c On the **VM/Host Groups** page, select the **vRealize Automation Virtual Appliances** VM/Host Group from the list provided and click the **Edit** button.

   d In the **Edit VM/Host Group** dialog box, click the **Add** button.

   e In the **Add VM/Host Group Member** dialog box, select vra01svr01c and click **OK**.

   The VM Group contains vra01svr01a, vra01svr01b**,** and vra01svr01c .

   f Click **OK** to save the update to the VM Group.

Upgrade the Operations Management Layer

3

After you complete the upgrade of the cloud management layer, you can proceed with the upgrade of the operations managemetn layer. The vRealize Operations Manager and vRealize Log Insight components continue to monitor existing and upgraded components using the latest capabilities of the new release. In addition, you perform post-upgrade configurations procedures for each and the deployment and configuration of vRealize Suite Lifecycle Manager, a new operations managment layer component in this release..

Table 3-1. Upgrade Sequence for the Operations Management Layer

Order	Component	Sub-Component
1	vRealize Operations Manager	-
2	Post-upgrade Configuration of vRealize Operations Manager	-
3	vRealize Log Insight	vRealize Log Insight Appliances
		vRealize Log Insight Agents
4	Post-upgrade Configuration of vRealize Log Insight	-
5	vRealize Suite Lifecycle Manager	-

- Upgrade vRealize Operations Manager

  When you upgrade the operations management layer as a part of the upgrade from the previous VMware Validated Design release, start with vRealize Operations Manager. Upgrade the operating system and solution on the vRealize Operations Manager virtual appliances, and the management packs for communication with the other management solutions. After the upgrade, perform additional configurations on the management pack adapters and dashboards for alignment with the design.

- Upgrade vRealize Log Insight

  After you complete the upgrade and post-upgrade configurations for vRealize Operations Manager, continue the operations management layer upgrade with the vRealize Log Insight clusters and agents in each region. Post-upgrade, you perform additional configurations so that the environment remains in alignment with the design.

- Deploy and Configure vRealize Suite Lifecycle Manager Post-Upgrade

  After you complete the upgrade and post-upgrade configurations for vRealize Operations and vRealize Log Insight in the operations management layer, you deploy and configure vRealize Suite Lifecycle Manager. vRealize Suite Lifecycle Manager automates the lifecycle management and drift analysis of the VMware vRealize Suite solutions in VMware Validated Design for simplified operational experience.

- Import the vRealize Product Configurations in vRealize Suite Lifecycle Manager

  After you have complete the deployment and configuration of vRealize Suite Lifecycle Manager, import the vRealize Suite product configurations for the operations management and cloud management layers in logical vRealize Suite Lifecycle Manager environments. Importing the product configurations provides alignment with this VMware Validated Design. You can perform lifecycle management and configuration drift analysis across the vRealize Suite products in the SDDC.

Upgrade vRealize Operations Manager

When you upgrade the operations management layer as a part of the upgrade from the previous VMware Validated Design release, start with vRealize Operations Manager. Upgrade the operating system and solution on the vRealize Operations Manager virtual appliances, and the management packs for communication with the other management solutions. After the upgrade, perform additional configurations on the management pack adapters and dashboards for alignment with the design.

When you upgrade the vRealize Operations Manager virtual appliance in the design, you perform the upgrade manually using the master node in the vRealize Operations Manager analytics cluster. The remaining nodes, such as, master replica, data, and remote collector nodes are updated automatically. After the upgrade of the vRealize Operations Manager virtual appliances is complete, update each of the management packs.

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

Region	Role	IP Address	Fully Qualified Domain Name
Region A	Master Node	192.168.11.31	vrops01svr01a.rainpole.local
	Master Replica Node	192.168.11.32	vrops01svr01b.rainpole.local
	Data Node 1	192.168.11.33	vrops01svr01c.rainpole.local
	Data Node 2	*192.168.11.34*	*vrops01svr01d.rainpole.local*
	Remote Collector Node 1	192.168.31.31	sfo01vropsc01a.sfo01.rainpole.local
	Remote Collector Node 2	192.168.31.32	sfo01vropsc01b.sfo01.rainpole.local
Region B	Remote Collector Node 1	192.168.32.31	lax01vropsc01a.lax01.rainpole.local
	Remote Collector Node 2	192.168.32.32	lax01vropsc01b.lax01.rainpole.local

Prerequisites

- Download the product upgrade `.pak` files of vRealize Operations Manager to a Windows host that has access to the environment.

  Table 3-2. PAK Files Required for vRealize Operations Manager Upgrade

PAK Type	PAK File
Operating System Update `.pak` file	vRealize_Operations_Manager-VA-OS-6.7.0.*build_number*.pak
Software Update `.pak` file	vRealize_Operations_Manager-VA-6.7.0.*build_number*.pak
vRealize Operations Manager Management for NSX for vSphere	vmware-MPforNSX-vSphere-*build_number*.pak

- Examine the health of vRealize Operations Manager cluster by using the Upgrade Assessment Tool. Remediate any issues before you begin the upgrade. See VMware Knowledge Base article 53545 and the product download page version 6.7.0.1.
- Preserve any customized content by cloning the content.

  Customized content includes alert definitions, symptom definitions, recommendations, and views.
- Verify that a current backup of each vRealize Operations Manager virtual appliance exists.
- On all vRealize Operations Manager virtual appliances, verify that the vRealize Log Insight agent configuration, located in the `/var/lib/loginsight-agent/liagent.ini` file, contains `ssl=no`.

Procedure

1 Take the vRealize Operations Manager Nodes Offline and Take Snapshots

  Before you perform the upgrade of vRealize Operations Manager, take the nodes in the cluster offline and take a snapshot of each node. If you must perform a rollback of vRealize Operations Manager to the previous state, these snapshots accelerate the rollback operation.

2 Upgrade the Operating System on the vRealize Operations Manager Appliances

  When you upgrade both the vRealize Operation Manager analytics cluster and the region-specific remote collectors, start the process by first upgrading the operating system of the vRealize Operations Manager virtual appliances. You use the administration user interface on the vRealize Operations Manager master node to perform the operation.

3 Upgrade the vRealize Operations Manager Software

  After you upgrade the operating system on the vRealize Operations Manager virtual appliances, upgrade the software on the appliances.

4 Upgrade the Management Pack for NSX for vSphere in vRealize Operations Manager

  After you complete the upgrade of vRealize Operations Manager, upgrade the Management Pack for NSX for vSphere to ensure continuous interoperability. The remaining management packs included in the VMware Validated Design are pre-installed with vRealize Operations Manager.

5 Delete the Snapshots of the vRealize Operations Manager Virtual Appliances

After you complete the upgrade of vRealize Operations and verify operations and functionality, delete the virtual machine snapshots.

What to do next

- Verify that vRealize Operations Manager is operational 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 perform the upgrade of vRealize Operations Manager, take the nodes in the cluster offline and take a snapshot of each node. If you must perform a rollback of vRealize Operations Manager to the previous state, these snapshots accelerate the rollback operation.

Table 3-4. vRealize Operations Manager Virtual Machines

Region	Folder	Role	Virtual Machine Name
Region A	sfo01-m01fd-vrops	Master Node	vrops01svr01a
	sfo01-m01fd-vrops	Master Replica Node	vrops01svr01b
	sfo01-m01fd-vrops	Data Node 1	vrops01svr01c
	sfo01-m01fd-vrops	Data Node *X*	vrops01svr01*x* .rainpole.local Additional node that you have joined to your vRealize Operations Manager analytics cluster.
	sfo01-m01fd-vropsrc	Remote Collector 1	sfo01vropsc01a
	sfo01-m01fd-vropsrc	Remote Collector 2	sfo01vropsc01b
Region B	lax01-m01fd-vropsrc	Remote Collector 1	lax01vropsc01a
	lax01-m01fd-vropsrc	Remote Collector 2	lax01vropsc01b

Procedure

1 Log in to the vRealize Operations Manager administrator interface on the master node of your analytics cluster.

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

b Log in using the following credentials.

Setting	Value
User Name	admin
Password	*vrops_admin_password*

2 Take all vRealize Operations Manager nodes in the cluster offline.

   a In the **Navigator**, click **System Status**.

   b On the **System Status** page, under **Cluster Status** click **Take Offline**.

   c In the **Take Cluster Offline** dialog, enter **`VMware Validated Design 4.3 Operations Management Layer Upgrade`** in the **Reason** text box and click **OK**.

3 Wait until all vRealize Operations Manager nodes in the cluster are offline and the **Cluster Status** becomes `Offline`.

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

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

   b Log in using the following credentials.

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

5 Take a snapshot for each vRealize Operations Manager node.

   a From the **Home** menu, select **VMs and Templates**.

   b In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vrops** tree.

   c Right-click the **vrops01svr01a** virtual machine and select **Snapshots > Take Snapshot**.

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

Setting	Value
Name	VMware Validated Design 4.3 Operations Management Layer Upgrade
Description	-
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

   e Repeat these steps for the remaining vRealize Operations Manager nodes in Region A and Region B.

Upgrade the Operating System on the vRealize Operations Manager Appliances

When you upgrade both the vRealize Operation Manager analytics cluster and the region-specific remote collectors, start the process by first upgrading the operating system of the vRealize Operations Manager virtual appliances. You use the administration user interface on the vRealize Operations Manager master node to perform the operation.

Procedure

1. Log in to the administrator user interface on the vRealize Operations Manager master node.
   a. Open a Web browser and go to **`https://vrops01svr01a.rainpole.local/admin`**.
   b. Log in using the following credentials.

Setting	Value
User Name	admin
Password	*vrops_admin_password*

2. In the **Navigator**, click **Software Update** and, on the **Software Update** page, click **Install a Software Update** .
3. In the **Select Software Update** wizard, click **Browse** and locate `vRealize_Operations_Manager-VA-OS-6.7.0.`*`build_number`*`.pak` on the local file system.
4. Select **Install the PAK file even if it is already installed**, click **Upload** and click **Next**.
5. On the **End User License Agreement** page, select the **I accept the terms of this agreement** check box and click **Next**.
6. On the **Update Information** dialog, review the **Important Update and Release Information** and click **Next**.
7. On the **Install Software Update** page, click **Install**.
8. Wait until the operating system software update is completed.

   You are logged out from the administrator user interface of the master node while the software update process restarts each of the vRealize Operations Manager nodes included in the deployment.
9. After the operating system update process is complete, log back in to the administrator user interface on the master node and verify that the cluster status is `ONLINE` on the **Cluster Status** page.

Upgrade the vRealize Operations Manager Software

After you upgrade the operating system on the vRealize Operations Manager virtual appliances, upgrade the software on the appliances.

Procedure

1 Log in to the administrator user interface on the vRealize Operations Manager master node.

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

   b Log in using the following credentials.

Setting	Value
User Name	admin
Password	*vrops_admin_password*

2 Take all vRealize Operations Manager nodes in the cluster offline.

   a In the **Navigator**, click **System Status.**

   b On the **System Status** page, under **Cluster Status** click **Take Offline**.

   c In the **Take Cluster Offline** dialog, enter **`VMware Validated Design 4.3 Operations Management Layer Upgrade`** in the **Reason** text box and click **OK**.

3 Wait until all vRealize Operations Manager nodes in the cluster are offline and the **Cluster Status** becomes `Offline`.

4 Perform the upgrade of vRealize Operations Manager software.

   a In the **Navigator**, click **Software Update**.

   b On the **Software Update** page , click **Install a Software Update**.

   c On the **Select Software Update** page of the **Add Software Update** wizard, click **Browse** and locate `vRealize_Operations_Manager-VA-6.7.0.`*`build_number`*`.pak` on the local file system.

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

   e On the **End User License Agreement** page, select the **I accept the terms of this agreement** check box and click **Next**.

   f On the **Update Information** page, review the **Important Update and Release Information** and click **Next**.

   g On the **Install Software Update** page, click **Install**.

5 Wait until the update of the vRealize Operations Manager software is completed.

   You are logged out from the administrator user interface of the master node while the software update process restarts each of the vRealize Operations Manager nodes included in the deployment.

6 After the software update process is complete, log back in to the administrator user interface on the master node and verify that the cluster status is `Online` on the **Cluster Status** page.

7 Before you log in to the vRealize Operations Manager user interface, clear your browser cache to ensure that all objects in the vRealize Operations Manager user interface are displayed correctly.

Upgrade the Management Pack for NSX for vSphere in vRealize Operations Manager

After you complete the upgrade of vRealize Operations Manager, upgrade the Management Pack for NSX for vSphere to ensure continuous interoperability. The remaining management packs included in the VMware Validated Design are pre-installed with vRealize Operations Manager.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 Upgrade the Management Pack for NSX for vSphere.

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

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

   c On the **Solutions** page, click **Add**.

   d On the **Select a Solution** page, browse your file system and locate the `.pak` file of Management Pack for NSX for vSphere and click **Open**.

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

   f On the **End User Agreement** page, select the **I accept the terms of this agreement** check box and click **Next**.

   g After the upgrade is complete, click **Finish**.

3 Verify that the NSX for vSphere adapters are collecting metrics.

   a On the **Solutions** page, select **Management Pack for NSX-vSphere** from the solution table.

   b Under **Configured Adapter Instances**, verify that the **Collection State** is `Collecting` and the **Collection Status** is `Data receiving`.

Delete the Snapshots of the vRealize Operations Manager Virtual Appliances

After you complete the upgrade of vRealize Operations and verify operations and functionality, delete the virtual machine snapshots.

Table 3-5. vRealize Operations Manager Virtual Machines

Region	Folder	Role	Virtual Machine Name
Region A	sfo01-m01fd-vrops	Master Node	vrops01svr01a
	sfo01-m01fd-vrops	Master Replica Node	vrops01svr01b
	sfo01-m01fd-vrops	Data Node 1	vrops01svr01c
	sfo01-m01fd-vrops	Data Node *X*	vrops01svr01*x* .rainpole.local Additional node that you have joined to your vRealize Operations Manager analytics cluster.
	sfo01-m01fd-vropsrc	Remote Collector 1	sfo01vropsc01a
	sfo01-m01fd-vropsrc	Remote Collector 2	sfo01vropsc01b
Region B	lax01-m01fd-vropsrc	Remote Collector 1	lax01vropsc01a
	lax01-m01fd-vropsrc	Remote Collector 2	lax01vropsc01b

Procedure

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

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

   b Log in using the following credentials.

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

2 In the **Navigator**, click **VMs and Templates** and expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vrops** tree.

3 Right-click the **vrops01svr01a** virtual machine and select **Snapshots > Manage Snapshots**.

4 In the **Snapshot Manager**, click the snapshot that you created before the vRealize Operations Manager upgrade and select **Delete**.

5 Click **Yes** in the confirmation dialog box and click **Close** in **Snapshot Manager**.

6 Repeat the procedure on the remaining vRealize Operations virtual machines.

Upgrade vRealize Log Insight

After you complete the upgrade and post-upgrade configurations for vRealize Operations Manager, continue the operations management layer upgrade with the vRealize Log Insight clusters and agents in each region. Post-upgrade, you perform additional configurations so that the environment remains in alignment with the design.

When you upgrade the vRealize Log Insght clusters in Region A and Region B in the design, you perform the upgrade manually using the master node in each vRealize Log Insight cluster. The remaining worker nodes are updated automatically.

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

After you upgrade the vRealize Log Insight virtual appliances and agents, upgrade each of the installed content packs.

Table 3-7. vRealize Log Insight Nodes in the SDDC

Region	Role	IP Address	FQDN
Region A	Integrated Load Balancer VIP	192.168.31.10	sfo01vrli01.sfo01.rainpole.local
	Master Node	192.168.31.11	sfo01vrli01a.sfo01.rainpole.local
	Worker Node 1	192.168.31.12	sfo01vrli01b.sfo01.rainpole.local
	Worker Node 2	192.168.31.13	sfo01vrli01c.sfo01.rainpole.local
	Worker Node x	192.168.31.x	sfo01vrli01x.sfo01.rainpole.local
Region B	Integrated Load Balancer VIP	192.168.32.10	lax01vrli01.lax01.rainpole.local
	Master Node	192.168.32.11	lax01vrli01a.lax01.rainpole.local
	Worker Node 1	192.168.32.12	lax01vrli01b.lax01.rainpole.local
	Worker Node 2	192.168.32.13	lax01vrli01c.lax01.rainpole.local
	Worker Node x	192.168.32.x	lax01vrli01x.lax01.rainpole.local

Prerequisites

- Download the product upgrade `.pak` files of vRealize Log Insight to a Windows host that has access to the environment.

  Table 3-6. PAK Files Required for vRealize Log Insight Upgrade

PAK Type	PAK File
Software Update `.pak` file	VMware-vRealize-Log-Insight-4.6.0-*build_version*.pak

- Verify that you have a user account that has the **Edit Admin** permission for the vRealize Log Insight Web interface.
- Verify that a current backup of each vRealize Log Insight virtual appliance exists.

Procedure

1 Upgrade vRealize Log Insight in Region A

  When you continue the upgrade the Operations Layer as a part of the upgrade to this VMware Validated Design release, start with the vRealize Log in Region A.

2 Upgrade vRealize Log Insight in Region B

  After you complete the upgrade the of vRealize Log Insight cluster in Region A, return to the previous procedures and continue the upgrade of the vRealize Log cluster in Region B.

3 Post-Upgrade Configuration of the vRealize Log Insight

After you upgrade vRealize Log Insight 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 is operational after the upgrade.

Upgrade vRealize Log Insight in Region A

When you continue the upgrade the Operations Layer as a part of the upgrade to this VMware Validated Design release, start with the vRealize Log in Region A.

Procedure

1 Take Snapshots of the vRealize Log Insight Appliances in Region A

Before you perform the upgrade of vRealize Log Insight, take a snapshot of each virtual machine in the environment. If you must perform a rollback of vRealize Log Insight to the previous state, these snapshots accelerate the rollback operation.

2 Upgrade the vRealize Log Insight Cluster in Region A

When you upgrade the vRealize Log Insight in Region A, use the user interface on the vRealize Log Insight master node to perform the operation. You perform the upgrade on the first node. The other nodes are automatically upgraded.

3 Upgrade the Content Packs on vRealize Log Insight in Region A

After you upgrade the vRealize Log Insight cluster, upgrade the vRealize Log Insight content packs in the environment to take advantage of the latest content pack features while monitoring the environment.

4 Upgrade the vRealize Log Insight Agents on the Windows Nodes in Region A

After you upgrade the vRealize Log Insight cluster, upgrade the vRealize Log Insight agents on the Windows virtual machines in the environment to take advantage of the latest features. In this design, these agents run on the vRealize Automation IaaS components along with Site Recovery Manager in Region A.

5 Delete the Snapshots of the vRealize Log Insight Virtual Appliances

After you complete the upgrade of vRealize Log Insight and verify operations and functionality, delete the virtual machine snapshots.

Take Snapshots of the vRealize Log Insight Appliances in Region A

Before you perform the upgrade of vRealize Log Insight, take a snapshot of each virtual machine in the environment. If you must perform a rollback of vRealize Log Insight to the previous state, these snapshots accelerate the rollback operation.

Table 3-8. vRealize Log Insight Virtual Machines

Region	Folder	Role	Virtual Machine Name
Region A	sfo01-m01fd-vrli	Master Node	sfo01vrli01a
	sfo01-m01fd-vrli	Worker Node 1	sfo01vrli01b
	sfo01-m01fd-vrli	Worker Node 2	sfo01vrli01c

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** menu, click **VMs and Templates**.

3 In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vrli** tree.

4 Right-click the **sfo01vrli01a** virtual machine and select **Snapshot > Take Snapshot**.

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

Setting	Value
Name	VMware Validated Design 4.3 Operations Management Layer Upgrade
Description	-
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

6 Repeat these steps for the remaining virtual machines in the Region A vRealize Log Insight cluster..

7 Take a snapshot of each node in the cluster.

Upgrade the vRealize Log Insight Cluster in Region A

When you upgrade the vRealize Log Insight in Region A, use the user interface on the vRealize Log Insight master node to perform the operation. You perform the upgrade on the first node. The other nodes are automatically upgraded.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://sfo01vrli01a.sfo01.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**.

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 node.

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 the remaining nodes in the cluster starts automatically.

   After the upgrade process for the cluster completes, the Integrated Load Balancer comes online and display as `Availabile`.

Upgrade the Content Packs on vRealize Log Insight in Region A

After you upgrade the vRealize Log Insight cluster, upgrade the vRealize Log Insight content packs in the environment to take advantage of the latest content pack features while monitoring the environment.

Using the Content Pack Marketplace in vRealize Log Insight, you download the latest content packs for the vRealize Log Insight cluster.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://sfo01vrli01.sfo01.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 **Content Pack**.

3 In the **Content Pack** pane, under **Content Pack Market Place**, click **Updates**.

4 In the **Log Insight Content Pack Marketplace** pane, click **Update All** to upgrade all content packs to the latest version.

5 After you upgrade the content packs, click each of the items under **Installed Content Packs** and verify that the `Version` number of each content pack matches the version for this validated design.

Upgrade the vRealize Log Insight Agents on the Windows Nodes in Region A

After you upgrade the vRealize Log Insight cluster, upgrade the vRealize Log Insight agents on the Windows virtual machines in the environment to take advantage of the latest features. In this design, these agents run on the vRealize Automation IaaS components along with Site Recovery Manager in Region A.

You download the latest agents from the vRealize Log Insight cluster and upgrade the agent on the vRealize Automation IaaS servers, Microsoft SQL Server and Site Reocovery Manager Server in Region A.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://sfo01vrli01.sfo01.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** link

5 In the **Download Log Insight Agent Version 4.6.0** dialog box, download the following vRealize Log Insight Agent files on the Windows host that you use to access the environment

Setting	Value
Download location	**`https://sfo01vrli01.sfo01.rainpole.local`**
Agent version	Windows MSI (32-bit/64-bit)
Save As	`VMware-Log-Insight-Agent-4.6.0-`*`build_number_Region_A_vRealize_Log_Insight_VIP_address`*`.msi`

6 Upgrade the vRealize Log Insight Agents for Windows.

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

SDDC Layer	Role	Fully Qualified Domain Name
Cloud Management	vRealize Automation IaaS Web Server	vra01iws01a.rainpole.local
		vra01iws01b.rainpole.local
	vRealize Automation IaaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local
		vra01ims01b.rainpole.local
	vRealize Automation IaaS DEM Worker	vra01dem01a.rainpole.local
		vra01dem01b.rainpole.local
	vRealize Automation IaaS Proxy Agent	sfo01ias01a.sfo01.rainpole.local
		sfo01ias01b.sfo01.rainpole.local
	Microsoft SQL Server	vra01mssql01.rainpole.local
Business Continuity	Site Recovery Manager	sfo01m01srm01.sfo01.rainpole.local

b Log in using the following credentials.

Setting	Value
User name	rainpole\svc-vra
Password	*svc-vra_user_password*

c Copy the `VMware-Log-Insight-Agent-4.6.0-`*`build_number_Region_A_vRealize_Log_Insight_VIP_address`*`.msi` file from the Windows host to the vRealize Automation Windows virtual machine in Region A.

d Open an administrative command prompt window, and navigate to the directory to where you saved the `.msi` file.

e Run the following command to install the vRealize Log Insight agent with custom values.

```
VMware-Log-Insight-Agent-4.6.0-build_number_192.168.31.10.msi SERVERPORT=9000 AUTOUPDATE=yes
LIAGENT_SSL=no
```

f In the **VMware vRealize Log Insight Agent Setup** wizard, accept the license agreement and click **Next**.

g With the Log Insight host name sfo01vrli01.sfo01.rainpole.local shown in the **Host** text box, click **Install**.

h When the installation is complete, click **Finish**.

i Repeat the steps on the remaining vRealize Automation IaaS virtual machines.

j Once the vRealize Automation IaaS components have been upgrade, repeat this process on the Site Recovery Manager virtual machine using the following credentials to log in.

Settings	Value
User name	Windows administrator user
Password	*windows_administrator_password*

7 After you upgrade the vRealize Log Insight agents for Region A, verify that the agent version in the vRealize Log Insight cluster is `4.6.0.xxxxxxx`.

a Open a Web browser and go to **`https://sfo01vrli01.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 On the **Agents** page, verify that the **Version** column shows `4.6.0.xxxxxxx`.

Delete the Snapshots of the vRealize Log Insight Virtual Appliances

After you complete the upgrade of vRealize Log Insight and verify operations and functionality, delete the virtual machine snapshots.

Table 3-9. vRealize Log Insight Virtual Machines

Region	Folder	Role	Virtual Machine Name
Region A	sfo01-m01fd-vrli	Master Node	sfo01vrli01a
	sfo01-m01fd-vrli	Worker Node 1	sfo01vrli01b
	sfo01-m01fd-vrli	Worker Node 2	sfo01vrli01c
Region B	lax01-m01fd-vrli	Master Node	lax01vrli01a
	lax01-m01fd-vrli	Worker Node 1	lax01vrli01b
	lax01-m01fd-vrli	Worker Node 2	lax01vrli01c

Procedure

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

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

   b Log in using the following credentials.

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

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

3 In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01fd-vrli** tree.

4 Right-click the **sfo01vrli01a** virtual machine and select **Manage Snapshots**.

5 On the **Snapshots** tab, click the snapshot that you created before the vRealize Log Insight upgrade and select **Delete**.

6 Click **Yes** in the confirmation dialog box and click **Close**.

7 Repeat the procedure on the remaining virtual machines in the Region A vRealize Log Insight cluster.

8 Repeat the procedure on the virtual machines in the Region B vRealize Log Insight cluster under the lax01m01vc01.lax01.rainpole.local vCenter Server.

Upgrade vRealize Log Insight in Region B

After you complete the upgrade the of vRealize Log Insight cluster in Region A, return to the previous procedures and continue the upgrade of the vRealize Log cluster in Region B.

Procedure

1 Take snapshots of the vRealize Log Insight virtual machines.

   Repeat Take Snapshots of the vRealize Log Insight Appliances in Region A in Region B by using the following details:

Table 3-10. vRealize Log Insight Virtual Machines in Region B

vCenter Server	Folder	Role	Virtual Machine Name
lax01m01vc01.lax01.rainpole.local	lax01-m01fd-vrli	Master Node	lax01vrli01a
	lax01-m01fd-vrli	Worker Node 1	lax01vrli01b
	lax01-m01fd-vrli	Worker Node 2	lax01vrli01c

2 Upgrade the vRealize Log Insight cluster.

   Repeat Upgrade the vRealize Log Insight Cluster in Region A in Region B at **`https://lax01vrli01a.lax01.rainpole.local`**.

3 Upgrade the content packs on the vRealize Log Insight cluster.

Repeat Upgrade the Content Packs on vRealize Log Insight in Region A in Region B at **`https://lax01vrli01a.lax01.rainpole.local`**.

4 Upgrade the vRealize Log Insight agents on the Windows Nodes.

Repeat Upgrade the vRealize Log Insight Agents on the Windows Nodes in Region A by using the following settings:

Table 3-11. MSI File of the vRealize Log Insight Agent for the Windows Nodes in Region B

Setting	Value
Download location	**`https://lax01vrli01.lax01.rainpole.local`**
Agent version	Windows MSI (32-bit/64-bit)
Save As	`VMware-Log-Insight-Agent-4.6.0-`*`build_number_Region_B_vRealize_Log_Insight_VIP_address`*`.msi`

Table 3-12. Windows Nodes to Update the Log Insight Agent On in Region B

SDDC Layer	Role	Fully Qualified Domain Name
Cloud Management	vRealize Automation Iaas Proxy Agent	lax01ias01a.lax01.rainpole.local
		lax01ias01b.lax01.rainpole.local
Business Continuity	Site Recovery Manager	lax01m01srm01.lax01.rainpole.local

Use the following command to update the agent on the IaaS or Site Recovery Manager virtual machine.

```
VMware-Log-Insight-Agent-4.6.0-build_number_192.168.32.10.msi SERVERPORT=9000 AUTOUPDATE=yes
LIAGENT_SSL=no
```

Post-Upgrade Configuration of the vRealize Log Insight

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

Procedure

1 Install Content Pack for vRealize Business in Region A

Install the vRealize Business for Cloud content pack to add the dashboards for viewing new log information about the Cloud Management Platform in vRealize Log Insight in Region A.

2 Install Content Pack for vRealize Business in Region B

Install the vRealize Business for Cloud content pack to add the dashboards for viewing new log information about the Cloud Management Platform in vRealize Log Insight in Region B.

3 Update the Content Pack for vRealize Operations Manager

With the latest version of vRealize Operations Manager's Log Insight Content Pack solution, you must clean up the old Agent Group and Content Pack, clean up the Agent Configuration on the vRealize Operation Manager Analytics and Remote Collector nodes, then apply the new configuring to the the vRealize Log Insight Agents on the nodes.

Install Content Pack for vRealize Business in Region A

Install the vRealize Business for Cloud content pack to add the dashboards for viewing new log information about the Cloud Management Platform in vRealize Log Insight in Region A.

Procedure

1 Log in to the vRealize Log Insight user interface.

a Open a Web browser and go to **`https://sfo01vrli01.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 **VMware - vRealize Business for Cloud** content pack and click its icon.

5 In the **Install Content Pack** dialog box, select the **I accept the terms of any licensing agreement** check box and click **Install**.

6 After the installation is completed, click **OK** in the **VMware - vRealize Business for Cloud Setup Instruction** dialog box.

After the installation is complete, the VMware - vRealize Business for Cloud content pack appears in the **Installed Content Packs** list on the left.

On the **Dashboards** page of vRealize Log Insight, new dashboards reporting on vRealize Business for Cloud appear.

Install Content Pack for vRealize Business in Region B

Install the vRealize Business for Cloud content pack to add the dashboards for viewing new log information about the Cloud Management Platform in vRealize Log Insight in Region B.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://lax01vrli01.lax01.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 **VMware - vRealize Business for Cloud** content pack and click its icon.

5 In the **Install Content Pack** dialog box, select the **I accept the terms of any licensing agreement** check box and click **Install**.

6 After the installation is complete, click **OK** in the **VMware - vRealize Business for Cloud Setup Instruction** dialog box.

After the installation is complete, the VMware - vRealize Business for Cloud content pack appears in the **Installed Content Packs** list on the left.

On the **Dashboards** page of vRealize Log Insight, new dashboards reporting on vRealize Business for Cloud appear.

Update the Content Pack for vRealize Operations Manager

With the latest version of vRealize Operations Manager's Log Insight Content Pack solution, you must clean up the old Agent Group and Content Pack, clean up the Agent Configuration on the vRealize Operation Manager Analytics and Remote Collector nodes, then apply the new configuring to the the vRealize Log Insight Agents on the nodes.

Procedure

1 Clean Up the Agent Group and Content Pack for vRealize Operations Manager

   Clean up the old agent group and content packs in vRealize Log Insight in preparation to apply the new vRealize Operations Manager solution.

2 Clean Up Log Insight Agent Configuration on the vRealize Operations Manager Analytics Cluster

   Before you install the new content pack for vRealize Operations Manager, clean up the old agent configuration that is saved on the analytics nodes.

3 Configure the Log Insight Agent on the Analytics Cluster to Forward Log Events to vRealize Log Insight in Region A

After you clean up the old vRealize Log Insight Agent configuration on vRealize Operations Manager, reconfigure the Log Insight agent on vRealize Operations Manager to send audit logs and system events to vRealize Log Insight.

4 Configure the Log Insight Agent on the Remote Collectors to Forward Log Events to vRealize Log Insight in Region A and Region B

After you configure the Log Insight agent on the analytics cluster of vRealize Operations Manager to send audit logs and system events to vRealize Log Insight, configure the remote collectors to send audit logs and system events to vRealize Log Insight.

Clean Up the Agent Group and Content Pack for vRealize Operations Manager

Clean up the old agent group and content packs in vRealize Log Insight in preparation to apply the new vRealize Operations Manager solution.

Procedure

1 Open the vRealize Log Insight user interface.

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

Region	vRealize Log Insight URL
Region A	`https://sfo01vrli01.sfo01.rainpole.local`
Region B	`https://lax01vrli01.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 From the drop-down menu at the top, point to the **vRops6 - Agent Group** from the **Active Groups** section and click the delete icon.

5 In the **Delete Agent Group** dialog box, click **Delete**.

6 In the vRealize Log Insight user interface, click the configuration drop-down menu icon and select **Content Packs**.

7 In the **Installed Content Packs** area on the left, click **VMware - vRops 6.x**.

8 In the central pane, click the gear icon, and from the drop-down menu, select **Uninstall**.

9 In the **Uninstall Content Pack** dialog box, click **Uninstall**.

10 After the uninstallation is complete, repeat this operation on vRealize Log Insight in Region B, lax01vrli01.lax01.rainpole.local.

Clean Up Log Insight Agent Configuration on the vRealize Operations Manager Analytics Cluster

Before you install the new content pack for vRealize Operations Manager, clean up the old agent configuration that is saved on the analytics nodes.

After you clean up the active agent group and content pack for the earlier version of vRealize Operations Manager, delete the agent configuration on the analytics cluster.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

3 Expand **Management** and click **Log Forwarding**.

4 Deselect **Output logs to external log server** and click **Apply Changes**.

   Most the vRealize Log Insight agent configuration settings are cleaned up. However, if you have upgraded over multiple release of the VMware Validated Design, additional items might persist. Clean up these items too.

5 Clean up any persistent configuration items in the Log Insight agent in vRealize Operations Manager Analytics nodes.

6 Open an SSH connection to the vRealize Operations Manager node using the following settings.

Setting	Value
Host name	■ vrops01svr01a.rainpole.local ■ vrops01svr01b.rainpole.local ■ vrops01svr01c.rainpole.local
User name	root
Password	*vrops_root_password*

7 Edit the `liagent.ini` file on each vRealize Operations Manager node using a text editor such as `vi`.

```
vi /var/lib/loginsight-agent/liagent.ini
```

8 Locate the [logging] section, and locate and remove any of following values.

```
[logging]
...
[filelog|ADAPTER-vmwareadapter]
tags = {"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_logtype":"ADAPTER",
"vmw_vr_ops_clustername":"vrops01svr01", "vmw_vr_ops_clusterrole":"Replica",
"vmw_vr_ops_nodename":"vrops01svr01b", "vmw_vr_ops_hostname":"vrops01svr01b.rainpole.local"}
include = *.log*
event_marker = ^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}
exclude_fields = hostname
directory = /data/vcops/log/adapters/VMwareAdapter

[filelog|ADAPTER-openapiadapter]
event_marker = ^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}
include = *.log*
tags = {"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_logtype":"ADAPTER",
"vmw_vr_ops_clustername":"vrops01svr01", "vmw_vr_ops_clusterrole":"Replica",
"vmw_vr_ops_nodename":"vrops01svr01b", "vmw_vr_ops_hostname":"vrops01svr01b.rainpole.local"}
directory = /data/vcops/log/adapters/OpenAPIAdapter
exclude_fields = hostname

[filelog|ADAPTER-vcopsadapter]
event_marker = ^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}
directory = /data/vcops/log/adapters/VCOpsAdapter
include = *.log*
exclude_fields = hostname
tags = {"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_logtype":"ADAPTER",
"vmw_vr_ops_clustername":"vrops01svr01", "vmw_vr_ops_clusterrole":"Replica",
"vmw_vr_ops_nodename":"vrops01svr01b", "vmw_vr_ops_hostname":"vrops01svr01b.rainpole.local"}
...
```

After you clean up any of the legacy items in the [logging] section, you have the agent's default configuration.

```
[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
hostname = sfo01vrli01.rainpole.local

; Set protocol to use:
; cfapi - Log Insight REST API
; syslog - Syslog protocol
; If omitted the default value is cfapi
proto = cfapi

; Log Insight server port to connect to. If omitted the default value is:
; for syslog: 512
; for cfapi without ssl: 9000
; for cfapi with ssl: 9543
port = 9000

; ssl - enable/disable SSL. Applies to cfapi protocol only.
; Possible values are yes or no. If omitted the default value is no.
```

```
ssl = no

; Time in minutes to force reconnection to the server
; If omitted the default value is 30
; reconnect=30

ssl_ca_path =
[storage]
; max_disk_buffer - max disk usage limit (data + logs) in MB:
; 100 - 2000 MB, default 200
; max_disk_buffer=200

[logging]
; debug_level - the level of debug messages to enable:
; 0 - no debug messages
; 1 - trace essential debug messages
; 2 - verbose debug messages (will have negative impact on performace)
; debug_level=0

[filelog|messages]
directory = /var/log
include = messages;messages.?

[filelog|syslog]
directory = /var/log
include = syslog;syslog.?

[update]
; Do not change this parameter
package_type = rpm

[common|global]
tags = {"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_clustername":"vrops01svr01arainpolelocal",
"vmw_vr_ops_clusterrole":"MASTER", "vmw_vr_ops_hostname":"vrops01svr01a.rainpole.local",
"vmw_vr_ops_nodename":"vrops01svr01a.rainpole.local"}
```

9 Press Escape and enter **`:wq!`** to save the file.

10 Repeat Step 6 to #unique_91/unique_91_Connect_42_substep_4422B385967A4F06981021282121C6B1 for the remaining analytics nodes.

Configure the Log Insight Agent on the Analytics Cluster to Forward Log Events to vRealize Log Insight in Region A

After you clean up the old vRealize Log Insight Agent configuration on vRealize Operations Manager, reconfigure the Log Insight agent on vRealize Operations Manager to send audit logs and system events to vRealize Log Insight.

Procedure

1 Log in to vRealize Operations Manager by using the operations interface.

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

3 Expand **Management** and click **Log Forwarding**.

4 Enter the following information and click **Apply Changes**.

Setting	Value
Output logs to external log server	Selected
Forwarded Logs	Selected
Log Insight Servers	sfo01vrli01.sfo01.rainpole.local
Host	sfo01vrli01.sfo01.rainpole.local
Port	9000
Use SSL	Deselected
Certificate Path	
Protocol	cfapi

All **VMware - vRops** dashboards become available on the home page of vRealize Log Insight. You see the **Total number of vRops Clusters** showing 1 and **Total number of vRops nodes over time** showing the host names of the vRealize Operations Manager Analytics nodes.

Configure the Log Insight Agent on the Remote Collectors to Forward Log Events to vRealize Log Insight in Region A and Region B

After you configure the Log Insight agent on the analytics cluster of vRealize Operations Manager to send audit logs and system events to vRealize Log Insight, configure the remote collectors to send audit logs and system events to vRealize Log Insight.

You must manually configure the remote collectors of vRealize Operations Manager with the new vRealize Log Insight settings to capture the latest audit logs and system events. You remove all obsolete `[filelog|*]` sections that are related to vRealize Operations Manager, and insert new `[filelog|*]` items. See VMware Knowledge Base article 55061.

Procedure

1 Open an SSH connection to the remote collector of vRealize Operations Manager using the following settings.

Setting	Value
Host name	■ sfo01vropsc01a.sfo01.rainpole.local ■ sfo01vropsc01b.sfo01.rainpole.local
Host name	■ lax01vropsc01a.lax01.rainpole.local ■ lax01vropsc01b.lax01.rainpole.local
User name	root
Password	*vrops_root_password*

2 Configure the Log Insight agent in the remote collector nodes of vRealize Operations Manager.

a Edit the `liagent.ini` file on each vRealize Operations Manager node using a text editor such as `vi`.

```
vi /var/lib/loginsight-agent/liagent.ini
```

b Locate the `[logging]` section, and delete all lines after `[filelog|syslog]` using the command **dG**.

The **dG** command deletes all lines after the line selected. After the command is complete, the `liagent.ini` file has the following contents:

```
[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
hostname=sfo01vrli01.rainpole.local

; Set protocol to use:
; cfapi - Log Insight REST API
; syslog - Syslog protocol
; If omitted the default value is cfapi
proto=cfapi

; Log Insight server port to connect to. If omitted the default value is:
; for syslog: 512
; for cfapi without ssl: 9000
; for cfapi with ssl: 9543
port=9000

;ssl - enable/disable SSL. Applies to cfapi protocol only.
; Possible values are yes or no. If omitted the default value is no.
ssl=no

; Time in minutes to force reconnection to the server
; If omitted the default value is 30
;reconnect=30

[storage]
;max_disk_buffer - max disk usage limit (data + logs) in MB:
; 100 - 2000 MB, default 200
;max_disk_buffer=200

[logging]
;debug_level - the level of debug messages to enable:
; 0 - no debug messages
; 1 - trace essential debug messages
; 2 - verbose debug messages (will have negative impact on performace)
;debug_level=0

[filelog|messages]
directory=/var/log
include=messages;messages.?
```

```
[filelog|syslog]
directory=/var/log
include=syslog;syslog.?

<Deleted from here down>
```

c After the `[filelog|syslog]` section, add the following block on each remote collector node.

```
[common|global]
tags={"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_clustername":"vrops01svr01arainpolelocal",
"vmw_vr_ops_clusterrole":"Remote Collector",
"vmw_vr_ops_nodename":"<Your vROPS Node Name Here>",
"vmw_vr_ops_hostname":"<Your vROPS Hostname Here>"}

[update]
; Do not change this parameter
package_type=rpm
```

d Modify the following parameters specifically for each node.

Parameter	Description	Location in liagent.ini
vmw_vr_ops_nodename	IP address or FQDN of the vRealize Operations Manager node	Replace each `<Your VROPS Node Name Here>` with the following names: ■ sfo01vropsc01a ■ sfo01vropsc01b
vmw_vr_ops_hostname	Name of the vRealize Operations Manager node that is set during node initial configuration	Replace each `<Your VROPS Hostname Here>` with the following names: ■ sfo01vropsc01a.sfo01.rainpole.local ■ sfo01vropsc01b.sfo01.rainpole.local

For example, on the first remote collector, you change the `[common|global]` section to add a context to the logs that are sent to the vRealize Log Insight cluster:

```
[common|filelog]
tags={"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_clustername":"vrops01svr01arainpolelocal",
"vmw_vr_ops_clusterrole":"Remote Collector", "vmw_vr_ops_nodename":"sfo01vropsc01a",
"vmw_vr_ops_hostname":"sfo01vropsc01a.sfo01.rainpole.local"}

[update]
; Do not change this parameter
package_type=rpm
```

e After the [common|global] section, add the following block on the remote collector.

```
[filelog|COLLECTOR]
event_marker = ^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}
directory = /usr/lib/vmware-vcops/user/log
include = collector*.log*
tags = {"vmw_vr_ops_logtype":"COLLECTOR"}
exclude = collector-wrapper.log*;collector-gc*.log*

[filelog|COLLECTOR-GC]
include = collector-gc-*.log*
directory = /usr/lib/vmware-vcops/user/log
event_marker = ^\d{4}-\d{2}-\d{2}
tags = {"vmw_vr_ops_logtype":"COLLECTOR"}

[filelog|COLLECTOR_wrapper]
tags = {"vmw_vr_ops_logtype":"COLLECTOR"}
directory = /usr/lib/vmware-vcops/user/log
include = collector-wrapper.log*
event_marker = ^[DEBUG|ERROR|FATAL|INFO|TRACE|WARN|STATUS ]

[filelog|ADAPTERS]
include = *.log*
event_marker = ^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}
tags = {"vmw_vr_ops_logtype":"ADAPTER"}
directory = /data/vcops/log/adapters/*

[filelog|SUITEAPI]
include = api.log*;http_api.log*;profiling_api.log*;api-gc.log*
event_marker = ^\d{4}-\d{2}-\d{2}
tags = {"vmw_vr_ops_logtype":"SUITEAPI"}
directory = /usr/lib/vmware-vcops/user/log

[filelog|SUITEAPI-api]
directory = /usr/lib/vmware-vcops/user/log/suite-api
tags = {"vmw_vr_ops_logtype":"SUITEAPI"}
event_marker = ^\d{2}-\w{3}-\d{4}[\s]\d{2}:\d{2}:\d{2}\.\d{3}
include = catalina*.log*;localhost*.log*

[filelog|ADMIN_UI-casa-catalina]
event_marker = ^\w{3}[\s]\d{1,}
directory = /usr/lib/vmware-vcops/user/log/casa
tags = {"vmw_vr_ops_logtype":"ADMIN_UI"}
include = catalina.out

[filelog|ADMIN_UI-casa]
directory = /usr/lib/vmware-vcops/user/log/casa
tags = {"vmw_vr_ops_logtype":"ADMIN_UI"}
include = *.log*
event_marker = ^\d{4}-\d{2}-\d{2}
exclude = catalina*;localhost*

[filelog|ADMIN_UI-casa-catalina-log-localhost-log]
include = catalina.*.log;localhost.*.log
exclude = localhost_access_log.*
```

```
tags = {"vmw_vr_ops_logtype":"ADMIN_UI"}
event_marker = ^\d{2}-\w{3}-\d{4}[\s]
directory = /usr/lib/vmware-vcops/user/log/casa

[filelog|ADMIN_UI-localhost_access]
directory = /usr/lib/vmware-vcops/user/log/casa
include = localhost_access_log.*
tags = {"vmw_vr_ops_logtype":"ADMIN_UI"}

[filelog|TOMCAT_WEBAPP]
tags = {"vmw_vr_ops_logtype":"TOMCAT_WEBAPP"}
include = localhost_access_log.*.txt
directory = /data/vcops/log/product-ui

[filelog|CALL_STACK]
event_marker = ^[^\s]
tags = {"vmw_vr_ops_logtype":"CALL_STACK"}
include = collector*.txt
directory = /usr/lib/vmware-vcops/user/log/callstack

[filelog|GEMFIRE]
event_marker = ^\d{4}-\d{2}-\d{2}
include = gemfire*.log*
tags = {"vmw_vr_ops_logtype":"GEMFIRE"}
directory = /usr/lib/vmware-vcops/user/log

[filelog|GEMFIRE-2]
tags = {"vmw_vr_ops_logtype":"GEMFIRE"}
directory = /usr/lib/vmware-vcops/user/log
include = gemfire-locator*.log;gemfire_vRealize*.log
event_marker = ^\[
exclude = *.marker;*.gfs;*wrapper.log*;gemfire-wrapper.log*

[filelog|OTHER-watchdog-log]
directory = /usr/lib/vmware-vcops/user/log/vcops-watchdog
tags = {"vmw_vr_ops_logtype":"OTHER"}
event_marker = ^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}
include = vcops-watchdog*.log

[filelog|OTHER-misc]
directory = /usr/lib/vmware-vcops/user/log
event_marker = ^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}
include = system-exit-*.log;zeroTimestampLogger-
*.log;vcopsConfigureRoles.log*;cassandradbupgrade.log;centralsqldbupgrade.log;dbupgrade.log;res
tartHttpd.log;activate_web_certificate.log;oom-handler-
cassandra.log;ip_version_configurator_*.log;upgradeVsutilitiesConfigs.py.log;hisdbupgrade.log;i
nstaller-tools.log;his-lock-trace-*.log;actions-data-*.log;LRUCacheProfiler-*.log*;datapurging-
*.log.*;setVSUtilitiesPermissions.py.log;hafailover-*.log;deletedMetricKeys-*.log;placement-
*.log;bm-controller.log;cassandraquery-*.log;cassandradriver-*.log;shardingManager-*.log;fsdb-
accessor-*.log;actionScheduler-*.log;casa.audit*.log*;function-invocation-counter-
*.log;onlineCapacity-*.log;functioncalls-*.log;opsapi.audit*.log*;distributed*.log*
tags = {"vmw_vr_ops_logtype":"OTHER"}

[filelog|OTHER-misc-singlelines]
include = evn-checker.log*;delete_tomcat_logs.log;tomcat-enterprise-wrapper.log;meta-
```

```
gemfire*.log*;ui-gc.log.*
tags = {"vmw_vr_ops_logtype":"OTHER"}
directory = /usr/lib/vmware-vcops/user/log

[filelog|OTHER-TELEMETRY]
include = telemetry.log*
directory = /usr/lib/vmware-vcops/user/log
event_marker = ^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}
tags = {"vmw_vr_ops_logtype":"TELEMETRY"}
```

Note Ensure that there are no extra carriage returns after a long line. Each `[]` section must be in a *value* = *value* format, for example, `tags = {"something"}`. Make sure the `[filelog|OTHER-misc]` section is included.

f Press Escape and enter **`:wq!`** to save the file.

g Restart the Log Insight agent on the node by running the following console command.

```
/etc/init.d/liagentd restart
```

h Verify that the Log Insight agent is running.

```
/etc/init.d/liagentd status
```

i Repeat the steps for the second remote collector node.

3 Repeat the steps for the remote collectors in Region B.

All **VMware - vRops** dashboards become available on the home page of vRealize Log Insight. You see the **Total number of vRops Clusters** showing 1 and **Total number of vRops nodes over time** showing the host names of the analytics and remote collector nodes of vRealize Operations Manager.

Deploy and Configure vRealize Suite Lifecycle Manager Post-Upgrade

After you complete the upgrade and post-upgrade configurations for vRealize Operations and vRealize Log Insight in the operations management layer, you deploy and configure vRealize Suite Lifecycle Manager. vRealize Suite Lifecycle Manager automates the lifecycle management and drift analysis of the VMware vRealize Suite solutions in VMware Validated Design for simplified operational experience.

Prerequisites

Table 3-13. Prerequisites for the Deployment of vRealize Suite Lifecycle Manager

Requirement	Value
IP Address	192.168.11.20
FQDN	vrslcm01svr01a.rainpole.local

Table 3-13. Prerequisites for the Deployment of vRealize Suite Lifecycle Manager (Continued)

Requirement	Value
Required storage	■ Virtual disk provisioning ■ Thin ■ Required storage: 135 GB
Application virtual network	xRegion01-VXLAN
Installation Package	Download the `.ova` file of the vRealize Suite Lifecycle Manager virtual appliance from My VMware to a Windows host that has access to the environment. See *VMware Validated Design Release Notes* for the version for this VMware Validated Design.
License	Verify that you have obtained a vRealize Suite license with a quantity that fulfills the requirements of this design.
Active Directory	Verify that you have a parent active directory with the following service accounts configured for the rainpole.local domain. ■ **svc-vrslcm-vsphere**
Certificate authority	■ Root Active Directory domain controller as a certificate authority for the environment. ■ CA-signed certificate for the vRealize Suite Lifecycle Manager that is generated by using the VMware Validated Design Certificate Generation Utility (`CertGenVVD`). See the *VMware Validated Design Planning and Preparation* documentation.
My VMware Account	My VMware account with permissions to view licenses and download products.

Procedure

1 Configure User Access in vSphere for Integration with vRealize Suite Lifecycle Manager in Region A

Configure an operations service account with the required permissions to enable vRealize Suite Lifecycle Manager to deploy and manage the vRealize Suite components of the Software-Defined Data Center (SDDC) on the Management vCenter Server.

2 Configure the Distributed Firewall for vRealize Suite Lifecycle Manager in Region A

Add vRealize Suite Lifecycle Manager to the distributed firewall in Region A to allow traffic to the user interface of this solution. Using a distributed firewall with your SDDC increases the security level of your environment by allowing only the network traffic that is required for the SDDC to run.

3 Deploy the vRealize Suite Lifecycle Manager Appliance in Region A

You deploy the vRealize Suite Lifecycle Manager appliance and configure storage, networking, and other key appliance attributes.

4 Configure the vRealize Suite Lifecycle Manager Appliance in Region A

You configure the vRealize Suite Lifecycle Manager appliance system settings, generate the certificate for product deployments, replace the appliance certificate, and configure NTP settings.

5 Register vRealize Suite Lifecycle Manager with My VMware

You can integrate vRealize Suite Lifecycle Manager directly with a My VMware account to access vRealize Suite licenses within an entitlement account and manage the download of product OVAs for install, patch, and upgrade. The My VMware account registration is also used to download content from the VMware Marketplace.

6 Add Data Centers and vCenter Server Instances to vRealize Suite Lifecycle Manager in Region A

Before you can create an environment for product deployments, you must add a data center and the associated Management vCenter Server instance to vRealize Suite Lifecycle Manager.

7 Add Data Center and vCenter Server to vRealize Suite Lifecycle Manager in Region B

Before you can create an environment for product deployments, you must add a data center and the associated Management vCenter Server instance to vRealize Suite Lifecycle Manager.

8 Configure Log Forwarding for vRealize Suite Lifecycle Manager in Region A

You configure the Log Insight agent in the vRealize Suite Lifecycle Manager appliance to forward logs to vRealize Log Insight.

9 Add vRealize Lifecycle Manager to the Agent Group for Management Virtual Appliances in Region A

After you deploy the vRealize Lifecycle Manager and configure the log agent on the appliance, add the virtual appliance to the agent group for the management virtual appliances. You use this agent group to configure the collection of logs from the operating system of the appliances centrally.

10 Enable Disaster Recovery of vRealize Suite Lifecycle Manager

After you complete the deployment and configuration of vRealize Suite Lifecycle Manager in Region A, enable the replication of the vRealize Suite Lifecycle Manager virtual appliance to Region B, and update the protection group and recovery plan for the operations management layer in Site Recovery Manager. vRealize Suite Lifecycle Manager can continue providing lifecycle management and drift analysis of the vRealize Suite solutions in the Software-Defined Data Center after a disaster recovery failover.

Configure User Access in vSphere for Integration with vRealize Suite Lifecycle Manager in Region A

Configure an operations service account with the required permissions to enable vRealize Suite Lifecycle Manager to deploy and manage the vRealize Suite components of the Software-Defined Data Center (SDDC) on the Management vCenter Server.

Define a User Role in vSphere for vRealize Suite Lifecycle Manager in Region A

Create a user role in the vSphere Web Client with the required privileges to enable vRealize Suite Lifecycle Manager to deploy and manage the vRealize Suite components.

Procedure

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

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

   b Log in using the following credentials.

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

2 On the **Home** page, under **Administration**, click **Roles**.

3 Create a role for vRealize Suite Lifecycle Manager in vSphere.

   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	vRealize Suite Lifecycle Manager User
Privileges	■ **Datastore.Allocate space** ■ **Datastore.Browse datastore** ■ **Datastore.Update virtual machine files** ■ **Host.Local operations.Add host to vCenter** ■ **Host.Local operations.Create virtual machine** ■ **Host.Local operations.Delete virtual machine** ■ **Host.Local operations.Reconfigure virtual machine** ■ **Network.Assign network** ■ **Resource.Assign vApp to resource pool** ■ **Resource.Assign virtual machine to resource pool** ■ **Virtual machine.*** (All privileges) ■ **vApp.*** (All privileges)

Configure User Privileges in vSphere for Integration with vRealize Suite Lifecycle Manager in Region A

Assign account permissions to the svc-vrslcm-vsphere user to deploy and manage SDDC components on the Management vCenter Server with vRealize Suite Lifecycle Manager.

Procedure

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

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

   b Log in using the following credentials.

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

2 Assign permissions to the service account.

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

   b In the **Navigator**, select the **sfo01m01vc01.sfo01.rainpole.local** vCenter server.

   c Click **Permissions** tab and click the **Add permission** icon.

   d In the **Add Permission** dialog box, click **Add** to associate a user or a group with a role.

   e 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.

   f From the list of users and groups, select **svc-vrslcm-vsphere**, click **Add**, and click **OK**.

   g In the **Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **vRealize Suite Lifecycle Manager User**, ensure that **Propagate to children** is selected, and click **OK**.

Configure the Distributed Firewall for vRealize Suite Lifecycle Manager in Region A

Add vRealize Suite Lifecycle Manager to the distributed firewall in Region A to allow traffic to the user interface of this solution. Using a distributed firewall with your SDDC increases the security level of your environment by allowing only the network traffic that is required for the SDDC to run.

Procedure

1 Create an IP Set for vRealize Suite Lifecycle Manager

   Create an IP set for the vRealize Suite Lifecycle Manager appliance in the management cluster. You use the IP set later to create a security group for use with the additional distributed firewall rules established for vRealize Suite Lifecycle Manager.

2 Create a Security Group for vRealize Suite Lifecycle Manager

   Create security groups for use in configuring firewall rules for the groups of applications in the SDDC.

3 Add Distributed Firewall Rule for vRealize Suite Lifecycle Manager

   A firewall rule consists of a section to segregate the firewall rules and the rule itself, which defines what network traffic is blocked or allowed.

Create an IP Set for vRealize Suite Lifecycle Manager

Create an IP set for the vRealize Suite Lifecycle Manager appliance in the management cluster. You use the IP set later to create a security group for use with the additional distributed firewall rules established for vRealize Suite Lifecycle Manager.

A single IP set is added to support vRealize Suite Lifecycle Manager.

Table 3-14. IP Set for vRealize Suite Lifecycle Manager

Name	IP Addresses
vRealize Suite Lifecycle Manager	*vRealize-Suite-Lifecycle-Manager_IP's*

Procedure

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

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

   b Log in using the following credentials.

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

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

3 In the **Navigator**, click **Groups and Tags** and click the **Grouping Objects** tab.

4 From the **NSX Manager** drop-down menu, select **172.16.11.65**.

5 Click **IP Sets**, and click the **Add** icon.

6 In the **New IP Set** dialog box, configure the IP set for vRealize Suite Lifecycle Manager and click **OK**.

Setting	Value
Name	vRealize Suite Lifecycle Manager
IP Addresses	192.168.11.20
Universal Synchronization	Selected

Create a Security Group for vRealize Suite Lifecycle Manager

Create security groups for use in configuring firewall rules for the groups of applications in the SDDC.

A security group is a collection of assets (or objects) from your vSphere inventory that you group together.

You perform this procedure multiple times to configure all the necessary security groups. In addition, you create the VMware Appliances and Windows Servers groups from the security groups you add in the previous repetitions of this procedure.

Table 3-15. Security Group for vRealize Suite Lifecycle Manager

Name	Object Type	Selected Object
vRealize Suite Lifecycle Manager	IP Set	vRealize Suite Lifecycle Manager
VMware Appliances	Security Group	vRealize Suite Lifecycle Manager

Procedure

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

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

   b Log in using the following credentials.

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

2 In the **Navigator**, click **Networking & Security** and click **Groups and Tags**.

3 From the **NSX Manager** drop-down menu, select **172.16.11.65**.

4 Click **Grouping Objects**, select **Security Group**, and click the **Add** icon.

   The **Add Security Group** wizard appears.

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

Setting	Value
Name	vRealize Suite Lifecycle Manager
Universal Synchronization	Selected

6 On the **Select objects to include** page, select **IP Sets** from the **Object Type** drop-down menu, select **vRealize Suite Lifecycle Manager** from the list of available objects, click the **Add** button, and click **Next**.

7 On the **Ready to Complete** page, verify the configuration values that you entered and click **Finish**.

8 On the **Security Group** tab, select the group label **VMware Appliances** and click the **Edit Security Group** icon.

   The **Edit Security Group** wizard appears.

9 On the **Name and description** page, click **Next**.

10 On the **Select objects to include** page, select **Security Group** from the **Object Type** drop-down menu, select **vRealize Suite Lifecycle Manager** from the list of available objects, click the **Add** button, and click **Next**.

11 On the **Ready to Complete** page, verify the configuration values that you entered and click **Finish**.

Add Distributed Firewall Rule for vRealize Suite Lifecycle Manager

A firewall rule consists of a section to segregate the firewall rules and the rule itself, which defines what network traffic is blocked or allowed.

You create firewall rules that allow administrators to connect to the different VMware solutions, rules to allow user access to the vRealize Automation portal, and to provide external connectivity to the SDDC.

Procedure

- Log in to vCenter Server by using the vSphere Web Client.
  a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.
  b Log in using the following credentials.

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

- From the **Home** menu, select **Networking & Security** and click **Firewall**.
- From the **NSX Manager** drop-down menu, select **172.16.11.65**.
- Create a distributed firewall rule to allow administrative access to the vRealize Suite Lifecycle Manager user.

Name	Source	Destination	Service / Port
Allow vRSLCM to Admins	Administrators	vRealize Suite Lifecycle Manager	HTTPS

  a In the **VMware Management Services** section, click **Add rule**.
  b In the **Name** cell, click the **Edit** icon to change the rule name to **`Allow vRSLCM to Admins`**.
  c Click the **Edit** icon in the **Source** column, change the **Object Type** to **Security Groups**, add **Administrators** to the **Selected Objects** list, and click **OK**.
  d Click the **Edit** icon in the **Destination** column, change the **Object Type** to **Security Groups**, add **vRealize Suite Lifecycle Manager** to the **Selected Objects** list, and click **OK**.
  e Click the **Edit** icon in the **Service** column, enter **HTTPS** in the filter, add **HTTPS** to the **Selected Objects** list, and click **OK**.
  f Click **Publish Changes**.

Deploy the vRealize Suite Lifecycle Manager Appliance in Region A

You deploy the vRealize Suite Lifecycle Manager appliance and configure storage, networking, and other key appliance attributes.

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** menu, select **Global Inventory Lists > vCenter Servers**.

3 Right-click **sfo01m01vc01.sfo01.rainpole.local** and select **Deploy OVF Template**.

4 On the **Select template** page, select **Local file**, browse to the location of the vRealize Suite Lifecycle Manager OVA file, and click **Next**.

5 On the **Select name and location** page, enter the following information, and click **Next**.

Setting	Value
Name	vrslcm01svr01a
Select a data center or folder	sfo01-m01fd-mgmt

6 On the **Select a resource** page, select **sfo01-m01-mgmt01** and click **Next**.

7 On the **Review details** page, review the virtual appliance details such as product, version, download size, and size on disk, and click **Next**.

8 On the **Accept license agreements** page, read and accept the End-User License Agreement, and click **Next**.

9 On the **Select configuration** page, leave the default value and click **Next**.

10 On the **Select storage** page, select the following parameters and click **Next.**

Setting	Value
Select virtual disk format	Thin provision
VM storage policy	vSAN Default Storage Policy
Datastores	sfo01-m01-vsan01

11 On the **Select networks** page, select the distributed port group that ends with `Mgmt-xRegion01-VXLAN` from the **Destination Network** drop-down menu and click **Next**.

12 On the **Customize template** page, configure the following values and click **Next**.

Option	Value
Hostname	vrslcm01svr01a.rainpole.local
Join the VMware Customer Experience Improvement Program	Selected
Common Name	vrslcm01svr01a.rainpole.local
Country Code	US
Organization Name	Rainpole
Organization Unit	Rainpole
Default Gateway	192.168.11.1
Domain Name	rainpole.local
Domain Name Servers	172.16.11.4,172.17.11.4
Domain Search Path	rainpole.local
Network 1 IP Address	192.168.11.20
Network 1 Netmask	255.255.255.0

13 On the **Ready to complete** page, click **Finish** and wait for the process to complete.

14 Power on the vRealize Suite Lifecycle Manager appliance.

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

b Expand the sfo01m01vc01.sfo01.rainpole.local tree.

c Select the vrslcm01svr01a virtual machine and from the **Actions** menu select **Power > Power on**.

Configure the vRealize Suite Lifecycle Manager Appliance in Region A

You configure the vRealize Suite Lifecycle Manager appliance system settings, generate the certificate for product deployments, replace the appliance certificate, and configure NTP settings.

Configure vRealize Suite Lifecycle Manager in Region A

After the deployment of the vRealize Suite Lifecycle Manager appliance, you perform an initial login and configure common system settings, such as the appliance passwords, the configuration drift interval, enablement of SSH, and joining the VMware Customer Experience Improvement Program.

Procedure

1 Log in to vRealize Suite Lifecycle Manager user interface for the first time.

   a Open a Web browser and go to **`https://vrslcm01svr01a.rainpole.local/vrlcm`**.

   b Log in using the following credentials.

Setting	Value
User name	admin@localhost
Password (default)	vmware

2 On the **Choose a new LCM VA root Password** page, provide the following values to set a new root password and click **Update Password**.

   The password must be at least eight characters long and contain at least one lowercase, uppercase, numeric, and special character.

Setting	Value
Password	*vrslcm_root_password*
Confirm Password	*vrslcm_root_password*

3 Close the **Welcome** dialog box.

4 In the **Navigator** pane, click the **Settings** icon.

5 Under **Settings**, click **System Settings** and configure the following values.

Setting	Value
SSH Service	Selected
Admin Password	*vrslcm_admin_password*
Confirm Admin Password	*vrslcm_admin_password*
Configuration Drift Interval	24 (default)
Restart Server	Deselected (default)
Schedule a restart	Deselected (default)
Join the VMware Customer Experience Improvement Program	Selected (default)

6 Click **Save**, and in the **Confirm Logout** dialog box, click **OK**.

   vRealize Suite Lifecycle Manager logs you out back to the vRealize Suite Lifecycle Manager login screen.

Generate Certificate for vRealize Suite Lifecycle Manager Environments in Region A

Before deploying a product with vRealize Suite Lifecycle Manager, you generate a self-signed certificate that is used during product path, solution path, or configuration file deployment.

Procedure

1 Log in to vRealize Suite Lifecycle Manager user interface.

   a Open a Web browser and go to **`https://vrslcm01svr01a.rainpole.local/vrlcm`**.

   b Log in using the following credentials.

Setting	Value
User name	admin@localhost
Password	*vrslcm_admin_password*

2 In the **Navigator**, click the **Settings** icon.

3 Under **Settings**, click the **Certificate** tab, enter the following values, and click **Generate Certificate**.

Setting	Value
Organization Name	Rainpole
Organizational Unit	Rainpole
Domain Name	rainpole.local,sfo01.rainpole.local,lax01.rainpole.local
Locality	San Francisco
State	California
Country Code	US
Passphrase	*vrslcm_generated_certificate_passphrase*

   A message `Certificate generate request triggered successfully` appears.

4 In the **Navigator**, click the **Requests** icon and validate that `ACTION#GENERATE_CERTIFICATE` displays as `COMPLETED`.

5 In the **Navigator**, click the **Settings** icon, click the **Certificate** tab, and click **View Certificate** to view the certificate details.

Replace Certificate on the vRealize Suite Lifecycle Manager Appliance in Region A

To establish a trusted connection to vRealize Suite Lifecycle Manager, you replace the SSL certificate on the appliance with a custom certificate signed by a certificate authority available on the parent Active Directory or on the intermediate Active Directory. See *Certificate Replacement* guide for additional information.

Procedure

1 Rename the certificates generated using the VMware Validated Design Certificate Generation Utility for vrslcm01svr01a.rainpole.local.

Original Certificate File Name	New Certificate File Name
vrslcm01svr01a.2.chain.pem	server.crt
vrslcm01svr01a-orig.key	server.key

2 Overwrite the existing `server.crt` and `server.key` files in the `/opt/vmware/vlcm/cert` directory with the previously generated CA signed certificate files.

   You can use SCP software like WinSCP.

3 Log in to vRealize Suite Lifecycle Manager appliance by using Secure Shell (SSH) client.

   a Open an SSH connection to vrslcm01svr01a.rainpole.local.

   b Log in using following credentials.

Setting	Value
User name	root
Password	*vrslcm_root_password*

4 Restart the vRealize Suite Lifecycle Manager services to update the appliance certificate.

   a Restart the system services by running the following command in the SSH session.

```
systemctl restart vlcm-xserver
```

   b Check the status of the system services by running the following command in the SSH session.

```
systemctl status vlcm-xserver
```

5 After restarting the services, verify that the certificate is updated on the appliance.

   a Close any opened Web browsers, open a new Web browser window, and go to **`https://vrslcm01svr01a.rainpole.local/vrlcm`**.

   b Verify that you see the new certificate in the browser.

Configure NTP on the vRealize Suite Lifecycle Manager Appliance in Region A

Configure NTP on the vRealize Suite Lifecycle Manager appliance to keep vRealize Suite Lifecycle Manager synchronized with the other SDDC components.

Prerequisites

Verify that the SSH service on the vRealize Suite Lifecycle Manager appliance is enabled.

Procedure

1 Log in to vRealize Suite Lifecycle Manager appliance by using Secure Shell (SSH) client.

   a Open an SSH connection to vrslcm01svr01a.rainpole.local.

   b Log in using following credentials.

Setting	Value
User name	root
Password	*vrslcm_root_password*

2 Configure the NTP source for the vRealize Suite Lifecycle Manager appliance.

   a Open the `/etc/systemd/timesyncd.conf` file for editing using a text editor such as `vi`.

   ```
   vi /etc/systemd/timesyncd.conf
   ```

   b Remove the comment for the **NTP** configuration and add the following NTP settings.

   ```
   NTP=ntp.sfo01.rainpole.local ntp.lax01.rainpole.local
   ```

3 Enable the `systemd-timesyncd` service and verify the status.

   a Run the following command to enable the network time synchronization.

   ```
   timedatectl set-ntp true
   ```

   b Run the following command to enable the NTP synchronization.

   ```
   systemctl restart systemd-timesyncd
   ```

   c Run the following command to verify the status of the service.

   ```
   timedatectl status
   ```

4 Log out of the session by entering `logout`.

Register vRealize Suite Lifecycle Manager with My VMware

You can integrate vRealize Suite Lifecycle Manager directly with a My VMware account to access vRealize Suite licenses within an entitlement account and manage the download of product OVAs for install, patch, and upgrade. The My VMware account registration is also used to download content from the VMware Marketplace.

If your organization restricts outbound access, configure a proxy server for the vRealize Suite Lifecycle Manager appliance.

Prerequisites

Before registering vRealize Suite Lifecycle Manager with My VMware, verify that you have created a My VMware account with permissions to view licenses and download products from your entitlement account. See .

Procedure

1 Log in to vRealize Suite Lifecycle Manager user interface.

   a Open a Web browser and go to **`https://vrslcm01svr01a.rainpole.local/vrlcm`**.

   b Log in using the following credentials.

Setting	Value
User name	admin@localhost
Password	*vrslcm_admin_password*

2 On the **Navigator** pane, click the **Settings** icon.

3 Register vRealize Suite Lifecycle Manager with My VMware.

   a On the **Settings** page, click the **My VMware** tab, enter your My VMware credentials, and click **Submit**.

Setting	Value
User Name	*my_vmware_username*
Password	*my_vmware_password*

   b In the **Download OVA** dialog box that appears prompting you to start a content download, click **NO**.

   After vRealize Suite Lifecycle Manager is registered with My VMware, you see a message `Service registered with My VMware credentials provided`.

4 (Optional) If the access to My VMware is behind a proxy, configure the proxy sSettings for vRealize Suite Lifecycle Manager.

   a In the **Navigator** pane, click the **Settings** icon and click the **My VMware** tab.

   b On the **My VMware** page, select **Configure Proxy**, enter the following values, and click **Submit**.

Setting	Value
Proxy Server	*proxy_server_fqdn_or_ip_address* (for example: proxy.rainpole.local)
Proxy Port	*proxy_server_port* (for example: 3128)
Proxy User Name	*proxy_server_username*
Proxy Password	*proxy_server_password*

Add Data Centers and vCenter Server Instances to vRealize Suite Lifecycle Manager in Region A

Before you can create an environment for product deployments, you must add a data center and the associated Management vCenter Server instance to vRealize Suite Lifecycle Manager.

You add a data center for the deployment in Region A for each of the following groups of components:

- Cross-region components, such as the analytics cluster of vRealize Operations Manager and the main components of the Cloud Management Platform.
- Local-region components, such as vRealize Log Insight and vRealize Log Insight Content Packs.

Procedure

1 Log in to vRealize Suite Lifecycle Manager user interface.

   a Open a Web browser and go to **`https://vrslcm01svr01a.rainpole.local/vrlcm`**.

   b Log in using the following credentials.

Setting	Value
User name	admin@localhost
Password	*vrslcm_admin_password*

2 In the **Navigator**, click the **Data Centers** icon.

3 Add the data centers.

   a On the **Data Centers** page, click the **Manage Data Centers** tab and click **Add Data Center**.

   b In the **Add Data Center** dialog box, add the data centers by entering the following information and clicking **Add**.

Setting	Value for Region A	Value for Cross-Region
Name	sfo01-m01dc	cross-region-dc
Location	San Francisco, California, US	San Francisco, California, US

4 Add the vCenter Server instances.

   a On the **Data Centers** page, click the **Manage vCenter Servers** tab.

   b From the **Select Data Center** drop-down menu, select sfo01-m01dc and click **Add vCenter Server**.

   c In the **Add vCenter Server Details** dialog box, enter the following vCenter Server information for each data center and click **Submit**.

Setting	Value for the sfo01-m01dc Data Center	Value for the cross-region-dc Data Center
Host Name	sfo01m01vc01.sfo01.rainpole.local	sfo01m01vc01.sfo01.rainpole.local
User Name	svc-vrslcm-vsphere@rainpole.local	svc-vrslcm-vsphere@rainpole.local
Password	*svc-vrslcm-vsphere_password*	*svc-vrslcm-vsphere_password*
vCenter Server Type	Management	Management

   d Repeat the steps to add the vCenter Server instance to the other data center.

5 In the **Navigator**, click **Requests** and validate that `VC_DATA_COLLECTION` for each vCenter Server instance shows `COMPLETED`.

Add Data Center and vCenter Server to vRealize Suite Lifecycle Manager in Region B

Before you can create an environment for product deployments, you must add a data center and the associated Management vCenter Server instance to vRealize Suite Lifecycle Manager.

You add a data center for the deployment in Region B for each of the following groups of components:

- Cross-region components, such as the remote collectors of vRealize Operations Manager, vSphere proxy agents of vRealize Automation, and the data collectors of vRealize Business.
- Local-region components, such as vRealize Log Insight and vRealize Log Insight Content Packs.

Procedure

1 Log in to vRealize Suite Lifecycle Manager user interface.

   a Open a Web browser and go to **`https://vrslcm01svr01a.rainpole.local/vrlcm`**.

   b Log in using the following credentials.

Setting	Value
User name	admin@localhost
Password	*vrslcm_admin_password*

2 In the **Navigator**, click the **Data Centers** icon.

3 Add the data center.

   a On the **Data Centers** page, click the **Manage Data Centers** tab and click **Add Data Center**.

   b In the **Add Data Center** dialog box, add the data center by entering the following information and click **Add**.

Setting	Value for Region B
Name	lax01-m01dc
Location	Los Angeles, California, US

4 Add the vCenter Server instance.

   a On the **Data Centers** page, click the **Manage vCenter Servers** tab.

   b From the **Select Data Center** drop-down menu, select lax01-m01dc data center and click **Add vCenter Server**.

c In the **Add vCenter Server Details** dialog box, enter the following information for each data center and click **Submit**.

Setting	Value for the lax01-m01dc Data Center	Value for the cross-region-dc Data Center
Host Name	lax01m01vc01.lax01.rainpole.local	lax01m01vc01.lax01.rainpole.local
User Name	svc-vrslcm-vsphere@rainpole.local	svc-vrslcm-vsphere@rainpole.local
Password	*svc-vrslcm-vsphere_password*	*svc-vrslcm-vsphere_password*
vCenter Server Type	Management	Management

d Repeat the steps to add the vCenter Server to the other data center.

5 In the **Navigator**, click **Requests** and validate that `VC_DATA_COLLECTION` for each vCenter Server shows `COMPLETED`.

Configure Log Forwarding for vRealize Suite Lifecycle Manager in Region A

You configure the Log Insight agent in the vRealize Suite Lifecycle Manager appliance to forward logs to vRealize Log Insight.

Procedure

1 Log in to vRealize Suite Lifecycle Manager appliance by using Secure Shell (SSH) client.

a Open an SSH connection to vrslcm01svr01a.rainpole.local.

b Log in using following credentials.

Setting	Value
User name	root
Password	*vrslcm_root_password*

2 Edit the `liagent.ini` file on each vRealize Lifecycle Manager node using a text editor such as `vi`.

```
vi /var/lib/loginsight-agent/liagent.ini
```

3 Locate the `[server]` section, remove the comment for the following parameters and insert the following values.

```
[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
hostname=sfo01vrli01.sfo01.rainpole.local
; Set protocol to use:
; cfapi - Log Insight REST API
; syslog - Syslog protocol
; If omitted the default value is cfapi
;
proto=cfapi
; Log Insight server port to connect to. If omitted the default value is:
```

```
; for syslog: 512
; for cfapi without ssl: 9000
; for cfapi with ssl: 9543
port=9000
;ssl – enable/disable SSL. Applies to cfapi protocol only.
; Possible values are yes or no. If omitted the default value is no.
ssl=no
; Time in minutes to force reconnection to the server
; If omitted the default value is 30
;reconnect=30
```

4 Press Escape and enter **`:wq!`** to save the file.

5 Restart the Log Insight agent on the node by running the following console command.

```
/etc/init.d/liagentd restart
```

6 Verify that the Log Insight agent is running.

```
/etc/init.d/liagentd status
```

Add vRealize Lifecycle Manager to the Agent Group for Management Virtual Appliances in Region A

After you deploy the vRealize Lifecycle Manager and configure the log agent on the appliance, add the virtual appliance to the agent group for the management virtual appliances. You use this agent group to configure the collection of logs from the operating system of the appliances centrally.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://sfo01vrli01.sfo01.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 From the **All Agents** drop-down menu, select **VA - Linux Agent Group** from the **Active Groups** section.

5 In the agent filter text boxes, add the host name of the vRealize Lifecycle Manager appliance to the list of management virtual appliances in the region pressing Enter after each host name.

Filter	Operator	Values
Hostname	Matches	■ vrops01svr01a.rainpole.local ■ vrops01svr01b.rainpole.local ■ vrops01svr01c.rainpole.local ■ sfo01vropsc01a.sfo01.rainpole.local ■ sfo01vropsc01b.sfo01.rainpole.local ■ vra01svr01a.rainpole.local ■ vra01svr01b.rainpole.local ■ vra01svr01c.rainpole.local ■ vrb01svr01.rainpole.local ■ sfo01vrbc01.sfo01.rainpole.local ■ **vrslcm01svr01a.rainpole.local**

6 Click **Refresh** and verify that all the agents listed in the filter appear in the **Agents** list.

7 Click **Save New Group** at the bottom of the page.

Enable Disaster Recovery of vRealize Suite Lifecycle Manager

After you complete the deployment and configuration of vRealize Suite Lifecycle Manager in Region A, enable the replication of the vRealize Suite Lifecycle Manager virtual appliance to Region B, and update the protection group and recovery plan for the operations management layer in Site Recovery Manager. vRealize Suite Lifecycle Manager can continue providing lifecycle management and drift analysis of the vRealize Suite solutions in the Software-Defined Data Center after a disaster recovery failover.

Procedure

1 Replicate the vRealize Suite Lifecycle Manager Appliance in Region A

After you complete the deployment and configuration of vRealize Suite Lifecycle Manager, support the failover to Region B by enabling replication of the vRealize Suite Lifecycle Manager virtual appliance. After you configure the replication, you update the operations management protection group to protect the newly replicated vRealize Suite Lifecycle Manager virtual appliance.

2 Update the Protection Group for the Operations Management Layer

After you configure the replication of the vRealize Suite Lifecycle Manager virtual appliance, update the operations management protection group to protect the newly-replicated vRealize Suite Lifecycle Manager virtual appliance together with the other operations management virtual machines.

3 Update the Recovery Plan for the Operations Management Layer

After you update the protection group for the operations management layer, update the existing recovery plan to include the vRealize Suite Lifecycle Manager virtual appliance.

Replicate the vRealize Suite Lifecycle Manager Appliance in Region A

After you complete the deployment and configuration of vRealize Suite Lifecycle Manager, support the failover to Region B by enabling replication of the vRealize Suite Lifecycle Manager virtual appliance. After you configure the replication, you update the operations management protection group to protect the newly replicated vRealize Suite Lifecycle Manager virtual appliance.

Procedure

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

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

   b Log in using the following credentials.

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

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

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

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

4 Select the new vRealize Suite Lifecycle Manager virtual appliance

New vRealize Automation Component	Virtual Machine Name
vRealize Suite Lifecycle Manager Virtual Appliance	vrslcm01svr01a

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

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

7 On the **Target site** page, select the **lax01m01vc01.lax01.rainpole.local** vCenter Server in Region B and click **Next**.

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

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

   a Click the **Edit** link.

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

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

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

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

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

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

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

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

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

13 (Optional) Monitor the replication progress.

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

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

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

Update the Protection Group for the Operations Management Layer

After you configure the replication of the vRealize Suite Lifecycle Manager virtual appliance, update the operations management protection group to protect the newly-replicated vRealize Suite Lifecycle Manager virtual appliance together with the other operations management virtual machines.

Procedure

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

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

b Log in using the following credentials.

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

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

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

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

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

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

6 Select the **SDDC Operations Management PG** protection group and click the **Edit Protection Group** icon.

   The **Edit Protection Group** wizard appears.

7 On the **Name and location** page, click **Next**.

8 On the **Protection group type** page, click **Next**.

9 On the **Virtual machines** page, select vrslcm01svr01a under **Replicated Virtual Machines** and click **Next**.

10 On the **Ready to complete** page, review the protection group settings and click **Next**.

11 On the **Apply changes** page, monitor the updates and click **Finish**.

   - `Reconfigure protection group` updates to a checked status.
   - `Protect virtual machines` updates to a checked status.

12 Verify that vrslcm01svr01a had been added to the protection group.

   a Click the **SDDC Operations Management PG** protection group.

   a Click the **Related Objects** tab, and click the **Virtual Machines** option.

   b Verify that vrslcm01svr01a is listed with a **Protection Status** of `OK`.

Update the Recovery Plan for the Operations Management Layer

After you update the protection group for the operations management layer, update the existing recovery plan to include the vRealize Suite Lifecycle Manager virtual appliance.

Procedure

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

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

   b Log in using the following credentials.

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

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

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

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

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

6 Change the priority of the vrslcm01svr01a virtual machine.

   a On the **Virtual Machines** tab, right-click vrslcm01svr01a and select **All Priority Actions > 4 (Low)**.

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

Import the vRealize Product Configurations in vRealize Suite Lifecycle Manager

After you have complete the deployment and configuration of vRealize Suite Lifecycle Manager, import the vRealize Suite product configurations for the operations management and cloud management layers in logical vRealize Suite Lifecycle Manager environments. Importing the product configurations provides alignment with this VMware Validated Design. You can perform lifecycle management and configuration drift analysis across the vRealize Suite products in the SDDC.

Procedure

1 Import the Cross-Region Environment in vRealize Suite Lifecycle Manager

   When you import vRealize Operations Manager, vRealize Automation, and vRealize Business using vRealize Suite Lifecycle Manager, you first create an environment. You import the products in the environment providing the vCenter Server, and compute, network, and storage location of the product deployments.

2 Import the Region A Environment in vRealize Suite Lifecycle Manager

   When you import vRealize Log Insight in Region A using vRealize Suite Lifecycle Manager, you first create a new environment. You import the product instance in the environment providing the vCenter Server, and compute, network and storage location of the product deployments.

3 Import the Region B Environment in vRealize Suite Lifecycle Manager

   When you import vRealize Log Insight in Region B using vRealize Suite Lifecycle Manager, you first create a new environment. You import the product instance in the environment providing the vCenter Server, and compute, network and storage location of the product deployments.

4 Save a Baseline for Environment Configuration Drift

   vRealize Suite Lifecycle Manager uses the product baseline to generate configuration drift reports that show the difference between the current product configuration and the baseline configuration. After you import the vRealize Suite product deployments back into vRealize Suite Lifecycle Manager, save a baseline to monitor each environment for configuration drift.

Import the Cross-Region Environment in vRealize Suite Lifecycle Manager

When you import vRealize Operations Manager, vRealize Automation, and vRealize Business using vRealize Suite Lifecycle Manager, you first create an environment. You import the products in the environment providing the vCenter Server, and compute, network, and storage location of the product deployments.

Procedure

1 Log in to vRealize Suite Lifecycle Manager user interface.

   a Open a Web browser and go to **`https://vrslcm01svr01a.rainpole.local/vrlcm`**.

   b Log in using the following credentials.

Setting	Value
User name	admin@localhost
Password	*vrslcm_admin_password*

2 To start the import, on the **Home** page, click **Create Environment**.

3 On the **Create Environment** page, enter the following information, and click **Next**.

Setting	Value
Data Center	cross-region-dc
Environment Type	Production
Environment Name	Cross-Region-Env
Administrator Email	*deployment_admin_email*
Default Password	*deployment_admin_password*
Confirm Default Password	*deployment_admin_password*
Join the VMware Customer Experience Improvement Program	Selected

4 On the **Products** tab, select the following option for product installation for each of the following vRealize Suite products and click **Next**.

Product	Option
vRealize Operations	Import
vRealize Automation	Import
vRealize Business for Cloud	Import

5 On the **End User License Agreement** page, read the EULA, select **I agree to the terms and conditions**, and click **Next**.

6 On the **License Details** page, add or select the vRealize Suite license and click **Next**.

- Select **Select vRealize Suite License**, and select the license.
- Select **Add vRealize Suite License**, provide the vRealize Suite or a vCloud Suite license key, and click **Next**.

7 On the **Infrastructure Details** page, enter the following information, and click **Next**.

Setting	Value
Select vCenter Server	sfo01m01vc01.sfo01.rainpole.local
Select Cluster	sfo01-m01-mgmt01 (sfo01-m01dc)
Select Network	Distributed port group that ends with `Mgmt-xRegion01-VXLAN`
Select Datastore	sfo01-m01-vsan01
Select Disk Format	Thin

8 On the **Network Details** page, enter the following information and click **Next**.

Setting	Value
Default Gateway	192.168.11.1
Domain Name	rainpole.local
Domain Search Path	rainpole.local
Domain Name Servers	172.16.11.4,172.17.11.4
Netmask	255.255.255.0

9 On the **Certificate Details** page, select **Use Generated Certificate** in **Manage Certificate** and click **Next**.

10 On the **Product Details** page, click the **vRealize Automation** tab and enter the following settings in the **Product Properties for Import** pane.

Setting	Value
vRA Root Password	*vra_appA_root_password*
vRA Default Administrator Password	*vra_administrator_password*
vRA Tenant User Name	vra-localdefaultadmin
vRA Primary Node FQDN	vra01svr01a.rainpole.local
IaaS Username	rainpole.local\svc-vra
vRA Tenant Password	*vra-localdefaultadmin_password*
IaaS Password	*svc-vra_password*

11 On the **vRealize Automation** tab, click **Add Another** for **vCenters** and select lax01m01vc01.lax01.rainpole.local from the **vCenter Host** drop-down menu

12 On the **Product Details** page, select the **vRealize Business for Cloud** tab and enter the following information for **Product Properties for Import**.

Setting	Value
vRB FQDN	vrb01svr01.rainpole.local
vRB Root Password	*vrb_server_root_password*
Is vRB Standalone	Deselected
Is vIDM Enabled	Deselected
vRA Cafe Host Name	vra01svr01.rainpole.local
vRA Cafe SSO Admin User	*vra-localdefaultadmin*
vRA Cafe SSO Password	*vra_administrator_password*

13 On the **vRealize Business for Cloud** tab, click **Add Another** for **vCenters** and select lax01m01vc01.lax01.rainpole.local from the **vCenter Host**drop-down menu.

14 On the **Product Details** page, click the **vRealize Operations** tab and enter the following settings in the **Product Properties for Import** pane.

Setting	Value
vROPS Root Password	*vrops_root_password*
vROPS Master Node IP Address	192.168.11.31
vROPS Admin Password	*vrops_admin_password*

15 On the **vRealize Operations** tab, click **Add Another** for **vCenters** and select lax01m01vc01.lax01.rainpole.local from the **vCenter Host** drop-down menu.

16 Click **Next**.

17 On the **Summary** page, review the information.

18 Click **Submit** to start the import.

19 In the **Navigator** pane, click **Requests** and validate that `CREATE_ENVIRONMENT` for `Environment Name: Cross-Region` in the **Request Info** column is `INPROGRESS`.

The progress might change from `SUBMITTED` to `INPROGRESS` state in several minutes.

20 Select the `INPROGRESS` state for `Environment Name: Cross-Region` in the **Request Info** column.

21 On the **Requests** page, monitor the steps of the import graph until the request is marked as `COMPLETED`.

Import the Region A Environment in vRealize Suite Lifecycle Manager

When you import vRealize Log Insight in Region A using vRealize Suite Lifecycle Manager, you first create a new environment. You import the product instance in the environment providing the vCenter Server, and compute, network and storage location of the product deployments.

Procedure

1 Log in to vRealize Suite Lifecycle Manager user interface.

   a Open a Web browser and go to **`https://vrslcm01svr01a.rainpole.local/vrlcm`**.

   b Log in using the following credentials.

Setting	Value
User name	admin@localhost
Password	*vrslcm_admin_password*

2 To start the import, on the **Home** page, click **Create Environment**.

3 On the **Create Environment** page, enter the following information, and click **Next**.

Setting	Value
Data Center	sfo01-m01dc
Environment Type	Production
Environment Name	SFO-Region-Env
Administrator Email	*deployment_admin_email*
Default Password	*deployment_admin_password*
Confirm Default Password	*deployment_admin_password*
Join the VMware Customer Experience Improvement Program	Selected

4 On the **Products** tab, select the following option for product installation and click **Next**.

Product	Option
vRealize Log Insight	Import

5 On the **End User License Agreement** page, read the EULA, select **I agree to the terms and conditions**, and click **Next**.

6 On the **License Details** page, select or add the vRealize Suite license and click **Next**.

- Select **Select vRealize Suite License** and select the license.
- Select **Add vRealize Suite License**, provide the vRealize Suite or a vCloud Suite license key, and click **Next**.

7 On the **Infrastructure Details** page, enter the following settings, and click **Next**.

Setting	Value
Select vCenter Server	sfo01m01vc01.sfo01.rainpole.local
Select Cluster	sfo01-m01-mgmt01 (sfo01-m01dc)
Select Network	Distributed port group that ends with `Mgmt-RegionA01-VXLAN`
Select Datastore	sfo01-m01-vsan01
Select Disk Format	Thin

8 On the **Network Details** page, enter the following information and click **Next**.

Setting	Value
Default Gateway	192.168.31.1
Domain Name	sfo01.rainpole.local
Domain Search Path	sfo01.rainpole.local,rainpole.local
Domain Name Servers	172.16.11.5,172.16.11.4
Netmask	255.255.255.0

9 On the **Certificate Details** page, select **Use Generated Certificate** in **Manage Certificate** and click **Next**.

10 On the **Product Details** page, click the **vRealize Log Insight** tab and enter the following information in the **Product Properties for Import** pane.

Setting	Value
vRLI Master Node FQDN	sfo01vrli01a.sfo01.rainpole.local
vRLI root Password	*vrli_root_password*
vRLI Admin Password	*vrli_admin_password*

11 Click **Next**.

12 On the **Summary** page, review the information.

13 Click **Submit** to start the import.

14 In the **Navigator** pane, click **Requests** and validate that `CREATE_ENVIRONMENT` for `Environment Name: SFO-Region` in the **Request Info** column is `INPROGRESS`.

The progress might change from `SUBMITTED` to `INPROGRESS` state in several minutes.

15 Select the `INPROGRESS` state for `Environment Name: SFO-Region` in the **Request Info** column.

16 On the **Requests** page, monitor the steps of the import graph until the request is marked as `COMPLETED`.

Import the Region B Environment in vRealize Suite Lifecycle Manager

When you import vRealize Log Insight in Region B using vRealize Suite Lifecycle Manager, you first create a new environment. You import the product instance in the environment providing the vCenter Server, and compute, network and storage location of the product deployments.

Procedure

1 Login to vRealize Suite Lifecycle Manager

   a Open a Web browser and go to **`https://vrs01lcm01.rainpole.local/vrlcm`**.

   b Log in using following credentials.

Setting	Value
User name	admin@localhost
Password	*vrslcm_admin_password*

2 To start the import, on the **Home** page, click **Create Environment**.

3 On the **Create Environment** page, enter the following information, and click **Next**.

Setting	Value
Data Center	lax01-m01dc
Environment Type	Production
Environment Name	LAX-Region-Env
Administrator Email	*deployment_admin_email*
Default Password	*deployment_admin_password*
Confirm Default Password	*deployment_admin_password*
Join the VMware Customer Experience Improvement Program	Selected

4 On the **Products** tab, select the following option for product installation and click **Next**.

Product	Option
vRealize Log Insight	Import

5 On the **End User License Agreement** page, read the EULA, select **I agree to the terms and conditions**, and click **Next**.

6 On the **License Details** page, select or add the vRealize Suite license and click **Next**.

- Select **Select vRealize Suite License** and select the license.
- Select **Add vRealize Suite License**, provide the vRealize Suite or a vCloud Suite license key, and click **Next**.

7 On the **Infrastructure Details** page, enter the following information, and click **Next**.

Setting	Value
Select vCenter Server	lax01m01vc01.lax01.rainpole.local
Select Cluster	lax01-m01-mgmt01 (lax01-m01dc)
Select Network	Distributed port group that ends with `Mgmt-RegionB01-VXLAN`
Select Datastore	lax01-m01-vsan01
Select Disk Format	Thin

8 On the **Network Details** page, enter the following settings and click **Next**.

Setting	Value
Default Gateway	192.168.32.1
Domain Name	lax01.rainpole.local
Domain Search Path	lax01.rainpole.local,rainpole.local
Domain Name Servers	172.17.11.5,172.17.11.4
Netmask	255.255.255.0

9 On the **Certificate Details** page, select **Use Generated Certificate** in **Manage Certificate** and click **Next**.

10 On the **Product Details** page, select the **vRealize Log Insight** tab and enter the following information in the **Product Properties for Import** pane.

Setting	Value
vRLI Master Node FQDN	lax01vrli01a.lax01.rainpole.local
vRLI root Password	*vrli_root_password*
vRLI Admin Password	*vrli_admin_password*

11 Click **Next**.

12 On the **Summary** page, review the information.

13 Click **Submit** to start the import.

14 In the **Navigator** pane, click **Requests** and validate that `CREATE_ENVIRONMENT` for `Environment Name: LAX-Region` in the **Request Info** column is `INPROGRESS`.

The progress might change from `SUBMITTED` to `INPROGRESS` state in several minutes.

15 Select the `INPROGRESS` state for `Environment Name: LAX-Region` in the **Request Info** column.

16 In the **Requests** page, monitor the steps of the import graph until the request is marked as `COMPLETED`.

Save a Baseline for Environment Configuration Drift

vRealize Suite Lifecycle Manager uses the product baseline to generate configuration drift reports that show the difference between the current product configuration and the baseline configuration. After you import the vRealize Suite product deployments back into vRealize Suite Lifecycle Manager, save a baseline to monitor each environment for configuration drift.

Environment	Task
Cross-Region-Env	Save Baseline
SFO-Region-Env	Save Baseline
LAX-Region-Env	Save Baseline

Procedure

1 Log in to vRealize Suite Lifecycle Manager user interface.

   a Open a Web browser and go to **`https://vrslcm01svr01a.rainpole.local/vrlcm`**.

   b Log in using the following credentials.

Setting	Value
User name	admin@localhost
Password	*vrslcm_admin_password*

2 On the **Home** page, click **Manage Environments**.

3 On the **Environments** page, click the eclipse menu ... on cross-region environment card.

4 Under **Configuration Drift**, select **Save Baseline** to save the configuration state.

5 Repeat the step for the remaining imported environments.

6 Verify the `Baseline Save Initiated` banner appears on the environment card.

Update the Virtual Infrastructure and Business Continuity Layers

4

After you upgrade the cloud management and operations management layers, upgrade the components of the virtual infrastructure and business continuity layers of the SDDC. You upgrade the virtual infrastructure and business continuity layers last to reduce the time to upgrade the whole stack and prevent from errors caused by incompatibility between product versions.

Table 4-1. Upgrade Sequence for the Virtual Infrastructure and Business Continuity Layers in VMware Validated Design

Order	Component	Sub-Component
1	Backup solution based on VMware vSphere Storage APIs – Data Protection (VADP)	-
2	NSX for vSphere	NSX Manager instances
		NSX Controller instances
		NSX Networking fabric
		NSX Edges
		Post-upgrade configuration of NSX
3	Platform Services Controller instances	-
	vCenter Server instances for the management clusters	-
4	vSphere Replication	-
	Site Recovery Manager	-
5	vSphere Update Manager Download Service	-
6	ESXi in the management clusters	-
7	vCenter Server instances for the shared edge and compute clusters	
8	ESXi in the shared edge and compute clusters	
9	Post-upgrade reconfiguration for virtual infrastructure	-

Procedure

1 Review and Update vSphere Storage APIs – Data Protection Based Backup Solution

Before you upgrade the virtual infrastructure layer, verify that your vSphere Storage APIs – Data Protection (VADP) based backup solution is compatible with the version of vSphere in this release of VMware Validated Design.

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

When you upgrade the virtual infrastructure layer you begin with the NSX instances in the VMware Validated Design. You maintain the compatibility between the product versions in the stack and in the virtual infrastructure layer. You upgrade each functional group of components of the NSX deployment in Region A and Region B.

3 Update the Components for the Management Cluster

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

4 Update the Components for the Shared Edge and Compute Clusters

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

5 Global Post-Upgrade Configuration of the Virtual Infrastucture Layer

After you update all virtual infrastructure layer, perform global post-upgrade configuration according to address the dependencies between these components and to align your environment to the guidance in this validated design.

Review and Update vSphere Storage APIs – Data Protection Based Backup Solution

Before you upgrade the virtual infrastructure layer, verify that your vSphere Storage APIs – Data Protection (VADP) based backup solution is compatible with the version of vSphere in this release of VMware Validated Design.

Perform the upgrade outside of the usual backup windows.

Prerequisites

- Verify that backup solution is compatible with vSphere 6.5 Update 2. Contact your backup solution vendor product compatability matricies.
- Verfiy that all customizations or integrations are compatible with the backup solution. Contact your backup solution vendor.
- Verify that the backup solution is fully operational and compatible with any other clients, such as, reporting tools, web browsers, etc. Contact your backup solution vendor and their product compatability matricies
- Allocate adequate time for the duration of maintenance window. Contact your backup solution vendor to estimate the time required to upgrade and verify solution operations.
- Verify that no alarms exist for the backup solution in both the vSphere Web Client and backup solution management interfaces.

What to do next

- Verify that backup solution functions flawlessly after the upgrade. Consult the documentation of the backup vendor for details on operational verification.

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

When you upgrade the virtual infrastructure layer you begin with the NSX instances in the VMware Validated Design. You maintain the compatibility between the product versions in the stack and in the virtual infrastructure layer. You upgrade each functional group of components of the NSX deployment in Region A and Region B.

Upgrading NSX is a multi-step process. You must upgrade the paired NSX Manager instances for Cross-vCenter networking and security, the NSX Controller nodes, the ESXi VIBs, and the NSX Edge devices, starting with the universal distributed logical routers. 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 for vSphere Components in the SDDC

Region	Role	IP Address	FQDN
Region A	NSX Manager for the management cluster that is running as primary	172.16.11.65	sfo01m01nsx01.sfo01.rainpole.local
	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	sfo01w01nsx01.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	-

Table 4-2. NSX for vSphere Components in the SDDC (Continued)

Region	Role	IP Address	FQDN
Region B	NSX Manager for the management cluster that is running as secondary	172.17.11.65	lax01m01nsx01.lax01.rainpole.local
	NSX Manager for the shared edge and compute cluster that is running as secondary	172.17.11.66	lax01w01nsx01.lax01.rainpole.local

Note You might receive several false alerts from vRealize Operations Manager and vRealize Log Insight during the NSX upgrade procedure.

Prerequisites

- Download the NSX upgrade bundle, `VMware-NSX-Manager-upgrade-bundle-6.4.1-build_number.tar.gz`, from My VMware to a Windows host that has access to your environment.
- Review Operational Impacts of NSX Upgrade in *NSX Upgrade Guide* to understand the impact that each component might have on your environment.
- Review Upgrade NSX in a Cross-vCenter NSX Environment and Upgrade NSX Using Upgrade Coordinator in *NSX Upgrade Guide* to understand the prerequisites and the detailed upgrade guidance provided for your environment.
- Verify that any virtual networking integration in the environment has been quiesced of all activities, including but not limited to the following operations:
  - Users ordering new virtual machines backed by virtual wires over the cloud management platform
  - Third-party integration that automates the ordering or deployment of new virtual machines that are backed by virtual wires
  - 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. If the file system usage is at 100 percent, perform a clean-up.
  a Open an SSH connection to the NSX Manager instance you are upgrading using the **admin** account and run the `show filesystems` command to show the filesystem usage.
  b If the filesystem usage is at 100 percent, enter Privileged mode and clear the logs by running the following commands.

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

  c Reboot the NSX Manager appliance to apply the log clean-up.
- Back up the NSX configuration and download the technical support logs.

- Back up the NSX Manager pair, both primary and secondary instances. For more information, see Back Up and Restore NSX Manager in *NSX Upgrade Guide*.
- Verify that each NSX Controller is in normal, connected state.
- Verify that **Host Preparation > Installation Status** of all clusters has the green check mark and the proper NSX for vSphere version.
- 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 by using the ESXi Host Client.
  b Select **Host > Manage**.
  c On the **Packages** tab, search for **esx–n**.
  d Note the current version of the following VIB.
    - esx-nsxv

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 Controller Clusters

After you upgrade the NSX Manager instances in Region A and Region B, upgrade the NSX Controller cluster for the management cluster and the shared edge and compute cluster. You upgrade the NSX Controllers clusters immediately after the upgrade the NSX Manager instance to keep their versions aligned.

3 Upgrade the NSX Components on the ESXi Hosts

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

4 Upgrade the NSX Edge Instances

After you upgrade the control and data plane components of NSX for vSphere, upgrade the NSX Edge services gateway, universal distributed logical router, and load balancer instances.

5 Post-Upgrade Configuration of NSX for vSphere

After you complete the upgrade of the NSX components in the virtual infrastructure layer, perform the post-upgrade configuration changes to the environment according to the design objectives and deployment guidance to ensure your environment remains aligned to this VMware Validated Design.

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. Next, you continue with the NSX Manager nodes for the shared edge and compute cluster. You must upgrade the primary and all secondary NSX Manager instances to the same version in the same maintenance window. However, you can perform the upgrade of the management clusters and the shared edge and compute clusters in the same or separate maintenance windows.

Table 4-3. NSX Manager Nodes in the SDDC

Order	Region	NSX Manager Instance	NSX Appliance URL	vCenter Server URL
1	Region A	Primary NSX Manager for the management cluster	https://sfo01m01nsx01.sfo01.rainpole.local	sfo01m01vc01.sfo01.rainpole.local
2	Region B	Secondary NSX Manager for the management cluster	https://lax01m01nsx01.lax01.rainpole.local	lax01m01vc01.lax01.rainpole.local
3	Region A	Primary NSX Manager for the shared edge and compute cluster	https://sfo01w01nsx01.sfo01.rainpole.local	sfo01w01vc01.sfo01.rainpole.local
4	Region B	Secondary NSX Manager for the shared edge and compute cluster	https://lax01w01nsx01.lax01.rainpole.local	lax01w01vc01.lax01.rainpole.local

Procedure

1 Log in to the Management NSX Manager appliance user interface.

   a Open a Web browser and go to **`https://sfo01m01nsx01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 Click **Upgrade** and on the **Upgrade** page, click **Upload Bundle**.

3 In the **Upgrade** dialog box, locate the `VMware-NSX-Manager-upgrade-bundle-6.4.1-`*`build_number`*`.tar.gz` upgrade bundle on your file system.

4 Click **Open** and click **Continue**.

   The NSX Manager starts uploading the bundle.

5 After the upload is complete, in the **Upgrade** dialog box, configure the following settings and click **Upgrade**.

Setting	Value
Do you want to enable SSH?	Yes
Do you want to join the VMware Customer Experience Program	Yes

6 Log in to the Management NSX Manager appliance user interface.

a Open a Web browser and go to **`https://sfo01m01nsx01.sfo01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

7 Verify that the **Upgrade** tab shows the following configuration.

Setting	Expected Value
Upgrade State	Complete
Current Software Version	*The version and build in the upgrade bundle .*

8 Wait for the NSX for vSphere upgrade to complete.

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

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

b Log in using the following credentials.

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

10 In the vSphere Web Client, check for the latest NSX plug-in.

a From the **Home** menu, select **Administration**.

b In the **Navigator** pane, under **Solutions**, click **Client Plug-Ins**.

c On the **Client Plug-Ins** page, click **Check for New Plug-ins**.

d In the pop-up window **Checking for New Plug-ins** at the bottom, click **Go to the Event Console**.

e In the **Events Console**, enter **`plug-in`** in the filter.

Two events have recently occurred.

```
The deployment of plug-in NSX user interface plugin 6.4.1.build_number has started
The deployment of plug-in NSX user interface plugin 6.4.1.build_number is successful
```

f Log out from and back in to the vSphere Web Client, navigate back to the **Client Plug-Ins** page, and verify that the **vShield Manager Version** has been upgraded to 6.4.1.

11 Perform a fresh backup of the primary NSX Manager, sfo01m01nsx01.sfo01.rainpole.local.

You cannot restore from previous backups in the new NSX Manager version.

12 To complete the NSX Manager upgrade in the management cluster, repeat the steps for the secondary NSX Manager, lax01m01nsx01.lax01.rainpole.local.

13 Repeat the procedure for the shared edge and compute cluster.

You start with the primary NSX Manager, sfo01w01nsx01.sfo01.rainpole.local, and complete the upgrade with the secondary NSX Manager, lax01w01nsx01.lax01.rainpole.local.

Upgrade the NSX Controller Clusters

After you upgrade the NSX Manager instances in Region A and Region B, upgrade the NSX Controller cluster for the management cluster and the shared edge and compute cluster. You upgrade the NSX Controllers clusters immediately after the upgrade the NSX Manager instance to keep their versions aligned.

You can use the Upgrade Coordinator functionality to orchestrate the upgrade the NSX components in the deployment. You can select individual components, or group multiple components together and adjust the number of components to be upgraded according to the duration of the maintenance window.

For this VMware Validated Design, you upgrade each component one-by-one to maintain control. For information about upgrading multiple components during the same maintenance window, see *Upgrade NSX Using Upgrade Coordinator* in the NSX Upgrade Guide.

For each primary NSX Manager instance, you start an upgrade of the NSX Controller cluster. You upgrade the NSX Controller cluster for the management cluster in Region A first. Next, repeat the upgrade procedure on 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, but you must perform the upgrade immediately after the upgrade of the primary NSX Manager.

Table 4-4. NSX Controller Nodes in Region A

Order	Region	NSX Manager	NSX Manager IP Address	NSX Controller IP Address
1	Region A	Primary NSX Manager for the management cluster	172.16.11.65	172.16.11.118
				172.16.11.119
				172.16.11.120
2	Region A	Primary NSX Manager for the shared edge and compute cluster	172.16.11.66	172.16.31.118
				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://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

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

3 In the **Navigator** pane, under **Networking & Security**, click **Installation and Upgrade**.

4 On the **Upgrade** tab, select the **172.16.11.65 | Primary** NSX Manager instance from the drop-down menu.

5 Click **Plan Upgrade** in the central pane.

6 On the **Select Upgrade Plan** page of the **Upgrade Components** wizard, click **Plan Your Upgrade** and click **Next**.

7 On the **Plan Content** page, configure the following settings and click **Next**.

Setting		Value
Select Components	Clusters	Deselected
	Universal Logical Routers	Deselected
	NSX Edges	Deselected
	Service VMs	Deselected
Define Pause Upgrade Options	Pause between components	Enabled
	Pause on error	Enabled

8 On the **Review Plan** page, verify that **Pause between components** and **Pause on error** are set to `Yes`, and click **Start Upgrade**.

9 During the upgrade of the NSX Controller nodes, monitor the progress.

- **Upgrade** tab

  Click **View Details**. The **Upgrade Plan Progress** dialog box shows the overall progress of the controller upgrade.

- **Management** tab

  The **Status** column changes from `Connected`, at which point after the controller has been upgraded, the status turns to `Disconnected`, at which point the controller is back in the list and upgraded, and finally to `Connected` once again.

The **Upgrade Status** column shows the following stages:

1. `Not Started`
2. `Downloading Upgrade File`
3. `Download complete`
4. `Queued For Upgrade`
5. `Upgrade in progress` for each NSX Controller

   Note During this time, the other NSX Controllers might be in different states.

6. `Waiting to Rebooting`
7. `Rebooting`
8. `Upgraded`

10 After the upgrade is completed for each NSX Controller node, to confirm that all controllers are connected to the NSX Manager, on the **Management** tab, and in the **NSX Controller nodes** section, verify that the upgraded NSX Controller has the following configuration.

Setting	Expected Value
Status	Connected
Software Version	6.4.1.*build_number*

11 After the upgrade is complete for all NSX Controllers, on the **Upgrade** tab, click **Resume**.

12 After the upgrade of the NSX Controller cluster for the management cluster is completed, repeat the procedure on the NSX Controller cluster 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 Cluster instances in Region A and Region B, update the NSX Virtual Infrastructure Bundle (VIB) 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 cluster. You run the upgrade on the hosts of the management cluster first.

Table 4-5. NSX Manager Instances and Associated Clusters

Region	NSX Manager	NSX Manager IP Address	Cluster
Region A	Primary NSX Manager for the management cluster	172.16.11.65	**sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01-mgmt01**
	Primary NSX Manager for the shared edge and compute cluster	172.16.11.66	**sfo01w01vc01.sfo01.rainpole.local > sfo01-w01dc > sfo01-w01-comp01**

Table 4-5. NSX Manager Instances and Associated Clusters (Continued)

Region	NSX Manager	NSX Manager IP Address	Cluster
Region B	Secondary NSX Manager for the management cluster	172.17.11.65	**lax01m01vc01.lax01.rainpole.local > lax01-m01dc > lax01-m01-mgmt01**
	Secondary NSX Manager for the shared edge and compute cluster	172.17.11.66	**lax01w01vc01.lax01.rainpole.local > lax01-w01dc > lax01-w01-comp01**

Prerequisites

- Verify that vSphere DRS is enabled are set to `Fully Automated` on the clusters.
- Verify that vSphere vMotion functions correctly between the ESXI hosts in each cluster.
- Verify that all ESXi hosts are connected to vCenter Server.
- Verify that no ESXi hosts are in maintenance mode in vCenter Server.

Procedure

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

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

   b Log in using the following credentials.

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

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

3 In the **Navigator** pane, under **Networking & Security**, click **Installation and Upgrade**.

4 Click the **Upgrade** tab, select the **172.16.11.65 | Primary** NSX Manager instance from the drop-down menu.

5 Click **Plan Upgrade** in the central pane.

6 On the **Select Upgrade Plan** page of the **Upgrade Components** wizard, click **Plan Your Upgrade** and click **Next**.

7 On the **Plan Content** page, configure the following settings and click **Next**.

Setting		Value
Select Components	Clusters	Selected
	Universal Logical Routers	Deselected
	NSX Edges	Deselected
	Service VMs	Deselected

Setting		Value
Define Pause Upgrade Options	Pause between components	Enabled
	Pause on error	Enabled

8 On the **Plan Host Clusters** page, select the **Default Cluster Upgrade Group** radio button, and click **Edit**.

9 In the Edit Upgrade Group dialog box, verify that the following settings are configured, click **OK**, and on the **Plan Host Clusters** page click **Next**.

Setting	Expected Value
Selected Objects	sfo01-m01-mgmt01
Upgrade order	Serial

10 On the **Review Plan** page, verify that **Pause between components** and **Pause on error** are set to `Yes`, and click **Start Upgrade**.

11 Revalidate that the NSX Controllers are of version 6.4.*build_number*, and click **Resume** to proceed to the upgrade of the next cluster.

12 Monitor the progress.

- **Upgrade** tab

  Click **View Details**. The **Upgrade Plan Progress** dialog box shows the overall progress of the cluster upgrade. Click the **Details** button for additional information about each step.

- **Host Preparation** tab

  The **Installation Status** changes to `In Progress` while each of the ESXi host is updated. Each host is placed in to maintenance mode with its virtual machines migrated to another host, and updated.

13 Wait for the update of each ESXi host in the management cluster in Region A.

After the update of all ESXi hosts is completed, they are in a ready state, indicated by a green check mark, with a VIB version of `6.4.1.`*`build_number`*.

14 After the upgrade is completed for the management cluster in Region A, click **Resume**.

15 Repeat the steps to update the NSX components on the remaining clusters in Region A and Region B.

16 When you perform the upgrade on a secondary node in Region B, when prompted, provide the following user name and password in the **Enter Secondary Manager Credentials** dialog box and click **OK**.

Setting	Value
User name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_user_ password*

Upgrade the NSX Edge Instances

After you upgrade the control and data plane components of NSX for vSphere, upgrade the NSX Edge services gateway, universal distributed logical router, and load balancer instances.

For each NSX Manager instance in Region A and Region B, you run an upgrade for each universal distributed logical router (UDLR), distributed logical router (DLR), and the associated edge services gateways (ESG) in each region. By using the Upgrade Coordinator, you create an upgrade plan for the edge devices for the management cluster in Region A first. Then, proceed with the remaining clusters in each region.

Table 4-6. NSX Manager Instances and Associated Host Clusters

Region	NSX Manager	NSX Manager IP Address	Host Cluster
Region A	Primary NSX Manager for the management cluster	172.16.11.65	sfo01-m01-mgmt01
	Primary NSX Manager for the shared edge and compute cluster	172.16.11.66	sfo01-w01-comp01
Region B	Secondary NSX Manager for the management cluster	172.17.11.65	lax01-m01-mgmt01
	Secondary NSX Manager for the shared edge and compute cluster	172.17.11.66	lax01-w01-comp01

Table 4-7. NSX Edge Instances Upgrade Ordering for the Management Clusters

Order	Management UDLR in Region A	Management Edge in Region A with Availability Zones	Management Edge in Region B
1	sfo01m01udlr01	-	-

2	-	■ sfo01m01esg01
		■ sfo01m01esg02
		■ If using multiple availability zones
		  ■ sfo02m01esg01
		  ■ sfo02m01esg02
		■ sfo01m01lb01
		■ sfo01psc01
			-

3	-	-	■ lax01m01esg01 ■ lax01m01esg02 ■ lax01m01lb01 ■ lax01m01psc01

Table 4-8. NSX Edge Instances Upgrade Ordering Continued for the Shared Edge and Compute Clusters

Order	Compute UDLR in Region A	Edge and Compute in Region A	Edge and Compute in Region B
4	sfo01w01udlr01	-	-
5	-	■ sfo01w01dlr01 ■ sfo01w01esg01 ■ sfo01w01esg02	-
6	-	-	■ lax01w01dlr01 ■ lax01w01esg01 ■ lax01w01esg02

Procedure

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

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

   b Log in using the following credentials.

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

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

3 In the **Navigator** pane, under **Networking & Security**, click **Installation and Upgrade**.

4 Click the **Upgrade** tab, select the **172.16.11.65 | Primary** NSX Manager instance from the drop-down.

5 Click **Plan Upgrade** in the central pane.

6 On the **Select Upgrade Plan** page of the **Upgrade Components** wizard, click **Plan Your Upgrade,** and click **Next**.

7 On the **Plan Content** page, configure the following settings and click **Next**.

Setting		Value
Select Components	Universal Logical Routers	Selected
	NSX Edges	Selected
	Service VMs	Deselected
Define Pause Upgrade Options	Pause between components	Enabled
	Pause on error	Enabled

8 On the **Universal Logical Routers** page, select **universal_routers_*host_cluster***, and click **Edit**.

9 In the **Edit Upgrade Group** dialog box, verify that the following settings are configured, click **OK**.

Setting	Expected Value
Selected Objects	*Management UDLR in Region A* per NSX Edge Instances Upgrade Ordering
Upgrade order	Serial

10 On the **Plan NSX Edges** page, select **edge_*host cluster***, and click **Edit**.

11 In the **Edit Upgrade Group** dialog box, verify that the following settings are configured, click **OK**, and click **Next**.

Setting	Expected Value
Selected Objects	*Management Edge in Region A* per NSX Edge Instances Upgrade Ordering
Upgrade order	Serial

Performing the upgrade in a serialized order minimizes disruption on both the management and shared and edge compute clusters.

12 On the **Review Plan** page, verify that **Pause between components** and **Pause on error** are set to `Yes`, and click **Start Upgrade**.

13 Verify that the NSX Controllers are of version `6.4.1`*`build_number`*, and click **Resume** to proceed to the universal logical router upgrade.

14 Monitor the progress.

- **Upgrade** tab

  Click **View Details**. In the **Upgrade Plan Progress** dialog box, you can monitor the overall progress of the Universal Logical Router upgrade.

- **NSX Edges** section under the **Networking & Security** in the left pane

  The **Status** changes to `Busy` as the UDLR is updated.

15 After a successful upgrade of the UDLR, on the **NSX Edge** page under the **Networking & Security**, verify that the **Status** column for the edge device shows `Deployed`, and the **Version** column contains the upgraded version of `6.4.1`.

16 Click the **Upgrade** tab again, and click **Resume** to proceed with the NSX Edges upgrade.

17 Wait for upgrade of each NSX Edge instance by monitoring the progress.

18 After all the NSX Edge instances are upgraded, on the **NSX Edge** page under the **Networking & Security**, verify that the **Status** column for each edge device shows `Deployed`, and the **Version** column contains the upgraded version of `6.4.1`.

19 Repeat the steps to upgrade the NSX Edge instances in the management cluster of Region B .

20 When performing the upgrade to the secondary nodes in Region B, when prompted to provide a user name and password in the **Enter Secondary Manager Credentials**, enter the following credentials and click **OK**.

Setting	Value
User name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_user_ password*

21 Repeat the steps to upgrade the NSX Edge instances in the shared edge and compute cluster, starting with Region A and followed by Region B.

Post-Upgrade Configuration of NSX for vSphere

After you complete the upgrade of the NSX components in the virtual infrastructure layer, perform the post-upgrade configuration changes to the environment according to the design objectives and deployment guidance to ensure your environment remains aligned to this VMware Validated Design.

Disable BGP Graceful Restart for the Management NSX Edges in Region A

After you upgrade the NSX components for the virtual infrastructure layer, disable the graceful restart on the BGP configuration for the management cluster in NSX Edges in the Region A. You avoid potential traffic loss because the physical network and logical routers will clear the forwarding table during an ESG failure.

Table 4-9. NSX Edges for the Management Cluster in Region A

NSX Edge Name	NSX Edge Type
sfo01m01udlr01	Universal Distributed Logical Router
sfo01m01esg01	NSX Edge
sfo01m01esg02	NSX Edge
sfo02m01esg01	NSX Edge
sfo02m01esg01	NSX Edge

Procedure

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

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

b Log in using the following credentials.

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

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

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

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

5 Double-click **sfo01m01udlr01**.

6 On the **Manage** tab, click **Routing**.

7 Select **BGP**, and on the **BGP** page, click **Edit**.

8 In the **Edit BGP Configuration** dialog box, deselect the **Enable Graceful Restart** option and click **OK**.

9 Click **Publish Changes**.

10 Repeat the procedure for the other NSX Edge devices in the management cluster.

Disable BGP Graceful Restart on the Shared Edge and Compute NSX Edges in Region A

After you upgrade the NSX components for the virtual infrastructure layer, disable the graceful restart on the BGP configuration for the shared edge and compute cluster NSX Edges in the Region A. You avoid potential traffic loss because the physical network and logical routers will clear the forwarding table during an ESG failure.

Table 4-10. NSX Edges for the Shared Edge and Compute Cluster in Region A

NSX Edge Name	NSX Edge Type
sfo01w01udlr01	Universal Distributed Logical Router
sfo01w01dlr01	Logical Router
sfo01w01esg01	NSX Edge
sfo01w01esg02	NSX Edge

Procedure

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

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

b Log in using the following credentials.

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

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

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

4 Select **172.16.11.66** from the **NSX Manager** drop-down menu.

5 Double-click **sfo01w01udlr01**.

6 On the **Manage** tab, click **Routing**.

7 Select **BGP**, and on the **BGP** page, click **Edit**.

8 In the **Edit BGP Configuration** dialog box, deselect the **Enable Graceful Restart** option and click **OK**.

9 Click **Publish Changes**.

10 Repeat these steps for the other NSX Edges in the shared edge and compute cluster.

Disable Graceful Restart on the BGP Configuration for Management NSX Edges in Region B

After you upgrade the NSX components for the virtual infrastructure layer, disable the graceful restart on the BGP configuration for the management cluster NSX Edges in the Region B. You avoid potential traffic loss because the physical network and logical routers will clear the forwarding table during an ESG failure.

Table 4-11. NSX Edges for the Management Cluster in Region B

Device Name	Type
lax01m01esg01	NSX Edge
lax01m01esg02	NSX Edge

Procedure

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

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

   b Log in using the following credentials.

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

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

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

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

5 Double-click **lax01m01esg01**.

6 On the **Manage** tab, click **Routing**.

7 Select **BGP**, and on the **BGP** page, click **Edit**.

8 In the **Edit BGP Configuration** dialog box, deselect the **Enable Graceful Restart** option and click **OK**.

9 Click **Publish Changes**.

10 Repeat these steps for the other NSX Edge in the management cluster.

Disable BGP Graceful Restart on the Shared Edge and Computer NSX Edges in Region B

After you upgrade the NSX components for the virtual infrastructure layer, disable the graceful restart on the BGP configuration for the shared edge and compute cluster NSX Edges in the Region B. You avoid potential traffic loss because the physical network and logical routers will clear the forwarding table during an ESG failure.

Table 4-12. NSX Edges for the Shared Edge and Compute Cluster in Region B

NSX Edge Name	NSX Edge Type
lax01w01dlr01	Logical Router
lax01w01esg01	NSX Edge
lax01w01esg02	NSX Edge

Procedure

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

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

   b Log in using the following credentials.

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

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

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

4 Select **172.17.11.66** from the **NSX Manager** drop-down menu.

5 Double-click **lax01w01dlr01**.

6 On the **Manage** tab, click **Routing**.

7 Select **BGP**, and on the **BGP** page, click **Edit**.

8 In the **Edit BGP Configuration** dialog box, deselect the **Enable Graceful Restart** option and click **OK**.

9 Click **Publish Changes**.

10 Repeat these steps for the other NSX Edges in the shared edge and compute cluster.

Update the Components for the Management Cluster

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

Procedure

1 Update vSphere and Disaster Recovery Components for the Management Clusters

When you update the vSphere layer for the management components in the SDDC, you upgrade the Management Platform Services Controller, Management vCenter Server, vSphere Replication appliance, and Site Recovery Manager system in Region A. Then, you repeat this operation in Region B

2 Complete vSphere Update for the Management Cluster

After you update the management components from the virtual infrastructure layer of the SDDC that provide infrastructure management and disaster recovery, update the Update Manager Download Service (UMDS) instances followed by the ESXi hosts, and the VMware Tools on the management virtual machines in Region A and Region B.

Update vSphere and Disaster Recovery Components for the Management Clusters

When you update the vSphere layer for the management components in the SDDC, you upgrade the Management Platform Services Controller, Management vCenter Server, vSphere Replication appliance, and Site Recovery Manager system in Region A. Then, you repeat this operation in Region B

Upgrading the vSphere and disaster recovery layers in VMware Validated Design for the management clusters is a multi-step operation. 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 is with least impact on your ability to perform disaster recovery operations in the SDDC using the management components and with minimal operational impact to your tenant workloads and provisioning operations.

Table 4-13. Management vSphere and Disaster Recovery Nodes in the SDDC

Region	Role	IP Address	Fully Qualified Domain Name
Region A	Management Platform Services Controller that is configured in a highly available pair	172.16.11.61	sfo01m01psc01.sfo01.rainpole.local
	Compute Platform Services Controller that is configured in a highly available pair	172.16.11.63	sfo01w01psc01.sfo01.rainpole.local
	Management vCenter Server	172.16.11.62	sfo01m01vc01.sfo01.rainpole.local
	vSphere Replication	172.16.11.123	sfo01m01vrms01.sfo01.rainpole.local
	Site Recovery Manager	172.16.11.124	sfo01m01srm01.sfo01.rainpole.local
Region B	Management Platform Services Controller that is configured in a highly available pair	172.17.11.61	lax01m01psc01.lax01.rainpole.local

Table 4-13. Management vSphere and Disaster Recovery Nodes in the SDDC (Continued)

Region	Role	IP Address	Fully Qualified Domain Name
	Compute Platform Services Controller that is configured in a highly available pair	172.17.11.63	lax01w01psc01.lax01.rainpole.local
	Management vCenter Server	172.17.11.62	lax01m01vc01.lax01.rainpole.local
	vSphere Replication	172.17.11.123	lax01m01vrms01.lax01.rainpole.local
	Site Recovery Manager	172.17.11.124	lax01m01srm01.lax01.rainpole.local

Prerequisites

- For Management vCenter Server and Platform Services Controller virtual appliances:
  - Download the vCenter Server Appliance update `VMware-vCenter-Server-Appliance-6.5.0.x-build_number-patch-FP.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 all management ESXi hosts have the lockdown mode disabled during the upgrade.
  - Verify that any integration with the Management vCenter Server instances in the environment has been quiesced of all activities. Such activities include but are not limited to users performing active backups of components or provisioning of new virtual machines by using vRealize Automation. Without quiescing the environment, rollback operations can be disrupted by orphaned objects that might be generated after you have taken snapshots. You might also have to extend the time of the maintenance windows.
  - Verify that current backups of all Platform Services Controller and Management vCenter Server virtual appliances exist.
- For vSphere Replication
  - Download the vSphere Replication update `VMWare-vSphere_Replication-6.5.1-build_number.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 backup of the each vSphere Replication appliance that has been configured as a pair.
  - Verify that the Management Platform Services Controller and Management vCenter Server virtual appliances are successfully updated.
  - Verify that all services on the Management Platform Services Controller and Management vCenter Server virtual appliances are running.
- For Site Recovery Manager
  - Download the Site Recovery Manager update `VMware-srm-6.5.1-build_number.exe` file.
  - Create a backup of each Site Recovery Manager system that has been configured as a pair.
  - Verify that the Management Platform Services Controller and Management vCenter Server virtual appliances are successfully upgraded.
  - Verify that all services on the Management Platform Services Controller and Management vCenter Server instances 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. Take Snapshots of the Management vCenter Server and Platform Services Controller Instances in Region A and Region B

   Before you perform the update, take a snapshot of the Management vCenter Server virtual appliance and the Platform Services Controller virtual appliances in Region A and Region B. If you must perform a rollback to the previous state, these snapshots accelerate a rollback operation.

2. Update the Platform Services Controller Instances in Region A
3. Update Management vCenter Server in Region A
4. Update the vSphere Replication in Region A

   After you update the Management Platform Services Controller and vCenter Server virtual appliances in Region A, update the vSphere Replication virtual appliance in Region A.

5. Update Site Recovery Manager in Region A

   After you update vSphere Replication in Region A, proceed with the Site Recovery Manager update in Region A.

6. Update Platform Services Controller Instances in Region B
7. Update Management vCenter Server in Region B
8. Update the vSphere Replication in Region B

   Continue your update of the vSphere and disaster recovery components in the SDDC. After you update the Management vCenter Server virtual appliances in Region B, update the vSphere Replication virtual appliance in Region B.

9. Update Site Recovery Manager in Region B

   After you upgrade vSphere Replication in Region B, proceed to upgrading the Site Recovery Manager system in Region B to complete the upgrade of the infrastructure management components of the SDDC.

10. Delete the Snapshots of the vSphere Components in Region A and Region B

    After you complete the update of the management components in Region A and Region B and validate their stability, remove the snapshots from the virtual appliances.

What to do next

- Verify that the vSphere and Disaster Recovery components are functional.

Take Snapshots of the Management vCenter Server and Platform Services Controller Instances in Region A and Region B

Before you perform the update, take a snapshot of the Management vCenter Server virtual appliance and the Platform Services Controller virtual appliances in Region A and Region B. If you must perform a rollback to the previous state, these snapshots accelerate a rollback operation.

Region	Folder	Role	Virtual Machine Name
Region A	sfo01-m01fd-mgmt	vCenter Server	sfo01m01vc01
	sfo01-m01fd-mgmt	Platform Services Controller	sfo01m01psc01
	sfo01-m01fd-mgmt	Platform Services Controller	sfo01w01psc01
Region B	lax01-m01fd-mgmt	vCenter Server	lax01m01vc01
	lax01-m01fd-mgmt	Platform Services Controller	lax01m01psc01
	lax01-m01fd-mgmt	Platform Services Controller	lax01w01psc01

Procedure

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

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

   b Log in using the following credentials.

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

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

3 In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-mgmt** tree.

4 Right-click the **sfo01m01vc01** virtual machine and select **Snapshots > Take Snapshot**.

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

Setting	Value
Name	VMware Validated Design 4.3 Virtual Infrastructure Layer Upgrade
Description	-
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

6 Repeat the procedure for the Management vCenter Server virtual appliance in Region B and Platform Services Controller virtual appliances in each region.

Update the Platform Services Controller Instances in Region A

When you update the vSphere components in Region A and Region B, update the Platform Services Controller virtual appliances configured in a highly available pair in Region A first.

Table 4-14. Platform Services Controller Instances in Region A

Role	Virtual Machine Name	Fully Qualified Domain Name
Platform Services Controller for the management cluster	sfo01m01psc01	sfo01m01psc01.sfo01.rainpole.local
Platform Services Controller for the shared edge and compute cluster	sfo01w01psc01	sfo01w01psc01.sfo01.rainpole.local

Prerequisites

- Verify that current backups of the Platform Services Controller virtual appliances in Region A exist.
- Mount the update `VMware-vCenter-Server-Appliance-6.5.0.x-build_number-patch-FP.iso` file to the virtual appliances from the vSphere Web Client.

Procedure

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

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

   b Log in using the following credentials.

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

2 On the load balancer for the Platform Services Controller virtual appliances, direct the traffic only to the Compute Platform Services Controller and disable health monitoring for the Management Platform Services Controller.

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

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

   c From the **NSX Manager** drop-down menu, select the NSX Manager for the management cluster in Region A **172.16.11.65** and double-click the **sfo01psc01** device to open its settings.

   d On the **Manage** tab, click the **Load Balancer** tab and click **Pools**.

   e Select **psc-https-443** and click **Edit**.

   f In the **Edit Pool** dialog box, select the **sfo01m01psc01** node from the member nodes, click **Edit**, select **Disable** from the **State** drop-down menu and click **OK**.

   g Repeat the steps on the remaining **psc-tcp-389** load balancer pool.

   h On the **Pools** page, click **Show Pools Statistics** and verify that both psc-https-443 and psc-tcp-389 report status `DOWN` for sfo01m01psc01.

3 Log in to the appliance management interface (VAMI) of the Management Platform Services Controller.

   a Open a Web browser and go to **`https://sfo01m01psc01.sfo01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*mgmtpsc_root_password*

4 Upgrade the appliance.

   a In the appliance management interface, click **Update** in the left pane.

   b In the **Update** pane, click **Check Updates** and select **Check CDROM**.

   c Verify that the **Available Updates** shown match the version in VMware Software Versions in the Upgrade, click **Install Updates** and select **Install CDROM Updates**.

   d In the **End User License Agreement** dialog box, accept the EULA and click **Install**.

   e After the update completes, click **OK** in the **Installing Upgrades** dialog box.

5 Restart the appliance to apply the upgrade.

   a Click the **Summary** tab, and click **Reboot**.

   b In the **System Reboot** dialog box, click **Yes**.

6 After the restart completes, log back in to the virtual appliance management interface, and verify the version number in the **Update** pane.

7 Enable the traffic direction to the Management Platform Services Controller and enable health monitoring on the load balancer.

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

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

   c From the **NSX Manager** drop-down menu, select the NSX Manager for the management cluster in Region A **172.16.11.65** and double-click the **sfo01psc01** device to open its settings.

   d On the **Manage** tab, click the **Load Balancer** tab and click **Pools**.

   e Select **psc-https-443** and click **Edit**.

   f In the **Edit Pool** dialog box, select the **sfo01m01psc01** node from the member nodes, click **Edit**, select **Enable** from the **State** drop-down menu and click **OK**.

   g Repeat the steps on the other load balancer pool, **psc-tcp-443**.

   h On the **Pools** page, click **Show Pools Statistics** and confirm that both **psc-https-443** and **psc-tcp-443** report status `UP` for sfo01m01psc01.

8 Disconnect the attached update `.iso` file from the Platform Services Controller virtual appliance.

9 Repeat the procedure on the sfo01w01psc01 virtual appliance..

Update Management vCenter Server in Region A

When you update the vSphere components in Region A and Region B, after you complete the upgrade to the Platform Services Controller virtual appliances in Region A first, you update the Management vCenter Server in Region A.

Prerequisites

- Verify that a current backup of the Management vCenter Server virtual appliance in Region A exists. See the *VMware Validated Design Backup and Restore* documentation.
- Mount the update `VMware-vCenter-Server-Appliance-6.5.0.x-build_number-patch-FP.iso` file to the virtual appliance.

Procedure

1 Log in to the appliance management interface (VAMI) of the Management vCenter Server.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*mgmtvc_root_password*

2 Upgrade the appliance.

   a In the appliance management interface, click **Update** in the left pane.

   b In the **Update** pane, click **Check Updates** and select **Check CDROM**.

   c Verify that the **Available Updates** shown match the version in VMware Software Versions in the Upgrade, click **Install Updates** and select **Install CDROM Updates**.

   d In the **End User License Agreement** dialog box, accept the EULA and click **Install**.

   e After the update completes, click **OK** in the **Installing Upgrades** dialog box.

3 Restart the appliance to apply the upgrade.

   a Click the **Summary** tab, and click **Reboot**.

   b In the **System Reboot** dialog box, click **Yes**.

4 After the restart completes, log back in to the virtual appliance management interface, and verify the version number in the **Update** pane.

5 Disconnect the attached update `.iso` from the Management vCenter Server virtual appliance.

Update the vSphere Replication in Region A

After you update the Management Platform Services Controller and vCenter Server virtual appliances in Region A, update the vSphere Replication virtual appliance in Region A.

Prerequisites

- Verify that a current backup of the vSphere Replication virtual appliances in both Region A and Region B exists.
- Mount the upgrade `VMWare-vSphere_Replication-6.5.1-build_number.iso` file to the virtual appliance.

Procedure

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

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

   b Log in using the following credentials.

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

2 Take a snapshot of the vSphere Replication virtual appliance in Region A.

   a From the **Home** menu, click **VMs and Templates** and expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-bcdr** tree.

   b Right-click the **sfo01m01vrms01** virtual machine and select **Snapshots > Take Snapshot**.

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

Setting	Value
Name	VMware Validated Design 4.3 Business Continuity Layer Upgrade
Description	-
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

3 Log in to the Virtual Appliance Management Interface of the vSphere Replication virtual appliance.

   a Open a Web browser and go to **`https://sfo01m01vrms01.sfo01.rainpole.local:5480`** .

   b Log in using the following credentials.

Settings	Value
User name	root
Password	*vr_sfo_root_password*

4 Click the **Update** tab and click **Settings**.

5 Under the **Update Repository** section, select the **Use CDROM Updates** radio button and click **Save Settings**.

6 Click **Status** and click **Check Updates** to load the update from the `.iso` file.

7 Validate that **Available Updates** match the version defined by *VMware Validated Design Software Components* and click **Install Updates**.

8 In the **Install Update** dialog box, click **OK.**

9 After the update completes, click the **System** tab and click **Reboot**.

10 In the **System Reboot** dialog box, click **Reboot**.

   During the update process, after you have initiated the reboot, the virtual appliance reboots two times during the update.

11 After the vSphere Replication virtual appliance restarts, log in to the Virtual Appliance Management Interface and re-register the vSphere Replication virtual appliance with the Platform Services Controller.

   a Open a Web browser and go to **`https://sfo01m01vrms01.sfo01.rainpole.local:5480`**.

   b Log in using the following credentials.

Settings	Value
User name	root
Password	*vr_sfo_root_password*

   c On the **VR** tab, click **Configuration**.

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	sfo01psc01.sfo01.rainpole.local
SSO Administrator	svc-vr@rainpole.local
Password	*svc-vr_password*
VRM Host	172.16.11.123
VRM Site Name	sfo01m01vc01.sfo01.rainpole.local
vCenter Server Address	sfo01m01vc01.sfo01.rainpole.local
vCenter Server Port	80
vCenter Server Admin Mail	*vcenter_server_admin_email*

e After the restart is completed, ensure that the **Service Status** section on the **Configuration** tab shows that the VRM service is `running`.

12 Close all browser sessions to the vSphere Web Client and clear the browser cache.

13 Disconnect the attached update `.iso` from the vSphere Replication virtual appliance.

Update Site Recovery Manager in Region A

After you update vSphere Replication in Region A, proceed with the Site Recovery Manager update in Region A.

Prerequisites

Verify that current backups of the Site Recovery Manager virtual machines in Regions A and Region B exist.

Procedure

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

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

b Log in using the following credentials.

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

2 Take a snapshot of the Site Recovery Manager Windows virtual machine.

   a From the **Home** menu, select **VMs and Templates** and expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-bcdr** tree.

   b Right-click the **sfo01m01srm01** virtual machine and select **Snapshots > Take Snapshot**.

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

Setting	Value
Name	VMware Validated Design 4.3 Business Continuity Layer Upgrade
Description	-
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 Site Recovery Manager virtual machine by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to **`sfo01m01srm01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	*Windows_administrator_password*

4 Copy the upgrade `VMware-srm-6.x.x.exe` file to the Site Recovery Manager virtual machine.

5 Navigate to the folder where you downloaded the VMware Site Recovery Manager update installer, right-click and select **Run as Administrator** to start the installation wizard.

6 On the **Select Language** dialog box click **OK**.

7 On the **Welcome** page, click **Next**.

8 On the **VMware Patents** page, click **Next**.

9 On the **End User License Agreement** page, select **I agree to the terms in the license agreement**, and click **Next**.

10 On the **Installation Prerequisites** page, click **Next**.

11 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	sfo01psc01.sfo01.rainpole.local
HTTPS Port	443

Setting	Value
Username	svc-srm@rainpole.local
Password	svc-*srm_password*

12 If prompted, in the **Platform Services Controller Certificate** dialog box, review the details of the certificate and click **Accept**.

13 On the **VMware vCenter Server** page, validate that the settings for vCenter Server sfo01m01vc01.sfo01.rainpole.local are correct, and click **Next**.

14 If prompted, in the **vCenter Server Certificate** dialog box, review the details of the certificate and click **Accept**.

15 On the **Site Recovery Manager Extension** page, verify that the following settings are intact and click **Next**.

Setting	Value
Administrator E-Mail	*srm_admin_sfo_email_address*
Local Host	172.16.11.124
Listener Port	9086

16 If prompted, about the Platform Services Controller being already registered, in the **VMware vCenter Site Recovery Manager** dialog box, click **Yes** on the **Your Site Recovery Manager extension is already registered** prompt and click **Yes** on the **Existing Site Recovery Manager registrations** prompt.

17 On the **Certificate Type** page, select **Use existing certificate** and click **Next**.

18 On the **Embedded Database Configuration** page, re-enter the Site Recovery Manager **srm_db_admin** password for the database, validate the following settings and click **Next**.

Setting	Value
Data Source Name	SRM_SITE_SFO
Database User Name	srm_db_admin
Database Password	*srm_db_admin_sfo_password*
Database Port	5678
Connection Count	5
Max. Connections	20

19 On the **Site Recovery Manager Service Account** page, click **Use Local System account** and click **Next**.

20 On the **Ready to Install the Program** page, click **Install**.

21 After you upgrade Site Recovery Manager, close all browser sessions to the vSphere Web Client and clear the browser cache.

22 Check for the latest Site Recovery Manager plug-in in the vSphere Web Client.

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

b Log in using the following credentials.

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

c From the **Home** menu, select **Administration**.

d In the **Navigator** pane, under **Solutions**, click **Client Plug-Ins**.

e In the **Client Plug-Ins** section, click the **Check for New Plug-ins** button.

f In the **Checking for New Plug-ins** pop-up window, click **Go to the Event Console**.

g In the **Events Console**, enter **`plug-in`** in the filter text box and locate the following events.

```
The deployment of plug-in Site Recovery Manager 6.5.1.xxxxx has started
The deployment of plug-in Site Recovery Manager 6.5.1.xxxxx is successful
```

h After you locate both events, log out and back in to the vSphere Web Client, navigate back to the **Client Plug-Ins** section, and verify that the **SRM Client** version has been updated properly.

i If the new client plug-in does not appear, restart the vSphere Web Client service on the Management vCenter Server using SSH.

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

Update Platform Services Controller Instances in Region B

After you complete the update of the management virtual infrastructure and disaster recovery layers in Region A, you upgrade the Platform Services Controller instances for the management cluster in Region B.

Role	Virtual Machine Name	Fully Qualified Domain Nam
Platform Services Controller for the management cluster	lax01m01psc01	lax01m01psc01.lax01.rainpole.local
Platform Services Controller for the shared edge and compute cluster	lax01w01psc01	lax01w01vc01.lax01.rainpole.local

Prerequisites

- Verify that current backups of the Platform Services Controller virtual appliances in Region B exist.
- Mount the update `VMware-vCenter-Server-Appliance-6.5.0.x-build_number-patch-FP.iso` file to the virtual appliances.

Procedure

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

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

   b Log in using the following credentials.

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

2 On the load balancer for the Platform Services Controller instances, direct the traffic only to the Compute Platform Services Controller and disable health monitoring for the Management Platform Services Controller.

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

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

   c From the **NSX Manager** drop-down menu, select the NSX Manager for the management cluster in Region B **172.17.11.65** and double-click the **lax01psc01** device to open its settings.

   d On the **Manage** tab, click the **Load Balancer** tab and click **Pools**.

   e Select **psc-https-443** and click **Edit**.

   f In the **Edit Pool** dialog box, select the **lax01m01psc01** node from the member nodes, click **Edit**, select **Disable** from the **State** drop-down menu and click **OK**.

   g Repeat the steps on the other load balancer pool, **psc-tcp-443**.

   h On the **Pools** page, click **Show Pools Statistics** and verify that both psc-https-443 and psc-tcp-443 report status `DOWN` for lax01m01psc01.

3 Log in to the appliance management interface (VAMI) of the Management Platform Services Controller.

   a Open a Web browser and go to **`https://lax01m01psc01.lax01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*mgmtpsc_root_password*

4 Upgrade the appliance.

   a In the appliance management interface, click **Update** in the left pane.

   b In the **Update** pane, click **Check Updates** and select **Check CDROM**.

c Verify that the **Available Updates** shown match the version in VMware Software Versions in the Upgrade, click **Install Updates** and select **Install CDROM Updates**.

d In the **End User License Agreement** dialog box, accept the EULA and click **Install**.

e After the update completes, click **OK** in the **Installing Upgrades** dialog box.

5 Restart the appliance to apply the upgrade.

a Click the **Summary** tab, and click **Reboot**.

b In the **System Reboot** dialog box, click **Yes**.

6 After the restart completes, log back in to the virtual appliance management interface, and verify the version number in the **Update** pane.

7 Enable the traffic direction to the Management Platform Services Controller and enable health monitoring on the load balancer.

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

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

c From the **NSX Manager** drop-down menu, select the NSX Manager for the management cluster in Region A **172.17.11.65** and double-click the **lax01psc01** device to open its settings.

d On the **Manage** tab, click the **Load Balancer** tab and click **Pools**.

e Select **psc-https-443** and click **Edit**.

f In the **Edit Pool** dialog box, select the **lax01m01psc01** node from the member nodes, click **Edit**, select **Enable** from the **State** drop-down menu and click **OK**.

g Repeat the steps on the load balancer pool, **psc-tcp-443**.

h On the **Pools** page, click **Show Pools Statistics** and confirm that both **psc-https-443** and **psc-tcp-443** report status `UP` for lax01m01psc01.

8 Disconnect the attached update `.iso` file from the Platform Services Controller instance.

9 Repeat the procedure on the lax01w01psc01 virtual appliance.

Update Management vCenter Server in Region B

When you update the vSphere components in Region B, after you update the Platform Services Controller instances, you proceed with upgrading the Management vCenter Server in Region B.

Prerequisites

- Verify that a current backup of the Management vCenter Server virtual appliance in Regions B exists.
- Mount the update `VMware-vCenter-Server-Appliance-6.5.0.x-`*`build_number`*`-patch-FP.iso` file to the virtual appliance.

Procedure

1 Log in to the appliance management interface (VAMI) of the Management vCenter Server.

   a Open a Web browser and go to **`https://lax01m01vc01.lax01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vcenter_server_root_password*

2 Upgrade the appliance.

   a In the appliance management interface, click **Update** in the left pane.

   b In the **Update** pane, click **Check Updates** and select **Check CDROM**.

   c Verify that the **Available Updates** shown match the version in VMware Software Versions in the Upgrade, click **Install Updates** and select **Install CDROM Updates**.

   d In the **End User License Agreement** dialog box, accept the EULA and click **Install**.

   e After the update completes, click **OK** in the **Installing Upgrades** dialog box.

3 Restart the appliance to apply the upgrade.

   a Click the **Summary** tab, and click **Reboot**.

   b In the **System Reboot** dialog box, click **Yes**.

4 After the restart completes, log back in to the virtual appliance management interface, and verify the version number in the **Update** pane.

5 Disconnect the attached update `.iso` from the Management vCenter Server virtual appliance.

Update the vSphere Replication in Region B

Continue your update of the vSphere and disaster recovery components in the SDDC. After you update the Management vCenter Server virtual appliances in Region B, update the vSphere Replication virtual appliance in Region B.

Prerequisites

- Verify that a current backup of the vSphere Replication virtual appliance in Region B exists.
- Mount the update `VMWare-vSphere_Replication-6.5.1.`*`x-build_number`*`.iso` file to the virtual appliance.

Procedure

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

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

   b Log in using the following credentials.

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

2 Take a snapshot of the vSphere Replication virtual appliance in Region B.

   a From the **Home** menu, click **VMs and Templates** and expand the **lax01m01vc01.lax01.rainpole.local > lax01-m01dc > lax01-m01fd-bcdr** tree.

   b Right-click the **lax01m01vrms01** virtual machine and select **Snapshots > Take Snapshot**.

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

Setting	Value
Name	VMware Validated Design 4.3 Business Continuity Layer Upgrade
Description	-
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

3 Log in to the Virtual Appliance Management Interface of the vSphere Replication virtual appliance.

   a Open a Web browser and go to **`https://lax01m01vrms01.lax01.rainpole.local:5480`**.

   b Log in using the following credentials.

Settings	Value
User name	root
Password	*vr_lax_root_password*

4 Click the **Update** tab and click **Settings**.

5 Under the **Update Repository** section, select the **Use CDROM Updates** radio button and click **Save Settings**.

6 Click **Status** and click **Check Updates** to load the update from the `.iso` file.

7 Validate that **Available Updates** match the version defined by *VMware Validated Design Software Components* and click **Install Updates**.

8 In the **Install Update** dialog box, click **OK.**

9 After the update completes, click the **System** tab and click **Reboot**.

10 In the **System Reboot** dialog box, click **Reboot**.

   During the update process, after you have initiated the reboot, the virtual appliance reboots two times during the update.

11 After the vSphere Replication virtual appliance reboots, log in to the Virtual Appliance Management Interface and re-register the vSphere Replication appliance with the Platform Services Controller.

   a Open a Web browser and go to **`https://lax01m01vrms01.lax01.rainpole.local:5480`**.

   b Log in using the following credentials.

Settings	Value
User name	root
Password	*vr_lax_root_password*

   c On the **VR** tab, click **Configuration**.

   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	lax01psc01.lax01.rainpole.local
SSO Administrator	svc-vr@rainpole.local
Password	*svc-vr_password*
VRM Host	172.17.11.123
VRM Site Name	lax01m01vc01.lax01.rainpole.local
vCenter Server Address	lax01m01vc01.lax01.rainpole.local
vCenter Server Port	80
vCenter Server Admin Mail	*vcenter_server_admin_email*

   e After the restart is completed, verify that the **Service Status** section on the **Configuration** tab reports that the VRM service is **`running`**.

12 Close all browser sessions to the vSphere Web Client and clear the browser cache.

13 Disconnect the attached update `.iso` from the vSphere Replication virtual appliance.

Update Site Recovery Manager in Region B

After you upgrade vSphere Replication in Region B, proceed to upgrading the Site Recovery Manager system in Region B to complete the upgrade of the infrastructure management components of the SDDC.

Procedure

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

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

   b Log in using the following credentials.

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

2 Take a snapshot of the Site Recovery Manager virtual machine in Region B.

   a From the **Home** menu, click **VMs and Templates** and expand the **lax01m01vc01.lax01.rainpole.local > lax01-m01dc > lax01-m01fd-bcdr** tree.

   b Right-click the **lax01m01srm01** virtual machine and select **Snapshots > Take Snapshot**.

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

Setting	Value
Name	VMware Validated Design 4.3 Business Continuity Layer Upgrade
Description	-
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 Site Recovery Manager virtual machine by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to the virtual machine **`lax01m01srm01.lax01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	*Windows_administrator_password*

4 Copy the update`VMware-srm-6.5.1-`*`build_number`*`.exe` file to the Site Recovery Manager Windows virtual machine .

5 Navigate to the folder where you downloaded the VMware Site Recovery Manager update installer, right-click, and select **Run as Administrator** to start the installation wizard.

6 In the **Select Language** dialog box, click **OK**.

7 On the **Welcome** page, click **Next**.

8 On the **VMware Patents** page, click **Next**.

9 On the **End User License Agreement** page, select **I agree to the terms in the license agreement**, and click **Next**.

10 On the **Installation Prerequisites** page, click **Next**.

11 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	lax01psc01.lax01.rainpole.local
HTTPS Port	443
Username	svc-srm@rainpole.local
Password	*svc-srm_password*

12 If prompted, in the **Platform Services Controller Certificate** dialog box, review the details of the certificate and click **Accept**.

13 On the **VMware vCenter Server** page, validate that the settings for vCenter Server lax01m01vc01.lax01.rainpole.local are correct, and click **Next**.

14 If prompted, in the **vCenter Server Certificate** dialog box, review the details of the certificate and click **Accept**.

15 On the **Site Recovery Manager Extension** page, verify that the following settings are intact and click **Next**.

Setting	Value
Administrator E-Mail	*srm_admin_lax_email_address*
Local Host:	172.17.11.124
Listener Port:	9086

16 If prompted, about the Platform Services Controller being already registered, in the **VMware vCenter Site Recovery Manager** dialog box, click **Yes** on the **Your Site Recovery Manager extension is already registered** prompt and click **Yes** on the **Existing Site Recovery Manager registrations** prompt.

17 On the **Certificate Type** page, select **Use existing certificate** and click **Next**.

18 On the **Embedded Database Configuration** page, re-enter the Site Recovery Manager **srm_db_admin** password for the database, validate the following settings, and click **Next**.

Setting	Value
Data Source Name	SRM_SITE_LAX
Database User Name	srm_db_admin
Database Password	*srm_db_admin_lax_password*
Database Port	5678

Setting	Value
Connection Count	5
Max. Connections	20

19 On the **Site Recovery Manager Service Account** page, click **Use Local System account** and click **Next**.

20 On the **Ready to Install the Program** page, click **Install**.

21 After you upgrade the Site Recovery Manager, close all browser sessions to the vSphere Web Client and clear the browser cache.

22 Check for the latest Site Recovery Manager plug-in in the vSphere Web Client.

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

b Log in using the following credentials.

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

c From the **Home** menu, select **Administration**.

d In the **Navigator** pane, under **Solutions**, click **Client Plug-Ins**.

e In the **Client Plug-Ins** section, click the **Check for New Plug-ins** button.

f In the **Checking for New Plug-ins** pop-up window, click **Go to the Event Console**.

g In the **Events Console**, enter **`plug-in`** in the filter text box and locate the following events.

```
The deployment of plug-in Site Recovery Manager 6.5.1.xxxxx has started
The deployment of plug-in Site Recovery Manager 6.5.1.xxxxx is successful
```

h After you locate both events, log out and back in to the vSphere Web Client, navigate back to the **Client Plug-Ins** section, and verify that the **SRM Client Version** has been updated properly.

23 Restart the vSphere Web Client service on the Management vCenter Server using SSH.

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

24 Reconnect the Site Recovery Manager instances in Region A and Region B.

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

b Log in using the following credentials.

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

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

d On the **Site Recovery** page, click **Sites**

e On the **Sites** page, right-click **sfo01m01vc01.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**.

Setting	Value
PSC address	lax01psc01.lax01.rainpole.local
Port	443

g On the **Select vCenter Server** page, enter the password for the **svc-vr@rainpole.local** user, validate the following settings, and click **Finish**.

Setting	Value
vCenter Servers with matching SRM Extension	lax01m01vc01.lax01.rainpole.local
Username	svc-vr@rainpole.local
Password	*svc-vr_password*

h If prompted, in the **Security Alert** dialog box, review the certificate thumbprints for lax01m01vc01.lax01.rainpole.local and lax01psc01.lax01.rainpole.local, and click **Yes**.

i If prompted, in the **Security Alert** dialog box, review the certificate thumbprints for sfo01m01vc01.sfo01.rainpole.local and sfo01psc01.sfo01.rainpole.local , and click **Yes**.

25 On the **Sites** page in the **Navigator** pane, click **sfo01m01vc01.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`.

Delete the Snapshots of the vSphere Components in Region A and Region B

After you complete the update of the management components in Region A and Region B and validate their stability, remove the snapshots from the virtual appliances.

Region	Folder	Role	Virtual Machine Name
Region A	sfo01-m01fd-mgmt	vCenter Server	sfo01m01vc01
	sfo01-m01fd-mgmt	Platform Services Controller	sfo01m01psc01
	sfo01-m01fd-mgmt	Platform Services Controller	sfo01w01psc01
Region B	lax01-m01fd-mgmt	vCenter Server	lax01m01vc01
	lax01-m01fd-mgmt	Platform Services Controller	lax01m01psc01
	lax01-m01fd-mgmt	Platform Services Controller	lax01w01psc01

Procedure

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

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

   b Log in using the following credentials.

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

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

3 In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-mgmt** tree.

4 Right-click the **sfo01m01vc01** virtual machine and select **Snapshots > Delete All Snapshots**.

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

6 Repeat the procedure for the Management vCenter Server in Region B and the Platform Services Controller virtual appliances in both regions.

Complete vSphere Update for the Management Cluster

After you update the management components from the virtual infrastructure layer of the SDDC that provide infrastructure management and disaster recovery, update the Update Manager Download Service (UMDS) instances followed by the ESXi hosts, and the VMware Tools on the management virtual machines in Region A and Region B.

Upgrading the remaining components of vSphere in the management clusters is a multi-step operation in which you must upgrade the UMDS instances and management ESXi hosts,. Then, you repeat these operations in Region B. This sequence is with least impact on your ability to perform disaster recovery operations in the SDDC using the management components and with minimal operational impact to your tenant workloads and provisioning operations.

Table 4-15. Management ESXi Hosts and UMDS Nodes in the SDDC

Region	Cluster Name	IP Address	Fully Qualified Domain Name	vSAN Datastore
Region A	sfo01-m01-mgmt01	192.168.31.67	sfo01umds01.sfo01.rainpole.local	-
		172.16.11.101	sfo01m01esx01.sfo01.rainpole.local	sfo01-m01-vsan01
		172.16.11.102	sfo01m01esx02.sfo01.rainpole.local	
		172.16.11.103	sfo01m01esx03.sfo01.rainpole.local	
		172.16.11.104	sfo01m01esx04.sfo01.rainpole.local	
		172.16.11.1*xx*	sfo01m01esx*xx*.sfo01.rainpole.local	
Region B	lax01-m01-mgmt01	192.168.32.67	lax01umds01.lax01.rainpole.local	-
		172.17.11.101	lax01m01esx01.lax01.rainpole.local	lax01-m01-vsan01
		172.17.11.102	lax01m01esx02.lax01.rainpole.local	
		172.17.11.103	lax01m01esx03.lax01.rainpole.local	
		172.17.11.104	lax01m01esx04.lax01.rainpole.local	
		172.17.11.1*xx*	lax01m01esx*xx*.lax01.rainpole.local	

Table 4-16. Management Virtual Machines for VMware Tools Remediation in the SDDC

Region	Cluster Name	Folder	Role	Virtual Machine Name
Region A	sfo01-m01-mgmt01	sfo01-m01fd-mgmt	Update Manager Download Service	sfo01umds01
		sfo01-m01fd-vra	vRealize Automation IaaS Web Server	vra01iws01a
				vra01iws01b
			vRealize Automation IaaS Manager Service	vra01ims01a
				vra01ims01b

Table 4-16. Management Virtual Machines for VMware Tools Remediation in the SDDC (Continued)

Region	Cluster Name	Folder	Role	Virtual Machine Name
			vRealize Automation IaaS DEM Workers	vra01dem01a
				vra01dem01b
			Microsoft SQL Server	vra01mssql01
		sfo01-m01fd-vraias	vRealize Automation IaaS Proxy Agent	sfo01ias01a
				sfo01ias01b
		sfo01m01srm01	Site Recovery Manager	sfo01m01srm01
Region B	lax01-m01-mgmt01	lax01-m01fd-mgmt	Update Manager Download Service	lax01umds01
		lax01-m01fd-mgmt	vRealize Automation IaaS Proxy Agent	lax01ias01a
				lax01ias01b

Prerequisites

- For Update Manager Download Service instances
  - Verify that a current backup of all Update Manager Download Service virtual machines exists.
  - Download the vCenter Server Appliance installer `VMware-VCSA-all-6.5.0-`*`build_number`*`.iso` file to a shared datastore for mounting to the virtual appliances. If you have space on your NFS datastore, upload the file there.
- For ESXi hosts and vSAN clusters
  - Verify that the system hardware complies with the ESXi requirements. See VMware Compatibility Guide. Check for the following compatibility areas:
    - System compatibility
    - I/O compatibility with network and host bus adapter (HBA) cards
    - Storage compatibility
    - Backup software compatibility
    - Compatibility of the firmware for the network and host bus adapter (HBA) cards. Upgrade the firmware accordingly.
    - BIOS compatibility. Upgrade the BIOS on the ESXi hosts accordingly.
  - Verify that vSphere DRS on the management cluster is set to `Fully Automated` for the duration of the upgrade operations to have management workloads automatically migrated from hosts while they are being upgraded.
- For VMware Tools
  - Verify that all ESXi hosts in the management cluster have been upgraded.

- 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 might automate the ordering of new virtual machines.
- Verify that the maintenance window is in a time period in which no backup jobs are running or scheduled to run.
- Verify that a backup of all UMDS virtual machines exist.

Procedure

1 Upgrade vSphere Update Manager Download Service in Region A

After you update of the vCenter Server instances in Region A and Region B, update the vSphere Update Manager Download Service (UMDS) so that you can update the ESXi hosts.

2 Update the ESXi Hosts in the Management Cluster in Region A

After you update UMDS, you can proceed with updating the management ESXi hosts in Region A. You use vSphere Update Manager for automated host update across the management cluster.

3 Remediate VMware Tools in the Management Cluster in Region A

After you update the ESXi hosts running the management virtual machines, update the VMware Tools on the virtual machines of the management components in Region A. To remediate the management virtual machines that are running earlier version of VMware Tools, create a baseline group so that vSphere Update Manager on the Management vCenter Server in Region A can automatically identify them.

4 Update vSphere Update Manager Download Service, Management ESXi Hosts, and VMware Tools in Region B

In a dual-region SDDC, after you complete the update of the virtual infrastructure components for the management cluster in Region A, start the update of vSphere Update Manager Download Service (UMDS), management ESXi hosts, and VMware Tools in Region B. Upgrading both regions enables failover and failback between Region A and Region B.

What to do next

- Verify that the Update Manager Download Service is operational after the upgrade.
- Verify that the management ESXi hosts are operational after the upgrade.
- Verify that the management virtual machines are operational after the upgrade.

Upgrade vSphere Update Manager Download Service in Region A

After you update of the vCenter Server instances in Region A and Region B, update the vSphere Update Manager Download Service (UMDS) so that you can update the ESXi hosts.

You cannot update UMDS that runs on a Linux-based operating system. You uninstall the current version of UMDS, perform a fresh installation of UMDS according to all system requirements, and use the existing patch store configured for the UMDS instance that you uninstalled.

Prerequisites

- Verify that a current backup of the UMDS virtual machine exists.
- Download the installer `VMware-VCSA-all-6.5.0-build_number.iso` file of the vCenter Server Appliance to a shared datastore for mounting to the virtual appliance. If you have space on your NFS datastore, upload the file there.

Region	IP Address	Fully Qualified Domain Name	Cluster Name	Folder name
Region A	192.168.31.67	sfo01umds01.sfo01.rainpole.local	sfo01-m01-mgmt01	sfo01-m01fd-mgmt

Procedure

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

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

   b Log in using the following credentials.

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

2 Take a snapshot of the UMDS virtual machine in Region A.

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

   b In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01fd-mgmt** tree.

   c Right-click the **sfo01umds01** virtual machine and select **Snapshots > Take Snapshot**.

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

Setting	Value
Name	VMware Validated Design 4.3 Virtual Infrastructure Layer Upgrade
Description	-
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

3 Mount the `.iso` to the virtual machine.

4 Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.

a Open an SSH connection to sfo01umds01.sfo01.rainpole.local.

b Log in using the following credentials.

Setting	Value
User name	svc-umds
Password	*svc-umds_password*

5 Uninstall the current version of Update Manager Download Service.

a Navigate to the UMDS installation directory by running the following command.

```
cd /usr/local/vmware-umds
```

b Run the following command to uninstall UMDS.

```
sudo ./vmware-uninstall-umds.pl
```

c Enter **Yes** to confirm.

6 Prepare for running the installation script.

a Mount the vCenter Server Appliance ISO to the UMDS virtual machine.

```
sudo mkdir -p /mnt/cdrom
sudo mount /dev/cdrom /mnt/cdrom
```

b Unarchive the VMware-UMDS-6.5.0-*build_number*.tar.gz file:

```
tar -xzvf /mnt/cdrom/umds/VMware-UMDS-6.5.0-build_number.tar.gz -C /tmp
```

7 Install the latest version of UMDS.

a Run the UMDS installation script.

```
sudo /tmp/vmware-umds-distrib/vmware-install.pl
```

b Read and accept the EULA.

c Press Enter to install UMDS in the default directory /usr/local/vmware-umds and enter **yes** to confirm directory creation.

d Enter the UMDS proxy settings if needed according to the settings of your environment.

e Press Enter to set the patch location to /var/lib/vmware-umds and enter **yes** to confirm directory creation.

f Provide the database details.

Option	Description
Provide the database DSN	UMDS_DSN
Provide the database username	*umds_db_user*
Provide the database password	*umds_db_user_password*

g Type **yes** and press Enter to install UMDS.

8 Disconnect the attached update `.iso` from the UMDS virtual machine.

Update the ESXi Hosts in the Management Cluster in Region A

After you update UMDS, you can proceed with updating the management ESXi hosts in Region A. You use vSphere Update Manager for automated host update across the management cluster.

Use different baseline types according to the storage type, vSAN or traditional, that you use in the management cluster for Region A.

Table 4-17. Management ESXi Hosts In Region A

Availability Zone	IP Address	Fully Qualified Domain Name	Cluster Name	vSAN Datastore
Availability Zone 1	172.16.11.101	sfo01m01esx01.sfo01.rainpole.local	sfo01-m01-mgmt01	sfo01-m01-vsan01
Availability Zone 1	172.16.11.102	sfo01m01esx02.sfo01.rainpole.local		
Availability Zone 1	172.16.11.103	sfo01m01esx03.sfo01.rainpole.local		
Availability Zone 1	172.16.11.104	sfo01m01esx03.sfo01.rainpole.local		
Availability Zone 1	172.16.11.1*xx*	sfo01m01esx*xx*.sfo01.rainpole.local		
Availability Zone 2	172.16.21.101	sfo02m01esx01.sfo01.rainpole.local		
Availability Zone 2	172.16.21.102	sfo02m01esx02.sfo01.rainpole.local		
Availability Zone 2	172.16.21.103	sfo02m01esx03.sfo01.rainpole.local		
Availability Zone 2	172.16.21.104	sfo02m01esx04.sfo01.rainpole.local		
Availability Zone 2	172.16.21.1*xx*	sfo02m01esx*xx*.sfo01.rainpole.local		
-	172.17.11.201	sfo03m01vsanw01.sfo01.rainpole.local **Note** vSAN Witness Host Appliance		

Prerequisites

- Verify that the system hardware complies with the following areas of the ESXi requirements. See VMware Compatibility Guide.
  - System compatibility
  - I/O compatibility with network and host bus adapter (HBA) cards
  - Storage compatibility
  - Backup software compatibility
  - Compatibility of the firmware for the network and host bus adapter (HBA) cards. Upgrade the firmware accordingly.
  - BIOS compatibility. Upgrade the BIOS on the ESXi hosts accordingly.
- Allocate sufficient disk space on the host for the upgrade.
- To have management workloads automatically migrated from hosts while they are being upgraded, verify that vSphere DRS on the management cluster is set to `Fully Automated` for the duration of the upgrade operations.
- If using vSAN in the management cluster, on the **Monitor** tab for the cluster in the vSphere Web Client, verify that these properties have the following values:
  - The **vSAN > Health** report indicates that the checks for the cluster, network, physical disk, data, limits, hardware compatibility, performance service, and online health are passed.
  - The **vSAN > Resyncing Components** report shows no **Resyncing Components** and **Bytes left to resync**.
  - The **vSAN > Physical Disks** report shows that the disks on all hosts in the cluster are in mounted state and their vSAN health status is healthy.
- If using Stretched vSAN in the management cluster, in addition to the above, on the **Monitor** tab for the cluster in the vSphere Web Client, verify that these properties have the following values:
  - The **vSAN > Health > Stretched cluster** report indicates that the checks for the site latency, witness host not found, witness house fault domain misconfigured, whitness hose within vCenter cluster are passed.

Procedure

1 Remediate the ESXi Management Hosts That Use vSAN in Region A

If the management cluster in Region A is vSAN-backed, to remediate the hosts in the cluster, use the system managed baseline that is automatically created in vSphere Update Manager on the Management vCenter Server in Region A.

2 Remediate the ESXi Management Hosts That Use vSAN Stretched Storage in Region A

If you are using multiple availability zones in Region A, to remediate the hosts in the cluster, use the system managed baseline automatically created in vSphere Update Manager on the Management vCenter Server in Region A. Apply the baseline according to a specific order of operations.

3 Remediate the ESXi Management Hosts That Use Traditional Storage in Region A

Create a baseline so that vSphere Update Manager on the Management vCenter Server in Region A can automatically identify an update to remediate your clusters that use traditional storage, such as NFS.

What to do next

- Verify that the management ESXi hosts are operational after the upgrade.

Remediate the ESXi Management Hosts That Use vSAN in Region A

If the management cluster in Region A is vSAN-backed, to remediate the hosts in the cluster, use the system managed baseline that is automatically created in vSphere Update Manager on 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://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.

b Log in using the following credentials.

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

2 Verify that the vSAN Build Recommendation Engine is healthy using your my.vmware.com credentials to download the latest recommendation from VMware.

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

b In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01m01-mgmt01** tree.

c On the **Monitor** tab, click the **vSAN** tab and select **Health**.

d Expand the **vSAN Build Recommendation** test name.

e Click the **vSAN Build Recommendation Engine Health** test name, and click the **Login to my.vmware.com** button.

f In the **Login** dialog box, enter the following settings and click **OK**.

Setting	Value
Username	*my.vmware.com_account_name*
Password	*my.vmware.com_account_password*

3 Verify that the system managed baseline for upgrade of vSAN-backed hosts is available in vSphere Update Manager in Region A .

   a From the **Home** menu, select **Update Manager**.

   b In the left **Servers** pane, click **sfo01m01vc01.sfo01.rainpole.local**.

   c In the right pane, on the **Manage** tab, click **Hosts Baselines**.

   d In the **Baseline Group** pane, expand the **System managed** group and verify that the `VSAN Cluster 'sfo01-m01-mgmt01'` baseline group contains the `VMware ESXi 6.5.0 U2 (vSAN 6.6.1 Update 2 build xxxxxx` host update baseline.

4 Scan the cluster for updates against the system managed baseline.

   a In the **Hosts Baselines** pane, click the **Go to compliance view** button to locate the sfo01-m01-mgmt01 cluster in the inventory.

   b On the **Update Manager** tab, click the **Scan for Updates** button.

   c In the **Scan for Updates** dialog box, under **Scan hosts for**, select **Patches and Extensions** and **Upgrades** , and click **OK**.

   After the scan is completed, the cluster state is `Non-Compliant`.

5 Remediate the cluster and upgrade to vSphere 6.5 Update 2.

   a On the **Update Manager** tab, click **Remediate**.

   b On the **Select baselines** page of the **Remediate** wizard, in the **Baselines Groups and Types** pane, select the **VSAN Cluster 'sfo01-m01-mgmt01'** baseline group, verify that all baselines in the **Baselines** pane are selected, and click **Next**.

   c On the **Select target objects** page, select all management hosts in the cluster and click **Next**.

   d On the **Patches and extensions** page, ensure that **VMware ESXi 6.5 Complete Update 2** is selected 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 selected clusters > 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 about 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 and click **OK**.

If the `Disable HA admission control` message from Recommended Changes is displayed, ignore it.

i After you address all pre-check items, click **Finish** to begin the upgrade.

6 After all ESXi hosts have been upgraded to the latest version, review the NSX status of the management cluster.

a Select **Home > Networking & Security**.

b Select **Installation and Upgrade** 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.

7 Review the Hardware Compatibility status of the management cluster.

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

b In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01m01-mgmt01** tree.

c On the **Monitor** tab, click **vSAN** tab and select **Health**.

d Locate and verify that the **Hardware compatibility** tests have passed.

e If a `Warning` test result is present, expand the **Hardware compatibility** tests, review individual tests for a `Warning` test result, and perform the following troubleshooting.

Test That Results in a Warning	Troubleshooting Guidance
Controller firmware	Update Storage Controller Drivers and Firmware in the *Administering VMware vSAN* documentation
Controller disk group	VMware Knowledge Base article vSAN Health Service - Hardware Compatibility - Disk Group Type Check
Controller driver	Update Storage Controller Drivers and Firmware in the *Administering VMware vSAN* documentation.
Controller	VMware Knowledge Base article vSAN Health Service - vSAN HCL Health - Controller Release Support
SCSI controller	VMware Knowledge Base article vSAN Health Service - vSAN HCL Health – SCSI Controller on vSAN HCL
vSAN HCL DB	VMware Knowledge Base article vSAN Health Service - vSAN HCL Health – vSAN HCL DB up-to-date

Remediate the ESXi Management Hosts That Use vSAN Stretched Storage in Region A

If you are using multiple availability zones in Region A, to remediate the hosts in the cluster, use the system managed baseline automatically created in vSphere Update Manager on the Management vCenter Server in Region A. Apply the baseline according to a specific order of operations.

Upgrading the hosts in the management cluster in Region A when using a multiple availability zone configuration on top of a vSAN stretched cluster requires the following order:

1 Upgrade the ESXi hosts in Availability Zone 1.

2 Upgrade the ESXi hosts in Availability Zone 2.

3 Upgrade the vSAN witness host appliance.

4 Upgrade any hardware components to ensure compatibility with vSAN 6.6.x.

Procedure

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

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

b Log in using the following credentials.

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

2 Verify that the vSAN Build Recommendation Engine is healthy using your my.vmware.com credentials to download the latest recommendation from VMware.

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

   b In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01m01-mgmt01** tree.

   c On the **Monitor** tab, click the **vSAN** tab and select **Health**.

   d Expand the **vSAN Build Recommendation** test name.

   e Click the **vSAN Build Recommendation Engine Health** test name, and click the **Login to my.vmware.com** button.

   f In the **Login** dialog box, enter the following settings and click **OK**.

Setting	Value
Username	*my.vmware.com_account_name*
Password	*my.vmware.com_account_password*

3 Verify that the system managed baseline for upgrade of vSAN-backed hosts is available in vSphere Update Manager in Region A .

   a From the **Home** menu, select **Update Manager**.

   b In the left **Servers** pane, click **sfo01m01vc01.sfo01.rainpole.local**.

   c In the right pane, on the **Manage** tab, click **Hosts Baselines**.

   d In the **Baseline Group** pane, expand the **System managed** group and verify that the `VSAN Cluster 'sfo01-m01-mgmt01'` baseline group contains the `VMware ESXi 6.5.0 U2 (vSAN 6.6.1 Update 2 build xxxxxx)` host update baseline.

4 Scan the cluster for updates against the system managed baseline.

   a In the **Hosts Baselines** pane, click the **Go to compliance view** button to locate the sfo01-m01-mgmt01 cluster in the inventory.

   b Move up the inventory tree in the **Navigator** pane, and select **sfo01-m01dc**.

   In the data center object you access the hosts in Availability Zone 1, Availability Zone 2 and the vSAN witness host. If you use the cluster object in the vSphere Web Client, you access only Availability Zone 1 and Availability Zone 2.

   c On the **Update Manager** tab, click the **Scan for Updates** button.

   d In the **Scan for Updates** dialog box, under **Scan hosts for**, select **Patches and Extensions** and **Upgrades** , and click **OK**.

   After the scan is complete, the cluster state is `Non-Compliant`.

5 Remediate the hosts in Availability Zone 1 of the stretched vSAN cluster and upgrade to vSphere 6.5 Update 2.

a On the **Update Manager** tab, click **Remediate**.

b On the **Select baselines** page of the **Remediate** wizard, in the **Baselines Groups and Types** pane, select the **VSAN Cluster 'sfo01-m01-mgmt01'** baseline group, verify that all baselines in the **Baselines** pane are selected, and click **Next**.

c On the **Select target objects** page, select all of the management hosts in that reside in Availability Zone 1 and click **Next**.

d On the **Patches and extensions** page, ensure that **VMware ESXi 6.5 Complete Update 2** is selected together with any recommended extensions 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 selected clusters > 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 about any identifiable problems that would prevent a successful upgrade.

Address any items reported in the **Pre-check Remediation** dialog box before you proceed with the upgrade and click **OK**.

If the `Disable HA admission control` message from Recommended Changes is displayed, ignore it.

i After you address all pre-check items, click **Finish** to begin the upgrade.

6 After the hosts in Availability Zone 1 are remediated, repeat Step 5 on the hosts in Availability Zone 2.

7 After the hosts in both Availability Zone 1 and Availability Zone 2 are remediated, update the vSAN witness host.

The vSAN witness host appears as light-blue in the list of target objects.

8 After all ESXi hosts are upgraded to the latest version, review the NSX status of the management cluster.

   a Select **Home > Networking & Security**.

   b Select **Installation and Upgrade** 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.

9 Review the Hardware Compatibility status of the management cluster.

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

   b In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01m01-mgmt01** tree.

   c On the **Monitor** tab, click **vSAN** tab and select **Health**.

   d Locate and verify that the **Hardware compatibility** tests have passed.

   e If a `Warning` test result is present, expand the **Hardware compatibility** tests, review individual tests for a `Warning` test result, and perform the following troubleshooting.

Test That Results in a Warning	Troubleshooting Guidance
Controller firmware	Update Storage Controller Drivers and Firmware in the *Administering VMware vSAN* documentation
Controller disk group	VMware Knowledge Base article vSAN Health Service - Hardware Compatibility - Disk Group Type Check
Controller driver	Update Storage Controller Drivers and Firmware in the *Administering VMware vSAN* documentation
Controller	VMware Knowledge Base article vSAN Health Service - vSAN HCL Health - Controller Release Support
SCSI controller	VMware Knowledge Base article vSAN Health Service - vSAN HCL Health – SCSI Controller on vSAN HCL
vSAN HCL DB	VMware Knowledge Base article vSAN Health Service - vSAN HCL Health – vSAN HCL DB up-to-date

Remediate the ESXi Management Hosts That Use Traditional Storage in Region A

Create a baseline so that vSphere Update Manager on the Management vCenter Server in Region A can automatically identify an update to remediate your clusters that use traditional storage, such as NFS.

Procedure

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

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

b Log in using the following credentials.

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

2 Create a new fixed baseline for ESXi 6.5 Update 2 in vSphere Update Manager in Region A

a From the **Home** menu, select **Update Manager**.

b In the **Servers** pane on the left, click **sfo01m01vc01.sfo01.rainpole.local**.

c In the right pane, on the **Manage** tab, click **Host Baselines**.

d In the **Host Baselines** pane, click **New Baseline**.

The **New Baseline** wizard appears.

e On the **Name and type** page, enter the following options and click **Next**

Setting	Value
Name	VMware ESXi 6.5 Update 2 for VMware Validated Design 4.3
Description	-
Baseline Type	Host Patch

f On the **Patch options** page, select **Fixed**.

g On the **Patches** page, type `Update 2` in the filter search box and press Enter.

h Select the box next to the host patch named **VMware ESXi 6.5 Complete Update 2** and click **Next**.

i On the **Ready to complete** page, review the baseline details and click **Finish.**

3 Attach and scan the cluster for updates against the new baseline.

a In the **Host Baselines** pane, click **Go to Compliance View** to locate the sfo01m01vc01.sfo01.rainpole.local vCenter Server and the sfo01-m01-mgmt01 cluster in the inventory.

b On the **Update Manager** tab, click **Attach Baseline**.

c In the **Attach Baseline** dialog box, select the **VMware ESXi 6.5 Update 2 for VMware Validated Design 4.3** baseline and click **OK**.

d After the baseline is attached, click **Scan for Updates** .

e In the **Scan for Updates** dialog box, under **Scan hosts for**, select **Upgrades** and **Patches and Extensions** and click **OK**.

After the scan is complete, the cluster status is `Non-Compliant`.

4 Remediate the hosts in the management cluster and upgrade to vSphere 6.5 Update 2.

a On the **Update Manager** tab for the cluster, click **Remediate**.

b In the **Remediate** wizard, on the **Select baselines** page, under **Baselines Groups and Types**, click **Patch Baselines**, and select the **VMware ESXi 6.5 Update 2 for VMware Validated Design 4.3** baseline and click **Next**.

c On the **Select Target objects** page, select all hosts in the cluster and click **Next**.

d On the **Patch and extensions** page, select the **VMware ESXi 6.5 Complete Update 2** 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.

5 Review the NSX status of the management cluster.

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.

Remediate VMware Tools in the Management Cluster in Region A

After you update the ESXi hosts running the management virtual machines, update the VMware Tools on the virtual machines of the management components in Region A. To remediate the management virtual machines that are running earlier version of VMware Tools, create a baseline group so that vSphere Update Manager on the Management vCenter Server in Region A can automatically identify them.

You remediate VMware Tools on the folders of the following management virtual machines:

Table 4-18. Management Virtual Machines for VMware Tools Remediation in Region a

Cluster Name	Folder	Role	Virtual Machine Name
sfo01-m01-mgmt01	sfo01-m01fd-mgmt	Update Manager Download Service	sfo01umds01
	sfo01-m01fd-vra	vRealize Automation IaaS Web Server	vra01iws01a
			vra01iws01b
		vRealize Automation IaaS Manager Service	vra01ims01a
			vra01ims01b
		vRealize Automation IaaS DEM Workers	vra01dem01a
			vra01dem01b
		Microsoft SQL Server	vra01mssql01
	sfo01-m01fd-vraias	vRealize Automation IaaS Proxy Agent	sfo01ias01a
			sfo01ias01b
	sfo01-m01fd-bcdr	Site Recovery Manager	sfo01m01srm01

Procedure

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

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

b Log in using the following credentials.

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

2 Create a fixed baseline for the VMware Tools that is packaged with ESXi 6.5 Update 2 Patch Release in vSphere Update Manager in Region A

   a From the **Home** menu, select **Update Manager**.

   b In the **Servers** pane on the left, click **sfo01m01vc01.sfo01.rainpole.local**.

   c In the right pane, on the **Manage** tab, click the **VMs/VAs Baselines** tab.

   d In the **VMs/VAs Baselines** pane, click **New Baseline Group**.

   The **New Baseline Group** wizard appears.

   e On the **Name** page, enter the following values and click **Next**.

Setting	Value
Name	VMware Tools for VMware Validated Design 4.3
Description	-

   f On the **Upgrades** page, select the following options and click **Next**.

Setting	Value
VM Hardware Upgrades	None
VMware Tools Upgrades	VMware Tools Upgrade to Match Host (Predefined)
VA Upgrades	None

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

3 Attach and scan the folder for updates against the new baseline.

   a In the **VMs/VAs Baselines** pane, click **Go to compliance view** to locate the sfo01m01vc01.sfo01.rainpole.local vCenter Server and to the sfo01-m01-mgmt01 cluster in the inventory.

   b In the **Navigator**, click **VMs and Templates** and expand the **sfo01-m01dc > sfo01-m01fd-bcdr** tree.

   c On the **Update Manager** tab, click **Attach Baseline**.

   d In the **Attach Baseline or Baseline Group** dialog box, under **Baseline Groups** pane, select the **VMware Tools for VMware Validated Design 4.3** baseline group and click **OK**.

   e After you attach the baseline, click **Scan for Updates**.

   f In the **Scan for Updates** dialog box, under **Scan for**, select only **VMware Tools upgrades** and click **OK**.

   After the scan is complete, the folder status is `Non-Compliant`.

4 Remediate the virtual machines and upgrade VMware Tools to ESXi 6.5 Update 2 Patch Release.

a On the **Update Manager** tab, click **Remediate**.

b In the **Remediate** wizard on the **Select baselines** page, under **Baselines Groups and Types** pane, select the baseline group **VMware Tools for VMware Validated Design 4.3** and click **Next**.

c On the **Select target objects** page, select the management virtual machines in the folder and click **Next**.

d On the **Schedule** page, configure the following settings and click **Next**.

Setting	Value	
Task name	sfo01-m01fd-bcdr - VMware Tools for VMware Validated Design 4.3	
Task description	-	
Apply upgrade at specific time	For powered on VMs	Run this action now
	For powered off VMs	Run this action now
	For suspended VMs	Run this action now

e On the **Rollback Options** page, configure the following settings and click **Next**.

Setting		Value
Take a snapshot of the VMs before remediation to enable rollback		Selected
Snapshot Retention		Do not delete snapshots
Snapshot Details	Name	VMware Tools for VMware Validated Design 4.3
	Description	-

f On the **Ready to complete** page, click **Finish** to begin the upgrade.

The Update Manager remedation process starts running and restarts the virtual machines.

5 After the VMware Tools upgrade is complete on each virtual machine in the folder, review the **Summary** tab for each virtual machine that has been remediated, and verify that the VMware Tools status is `Running` and version is `(Current)`.

6 Navigate back to the **sfo01-m01fd-bcdr** folder and run the **Scan for Updates** operation again to verify that the management virtual machines are `Compliant`.

Note Because of the use of Guest Managed VMware Tools in the virtual machines, the **Compliance Status** might report `Incompatible` for the overall folder.

7 Delete the snapshot from each virtual machine in the folder.

a From the **Home** menu, select **VMs and Templates**.

b In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01fd-bcdr** tree.

c Right-click each virtual machines and select **Snapshots Delete All Snapshots**.

d In the **Confirm Delete** dialog box, click **Yes**.

8 Repeat the procedure for the other management virtual machines using their folders in Region A.

What to do next

- Verify that the management virtual machines are operational after the upgrade.

Update vSphere Update Manager Download Service, Management ESXi Hosts, and VMware Tools in Region B

In a dual-region SDDC, after you complete the update of the virtual infrastructure components for the management cluster in Region A, start the update of vSphere Update Manager Download Service (UMDS), management ESXi hosts, and VMware Tools in Region B. Upgrading both regions enables failover and failback between Region A and Region B.

Table 4-19. General Parameters for Update of UMDS and Management ESXi in Region B

Component	Value
vSphere Web Client URL	https://lax01m01vc01.lax01.rainpole.local/vsphere-client
vCenter Server	lax01m01vc01.lax01.rainpole.local
Cluster	lax01-m01-mgmt01

Procedure

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

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

b Log in using the following credentials.

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

2 Upgrade the UMDS to the version that is compliant with new vSphere version.

Repeat Upgrade vSphere Update Manager Download Service in Region A in Region B by using the following details:

Table 4-20. Configuration for UMDS Update in Region B

Setting	Value
UMDS IP address	192.168.32.67
UMDS fully qualified domain name	lax01umds01.lax01.rainpole.local
vCenter Server	lax01m01vc01.lax01.rainpole.local
Data center	lax01-m01dc

Table 4-20. Configuration for UMDS Update in Region B (Continued)

Setting	Value
Cluster	lax01-m01-mgmt01
Folder	lax01-m01fd-mgmt
UMDS virtual machine	lax01umds01

3 Upgrade the management ESXi hosts in Region B.

Repeat Update the ESXi Hosts in the Management Cluster in Region A by using the following details:

Table 4-21. Management ESXi Hosts to Update in Region B

Host IP Address	Fully Qualified Domain Name	Cluster Name	vSAN Datastore	NSX Manager
172.17.11.101	lax01m01esx01.lax01.rainpole.local	lax01-m01-mgmt01	lax01-m01-vsan01	172.17.11.65
172.17.11.102	lax01m01esx02.lax01.rainpole.local			
172.17.11.103	lax01m01esx03.lax01.rainpole.local			
172.17.11.104	lax01m01esx04.lax01.rainpole.local			
172.17.11.1*xx*	lax01m01esx*xx*.lax01.rainpole.local			

4 Upgrade the VMware Tools on the management virtual machines in the management cluster in Region B.

Repeat Remediate VMware Tools in the Management Cluster in Region A by using the following details:

Table 4-22. Management Virtual Machines and Virtual Appliances In Region B

Cluster Name	Folder	Role	Virtual Machine Name
lax01-m01-mgmt01	lax01-m01fd-mgmt	Update Manager Download Service	lax01umds01
	lax01-m01fd-vraias	vRealize Automation IaaS Proxy Agent	lax01ias01a
			lax01ias01b
	lax01-m01fd-bcdr	Site Recovery Manager	lax01m01srm01

What to do next

Verify that UMDS, management ESXi hosts, and vSAN are operational.

Update the Components for the Shared Edge and Compute Clusters

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

Procedure

1 Update vSphere for the Shared Edge and Compute Clusters

After you update the components that support the management cluster in the SDDC, you update the Compute vCenter Server in Region A and repeat this operation in Region B.

2 Update the ESXi Hosts in the Shared Edge and Compute Cluster

Complete your update of the shared edge and compute clusters in the SDDC. Update the shared edge and compute ESXi hosts in Region A and Region B. You use vSphere Update Manager for automated host update across the shared edge and compute cluster.

Update vSphere for the Shared Edge and Compute Clusters

After you update the components that support the management cluster in the SDDC, you update the Compute vCenter Server in Region A and repeat this operation in Region B.

Updating the vCenter Server for the shared edge and compute cluster is a single-step operation. You update the Compute vCenter Server in Region A. You then repeat this operation in Region B.

Table 4-23. Compute vCenter Server Instances in the SDDC

Region	Role	IP Address	Fully Qualified Domain Name
Region A	Compute vCenter Server	172.16.11.64	sfo01w01vc01.sfo01.rainpole.local
Region B	Compute vCenter Server	172.17.11.64	lax01w01vc01.lax01.rainpole.local

Prerequisites

- Download the vCenter Server Appliance `VMware-vCenter-Server-Appliance-6.5.0.x-build_number-patch-FP.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 vSphere DRS on the shared edge and compute cluster is set to `Fully Automated` for the duration of the upgrade operations to have edge and tenant workloads automatically migrated from hosts while they are being upgraded.
- Verify that all compute ESXi hosts have the lockdown mode disabled during the upgrade.
- Ensure that any integration with the Compute vCenter Server instances in the environment has been quiesced of all activities. Such activities include but are not limited to the following operations:
  - Users performing active backups of components
  - Provisioning of new virtual machines by using vRealize Automation

  - Third-party integration that might automate the ordering or deployment of new virtual machines
  - Administrators manually creating new virtual objects
- Without quiescing the environment, rollback operations could be disrupted by orphaned objects that can be generated after you have taken snapshots. You might also have to extend the time of the maintenance windows.

  Verify that current backups of the Compute vCenter Server instances exist.

Procedure

1 Take Snapshots of the Compute vCenter Server Instances in Region A and Region B

  Before you start the update, take a snapshot of each Compute vCenter Server virtual appliance in Region A and Region B. If you must perform a rollback to the previous state, these snapshots accelerate a rollback operation.

2 Update the Compute vCenter Server in Region A

3 Update the Compute vCenter Server in Region B

  After you update the Compute vCenter Server in Region A, update the Compute vCenter Server in Region B to complete the upgrade of vCenter Server.

4 Delete Snapshots of the Compute vCenter Servers Instances in Region A and Region B

  After completing the update of the shared edge and compute components in Region A and Region B and validating their stability, remove the snapshots from the virtual appliances.

What to do next

- Verify that vCenter Server is operational after the upgrade.

Take Snapshots of the Compute vCenter Server Instances in Region A and Region B

Before you start the update, take a snapshot of each Compute vCenter Server virtual appliance in Region A and Region B. If you must perform a rollback to the previous state, these snapshots accelerate a rollback operation.

Table 4-24. Compute vCenter Server Instances in the SDDC

Region	Folder	Virtual Machine Name
Region A	sfo01-m01fd-mgmt	sfo01w01vc01
Region B	lax01-m01fd-mgmt	lax01w01vc01

Procedure

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

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

   b Log in using the following credentials.

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

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

3 In the **Navigator**, expand the **sf01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-mgmt** tree.

4 Right-click the **sfo01w01vc01** virtual machine and select **Snapshots > Take Snapshot**.

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

Setting	Value
Name	VMware Validated Design 4.3 Virtual Infrastructure Layer Upgrade
Description	-
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

6 Repeat the procedure for the Compute vCenter Server virtual appliance in Region B.

Update the Compute vCenter Server in Region A

After you update the components for the management clusters, update the Compute vCenter Server in Region A.

Prerequisites

- Verify that a current backup of the Compute vCenter Server virtual appliance in Region A exists.
- Mount the update `VMware-vCenter-Server-Appliance-6.5.0.x-build_number-patch-FP.iso` file to the virtual appliance.

Procedure

1 Log in to the appliance management interface (VAMI) of the Compute vCenter Server.

   a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*compvc_root_password*

2 Upgrade the appliance.

   a In the appliance management interface, click **Update** in the left pane.

   b In the **Update** pane, click **Check Updates** and select **Check CDROM**.

   c Verify that the **Available Updates** shown match the version in VMware Software Versions in the Upgrade, click **Install Updates** and select **Install CDROM Updates**.

   d In the **End User License Agreement** dialog box, accept the EULA and click **Install**.

   e After the update completes, click **OK** in the **Installing Upgrades** dialog box.

3 Restart the appliance to apply the upgrade.

   a Click the **Summary** tab, and click **Reboot**.

   b In the **System Reboot** dialog box, click **Yes**.

4 After the restart completes, log back in to the virtual appliance management interface, and verify the version number in the **Update** pane.

5 Disconnect the attached update `.iso` from the Compute vCenter Server appliance.

Update the Compute vCenter Server in Region B

After you update the Compute vCenter Server in Region A, update the Compute vCenter Server in Region B to complete the upgrade of vCenter Server.

Prerequisites

- Verify that current a backup of the Compute vCenter Server virtual appliance in Regions B exists.
- Mount the update `VMware-vCenter-Server-Appliance-6.5.0.x-build_number-patch-FP.iso` file to the virtual appliance.

Procedure

1 Log in to the appliance management interface (VAMI) of the Compute vCenter Server.

   a Open a Web browser and go to **`https://lax01w01vc01.lax01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*compvc_root_password*

2 Upgrade the appliance.

   a In the appliance management interface, click **Update** in the left pane.

   b In the **Update** pane, click **Check Updates** and select **Check CDROM**.

   c Verify that the **Available Updates** shown match the version in VMware Software Versions in the Upgrade, click **Install Updates** and select **Install CDROM Updates**.

   d In the **End User License Agreement** dialog box, accept the EULA and click **Install**.

   e After the update completes, click **OK** in the **Installing Upgrades** dialog box.

3 Restart the appliance to apply the upgrade.

   a Click the **Summary** tab, and click **Reboot**.

   b In the **System Reboot** dialog box, click **Yes**.

4 After the restart completes, log back in to the virtual appliance management interface, and verify the version number in the **Update** pane.

5 Disconnect the attached update `.iso` from the Compute vCenter Server virtual appliance.

Delete Snapshots of the Compute vCenter Servers Instances in Region A and Region B

After completing the update of the shared edge and compute components in Region A and Region B and validating their stability, remove the snapshots from the virtual appliances.

Table 4-25. Compute vCenter Server Instances in the SDDC

Region	Folder	Role	Virtual Machine Name
Region A	sfo01-m01fd-mgmt	vCenter Server	sfo01w01vc01
Region B	lax01-m01fd-mgmt	vCenter Server	lax01w01vc01

Procedure

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

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

   b Log in using the following credentials.

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

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

3 In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-mgmt** tree.

4 Right-click the **sfo01m01vc01** virtual machine and select **Snapshots > Delete All Snapshots**.

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

6 Repeat the procedure for the Compute vCenter Server in Region B.

Update the ESXi Hosts in the Shared Edge and Compute Cluster

Complete your update of the shared edge and compute clusters in the SDDC. Update the shared edge and compute ESXi hosts in Region A and Region B. You use vSphere Update Manager for automated host update across the shared edge and compute cluster.

Table 4-26. Shared Edge and Compute ESXi Hosts in the SDDC

Region	IP Address	Fully Qualified Domain Name	Cluster Name
Region A	172.16.31.101	sfo01w01esx01.sfo01.rainpole.local	sfo01-m01-mgmt01
	172.16.31.102	sfo01w01esx02.sfo01.rainpole.local	
	172.16.31.103	sfo01w01esx03.sfo01.rainpole.local	
	172.16.31.104	sfo01w01esx04.sfo01.rainpole.local	
	172.16.31.1*xx*	sfo01w01esx*xx*.sfo01.rainpole.local	
Region B	172.17.31.101	lax01w01esx01.lax01.rainpole.local	lax01-m01-mgmt01
	172.17.31.102	lax01w01esx02.lax01.rainpole.local	
	172.17.31.103	lax01w01esx03.lax01.rainpole.local	

Table 4-26. Shared Edge and Compute ESXi Hosts in the SDDC (Continued)

Region	IP Address	Fully Qualified Domain Name	Cluster Name
	172.17.31.104	lax01w01esx04.lax01.rainpole.local	
	172.17.31.1*xx*	lax01w01esx*xx*.lax01.rainpole.local	

Prerequisites

- Verify that the system hardware complies with the following areas of the ESXi requirements. See VMware Compatibility Guide.
  - System compatibility
  - I/O compatibility with network and host bus adapter (HBA) cards
  - Storage compatibility
  - Backup software compatibility
  - Compatibility of the firmware for the network and host bus adapter (HBA) cards. Upgrade the firmware accordingly.
  - BIOS compatibility. Upgrade the BIOS on the ESXi hosts accordingly.
- Verify that vSphere DRS on the shared edge and compute clusters are set to `Fully Automated` for the duration of the update operations to have tenant workloads automatically migrated from hosts while they are being updated.

What to do next

- Verify that the ESXi hosts in the shared edge and compute clusters are operational after the update.

Remediate the ESXi Shared Edge and Compute Hosts That Use Traditional Storage in Region A and Region B

Create a baseline so that vSphere Update Manager on the Compute vCenter Server in each region can automatically identify an update to remediate your clusters that use traditional storage, such as NFS.

Region	vCenter Server	Cluster	NSX Manager
Region A	sfo01w01vc01.sfo01.rainpole.local	sfo01-w01-comp1	172.16.11.66
Region B	sfo01w01vc01.sfo01.rainpole.local	lax01-w01-comp01	172.17.11.66

Procedure

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

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

b Log in using the following credentials.

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

2 Create a new fixed baseline for ESXi 6.5 Update 2 in vSphere Update Manager in Region A

a From the **Home** menu, select **Update Manager**.

b In the **Servers** pane on the left, click **sfo01w01vc01.sfo01.rainpole.local**.

c In the right pane, on the **Manage** tab, click **Host Baselines**.

d In the **Host Baselines** pane, click **New Baseline**.

The **New Baseline** wizard appears.

e On the **Name and type** page, enter the following options and click **Next**

Setting	Value
Name	VMware ESXi 6.5 Update 2 for VMware Validated Design 4.3
Description	-
Baseline Type	Host Patch

f On the **Patch options** page, select **Fixed**.

g On the **Patches** page, type `Update 2` in the filter search box and press Enter.

h Select the box next to the host patch named **VMware ESXi 6.5 Complete Update 2** and click **Next**.

i On the **Ready to complete** page, review the baseline details and click **Finish.**

3 Attach and scan the cluster for updates against the new baseline

a In the **Host Baselines** pane, click **Go to Compliance View** to locate the sfo01w01vc01.sfo01.rainpole.local vCenter Server and to the sfo01-w01-comp1 cluster in the inventory.

b On the **Update Manager** tab, click **Attach Baseline**.

c In the **Attach Baseline** dialog box, select the **VMware ESXi 6.5 Update 2 for VMware Validated Design 4.3** baseline and click **OK**.

d After the baseline is attached, click **Scan for Updates** .

e In the **Scan for Updates** dialog box, under **Scan hosts for**, select **Upgrades** and **Patches and Extensions** and click **OK**.

After the scan is complete, the cluster status is `Non-Compliant`.

4 Remediate the hosts in the shared edge and compute cluster and update to vSphere 6.5 Update 2.

a On the **Update Manager** tab, click **Remediate**.

b On the **Select baselines** page of the **Remediate** wizard, under **Baselines Groups and Types**, click **Patch Baselines**, and select the **VMware ESXi 6.5 Update 2 for VMware Validated Design 4.3** baseline, and click **Next**.

c On the **Select Target objects** page, select all hosts in the cluster and click **Next**.

d On the **Patch and extensions** page, select the **VMware ESXi 6.5 Complete Update 2** 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-update report of any identifiable problems that would prevent a successful update

- 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 update.

5 Review the NSX status of the shared edge and compute cluster.

   a Select **Home > Networking & Security**.

   b Select **Installation and Upgrade** in the **Navigator**.

   c On the **Host Preparation** tab, select **172.16.11.66** from the **NSX Manager** menu and verify that **Installation Status** for all management ESXi hosts is green.

6 Repeat this procedure on the shared edge and compute cluster in Region B.

Global Post-Upgrade Configuration of the Virtual Infrastucture Layer

After you update all virtual infrastructure layer, perform global post-upgrade configuration according to address the dependencies between these components and to align your environment to the guidance in this validated design.

Procedure

1 Post-Upgrade Configuration of the Virtual Infrastructure Components in Region A

   After you update all virtual infrastructure components in your environment, perform global post-upgrade configuration according to the dependencies between the components in Region A and to the guidance in this validated design.

2 Post-Upgrade Configuration of the Virtual Infrastructure Components in Region B

   After you update all virtual infrastructure components in your environment, perform global post-upgrade configuration according to the dependencies between the components in Region B and to the guidance in this validated design.

Post-Upgrade Configuration of the Virtual Infrastructure Components in Region A

After you update all virtual infrastructure components in your environment, perform global post-upgrade configuration according to the dependencies between the components in Region A and to the guidance in this validated design.

Set SDDC Deployment Details on the Management vCenter Server in Region A

Update the identity of your SDDC deployment on vCenter Server. You use this identity as a label in tools for automated SDDC deployment.

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Global Inventory Lists**.

3 In the **Navigator**, click **vCenter Servers** under **Resources**.

4 Click the **sfo01m01vc01.sfo01.rainpole.local** vCenter Server object and click the **Configure** tab in the central pane.

5 Under the **Settings** pane, click **Advanced Settings** and click the **Edit** button.

6 In the **Edit Advanced vCenter Server Settings** dialog box, configure the following properties and click **OK**.

   a Search for the **`config.SDDC.Deployed.Version`** property and change its value from 4.2.0 to **`4.3.0`**.

   b Add the `config.SDDC.Deployed.WorkloadDomain` and `config.SDDC.Deployed.InstanceId` properties.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard
config.SDDC.Deployed.Version	4.3.0
config.SDDC.Deployed.WorkloadDomain	Management
config.SDDC.Deployed.Method	DIY
config.SDDC.Deployed.InstanceId	unique_identifier*

Note * To generate a unique identifier, use the Online UUID Generator website https://www.uuidgenerator.net/ and copy/paste the UUID into the config.SDDC.Deployed.InstanceId value. The Online UUID Generator is a universally unique identifier that generates random numbers using a secure random number generator.

7 Click **OK** to close the window.

Set SDDC Deployment Details on the Compute vCenter Server in in Region A

Update the identity of your SDDC deployment on the Compute vCenter Server in Region A. You can use this identity as a label in tools for automated SDDC deployment.

Procedure

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

   a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`** .

   b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Global Inventory Lists**.

3 In the **Navigator**, click **vCenter Servers** under **Resources**.

4 Click the **sfo01w01vc01.sfo01.rainpole.local** vCenter Server object and click the **Configure** tab in the central pane.

5 Under the **Settings** pane, click **Advanced Settings** and click the **Edit** button.

6 In the **Edit Advanced vCenter Server Settings** dialog box, configure the following properties and click **OK**.

   a Search for the **`config.SDDC.Deployed.Version`** property and change its value from 4.2.0 to **`4.3.0`**.

   b Add the `config.SDDC.Deployed.WorkloadDomain` and `config.SDDC.Deployed.InstanceId` properties.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard
config.SDDC.Deployed.Version	4.3.0
config.SDDC.Deployed.WorkloadDomain	SharedEdgeAndCompute
config.SDDC.Deployed.Method	DIY
config.SDDC.Deployed.InstanceId	unique_identifier*

Note * Use the `unique_identifier` you generated for the Management vCenter Server. See *Set SDDC Deployment Details on the Management vCenter Server in in Region A*.

7 Click **OK** to close the window.

Post-Upgrade Configuration of the Virtual Infrastructure Components in Region B

After you update all virtual infrastructure components in your environment, perform global post-upgrade configuration according to the dependencies between the components in Region B and to the guidance in this validated design.

Procedure

1 Set SDDC Deployment Details on the Management vCenter Server in Region B

2 Set SDDC Deployment Details on the Compute vCenter Server in Region B

Set SDDC Deployment Details on the Management vCenter Server in Region B

Update the identity of your SDDC deployment on the Management vCenter Server in Region B. You use this identity as a label in tools for automated SDDC deployment.

Procedure

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

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

   b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Global Inventory Lists**.

3 In the **Navigator**, click **vCenter Servers** under **Resources**.

4 Click the **lax01m01vc01.lax01.rainpole.local** vCenter Server object and click the **Configure** tab in the central pane.

5 Under the **Settings** pane, click **Advanced Settings** and click the **Edit** button.

6 In the **Edit Advanced vCenter Server Settings** dialog box, configure the following properties and click **OK**.

   a Search for the **`config.SDDC.Deployed.Version`** property and change its value from 4.2.0 to **`4.3.0`**.

   b Add the `config.SDDC.Deployed.WorkloadDomain` and `config.SDDC.Deployed.InstanceId` properties.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard
config.SDDC.Deployed.Version	4.3.0
config.SDDC.Deployed.WorkloadDomain	Management
config.SDDC.Deployed.Method	DIY
config.SDDC.Deployed.InstanceId	unique_identifier*

Note * To generate a unique identifier, use the Online UUID Generator website https://www.uuidgenerator.net/ and copy/paste the UUID into the config.SDDC.Deployed.InstanceId value. The Online UUID Generator is a universally unique identifier that generates random numbers using a secure random number generator.

Set SDDC Deployment Details on the Compute vCenter Server in Region B

Update the identity of your SDDC deployment on the Compute vCenter Server in Region B. You use this identity as a label in tools for automated SDDC deployment.

Procedure

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

   a Open a Web browser and go to **`https://lax01w01vc01.lax01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 From the **Home** menu of the vSphere Web Client, select **Global Inventory Lists**.

3 In the **Navigator**, click **vCenter Servers** under **Resources**.

4 Click the **lax01w01vc01.lax01.rainpole.local** vCenter Server object and click the **Configure** tab in the central pane.

5 Under the **Settings** pane, click **Advanced Settings** and click the **Edit** button.

6 In the **Edit Advanced vCenter Server Settings** dialog box, configure the following properties and click **OK**.

   a Search for the **`config.SDDC.Deployed.Version`** property and change its value from 4.2.0 to **`4.3.0`**.

   b Add the `config.SDDC.Deployed.WorkloadDomain` and `config.SDDC.Deployed.InstanceId` properties.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard
config.SDDC.Deployed.Version	4.3.0
config.SDDC.Deployed.WorkloadDomain	SharedEdgeAndCompute
config.SDDC.Deployed.Method	DIY
config.SDDC.Deployed.InstanceId	unique_identifier*

Note * Use the `unique_identifier` you generated for the Management vCenter Server. See *Set SDDC Deployment Details on the Management vCenter Server in in Region A*.

7 Click **OK** to close the window.

SDDC Startup and Shutdown

5

When you perform patch, upgrade, recovery, or failover of the SDDC management applications, make sure that you start up and shut down the management virtual machines according to a predefined order.

This chapter includes the following topics:

Shutdown Order of the Management Virtual Machines

Shut down the virtual machines of the SDDC management stack by following a strict order to avoid data loss and faults in the components.

Before you begin:

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

Shutting down the management virtual machines:

- Refer to VMware Knowledge Base article 2142676 for information on verifying the state of the vSAN cluster before a shutdown.
- Shut down the virtual machines of the SDDC management stack by following the shutdown order provided in the following table.
- Ensure that the console of the virtual machine and its services are fully shut down before moving to the next virtual machine.

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

Virtual Machine Name in Region A	Virtual Machine Name in Region B	Shutdown Order
vRealize Suite Lifecycle Manager **Total Number of VMs (1)**	**vRealize Suite Lifecycle Manager** **Total Number of VMs (0)**	**1**
vrslcm01svr01a	-	1
vRealize Log Insight **Total Number of VMs (3)**	**vRealize Log Insight** **Total Number of VMs (3)**	**2**
sfo01vrli01c	lax01vrli01c	1
sfo01vrli01b	lax01vrli01b	1
sfo01vrli01a	lax01vrli01a	2
vRealize Operations Manager **Total Number of VMs (5)**	**vRealize Operations Manager** **Total Number of VMs (2)**	**2**
sfo01vropsc01b	lax01vropsc01b	1
sfo01vropsc01a	lax01vropsc01a	1
vrops01svr01c	-	2
vrops01svr01b	-	3
vrops01svr01a	-	4
vRealize Business for Cloud **Total Number of VMs (2)**	**Realize Business for Cloud** **Total Number of VMs (2)**	**3**
sfo01vrbc01	lax01vrbc01	1
vrb01svr01	-	2
vRealize Automation **Total Number of VMs (11)**	**vRealize Automation** **Total Number of VMs (2)**	**4**
vra01dem01a	-	1
vra01dem01b	-	1
sfo01ias01b	lax01ias01b	1
sfo01ias01a	lax01ias01a	1
vra01ims01b	-	2
vra01ims01a	-	2
vra01iws01b	-	3
vra01iws01a	-	4
vra01svr01b	-	5
vra01svr01a	-	5
vra01mssql01	-	6
Site Recovery Manager and vSphere Replication **Total Number of VMs (2)**	**Site Recovery Manager and vSphere Replication** **Total Number of VMs (2)**	**5**
sfo01m01vrms01	lax01m01vrms01	1
sfo01m01srm01	lax01m01srm01	2

Virtual Machine Name in Region A	Virtual Machine Name in Region B	Shutdown Order
Update Manager Download Service (UMDS) **Total Number of VMs (1)**	**Update Manager Download Service (UMDS)** **Total Number of VMs (1)**	**5**
sfo01umds01	lax01umds01	1
Core Stack **Total Number of VMs (26)**	**Core Stack** **Total Number of VMs (16)**	**6**
sfo01m01lb01 (0,1)	lax01m01lb01 (0,1)	1
sfo01m01udlr01 (0,1)	-	1
sfo01m01esg01	lax01m01esg01	1
sfo01m01esg02	lax01m01esg02	1
sfo01w01udlr01 (0,1)	-	1
sfo01w01dlr01 (0,1)	lax01w01dlr01 (0,1)	1
sfo01w01esg01	lax01w01esg01	1
sfo01w01esg02	lax01w01esg02	1
sfo01m01nsx01	lax01m01nsx01	2
sfo01w01nsx01	lax01w01nsx01	2
sfo01m01nsxc01	-	3
sfo01m01nsxc02	-	3
sfo01m01nsxc03	-	3
sfo01w01nsxc01	-	3
sfo01w01nsxc02	-	3
sfo01w01nsxc03	-	3
sfo01m01vc01	lax01m01vc01	4
sfo01w01vc01	lax01w01vc01	4
sfo01psc01 (0,1)	lax01psc01 (0,1)	5
sfo01w01psc01	lax01w01psc01	6
sfo01m01psc01	lax01m01psc01	6

Shutting down the ESXi hosts in the vSAN clusters:

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

Startup Order of the Management Virtual Machines

Start up the virtual machines of the SDDC management stack by following a strict order to guarantee the faultless operation of and the integration between the components.

Before you begin:

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

Starting up the ESXi hosts in the vSAN clusters:

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

Starting up the management virtual machines:

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

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
Core Stack Total Number of VMs (26)	**Core Stack Total Number of VMs (16)**	**1**
sfo01m01psc01	lax01m01psc01	1
sfo01w01psc01	lax01w01psc01	1
sfo01psc01 (0,1)	lax01psc01 (0,1)	2
sfo01m01vc01	lax01m01vc01	3
sfo01w01vc01	lax01w01vc01	3
sfo01m01nsx01	lax01m01nsx01	4
sfo01w01nsx01	lax01w01nsx01	4
sfo01m01nsxc01	-	5
sfo01m01nsxc02	-	5
sfo01m01nsxc03	-	5
sfo01w01nsxc01	-	5
sfo01w01nsxc02	-	5
sfo01w01nsxc03	-	5
sfo01m01lb01 (0,1)	lax01m01lb01 (0,1)	6
sfo01m01udlr01 (0,1)	-	6
sfo01m01esg01	lax01m01esg01	6
sfo01m01esg02	lax01m01esg02	6
sfo01w01udlr01 (0,1)	-	6
sfo01w01dlr01 (0,1)	lax01w01dlr01(0,1)	6

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
sfo01w01esg01	lax01w01esg01	6
sfo01w01esg02	lax01w01esg02	6
Update Manager Download Service (UMDS) **Total Number of VMs (1)**	**Update Manager Download Service (UMDS)** **Total Number of VMs (1)**	**2**
sfo01umds01	lax01umds01	1
Site Recovery Manager and vSphere Replication **Total Number of VMs (2)**	**Site Recovery Manager and vSphere Replication** **Total Number of VMs (2)**	**2**
sfo01m01vrms01	lax01m01vrms01	1
sfo01m01srm01	lax01m01srm01	1
vRealize Automation **Total Number of VMs (11)**	**vRealize Automation** **Total Number of VMs (2)**	**3**
vra01mssql01	-	1
vra01svr01a	-	2
vra01svr01b	-	2
vra01iws01a	-	3
vra01iws01b	-	4
vra01ims01a	-	5
vra01ims01b	-	6
sfo01ias01a	lax01ias01a	7
sfo01ias01b	lax01ias01b	7
vra01dem01a	-	7
vra01dem01b	-	7
vRealize Business for Cloud **Total Number of VMs (2)**	**vRealize Business for Cloud** **Total Number of VMs (1)**	**4**
vrb01svr01	-	1
sfo01vrbc01	lax01vrbc01	2
vRealize Operations **Manager Total Number of VMs (5)**	**vRealize Operations Manager** **Total Number of VMs (2)**	**5**
vrops01svr01a	-	1
vrops01svr01b	-	2
vrops01svr01c	-	3
sfo01vropsc01a	lax01vropsc01a	4
sfo01vropsc01b	lax01vropsc01b	4
vRealize Log Insight **Total Number of VMs (3)**	**vRealize Log Insight** **Total Number of VMs (3)**	**5**
sfo01vrli01a	lax01vrli01a	1

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
sfo01vrli01b	lax01vrli01b	2
sfo01vrli01c	lax01vrli01c	2
vRealize Suite Lifecycle Manager **Total Number of VMs (1)**	**vRealize Suite Lifecycle Manager** **Total Number of VMs (0)**	**6**
vrslcm01svr01a	-	1