Upgrade

24 OCT 2017
VMware Validated Design 4.1
VMware Validated Design for Software-Defined Data Center 4.1

vmware®

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

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

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

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

Intended Audience

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

VMware Technical Publications Glossary

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

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 successful SDDC upgrade.

This section includes the following topics:

Upgrade Policy

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

Updates That Are Validated by VMware Validated Designs

VMware Validated Design follows the lifecycle management principles contextualized around the SDDC.

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

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

Updates That Are Not Validated by VMware Validated Designs

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

Upgrade Paths and Application Upgrade Sequence

You must comply with the path and sequence for SDDC upgrade to version 4.1 of this VMware Validated Design.

Upgrade Paths

To upgrade to version 4.1, you must run version 4.0 of this VMware Validated Design.

Currently Installed Version	Upgrade Path
2.0	1 3.0 2 3.0.2 3 4.0
3.0	1 3.0.2 2 4.0
3.0.2	1 4.0 2 4.1
4.0	4.1

Upgrade Sequence

The upgrade process of VMware Validated Design follows a prescriptive path to properly isolate the VMware components in their respective 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. At the same time, the upgrade sequence reduces the overall upgrade window and the impact in the event of a failed upgrade or update. Follow this sequence also for interoperability with the broader components within the SDDC. In this way, the upgrade sequence allows for progressive, granular upgrade over the course of time.

Table 1-1. VMware Validated Design Upgrade Sequence

Order	Component	Sub-Component	Layer
1	vRealize Automation	vRealize Automation Appliances	Cloud Management
		vRealize Automation IaaS Components	

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

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

VMware Software Versions in the Upgrade

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

Table 1-2. Upgrade from VMware Validated Design for Software-Defined Data Center 4.0 to VMware Validated Design for Software-Defined Data Center 4.1

SDDC Layer	Product Name	Product Version in VMware Validated Design 4.0	Product Version in VMware Validated Design 4.1	Operation Type
Cloud Management	vRealize Automation	7.2	7.3	Upgrade
	vRealize Orchestrator (Deprecated)	7.2	7.3	Upgrade
	vRealize Business	7.2	7.3.1	Upgrade
Operations Management	vRealize Operations Manager	6.4	6.6.1	Upgrade
	vRealize Log Insight	4.0	4.5	Upgrade
Virtual Infrastructure	NSX for vSphere	6.3.1	6.3.3	Upgrade
	vCenter Server	6.5 a	6.5 Update 1	Upgrade
	Platform Services Controller	6.5 a	6.5 Update 1	Upgrade
	Update Manager Download Service	6.5 a	6.5 Update 1	Update
	ESXi	6.5 a	6.5 Update 1	Upgrade
	vSAN	6.5	6.6.1	Upgrade
Business Continuity and Disaster Recovery	Site Recovery Manager	6.5	6.5.1	Update
	vSphere Replication	6.5	6.5.1	Update
	vSphere Data Protection	6.1.3	6.1.4	Update

For information about the software components that are available in VMware Validated Design 4.0 and VMware Validated Design 4.1, see *VMware Validated Design Release Notes*.

Mapping Component Names Between Versions 4.0 and 4.1 of VMware Validated Design

VMware Validated Design 4.1 introduces a new naming convention for the management components and objects across the SDDC stack for fast identification of objects in the SDDC and for scale-out of the infrastructure blocks. Use the map between the names of the management components in Region A and Region B in version 4 and the names in version 4.1 to apply the upgrade guidance.

VMware Validated Design continuously accommodates new use cases. As a result, the naming convention across the SDDC stack must support extending the guidance with new use cases and transitioning between them with ease.

By using the naming convention, VMware Validated Design supports these different elements or types of infrastructure in the following way:

- Consistency between infrastructure blocks for easy understanding of the guidance
- Ability to scale across infrastructure blocks without adding operational overhead
- Naming Convention in VMware Validated Design 4.1

  The naming convention in version 4.1 of VMware Validated Design provides uniqueness of objects across the SDDC. You can identify managed objects directly if you use many components that are linked together, for example, multiple vCenter Server systems working in Enhanced Linking Mode or management dashboards in vRealize Operations Manager or vRealize Business monitoring multiple instances of the same component.
- Naming Changes in Region A

  If your SDDC is based on VMware Validated Design 4.0, use the map between the names in our SDDC and the new names in version 4.1 to apply the upgrade guidance in Region A.
- Naming Changes in Region B

  If your SDDC is based on VMware Validated Design 4.0, use the map between the names in our SDDC and the new names in version 4.1 to apply the upgrade guidance in Region B.

Naming Convention in VMware Validated Design 4.1

The naming convention in version 4.1 of VMware Validated Design provides uniqueness of objects across the SDDC. You can identify managed objects directly if you use many components that are linked together, for example, multiple vCenter Server systems working in Enhanced Linking Mode or management dashboards in vRealize Operations Manager or vRealize Business monitoring multiple instances of the same component.

This naming convention also enables you to scale out across infrastructure blocks, for example, in the following cases:

- Scale a Consolidated SDDC out to a Standard SDDC.
- Extend a Standard SDDC with a ROBO SDDC.

- Add blocks of infrastructure to support more availability zones.

The new naming convention covers the following components:

- Virtual machines and ESXi hosts
- Objects in the vCenter Server and NSX inventories

Elements of the Component Names in VMware Validated Design 4.1

The name of each component or object in this validated design consists of units that represent the location, purpose and numerical identifier of the component in the SDDC.

Table 1-3. Elements of the Component and Object Names in the SDDC

Element	Description	Used In
location	Defines the physical location of the component, for example, `sfo` and `lax`.	■ Host names ■ VM names ■ Virtual switch names ■ Names of placeholder objects in the vCenter Server inventory
az_id	Defines the ID of the availability zone of the component in the physical location. It is a two-character numerical value starting at `01`.	■ Host names ■ VM names ■ Virtual switch names ■ Names of vCenter Server container and managed objects
pod	Indicates the purpose of the pod the component is linked to. Possible values are as follows: ■ `m` for management ■ `w` for workload	■ Host names ■ VM names ■ Virtual switch names ■ Names of vCenter Server container and managed objects
pod_id	Defines the pod ID. It is a two-character numerical value starting at `01`.	■ Host names ■ VM names ■ Virtual switch names ■ Names of vCenter Server container and managed objects
mgmt_component	Defines the function of the management applications using up to six characters, for example, `vc`, `psc` and `nsx`.	■ Host names ■ VM names
mgmt_component_id	Defines the instance of the cluster. Two character numerical value starting at `01`.	■ Host names ■ VM names
cluster_type	Indicates the purpose of the cluster. Possible values are as follows: ■ `m` for management ■ `w` for workload	Cluster names
cluster_id	Defines the ID of the cluster. It is a two-character numerical value starting at `01`.	Cluster names

Table 1-3. Elements of the Component and Object Names in the SDDC (Continued)

Element	Description	Used In
virtual_switch_type	Indicates the switch type. Possible values are as follows: ■ `vss` for standard switch ■ `vds` for distributed switch	■ Virtual switch names
virtual_switch_id	Defines the ID of the switch. It is a two-character numerical value starting at `01`.	■ Virtual switch names
port_group_type	Defines the name of the port group.	■ Port group names in virtual switches
datastore_type	Indicates the datastore type. Possible values are as follows: ■ `vsan` for vSAN ■ `nfs` for NFS	■ Datastore names
datastore_id	Defines the ID of the datastore. It is a two-character numerical value starting at `01`.	■ Datastore names
object_type	Defines what the object type in the vCenter Server inventory. Possible values are: ■ `rp` for resource pool ■ `fd` for VM folder ■ `hp` for host profile ■ `cl` for content library	Names of vCenter Server container and managed objects
object_name	Defines the name of the object.	Names of vCenter Server container and managed objects
object_id	Defines the ID of the object. It is a two character numerical value starting at `01`.	Names of vCenter Server container and managed objects

Syntax of Component Names

Each component in this validated design is assigned a name according to its type.

Table 1-4. Name Syntax for the Management Objects in the SDDC

Name Attribute	Value
Component type	Virtual machine or host
Syntax	`<location><az_id><pod><pod_id><mgmt_component><mgmt_component_id>`
Example	sfo01m01vc01
Component type	Cluster
Syntax	`<location><az_id>–<pod><pod_id>–<cluster_name><cluster_id>`
Example	sfo01-m01-mgmt01
Component type	Virtual switch
Syntax	`<location><az_id>–<pod><pod_id>–<switch_name><switch_id>`
Example	sfo01-m01-vds01

Table 1-4. Name Syntax for the Management Objects in the SDDC (Continued)

Name Attribute	Value
Component type	Port group on a virtual switch
Syntax	<location><az_id>-<pod_type><pod_id>-<switch_type><switch_id>-<port_group_type>
Example	sfo01-m01-vds01-management
Component type	Datastore
Syntax	<location><az_id>-<pod_type><pod_id>-<datastore_type><datastore_id>
Example	■ sfo01-m01-vsan01 ■ sfo01-m01-nfs01
Component type	vCenter Server container and managed object, such as data center, resource pool, folder, host profile and content library
Syntax	<location><az_id>-<pod_type><pod_id><object_type>-<object_name><object_id> <object_id> is optional.
Example	■ Data center - sfo01-m01dc ■ Resource pool - lax01-w01rp-sddc-edge ■ Folder - sfo01-m01fd-mgmt ■ Host profile - sfo01-m01hp-mgmt01 ■ Content library - lax01-w01cl-lib01

Naming Changes in Region A

If your SDDC is based on VMware Validated Design 4.0, use the map between the names in our SDDC and the new names in version 4.1 to apply the upgrade guidance in Region A.

- Changed Host Names in Region A

  Identify host names that are different in the previous version of the VMware Validated Design and in the current version. Use this map when you follow the upgrade guidance in Region A.

- Changed Object Names in Region A

  Identify object names in the vCenter Server inventory that are different in the previous version of the VMware Validated Design and in the current version. Use this map when you follow the upgrade guidance in Region A.

Changed Host Names in Region A

Identify host names that are different in the previous version of the VMware Validated Design and in the current version. Use this map when you follow the upgrade guidance in Region A.

Table 1-5. Changed Host Names in the Virtual Infrastructure Layer in Region A

Component	Host Name in Version 4.0	Host Name in Version 4.1
vSphere (Management)	mgmt01psc01.sfo01.rainpole.local	sfo01m01psc01.sfo01.rainpole.local
	mgmt01vc01.sfo01.rainpole.local	sfo01m01vc01.sfo01.rainpole.local

Table 1-5. Changed Host Names in the Virtual Infrastructure Layer in Region A (Continued)

Component	Host Name in Version 4.0	Host Name in Version 4.1
	mgmt01umds01.sfo01.rainpole.local	sfo01umds01.sfo01.rainpole.local
	mgmt01esx01.sfo01.rainpole.local	sfo01m01esx01.sfo01.rainpole.local
	mgmt01esx02.sfo01.rainpole.local	sfo01m01esx02.sfo01.rainpole.local
	mgmt01esx03.sfo01.rainpole.local	sfo01m01esx03.sfo01.rainpole.local
	mgmt01esx04.sfo01.rainpole.local	sfo01m01esx04.sfo01.rainpole.local
	mgmt01esx0*x*.sfo01.rainpole.local	sfo01m01esx0*x*.sfo01.rainpole.local
vSphere (Shared Edge and Compute)	comp01psc01.sfo01.rainpole.local	sfo01m01psc01.sfo01.rainpole.local
	comp01vc01.sfo01.rainpole.local	sfo01m01vc01.sfo01.rainpole.local
	comp01esx01.sfo01.rainpole.local	sfo01w01esx01.sfo01.rainpole.local
	comp01esx02.sfo01.rainpole.local	sfo01w01esx02.sfo01.rainpole.local
	comp01esx03.sfo01.rainpole.local	sfo01w01esx03.sfo01.rainpole.local
	comp01esx04.sfo01.rainpole.local	sfo01w01esx04.sfo01.rainpole.local
	comp01esx0*x*.sfo01.rainpole.local	sfo01w01esx0*x*.sfo01.rainpole.local
NSX for vSphere (Management)	mgmt01nsxm01.sfo01.rainpole.local	sfo01m01nsx01.sfo01.rainpole.local
	mgmt01nsxc01.sfo01.rainpole.local	sfo01m01nsxc01.sfo01.rainpole.local
	mgmt01nsxc02.sfo01.rainpole.local	sfo01m01nsxc02.sfo01.rainpole.local
	mgmt01nsxc03.sfo01.rainpole.local	sfo01m01nsxc03.sfo01.rainpole.local
	SFO01PSC01	sfo01psc01.sfo01.rainpole.local
	SFOMGMT-LB01	sfo01m01lb01
	SFOMGMT-ESG01	sfo01m01esg01
	SFOMGMT-ESG02	sfo01m01esg02
	SFOMGMT-UDLR01	sfo01m01udlr01
NSX for vSphere (Shared Edge and Compute)	comp01nsxm01.sfo01.rainpole.local	sfo01w01nsx01.sfo01.rainpole.local
	comp01nsxc01.sfo01.rainpole.local	sfo01w01nsxc01.sfo01.rainpole.local
	comp01nsxc02.sfo01.rainpole.local	sfo01w01nsxc02.sfo01.rainpole.local
	comp01nsxc03.sfo01.rainpole.local	sfo01w01nsxc03.sfo01.rainpole.local
	SFOCOMP-ESG01	sfo01w01esg01
	SFOCOMP-ESG02	sfo01w01esg02
	SFOCOMP-UDLR01	sfo01w01udlr01
	SFOCOMP-DLR01	sfo01w01dlr01

Table 1-6. Changed Host Names in the Disaster Recovery Components in Region A

Component	Host Name in Version 4.0	Host Name in Version 4.1
Site Recovery Manager	mgmt01srm01.sfo01.rainpole.local	sfo01m01srm01.sfo01.rainpole.local
vSphere Replication	mgmt01vrms01.sfo01.rainpole.local	sfo01m01vrms01.sfo01.rainpole.local

Table 1-7. Changed Host Names in the Data Protection Component in Region A

Component	Host Name in Version 4.0	Host Name in Version 4.1
vSphere Data Protection	mgmt01vdp01.sfo01.rainpole.local	sfo01m01vdp01.sfo01.rainpole.local

Table 1-8. Changed Host Names in the Cloud Management Platform in Region A

Component	Host Name in Version 4.0	Host Name in Version 4.1
vRealize Automation	vra01svr01.rainpole.local	No Change
	vra01svr01a.rainpole.local	No Change
	vra01svr01b.rainpole.local	No Change
	vra01iws01.rainpole.local	No Change
	vra01iws01a.rainpole.local	No Change
	vra01iws01b.rainpole.local	No Change
	vra01ims01.rainpole.local	No Change
	vra01ims01a.rainpole.local	No Change
	vra01ims01b.rainpole.local	No Change
	vra01dem01.rainpole.local	vra01dem01a.rainpole.local
	vra01dem02.rainpole.local	vra01dem01b.rainpole.local
	vra01ias01.sfo01.rainpole.local	sfo01ias01a.sfo01.rainpole.local
	vra01ias02.sfo01.rainpole.local	sfo01ias01b.sfo01.rainpole.local
	vra01mssql01.rainpole.local	No Change
vRealize Business	vra01bus01.rainpole.local	vrb01svr01.rainpole.local
	vra01buc01.sfo01.rainpole.local	sfo01vrbc01.sfo01.rainpole.local

Table 1-9. Changed Host Names in the Operations Management Layer in Region A

Component	Host Name in Version 4.0	Host Name in Version 4.1
vRealize Operations Manager	vrops-cluster-01.rainpole.local	vrops01svr01.rainpole.local
	vrops-mstrn-01.rainpole.local	vrops01svr01a.rainpole.local
	vrops-repln-02.rainpole.local	vrops01svr01b.rainpole.local
	vrops-datan-03.rainpole.local	vrops01svr01c.rainpole.local
	vrops-datan-0*x*.rainpole.local	vrops01svr01*x*.rainpole.local
	vrops-rmtcol-01.sfo01.rainpole.local	sfo01vropsc01a.sfo01.rainpole.local
	vrops-rmtcol-02.sfo01.rainpole.local	sfo01vropsc01b.sfo01.rainpole.local

Table 1-9. Changed Host Names in the Operations Management Layer in Region A (Continued)

Component	Host Name in Version 4.0	Host Name in Version 4.1
vRealize Log Insight	vrli-cluster-01.sfo01.rainpole.local	sfo01vrli01.sfo01.rainpole.local
	vrli-mstr-01.sfo01.rainpole.local	sfo01vrli01a.sfo01.rainpole.local
	vrli-wrkr-01.sfo01.rainpole.local	sfo01vrli01b.sfo01.rainpole.local
	vrli-wrkr-02.sfo01.rainpole.local	sfo01vrli01c.sfo01.rainpole.local
	vrli-wrkr-0*x*.sfo01.rainpole.local	sfo01vrli01*x*.sfo01.rainpole.local

Changed Object Names in Region A

Identify object names in the vCenter Server inventory that are different in the previous version of the VMware Validated Design and in the current version. Use this map when you follow the upgrade guidance in Region A.

Table 1-10. Changed Object Names in the Inventory of Management vCenter Server in Region A

Inventory Object	Name in Version 4.0	Name in Version 4.1
Datacenter Name	SFO01	sfo01-m01dc
Cluster Name	SFO01-Mgmt01	sfo01-m01-mgmt01
Datastore Name (VSAN)	SFO01A-VSAN01-MGMT01	sfo01-m01-vsan01
Datastore Name (NFS)	SFO01A-NFS01-VDP01	sfo01-m01-vdp01
vSphere Distributed Switch	vDS-Mgmt	sfo01-m01-vds01
Port group (Management)	vDS-Mgmt-Management	sfo01-m01-vds01-management
Port group (vMotion)	vDS-Mgmt-vMotion	sfo01-m01-vds01-vmotion
Port group (vSAN)	vDS-Mgmt-VSAN	sfo01-m01-vds01-vsan
Port group (NFS)	vDS-Mgmt-NFS	sfo01-m01-vds01-nfs
Port group (Replication)	vDS-Mgmt-VR	sfo01-m01-vds01-replication
Port group (External Management)	vDS-Mgmt-Ext-Management	sfo01-m01-vds01-ext-management
Port group (Uplink01)	vDS-Mgmt-Uplink01	sfo01-m01-vds01-uplink01
Port group (Uplink02)	vDS-Mgmt-Uplink02	sfo01-m01-vds01-uplink02
Host Profile	SFO01-Mgmt01	sfo01-m01hp-mgmt01
Folder (Platform Services Controller & vCenter Server)	MGMT01	sfo01-m01fd-mgmt
Folder (vRealize Automation Region-Agnostic)	vRA01	sfo01-m01fd-vra
Folder (vRealize Automation Region-Specific)	vRA01IAS	sfo01-m01fd-vraias
Folder (vRealize Operations Region-Agnostic)	vROps01	sfo01-m01fd-vrops

Table 1-10. Changed Object Names in the Inventory of Management vCenter Server in Region A (Continued)

Inventory Object	Name in Version 4.0	Name in Version 4.1
Folder (vRealize Operations Region-Specific)	vROps01RC	sfo01-m01fd-vropsrc
Folder (vRealize Log Insight)	vRLI01	sfo01-m01fd-vrli
Folder (NSX for vSphere)	NSX01	sfo01-m01fd-nsx
Folder Business Continuity and Disaster Recovery)	BCDR01	sfo01-m01fd-bcdr

Table 1-11. Changed Object Names in the Inventory of the Compute vCenter Server in Region A

Inventory Object	Name in Version 4.0	Name in Version 4.1
Datacenter Name	SFO01	sfo01-w01dc
Cluster Name	SFO01-Comp01	sfo01-w01-comp01
Datastore Name (VSAN)	SFO01A-VSAN01-COMP01	sfo01-w01-vsan01
Datastore Name (NFS)	SFO01A-NFS01-VRALIB01	sfo01-w01-lib01
Resource Pool - Edge	SDDC-EdgeRP01	sfo01-w01rp-sddc-edge
Resource Pool -User Edge	User-EdgeRP01	sfo01-w01rp-user-edge
Resource Pool -User VMs	User-VMRP01	sfo01-w01rp-user-vm
vSphere Distributed Switch	vDS-Comp01	sfo01-w01-vds01
Port group (Management)	vDS-Comp01-Management	sfo01-w01-vds01-management
Port group (vMotion)	vDS-Comp01-vMotion	sfo01-w01-vds01-vmotion
Port group (NFS)	vDS-Comp01-NFS	sfo01-w01-vds01-nfs
Port group (vSAN)	vDS-Comp01-VSAN	sfo01-w01-vds01-vsan
Port group (Uplink01)	vDS-Comp01-Uplink01	sfo01-w01-vds01-uplink01
Port group (Uplink02)	vDS-Comp01-Uplink02	sfo01-w01-vds01-uplink02
Host Profile	SFO01-Comp01	sfo01-w01hp-comp01

Table 1-12. Changed Objects Names in the Inventory of the Management NSX Manager in Region A

Inventory Object	Name in Version 4.0	Name in Version 4.1
NSX IP Pool (NSX Controllers)	Mgmt01-NSXC01	sfo01-mgmt01-nsxc01

Table 1-13. Changed Objects Names in the Inventory of the Compute NSX Manager in Region A

Inventory Object	Name in Version 4.0	Name in Version 4.1
NSX IP Pool (NSX Controllers)	Comp01-NSXC01	sfo01-comp01-nsxc01

Naming Changes in Region B

If your SDDC is based on VMware Validated Design 4.0, use the map between the names in our SDDC and the new names in version 4.1 to apply the upgrade guidance in Region B.

- Changed Host Names in Region B

  Identify host names that are different in the previous version of the VMware Validated Design and in the current version. Use this map when you follow the upgrade guidance in Region B.

- Changed Object Names in Region B

  Identify object names in the vCenter Server inventory that are different in the previous version of the VMware Validated Design and in the current version. Use this map when you follow the upgrade guidance in Region B.

Changed Host Names in Region B

Identify host names that are different in the previous version of the VMware Validated Design and in the current version. Use this map when you follow the upgrade guidance in Region B.

Table 1-14. Changed Host Names in the Virtual Infrastructure Layer in Region B

Component	Host Name in Version 4.0	Host Name in Version 4.1
vSphere (Management)	mgmt01psc51.lax01.rainpole.local	lax01m01psc01.lax01.rainpole.local
	mgmt01vc51.lax01.rainpole.local	lax01m01vc01.lax01.rainpole.local
	mgmt01umds51.lax01.rainpole.local	lax01umds01.lax01.rainpole.local
	mgmt01esx51.lax01.rainpole.local	lax01m01esx01.lax01.rainpole.local
	mgmt01esx52.lax01.rainpole.local	lax01m01esx02.lax01.rainpole.local
	mgmt01esx53.lax01.rainpole.local	lax01m01esx03.lax01.rainpole.local
	mgmt01esx54.lax01.rainpole.local	lax01m01esx04.lax01.rainpole.local
	mgmt01esx5*x*.lax01.rainpole.local	lax01m01esx0*x*.lax01.rainpole.local
vSphere (Shared Edge and Compute)	comp01psc51.lax01.rainpole.local	lax01m01psc01.lax01.rainpole.local
	comp01vc51.lax01.rainpole.local	lax01m01vc01.lax01.rainpole.local
	comp01esx51.lax01.rainpole.local	lax01w01esx01.lax01.rainpole.local
	comp01esx52.lax01.rainpole.local	lax01w01esx02.lax01.rainpole.local
	comp01esx53.lax01.rainpole.local	lax01w01esx03.lax01.rainpole.local
	comp01esx54.lax01.rainpole.local	lax01w01esx04.lax01.rainpole.local
	comp01esx5*x*.lax01.rainpole.local	lax01w01esx0*x*.lax01.rainpole.local
NSX for vSphere (Management)	mgmt01nsxm51.lax01.rainpole.local	lax01m01nsx01.lax01.rainpole.local
	mgmt01nsxc51.lax01.rainpole.local	lax01m01nsxc01.lax01.rainpole.local
	mgmt01nsxc52.lax01.rainpole.local	lax01m01nsxc02.lax01.rainpole.local
	mgmt01nsxc53.lax01.rainpole.local	lax01m01nsxc03.lax01.rainpole.local
	LAX01PSC51	lax01psc01.lax01.rainpole.local

Table 1-14. Changed Host Names in the Virtual Infrastructure Layer in Region B (Continued)

Component	Host Name in Version 4.0	Host Name in Version 4.1
	LAXMGMT-LB01	lax01m01lb01
	LAXMGMT-ESG01	lax01m01esg01
	LAXMGMT-ESG02	lax01m01esg02
NSX for vSphere (Compute)	comp01nsxm51.lax01.rainpole.local	lax01w01nsx01.lax01.rainpole.local
	comp01nsxc51.lax01.rainpole.local	lax01w01nsxc01.lax01.rainpole.local
	comp01nsxc52.lax01.rainpole.local	lax01w01nsxc02.lax01.rainpole.local
	comp01nsxc53.lax01.rainpole.local	lax01w01nsxc03.lax01.rainpole.local
	LAXCOMP-ESG01	lax01w01esg01
	LAXCOMP-ESG02	lax01w01esg02
	LAXCOMP-DLR01	lax01w01dlr01

Table 1-15. Changed Host Names in the Disaster Recovery Components in Region B

Component	Host Name in Version 4.0	Host Name in Version 4.1
Site Recovery Manager	mgmt01srm51.lax01.rainpole.local	lax01m01srm01.lax01.rainpole.local
vSphere Replication	mgmt01vrms51.lax01.rainpole.local	lax01m01vrms01.lax01.rainpole.local

Table 1-16. Changed Host Names in the Data Protection Component in Region B

Component	Host Name in Version 4.0	Host Name in Version 4.1
vSphere Data Protection	mgmt01vdp51.lax01.rainpole.local	lax01m01vdp01.lax01.rainpole.local

Table 1-17. Changed Host Names in the Cloud Management Platform in Region B

Component	Host Name in Version 4.0	Host Name in Version 4.1
vRealize Automation	vra01ias51.lax01.rainpole.local	lax01ias01a.lax01.rainpole.local
	vra01ias52.lax01.rainpole.local	lax01ias01b.lax01.rainpole.local
vRealize Business	vra01buc51.lax01.rainpole.local	lax01vrbc01.lax01.rainpole.local

Table 1-18. Changed Host Names in the Operations Management Layer in Region B

Component	Host Name in Verison 4.0	Host Name in Verison 4.1
vRealize Operations Manager	vrops-rmtcol-51.lax01.rainpole.local	lax01vropsc01a.lax01.rainpole.local
	vrops-rmtcol-52.lax01.rainpole.local	lax01vropsc01b.lax01.rainpole.local
vRealize Log Insight	vrli-cluster-51.lax01.rainpole.local	lax01vrli01.lax01.rainpole.local
	vrli-mstr-51.lax01.rainpole.local	lax01vrli01a.lax01.rainpole.local
	vrli-wrkr-51.lax01.rainpole.local	lax01vrli01b.lax01.rainpole.local
	vrli-wrkr-52.lax01.rainpole.local	lax01vrli01c.lax01.rainpole.local
	vrli-wrkr-5*x*.lax01.rainpole.local	lax01vrli01*x*.lax01.rainpole.local

Changed Object Names in Region B

Identify object names in the vCenter Server inventory that are different in the previous version of the VMware Validated Design and in the current version. Use this map when you follow the upgrade guidance in Region B.

Table 1-19. Changed Object Names in the Inventory of the Management vCenter Server in Region B

Inventory Object	Name in Version 4.0	Name in Version 4.1
Datacenter Name	LAX01	lax01-m01dc
Cluster Name	LAX01-Mgmt01	lax01-m01-mgmt01
Datastore Name (VSAN)	LAX01A-VSAN01-MGMT01	lax01-m01-vsan01
Datastore Name (NFS)	LAX01A-NFS01-VDP01	lax01-m01-vdp01
vSphere Distributed Switch	vDS-Mgmt	lax01-m01-vds01
Port group (Management)	vDS-Mgmt-Management	lax01-m01-vds01-management
Port group (vMotion)	vDS-Mgmt-vMotion	lax01-m01-vds01-vmotion
Port group (vSAN)	vDS-Mgmt-VSAN	lax01-m01-vds01-vsan
Port group (NFS)	vDS-Mgmt-NFS	lax01-m01-vds01-nfs
Port group (Replication)	vDS-Mgmt-VR	lax01-m01-vds01-replication
Port group (External Management)	vDS-Mgmt-Ext-Management	lax01-m01-vds01-ext-management
Port group (Uplink01)	vDS-Mgmt-Uplink01	lax01-m01-vds01-uplink01
Port group (Uplink02)	vDS-Mgmt-Uplink02	lax01-m01-vds01-uplink02
Host Profile	LAX01-Mgmt01	lax01-m01hp-mgmt01
Folder (Platform Services Controller and vCenter Server)	MGMT51	lax01-m01fd-mgmt
Folder (vRealize Automation Region-Agnostic)	vRA051	lax01-m01fd-vra
Folder (vRealize Automation Region-Specific)	vRA51IAS	lax01-m01fd-vraias
Folder (vRealize Operations Region-Agnostic)	vROps51	lax01-m01fd-vrops
Folder (vRealize Operations Region-Specific)	vROps51RC	lax01-m01fd-vropsrc
Folder (vRealize Log Insight)	vRLI51	lax01-m01fd-vrli
Folder (NSX for vSphere)	NSX51	lax01-m01fd-nsx
Folder (Business Continuity and Disaster Recovery)	BCDR51	lax01-m01fd-bcdr

Table 1-20. Changed Object Names in the Inventory of the Compute vCenter Server in Region B

Inventory Object	Name in Version 4.0	Name in Version 4.1
Datacenter Name	LAX01	lax01-w01dc
Cluster Name	LAX01-Comp01	lax01-w01-comp01
Datastore Name (VSAN)	LAX01A-VSAN01-COMP01	lax01-w01-vsan01
Datastore Name (NFS)	LAX01A-NFS01-VRALIB01	lax01-w01-lib01
Resource Pool - Edge	SDDC-EdgeRP01	lax01-w01rp-sddc-edge
Resource Pool -User Edge	User-EdgeRP01	lax01-w01rp-user-edge
Resource Pool -User VMs	User-VMRP01	lax01-w01rp-user-vm
vSphere Distributed Switch	vDS-Comp01	lax01-w01-vds01
Port group (Management)	vDS-Comp01-Management	lax01-w01-vds01-management
Port group (vMotion)	vDS-Comp01-vMotion	lax01-w01-vds01-vmotion
Port group (NFS)	vDS-Comp01-NFS	lax01-w01-vds01-nfs
Port group (vSAN)	vDS-Comp01-VSAN	lax01-w01-vds01-vsan
Port group (Uplink01)	vDS-Comp01-Uplink01	lax01-w01-vds01-uplink01
Port group (Uplink02)	vDS-Comp01-Uplink02	lax01-w01-vds01-uplink02
Host Profile	LAX01-Comp01	lax01-w01hp-comp01

Table 1-21. Changed Objects Names in the Inventory of the Management NSX Manager in Region B

Inventory Object	Name in Version 4.0	Name in Version 4.1
NSX IP Pool (NSX Controllers)	Mgmt01-NSXC01	lax01-mgmt01-nsxc01

Table 1-22. Changed Objects Names in the Inventory of the Compute NSX Manager in Region B

Inventory Object	Name in Version 4.0	Name in Version 4.1
NSX IP Pool (NSX Controllers)	Comp01-NSXC01	lax01-comp01-nsxc01

System Requirements for the SDDC Upgrade

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

- Review the Release Notes for each VMware product in the SDDC.
- Review the *VMware Validated Design Planning and Preparation* documentation and the individual prerequisites for the upgrade of each VMware Validated Design layer to understand the hardware and software requirements that might impact the SDDC upgrade.
- Verify that the server hardware has been certified with vSphere 6.5 Update 1. For information, see the VMware Compatibility Guide.

- Ensure that the server hardware meets the updated memory requirements of the SDDC. See *ESXi Host Physical Design Specifications* in the *VMware Validated Design Architecture and Design* documentation.
- Review any custom integration that might have occurred outside of VMware Validated Design to ensure compatibility with the new versions of VMware products within the SDDC.
- Review any third-party products that might be used in your environment to ensure compatibility with the new versions of VMware products within the SDDC.

Best Practices in SDDC Upgrades

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

Planning for the SDDC Update or Upgrade

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

  The VMware Validated Design upgrade sequence is organized in such a way that the upgrade of each layer can be executed within a maintenance window.
- Perform backups and snapshots of the VMware management components.
- Allocate time in your maintenance window to run test cases and validate that all integrations, important business functionality, and system performance are acceptable. Add a time buffer for responding to errors without breaching the change window.
- Consider the impact of an update or upgrade to users.

  If you properly prepare for the upgrade, existing instances, networking, and storage should continue to operate.
- Performing an upgrade with operational workloads carries risks.

  Use vSphere vMotion to temporarily migrate workloads to other compute nodes during upgrade.
- Communicate the upgrade to your users so that they can plan for their own backups.

Considerations on Upgrade Failure

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

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

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

Post-Upgrade Operations

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

- Verify important functionality, integration, and system performance. See the *VMware Validated Design Operational Verification* documentation.
- Conduct a lessons learned meeting. Document improvements and ensure that they are incorporated in the next update or upgrade cycle.

Upgrade the Cloud Management Platform

2

You start the upgrade from VMware Validated Design 4.0 to VMware Validated Design 4.1 by upgrading the Cloud Management Platform. You upgrade vRealize Automation, migrate the vRealize Orchestrator cluster from being external to embedded within vRealize Automation, and then upgrade vRealize Business for Cloud. Then you configure the components and solutions from the virtual infrastructure and operations management layer that are connected to the platform.

Procedure

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

When you upgrade the Cloud Management Platform as a part of the upgrade from VMware Validated Design 4.0 to VMware Validated Design 4.1, you start with vRealize Automation. vRealize Automation is the central engine that connects to the rest of the Cloud Management Platform components like vRealize Orchestrator and vRealize Business.

2 Migrate vRealize Orchestrator Cluster to Embedded Configuration in vRealize Automation

After you upgrade the vRealize Automation, migrate your existing external vRealize Orchestrator cluster to a vRealize Orchestrator instance that is embedded in the vRealize Automation Appliance in Region A.

3 Upgrade vRealize Business and vRealize Business Data Collectors

After you upgrade the vRealize Automation nodes and migrate the vRealize Orchestrator cluster to an embedded instance, complete the upgrade the Cloud Management Platform to VMware Validated Design 4.1 by upgrading the vRealize Business server in Region A and the remote data collectors in Region A and Region B.

4 Post-Upgrade Configuration of the Cloud Management Platform

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

In this version of this validated design, the external vRealize Orchestrator cluster is replaced with the embedded vRealize Orchestrator components in the vRealize Automation Appliances. The upgrade sequence of the Cloud Management Platform consists of the following steps:

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

Order	Components	Sub-Component
1	vRealize Automation	vRealize Automation Appliances
		vRealize Automation IaaS Components
2	Standalone vRealize Orchestrator (Deprecated) **Note** vRealize Orchestrator will be migrated from an external cluster to being embedded in vRealize Automation.	-
3	vRealize Business for Cloud	vRealize Business Server
		vRealize Business Data Collectors
4	Post-Upgrade Configuration	-

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

When you upgrade the Cloud Management Platform as a part of the upgrade from VMware Validated Design 4.0 to VMware Validated Design 4.1, you start with vRealize Automation. vRealize Automation is the central engine that connects to the rest of the Cloud Management Platform components like vRealize Orchestrator and vRealize Business.

When you update the vRealize Automation instance as a part of the upgrade from VMware Validated Design 4.0 to VMware Validated Design 4.1, you first upgrade the vRealize Automation Appliances in Region A. Then, you perform automated upgrade of the 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.local
	vRealize Automation Server Appliance	192.168.11.51	vra01svr01a.rainpole.local
		192.168.11.52	vra01svr01b.rainpole.local
	vRealize Automation for IaaS Web Server VIP	192.168.11.56	vra01iws01.rainpole.local
	vRealize Automation for IaaS Web Server	192.168.11.54	vra01iws01a.rainpole.local
		192.168.11.55	vra01iws01b.rainpole.local
	vRealize Automation Model Manager IMS VIP	192.168.11.59	vra01ims01.rainpole.local
	vRealize Automation Model Manager IMS	192.168.11.57	vra01ims01a.rainpole.local
		192.168.11.58	vra01ims01b.rainpole.local

Table 2-5. vRealize Automation Nodes in the SDDC (Continued)

Region	Role	IP Address	Full Qualified Domain Name
	vRealize Automation DEM Workers	192.168.11.60	vra01dem01a.rainpole.local
		192.168.11.61	vra01dem01b.rainpole.local
	vRealize Automation 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 Proxy Agent	192.168.32.52	lax01ias01a.lax01.rainpole.local
		192.168.31.53	lax01ias01b.lax01.rainpole.local

Note VMware Validated Design 4.1 introduces a new convention for host and object names in the SDDC. The step-by-step upgrade guidance uses the new names for both the pre- and post-upgrade SDDC setups. For information about the new convention, see Mapping Component Names Between Versions 4.0 and 4.1 of VMware Validated Design.

Prerequisites

Verify that the vRealize Automation nodes have enough compute and storage resources for the operations and temporary objects created during upgrade.

Table 2-2. Hardware Requirements for Upgrading vRealize Automation

Node	Hardware Requirement for Each Node	Description
vRealize Automation Appliances	Disk space	■ Disk1 with 50 GB, Disk3 with 25 GB, and 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 database	Disk space	5 GB

Verify that the software that is required for the upgrade is available on the vRealize Automation nodes.

Table 2-3. Software Requirements for Upgrading vRealize Automation

Node	Software Requirement	Description
Primary IaaS Model Manager Windows virtual machine vra01iws01a.rainpole.local	Java Version	■ Java SE Runtime Environment 8 64- bits Update 111 or later installed. Remove versions earlier than Update 111. ■ After you install Java, set the environment variable `JAVA_HOME` to the location of the new version.

Verify that the condition of the SDDC and download the software that is required for the upgrade is available on the vRealize Automation nodes.

Table 2-4. Configuration Prerequisites for Upgrading vRealize Automation

Prerequisite Category	Description
Compatibility	Verify that any third-party integration that might have been configured with vRealize Automation is compatible with version 7.3. Contact the vendor of the third-party software to check compatibility and availability.
Backup	■ Verify that backups of the vRealize Automation Virtual Appliances and the Infrastructure-as-a-Service (IaaS) Virtual Machines exist. See the *VMware Validated Design Backup and Restore* documentation. ■ Verify that a backup the vRealize Automation database exists on the appliance. The default name of the database is `VRADB-01`.
Downloads	■ Download the vRealize Automation `VMware-vR-Appliance-7.3.0.xxx-xxxxxxx-updaterepo.iso` upgrade file to a shared datastore. You can then mount the `.iso` file to the vRealize Automation virtual machines from the vSphere Web Client. If you have space on your NFS datastore, upload the file there. ■ Download the vRealize Automation IaaS Management Agent `.msi` file to the Windows host that you use to access the data center. See the product download page for vRealize Automation.

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 of the upgrade. See the product download page version 1.7.0.
	■ Verify that all IaaS Windows nodes meet the following requirements in the appliance management interface at **`https://vra01svr01a.rainpole.local:5480`**:
	  ■ Have a `Last Connected` status of less than 30 seconds.
	  ■ Have a `Time Offset` status of less than 1 second.
	■ Verify that both vRealize Automation appliances meet the following requirements in the appliance management interface at **`https://vra01svr01a.rainpole.local:5480`** and **`https://vra01svr01b.rainpole.local:5480`** :
	  ■ 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.
	  ■ All Services are reporting a status of `REGISTERED`

Preparing the vRealize Automation environment	■ Make the system unavailable to end users and any automated components while you perform the upgrade. ■ 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. Without quiescing the environment, rollback operations might be disruptive, generating orphaned objects that were created after snapshots have been created. You might also have to extend the time of 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

Before you upgrade the vRealize Automation appliances and the IaaS nodes, direct the traffic to the primary nodes of vRealize Automation and to turn off the health check on it on the NSX load balancer for the management applications. Because upgrade on secondary nodes might not be initialized yet, directing traffic to such a node might lead to failed requests. Health checks might interfere with the upgrade and cause unpredictable behavior.

2 Take Snapshots of the vRealize Automation Nodes

Before you perform the upgrade operation on the vRealize Automation nodes, take snapshots of them that you can use to roll the upgrade back.

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

Start the upgrade of vRealize Automation by upgrading the Management Agent on the IaaS components so that you can then push an upgrade on these nodes centrally from the vRealize Automation appliance management console.

4 Upgrade the vRealize Automation Appliances and IaaS Components

When you upgrade the vRealize Automation and the IaaS components in the SDDC, start the update process from the primary vRealize Automation appliance using the upgrade `.iso` file. The upgrade process includes both the appliances and the IaaS components automatically.

What to do next

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

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

Before you upgrade the vRealize Automation appliances and the IaaS nodes, direct the traffic to the primary nodes of vRealize Automation and to turn off the health check on it on the NSX load balancer for the management applications. Because upgrade on secondary nodes might not be initialized yet, directing traffic to such a node might lead to failed requests. Health checks might interfere with the upgrade and cause unpredictable behavior.

The configuration disables the second pool member of three vRealize Automation VIPs (vra-svr-443, vra-iaas-web-443, vra-iaas-mgr-443). During the installation or power cycle of vRealize Automation, the service inside the second node might not be upgrade or initialized yet. In this period of time, if the load balancer passes a request to the second node, the request fails. If the second pool member is not disabled, you can experience random failures during vRealize Automation upgrade, and service initialization or registration failure during a vRealize Automation power cycle.

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

Server Pool on the sfo01m01lb01 Load Balancer	Secondary Member to Disable
vra-svr-443	According to which one is the primary node: ■ vra01svr01a ■ vra01svr01b
vra-svr-8444	According to which one is the primary node: ■ vra01svr01a ■ vra01svr01b
vra-iaas-web-443	vra01iws01b
vra-iaas-mgr-443	vra01ims01b

Procedure

1 Log in to the vRealize Automation appliance management console.

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

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vra_appA_root_password*

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

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 from Step 2, 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 Step 8 to Step 10 on the other load balancer pools.

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

Take Snapshots of the vRealize Automation Nodes

Before you perform the upgrade operation on the vRealize Automation nodes, take snapshots of them that you can use to roll the upgrade back.

Table 2-6. vRealize Automation Virtual Machines

Region	Folder	Role	Virtual Machine Name
Regoin A	sfo01-m01fd-vra	vRealize Automation Appliance	vra01svr01a.rainpole.local
	sfo01-m01fd-vra		vra01svr01b.rainpole.local
	sfo01-m01fd-vra	vRealize Orchestrator Appliance	vra01vro01a.rainpole.local
	sfo01-m01fd-vra		vra01vro01b.rainpole.local
	sfo01-m01fd-vra	vRealize Automation IaaS Web Server	vra01iws01a.rainpole.local
	sfo01-m01fd-vra		vra01iws01b.rainpole.local
	sfo01-m01fd-vra	vRealize Automation Model Manager Service	vra01ims01a.rainpole.local
	sfo01-m01fd-vra		vra01ims01b.rainpole.local
	sfo01-m01fd-vra	vRealize Automation DEM Workers	vra01dem01a.rainpole.local
	sfo01-m01fd-vra		vra01dem01b.rainpole.local
	sfo01-m01fd-vraias	vRealize Automation Proxy Agent	sfo01ias01a.sfo01.rainpole.local
	sfo01-m01fd-vraias		sfo01ias01b.sfo01.rainpole.local
Region B	lax01-m01fd-vraias	vRealize Automation Proxy Agent	lax01ias01a.lax01.rainpole.local
	lax01-m01fd-vraias		lax01ias01b.lax01.rainpole.local

Procedure

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

   a Open a Web browser and go to **`https://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 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 **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 other vRealize Automation nodes.

4 Take a snapshot of the vRealize Automation virtual machines.

   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 4.1 Cloud Management Platform Upgrade
Description	-
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

   c Repeat these steps for the other machines.

5 Power on the vRealize Automation nodes 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 other vRealize Automation nodes.

Upgrade the vRealize Automation IaaS Management Agent on Each IaaS Node

Start the upgrade of vRealize Automation by upgrading the Management Agent on the IaaS components so that you can then push an upgrade on these nodes centrally from the vRealize Automation appliance management console.

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

Region	Role	Fully Qualified Domain Name
Region A	vRealize Automation IaaS Web Serevr	vra01iws01a.rainpole.local
		vra01iws01b.rainpole.local

Region	Role	Fully Qualified Domain Name
	vRealize Automation Model Manager Service	vra01ims01a.rainpole.local
		vra01ims01b.rainpole.local
	vRealize Automation DEM Workers	vra01dem01a.rainpole.local
		vra01dem01b.rainpole.local
	vRealize Automation Proxy Agent	sfo01ias01a.sfo01.rainpole.local
		sfo01ias01b.sfo01.rainpole.local
Region B	vRealize Automation Proxy Agent	lax01ias01a.lax01.rainpole.local
		lax01ias01b.lax01.rainpole.local

Prerequisites

- Download the vRealize Automation IaaS Management Agent `.msi` file to the Windows host that you use to access the data center from product download page .
- Verify that the primary Windows virtual machine of the IaaS Web Server, vra01iws01a.rainpole.local, satisfies the following requirements:
  - Installed Java SE Runtime Environment 8 64-bit update 111 or later
  - `JAVA_HOME` environment variable set to the Java home directory

Procedure

1. On the Windows host that has access to the data center, log in to the IaaS Web server by using a Remote Desktop Protocol (RDP) client.
   a. Open an RDP connection to vra01iws01a.rainpole.local.
   b. Log in using the following credentials.

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

2. Copy the agent installer `.msi` file to the file system of vra01iws01a.rainpole.local.
3. Navigate to the folder where you downloaded the IaaS Management Agent upgrade installer, and start the installer.

   The agent installation wizard appears.
4. On the **Welcome** page, click **Next**.
5. On the **End User License Agreement** page, accept the license agreement, and click **Next**.

6 On the **Management Agent Account configuration** page, provide the following settings and click **Next**.

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

7 On the **Ready to Install** page, click **Install** and wait until the installer to completes the upgrade.

8 Restart the Windows virtual machine.

9 Repeat Step 1 to Step 8 on the other IaaS components.

10 After you upgrade all IaaS nodes, log in to the vRealize Automation appliance management console and verify the build number of the management agent on each node.

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

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vra_appA_root_password*

c Click **vRA Settings > Cluster** and verify that each of the IaaS components has a **ManagementAgent** build number of 7.3.0.10750 or later.

Upgrade the vRealize Automation Appliances and IaaS Components

When you upgrade the vRealize Automation and the IaaS components in the SDDC, start the update process from the primary vRealize Automation appliance using the upgrade `.iso` file. The upgrade process includes both the appliances and the IaaS components automatically.

Region	Role	Fully Qualified Domain Name
Region A	vRealize Automation Appliances	vra01svr01a.rainpole.local
		vra01svr01b.rainpole.local
	vRealize Automation IaaS Web Server	vra01iws01a.rainpole.local
		vra01iws01b.rainpole.local
	vRealize Automation Model Manager Service	vra01ims01a.rainpole.local
		vra01ims01b.rainpole.local
	vRealize Automation DEM Workers	vra01dem01a.rainpole.local
		vra01dem01b.rainpole.local
	vRealize Automation Proxy Agent	sfo01ias01a.sfo01.rainpole.local
		sfo01ias01b.sfo01.rainpole.local

Region	Role	Fully Qualified Domain Name
Region B	vRealize Automation Proxy Agent	lax01ias01a.lax01.rainpole.local
		lax01ias01b.lax01.rainpole.local

Prerequisites

- Verify that a backup of the vRealize Automation database exists.
- Verify that a backup of the vRealize Automation appliances and IaaS virtual machines exists. See *VMware Validated Design Backup and Restore*.
- Verify that the Windows virtual machine of the primary IaaS Web server, vra01iws01a.rainpole.local, satisfies the following requirements:
  - Installed Java SE Runtime Environment 8 64-bit update 111 or later
  - `JAVA_HOME` environment variable set to the new Java home directory for Update 111 or later
- Mount the upgrade `VMware-vR-Appliance-7.3.0.xxx-xxxxxxx-updaterepo.iso` file to the primary virtual appliance vra01svr01a.rainpole.local.

Procedure

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

Settings	Value
User Name	root
Password	*vra_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** and click **Check Updates** to load the update from the ISO file.
5. Verify that the loaded **Available Updates** match the version in this VMware Validated Design and click **Install Updates**.
6. After the update completes, restart the primary appliance.

   The secondary appliance restarts automatically.

7 After the appliances start again, log in to the management console of the primary vRealize Automation appliance.

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

   b Log in using the following credentials

Settings	Value
User Name	root
Password	*vra_root_password*

8 Click the **Update** tab, click the **Status** button, and monitor the IaaS upgrade.

9 After the update completes, using the **vRA Settings > Cluster** tab, verify that the version number is 7.3.*xxx* for all IaaS nodes and their components.

10 On the **vRA Settings > Licensing** tab, verify that the product license information is not lost and a valid license is still shown.

11 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 the step on the vra01svr01b.rainpole.local appliance.

Migrate vRealize Orchestrator Cluster to Embedded Configuration in vRealize Automation

After you upgrade the vRealize Automation, migrate your existing external vRealize Orchestrator cluster to a vRealize Orchestrator instance that is embedded in the vRealize Automation Appliance in Region A.

In this version of this validated design, the external vRealize Orchestrator cluster has been replaced with vRealize Orchestrator components that are embedded in the vRealize Automation appliances.

Note You must migrate vRealize Orchestrator from external to embedded configuration in the same maintenance window in which you are upgrading vRealize Automation.

Table 2-7. vRealize Orchestrator Nodes in the SDDC

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

Note VMware Validated Design 4.1 introduces a new convention for host and object names in the SDDC. The step-by-step upgrade guidance uses the new names for both the pre- and post-upgrade SDDC setups. For information about the new convention, see Mapping Component Names Between Versions 4.0 and 4.1 of VMware Validated Design.

Prerequisites

- Upgrade to vRealize Automation 7.3.
- Allocate 6 GB of memory to the primary and secondary vRealize Orchestrator virtual appliances (vra01vro01a.rainpole.local and vra01vro01b.rainpole.local).
- Verify that the vRealize Orchestrator node configuration is valid using the **Validate Configuration** option of the vRealize Orchestrator Control Center at **`https://vra01vro01a.rainpole.local:8283/vco-controlcenter`**.
- Verify that a backup of the vRealize Orchestrator nodes participating in the cluster exists. See the *VMware Validated Design Backup and Restore* documentation.
- Verify that a backup of the vRealize Orchestrator `vROCluster` database from the Microsoft SQL server exists. See the *VMware Validated Design Backup and Restore* documentation and documentation of the Microsoft SQL server.
- Verify that a backup of the vRealize Automation appliances and IaaS Windows virtual machines exists. ee the *VMware Validated Design Backup and Restore* documentation.
- Verify that a backup of the vRealize Automation database from the appliance exists.
- Direct the traffic to the primary vRealize Automation nodes if the Load Balancer has been reconfigured after the upgrade of vRealize Automation. See Direct Traffic to the Primary Nodes and Disable Health Monitoring for vRealize Automation on the Load Balancer.
- Verify that the vRealize Automation environment has been quiesced of all activities, including but not limited to, users ordering new virtual machines and third-party integration that may automate the order of new virtual machines. Without quiescing the environment, rollback operations might be disrupted by generate orphaned objects. You might also have to extend the time of the maintenance window.
- Verify that any third-party integration that might have been configured with vRealize Automation and vRealize Orchestrator is compatible with version 7.3. Contact the vendor of the third-party software to check compatibility and availability.

Procedure

1 Take Snapshots of vRealize Orchestrator and vRealize Automation and Start Control Center on vRealize Automation Appliance

When you upgrade the vRealize Orchestrator Cluster in the SDDC, start the update process by verifying the resource requirements of the vRealize Orchestrator Cluster and then taking snapshots of both the vRealize Automation and vRealize Orchestrator virtual machines.

2 Configure Load Balancing for vRealize Automation with Embedded vRealize Orchestrator

Before you export the configuration of an external Orchestrator server and import it to vRealize Automation 7.3,reconfigure the load balancer to handle the traffic to the Orchestrator servers that are built in to the vRealize Automation virtual appliances.

3 Configure Authentication Provider for vRealize Orchestrator in Region A

Configure vRealize Orchestrator to use the Rainpole local tenant in vRealize Automation for authentication. By associating vRealize Orchestrator authentication to a non-default tenant, vRealize Orchestrator executes workflows with end-user permissions. If vRealize Orchestrator authenticates using the default tenant, Orchestrator users will always have administrative rights.

4 Migrate the External vRealize Orchestrator Cluster in vRealize Automation in Region A

Export the configuration from your existing external Orchestrator cluster and import it to the Orchestrator server that is built in to the vRealize Automation primary appliance. Migrate the Orchestrator database from the external Microsoft SQL server to the PostgreSQL server on the appliance.

5 Rejoin the Secondary vRealize Automation Appliance to the Primary Appliance

Re-join the secondary vRealize Automation appliance vra01svr01b.rainpole.local to the cluster where the vra01svr01b.rainpole.local appliance is primary. As a result, the secondary appliance re-synchronizes with the primary appliance for the latest data and configuration settings after the migration to embedded vRealize Orchestrator.

6 Verify the Migration of the vRealize Orchestrator Workflows and Configuration in Region A

After performing the migration from external to embedded vRealize Orchestrator in vRealize Automation, verify that standard and custom workflows have been migrated successfully.

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

After you upgrade the vRealize Automation components and migrate the vRealize Orchestrator to the vRealize Automation appliance, restore health checks on and distribution of traffic, including Orchestrator traffic, between the primary and secondary components of vRealize Automation for a fault-tolerant Cloud Management Platform.

8 Reconfigure vRealize Automation to Use Embedded vRealize Orchestrator

After you export the configuration of an external Orchestrator server cluster and import it to vRealize Orchestrator embedded in the vRealize Automation 7.3 cluster, direct vRealize Automation to the embedded vRealize Orchestrator instances.

9 Delete the Snapshots of the vRealize Orchestrator and vRealize Automation Appliances

After you complete the migration of the vRealize Orchestrator nodes, clean up the virtual machine snapshots you have taken before the upgrade of vRealize Automation and vRealize Orchestrator migration to embedded deployment.

What to do next

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

Take Snapshots of vRealize Orchestrator and vRealize Automation and Start Control Center on vRealize Automation Appliance

When you upgrade the vRealize Orchestrator Cluster in the SDDC, start the update process by verifying the resource requirements of the vRealize Orchestrator Cluster and then taking snapshots of both the vRealize Automation and vRealize Orchestrator virtual machines.

Region	Folder	Role	Virtual Machine Name
Regoin A	sfo01-m01fd-vra	vRealize Automation Appliance	vra01svr01a.rainpole.local
	sfo01-m01fd-vra		vra01svr01b.rainpole.local
	sfo01-m01fd-vra	vRealize Orchestrator Appliance	vra01vro01a.rainpole.local
	sfo01-m01fd-vra		vra01vro01b.rainpole.local
	sfo01-m01fd-vra	vRealize Automation IaaS Web Server	vra01iws01a.rainpole.local
	sfo01-m01fd-vra		vra01iws01b.rainpole.local
	sfo01-m01fd-vra	vRealize Automation Model Manager Service	vra01ims01a.rainpole.local
	sfo01-m01fd-vra		vra01ims01b.rainpole.local
	sfo01-m01fd-vra	vRealize Automation DEM Workers	vra01dem01a.rainpole.local
	sfo01-m01fd-vra		vra01dem01b.rainpole.local
	sfo01-m01fd-vra	Microsoft SQL Server	vra01mssql01.rainpole.local
	sfo01-m01fd-vraias	vRealize Automation Proxy Agent	sfo01ias01a.sfo01.rainpole.local
	sfo01-m01fd-vraias		sfo01ias01b.sfo01.rainpole.local
Region B	lax01-m01fd-vraias	vRealize Automation Proxy Agent	lax01ias01a.lax01.rainpole.local
	lax01-m01fd-vraias		lax01ias01b.lax01.rainpole.local

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 Shut down the vRealize Orchestrator and vRealize Automation 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 **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 other vRealize Orchestrator and vRealize Automation nodes.

4 Verify that both vRealize Orchestrator nodes vra01vro01a.rainpole.local and vra01vro01b.rainpole.local have their memory increased to 6 GB.

   a In the **Navigator**, click **VMs and Templates** and navigate to the vra01vro01a.rainpole.local virtual machine.

   b Right-click the **vra01vro01a.rainpole.local** virtual machine and select **Edit Settings**.

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

Setting	Value
CPU	2
Memory	6144 MB (6 GB)

   d Repeat these steps for vra01vro01b.rainpole.local.

5 Take a snapshot of each node in the vRealize Orchestrator cluster and vRealize Automation components.

   a In the **Navigator**, click **VMs and Templates** and navigate to the vra01vro01a.rainpole.local virtual machine.

   b Right-click the **vra01vro01a.rainpole.local** virtual machine and select **Snapshot > Take Snapshot**.

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

Setting	Value
Name	VMware Validated Design 4.1 Cloud Management Platform vRealize Orchestrator Migration
Description	-
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

d Repeat these steps for vra01vro01b.rainpole.local and for the other components of the vRealize Automation components.

Performing this operation results in having two layers of snapshots for the vRealize Automation components: `VMware Validated Design 4.1 Cloud Management Platform Upgrade` and `VMware Validated Design 4.1 Cloud Management Platform vRealize Orchestrator Migration`. In this way, you can perform a rollback to vRealize Automation stack version 7.3 with external vRealize Orchestrator if the vRealize Orchestrator migration fails. In addition, if the allocated maintenance window is exceeded, you must roll the entire vRealize Automation stack back to version 7.2 and then perform the upgrade again later.

6 Power the vRealize Automation and vRealize Orchestrator nodes back on 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 other vRealize Automation and vRealize Orchestrator nodes.

7 Log in to the vRealize Automation appliance and run the following commands to start the vRealize Orchestrator services.

a Open an SSH client to the primary vRealize Orchestrator virtual appliance **vra01svr01a.rainpole.local**

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vra_appA_root_password*

c Start the Control Center service of the built-in vRealize Orchestrator server.

```
service vco-configurator start
```

Configure Load Balancing for vRealize Automation with Embedded vRealize Orchestrator

Before you export the configuration of an external Orchestrator server and import it to vRealize Automation 7.3,reconfigure the load balancer to handle the traffic to the Orchestrator servers that are built in to the vRealize Automation virtual appliances.

You port the load balancing settings for vRealize Orchestrator to the vRealize Automation appliance nodes. Redefine health checks and Orchestrator pool members, and associate the new components with the vRealize Automation application profile.

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 and click **Load Balancer**.

6 Select **Service Monitoring**.

a Click the **Add** icon, in the **New Service Monitor** dialog box, configure the values for the service monitor you are adding, and click **OK**.

Setting	Value
Name	vra-vro-8283-monitor
Interval	3
Timeout	10
Max Retries	3
Type	HTTPS
Expected	
Method	GET
URL	/vco-controlcenter/docs
Send	
Receive	
Extension	

7 On the **Load Balancer** tab, select **Pools** and add a pool for Orchestrator traffic that consists of the vRealize Automation appliances.

a Click the **Add** icon, in the **New Pool** dialog box, configure the following values.

Setting	Value
Name	vra-vro-8283
Algorithm	ROUND-ROBIN
Monitors	NONE

b Under **Members**, click the **Add** icon to add the primary vRealize Automation appliance as the first pool member.

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

Setting	Value
Name	vra01svr01a
IP Address/VC Container	192.168.11.51
State	Enable
Port	8283
Monitor Port	8283
Weight	1

d Under **Members**, click the **Add** icon to add the secondary vRealize Automation appliance as the second pool member.

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

Setting	Value
Name	vra01svr01b
IP Address/VC Container	192.168.11.52
State	Disable
Port	8283
Monitor Port	8283
Weight	1

f Click **OK** in the **New Pool** dialog box to save the server pool for traffic to the embedded Orchestrator.

8 Select **Virtual Servers** and add a virtual server to associate the vRealize Automation application profile with the pool for traffic to the embedded Orchestrator.

a Click the **Add** icon .

b In the **New Virtual Server** dialog box, enter the following values, and click **OK**.

Setting	Value
Enable Virtual server	Selected
Application Profile	vRealize-https-persist
Name	vra-vro-8283
Description	Embedded vRealize Orchestrator Control Center
IP Address	192.168.11.53
Protocol	HTTPS
Port	8283
Default Pool	vra-vro-8283

9 Repeat Step 4 to Step 8 on the lax01m01lb01 load balancer using the NSX Manager for the management cluster in Region B 172.17.11.65.

10 Verify that the load balancer is properly configured by logging in to the Control Center of the embedded vRealize Orchestrator instance.

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*

Configure Authentication Provider for vRealize Orchestrator in Region A

Configure vRealize Orchestrator to use the Rainpole local tenant in vRealize Automation for authentication. By associating vRealize Orchestrator authentication to a non-default tenant, vRealize Orchestrator executes workflows with end-user permissions. If vRealize Orchestrator authenticates using the default tenant, Orchestrator users will always have administrative rights.

Procedure

1 Log in to the 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	root
Password	*vra_appA_root_password*

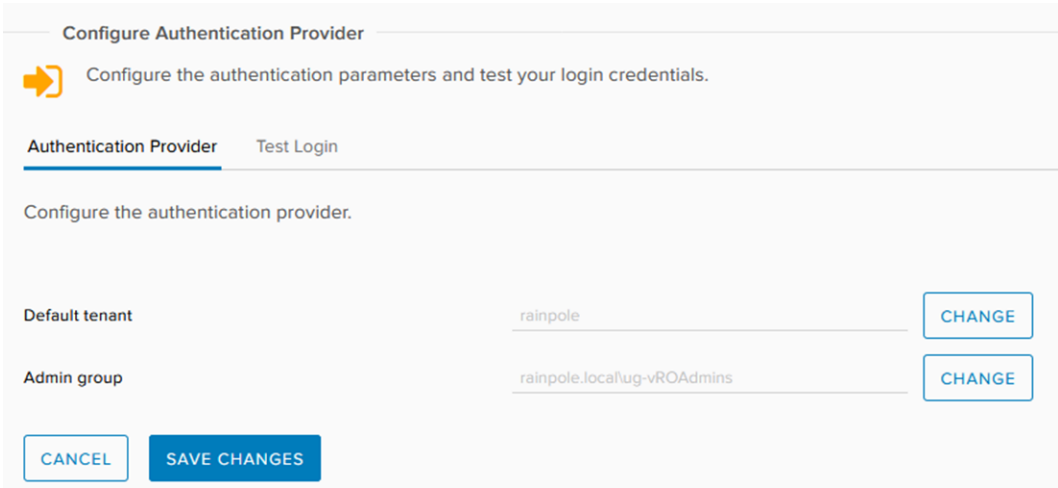
2 Configure vRealize Automation as a vRealize Orchestrator authentication provider.

   a On the **Home** page, under **Manage**, click **Configure Authentication Provider**.

   b In the **Default Tenant** text box, click the **Change** button, enter **rainpole**, and click **Apply**.

   c In the **Admin group** text box, enter **ug–vRO** and click **Search**.

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



The control center logs you out.

3 Verify that you can successfully log in as svc-vra.

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

   b Log in using the following credentials.

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

4 Log out of control center.

5 Open an SSH connection to both vRealize Automation appliances vra01svr01a.rainpole.local and vra01svr01b.rainpole.local, and run the following commands to restart the vRealize Orchestrator services.

```
service vco-server restart
service vco-configurator restart
```

6 Log back in to control center as the svc-vra user.

Note The log in process might be delayed due to the vRealize Orchestrator services restarting.

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

   b Log in using the following credentials.

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

Migrate the External vRealize Orchestrator Cluster in vRealize Automation in Region A

Export the configuration from your existing external Orchestrator cluster and import it to the Orchestrator server that is built in to the vRealize Automation primary appliance. Migrate the Orchestrator database from the external Microsoft SQL server to the PostgreSQL server on the appliance.

Procedure

1 Export the configuration from the external Orchestrator cluster.

   a Open an SSH connection to the primary vRealize Orchestrator virtual appliance **`vra01vro01a.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vro_appA_root_password*

   c Run the following command to export the vRealize Orchestrator configuration as a `/tmp/vro-config.zip` file.

```
/usr/lib/vco/tools/configuration-cli/bin/vro-configure.sh export --skipLicense --path /tmp/vro-config.zip
```

2 Migrate the exported configuration to the embedded Orchestrator instance on the primary vRealize Automation appliance.

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

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vra_appA_root_password*

   c Stop the Orchestrator server and the Control Center services of the built-in vRealize Orchestrator server.

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

   d By using `scp` copy the exported vRealize Orchestrator configuration ZIP file to vRealize Automation.

```
scp root@vra01vro01a.rainpole.local:/tmp/vro-config.zip /tmp/vro-config.zip
```

e When prompted, accept the SSL certificate from the vRealize Orchestrator appliance by typing **yes**.

f Change the ownership of the exported Orchestrator configuration file.

```
chown vco:vco /tmp/vro-config.zip
```

g Import the Orchestrator configuration file to the built-in vRealize Orchestrator server using `vro-configure` .

```
/usr/lib/vco/tools/configuration-cli/bin/vro-configure.sh import --skipDatabaseSettings --
skipLicense --skipSettings --skipSslCertificate --skipTrustStore --notForceImportPlugins --
notRemoveMissingPlugins --path /tmp/vro-config.zip
```

h Set the Control Center service of the built-in vRealize Orchestrator server on vRealize Automation appliance vra01svr01a.rainpole.local to automatically start on restart of the appliance.

```
chkconfig vco-configurator on
```

3 Migrate the external vRealize Orchestrator database to the PostgreSQL server running on the vRealize Automation appliance.

a Run the following command to migrate the external vRealize Orchestrator database `vROCluster` from the vra01mssql01.rainpole.local Microsoft SQL node using the svc-vro service account for the PostgreSQL database.

```
/usr/lib/vco/tools/configuration-cli/bin/vro-configure.sh db-migrate --sourceJdbcUrl
jdbc:jtds:sqlserver://vra01mssql01:1433/VROCluster\;domain=rainpole.local --sourceDbUsername
svc-vro --sourceDbPassword svc-vro_password
```

b Clean up irrelevant data from the imported vRealize Orchestrator database.

```
sudo -u postgres -i -- /opt/vmware/vpostgres/current/bin/psql vcac -c "DELETE FROM
vmo_clustermember;"
```

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
```

Rejoin the Secondary vRealize Automation Appliance to the Primary Appliance

Re-join the secondary vRealize Automation appliance vra01svr01b.rainpole.local to the cluster where the vra01svr01b.rainpole.local appliance is primary. As a result, the secondary appliance re-synchronizes with the primary appliance for the latest data and configuration settings after the migration to embedded vRealize Orchestrator.

Procedure

1 Log in to the appliance management console of the secondary vRealize Automation appliance.

   a Open a Web browser and go to **`https://vra01svr01b.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vra_appB_root_password*

2 Rejoin the secondary appliance to the primary appliance.

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

   b Under the **Distributed Deployment Information** pane, enter the following settings and click **Join Cluster**.

Setting	Value
Leading Cluster Node	vra01svr01a.rainpole.local
Admin User	root
Password	*vra_appA_root_password*

   c When prompted, accept the certificate of the primary vRealize Automation appliance.

   d Allow for the vra01svr01b.rainpole.local to re-synchronize with vra01svr01a.rainpole.local.

3 Verify on the secondary appliance that all services are registered and license information is valid.

   a After the synchronization is complete, click the **Services** tab and verify that all services on vra01svr01b.rainpole.local are registered.

   b Click the **vRA Settings > Licensing** tab and verify that the product license licensing information is available and valid.

   Note If the license is removed, enter the license key in the **New License Key** field and click **Submit Key**. Verify that the license has been successfully applied. Repeat this step for **vra01svr01a.rainpole.local** appliance.

4 Log in to the secondary vRealize Automation appliance using a Secure Shell (SSH) client.

   a Open an SSH connection to vra01svr01b.rainpole.local.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vra_appA_root_password*

5 Restart the Orchestrator server and Control Center services on the appliance and verify if they are running.

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

6 Set the Control Center service of the built-in vRealize Orchestrator server on vra01svr01b.rainpole.local to automatically start on restart of the appliance.

```
chkconfig vco-configurator on
```

7 Verify that the vRealize Orchestrator cluster is synchronized on the primary vRealize Automation appliance.

   a Open a Web browser and go to **`https://vra01svr01a.rainpole.local:8283/vco-controlcenter`**.

   b Log in using the following credentials.

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

   c On the home page, click **Validate Configuration** under **Manage** and verify that the report shows no errors for any component.

   d On the home page, click **Orchestrator Cluster Management**, and verify that only the vRealize Automation appliances are present and that the `Configuration Synchronization State` is a green `Synchronized`.

8 If you cannot access the vRealize Orchestrator Control Center on the primary appliance, reset the authentication provider and reconfigure the vRealize Orchestrator registration.

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

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vra_appA_root_password*

c Reset the authentication provider for vRealize Orchestrator.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication
```

d Remove the vRealize Orchestrator registration file.

```
rm /etc/vco/app-server/vco-registration-id
```

e Reconfigure the vRealize Orchestrator registration.

```
vcac-vami vco-service-reconfigure
```

f Restart the Orchestrator server and the Control Center services of the built-in vRealize Orchestrator server.

```
service vco-server restart && service vco-configurator restart
```

Verify the Migration of the vRealize Orchestrator Workflows and Configuration in Region A

After performing the migration from external to embedded vRealize Orchestrator in vRealize Automation, verify that standard and custom workflows have been migrated successfully.

Procedure

1 Download and install the vRealize Orchestrator Client.

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

b Click **vRealize Orchestrator Client** and download the `.jnlp` file of the vRealize Orchestrator client.

c On the **VMware vRealize Orchestrator Login** page, log in to the embedded vRealize Orchestrator by using the following credentials.

2 Open the downloaded Orchestrator `.jnlp` file, and in the **VMware vRealize Orchestrator Login** dialog box log in to vRealize Orchestrator using the following credentials.

Setting	Value
Host name	vra01svr01.rainpole.local:443
User name	svc-vra
Password	*svc-vra_password*

3 In the left navigation pane, click the **Workflows** tab, and navigate to different sub-folders in the `Library` and `System` folders to verify that all the standard and custom workflows have been migrated from your external vRealize Orchestrator instance.

4 To verify that the vRealize Automation and vCenter Server plug-ins are working and configured properly, click the **Inventory** tab in the left navigation pane.

   a Expand **vRealize Automation Infrastructure** and verify that the **IaaS host for vra01svr01.rainpole.local** entry is listed.

   b Expand **vRealize Automation** and verify that the vRealize Automation cluster is listed.

   c Expand **vSphere vCenter Plug-in** and verify that all the vCenter Server instances that the external vRealize Orchestrator were integrated with are also listed.

   d Verify that all the other plug-in endpoints that were configured in the external vRealize Orchestrator have been configured similarly in the embedded vRealize Orchestrator.

5 Execute some custom workflows in the embedded vRealize Orchestrator to verify that they work as expected.

   These workflows can then be safely used in vRealize Automation blueprints.

   For example, execute complex workflows that involve integration with external systems.

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

After you upgrade the vRealize Automation components and migrate the vRealize Orchestrator to the vRealize Automation appliance, restore health checks on and distribution of traffic, including Orchestrator traffic, between the primary and secondary components of vRealize Automation for a fault-tolerant Cloud Management Platform.

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

Server Pool on the 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-iaas-web-443	vra01iws01b	vra-iaas-web-443-monitor
vra-iaas-mgr-443	vra01ims01b	vra-iaas-mgr-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 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 Step 6 to Step 8 on the other load balancer pools.

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

Reconfigure vRealize Automation to Use Embedded vRealize Orchestrator

After you export the configuration of an external Orchestrator server cluster and import it to vRealize Orchestrator embedded in the vRealize Automation 7.3 cluster, direct vRealize Automation to the embedded vRealize Orchestrator instances.

Procedure

1 Log in to the vRealize Automation portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator
Password	*vra_administrator_password*
Domain	vsphere.local

2 Click **Administration > vRO Configuration > Server Configuration**.

3 Select the **Use the default Orchestrator server** radio button and click **Test Connection**.

4 When prompted, click **OK** in the **Delete Endpoints** warning message.

5 After the `Successfully connected to the Orchestrator server` message appears, click **OK** to complete the configuration.

6 Lot out from the vRealize Automation portal.

7 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	*itac-tenantadmin_password*
Domain	Rainpole.local

8 Create a new endpoint for the embedded vRealize Orchestrator instance.

   a Click **Infrastructure > Endpoints > Endpoints**.

   b Select **New > Orchestration > vRealize Orchestrator** , enter the following values, and click **OK**.

Setting	Value
Name	vra01svr01.rainpole.local
Address	https://vra01svr01.rainpole.local/vco
User name	svc-vra@rainpole.local
Password	*svc-vra_password*
Priority	1

9 Start the data collection about compute resources for the newly-created endpoint.

   a On the **Endpoints** page, select the vRealize Orchestrator endpoint vra01svr01.rainpole.local and click **Actions > Data Collection**.

   b Click **Start** to begin the data collection process and wait several minutes until the data collection process completes.

   c Click **Refresh** to verify that the data collection successfully completed.

   A message that data collection succeeded appears.

Delete the Snapshots of the vRealize Orchestrator and vRealize Automation Appliances

After you complete the migration of the vRealize Orchestrator nodes, clean up the virtual machine snapshots you have taken before the upgrade of vRealize Automation and vRealize Orchestrator migration to embedded deployment.

Table 2-8. vRealize Automation and Orchestrator Virtual Machines

Region	Folder	Role	Virtual Machine Name
Regoin A	sfo01-m01fd-vra	vRealize Automation Appliance	vra01svr01a.rainpole.local
	sfo01-m01fd-vra		vra01svr01b.rainpole.local
	sfo01-m01fd-vra	vRealize Orchestrator Appliance	vra01vro01a.rainpole.local
	sfo01-m01fd-vra		vra01vro01b.rainpole.local
	sfo01-m01fd-vra	vRealize Automation IaaS Web Server	vra01iws01a.rainpole.local
	sfo01-m01fd-vra		vra01iws01b.rainpole.local
	sfo01-m01fd-vra	vRealize Automation Model Manager Service	vra01ims01a.rainpole.local
	sfo01-m01fd-vra		vra01ims01b.rainpole.local
	sfo01-m01fd-vra	vRealize Automation DEM Workers	vra01dem01a.rainpole.local
	sfo01-m01fd-vra		vra01dem01b.rainpole.local
	sfo01-m01fd-vra	Microsoft SQL Server	vra01mssql01.rainpole.local

Table 2-8. vRealize Automation and Orchestrator Virtual Machines (Continued)

Region	Folder	Role	Virtual Machine Name
	sfo01-m01fd-vraias	vRealize Automation Proxy Agent	sfo01ias01a.sfo01.rainpole.local
	sfo01-m01fd-vraias		sfo01ias01b.sfo01.rainpole.local
Region B	lax01-m01fd-vraias	vRealize Automation Proxy Agent	lax01ias01a.lax01.rainpole.local
	lax01-m01fd-vraias		lax01ias01b.lax01.rainpole.local

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-vra** tree.

4 Right-click the **vra01vro01a.rainpole.local** virtual machine and select **Snapshots > Delete All Snapshots**.

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

6 Repeat the procedure for the vra01vro01b.rainpole.local virtual appliance and the vRealize Automation components.

Upgrade vRealize Business and vRealize Business Data Collectors

After you upgrade the vRealize Automation nodes and migrate the vRealize Orchestrator cluster to an embedded instance, complete the upgrade the Cloud Management Platform to VMware Validated Design 4.1 by upgrading the vRealize Business server in Region A and the remote data collectors in Region A and Region B.

Table 2-9. 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

Note VMware Validated Design 4.1 introduces a new convention for host and object names in the SDDC. The step-by-step upgrade guidance uses the new names for both the pre- and post-upgrade SDDC setups. For information about the new convention, see Mapping Component Names Between Versions 4.0 and 4.1 of VMware Validated Design.

Prerequisites

- Download the vRealize Business upgrade `vRealize-Business-Standard-x.x.xxx-xxxxxxx-updaterepo.iso` file to a shared datastore for mounting to the virtual appliances.

  If you have space on your NFS datastore, upload the file there.
- Allocate 8 GB RAM and 4 vCPUs to the vRealize Business Server appliance.
- Verify that backups of the vRealize Business appliances exist. See the *VMware Validated Design Backup and Restore* documentation.

Procedure

1 Upgrade the vRealize Business Server Appliance

  When you upgrade the vRealize Business server appliance and the region-specific data collectors in the SDDC, start the process from the vRealize Business server by using the virtual appliance management interface.

2 Upgrade the vRealize Business Data Collectors

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

3 Delete the Snapshots of the vRealize Business Appliances

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

What to do next

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

Upgrade the vRealize Business Server Appliance

When you upgrade the vRealize Business server appliance and the region-specific data collectors in the SDDC, start the process from the vRealize Business server by using the virtual appliance management interface.

Prerequisites

- Mount the upgrade `vRealize-Business-for-Cloud-7.3.x.xxx-xxxxxxx-updaterepo.iso` file to the virtual appliance vrb01svr01.rainpole.local.

Procedure

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

a Open a Web browser and go to **`https://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 vRealize Business server appliance.

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.rainpole.local** virtual machine and select **Snapshot > Take Snapshot**.

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

Setting	Value
Name	VMware Validated Design 4.1 Cloud Management Platform Upgrade
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

3 Log in to the appliance management interface of the vRealize Business server appliance.

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

   b Log in using the following credentials.

Setting	Value
User Name	root
Password	*vrb_root_password*

4 Unregister vRealize Business from the Rainpole tenant 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	rainpole
SSO Admin User	administrator
SSO Admin Password	*vra_administrator_password*

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

5 Start the upgrade of the appliance.

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

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

   c Click the **Status** button and click **Check Updates** to load the update from the ISO.

   d Click **Install Updates**.

6 After the reboot is complete, log in to the appliance management interface of the vRealize Business server appliance.

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

   b Log in using the following credentials.

Setting	Value
User Name	root
Password	*vrb_root_password*

7 Re-register vRealize Business with the default tenant in vRealize Automation.

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

b Enter the following settings.

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

c Select the **Accept "vRealize Automation" certificate** check box to accept the certificate of vRealize Automation and click **Register**.

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

What to do next

Login and verify that the license key for vRealize Business for Cloud is still valid within vRealize Automation. For more information, see the *Update Licenses for vRealize Business for Cloud* section of the vRealize Business for Cloud 7.3 Installation and Administration documentation.

Upgrade the vRealize Business Data Collectors

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

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

Prerequisites

- Mount the upgrade `vRealize-Business-for-Cloud-7.3.x.xxx-xxxxxxx-updaterepo.iso` file to the sfo01vrbc01.sfo01.rainpole.local and lax01vrbc01.lax01.rainpole.local virtual appliances.

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 vRealize Business Server remote data collector.

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

   b Right-click the **sfo01vrbc01.sfo01.rainpole.local** virtual machine and select **Snapshot > Take Snapshot**.

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

Setting	Value
Name	VMware Validated Design 4.1 Cloud Management Platform Upgrade
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

   d Repeat this process for lax01vrbc01.lax01.rainpole.local under the lax01m01vc01.lax01.rainpole.local vCenter Server.

3 Log in to the appliance management interface of the vRealize Business data collector appliance.

   a Open a Web browser and go the following URL.

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

   b Log in using the following credentials.

Setting	Value
User Name	root
Password	*vrb_collector_root_password*

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

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

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

7 Repeat this operation on the other remote data collector lax01vrbc01.lax01.rainpole.local.

What to do next

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

Delete the Snapshots of the vRealize Business Appliances

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

Table 2-10. vRealize Business Virtual Machines in the SDDC

Region	VM Folder	Virtual Machine
Region A	sfo01-m01fd-vra	vrb01svr01.rainpole.local
	sfo01-m01fd-vraias	sfo01vrbc01.sfo01.rainpole.local
Region B	lax01-m01fd-vraias	lax01vrbc01.lax01.rainpole.local

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.rainpole.local** virtual machine and select **Manage Snapshots**.

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

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

6 Repeat the procedure for the data collectors of vRealize Business.

Post-Upgrade Configuration of the Cloud Management Platform

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

Procedure

1 Update the Load Balancing Service Monitoring Timeout Setting in Region A and Region B

   Increase the timeout in the health checks for the vRealize Automation components to make the environment complaint with the deployment guidelines of this version of the validated design.

2 Create an NSX Endpoint in vRealize Automation in Region A

After you upgrade vRealize Automation, create an endpoint for NSX in the shared edge and compute pod according to the deployment guidelines of this validated design. In this way, vRealize Automation can communicate with NSX Manager to discover networking resources for tenant workloads.

3 Configure Embedded vRealize Orchestrator to Forward Log Events to vRealize Log Insight in Region A

After migrating vRealize Orchestrator from an external cluster to embedded deployment in vRealize Automation, update the vRealize Log Insight agent and configure the agent group for the embedded Orchestrator instance to continue collecting log data in the vRealize Orchestrator dashboards.

4 Decomission the External vRealize Orchestrator Cluster

After you migrate vRealize Orchestrator from an external cluster to the vRealize Automation Appliance, decommission the external cluster. You clean up the vRealize Orchestrator virtual machines, update the load balancers for the management applications, remove the dedicated endpoint in vRealize Automation, and so on.

Update the Load Balancing Service Monitoring Timeout Setting in Region A and Region B

Increase the timeout in the health checks for the vRealize Automation components to make the environment complaint with the deployment guidelines of this version of the validated design.

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 **Service Monitoring**.

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

7 On the **Edit Service Monitor** dialog box, change the **Timeout** value to **`10`** and click **OK**.

8 Repeat Step 6 to Step 7 to change the health check timeout on the vra-iaas-web-443-monitor and vra-iaas-mgr-443-monitor monitors.

9 Repeat Step 4 to Step 8 on the lax01m01lb01 load balancer that is connected to the NSX Manager 172.17.11.65 in Region B.

Create an NSX Endpoint in vRealize Automation in Region A

After you upgrade vRealize Automation, create an endpoint for NSX in the shared edge and compute pod according to the deployment guidelines of this validated design. In this way, vRealize Automation can communicate with NSX Manager to discover networking resources for tenant workloads.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	*itac-tenantadmin_password*
Domain	Rainpole.local

2 Navigate to **Infrastructure > Endpoints > Endpoints** and click **New > Network and Security > NSX**.

3 On the **General** page, configure the vRealize Automation endpoint with the following settings.

Setting	Value
Name	SFO-NSXEndpoint
Address	https://sfo01w01nsx01.sfo01.rainpole.local
User Name	rainpole\svc-vra
Password	*svc_vra_password*

4 Click **Test Connection**.

5 Click the **Associations** tab, click **New**, select **sfo01w01vc01.sfo01.rainpole.local** from the **Name** drop-down menu, and click **OK**.

6 If a **Security Alert** window appears, click **OK**.

7 Click **OK** to create the endpoint.

Configure Embedded vRealize Orchestrator to Forward Log Events to vRealize Log Insight in Region A

After migrating vRealize Orchestrator from an external cluster to embedded deployment in vRealize Automation, update the vRealize Log Insight agent and configure the agent group for the embedded Orchestrator instance to continue collecting log data in the vRealize Orchestrator dashboards.

Procedure

1 Reconfigure the vRealize Log Insight agents for vRealize Orchestrator.

   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 Locate the agent group for vRealize Orchestrator.

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

   b Under **Management**, click **Agents**.

   c From the drop-down menu at the top, select **vRO7 - Agent Group** from the **All Agents** section.

3 Add the agents on the vRealize Automation appliances to the group.

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

Filter	Operator	Values
Hostname	matches	■ vra01svr01a.rainpole.local ■ vra01svr01b.rainpole.local

   b Click **Refresh** and verify that in the **Agents** list vRealize Log Insight receives data from the vRealize Automation agents.

4 Remove the agents on the deprecated vRealize Orchestrator appliances.

   a In the **agent filter** fields, locate the following values and delete them from the agent group.

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

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

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

6 Verify that the vRealize Log Insight server is receiving log events from the vRealize Orchestrator appliances.

   a Click on **Dashboards**, select **VMware - Orchestrator - 7.0.1+** from the **Navigator** menu on the left side.

   b Verify that the **Server nodes grouped by hostname** widget on the **Server overview** dashboard shows the two vRealize Automation hosts.

Decomission the External vRealize Orchestrator Cluster

After you migrate vRealize Orchestrator from an external cluster to the vRealize Automation Appliance, decommission the external cluster. You clean up the vRealize Orchestrator virtual machines, update the load balancers for the management applications, remove the dedicated endpoint in vRealize Automation, and so on.

Prerequisites

- Upgrade vRealize Automation to version 7.3
- Migrate workflows and configuration data from the external vRealize Orchestrator cluster to the embedded vRealize Orchestrator.
- Configure vRealize Automation to utilize the embedded vRealize Orchestrator components.
- Configure the other applications that use the external vRealize Orchestrator to use the embedded vRealize Orchestrator.
- Configure vRealize Automation blueprints to use the embedded vRealize Orchestrator so that these blueprints can be provisioned successfully.

Remove the vRealize Orchestrator Virtual Machines from the vCenter Server Inventory

Delete the virtual machines that are part of the external vRealize Orchestrator cluster from the inventory. vRealize Orchestrator has been migrated to an instance that is embedded in the vRealize Automation Appliance according to the objectives of this version of the validated design.

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** tree.

3 Click the **sfo01-m01fd-vra** folder and click the **VMs > Virtual Machines** tab.

4 Select the **vra01vro01a.rainpole.local** and **vra01vro01b.rainpole.local** virtual machines and click the **Shut Down Guest OS** button.

5 Select the two Orchestrator virtual machines again and select **Actions > Remove from Inventory** and click **Yes** to confirm.

Note You can clean up the virtual machines at a later time after verifying that the SDDC is in a working state after the upgrade.

6 Clean up the Orchestrator database `vROCluster` on the external Microsoft SQL server.

Remove the Components for External vRealize Orchestrator from the Load Balancer

On the management load balancers in Region A and Region B, clean up the configuration that is related to the external vRealize Orchestrator. It is longer needed after the migration to embedded vRealize Orchestrator.

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 and click **Load Balancer**.

6 Select **Virtual Servers**, click the **vra-vro-8281** virtual server, click the **Delete** icon and click **Yes** to confirm.

7 Select **Pools**, select the **vra-vro-8281** pool, click the **Delete** icon and click **Yes** to confirm.

8 Select **Service Monitoring**, select the **vra-vro-8281-monitor** service monitor, click the **Delete** icon and click **Yes** to confirm.

9 Repeat Step 4 to Step 8 on the lax01m01lb01 load balancer that is connected to the 172.17.11.65 NSX Manager in Region B.

Delete the Endpoint for the External vRealize Orchestrator in vRealize Automation

After you migrate to embedded vRealize Orchestrator, delete the endpoint in vRealize Automation that is connected to the external Orchestrator cluster.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	*itac-tenantadmin_password*
Domain	Rainpole.local

2 Click **Infrastructure > Endpoints > Endpoints**.

3 Select the **vra01vro01.rainpole.local** endpoint and click the **Delete** icon. .

4 Click **Yes** in the **Delete** warning dialog box.

Remove vRealize Orchestrator from Existing Protection Group

After upgrading the Cloud Management Platform components, and migrating vRealize Orchestrator to the vRealize Automation Appliance, you no longer need to protect the external vRealize Orchestrator cluster up 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 home page, click **Sites** and select the **sfo01m01vc01.sfo01.rainpole.local** protected site.

4 On the **Related Objects** tab, click the **Protection Groups** tab and right click **vRA-vRO-vRB-PG** Protection Group and select **Edit Protection Group**.

   The **Edit Protection Group** wizard appears.

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

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

6 On the **Protection group type** page, verify the following settings and click **Next**.

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

7 On the **Virtual machines** page, deselect the virtual machines of vRealize Orchestrator appears as **Not Found:vm-id** from the list of virtual machines, and click **Next**.

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

9 On the **Apply Changes** page, click **Finish.**

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

10 On the **Related Objects** tab, click the **Recovery Plans** tab and right click **vRA-vRO-vRB-RP** Protection Group and select **Edit Plan..**

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

Property	Value
Name	SDDC Cloud Management RP
Description	Recovery Plan for Cloud Management
Site pair	sfo01m01vc01.sfo01.rainpole.local - lax01m01vc01.lax01.rainpole.local

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

13 On the **Protection groups** page, verify the protection group for the recovery plan and click **Next**

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

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

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

Remove vRealize Orchestrator from Existing Backup Jobs in Region A

After upgrading the Cloud Management Platform components, and migrating vRealize Orchestrator to the vRealize Automation Appliance, you no longer need to back the external vRealize Orchestrator cluster up by using vSphere Data Protection.

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

3 On the **Welcome to vSphere Data Protection** page, select **sfo01m01vdp01** from the **VDP Appliance** drop-down menu and click **Connect**.

4 Click the **Backup** tab.

5 Locate the **Cloud Management Platform Backups** backup job.

6 From the **Backup job actions** menu, click **Edit**.

7 On the **Editing backup job** page, in the left pane, click **2 Backup Sources**.

8 On the **Backup Sources** page, fully expand the virtual machines tree.

Object	Value
vCenter Server	sfo01m01vc01.sfo01.rainpole.local
Data center	sfo01-m01dc
Cluster	sfo01-m01-mgmt01

9 Locate the following virtual machines for vRealize Orchestrator, and deselect them from the job.

vRealize Automation Component	VM Name
vRealize Orchestrator	vra01vro01a.rainpole.local
	vra01vro01b.rainpole.local

10 In the left pane, click **6 Ready to Complete**.

11 On the **Ready to Complete** page, verify that the backup job has the following configuration and click **Finish**.

Setting	Value
Name	Cloud Management Platform Backups
Select Sources:	■ vra01svr01a.rainpole.local ■ vra01svr01b.rainpole.local ■ vra01ims01a.rainpole.local ■ vra01ims01b.rainpole.local ■ vra01iws01a.rainpole.local ■ vra01iws01b.rainpole.local ■ vra01mssql01.rainpole.local ■ sfo01ias01a.sfo01.rainpole.local ■ sfo01ias01b.sfo01.rainpole.local ■ vra01dem01a.rainpole.local ■ vra01dem01b.rainpole.local ■ vrb01svr01.rainpole.local ■ sfo01vrbc01.sfo01.rainpole.local
Backup Destination	VDP Appliance storage
Fall back to non-quiesced backup if quiescence fails	Yes
Backup schedule	Daily
Retention Policy	3 Days

Upgrade Operations Management Components

3

After you upgrade the Cloud Management Platform, upgrade vRealize Operations Manager and vRealize Log Insight which are the components of the Operations Management stack to continue monitoring the existing and upgraded components by using the latest capabilities in the new release.

Table 3-1. Upgrade Sequence for the Operations Management Layer

Order	Component	Sub-Component
1	vRealize Operations Manager	-
2	Post-Upgrade Reconfiguration of vRealize Operations Manager	-
3	vRealize Log Insight	vRealize Log Insight Appliances
		vRealize Log Insight Agents
4	Post-Upgrade Reconfiguration of vRealize Log Insight	-

- Upgrade vRealize Operations Manager

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

- Upgrade vRealize Log Insight

  Upgrade the vRealize Log Insight clusters and agents in Region A and Region B so that you can use the new features of and have an environment that is compliant with VMware Validated Design version 4.1 .

Upgrade vRealize Operations Manager

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

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

Table 3-3. 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

Note VMware Validated Design 4.1 introduces a new convention for host and object names in the SDDC. The step-by-step upgrade guidance uses the new names for both the pre- and post-upgrade SDDC setups. For information about the new convention, see Mapping Component Names Between Versions 4.0 and 4.1 of VMware Validated Design.

Prerequisites

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

  Table 3-2. PAK Files That Are Required for vRealize Operations Manager Upgrade

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

- Clone any customized content to preserve it.

  Customized content can include alert definitions, symptom definitions, recommendations, and views.

- Verify that a backup of the vRealize Operations Manager virtual appliances exists. See *VMware Validated Design Backup and Restore*.

Procedure

1 Take the vRealize Operations Manager Nodes Offline and Take Snapshots

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

2 Upgrade the Operating System of the vRealize Operations Manager Appliances

  When you upgrade the vRealize Operation Manager analytics cluster and the region-specific remote collectors in the SDDC, start the upgrade process by upgrading the operating system of the virtual appliances first. You use the vRealize Operations Manager administration interface of the master node.

3 Upgrade the vRealize Operations Manager Software

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

4 Upgrade the Management Pack for NSX for vSphere in vRealize Operations Manager

  Upgrade the vRealize Operations Manager Management Pack for NSX for vSphere to provide continuous interoperability with the different components of the SDDC. The other management packs in VMware Validated Design 4.0 are pre-installed in the version of vRealize Operations Manager in VMware Validated Design 4.1.

5 Delete the Snapshots of the vRealize Operations Manager Appliances

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

6 Post-Upgrade Configuration of vRealize Operations Manager

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

What to do next

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

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-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 master node vRealize Operations Manager administrator interface of your 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 nodes 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 4.1 Operations Upgrade`** in the **Reason** text box and click **OK**.

3 Wait until all nodes in the analytics cluster are offline and the **Cluster Status** states `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 of each node in the cluster.

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 4.1 Operations Upgrade
Description	-
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

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

Upgrade the Operating System of the vRealize Operations Manager Appliances

When you upgrade the vRealize Operation Manager analytics cluster and the region-specific remote collectors in the SDDC, start the upgrade process by upgrading the operating system of the virtual appliances first. You use the vRealize Operations Manager administration interface of the master node.

Procedure

1 Log in to the administrator interface of the vRealize Operations Manager master node.

a Open a Web browser and go to **`https://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-x.x.x.xxxxxxx.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, click 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 update of the operation system is complete.

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

9 After the software update is complete, log back in to the administrator interface of the master node and verify that the cluster is online on the **Cluster Status** page.

Upgrade the vRealize Operations Manager Software

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

Procedure

1 Log in to the administrator interface of the vRealize Operations Manager master node.

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

b Log in using the following credentials.

Setting	Value
User Name	admin
Password	*vrops_admin_password*

2 Take all nodes offline to put the cluster in maintenance mode.

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 box, enter **`VMware Validated Design 4.1 Operations Upgrade`** in the **Reason** text box and click **OK**.

3 Wait until all nodes in the analytics cluster are offline and the **Cluster Status** becomes `Offline`.

4 Perform the upgrade of vRealize Operations Manager virtual appliance.

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-x.x.x.xxxxxxx.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 I**mportant Update and Release Information** and click **Next**.

g On the **Install Software Update** page, click **Install**.

5 Wait until the update of the operation system is complete.

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

6 After the software update is complete, log back in to the administrator interface of the master node, and on the **Cluster Status** page, verify if the cluster is online automatically.

7 After verifying that the cluster has come back online automatically, before logging back into the operations UI, clear your browser cache to view all objects in the vRealize Operations Manager operations interface correctly.

Upgrade the Management Pack for NSX for vSphere in vRealize Operations Manager

Upgrade the vRealize Operations Manager Management Pack for NSX for vSphere to provide continuous interoperability with the different components of the SDDC. The other management packs in VMware Validated Design 4.0 are pre-installed in the version of vRealize Operations Manager in VMware Validated Design 4.1.

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 management pack `.pak` file 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`.

What to do next

After you update the management pack software, you must reconnect the adapter instances for NSX for vSphere. See Post-Upgrade Configuration of vRealize Operations Manager.

Delete the Snapshots of the vRealize Operations Manager Appliances

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

Procedure

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

   a Open a Web browser and go to **`https://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 Delete the snapshot of each node in the cluster.

   a From the **Home** menu, click **VMs and Templates**.

   b In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01fd-vrops** tree.

   c Right-click the **vrops01svr01a** virtual machine and select **Snapshots > Manage Snapshots**.

   d On the **Snapshots tab**, click the snapshot that you created before the vRealize Operations Manager update and select **Delete a VM Snapshot**.

3 Repeat the procedure for the other virtual machines of vRealize Operations Manager.

Region	Role	Virtual Machine Name
Region A	Master Replica Node	vrops01svr01b
	Data Node 1	vrops01svr01c
	Remote Collector 1	sfo01vropsc01a
	Remote Collector 2	sfo01vropsc01b

Region	Role	Virtual Machine Name
Region B	Remote Collector 1	lax01vropsc01a
	Remote Collector 2	lax01vropsc01b

Post-Upgrade Configuration of vRealize Operations Manager

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

Procedure

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

In this version of the validated design, you dedicate service accounts on vSphere for each integration with vRealize Operations Manager and you assign them global permissions accordingly. This version also introduces a naming convention for service accounts for consistency.

2 Configure Adapter Credentials for Dedicated Service Accounts in vRealize Operations Manager

After you upgrade vRealize Operations Manager to the version used in this design, for collecting statistics you dedicate service accounts on vSphere for safe application-to-application communication. Configure the adapters in vRealize Operations Manager for the products where you introduce these service accounts.

3 Connect vRealize Operations Manager to vRealize Business in Region A

In this version of this validated design, you can view infrastructure performance, cost information, and troubleshooting tips that are provided by vRealize Business for Cloud in the operations interface of vRealize Operations Manager. Configure the vRealize Operations Manager Management Pack for vRealize Business to connect to the vRealize Business instance in the SDDC.

4 Enable vSAN Monitoring in vRealize Operations Manager

In this version of this validated design, you can view vSAN topology and collect data about vSAN capacity and issues in vRealize Operations Manager. Configure the vRealize Operations Management Pack for vSAN to enable this monitoring.

5 Configure User Privileges on vRealize Automation for Integration with vRealize Operations Manager

In version 7.3 of vRealize Automation and later, assign the infrastructure architect role to the svc-vrops-vra service account in the addition to the software architect role. vRealize Operations Manager must have both roles to collect statistics about the operation of vRealize Automation.

6 Clean Up Obsolete Service Accounts for vRealize Operations Manager in vSphere

In this version of the design, you change the service account configuration for vRealize Operations Manager in vSphere to dedicate a service account to each solution in vRealize Operations Manager and to follow a consistent naming convention for accounts. Remove the global permissions for the deprecated accounts in vSphere in Region A to restrict unauthorized access to the SDDC.

Configure User Privileges in vSphere for Integration with vRealize Operations Manager

In this version of the validated design, you dedicate service accounts on vSphere for each integration with vRealize Operations Manager and you assign them global permissions accordingly. This version also introduces a naming convention for service accounts for consistency.

- The svc-vrops-vsphere and svc-vrops-nsx users have read-only access on all objects in vCenter Server.
- The svc-vrops-mpsd and svc-vrops-vsan users have rights that are specifically required for access to storage device and VSAN information, respectively, in vRealize Operations Manager on all objects in vCenter Server.

You assign global permissions to these service accounts by assigning them the following roles:

User	Role
svc-vrops-vsphere@rainpole.local	Read-only
svc-vrops-nsx@rainpole.local	Read-only
svc-vrops-vsan@rainpole.local	MPSD Metrics User
svc-vrops-mpsd@rainpole.local	MPSD Metrics User

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 **Administration**.
3. Click **Global Permissions** in the **Access Control** area.
4. Click **Add permission** on the **Manage** tab.
5. In the **Global Permissions Root - Add Permission** dialog box, click **Add** to associate a user or a group with a role.
6. In the **Select Users/Groups** dialog box, select the first user
   a. From the **Domain** drop-down menu, select **rainpole.local**
   b. In the filter box type **`svc-vrops`** and press **Enter**.
   c. From the list of users and groups, select **svc-vrops-vsphere**, click **Add**, and click **OK**.

7 Select a role.

   a In the **Global Permissions Root - Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **Read-only**.

   b Ensure that **Propagate to children** is selected and click **OK**.

8 Repeat the steps to assign global permissions to the other service accounts.

Configure Adapter Credentials for Dedicated Service Accounts in vRealize Operations Manager

After you upgrade vRealize Operations Manager to the version used in this design, for collecting statistics you dedicate service accounts on vSphere for safe application-to-application communication. Configure the adapters in vRealize Operations Manager for the products where you introduce these service accounts.

In this version of the validated design, you redefine services accounts to follow a consistent naming convention or add new accounts for extending the set of monitored products. This validated design changes or introduces service accounts for vRealize Operations Manager for the following areas:

- vSphere
- NSX Manager
- Storage devices

Reconfigure the vCenter Adapter Instances with a New Service Account in vRealize Operations Manager

After you have upgraded the analytics cluster, reconfigure the vCenter Adapter instances to use the svc-vrops-vsphere service account that is specifically dedicated to collecting data about vSphere object from the vCenter Server inventory. This version of the validated design introduces a separate service account for vRealize Operations Manager for each integration with another management product.

You replace the svc-vrops service account from the earlier version of this validated design with svc-vrops-vsphere in the credentials for the following adapters:

Region	vCenter Server	Display Name
Region A	Management	vCenter Adapter - sfo01m01vc01
	Shared edge and compute	vCenter Adapter - sfo01w01vc01
Region B	Management	vCenter Adapter - lax01m01vc01
	Shared edge and compute	vCenter Adapter - lax01w01vc01

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, click **Solutions**.

4 On the **Solutions** page, select the **VMware vSphere** solution, and click the **Configure** icon at the top.

   The **Manage Solution - VMware vSphere** dialog box appears.

5 In the **Instance Name** pane, select **vCenter Adapter - sfo01m01vc01.**

6 In the **Instance Settings** pane, click the **Edit Credential** icon.

7 In the **Manage Credentials** dialog box, change the service account credentials and click **OK**.

Setting	Value
User Name	svc-vrops-vsphere@rainpole.local
Password	*svc-vrops-vsphere-password*

8 Click **Test Connection** to validate the connection to the vCenter Server instance.

9 In the **Review and Accept Certificate** dialog box, verify the certificate information and click **Accept**.

10 Click **OK** in the **Info** dialog box.

11 Click **Save Settings**.

12 In the **Info** dialog box, click **OK**.

13 Repeat the procedure for the remaining vCenter Adapter instances.

14 In the **Manage Solution - VMware vSphere** dialog box, click **Close**.

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

After you have upgraded the analytics cluster, reconfigure the NSX-vSphere Adapter instances to use the svc-vrops-nsx service account that is specifically dedicated to collecting data about NSX objects from NSX Manager and vCenter Server. This version of the validated design introduces a separate service account for vRealize Operations Manager for each integration with another management product.

You replace the svc-vrops service account from the earlier version of this validated design with svc-vrops-nsx in the credentials for the following adapters:

Region	NSX Manager	Display Name
Region A	Management	NSX Adapter - sfo01m01nsx01
	Shared edge and compute	NSX Adapter - sfo01w01nsx01
Region B	Management	NSX Adapter - lax01m01nsx01
	Shared edge and compute	NSX Adapter - lax01w01nsx01

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, click **Solutions**.

4 On the **Solutions** page, select the **Management Pack for NSX-vSphere** solution, and click the **Configure** icon.

   The **Manage Solution - Management Pack for NSX-vSphere** dalog box appears.

5 From the **Adapter Type** table at the top, select **NSX-vSphere Adapter**.

6 In the **Instance Name** pane, select **NSX Adapter - sfo01m01nsx01**.

7 In the **Instance Settings** pane, click the **Edit Credential** icon.

8 In the **Manage Credentials** dialog box, change the service account credentials and click **OK**.

Setting	Value
vCenter User Name	svc-vrops-nsx@rainpole.local
vCenter Password	*svc_vrops_nsx_password*

9 Click **Test Connection** to validate the connection to the NSX Manager instance.

10 In the **Review and Accept Certificate** dialog box, verify the certificate information and click **Accept**.

11 Click **OK** in the **Info** dialog box.

12 Click **Save Settings**.

13 In the **Info** dialog box, click **OK**.

14 Repeat the procedure for the remaining NSX-vSphere Adapter instances.

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

Reconfigure the Storage Device Adapters in vRealize Operations Manager

After you have upgraded the analytics cluster, reconfigure the Storage Devices Adapter instances to use the svc-vrops-mpsd service account that replaces the service account from the earlier version of this validated design. This version of the validated design introduces a consistent naming convention for service accounts for vRealize Operations Manager. As a result, you reintroduce certain service accounts under new names for compliance with this convention.

You replace the svc-mpsd-vrops service account from the earlier version of this validated design with svc-vrops-mpsd in the credentials for the following adapters:

Region	vCenter Server	Display Name
Region A	Management	Storage Devices Adapter - sfo01m01vc01
	Shared edge and compute	Storage Devices Adapter - sfo01w01vc01
Region B	Management	Storage Devices Adapter - lax01m01vc01
	Shared edge and compute	Storage Devices Adapter - lax01w01vc01

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, click **Solutions**.

4 On the **Solutions** page, select **Management Pack for Storage Devices** from the solution table and click **Configure**.

   The **Manage Solution - Management Pack for Storage Devices** dialog box appears.

5 In the **Instance Name** pane, select **Storage Devices Adapter - sfo01m01vc01**.

6 In the **Instance Settings** pane, click the **Edit Credential** icon.

7 In the **Manage Credentials** dialog box, update the following values and click **OK**.

Setting	Value
User Name	svc-vrops-mpsd@rainpole.local
Password	*svc-vrops-mpsd-password*

8 Click **Test Connection** to validate the connection to the vCenter Server instance.

9 In the **Review and Accept Certificate** dialog box, verify the certificate information and click **Accept**.

10 Click **OK** in the **Info** dialog box.

11 Click **Save Settings**.

12 In the **Info** dialog box, click **OK**.

13 Repeat the procedure for the remaining Storage Adapter instances.

14 In the **Manage Solution - Management Pack for Storage Devices** dialog box, click **Close**.

Connect vRealize Operations Manager to vRealize Business in Region A

In this version of this validated design, you can view infrastructure performance, cost information, and troubleshooting tips that are provided by vRealize Business for Cloud in the operations interface of vRealize Operations Manager. Configure the vRealize Operations Manager Management Pack for vRealize Business to connect to the vRealize Business instance in the SDDC.

You can connect vRealize Operations Manager to a single instance of vRealize Business for Cloud.

Configure vRealize Business Adapter in vRealize Operations Manager

Configure a vRealize Business adapter to collect monitoring data from vRealize Business and launch the dashboards of vRealize Business in 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 On the main navigation bar, click **Administration**.

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

4 From the solution table on the **Solutions** page, select the **VMware vRealize Business for Cloud** solution, and click **Configure**.

   The **Manage Solution - VMware vRealize Business for Cloud** dialog box appears.

5 In the **Instance Settings** pane, enter the settings for connection to vRealize Business for Cloud.

   a Enter the display name, description and FQDN of the vRealize Business for Cloud server.

Setting	Value for vRealize Business for Cloud Server
Display Name	vRealize Business Adapter - vrb01svr01
Description	vRealize Business for Cloud Server
vRealize Business for Cloud server	vrb01svr01.rainpole.local

   b Click **Test Connection** to validate the connection to the vRealize Business server.

   c Click **OK** in the **Info** dialog box.

   d Expand the **Advanced Settings** section of settings.

   e From the **Collectors/Groups** drop-down menu, make sure that the **Default collector group** is selected.

6 Click **Save Settings**.

7 Click **OK** in the **Info** dialog box.

8 In the **Manage Solution - VMware vRealize Business for Cloud** dialog box, click **Close**.

   The **vRBC Adapter** appears on the **Solutions** page of the vRealize Operations Manager operations interface. The **Collection State** of the adapter is `Collecting` and the **Collection Status** is `Data receiving`.

Verify Connectivity to vRealize Business for Cloud in Region A

To verify integration of vRealize Business for Cloud with vRealize Operations Manager, run a Private Cloud Reclamation report from the vRealize Operations Manager operations interface. If the integration is interrupted, re-register the Compute vCenter Server in Region A with vRealize Business.

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 **Home**.

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

4 Log in to vRealize Business using the following credentials.

Setting	Value
User name	itac-tenantadmin
Tenant	rainpole
Password	*itac-tenantadmin_password*

The dashboard of vRealize Business opens on the **Business Management** page of the vRealize Operations Manager operations interface.

5 On the **Business Management** page, click **Overview** and locate the **Private Cloud Reclamation** widget on the right.

6 If on running the report, the integration message `Cost Savings from Private Cloud reclamation requires integration with vRealize Operations Manager` appears, re-register vRealize Business with the Compute vCenter Server in Region A.

a Open a Web browser and go to **`https://sfo01vrbc01.sfo01.rainpole.local:9443/dc-ui`**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_collector_root_password*

c Click **Manage Private Cloud Connections** and select **vCenter Server**.

d Select the Compute vCenter Server **sfo01w01vc01.sfo01.rainpole.local** and click the **Delete** icon.

The connection to Compute vCenter Server is removed.

e Click **Add**.

f In the **Add vCenter Server Connections** dialog box, enter the following settings and click **Save**.

Setting	Value
Name	sfo01w01vc01.sfo01.rainpole.local
vCenter Server	sfo01w01vc01.sfo01.rainpole.local
Username	svc-vra@rainpole.local
Password	*svc_vra_password*

g In the **SSL Certificate** dialog box, click **Install**.

h In the **Success** dialog box, click **OK**.

7 Wait several minutes for vRealize Business to initiate a synchronization, run the report again and verify that it is generated successfully.

Enable vSAN Monitoring in vRealize Operations Manager

In this version of this validated design, you can view vSAN topology and collect data about vSAN capacity and issues in vRealize Operations Manager. Configure the vRealize Operations Management Pack for vSAN to enable this monitoring.

Turn On vSAN Performance Service

When you create a vSAN cluster, the performance service is disabled. Turn on the vSAN performance service to monitor the performance of vSAN clusters, hosts, disks, and VMs in Region A and B in the operations interface of vRealize Operations Manager.

When you turn on the performance service, vSAN places a Stats database object in the datastore to collect statistical data. The Stats database is a namespace object in the vSAN datastore of the cluster.

Region	Management vCenter Server	Cluster Name
Region A	sfo01m01vc01.sfo01.rainpole.local	sfo01-m01-mgmt01
Region B	lax01m01vc01.lax01.rainpole.local	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://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 Enable the vSAN performance service.

   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** tree.

   c Click the **sfo01-m01-mgmt01** cluster object and click the **Configure** tab.

   d Under **vSAN**, select **Health and Performance**.

   e Next to the **Performance Service** settings, click **Edit**, configure the following settings and click **OK**.

Setting	Value for sfo01-m01-mgmt01	Value for lax01-m01-mgmt01
Region	Region A	Region B
Turn ON vSAN performance service	Selected	Selected
Storage policy	vSAN Default Storage Policy	vSAN Default Storage Policy

3 Repeat the procedure for the lax01-m01-mgmt01 cluster in the lax01m01vc01.lax01.rainpole.local.

Add a vSAN Adapter Instances in vRealize Operations Manager

Configure vSAN Adapters to collect monitoring data about vSAN usage in the SDDC in Region A and B in to 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 On the main navigation bar, click **Administration**.

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

4 On the **Solutions** page, select **VMware vSAN** from the solution table, and click **Configure**.

The **Manage Solution - VMware vSAN** page dialog box appears.

5 In the **Instance Settings** pane, enter the following settings.

Setting	Management vCenter in Region A	Management vCenter in Region B
Display Name	vSAN Adapter - sfo01m01vc01	vSAN Adapter - lax01m01vc01
Description	Management vCenter Server vSAN Adapter for sfo01	Management vCenter Server vSAN Adapter for lax01
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.sfo01.rainpole.local

6 Click the **Add** icon next to the **Credential** text box, and configure the credentials for connection to vCenter Server, and click **OK**.

Setting	Management vCenter in Region A	Management vCenter in Region B
Credential name	vSAN Adapter Credentials - sfo01m01vc01	vSAN Adapter Credentials - lax01m01vc01
vCenter User Name	svc-vrops-vsan@rainpole.local	svc-vrops-vsan@rainpole.local
vCenter Password	*svc-vrops-vsan-password*	*svc-vrops-vsan-password*

7 Validate the connection to vCenter Server.

a Click **Test Connection** to validate the connection to vCenter Server.

b In the **Review and Accept Certificate** dialog box, verify the vCenter Server certificate information and click **Accept**.

c Click **OK** in the **Info** dialog box.

8 Select the group of remote collectors to collect data from vCenter Server.

   a Expand the **Advanced Settings** section of settings.

   b From the **Collectors/Groups** drop-down menu, select the corresponding collector group.

Setting	Region A	Region B
Collector group	sfo01-remote-collectors	lax01-remote-collectors

9 Click **Save Settings** and click **OK** in the **Info** dialog box that appears.

10 In the **Instance Name** pane, click **Add** to create an adapter for the management vSAN cluster in Region B and repeat Step 5 to Step 9.

11 If you have a vSAN datastore configured in the shared edge and compute clusters repeat Step 5 to Step 9 for the Compute vCenter Server for both regions.

12 In the **Manage Solution - VMware vSAN** dialog box, click **Close**.

The vSAN Adapters appear on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapters is `Collecting` and the **Collection Status** is `Data receiving`.

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

In version 7.3 of vRealize Automation and later, assign the infrastructure architect role to the svc-vrops-vra service account in the addition to the software architect role. vRealize Operations Manager must have both roles to collect statistics about the operation of vRealize Automation.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	*itac-tenantadmin_password*
Domain	Rainpole.local

2 Navigate to **Administration > Users & Groups > Directory Users and Groups** to assign the infrastructure architect role to the svc-vrops-vra service account.

3 Enter **`svc-vrops-vra`** in the search box, click the **Search** icon and click **svc-vrops-vra (svc-vrops-vra@rainpole.local)** user.

   The settings of the svc-vrops-vra account appear.

4 On the **General** tab, select **Infrastructure Architect** under **Add roles to this User**, and click **Finish**.

Clean Up Obsolete Service Accounts for vRealize Operations Manager in vSphere

In this version of the design, you change the service account configuration for vRealize Operations Manager in vSphere to dedicate a service account to each solution in vRealize Operations Manager and to follow a consistent naming convention for accounts. Remove the global permissions for the deprecated accounts in vSphere in Region A to restrict unauthorized access to the SDDC.

Table 3-4. Changes in Service Account

Service Account in Verison 4.0	Service Account in Version 4.1	Role
svc-vrops@rainpole.local	■ svc-vrops-vsphere@rainpole.local ■ svc-vrops-nsx@rainpole.local	Read-only
svc-mpsd-vrops@rainpole.local	■ svc-vrops-mpsd@rainpole.local ■ svc-vrops-vsan@rainpole.local	MPSD Metrics User

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 **Administration**.

3 Click **Global Permissions** under **Access Control.**

4 Locate the `svc-vrops` service account and click **Remove permission** on the **Manage** tab.

5 In the **Delete Permission** dialog box, click **Yes** to remove the service account.

6 Repeat the steps remove the `svc-mpsd-vrops` global service account.

Upgrade vRealize Log Insight

Upgrade the vRealize Log Insight clusters and agents in Region A and Region B so that you can use the new features of and have an environment that is compliant with VMware Validated Design version 4.1 .

Upgrade both of the vRealize Log Insight clusters in Region A and Region B from the user interface of the master nodes; upgrade by using the Integrated Load Balancer IP address is not supported. All the other nodes are upgraded automatically. The upgrade path for vRealize Log Insight will be in multiple increments in order to take you from version 4.0 to version 4.5 as you must upgrade to each intermediate release.

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

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

Table 3-6. 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

Note VMware Validated Design 4.1 introduces a new convention for host and object names in the SDDC. The step-by-step upgrade guidance uses the new names for both the pre- and post-upgrade SDDC setups. For information about the new convention, see Mapping Component Names Between Versions 4.0 and 4.1 of VMware Validated Design.

Prerequisites

- Download the vRealize Log Insight product upgrade `VMware-vRealize-Log-Insight-x.x.x-xxxxxxx.pak` files for the appropriate version(s) on the Windows host that has access to the data center.

  Table 3-5. PAK Files That Are Required for vRealize Log Insight Upgrade

PAK Type	PAK File
Software update .pak file for version 4.3	VMware-vRealize-Log-Insight-4.3.0-xxxxxxx.pak
Software update .pak file for version 4.5	VMware-vRealize-Log-Insight-4.5.0-xxxxxxx.pak

- Verify that you have a user account with the minimum of **Edit Admin** permission for the vRealize Log Insight Web Interface.
- Verify that a backup of the vRealize Log Insight Virtual Appliances exists

Procedure

1 Take Snapshots of the vRealize Log Insight Nodes

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

2 Upgrade the vRealize Log Insight Clusters

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

3 Upgrade the Content Packs on vRealize Log Insight

After upgrading the vRealize Log Insight, upgrade the content packs in the environment to take advantage of the latest features of the packs while monitoring the environment.

4 Upgrade the vRealize Log Insight Agents on the Windows Nodes

After upgrading the vRealize Log Insight, upgrade the individual vRealize Log Insight agents on the Windows hosts within the environment to take advantage of the latest features. In this version of this validated design, log agents run on the Windows nodes of vRealize Automation.

5 Delete the Snapshots of the vRealize Log Insight Appliances

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

6 Post-Upgrade Configuration of the vRealize Log Insight

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

What to do next

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

Take Snapshots of the vRealize Log Insight Nodes

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

Table 3-7. 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, click **VMs and Templates**.

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

4 Take a snapshot of each node in the cluster.

   a Right-click the **sfo01vrli01a** 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 4.1 Operations Upgrade
Description	-
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

   c Repeat these steps for the other virtual machines in the cluster in Region A.

5 Repeat the procedure for the nodes in Region B under the lax01m01vc01.lax01.rainpole.local vCenter Server in the vSphere Web Client.

Upgrade the vRealize Log Insight Clusters

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

When upgrading the two vRealize Log Insight clusters in Region A or Region B, you can upgrade two vRealize Log Insight instances one after the other or in parallel. The upgrade of vRealize Log Insight from version 4.0 to version 4.5 has multiple increments because you must upgrade to each of the intermediate releases.

Table 3-8. Upgrade Path for vRealize Log Insight

Increment	Upgrade From	Upgrade To	PAK File
1	vRealize Log Insight 4.0	vRealize Log Insight 4.3	`VMware-vRealize-Log-Insight-4.3.0-xxxxxxx.pak`
2	vRealize Log Insight 4.3	vRealize Log Insight 4.5	`VMware-vRealize-Log-Insight-4.5.0-xxxxxxx.pak`

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 **Cluster** and click **Upgrade Cluster**.

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

5 In the **Upgrade Log Insight** dialog box, click **Upgrade** and wait until the `.pak` file uploads to the master appliance.

6 On the **End User License Agreement** page, click **Accept**.

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

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

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

8 After the upgrade process for the whole cluster completes, the Integrated Load Balancer comes back online.

9 After the Integrated Load Balancer becomes `Availabile`, repeat this process using the vRealize Log Insight `.pak` file for the second increment.

10 Repeat the two-step upgrade on the cluster in Region B.

Upgrade the Content Packs on vRealize Log Insight

After upgrading the vRealize Log Insight, upgrade the content packs in the environment to take advantage of the latest features of the packs while monitoring the environment.

You download the latest content packs for the vRealize Log Insight clusters in each region from the Content Pack Marketplace. You can start with downloading and updating the content packs in Region A. Then repeat this task with downloading and updating the content packs in Region B.

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 **og Insight Content Pack Marketplace** pane, click **Update All** to upgrade all content packs to their latest version.

5 Once the content packs have been upgraded, click each of the items under **Installed Content Packs** on the left and verify that the `Version` number of each content pack matches the version for this validated design.

6 Repeat the procedure on the cluster in Region B by logging in to the https://lax01vrli01.lax01.rainpole.local.

Upgrade the vRealize Log Insight Agents on the Windows Nodes

After upgrading the vRealize Log Insight, upgrade the individual vRealize Log Insight agents on the Windows hosts within the environment to take advantage of the latest features. In this version of this validated design, log agents run on the Windows nodes of vRealize Automation.

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

Procedure

1 Log in to the vRealize Log Insight user interface of the master node.

   a Open a Web browser and go the load balancer of the cluster that you are updating.

Region	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 Click the **Download Log Insight Agent Version** link

5 In the **Download Log Insight Agent Version 4.5.0** dialog box, download the following agent files on the Windows host that you use to access the data center.

Region	Download Location	Agent Version	Save As
Region A	https://sfo01vrli01.sfo01.rainpole.local	Windows MSI (32-bit/64-bit)	`VMware-Log-Insight-Agent-4.5.0-`*`build_number_Region_A_vRealize_Log_Insight_VIP_address`*`.msi`
Region B	https://lax01vrli01.lax01.rainpole.local	Windows MSI (32-bit/64-bit)	`VMware-Log-Insight-Agent-4.5.0-`*`build_number_Region_B_vRealize_Log_Insight_VIP_address`*`.msi`

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

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

SDDC Layer	Role	Host Name
Cloud Management	IaaS Web Server	vra01iws01a.rainpole.local
		vra01iws01b.rainpole.local
	IaaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local
		vra01ims01b.rainpole.local
	IaaS DEM Worker	vra01dem01a.rainpole.local
		vra01dem01b.rainpole.local
	vSphere Proxy Agent	sfo01ias01a.sfo01.rainpole.local
		sfo01ias01b.sfo01.rainpole.local
	Microsoft SQL Server	vra01mssql01.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-4.5.0-`*`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 the following command to install the vRealize Log Insight agent with custom values.

```
VMware-Log-Insight-Agent-4.5.0-5626690_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 other vRealize Automation virtual machines.

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

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

SDDC Layer	Role	Host Name
Cloud Management	vSphere Proxy Agent	lax01ias01a.lax01.rainpole.local
		lax01ias01b.lax01.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-4.5.0-`*`build_number_Region_B_vRealize_Log_Insight_VIP_address`*`.msi` file from the Windows host to the vRealize Automation virtual machines in Region B.

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-4.5.0-5626690_192.168.32.10.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 lax01vrli01.lax01.rainpole.local shown in the **Host** text box, click **Install**.

h When the installation is complete, click **Finish**.

i Repeat the steps on the other vRealize Automation virtual machines.

8 After you upgrade the vRealize Log Insight agents for both Region A and Region B, verify that the agent version in the vRealize Log Insight cluster is `4.5.0.xxxxxxx`.

a Open a Web browser and go the load balancer of the cluster that you are updating.

Region	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*

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 `4.5.0.xxxxxxx`.

Delete the Snapshots of the vRealize Log Insight Appliances

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

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,

3 In the **Navigator**, click **VMs and Templates** and 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 update and select **Delete**.

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

7 Repeat the procedure on the other virtual machines of vRealize Log Insight in Region A.

8 Repeat the procedure on the virtual machines of vRealize Log Insight in Region B under the lax01m01vc01.lax01.rainpole.local vCenter Server.

Post-Upgrade Configuration of the vRealize Log Insight

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

Procedure

1 Enable the vRealize Log Insight Integration with vRealize Operations Manager for Region B

After the upgrade, configure vRealize Log Insight in Region B with vRealize Operations Manager to send alerts to vRealize Operations Manager from the nodes in Region B.

2 Connect vRealize Operations Manager to vRealize Log Insight

Configure a vRealize Log Insight Adapter to integrate vRealize Log Insight with vRealize Operations Manager in your environment. You can access unstructured log data about any object in your environment by using Launch in Context in vRealize Operations Manager .

3 Update the Host Profiles for the Management and Shared Edge and Compute Clusters in Region A and Region B with Syslog Settings

To have a consistent logging configuration across all ESXi hosts in the clusters in Region A, update the host profile in each cluster to accommodate the syslog settings for connection to vRealize Log Insight.

4 Configure the NSX Edge Instances to Forward Log Events to vRealize Log Insight in Region A and Region B

Redirect log information from the edge services gateways, universal distributed logical router and load balancer in to the vRealize Log Insight cluster in the region. Extend the set of monitored NSX devices from the earlier version of this validated design to the full set of the NSX devices in the environment.

5 Reconfigure the NSX Controllers to Forward Events to vRealize Log Insight in Region A and Region B

Reconfigure the NSX Controller instances for the management cluster and shared compute and edge cluster to forward log information to vRealize Log Insight in Region A and Region B under their IP addresses by using the NSX REST API. To enable log forwarding, you can use a REST client, such as the Postman application for Google Chrome.

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

vRealize Log Insight Agent comes pre-installed on the vRealize Business virtual appliances. Configure the `liagent.ini` configuration file on each virtual appliance.

7 Update vRealize Log Insight Linux Agent Configuration on the vRealize Automation Virtual Appliances in Region A

vRealize Log Insight Agent comes pre-installed on the vRealize Automation virtual appliance. Configure the `liagent.ini` configuration file on each virtual appliance.

8 Install the Linux Content Pack and Configure the Virtual Appliance Agent Group for vRealize Log Insight for Region A and Region B

Install the content pack for VMware Linux to add the dashboards for viewing log information about the management virtual appliances in vRealize Log Insight for both Region A and Region B.

9 Reconfigure Event Forwarding Between Region A and Region B

According to vRealize Log Insight Design, vRealize Log Insight is not failed over to the recovery region. Update the existing log forwarding between regions to use the Site tag.

Enable the vRealize Log Insight Integration with vRealize Operations Manager for Region B

After the upgrade, configure vRealize Log Insight in Region B with vRealize Operations Manager to send alerts to vRealize Operations Manager from the nodes 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 **Administration**.

3 Under **Integration**, click **vRealize Operations**.

4 On the **vRealize Operations Manager** page, configure the integration settings for vRealize Operations Manager.

Setting	Value
Hostname	vrops01svr01.rainpole.local
Username	svc-vrli-vrops@rainpole.local
Password	*svc-vrli-vrops_password*
Enable alerts integration	Selected
Enable launch in context	Deselected

5 Click **Test Connection** to validation the connection and click **Save**.

A progress dialog box appears.

6 Click **OK** to close the dialog.

Connect vRealize Operations Manager to vRealize Log Insight

Configure a vRealize Log Insight Adapter to integrate vRealize Log Insight with vRealize Operations Manager in your environment. You can access unstructured log data about any object in your environment by using Launch in Context in 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 On the main navigation bar, click **Administration**.

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

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

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

5 In the **Instance Settings** pane, enter the following settings.

Setting	vRealize Log Insight in Region A	vRealize Log Insight in Region B
Display Name	Log Insight Adapter - sfo01vrli01	Log Insight Adapter - lax01vrli01
Description	vRealize Log Insight for sfo01	vRealize Log Insight for lax01
Log Insight server	sfo01vrli01.sfo01.rainpole.local	lax01vrli01.lax01.rainpole.local

6 Validate the connection to vRealize Log Insight.

   a Click **Test Connection** to validate the connection to vRealize Log Insight.

   b Click **OK** in the **Info** dialog box.

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

Setting	Region A	Region B
Collectors/Groups	sfo01-remote-collectors	lax01-remote-collectors

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

9 Repeate the procedure to create an adapter for the vRealize Log Insight in Region B.

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

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

Update the Host Profiles for the Management and Shared Edge and Compute Clusters in Region A and Region B with Syslog Settings

To have a consistent logging configuration across all ESXi hosts in the clusters in Region A, update the host profile in each cluster to accommodate the syslog settings for connection to vRealize Log Insight.

Setting	Value for the Management Cluster	Value for the Shared Edge and Computer Cluster in Region A	Value for the Management Cluster in Region B	Value for the Shared Edge and Computer Cluster in Region B
vCenter Server URL	https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client/	https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client/	https://lax01m01vc01.lax01.rainpole.local/vsphere-client/	https://lax01w01vc01.lax01.rainpole.local/vsphere-client/
Host Profiles	sfo01-m01hp-mgmt01	sfo01-w01hp-comp01	lax01-m01hp-mgmt01	lax01-w01hp-comp01
First ESXi host	sfo01m01esx01.sfo01.rainpole.local	sfo01w01esx01.sfo01.rainpole.local	lax01m01esx01.lax01.rainpole.local	lax01w01esx01.lax01.rainpole.local
Syslog.global.logHost	udp://sfo01vrli01.sfo01.rainpole.local:514	udp://sfo01vrli01.sfo01.rainpole.local:514	udp://lax01vrli01.lax01.rainpole.local:514	udp://lax01vrli01.lax01.rainpole.local:514

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 Update the host profile for the management cluster.

   a From the **Home** menu of the vSphere Web Client, select **Policies and Profiles**.

   b In the **Navigator**, click **Host Profiles**, right-click the **sfo01-m01hp-mgmt01** host profile, and select **Copy Settings from Host**.

   c Select **sfo01m01esx01.sfo01.rainpole.local**, click **OK**.

3 Verify that the syslog host settings have been updated.

   a On the **Host Profiles** page in the **Navigator**, click **sfo01-m01hp-mgmt01** .

   b On the **Configure** tab, click **Settings**.

   c In **Filter** search box, type **Syslog.global.logHost**.

   d Select the **Syslog.global.logHost** entry from the list and verify that the value of the property.

Setting	Region A	Region B
Syslog.global.logHost	udp://sfo01vrli01.sfo01.rainpole.local:514	udp://lax01vrli01.lax01.rainpole.local:514

4 Verify compliance for the hosts in the management cluster.

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

   b Click the **sfo01-m01-mgmt01** cluster, click the **Monitor** tab, and click **Profile Compliance**.

   c Click the **Check Compliance Now button**.

   d Verify all hosts are compliant with the attached profile.

5 Repeat the procedure with a host in the shared edge and compute cluster in Region A.

6 Repeat the procedure with a host for the clusters in Region B.

Configure the NSX Edge Instances to Forward Log Events to vRealize Log Insight in Region A and Region B

Redirect log information from the edge services gateways, universal distributed logical router and load balancer in to the vRealize Log Insight cluster in the region. Extend the set of monitored NSX devices from the earlier version of this validated design to the full set of the NSX devices in the environment.

Procedure

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

   a Open a Web browser and go to **`https://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 On the **NSX Edges** page, from the **NSX Manager** drop-down menu select the IP address of the NSX Manager instance that handles the network device.

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

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

5 Double-click the edge device to open its user interface.

Traffic	Management NSX Edge Services Gateway		Compute NSX Edge Services Gateway	
Region	Region A	Region B	Region A	Region B
East-West Routing	sfo01m01udlr01	-	sfo01w01udlr01	-
East-West Routing	-	-	sfo01w01dlr01	lax01w01dlr01
Load Balancer for the Platform Services Controller pair	sfo01psc01	lax01psc01	-	-

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

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

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

Setting	Region A	Region B
Syslog Server 1	192.168.31.10	192.168.32.10
Protocol	udp	udp

9 Repeat the steps for the remaining NSX Edge devices connected to the NSX Manager instances.

10 Verify that all Edge Services Gateways in both Region A and Region B are forwarding logs to the vRealize Log Insight clusters in the regions.

a Open a Web browser and go the master node for the cluster that you are updating.

Region	URL
Region A	https://sfo01vrli01a.sfo01.rainpole.local
Region B	https://lax01vrli01a.lax01.rainpole.local

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

c On the main navigation bar, click **Dashboards** and in the **VMware - NSX-vSphere** dashboards verify that all NSX Edge devices in both Region A and Region B are forwarding logs to the respective vRealize Log Insight clusters.

Traffic	Management NSX Edge Services Gateway		Compute NSX Edge Services Gateway	
Region	Region A	Region B	Region A	Region B
North-South Routing	sfo01m01esg01	lax01m01esg01	sfo01w01esg01	lax01m01esg01
North-South Routing	sfo01m01esg02	lax01m01esg01	sfo01w01esg01	lax01m01esg01
East-West Routing	sfo01m01udlr01	-	sfo01w01udlr01	-
East-West Routing	-	-	sfo01w01dlr01	lax01w01dlr01
Load Balancer	sfo01m01lb01	lax01m01lb01	-	-
PSC Load Balancer	sfo01psc01	lax01psc01	-	-

Reconfigure the NSX Controllers to Forward Events to vRealize Log Insight in Region A and Region B

Reconfigure the NSX Controller instances for the management cluster and shared compute and edge cluster to forward log information to vRealize Log Insight in Region A and Region B under their IP addresses by using the NSX REST API. To enable log forwarding, you can use a REST client, such as the Postman application for Google Chrome.

Procedure

1. Log in to the Windows host that has access to your data center.
2. In a Chrome browser, start the Postman application and log in.
3. Specify the request headers for requests to the NSX Manager.
   a. On the **Authorization** tab, configure the following authorization settings and click **Update Request**.

Setting	Value
Type	Basic Auth
User name	admin
Password	*sfo01m01nsx01_admin_password* *sfo01w01nsx01_admin_password* *lax01m01nsx01_admin_password* *lax01w01nsx01_admin_password*

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

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

Request Header Attribute	Value
Content-Type	application/xml

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

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

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

b In the **URL** text box, enter the following URL, and click **Send**.

Region	NSX Manager	URL
Region A	NSX Manager for the management cluster	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller
	NSX Manager for the shared edge and compute cluster	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller
Region B	NSX Manager for the management cluster	https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller
	NSX Manager for the shared edge and compute cluster	https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/controller

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

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

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

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

Controller IDs have the `controller-`*`id`* format where id represents the sequence number of the controller in the cluster, for example, `controller-1`

e Repeat the steps for the other NSX Manager

5 For each NSX Controller, send a request to retrieve the current remote syslog configuration.

a In the request pane at the top, select **GET** from the drop-down menu that contains the HTTP request methods, and in the **URL** text box, enter the following URL. Replace *controller-ID* with the controller IDs you have written down.

Region	NSX Manager	NSX Controller in the Controller Cluster	GET URL
Region A	NSX Manager for the management cluster	NSX Controller 1	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-1**/syslog
		NSX Controller 2	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-2**/syslog
		NSX Controller 3	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-3**/syslog
Region B		NSX Controller 4	https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/**controller-4**/syslog
		NSX Controller 5	https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/**controller-5**/syslog
		NSX Controller 6	https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/**controller-6**/syslog
Region A	NSX Manager for the shared edge and compute cluster	NSX Controller 1	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-1**/syslog
		NSX Controller 2	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-2**/syslog
		NSX Controller 3	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-3**/syslog
Region B		NSX Controller 4	https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/**controller-4**/syslog
		NSX Controller 5	https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/**controller-5**/syslog
		NSX Controller 6	https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/**controller-6**/syslog

b Confirm that the controllers are sending to the fully qualified domain name of the vRealize Log Insight cluster in Region A and Region B.

c In the **Request** pane, from the **Method** drop-down menu, select **DELETE**, in the **URL** text box, enter the controller-specific syslog URL from Step 4, and click the**SEND** button.

d Repeat the steps for the other NSX Controllers in the management cluster and in the shared edge and compute cluster for both Region A and Region B.

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

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

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

NSX Manager	NSX Controller in the Controller Cluster	Region	GET URL
NSX Manager for the management cluster	NSX Controller 1	Region A	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-1**/syslog
	NSX Controller 2	Region A	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-2**/syslog
	NSX Controller 3	Region A	https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-3**/syslog
	NSX Controller 4	Region B	https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/**controller-4**/syslog
	NSX Controller 5	Region B	https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/**controller-5**/syslog
	NSX Controller 6	Region B	https://lax01m01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/**controller-6**/syslog
NSX Manager for the shared edge and compute cluster	NSX Controller 1	Region A	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-1**/syslog
	NSX Controller 2	Region A	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-2**/syslog
	NSX Controller 3	Region A	https://sfo01w01nsx01.sfo01.rainpole.local/api/2.0/vdn/controller/**controller-3**/syslog
	NSX Controller 4	Region B	https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/**controller-4**/syslog
	NSX Controller 5	Region B	https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/**controller-5**/syslog
	NSX Controller 6	Region B	https://lax01w01nsx01.lax01.rainpole.local/api/2.0/vdn/controller/**controller-6**/syslog

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

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

Setting	Value for Region A	Value for Region B
NSX Controller Syslog Server Settings	<controllerSyslogServer> <syslogServer>192.168.31.10</syslogServer> <port>514</port> <protocol>UDP</protocol> <level>INFO</level> </controllerSyslogServer>	<controllerSyslogServer> <syslogServer>192.168.32.10</syslogServer> <port>514</port> <protocol>UDP</protocol> <level>INFO</level> </controllerSyslogServer>

d Repeat the steps for the other NSX Controllers in the management cluster and in the shared edge and compute cluster.

7 Verify the syslog configuration on each NSX Controller.

a In the **Request** pane, from the **Method** drop-down menu, select **GET**, in the **URL** text box, enter the controller-specific syslog URL from Step 4, and click the**SEND** button.

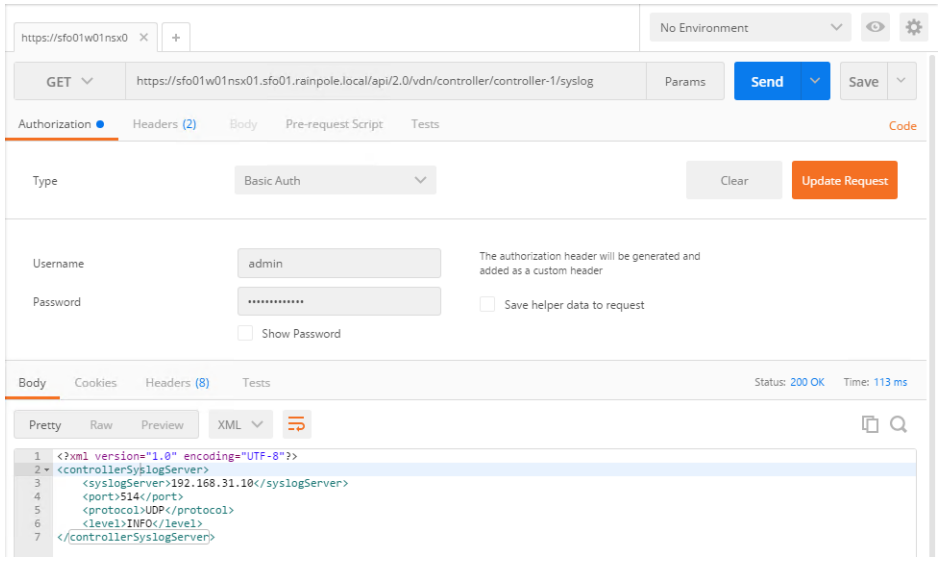
b After the NSX Manager sends a response back, click the **Body** tab under **Response**.

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

c Verify that the value of the <syslogServer> element have been configured properly per region.

Setting	Value for Region A	Value for Region B
NSX Controller Syslog Server Settings	192.168.31.10	192.168.32.10

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



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

vRealize Log Insight Agent comes pre-installed on the vRealize Business virtual appliances. Configure the `liagent.ini` configuration file on each virtual appliance.

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 in Region A	https://sfo01vrbc01.sfo01.rainpole.local:5480
vRealzie Business Data Collector in Region A	https://lax01vrbc01.lax01.rainpole.local:5480

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_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** is `Enabled`.

f Repeat the step for the other vRealize Business appliance.

2 Configure the vRealize Log Insight agent in on the vRealize Business appliances.

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

Setting	Value
Host name	■ vrb01svr01.rainpole.local ■ sfo01vrbc01.sfo01.rainpole.local ■ lax01vrbc01.lax01.rainpole.local
User name	root
Password	*vrb_server_appliance_root_password*

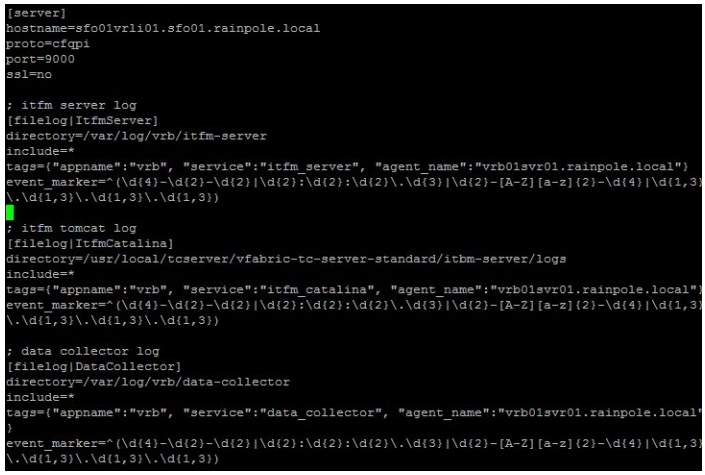
b Edit the `liagent.ini` file using a text editor such as `vi`.

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

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

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

d Replace all instances of the *FQDN_localhost* parameter in the `agent_name` property with **`vrb01svr01.rainpole.local`**.



e Press Esc 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 auto-run by default for the Log Insight agent.

```
chkconfig liagentd on
```

i Repeat the steps to configure the `liagent.ini` on the vRealize Business Data Collectors using the following values:

Setting	Value for sfo01vrbc01.sfo01.rainpole.local	Value for lax01vrbc01.lax01.rainpole.local
`Hostname`	sfo01vrli01.sfo01.rainpole.local	lax01vrli01.lax01.rainpole.local
`FQDN_localhost`	sfo01vrbc01.sfo01.rainpole.local	lax01vrbc01.lax01.rainpole.local

3 Confirm that the Log Insight agents are working in the vRealize Log Insight Web interface for Region A.

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 Verify that vrb01svr01.rainpole.local and sfo01vrbc01.sfo01.rainpole.local appear on the page.

4 Repeat the step to verify that the Log Insight agent is working in the vRealize Log Insight Web interface for Region B .

Setting	Value
vRealize Log Insight URL	https://lax01vrli01.lax01.rainpole.local
Component where the agent is running	lax01vrbc01.lax01.rainpole.local

Update vRealize Log Insight Linux Agent Configuration on the vRealize Automation Virtual Appliances in Region A

vRealize Log Insight Agent comes pre-installed on the vRealize Automation virtual appliance. Configure the `liagent.ini` configuration file on each virtual appliance.

Procedure

1 Open a Web browser and log in to the following URL.

Setting	Value for vRealize Appliance A	Value for vRealize Appliance B
URL	https://vra01svr01a.rainpole.local:5480	https://vra01svr01b.rainpole.local:5480
User name	root	root
Password	*vra_applianceA_root_password*	*vra_applianceB_root_password*

2 On the **VRA Settings** tab, click the **Logs** tab.

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

4 Verify the following values remain unchanged post-upgrade in the **Server and Protocol** section.

Setting	Value
Host	sfo01vrli01.sfo01.rainpole.local
Port	9000

Setting	Value
Protocol	CFAPI
SSL Enabled	Unchecked

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

6 Enter the following values and click **Save Settings**.

Setting	Value
Reconnect	30
Max Buffer Size	2000

7 Verify that these settings have been replicated to secondary vRealize Automation appliance vra01svr01b.rainpole.local

Install the Linux Content Pack and Configure the Virtual Appliance Agent Group for vRealize Log Insight for Region A and Region B

Install the content pack for VMware Linux to add the dashboards for viewing log information about the management virtual appliances in vRealize Log Insight for both Region A and Region B.

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 Install the content pack for VMware Linux.

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

b Under **Content Pack Marketplace**, select **Marketplace**.

c In the list of content packs, locate the **Linux** content pack and click its icon.

d In the **Install Content Pack** dialog box, accept the License Agreement and click **Install**.

After the installation is complete, the **Linux** content pack appears in the **Installed Content Packs** list on the left.

3 Configure the Log Insight Linux agent group for the virtual appliances from the vRealize Log Insight user interface.

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

b Under **Management**, click **Agents**.

c From the drop-down at the top, select **Linux** from the **Available Templates** section.

d Click **Copy Template**.

e In the **Copy Agent Group** dialog box, enter **`vAppliances - Agent Group`** in the **Name** text box and click **Copy**.

f In the agent filter fields, use the following selections.

Press ENTER to separate the host name values.

Filter	Operator	Values for Region A	Values for Region B
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 ■ vrb01svr01.rainpole.local ■ sfo01vrbc01.sfo01.rainpole.local	■ lax01vropsc01a.lax01.rainpole.local ■ lax01vropsc01b.lax01.rainpole.local ■ lax01vrbc01.lax01.rainpole.local

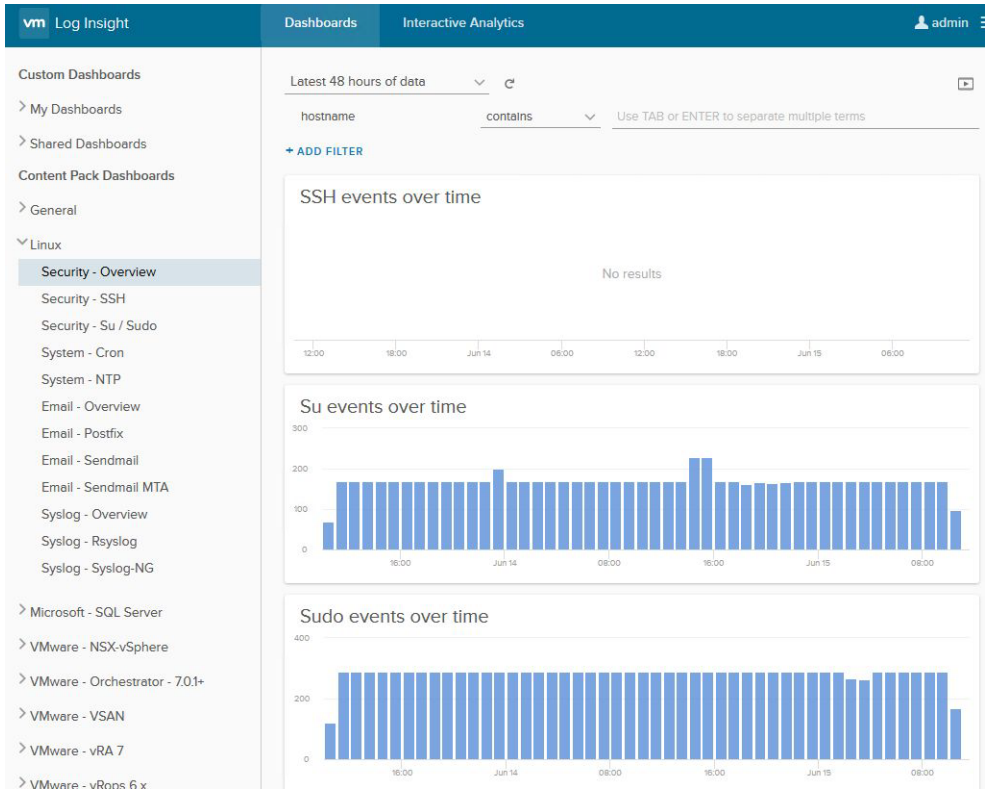
g Click **Refresh** and verify that all the agents listed in the filter appear in the **Agents** list.

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

4 Verify that log data is showing up on the Linux dashboards for both Region A and Region B.

a On the main navigation bar, click **Dashboards**.

b Expand **Linux** and click **Security - Overview**.



Reconfigure Event Forwarding Between Region A and Region B

According to vRealize Log Insight Design, vRealize Log Insight is not failed over to the recovery region. Update the existing log forwarding between regions to use the Site tag.

See *vRealize Log Insight Design* and *Logging Architecture* in the *VMware Validated Design Architecture and Design* documentation.

Reconfigure Event Forwarding in Region A

Update the tag used for the log forwarding from vRealize Log Insight in Region A to vRealize Log Insight in Region B to keep aligned to this version of this VMware Validated Design. This version uses a tag called `site` for alignment when extending the environment with a ROBO SDDC.

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 **Administration**.

3 Under **Management**, click **Event Forwarding**.

4 On the **Event Forwarding** page, click **SFO01 to LAX01** and update the following forwarding settings in the **Edit Destination** dialog box.

   Replace the tag that labels the logs in Region A from `tag` to `site`.

Forwarding Destination Setting	Value
Tags	**`site='SFO01'`**
Filter	
Filter Type	tag
Operator	does not match
Value	'LAX01'

5 In the **Edit Destination** dialog box, click **Test** to verify that the connection settings remain correct.

6 Click **Save** to update the forwarding destination.

The **Event Forwarding** page in the vRealize Log Insight user interface starts showing a summary of the forwarded events.

Reconfigure Event Forwarding in Region B

Update the tag used for the log forwarding from vRealize Log Insight in Region B to vRealize Log Insight in Region A to keep aligned to the VMware Validated Design.

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 **Administration**.

3 Under **Management**, click **Event Forwarding**.

4 On the **Event Forwarding** page, click **LAX01 to SFO01** and edit the following forwarding settings in the **Edit Destination** dialog box.

   a Update the **Tags** from `tag`='LAX01' to **`site`**='LAX01'.

   b Click **Remove Filter** to remove deprecated **Filter** for `Tag Does Not Match 'SFO01'`.

   c Click **Add Filter** for `Site Does Not Match 'SFO01'`.

Forwarding Destination Option	Value
Tags	site='LAX01'
Filter	
Filter Type	site
Operator	does not match
Value	'SFO01'

5 In the **Edit Destination** dialog box, click **Test** to verify that the connection settings remain correct.

6 Click **Save** to update the forwarding destination.

The **Event Forwarding** page in the vRealize Log Insight user interface starts showing a summary of the forwarded events.

Update Log Filters in Region A

After you configure log forwarding in Region B to tag log events based on the site, update the filter used in Region A to avoid forwarding log events already forwarded to Region A back to their source Log Insight deployment in Region B.

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 **Administration**.

3 Under **Management**, click **Event Forwarding**.

4 On the **Event Forwarding** page, click **SFO01 to LAX01** and edit the following forwarding settings in the **Edit Destination** dialog box.

   a Click **Remove Filter** to remove deprecated **Filter** for `tag Does Not Match 'LAX01'`.

   b Click **Add Filter** for `site Does Not Match 'LAX01'`.

Forward Destination Setting	Value
Filter Type	site
Operator	does not match
Value	'LAX01'

5 In the **Edit Destination** dialog box, click **Test** to verify that the connection settings remain correct.

6 Click **Save**.

The **Event Forwarding** page in the vRealize Log Insight user interface shows a summary of the forwarded events.

Upgrade Virtual Infrastructure

4

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

Procedure

1 Update vSphere Data Protection

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

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

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

3 Upgrade the Components for the Management Cluster

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

4 Upgrade the Components for the Shared Edge and Compute Cluster

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

5 Global Post-Upgrade Configuration of the Virtual Infrastructure Components

After you upgrade all virtual infrastructure components, perform global post-upgrade configuration according to address the dependencies between these components and to align your environment to the guidance in this validated design.

Table 4-1. VMware Validated Design Upgrade Sequence for the Virtual Infrastructure and Business Continuity Layers

Order	Component	Sub-Component
1	vSphere Data Protection	-
2	Post-Upgrade Reconfiguration for Business Continuity (Backup and Restore)	-
3	NSX for vSphere	NSX Managers

Table 4-1. VMware Validated Design Upgrade Sequence for the Virtual Infrastructure and Business Continuity Layers (Continued)

Order	Component	Sub-Component
		NSX Controllers
		NSX Networking Fabric
		NSX Edges
4	Post-Upgrade Reconfiguration for Virtual Infrastructure (Networking)	-
5	Platform Services Controllers	-
	vCenter Server	-
	vSphere Replication	-
	Site Recovery Manager	-
6	Post-Upgrade Reconfiguration ■ Business Continuity (Disaster Recovery) ■ Virtual Infrastructure (Compute Infrastructure)	-
7	vSphere Update Manager Download Service	-
8	ESXi	-
9	Post-Upgrade Reconfiguration for Virtual Infrastructure (Compute Infrastructure)	-
10	vSAN	-
11	Post-Upgrade Reconfiguration for Virtual Infrastructure (Storage)	-

Update vSphere Data Protection

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

Perform the upgrade outside of the backup windows.

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

Table 4-2. vSphere Data Protection Nodes in the SDDC

Region	Role	IP Address	Fully Qualified Domain Name
Region A	Backup Node	172.16.11.81	sfo01m01vdp01.sfo01.rainpole.local
Region B	Backup Node	172.17.11.81	lax01m01vdp01.lax01.rainpole.local

Note VMware Validated Design 4.1 introduces a new convention for host and object names in the SDDC. The step-by-step upgrade guidance uses the new names for both the pre- and post-upgrade SDDC setups. For information about the new convention, see Mapping Component Names Between Versions 4.0 and 4.1 of VMware Validated Design.

Prerequisites

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

- Download the vSphere Data Protection upgrade `vSphereDataProtection-6.1.x.iso` file to a shared datastore for mounting to the virtual appliances.

  If you have space on your NFS datastore, upload the file there.
- Verify that approximately 2 GB are free on Hard Disk 1.

  Use the `mccli server show-prop` command on each appliance over SSH.
- Verify that the maintenance window is in a time period in which no backup jobs are running or scheduled to run.
- Verify that no alarms on the vSphere Data Protection virtual appliances exist in both the vSphere Web Client and the vSphere Data Protection configuration interface.

Procedure

1 Take Snapshots of the vSphere Data Protection Appliances

  Before you start the upgrade, take a snapshot of each vSphere Data Protection node so that you can roll the update back if a failure occurs.

2 Update the vSphere Data Protection Appliances

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

3 Delete the Snapshots of the vSphere Data Protection Appliances

  After you complete the upgrade of vSphere Data Protection, clear the snapshots you created as a way to roll the upgrade back.

4 Post-Upgrade Configuration of vSphere Data Protection

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

What to do next

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

Take Snapshots of the vSphere Data Protection Appliances

Before you start the upgrade, take a snapshot of each vSphere Data Protection node so that you can roll the update back if a failure occurs.

Table 4-3. vSphere Data Protection Appliances in the SDDC

Region	Folder	Virtual Machine Name
Region A	sfo01-m01fd-bcdr	sfo01m01vdp01
Region B	lax01-m01fd-bcdr	lax01m01vdp01

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 **VMs and Templates**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-bcdr** tree.

3 Right-click the **sfo01m01vdp01** virtual machine and select **Power > Shut Down Guest OS** and click **Yes** in the confirmation dialog box that appears.

4 After the appliance is powered off, change the disk mode of the vSphere Data Protection appliance.

   a Right-click **sfo01m01vdp01** and select **Edit Settings**.

   b On the **Virtual Hardware** tab, expand Hard disk 2, select **Dependent** from the **Disk Mode** drop-down menu.

   c Click **Manage other disks** and repeat the step to change the disk mode on Hard Disk 3 to Hard disk 7 and click **OK**.

5 Take a snapshot of each node in the cluster.

a Right-click the **sfo01m01vdp01** virtual machine and select **Snapshots > Take Snapshot**.

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

Setting	Value
Name	VMware Validated Design 4.1 BCDR Upgrade
Snapshot the virtual machine's memory	Deselected
Quiesce guest file system (Needs VMware Tools installed)	Deselected

6 After the snapshot is taken, right-click the **sfo01m01vdp01** virtual machine and select **Power > Power On**.

7 Repeat the procedure on lax01m01vdp01 under the lax01m01vc01.lax01.rainpole.local vCenter Server in Region B.

Update the vSphere Data Protection Appliances

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

Procedure

1 Log in to the vSphere Data Protection configuration interface.

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

Region	URL
Region A	https://sfo01m01vdp01.sfo01.rainpole.local:8543/vdp-configure/
Region B	https://lax01m01vdp01.lax01.rainpole.local:8543/vdp-configure/

b Log in use the following credentials.

Setting	Value
User Name	root
Password	*vdp_root_password*

2 Mount the upgrade `vSphereDataProtection-6.1.x.iso` file to the vSphere Data Protection appliance.

3 On the **Configuration** tab, verify that all the services are running.

If any of the services are not running, the upgrade might fail.

4 Click the **Upgrade** tab.

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

5 Select the upgrade you want to install and click **Upgrade VDP**.

6 Repeat the procedure for the other vSphere Data Protection appliance.

What to do next

Once your vSphere Data Protection node has been upgraded to the latest version, if you leverage a vSphere Data Protection external proxy agent within your VMware Validated Design environment, you will need to upgrade the proxy to the latest version. Consult the *Upgrading Proxy Software* in the VMware vSphere Data Protection Administration Guide for guidance on performing this operation.

Delete the Snapshots of the vSphere Data Protection Appliances

After you complete the upgrade of vSphere Data Protection, clear the snapshots you created as a way to roll the upgrade back.

Table 4-4. vSphere Data Protection Appliances in the SDDC

Region	Folder	Virtual Machine Name
Region A	sfo01-m01fd-bcdr	sfo01m01vdp01
Region B	lax01-m01fd-bcdr	lax01m01vdp01

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 **VMs and Templates**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-bcdr** tree.

3 Right-click the **sfo01m01vdp01** virtual machine, select **Power > Shut Down Guest OS**, and click **Yes** in the confirmation dialog box that appears.

4 After the appliance is powered off, right-click the **sfo01m01vdp01** virtual machine and select **Snapshots > Manage Snapshots**.

5 On the **Snapshots** tab, click the snapshot that you created before the vSphere Data Protection upgrade in Region A and click **Delete a VM Snapshot**.

6 Change the disk mode of the vSphere Data Protection appliance.

   a Right-click **sfo01m01vdp01** and select **Edit Settings**.

   b On the **Virtual Hardware** tab, expand Hard disk 2, select **Independent - Persistent** from the **Disk Mode** drop-down menu.

   c Click **Manage other disks** and repeat the step to change the disk mode on Hard Disk 3 to Hard disk 7 and click **OK**.

7 After the snapshot has been consolidated, right-click the **sfo01m01vdp01** virtual machine and select **Power > Power On**.

8 Repeat the procedure on the lax01m01vdp01 virtual machine under the lax01m01vc01.lax01.rainpole.local vCenter Server in Region B.

Post-Upgrade Configuration of vSphere Data Protection

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

Create vSphere Update Manager Download Service Backup Jobs in Region A and Region B.

Include the vSphere Update Manager Download Service in a new backup routine in vSphere Data Protection for Region A and Region B.

Procedure

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

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

   b Log in using the following credentials.

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

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

3 On the **Welcome to vSphere Data Protection** page, select one of the vSphere Data Protection nodes from the **VDP Appliance** drop-down menu and click **Connect**.

Region	Node Name
Region A	sfo01m01vdp01
Region B	lax01m01vdp01

4 Click the **Backup** tab.

5 From the **Backup job actions** menu, select **New** to open the **Create a new backup job** wizard.

6 On the **Job Type** page, select **Guest Images**, and click **Next**.

7 On the **Data Type** page, select **Full Image**, leave the **Fall back to the non-quiesced backup if quiescence fails** check box selected, and click **Next**.

8 On the **Backup Sources** page, fully expand the Virtual Machines tree.

Object	Values in Region A	Values in Region B
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
Data center	sfo01-m01dc	lax01-m01dc
Cluster	sfo01-m01-mgmt01	lax01-m01-mgmt01

9 Locate the below virtual machines for the vRealize Orchestrator components, and de-select them from the job.

vSphere Components	VM Name in Region A	VM Name in Region B
vSphere Update Manager Download Service	sfo01umds01	lax01umds01

10 On the **Schedule** page, set **Backup Schedule to Daily** and click **Next**.

11 On the **Retention Policy** page, set **Keepfor** `3 days` and click **Next**.

12 On the **Job Name** page, enter `vSphere Update Manager Download Service Backups` as a name for the backup job and click **Next**.

13 On the **Ready to Complete** page, verify the following, then click **Finish**.

14 In the dialog box that shows a confirmation that the job is created, click **OK**.

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

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

Upgrading NSX for vSphere is a multi-step operation where you must upgrade the NSX Managers paired instances for Cross-vCenter Networking and Security, the NSX Controller nodes, the ESXi VIBs, and the NSX Edge devices. This upgrade operation is split between the management cluster pairs and the shared edge and compute cluster pairs.

You might perform the upgrades of these components in different maintenance windows.

Table 4-5. NSX Nodes 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	-
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 VMware Validated Design 4.1 introduces a new convention for host and object names in the SDDC. The step-by-step upgrade guidance uses the new names for both the pre- and post-upgrade SDDC setups. For information about the new convention, see Mapping Component Names Between Versions 4.0 and 4.1 of VMware Validated Design.

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

Prerequisites

- Download the NSX update bundle `VMware-NSX-Manager-upgrade-bundle-6.3.x-xxxxxxx.tar.gz` on the Windows host that has access to your data center.
- Review Operational Impacts of NSX Upgrade from *NSX Upgrade Guide* to understand the impact that each component might have on your VMware Validated Design environment.

- Verify that any virtual networking integration within the environment has been quiesced of all activities, including but not limited to: users ordering new virtual machines backed by virtual wires over the Cloud Management Platform (CMP); third-party integration that automates the ordering or deployment of new virtual machines that are backed by virtual wires; and administrators manually creating new NSX-based components.

  Without quiescing the environment, rollback operations might be disrupted by generated orphaned objects. You might also have to extend the time of the maintenance windows.
- Validate the NSX Manager file system usage, and perform a cleanup if file system usage is at 100 percent.
  a Open an SSH connection using the `admin` account to the NSX Manager instance you are upgrading and run the `show filesystems` command to show the filesystem usage.
  b If the filesystem usage is at 100 percent, enter Privileged mode and purge the logs by running the following commands.

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

  c Reboot the NSX Manager appliance for the log cleanup to take effect.
- Back up the NSX configuration and download technical support logs before upgrading. See *Backing Up and Restoring the NSX Instances in Region A* and *Backing Up and Restoring the NSX Instances in Region B* from the *VMware Validated Design Backup and Restore* documentation.
- Take a backup of the NSX Manager pair, both the primary and secondary, and of NSX Controller virtual machines. For more information, see Back Up and Restore NSX Manager from *NSX Upgrade Guide*.
- Verify that all of the controllers are in normal, connected state.
- Get the current version of the NSX VIBs on the hosts in the management cluster and in the shared edge and compute cluster.
  a Log in to one of the hosts in the cluster via the ESXi Host Client, and using the Packages section, search for **esx-v**.
  b Note the current version of the following VIBs.
    - esx-vsip
    - esx-vxlan

Procedure

1 Upgrade the NSX Manager Instances

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

2 Upgrade the NSX Controllers

After you upgrade the NSX Manager instances in Region A and Region B, upgrade the NSX Controller instances for the management cluster and for the shared edge and compute cluster.

3 Upgrade the NSX Components on the ESXi Hosts

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

4 Upgrade NSX Edge Instances

After you upgrade the control and data plane of the NSX core components, propagate the upgrade to the NSX Edge services gateways, universal distributed logical router and load balancer instances.

What to do next

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

Upgrade the NSX Manager Instances

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

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

Table 4-6. NSX Manager Details

Order	Region	NSX Manager Instance	NSX Appliance URL	vCenter Server URL
1	Region A	NSX Manager for the management cluster that is configured as primary	https://sfo01m01nsx01.sfo01.rainpole.local	sfo01m01vc01.sfo01.rainpole.local
2	Region B	NSX Manager for the management cluster that is as secondary	https://lax01m01nsx01.lax01.rainpole.local	lax01m01vc01.lax01.rainpole.local
3	Region A	NSX Manager for the shared edge and compute cluster that is as primary	https://sfo01w01nsx01.sfo01.rainpole.local	sfo01w01vc01.sfo01.rainpole.local
4	Region B	NSX Manager for the shared edge and compute cluster that is as secondary.	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, browse your file system to locate the `VMware-NSX-Manager-upgrade-bundle-6.3.`*`x-build_number`*`.tar.gz` upgrade bundle.

4 Once the file has been located, click **Open** and click **Continue**.

   The NSX Manager starts uploading the bundle.

5 After the upload is complete, in the **Upgrade** dialog box, select **Yes** next to **Do you want to enable SSH?** and **Do you want to join the VMware Customer Experience Program**, and click **Upgrade**.

6 After the upgrade is complete, if not already logged in, log in to the NSX Manager instance for the management cluster again and verify that the **Upgrade** tab shows the following configuration.

Setting	Expected Value
Upgrade State	Complete
Current Software Version	*the version and build in the upgrade bundle you installed*

   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 After you upgrade the NSX Manager, check for the latest NSX plug-in within 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 **Check for New Plug-ins**.

f In the pop-up window **Checking for New Plug-ins**, click **Go to the Event Console**.

g In the **Events Console**, using the filter, enter **`plug-in`**. You should observe two events that recently occurred:

```
The     deployment of plug-in NSX user interface plugin 6.3.3.xxxxxxx has started
The deployment of plug-in NSX user interface plugin 6.3.3.xxxxxxx is successful
```

h Once both events were observed, log out and back into the vSphere Web Client, navigate back to the **Client Plug-Ins** section, and verify that the **vShield Manager Version** has been updated properly.

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

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

9 Repeat the steps for the secondary NSX Manager lax01m01nsx01.lax01.rainpole.local to complete the NSX Manager upgrade in the management cluster.

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

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

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

You start with the primary NSX Manager sfo01w01nsx01.sfo01.rainpole.local and complete the upgrade with the secondary NSX Manager lax01w01nsx01.lax01.rainpole.local.

Upgrade the NSX Controllers

After you upgrade the NSX Manager instances in Region A and Region B, upgrade the NSX Controller instances for the management cluster and for the shared edge and compute cluster.

For each NSX Manager that has the primary role, you start an upgrade for the connected NSX Controller cluster. During the upgrade to NSX 6.3.3, the underlying operating system of the NSX Controller changes. Instead of previous versions of NSX where an in-place upgrade of the software occurs, the existing controllers are deleted one at a time, and new Photon OS based controllers are deployed using the same IP addresses and configuration state of the prior controller. The controllers are upgraded one at a time so that high availability remains persistent during the upgrade.

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

Table 4-7. NSX Controller Properties 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**.

4 Under **NSX Managers**, select the **172.16.11.65** NSX Manager instance and click **Upgrade Available** in the **Controller Cluster Status** column.

5 In the **Upgrade Controller** dialog, click **Yes**.

6 In the **Special Upgrade** dialog, click **Proceed**.

   The **Status** column starts with reporting `Removing`, at which point the Controller will be removed from the list, then changes to `Deploying`, at which point the Controller will be return to the list, and finally to `Connected` once again.

   The **Upgrade Status** column shows the following stages:

   a `Queued For Upgrade`

   b `Upgrade in progress` for each NSX controller

   c `Waiting to Rebooting`

   d `Rebooting`

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

Setting	Expected Value
Status	Connected
Software Version	6.3.*build_number*

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

Upgrade the NSX Components on the ESXi Hosts

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

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

Table 4-8. NSX Manager Instances and Associated Host Clusters

Region	NSX Manager	NSX Manager IP Address	Host Clusters
Region A	NSX Manager for the management cluster	172.16.11.65	**sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01-mgmt01**
	NSX Manager for the shared edge and compute cluster	172.16.11.66	**sfo01w01vc01.sfo01.rainpole.local > sfo01-w01dc > sfo01-w01-comp01**
Region B	NSX Manager for the management cluster	172.17.11.65	**lax01m01vc01.lax01.rainpole.local > lax01-m01dc > lax01-m01-mgmt01**
	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 on the host clusters, and is set to `Fully Automated`.
- Verify that vSphere vMotion functions correctly between all ESXi hosts within the cluster.
- Verify that all ESXi hosts are in a connected state with vCenter Server.
- Verify that no ESXi hosts are in maintenance mode within 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 click the **Host Preparation** tab.

4 From the **NSX Manager** drop-down menu, select the IP address **172.16.11.65 (Role: Primary)** of the NSX Manager for the management cluster in Region A.

5 If the **Installation Status** reports `Not Ready`, click on the **Actions** button and select **Resolve**.

   Allow for the ESXi hosts to re-synchronize with NSX. After synchronization is complete, all of the ESXi hosts should display a ready state, indicated by a green check mark, with a version of `6.3.1.`*`build_number`*.

6 Under **NSX Components Installation on Hosts**, click **Upgrade available** next to the **sfo01-m01-mgmt01** cluster.

7 In the **Upgrade** confirmation dialog box, click **Yes**.

8 After all ESXi hosts have **Installation Status** to `Not Ready`, click the **Actions** button and select **Resolve** once again.

   The **Installation Status** changes to `In Progress...` as each of the ESXi host is updated. Each host is placed into maintenance mode with the virtual machines on migrated from the host, and updated. During this time, you mught use the **Refresh** button to periodically refresh the session to see the dynamically changing installation status.

9 Allow for each ESXi host to be updated in the management cluster in Region A.

   After all hosts are updated completed, they are in a ready state, indicated by a green check mark, with a version of `6.3.3.`*`build_number`*.

10 Repeat the steps to update the NSX components on the other clusters in Region A and Region B.

Upgrade NSX Edge Instances

After you upgrade the control and data plane of the NSX core components, propagate the upgrade to the NSX Edge services gateways, universal distributed logical router and load balancer instances.

Prerequisites

All ESXi hosts in Region A and Region B have had their NSX VIBs updated to the appropriate version matching the NSX 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, select **Networking & Security**.

3 In the **Navigator** pane, under **Networking & Security**, click **NSX Edges**.

4 On the **NSX Edges** page, select the IP address of the NSX Manager instance from the **NSX Manager** drop-down menu.

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

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

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

   Perform the upgrade in the following order as to minimize disruption on both the management and shared and edge compute pods. Allow each NSX Edge instance to be updated before proceeding with update of the next NSX Edge instance.

Order	Management Edge in Region A	Management Edge in Region B	Compute Edge in Region A	Compute Edge in Region B
1	sfo01m01esg01	-	-	-
2	-	lax01m01esg01	-	-
3	sfo01m01esg02	-	-	-
4	-	lax01m01esg02	-	-
5	sfo01m01lb01	-	-	-
6	-	lax01m01lb01	-	-
7	sfo01psc01		-	-
8	-	lax01psc01	-	-
9	sfo01m01udlr01	-	-	-
10	-	-	sfo01w01esg01	-
11	-	-	-	lax01w01esg01
12	-	-	sfo01w01esg02	-
13	-	-	-	lax01w01esg02
14	-	-	sfo01w01dlr01	-
15	-	-	-	lax01w01dlr01
16	-	-	sfo01w01udlr01	-

6 After all the NSX edges are upgraded successfully, verify that the **Status** column for the edge device shows `Deployed`, and the **Version** column contains the upgraded version of `6.3.3`.

Upgrade the Components for the Management Cluster

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

Procedure

1 Upgrade 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 Upgrade for the Management Cluster

After you upgrade the management components from the virtual infrastructure layer of the SDDC that are provide infrastructure management and disaster recovery, upgrade the Update Manager Download Service (UMDS) instances followed by the ESXi hosts, VMware Tools on the management virtual machines, and finally the vSAN storage in Region A and Region B.

Upgrade 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 VMware Validated Design vSphere and disaster recovery layers for the management clusters is a multi-step operation in which you must upgrade the Management Platform Services Controller, Management vCenter Server, vSphere Replication Appliance and Site Recovery Manager system in Region A before you repeat this operation in Region B, accordingly. This sequence 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 4-9. 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	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
	Compute Platform Services Controller that is configured in a highly-available pair	172.17.11.63	lax01w01psc01.lax01.rainpole.local
	Management vCenter	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

Note VMware Validated Design 4.1 introduces a new convention for host and object names in the SDDC. The step-by-step upgrade guidance uses the new names for both the pre- and post-upgrade SDDC setups. For information about the new convention, see Mapping Component Names Between Versions 4.0 and 4.1 of VMware Validated Design.

Prerequisites

- For Management vCenter Server and Platform Services Controller instances
  - 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 for the duration of the upgrade.
  - Ensure that any integration with the Management vCenter Server instances in 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 could be disrupted by orphaned objects that could be generated after you have taken snapshots. You might also have to extend the time of the maintenance windows.
  - Verify that a backup of all Platform Services Controller and Management vCenter Server instances exists. See the *VMware Validated Design Backup and Restore* documentation.
- For vSphere Replication
  - Download the vSphere Replication Upgrade `VMware-vSphere_Replication-6.x.x-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 instances are successfully upgraded.
  - Verify that all services on the Management Platform Services Controller and Management vCenter Server instances are running.
- For Site Recovery Manager
  - Download the Site Recovery Manager Upgrade `VMware-srm-6.x.x.exe` file.
  - Create a backup of the each Site Recovery Manager system that has been configured as a pair.
  - Verify that the Management Platform Services Controller and Management vCenter Server instances are successfully upgraded.
  - Verify that all services on the Management Platform Services 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 start the update, take a snapshot of each Management vCenter Server Virtual Appliance in Region A and Region B as well as all Platform Services Controller instances so that you can roll the upgrade back if a failure occurs.

2 Upgrade the Platform Services Controller Instances in Region A

3 Upgrade Management vCenter Server in Region A

4 Upgrade vSphere Replication Appliance in Region A

After you upgrade the Management Platform Services Controller and vCenter Server, upgrade the vSphere Replication appliance in Region A.

5 Upgrade Site Recovery Manager in Region A

After you upgrade the vSphere Replication appliance in Region A, proceed to Site Recovery Manager upgrade in Region A.

6 Upgrade Platform Services Controller Instances in Region B

7 Upgrade Management vCenter Server in Region B

8 Upgrade vSphere Replication Appliance in Region B

To continue your upgrade of the vSphere and disaster recovery instances in the SDDC, after you upgrade the Management vCenter Server, upgrade the vSphere Replication appliance in Region B.

9 Upgrade Site Recovery Manager in Region B

After you upgrade the vSphere Replication appliance, proceed to upgrading the Site Recovery Manager system in Region B to complete the upgrade of the infrastructure management components of the SDDC.

10 Clean Up the Snapshots of the vSphere and Disaster Recovery Components in Region A and Region B

After you complete the upgrade of the management components of the virtual infrastructure layer in Region A and Region B, and you validate their operational state, remove the snapshots from the nodes.

What to do next

- Verify that the vSphere and Disaster Recovery components are functional. See the *VMware Validated Design Operational Verification* documentation.

Take Snapshots of the Management vCenter Server and Platform Services Controller Instances in Region A and Region B

Before you start the update, take a snapshot of each Management vCenter Server Virtual Appliance in Region A and Region B as well as all Platform Services Controller instances so that you can roll the upgrade back if a failure occurs.

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 for sfo01m01vc01** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	VMware Validated Design 4.1 Virtual Infrastructure
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 in Region B and Platform Services Controller instances in both regions.

Upgrade the Platform Services Controller Instances in Region A

When you upgrade the vSphere components in Region A and Region B, upgrade the Platform Services Controller instances that are configured in a highly-available pair in Region A first.

Table 4-10. Platform Services Controller Instances in Region A

Role	Fully Qualified Domain Name
Platform Services Controller for the management cluster	sfo01m01psc01.sfo01.rainpole.local
Platform Services Controller for the shared edge and compute cluster	sfo01w01psc01.sfo01.rainpole.local

Prerequisites

- Verify that a backup of the Platform Services Controllers virtual appliances in Region A exists. See the *VMware Validated Design Backup and Restore* documentation.

- Mount the upgrade `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://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 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 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 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 sfo01m01psc01.

3 Log into 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 Eject the attached upgrade `.iso` file from the Platform Services Controller instance.
9 Repeat the steps on the sfo01w01psc01 node.

Upgrade Management vCenter Server in Region A

When you upgrade the vSphere components in Region A and Region B, after you complete the upgrade to the Platform Services Controller instances first in Region A, you upgrade the Management vCenter Server in Region A.

Prerequisites

- Verify that a backup of the Management vCenter Server virtual appliance in Region A exists. See the *VMware Validated Design Backup and Restore* documentation.

- Mount the upgrade `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 Eject the attached upgrade `.iso` from the Management vCenter Server appliance.

Upgrade vSphere Replication Appliance in Region A

After you upgrade the Management Platform Services Controller and vCenter Server, upgrade the vSphere Replication appliance in Region A.

Prerequisites

- Verify that a backup of the vSphere Replication Virtual Appliances in both Regions A and B exists.
- Mount the upgrade `VMware-vSphere_Replication-6.x.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://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 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 4.1 BCDR Upgrade
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 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 upgrade completes, click the **System** tab and click **Reboot**.

10 In the **System Reboot** dialog box, click **Reboot**.

   During the upgrade process, after you have initiated the reboot of the appliance, the appliance will reboot two times during the upgrade.

11 After the vSphere Replication appliance restarts, 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://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 complete, ensure that the **Service Status** section on the **Configuration** tab shows that the VRM service is `running`.

12 Close all browser sessions to vCenter Server and clear the browser's cache.

13 Eject the attached upgrade ISO from the vSphere Replication virtual appliance.

Upgrade Site Recovery Manager in Region A

After you upgrade the vSphere Replication appliance in Region A, proceed to Site Recovery Manager upgrade in Region A.

Prerequisites

Verify that a backup of the Site Recovery Manager virtual machines in both Regions A and B exists.

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 machine.

   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 **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 4.1 BCDR 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 sfo01m01srm01.sfo01.rainpole.local by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to the virtual machine 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 Windows virtual machine of Site Recovery Manager.

5 Navigate to the folder where you downloaded the VMware Site Recovery Manager upgrade 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
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, then 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, then 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_admin password for the database, validate the following settings and click **Next**.

Setting	Value
Data Source Name	SRM_SITE_SFO
Database User Name	srm_admin
Database Password	*srm_admin_sfo_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**.

Note If you have deployed your VMware Validated Design SDDC via the Deployment Tool Kit, consult the Release Notes prior to upgrading Site Recovery Manager.

21 After you upgrade the Site Recovery Manager, close all browser sessions to vCenter Server and clear the browser's 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 pop-up windows **Checking for New Plug-ins**, click **Go to the Event Console**.

g In the **Events Console**, using the filter, enter **`plug-in`**.

You should observe two events that recently occurred:

```
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 both of these events have been observed, 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.

Note If the new client plug-in does not appear, restart the vSphere Web Client service on the vCenter Server using SSH.

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

Upgrade Platform Services Controller Instances in Region B

After you complete the upgrade 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	Fully Qualified Domain Nam
Platform Services Controller for the management cluster	lax01m01psc01.lax01.rainpole.local
Platform Services Controller for the shared edge and compute cluster	lax01w01psc01le.lax01.rainpole.local

Prerequisites

- Verify that a backup of the Platform Services Controllers Virtual Appliances in Region B exists.
- Mount the upgrade `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 into 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 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 lax01m01psc01.

8 Eject the attached upgrade `.iso` file from the Platform Services Controller instance.

9 Repeat the procedure on the lax01w01psc01 node.

Upgrade Management vCenter Server in Region B

When you upgrade the vSphere components in Region B, after you upgrade the Platform Services Controller instances, you proceed with upgrading the Management vCenter Server in Region B.

Prerequisites

- Verify that a backup of the Management vCenter Server Virtual Appliance in Regions B exists.
- Mount the upgrade `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 Eject the attached upgrade `.iso` from the Management vCenter Server appliance.

Upgrade vSphere Replication Appliance in Region B

To continue your upgrade of the vSphere and disaster recovery instances in the SDDC, after you upgrade the Management vCenter Server, upgrade the vSphere Replication appliance in Region B.

Prerequisites

- Verify that a backup of the vSphere Replication virtual appliance in Region B exists.
- Mount the upgrade `VMWare-vSphere_Replication-6.x.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 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 4.1 BCDR Upgrade
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 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 upgrade completes, click the **System** tab and click **Reboot**.

10 In the **System Reboot** dialog box, click **Reboot**.

During the upgrade process, after you have initiated the reboot of the appliance, the appliance will reboot two times during the upgrade.

11 After the vSphere Replication 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 complete, verify that the **Service Status** section on the **Configuration** tab reports that VRM service is **`running`**.

12 Close all browser sessions to vCenter Server and clear the browser's cache.

13 Eject the attached upgrade ISO from the vSphere Replication virtual appliance.

Upgrade Site Recovery Manager in Region B

After you upgrade the vSphere Replication appliance, 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 vSphere Replication appliance in Region A.

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 4.1 BCDR 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 lax01m01srm01.lax01.rainpole.local 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 upgrade `VMware-srm-6.x.x.exe` file to the Windows virtual machine of Site Recovery Manager.

5 Navigate to the folder where you downloaded the VMware Site Recovery Manager upgrade installer, 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	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, then 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, then 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_admin password for the database, validate the following settings and click **Next**.

Setting	Value
Data Source Name	SRM_SITE_LAX
Database User Name	srm_admin
Database Password	*srm_admin_lax_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**.

Note If you have deployed your VMware Validated Design SDDC via the Deployment Tool Kit, consult the Release Notes prior to upgrading Site Recovery Manager.

21 After you upgrade the Site Recovery Manager, close all browser sessions to vCenter Server and clear the browser's cache.

22 Check for the latest Site Recovery Manager plug-in within 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 pop-up windows **Checking for New Plug-ins**, click **Go to the Event Console**.

g In the **Events Console**, using the filter, enter **`plug-in`**.

You should observe two events that recently occurred:

```
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 both of these events have been observed, 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.

Note If the new client plug-in does not appear, restart the vSphere Web Client service on the vCenter Server using SSH.

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

23 After you restart the vSphere Web Client, reconnect the Site Recovery Manager instances in Region A and Region B.

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

Settings	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, review the certificate thumbprints for lax01m01vc01.lax01.rainpole.local and lax01psc01.lax01.rainpole.local, then click **Yes**.

i If prompted, in the **Security Alert** dialog, review the certificate thumbprints for sfo01m01vc01.sfo01.rainpole.local and sfo01psc01.sfo01.rainpole.local, then click **Yes**.

24 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`.

Clean Up the Snapshots of the vSphere and Disaster Recovery Components in Region A and Region B

After you complete the upgrade of the management components of the virtual infrastructure layer in Region A and Region B, and you validate their operational state, remove the snapshots from the nodes.

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
	sfo01-m01fd-bdcr	vSphere Replication	sfo01m01vrms01
	sfo01-m01fd-bdcr	Site Recovery Manager	sfo01m01srm01
Region B	lax01-m01fd-mgmt	vCenter Server	lax01m01vc01
	lax01-m01fd-mgmt	Platform Services Controller	lax01m01psc01
	lax01-m01fd-mgmt	Platform Services Controller	lax01w01psc01
	lax01-m01fd-bdcr	vSphere Replication	lax01m01vrms01
	lax01-m01fd-bdcr	Site Recovery Manager	lax01m01srm01

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, the Platform Services Controller instances, vSphere Replication and Site Recovery Manager virtual machines in both regions.

Complete vSphere Upgrade for the Management Cluster

After you upgrade the management components from the virtual infrastructure layer of the SDDC that are provide infrastructure management and disaster recovery, upgrade the Update Manager Download Service (UMDS) instances followed by the ESXi hosts, VMware Tools on the management virtual machines, and finally the vSAN storage 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, management ESXi hosts, and the vSAN on-disk format in Region A. 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 4-11. 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	-

Table 4-11. Management ESXi Hosts and UMDS Nodes in the SDDC (Continued)

Region	Cluster Name	IP Address	Fully Qualified Domain Name	vSAN Datastore
		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 4-12. 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.rainpole.local
				vra01iws01b.rainpole.local
			vRealize Automation Model Manager Service	vra01ims01a.rainpole.local
				vra01ims01b.rainpole.local
			vRealize Automation DEM Workers	vra01dem01a.rainpole.local
				vra01dem01b.rainpole.local
			Microsoft SQL Server	vra01mssql01.rainpole.local
		sfo01-m01fd-vraias	vRealize Automation Proxy Agent	sfo01ias01a.sfo01.rainpole.local
				sfo01ias01b.sfo01.rainpole.local
		sfo01-m01fd-bcdr	vSphere Data Protection	sfo01m01vdp01
			Site Recovery Manager	sfo01m01srm01
Region B	lax01-m01-mgmt01	lax01-m01fd-mgmt	Update Manager Download Service	lax01umds01
		lax01-m01fd-vraias	vRealize Automation Proxy Agent	lax01ias01a.lax01.rainpole.local
				lax01ias01b.lax01.rainpole.local
		lax01-m01fd-bcdr	vSphere Data Protection	lax01m01vdp01
			Site Recovery Manager	lax01m01srm01

Note VMware Validated Design 4.1 introduces a new convention for host and object names in the SDDC. The step-by-step upgrade guidance uses the new names for both the pre- and post-upgrade SDDC setups. For information about the new convention, see Mapping Component Names Between Versions 4.0 and 4.1 of VMware Validated Design.

Prerequisites

- For Update Manager Download Service instances
  - Verify that a backup of all Update Manager Download Service virtual machines exists. See the *VMware Validated Design Backup and Restore* documentation.
  - 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
  - Verify that the firmware for the network and host bus adapter (HBA) cards have been updated for compatibility.
  - Verify that the BIOS on the ESXi hosts is updated for compatibility.
  - Allocate sufficient disk space on the host for the upgrade.
  - 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. See the *VMware Validated Design Backup and Restore* documentation.

Procedure

1 Upgrade vSphere Update Manager Download Service in Region A

After you upgrade of the vCenter Server instances in Region A and Region B, upgrade the vSphere Update Manager Download Service (UMDS) to the latest version so that you can upgrade the ESXi hosts.

2 Upgrade the ESXi Hosts in the Management Cluster in Region A

After you upgrade UMDS, you can proceed with upgrading the management ESXi hosts in Region A to the version used in VMware Validated Design 4.1. You use vSphere Update Manager for automated host upgrade across the management cluster.

3 Remediate VMware Tools in the Management Cluster in Region A

After you upgrade the ESXi hosts running the management virtual machines, upgrade the VMware Tools in Region A to the version used in VMware Validated Design 4.1. 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 Upgrade the On-Disk Version of vSAN on the Management Hosts in Region A

Using the vSphere Web Client, update the on-disk format version of vSAN on the hosts in the management cluster for Region A after you upgrade the hosts and VMware Tools in the cluster.

5 Upgrade Update Manager Download Service, Management ESXi Hosts, VMware Tools and vSAN On-Disk Format in Region B

In a dual-region SDDC, after you complete the upgrade of the virtual infrastructure components for the management pod in Region A, start the upgrade of vSphere Update Manager Download Service (UMDS), management ESXi hosts, VMware Tools and vSAN 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. See *Verify the Status of the vSphere Update Manager Download Service* in the *VMware Validated Design Operational Verification* documentation.
- Verify that the management ESXi hosts are operational after the upgrade. See *Verify the ESXi Hosts* in the *VMware Validated Design Operational Verification* documentation.
- Verify that the management virtual machines are operational after the upgrade. See the *VMware Validated Design Operational Verification* documentation.

Upgrade vSphere Update Manager Download Service in Region A

After you upgrade of the vCenter Server instances in Region A and Region B, upgrade the vSphere Update Manager Download Service (UMDS) to the latest version so that you can upgrade the ESXi hosts.

You cannot upgrade 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 that you uninstalled.

Prerequisites

- Verify that a backup of the UMDS virtual machine exists. See *VMware Validated Design Backup and Restore*.

- 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
Region B	192.168.32.67	lax01umds01.lax01.rainpole.local	lax01-m01-mgmt01	lax01-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 Update Manager Download Service 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.localsfo01-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 4.1 Virtual Infrastructure
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.

```
./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 Eject the attached upgrade `.iso` from the UMDS system.

Upgrade the ESXi Hosts in the Management Cluster in Region A

After you upgrade UMDS, you can proceed with upgrading the management ESXi hosts in Region A to the version used in VMware Validated Design 4.1. You use vSphere Update Manager for automated host upgrade 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 4-13. Management ESXi Hosts In Region A

IP Address	Fully Qualified Domain Name	Cluster Name	vSAN Datastore
172.16.11.101	sfo01m01esx01.sfo01.rainpole.local	sfo01-m01-mgmt01	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		

Prerequisites

- 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
- Verify that the firmware for the network and host bus adapter (HBA) cards have been updated for compatibility.
- Verify that the BIOS on the ESXi hosts is updated for compatibility.
- Allocate sufficient disk space on the host for the upgrade.
- 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.
- If using vSAN in the management cluster, verify the following health properties on the **Monitor** tab for the cluster in the vSphere Web Client:
  - 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.

Procedure

1 Remediate the ESXi Management Hosts that Use vSAN in Region A

If the management cluster in Region A is vSAN-backed, use the system managed baseline automatically created in vSphere Update Manager on the Management vCenter Server in Region A to remediate the hosts in the cluster.

2 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. See *Validate the ESXi Hosts* in the *VMware Validated Design Operational Verification* documentation.

Remediate the ESXi Management Hosts that Use vSAN in Region A

If the management cluster in Region A is vSAN-backed, use the system managed baseline automatically created in vSphere Update Manager on the Management vCenter Server in Region A to remediate the hosts in the cluster.

Procedure

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

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

b Log in using the following credentials.

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

2 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 Locate and 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 box, locate the **System managed** group.

e Expand the **System managed** group, and verify that `VSAN Cluster 'sfo01-m01-mgmt01'` baseline group containing the `VMware ESXi 6.5.0 U1 (build xxxxxxx)` host upgrade baseline is present.

Note If an additional host patch baseline `vSAN recommended patch to be applied on top of ESXi 6.5 U1` is present, you include in the remediation operation.

4 Scan the cluster for updates against the system managed baseline.

a Next to the **Hosts Baselines** pane, click **Go to compliance view** button to locate the sfo01-m01-mgmt01 cluster.

b On the **Update Manager** tab, click **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 complete, the cluster state is `Non-Compliant`.

5 Remediate the cluster and upgrade to vSphere 6.5 Update 1.

a On the **Update Manager** tab, click **Remediate**.

b In the **Remediate** wizard, on the **Select baselines** page, 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 the cluster and click **Next**.

d If presented with the **EULA** page, select **I accept the terms and license agreement** and click **Next**.

e If presented with the **Patches and extensions** page, select the patch associated with the **vSAN recommended patch to be applied on top of ESXi 6.5 U1** host patch baseline and click **Next**.

f On the **Advanced options** page, click **Next**

g On the **Host remediation options** page, deselect **Retry entering maintenance mode in case of failure** and click **Next**.

h 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

i 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.

j 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** 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 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 1 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 **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 1 for VMware Validated Design 4.1
Description	-
Baseline Type	Host Patch

f On the **Patch options** page, select **Fixed**.

g On the **Patches** page, type `Update 1` in the Filter search box and press Enter, check the box next to the patch names **VMware ESXi 6.5 Complete Update 1** and click **Next**.

h 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 to the sfo01-m01-mgmt01 cluster.

b On the **Update Manager** tab, click **Attach Baseline**.

c In the **Attach Baseline** dialog box, select the **VMware ESXi 6.5 Update 1 for VMware Validated Design 4.1** 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 1.

a On the **Update Manager** tab, 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 1 for VMware Validated Design 4.1** baseline and click **Next**.

c On the **Select Target objectst** page, select all of the management hosts in the cluster and click **Next**.

d On the **Patch and extensions** page, select the **VMware ESXi 6.5 Complete Update 1** patch 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 hists 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 upgrade the ESXi hosts running the management virtual machines, upgrade the VMware Tools in Region A to the version used in VMware Validated Design 4.1. 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 4-14. 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.rainpole.local
			vra01iws01b.rainpole.local
		vRealize Automation Model Manager Service	vra01ims01a.rainpole.local
			vra01ims01b.rainpole.local
		vRealize Automation DEM Workers	vra01dem01a.rainpole.local

Table 4-14. Management Virtual Machines for VMware Tools Remediation in Region A (Continued)

Cluster Name	Folder	Role	Virtual Machine Name
			vra01dem01b.rainpole.local
		Microsoft SQL Server	vra01mssql01.rainpole.local
	sfo01-m01fd-vraias	vRealize Automation Proxy Agent	sfo01ias01a.sfo01.rainpole.local
			sfo01ias01b.sfo01.rainpole.local
	sfo01-m01fd-bcdr	vSphere Data Protection	sfo01m01vdp01
		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 VMware Tools that is packaged with ESXi 6.5 Update 1 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 **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 6.5 Update 1 for VMware Validated Design 4.1
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 On 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.

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 6.5 Update 1 for VMware Validated Design 4.1** 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 vSphere 6.5 Update 1.

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 6.5 Update 1 for VMware Validated Design 4.1** 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 6.5 Update 1 Upgrade	
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 section	
Name	VMware Tools 6.5 Update 1 for VMware Validated Design 4.1
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 Due to the use of Guest Managed VMware Tools in the virtual machines, the **Compliance Status** might report `Incompatible` for the overall folder.

7 Remove the snapshot from each virtual machine in the folder.

a From the **Home** menu, click **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 **SnapshotsDelete All Snapshots**.

d In the **Confirm Delete** dialog box, click **Yes**.

8 Repeat these steps for the other management virtual machines using their folder in Region A .

9 Repeat these steps for the management virtual machines in Region B.

What to do next

- Verify that the management virtual machines are operational after the upgrade. See *Validate the Cloud Management Platform, vSphere Data Protection, Site Recovery Manager, and Update Manager Download Service* in the *VMware Validated Design Operational Verification* documentation.

Upgrade the On-Disk Version of vSAN on the Management Hosts in Region A

Using the vSphere Web Client, update the on-disk format version of vSAN on the hosts in the management cluster for Region A after you upgrade the hosts and VMware Tools in the cluster.

Table 4-15. Management ESXi Hosts and The Associated VSAN Cluster In Region A

IP Address	Fully Qualified Domain Name	Cluster Name	Virtual SAN Datastore
172.16.11.101	sfo01m01esx01.sfo01.rainpole.local	sfo01-m01-mgmt01	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		
172.16.11.1xx	sfo01m01esxxx.sfo01.rainpole.local		

Procedure

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

   a Open a Web browser and go to **`https://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 **Hosts and Clusters**.

3 In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-mc01dc** tree and select the **sfo01-m01-mgmt01** cluster.

4 Click the **Configure** tab, and under **vSAN** click **General**.

5 Under the **On-Disk Format Version** section, click **Pre-check Update**.

   Note If pre-check fails during the review phase, click **Detail** to review the issue and remediate them before re-attempting the Pre-check Upgrade operation.

6 Verify that you cluster meets all of the requirements to upgrade the on-disk version.

7 After all requirements are satisfied, and the disk pre-check status is `Ready to Upgrade`, click **Upgrade** and click **Yes** in the **Upgrade** confirmation message

   Wait for vSAN on-disk format to be upgraded to the latest version. You can monitor the progress of the upgrade in the **Disk format version** section.

Upgrade Update Manager Download Service, Management ESXi Hosts, VMware Tools and vSAN On-Disk Format in Region B

In a dual-region SDDC, after you complete the upgrade of the virtual infrastructure components for the management pod in Region A, start the upgrade of vSphere Update Manager Download Service (UMDS), management ESXi hosts, VMware Tools and vSAN in Region B. Upgrading both regions enables failover and failback between Region A and Region B.

Table 4-16. General Parameters for Upgrade of UMDS, Management ESXi and vSAN 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 4-17. Configuration for UMDS Upgrade 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
Cluster	lax01-m01-mgmt01
Folder	lax01-m01fd-mgmt
UMDS virtual machine	lax01umds01

3 Upgrade the managing ESXi hosts in Region B.

   Repeat Upgrade the ESXi Hosts in the Management Cluster in Region A by using the following details:

Table 4-18. Management ESXi Hosts to Upgrade in Region B

Host IP Address	Fully Qualified Domain Name	Cluster Name	vSAN Datastore	NSX Manager for the Management Cluster
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 4-19. Management Virtual Machines and Virtual Appliances In Region B

Cluster Name	Folder	Role	Virtual Machine Name
lax01-m01-mgmt01	lax01-m01d-mgmt	Update Manager Download Service	lax01umds01
	lax01-m01fd-vraias	vRealize Automation Proxy Agent	lax01ias01a.lax01.rainpole.local
			lax01ias01b.lax01.rainpole.local
	lax01-m01fd-bcdr	vSphere Data Protection	lax01m01vdp01
		Site Recovery Manager	lax01m01srm01

5 Upgrade the on-disk format of vSAN on the hosts in the management cluster in Region B.

Repeat Upgrade the On-Disk Version of vSAN on the Management Hosts in Region A.

What to do next

Verify that UMDS, management hosts and vSAN are operational. See *Validate vSphere* in the *VMware Validated Design Operational Verification* documentation.

Upgrade the Components for the Shared Edge and Compute Cluster

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

Procedure

1 Upgrade vSphere for the Shared Edge and Compute Cluster

When you upgrade the components that support the management cluster in the SDDC , you upgrade the Compute vCenter Server in Region A and repeat this operation in Region B.

2 Upgrade the ESXi Hosts in the Shared Edge and Compute Cluster

To complete your upgrade of the shared edge and compute cluster 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 upgrade across the shared edge and compute cluster.

Upgrade vSphere for the Shared Edge and Compute Cluster

When you upgrade the components that support the management cluster in the SDDC , you upgrade the Compute vCenter Server in Region A and repeat this operation in Region B.

Compared with from the earlier version of this design, upgrading the VMware Validated Design vSphere layer for the shared edge and compute cluster has been simplified to a single-step operation. In this version, you upgrade the Compute vCenter Server in Region A. Then, you repeating this operation in Region B.

Table 4-20. Compute vSphere and Disaster Recovery Nodes 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

Note VMware Validated Design 4.1 introduces a new convention for host and object names in the SDDC. The step-by-step upgrade guidance uses the new names for both the pre- and post-upgrade SDDC setups. For information about the new convention, see Mapping Component Names Between Versions 4.0 and 4.1 of VMware Validated Design.

Prerequisites

- Download the vCenter Server Appliance `VMware-vCenter-Server-Appliance-6.5.0.x-build_number-patch-FP.is` file.
- 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 management workloads automatically migrated from hosts while they are being upgraded.

- Verify that all compute ESXi hosts have the lockdown mode disabled for the duration of the upgrade.
- Ensure that any integration with the Compute vCenter Server instances in the environment has been quiesced of all activities, including but not limited to, users requesting new virtual machines with or without virtual wires by using the vRealize Automation Cloud Management Platform (CMP), third-party integration that might automate the ordering or deployment of new virtual machines, and administrators manually creating new virtual objects. Without quiescing the environment, rollback operations could be disrupted by orphaned objects that are generated after you have taken snapshots. You might also have to extend the time of the maintenance windows.
- Verify that a backup of the Compute vCenter Server instances exists. See the *VMware Validated Design Backup and Restore* documentation.

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 appliance in Region A and Region B so that you can roll the update back if a failure occurs.

2 Upgrade the Compute vCenter Server in Region A

3 Upgrade the Compute vCenter Server in Region B

When you upgrade the Compute vCenter Server in Region A, upgrade the Compute vCenter Server in Region B to complete the upgrade of vCenter Server.

4 Cleanup Snapshots of the Shared Edge and Compute vCenter Servers in Region A and Region B

After completing the upgrade of the Shared Edge and Compute components in Region A and Region B, and validated their stability, remove the snapshots from the nodes.

What to do next

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

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 appliance in Region A and Region B so that you can roll the update back if a failure occurs.

Table 4-21. 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 **sf01w01vc01.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 for sfo01w01vc01** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	VMware Validated Design 4.1 Virtual Infrastructure
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 in Region B.

Upgrade the Compute vCenter Server in Region A

After you upgrade the components for the management clusters, upgrade the Compute vCenter Server in Region A.

Prerequisites

- Verify that a backup of the Compute vCenter Server Virtual Appliance in Region A exists. See the *VMware Validated Design Backup and Restore* documentation.
- Mount the upgrade `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 Eject the attached upgrade `.iso` from the Compute vCenter Server appliance.

Upgrade the Compute vCenter Server in Region B

When you upgrade the Compute vCenter Server in Region A, upgrade the Compute vCenter Server in Region B to complete the upgrade of vCenter Server.

Prerequisites

- Verify that a backup of the Compute vCenter Server Virtual Appliance in Regions B exists.
- Mount the upgrade `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 Eject the attached upgrade `.iso` from the Compute vCenter Server appliance.

Cleanup Snapshots of the Shared Edge and Compute vCenter Servers in Region A and Region B

After completing the upgrade of the Shared Edge and Compute components in Region A and Region B, and validated their stability, remove the snapshots from the nodes.

Prerequisites

- Verify that a backup of the Management vCenter Server Virtual Appliances exist.

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 **sfo01w01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-mgmt** tree.

4 Right-click the **sfo01w01vc01** 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.

Region	Folder	Role	Virtual Machine Name
Region B	lax01-m01fd-mgmt	vCenter Server	lax01w01vc01

Upgrade the ESXi Hosts in the Shared Edge and Compute Cluster

To complete your upgrade of the shared edge and compute cluster 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 upgrade across the shared edge and compute cluster.

Table 4-22. 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

Table 4-22. Shared Edge and Compute ESXi Hosts in the SDDC (Continued)

Region	IP Address	Fully Qualified Domain Name	Cluster Name
	172.17.31.102	lax01w01esx02.lax01.rainpole.local	
	172.17.31.103	lax01w01esx03.lax01.rainpole.local	
	172.17.31.104	lax01w01esx04.lax01.rainpole.local	
	172.17.31.1*xx*	lax01w01esx*xx*.lax01.rainpole.local	

Note VMware Validated Design 4.1 introduces a new convention for host and object names in the SDDC. The step-by-step upgrade guidance uses the new names for both the pre- and post-upgrade SDDC setups. For information about the new convention, see Mapping Component Names Between Versions 4.0 and 4.1 of VMware Validated Design.

Prerequisites

- 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
- Verify that the firmware for the network and host bus adapter (HBA) cards have been updated for compatibility.
- Verify that the BIOS on the ESXi hosts is updated for compatibility.
- Allocate sufficient disk space on the host for the upgrade.
- 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 tenant workloads automatically migrated from hosts while they are being upgraded.

What to do next

- Verify that the ESXi hosts in the shared edge and compute cluster are operational after the upgrade. See *Validate ESXi Hosts* in the *VMware Validated Design Operational Verification* documentation.

Use vSphere Update Manager to Remediate the ESXi Shared Edge and Compute Cluster 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.

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 1 in vSphere Update Manager in Region A

   a From the **Home** menu, select **Update Manager**.

   b In the left **Servers** pane, 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 1 for VMware Validated Design 4.1
Description	-
Baseline Type	Host Patch

   f On the **Patch options** page, select **Fixed**.

   g On the **Patches** page, type `Update 1` in the Filter search box and press Enter, check the box next to the patch names **VMware ESXi 6.5 Complete Update 1** and click **Next**.

   h 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.

   b On the **Update Manager** tab, click **Attach Baseline**.

c In the **Attach Baseline** dialog box, select the **VMware ESXi 6.5 Update 1 for VMware Validated Design 4.1** 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 upgrade to vSphere 6.5 Update 1.

a On the **Update Manager** tab, 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 1 for VMware Validated Design 4.1** baseline and click **Next**.

c On the **Select Target objectst** page, select all of the management hosts in the cluster and click **Next**.

d On the **Patch and extensions** page, select the **VMware ESXi 6.5 Complete Update 1** patch 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 hists 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 shared edge and compute cluster.

   a Select **Home > Networking & Security**.

   b Select **Installation** in the **Navigator**.

   c On the **Host Preparation** tab, select **172.16.11.66** from the **NSX Manager** menu and verify that **Installation Status** for all management ESXi hosts is green.

6 Repeat this procedure on the lax01w01vc01.lax01.rainpole.local vCenter Server using the VMware ESXi 6.5 Update 1 for VMware Validated Design 4.1 baseline.

Global Post-Upgrade Configuration of the Virtual Infrastructure Components

After you upgrade all virtual infrastructure components, 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 upgrade 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 upgrade 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 upgrade 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

Set an identity of your SDDC deployment on the Management vCenter Server in Region A. You can also 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, set the following value pairs one by one, clicking **Add** after each entry.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard
config.SDDC.Deployed.Version	4.1.0
config.SDDC.Deployed.Method	DIY

7 Click **OK** to close the dialog box.

Configure Uplinks in vSphere Distributed Switch for the Management Cluster in Region A

After all the upgrade tasks for vSphere vCenter in Region A are completed, configure uplink01 and uplink02 in vSphere Distributed Switch to handle the traffic of the management applications in the SDDC.

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 Configure the uplinks for the **sfo01-m01-vds01-uplink01** and **sfo01-m01-vds01-uplink02** port groups.

   a From the **Home** menu, click **Networking**.

   b Expand the **sfo01m01vc01.sfo01.rainpole.local sfo01-m01-vds01** tree.

   c Under **sfo01-m01-vds01** distributed switch, right click the **sfo01-m01-vds01-uplink01** port group, and click **Edit Settings**.

   d In the **Edit Settings** dialog box, click **Teaming and failover**.

   e Select **Load balancing** as **Route based on originating virtual port**.

   f In **Failover order** pane, move **dvUplink2** to **Unused uplinks** and click **OK**.

   g Under **sfo01-m01-vds01** distributed switch, right click the **sfo01-m01-vds01-uplink02** port group, and click **Edit Settings**.

   h In the **Edit Settings** dialog box, select **Teaming and failover**.

   i Select **Load balancing** as **Route based on originating virtual port**.

   j In **Failover order** pane, move **dvUplink1** to **Unused uplinks** and click **OK**.

Enable CDO mode for the NSX Management Cluster in Region A

After all the NSX components upgrade completed, enable CDO mode on the transport zone.

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 Enable CDO mode on transport zone.

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

   b On the **Installation** page, click the **Logical Network Preparation** tab and click **Transport Zones**.

   c From the **NSX Manager** drop-down menu, select the IP address **172.16.11.65 (Role: Primary)** of the NSX Manager for the management cluster in Region A.

   d Right click **Mgmt Universal Transport Zone**, choose **Enable CDO mode**, and click **Yes** in the dialog to enable CDO mode.

Update the Host Profile for the Management Cluster in Region A

After completing the upgrades for the ESXi hosts and upgrading the vSAN On-Disk format to the latest version in the management cluster in Region A, update the host profile to collect the changes inherent to vSphere 6.5 Update 1 and vSAN 6.6.1, and to configuring networking post-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 Update the host profile for the management cluster.
   a From the **Home** menu of the vSphere Web Client, select **Policies and Profiles**.
   b In the **Navigator**, click **Host Profiles**, right-click the **sfo01-m01hp-mgmt01** host profile, and select **Copy Settings from Host**.
   c Select **sfo01m01esx01.sfo01.rainpole.local**, click **OK**.
3 Verify compliance for the hosts in the management cluster.
   a From the vSphere Web Client **Home** menu, select **Hosts and Clusters**.
   b Click the **sfo01-m01-mgmt01** cluster, click the **Monitor** tab, and click **Profile Compliance**.
   c Click the **Check Compliance Now button**.
   d Verify all hosts are compliant with the attached profile.

Add a Persistent Static Route to the Hosts in Region B on vSphere Replication in Region A

On vSphere Replication in Region A, make the static route to the hosts in Region B persistent across restarts for the virtual NIC that is dedicated to replication traffic. Using a persistent route for replication traffic aligns your environment to the guidance of this validated design.

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 **Hosts and Clusters** and expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01-mgmt01** tree.
3 Right-click the **sfo01m01vrms01** virtual appliance and select **Open Console** to open the remote console to the appliance.
4 Press ALT+F2 to switch to the command prompt.
5 Log in using the following credentials.

Setting	Value
User name	root
Password	*vr_root_password*

6 Open the `/etc/sysconfig/network/routes` file using `vi` editor.

```
vi /etc/sysconfig/network/routes
```

7 To create a route to the recovery region for the hosts in Region A, add the following line after the default gateway and save the file.

```
172.17.16.0/24 172.16.16.253 dev eth1
```

8 Restart the network service on the virtual appliance.

```
service network restart
```

9 After the network service restarts, verify the routing table.

```
route –n
```

Set SDDC Deployment Details on the Compute vCenter Server in Region A

Set an identity of your SDDC deployment on the Compute vCenter Server in Region A. You can also 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, set the following value pairs one by one, clicking **Add** after each entry.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard

Name	Value
config.SDDC.Deployed.Version	4.1.0
config.SDDC.Deployed.Method	DIY

7 Click **OK** to close the dialog box.

Configure Uplinks in vSphere Distributed Switch for the Shared Edge and Compute Cluster in Region A

After all the upgrade tasks for vSphere vCenter in Region A are completed, configure the uplink01,uplink02 in vSphere Distributed Switch to handle the traffic of the compute applications in the SDDC.

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 Configure the uplinks for the **sfo01-w01-vds01-uplink01** and **sfo01-w01-vds01-uplink02** port groups.

a From the **Home** menu, click **Networking**.

b Expand the **sfo01w01vc01.sfo01.rainpole.local > sfo01-w01-vds01** tree.

c Under **sfo01-w01-vds01** distributed switch, right click the **sfo01-w01-vds01-uplink01** port group, and click **Edit Settings**.

d In the **Edit Settings** dialog box, select **Teaming and failover**.

e Select **Load balancing** as **Route based on originating virtual port**.

f In **Failover order** pane, move **dvUplink2** to **Unused uplinks** and click **OK**.

g Under **sfo01-w01-vds01** distributed switch, right click the **sfo01-w01-vds01-uplink02** port group, and click **Edit Settings**.

h In the **Edit Settings** dialog box, select **Teaming and failover**.

i Select **Load balancing** as **Route based on originating virtual port**.

j In **Failover order** pane, move **dvUplink1** to **Unused uplinks** and click **OK**.

Enable CDO mode for NSX Shared Edge and Compute Cluster in Region A

After all the NSX components upgrade completed, enable CDO mode on the transport zone for shared edge and compute cluster.

Procedure

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

   a Open a Web browser and go to **`https://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 Enable CDO mode on transport zone.

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

   b On the **Installation** page, click the **Logical Network Preparation** tab and click **Transport Zones**.

   c From the **NSX Manager** drop-down menu, select the IP address **172.16.11.66 (Role: Primary)** of the NSX Manager for the shared edge and compute cluster in Region A.

   d Right click **Comp Universal Transport Zone**, choose **Enable CDO mode**, and click **Yes** in the dialog to enable CDO mode.

Update the Host Profile for the Shared Edge and Compute Cluster in Region A

After completing the upgrades for the ESXi hosts in the shared edge and compute cluster in Region A, update the host profile to pick up the changes inherent to vSphere 6.5 Update 1 and to configuring networking post-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 Update the host profile for the shared edge and compute cluster.

   a From the **Home** menu of the vSphere Web Client, select **Policies and Profiles**.

   b In the **Navigator**, click **Host Profiles**, right-click the **sfo01-w01hp-comp01** host profile, and select **Copy Settings from Host**.

   c Select **sfo01w01esx01.sfo01.rainpole.local**, click **OK**.

3 Verify compliance for the hosts in the shared edge and compute cluster.

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

   b Click the **sfo01-w01-comp01** cluster, click the **Monitor** tab, and click **Profile Compliance**.

   c Click the **Check Compliance Now** button.

   d Verify all hosts are compliant with the attached profile.

Post-Upgrade Configuration of the Virtual Infrastructure Components in Region B

After you upgrade 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

   Set an identity of your SDDC deployment on the Management vCenter Server in Region B. You can also use this identity as a label in tools for automated SDDC deployment.

2 Configure Uplinks in vSphere Distributed Switch for the Management Cluster in Region B

   After all the upgrade tasks for vSphere vCenter in Region B are completed, configure uplink01 and uplink02 in vSphere Distributed Switch to handle the traffic of the management applications in the SDDC.

3 Update the Host Profile for the Management Cluster in Region B

   After completing the upgrades for the ESXi hosts and upgrading the vSAN On-Disk Format version to the latest in the management cluster in Region B, update the host profile to pick up the changes inherent to vSphere 6.5 Update 1 and vSAN 6.6.1.

4 Add a Persistent Static Route to the Hosts in Region A on vSphere Replication in Region B

   On vSphere Replication in Region B, make the static route to the hosts in Region A persistent across restarts for the virtual NIC that is dedicated to replication traffic. Using a persistent route for replication traffic aligns your environment to the guidance of this validated design.

5 Set SDDC Deployment Details on the Compute vCenter Server in Region B

   Set an identity of your SDDC deployment on the Compute vCenter Server in Region B. You can also use this identity as a label in tools for automated SDDC deployment.

6 Configure Uplinks in vSphere Distributed Switch for the Shared Edge and Compute Cluster in Region B

After all the upgrade tasks for vSphere vCenter in Region B are completed, configure the uplink01,uplink02 in vSphere Distributed Switch to handle the traffic of the compute applications in the SDDC.

7 Update the Host Profile for the Shared Edge and Compute Cluster in Region B

After completing the upgrades for the ESXi hosts in the shared edge and compute cluster in Region B, update the host profile pick up the changes inherent to vSphere 6.5 Update 1.

Set SDDC Deployment Details on the Management vCenter Server in Region B

Set an identity of your SDDC deployment on the Management vCenter Server in Region B. You can also 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, set the following value pairs one by one, clicking **Add** after each entry.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard
config.SDDC.Deployed.Version	4.1.0
config.SDDC.Deployed.Method	DIY

7 Click **OK** to close the window.

Configure Uplinks in vSphere Distributed Switch for the Management Cluster in Region B

After all the upgrade tasks for vSphere vCenter in Region B are completed, configure uplink01 and uplink02 in vSphere Distributed Switch to handle the traffic of the management applications in the SDDC.

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 Configure the uplinks for the **lax01-m01-vds01-uplink01** and **lax01-m01-vds01-uplink02** port groups.

   a From the **Home** menu, click **Networking**.

   b Expand the **lax01m01vc01.sfo01.rainpole.local** tree and expand the **lax01-m01-vds01** .

   c Under **lax01-m01-vds01** distributed switch, right click the **lax01-m01-vds01-uplink01** port group, and click **Edit Settings**.

   d In the **Edit Settings** wizard, click **Teaming and failover**.

   e Select **Load balancing** as **Route based on originating virtual port**.

   f In **Failover order** pane, move **dvUplink2** to **Unused uplinks** and click **OK**.

   g Under **lax01-m01-vds01** distributed switch, right click the **lax01-m01-vds01-uplink02** port group, and click **Edit Settings**.

   h In the **Edit Settings** wizard, select **Teaming and failover**.

   i Select **Load balancing** as **Route based on originating virtual port**.

   j In **Failover order** pane, move **dvUplink1** to **Unused uplinks** and click **OK**.

Update the Host Profile for the Management Cluster in Region B

After completing the upgrades for the ESXi hosts and upgrading the vSAN On-Disk Format version to the latest in the management cluster in Region B, update the host profile to pick up the changes inherent to vSphere 6.5 Update 1 and vSAN 6.6.1.

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 Update the host profile for the management cluster.

   a From the **Home** menu of the vSphere Web Client, select **Policies and Profiles**.

   b In the **Navigator**, click **Host Profiles**, right-click the **lax01-m01hp-mgmt01** host profile, and select **Copy Settings from Host**.

   c Select **lax01m01esx01.lax01.rainpole.local**, click **OK**.

3 Verify compliance for the hosts in the management cluster.

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

   b Click the **lax01-m01-mgmt01** cluster, click the **Monitor** tab, and click **Profile Compliance**.

   c Click the **Check Compliance Now** button.

   d Verify all hosts are compliant with the attached profile.

Add a Persistent Static Route to the Hosts in Region A on vSphere Replication in Region B

On vSphere Replication in Region B, make the static route to the hosts in Region A persistent across restarts for the virtual NIC that is dedicated to replication traffic. Using a persistent route for replication traffic aligns your environment to the guidance of this validated design.

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, click **Hosts and Clusters** and expand the **lax01m01vc01.lax01.rainpole.local > lax01-m01-mgmt01** tree.

3 Right-click the **lax01m01vrms01** virtual appliance and select **Open Console** to open the remote console to the appliance.

4 Press ALT+F2 to switch to the command prompt.

5 Log in using the following credentials.

Setting	Value
User name	root
Password	*vr_root_password*

6 Open the `/etc/sysconfig/network/routes` file using `vi` editor.

```
vi /etc/sysconfig/network/routes
```

7 To create a route to the recovery region for the hosts in Region A, add the following line after the default gateway and save the file.

```
172.16.16.0/24 172.17.16.253 dev eth1
```

8 Restart the network service on the virtual appliance.

```
service network restart
```

9 After the network service restarts, verify the routing table.

```
route –n
```

Set SDDC Deployment Details on the Compute vCenter Server in Region B

Set an identity of your SDDC deployment on the Compute vCenter Server in Region B. You can also 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, set the following value pairs one by one, clicking **Add** after each entry.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard
config.SDDC.Deployed.Version	4.1.0
config.SDDC.Deployed.Method	DIY

7 Click **OK** to close the window.

Configure Uplinks in vSphere Distributed Switch for the Shared Edge and Compute Cluster in Region B

After all the upgrade tasks for vSphere vCenter in Region B are completed, configure the uplink01,uplink02 in vSphere Distributed Switch to handle the traffic of the compute applications in the SDDC.

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 Configure the uplinks for the **lax01-w01-vds01-uplink01** and **lax01-w01-vds01-uplink02** port groups.

   a From the **Home** menu, click **Networking**.

   b Expand the **lax01w01vc01.sfo01.rainpole.local** tree and expand the **lax01-w01-vds01**.

   c Under **lax01-w01-vds01** distributed switch, right click the **lax01-w01-vds01-uplink01** port group, and click **Edit Settings**.

   d In the **Edit Settings** wizard, select **Teaming and failover**.

   e Select **Load balancing** as **Route based on originating virtual port**.

   f In **Failover order** pane, move **dvUplink2** to **Unused uplinks** and click **OK**.

   g Under **lax01-w01-vds01** distributed switch, right click the **lax01-w01-vds01-uplink02** port group, and click **Edit Settings**.

   h In the **Edit Settings** wizard, select **Teaming and failover**.

   i Select **Load balancing** as **Route based on originating virtual port**.

   j In **Failover order** pane, move **dvUplink1** to **Unused uplinks** and click **OK**.

Update the Host Profile for the Shared Edge and Compute Cluster in Region B

After completing the upgrades for the ESXi hosts in the shared edge and compute cluster in Region B, update the host profile pick up the changes inherent to vSphere 6.5 Update 1.

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 Update the host profile for the shared edge and compute cluster.

   a From the **Home** menu of the vSphere Web Client, select **Policies and Profiles**.

   b In the **Navigator**, click **Host Profiles**, right-click the **lax01-w01hp-comp01** host profile, and select **Copy Settings from Host**.

   c Select **lax01w01esx01.lax01.rainpole.local**, click **OK**.

3 Verify compliance for the hosts in the shared edge and compute cluster.

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

   b Click the **lax01-w01-comp01** cluster, click the **Monitor** tab, and click **Profile Compliance**.

   c Click the **Check Compliance Now** button.

   d Verify all hosts are compliant with the attached profile.

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 section includes the following topics:

- Shutdown Order of the Management Virtual Machines
- Startup Order of the Management Virtual Machines

Shutdown Order of the Management Virtual Machines

Shut down the virtual machines of the SDDC management stack by following a strict order to avoid data loss and faults in the applications.

Ensure that the console of the VM and its services are fully shut down before moving to the next VM.

Virtual Machine Name in Region A	Virtual Machine Name in Region B	Shutdown Order
vSphere Data Protection **Total Number of VMs (1)**	**vSphere Data Protection** **Total Number of VMs (1)**	**1**
sfo01m01vdp01	lax01m01vdp01	1
vRealize Log Insight **Total Number of VMs (3)**	**vRealize Log Insight** **Total Number of VMs (3)**	**1**
sfo01vrli01c	lax01vrli01c	1
sfo01vrli01b	lax01vrli01b	1
sfo01vrli01a	lax01vrli01a	2
vRealize Operations Manager **Total Number of VMs (5)**	**vRealize Operations Manager** **Total Number of VMs (2)**	**1**
sfo01vropsc01b	lax01vropsc01b	1
sfo01vropsc01a	lax01vropsc01a	1
vrops01svr01c	-	2
vrops01svr01b	-	3
vrops01svr01a	-	4
vRealize Business for Cloud **Total Number of VMs (2)**	**Realize Business for Cloud** **Total Number of VMs (2)**	**2**

Virtual Machine Name in Region A	Virtual Machine Name in Region B	Shutdown Order
sfo01vrbc01	lax01vrbc01	1
vrb01svr01	-	2
vRealize Automation **Total Number of VMs (11)**	**vRealize Automation** **Total Number of VMs (2)**	**3**
vra01dem01a	-	1
vra01dem01b	-	1
sfo01ias01b	lax01ias01b	1
sfo01ias01a	lax01ias01a	1
vra01ims01b	-	2
vra01ims01a	-	2
vra01iws01b	-	3
vra01iws01a	-	4
vra01svr01b	-	5
vra01svr01a	-	5
vra01mssql01	-	6
Site Recovery Manager and vSphere Replication **Total Number of VMs (2)**	**Site Recovery Manager and vSphere Replication** **Total Number of VMs (2)**	**4**
sfo01m01vrms01	lax01m01vrms01	1
sfo01m01srm01	lax01m01srm01	2
Update Manager Download Service (UMDS) **Total Number of VMs (1)**	**Update Manager Download Service (UMDS)** **Total Number of VMs (1)**	**4**
sfo01umds01	lax01umds01	1
Core Stack **Total Number of VMs (21)**	**Core Stack** **Total Number of VMs (13)**	**5**
sfo01m01lb01 (0,1)	lax01m01lb01 (0,1)	1
sfo01m01udlr01 (0,1)	-	1
sfo01m01esg01	lax01m01esg01	1
sfo01m01esg02	lax01m01esg02	1
sfo01w01udlr01 (0,1)	-	1
sfo01w01dlr01 (0,1)	lax01w01dlr01 (0,1)	1
sfo01w01esg01	lax01w01esg01	1
sfo01w01esg02	lax01w01esg02	1
sfo01m01nsx01	lax01m01nsx01	2
sfo01w01nsx01	lax01w01nsx01	2
sfo01m01nsxc01	-	3
sfo01m01nsxc02	-	3

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

Note For more information about shutting down and starting up vCenter Server when using a vSAN datastore, see VMware Knowledge Base article 2142676.

Startup Order of the Management Virtual Machines

Start up the virtual machines of the SDDC management stack by following a strict order to guarantee the faultless operation of and the integration between the applications.

Before you begin, verify that external dependencies for your SDDC, such as Active Directory, DNS, and NTP are available.

Ensure that the console of the VM and its services are all up before moving to the next VM.

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
Core Stack Total Number of VMs (21)	**Core Stack Total Number of VMs (13)**	**1**
sfo01m01psc01	lax01m01psc01	1
sfo01w01psc01	lax01w01psc01	1
sfo01psc01 (0,1)	lax01psc01 (0,1)	2
sfo01m01vc01	lax01m01vc01	3
sfo01w01vc01	lax01w01vc01	3
sfo01m01nsx01	lax01m01nsx01	4
sfo01w01nsx01	lax01w01nsx01	4
sfo01m01nsxc01	-	5
sfo01m01nsxc02	-	5
sfo01m01nsxc03	-	5
sfo01w01nsxc01	-	5
sfo01w01nsxc02	-	5
sfo01w01nsxc03	-	5

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
sfo01m01lb01 (0,1)	lax01m01lb01 (0,1)	6
sfo01m01udlr01 (0,1)	-	6
sfo01m01esg01	lax01m01esg01	6
sfo01m01esg02	lax01m01esg02	6
sfo01w01udlr01 (0,1)	-	6
sfo01w01dlr01 (0,1)	lax01w01dlr01(0,1)	6
sfo01w01esg01	lax01w01esg01	6
sfo01w01esg02	lax01w01esg02	6
Update Manager Download Service (UMDS) Total Number of VMs (1)	**Update Manager Download Service (UMDS) Total Number of VMs (1)**	**2**
sfo01umds01	lax01umds01	1
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

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
sfo01vropsc01a	lax01vropsc01a	4
sfo01vropsc01b	lax01vropsc01b	4
vRealize Log Insight Total Number of VMs (3)	**vRealize Log Insight Total Number of VMs (3)**	**5**
sfo01vrli01a	lax01vrli01a	1
sfo01vrli01b	lax01vrli01b	2
sfo01vrli01c	lax01vrli01c	2
vSphere Data Protection Total Number of VMs (1)	**vSphere Data Protection Total Number of VMs (1)**	**5**
sfo01m01vdp01	lax01m01vdp01	1