

# Upgrade

13 FEB 2018

VMware Validated Design 4.2

VMware Validated Design for Software-Defined Data  
Center 4.2



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](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2016–2018 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

About VMware Validated Design Upgrade	5
<b>1 SDDC Upgrade Overview</b>	<b>6</b>
Upgrade Policy	6
Upgrade Paths and Application Upgrade Sequence	7
VMware Software Versions in the Upgrade	9
System Requirements for the SDDC Upgrade	10
Best Practices in SDDC Upgrades	10
<b>2 Upgrade the Cloud Management Layer</b>	<b>12</b>
Configuration Changes to the Cloud Management Layer	12
Tenant User Groups, Accounts and Objects in VMware Validated Design 4.2	13
Assign Tenant Administrative Roles to Local Users	14
Assign Tenant Administrative Roles to Active Directory Users	15
Configure User Roles in vRealize Automation	16
Reconfigure Business Groups	18
Reconfigure Entitlements	18
Clean Up Obsolete Tenant User Accounts and Groups	19
<b>3 Upgrade the Operations Management Layer</b>	<b>22</b>
Configuration Changes of vRealize Operations Manager	22
Disable the vSAN Dashboards of the Management Pack for Storage Devices in Region A	23
Define a User Role in vSphere for vCenter Adapters in vRealize Operations Manager in Region A	24
Upgrade vRealize Log Insight	25
Take Snapshots of the vRealize Log Insight Nodes	27
Upgrade the vRealize Log Insight Clusters	28
Upgrade the Content Packs on vRealize Log Insight	29
Delete the Snapshots of the vRealize Log Insight Appliances	30
Post-Upgrade Configuration of the vRealize Log Insight	31
<b>4 Upgrade the Virtual Infrastructure and Business Continuity Layers</b>	<b>35</b>
Review and Update vSphere Storage APIs for Data Protection Based Backup Solution	36
Upgrade the NSX Components for the Management and Shared Edge and Compute Clusters	37
Upgrade the NSX Manager Instances	39
Upgrade the NSX Controller Instances	42
Upgrade the NSX Components on the ESXi Hosts	44
Upgrade NSX Edge Instances	47

- Upgrade the Components for the Management Cluster 50
  - Upgrade vSphereComponents for the Management Clusters 50
  - Complete vSphere Upgrade for the Management Cluster 60
- Upgrade the Components for the Shared Edge and Compute Cluster 77
  - Upgrade vSphere for the Shared Edge and Compute Cluster 78
  - Upgrade the ESXi Hosts in the Shared Edge and Compute Cluster 82
- Global Post-Upgrade Configuration of the Virtual Infrastructure Layer 86
  - Post-Upgrade Configuration of the Virtual Infrastructure Components in Region A 87
  - Post-Upgrade Configuration of the Virtual Infrastructure Components in Region B 89
- Post-Upgrade Configuration of the Business Continuity Layer for the Management Cluster 92
  - Connect vRealize Operations Manager to Site Recover Manager 92
  - Connect vRealize Log Insight to Site Recovery Manager 95

## **5 SDDC Startup and Shutdown 99**

- Shutdown Order of the Management Virtual Machines 99
- Startup Order of the Management Virtual Machines 101

# About VMware Validated Design Upgrade

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

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

---

**Note** The *VMware Validated Design Upgrade* document 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

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

## Required VMware Software

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

# SDDC Upgrade Overview

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

This chapter includes the following topics:

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

## Upgrade Policy

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

## Updates That Are Validated by VMware Validated Designs

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

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

The upgrade of VMware Validated Design provides 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 VMware Knowledge Base articles about 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 follow the path and sequence for specified for SDDC upgrade to version 4.2 of this VMware Validated Design.

### Upgrade Paths

To upgrade to version 4.2, you must run version 4.1 of this VMware Validated Design.

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

### 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	Upgraded/Updated	Component	Sub-Component (in Order)	Layer
1	No	vRealize Automation	vRealize Automation Appliances vRealize Orchestrator (Embedded) vRealize Automation IaaS Components	Cloud Management
2	No	vRealize Business for Cloud	vRealize Business for Cloud Appliance	

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

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

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

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

## VMware Software Versions in the Upgrade

You upgrade each management product 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 4.1 to VMware Validated Design for Software-Defined Data Center 4.2**

SDDC Layer	Product Name	Product Version in VMware Validated Design 4.1	Product Version in VMware Validated Design 4.2	Operation Type
Cloud Management	vRealize Automation with Embedded vRealize Orchestrator	7.3	7.3	-
	vRealize Business	7.3.1	7.3.1	-
Operations Management	vRealize Operations Manager	6.6.1	6.6.1	-
	vRealize Log Insight	4.5	4.5.1	Upgrade
	vRealize Log Insight Agent	4.5	4.5	-
Virtual Infrastructure	NSX for vSphere	6.3.4	6.4.0	Update
	vCenter Server	6.5 Update 1	6.5 Update 1 d	Update
	Platform Services Controller	6.5 Update 1	6.5 Update 1 d	Update
	Update Manager Download Service	6.5 Update 1	6.5 Update 1 d	Update
	ESXi	6.5 Update 1	6.5 Update 1 Patch Release ESXi650-201712001	Update
	vSAN	6.6.1	6.6.1	-
Business Continuity and Disaster Recovery	Site Recovery Manager	6.5.1	6.5.1	-
	vSphere Replication	6.5.1	6.5.1	-
	Backup solution based on VMware vSphere Storage APIs for Data Protection	Compatible Version	Compatible Version	N/A

For information about the software components that are available in VMware Validated Design 4.1 and VMware Validated Design 4.2, see *VMware Validated Design Release Notes*.

## System Requirements for the SDDC Upgrade

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

- Review the release notes 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 and later. For information, see the [VMware Compatibility Guide](#).
- Verify that the *VMware vSphere Storage APIs for Data Protection*-based backup solution that you selected is certified against vSphere 6.5 Update 1. For more information, see the compatibility matrix of your vendor.

The vSphere Data Protection product is deprecated. VMware Validated Design does not provide guidance for its usage and lifecycle management during the upgrade process.

- Review any custom integration that might have occurred outside of the VMware Validated Design framework 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 the VMware products in 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 tenants.  
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.
- Ensure that no management virtual machines or virtual appliances are running on snapshot before you perform the upgrade of the respective layer. Each layer's guidance covers the use of snapshots.
- 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 exceeding the change window.

- Consider the impact of an update or upgrade to tenant workloads.  
If you properly prepare for the upgrade, existing instances, networking, and storage must continue to operate.
- Use vSphere vMotion to temporarily migrate workloads to other compute nodes during upgrade.  
Performing an upgrade with operational workloads carries risks.
- Communicate the upgrade to your tenants so that they can plan backups.
- If possible, communicate the upgrade to your VMware Technical Account Manager and/or Global Support Service representative.

## 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. Evaluate 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 Layer

# 2

You start the upgrade from VMware Validated Design 4.1 to VMware Validated Design 4.2 by reviewing and implementing the changes to the cloud management platform layer.

This version of this validated design does not have build changes to the cloud management platform layer. Implement minor configuration changes to stay aligned with VMware Validated Design.

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

Order	Components	Sub-Component
1	vRealize Automation	vRealize Automation Appliances with Embedded vRealize Orchestrator vRealize Automation IaaS Components
2	vRealize Business for Cloud	vRealize Business Server vRealize Business Data Collectors
3	Configuration Changes	-

## Configuration Changes to the Cloud Management Layer

Perform the configuration changes to the environment according to the objectives and deployment guidelines of this validated design, ensuring that your environment remains aligned to VMware Validated Design.

### Procedure

#### 1 [Tenant User Groups, Accounts and Objects in VMware Validated Design 4.2](#)

Earlier versions of VMware Validated Design use the ITAC prefix in the names of tenant users, user groups, and inventory objects. To ensure alignment with the development and standards of the VMware Validated Design guidance, the upgrade requires certain changes.

#### 2 [Assign Tenant Administrative Roles to Local Users](#)

Add the newly-introduced local accounts for the administrators of the default tenant and of the Rainpole tenant. Assign them tenant and infrastructure administrator roles.

### 3 Assign Tenant Administrative Roles to Active Directory Users

After vRealize Automation Directories Management is associated with your Active Directory domain, domain users can administer the tenant. Assign the aligned domain user groups to tenant and infrastructure administrator roles.

### 4 Configure User Roles in vRealize Automation

You assign user roles in the context of a specific tenant. However, some roles for the default tenant can manage system-wide configuration settings that apply to multiple tenants.

### 5 Reconfigure Business Groups

Assign the group manager role for the Production and Development business groups to the ug-vra-admins user group to align the configuration of the Rainpole tenant with the new convention for the names of tenant accounts and objects.

### 6 Reconfigure Entitlements

Grant access the ug-vra-admins user group access to the single-machine blueprint entitlements for the Production and Development groups to align the Rainpole tenant configuration with the new convention for the names of tenant accounts and objects.

### 7 Clean Up Obsolete Tenant User Accounts and Groups

After you create and configure the tenant account names and objects according to the naming scheme in this version of the validated design, in the vRealize Automation portal clean up the roles and permissions assigned to the obsolete user accounts and groups. The names of the obsolete accounts and groups have the ITAC prefix.

## Tenant User Groups, Accounts and Objects in VMware Validated Design 4.2

Earlier versions of VMware Validated Design use the ITAC prefix in the names of tenant users, user groups, and inventory objects. To ensure alignment with the development and standards of the VMware Validated Design guidance, the upgrade requires certain changes.

Track the following changes in VMware Validated Design 4.2 to tenant user groups, accounts and objects in the SDDC.

**Table 2-2. Changes in Account Names in VMware Validated Design 4.2**

Name in VMware Validated Design 4.1	Name in VMware Validated Design 4.2
ITAC-LocalDefaultAdmin	vra-localdefaultadmin
ITAC-LocalRainpoleAdmin	vra-localrainpoleadmin
ITAC-TenantAdmin	vra-admin-rainpole
ITAC-Tenantarchitect	vra-arch-rainpole

**Table 2-3. Changes in User Group Names in VMware Validated Design 4.2**

Name in VMware Validated Design 4.1	Name in VMware Validated Design 4.2
ug-ITAC-TenantAdmins	ug-vra-admins-rainpole
ug-ITAC-TenantArchitects	ug-vra-archs-rainpole

**Table 2-4. Changes in Customization Specifications in VMware Validated Design 4.2**

Name in VMware Validated Design 4.1	Name in VMware Validated Design 4.2
itac-linux-custom-spec	os-linux-custom-spec
itac-windows-joindomain-custom-spec	os-windows-joindomain-custom-spec

## Assign Tenant Administrative Roles to Local Users

Add the newly-introduced local accounts for the administrators of the default tenant and of the Rainpole tenant. Assign them tenant and infrastructure administrator roles.

### 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	<i>vra_administrator_password</i>
Domain	vsphere.local

- 2 On the **Tenants** page, click the default tenant vsphere.local to edit its settings.
- 3 On the **Local users** tab, click **New** to add a local user to the default tenant.
- 4 In the **User Details** dialog box, specify the following settings, click **OK**, and click **Next**.

Setting	Value
First name	vRA
Last name	LocalDefaultAdmin
Email	vra-localdefaultadmin@vsphere.local
User name	vra-localdefaultadmin
Password	<i>vra-localdefaultadmin_password</i>
Confirm password	<i>vra-localdefaultadmin_password</i>

- 5 On the **Administrators** tab, specify tenant and infrastructure administrators.
  - a In the **Tenant administrators** search text box, enter `vra-localdefaultadmin` and press Enter.
  - b In the **laaS administrators** search text box, enter `vra-localdefaultadmin` and press Enter.
  - c Click **Finish**.
- 6 On the **Tenants** page, click the **Rainpole** tenant to edit its settings.
- 7 On the **Local users** tab, click **New** to add a local user to the default tenant.
- 8 In the **User Details** dialog box, specify the following settings, click **OK**, and click **Next**.

Setting	Value
First name	vRA
Last name	LocalRainpoleAdmin
Email	vra-localrainpoleadmin@vsphere.local
User name	vra-localrainpoleadmin
Password	<i>vra-localrainpoleadmin_password</i>
Confirm password	<i>vra-localrainpoleadmin_password</i>

- 9 On the **Administrators** tab, specify tenant and infrastructure administrators.
  - a In the **Tenant administrators** search text box, enter `vra-localrainpoleadmin` and press **Enter**.
  - b In the **laaS administrators** search text box, enter `vra-localrainpoleadmin` and press **Enter**.
  - c Click **Finish**.
- 10 Log out of the vRealize Automation portal

## Assign Tenant Administrative Roles to Active Directory Users

After vRealize Automation Directories Management is associated with your Active Directory domain, domain users can administer the tenant. Assign the aligned domain user groups to tenant and infrastructure administrator roles.

### 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	vra-localrainpoleadmin
Password	<i>vra-localrainpoleadmin_password</i>
Domain	vsphere.local

- 2 Navigate to **Administration > Directories Management > Directories**.
  - 3 Click the **rainpole.local** directory.
  - 4 On the **Settings** tab for the rainpole.local directory, click **Sync Settings**.
  - 5 On the **Groups** tab, under **Specify the group DNs**, click **Select** next to the **dc=local,dc=rainpole** text box.
  - 6 Select the following groups and click **Save & Sync**.
    - ug-vra-admins-rainpole
    - ug-vra-archs-rainpole
  - 7 Log out of the vRealize Automation portal
  - 8 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  | <i>vra_administrator_password</i> |
| Domain    | vsphere.local                     |
- 9 On the **Tenants** page, click the **Rainpole** tenant to edit its settings.
  - 10 On the **Administrators** tab, assign domain user groups for tenant and infrastructure administrators.
    - a Enter **ug-vra-admins-rainpole** in the Tenant administrators search text box and press Enter.
    - b Enter **ug-vra-admins-rainpole** in the IaaS administrators search text box and press Enter.
  - 11 Log out of the vRealize Automation portal.

## Configure User Roles in vRealize Automation

You assign user roles in the context of a specific tenant. However, some roles for the default tenant can manage system-wide configuration settings that apply to multiple tenants.

Roles are sets of privileges that you associate with users to determine what tasks they can perform. Based on their responsibilities, individuals might have one or more roles associated with their user account.

You assign tenant architect and administrator roles to the **ug-vra-admins-rainpole** and **ug-vra-archs-rainpole** user groups.

**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	vra-admin-rainpole
Password	<i>vra-admin-rainpole_password</i>
Domain	rainpole.local

- 2 On the **Administration** tab, navigate to **Users & Groups > Directory Users and Groups**.

- 3 Enter **ug-vra-admins-rainpole** in the search box and press Enter.

The ug-vra-admins-rainpole (ug-vra-admins-rainpole@rainpole.local) group name appears in the **Name** text box.

- 4 Click the **ug-vra-admins-rainpole (ug-vra-admins-rainpole@rainpole.local)** user group.

- 5 In the **Add Roles to this Group** list, select the following roles, and click **Finish**.

- Application Architect
- Approval Administrator
- Business Management Administrator
- Container Administrator
- Container Architect
- Infrastructure Architect
- Software Architect
- Tenant Administrator
- XaaS Architect

- 6 Search for **ug-vra-archs-rainpole** in the **Tenant Administrators** search box .

The ug-vra-archs-rainpole (ug-vra-archs-rainpole@rainpole.local) group appears in the **Name** text box.

- 7 Click the **ug-vra-archs-rainpole (ug-vra-archs-rainpole@rainpole.local)** user group.

- 8 In the **Add Roles to this Group** list, select the following user groups, and click **Finish**.

- Application Architect
- Container Architect
- Infrastructure Architect
- Software Architect

- XaaS Architect

## Reconfigure Business Groups

Assign the group manager role for the Production and Development business groups to the ug-vra-admins user group to align the configuration of the Rainpole tenant with the new convention for the names of tenant accounts and objects.

### 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	vra-admin-rainpole
Password	vra-admin-rainpole_password
Domain	rainpole.local

- 2 Navigate to **Administration > Users and Groups > Business Groups**.
- 3 Click **Production**.
- 4 On the **General** tab, change the value in the **Send manager emails to** text box to **vra-admin-rainpole@rainpole.local**.
- 5 On the **Members** tab, assign the group manager role to the ug-vra-admins user group.
  - a Under **Group manager role**, remove **ug-ITAC-TenantAdmins (ug-ITAC-TenantAdmins@rainpole.local)**.
  - b Enter **ug-vra-admins-rainpole** in the **Group manager role** text box and click **Finish**.
- 6 Repeat [Step 3](#) to [Step 5](#) for the Development business group

## Reconfigure Entitlements

Grant access the ug-vra-admins user group access to the single-machine blueprint entitlements for the Production and Development groups to align the Rainpole tenant configuration with the new convention for the names of tenant accounts and objects.

**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	vra-admin-rainpole
Password	vra-admin-rainpole_password
Domain	rainpole.local

- 2 Click the **Administration** tab, and click **Catalog Management > Entitlements**.
- 3 Click **Prod-SingleVM-Entitlement**.  
The **Edit Entitlement** page appears.
- 4 On the **Edit Entitlement** page, replace the obsolete administrator user group for the Rainpole tenant with the new group.
  - a Remove **ug-ITAC-TenantAdmins (ug-ITAC-TenantAdmins@rainpole.local)**
  - b Enter **ug-vra-admins-rainpole** in the **Users & Groups** text box and press Enter.
  - c Click **Finish**
- 5 Repeat [Step 3](#) and [Step 4](#) for Dev-SingleVM-Entitlement.

## Clean Up Obsolete Tenant User Accounts and Groups

After you create and configure the tenant account names and objects according to the naming scheme in this version of the validated design, in the vRealize Automation portal clean up the roles and permissions assigned to the obsolete user accounts and groups. The names of the obsolete accounts and groups have the ITAC prefix.

**Procedure**

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

Setting	Value
User name	administrator
Password	vra_administrator_password
Domain	vsphere.local

- 2 On the **Tenants** page, click the **Rainpole** tenant to edit its settings.

- 3 To remove the obsolete administrator account of the Rainpole tenant from the local user accounts, on the **Local Users** tab, select the **ITAC-LocalRainpoleAdmin** and delete it.
- 4 Remove the tenant administrator and IaaS administrator roles from the obsolete tenant administrator account.
  - a Click the **Administrators** tab.
  - b In the **Tenant administrators** table, place your mouse over **ug-ITAC-TenantAdmins**.
  - c Click the delete icon that appears next to **ug-ITAC-TenantAdmins**.
  - d In the **IaaS administrators** table, place your mouse over **ug-ITAC-TenantAdmins**.
  - e Click the delete button that appears next to **ug-ITAC-TenantAdmins**.
  - f Click **Finish**.
- 5 Log in to the vRealize Automation Rainpole portal.
  - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
  - b Log in using the following credentials.

Setting	Value
User name	vra-localrainpoleadmin
Password	vra-localrainpoleadmin_password
Domain	vsphere.local

- 6 Disable the privileged access of the obsolete tenant administrator account.
  - a On the **Administration** tab, navigate to **Users & Groups > Directory Users and Groups**.
  - b Enter **ug-ITAC-TenantAdmins** in the search box and press Enter.  
 The **ug-ITAC-TenantAdmins (ug-ITAC-TenantAdmins@rainpole.local)** group name appears in the **Name** text box.
  - c Click **ug-ITAC-TenantAdmins(ug-ITAC-TenantAdmins@rainpole.local)**.
  - d In the **Add Roles to this Group** list, deselect the following roles and click **Finish**.
    - Application Architect
    - Approval Administrator
    - Business Management Administrator
    - Container Administrator
    - Container Architect
    - Infrastructure Architect
    - Software Architect
    - XaaS Architect

7 Disable the privileged access of the obsolete tenant architect account.

a On the **Administration** tab, navigate to **Users & Groups > Directory Users and Groups**.

b Enter **ug-ITAC-TenantArchitects** in the search box and press Enter.

The ug-ITAC-TenantArchitects (ug-ITAC-TenantArchitects@rainpole.local) group name appears in the **Name** text box.

c Click **ug-ITAC-TenantArchitects (ug-ITAC-TenantArchitects@rainpole.local)** .

d In the **Add Roles to this Group** list, deselect the following roles and click **Finish**.

- Application Architect
- Container Architect
- Infrastructure Architect
- Software Architect
- XaaS Architect

# Upgrade the Operations Management Layer

# 3

After you upgrade the cloud management layer, upgrade vRealize Operations Manager and vRealize Log Insight which are the components of the operations management layer 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	Reconfiguration of vRealize Operations Manager	-
2	vRealize Log Insight	vRealize Log Insight Appliances vRealize Log Insight Agents
3	Post-Upgrade Reconfiguration of vRealize Log Insight	-

- [Configuration Changes of vRealize Operations Manager](#)

Perform the configuration changes to the environment according to the objectives and deployment guidelines of this validated design so that your environment remains aligned with VMware 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 and have an environment that is compliant with VMware Validated Design for Software-Defined Data Center 4.2.

## Configuration Changes of vRealize Operations Manager

Perform the configuration changes to the environment according to the objectives and deployment guidelines of this validated design so that your environment remains aligned with VMware Validated Design.

## Procedure

### 1 [Disable the vSAN Dashboards of the Management Pack for Storage Devices in Region A](#)

Use the vRealize Operations Management Pack for Storage Devices to monitor fabric-based storage such as the NFS datastores in this validated design. To monitor the vSAN datastores for the management applications, disable the vSAN dashboards of management pack for Storage Devices and use the dashboards of the vRealize Operations Management Pack for vSAN. The management pack for vSAN comes pre-installed with vRealize Operations Manager.

### 2 [Define a User Role in vSphere for vCenter Adapters in vRealize Operations Manager in Region A](#)

In vSphere, create a user role with privileges that are required to query information from vCenter Server and receive metric data in vRealize Operations Manager. In vRealize Operations Manager, you can also run actions or tasks on the objects it manages in vCenter Server. Add the privileges to the role that are required for typical virtual machine lifecycle operations, such as snapshot management and virtual machine resource configuration.

## Disable the vSAN Dashboards of the Management Pack for Storage Devices in Region A

Use the vRealize Operations Management Pack for Storage Devices to monitor fabric-based storage such as the NFS datastores in this validated design. To monitor the vSAN datastores for the management applications, disable the vSAN dashboards of management pack for Storage Devices and use the dashboards of the vRealize Operations Management Pack for vSAN. The management pack for vSAN comes pre-installed with vRealize Operations Manager.

### Procedure

#### 1 Log in to vRealize Operations Manager by using Secure Shell (SSH) client.

- a Open an SSH connection to vrops01svr01a.rainpole.local.
- b Log in using the following credentials.

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

#### 2 Disable the vSAN dashboards provided by the vRealize Operations Manager Management Pack for Storage Devices by running the following commands.

```
cd /usr/lib/vmware-vcops/tools/opscli
$VMWARE_PYTHON_BIN ./ops-cli.py dashboard hide all 'VirtualSAN Heatmap'
$VMWARE_PYTHON_BIN ./ops-cli.py dashboard hide all 'VirtualSAN Entity Usage'
$VMWARE_PYTHON_BIN ./ops-cli.py dashboard hide all 'VirtualSAN Cluster Insights'
$VMWARE_PYTHON_BIN ./ops-cli.py dashboard hide all 'VirtualSAN Device Insights'
$VMWARE_PYTHON_BIN ./ops-cli.py dashboard hide all 'VirtualSAN Troubleshooting'
```

- 3 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	<i>vrops_admin_password</i>

- 4 On the main navigation bar, click **Dashboards** and verify that the following dashboards are no longer visible.
  - VirtualSAN Heatmap
  - VirtualSAN Entity Usage
  - VirtualSAN Cluster Insights
  - VirtualSAN Device Insights
  - VirtualSAN Troubleshooting

## Define a User Role in vSphere for vCenter Adapters in vRealize Operations Manager in Region A

In vSphere, create a user role with privileges that are required to query information from vCenter Server and receive metric data in vRealize Operations Manager. In vRealize Operations Manager, you can also run actions or tasks on the objects it manages in vCenter Server. Add the privileges to the role that are required for typical virtual machine lifecycle operations, such as snapshot management and virtual machine resource configuration.

### 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	<i>vsphere_admin_password</i>

- 2 On the **Home** page of the vSphere Web Client, click **Roles** under **Administration**.

- 3 Create a role for collecting data from and performing actions on vCenter Server.
  - a On the **Roles** page, click the **Create role action** icon.
  - b In the **Create Role** dialog box, configure the role using the following configuration settings, and click **OK**.

Setting	Value
Role name	vSphere Actions User
Privilege	<ul style="list-style-type: none"> <li>■ <b>Virtual Machine.Configuration.Change CPU Count</b></li> <li>■ <b>Virtual Machine.Configuration. Change Resource</b></li> <li>■ <b>Virtual Machine.Configuration. Memory</b></li> <li>■ <b>Virtual Machine.Interaction. Power Off</b></li> <li>■ <b>Virtual Machine.Interaction. Power On</b></li> <li>■ <b>Virtual Machine.Snapshot Management. Create Snapshot</b></li> <li>■ <b>Virtual Machine.Snapshot Management. Remove Snapshot</b></li> </ul>

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

The Management vCenter Server in Region A propagates the role to the other linked vCenter Server instances.

- 4 Update the permissions of the svc-vrops-vsphere service account.
  - a In the **Navigator** pane, under **Access Control**, click **Global Permissions**.
  - b Select the svc-vrops-vsphere service account and click **Edit**.
  - c In the **Global Permissions Root – Change Role On Permissions** dialog box, under **Assigned Role**, select **vSphere Actions User**.
  - d Verify that **Propagate to children** is selected and click **OK**.

## 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 and have an environment that is compliant with VMware Validated Design for Software-Defined Data Center 4.2.

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.

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 3-3. vRealize Log Insight Nodes in the SDDC**

Region	Role	IP Address	FQDN
Region A	Integrated load balancer VIP	192.168.31.10	sfo01vrli01.sfo01.rainpole.local
	Master node	192.168.31.11	sfo01vrli01a.sfo01.rainpole.local
	Worker node 1	192.168.31.12	sfo01vrli01b.sfo01.rainpole.local
	Worker node 2	192.168.31.13	sfo01vrli01c.sfo01.rainpole.local
	Worker node x	192.168.31.x	sfo01vrli01x.sfo01.rainpole.local
Region B	Integrated load balancer VIP	192.168.32.10	lax01vrli01.lax01.rainpole.local
	Master node	192.168.32.11	lax01vrli01a.lax01.rainpole.local
	Worker node 1	192.168.32.12	lax01vrli01b.lax01.rainpole.local
	Worker node 2	192.168.32.13	lax01vrli01c.lax01.rainpole.local
	Worker node x	192.168.32.x	lax01vrli01x.lax01.rainpole.local

**Prerequisites**

- Download the vRealize Log Insight product upgrade `VMware-vRealize-Log-Insight-4.5.1-xxxxxxx.pak` files for the appropriate version(s) on the Windows host that has access to the data center.

**Table 3-2. PAK Files That Are Required for vRealize Log Insight Upgrade**

PAK Type	PAK File
Software update .pak file for version 4.5.1	VMware-vRealize-Log-Insight-4.5.1-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 nodes, upgrade the content packs in the environment to take advantage of the latest features of the packs while monitoring the environment.

**4 Delete the Snapshots of the vRealize Log Insight Appliances**

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

## 5 Post-Upgrade Configuration of the vRealize Log Insight

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

### What to do next

- Verify that vRealize Log Insight 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 3-4. 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
	sfo01-m01fd-vrli	Worker Node 1	lax01vrli01b
	sfo01-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 4.2 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.

**Table 3-5. Upgrade Path for vRealize Log Insight**

Upgrade From	Upgrade To	PAK File
vRealize Log Insight 4.5	vRealize Log Insight 4.5.1	VMware-vRealize-Log-Insight-4.5.1-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	<a href="https://sfo01vrli01.sfo01.rainpole.local">https://sfo01vrli01.sfo01.rainpole.local</a>
Region B	<a href="https://lax01vrli01.lax01.rainpole.local">https://lax01vrli01.lax01.rainpole.local</a>

- b Log in using the following credentials.

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

- 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 Available, repeat this process using the vRealize Log Insight .pak file for the second increment.
- 10 Repeat the upgrade on the cluster in Region B.

## Upgrade the Content Packs on vRealize Log Insight

After upgrading the vRealize Log Insight nodes, 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	<i>vrli_admin_password</i>

- 2 Click the configuration drop-down menu icon  and select **Content Pack**.
- 3 In the **Content Pack** pane, under **Content Pack Market Place**, click **Updates**.
- 4 In the **Log Insight Content Pack Marketplace** pane, click **Update All** to upgrade all content packs to 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>.

## 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 3-6. 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
	sfo01-m01fd-vrli	Worker Node 1	lax01vrli01b
	sfo01-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 vRealize Log Insight components of the SDDC, configure the environment according to the objectives and deployment guidelines of this validated design.

### Procedure

#### 1 [Rename Agent Groups in vRealize Log Insight](#)

In the VMware Validated Design 4.2, to simplify the Agent Groups for future compatibility, the naming convention has been updated for both Region A and Region B.

#### 2 [Configure Privileges for the Service Account for vRealize Log Insight in vSphere](#)

In this version of VMware Validated Design, all service account names are aligned to a naming convention where the account name indicates the direction of application-to-application communication. Assign vCenter Single Sign-On administrative global permissions to the new service account svc-vrli-vsphere so that you can receive log information from vSphere in vRealize Log Insight in Region A and Region B.

#### 3 [Update vRealize Log Insight with the New Service Account](#)

After you configure the svc-vrli-vsphere Active Directory user with the vSphere privileges that are required for retrieving log information from the vCenter Server instances and ESXi hosts, re-connect vRealize Log Insight to vSphere by using the svc-vrli-vsphere service account.

### Rename Agent Groups in vRealize Log Insight

In the VMware Validated Design 4.2, to simplify the Agent Groups for future compatibility, the naming convention has been updated for both Region A and Region B.

Update the agent group names within vRealize Log Insight to remain aligned to the VMware Validated Design.

Region	URL	Old Agent Group Name	New Agent Group Name
Region A	https://sfo01vrli01.sfo01.rainpole.local	vROps6 - Agent Group	vROPs - Appliance Agent Group
		vRA7 - Windows Agent Group	vRA - Windows Agent Group
		vRA7 - Linux Agent Group	vRA - Appliance Agent Group
		vRA7 - Microsoft SQL Server Agent Group	vRA - SQL Agent Group
		vRO7 - Agent Group	vRO - Appliance Agent Group
		vAppliances - Agent Group	VA - Linux Agent Group
Region B	https://lax01vrli01.lax01.rainpole.local	vROps6 - Agent Group	vROPs - Appliance Agent Group
		vRA7 - Windows Agent Group	vRA - Windows Agent Group
		vAppliances - Agent Group	VA - Linux Agent Group

**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	<a href="https://sfo01vrli01.sfo01.rainpole.local">https://sfo01vrli01.sfo01.rainpole.local</a>
Region B	<a href="https://lax01vrli01.lax01.rainpole.local">https://lax01vrli01.lax01.rainpole.local</a>

- b Log in using the following credentials.

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

- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Management**, click **Agents**.
- 4 In the **All Agents** drop-down menu, select the **vROps6 - Agent Group** agent group and click the pencil icon to edit it.
- 5 In the **Edit Agent Group** dialog, change the Name field from **vROps6 - Agent Group** to **vROPs - Appliance Agent Group**, and click **Save**.
- 6 Repeat the procedure for the remaining Agent Groups in Region A and the Agent Groups in Region B.

## Configure Privileges for the Service Account for vRealize Log Insight in vSphere

In this version of VMware Validated Design, all service account names are aligned to a naming convention where the account name indicates the direction of application-to-application communication. Assign vCenter Single Sign-On administrative global permissions to the new service account `svc-vrli-vsphere` so that you can receive log information from vSphere in vRealize Log Insight in Region A and Region B.

**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	<i>vsphere_admin_password</i>

- 2 From the **Home** menu, select **Administration**.
- 3 In the vSphere Web Client, select **Administration** from the **Home** menu and click **Users and Groups** under **Users and Groups**.
- 4 On the **Groups** tab, click the **Administrators** group and click the **Add Member** icon under **Group Members**.
- 5 In the **Add Principals** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc**, and press Enter.
- 6 From the list of users and groups, select the **svc-vrli-vsphere** user, click **Add**, and click **OK**.

The global vCenter Single Sign-On administrative permissions of the svc-vrli-vsphere account propagate to all other linked vCenter Server instances.

## Update vRealize Log Insight with the New Service Account

After you configure the svc-vrli-vsphere Active Directory user with the vSphere privileges that are required for retrieving log information from the vCenter Server instances and ESXi hosts, re-connect vRealize Log Insight to vSphere by using the svc-vrli-vsphere service account.

### 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	<i>vrli_admin_password</i>

- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Integration**, click **vSphere**.

- 4 In the **vCenter Servers** pane, update the service account for connection to the vCenter Server instances in the region.
- a Update the user name to `svc-vrli-vsphere@rainpole.local`, click **Update Password** and then click **Test Connection**.

vCenter Server Option	Value
Hostname	<ul style="list-style-type: none"> <li>■ sfo01m01vc01.sfo01.rainpole.local for Management vCenter Server</li> <li>■ sfo01w01vc01.sfo01.rainpole.local for Compute vCenter Server</li> </ul>
Username	<b>svc-vrli-vsphere@rainpole.local</b>
Password	<i>svc-vrli-vsphere_user_password</i>
Collect vCenter Server events, tasks and alarms	Selected
Configure ESXi hosts to send logs to Log Insight	Selected

- b Click **View Details** and examine the list of ESXi hosts that are connected to the vCenter Server instance to verify that they are still connected to the correct vCenter Server.
- c In the **Advanced Options** configuration window, select **Automatically configure all ESXi hosts**, select **UDP** under **Syslog protocol**, and click **OK**.
- 5 Repeat the steps to update the settings for the second vCenter Server instance in Region A.
- 6 Click **Save**.

A progress dialog box appears.

- 7 Click **OK** in the confirmation dialog box that appears after vRealize Log Insight contacts the vCenter Server instances.
- 8 Repeat the procedure for Region B using the following information.

vCenter Server Option	Value
Hostname	<ul style="list-style-type: none"> <li>■ lax01m01vc01.lax01.rainpole.local for Management vCenter Server</li> <li>■ lax01w01vc01.lax01.rainpole.local for Compute vCenter Server</li> </ul>
Username	<b>svc-vrli-vsphere@rainpole.local</b>
Password	<i>svc-vrli-vsphere_user_password</i>
Collect vCenter Server events, tasks and alarms	Selected
Configure ESXi hosts to send logs to Log Insight	Selected

You see the vSphere dashboards under the **VMware - vSphere** content pack dashboard category.

# Upgrade the Virtual Infrastructure and Business Continuity Layers

# 4

After you upgrade the cloud management platform layer and operations management layer, you must upgrade the components of the virtual infrastructure and business continuity layers of the SDDC.

## Procedure

### 1 [Review and Update vSphere Storage APIs for Data Protection Based Backup Solution](#)

Before you upgrade the vSphere components in the virtual infrastructure layer, verify that the backup solution that is based on vSphere Storage APIs for Data Protection (VADP) in your organization is compatible with version 4.2 of VMware Validated Design.

### 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 Layer](#)

After you upgrade all virtual infrastructure layer, perform global post-upgrade configuration according to address the dependencies between these components and to align your environment to the guidance in this validated design.

### 6 [Post-Upgrade Configuration of the Business Continuity Layer for the Management Cluster](#)

After you upgrade the business continuity and virtual infrastructure layers of the SDDC, configure the environment according to the objectives and deployment guidelines of this validated design.

**Table 4-1. VMware Validated Design Upgrade Sequence for the Virtual Infrastructure and Business Continuity Layers**

Order	Component	Sub-Component
1	Backup solution based on VMware vSphere Storage APIs	-
2	NSX for vSphere	NSX Manager instances
		NSX Controller instances
		NSX Networking Fabric
		NSX Edges
3	Post-upgrade reconfiguration for virtual infrastructure (networking)	-
4	Platform Services Controller instances	-
	vCenter Server	-
5	Post-upgrade reconfiguration for virtual infrastructure (compute infrastructure)	-
6	vSphere Update Manager Download Service	-
7	ESXi	-
8	Post-upgrade reconfiguration for virtual infrastructure (compute infrastructure)	-

## Review and Update vSphere Storage APIs for Data Protection Based Backup Solution

Before you upgrade the vSphere components in the virtual infrastructure layer, verify that the backup solution that is based on vSphere Storage APIs for Data Protection (VADP) in your organization is compatible with version 4.2 of VMware Validated Design.

Perform the upgrade outside of the usual backup windows.

### Prerequisites

- Ensure that VADP-based Backup Solution is compatible with vSphere 6.5 Update 1 and later. See the *VMware Validated Design Release Notes* for version 4.2 for specific versions.
- Ensure that any customization or integration that might have been configured outside of what is prescribed in VMware Validated Design with the VADP-based Backup Solution has been validated by the vendor and is compatible with the backup solution, for example, backup integration for vRealize Automation blueprints.
- Engage your backup solution vendor or team to verify that the system is fully operational and compatible with any other clients, such as reporting tools, Web browser, and so on.
- Allocate adequate time for the duration of maintenance window before starting the upgrade. Engage your backup vendor to get an estimate on the upgrade duration.

- Verify that no alarms on the backup solution exist in both the vSphere Web Client and the management interface of the solution.

#### What to do next

- Verify that backup solution functions flawlessly after the upgrade. Consult the documentation of the backup vendor for details on operational verification.

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

When you upgrade the 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 paired NSX Manager instances for Cross-vCenter networking and security, the NSX Controller nodes, the ESXi VIBs, and the NSX Edge devices, starting with the universal distributed logical routers. This upgrade operation is split between the management cluster pairs and the shared edge and compute cluster pairs.

You might perform the upgrades of these components in different maintenance windows.

**Table 4-2. NSX 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	-

**Table 4-2. NSX Nodes in the SDDC (Continued)**

Region	Role	IP Address	FQDN
Region B	NSX Manager for the management cluster that is running as secondary	172.17.11.65	lax01m01nsx01.lax01.rainpole.local
	NSX Manager for the shared edge and compute cluster that is running as secondary	172.17.11.66	lax01w01nsx01.lax01.rainpole.local

**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-6.4.x-xxxxxxx.tar.gz` on the Windows host that has access to your data center.
- Review [Operational Impacts of NSX Upgrade](#) in *NSX Upgrade Guide* to understand the impact that each component might have on your VMware Validated Design environment.
- Review [Upgrade NSX in a Cross-vCenter NSX Environment](#) and [Upgrade NSX Using Upgrade Coordinator](#) in *NSX Upgrade Guide* to understand the complete list of prerequisites required and the detailed upgrade guidance provided to 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; 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 to the NSX Manager instance you are upgrading using the **admin** account and run the `show filesystems` command to show the filesystem usage.
  - b If the filesystem usage is at 100 percent, enter Privileged mode and clear the logs by running the following commands.

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

- c Reboot the NSX Manager appliance for the log cleanup to take effect.
- Back up the NSX configuration and download technical support logs before upgrading.

- Take a backup of the NSX Manager pair, both primary and secondary instances, and of the NSX Controller virtual machines. For more information, see [Back Up and Restore NSX Manager](#) in *NSX Upgrade Guide*.
- Verify that all of the controllers are in normal, connected state .
- Verify that **Host Preparation > Installation Status** of all clusters has the green check mark and the proper NSX version.
- Get the current version of the NSX VIBs on the hosts in the management cluster and in the shared edge and compute cluster.
  - a Log in to one of the hosts in the cluster by using the ESXi Host Client.
  - b Select **Host > Manage**.
  - c On the **Packages** tab, search for **esx-n**.
  - d Note the current version of the following VIB.
    - esx-nsxv

## Procedure

### 1 [Upgrade the NSX Manager Instances](#)

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

### 2 [Upgrade the NSX Controller Instances](#)

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. You upgrade the controllers immediately after the upgrade of the connected NSX Manager instance to keep their versions identical.

### 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, upgrade the NSX Edge services gateway, universal distributed logical router and load balancer instances.

## 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. You must upgrade the primary and all secondary NSX Manager instances to the same NSX version in the same maintenance window. However, you can perform the upgrade of the management clusters and the shared edge and compute clusters in the same or separate maintenance windows.

**Table 4-3. NSX Manager Nodes in the SDDC**

Order	Region	NSX Manager Instance	NSX Appliance URL	vCenter Server URL
1	Region A	NSX Manager for the management cluster that is primary	https://sfo01m01nsx01.sfo01.rainpole.local	sfo01m01vc01.sfo01.rainpole.local
2	Region B	NSX Manager for the management cluster that is 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 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	<i>nsx_manager_admin_password</i>

- 2 Click **Upgrade** and on the **Upgrade** page, click **Upload Bundle**.
- 3 In the **Upgrade** dialog box, locate the `VMware-NSX-Manager-upgrade-bundle-6.4.x-build_number.tar.gz` upgrade bundle in your file system.
- 4 Click **Open** and click **Continue**.  
The NSX Manager starts uploading the bundle.
- 5 After the upload is complete, in the **Upgrade** dialog box, configure the following settings and click **Upgrade**.

Setting	Value
Do you want to enable SSH?	Yes
Do you want to join the VMware Customer Experience Program	Yes

- 6 Log in to the Management NSX Manager appliance user interface.
  - a Open a Web browser and go to **https://sfo01m01nsx01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

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

- 7 Verify that the **Upgrade** tab shows the following configuration.

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

- 8 Wait for the you upgrade to complete.
- 9 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

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

- 10 In the vSphere Web Client, check for the latest NSX plug-in.
  - a From the **Home** menu, select **Administration**.
  - b In the **Navigator** pane, under **Solutions**, click **Client Plug-Ins**.
  - c On the **Client Plug-Ins** page, click **Check for New Plug-ins**.
  - d In the pop-up window **Checking for New Plug-ins** at the bottom, click **Go to the Event Console**.
  - e In the **Events Console**, enter **plug-in** in the filter.

Two events have recently occurred.

The deployment of plug-in NSX user interface plugin 6.4.0.xxxxxxx has started  
The deployment of plug-in NSX user interface plugin 6.4.0.xxxxxxx is successful

- f Log out from and back in to the vSphere Web Client, navigate back to the **Client Plug-Ins** page, and verify that the **vShield Manager Version** has been updated to 6.4.0.
- 11 Perform a fresh backup of the primary NSX Manager because the old backups can not be restored to the new NSX Manager version.

- 12 Repeat the steps for the secondary NSX Manager lax01m01nsx01.lax01.rainpole.local to complete the NSX Manager upgrade in the management cluster.
- 13 Repeat the procedure for the shared edge and compute cluster.

You start with the primary NSX Manager sfo01w01nsx01.sfo01.rainpole.local and complete the upgrade with the secondary NSX Manager lax01w01nsx01.lax01.rainpole.local.

## Upgrade the NSX Controller Instances

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. You upgrade the controllers immediately after the upgrade of the connected NSX Manager instance to keep their versions identical.

Since version 6.4.0 of NSX for vSphere, you can use the Upgrade Coordinator functionality to orchestrate the upgrade of each component in the NSX deployment. You can specify individual components or string multiple components together in an automated fashion and adjust the number of components to be upgraded according to the size of the maintenance window.

For VMware Validated Design, you upgrade each component one-by-one so that you can have as high level of control as possible on the upgrade. For information about upgrading multiple components during the same maintenance window, see *Upgrade NSX Using Upgrade Coordinator* in the [NSX Upgrade Guide](#).

For each NSX Manager instance that has the primary role, you start an upgrade of the connected NSX Controller cluster. You upgrade the NSX Controller cluster for the management cluster in Region A first. Repeat the upgrade procedure on the NSX Controller cluster for the shared edge and compute cluster in Region A. You can perform these operations in the same or separate maintenance windows but you must do the upgrade immediately after the upgrade of the connected NSX Manager.

**Table 4-4. NSX Controller Nodes in Region A**

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

## Procedure

- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Networking & Security**.
- 3 In the **Navigator** pane, under **Networking & Security**, click **Installation and Upgrade**.
- 4 On the **Upgrade** tab, select the **172.16.11.65 | Primary** NSX Manager instance from the drop-down menu.
- 5 Click **Plan Upgrade** in the central pane.
- 6 On the **Select Upgrade Plan** page of the **Upgrade Components** wizard, click **Plan Your Upgrade** and click **Next**.
- 7 On the **Plan Content** page, configure the following settings and click **Next**.

Setting		Value
Select Components	Clusters	Deselected
	Universal Logical Routers	Deselected
	NSX Edges	Deselected
	Service VMs	Deselected
Define Pause Upgrade Options	Pause between components	Enabled
	Pause on error	Enabled

- 8 On the **Review Plan** page, verify that **Pause between components** and **Pause on error** are set to Yes, and click **Start Upgrade**.
- 9 During the upgrade of the NSX Controller nodes, monitor the progress by using the following means.
  - **Upgrade tab**  
Click **View Details**. The **Upgrade Plan Progress** dialog box shows the overall progress of the controller upgrade. Click the **Details** button for additional information about each step.
  - **Management tab**  
The **Status** column changes from Connected, at which point once the Controller has been upgraded, the status will turn to Disconnected, at which point the Controller is back in the list and upgraded, and finally to Connected once again.

The **Upgrade Status** column shows the following stages:

- 1 Not Started
- 2 Downloading Upgrade File
- 3 Download complete
- 4 Queued For Upgrade
- 5 Upgrade in progress for each NSX controller.

---

**Note** During this time, the other controllers might be in different states.

---

- 6 Waiting to Rebooting
- 7 Rebooting
- 8 Upgraded

- 10** After the upgrade is complete for each NSX Controller, on the **Management** tab, confirm that all are connected to the NSX Manager, and in the **NSX Controller nodes** section verify that the upgraded NSX Controller has the following configuration.

Setting	Expected Value
Status	Connected
Software Version	6.4.build_number

- 11** After the upgrade is complete for all NSX Controllers, on the **Upgrade** tab, click **Resume**.
- 12** After the upgrade of the NSX Controller cluster of the management cluster is complete, repeat the procedure 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 first.

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

Region	NSX Manager	NSX Manager IP Address	Host Cluster
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

**Table 4-5. NSX Manager Instances and Associated Host Clusters (Continued)**

Region	NSX Manager	NSX Manager IP Address	Host Cluster
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 Upgrade**.
- 4 Click the **Upgrade** tab, select the **172.16.11.65 | Primary** NSX Manager instance from the drop-down menu.
- 5 Click **Plan Upgrade** in the central pane.
- 6 On the **Select Upgrade Plan** page of the **Upgrade Components** wizard, click **Plan Your Upgrade** and click **Next**.
- 7 On the **Plan Content** page, configure the following settings and click **Next**.

Setting	Value
Select Components	Universal Logical Routers Deselected
	NSX Edges Deselected
	Service VMs Deselected

Setting	Value	
Define Pause Upgrade Options	Pause between components	Enabled
	Pause on error	Enabled

- 8 On the **Plan Host Clusters** page, select the **Default Cluster Upgrade Group** radio button, and click **Edit**.
- 9 In the Edit Upgrade Group dialog box, verify that the following settings are configured, click **OK**, and on the **Plan Host Clusters** page click **Next**.

Setting	Expected Value
Selected Objects	sfo01-m01-mgmt01
Upgrade order	Serial

- 10 On the **Review Plan** page, verify that **Pause between components** and **Pause on error** are set to Yes, and click **Start Upgrade**.
- 11 Revalidate that the NSX Controllers are of version *6.4.build\_number*, and click **Resume** to proceed to the upgrade of the next cluster.
- 12 Monitor the progress by using the following means.

- **Upgrade tab**

Click **View Details**. The **Upgrade Plan Progress** dialog box shows the overall progress of the cluster upgrade. Click the **Details** button for additional information about each step.

- **Host Preparation tab**

The **Installation Status** changes to In Progress while each of the ESXi host is updated. Each host is placed to maintenance mode with its virtual machines migrated from the host, and updated.

- 13 Wait for the update of each ESXi host in the management cluster in Region A.  
After the update of all hosts is completed, they are in a ready state, indicated by a green check mark, with a VIB version of *6.4.0.build\_number*.
- 14 After the upgrade is complete for the management cluster in Region A, click **Resume**.
- 15 Repeat the steps to update the NSX components on the other clusters in Region A and Region B.

When you perform the upgrade on a secondary node in Region B, when prompted, provide the following user name and password in the **Enter Secondary Manager Credentials** dialog box and click **OK**.

Setting	Value
User name	svc-nsxmanager@rainpole.local
Password	svc-nsxmanager_user_password

## Upgrade NSX Edge Instances

After you upgrade the control and data plane of the NSX core components, upgrade the NSX Edge services gateway, universal distributed logical router and load balancer instances.

For each NSX Manager instance in Region A and Region B, you run an upgrade for each universal distributed logical router (UDLR) and the associated edge services gateways (ESG). By using the Upgrade Coordinator, create an upgrade plan for the edge devices in Region A first. Then proceed with the other clusters in the two regions.

**Table 4-6. NSX Manager Instances and Associated Host Clusters**

Region	NSX Manager	NSX Manager IP Address	Host Cluster
Region A	Primary NSX Manager for the management cluster	172.16.11.65	sfo01-m01-mgmt01
	Primary NSX Manager for the shared edge and compute cluster	172.16.11.66	sfo01-w01-comp01
Region B	Secondary NSX Manager for the management cluster	172.17.11.65	lax01-m01-mgmt01
	Secondary NSX Manager for the shared edge and compute cluster	172.17.11.66	lax01-w01-comp01

**Table 4-7. NSX Edge Instances Upgrade Ordering - Management Clusters**

Order	Management UDLR in Region A	Management Edge in Region A	Management Edge in Region B
1	sfo01m01udlr01	-	-
2	-	<ul style="list-style-type: none"> <li>■ sfo01m01esg01</li> <li>■ sfo01m01esg02</li> <li>■ sfo01m01lb01</li> <li>■ sfo01psc01</li> </ul>	-
3	-	-	<ul style="list-style-type: none"> <li>■ lax01m01esg01</li> <li>■ lax01m01esg02</li> <li>■ lax01m01lb01</li> <li>■ lax01m01psc01</li> </ul>

**Table 4-8. NSX Edge Instances Upgrade Ordering Continued - Shared Edge and Compute Clusters**

Order	Compute UDLR in Region A	Compute Edge in Region A	Compute Edge in Region B
4	sfo01w01udlr01	-	-
5	-	<ul style="list-style-type: none"> <li>■ sfo01w01dlr01</li> <li>■ sfo01w01esg01</li> <li>■ sfo01w01esg02</li> </ul>	-
6	-	-	<ul style="list-style-type: none"> <li>■ lax01w01dlr01</li> <li>■ lax01w01esg01</li> <li>■ lax01w01esg02</li> </ul>

**Procedure**

- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to <https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client>.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator** pane, under **Networking & Security**, click **Installation and Upgrade**.
- 3 Click the **Upgrade** tab, select the **172.16.11.65 | Primary** NSX Manager instance from the drop-down.
- 4 Click **Plan Upgrade** in the central pane.
- 5 On the **Select Upgrade Plan** page of the **Upgrade Components** wizard, click **Plan Your Upgrade**, and click **Next**.
- 6 On the **Plan Content** page, configure the following settings and click **Next**.

Setting	Value
Select Components	Service VMs Deselected
Define Pause Upgrade Options	Pause between components Enabled
	Pause on error Enabled

- 7 On the **Universal Logical Routers** page, select **universal\_routers\_host\_cluster**, and click **Edit**.

- 8 In the **Edit Upgrade Group** dialog box, verify that the following settings are configured, click **OK**.

Setting	Expected Value
Selected Objects	Management UDLR in Region A per NSX Edge Instances Upgrade Ordering
Upgrade order	Serial

- 9 On the **Plan NSX Edges** page, select **edge\_host cluster**, and click **Edit**.
- 10 In the **Edit Upgrade Group** dialog box, verify that the following settings are configured, click **OK** and click **Next**.

Setting	Expected Value
Selected Objects	Management Edge in Region A per NSX Edge Instances Upgrade Ordering
Upgrade order	Serial

Performing the upgrade in a serialized order minimizes disruption on both the management and shared and edge compute clusters.

- 11 On the **Review Plan** page, verify that **Pause between components** and **Pause on error** are set to **Yes**, and click **Start Upgrade**.
- 12 Revalidate that the NSX Controllers are of version *6.4.build\_number*, and click **Resume** to proceed to the universal logical router upgrade.
- 13 Monitor the progress by using the following means.
- Via the **Upgrade** tab:
 

Click on **View Details**. In the **Upgrade Plan Progress** dialog, you can monitor the overall progress of the Universal Logical Router upgrade. Additional information for each step can be found by clicking on the **Details** button.
  - Via the **NSX Edges** section under the **Networking & Security** in the left pane:
 

The **Status** changes to **Busy** as the UDLR is updated.
- 14 After a successful upgrade of the UDLR, on the **NSX Edge** page under the **Networking & Security**, verify that the **Status** column for the edge device shows **DepLoyed**, and the **Version** column contains the upgraded version of *6.4.0*.
- 15 Click the **Upgrade** tab again, and click **Resume** to proceed with the NSX Edges upgrade.
- 16 Wait for upgrade of each edge monitoring the progress.
- 17 After all the NSX Edges are upgraded, on the **NSX Edge** page under the **Networking & Security**, verify that the **Status** column for each edge device shows **DepLoyed**, and the **Version** column contains the upgraded version of *6.4.0*.

- 18 Repeat the steps to upgrade the ESGs in the management cluster in Region B .

When performing the upgrade to the secondary nodes in Region B, when prompted to provide a user name and password in the **Enter Secondary Manager Credentials**, enter the following credentials and click **OK**.

Setting	Value
User name	svc-nsxmanager@rainpole.local
Password	svc-nsxmanager_user_password

- 19 Repeat the steps to upgrade the NSX Edge devices in the shared edge and compute cluster, starting from Region A.

## 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 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 and Management vCenter Server 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 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 and Management vCenter Server in Region A. Then, you repeat this operation in Region B.

Upgrading the VMware Validated Design vSphere for the management clusters is a multi-step operation in which you must upgrade the Management Platform Services Controller and Management vCenter Server, 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 Server	172.16.11.62	sfo01m01vc01.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 Server	172.17.11.62	lax01m01vc01.lax01.rainpole.local

### 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 the environment has been quiesced of all activities. Such activities include but are not limited to users performing active backups of components or provisioning of new virtual machines by using vRealize Automation. Without quiescing the environment, rollback operations 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.

### 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 Platform Services Controller Instances in Region B](#)

#### 5 [Upgrade Management vCenter Server in Region B](#)

## 6 Clean Up the Snapshots of the vSphere 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.

## 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** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	VMware Validated Design 4.2 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	<i>mgmtpsc_root_password</i>

- 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 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	lax01w01vc01.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	<i>mgmtpsc_root_password</i>

- 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.

## Clean Up the Snapshots of the vSphere 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
Region B	lax01-m01fd-mgmt	vCenter Server	lax01m01vc01
	lax01-m01fd-mgmt	Platform Services Controller	lax01m01psc01
	lax01-m01fd-mgmt	Platform Services Controller	lax01w01psc01

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

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

- 3 In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-mgmt** tree.
- 4 Right-click the **sfo01m01vc01** virtual machine and select **Snapshots > Delete All Snapshots**.
- 5 Click **Yes** in the confirmation dialog box.
- 6 Repeat the procedure for the Management vCenter Server in Region B and the Platform Services Controller instances 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	
		172.16.11.1xx	sfo01m01esxxx.sfo01.rainpole.local	
Region B	lax01-m01-mgmt01	192.168.32.67	lax01umds01.lax01.rainpole.local	-
		172.17.11.101	lax01m01esx01.lax01.rainpole.local	lax01-m01-vsan01
		172.17.11.102	lax01m01esx02.lax01.rainpole.local	
		172.17.11.103	lax01m01esx03.lax01.rainpole.local	

**Table 4-11. Management ESXi Hosts and UMDS Nodes in the SDDC (Continued)**

Region	Cluster Name	IP Address	Fully Qualified Domain Name	vSAN Datastore
		172.17.11.104	lax01m01esx04.lax01.rainpole.local	
		172.17.11.1xx	lax01m01esxxx.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
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

**Prerequisites**

- For Update Manager Download Service instances
  - Verify that a backup of all Update Manager Download Service virtual machines exists.
  - Download the vCenter Server Appliance installer `VMware-VCSA-all-6.5.0-build_number.iso` file to a shared datastore for mounting to the virtual appliances. If you have space on your NFS datastore, upload the file there.
- For ESXi hosts and vSAN clusters
  - Verify that the system hardware complies with the ESXi requirements. See [VMware Compatibility Guide](#). Check for the following compatibility areas:
    - System compatibility
    - I/O compatibility with network and host bus adapter (HBA) cards
    - Storage compatibility

- Backup software compatibility
- Compatibility of the firmware for the network and host bus adapter (HBA) cards. Upgrade the firmware accordingly.
- BIOS compatibility. Upgrade the BIOS on the ESXi hosts accordingly.
- Verify that vSphere DRS on the management cluster is set to Fully Automated for the duration of the upgrade operations to have management workloads automatically migrated from hosts while they are being upgraded.
- For VMware Tools
  - Verify that all ESXi hosts in the management cluster have been upgraded.
  - Verify that the vRealize Automation environment has been quiesced of all activities, including but not limited to, users ordering new virtual machines and third-party integration that might automate the ordering of new virtual machines.
  - Verify that the maintenance window is in a time period in which no backup jobs are running or scheduled to run.
  - Verify that a backup of all UMDS virtual machines exist.

## Procedure

### 1 [Upgrade vSphere Update Manager Download Service in Region A](#)

After you 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 4.2. 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 on the virtual machines of the management components in Region A to the version used in VMware Validated Design 4.2. 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 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.
- Verify that the management ESXi hosts are operational after the upgrade.
- Verify that the management virtual machines are operational after the upgrade.

**Upgrade vSphere Update Manager Download Service in Region A**

After you 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.
- 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.local > sfo01-m01fd-mgmt** tree.

- c Right-click the **sfo01umds01** virtual machine and select **Snapshots > Take Snapshot**.
- d In the **Take VM Snapshot** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	VMware Validated Design 4.2 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	<code>svc-umds</code>
Password	<code>svc-umds_password</code>

- 5 Uninstall the current version of Update Manager Download Service.
  - a Navigate to the UMDS installation directory by running the following command.

```
cd /usr/local/vmware-umds
```

- b Run the following command to uninstall UMDS.

```
sudo ./vmware-uninstall-umds.pl
```

- c Enter **Yes** to confirm.

- 6 Prepare for running the installation script.

- a Mount the vCenter Server Appliance ISO to the UMDS virtual machine.

```
sudo mkdir -p /mnt/cdrom
sudo mount /dev/cdrom /mnt/cdrom
```

- b Unarchive the `VMware-UMDS-6.5.0-build_number.tar.gz` file:

```
tar -xzf /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	<i>umds_db_user</i>
Provide the database password	<i>umds_db_user_password</i>

- 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 4.2. 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	sfo01m01esx03.sfo01.rainpole.local		
172.16.11.1xx	sfo01m01esxxx.sfo01.rainpole.local		

### Prerequisites

- Verify that the system hardware complies with the following areas of the ESXi requirements. See [VMware Compatibility Guide](#).
  - System compatibility

- I/O compatibility with network and host bus adapter (HBA) cards
- Storage compatibility
- Backup software compatibility
- Compatibility of the firmware for the network and host bus adapter (HBA) cards. Upgrade the firmware accordingly.
- BIOS compatibility. Upgrade the BIOS on the ESXi hosts accordingly.
- Allocate sufficient disk space on the host for the upgrade.
- To have management workloads automatically migrated from hosts while they are being upgraded, verify that vSphere DRS on the management cluster is set to Fully Automated for the duration of the upgrade operations.
- If using vSAN in the management cluster, on the **Monitor** tab for the cluster in the vSphere Web Client, verify that these properties have the following values:
  - The **vSAN > Health** report indicates that the checks for the cluster, network, physical disk, data, limits, hardware compatibility, performance service, and online health are passed.
  - The **vSAN > Resyncing Components** report shows no **Resyncing Components** and **Bytes left to resync**.
  - The **vSAN > Physical Disks** report shows that the disks on all hosts in the cluster are in mounted state and their vSAN health status is healthy.

## Procedure

### 1 [Remediate the ESXi Management Hosts that Use vSAN in Region A](#)

If the management cluster in Region A is vSAN-backed, to remediate the hosts in the cluster, use the system managed baseline automatically created in vSphere Update Manager on the Management vCenter Server in Region A.

### 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.

### **Remediate the ESXi Management Hosts that Use vSAN in Region A**

If the management cluster in Region A is vSAN-backed, to remediate the hosts in the cluster, use the system managed baseline automatically created in vSphere Update Manager on the Management vCenter Server in Region A.

## Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Verify that the vSAN Build Recommendation Engine is healthy using your my.vmware.com credentials to download the latest recommendation from VMware.
  - a From the **Home** menu of the vSphere Web Client, select **Hosts and Clusters**.
  - b In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01m01-mgmt01** tree.
  - c On the **Monitor** tab, click the **vSAN** tab and select **Health**.
  - d Expand the **vSAN Build Recommendation** test name.
  - e Click the **vSAN Build Recommendation Engine Health** test name, and click the **Login to my.vmware.com** button.
  - f In the **Login** dialog box, enter the following settings and click **OK**.

Setting	Value
Username	my.vmware.com_account_name
Password	my.vmware.com_account_password

- 3 Verify that the system managed baseline for upgrade of vSAN-backed hosts is available in vSphere Update Manager in Region A .
  - a From the **Home** menu, select **Update Manager**.
  - b In the left **Servers** pane, click **sfo01m01vc01.sfo01.rainpole.local**.
  - c In the right pane, on the **Manage** tab, click **Hosts Baselines**.
  - d In the **Baseline Group** pane, expand the **System managed** group and verify that the vSAN Cluster 'sfo01-m01-mgmt01' baseline group contains the following baselines.

Baselines	Type
VMware ESXi 6.5.0 U1 (vSAN 6.6.1, build <i>build_number</i> )	Host Patch
vSAN recommended patch to be applied on top of ESXi 6.5 U1: ESXi650-201712401-BG	Host Patch

- 4 Scan the cluster for updates against the system managed baseline.
  - a In the **Hosts Baselines** pane, click the **Go to compliance view** button to locate the sfo01-m01-mgmt01 cluster in the inventory.
  - b On the **Update Manager** tab, click the **Scan for Updates** button.
  - c In the **Scan for Updates** dialog box, under **Scan hosts for**, select **Patches and Extensions and Upgrades** , and click **OK**.

After the scan is 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 On the **Select baselines** page of the **Remediate** wizard, in the **Baselines Groups and Types** pane, select the **VSAN Cluster 'sfo01-m01-mgmt01'** baseline group, verify that all baselines in the **Baselines** pane are selected, and click **Next**.
  - c On the **Select target objects** page, select all of the management hosts in 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 have passed.
  - e If a Warning test result is present, expand the **Hardware compatibility** tests, review individual tests for a Warning test result, and perform the following troubleshooting.

Test That Results in a Warning	Troubleshooting Guidance
Controller firmware	<a href="#">Update Storage Controller Drivers and Firmware</a> in the <i>Administering VMware vSAN</i> documentation
Controller disk group	VMware Knowledge Base article <a href="#">vSAN Health Service - Hardware Compatibility - Disk Group Type Check</a>
Controller driver	<a href="#">Update Storage Controller Drivers and Firmware</a> in the <i>Administering VMware vSAN</i> documentation.
Controller	VMware Knowledge Base article <a href="#">vSAN Health Service - vSAN HCL Health - Controller Release Support</a>
SCSI controller	VMware Knowledge Base article <a href="#">vSAN Health Service - vSAN HCL Health – SCSI Controller on vSAN HCL</a>
vSAN HCL DB	VMware Knowledge Base article <a href="#">vSAN Health Service - vSAN HCL Health – vSAN HCL DB up-to-date</a>

## 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 Patch Release ESXi650-201712001 in vSphere Update Manager in Region A
  - a From the **Home** menu, select **Update Manager**.
  - b In the **Servers** pane on the left, click **sfo01m01vc01.sfo01.rainpole.local**.
  - c In the right pane, on the **Manage** tab, click **Host Baselines**.
  - d In the **Host Baselines** pane, click **New Baseline**.  
The **New Baseline** wizard appears.
  - e On the **Name and type** page, enter the following options and click **Next**

Setting	Value
Name	VMware ESXi 6.5 Update 1 Patch Release ESXi650-201712001 for VMware Validated Design 4.2
Description	<a href="https://kb.vmware.com/s/article/2151102">https://kb.vmware.com/s/article/2151102</a>
Baseline Type	Host Patch

- f On the **Patch options** page, select **Fixed**.

- g On the **Patches** page, verify the following patch names are selected and click **Next**.

Patch Name	Patch ID
Updates esx-base, esx-tboot, vsan, and vsanhealth VIBs	ESXi650-201712401-BG
Updates vmkusb VIB	ESXi650-201712402-BG
Updates vmkata VIB	ESXi650-201712403-BG
Updates esx-dvfilter-generic-fastpath VIB	ESXi650-201712404-BG
Updates nvmxnet3 VIB	ESXi650-201712405-BG
Updates igbn VIB	ESXi650-201712406-BG
Updates ntg3 VIB	ESXi650-201712407-BG
Updates misc-drivers VIB	ESXi650-201712408-BG
Updates nvme VIB	ESXi650-201712409-BG
Updates esx-base, esx-tboot, vsan, and vsanhealth VIBs	ESXi650-201712101-SG
Updates tools-light VIB	ESXi650-201712102-SG
Updates esx-ui VIB	ESXi650-201712103-SG

- h On the **Ready to complete** page, review the baseline details, verify that all required patch names are present, and click **Finish**.

- 3 Attach and scan the cluster for updates against the new baseline.

- In the **Host Baselines** pane, click **Go to Compliance View** to locate the sfo01m01vc01.sfo01.rainpole.local vCenter Server and the sfo01-m01-mgmt01 cluster in the inventory.
- On the **Update Manager** tab, click **Attach Baseline**.
- In the **Attach Baseline** dialog box, select the **VMware ESXi 6.5 Update 1 Patch Release ESXi650-201712001 for VMware Validated Design 4.2** baseline and click **OK**.
- After the baseline is attached, click **Scan for Updates**.
- 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 Patch Release ESXi650-201712001.

- On the **Update Manager** tab for the cluster, click **Remediate**.
- 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 Patch Release ESXi650-201712001 for VMware Validated Design 4.2** baseline and click **Next**.
- On the **Select Target objects** page, select all management hosts in the cluster and click **Next**.
- On the **Patch and extensions** page, verify that all patches are selected and click **Next**.

- e On the **Advanced options** page, click **Next**
- f On the **Host remediation options** page, deselect **Retry entering maintenance mode in case of failure** and click **Next**.
- g On the **Cluster remediation options** page, select the following options and click **Next**.

Setting	Value
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters	Selected
Disable High Availability admission control if it is enabled for any of the selected clusters	Selected
Enable parallel remediation for the hosts in the cluster > Automatically determine the maximum number of concurrently remediated hosts in a cluster	Selected
Migrate powered off or suspended VMs to other hosts in the cluster, if a host must enter maintenance mode	Selected

- h On the **Ready to complete** page, click **Pre-check Remediation** to generate a pre-upgrade report of any identifiable problems that would prevent a successful upgrade.

Address any items reported in the **Pre-check Remediation** dialog box before proceeding with the upgrade. Click **OK** to close the screen. Ignore the **Disable HA admission control** message from **Recommended Changes**.

- i After you address all pre-check items, click **Finish** to begin the upgrade.

## 5 Review the NSX status of the management cluster.

- a Select **Home > Networking & Security**.
- b Select **Installation** in the **Navigator**.
- c On the **Host Preparation** tab, select **172.16.11.65** from the **NSX Manager** menu and verify that **Installation Status** for all management ESXi hosts is green.

## Remediate VMware Tools in the Management Cluster in Region A

After you upgrade the ESXi hosts running the management virtual machines, upgrade the VMware Tools on the virtual machines of the management components in Region A to the version used in VMware Validated Design 4.2. 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

**Table 4-14. Management Virtual Machines for VMware Tools Remediation in Region A (Continued)**

Cluster Name	Folder	Role	Virtual Machine Name
			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	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 Patch Release ESXi650-201712001 in vSphere Update Manager in Region A
  - a From the **Home** menu, select **Update Manager**.
  - b In the **Servers** pane on the left, click **sfo01m01vc01.sfo01.rainpole.local**.
  - c In the right pane, on the **Manage** tab, click the **VMs/VAs Baselines** tab.
  - d In the **VMs/VAs Baselines** pane, click **New Baseline Group**.  
The **New Baseline Group** wizard appears.
  - e On the **Name** page, enter the following values and click **Next**.

Setting	Value
Name	VMware Tools for VMware Validated Design 4.2
Description	-

- f On the **Upgrades** page, select the following options and click **Next**.

Setting	Value
VM Hardware Upgrades	None
VMware Tools Upgrades	VMware Tools Upgrade to Match Host (Predefined)
VA Upgrades	None

- g On the **Ready to complete** page, click **Finish**.

- 3 Attach and scan the folder for updates against the new baseline.

- a In the **VMs/VAs Baselines** pane, click **Go to compliance view** to locate the sfo01m01vc01.sfo01.rainpole.local vCenter Server and to the sfo01-m01-mgmt01 cluster in the inventory.
- b In the **Navigator**, click **VMs and Templates** and expand the **sfo01-m01dc > sfo01-m01fd-bcdr** tree.
- c On the **Update Manager** tab, click **Attach Baseline**.
- d In the **Attach Baseline or Baseline Group** dialog box, under **Baseline Groups** pane, select the **VMware Tools for VMware Validated Design 4.2** baseline group and click **OK**.
- e After you attach the baseline, click **Scan for Updates**.
- f In the **Scan for Updates** dialog box, under **Scan for**, select only **VMware Tools upgrades** and click **OK**.

After the scan is complete, the folder status is Non-Compliant.

- 4 Remediate the virtual machines and upgrade VMware Tools to ESXi 6.5 Update 1 Patch Release ESXi650-201712001.

- a On the **Update Manager** tab, click **Remediate**.
- b In the **Remediate** wizard on the **Select baselines** page, under **Baselines Groups and Types** pane, select the baseline group **VMware Tools for VMware Validated Design 4.2** and click **Next**.
- c On the **Select target objects** page, select the management virtual machines in the folder and click **Next**.
- d On the **Schedule** page, configure the following settings and click **Next**.

Setting	Value	
Task name	sfo01-m01fd-bcdr - VMware Tools for VMware Validated Design 4.2	
Task description	-	
Apply upgrade at specific time	For powered on VMs	Run this action now
	For powered off VMs	Run this action now
	For suspended VMs	Run this action now

- e On the **Rollback Options** page, configure the following settings and click **Next**.

Setting		Value
Take a snapshot of the VMs before remediation to enable rollback		Selected
Snapshot Retention		Do not delete snapshots
Snapshot Details	Name	VMware Tools for VMware Validated Design 4.2
	Description	-

- f On the **Ready to complete** page, click **Finish** to begin the upgrade.

The Update Manager remediation process starts running and restarts the virtual machines.

- 5 After the VMware Tools upgrade is complete on each virtual machine in the folder, review the **Summary** tab for each virtual machine that has been remediated, and verify that the VMware Tools status is *Running* and version is (*Current*).
- 6 Navigate back to the **sfo01-m01fd-bcdr** folder and run the **Scan for Updates** operation again to verify that the management virtual machines are *Compliant*.

**Note** Because of the use of Guest Managed VMware Tools in the virtual machines, the **Compliance Status** might report *Incompatible* for the overall folder.

- 7 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 **Snapshots Delete All Snapshots**.
  - d In the **Confirm Delete** dialog box, click **Yes**.
- 8 Repeat the procedure for the other management virtual machines using their folder in Region A.

#### What to do next

- Verify that the management virtual machines are operational after the upgrade.

## 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 4-15. 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 4-16. 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 4-17. 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-vsant01	172.17.11.65
172.17.11.102	lax01m01esx02.lax01.rainpole.local			

**Table 4-17. Management ESXi Hosts to Upgrade in Region B (Continued)**

Host IP Address	Fully Qualified Domain Name	Cluster Name	vSAN Datastore	NSX Manager for the Management Cluster
172.17.11.103	lax01m01esx03.lax01.rainpole.local			
172.17.11.104	lax01m01esx04.lax01.rainpole.local			
172.17.11.1xx	lax01m01esxxx.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 4-18. Management Virtual Machines and Virtual Appliances In Region B**

Cluster Name	Folder	Role	Virtual Machine Name
lax01-m01-mgmt01	lax01-m01fd-mgmt	Update Manager Download Service	lax01umds01
	lax01-m01fd-vraias	vRealize Automation Proxy Agent	lax01ias01a.lax01.rainpole.local lax01ias01b.lax01.rainpole.local

### What to do next

Verify that UMDS, management hosts and vSAN are operational.

## 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](#)

After 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

After 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.

Upgrading the VMware Validated Design vSphere layer for the shared edge and compute cluster is a single-step operation. In this version, you upgrade the Compute vCenter Server in Region A. Then, you repeat this operation in Region B.

**Table 4-19. 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

### Prerequisites

- Download the vCenter Server Appliance `VMware-vCenter-Server-Appliance-6.5.0.x-build_number-patch-FP.iso` 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. Such activities include but are not limited to users performing active backups of components, provisioning of new virtual machines by using vRealize Automation, third-party integration that might automate the ordering or deployment of new virtual machines, and administrators manually creating new virtual objects. 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 the Compute vCenter Server instances exists.

### 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 Clean Up 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 validating their stability, remove the snapshots from the nodes.

##### What to do next

- Verify that vCenter Server are operational after the upgrade.

## Take Snapshots of the Compute vCenter Server Instances in Region A and Region B

Before you start the update, take a snapshot of each Compute vCenter Server appliance in Region A and Region B so that you can roll the update back if a failure occurs.

**Table 4-20. Compute vCenter Server Instances in the SDDC**

Region	Folder	Virtual Machine Name
Region A	sfo01-m01fd-mgmt	sfo01w01vc01
Region B	lax01-m01fd-mgmt	lax01w01vc01

### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, click **VMs and Templates**.
- 3 In the **Navigator**, expand the **sf01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-mgmt** tree.
- 4 Right-click the **sfo01w01vc01** virtual machine and select **Snapshots > Take Snapshot**.
- 5 In the **Take VM Snapshot** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	VMware Validated Design 4.2 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	<code>compvc_root_password</code>

- 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.

## Clean Up 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 validating their stability, remove the snapshots from the nodes.

**Procedure**

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **VMs and Templates**.
- 3 In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-mgmt** tree.
- 4 Right-click the **sfo01m01vc01** virtual machine and select **Snapshots > Delete All Snapshots**.
- 5 Click **Yes** in the confirmation dialog box.
- 6 Repeat the procedure for the Compute vCenter Server in Region B.

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 4-21. 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	
	172.16.31.1xx	sfo01w01esxxx.sfo01.rainpole.local	
Region B	172.17.31.101	lax01w01esx01.lax01.rainpole.local	lax01-m01-mgmt01

**Table 4-21. 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	
	172.17.31.1xx	lax01w01esxxx.lax01.rainpole.local	

**Prerequisites**

- Verify that the system hardware complies with the following areas of the ESXi requirements. See [VMware Compatibility Guide](#).
  - System compatibility
  - I/O compatibility with network and host bus adapter (HBA) cards
  - Storage compatibility
  - Backup software compatibility
  - Compatibility of the firmware for the network and host bus adapter (HBA) cards. Upgrade the firmware accordingly.
  - BIOS compatibility. Upgrade the BIOS on the ESXi hosts accordingly.
- Verify that vSphere DRS on the shared edge and compute 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.

### **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 Patch Release ESXi650-201712001 in vSphere Update Manager in Region A
  - a From the **Home** menu, select **Update Manager**.
  - b In the **Servers** pane on the left, click **sfo01w01vc01.sfo01.rainpole.local**.
  - c In the right pane, on the **Manage** tab, click **Host Baselines**.
  - d In the **Host Baselines** pane, click **New Baseline**.  
The **New Baseline** wizard appears.
  - e On the **Name and type** page, enter the following options and click **Next**

Setting	Value
Name	VMware ESXi 6.5 Update 1 Patch Release ESXi650-201712001 for VMware Validated Design 4.2
Description	<a href="https://kb.vmware.com/s/article/2151102">https://kb.vmware.com/s/article/2151102</a>
Baseline Type	Host Patch

- f On the **Patch options** page, select **Fixed**.

- g On the **Patches** page, verify the following patch names are selected and click **Next**.

Patch Name	Patch ID
Updates esx-base, esx-tboot, vsan, and vsanhealth VIBs	ESXi650-201712401-BG
Updates vmkusb VIB	ESXi650-201712402-BG
Updates vmkata VIB	ESXi650-201712403-BG
Updates esx-dvfilter-generic-fastpath VIB	ESXi650-201712404-BG
Updates nvmxnet3 VIB	ESXi650-201712405-BG
Updates igbn VIB	ESXi650-201712406-BG
Updates ntg3 VIB	ESXi650-201712407-BG
Updates misc-drivers VIB	ESXi650-201712408-BG
Updates nvme VIB	ESXi650-201712409-BG
Updates esx-base, esx-tboot, vsan, and vsanhealth VIBs	ESXi650-201712101-SG
Updates tools-light VIB	ESXi650-201712102-SG
Updates esx-ui VIB	ESXi650-201712103-SG

- h On the **Ready to complete** page, review the baseline details, verify that all required patch names are present, and click **Finish**.

### 3 Attach and scan the cluster for updates against the new baseline

- In the **Host Baselines** pane, click **Go to Compliance View** to locate the sfo01w01vc01.sfo01.rainpole.local vCenter Server and to the sfo01-w01-comp1 cluster in the inventory.
- On the **Update Manager** tab, click **Attach Baseline**.
- In the **Attach Baseline** dialog box, select the **VMware ESXi 6.5 Update 1 Patch Release ESXi650-201712001 for VMware Validated Design 4.2** baseline and click **OK**.
- After the baseline is attached, click **Scan for Updates**.
- 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 Patch Release ESXi650-201712001.

- On the **Update Manager** tab, click **Remediate**.
- On the **Select baselines** page of the **Remediate** wizard, under **Baselines Groups and Types**, click **Patch Baselines**, and select the **VMware ESXi 6.5 Update 1 Patch Release ESXi650-201712001 for VMware Validated Design 4.2** baseline and click **Next**.
- On the **Select Target objects** page, select all hosts in the cluster and click **Next**.
- On the **Patch and extensions** page, ensure all patches are selected, and click **Next**.

- e On the **Advanced options** page, click **Next**
- f On the **Host remediation options** page, deselect **Retry entering maintenance mode in case of failure** and click **Next**.
- g On the **Cluster remediation options** page, select the following options and click **Next**.

Setting	Value
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters	Selected
Disable High Availability admission control if it is enabled for any of the selected clusters	Selected
Enable parallel remediation for the hosts in the cluster > Automatically determine the maximum number of concurrently remediated hosts in a cluster	Selected
Migrate powered off or suspended VMs to other hosts in the cluster, if a host must enter maintenance mode	Selected

- h On the **Ready to complete** page, click **Pre-check Remediation** to generate a pre-upgrade report of any identifiable problems that would prevent a successful upgrade.

Address any items reported in the **Pre-check Remediation** dialog box before proceeding with the upgrade. Click **OK** to close the screen. Ignore the **Disable HA admission control** message from **Recommended Changes**.

- i After you address all pre-check items, click **Finish** to begin the upgrade.

- 5 Review the NSX status of the 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 Patch Release ESXi650-201712001 for VMware Validated Design 4.2 baseline.

## Global Post-Upgrade Configuration of the Virtual Infrastructure Layer

After you upgrade all virtual infrastructure layer, perform global post-upgrade configuration according to address the dependencies between these components and to align your environment to the guidance in this validated design.

## Procedure

### 1 Post-Upgrade Configuration of the Virtual Infrastructure Components in Region A

After you 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

Update the identity of your SDDC deployment on vCenter Server. You use this identity as a label in tools for automated SDDC deployment.

#### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Global Inventory Lists**.
- 3 In the **Navigator**, click **vCenter Servers** under **Resources**.
- 4 Click the `sfo01m01vc01.sfo01.rainpole.local` vCenter Server object and click the **Configure** tab in the central pane.
- 5 Under the **Settings** pane, click **Advanced Settings** and click the **Edit** button.

- 6 In the **Edit Advanced vCenter Server Settings** dialog box, configure the following properties and click **OK**.
  - a Search for the **config.SDDC.Deployed.Version** property and change its value from 4.1.0 to **4.2.0**.
  - b Add the **config.SDDC.Deployed.WorkloadDomain** and **config.SDDC.Deployed.InstanceId** properties.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard
config.SDDC.Deployed.Version	4.2.0
config.SDDC.Deployed.WorkloadDomain	Management
config.SDDC.Deployed.Method	DIY
config.SDDC.Deployed.InstanceId	unique_identifier*

---

**Note** \* To generate a unique identifier, use the Online UUID Generator website <https://www.uuidgenerator.net/> and copy/paste the UUID into the config.SDDC.Deployed.InstanceId value. The Online UUID Generator is a universally unique identifier that generates random numbers using a secure random number generator.

---

- 7 Click **OK** to close the window.

## Set SDDC Deployment Details on the Compute vCenter Server in Region A

Update the identity of your SDDC deployment on the Compute vCenter Server in Region A. You can use this identity as a label in tools for automated SDDC deployment.

### Procedure

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Global Inventory Lists**.
- 3 In the **Navigator**, click **vCenter Servers** under **Resources**.
- 4 Click the **sfo01w01vc01.sfo01.rainpole.local** vCenter Server object and click the **Configure** tab in the central pane.

- 5 Under the **Settings** pane, click **Advanced Settings** and click the **Edit** button.
- 6 In the **Edit Advanced vCenter Server Settings** dialog box, configure the following properties and click **OK**.
  - a Search for the **config.SDDC.Deployed.Version** property and change its value from 4.1.0 to **4.2.0**.
  - b Add the **config.SDDC.Deployed.WorkloadDomain** and **config.SDDC.Deployed.InstanceId** properties.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard
config.SDDC.Deployed.Version	4.2.0
config.SDDC.Deployed.WorkloadDomain	SharedEdgeAndCompute
config.SDDC.Deployed.Method	DIY
config.SDDC.Deployed.InstanceId	unique_identifier*

**Note** \* To generate a unique identifier, use the Online UUID Generator website <https://www.uuidgenerator.net/> and copy/paste the UUID into the config.SDDC.Deployed.InstanceId value. The Online UUID Generator is a universally unique identifier that generates random numbers using a secure random number generator.

- 7 Click **OK** to close the window.

## 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](#)
- 2 [Set SDDC Deployment Details on the Compute vCenter Server in Region B](#)

### Set SDDC Deployment Details on the Management vCenter Server in Region B

Update the identity of your SDDC deployment on the Management vCenter Server in Region B. You use this identity as a label in tools for automated SDDC deployment.

**Procedure**

- 1 Log in to the Management vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to `https://lax01m01vc01.lax01.rainpole.local/vsphere-client`.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Global Inventory Lists**.
- 3 In the **Navigator**, click **vCenter Servers** under **Resources**.
- 4 Click the `lax01m01vc01.lax01.rainpole.local` vCenter Server object and click the **Configure** tab in the central pane.
- 5 Under the **Settings** pane, click **Advanced Settings** and click the **Edit** button.
- 6 In the **Edit Advanced vCenter Server Settings** dialog box, configure the following properties and click **OK**.
  - a Search for the `config.SDDC.Deployed.Version` property and change its value from 4.1.0 to **4.2.0**.
  - b Add the `config.SDDC.Deployed.WorkloadDomain` and `config.SDDC.Deployed.InstanceId` properties.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard
config.SDDC.Deployed.Version	4.2.0
config.SDDC.Deployed.WorkloadDomain	Management
config.SDDC.Deployed.Method	DIY
config.SDDC.Deployed.InstanceId	unique_identifier*

**Note** \* To generate a unique identifier, use the Online UUID Generator website <https://www.uuidgenerator.net/> and copy/paste the UUID into the `config.SDDC.Deployed.InstanceId` value. The Online UUID Generator is a universally unique identifier that generates random numbers using a secure random number generator.

**Set SDDC Deployment Details on the Compute vCenter Server in Region B**

Update the identity of your SDDC deployment on the Compute vCenter Server in Region B. You use this identity as a label in tools for automated SDDC deployment.

**Procedure**

- 1 Log in to the Compute vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to **https://lax01w01vc01.lax01.rainpole.local/vsphere-client**.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu of the vSphere Web Client, select **Global Inventory Lists**.
- 3 In the **Navigator**, click **vCenter Servers** under **Resources**.
- 4 Click the **lax01w01vc01.lax01.rainpole.local** vCenter Server object and click the **Configure** tab in the central pane.
- 5 Under the **Settings** pane, click **Advanced Settings** and click the **Edit** button.
- 6 In the **Edit Advanced vCenter Server Settings** dialog box, configure the following properties and click **OK**.
  - a Search for the **config.SDDC.Deployed.Version** property and change its value from 4.1.0 to **4.2.0**.
  - b Add the **config.SDDC.Deployed.WorkloadDomain** and **config.SDDC.Deployed.InstanceId** properties.

Name	Value
config.SDDC.Deployed.Type	VVD
config.SDDC.Deployed.Flavor	Standard
config.SDDC.Deployed.Version	4.2.0
config.SDDC.Deployed.WorkloadDomain	SharedEdgeAndCompute
config.SDDC.Deployed.Method	DIY
config.SDDC.Deployed.InstanceId	unique_identifier*

**Note** \* To generate a unique identifier, use the Online UUID Generator website <https://www.uuidgenerator.net/> and copy/paste the UUID into the config.SDDC.Deployed.InstanceId value. The Online UUID Generator is a universally unique identifier that generates random numbers using a secure random number generator.

- 7 Click **OK** to close the window.

## Post-Upgrade Configuration of the Business Continuity Layer for the Management Cluster

After you upgrade the business continuity and virtual infrastructure layers of the SDDC, configure the environment according to the objectives and deployment guidelines of this validated design.

Add capabilities for monitoring Site Recovery Manager in vRealize Operations Manager and vRealize Log Insight.

### Connect vRealize Operations Manager to Site Recover Manager

Install and configure the vRealize Operations Management Pack for Site Recovery Manager to monitor the health and configuration of the Site Recovery Manager instances, and the status of the protection groups and recovery plans for failing over the management components of the SDDC.

### Configure User Privileges for Site Recovery Manager Adapters in vRealize Operations Manager

Assign read-only permissions to the service account `svc-vrops-srm` on the sites that are required for collecting data about Site Recovery Manager instances in vRealize Operations Manager.

#### Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
  - a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.
  - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 On the **Home** page of the vSphere Web Client, select **Site Recovery**.
- 3 In the **Navigator**, under **Sites**, click **Sites**.
- 4 On the **Sites** page, click the `sfo01m01vc01.sfo01.rainpole.local` site.
- 5 On the **Manage** tab, click **Permissions** tab.
- 6 On the **Permissions** tab, click **Add permission**.
- 7 In the **Add Permission** dialog box, click **Add**.
- 8 Add the service account.
  - a In the **Select Users/Groups** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type `svc-vrops-srm`, and press Enter.
  - b From the list of users and groups, select `svc-vrops-srm`, click **Add**, and click **OK**.

- 9 Associate the service account with the read-only role.
  - a In the **Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **Read-only**.
  - b Verify that **Propagate to children** is selected and click **OK**.
- 10 Repeat the steps to assign read-only permissions to the svc-vrops-srm service account on the site instance for Region B.

## Install the vRealize Operations Manager Management Pack for Site Recovery Manager

Install the .pak file for the management pack for Site Recovery Manager to add the management pack as a solution 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, click the **Add** icon.
- 5 On the **Select Solution** page from the **Add Solution** wizard, browse to the .pak file of the vRealize Operations Manager Management Pack for Site Recovery Manager and click **Upload**.  
After the management pack file has been uploaded, you see details about the management pack.
- 6 After the upload is complete, click **Next**.
- 7 On the **End User License Agreement** page, accept the license agreement and click **Next**.  
The installation of the management pack starts. You see its progress on the **Install** page.
- 8 After the installation is complete, click **Finish** on the **Install** page.

The Srm Adapter solution appears on the **Solutions** page of the vRealize Operations Manager user interface.

## Add SRM Adapter Instances to vRealize Operations Manager

In a dual-region SDDC, configure SRM Adapters to collect monitoring data in vRealize Operations Manager about the Site Recovery Manager instances and failover objects.

## 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 **Srm Adapter** from the solution table, and click **Configure**.  
The **Manage Solution - Srm Adapter** dialog box appears.
- 5 Under **Instance Settings**, enter the settings for the connection to Site Recovery Manager instances.
  - a If you already have added another Srm Adapter, click the **Add** icon on the left side to add an adapter settings.
  - b Enter the settings for connection to Site Recovery Manager.

Setting	Value for Site Recovery Manager in Region A	Value for Site Recovery Manager in Region B
Display Name	SRM Adapter - sfo01m01srm01	SRM Adapter - lax01m01srm01
Description	Site Recovery Manager Adapter for sfo01	Site Recovery Manager Adapter for lax01
SRM Host	sfo01m01srm01.sfo01.rainpole.local	lax01m01srm01.lax01.rainpole.local
SRM Port	9086	9086

- c Click the **Add** icon next to the **Credential** text box, configure the credentials for connection to Site Recovery Manager instances, and click **OK**.

Setting	Value for Site Recovery Manager in Region A	Value for Site Recovery Manager in Region B
Credential name	SRM Adapter Credentials - sfo01m01srm01	SRM Adapter Credentials - lax01m01srm01
Username	svc-vrops-srm@rainpole.local	svc-vrops-srm@rainpole.local
Password	svc-vrops-srm_password	svc-vrops-srm_password

- d Click **Test Connection** to validate the connection to Site Recovery Manager.  
The Site Recovery Manager certificate appears.
  - e In the **Review and Accept Certificate** dialog box, verify the Site Recovery Manager certificate information and click **Accept**.

- f Click **OK** in the **Info** dialog box.
- g Expand the **Advanced Settings** section of settings.
- h From the **Collectors/Groups** drop-down menu, select the collector group for the region.

Site Recovery Manager Instance	Remote Collector Group
Site Recovery Manager in Region A	sfo01-remote-collectors
Site Recovery Manager in Region B	lax01-remote-collectors

- i Click **Save Settings**.
  - j Click **OK** in the **Info** dialog box that appears.
  - k Repeat the steps for the Site Recovery Manager in Region B.
- 6 In the **Manage Solution - Srm Adapter** dialog box, click **Close**.

The SRM Adapter instances appear on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is **Collecting** and the **Collection Status** is **Data receiving**.

## Connect vRealize Log Insight to Site Recovery Manager

Monitor Site Recovery Manager operation by tracking its logs in vRealize Log Insight. In each region, install the content pack for Site Recovery Manager in vRealize Log Insight and install the Log Insight Agent on the Windows virtual machine of the Site Recovery Manager instance.

### Install the vRealize Log Insight Content Pack for Site Recovery Manager

Install the content pack for Site Recovery Manager to add the dashboards for viewing log information in vRealize Log Insight in Region A and 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	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.
- 3 Under **Content Pack Marketplace**, select **Marketplace**.
- 4 In the list of content packs, locate the **VMware - SRM** content pack and click its icon.

- 5 In the **Install Content Pack** dialog box, accept the **License Agreement** and click **Install**.
- 6 In the **VMware - SRM Content Pack Setup Instructions** dialog box, click **OK**.
- 7 Repeat the steps on vRealize Log Insight in Region B lax01vrli01.lax01.rainpole.local

After the installation is complete, the VMware - SRM content pack appears in the **Installed Content Packs** list on the left in vRealize Log Insight.

## Configure Site Recovery Manager to Forward Log Events to vRealize Log Insight

Install the vRealize Log Insight agent on the Site Recovery Manager instances in Region A and Region B to collect and forward events to vRealize Log Insight.

In each region, you perform the following operations:

- 1 Install the Windows Log Insight Agent on the Site Recovery Manager virtual machine and connect it to the vRealize Log Insight instance in the region.
- 2 Create an agent group for central configuration of the Log Insight Agent on the Site Recovery Manager instance.

**Table 4-22. Settings for Forwarding Events from Site Recovery Manager to vRealize Log insight**

Setting	Value for Site Recovery Manager in Region A	Value for Site Recovery Manager in Region B
FQDN of the Site Recovery Manager virtual machine	sfo01m01srm01.sfo01.rainpole.local	lax01m01srm01.lax01.rainpole.local
vRealize Log Insight URL	https://sfo01vrli01.sfo01.rainpole.local	https://lax01vrli01.lax01.rainpole.local
Host names in the agent group in vRealize Log Insight	sfo01m01srm01.sfo01.rainpole.local	lax01m01srm01.lax01.rainpole.local

### Procedure

- 1 Install Log Insight Windows agents in the virtual machines of the Site Recovery Manager nodes.
  - a Open a Remote Desktop Protocol (RDP) connection to **sfo01m01srm01.sfo01.rainpole.local**.
  - b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	<i>windows_administrator_user</i>

- c On the Windows host, open a Web browser and go to **https://sfo01vrli01.sfo01.rainpole.local**.

- d Log in using the following credentials.

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

- e Click the **Configuration** drop-down menu icon  and select **Administration**.
- f Under **Management**, click **Agents**.
- g On the **Agents** page, click the **Download Log Insight Agent Version** link.
- h In the **Download Log Insight Agent Version** dialog box, click **Windows MSI (32-bit/64-bit)** and save the .msi file to the vRealize Automation virtual machine.
- i Open an administrative command prompt window, and navigate to the directory where you saved the .msi file.
- j 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
```

- k In the **VMware vRealize Log Insight Agent Setup** wizard, accept the license agreement and click **Next**.
- l With the Log Insight host name **sfo01m01srm01.sfo01.rainpole.local** selected in the **Host** text box, click **Install**.
- m After the installation is complete, click **Finish**.
- 2 Create an agent group for Site Recovery Manager in 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	<i>vrlj_admin_password</i>

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

- h Configure the following agent filter.

Press Enter to separate the host names.

Filter	Operator	Values
Hostname	matches	sfo01m01srm01.sfo01.rainpole.local

- i Click **Refresh** and verify that all the agents listed in the filter appear in the **Agents** list.
  - j Click **Save New Group** at the bottom of the page.
- 3 Repeat the procedure on Site Recovery Manager and vRealize Log Insight in Region B.

All VMware Site Recovery Manager dashboards become available on the vRealize Log Insight Home page.

# SDDC Startup and Shutdown

When you perform patch, upgrade, recovery, or failover of the SDDC management applications, make sure that you start up and shut down the management virtual machines according to a predefined order.

This chapter includes the following topics:

- [Shutdown Order of the Management Virtual Machines](#)
- [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 components.

Before you begin:

- Verify that virtual machines are not running on snapshots.
- Ensure verified backups of all management and tenant virtual machines are available.
- If a data protection solution is running on the management clusters, ensure the solution is properly shutdown following the vendor guidance.
- If the hosts in a vSAN cluster will be shut down, appropriately shut down the tenant workloads in the shared edge and compute cluster.

Shutting down the management virtual machines:

- Refer to VMware Knowledge Base article [2142676](#) for information on verifying the state of the vSAN cluster prior to a shutdown.
- Shut down the virtual machines of the SDDC management stack by following the shutdown order provided in the table below.
- Ensure that the console of the virtual machine and its services are fully shut down before moving to the next virtual machine.

---

**Note** The vCenter Server instances, NSX Load-balancers for the Platform Services Controllers in, and the Platform Services Controllers and the management clusters will be the last virtual machines to be shut down.

---

Virtual Machine Name in Region A	Virtual Machine Name in Region B	Shutdown Order
<b>vRealize Log Insight</b>	<b>vRealize Log Insight</b>	<b>1</b>
<b>Total Number of VMs (3)</b>	<b>Total Number of VMs (3)</b>	
sfo01vrli01c	lax01vrli01c	1
sfo01vrli01b	lax01vrli01b	1
sfo01vrli01a	lax01vrli01a	2
<b>vRealize Operations Manager</b>	<b>vRealize Operations Manager</b>	<b>1</b>
<b>Total Number of VMs (5)</b>	<b>Total Number of VMs (2)</b>	
sfo01vropsc01b	lax01vropsc01b	1
sfo01vropsc01a	lax01vropsc01a	1
vropsc01svr01c	-	2
vropsc01svr01b	-	3
vropsc01svr01a	-	4
<b>vRealize Business for Cloud</b>	<b>Realize Business for Cloud</b>	<b>2</b>
<b>Total Number of VMs (2)</b>	<b>Total Number of VMs (2)</b>	
sfo01vrbc01	lax01vrbc01	1
vrb01svr01	-	2
<b>vRealize Automation</b>	<b>vRealize Automation</b>	<b>3</b>
<b>Total Number of VMs (11)</b>	<b>Total Number of VMs (2)</b>	
vra01dem01a	-	1
vra01dem01b	-	1
sfo01ias01b	lax01ias01b	1
sfo01ias01a	lax01ias01a	1
vra01ims01b	-	2
vra01ims01a	-	2
vra01iws01b	-	3
vra01iws01a	-	4
vra01svr01b	-	5
vra01svr01a	-	5
vra01mssql01	-	6
<b>Site Recovery Manager and vSphere Replication</b>	<b>Site Recovery Manager and vSphere Replication</b>	<b>4</b>
<b>Total Number of VMs (2)</b>	<b>Total Number of VMs (2)</b>	
sfo01m01vrms01	lax01m01vrms01	1
sfo01m01srm01	lax01m01srm01	2
<b>Update Manager Download Service (UMDS)</b>	<b>Update Manager Download Service (UMDS)</b>	<b>4</b>
<b>Total Number of VMs (1)</b>	<b>Total Number of VMs (1)</b>	
sfo01umds01	lax01umds01	1

Virtual Machine Name in Region A	Virtual Machine Name in Region B	Shutdown Order
<b>Core Stack</b>	<b>Core Stack</b>	<b>5</b>
<b>Total Number of VMs (26)</b>	<b>Total Number of VMs (16)</b>	
sfo01m01lb01 (0,1)	lax01m01lb01 (0,1)	1
sfo01m01udlr01 (0,1)	-	1
sfo01m01esg01	lax01m01esg01	1
sfo01m01esg02	lax01m01esg02	1
sfo01w01udlr01 (0,1)	-	1
sfo01w01dlr01 (0,1)	lax01w01dlr01 (0,1)	1
sfo01w01esg01	lax01w01esg01	1
sfo01w01esg02	lax01w01esg02	1
sfo01m01nsx01	lax01m01nsx01	2
sfo01w01nsx01	lax01w01nsx01	2
sfo01m01nsxc01	-	3
sfo01m01nsxc02	-	3
sfo01m01nsxc03	-	3
sfo01w01nsxc01	-	3
sfo01w01nsxc02	-	3
sfo01w01nsxc03	-	3
sfo01m01vc01	lax01m01vc01	4
sfo01w01vc01	lax01w01vc01	4
sfo01psc01 (0,1)	lax01psc01 (0,1)	5
sfo01w01psc01	lax01w01psc01	6
sfo01m01psc01	lax01m01psc01	6

Shutting down the ESXi hosts in the vSAN clusters:

- Refer to VMware Knowledge Base article [2142676](#) for information on preparing and shutting down ESXi hosts in vSAN clusters.

## Startup Order of the Management Virtual Machines

Start up the virtual machines of the SDDC management stack by following a strict order to guarantee the faultless operation of and the integration between the components.

Before you begin:

- Verify that external dependencies for the SDDC, such as, Active Directory, DNS, NTP, SMTP, and FTP/SFTP are available.

Starting up the ESXi hosts in the vSAN clusters:

- If the vSAN clusters have been shut down, refer to VMware Knowledge Base article [2142676](#) for information on starting up hosts and exiting maintenance mode.

Starting up the management virtual machines:

- Start up the virtual machines by following the start up order provides in the table below.
- Ensure that the console of the virtual machine and its services are all up before moving to the next virtual machine.
- Refer to VMware Knowledge Base article [2142676](#) for information on checking the health of the vSAN clusters before starting up tenant workloads.
- If a data protection solution is deployed on the management cluster, ensure the solution is properly started, and operational following the vendor guidance.

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
<b>Core Stack Total Number of VMs (26)</b>	<b>Core Stack Total Number of VMs (16)</b>	<b>1</b>
sfo01m01psc01	lax01m01psc01	1
sfo01w01psc01	lax01w01psc01	1
sfo01psc01 (0,1)	lax01psc01 (0,1)	2
sfo01m01vc01	lax01m01vc01	3
sfo01w01vc01	lax01w01vc01	3
sfo01m01nsx01	lax01m01nsx01	4
sfo01w01nsx01	lax01w01nsx01	4
sfo01m01nsxc01	-	5
sfo01m01nsxc02	-	5
sfo01m01nsxc03	-	5
sfo01w01nsxc01	-	5
sfo01w01nsxc02	-	5
sfo01w01nsxc03	-	5
sfo01m01lb01 (0,1)	lax01m01lb01 (0,1)	6
sfo01m01udlr01 (0,1)	-	6
sfo01m01esg01	lax01m01esg01	6
sfo01m01esg02	lax01m01esg02	6
sfo01w01udlr01 (0,1)	-	6
sfo01w01dlr01 (0,1)	lax01w01dlr01(0,1)	6
sfo01w01esg01	lax01w01esg01	6
sfo01w01esg02	lax01w01esg02	6

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
<b>Update Manager Download Service (UMDS) Total Number of VMs (1)</b>	<b>Update Manager Download Service (UMDS) Total Number of VMs (1)</b>	<b>2</b>
sfo01umds01	lax01umds01	1
<b>Site Recovery Manager and vSphere Replication Total Number of VMs (2)</b>	<b>Site Recovery Manager and vSphere Replication Total Number of VMs (2)</b>	<b>2</b>
sfo01m01vrms01	lax01m01vrms01	1
sfo01m01srm01	lax01m01srm01	1
<b>vRealize Automation Total Number of VMs (11)</b>	<b>vRealize Automation Total Number of VMs (2)</b>	<b>3</b>
vra01mssql01	-	1
vra01svr01a	-	2
vra01svr01b	-	2
vra01iws01a	-	3
vra01iws01b	-	4
vra01ims01a	-	5
vra01ims01b	-	6
sfo01ias01a	lax01ias01a	7
sfo01ias01b	lax01ias01b	7
vra01dem01a	-	7
vra01dem01b	-	7
<b>vRealize Business for Cloud Total Number of VMs (2)</b>	<b>vRealize Business for Cloud Total Number of VMs (1)</b>	<b>4</b>
vr01svr01	-	1
sfo01vrbc01	lax01vrbc01	2
<b>vRealize Operations Manager Total Number of VMs (5)</b>	<b>vRealize Operations Manager Total Number of VMs (2)</b>	<b>5</b>
vrops01svr01a	-	1
vrops01svr01b	-	2
vrops01svr01c	-	3
sfo01vropsc01a	lax01vropsc01a	4
sfo01vropsc01b	lax01vropsc01b	4
<b>vRealize Log Insight Total Number of VMs (3)</b>	<b>vRealize Log Insight Total Number of VMs (3)</b>	<b>5</b>
sfo01vrli01a	lax01vrli01a	1
sfo01vrli01b	lax01vrli01b	2
sfo01vrli01c	lax01vrli01c	2