VMware Validated Design™ Upgrade Guide

VMware Validated Design for Software-Defined Data Center 3.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-002303-00

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

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com

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

Contents

1. Purpose and Intended Audience

VMware Validated Design Upgrade Guide provides step-by-step instructions for updating VMware solutions in the software-defined data center (SDDC).

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

Note The *VMware Validated Design Upgrade Guide* is validated with certain product versions. See *Upgrade Overview* for more information about supported product versions for this release.

VMware Validated Design Upgrade Guide 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.

2. Upgrade Overview

Data center updates and upgrades require a lot of time and effort. The VMware Validated Designs reduce risk and time in performing updates and upgrades by validating the procedures and software versions associated with each VMware Validated Design release.

SDDC Layer	Product Name	Product Version		Operation Type
		VMware Validated Design 2.0	VMware Validated Design 3.0	
Virtual Infrastructure	NSX for vSphere	6.2.2	6.2.4	Update
Operations Management	vRealize Log Insight	3.3.1	3.3.2	Update

Updates Validated by VMware Validated Designs

VMware Validated designs validate the following component updates and upgrade cases:

- Product Upgrade. Usually impacts SDDC design, and might include new features and bug fixes.
- Product Update. Usually includes new features, feature enhancements, and bug fixes, but does not include a change in the design.

Updates Not Validated by VMware Validated Designs

The VMware Validated Design is not scaled or functionally tested against individual patches, express patches or hot fixes. Patch your environment by following VMware best practices and KB articles. If an issue occurs during or after a VMware patch, contact VMware Technical Support.

Planning for an Update or Upgrade

Preparation and knowledge of the available software, tools, and resources can contribute to a successful upgrade. In addition to following VMware Validated Designs, understand how your Software-Defined Data Center is operating. You should check whether errors are present and know the performance level of important business functionality.

If you have issues during the update or upgrade process, contact VMware Technical Support.

Consider the following guidelines before you perform an update:

- Review the VMware product release notes.
- Schedule a maintenance window that is suitable for your organization and users.
- Allocate time in your maintenance window to run test cases and validate that all integrations, important business functionality, and system performance are acceptable. Add a time buffer for responding to errors without breaching the change window.
- Consider the impact of an update or upgrade to users. If you properly prepare for the upgrade, existing instances, networking, and storage should continue to operate.
- Consider the approach to upgrading your environment. Perform an upgrade with operational workloads carries risks. Consider using vSphere vMotion to temporarily migrate workloads to other compute nodes while performing an upgrade. Provide a notice to your users, including time to perform their own backups.
- Perform backups and snapshots of the VMware management components. Like all system upgrades, your update or upgrade might fail.

- Use the following procedures and evaluate them by using a test environment similar to your production environment.
  - After the update or upgrade, see VMware Validated Design Operational Verification for instructions to verify important functionality, integration and system performance.
  - After the update or upgrade, conduct a lessons learned meeting. Document improvements and ensure that they are incorporated in the next update or upgrade cycle.

3. Update NSX Manager and Controller Instances

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

Prerequisites

Before you update NSX for vSphere, verify that your environment can accommodate the update.

- Validate the NSX Manager file system usage, and perform a cleanup if file system usage is at 100 percent.
  - SSH to NSX Manager run `show filesystems` to show the `/dev/sda2` filesystem usage.
  - If the usage is 100 percent, run the `purge log manager` and `purge log system` commands.
  - Reboot the NSX Manager appliance for the log cleanup to take effect.
- Back up the NSX configuration and download technical support logs before upgrading. See *Backing Up and Restoring the NSX Instances in Region A* and *Backing Up and Restoring the NSX Instances in Region B*.
- Take a snapshot of the NSX Manager and NSX Controller virtual machines.
- Download the update bundle.
- Ensure that all of the controllers are in the normal state. Upgrading is not possible when one or more of the controllers are disconnected.
- Log into one of the hosts in the cluster and run the `esxcli software vib list | grep esx` command. Note the current version of the following VIBs:
  - `esx-dvfilter-switch-security`
  - `esx-vsip`
  - `esx-vxlan`

Procedure

1. Update the NSX Manager for the management cluster
2. Update the NSX Manager for the shared edge and compute cluster
3. Update the NSX Controllers for the management cluster
4. Update the NSX Controllers for the shared edge and compute cluster
5. Update the NSX components on the ESXi hosts in the management cluster
6. Update the NSX components on the ESXi hosts in the shared edge and compute cluster

- Update the NSX Manager Instances
- Upgrade the NSX Controllers
- Upgrade the NSX Components on the ESXi Hosts

- Change VXLAN Port
- Upgrade NSX Edge Instances

3.1 Update the NSX Manager Instances

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

In each region, you upgrade the NSX Manager for the management cluster first and then the NSX Manager for the shared edge and compute cluster.

Order	Region	NSX Manager Instance	NSX Appliance URL	vCenter Server URL
1	Region A	NSX Manager for the management cluster	https://mgmt01nsxm01.sfo01.rainpole.local	mgmt01vc01.sfo01.rainpole.local
2		NSX Manager for the shared edge and compute cluster	https://comp01nsxm01.sfo01.rainpole.local	comp01vc01.sfo01.rainpole.local
3	Region B	NSX Manager for the management cluster	https://mgmt01nsxm51.lax01.rainpole.local	mgmt01vc51.lax01.rainpole.local
4		NSX Manager for the shared edge and compute cluster	https://comp01nsxm51.lax01.rainpole.local	comp01vc51.lax01.rainpole.local

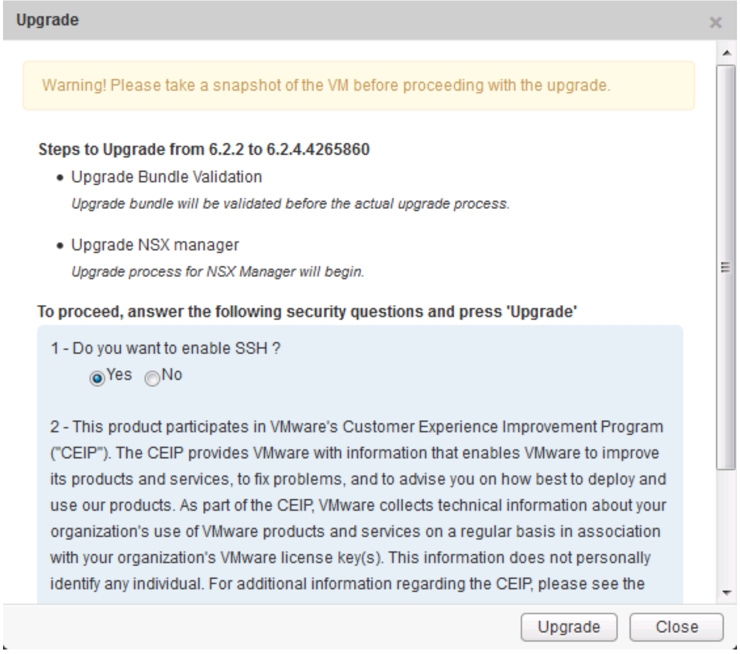
Procedure

1. Open the user interface of the NSX Manager appliance.
   a. Open a Web browser, go to `https://mgmt01nsxm01.sfo01.rainpole.local`.
   b. Use the following credentials.

Setting	Value
User Name	admin
Password	*mgmtnsx_admin_password*

2. In the appliance user interface, click **Upgrade**.
3. On the **Upgrade** page, click the **Upgrade** and browse your file system to locate the `.tar.gz` upgrade bundle.
4. Once the file has been located, click **Open** and then click **Continue**.

   The NSX Manager starts uploading the bundle.
5. After the upload is complete, in the **Upgrade** dialog box, select **Yes** next to **Do you want to enable SSH?** and **Do you want to join the VMware Customer Experience Program**, and click **Upgrade**.



Warning! Please take a snapshot of the VM before proceeding with the upgrade.

Steps to Upgrade from 6.2.2 to 6.2.4.4265860

- Upgrade Bundle Validation
  Upgrade bundle will be validated before the actual upgrade process.
- Upgrade NSX manager
  Upgrade process for NSX Manager will begin.

To proceed, answer the following security questions and press 'Upgrade'

1 - Do you want to enable SSH ?
● Yes ○ No

2 - This product participates in VMware's Customer Experience Improvement Program ("CEIP"). The CEIP provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s). This information does not personally identify any individual. For additional information regarding the CEIP, please see the

6. After the upgrade is complete, log in to the NSX Manager instance for the management cluster again and confirm that the upgade state is complete.

   a. If not already open, in a web browser, go to `https://mgmt01nsxm01.sfo01.rainpole.local`.

   b. Log in using the following credentials.

Setting	Value
User Name	admin
Password	*mgmtnsx_admin_password*

   c. On the home page of the appliance user interface, click **Upgrade** and on the **Upgrade** page verify that the **Upgrade State** is **Complete**.

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

   a. Open an SSH connection to the `mgmt01vc01.sfo01.rainpole.local` vCenter Server Appliance that the NSX manager is connected to.

   b. Log in using the following credentials.

Setting	Value
User Name	root
Password	*mgmtvc_root_password*

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

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

```
service-control –-start vsphere-client
```

8. Perform a fresh NSX Manager backup as the old backups cannot be restored to the new NSX Manager version.
9. Repeat the steps for the other NSX Manager instances in Region A and Region B.

3.2 Upgrade the NSX Controllers

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

For each NSX Manager, you start an upgrade for the connected NSX Controller cluster. During the upgrade, an upgrade file is downloaded to each controller node. The controllers are upgraded one at a time.

You start with the upgrading the NSX Controller cluster for the management cluster in Region A and then repeat the upgrade procedure for the NSX Controller cluster for the shared edge and compute cluster in Region A.

NSX Controller Properties in Region A

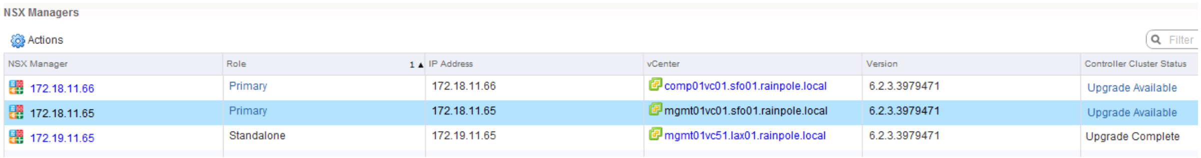
Region	NSX Manager	NSX Manager IP Address	NSX Controller IP Address
Region A	NSX Manager for the management cluster	172.16.11.65	172.16.11.118
			172.16.11.119
			172.16.11.120
	NSX Manager for the shared edge and compute cluster	172.16.11.66	172.16.31.118
			172.16.31.119
			172.16.31.120

Procedure

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

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

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



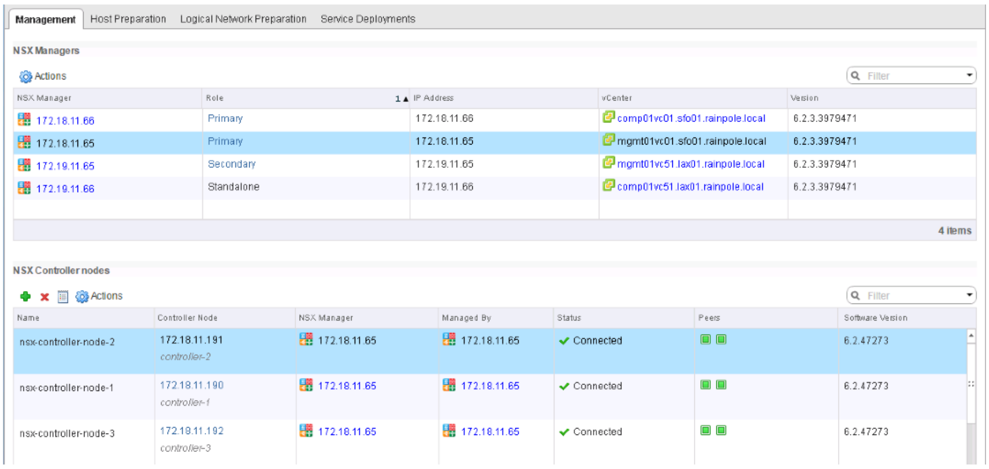
NSX Managers

Actions

NSX Manager	Role	IP Address	vCenter	Version	Controller Cluster Status
172.18.11.66	Primary	172.18.11.66	comp01vc01.sfo01.rainpole.local	6.2.3.3979471	Upgrade Available
172.18.11.65	Primary	172.18.11.65	mgmt01vc01.sfo01.rainpole.local	6.2.3.3979471	Upgrade Available
172.19.11.65	Standalone	172.19.11.65	mgmt01vc51.lax01.rainpole.local	6.2.3.3979471	Upgrade Complete

4. In the **Upgrade Controller** dialog, click **Yes**.

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



NSX Managers

Actions

NSX Manager	Role	IP Address	vCenter	Version
172.18.11.66	Primary	172.18.11.66	comp01vc01.sfo01.rainpole.local	6.2.3.3979471
172.18.11.65	Primary	172.18.11.65	mgmt01vc01.sfo01.rainpole.local	6.2.3.3979471
172.19.11.65	Secondary	172.19.11.65	mgmt01vc51.lax01.rainpole.local	6.2.3.3979471
172.19.11.66	Standalone	172.19.11.66	comp01vc51.lax01.rainpole.local	6.2.3.3979471

4 items

NSX Controller nodes

Actions

Name	Controller Node	NSX Manager	Managed By	Status	Peers	Software Version
nsx-controller-node-2	172.18.11.191 controller-2	172.18.11.65	172.18.11.65	✓ Connected	🟩 🟩	6.2.47273
nsx-controller-node-1	172.18.11.190 controller-1	172.18.11.65	172.18.11.65	✓ Connected	🟩 🟩	6.2.47273
nsx-controller-node-3	172.18.11.192 controller-3	172.18.11.65	172.18.11.65	✓ Connected	🟩 🟩	6.2.47273

5. Repeat the steps to start an upgrade of the nodes of the NSX Controller clusters for the shared edge and compute cluster in Region A.

3.3 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, compute and edge clusters.

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

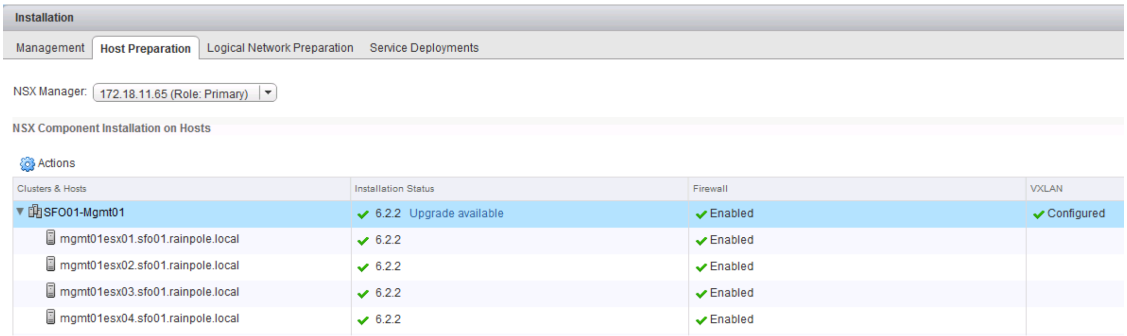
Region	NSX Manager	NSX Manager IP Address	Host Clusters
Region A	NSX Manager for the management cluster	172.16.11.65	SFO01-Mgmt01
	NSX Manager for the shared edge and compute cluster	172.16.11.66	SFO01-Comp01
Region B	NSX Manager for the management cluster	172.17.11.65	LAX01-Mgmt01
	NSX Manager for the shared edge and compute cluster	172.17.11.66	LAX01-Comp01

Procedure

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

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

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



NSX Manager: 172.18.11.65 (Role: Primary)

NSX Component Installation on Hosts

Clusters & Hosts	Installation Status	Firewall	VXLAN
SFO01-Mgmt01	✓ 6.2.2 Upgrade available	✓ Enabled	✓ Configured
mgmt01esx01.sfo01.rainpole.local	✓ 6.2.2	✓ Enabled	
mgmt01esx02.sfo01.rainpole.local	✓ 6.2.2	✓ Enabled	
mgmt01esx03.sfo01.rainpole.local	✓ 6.2.2	✓ Enabled	
mgmt01esx04.sfo01.rainpole.local	✓ 6.2.2	✓ Enabled	

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

   If the hosts must be in maintenance mode, for example, because of high availability requirements or DRS rules, the upgrade process stops and the cluster **Installation Status** becomes **Not Ready**.

7. If the **Installation Status** is **Not Ready** because the hosts must be in maintenance mode, manually evacuate the hosts, select the cluster again and click the **Resolve** action.
8. Repeat the steps to update the NSX components on the clusters in Region A and Region B.

3.4 Change the VXLAN Port

In NSX for vSphere 6.2.3 or later, the default VXLAN UDP port is 4789. This port is the standard port that is assigned by IANA. In earlier versions of NSX for vSphere, the default VXLAN UDP port number was 8472. After you upgrade NSX for vSphere, you must change the VXLAN port to enable the communication with NSX components that are based on a version 6.2.3 or later.

The cross-vCenter NSX setup does not require that you use 4789 for the VXLAN port. However, all hosts in a cross-vCenter NSX environment must be configured to use the same VXLAN port. Switching to VXLAN port 4789 ensures that new NSX installations added to the cross-vCenter NSX environment use the same port as the existing NSX deployments.

Prerequisites

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

Procedure

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

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

2. In the **Navigator**, click **Networking & Security**, and click **Installation**.
3. Click the **Logical Network Preparation** tab and click **VXLAN Transport**.
4. From the NSX Manager drop-down menu, select the IP address of the NSX Manager instance.

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

5. Click the **Change** button next to **VXLAN Port** and enter port number **4789**.

   Some time passes for NSX to propagate the port change to all hosts.
6. (Optional) In the REST client, check the progress of the port update on the NSX Manager instances.
   a. Log in to the Windows host that has access to your data center.
   b. In a Firefox browser, go to **`chrome://restclient/content/restclient.html`**.
   c. From the **Authentication** drop-down menu, select **Basic Authentication**.
   d. In the **Basic Authorization** dialog box, enter the following credentials, select **Remember me** and click **Okay**.

Authentication Attribute	Value
Username	admin
Password	*mngnsx_admin_password*

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

e. From the **Headers** drop-down menu, select **Custom Header**.

f. In the **Request Header** dialog box, enter the following header details and click **Okay**.

Request Header Attribute	Value
Name	`Content-Type`
Value	`application/xml`

The `Content-Type:application/xml` header appears in the Headers pane.

g. In the **Request** pane, from the **Method** drop-down menu, select **GET**.

h. In the **URL** text box, enter the following request URL and click **Send**.

NSX Manager Instance	Region	Request URL
NSX Manager for the management cluster	Region A	https://mgmt01nsxm01.sfo01.rainpole.local/api/2.0/vdn/config/vxlan/udp/port/taskStatus
NSX Manager for the shared edge and compute cluster	Region A	https://comp01nsxm01.sfo01.rainpole.local/api/2.0/vdn/config/vxlan/udp/port/taskStatus
NSX Manager for the management cluster	Region B	https://mgmt01nsxm51.lax01.rainpole.local/api/2.0/vdn/config/vxlan/udp/port/taskStatus
NSX Manager for the shared edge and compute cluster	Region B	https://comp01nsxm51.lax01.rainpole.local/api/2.0/vdn/config/vxlan/udp/port/taskStatus

The REST Client sends a query to the NSX Manager about the VXLAN UDP port status.

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

j. Within the `<vxlanPortUpdatingStatus>` element, locate the `<taskPhase>` and `<taskStatus>` elements for NSX Manager.

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
    <prevPort>8472</prevPort>
    <targetPort>4789</targetPort>
    <taskPhase>PHASE_TWO</taskPhase>
    <taskStatus>PAUSED</taskStatus>
```

```
</vxlanPortUpdatingStatus>
...
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
    <prevPort>8472</prevPort>
    <targetPort>4789</targetPort>
    <taskPhase>FINISHED</taskPhase>
    <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

3.5 Upgrade NSX Edge Instances

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

Procedure

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

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

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

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

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

5. For each NSX Edge instance, select **Upgrade Version** from the **Actions** menu.

Management Edge in Region A	Compute Edge in Region A	Management Edge in Region B	Compute Edge in Region B

SFOMGMT-ESG01	SFOMGMT-ESG01	LAXMGMT-ESG01	LAXCOMP-ESG01
SFOMGMT-ESG02	SFOCOMP-ESG02	LAXMGMT-ESG02	LAXCOMP-ESG02
UDLR01	UDLR01	-	-
SFOMGMT-LB01	-	LAXMGMT-LB01	-

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

4. Update vRealize Log Insight

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

Prerequisites

- Create a snapshot or backup copy of each vRealize Log Insight virtual appliance.
- Obtain a copy of the vRealize Log Insight upgrade bundle `.pak` file.
- Verify that you have a user with the `Edit Admin` permission for the vRealize Log Insight Web Interface.

vRealize Log Insight Nodes in the SDDC

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

4.1 Update the vRealize Log Insight Cluster

Start the update process from the vRealize Log Insight user interface of the master node.

Update the two vRealize Log Insight clusters subsequently.

Procedure

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

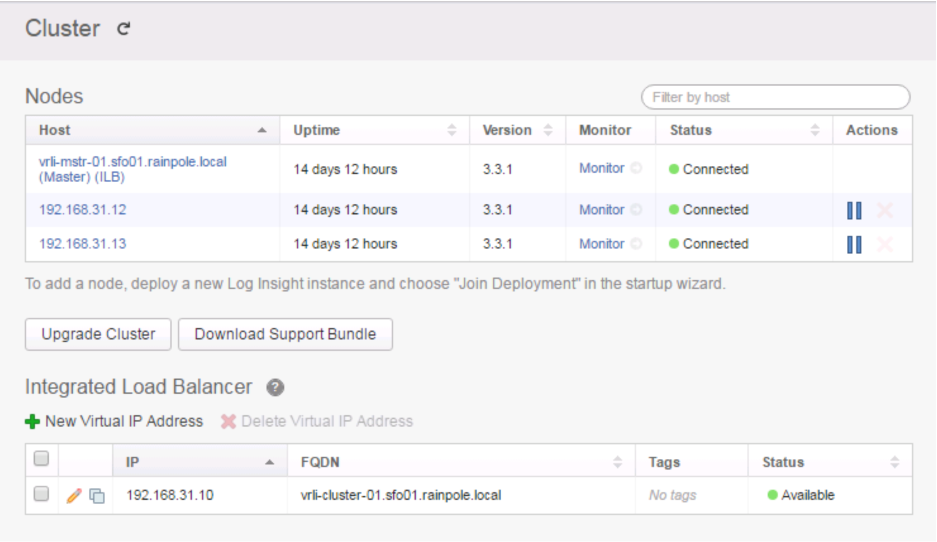
   a. Open a Web browser and go the master node for the cluster that you are updating.

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

   b. Log in using the following credentials.

Setting	Value
User Name	admin
Password	*vrli_admin_password*

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



Cluster

Nodes

Host	Uptime	Version	Monitor	Status	Actions
vrli-mstr-01.sfo01.rainpole.local (Master) (ILB)	14 days 12 hours	3.3.1	Monitor	● Connected	
192.168.31.12	14 days 12 hours	3.3.1	Monitor	● Connected	❚❚ ✕
192.168.31.13	14 days 12 hours	3.3.1	Monitor	● Connected	❚❚ ✕

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

Integrated Load Balancer

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

4. Click the **Upgrade Cluster** button.
5. Browse to the location of the vRealize Log Insight `.pak` file on your local file system and click **Open**.
6. In the **Upgrade Log Insight** dialog box, click **Upgrade** and wait until the `.pak` file uploads to the master appliance.
7. On the **End User License Agreement** page, click **Accept**.

   The **Upgrade Log Insight** progress dialog box opens.
8. When the update of the master node completes, the **Upgrade Successful** dialog box appears, click **OK**.

Update of all other nodes in the cluster starts automatically.

9. When the update process for the whole cluster completes, perform the procedure for the cluster in Region B.

4.2 Re-Enable the Integrated Load Balancer of vRealize Log Insight

After you perform an upgrade of the vRealize Log Insight cluster, you must re-enable the Integrated Load Balancer for balancing incoming ingestion traffic of syslog data among the Log Insight nodes and for high availability.

Procedure

1. Log in to the vRealize Log Insight user interface of the master node.
   a. Open a Web browser and go the following URL.

Region	URL
Region A	vrli-mstr-01.sfo01.rainpole.local
Region B	*vrli-mstr-51.lax01.rainpole.local*

   b. Log in using the following credentials.

Setting	Value
User Name	admin
Password	*vrli_admin_password*

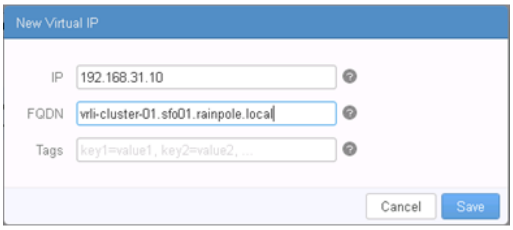
2. Click the configuration drop-down menu icon ☰ and select **Administration**.
3. Under **Management**, click **Cluster**.
4. Under **Integrated Load Balancer**, select the check box next to the existing load balancer with status **Unavailable**.

Region	Load Balancer
Region A	192.168.31.10
Region B	192.168.31.10

5. Disable the load balancer.
   a. Click **Delete Virtual IP Address**.
   b. In the **Delete Virtual IPs** dialog box, click **Delete**.
6. Re-enable the load balancer.
   a. Under **Integrated Load Balancer**, click **New Virtual IP Address**.
   b. In the **New Virtual IP** dialog box, enter the following settings and click **Save**.

Setting	Region A Value	Region B Value

IP Address	192.168.31.10	192.168.32.10
FQDN	*vrli-cluster-01.sfo01.rainpole.local*	*vrli-cluster-51.lax01.rainpole.local*



New Virtual IP

IP 192.168.31.10

FQDN vrli-cluster-01.sfo01.rainpole.local

Tags key1=value1, key2=value2, ...

7. Verify that the update completed successfully and remove the snapshots created before the update procedure. See Validate vRealize Log Insight in the Operational Verification documentation.
8. Repeat the steps for the vRealize Log Insight instance in the other region.