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
Contents

1 About vCloud NFV Platform Upgrade Guide 4

2 Overview of the vCloud NFV Platform Upgrade 5
   Acronyms and Definitions 5
   vCloud NFV Platform Topology 6
   Upgrade Sequence 7
   Upgrade Checklist 8

3 vCloud NFV Platform Upgrade Paths 9
   vCloud NFV 1.5.4 to vCloud NFV 2.1 9
       Platform Components for vCloud NFV 1.5.4 and vCloud NFV 2.1 9
       Network Topology 11

4 Upgrading vCloud NFV Platform 13
   Upgrading vCloud Director 13
   Upgrading VMware NSX Data Center for vSphere 14
   Upgrading VMware vSphere Environment 15
       Upgrade Platform Services Controllers 15
       Upgrading vCenter Server 16
   Upgrading vSphere Replication 17
   Upgrading vSphere Site Recovery Manager 17
   Upgrading vRealize Products for vCloud NFV 17
   Upgrading ESXi Hosts 18
   Upgrading the vSAN Cluster 18
   Post-Upgrade Checklist 18

Authors and Contributors 21
About vCloud NFV Platform Upgrade Guide

The vCloud NFV Platform Upgrade Guide provides information for upgrading the VMware vCloud NFV® platform from earlier versions based on the vCloud NFV Reference Architecture. The procedures in this guide are validated in the VMware labs.

Intended Audience

This guide is intended for users who want to upgrade the vCloud NFV platform from version 1.5.4 to 2.1.

To upgrade the vCloud NFV platform, you must

- Have knowledge about the deployment and configuration of the vCloud NFV platform product components.
- Be familiar with the vCloud NFV 2.0 Reference Architecture.
Overview of the vCloud NFV Platform Upgrade

This Platform Upgrade Guide provides the high-level upgrade steps that are essential to upgrade the vCloud NFV platform. This guide is best used together with the product documentation of each vCloud NFV component.

Note For more information about the vCloud NFV reference architecture and design, contact your VMware account manager or support team.

This Platform Upgrade guide provides information about the following upgrade path:

- vCloud NFV 1.5.4 to vCloud NFV 2.1
  vCloud NFV 2.1 release is based on NSX Data Center for vSphere. With this upgrade path, users can upgrade NSX Data Center for vSphere to its latest version that is available as part of the release bundle.

This chapter includes the following topics:

- Acronyms and Definitions
- vCloud NFV Platform Topology
- Upgrade Sequence
- Upgrade Checklist

Acronyms and Definitions

VMware vCloud NFV Platform uses a specific set of acronyms that apply to the NFV technology and the Telco industry.

NFV Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFVI</td>
<td>Network Functions Virtualization Infrastructure</td>
</tr>
<tr>
<td>PSC</td>
<td>Platform Services Controller</td>
</tr>
<tr>
<td>VDS</td>
<td>vSphere Distributed Switch</td>
</tr>
<tr>
<td>VIB</td>
<td>vSphere Installation Bundle</td>
</tr>
<tr>
<td>VIM</td>
<td>Virtualized Infrastructure Manager</td>
</tr>
</tbody>
</table>

VMware, Inc.
vCloud NFV Platform Topology

The vCloud NFV 2.x platform topology is based on the vCloud NFV reference architecture.

vCloud NFV is based on the 3-Pod design that consists of Management Pod, Edge Pod, and Resource Pod. Management Pod contains all the management components such as vCenter Server, NSX Manager, vCloud Director (VIM), and Operation and Analytics.

Figure 2-1. Layered Abstractions of the NFV Environment

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VNF</td>
<td>Virtual Network Function</td>
</tr>
<tr>
<td>VUM</td>
<td>VMware Update Manager</td>
</tr>
</tbody>
</table>
Upgrade Sequence

The vCloud NFV platform architecture components have interdependencies. When upgrading components, you must follow a particular upgrade sequence for the minimal impact to the running workloads and to ensure that there are no interoperability issues during the platform upgrade process.

**Note**
- This upgrade sequence applies to both 2-Pod and 3-Pod design.
- When you upgrade vCenter Server to 6.5 version, the connectivity of the vCenter Server with VMware vSphere® Replication™ and VMware Site Recovery Manager™ will not work. To enable the connectivity, upgrade VMware vSphere® Replication™ and VMware Site Recovery Manager™ to the compatible versions.
- After upgrading VMware vCenter Server, verify whether the host preparation is required for NSX Data Center for vSphere by scanning the baseline using VMware Update Manager. The scan result must not show any warning/error for conflicting VIBs for vxlan and vdpi.

**Upgrade Sequence**

The following table describes the sequence in which the NFV Reference Architecture (RA) components must be upgraded:

<table>
<thead>
<tr>
<th>NFV RA components</th>
<th>Management Pod</th>
<th>Resource and Edge Pod</th>
<th>Disaster Recovery Pod</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vCloud Director® Database</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMware vCloud Director® Cells</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMware NSX® Manager™ / VMware NSX® Controllers™</td>
<td>3</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>VMware NSX® Edge™ / Distributed Logical Router (DLR)</td>
<td>4</td>
<td>23</td>
<td>4</td>
</tr>
<tr>
<td>VMware Platform Services Controller™ (External)</td>
<td>5</td>
<td>16</td>
<td>5</td>
</tr>
<tr>
<td>VMware vCenter™ Server</td>
<td>6</td>
<td>17</td>
<td>6</td>
</tr>
<tr>
<td>VMware vSphere® Update Manager™</td>
<td>7</td>
<td>18</td>
<td>7</td>
</tr>
<tr>
<td>VMware vSphere® Replication™</td>
<td>8</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>VMware Site Recovery Manager™</td>
<td>9</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>NSX Data Center for vSphere Host preparation *</td>
<td></td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>VMware ESXi™ *</td>
<td>10</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>NSX Fabric (Host VIBs for ESXi) *</td>
<td></td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>VMware vSAN™</td>
<td>11</td>
<td>22</td>
<td>21</td>
</tr>
<tr>
<td>VMware vRealize® Network Insight</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMware vRealize® Orchestrate</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMware vRealize® Log Insight™</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMware vRealize® Operations™</td>
<td>12</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
* ESXi reboot is required.

**Upgrade Checklist**

The vCloud NFV Platform components follow strict upgrade guidelines. You must adhere to the checklist before performing an upgrade.

1. Ensure that the vCloud NFV 1.5.4 bundle is configured properly and is functional.
2. Ensure that the vCloud NFV 2.1 bundle is downloaded and available.
3. Ensure that enough storage capacity is available for backups and snapshots.
4. Take a snapshot and backup of each management component in the cluster before the upgrade.
5. Ensure that all components in the production network are patch current. For the list of components, see Upgrade Sequence.
6. Develop the upgrade sequence plan for the NFV solution deployed in the production network, based on the components identified in the previous step.
vCloud NFV Platform Upgrade

Paths

The vCloud NFV 2.1 platform supports the vCloud NFV upgrade from version 1.5.4 to 2.1.

This chapter includes the following topics:

- vCloud NFV 1.5.4 to vCloud NFV 2.1

vCloud NFV 1.5.4 to vCloud NFV 2.1

vCloud NFV 2.1 is a purpose-built carrier-grade cloud services platform with significant NFV-focused features that are designed to support CSP requirements. This section provides details about the platform components and network topology for the release.

Platform Components for vCloud NFV 1.5.4 and vCloud NFV 2.1

vCloud NFV includes required and recommended components. The required components are mandatory for the solution to function and the recommended components provide useful additional capabilities.
Figure 3-1. Virtual Building Blocks NFV

Note  Based on the upgrade path, review the appropriate VMware components required for the NFV solution.

<table>
<thead>
<tr>
<th>Component</th>
<th>vCloud NF 1.5.4</th>
<th>vCloud NFV 2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESXi™</td>
<td>6.0 U3a</td>
<td>6.5 U3</td>
</tr>
<tr>
<td>VMware vCenter™ Server Appliance™</td>
<td>6.0 U3c</td>
<td>6.5 U3d</td>
</tr>
<tr>
<td>VMware Virtual SAN™</td>
<td>6.0</td>
<td>6.5.0</td>
</tr>
<tr>
<td>VMware vSphere® Replication™</td>
<td>6.1.2.1</td>
<td>6.5.1.3</td>
</tr>
<tr>
<td>VMware vCloud Director® for Service Providers</td>
<td>8.10.1.1</td>
<td>9.1.0.3</td>
</tr>
<tr>
<td>VMware vRealize® Operations™</td>
<td>6.6.1</td>
<td>7.5</td>
</tr>
<tr>
<td>VMware vRealize® Log Insight™</td>
<td>4.5.1</td>
<td>4.8.0</td>
</tr>
<tr>
<td>VMware vRealize® Orchestrator Appliance</td>
<td>7.3.0</td>
<td>7.4.0</td>
</tr>
<tr>
<td>VMware Site Recovery Manager™</td>
<td>6.1.2.1</td>
<td>6.5.1.3</td>
</tr>
</tbody>
</table>
### Network Topology

The vCloud NFV platform consists of various network segments. These network segments are primarily divided into infrastructure networks and tenant networks.

The infrastructure network traffic includes VMkernel traffic such as VMware vSphere® vMotion®, VMware Virtual SAN™, VMware vSphere® Replication™, and host management. Tenant networks (physical VLAN networks) such as VM Management VLAN connect the management virtual machines (VMs) to the hypervisor.

All ESXi hosts in the vCloud NFV platform are configured with VMware vSphere® Distributed Switches™ (VDS), which provide the consistent network configuration across multiple hosts as required by VMware NSX Data Center for vSphere. The hypervisor VMkernel networks are configured on an infrastructure VDS, and the tenant networks are configured on a tenant VDS on each of the ESXi hosts.

### Infrastructure Networks

Each ESXi host has multiple VMkernel port groups configured for each infrastructure network. The infrastructure networks are

- **vMotion Network**: Used for the vSphere vMotion traffic.
- **Virtual SAN Network**: Used for the Virtual SAN shared storage traffic.
- **ESXi Management**: Used for the ESXi host management traffic.
- **Replication Network**: Used for communication between hosts at the protected and recovery sites.

### Tenant Networks

Tenant networks are used to interconnect the VMs of the vCloud NFV platform. These networks are configured on a dedicated tenant VDS in each of the pods. The tenant networks are

- **VNF Network**: Overlay network for VNF to VNF communication.
- **Management VLAN**: VLAN-based network for the management component communication.

### Management, Edge, and Resource Pods

The vCloud NFV infrastructure platform contains a Management pod, a Resource pod, and an Edge pod. Separate vCenter and NSX Manager instances are used to manage the Management pod. The NSX Manager in the Management pod is leveraged to provide network services such as load balancing to vCloud Director Cells.
Figure 3-2. The vCloud NFV Host Network Design
Upgrading vCloud NFV Platform

Upgrading NFV includes upgrading vCloud Director, NSX Data Center for vSphere, the required NSX components, vCenter Server, vRealize Suite of products, vSphere Site Recovery Manager, and ESXi hosts.

This chapter includes the following topics:

- Upgrading vCloud Director
- Upgrading VMware NSX Data Center for vSphere
- Upgrading VMware vSphere Environment
- Upgrading vSphere Replication
- Upgrading vSphere Site Recovery Manager
- Upgrading vRealize Products for vCloud NFV
- Upgrading ESXi Hosts
- Upgrading the vSAN Cluster
- Post-Upgrade Checklist

Upgrading vCloud Director

This section provides instructions for upgrading the vCloud Director from version 8.10.1.1 to 9.1.0.3. The vCloud Director installer verifies that the target server meets all upgrade prerequisites and upgrades the vCloud Director on the server.

Prerequisites

- Verify that you have superuser credentials for the servers in your vCloud Director server group.
- Verify that the vCloud Director database, vSphere components, and the NSX components are compatible with the new version of vCloud Director.
- Verify that all ESXi hosts are enabled. Starting with vCloud Director 9.1.0.3, disabled ESXi hosts are unsupported.
- Take a backup or snapshot of the vCloud Director cells before upgrading them.
Back up your existing database before you upgrade it. Use the backup procedures that your database software vendor recommends.

**Procedure**

1. Upgrade the vCloud Director. See [Upgrading vCloud Director](#).
2. Upgrade the vCloud Director database. See [Upgrade vCloud Director Database](#).

   **Note** All cells in a vCloud Director server group use the same database. Regardless of how many cells you are upgrading, you need to upgrade the database only once.

3. If you are using Microsoft SQL Server 2012, follow this procedure:
   a. Install Windows Server 2012 R2 Update 1 (Microsoft [KB2919355](#)).
      
      **Important**
      - If you have issues when installing, see [Microsoft KB 2919442](#).
   c. Install the latest SQL Server Management Studio (SSMS).

4. Upgrade vCloud Director on the remaining cells in the group.

---

**Upgrading VMware NSX Data Center for vSphere**

Upgrading VMware NSX® Data Center for vSphere® involves upgrading NSX Manager Appliance, NSX Controller cluster, NSX host clusters, and NSX Edge, in the order specified.

**Prerequisites**

- Refer to the following topics in the NSX Upgrade guide:
  - System Requirements for NSX
  - Preparing for the NSX Upgrade
  - Take a backup of the NSX components before starting any upgrade. For more information, see the NSX Backup and Restore section.

**Note** The upgrade process is managed by NSX Manager. If the upgrade of a component fails or is interrupted and you repeat or restart the upgrade, the upgrade process begins from the point at which it stopped. The upgrade process does not start over from the beginning.

**Procedure**

1. Upgrade the NSX Manager Appliance.
2. Upgrade the NSX Controller Cluster.
3. Upgrade the NSX host configuration.
4 Upgrade NSX Edge Appliance.

Edge Services Gateway instances can be upgraded at any time after the NSX Manager upgrade. However, logical routers cannot be upgraded until the NSX Controller cluster and host clusters are upgraded. For more information about upgrade dependencies, see the Operational Impacts of NSX Upgrades section of the NSX Upgrade Guide.

Upgrading VMware vSphere Environment

This section describes upgrading VMware vSphere includes upgrading External Platform Services Controllers (PSCs) and vCenter Server sequentially.

Upgrade Platform Services Controllers

This section describes upgrading PSCs. To upgrade a PSC, follow this procedure.

The PSC upgrade from version 6.0 to 6.5 is a two-stage process:

- **Stage 1: Deploy the OVA file of the new PSC appliance.** In this first stage of the upgrade process, deploy the OVA file of the new PSC appliance 6.5 version.
- **Stage 2: Transfer data and set up the newly deployed PSC appliance.** When the OVA deployment is complete, transfer data from the old appliance and start the services of the newly deployed PSC appliance 6.5 version.

**Prerequisites**

- Ensure that you backed up all data on the source appliance before starting the upgrade.
- Refer to the Prerequisites for Upgrading the vCenter Server Appliance or Platform Services Controller Appliance.
- Upgrade PSCs sequentially.
- Migration Assistant should be running inside Windows-based PSC. See Download and Run VMware Migration Assistant on the Source Windows Machine.

**Procedure**

1 Upgrade the PSC Appliance from version 6.0 to 6.5. For more information, see Upgrade a Platform Services Controller Appliance 6.0 by Using the GUI.
   
   a Download the VMware vCenter Server Appliance (VCSA) 6.5 ISO Appliance build from [my.vmware.com](http://my.vmware.com).
   
   b Mount the ISO and navigate to the `vcsa-ui-installer` directory. Start the installer by double-clicking the Installer file.
   
   c Click **Upgrade** on the 6.5 Installer page.
Migrate Windows-based PSC 6.0 to Appliance-based PSC 6.5 version. For more information, see GUI Migration of vCenter Server with an External vCenter Single Sign-On or Platform Services Controller to an Appliance.

a. Download the VMware VCSA 6.5 ISO Appliance from my.vmware.com.
b. Mount the ISO and navigate to the `vcsa-ui-installer` directory. Start the installer by double-clicking the Installer file.
c. Click Migrate on the 6.5 Installer page.

Upgrading vCenter Server

This section describes upgrading vCenter Server. To upgrade the vCenter Server appliance, follow this procedure.

The vCenter Server upgrade from version 6.0 to version 6.5 is a two-stage process.

- **Stage 1: Deploy a new vCenter Server appliance to the target.** Deploy a new appliance to the target vCenter Server or ESXi host.
- **Stage 2: Copy data from the source vCenter Server appliance.** Complete the upgrade process by copying data from the source appliance to the deployed appliance.

**Note**
- VMware vSphere Update Manager is now embedded in the vCenter Server Appliance version 6.5.
- vCenter Update Manager is unavailable after upgrading to vCenter Server Appliance 6.5. For more details, see VMware Knowledge Base article 60430.

**Prerequisites**
- Ensure that you backed up all data on the source appliance before starting the upgrade.
- **Prerequisites for Upgrading the vCenter Server Appliance or Platform Services Controller Appliance.**
- Migration Assistant should be running inside the Windows-based vCenter Server and Update Manager. See Download and Run VMware Migration Assistant on the Source Windows Machine.

**Procedure**

1. Upgrade vCenter Server Appliance from version 6.0 to 6.5. For more information, see GUI Migration of vCenter Server with an External vCenter Single Sign-On or Platform Services Controller to an Appliance.
   - a. Download the VMware VCSA 6.5 ISO Appliance build from my.vmware.com.
   - b. Mount the ISO and navigate to the vcsa-ui-installer directory. Start the installer by double-clicking the Installer file.
   - c. Click Upgrade on the 6.5 Installer page.
2 Migrate Windows-based vCenter Server 6.0 to Appliance-based vCenter Server 6.5. For more information, see Migrating vCenter Server for Windows to vCenter Server Appliance.

a Download the VMware VCSA 6.5 ISO Appliance from my.vmware.com.

b Mount the ISO and navigate to the vcsa-ui-installer directory. Start the installer by double-clicking the Installer file.

c Click Migrate on the 6.5 Installer page.

Upgrading vSphere Replication

To upgrade vSphere Replication, you must upgrade the required components in your vSphere environment in a specific order.

Note Before upgrading the components on the recovery site, you must upgrade all components on the protected site. If you have issues that prevent you from using the protected site while completing the upgrade, use the recovery site to restore the protected site to its original state. The ESXi host can be upgraded at any time.

To upgrade vSphere Replication, see Upgrading vSphere Replication.

Upgrading vSphere Site Recovery Manager

To upgrade Site Recovery Manager (SRM), perform several tasks in order. You must complete all the upgrade tasks on the protected site first and then complete the tasks on the recovery site.

Note During the upgrade, SRM is unavailable until you upgrade SRM and vSphere Replication to the latest version 6.5.1.2.

For information about prerequisites, best practices, and steps for upgrading SRM, see Upgrade Site Recovery Manager.

Upgrading vRealize Products for vCloud NFV

You must follow a specific sequence to upgrade vRealize Log Insight, vRealize Operations Manager, vRealize Orchestrator, and vRealize Network Insight.

Procedure

1 Upgrade vRealize Log Insight. For more information, see Upgrading to vRealize Log Insight 4.8.

You must upgrade agents in the required VMs to capture data appropriately. For example, upgrade the agents in these VMs: Domain Name System (DNS), vRealize Orchestrator, vRealize Orchestrator Database, vCloud Director Cells, vCloud Director Database, Site Recovery Manager. For more details, See Installing or Upgrading vRealize Log Insight Agents.
2 Upgrade vRealize Operations Manager. For more information, see vRealize Operations Manager Software Updates 7.5.

**Important** Before upgrading, refer to Before Upgrading to vRealize Operations Manager 7.5.

3 Upgrade vRealize Orchestrator. For more information, see Upgrade an Orchestrator Cluster 6.0.x and Later to 7.4.

While upgrading vRealize Orchestrator, you need to deploy a new node. For more information, see Configuring a Standalone Orchestrator Server.

4 Upgrade vRealize Network Insight. For more information, see Upgrading vRealize Network Insight 4.2.

**Note** KB 60368 article provides information on how to fix an issue that prevents from logging in to VMware vRealize Network Insight (vRNI) from the Chrome browser.

## Upgrading ESXi Hosts

When upgrading ESXi on a host, you must also install new NSX VIBs on the host to be compatible with the new ESXi version.

For instructions to upgrade ESXi hosts in the VMware NSX Data Center for vSphere environment, see Upgrading ESXi 6.5 in an NSX Environment.

## Upgrading the vSAN Cluster

Upgrading vSAN is a multistage process and you must perform the upgrade in a specific sequence.

**Note** The disk format upgrade is optional. If you use a previous disk format version, your vSAN cluster continues to run smoothly. For best results, upgrade the objects to use the latest on-disk format. The latest on-disk format provides the complete feature set of vSAN. To understand the vSAN upgrade process, see About the Virtual SAN Disk Format.

To upgrade vSAN Cluster, see Upgrading the vSAN Cluster.

## Post-Upgrade Checklist

After upgrading the vCloud NFV platform, you must verify that all components work as expected.

<table>
<thead>
<tr>
<th>Category</th>
<th>Component</th>
<th>Verify</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Infrastructure</td>
<td>Network</td>
<td>- Switches are reachable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- All VLAN communications are working properly.</td>
</tr>
<tr>
<td></td>
<td>Compute</td>
<td>- In a browser window, open https://esxi_host.</td>
</tr>
<tr>
<td>Category</td>
<td>Component</td>
<td>Verify</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Storage</td>
<td>vSAN is accessible and is in a healthy state.</td>
<td></td>
</tr>
</tbody>
</table>
| NFVI and VIM                | Management and Resource vCenter Server | Management and Resource vCenter Servers are accessible.  
|                             |                                    | All cluster properties are correct.                                    |
|                             |                                    | All vSphere Distributed Switches are working properly.                 |
| vCloud Director             | vCloud Director is accessible using its load balancer and using individual Cell FQDN.  
|                             | vCloud Director is successfully upgraded, registered with vCenter Server, and configured to work with VMware NSX Data Center for vSphere. |
| Site Recovery Manager       | Site Recovery Manager is successfully upgraded on the protected (the Management Pod) and recovery sites and the sites are paired.  
|                             |                                    | The protected and recovery sites are connected, and the pair appears on the home page of the Site Recovery user interface.  
|                             |                                    | Both SRMs from the protected and recovery sites are accessible.         |
| vSphere Replication         | The vSphere Replication appliance is successfully upgraded on the protected (Management Pod) and recovery sites, and sites are paired.  
|                             | vSphere Replication servers are registered with respective vCenter Server for both the protected and recovery sites. |
| VMware NSX for vSphere      | NSX Manager and its component connection status must be up and in Green color. |
| Operations Management       | vRealize Log Insight is accessible and the network data is actively collected and stored.  
<p>|                             |                                    | All configured content pack components are accessible.                 |
| vRealize Operations Manager | vRealize Operations Manager is accessible.                                    |
|                             | All configured management components are accessible.                           |</p>
<table>
<thead>
<tr>
<th>Category</th>
<th>Component</th>
<th>Verify</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vRealize Network Insight</td>
<td>- vRealize Network Insight is accessible and the syslog data is actively received and stored.</td>
</tr>
<tr>
<td></td>
<td>vRealize Orchestrator</td>
<td>- vRealize Orchestrator is accessible.</td>
</tr>
<tr>
<td>Delete Snapshots</td>
<td>All Management Components</td>
<td>- Delete the Snapshots that you took before the upgrade as a prerequisite.</td>
</tr>
</tbody>
</table>
Authors and Contributors

The author of this guide is:

- Ashish Chorge, NFV Solution Engineering, VMware.

Many thanks for contributions from:

- Andrea Li, Lead Solutions Test Architect, NFV Solutions Engineering, VMware.
- Michelle Han, Director, Solutions Testing and Validation, NFV Solutions Engineering, VMware.
- Ramesh Tammana, Senior Manager Solutions Engineering - Telecommunications, VMware.
- Sudesh Tendulkar, Staff Solutions Architect, NFV Solution Engineering, VMware.

Special thanks for their valuable feedback to: