vSAN 6.7 Upgrade Considerations

First Published On: 07-28-2017
Last Updated On: 06-06-2018
Table Of Contents

1. Introduction
   1.1. Overview
   1.2. Supported Upgrade Paths for vSAN 6.6.1
2. vSAN 6.7 On Disk Upgrade Considerations
   2.1. vSAN on-disk format versions and data services
   2.2. On-Disk Format disk evacuation considerations
3. vSAN 6.7 Upgrade and Networking communications
   3.1. vSAN 6.6.1 Upgrade and vSAN Cluster communication
   3.2. vSAN Networking behaviors in mixed vSAN clusters
4. vSAN On-Disk Format Conversion Process
   4.1. vSAN Disk Format Upgrade Process
   4.2. Allow Reduced Redundancy
5. vSAN VUM Integration
   5.1. vSAN VUM Integration Overview
   5.2. vSAN VUM Configuration
   5.3. vSAN VUM Generated Recommendations
6. vSAN Witness Appliance Upgrade Considerations
   6.1. VMware vSAN Witness Appliance Upgrade
7. vSphere Upgrade Overview
   7.1. vCenter Server Upgrade Documentation and Software.
   7.2. vSphere ESXi Upgrade Documentation and Software.
8. vSAN 6.7 Upgrade Check list
   8.1. VMware vSAN Upgrade Check list
9. Appendix A: Upgrade Troubleshooting
   9.1. vSphere Upgrade troubleshooting
   9.2. vSAN On-Disk Upgrade Troubleshooting
   9.3. Troubleshooting Unicast Communications
10. Appendix B: vSAN On-disk Format Upgrade example
    10.1. vSAN disk format conversion upgrade to Version 5.0
1. Introduction

vSAN 6.7 Upgrade Overview
1.1 Overview

Introduction

With the general availability of VMware vSphere 6.5 Update 1, also included is vSAN 6.6.1, which adds, even more, new features on top of the major vSAN 6.6 release that launched, namely

- VMware vSphere Update Manager (VUM) integration
- Storage Device Serviceability enhancement
- Performance Diagnostics in vSAN

Upgrading VMware vSAN is a multistage process, in which you must perform the upgrade procedures in the order described here.

Before you attempt to upgrade, make sure you understand the complete vSphere upgrade process to ensure a smooth and uninterrupted upgrade.

If you are not familiar with the general vSphere upgrade procedure, you must first review the vSphere Upgrade Documentation and verify any potential interoperability issues with other VMware Solutions before an upgrade.

Please review VMware product interoperability matrix for more product interoperability concerns. For specific supported upgrade paths please review the VMware product interoperability upgrade section.

This upgrade guide will guide you through the process of upgrading from a previous release of vSAN.
Overview of High Level VMware vSAN Cluster Upgrade tasks

- **Plan Upgrade**
  - Review the vSphere release notes vSphere vCenter 6.5 U1 and ESXi 6.5 U1 release notes
  - Verify your server hardware against the VMware vSAN Hardware compatibility matrix
  - Before upgrading confirm if your VMware vSAN/vSphere solution is using any other solutions or plugins by reviewing the VMware product interoperability matrix for guidance.

- **Backup configuration**
  - For vCenter 6.x Backup and restore options
    - Please review VMware KB 2149237 [https://kb.vmware.com/kb/2149237](https://kb.vmware.com/kb/2149237) for guidance.
  - For vCenter versions prior to 6.x
    - Please review VMware KB 2119754 [https://kb.vmware.com/kb/2119754](https://kb.vmware.com/kb/2119754) for guidance.
  - ESXi configurations can be backed up via command line.
    - Please review vSphere Documentation Backing Up Configuration Information with vicfg-cfgbackup for guidance.
  - ESXi systems can also be reverted to a previous image if a host was updated.
    - Please review VMware KB [https://kb.vmware.com/kb/1033604](https://kb.vmware.com/kb/1033604) for guidance.

- **Patch or Upgrade vCenter Server**
  - Please review vSphere documentation [vCenter 6.5 Upgrade](https://kb.vmware.com/kb/1033604) for guidance.
If patching vCenter Appliance please review VMware documentation Patching and Updating vCenter Server 6.5 Deployments for guidance.

- **Patch or Upgrade ESXi**
  - Please review VMware documentation ESXi Upgrade for guidance.

- **HCL Verification**
  - Verify vSAN Storage IO components are valid against VMware vSAN HCL.
  - Update the vSAN HCL Database file, please review VMware KB https://kb.vmware.com/kb/2145116.
  - Driver and firmware for both controllers and disks must be checked for compliance against VMware vSAN HCL.

- **Perform Disk Format Version upgrade to Version 5.0**
  - Depending on the prior version of vSAN and the default Disk Format Version, an object and disk format conversion may take place.
  - This can be a potentially time consuming process if data evacuation is required.

**Note:** Once you upgrade the on-disk format, you cannot roll back software on the hosts or add certain older hosts to the cluster. For more details see VMware KB https://kb.vmware.com/kb/2148493.

1.2 Supported Upgrade Paths for vSAN 6.6.1
Below table describes the supported upgrade paths for VMware vSAN enabled hosts.

<table>
<thead>
<tr>
<th>Source vSAN Version</th>
<th>Source vSphere Release</th>
<th>Target vSAN Version</th>
<th>Target vSphere Release</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5</td>
<td>vSphere ESXi 5.5 with patch ESXi550-201504001</td>
<td>6.6.1</td>
<td>vSphere ESXi 6.5 Update 1</td>
<td>ESXi 6.5. U1 Build 5969303</td>
</tr>
<tr>
<td>6.0</td>
<td>vSphere 6.0 GA</td>
<td>6.6.1</td>
<td>vSphere ESXi 6.5 Update 1</td>
<td>ESXi 6.5. U1 Build 5969303</td>
</tr>
<tr>
<td>6.1</td>
<td>vSphere 6.0 Update 1.</td>
<td>6.6.1</td>
<td>vSphere ESXi 6.5 Update 1</td>
<td>ESXi 6.5. U1 Build 5969303</td>
</tr>
<tr>
<td>6.2</td>
<td>vSphere 6.0 Update 2</td>
<td>6.6.1</td>
<td>vSphere ESXi 6.5 Update 1</td>
<td>ESXi 6.5. U1 Build 5969303</td>
</tr>
<tr>
<td>6.2</td>
<td>vSphere 6.0 Update 3</td>
<td>6.6.1</td>
<td>vSphere ESXi 6.5 Update 1</td>
<td>ESXi 6.5. U1 Build 5969303</td>
</tr>
<tr>
<td>6.5</td>
<td>vSphere 6.5 GA</td>
<td>6.6.1</td>
<td>vSphere ESXi 6.5 Update 1</td>
<td>ESXi 6.5. U1 Build 5969303</td>
</tr>
<tr>
<td>6.6</td>
<td>vSphere 6.5 EP2 ESXi650-201704001</td>
<td>6.6.1</td>
<td>vSphere ESXi 6.5 Update 1</td>
<td>ESXi 6.5. U1 Build 5969303</td>
</tr>
</tbody>
</table>

Table 1. Supported Upgrade Paths.

1. VMware does not support upgrading from vSphere 6.0 U3 to vSphere 6.5 GA as per vSphere upgrade policy. VMware however does support upgrading from vSphere 6.0 U3 to vSphere 6.5 Update 1. Please see VMware KB [https://kb.vmware.com/kb/2149840](https://kb.vmware.com/kb/2149840) and vSphere upgrade matrix [http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#upgrade](http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#upgrade) for latest information on this guidance.

For further information regarding upgrade requirements please see VMware KB vSAN upgrade requirements [https://kb.vmware.com/kb/2145248](https://kb.vmware.com/kb/2145248).
2. vSAN 6.7 On Disk Upgrade Considerations

VMware vSAN 6.7 On Disk Format Upgrade Considerations and recommendations pertaining to upgrading to vSAN 6.7
2.1 vSAN on-disk format versions and data services

As of vSAN 6.7 and vSAN 6.6, the versioning of major vSAN releases may depend on the version number of the vSAN on-disk format. Going forward, every major vSAN software release maps to a single vSAN On-Disk format version. As of vSAN 6.7 the disk format version is 6.0.

vSAN gets upgraded in two phases: First, the hypervisor software, vSphere (vCenter and ESXi) and then the on-disk disk format.

The table below describes the existing versioning up to and including vSAN 6.7 The table also lists the features introduced with each on-disk format version.

<table>
<thead>
<tr>
<th>Disk Format Version</th>
<th>vSphere Release</th>
<th>vSAN Version</th>
<th>Data Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1</td>
<td>vSphere 5.5 Update 1, Update 2, Update 3.</td>
<td>5.5</td>
<td></td>
</tr>
<tr>
<td>Version 2</td>
<td>vSphere 6.0</td>
<td>6.0</td>
<td>All Flash, vSAN Sparse Snapshots.</td>
</tr>
<tr>
<td>Version 2</td>
<td>vSphere 6.0 Update 1.</td>
<td>6.1</td>
<td>Stretch Cluster</td>
</tr>
<tr>
<td>Version 3</td>
<td>vSphere 6.0 Update 2 / vSphere 6.0 Update 3.</td>
<td>6.2</td>
<td>De-duplication and Compression, Checksum.</td>
</tr>
<tr>
<td>Version 3</td>
<td>vSphere 6.5 GA</td>
<td>6.5</td>
<td></td>
</tr>
<tr>
<td>Version 5.0</td>
<td>vSphere 6.5 EP2</td>
<td>6.6</td>
<td>Encryption (data at rest)</td>
</tr>
<tr>
<td>Version 5.0</td>
<td>vSphere 6.5 U1</td>
<td>6.6.1</td>
<td></td>
</tr>
<tr>
<td>Version 6.0</td>
<td>vSphere 6.7</td>
<td>6.7</td>
<td></td>
</tr>
</tbody>
</table>

Table 2. On-disk version data-services feature mapping
On Disk Format Upgrades and data evacuation

Depending on the source version of vSAN, the vSAN on disk format may get upgraded.

The On-Disk Format exposes your environment to the complete feature set of vSAN. An On-Disk Format Upgrade may require an object conversion process and disk group data evacuation.

As a result, the disk format upgrade can be quite time-consuming. This depends on how many objects and on the size of disk groups.

If a disk group evacuation is necessary, each disk group is upgraded one at a time. For each disk group upgrade, all data from each capacity device is evacuated and the disk group is removed from the vSAN cluster. The disk group is then added back to vSAN with the new on-disk format.

Disk Format Version 6.

While V6.0 is a new disk format version for vSAN 6.7, it does not add addition features or data services at this time. However VMware recommends as a best practice to upgrade to latest Disk Format Version.

Note Once you upgrade the on-disk format to V6.0, you cannot roll back software on the hosts or add certain older hosts to the cluster. For more details see VMware KB https://kb.vmware.com/kb/2148493

When performing a disk format version from V5.0 to 6.0 This disk format conversion does not require a data evacuation, but an in-place metadata update.

The same guidance applies for V3.0 to v6.0 or indeed V3.0 to V5.0.

The following table summarizes the disk format upgrade conversion, and data movement.

<table>
<thead>
<tr>
<th>Source vSAN Version</th>
<th>Target vSAN Version</th>
<th>DFC Conversion</th>
<th>Source To Target Disk Version Change</th>
<th>1MB Object Alignment</th>
<th>vSAN Object Conversion</th>
<th>Data Evacuation</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSAN 5.5 U1</td>
<td>vSAN 5.5 Update X</td>
<td>No</td>
<td>V 1.0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Copyright © 2019 VMware, Inc. All rights reserved.
# vSAN 6.7 Upgrade Considerations

<table>
<thead>
<tr>
<th>Source vSAN Version</th>
<th>Target vSAN Version</th>
<th>DFC Conversion</th>
<th>Source To Target Disk Version Change</th>
<th>1MB Object Alignment</th>
<th>vSAN Object Conversion</th>
<th>Data Evacuation</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSAN 5.5 UX</td>
<td>vSAN 6.0 vSAN 6.1 vSAN 6.2 vSAN 6.5 vSAN 6.6 vSAN 6.6.1 vSAN 6.7</td>
<td>Yes</td>
<td>V1.0 -&gt; V3.0 / V5.0 / V6</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>vSAN 6.0 / 6.1</td>
<td>vSAN 6.2</td>
<td>Yes</td>
<td>V2.0 -&gt; V3.0</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>vSAN 6.2</td>
<td>vSAN 6.5</td>
<td>No</td>
<td>V3.0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>vSAN 6.0 / 6.1</td>
<td>vSAN 6.6 vSAN 6.6.x</td>
<td>Yes</td>
<td>V2.0 -&gt; V5.0</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>vSAN 6.2</td>
<td>vSAN 6.6 vSAN 6.6.x</td>
<td>Yes</td>
<td>V3.0 -&gt; V5.0</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>vSAN 6.5</td>
<td>vSAN 6.6 vSAN 6.6.x</td>
<td>Yes</td>
<td>V3.0 -&gt; V5.0</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>vSAN 6.6</td>
<td>vSAN 6.6.1 vSAN 6.6.2</td>
<td>No</td>
<td>V5.0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Copyright © 2019 VMware, Inc. All rights reserved.
Table 3. vSAN On-disk Conversion

vSphere 6.7 still supports all vSAN Disk format versions from V1 to latest version. Thus older disk format versions are supported to be upgraded to latest versions even if vSphere versions are mismatched.

For example it is supported to start with vSAN 6.0/6.1 with Disk Format Version 1.0 and upgrade to vSAN 6.7 and Disk Format Version 6.0.

For vSAN on-disk format version support matrix see VMware KB "Understanding vSAN on-disk format versions and compatibility (2145267)" [https://kb.vmware.com/s/article/2145267](https://kb.vmware.com/s/article/2145267)

3. vSAN 6.6 has a new disk format version V5.0 rather than a new ondisk format. Updating disk groups from Version 3 to Version 5.0 is a metadata update and does not require data evacuation.

4. vSAN 6.7 has a new disk format version V6.0 rather than a new ondisk format. Updating disk groups from Version 3 to Version 6.0 is a metadata update and does not require data evacuation.

5. vSAN 6.7 has a new disk format version V6.0 rather than a new ondisk format. Updating disk groups from Version 5 to Version 6.0 is a metadata update and does not require data evacuation.

Note: Encryption at Rest can be configured during Version 5.0 / V6.0 Disk Group format upgrade, but requires the presence of a Key Management Server (KMS) registered to the vCenter server. Data evacuation must be performed to enable encryption at rest. Enabling vSAN Encryption at Rest is out of scope in this document. For more information please review vSAN documentation [Using Encryption on a vSAN Cluster](https://www.vmware.com/support/pubs/doc.html#vSAN).
VMware vSAN 6.6.1 On Disk Format Upgrade Considerations

Depending on the source version of VMware vSAN, the VMware vSAN on disk format may get upgraded. The On-Disk Format exposes your environment to the complete feature set of VMware vSAN.

An On-Disk Format Upgrade may require an object conversion process and disk group data evacuation. As a result, the disk format upgrade can be quite time-consuming. This depends on how many objects and on the size of disk groups.

Each disk group is upgraded one at a time. For each disk group upgrade, all data from each capacity device is evacuated and the disk group is removed from the VMware vSAN cluster. The disk group is then added back to VMware vSAN with the new on-disk format.

This can be IO intensive operation, due care must be taken to ensure a vSAN Cluster is in optimal condition to perform a disk evacuation

- All hosts are connected and have correct software version.
- All disks are healthy.
- All storage controllers and drives adhere to the vSAN HCL minimum requirements.
- Automatic disk claiming is disabled.
- All objects are accessible and healthy.
- Adequate capacity is available across the vSAN Datastore.

vSAN 6.6.1 (6.6) Disk group evacuation pre-check

With the vSAN 6.6.1 (6.6) release, administrators can now pre-check what may happen when disk group data evacuation is performed. This is valuable to check prior to performing a disk format conversion that requires data evacuation. This will quickly determine how much data needs to be moved and if it is safe to do so.

The example below shows how this is achieved

From a vSAN enabled cluster, **Select Configure -> vSAN -> Disk Management** Select an appropriate disk group and use the **pre-check evacuation icon** to determine how much data will be moved.

![Figure 1. pre-check data evacuation](image)

Disk evacuation pre-check will estimate how much data will be moved and if it is possible to do so.
Figure 2. Evacuate data estimate

Note: the vSphere Ruby vSphere Console (RVC) also has a `vsan.whatif_host_failures` command to determine if you have enough capacity to successfully finish the upgrade or perform a component rebuild in case you encounter a failure during the upgrade. This is an alternative to above approach and can be used on vSAN environments prior to vSAN version 6.6. Please review vSphere Documentation, Upgrade vSAN Disk Format Using RVC for more details.
3. vSAN 6.7 Upgrade and Networking communications

vSAN 6.7 Upgrade Considerations for vSAN Networking
This chapter discusses the effect of upgrading vSAN nodes and disk group software versions on vSAN Networking.
3.1 vSAN 6.6.1 Upgrade and vSAN Cluster communication

vSAN 6.6.1 Upgrade and Mixed Cluster Networking Considerations

Upgrading host and disk group software versions influences vSAN Cluster Networking modes used for vSAN cluster communications.

In VMware vSAN 6.6, 6.6.1 and later releases, multicast is no longer required on the physical switches that support the VMware vSAN cluster. VMware vSAN 6.6 and vSAN 6.6.1 now communicates using unicast for vSAN Cluster updates. However during upgrade there will be a transition from multicast to unicast. Transitioning from multicast to unicast has implications depending on combination of vSphere software versions and vSAN disk group format versions during the upgrade process.

During a VMware vSAN cluster upgrade, VMware vSAN nodes will be in mixed mode from a software versioning perspective, i.e. some nodes can be running on releases prior to VMware vSAN 6.6 or vSAN 6.6.1, while others can run at versions earlier than VMware vSAN 6.6.1 / 6.6. While this is supported for the duration of the upgrade process, the following multicast and unicast behavior is noted:

- A VMware vSAN cluster will continue to operate in multicast mode until all participating cluster nodes are upgraded to VMware vSAN 6.6.1 or vSAN 6.6.

- A uniform VMware vSAN 6.6.1 / 6.6 Cluster will communicate using unicast with legacy disk-groups present. A legacy disk group is any disk group at Version 3.0 or below.
  - However, a VMware vSAN 6.6.1 / 6.6 cluster will switch to back multicast mode when non-vSAN 6.6.1 / 6.6 nodes are added.
- VMware vSAN 6.6 clusters, where at least one node has a v5.0 on-disk format disk group will permanently communicate in unicast.
  - A non-vSAN 6.6 node added to this cluster will not be able to communicate with the VMware vSAN 6.6 nodes via multicast and it will be partitioned.

vSAN Networking Mode is now displayed on the vSAN Cluster Configuration page on the vSphere Client as can be seen on Figure 4 below.

![Figure 4. Networking Mode](image)

vSAN Networking Mode can also be determined by using esxcli from a host command-line shell.
**esxcli vsan cluster get** displays vSAN Cluster Summary and what communications mode vSAN is using, as can be seen on Figure 5.

![Image 1](image1.png)

**Figure 5. unicast mode enabled at cluster level**

**esxcli vsan cluster unicastagent list** displays all vSAN nodes operating in unicast mode as can be seen on Figure 6.

![Image 2](image2.png)

**Figure 6. list of vSAN nodes communicating in unicast**

### 3.2 vSAN Networking behaviors in mixed vSAN clusters

**Expected Networking communications in mixed Cluster mode.**

The following table summarizes the possible combinations when a vSAN cluster can switch to unicast or to multicast and when the change is made permanent.
<table>
<thead>
<tr>
<th>vSAN Cluster Software Configuration</th>
<th>Disk Format Version (s)</th>
<th>vSAN Communication Mode</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.6.1 Only Nodes 6.6 Only Nodes</td>
<td>Version 5</td>
<td>Unicast</td>
<td>Cluster permanently operates in unicast. The Cluster cannot revert to multicast. Any new pre vSAN 6.6 nodes added to cluster in this state will be partitioned away. (e.g. vSAN 6.2 nodes)</td>
</tr>
<tr>
<td>6.6.1 Only Nodes 6.6 Only Nodes</td>
<td>Version 3.0 or below</td>
<td>Unicast</td>
<td>6.6.1 and 6.6 nodes operate will operate in unicast mode. The Clusters will switch to multicast when pre vSAN 6.6 nodes are added. (e.g. vSAN 6.2 nodes)</td>
</tr>
<tr>
<td>Mixed 6.6.1 (6.6) and vSAN pre-6.6 Nodes</td>
<td>Version 3.0 or Version 2.0</td>
<td>Multicast</td>
<td>vSAN cluster operates in multicast mode. All vSAN nodes must be upgraded to 6.6 or 6.6.1 to switch to unicast mode. A subsequent disk format upgrade to v5 will make unicast mode permanent.</td>
</tr>
<tr>
<td>Mixed 6.6.1 (6.6) and vSAN 5.X Nodes</td>
<td>Version 1.0</td>
<td>Multicast</td>
<td>vSAN Cluster operates in multicast mode. All VMware vSAN nodes must be upgraded to 6.6.1 (6.6) to switch to unicast mode. A subsequent disk format upgrade to V5.0 will make unicast mode permanent.</td>
</tr>
<tr>
<td>Mixed 6.6.1 (6.6) and vSAN 5.X Nodes</td>
<td>Version 5.0 and Version 1.0</td>
<td>Unicast</td>
<td>6.6.1 (6.6) nodes operate in unicast mode. vSAN 5.x nodes with v1 disks operate in multicast mode during host software upgrade.</td>
</tr>
</tbody>
</table>

Table 5. vSAN communications mode during upgrades
4. vSAN On-Disk Format Conversion Process

Explanation on the possible workflows and vSAN cluster changes made during on-disk format conversion upgrade
4.1 vSAN Disk Format Upgrade Process

Disk Format Upgrade Process

When you initiate an upgrade of the on-disk format, VMware vSAN may perform several operations. Table 6 summarizes each process that may take place during the disk format upgrade. The workflow for Version 1.0 and/or Version 2.0 on-disk format upgrade process to V5.0 is described here.

<table>
<thead>
<tr>
<th>Percentage Complete</th>
<th>Description</th>
</tr>
</thead>
</table>
| 0%-5%               | Cluster check. Cluster components are checked and prepared for the upgrade. This process takes a few minutes. VMware vSAN verifies that no outstanding issues exist that can prevent completion of the upgrade.  
  - All hosts are connected.  
  - All hosts have the correct software version.  
  - All disks are healthy.  
  - Automatic disk claiming is disabled.  
  - All objects are accessible |
| 5%-10%              | Disk group upgrade. (Version 2.0 source only) VMware vSAN performs the initial disk upgrade with no data migration. This process takes a few minutes. This will convert disk groups to an interim disk group Version 2.5 during upgrade. |
| 10%-15%             | Object realignment (Version 2.0 to Version 5.0/ 3.0). VMware vSAN modifies the layout of all objects to ensure that they are properly aligned. This process can take a few minutes for a small system with few snapshots. However it can take many hours or even days for large a system with many snapshots, many fragmented writes, and many unaligned objects. |
| 15%-95%             | Disk group removal and reformat (if required). Each disk group is removed in a gradual fashion from the cluster, by default, to ensure object accessibility. Once an individual disk group has been removed, it will be added back to the cluster before moving onto the next disk group. The time required for this process varies, depending on the megabytes allocated and the system utilization. A system at or near its I/O capacity transfers slowly. |
| 95%-100%            | Final object version upgrade. Object conversion to the new on-disk format and re-synchronization is completed. The time required for this process varies, depending on the amount of space used and whether the Allow Reduced Redundancy option is selected. |

Table 6. on-disk format process
3. When converting from Version 1.0 to Version 5.0 vSAN realigns objects and their components to have a 1 MB address space and then performs a data evacuation.

4. For more information regarding VMware vSAN on disk upgrade process and troubleshooting please review VMware Knowledge base article 2144881 https://kb.vmware.com/kb/2144881

---

**On-Disk Version 3 to Version 5 Upgrades.**

Converting from on-disk Version 3.0 to Version 5.0 requires a **meta-data update only** to the disk group format. **No data evacuation is required**. As a consequence it is not necessary to set Allow Reduced Redundancy on 2-Node 3-Node Clusters.

---

### 4.2 Allow Reduced Redundancy

**Allow Reduced Redundancy**

When you allow reduced redundancy, your Virtual Machines may be temporarily **unprotected** for the duration of the disk format upgrade, as this method does not evacuate data to the other hosts in the cluster. During disk format upgrade with the allow reduced redundancy option selected, a single point of failure maybe exposed. vSAN restores full compliance and redundancy after the format conversion is completed. Ensure that you have followed all VMware best practices and your business practices related to the backup of important data and virtual machines.

There is a large amount of operational risk associated with selecting this option for example in a 3 node cluster, setting Allow Reduced Redundancy, will remove a component of an object to remove and add a disk group. This means the object cannot tolerate another failure if another host or disk group goes unavailable. It is highly recommended by VMware that more nodes or capacity should be added to a cluster to ensure there are adequate resources to perform a disk format conversion.

However, in some vSAN Cluster topologies setting “Allow Reduced Redundancy” is necessary, e.g. 2-Node vSAN Cluster topologies

**Upgrading the On-disk Format for vSAN Clusters with Limited Capacity or small vSAN Clusters.**

As discussed, upgrading from on-disk Version 1 or Version 2.0 to Version 5 requires data evacuation. When a data evacuation is required during an upgrade of the VMware vSAN on-disk format, disk groups are removed and upgraded to the target on-disk format version, as the disk groups are added back to the cluster.

This process may fail for VMware vSAN Clusters deployed in the following scenarios when the source on-disk format is Version 1.0 or Version 2.0 and the target Version is Version 5 (or indeed Version 3.0):

- Three-Node clusters.
- 2-Node / 2-Node direct connect cluster.
- Stretch Clusters that contain a single vSAN Disk Group.
- Clusters with Failure Tolerance method set to RAID-5/6 (Erasure Coding) with minimum number of hosts (Four Nodes for Raid-5; Six Nodes for Raid-6).
Clusters without enough capacity to fully evacuate each disk group

With the introduction of VMware vSAN 6.6 and 6.6.1 we can enable "Allowed Reduced Redundancy" option from the vSphere Web Client when invoking the on-disk format upgrade process.

Please see Figure 7 below when invoking an on-disk format upgrade conversion.

![Figure 7. Allowed Reduced Redundancy checkbox.](image)

A vSAN administrator may also use the Ruby vSphere Console (RVC) to set “allowed Reduced Redundancy” please see VMware KB 2144944 [https://kb.vmware.com/kb/2144944](https://kb.vmware.com/kb/2144944) for further guidance.

For more information on the Ruby vSphere Console see [VMware vSAN documentation](https://www.vmware.com/support/pubs/vsan-6.7.html)
5. vSAN VUM Integration

This chapter will highlight the integration for vSAN 6.7 and vSphere Update Manager and how to streamline software upgrades for vSAN nodes.
5.1 vSAN VUM Integration Overview

vSAN and vSphere Update Manager integration

With the release of vSAN 6.6.1, vSphere Update Manager (VUM) automatically generates upgrade recommendations to ensure a vSAN cluster is running the latest supported versions of vSphere and vSAN.

VUM automatically pulls and combines information from the VMware Compatibility Guide and vSAN Release Catalog with information about the currently installed ESXi release. The vSAN release catalog, hosted on the VMware Cloud, maintains information about available releases, preference order for releases, and critical patches needed for each release. In addition, VUM identifies new, asynchronously-released drivers that need to be installed for select hardware vendors. Recommendations for upgrades, patches, and drivers are automatically generated using this information and awareness of the underlying hardware configuration. This new enhancement to VUM makes it much easier to determine the latest supported vSphere and vSAN versions for an environment.

System Requirements

- vCenter Server 6.5 Update 1
  - Windows vCenter Server will require VMware Update Manager 6.5 Update 1 installed separately
  - vCenter Appliance contains Update Manager by default
- vCenter Server Update Manager requires Internet access to download ISO images and patches.
  - Please review VMware vCenter Update Manager network port requirements [https://kb.vmware.com/kb/1004543](https://kb.vmware.com/kb/1004543)
- Internet Access to my.vmware.com required
- Internet Access or Offline Access to vSAN HCL Database
- ESXi 6.0 Update 2 and later

Note: You do not need to participate in the Customer Experience Improvement Program (CEIP) to use this feature.

How VUM creates Recommendations for vSAN

vSAN automatically generates a read-only system baseline and baseline groups for use with vSphere Update Manager. This is achieved by downloading the vSAN HCL database and the vSAN Releases Database from my.vmware.com and creating the necessary recommendations.

System Baselines are created and maintained based on the latest data from VMware Cloud. System baselines are a new type of baseline available now on vSAN VUM. This baseline is read-only and as a result cannot be edited. One baseline is generated per vSAN cluster.

We can have 3 system baselines:

- Upgrade / Update Baseline (Major and Update releases)
- Patch Baseline (Critical Patches)
- Driver Baseline (Drivers from HCL DB)

vSAN system baselines do not affect user-defined baselines. vSAN system baselines are refreshed automatically every 24 hours, however the following events can also trigger vSAN Updates to VUM:

- If a host is added/removed to a vSAN enabled Cluster
- The vSAN (vSAN health Service) management service restarts.
- vSAN detects updates to the vSAN release catalog.
- vSAN detects updates to the vSAN HCL.
The vSAN HCL database is not checked on releases prior to vSAN 6.2 (vSphere 6.0 U2). Controller firmware is NOT re-mediated through VUM. If a vSAN node or cluster controller hardware is not on vSAN HCL VUM will still recommend the latest release.

The vSAN Configuration Assist and Updates feature handles firmware updates for more information please review vSAN 6.6.1 Administration guide

vSAN Health Checks

A new vSAN Health group, vSAN Build Recommendation, is available now for vSAN VUM integration. This includes two new health tests.

vSAN Build Recommendation Engine Health

Check that the vSAN VUM build engine has all dependencies met such as internet access, login to my.vmware.com, metadata up-to-date.

For more information please review VMware KB https://kb.vmware.com/kb/2150914

vSAN build recommendation

Health test to test for vSAN build recommendations appropriate to the vSAN cluster, existing hardware based on the vSAN release matrix and vSAN HCL database.

For more information please review VMware KB https://kb.vmware.com/kb/2150915

Not Supported

At this time VMware vSphere Update Manager Download Service (UMDS) is not supported for vSAN VUM integration. Offline ISO depots are also not supported.

Remediation

Remediation is not automatic and has to be instigated to by the administrator and the administrator is not required to follow the system baseline recommendations if they so choose.

A single host can be re-mediated in a given vSAN Cluster or you can re-mediate the entire vSAN Cluster.
5.2 vSAN VUM Configuration

vSAN VUM Configuration steps

The main configuration step required for vSAN VUM integration is simply supplying my.vmware.com credentials to download applicable updates.

When vCenter Server (and vCenter Update Manager) has been upgraded to vSphere 6.5 Update 1, as discussed two new health checks for vSAN VUM integration will be made available to vSAN Health Service.

my.vmware.com credentials must be updated on the vSAN Build Recommendation Engine Health test

Procedure

1. From the vSphere WebClient, select vSAN Cluster > Monitor > vSAN > Health
2. locate vSAN Build Recommendation Engine Health test
   As can be seen in the supplied screenshot, the test is failing with warning as my.vmware.com login credentials are not supplied.
3. Select "Login to my.vmware.com" and enter in valid username and password and click ok.

Once this initial configuration is complete, the vSAN VUM engine will build a system baseline based on the existing vSAN cluster, using vSAN build recommendations and vSAN HCL Database. This may take up to ten minutes to complete. For more information, please review VMware KB [https://kb.vmware.com/kb/2150914](https://kb.vmware.com/kb/2150914).

Older vSphere Releases and vSAN VUM Integration

For hosts running 6.0 Update 1 and earlier, you must use RVC to enter My VMware credentials using vsan.login_iso_depot RVC command.

The Ruby vSphere Console (RVC) provides a command-line interface used for managing and troubleshooting the vSAN cluster. RVC gives you a cluster-wide view, instead of the host-centric view offered by esxcli. RVC is bundled with vCenter Server Appliance and vCenter Server for Windows, so you do not need to install it separately. For information about the RVC commands, please review [RVC Command Reference Guide](https://kb.vmware.com/kb/2150914).

Procedure

1. Login to rvc onto vCenter server with appropriate credentials.
2. issue vsan.login_iso_depot --username <my vmware login> --password <your password>

While vSAN build recommendations will be generated, vSAN HCL recommendations will not be generated with hosts running 6.0 Update 1 and earlier.
5.3 vSAN VUM Generated Recommendations

Recommendations and Remediation

In this section we will review common vSAN VUM recommendations and system defined upgrade base lines

Upgrade Scenario 1: Host Upgrade, vSAN nodes HCL compliant

vSAN 6.0 U3 cluster
Storage Controller on vSAN VCG but driver out of date

In this scenario vSAN VUM has detected the vSAN cluster is running vSphere 6.0 U3 and recommending to upgrade to vSphere 6.5 U1 (vSAN 6.6.1)

However the controller used for vSAN disk groups has an older driver, Health check has flagged this as an issue, and recommended that the storage driver get updated
The system generated baseline has been created, attached, and the vSAN cluster has been scanned for compliance.

The system baseline is "host upgrade" base line as its an upgrade from 6.0 to 6.5 U1

There are four hosts to remediate in "Cluster1", the administrator is informed that the hardware is supported.

we are alerted that the controller driver needs to be updated.

Once remediation was completed the vSAN Cluster is compliant from build and HCL driver perspective as the ESXi 6.5 U1 image contained the correct storage driver.

Upgrade Scenario 2: Host Upgrade, vSAN nodes NOT HCL compliant

vSAN 6.6 Cluster (vSphere 6.5 EP2)
Storage controller not on HCL

In this scenario vSAN VUM has detected the vSAN cluster is running vSphere 6.5 EP2 (or vSAN 6.6) and recommending to upgrade to vSphere 6.5 U1 (vSAN 6.6.1)
it is also detected by the vSAN Health checks that the storage controller used is not on the vSAN HCL.

Although the controller used is not detected to be on the HCL, vSAN VUM will still generate an upgrade recommendation to upgrade to vSphere 6.5 U1 as the resulting upgrade will still keep the same status quo.

To elaborate the cluster will still have a controller that is not detected to be on the HCL at the target vSphere version, but the cluster will be upgraded to most recent version of vSAN (6.6.1)
6. vSAN Witness Appliance Upgrade Considerations

This chapter discusses vSAN Witness appliance upgrade and recommendations for 2-Node and Stretch Cluster Topologies.
6.1 VMware vSAN Witness Appliance Upgrade

VMware vSAN Witness Appliance Upgrade Considerations

Specific VMware vSAN configurations, such as a stretched cluster and 2-Node deployments, require a vSAN witness host. Instead of using a dedicated physical ESXi host as a witness host, you can deploy the VMware vSAN witness appliance. The appliance is a pre-configured virtual machine that runs ESXi and is distributed as an OVA file.

Unlike a general-purpose ESXi host, the witness appliance does not run virtual machines. Its only purpose is to serve as a vSAN witness.

However upgrading a VMware vSAN Witness Appliance can use the same process as vSphere ESXi Nodes and does not require special handling from a vSphere Upgrade perspective.

VMware vSAN Witness nodes are located outside of VMware vSAN enabled vSphere Cluster, but are managed by the same vCenter instance, as a result they can be re-mediated using Update Manager or `esxcli software update` in the same way with a VMware vSAN data node.

**Note**: all vSAN nodes, including witness nodes must be upgraded to vSAN 6.6.1 to enable the cluster to communicate in unicast mode and allow on-disk Format Upgrades to Version 5.0 to proceed.

As we can see in Figure 8, we have a VMware vSAN Witness Node attached to a Stretch Cluster. We note that the cluster is still communicating in Multicast mode and On-disk Format Version Pre-Check Upgrade checks for presence of older versions of software

![Figure 8. Pre-check fails due to witness host at older vSphere version](image)

Using VMware Update Manager with Stretched Clusters and 2-Node Deployments

Using vSphere Update Manager to upgrade hosts in parallel might result in the witness host being upgraded in parallel with one of the data hosts in a stretched cluster / 2-Node configurations. To avoid upgrade problems, do not configure VMware Update Manager to upgrade a witness host in parallel with the data hosts in a stretched cluster.
Upgrade the witness host after all data hosts have been successfully upgraded and have exited maintenance mode.

**Replace or Upgrade vSAN Witness Appliance?**

With the release of vSAN 6.6 and vSAN 6.6.1 we now have the functionality to replace a faulty vSAN witness appliance from the vSphere web client, as can be seen on Figure 9.

![Figure 9. Change Witness host workflow with vSAN 6.6](image)

However, the “change witness host procedure” should **not be used** as a method to upgrade a witness node for the following reasons:

- As per the [vSAN 6.6.1 release notes](https://www.vmware.com/support/pubs/ps5001.html) and [vSAN 6.6 release notes](https://www.vmware.com/support/pubs/ps4659.html) “known issues”, if a vSAN node is replaced before an on-disk format conversion is performed, then the disk group created may be at an incompatible version than the vSAN data nodes, and in this case the witness host will not be able to store witness components.
- If a witness host is changed rather than replaced in this manner, then all witness objects will have to be rebuilt on the witness node disk group and depending on how many objects this may take time. The vSAN cluster objects are exposed to a double failure, while the witness node’s objects are being rebuilt. An inplace upgrade will avoid this exposure.
7. vSphere Upgrade Overview

This chapter gives a brief overview of existing upgrade guidance and vSphere software versions needed to reach vSAN 6.7 supported levels.
7.1 vCenter Server Upgrade Documentation and Software.

vCenter Server Upgrade documentation and software.

VMware provides many options to upgrade to vCenter Server 6.5. You can upgrade or migrate from vCenter 5.5 or 6.0 to VMware vCenter version 6.5 using the method that best addresses your deployment goals and requirements.

Please review vCenter 6.5 Upgrade process.

As mentioned VMware vSAN 6.6.1 leverages a vSphere patch release to deliver a new VMware vSAN release with major features. vSAN 6.6.1 is delivered as a full vSphere Update, i.e. vSphere 6.5 Update 1. Due care must be taken to ensure vCenter Server Instances that are managing VMware vSAN clusters are upgraded BEFORE upgrading VMware vSAN enabled hosts to vSAN 6.6.1 or vSAN 6.6. This is extremely important to adhere to, to ensure a smooth upgrade and avoid unexpected outages.

Note: vCenter Servers must be upgraded to vSphere 6.5 Update 1 before vSAN hosts are upgraded to vSAN 6.6 or vSAN 6.6.1

Windows Based vCenter Systems

Windows based vCenter systems can be directly installed or upgraded from ISO to vSphere vCenter Server Version 6.5 Update 1 [https://my.vmware.com/group/vmware/details?productId=646&rPlId=15839&downloadGroup=VC65U1#errorCheckDiv](https://my.vmware.com/group/vmware/details?productId=646&rPlId=15839&downloadGroup=VC65U1#errorCheckDiv)

vCenter Server Appliances (VCSA)

VCSA appliances can be patched or upgraded to vSphere 6.5 Update 1 (which contains vSAN 6.6.1) depending on what version of vCenter Appliance has already been deployed.

- For Customers that have deployed VCSA Version 6.5 they must patch the VCSA appliance to vCenter Server Version 6.5 Update 1
  The VMware vCenter Server Appliance Update Bundle can be downloaded directly from [https://my.vmware.com/group/vmware/details?downloadGroup=VC650D&productId=646&rPlId=15839#errorCheckDiv](https://my.vmware.com/group/vmware/details?downloadGroup=VC650D&productId=646&rPlId=15839#errorCheckDiv)
  Please review VMware KB [https://kb.vmware.com/kb/2149879](https://kb.vmware.com/kb/2149879)
  Please see vSphere Documentation [Patching the vCenter Server Appliance and Platform Services Controller Appliance](https://kb.vmware.com/kb/2149879) for patching guidance.

- For Customers on earlier releases of vCenter Server Appliance, i.e. VCSA 5.5 or VCSA 6.0 customers can upgrade to VCSA 6.5 Update 1. The VCSA upgrade ISO can be downloaded directly from [https://my.vmware.com/group/vmware/details?productId=646&rPlId=15839&downloadGroup=VC65U1#errorCheckDiv](https://my.vmware.com/group/vmware/details?productId=646&rPlId=15839&downloadGroup=VC65U1#errorCheckDiv)
  Please review vSphere documentation [About the Upgrade Process of the vCenter Server Appliance and Platform Services Controller Appliance](https://kb.vmware.com/kb/2149879) for upgrade guidance.
7.2 vSphere ESXi Upgrade Documentation and Software.

vSphere ESXi Upgrade reference documentation and software download locations

After you upgrade the vCenter Server, the next task for the VMware vSAN cluster upgrade is upgrading the ESXi hosts to use the current version.

VMware provides several ESXi upgrade options. Choose the upgrade option that works best with the type of host that you are upgrading.

For more information about various upgrade options, see the vSphere Documentation, Overview of the ESXi host Upgrade Process

Before you attempt to upgrade the ESXi hosts, review the requirements and best practices as discussed in vSphere documentation, Upgrading ESXi Hosts.

vSphere ESXi 6.5 Deployments

VMware vSAN customers can simply patch existing ESXi 6.5 systems to vSphere 6.5 Update 1 and can be downloaded at https://my.vmware.com/group/vmware/patch

Earlier vSphere ESXi versions

Customers can upgrade directly from prior releases using an ISO upgrade method or via the new vSAN VMware vSphere Update Manager (VUM) integration process.

Customized OEM ISOS

Selected partners may provide customized ISO’s for vSphere 6.5 U1 (vSAN 6.6.1)

For more information, please reach out to your hardware support team.

VMware vSAN Witness Appliance Upgrade

Existing VMware vSAN Witness Appliances can also be patched as per ESXi host upgrade process.

However, new Witness Appliance’s for VMware vSAN 6.6.1 (6.5U1) can be downloaded in OVA file (VMware-vSAN-Witness-6.5.0.update01-5969303.ova) format from https://my.vmware.com/group/vmware/details?downloadGroup=WITNESS_OVA_651&productId=646
vSphere Update Manager and Maintenance Mode

With VMware vSAN enabled, there are three host maintenance mode Options

- **Full Data Migration.** Evacuate all the components to other hosts in the cluster.
- **Ensure Accessibility.** Evacuate enough components to ensure that virtual machines can continue to run, albeit at risk.
- **No Data Migration.** Don’t evacuate any components from this host.

If you have multiple hosts in the VMware vSAN cluster, and you use vSphere Update Manager to upgrade the hosts, the default evacuation mode is Ensure data accessibility. If you use this mode, and while upgrading VMware vSAN you encounter a failure, your data maybe at risk during upgrade.

**Note:** Since the release of vSAN 6.1 default Maintenance mode behavior can be controlled via ESXi advanced system setting option `VSAN.DefaultHostDecommissionMode`, which defaults to the value `ensureAccessibility`. This value should be verified before using vSphere Update Manager.
8. vSAN 6.7 Upgrade Check list

Simple Check list before upgrading to vSAN 6.7
8.1 VMware vSAN Upgrade Check list

VMware vSAN Upgrade:- Plan and Check

In summary, plan and design your upgrade to be failsafe as possible. Before you attempt to upgrade VMware vSAN, verify that your environment meets the vSphere hardware and software requirements. Below is an optional check list that can be used as a reference.

<table>
<thead>
<tr>
<th>Upgrade Perquisites</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software, hardware, drivers, firmware, and storage I/O controllers</td>
<td>Verify that the software and hardware components, drivers, firmware, and storage I/O controllers that you plan on using are supported by VMware vSAN for 6.6 and later, and are listed on the <a href="https://www.vmware.com">VMware vSAN Compatibility Guide</a> website. Strict adherence to the vSAN Compatibility guide is crucial.</td>
</tr>
<tr>
<td>Virtual Machines</td>
<td>Verify that you have backed up your virtual machines.</td>
</tr>
</tbody>
</table>
| VMware vSAN Version                                      | Verify that you are using the latest patched version of VMware vSAN prior to upgrade. Please review VMware KB 2146381 [https://kb.vmware.com/kb/2146381](https://kb.vmware.com/kb/2146381)  
If you are currently running a beta version and plan on upgrading VMware vSAN to 6.6.1, your upgrade will fail. Do not upgrade from a beta version of vSAN, you must perform a fresh deployment of VMware vSAN. |
| VMware vSAN Host Software upgrade | **Manual remediation:** Verify that you have placed the VMware vSAN hosts in maintenance mode and selected the Ensure data accessibility or Evacuate all data option prior to rebooting each VMware vSAN node.  
**vSphere Update Manager:** with vSAN 6.6.1 we can use predefined system baselines for vSAN upgrade via the VMware vSphere Update Manager (VUM) integration. You can use the vSphere Update Manager (VUM) for automating and testing the upgrade process. However, when you use VUM to upgrade VMware vSAN hosts, the default evacuation mode is Ensure data accessibility. When you use the Ensure data accessibility mode, your data is not completely protected, and if you encounter a failure while upgrading VMware vSAN, you might experience unexpected data loss. However, the Ensure data accessibility mode is faster than the Evacuate all data mode, because you do not need to move all data to another host in the cluster.  

For information about various evacuation modes, see the vSAN Administration guide documentation, [Place a Member of VMware vSAN Cluster in Maintenance Mode](https://www.vmware.com/support/publishing.html). |
| VMware vSAN on-disk format | Verify if object and on-disk format upgrade is required or not. Please see VMware KB 2145248 [https://kb.vmware.com/kb/2145248](https://kb.vmware.com/kb/2145248) |
| VMware vSAN Datastore Free space | Verify that you have enough capacity available if on disk format is required. If you do not have free space equal to the consumed capacity of the largest disk group, with the space available on disk groups other than the disk groups that are being converted, you must choose **Allow reduced redundancy** as the data migration option. See VMware KB 2144944 [https://kb.vmware.com/kb/2144944](https://kb.vmware.com/kb/2144944)

For example, the largest disk group in a cluster has 10 TB of physical capacity, but only 5 TB is being consumed. An additional 5 TB of spare capacity will be needed elsewhere in the cluster, excluding the disk groups that are being migrated. When upgrading the VMware vSAN disk format, verify that the hosts are not in maintenance mode. When any member host of a VMware vSAN cluster enters maintenance mode, the cluster capacity is automatically reduced, because the member host no longer contributes storage to the cluster and the capacity on the host is unavailable for data. For information about various evacuation modes, see the [Place a Member of VMware vSAN Cluster in Maintenance Mode](https://kb.vmware.com/kb/2144944).

Use the vSAN 6.6 Disk Group pre-check evacuation can be used prior to data evacuation. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSAN 2 Node and Three Node Clusters</td>
<td>If Data Evacuation is required on three node or 2-Node vSAN cluster, you must choose <strong>Allow reduced redundancy</strong> as the data migration option. See VMware KB 2144944 <a href="https://kb.vmware.com/kb/2144944">https://kb.vmware.com/kb/2144944</a> for more details</td>
</tr>
</tbody>
</table>
9. Appendix A: Upgrade Troubleshooting

In this section we will go through some common issues and troubleshooting approaches if issues are encountered during vSAN 6.6 and vSAN 6.6.1 upgrades
9.1 vSphere Upgrade troubleshooting

Upgrade Related documentation and links

Below is a list of online resources for vSphere upgrade related documentation and related VMware KBs.


vSphere vCenter and ESXi Upgrade Troubleshooting related KBs

See VMware KB [https://kb.vmware.com/kb/2105258](https://kb.vmware.com/kb/2105258) for Windows based systems

See VMware KB [https://kb.vmware.com/kb/2106760](https://kb.vmware.com/kb/2106760) for vCenter Appliance (VCSA)

See VMware KB [https://kb.vmware.com/kb/1004107](https://kb.vmware.com/kb/1004107) for ESXi systems

Collecting diagnostic information

See VMware KB 1011641 [https://kb.vmware.com/kb/1011641](https://kb.vmware.com/kb/1011641) on how to collect diagnostic data for vCenter and ESXi hosts.

See VMware KB 2072796 [https://kb.vmware.com/kb/2072796](https://kb.vmware.com/kb/2072796) on how to collect vSAN support logs and upload to VMware.

See VMware KB 1027932 [https://kb.vmware.com/kb/1027932](https://kb.vmware.com/kb/1027932) on how to collect diagnostic information using PowerCLI.

Useful VMware KBs for vSAN

- VMware KB [https://kb.vmware.com/kb/2149840](https://kb.vmware.com/kb/2149840) - Supported upgrade paths for vSAN 6.6.
- VMware KB [https://kb.vmware.com/kb/2145248](https://kb.vmware.com/kb/2145248) - vSAN upgrade requirements.
- VMware KB [https://kb.vmware.com/kb/2146381](https://kb.vmware.com/kb/2146381) - vSAN (VSAN) Upgrade Best Practices.
- VMware KB [https://kb.vmware.com/kb/2149676](https://kb.vmware.com/kb/2149676) - Transient alarms might be observed during vSAN reconfiguration operations.
- VMware KB [https://kb.vmware.com/kb/2149677](https://kb.vmware.com/kb/2149677) - vSAN health check times out when a tested host becomes unresponsive.
- VMware KB [https://kb.vmware.com/kb/2149693](https://kb.vmware.com/kb/2149693) - Mixed vSAN clusters or partitioned clusters might produce inconsistent health check results.

9.2 vSAN On-Disk Upgrade Troubleshooting
vSAN on-disk format conversion upgrade monitoring

This section covers how to monitor and troubleshoot vSAN on-disk format conversions

Monitoring

vSAN 6.6 on-disk format conversion can be monitored from the vSphere 6.6 Cluster configuration summary. Figure 10 shows upgrade in progress for vSAN 6.6 Version 5.0 format.

vSAN on-disk format conversion can also be monitored from the Ruby vSphere Console, see https://kb.vmware.com/kb/2146218

vSAN Health Checks

Certain vSAN reconfiguration operations, such as disk format conversion upgrade or enable / disable encryption or de-duplication will trigger configuration changes and updates at the vSAN host level. The tasks might result in temporary inconsistencies between the disks and hosts in vSAN environment.

If the reconfiguration operations and related tasks take longer to finish, the vSAN health service detects these inconsistencies and reports them as alerts in the vSphere Events/Alarms view.

These transient alarms are automatically cleared after the vSAN reconfiguration operation and all related tasks the operation triggers complete. You can safely ignore the alarms.

After the vSAN reconfiguration operation and the related tasks complete, vSAN reruns the health test to rule out any potential configuration issues.

Logs

vSAN On-Disk format conversion is tracked by the vCenter vSAN Health Service. The vmware-vsan-health-service.log can be interrogated from vCenter as follows:

- Windows: %Programdata%\VMware\vCenterServer\logs\vsan-health\vmware-vsan-health-service.log
- vCenter Server Appliance: /storage/log/vmware/vsan-health/vmware-vsan-health-service.log

Related vCenter tasks and events can be tracked from vSphere Web Client and associated vSphere logs.

vCenter outage during On-disk format conversion

If vCenter server system has an unexpected outage or failure during on disk format conversion procedure, the on-disk upgrade will stop.
Once services have been restored the upgrade can be restarted from any point, but the user will have to manually restart the process.

**vSAN on-disk format Object conversion troubleshooting**

When upgrading the on-disk format, from Version 2.0 to Version 5.0, during the 10% - 15% phase, vSAN may realign objects to prepare them for new features. The process is performed in two steps:

- In the first step, vSAN realigns objects and their components to have a 1 MB address space. The process fails in this step if the cluster is unstable or if there is not enough disk space.
- In the second step, vSAN realigns vsanSparse objects to be 4k aligned. The process fails if there are objects which cannot be upgraded to version 2.5.

**vSAN on-disk upgrade fails at 10%**

In some cases when objects cannot upgraded the process may fail with a “General vSAN error” as illustrated by Figure 11.

![Figure 11. vsanSparse object realignment General vSAN Error](image)

There may be many reasons for object conversion failures, such as:

- A vSAN object maybe left “orphaned” on a vSAN data-store and no longer referenced by anything. For example a Virtual Machine Swap object.
- A Virtual Disk descriptor chain may not be not complete or corrupted. For example an incomplete snapshot chain or a missing descriptor file due to a prior failed Virtual Machine delete process.

Please refer to VMware KB 2144881 [https://kb.vmware.com/kb/2144881](https://kb.vmware.com/kb/2144881) for more details and remediation examples.
Handling new vSAN disk-groups in mixed vSAN mode

In earlier versions of vSAN, when vSphere hosts were upgraded, but the on-disk format conversion was not performed, new disk-groups were formatted with the version tied to the vSphere host version, which made them incompatible with existing vSAN disk groups that were not yet upgraded. This would cause object and disk-group incompatibility issues on a vSAN cluster.

For example, a disk-group failure may trigger this mis-matched state, as during repair, if a disk group gets re-created by an administrator, there could be a situation that new disk groups will be formatted with a later version than the existing vSAN disk-groups in the cluster.

With vSAN 6.6.1 and 6.6, existing vSAN data node disk-group versions will be checked against the vSAN Cluster disk-group version prior to a disk-group being repaired or a new disk-group added to increase capacity. New disk groups added will match the vSAN cluster version.

However, there is an exception which is the vSAN Witness Appliance Disk group combined with Replace Witness host procedure.

If a vSAN witness node is replaced in this mis-matched state using the vSAN 6.6.1 Replace witness workflow, the on-disk format version of the witness host might be later than the on-disk format version of the data hosts. In this case, the witness host cannot store components. To address this, use the following procedure.

1. Delete the disk group on the new witness host.
2. Modify the ESXi host advanced parameter `Virsto.DiskFormatVersion` to enable formatting of disk groups with an earlier on-disk format.
   For more information on the correct values to set per vSAN on-disk version, please review VMware KB 2146221 [https://kb.vmware.com/vmware-kb/2146221](https://kb.vmware.com/vmware-kb/2146221).
   Figure 12 shows an example of the advanced host parameter.
3. Recreate a new disk group on the witness host with a vSAN on-disk format version that matches the data hosts.
4. Modify the ESXi host advanced parameter `Virsto.DiskFormatVersion` back to the default value.
9.3 Troubleshooting Unicast Communications

vSAN 6.6 Unicast Troubleshooting

As discussed vSAN now communicates in unicast mode. Below is a list of esxcli commands and common vSAN cluster event logs for unicast communications.

Use `esxcli vsan cluster unicast agent list` to ensure that all nodes are listed as neighbors on all other nodes in the cluster.

```
NodeUid                      IsWitness Supports Unicast IP Address   Port   Iface
----------------------------------------------  -------  ---------------  ---------   --------
58e0a5d0-10b6-282c-4c2b-246e962f4850   0        true            172.30.0.7   12321   
58e0a66e-db18-f3a8-b830-246a962c2408   0        true            172.30.0.8   12321   
00000000-0000-0000-0000-000000000000  1        true            147.80.0.151 12321
```

In the above output the following is displayed

the VSAN uuid of each neighbor (a neighbor is any other node in the vsan cluster)
- if the node is acting as a witness node (1) or a data node (0)
- If this node is running software that allows unicast mode
- IP address and Port number

**Note:** vSAN Witness UUID is marked all zeros which is expected.
Use `esxcli vsan cluster get` lists the cluster state and if the vSAN cluster is operating in unicast mode

Cluster Information
- Enabled: true
- Current Local Time: 2017-04-19T18:34:40Z
- Local Node UUID: 58e0a66e-db18-f3a8-b830-246e962c2408
- Local Node Type: NORMAL
- Local Node State: AGENT
- Local Node Health State: HEALTHY
- Sub-Cluster Master UUID: 58e0a5d0-10b6-282c-4c2b-246e962f4850
- Sub-Cluster Backup UUID: 58e0a6d9-8a67-a4bf-2f30-246e962f4990
- Sub-Cluster UUID: 52cfbc15-cf7a-b909-3000-9deb499e2ec7
- Sub-Cluster Membership Entry Revision: 22
- Sub-Cluster Member Count: 4
- Sub-Cluster Member UUIDs: 58e0a5d0-10b6-282c-4c2b-246e962f4850, 58e0a66e-db18-f3a8-b830-246e962c2408, 58e0a63a-7775-aad6-2c67-246e962f5270, 58e0c39e-04f1-d837-1979-005056b9a2e0
- Sub-Cluster Membership UUID: c092ee58-ee4e-bela-8b4b-246e962f4850

**Unicast Mode Enabled**: true
- Maintenance Mode Enabled: true
- OFF

**Unicast Behaviors**
- A vSAN 6.6.1 (6.6) node will always run in unicast mode if it has no neighbors i.e. `esxcli vsan cluster unicastagent` list is empty.
- A vSAN 6.6.1 (6.6) node will always run in unicast mode if all neighbors attribute "Supports unicast" is set to true.
- If one or more neighbor nodes have their "Supports Unicast" attribute set to false - then the node will run in multicast mode if there are no v5 disks in the cluster.
- As soon as there is even one v5 disk in the cluster all vSAN 6.6.1 (6.6) nodes will transition to unicast mode and stay in this mode.
- A vSAN 6.6.1 (6.6) unicast node cannot form a cluster with a multicast node.
- A vSAN 6.6.1 (6.6) unicast node that does **not** list another node as its neighbor cannot form a cluster with that node (even if that node lists this node as a neighbor).

**Useful VMkernel log entries**
- This log is printed when a vSAN 6.6.1 (6.6) node is removed as a neighbor vSAN cluster. (/var/log/vmkernel.log)
- `CMMDNSNet: CMMDNSNet_RemoveUnicastHost:683: Remove unicast node: 172.3.0.5;12321`
- `CMMDNSNet: CMMDNSNetAddUnicastHostInt:605: Add unicast node: 172.3.0.5;12321`
- `CMMDNSUpdateUcastAgentVersion:367: Current ucastNeigh 8 mcastNeigh 0 reconfigNeeded 0`
- If `reconfigNeeded` is set to 1 -- then vSAN will re-evaluate if it should be running in unicast or multicast mode.
- These entries are printed when cmmds decides to go from unicast to multicast mode or vice versa.
- `CMMDSTestAndSetUcastOnlyMode:1280: isWitness:0 VFV:5 ucastonlymode:1 ucastNeighbor:0 nonUcastNeighbor:0`
- `CMMDSTestAndSetUcastOnlyMode:1316: Toggling unicast only mode from 1 to 0`

**Useful vCenter vsan-health logs**
- When it is necessary to update hosts' unicast info, the following log entry about "UpdateMemberInfo" will be printed, it lists all hosts which needs to be updated.
This log entries would be printed on the `vmware-vsan-health-service.log` on vCenter Server system. Below is an example

```plaintext
INFO vsan-health[Sched-63_noOpId] [VsanMgmtAdapters::UpdateMemberInfos] Update member infos for hosts: [u'host-34(esxi-dell-g.rainpole.com)', u'host-32(esxi-dell-e.rainpole.com)', u'host-37 (esxi-dell-m.rainpole.com)', u'host-36(esxi-dell-n.rainpole.com)', u'host-39(esxi-dell-p.rainpole.com)', u'host-35(esxi-dell-h.rainpole.com)', u'host-38(esxi-dell-o.rainpole.com)', u'host-33(esxi-dell-f.rainpole.com)', u'host-56(witness-01.rainpole.com)']
```

### vSAN 6.6.1 vSAN false network partition with unicast communications

There could be a situation when vCenter and vSAN nodes are rebooted a vSAN 6.6.1 or 6.6 cluster may become partitioned from a vSAN unicast perspective. This is due in the situation of simultaneous a vCenter restart and ESXI restart, the vSAN node properties may not be updated correctly to vCenter, or specifically vCenter vSAN Health Service. As a result vSAN node may be in a partitioned state. This has been documented on the vSAN 6.6 release notes and vSAN 6.6.1 release notes

#### Symptoms

The below example illustrates the issue and symptoms

1. vCenter server is restarted
2. One or more vSAN host also gets restarted or disconnected from vCenter
3. No vSAN nodes were administratively added or removed from the vSAN cluster.

In this situation a vSAN host or hosts may become partitioned for no obvious reason

If vSAN Health Service does not discover the vSAN node correctly it will push empty unicast information to the host and this is what triggers the partition

#### Resolution

To resolve, restarting the vsan-health service can resolve the issue. To restart the vsan-health service, connect to the vCSA appliance and run the following shell command on VCSA appliance

```
/usr/lib/vmware-vmon/vmon-cli -r vsan-health
```

For more information, see VMware KB 2054085 Stopping, starting, or restarting vCenter Server Appliance services (2054085).

For Windows based vCenter systems, restart the vSAN health service from the Windows OS management interface (services.msc)

For more information, see VMware KB 1003895, How to stop, start, or restart vCenter Server services

Other services on the vCenter system should not be interrupted if the vsan health service is restarted manually.

---

Copyright © 2019 VMware, Inc. All rights reserved.
10. Appendix B: vSAN On-disk Format Upgrade example

Appendix D goes through vSAN on-disk format Version 5.0 to Version 6.0 upgrade workflow.
10.1 vSAN disk format conversion upgrade to Version 5.0

VMware vSAN On-disk Format Upgrade

As already discussed When you initiate an upgrade of the on-disk format, VMware vSAN may perform several operations, such as object conversion and disk group removal and creation.

As illustrated on Figure 26 with the release of VMware vSAN 6.6.1 and vSAN 6.6 we have now includes an on-disk format pre-check that can be executed prior to initiating a on-disk format conversion or DFC for short.

This should be run before initiating on-disk format upgrade task

This checks for the following

- All hosts are connected. For example, if there are host connectivity issues, they will be listed under Details Figure 27 shows that prec-check fails as one host in the vSAN Cluster is not responding.

- All hosts have the correct software version.
- All disks are healthy.
- Automatic disk claiming is disabled.

Once all pre-checks have passed as illustrated on Figure 28, on-disk format upgrade can be initiated
For more information regarding VMware vSAN on disk upgrade process and troubleshooting see Knowledge base article VMware KB 2144881.

Sample Procedure – On-disk Format Upgrade from Version 3.0 to Version 5.0

As already discussed earlier in this document, upgrading the vSAN on-disk format can be a long running operation if going from some older VMware vSAN On-disk Format Versions.

However, going from Version 3.0 to Version 5.0 requires a meta-data update only.

**No data evacuation is required**

- Select Upgrade from On-disk Format Version, From Cluster -> Configure – vSAN -> General. A popup will be displayed as illustrated on Figure 29.

![Figure 29. on disk format conversion guidance and acceptance](image)

- Since this is a meta-data update only, there is no requirement to select “Allow Reduced Redundancy” as it is simply a meta-data update and not a data evacuation. Select Yes to initiate Upgrade.

**Note:** Once you upgrade the on-disk format, you cannot roll back software on the ESXi hosts or add certain older hosts to the cluster. For more details see VMware KB [https://kb.vmware.com/kb/2148493](https://kb.vmware.com/kb/2148493).

- With vSAN 6.6, the On-disk format Upgrade progress indicator is used to track progress from the vSphere Client as shown on Figure 30.
Figure 30. On disk format progress bar, Version 3.0 to Version 5.0

• General guidance on progress bar is as follows for Version 3 to Version 5 Upgrades
  ◦ Between 5% to 20% is where the disk groups will get “stamped” to Version 5.0
  ◦ As each disk group will be updated sequentially in a given cluster. It may take up to one
    minute to update per disk group. Depending how many disk-groups are configured in
    each cluster, this could potentially take a long period of time.
• Progress can also be tracked from RVC using

\[
\text{vsan.upgrade\_status /localhost/<datacenter>/computers/<cluster>/ -r 60}
\]

Once the disk conversion has completed all disks should now be at Version 5.0. the new version will be
displayed on the Cluster summary as illustrated on Figure 31.

Figure 31. On-disk format version complete