# Table of Contents

Lab Overview - HOL-1908-01-HCI - vSAN 6.7 Getting Started......................................................... 2  
   Lab Guidance .......................................................................................................................... 3  
Module 1 - vSAN 6.7 Sizing, Setup and Enablement (30 Minutes) .............................................. 10  
   Introduction.......................................................................................................................... 11  
   vSAN 6.7 What’s New and Use Cases .................................................................................. 12  
   Enabling vSAN...................................................................................................................... 16  
   vSAN Sizing.......................................................................................................................... 28  
   Hands-on Labs Interactive Simulation: vSAN Sizing ............................................................. 33  
   Conclusion............................................................................................................................. 34  
Module 2 - vSAN 6.7 Monitoring Health, Capacity and Performance (45 Minutes) ... 36  
   Introduction.......................................................................................................................... 37  
   Enabling vRealize Operations within vCenter ....................................................................... 38  
   vSAN Health Check Validation ............................................................................................ 45  
   Monitoring vSAN Capacity.................................................................................................. 54  
   Monitoring vSAN Performance ............................................................................................ 59  
   vRealize Operations within vCenter Monitoring .................................................................. 63  
   Conclusion............................................................................................................................. 82  
Module 3 - vSAN 6.7 Day 2 Operations (30 Minutes) ................................................................. 84  
   Introduction.......................................................................................................................... 85  
   Adding vSAN Capacity......................................................................................................... 86  
   Storage Policy Based Management ...................................................................................... 106  
   vSAN Maintenance ............................................................................................................... 138  
   Updating vSAN ................................................................................................................. 150  
   Conclusion............................................................................................................................. 153  
Module 4 - vSAN 6.7 Availability (30 Minutes) ........................................................................ 155  
   Introduction.......................................................................................................................... 156  
   vSAN Availability and Fault Domains .................................................................................. 157  
   Active/Active vSAN Stretched Clusters ............................................................................. 169  
   Disaster Recovery with vSAN ............................................................................................. 192  
   Conclusion............................................................................................................................. 194  
Module 5 - vSAN 6.7 Interoperability (45 Minutes) ................................................................ 196  
   Introduction.......................................................................................................................... 197  
   vRealize Network Log Insight with vSAN .......................................................................... 198  
   vSAN iSCSI Integration ...................................................................................................... 220  
   vSAN CLI Interfaces .......................................................................................................... 258  
   PowerCLI vSAN Commands ............................................................................................. 267  
   Conclusion............................................................................................................................. 284  
Module 6 - vSAN 6.7 Security (30 Minutes) ............................................................................ 285  
   Introduction.......................................................................................................................... 286  
   DISA STIG (FIPS 140-2) Validated ...................................................................................... 287  
   vSAN Encryption ............................................................................................................... 288  
   Conclusion............................................................................................................................. 311
Lab Overview - HOL-1908-01-HCI - vSAN
6.7 Getting Started
Lab Guidance

Note: It may take more than 90 minutes to complete this lab. You should expect to only finish 2-3 of the modules during your time. The modules are independent of each other so you can start at the beginning of any module and proceed from there. You can use the Table of Contents to access any module of your choosing.

The Table of Contents can be accessed in the upper right-hand corner of the Lab Manual.

vSAN delivers flash-optimized, secure shared storage with the simplicity of a VMware vSphere-native experience for all of your critical virtualized workloads. Learn how to size and enable vSAN environments including monitoring the health, capacity and performance of vSAN within vCenter and also via, built-in, vRealize Operations for vCenter Dashboards. Explore the all new, intuitive vSAN HTML5 user interface used to perform Day-2 Operations, maintain virtual machine availability, enable vSAN Encryption and discover Interoperability with vRealize Log Insight, iSCSI Integration and CLI Interfaces.

Lab Module List:

- **Module 1 - vSAN 6.7 Sizing, Setup and Enablement** [30 mins] [Basic]
  - In this module we will introduce to VMware vSAN. We will cover the vSAN features and show you how to enable vSAN using the new vSphere Client ( HTML5 UI )

- **Module 2 - vSAN 6.7 Monitoring Health, Capacity and Performance** [45 mins] [Advanced]
  - In this module we will show you how to enable vRealize Operations within vCenter Server. We will cover the vSAN Health Check and how you can monitor your vSAN environment.

- **Module 3 - vSAN 6.7 Day 2 Operations** [30 mins] [Basic]
  - In this module we will cover Storage Based Policy Management and how to maintain your vSAN environment. We will also demonstrate how to expand the capacity of the vSAN Datastore.

- **Module 4 - vSAN 6.7 Availability** [30 mins] [Advanced]
  - In this module we will cover vSAN availability and Fault Domains. We will demonstrate how to create a vSAN Stretched Cluster.

- **Module 5 - vSAN 6.7 Interoperability** [45 mins] [Advanced]
In this module we will introduce vRealize Log Insight with vSAN. We will cover the vSAN iSCSI integration and demonstrate how you use vSAN iSCSI and Windows Server Failover Cluster. We will also cover how to monitor your vSAN environment with command line tools like ESXCLI and PowerCLI.

- **Module 6 - vSAN 6.7 Security** [30 mins] [Advanced]

- In this module we will introduce to vSAN Encryption. We will enable a Key Management Server and demonstrate how to configure vSAN Encryption.

**Lab Captains:**

- John Browne, Staff Technical Support Specialist, Cork, Ireland
- Ken Osborn, Staff Solutions Engineer vSAN/HCI, Minnesota, USA

**Special Thanks for their guidance and assistance:**

- Cormac Hogan, Director & Chief Technologist, Storage Product Marketing
- Jeff Hunter, Group Manager, vSAN Tech Marketing
- Pete Flecha, Senior Technical Marketing Architect
- Myles Gray, Senior Technical Marketing Architect
- GS Khalsa, Senior Technical Marketing Architect
- Jase McCarty, Staff Technical Marketing Architect
- John Nicholson, Senior Technical Marketing Architect
- Pete Koehler, Senior Technical Marketing Architect

This lab manual can be downloaded from the Hands-on Labs Document site found here:

[http://docs.hol.vmware.com](http://docs.hol.vmware.com)

This lab may be available in other languages. To set your language preference and have a localized manual deployed with your lab, you may utilize this document to help guide you through the process:

Location of the Main Console

1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.
2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.
3. Your lab starts with 90 minutes on the timer. The lab can not be saved. All your work must be done during the lab session. But you can click the **EXTEND** to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

Alternate Methods of Keyboard Data Entry

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.
Click and Drag Lab Manual Content Into Console Active Window

You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

Accessing the Online International Keyboard

You can also use the Online International Keyboard found in the Main Console.

1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.
Click once in active console window

In this example, you will use the Online Keyboard to enter the "@" sign used in email addresses. The "@" sign is Shift-2 on US keyboard layouts.

1. Click once in the active console window.
2. Click on the **Shift** key.

Click on the @ key

1. Click on the "@ key".

Notice the @ sign entered in the active console window.
Activation Prompt or Watermark

When you first start your lab, you may notice a watermark on the desktop indicating that Windows is not activated.

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple datacenters. However, these datacenters may not have identical processors, which triggers a Microsoft activation check through the Internet.

Rest assured, VMware and the Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet, which is required for Windows to verify the activation. Without full access to the Internet, this automated process fails and you see this watermark.

This cosmetic issue has no effect on your lab.

Look at the lower right portion of the screen
Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes your lab has not changed to "Ready", please ask for assistance.
Module 1 - vSAN 6.7 Sizing, Setup and Enablement (30 Minutes)
Introduction

vSAN delivers flash-optimized, secure shared storage with the simplicity of a VMware vSphere-native experience for all your critical virtualized workloads. vSAN runs on industry-standard x86 servers and components that help lower TCO by up to 50% versus traditional storage. It delivers the agility to easily scale IT with a comprehensive suite of software solutions and offers the first native software-based, FIPS 140-2 validated HCI encryption.

vSAN 6.7 delivers a new HCI experience architected for the hybrid cloud with operational efficiencies that reduce time to value through a new, intuitive user interface, and provides consistent application performance and availability through advanced self-healing and proactive support insights. Seamless integration with VMware's complete software-defined data center (SDDC) stack and leading hybrid cloud offerings makes it the most complete platform for platform for virtual machines, whether running business-critical databases, virtual desktops or next-generation applications.
vSAN 6.7 What's New and Use Cases

Before we jump into the Lab, let’s take a moment to review What’s New with vSAN 6.7 and Use Cases that are utilized for vSAN.

vSAN 6.7 What's New

vSAN 6.7 delivers a new HCI experience with enhanced operational efficiencies that reduces time-to-expertise and accelerates decision making. This release provides a more consistent, resilient and secure application experience, and leverages people, technology and analytics to deliver an enhanced support experience with simpler, faster time to resolution. More businesses build their digital foundation from edge to core to cloud with VMware vSAN than any other HCI solution.

Product Enhancements

The most significant new capabilities and updates of vSAN 6.7 include:

- **HTML5 User Interface**
  A completely redesigned user interface delivers a modern management experience. The new interface was built using the same framework as other VMware products, so you’ll have a unified and intuitive experience managing the most complete SDDC stack. In addition, the new UI delivers optimized workflows to reduce the number of clicks to perform many functions.

- **vRealize Operations within vCenter**
  Customers get two ways to manage their vSAN environments with vRealize Operations: Global operations overview in vCenter, and advanced monitoring, troubleshooting and capacity management with vRealize Operations. Customers gain a single pane of glass to monitor and control their HCI environment through vRealize Operations insights directly within vCenter, providing an overview of vSAN and vSphere environments as well as surfacing up critical alerts and operations insights.

- **Introducing vSAN ReadyCare**
  vSAN ReadyCare support highlights VMware’s commitment to vSAN customers and delivers holistic support through people, analytics and technology. Through predictive modelling in vSAN Support Insight, VMware analyzes anonymous data from thousands of vSAN customers and pushes alerts to customers before issues arise.

- **FIPS 140-2 Validated Encryption**
vSAN offered the first native HCI encryption solution for data-at-rest, and now with vSAN 6.7, vSAN Encryption is the first FIPS 140-2 validated software solution, meeting stringent US Federal Government requirements.

- **Increased Application Resiliency**

  vSAN delivers a more consistent application experience for end users with intelligent, self-healing capabilities that include adaptive resynchronization and replica consolidation. Adaptive Resync intelligently manages IO traffic to minimize disruptions to applications during resync operations. Replica consolidation reduces the time and effort to enter a host into maintenance mode.

- **Enhanced Stretched Cluster Availability**

  Stretched Cluster deployments are further enhanced with intelligent witness traffic separation, primary site override, and efficient resyncs. Witness traffic separation and efficient resync optimizes the path and size of data transmitted over each link, making failovers transparent to application end users. Primary site override heightens availability of workloads by better logic in the event of site failure.

- **Increased Support for Business-Critical Application Deployments**

  vSAN now supports more mission-critical application deployments through Windows Server Failover Clusters (WSFC) support, which reduces complexity of storage management for those workloads and helps customers accelerate their move toward a unified SDDC experience.

- **Proactive Support via vSAN Support Insight**

  Proactive support increases the reliability of vSAN through alerts before infrastructure problems arise, as well as reduced reactive support times by gathering data periodically. This feature requires enrollment in the Customer Experience Improvement Program.

- **Adaptive Core Dump Support**

  Adaptive Core Dump Support reduces vSAN support time to resolution for a greater number of deployment types by automatically configuring the direction and size of valuable data used to expedite support.

- **Increased Hardware Support**

  vSAN now supports 4Kn disk drives, future proofing vSAN deployments and creating an opportunity for you to lower your storage TCO.

**vSAN Customer Benefits and Use Cases**

**Evolve Without Risk**
Seamlessly extend virtualization to storage with a secure, integrated hyper-converged solution that simply works with your VMware environment using existing management tools, skillsets and hardware platform of choice.

**Reduce TCO**

Make limited budgets go farther with 50% lower total cost of ownership by consolidating core data center functions on the broadest choice of industry-standard x86 hardware and the most proven hypervisor.

**Scale to Tomorrow**

Prepare for tomorrow’s IT needs in the cross-cloud era with software-defined infrastructure that leverages the latest hardware technologies, supports next-gen applications and provides a stepping stone to the cloud.

**Why vSAN?**

*Why Customers are Deploying vSAN Today*

- **Fully integrated SDDC stack, Available Today**
- **No new tools to learn, vCenter is already familiar tool for unified management**
- **Deployment flexibility on public and private clouds**
- **Most secure HCI solution (vSAN now has FIPS 140-2 validated encryption for data at rest)**
- **Best price-performance for VM consolidated workloads**
vSAN Use Cases

Supporting a Broad Variety of Use Cases

- Business Critical Apps
- Databases (SQL/Oracle)
- DR/DA
- Management Clusters
- Virtual Desktops (VDI)
- Cloud Native Apps
- Containers
- ROBO

vSAN Customer Examples

vSAN Customers From the Edge to Core to Cloud

- 300,000 sensors
  - Big data analysis
  - Less “ground” time
- $500M ad day
  - 3 sites to 1 SDDC
  - Speed and reliability
- 10+ PB on All-Flash vSAN
  - Two 32 Node Clusters
Enabling vSAN

To use vSAN, you must create a host cluster and enable vSAN on the cluster.

A vSAN cluster can include hosts with capacity and hosts without capacity.

Follow these guidelines when you create a vSAN cluster.

• A vSAN cluster must include a minimum of three ESXi hosts. For a vSAN cluster to tolerate host and device failures, at least three hosts that join the vSAN cluster must contribute capacity to the cluster. For best results, consider adding four or more hosts contributing capacity to the cluster.
• All hosts in the vSAN cluster must have the same on-disk format.
• Before you move a host from a vSAN cluster to another cluster, make sure that the destination cluster is vSAN enabled.
• To be able to access the vSAN datastore, an ESXi host must be a member of the vSAN cluster.

After you enable vSAN, the vSAN storage provider is automatically registered with vCenter Server and the vSAN datastore is created.

Open Chrome Browser from Windows Quick Launch TaskBar

1. Click on the Chrome Icon on the Windows Quick Launch Task Bar.
Login to vSphere Client

1. On the vSphere Client login screen, select "**Use Windows session authentication**"
2. Click **Login**
You will be presented with the vSphere Client Home page.

To minimize or maximize the Recent Tasks, Alarms panes, click the arrow.

If the Home page is not the initial screen that appears, select **Home** from the top menu in the vSphere Client.

1. Select **Hosts and Clusters**
Enable vSAN

In your lab environment, vSAN is currently Turned Off. In this lesson we will show you how to enable or turn on vSAN in a few easy steps.

A quick note about the Lab environment: The Cluster called RegionA01-COMP01 currently contains 3 ESXi hosts that will contribute storage in the form of cache and capacity to form the vSAN datastore.

1. Select RegionA01-COMP01
2. Select Configure
3. Select vSAN > Services
4. Select Configure
Configure VSAN

As part of the basic configuration keep the default selection of **Single site cluster**

Click **NEXT**

Configure VSAN

When using an All-Flash configuration, you have the option to enable Deduplication and Compression. vSAN Encryption will be covered in a later module

1. Enable **Deduplication and Compression**
2. Select **Allow Reduced Redundancy**
Selecting Allow Reduced Redundancy, vSAN will be able to reduce the protection level of your VMs, if needed, during operations of enabling Deduplication and Compression. This option is only usable if your setup is at the limit of the protection level, configured by the Storage Policy of a Specific VM.

Click NEXT

**Claim Disks by Disk model / size**

![Image of Claim Disks interface]

**Important**: Each of our Hosts has 6 Storage Devices. For this lesson, we are only going to claim 3 of these devices per Host (1x Cache Device and 2x Capacity Devices).

1. Click to Expand the **Cache Device** view
2. For each Host, **set one Cache Device to 'Do not claim'** (when finished, you will have 1x Cache Device per Host)
3. Click to Minimize the **Cache Device** View (not shown)

**Do Not click Next just yet**. Move to the next step in the Lab Manual.
Claim Disks by Disk model / size

**Important:** Each of our Hosts has 6 Storage Devices. For this lesson, we are only going to claim 3 of these devices per Host (1x Cache Device and 2x Capacity Devices).

1. Click to Expand the Capacity Device view
2. For each Host, set two Capacity Devices to 'Do not claim'
3. Use the Down Arrow on your keyboard and repeat Step 2 for the remaining two Hosts (when finished, you will have 2x Capacity Devices per Host)

**Do Not click Next just yet.** Move to the next step in the Lab Manual.
1. From the Group by: drop down list, select **Host**

This is a view of the storage from the Host perspective. In this exercise we are creating one Diskgroup on each ESXi Host.

The Disk Group will contain one **5 GB Cache** disk and **2 x 10 GB Capacity** disks.

2. Verify that you are claiming **60.00 GB** of Capacity and **15.00 GB** of Cache for **75.00 GB** total.

3. Click **NEXT**
Create Fault Domains

We will not create Fault Domains right now. By default, each ESXi host in itself is a Fault Domain.

1. Click **NEXT**
Review and verify your selection.

1. Here we can determine that we will create a vSAN datastore with a capacity of **60.00 GB** and cache of **15.00 GB**.

This is an All Flash vSAN Cluster, where both the Cache and Capacity disks are SSD/Flash disks.

2. Click **FINISH**
Monitor Progress

1. Select **Recent Tasks** in the lower left-hand corner
2. Select **Running** via the drop-down selector
3. Minimize the **Recent Tasks** view (not shown)

Monitor until all tasks are complete
vSAN Enabled

Once the configuration process is complete,

1. Select Configure
2. Select vSAN > Services

It may take a few minutes for the cluster to complete all its updates, and you may see some alerts in vCenter until vSAN has settled.

After that, you should see the Health and Performance services are enabled by default.

Conclusion

Enabling vSAN creates a vSAN datastore and registers the vSAN storage provider. vSAN storage providers are built-in software components that communicate the storage capabilities of the datastore to vCenter Server.
vSAN Sizing

In the previous lesson, we enabled our lab vSAN Cluster. Prior to enabling vSAN in your environments, how do you know how to properly size your vSAN Cluster in terms of necessary Compute, Memory and local Storage? In this section, we will examine how to utilize HCI Assessment powered by Live Optics to Capture Performance metrics and then input these metrics into our vSAN Online Sizer to create a proposed vSAN Build. With this Build information in-hand, you are then free to choose the vSAN Ready Node vendor that best meets your standards via our VMware vSAN Compatibility Guide.

HCI Assessment powered by Live Optics

Live Optics is a tool widely adopted across the industry which is used to capture workload metrics which allows customers to assess their current environments. The VMware HCI assessment will capture metrics required for sizing and designing an HCI solution and will allow you to translate data into the vSAN ReadyNode Sizer to build a custom vSAN solution.

In the next few pages, we will review the outcome of an actual Live Optics study and then we will enter this information into our ReadNode Sizer to come up with a vSAN Build Recommendation. Note that there is no financial charge for conducting a VMware HCI assessment.
The Environment View shows us high level characteristics that are important to consider, such as:

1. 95% of the time **IOPS** were at 10,790
2. **Capacity** Information (Used, Free and Total)

Additional high level metrics are also present (CPU, Memory, Network, etc.)
Performance View

Drilling down further, we can review:

1. Read/Write Ratios (these are especially important as they help us size our vSAN Cache tier correctly).
Hypervisor

<table>
<thead>
<tr>
<th>Guest VMs</th>
<th>Hypervisor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total Guest VMs</strong></td>
<td>401</td>
</tr>
<tr>
<td><strong>Total Running VMs</strong></td>
<td>392</td>
</tr>
<tr>
<td><strong>Total Idle (not-running) VMs</strong></td>
<td>9</td>
</tr>
<tr>
<td><strong>Total vCPU</strong></td>
<td>1672</td>
</tr>
<tr>
<td><strong>Total provisioned guest VM memory</strong></td>
<td>4.77 TB</td>
</tr>
<tr>
<td><strong>Total used guest VM memory</strong></td>
<td>622.94 GB</td>
</tr>
<tr>
<td><strong>Total provisioned guest VM disk space</strong></td>
<td>107.59 TB</td>
</tr>
<tr>
<td><strong>Total used guest VM disk space</strong></td>
<td>107.29 TB</td>
</tr>
<tr>
<td><strong>Total hypervisor CPU cores</strong></td>
<td>192</td>
</tr>
<tr>
<td><strong>Avg. vCPU per guest VM</strong></td>
<td>4.17</td>
</tr>
<tr>
<td><strong>Avg. provisioned memory per guest VM</strong></td>
<td>12.18 GB</td>
</tr>
<tr>
<td><strong>Avg. used memory per guest VM</strong></td>
<td>1.55 GB</td>
</tr>
<tr>
<td><strong>vCPU to Server Core ratio</strong></td>
<td>8.71 : 1</td>
</tr>
</tbody>
</table>

Live Optics also provides additional useful information such as Total Guest VMs, Total vCPU’s, Total provisioned guest VM memory vs used, Total provisioned guest VM disk space, Average vCPU per guest VM, Averaged used memory per guest VM, vCPU to Server Core ration, etc.
Live Optics also captures individual Virtual Machine information that can be useful as part of our vSAN Build decisions.

Let's take the Live Optics data we have gathered and enter it into our online vSAN ReadyNode Sizer next to come up with a vSAN Recommendation!
Hands-on Labs Interactive Simulation: vSAN Sizing

This part of the lab is presented as a Hands-on Labs Interactive Simulation. This will allow you to experience steps which are too time-consuming or resource intensive to do live in the lab environment. In this simulation, you can use the software interface as if you are interacting with a live environment.

The orange boxes show where to click, and the left and right arrow keys can also be used to move through the simulation in either direction.

1. Click here to open the interactive simulation. It will open in a new browser window or tab.
2. When finished, click the “Return to the lab” link to continue with this lab.

The lab continues to run in the background. If the lab goes into standby mode, you can resume it after completing the module.
Conclusion

In this module, we showed you how to enable vSAN in just a few clicks. In addition, we reviewed What's New with vSAN 6.7 including Customer Use Cases.

You've finished Module 1

Congratulations on completing Module 1.

If you are looking for additional information on topic:

- vSAN Customer References by Industry
- vSAN Use Cases
- vSAN Operations Guide
- vSAN Design and Sizing Guide
- vSAN Compatibility Guide
- Go to VMware Storage Hub for all things related to vSAN.

Proceed to any remaining module below which interests you most.

- **Module 2 - vSAN 6.7 Monitoring Health, Capacity and Performance** (45 minutes) (Basic)

Module 2 demonstrates how to monitor the Health, Capacity and Performance of your vSAN Environment utilizing vCenter and vRealize Operations Manager.

- **Module 3 - vSAN 6.7 Day-2 Operations** (30 minutes) (Basic)

Module 3 describes how to perform Day-2 Activities on your vSAN Cluster such as utilizing Storage Policy-Based Management, determining Maintenance Mode options and adding additional capacity.

- **Module 4 - vSAN Availability** (30 minutes) (Basic)

Module 4 discusses vSAN Failure Domains, Active/Active Datacenters with vSAN Stretched Cluster and vSAN Disaster Recovery Scenarios.

- **Module 5 - vSAN Interoperability** (45 minutes) (Intermediate)

Module 5 illustrates utilizing vRealize Log Insight to review centralized vSAN Logs, vSAN iSCSI integration and vSAN CLI interfaces.

- **Module 6 - vSAN Encryption** (30 minutes) (Intermediate)

Module 6 discusses vSAN security parameters such as FIPS 104-2 Validation and vSAN Data-at-rest Encryption.
How to End Lab

To end your lab click on the **END** button.
Module 2 - vSAN 6.7
Monitoring Health, Capacity and Performance (45 Minutes)
Introduction

A critical aspect of enabling a vSAN Datastore is validating the Health of the environment. vSAN has over a hundred out of the box Health Checks to not only validate initial Health but also report ongoing runtime Health. vSAN 6.7 introduces exciting new ways to monitor the Health, Capacity and Performance of your Cluster via vRealize Operations within vCenter, all within the same User Interface that VI Administrators use today.
Enabling vRealize Operations within vCenter

It takes approximately 30 minutes to enable vRealize Operations for vCenter within our Lab environment.

In these next steps, we will ask you to walk through the steps necessary to enable vRealize Operations for vCenter and then we will return to it later in the Module.

Lab Preparation

We will use our Module Switcher PowerCLI Application to prepare the environment.

Module Switcher

Double-Click the Module Switcher Desktop Shortcut called HOL-1908 HCI

Module 2 Start

1. Click the Module 2 - Start button

This Startup Routine can take a few minutes to complete - thank you for your patience!
Monitor Progress

Monitor Progress until Complete.

- Press Enter to continue (and close the PowerCLI Window)

Lab Prep Complete

Your Lab has been successfully prepared for Module 2!

1. Click Close to safely stop the Module Switcher

Please Note that you cannot 'go back' and take Modules prior to the one you are currently in unless you end the lab and start it over again (for example: If you Start with Module 4, you cannot use the Module Switcher to Start Labs 1, 2 or 3).

Open Chrome Browser from Windows Quick Launch TaskBar

1. Click on the Chrome Icon on the Windows Quick Launch Task Bar.
Login to vSphere Client

1. On the vSphere Client login screen, select "Use Windows session authentication"
2. Click Login
vRealize Operations

1. Select **Menu**
2. Click **vRealize Operations**

Note that you receive a message indicating that vRealize Operations is not present. We will correct that condition next.

**Configure Existing Instance**

1. Scroll **Down**
2. Click **Configure Existing Instance**

Note that you have the option to Install a new instance of vRealize Operations or Configure an existing instance. In our Lab, vRealize Operations has already been installed and this is the instance that we will tie into.
Instance Details

1. Enter parameters:

   INSTANCE FQDN: vrops-01a.corp.local
   USERNAME: admin
   PASSWORD: VMware1!

2. Select **Test Connection** to validate credentials (re-enter if necessary)

3. Click **Next**
vCenter Details

1. Enter parameters:

- INSTANCE FQDN: vcsa-01a.corp.local
- USERNAME: administrator@corp.local
- PASSWORD: VMware1!

2. Select **Test Connection** to validate credentials (re-enter if necessary)

3. Click **Next**
1. Click **Configure**

Configuration will take several minutes in our Lab. While we wait, let's examine vSAN Health and vCenter Capacity & Performance Monitoring before utilizing vRealize Operations for vCenter.
vSAN Health Check Validation

One of the ways to monitor your vSAN environment is to use the vSAN Health Check.

The vSAN Health runs a comprehensive health check on your vSAN environment to verify that it is running correctly and will alert you if it finds some inconsistencies and options on how to fix these.

vSAN Health Check

Running individual commands from one host to all other hosts in the cluster can be tedious and time consuming. Fortunately, since vSAN 6.0, vSAN has a health check system, part of which tests the network connectivity between all hosts in the cluster. One of the first tasks to do after setting up any vSAN cluster is to perform a vSAN Health Check. This will reduce the time to detect and resolve any networking issue, or any other vSAN issues in the cluster.

Use Health Check to Verify vSAN Functionality

To run a vSAN Health Check,

1. Select the vSAN Cluster called RegionA01-COMP01
2. Select Monitor
3. Select vSAN > Health

You will see the categories of Health Checks that can be run and their status
4. To run the tests at any time click the **RETEST** button.

Note that some of the Health Checks are in a Warning State. This is due to the fact that we are running a vSAN cluster in a nested virtualized environment.

**Network Health Check**

To see the individual tests that can be run from within a vSAN Health category.

1. Expand the **Network** health category.
To get additional information on a Health Check item, select the appropriate check and examine the details pane on the right for information on how to resolve the issue.

1. Select **All hosts have matching subnets**

Here we have the details and the results of the Health Check that was performed, in this case we can see that all the ESXi host in the vSAN Cluster have matching subnets.
Inducing a vSAN Health Check Failure

Let's induce a vSAN Health Check failure to test the health check.

1. Right click the ESXi host called esx-01a.corp.local
2. Select Connection
3. Select Disconnect

Answer OK to disconnect the selected host.
Inducing a vSAN Health Check Failure

1. Select the vSAN Cluster called RegionA01-COMP01
2. Select Monitor
3. Select vSAN > Health

Here we will see a vSAN Network Health Check that has failed (if you do not see this Alert, then click 'RETEST' in the upper right-hand corner).
Inducing a vSAN Health Check Failure

1. Click the **Hosts Disconnected from VC** to get additional information.

Here we can see that the ESXi host called **esxi-01a.corp.local** is showing as **Disconnected**.
Inducing a vSAN Health Check Failure

Each details view under the Info tab also contains an Ask VMware button where appropriate, which will take you to a VMware Knowledge Base article detailing the issue, and how to troubleshoot and resolve it.

1. Select Info
Resolving a vSAN Health Check Failure

1. Right click the ESXi host called esx-01a.corp.local
2. Select Connection
3. Select Connect

Answer OK to reconnect the selected host.
Resolving a vSAN Health Check Failure

1. Select the vSAN Cluster called RegionA01-COMP01
2. Select Monitor
3. Select vSAN > Health
4. The Hosts disconnect from VC test has passed again as all the ESXi host in the vSAN Cluster are connected.

Conclusion

You can use the vSAN health checks to monitor the status of cluster components, diagnose issues, and troubleshoot problems. The health checks cover hardware compatibility, network configuration and operation, advanced vSAN configuration options, storage device health, and virtual machine objects.
Monitoring vSAN Capacity

The capacity of the vSAN datastore can be monitored from a number of locations within the vSphere Client. First, one can select the datastore view, and view the summary tab for the vSAN datastore. This will show you the capacity, used and free space.

Datastore View

1. Select **Storage**
2. Select **vsanDatastore**
3. Click **Summary**
4. Note the amount of **Used** and **Free Capacity** Information
Capacity Overview

1. Select **Hosts and Clusters**
2. Select **RegionA01-COMP01**
3. Select **Monitor**
4. Scroll down and Click **vSAN\Capacity**
5. Note the **Capacity Overview** and **Deduplication and Compression Overview** Information

The Capacity Overview displays the storage capacity of the vSAN datastore, including used space and free space. The Deduplication and Compression Overview indicates storage usage before and after space savings are applied, including a Ratio indicator.
Used Capacity Object Types

1. Scroll Down to view the **Used Capacity Breakdown**
2. Note the **Object types** usage amounts

These are all the different object types one might find on the vSAN datastore. We have VMDKs, VM Home namespaces, and swap objects for virtual machines. We also have performance management objects when the vSAN performance logging service is enabled. There are also the overheads associated with on-disk format file system, and checksum overhead. Other (not shown) refers to objects such as templates and ISO images, and anything else that doesn't fit into a category above.

It's important to note that the percentages shown are based on the current amount of **Used vSAN Datastore space**. These percentages will change as more Virtual Machines are stored within vSAN (e.g. the **File system overhead %** will decrease, as one example).
Used Capacity Data Types

1. Select **Data Types** from the **Group by:** drop-down list
2. Note the **Data types** usage amounts

In this view, we can see how much data is taken up for VM data, and then, depending on the policy, we can see any capacity consumed to create replica copies of the data, witness components or RAID-5/RAID-6 parity components.

Physical Disks Capacity

1. Select **Physical Disks**
2. Scroll Over to the Right
3. Note the **Capacity** and **Used Capacity** amounts

Here we can see the amount of Used Capacity per Physical Disk.
Monitoring vSAN Performance

A healthy vSAN environment is one that is performing well. vSAN includes many graphs that provide performance information at the cluster, host, network adapter, virtual machine, and virtual disk levels. There are many data points that can be viewed such as IOPS, throughput, latency, packet loss rate, write buffer free percentage, cache de-stage rate, and congestion. Time range can be modified to show information from the last 1-24 hours or a custom date and time range. It is also possible to save performance data for later viewing.

Performance Service

With vSAN 6.7, the performance service is automatically enabled at the cluster level. The performance service is responsible for collecting and presenting Cluster, Host and Virtual Machine performance related metrics for vSAN powered environments. The performance service is integrated into ESXi, running on each host, and collects the data in a database, as an object on a vSAN datastore. The performance service database is stored as a vSAN object independent of vCenter Server. A storage policy is assigned to the object to control space consumption and availability of that object. If it becomes unavailable, performance history for the cluster cannot be viewed until access to the object is restored.

Performance Metrics are stored for 90 days and are captured at 5 minute intervals.

Validate Performance Service
1. Select **RegionA01-COMP01**
2. Select **Configure**
3. Select **vSAN\Services**
4. Select **Performance Service**
5. Note that the Performance Stats Database Object is reported as **Healthy**
6. Note that the Stats DB is using the **vSAN Default Storage Policy** (RAID-1, Failures to Tolerate = 1) and is reporting **Compliant** status

Let's examine the various Performance views next at a Cluster, Host and Virtual Machine level.

**Cluster Performance**

1. Select **RegionA01-COMP01**
2. Select **Monitor**
3. Select **vSAN\Performance**
4. Note that we can choose to view **VM**, **Backend** and **iSCSI** Performance views at the Cluster level (you can also customize the **Time Range** if desired).
5. Scroll-down to view the various metrics that are collected (**IOPS**, **Throughput**, **Latency**, etc.)

“Front End” **VM** traffic is defined as the type of storage traffic being generated by the VMs themselves (the reads they are requesting, and the writes they are committing).

“Back End” **vSAN** traffic accounts for replica traffic (I/Os in order to make the data...
redundant/highly available), and well as synchronization traffic. Both of these traffic types take place on the dedicated vSAN vmkernel interface(s) per vSphere Host.

**Host Performance**

1. Select **esx-01a.corp.local**
2. Select **Monitor**
3. Select **vSAN\Performance**
4. Note that we can choose to view **VM**, **Backend**, **Disks**, **Physical Adapters**, **Host Network** and **iSCSI** Performance views at the Host level (you can also customize the **Time Range** if desired).
5. Scroll-down to view the various metrics that are collected (**IOPS**, **Throughput**, **Latency**, etc.)

In this view we can see more Performance related metrics at the Host level vs. Cluster. Feel free to examine the various categories indicated in Step 4 to get a feel for the information that is available.
Virtual Machine Performance

1. Select **vSAN-VM**
2. Select **Monitor**
3. Select **vSAN\Performance**
4. Note that we can choose to view **VM** and **Virtual Disks** Performance views at the Virtual Machine level (you can also customize the **Time Range** if desired).
5. Scroll-down to view the various metrics that are collected (**IOPS**, **Throughput**, **Latency**, etc.)

Next we will examine the vSAN information that is accessible via the new built-in vRealize Operations for vCenter Dashboards as well as within vRealize Operations itself.
vRealize Operations within vCenter Monitoring

vSphere and vSAN 6.7 now includes vRealize Operations within vCenter. This new feature allows vSphere customers to see a subset of intelligence offered up by vRealize Operations (vR Ops) through a single vCenter user interface. Light-weight purpose-built dashboards are included for both vSphere and vSAN. It is easy to deploy, provides multi-cluster visibility, and does not require any additional licensing.

Chrome Browser Zoom

In our VMware Learning Platform (Lab) environment we have a limited amount of screen real estate (1024x768). Let's reduce our Chrome Browser Zoom so that we can view more on screen:

1. Select the **Vertical Ellipses** in the upper-right hand corner of your Chrome Browser
2. Click the ‘-’ sign to reduce your **Zoom** to **80%**
vRealize Operations

1. Select **Menu**
2. Click **vRealize Operations**
Integrated Dashboards

There are three dashboards for vSphere/vCenter, and three dashboards built specifically for vSAN. These dashboards do not replace the dashboards found in the full vR Ops product, but place a subset of the most important information directly within vCenter, for a single, unified pane of visibility. These dashboards contain widgets designed to maintain clarity and simplicity, and unlike the full vR Ops UI, will have a minimal amount of customization available. The vCenter Overview dashboard gives an aggregate view of the activity and status of your clusters managed across vCenter.

Let's examine the vSAN Dashboards:

1. Select **Quick Links**
2. Click **vSAN > Overview**

**NOTE:** If you receive messages like, "You do not have any vSAN Clusters" or "Unfortunately, you have no Clusters configured!" this is due to vR Ops for vCenter not being fully configured yet and you will need to wait longer for this to complete. Thank you for your patience.
vSAN Overview

The vSAN Overview dashboard gives an aggregate view of the activity and status of your clusters, but only for those running vSAN. Administrators can view rollup statistics for hosts, VMs, alerts, capacity, performance metrics, and more.

1. Note that information for all vSAN Clusters is aggregated in the top display panel
2. Scroll-down to examine the additional Dashboard information presented

We will examine the Cluster View Dashboard next
Quick Links

1. Select Quick Links
2. Click vSAN\Cluster View
The vSAN Cluster View dashboard provides more details specific to the selected vSAN cluster.

1. Note that you choose additional vSAN Clusters via the Change Cluster drop-down menu (our Lab environment only contains a single vSAN Cluster)
2. Scroll-down to review vSAN related metrics such as Remaining Capacity, Component Limits, IOPS, throughput, and read/write latency for the selected cluster

Let's examine our final vRealize Operations within vCenter vSAN related Dashboard.
Quick Links

1. Select **Quick Links**
2. Click **vSAN\Alerts**
Alert Lists

1. The Alerts List will surface Critical, Immediate, Warning and Info Alerts which can be examined in further detail if desired.

Note: Issues in your Lab may differ from those shown in the screenshot.

For our final lesson within this module, we will log directly into vRealize Operations to examine the vSAN related Dashboards that are available.
Quick Links

1. Select **Quick Links**
2. Click **Open vRealize Operations**
vSAN integration is now fully built into vRealize Operations 6.6 and later, which means the same level of monitoring and analytics for vSphere is easily extended to vSAN. The APIs in vSAN were significantly enhanced to allow vR Ops to fetch data directly from vSAN. This results in more detailed information for vR Ops to analyze, and make visible. Out of the box, vR Ops provides the following:

- Four, prebuilt vSAN dashboards with multi-cluster visibility and analytics.
• Dashboards display vSAN and non-vSAN metrics together to show critical correlation across various resources.
• Native integration into vR Ops means that no additional Management Packs need to be installed.
• Dashboards can be cloned, and are fully customizable.

vRealize Operations uses vSAN's enhanced set of APIs to fetch data collected by the vSAN health and performance service. The vSAN health and performance service was introduced in vSAN 6.2, and provides a way for vSAN administrators to look at basic performance metrics of vSAN directly in vCenter. Unlike other metrics, vSAN performance metrics are not stored in vCenter. It is housed as an object that resides on the vSAN datastore. With each subsequent release of vSAN, additional metrics have been exposed in the performance service. However, the metrics in the performance services are not customizable, and have a limited window in which data can be viewed (1 hour to 24 hours), and a limited retention time (90 days). vR Ops fetches this vSAN performance data, and provides the user with much more flexibility in manipulation and retention of the data. vR Ops requires that the vSAN health and performance service be enabled to properly collect vSAN related metrics.

**Dashboards**

1. Select the **Home** drop-down menu
2. Click **Dashboards**
vRealize Operations handily groups out of box dashboards by activity type including **Operations**, **Capacity & Utilization** and **Performance Troubleshooting**.

We will examine vSAN Operations first:

1. Select **Dashboards**
2. Select the **All Dashboards** drop-down menu
3. Hover over **Operations**
4. Click **vSAN Operations Overview**
vSAN Operations Overview

The vSAN Operations Overview dashboard aims to provide a broad overview of the status of one or more vSAN powered clusters in an environment. This dashboard allows an administrator to see aggregate cluster statistics, along with cluster specific measurements. Not only does this dashboard touch on some of the key indicators of storage such as IOPS, throughput, and latency, it also provides other measurements that contribute to the health and well-being of the cluster, such as the host count, CPU and Memory utilization, and alert volume.

1. Click the ‘<<‘ chevron to give yourself more screen real estate
2. Scroll-down to view more information
1. Select the **All Dashboards** drop-down menu
2. Hover over **Capacity & Utilization**
3. Click **vSAN Capacity Overview**

### vSAN Capacity Overview

The vSAN Capacity Overview dashboard provides a wealth of vSAN capacity information not available in the point-in-time storage capacity statistics found in vCenter. This dashboard takes advantage of vR Ops' ability to capture capacity utilization over a period of time, which offers extensive insight into past trends of capacity usage.
Capacity is about more than just storage resource usage. It is about CPU and memory capacity as well. This dashboard gives a window into remaining CPU and memory capacity for a vSAN cluster. This data, paired with the storage utilization data will give an administrator a better understanding if scaling up (adding more storage to each host) or scaling out (adding more hosts) will be the best approach for an environment.

1. **Scroll-down** to view more information

### All Dashboards

![Dashboard Menu](image)

1. Select the **All Dashboards** drop-down menu
2. Hover over **Performance Troubleshooting**
3. Click **Troubleshoot vSAN**
Troubleshoot vSAN

The Troubleshoot vSAN dashboard assembles a collection of alerts, metrics, and trending results to help determine the source of what changed in an environment, and when the change occurred. It assembles them in a systematic, layered approach to assist with troubleshooting and root cause analysis of an environment.

The dashboard begins with widgets showing any active alerts for the selected cluster, and identifies the hosts contributing to the alerts. Also displayed are key performance indicators at the cluster level. Highlighting the desired cluster will expose trending of cluster related resources (CPU Workload, Memory workload, Capacity remaining, etc.) over the past 12 hours. Widgets for VM read and write latency show a history of storage performance for the past 24 hours.

1. Scroll-down to view more information

Troubleshoot vSAN, cont.

1. Click the down Chevrons to expand Capacity Disks
Troubleshoot vSAN, cont.

1. Hover over the **Capacity Disks** toolbar and click the **Show Toolbar** icon
2. Expand the **1-Bus Resets** pull-down menu

The Troubleshoot vSAN dashboard also looks at the health and performance of cache and capacity disks of the selected vSAN cluster. These widgets allow you to choose from one of the seven defined data types, and will then render the amount of activity in the heat map. The data types that can be viewed include bus resets, commands aborted per second, and five types of SMART data measurements.

All Dashboards
1. Select the **All Dashboards** drop-down menu
2. Hover over **Operations**
3. Click **Migrate to vSAN**

**Migrate to vSAN**

The Migrate to vSAN dashboard is designed to assist with migration efforts over to vSAN. The dashboard provides a comparison of critical storage metrics of a VM running on a data store running on traditional storage against a VM powered by vSAN. This dashboard recognizes the phased approach that can occur when transitioning to a new storage system, and is intended to monitor what matters most in the transition: the effective performance behavior between storage systems as seen by the application, or VM.

While each VM's workload will be unique, and not an exact moment by moment mirror of another VM's workload, one can compare similar systems effectively. For example, applications farms such as SQL clusters, ERP systems, SharePoint servers, or some other multi-tiered application use a cluster of VMs to provide back-end, middle-tier, or front-end services. Any of these examples would be an ideal scenario for comparison, as one of the systems in the application farm can be migrated over to vSAN, and compared to a similar system running on the legacy storage.

1. Note that we have a non-vSAN Datastore in our Lab (freeNAS appliance: RegionA01-ISCSI01-...)
2. **Scroll-down** to compare **Non vSAN VM IOPS and Latency** vs. vSAN VM IOPS and Latency

- The **Non vSAN VM widgets** will show the aggregate virtual disk IOPS, read latency, and write latency of the selected VM running on a legacy data store. The **vSAN VM widgets** will show the same metrics of the selected VM running on a vSAN powered data store.
• Thanks to the power of customization, you may wish to simplify this dashboard. This might allow you to utilize a larger portion of the screen for key metrics, and simplify operation, or reduce the time window of observation to a smaller window.
Conclusion

In this module, we showed you how to validate vSAN Health, Monitor vSAN Capacity & Performance as well as utilize vRealize Operations for vCenter and vRealize Operations Dashboards.

You've finished Module 2

Congratulations on completing Module 2.

If you are looking for additional information on topic:

- vSAN Operations Guide
- vRealize Operations within vCenter for vSAN 6.7
- vSAN vRealize Operations in vSAN Environments
- Go to VMware Storage Hub for all things related to vSAN.

Proceed to any remaining module below which interests you most.

- **Module 3 - vSAN 6.7 Day-2 Operations** (30 minutes) (Basic)
  Module 3 describes how to perform Day-2 Activities on your vSAN Cluster such as utilizing Storage Policy-Based Management, determining Maintenance Mode options and adding additional capacity.

- **Module 4 - vSAN Availability** (30 minutes) (Basic)
  Module 4 discusses vSAN Failure Domains, Active/Active Datacenters with vSAN Stretched Cluster and vSAN Disaster Recovery Scenarios.

- **Module 5 - vSAN Interoperability** (45 minutes) (Intermediate)
  Module 5 illustrates utilizing vRealize Log Insight to review centralized vSAN Logs, vSAN iSCSI integration and vSAN CLI interfaces.

- **Module 6 - vSAN Encryption** (30 minutes) (Intermediate)
  Module 6 discusses vSAN security parameters such as FIPS 104-2 Validation and vSAN Data-at-rest Encryption.
How to End Lab

To end your lab click on the **END** button.
Module 3 - vSAN 6.7 Day 2 Operations (30 Minutes)
Introduction

What happens after you've successfully enabled your vSAN Cluster?

Now it's time to learn how to utilize the Day 2 power of Storage Policy Based Management as well as what to expect when performing Maintenance activities, adding additional Capacity and updating vSAN.
Adding vSAN Capacity

One of the really nice features is the simplistic scale-out nature of vSAN. If you need more compute or storage resources in the cluster, simply add another host to the cluster.

Lab Preparation

If you have completed the previous modules by completing the steps as outlined, then you can skip the next few steps to prepare your environment for this lesson.

Click here to go to the lesson.

If you have skipped to this module, we will use our Module Switcher PowerCLI Application to prepare the environment.

Module Switcher

Double-Click the Module Switcher Desktop Shortcut called HOL-1908 HCI

Module 3 Start

1. Click the Module 3 - Start button
This Startup Routine can take a few minutes to complete - thank you for your patience!

Monitor Progress

Monitor Progress until Complete.

- Press Enter to continue (and close the PowerCLI Window)

Lab Prep Complete

Your Lab has been successfully prepared for Module 3!

1. Click Close to safely stop the Module Switcher

Please Note that you cannot 'go back' and take Modules prior to the one you are currently in unless you end the lab and start it over again (for example: If you Start Module 4, you cannot use the Module Switcher to Start Labs 1, 2 or 3).

Open Chrome Browser from Windows Quick Launch TaskBar

1. Click on the Chrome Icon on the Windows Quick Launch Task Bar.
Login to vSphere Client

1. On the vSphere Client login screen, select "Use Windows session authentication"
2. Click Login
Examine the Default Storage Policy

1. From the **Menu** page of the vSphere Client
2. Select **Hosts and Clusters**
Lab Environment Review - Capacity

Let's have a look at how our cluster capacity looks.

1. Select the vSAN Cluster called RegionA01-COMP01
2. Select Monitor
3. Select vSAN > Capacity

The vSAN datastore is ~59.98 GB in size with ~54.16 GB free.

Lab Environment Review - Compute

Let's have a look at how our cluster currently looks.
There are currently three hosts in the cluster, and there are additional hosts not in the cluster.

1. Select the ESXi host called **esx-04a.corp.local**
2. Select **Configure**
3. Select **Storage > Storage Devices**

On the ESXi host you can see that we have some devices that we can use to expand our vSAN Datastore (there are multiple 5 GB Flash and the 10 GB Flash devices).
Add Additional nodes to cluster

We are now going to add the esx-04a.corp.local to the vSAN Cluster.

Drag and drop esx-04a.corp.local into RegionA01-COMP01 cluster

If the Drag and Drop does not seem to be working for you, right click the ESXi host called esx-04a.corp.local an select Move to .... Select the cluster called RegionA01-COMP01.
Move Host into Cluster

1. If prompted, Click **OK**
Take Host out of Maintenance Mode

The ESXi host is still in Maintenance Mode.

1. Right click the ESXi host called esx-04a.corp.local
2. Select Maintenance Mode
3. Select Exit Maintenance Mode

If the Exit Maintenance Mode option is not available, refresh the vSphere Client and try the operation again.
Now that we have taken the host out of maintenance mode, we can see a few informational messages on the Summary screen.

1. Select the ESXi host called **esx-04a.corp.local**
2. Select **Summary**

These messages are telling us that we have hosts in the vSAN Cluster that cannot communicate with each other over the vSAN Network.
Let's review the current state of the Networking on the ESXi host.

1. Select the ESXi host called \textit{esx-04a.corp.local}
2. Select \textbf{Configure}
3. Select \textbf{Networking > VMkernel adapters}

There are 3 VMkernel adapters configured, one for Management traffic, one for traditional Storage traffic and one for vMotion traffic.

We will now configure a VMkernel adapter for the vSAN Network traffic for this host.

4. Select \textbf{Add Networking}

\textbf{Configure vSAN Networking}

<table>
<thead>
<tr>
<th>esx-04a.corp.local - Add Networking</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1Select connection type</strong></td>
</tr>
<tr>
<td>2 Select target device</td>
</tr>
<tr>
<td>3 Port properties</td>
</tr>
<tr>
<td>4 IPv4 settings</td>
</tr>
<tr>
<td>5 Ready to complete</td>
</tr>
</tbody>
</table>

1. Select \textbf{VMkernel Network Adapter}

Click \textbf{NEXT}
Configure vSAN Networking

1. Click the **Browse** button
2. Select the VMkernel adapter called **vSAN-RegionA01-vDS-COMP**

Click **NEXT**
Configure vSAN Networking

1. Enable the **vSAN** service

Click **NEXT**
1. Select **Use static IPv4 settings**

Enter the following information for the Network configuration:

- IPv4 address : 192.168.130.54
- Subnet mask : 255.255.255.0
- Override default gateway for this adapter : Enabled
- Default gateway : 192.168.130.1

Click **NEXT**
Configure vSAN Networking

esx-04a.corp.local - Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings

Ready to complete
Review your settings selections before finishing the wizard.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed port group</td>
<td>vsAN-RegionACI-vDS-COMP</td>
</tr>
<tr>
<td>Distributed switch</td>
<td>RegionACI-vDS-COMP</td>
</tr>
<tr>
<td>vMotion</td>
<td>Disabled</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fault Tolerance logging</td>
<td>Disabled</td>
</tr>
<tr>
<td>Management</td>
<td>Disabled</td>
</tr>
<tr>
<td>vSphere Replication</td>
<td>Disabled</td>
</tr>
<tr>
<td>vSphere Replication NFC</td>
<td>Disabled</td>
</tr>
<tr>
<td>vSAN</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

NIC settings
- MTU: 1500
- TCP/IP stack: Default

IPv4 settings
- IPv4 address: 192.168.130.54 (static)
- Subnet mask: 255.255.255.0
- Default gateway for IPv4: 192.168.130.1

Review the configuration settings
Click **FINISH**
Verify vSAN Networking

Select the VMkernel adapter called **vSAN-RegionA01-vDS-COMP**

Review the properties of the VMkernel adapter.

After a while the Alarms should disappear from the host.
Create a Disk Group on a New Host

Now that we have configured the Networking, we will grow our vSAN Datastore by using the local storage on the ESXi host.

1. Select vSAN Cluster called RegionA01-COMP01
2. Select Configure
3. Select vSAN > Disk Management
4. Select esx-04a.corp.local (do not click host name hyperlink directly, click beside the name)

The ESXi host called esx-04a.corp.local is now part of the vSAN Cluster, but it is not contributing any storage to the Disk Groups yet.

5. Click Create a new Disk Group
Create a Disk Group on a New Host

As before, we select a flash device as cache disk and three flash devices as capacity disks. This is so that all hosts in the cluster maintain a uniform configuration.

1. Select one **5 GB flash** drive for the **Cache** tier
2. Select 2x **10 GB** flash drives for the **Capacity** tier

Click **CREATE**
Verify a Disk Group on a New Host

Once the disk group has been created, the disk management view should be revisited,

Verify that the:

1. vSAN Health Status is Healthy
2. That all the Disk Groups are in the same Network Partition Group
3. The Disk Format Version is the same on all Disk Groups
Verify New vSAN Datastore Capacity

The final step is to ensure that the vSAN datastore has now grown in accordance to the capacity devices in the disk group that was just added on the fourth host. Return to the Capacity view and examine the total and free capacity fields.

1. Select the vSAN Cluster called **RegionA01-COMP01**
2. Select **Monitor**
3. Select **vSAN > Capacity**

The vSAN datastore has now grown to ~79.98 GB in size with ~72.24 GB free.

**Conclusion**

In this module we show you how to expand the capacity of the vSAN Cluster by adding addition ESXi hosts.

Although compute-only hosts can exist in a vSAN environment and consume capacity from other hosts in the cluster, add uniformly configured hosts to provide smooth operation. For best results, add hosts configured with both cache and capacity devices.
Storage Policy Based Management

As an abstraction layer, SPBM abstracts storage services delivered by Virtual Volumes, vSAN, I/O filters, or other storage entities.

Multiple partners and vendors can provide Virtual Volumes, vSAN, or I/O filters support. Rather than integrating with each individual vendor or type of storage and data service, SPBM provides a universal framework for many types of storage entities.

SPBM offers the following mechanisms:

- Advertisement of storage capabilities and data services that storage arrays and other entities, such as I/O filters, offer.
- Bidirectional communications between ESXi and vCenter Server on one side, and storage arrays and entities on the other.
- Virtual machine provisioning based on VM storage policies.

Examine the Default Storage Policy

vSAN requires that the virtual machines deployed on the vSAN datastores are assigned at least one storage policy. When provisioning a virtual machine, if you do not explicitly assign a storage policy to the virtual machine the vSAN Default Storage Policy is assigned to the virtual machine.

The default policy contains vSAN rule sets and a set of basic storage capabilities, typically used for the placement of virtual machines deployed on vSAN datastores.
vSAN Default Storage Policy Specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary level of failures to tolerate</td>
<td>1</td>
</tr>
<tr>
<td>Number of disk stripes per object</td>
<td>1</td>
</tr>
<tr>
<td>Flash read cache reservation, or flash capacity used for the read cache</td>
<td>0</td>
</tr>
<tr>
<td>Object space reservation</td>
<td>0</td>
</tr>
<tr>
<td>Note: Setting the Object space reservation to zero means that the virtual disk is thin provisioned, by default.</td>
<td></td>
</tr>
<tr>
<td>Force provisioning</td>
<td>No</td>
</tr>
</tbody>
</table>

The following characteristics apply to the **vSAN Default Storage Policy**.

- The vSAN default storage policy is assigned to all virtual machine objects if you do not assign any other vSAN policy when you provision a virtual machine.
- The vSAN default policy only applies to vSAN datastores. You cannot apply the default storage policy to non-vSAN datastores, such as NFS or a VMFS datastore.
- You can clone the default policy and use it as a template to create a user-defined storage policy.
- You cannot delete the default policy.

Open Chrome Browser from Windows Quick Launch TaskBar

1. Click on the **Chrome** Icon on the Windows Quick Launch Task Bar.
1. On the vSphere Client login screen, select "Use Windows session authentication"
2. Click Login
Examine the Default Storage Policy

1. From the **Menu** page of the vSphere Client
2. Select **Policies and Profiles**
Examine the Default Storage Policy

1. Select **VM Storage Policies**
2. Select the VM Storage Policy called **vSAN Default Storage Policy**
3. Select **Rules**.

The default rules for the Storage Policy are displayed.
Examine the Default Storage Policy

1. Select the VM Storage Policy called **vSAN Default Storage Policy**
2. Select **Storage Compatibility**

Here we can see that the **vsanDatastore** is compatible with this storage policy.

**Deploy VM with Default Policy**

We will now clone a VM and apply the Default Storage Policy
1. Select **Menu**
2. Select **Hosts and Clusters**

**Deploy VM with Default Policy**

We will clone the VM called CORE-A (which currently resides on a Local VMFS datastore) to the vSAN Datastore and apply the Default Storage Policy.

1. Expand the ESXi host called **esx-07a.corp.local** and right click the VM called **CORE-A**
2. Select **Clone**
3. Select **Clone to Virtual Machine**
Deploy VM with Default Policy

Give the Virtual Machine a name:

vSAN Default Storage Policy

Click NEXT

Deploy VM with Default Policy
1. Expand the Compute resource called **RegionA01-COMP01**
2. Select the ESXi host called **esx-01a.corp.local**

Click **NEXT**

**Deploy VM with Default Policy**

1. For the VM Storage Policy, select **vSAN Default Storage Policy**

The resulting list of compatible datastores will be presented, in our case the vsanDatastore. In the lower section of the screen we can see that the vSAN storage consumption would be 200.00 MB disk space and 0.00 B reserved Flash space.

Since we have a VM with 100 MB disk and the Default Storage Policy, the VSAN disk consumption will be 200.00 MB disk.

Click **NEXT**

Click **NEXT** on the **Select clone options**
Deploy VM with Default Policy

Click **FINISH**

Wait for the Clone operation to complete.

Check the **Recent Tasks** for a status update on the Clone virtual machine task.
Verify VM has Default Storage Policy

Once the clone operation has completed,

1. Select the VM called vSAN Default Storage Policy
2. Select Summary
3. Select Related Objects

The VM is now residing on the vsanDatastore

4. Select VM Storage Policies

Here we can see that the VM Storage Policy for this VM is set to vSAN Default Storage Policy and the policy is compliant.
VM Disk Policies

1. Select the VM called **vSan Default Storage Policy**
2. Select **Configure**
3. Select **Policies**
4. Select **Hard Disk 1**

Here we can see the VM Storage Policy that is applied to **VM Home Object** and the **Hard Disk Object**.
VM Disk Policies

1. Select the **RegionA01-COMP01**
2. Select **Monitor**
3. Select **vSAN > Virtual Objects**
4. Select **vSAN Default Storage Policy > Hard Disk 1**

Verify that the Placement and Availability is **Healthy** and the **vSAN Default Storage Policy** is applied.

5. Click **View Placement Details**

VM Disk Policies
Here we can see the Component layout for the Hard Disk.

1. There are 2 Components spread across 2 different ESXi Hosts
2. The Witness component on another ESXi host.

Click **CLOSE**

**New VM Storage Policy ( Raid 5/6 - Erasure coding )**

**Overview of RAID-5**

- Number of failure to Tolerate = 1
- Failure Tolerance Method = Capacity
- Uses x1.33 rather than x2 capacity when compared to RAID-1
- Requires a minimum of 4 hosts in the vSAN cluster

Note that there is a requirement on the number of hosts needed to implement RAID-5 or RAID-6 configurations on vSAN.

For RAID-5, a minimum of 4 hosts are required; for RAID-6, a minimum of 6 hosts are required.

The objects are then deployed across the storage on each of the hosts, along with a parity calculation. The configuration uses distributed parity, so there is no dedicated parity disk. When a failure occurs in the cluster, and it impacts the objects that were deployed using RAID-5 or RAID-6, the data is still available and can be calculated using the remaining data and parity if necessary.
A new policy setting has been introduced to accommodate the new RAID-5/RAID-6 configurations.

This new policy setting is called Failure Tolerance Method. This policy setting takes two values: performance and capacity. When it is left at the default value of performance, objects continue to be deployed with a RAID-1/mirror configuration for the best performance. When the setting is changed to capacity, objects are now deployed with either a RAID-5 or RAID-6 configuration.

The RAID-5 or RAID-6 configuration is determined by the number of failures to tolerate setting. If this is set to 1, the configuration is RAID-5. If this is set to 2, then the configuration is a RAID-6.

**New VM Storage Policy (Raid 5/6 - Erasure coding)**

First we need to create a VM Storage Policy that will define the Failure Tolerance method of Raid5/6.

1. From the **Menu** page of the vSphere Client
2. Select **Policies and Profiles**
New VM Storage Policy (Raid 5/6 - Erasure coding)

1. Select VM Storage Policies
2. Select Create VM Storage policy

New VM Storage Policy (Raid 5/6 - Erasure coding)

Create a new VM Storage Policy using the following name:

PFTT=1-Raid5

Click NEXT
New VM Storage Policy (Raid 5/6 - Erasure coding)

Select **Enable rules for "vSAN" storage**

Click **NEXT**

New VM Storage Policy (Raid 5/6 - Erasure coding)

1. Select the following options:

Site disaster tolerance: None (standard cluster)
Failures to tolerate: 1 failure - Raid-5 (Erasure Coding)

2. Click **Advanced Policy Rules**
New VM Storage Policy (Raid 5/6 - Erasure coding)

Review the options that are available here, but leave at the default settings.

Click NEXT

New VM Storage Policy (Raid 5/6 - Erasure coding)

Verify that the vsanDatastore is compatible against the VM Storage Policy.

Click NEXT
New VM Storage Policy ( Raid 5/6 - Erasure coding )

<table>
<thead>
<tr>
<th>Create VM Storage Policy</th>
<th>Review and finish</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Name and description</td>
<td>General</td>
</tr>
<tr>
<td>2 Policy structure</td>
<td>Name</td>
</tr>
<tr>
<td>3 vSAN</td>
<td>Description</td>
</tr>
<tr>
<td>4 Storage compatibility</td>
<td>VSAN</td>
</tr>
<tr>
<td>5 Review and finish</td>
<td>Site disaster tolerance</td>
</tr>
<tr>
<td></td>
<td>Failures to tolerate</td>
</tr>
<tr>
<td></td>
<td>Advanced Policy Rules</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Review the settings and click **FINISH**
New VM Storage Policy (Raid 5/6 - Erasure coding)

Here we can see the rules that make up our VM Storage Policy.
Assign VM Storage Policy to an existing VM

Now that we have created a new VM Storage Policy, let's assign that policy to an existing VM on the vSAN datastore.

1. Select **Menu** on the vSphere Client
2. Select **Hosts and Clusters**

**Assign VM Storage Policy to an existing VM**

1. Select the VM called **vSAN Default Storage Policy**
2. Select **Configure**
3. Select **More > Policies**

Here we can see that the **vSAN Default Storage Policy** is assigned to this VM.

4. Select **EDIT VM STORAGE POLICY**
Assign VM Storage Policy to an existing VM

1. Change the VM storage Policy from the dropdown list to PFTT=1-Raid5

Click OK

Assign VM Storage Policy to an existing VM

Verify that the VM Storage Policy has been changed and that the VM is compliant against the new storage Policy.
Assign VM Storage Policy to an exiting VM

1. Select the cluster called **RegionA01-COMP01**
2. Select **Monitor**
3. Select **vSAN > Virtual Objects**
4. Select **View Placement Details**

Assign VM Storage Policy to an exiting VM

Here we can see the new revised Component layout for the VM with the **Raid-5 Storage Policy**.
We now have a components spread across 4 ESXi hosts.

Click **CLOSE**

**Modify an existing VM Storage Policy**

1. From the **Home** page of the vSphere Client
2. Select **Policies and Profiles**
Modify an existing VM Storage Policy

1. Select VM Storage Policies
2. Select the VM Storage Policy called PFTT=1-Raid5
3. Select Edit Settings

On the Name and Description dialog, Click NEXT
Modify an existing VM Storage Policy

On the Policy structure dialog, Click NEXT

Modify an existing VM Storage Policy

1. On the vSAN dialog, select Advanced Policy Rules
2. Modify the Number of disk stripes per object to 2

Click NEXT
Modify an existing VM Storage Policy

On the Storage compatibility dialog, click **NEXT**

Modify an existing VM Storage Policy

On the Review and Finish dialog, click **FINISH**
Modify an existing VM Storage Policy

The VM storage policy is in use by 1 virtual machine(s). Changing the VM storage policy will make it out of sync with those 1 virtual machine(s).

1. Select **Manually later**
2. Select **Yes**

Modify an existing VM Storage Policy

1. Select **VM Compliance**
2. You will see that the Compliance Status of the VM has now changed to **Out of Date** since we have changed the VM Storage Policy that this VM has been using.
3. Click **Reapply VM Storage Policy**

**Modify an existing VM Storage Policy**

Reapplying the selected VM storage policy might take significant time and system resources because it will affect 1 VM(s) and will move 88 MB of data residing on vSAN datastores.

1. Click **Show predicted storage impact**

**Modify an existing VM Storage Policy**

The changes in the VM storage policies will lead to changes in the storage consumption on some datastores. The storage impact can be predicted only for vSAN datastores, but datastores of other types could also be affected.

After you reapply the VM storage policies, the storage consumption of the affected datastores is shown.

Click **CLOSE**
Modify an existing VM Storage Policy

Click OK to reapply the VM Storage Policy.

Modify an existing VM Storage Policy

Once the VM Storage Policy has been reapplied, versify that the VM is in a Compliant state again with the VM Storage Policy.
Modify an existing VM Storage Policy

1. From the **Home** page of the vSphere Client
2. Select **Hosts and Clusters**

![Diagram of vSphere Client interface]

**Modify an existing VM Storage Policy**

1. Select the cluster called **RegionA01-COMP01**
2. Select **Monitor**
3. Select **vSAN > Virtual Objects**
4. Select **View Placement Details**
Modify an existing VM Storage Policy

Here we can see the new revised Component layout for the VM with the **Raid-5 Storage Policy**.

We now have components spread across 4 ESXi hosts with a Raid-0.

Click **CLOSE**

**Conclusion**

Storage Policy Based Management (SPBM) is a major element of your software-defined storage environment. It is a storage policy framework that provides a single unified control panel across a broad range of data services and storage solutions.

The framework helps to align storage with application demands of your virtual machines.
vSAN Maintenance

Before you shut down, reboot, or disconnect a host that is a member of a vSAN cluster, you must place the host in maintenance mode. When you place a host in maintenance mode, you must select a data evacuation mode, such as Full data migration to other hosts, Ensure data accessibility from other hosts or No data migration. In this Lesson, we will examine the various Maintenance Mode options as well as discuss when you might want to use one method vs. another.

Virtual Objects

Let's examine the component layout across the vSAN Datastore for the Virtual Machine, vSAN-VM:

1. Select RegionA01-COMP01
2. Select Monitor
3. Select Virtual Objects
4. View Placement Details
5. Examine the components

Let's examine the component layout across the vSAN Datastore for the Virtual Machine, vSAN-VM:
4. Enable the Checkbox for **Hard disk 1**
5. Click **View Placement Details**

### Physical Placement

This Virtual Machine is using the Default vSAN Storage Policy (Primary Failures to Tolerate = 1) (PFTT).

1. PFTT=1 means that two of the VM's vSAN Components are in a RAID-1 Mirror across different vSphere Hosts as evidenced by the two **Component replicas** shown. A third **Witness** component is also present. Furthermore, we can see that all three components are reporting an **Active** (green) status.

**Note:** VM Object layout may be different in your lab vs. screenshot example
Maintenance Mode

1. Right-click esx-01a.corp.local
2. Select Maintenance Mode \ Enter Maintenance Mode

Maintenance Mode, cont.

vSAN data migration:
Specify how vSAN will evacuate data residing on the host before entering maintenance mode

- Full data migration
  - Sufficient capacity on other hosts. 436 MB will be moved.
- Ensure accessibility
  - No data will be moved. 4 objects will become non-compliant with storage policy.
- No data migration
  - 4 objects will become non-compliant with storage policy.

Note that there are three vSAN data migration options:

1. Full data migration
2. Ensure accessibility
3. No data migration

Let's examine these choices in more detail.

**Full data migration**

This option moves all of the vSAN components from the Host entering maintenance mode to other Hosts in the vSAN cluster. This option is commonly used when a Host will be offline for an extended period of time or permanently decommissioned.

**Note:** In order to maintain PFTT=1, we must have a 4th Host in our Cluster to Migrate any impacted Components to. In our current 3-Node Cluster, we do not have enough Hosts to satisfy this Maintenance Mode choice.
Ensure accessibility

1. vSAN will verify whether the majority of a Virtual Machine's objects remain accessible even though one or more components will be absent due to the host entering maintenance mode.
2. If the majority of a Virtual Machine's objects will remain accessible, vSAN will not migrate impacted component(s).

If the VM's objects would become inaccessible, vSAN will migrate the necessary number of components to other hosts ensuring that the object accessibility. This option is the default and it is commonly used when the host will be offline for just a short amount of time, e.g., a host reboot. It minimizes the amount of data that is migrated while ensuring all objects remain accessible. However, the level of failure tolerance will likely be reduced for some objects until the host exits maintenance mode.

Note: This is the only evacuation mode available if you are working with a three-host cluster or a vSAN cluster configured with three fault domains.
No data migration

Data is not migrated from the host as it enters maintenance mode. This option can also be used when the host will be offline for a short period of time. All objects will remain accessible as long as they have a storage policy assigned where the Primary Level of Failures to Tolerate is set to one or higher.

1. This Virtual Machine (utilizing a PFTT=0 policy) will not be accessible when the Host enters Maintenance mode as it's storage component will not be migrated and will therefore be offline.
Enter Maintenance Mode

A host in maintenance mode does not perform any activities on virtual machines, including virtual machine provisioning. The host configuration is still enabled. The Enter Maintenance Mode task does not complete until the above state is completed. You might need to either power off or migrate the virtual machines from the host manually. You can cancel the Enter Maintenance Mode task at any time.

There are hosts in a vSAN cluster. Once the hosts are removed from the cluster, they will not have access to the vSAN datastore and the state of any virtual machines on that datastore.

vSAN data migration:
Specify how vSAN will evacuate data residing on the host before entering maintenance mode

- Full data migration
  - Sufficient capacity on other hosts. 436 MB will be moved.

1. Ensure accessibility
   - No data will be moved. 4 objects will become non-compliant with storage policy.

- No data migration
  - 4 objects will become non-compliant with storage policy.

See full results

1. Validate that **Ensure accessibility** is selected
2. Click **See full results**
Pre-check evacuation

1. Select **Ensure data accessibility from other hosts**. Note that No data will be moved.
2. Note that the Virtual Machines objects will become **non-compliant** with their storage policy.

As we learned earlier, the Virtual Machine storage will still be accessible as there are enough remaining components elsewhere on the Cluster. Non-compliant, in this case, does not mean that the VM is not available.

3. Click **CLOSE**
Enter Maintenance Mode, cont.

1. Validate that Ensure accessibility is still selected
2. Click OK to enter Maintenance Mode
3. Click OK to acknowledge Warning message (not shown)

Enter Maintenance Mode, cont.

1. Select Recent Tasks (lower-left hand corner)
2. Monitor Enter Maintenance Mode progress until complete

Virtual Objects

1. Notice that our vSAN-VM is still online as evidenced by the Green Play Icon (you could perform a ping test as well but we will skip that for now)
2. Select RegionA01-COMP01
3. Select Monitor
4. Select vSAN\Virtual Objects
5. Note that the VM is currently in a Reduced availability with no rebuild status. Additionally, a delay timer is counting down (more on that in a moment)
6. Select Hard disk 1
7. Click View Placement Details
Physical Placement

1. Note that one of the Virtual Machine's Objects are now in an **Absent** state

vSAN waits 60 minutes before rebuilding any objects located on the unavailable host (hence the **rebuild timer** notification we saw previously). If the Host does not return within 60 minutes, vSAN marks the impacted Objects as **Degraded** and attempts to rebuild them on another Host in the cluster (assuming there is an available Host, which in our current 3-Node Cluster, there is not).

(The timer length is configurable and you can find a link to a KB article in the Conclusion section for this Module with more details).

2. Click **Close**
Exit Maintenance Mode

1. Right-click **esx-01a.corp.local**
2. Hover over **Maintenance Mode**
3. Click **Exit Maintenance Mode**

**Healthy**

Note that the Virtual Machine is once again reporting a **Healthy** (green) status. vSAN has automatically 'caught up' the Object that was on the Maintenance Mode Host as part of putting the Host back into service.

(You might need to refresh the vSphere client in order to confirm Healthy status)
Updating vSAN

With the release of vSAN 6.6.1 and later versions, 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.

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 new type of baseline available now on vSAN VUM. This baseline is read only and as a result cannot be edited. One base line 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.

**vSAN Health Checks**

1. Select the **RegionA01-COMP01** Cluster
2. Select **Monitor**
3. Click vSAN\Health
vSAN Health Checks, cont.

Within the vSAN Health Check a **vSAN Build Recommendation** is available for vSAN VUM integration that includes two health tests:

1. **vSAN Build Recommendation Engine Health**

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

2. **vSAN build recommendation**

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

3. (Optional) Click one of these Health Tests and examine the details surrounding the tests by selecting 'Info' (not shown)

**Note:** Our Hands On Lab does not have the necessary Internet connectivity therefore we cannot configure this functionality within the Lab.

**Remediation**

VMware Updating Manager (VUM) Remediation is not automatic and has to be instigated to by the administrator. The administrator is not required to follow the system baseline recommendations that have been automatically created if they so choose.

A single host can be remediated in a given vSAN Cluster or you can remediate the entire vSAN Cluster at one time.
Conclusion

In this module, we showed you how to leverage powerful Storage Policy Based Management, examine Maintenance Mode considerations when performing vSAN Cluster Maintenance, easily add Additional vSAN Capacity and explore built-in VMware Update Manager capabilities for updating vSAN.

You've finished Module 3

Congratulations on completing Module 3.

If you are looking for additional information on topic:

- vSAN Storage Policy Based Management
- vSAN Maintenance Mode procedures
- Changing the CLOM.Delay (rebuild timer)
- vSAN Scale Up by Adding Additional Disks
- vSAN Scale Out by Adding A Host
- vSAN 6.7 Upgrade Considerations
- Go to VMware Storage Hub for all things related to vSAN.

Proceed to any remaining module below which interests you most.

- **Module 4 - vSAN Availability** (30 minutes) (Basic)

  Module 4 discusses vSAN Failure Domains, Active/Active Datacenters with vSAN Stretched Cluster and vSAN Disaster Recovery Scenarios.

- **Module 5 - vSAN Interoperability** (45 minutes) (Intermediate)

  Module 5 illustrates utilizing vRealize Log Insight to review centralized vSAN Logs, vSAN iSCSI integration and vSAN CLI interfaces.

- **Module 6 - vSAN Encryption** (30 minutes) (Intermediate)

  Module 6 discusses vSAN security parameters such as FIPS 104-2 Validation and vSAN Data-at-rest Encryption.

How to End Lab

![End button](image-url)
To end your lab click on the **END** button.
Module 4 - vSAN 6.7
Availability (30 Minutes)
Introduction

Understanding vSAN Availability is a critical aspect of running a vSAN Environment. Learning when to introduce vSAN as a Disaster Recovery solution and how to enable vSAN Stretched Clusters are equally important.
vSAN Availability and Fault Domains

vSAN has built-in availability capabilities that protect you from hardware failures which can occur at a Disk, Host or Network Layer when utilizing vSAN Hyper-Converged Infrastructure.

In this Lesson, we will define Fault Domains as applicable to vSAN as well as review different availability mechanisms. We'll also ask you to configure Fault Domains for Rack Isolation (protecting against a single Rack failure). Lastly, we will end the lesson with a discussion of different failure scenarios as well as design recommendations to help alleviate or mitigate these situations.

Lab Preparation

If you have completed the previous module by completing the steps as outlined, then you can skip the next few steps to prepare your environment for this lesson.

Click here to go to the lesson.

If you have skipped to this module, we will use our Module Switcher PowerCLI Application to prepare the environment.

Module Switcher

Double-Click the Module Switcher Desktop Shortcut called HOL-1908 HCI
Module 4 Start

1. Click the **Module 4 - Start** button

This Startup Routine can take a few minutes to complete - thank you for your patience!

**Monitor Progress**

Monitor Progress until Complete.

- Press **Enter** to continue (and close the PowerCLI Window)

**Lab Prep Complete**

Your Lab has been successfully prepared for Module 4!
1. Click Close to safely stop the Module Switcher

Please Note that you cannot 'go back' and take Modules prior to the one you are currently in unless you end the lab and start it over again (for example: If you Start with Module 4, you cannot use the Module Switcher to Start Labs 1, 2 or 3).

**Open Chrome Browser from Windows Quick Launch TaskBar**

1. Click on the **Chrome** Icon on the Windows Quick Launch Task Bar.

**Login to vSphere Client**

1. On the vSphere Client login screen, select "**Use Windows session authentication**"
Fault Domains

"Fault domain" is a term that comes up often in availability discussions. In IT, a fault domain usually refers to a group of servers, storage, and/or networking components that would be impacted collectively by an outage. A common example of this is a server rack. If a top-of-rack switch or the power distribution unit for a server rack would fail, it would take all the servers in that rack offline even though the server hardware is functioning properly. That server rack is considered a fault domain.

Each host in a vSAN cluster is an implicit fault domain. vSAN automatically distributes components of a vSAN object across fault domains in a cluster based on the Number of Failures to Tolerate rule in the assigned storage policy.

Fault Domains, cont.

Our screenshot shows a simple example of component distribution across hosts (fault domains). The two larger components are mirrored copies of the object and the smaller component represents the witness component.

When determining how many hosts or Fault Domains a cluster is comprised of, it is important to remember the following:

- For vSAN objects that will be protected with Mirroring, there must be $2n+1$ hosts or Fault Domains for the level of protection chosen.
  - Protecting from 1 Failure would require $(2x1+1)$ or 3 hosts
  - Protecting from 2 Failures would require $(2x2+1)$ or 5 hosts
  - Protecting from 3 Failures would require $(2x3+1)$ or 7 hosts

- For vSAN objects that will be protected with Erasure Coding, there must be $2n+2$ hosts or Fault Domains for the level of protection chosen.
  - RAID5 (3+1) requires $(2x1+2)$ or 4 hosts
  - RAID6 (4+2) requires $(2x2+2)$ or 6 hosts

Also consider that the loss of a Fault Domain, or hosts when Fault Domains are not configured, could result in no location to immediately rebuild to. VMware recommends having an additional host or Fault Domain to provide for the ability to rebuild in the event of a failure.
Using Fault Domains for Rack Isolation

Our screenshot shows a simple example of component distribution across hosts (fault domains). The two larger components are mirrored copies of the object and the smaller component represents the witness component.

When determining how many hosts or Fault Domains a cluster is comprised of, it is important to remember the following:

- For vSAN objects that will be protected with Mirroring, there must be $2n+1$ hosts or Fault Domains for the level of protection chosen.
  - Protecting from 1 Failure would require $(2 \times 1 + 1)$ or 3 hosts
  - Protecting from 2 Failures would require $(2 \times 2 + 1)$ or 5 hosts
  - Protecting from 3 Failures would require $(2 \times 3 + 1)$ or 7 hosts

- For vSAN objects that will be protected with Erasure Coding, there must be $2n+2$ hosts or Fault Domains for the level of protection chosen.
  - RAID5 $(3+1)$ requires $(2 \times 1 + 2)$ or 4 hosts
  - RAID6 $(4+2)$ requires $(2 \times 2 + 2)$ or 6 hosts

Also consider that the loss of a Fault Domain, or hosts when Fault Domains are not configured, could result in no location to immediately rebuild to. VMware recommends having an additional host or Fault Domain to provide for the ability to rebuild in the event of a failure.

Using Fault Domains for Rack Isolation, cont.

The failure of a disk or entire host can be tolerated in the previous discussion scenarios. However, this does not protect against the failure of larger fault domains such as an entire server rack. Consider our next example, which is a 12-node vSAN cluster. It is possible that multiple components that make up an object could reside in the same server rack. If there is a rack failure, the object would be offline.
To mitigate this risk, we can place the servers in a vSAN cluster across server racks and configure a fault domain for each rack in the vCenter\vSAN UI. This instructs vSAN to distribute components across server racks to eliminate the risk of a rack failure taking multiple objects offline. This feature is commonly referred to as "Rack Awareness". The screenshot shows component placement when three servers in each rack are configured as separate vSAN fault domains.

We do not have 12 vSphere Servers in our Lab but we can still show you how to configure Fault Domains using our 3 Hosts, next.
Configure Fault Domains

1. Select RegionA01-COMP01
2. Select Configure
3. Select Fault Domains
4. Click the Create a new fault domain... icon
New Fault Domain

1. Enter Name: **Rack 1**
2. Select **esx-01a.corp.local**
3. Click **OK**

New Fault Domain, cont.

1. Note that our **Rack 1** Fault Domain has been created containing **esx-01a.corp.local**
2. Click the **Create a new fault domain...** icon
New Fault Domain, cont.

1. Enter Name: **Rack 2**
2. Select **esx-02a.corp.local**
3. Click **OK**

*(Not Shown)* Repeat these steps to create your third Fault Domain:

1. Enter Name: **Rack 3**
2. Select **esx-03a.corp.local**
3. Click **OK**
New Fault Domain, cont.

We now have the minimum required amount of Racks (3) populated with vSphere Hosts. vSAN will ensure that components are distributed among the Racks so that desired Failures to Tolerate can be achieved in the event of a Single Rack Failure.

Next, we will examine different failure scenarios and also provide recommendations for how to alleviate and/or mitigate.

What happens if a storage device fails in a vSAN host?

Virtual Machines are protected by storage policies that include failure tolerance. For example, a storage policy with a Primary Level of Failures to Tolerate (PFTT) rule set to one with RAID-1 mirroring will create two copies of an object with each copy on a separate host. This means the VMs with this policy assigned can withstand the failure of a disk or an entire host without data loss.

When a device is degraded and error codes are sensed by vSAN, all of the vSAN components on the affected drive are marked degraded and the rebuilding process starts immediately to restore redundancy. If the device fails without warning (no error codes received from the device), vSAN will wait for 60 minutes by default and then rebuild the affected data on other disks in the cluster. The 60-minute timer is in place to avoid unnecessary movement of large amounts of data. As an example, a disk is inadvertently pulled from the server chassis and reseated approximately 10 minutes later. It would be inefficient and resource intensive to begin rebuilding several gigabytes of data when the disk is offline briefly.

When failure of a device is anticipated due to multiple sustained periods of high latency, vSAN evaluates the data on the device. If there are replicas of the data on other devices in the cluster, vSAN will mark these components as absent. Absent components are not rebuilt immediately as it is possible the cause of the issue is temporary. vSAN waits for
60 minutes by default before starting the rebuilding process. This does not affect the availability of a VM as the data is still accessible using one or more other replicas in the cluster. If the only replica of data is located on a suspect device, vSAN will immediately start the evacuation of this data to other healthy storage devices.

**Note**: The failure of a cache tier device will cause the entire disk group to go offline. Another similar scenario is a cluster with deduplication and compression enabled. The failure of any disk (cache or capacity) will cause the entire disk group to go offline due to the way deduplicated data is distributed across disks.

**Recommendation**: Consider the number and size of disk groups in your cluster with deduplication and compression enabled. While larger disk groups might improve deduplication efficiency, this also increases the impact to the cluster when a disk fails. Requirements for each organization are different so there is no set rule for disk group sizing.

**What happens if a host fails in a vSAN cluster?**

vSAN will wait for 60 minutes by default and then rebuild the affected data on other hosts in the cluster. The 60-minute timer is in place to avoid unnecessary movement of large amounts of data. As an example, a reboot takes the host offline for approximately 10 minutes. It would be inefficient and resource intensive to begin rebuilding several gigabytes or terabytes of data when the host is offline briefly.

vSphere HA is tightly integrated with vSAN. The VMs that were running on a failed host are rebooted on other healthy hosts in the cluster in a matter of minutes.

**Recommendation**: Enable vSphere HA for a vSAN cluster.

**How does vSAN handle a network partition?**

vSAN uses a quorum voting algorithm to help protect against split-brain scenarios and ensure data integrity. An object is available for reads and writes as long as greater than 50% of its components are accessible.

As an example, a VM has a virtual disk with a data component on Host1, a second mirrored data component on Host2, and a witness component on Host3. Host1 is isolated from Host2 and Host3. Host2 and Host3 are still connected over the network. Since Host2 and Host3 have greater than 50% of the components (a data component and a witness component), the VMs virtual disk is accessible.

However, if all three hosts in our example above are isolated from each other, none of the hosts have access to greater than 50% of the components. vSAN makes the object inaccessible until the hosts are able to communicate over the network. This helps ensure data integrity.
**Recommendation**: Build your vSAN network with the same level of resiliency as any other storage fabric.

**How is vSAN impacted if vCenter Server is offline?**

When vCenter Server is offline, vSAN continues to function normally. VMs continue to run and application availability is not impacted. Management features such as changing a storage policy, monitoring performance, and adding a disk group are not available.

vSAN has a highly available control plane for health checks using the VMware Host Client even if vCenter Server is offline. Hosts in a vSAN cluster cooperate in a distributed fashion to check the health of the entire cluster. Any host in the cluster can be used to view vSAN Health. This provides redundancy for the vSAN Health data to help ensure administrators always have this information available.
Active/Active vSAN Stretched Clusters

Before delving into the installation of a vSAN Stretched Cluster, there are a number of important features to highlight that are specific to stretch cluster environments.

Launch vSphere Client

If not already open from a prior Lab Module, launch the vSphere Web Client using the Google Chrome icon in the Windows Taskbar.

1. Select the "Use Windows session authentication" checkbox
2. Click Login
Witness Host must not be part of the vSAN Cluster

When configuring your vSAN stretched cluster, only data hosts must be in the cluster object in vCenter.

1. The vSAN Witness Host must remain outside of the cluster, and must not be added to the cluster at any point. In your lab environment, we have already deployed the vSAN Witness host.

Thus for a 1 (host) +1 (host) +1 (witness) configuration, there is one ESXi host at each site and one ESXi witness host.
Networking

The vSAN Witness Appliance contains two network adapters that are connected to separate vSphere Standard Switches (VSS).

The vSAN Witness Appliance Management VMkernel is attached to one VSS, and the WitnessPG is attached to the other VSS. The Management VMkernel (vmk0) is used to communicate with the vCenter Server for appliance management. The WitnessPG VMkernel interface (vmk1) is used to communicate with the vSAN Network. This is the recommended configuration. These network adapters can be connected to different, or the same, networks, provided they have connectivity to their appropriate services.

The Management VMkernel interface could be tagged to include vSAN Network traffic as well as Management traffic. In this case, vmk0 would require connectivity to both vCenter Server and the vSAN Network. In many nested ESXi environments (such as the platform VMware uses for this Hands On Lab), there is a recommendation to enable promiscuous mode to allow all Ethernet frames to pass to all VMs that are attached to the port group, even if it is not intended for that particular VM. The reason promiscuous mode is enabled in many nested environments is to prevent a virtual switch from dropping packets for (nested) vmnics that it does not know about on nested ESXi hosts.

The Witness has a portgroup pre-defined called witnessPg. Here the VMkernel port to be used for vSAN traffic is visible. If there is no DHCP server on the vSAN network (which is likely), then the VMkernel adapter will not have a valid IP address.

1. Select the ESXi host called esx-08a.corp.local
2. Select Configure
3. Select Networking -> VMkernel adapters
4. Select vmk1 to view the properties of the witnessPg.
5. Validate that "vSAN" is an enabled service as depicted in the screenshot.

Creating a New vSAN - 2 Node Stretched Cluster

Creating a vSAN stretched cluster from a group of hosts that doesn’t already have vSAN configured is relatively simple. A new vSAN cluster wizard makes the process very easy.

In this lesson we will steps you through each of these steps.

- Creating a vSphere Cluster
- Adding ESXi hosts to the vSphere Cluster
- Prepare the ESXi hosts for Witness Traffic Seperation (WTS)
- Forming the 2 Node vSAN Cluster

Create a new vSphere Cluster

The first step is to create a vSphere Cluster for the 2 ESXi hosts that we will use to form the 2 Node vSAN Stretched Cluster.

1. Right click the Datacenter called RegionA01
2. Select New Cluster ...
Create vSphere Cluster

1. Give the vSphere Cluster a name:

2-Node-Stretched-Cluster

Click OK

Move Hosts into Cluster

Once we have the vSphere Cluster created, move the 2 ESXi hosts called esx-05a.corp.local and esx-06a.corp.local into the vSphere Cluster.
This can be achieved in either of 2 ways:

Drag the ESXi host and drop it on top of the vSphere cluster called 2-Node-Stretched-Cluster

or

Right click the ESXi host and select Move To..., select the vSphere cluster called 2-Node-Stretched-Cluster and click OK

**Take Hosts out of Maintenance Mode**

Take the ESXi hosts esx-05a.corp.local and esx-06a.corp.local out of Maintenance Mode.

1. Right click the ESXi host **esx-05a.corp.local**
2. Select **Maintenance Mode**
3. Select **Exit Maintenance Mode**

Repeat these steps for the other ESXi host **esx-06a.corp.local**
Verify vSphere Environment

Verify that your **2-Node-Stretched-Cluster** looks like the screenshot before we continue.

Verify that you have a vSphere Cluster containing 2 ESXi host and that they are not in Maintenance Mode.

Verify Networking

Verify that each of the ESXi hosts have a VMkernel port for vSAN and the vSAN traffic service is enabled.
1. Select ESXi host called **esx-05a.corp.local**
2. Select **Configure**
3. Select **Networking -> VMkernel Adapters**
4. Select **vmk3 (vSAN enabled port-group)**
5. Verify that the **vSAN service** is enabled on the port-group.

### Verify Storage

Verify that each of the ESXi hosts have a Storage devices available to create the vSAN Disk Groups and enable the creation of a vSAN Datastore.

As shown in the screenshot, we will use the 1 x 5 GB disks for the cache tier and the 2 x 10 GB disks for the Capacity tier when creating the vSAN Disk Groups.

1. Select ESXi host called **esx-05a.corp.local**
2. Select **Configure**
3. Select **Storage -> Storage Devices**
VMware vSAN 6.5 and later supports the ability to directly connect two vSAN data nodes using one or more crossover cables. This is accomplished by tagging an alternate VMkernel port with a traffic type of “Witness”. The data and metadata communication paths can now be separated. Metadata traffic destined for the Witness vSAN VMkernel interface, can be done through an alternate VMkernel port. It is called “Witness Traffic Separation” (or WTS).

With the ability to directly connect the vSAN data network across hosts, and send witness traffic down an alternate route, there is no requirement for a high speed switch for the data network in this design.

This lowers the total cost of infrastructure to deploy 2 Node vSAN. This can be a significant cost savings when deploying vSAN 2 Node at scale.

**Preparing your ESXi hosts for Witness Traffic Separation (WTS)**

To prepare the ESXi hosts for the 2 Node vSAN Stretched Cluster, open a Putty session to the following hosts.

You will find the PuTTY application on the taskbar of your Main Console.
Click on `esx-05a.corp.local` and click the load button and click **Open**

Click on `esx-06a.corp.local` and click the load button and click **Open**

**Preparing your ESXi hosts for Witness Traffic Separation (WTS)**

Let's first have a look at what traffic types are configured.

1. Run the following command on host `esx-05a.corp.local` and `esx-06a.corp.local`:

   ```
esxcli vsan network list
   ```

2. Here you will see that we have a **Traffic Type: vsan** configured on each host.
Preparing your ESXi hosts for Witness Traffic Separation (WTS)

To use ports for vSAN today, VMkernel ports must be tagged to have “vsan” traffic. This is easily done in the vSphere Web Client.

To tag a VMkernel interface for “Witness” traffic, today it has to be done at the command line.

To add a new interface with **Witness traffic** as the type, the command is:

```
esxcli vsan network ipv4 add -i vmk0 -T=witness
```

1. Run this command on both **esx-05a.corp.local** and **esx-06a.corp.local**

Note: Remember it is the Management Network that we are going to use for the Witness Traffic, which in our environment is vmk0
Preparing your ESXi hosts for Witness Traffic Separation (WTS)

Let's look at what traffic types are configured now.

1. Run the following command on host esx-05a.corp.local and esx-06a.corp.local:
   
   ```
   esxcli vsan network list
   ```

   Here you will see that we have a **Traffic Type : vsan** and **Traffic Type : witness** configured on each host.

Now that we have configured the Networking, let's create our 2 Node vSAN Stretched Cluster.
Create a 2 Node vSAN Cluster

The following steps should be followed to install a new vSAN stretched cluster. This example is a 1+1+1 deployment, meaning one ESXi hosts at the preferred site, one ESXi hosts at the secondary site and 1 witness host.

To setup vSAN and configure stretch cluster navigate to

1. The cluster called **2-Node-Stretched-Cluster**
2. Select **Configure**
3. Select **vSAN -> Services**
4. Click **Configure** to begin the vSAN wizard.

**Configure vSAN as a Stretched Cluster**
The initial wizard allows for choosing various options like disk claiming method, enabling Deduplication and Compression (All-Flash architectures only with Advanced or greater licensing), as well as configuring fault domains or stretched cluster.

1. Select **Two host vSAN cluster**

   Click **NEXT**

**Configure vSAN as a Stretched Cluster**

Leave the Services as default

Click **NEXT**
Configure vSAN as a Stretched Cluster

Disks will be selected for their appropriate role (cache and capacity) in the vSAN cluster.

As shown in the screenshot, the 5 GB disks from each of the ESXi hosts have been selected as the Cache tier, and the 10 GB disks have been selected for the Capacity tier.

Click **NEXT**
Configure vSAN as a Stretched Cluster

The Witness host detailed earlier must be selected to act as the witness to the two Fault Domains.

1. Expand the Datacenter RegionA01 and select esx-08a.corp.local

Click NEXT
Configure vSAN as a Stretched Cluster

Just like physical vSAN hosts, the witness needs a cache tier and a capacity tier.

Note: The witness does not actually require SSD backing and may reside on a traditional mechanical drive.

1. Select the **cache tier** disk
2. Select the **capacity tier** disk

Click **NEXT**
Ready to Complete

Review the vSAN Stretched Cluster configuration for accuracy.

Select **FINISH**.

Monitor Tasks

You can monitor the tasks in the Recent Tasks window.

You will see tasks for the Reconfigure vSAN cluster, Creating disk groups, Converting to Stretched Cluster and Adding disks to the Disk groups.
vSAN Cluster Created

Let's now verify that we have created the vSAN stretched cluster.

1. Select **2-Node-Stretched Cluster**
2. Select **Configure**
3. Select **vSAN > Services**

Disk Management

Let's now have a look at the Disk Groups that have been created.
1. Select **vSAN > Disk Management**

We can see that we have a disk group on the ESXi hosts called esx-05a.corp.local and esx-06a.corp.local. We also have a disk group on esx-08a.corp.local which is the vSAN witness host in our Stretched Cluster configuration.

**Fault Domains and Stretched Cluster**

![Image of Fault Domains and Stretched Cluster configuration]

Lets now have a look at the Fault Domains and Stretched Cluster configuration.

1. Select **vSAN > Fault Domains**
2. vSAN Stretched Cluster is enabled with the witness host **esx-08a.corp.local**.
3. We can also see the **2 Fault Domains** that have been created and their respective ESXi hosts.

**Conclusion**

This concludes the lesson on creating a vSAN 6.7 2 Node Stretched Cluster with witness traffic separation.

**Monitoring a vSAN Stretched Cluster**

One of the ways to monitor your vSAN environment is to use the vSAN Health Check.
The vSAN Health runs a comprehensive health check on your vSAN environment to verify that it is running correctly and will alert you if it finds some inconsistencies and options on how to fix these.

**vSAN Health Check**

Let's have a look at how the health check works and what we can report on.

1. Select **2-Node-Stretched-Cluster**
2. Select **Monitor**
3. Select **vSAN > Health**

Here you will see the high level list of the vSAN Health checks that can be performed.

4. Expand the **Stretched cluster** health checks
vSAN Health Check

Let's drill in deeper to the individual tests.

1. Select **Site latency health**
2. To the right of the screen, you will see the results of these tests.

Spend some time having a look at the other tests and the data that we return from the tests.

**Conclusion**

The vSAN health check is great help to get more deeper into the testing performance and health check of vSAN installations. The vSAN Health Check should be the first place you should go to monitor your vSAN environment.
It is good practice to rerun the vSAN Health Check so that you retrieve the current state of the environment.
Disaster Recovery with vSAN

vSAN can be successfully utilized for several different Disaster Recovery Scenarios such as the previously discussed 'Active/Active' Stretched Cluster configuration, an inexpensive Disaster Recovery target site (enabled through a feature like vSphere Replication) or a combination of both with automation via VMware Site Recovery Manager (SRM).

Outside of the scope of this Lab/Lesson, VMware also enables an add-on for VMware Cloud on AWS (VMC) called VMware Site Recovery (Disaster Recovery as a Service) that enables fast deployment of new DR initiatives or seamlessly extends existing on-premises VMware deployments to VMware Cloud on AWS, all by utilizing vSAN hyper-converged infrastructure.

vSAN as a Target DR Site

A popular Use Case for vSAN is leveraging lower cost Hyper Converged-Infrastructure as a DR target when using Traditional storage in your Primary site. Since both locations are running VMware vSphere Infrastructure, there are no Virtual Machine container configuration changes necessary between the two locations and vSphere Replication can be utilized as your replication engine to protect VM's from the Primary Site to a DR Cluster powered by vSAN.

Due to the flexibility of of Software Policy-Based Management policies, you can also choose to utilize less stringent Failures to Tolerate (FTT) policies at the DR site. This flexibility can dramatically reduce costs in protection of your critical systems, by consuming less capacity as one example.
vSAN and Disaster Recovery with vSphere Replication and SRM

Active-Active data centers using vSAN stretched clustering is ideal for situations where you need an Recovery Point Objective (RPO) of zero.

Since stretched clusters essentially utilize synchronous replication between the two locations, an RPO of zero is achieved. That means no loss of data if one of the locations in the stretched cluster is offline. vSphere HA automates the recovery of virtual machines affected by an outage at either location in the stretched cluster. Recovery time for these virtual machines is typically measured in minutes.

If there are additional data center needs such as failover to another remote site, vSAN can take advantage of the capabilities provided by vSphere Replication, and SRM to protect a site in addition to, or instead of a stretched cluster arrangement. All of these tools are software defined, and do not rely on any hardware specific functionality. These capabilities are key ingredients to creating an agile data center.
Conclusion

In this lesson we examined vSAN Availability characteristics and Fault Domains. We explored vSAN Stretched Clusters and looked at how to configure a 2-Node vSAN Stretched Cluster. As part of this process, we gave you some background and some important features to understand before you configure your stretched vSAN Cluster environment. We finished the Module by discussing vSAN Disaster Recovery options with vSAN.

You've finished Module 4

Congratulations on completing Module 4.

If you are looking for additional information on topic:

- vSAN Fault Domains
- vSAN Fault Domains FAQ
- vSAN Design and Sizing Guide (Fault Domains)
- vSAN Stretched Cluster & 2 Node Guide
- vSAN Disaster Recovery Solution Overview
- vSAN and SRM RPO and RTO
- VMware Site Recovery for AWS overview
- Go to VMware Storage Hub for all things related to vSAN.

Proceed to any remaining module below which interests you most.

- **Module 5 - vSAN Interoperability** (45 minutes) (Intermediate)

Module 5 illustrates utilizing vRealize Log Insight to review centralized vSAN Logs, vSAN iSCSI integration and vSAN CLI interfaces.

- **Module 6 - vSAN Encryption** (30 minutes) (Intermediate)

Module 6 discusses vSAN security parameters such as FIPS 104-2 Validation and vSAN Data-at-rest Encryption.

How to End the Lab
If you would like to end your lab click on the **END** button.
Module 5 - vSAN 6.7
Interoperability (45 Minutes)
Introduction

vSAN has deep interoperability with other existing VMware technologies as well as industry capabilities such as iSCSI integration and administration via Command Line Interfaces.
vRealize Network Log Insight with vSAN

VMware vRealize Log Insight is a log aggregation, management, and analytics solution that gives the data center administrator an easy way to see context, correlation, and meaning behind otherwise obfuscated log content. Log Insight can aggregate log data from a variety of sources, and is extensible to over 40 applications using its content pack framework. When used correctly, with the right tools, log data can provide context and understanding to changing conditions in the data center.

Log Insight paired with vSAN is an easy way to gain a level of visibility and operational intelligence not only to vSAN, but to your entire environment.

Lab Preparation

It is necessary to run the ModuleSwitcher for this Lab, please complete the following steps.

Module Switcher

Double-Click the Module Switcher Desktop Shortcut called **HOL-1908 HCI**

Module 5 Start
1. Click the **Module 5 - Start** button

This Startup Routine can take a few minutes to complete - thank you for your patience!

**Monitor Progress**

![Monitor Progress Image](image)

Monitor Progress until Complete.

- Press **Enter** to continue (and close the PowerCLI Window)

**Lab Prep Complete**

![Lab Prep Complete Image](image)

Your Lab has been successfully prepared for Module 5!

1. Click Close to safely stop the Module Switcher

Please Note that you cannot 'go back' and take Modules prior to the one you are currently in unless you end the lab and start it over again (for example: If you Start with Module 4, you cannot use the Module Switcher to Start Labs 1, 2 or 3).

**Open Chrome Browser from Windows Quick Launch TaskBar**

![Open Chrome Browser Image](image)
1. Click on the **Chrome** Icon on the Windows Quick Launch Task Bar.

**Login to vSphere Client**

![vSphere login screen]

1. On the vSphere Client login screen, select "**Use Windows session authentication**"
2. Click **Login**

**New Browser Tab**

![New Tab icon]

1. Click **New Tab** icon
1. Select **HOL Admin** via Bookmark Bar
2. Click **log-01a**

**Login**

1. Enter the following **User Name** and **Password** parameters (password is case sensitive)

   ```
   admin
   VMware1!
   ```
2. Click **LOGIN**
Interactive Analytics

1. Click **Interactive Analytics**
2. Type **vsan** (and notice that there are thousands of results associated with this keyword)

In addition to the out of box Dashboards we just reviewed, Log Insight allows for user to quickly search across multiple log files via the Interactive Analytics capability.

Let's search for a potential Configuration error on our vSAN Cluster and try to determine when this change might have been made.
vSAN Configuration Consistency

1. Type vsan configuration
2. Change drop-down to All time
3. Note that vCenter (vcsa-01a.corp.local) has forwarded a log entry indicating that 'vSAN extended configuration in sync' has gone into Red status.
4. We can also see that the event is graphically displayed in the top Chart.

Set Filter

1. Click the Filter Widget for the event containing 'Gray to Red' (or 'Green to Red', either will work)
2. Select Events Like This to filter only on these events (not shown)

Create Alert

1. Click the Create Alert from Query... icon
New Alert

1. Note that we can provide a **Name** for our Alert as well as an optional **Description** and **Recommendation** steps
2. Note that we can send Alerts via **Email** or **Webhook**
3. Note that we can specify additional logic for how to handle the **Alert**
4. (It is also possible to configure Alerts that are sent to vRealize Operations for further action)
5. Click **Cancel**

Finally, Let's examine this Configuration inconsistency in vCenter and correct the condition before moving on to examine the built-in vSAN Dashboards that are present in Log Insight.
1. Select **RegionA01-COMP01**
2. Select **Monitor**
3. Select **vSAN\Health**
4. Select Cluster\**Advanced vSAN Configuration in sync** alert
5. Note that one of our Hosts has a different timeout value set for **VSAN.ComRepairDelay** (90 minutes vs. 60).
6. Click **esx-01a.corp.local**

The vSAN **ComRepairDelay** advanced setting specifies the amount of time vSAN waits before rebuilding a disk object after a host is either in a failed state or in Maintenance Mode. By default, the repair delay value is set to 60 minutes; this means that in the event of a host failure, vSAN waits 60 minutes before rebuilding any disk objects located on that particular host. This is because vSAN is not certain if the failure is transient or permanent. It's possible to increase modify this value (and also to forget to set it back or make sure that the setting is uniform across the cluster).
1. Scroll down to System
2. Select System | Advanced System Settings
3. Click EDIT...
1. Type `vsan.clomrepair`
2. Double-click `Value` and change to `60`
3. Click `OK`
vSAN Health

1. Select RegionA01-COMP01
2. Select Monitor
3. Select vSAN\Health
4. Click RETEST
5. Expand Cluster
6. Note that vSAN cluster configuration consistency now reports Healthy (green) status

Using Log Insight in this example helped us identify not only that there was a configuration inconsistency but also identified the exact date/time this change was made and furthermore enabled us to create an Email Alert if we so chose.

Next we will examine the built in vSAN Log Insight dashboards.
vSAN Dashboards

1. Click VMware - vSAN to expand vSAN Dashboards

Log Insight still uses the content pack framework from previous editions, but vSAN dashboards are now included at the time of installation, making it easy to deploy and use in a vSAN powered environment.

Out of the box, vRealize Log Insight provides the following:

- Ten, prebuilt vSAN dashboards that disseminate key log data entries. Intimate knowledge of log syntax not required.
- Captures and intelligently disseminates all vSAN urgent traces.
- User friendly drill-down filtering abilities all within the UI.
- Exposes back-end vSAN activity to better understand historical conditions and non-error related activities.
- Dashboard widgets with predefined filters to discern various host and object states.
- Dashboards can be cloned, and are fully customizable, allowing as a good stepping stone for additional customization.

Let's examine the vSAN Dashboards next. Don't be alarmed if you see plenty of 'no results' in the widgets, we just recently formed our vSAN Datastore after all!

In general, do not be overly concerned if you do not see much activity in vSAN related widgets. Often times Log Insight may not always show a lot of information in the
dashboards. This is quite common for environments that do not have much activity on them, have fully operational hardware, or do not consume much capacity. Lack of data in Log Insight is not a bad thing, and will likely report more events once there is more activity in the environment as capacity and workload increases.

**Host State Information**

![Dashboard Screenshot]

1. Click **Host State Information**
2. Scroll-down to view more **Widgets**

The Host state information dashboard is a good overview of how vSAN treats host membership and roles. Its primary focus will be around activities of the host itself, such as additions or changes in host membership to a vSAN cluster.

Optional (Read for Additional Details or click '>' to proceed to next Lab Manual page):

This dashboard consists of seven widgets, and will capture log entries for hosts entering and exiting maintenance mode, vSAN host discovery events. It will also capture when hosts rejoin a cluster, and role initialization. This dashboard is most helpful in understanding if a vSAN host is being recognized correctly.
Diskgroup Failures

1. Click **Diskgroup Failures**
2. Scroll-down to view more **Widgets**

The disk group failures dashboard is a collection of widgets that look a disk group activity. Disk groups are an important construct of vSAN, and this dashboard gives visibility to disk group failure events that are logged by vCenter, but not readily visible.

Optional (Read for Additional Details or click '>' to proceed to next Lab Manual page):

All seven widgets in this dashboard will report any event activity associated with the one or more disk groups of each host in a vSAN cluster. Note the "Component creation failure" widgets near the bottom. These can be extremely helpful in understanding why an object isn't able to meet a specific policy compliance due to insufficient capacity remaining, or exceeding the component maximum for the host.
1. Click **Networking**

The networking dashboard filters log events display vSAN network creation events in a cluster. It is common to see events in this dashboard when hosts are coming online, or vSAN is being enabled on the hosts across a cluster. These are not errors, but simply confirmation that vSAN is now using a specific VMkernel NIC on a specific host for vSAN traffic.

Optional (Read for Additional Details or click '>' to proceed to next Lab Manual page):

The networking dashboard contains two widgets, but can work nicely in conjunction with the "Host State Information" dashboard, or perhaps other network related dashboards found in the content pack for vSphere. East-west host connectivity is critically important to the operation of vSAN, and using this dashboard with other dashboards found in the vSAN and vSphere content packs will provide the visibility needed to understand if there are any issues with east-west connectivity.
Congestion

1. Click Congestion
2. Scroll-down to view more Widgets

The Congestion dashboard aims to provide better visibility of events generated from congestions. Congestions is a unique measurement introduced to vSAN. It's how vSAN measures pressure throughout the stack, and use these measurements to introduce flow control to smooth out this traffic so that VMs have enough resources for guest VM storage needs.

Optional (Read for Additional Details or click '>' to proceed to next Lab Manual page):

This dashboard has five widgets that capture congestion related log events. This dashboard can be most helpful when viewed in conjunction with the congestion metrics provided in the vSAN performance service. The value of the congestions metrics is not for meaningful interpretation of an absolute value, but identifying a change over the course of time. Capturing log events related to congestions can provide more context behind any spikes or other statistical outliers found in the vSAN performance service.
Object Configurations

1. Click **Object Configurations**
2. Scroll-down to view more **Widgets**

The object configurations dashboard takes a high-level view of activities of objects. This will generally report activities when vSAN is seeing that an object isn’t meeting compliance with its assigned storage policy, or perhaps some other activity such as assigning a policy to a new or existing VM. This dashboard, in combination with object events dashboard are often the two most useful dashboards in the content pack for vSAN.

Optional (Read for Additional Details or click '>' to proceed to next Lab Manual page):

The seven widgets in this dashboard capture events such as create (placement), change, and repair configurations, as well as rebalance, decommissioning, cleanup and vote rebalance configurations. As with many other widgets found across dashboards in the vSAN content pack, log events such as object configuration changes are not necessarily an alert to something not operating as expected. These log events help capture log entries in a manner that can provide context to some other operational activity.
Decommissioning

The decommissioning dashboard focuses primarily on hosts that are entering maintenance mode. Entering maintenance mode may be for planned maintenance activities, or in preparation for host or disk group decommissioning. Event activities will be captured for all of these conditions.

Optional (Read for Additional Details or click '>' to proceed to next Lab Manual page):

The six widgets in this dashboard can often be helpful in rolling upgrades across one or more vSAN clusters, as you can see the order in which hosts went through an upgrade process. A "disk decommissioning failed" widget can assist in situations where disks are unable to be decommissioned from a disk group, or entire disk groups are unable to be decommissioned successfully.

1. Click **Decommissioning**
2. Scroll-down to view more **Widgets**
Configuration Failures

1. Click Configuration Failures
2. Scroll-down to view more Widgets

The configuration failures dashboard presents widgets that are focused on attempting to configure and object based on a certain policy. If the environment cannot accept a particular performance or protection level for a VM based on the environmental conditions, such as cluster size, and disk layout, vSAN prevent that policy from being applied, and will generate an event. These types of events will show up in the configuration failures dashboard.

Optional (Read for Additional Details or click '>' to proceed to next Lab Manual page):

The six widgets in this dashboard target specific failure events in configuration changes. These are most commonly due to policy changes attempting to be made to a VM, but the cluster does not have the required conditions for support. For example, errors of "Insufficient fault domains" could be a result of attempting to change a VM's primary level of failures to tolerate (FTT) of 3 while having less than the required minimum level of hosts (7) to support FTT=3 when using a failure tolerance method (FTM) of RAID-1 mirroring.
**Operation Failures**

1. Click **Operation Failures**
2. Scroll-down to view more **Widgets**

The Operation Failures dashboard shown is a failures based dashboard that targets vSAN related operations, and if they did not end in success. The types of failure events captured here focus on the creation and configuration for objects and components. It will also touch on some levels of congestion, and resync operations.

Optional (Read for Additional Details or click '>' to proceed to next Lab Manual page):

The Operations Failures dashboard consists of five widgets. Two of the widgets capture activities around resync start events, and ingress congestion. These are included in this dashboard, as often these types of events will be related to each other. For example, object component creation failure events, which is monitored in this dashboard may be the result of network connectivity or partitioning issues. Therefore, having resync operation start events in the same dashboard can offer additional insight into possible causes.

**Health**
1. Click **Health**

The Health dashboard gives a good overview of health status changes for object components, capacity devices, and cache tier devices. In particular, the disk health changes may be correlated to degraded device handling events as seen in the vSAN UI in vCenter.

Optional (Read for Additional Details or click '>' to proceed to next Lab Manual page):

This three-widget dashboard is an effective way to determine if is a historical issue with a device that over the course of time, was not noticeable in the vCenter UI. Permanent Device Loss (PDL) events can be the result of failed devices, or a supporting device such as a storage controller. Occasionally, the disk health change widget may report component "absent" messages which may be part of other operations.

**Object Events**

1. Click **Object Events**
2. Scroll-down to view more **Widgets**

The Object Events dashboard shown reports component state changes. This dashboard provides an easy way to track when a component that has gone into an undesired state (degraded, absent, stale) and seeing potential related activities over a period of time.

This Concludes our vRealize Log Insight Lesson.

Optional (Read for Additional Details or click '>' to proceed to next Lab Manual page):

This dashboard consists of five widgets, and may be the most useful dashboard integrated into the vSAN content pack. The state changes provide context to a series of events that otherwise may go unnoticed. For instance, this dashboard will immediately report what objects lost "liveness." This will also be reflected in the object component states of degraded, absent, or stale. Subsequent resyncing events are
captured in the "Object component state - Resyncing" widget at a time based on the type of failure that occurred. Component resyncing can begin immediately if vSAN receives a sense code that places that device in a degraded state, or resyncing can begin 60 minutes after a period in which an object component went absent.
vSAN ISCSI Integration

With vSAN 6.7, support has been added for Windows Server Failover Clustering (WSFC) when using iSCSI targets on the vSAN datastore. Support for this feature includes Virtual Machine workloads, which previously were not supported when connecting to the vSAN iSCSI target.

In this lab, we will guide you through setting up the iSCSI service, creating an iSCSI target with LUNs that will be used by a pair of Microsoft servers that have been clustered.

We will also do some basic configuration within the Windows servers so you get an understanding of the basic requirements for WSFC.

Typically, Windows Server Failover Clustering requires multiple LUNs, for quorum and data disks. In this lab task we will create an iSCSI target for use with our Windows cluster and configure 2 LUNs on the target.

Enable the vSAN iSCSI service

To enable vSAN iSCSI services, we first need to enable the service

1. Select the cluster called RegionA01-COMP01 in the inventory pane.
2. Select the Configure tab.
3. Click on vSAN > Services.
4. Click on EDIT.
Enable the vSAN iSCSI service

1. Enable the vSAN iSCSI target service

Leave the rest of the options at their default value.

The Storage policy that we will use for the home object will be the **vSAN Default Storage Policy**

Click **APPLY**
Verify the vSAN iSCSI service

1. Expand the vSAN iSCSI Target Service

Verify that the setting are correct and we have a compliant status and the Home object health is Healthy.
Add an iSCSI Target

Once the iSCSI Target service has been enabled, we will now create the iSCSI Targets

1. Select **vSAN > iSCSI Target Service**
2. Select **iSCSI Targets**
3. Click **Add**
Add an iSCSI Target

1. Provide an alias that identifies this target and its usage. Enter **WSFC Target**. The IQN will be automatically generated by ESXi when you finish the wizard.

Click **OK**.

**Verify the iSCSI Target was created**
Verify that the iSCSI target was created.

1. Note that the iSCSI Target IQN was automatically created for you.

Now that we have the iSCI Target created, let's create some iSCSI LUNs.

2. In the vSAN iSCSI LUNS panel, Click Add

**Create first iSCSI Luns**

![Add LUN To Target](image)

Enter the following values to create the first vSAN iSCSI LUN:

- **ID**: 10
- **Alias**: LUN-10
- **Storage Policy**: vSAN Default Storage Policy
- **Size**: 5 GB

Click ADD

**Create Second iSCSI LUN**

In the vSAN iSCSI LUNS panel, Click Add

Enter the following values to create the second vSAN iSCSI LUN:

- **ID**: 11
- **Alias**: LUN-11
- **Storage Policy**: vSAN Default Storage Policy
- **Size**: 5 GB

Click ADD
Verify iSCSI LUN creation

Verify that the iSCSI LUNS have been created and they are Healthy and Compliant.
Create an Initiator Group

In this section, we will create an Initiator Group to limit access to our iSCSI target only to our Windows server.

1. Select **vSAN > iSCSI Target Service**
2. Select **INITIATOR GROUPS**
3. Click **Add**
Create an Initiator Group

1. Enter the value `WSFC_Cluster` in the Group Name field. (Note that spaces are not allowed)

We will add the Member Initiators to the group later.

Click **Create**.

Verify Initiator Group creation
Verify that the vSAN iSCSI Initiator Group has been created.

**Add the Initiator Group to the iSCSI Target**

1. Select the **iSCSI TARGETS** tab.
2. Click the **Add** link in the **Allowed Initiators** panel.

**Add the Initiator Group to the iSCSI Target**

1. Select the **Initiator Group** radio button
2. Select the **WSFC_Cluster** group.
Click Create

Add the Initiator Group to the iSCSI Target

In preparation for the next task, we need to take a note of the target IQN.

1. Highlight the IQN name for the WSFC Target as shown, right-click and select Copy. Paste the IQN into Notepad or Notepad++ for later use.

2. Also, note that the target has an assigned I/O Owner Host. Take note of the current owner host in your environment (it may differ from the one shown).

Configure the Windows Servers to access the iSCSI Target

Open the 'Remote Desktop Manager' application to the WSFC-01a Server
Configure the Windows Servers to access the iSCSI Target

You will be automatically logged into the Windows Host.

On the windows task bar open **Server Manager**.

Configure the Windows Servers to access the iSCSI Target

1. Click **Tools**.

There are three services that need to be enabled to allow for WSFC support as highlighted in the graphic - Failover Cluster Manager, iSCSI Initiator and MPIO.
By default, only the iSCSI Initiator service is installed by default on Windows servers. The other services are added using the 'Add roles and features' wizard. For our lab, we have preinstalled these services.

2. Click **Tools > MPIO**.

**Configure MPIO on the Windows Servers**

![MPIO Properties dialog box](image)

We have already configured MPIO in this Lab environment.

1. In the MPIO Properties dialog box, select the **Discover Multi-Paths** tab. Verify that **Add support for iSCSI devices is enabled.**
Configure the Windows iSCSI Initiator to connection the vSAN iSCSI Target

Click **Tools > iSCSI Initiator.**

1. In the iSCSI Initiator Properties dialog box, select the **Discovery** tab.
2. Click **Discover Portal** to add a target IP address.
Configure the Windows iSCSI Initiator to connection the vSAN iSCSI Target

Add the IP address of the VMkernel port configured for iSCSI (vmk3 in our case) for host esx-01a. Keep the default value (3260) for the Port.

Repeat this step and add entries for each ESXi Host vmk3 IP Address

```
esx-01a 192.168.130.51
esx-02a 192.168.130.52
esx-03a 192.168.130.53
esx-04a 192.168.130.54
```
Configure the Windows iSCSI Initiator to connection the vSAN iSCSI Target

1. Select the **Targets** tab.
2. You should see that the vSAN iSCSI Target IQN appears in the list of Discovered Targets.
3. You can cross-check the IQN with the value you copied into your Notepad. Its status should show as **Inactive**.
4. Highlight the vSAN iSCSI Target IQN and click **Connect**
Configure the Windows iSCSI Initiator to connection the vSAN iSCSI Target

1. In the **Connect To Target** dialog box, select the **Enable Multi-path** option.
2. Click **OK**

You will get an Authorization Failure message. Click OK and leave the iSCSI Initiator Properties dialog box open.

Configure the Windows iSCSI Initiator to connection the vSAN iSCSI Target

Return back to the vSphere Client.

1. Select the Cluster called **RegionA01-COMP01**
2. Select the **Configure** tab.
3. Select **vSAN > iSCSI Target Service**.
4. Select the **Initiator Groups** tab.
5. Click the **Add** link in the Initiators panel.

Configure the Windows iSCSI Initiator to connection the vSAN iSCSI Target

![Add Initiators](image)

Enter the following IQN's in the **Member initiator name** field and click **Add**.


Click **FINISH**
Verify the Initiators have been added

Verify that the 2 Initiators have been added.
Configure the Windows iSCSI Initiator to connection the vSAN iSCSI Target

The iSCSI Initiator Properties dialog should still be open. If not, open it.

In the Targets tab, select the **vSAN Target IQN** and click the **Connect**.

In the **Connect To Target** dialog box, ensure that you select **Enable multi-path**.

Click **OK**

**Configure the other Windows Server**

In the next few steps we will configure the other Windows Server.
Configure the Windows Servers to access the iSCSI Target

Open the 'Remote Desktop Manager' application to the **WSFC-02a** Server

Configure the Windows Servers to access the iSCSI Target

You will be automatically logged into the Windows Host.

On the windows task bar open **Server Manager**
Configure the Windows Servers to access the iSCSI Target

1. Click **Tools**.

There are three services that need to be enabled to allow for WSFC support as highlighted in the graphic - Failover Cluster Manager, iSCSI Initiator and MPIO.

By default, only the iSCSI Initiator service is installed by default on Windows servers. The other services are added using the 'Add roles and features' wizard. For our lab, we have preinstalled these services.

2. Click **Tools > MPIO**.
Configure MPIO on the Windows Servers

We have already configured MPIO in this Lab environment.

1. In the MPIO Properties dialog box, select the Discover Multi-Paths tab. Verify that Add support for iSCSI devices is enabled.
Configure the Windows iSCSI Initiator to connection the vSAN iSCSI Target

Click **Tools > iSCSI Initiator.**

1. In the iSCSI Initiator Properties dialog box, select the **Discovery** tab.
2. Click **Discover Portal** to add a target IP address.
Configure the Windows iSCSI Initiator to connection the vSAN iSCSI Target

Add the IP address of the VMkernel port configured for iSCSI (vmk3 in our case) for host esx-01a. Keep the default value (3260) for the Port.

Repeat this step and add entries for each ESXI host: Host vmk3 IP Address

<table>
<thead>
<tr>
<th>Host</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>esx-01a</td>
<td>192.168.130.51</td>
</tr>
<tr>
<td>esx-02a</td>
<td>192.168.130.52</td>
</tr>
<tr>
<td>esx-03a</td>
<td>192.168.130.53</td>
</tr>
<tr>
<td>esx-04a</td>
<td>192.168.130.54</td>
</tr>
</tbody>
</table>
Configure the Windows iSCSI Initiator to connection the vSAN iSCSI Target

1. Select the **Targets** tab.
2. You should see that the **vSAN iSCSI Target IQN** appears in the list of Discovered Targets.
3. You can cross-check the IQN with the value you copied into your Notepad. Its status should show as **Inactive**.
4. Highlight the vSAN iSCSI Target IQN and click **Connect**
Configure the Windows iSCSI Initiator to connection the vSAN iSCSI Target

1. In the Connect To Target dialog box, select the Enable Multi-path option.
2. Click OK

You will get an Authorization Failure message. Click OK and leave the iSCSI Initiator Properties dialog box open.

Configure the Windows iSCSI Initiator to connection the vSAN iSCSI Target

The iSCSI Initiator Properties dialog should still be open. If not, open it.
In the Targets tab, select the **vSAN Target IQN** and click the **Connect**.

In the **Connect To Target** dialog box, ensure that you select **Enable multi-path**.

Click **OK**

## Set up Windows Server Failover Cluster

If you have completed the previous task correctly, both your Windows servers should be able to access the iSCSI target and should have discovered two LUNs. Ensure that the vSAN iSCSI Target Initiator Group contains both Windows iSCSI Initiator IQNs.

If either of these statements is untrue, please review the previous task and do not proceed until you have resolved the issue.

We have chosen to include the Windows Server Failover Cluster configuration to familiarize you with the steps that are required to set this up from the Microsoft perspective. While you won't have to fix any issues on the Microsoft side, we feel it would be an advantage to have some understanding of the set up, in order to properly understand what happens on the vSphere side.
Format the Luns

Open an RDP connection to the **WSFC-01a server**, if you have not already done so.

Right-click the Start Menu icon and select **Disk Management**. You will see the 2 x 5 GB vSAN iSCSI luns that we have presented to this Windows Host.

Right-click on the two offline disks and click **Online**. (You will need to click in the grey area where the disk number is shown)
Format the Luns

1. Right-click in the grey area on the left on the first disk that shows 'Not Initialized' (it should be Disk 1) and select **Initialize Disk**. (Again click in the grey area to the left)
2. In the Initialize Disk dialog box, select **Disk 1** and **Disk 2**. Keep the **GPT** option selected.
3. Click **OK**.
Format the Luns

1. Right-click on the box reading 'Unallocated' for Disk 1 and click New Simple Volume...
2. Click Next, Next, Next. Change the Volume label value to Data. Complete the wizard by clicking Next and Finish.

Repeat the previous 2 steps for the second disk and assign a Volume label of Quorum.
Test the Cluster

1. Open the **Server Manager** via the Start menu.
2. Select **Tools**
3. Select **Failover Cluster Manager**.

Validate Cluster

1. Click **Validate Configuration**.
1. In the Failover Cluster Manager dialog box, select **Validate Configuration** in the **Management** panel.

Click **Next** on the **Before you begin** page

**Validate the Cluster**

![Validate a Configuration Wizard](image)

Enter the Fully Qualified Domain Names (FQDN) of the two Windows servers, one at a time, into the **Enter name** field and click **Add**.

```
wsfc-01a.corp.local
wsfc-02a.corp.local
```

Click **Next**
Validate the Cluster

1. Leave the Run all tests option selected and click Next.

Click Next to begin the tests

Validate the Cluster

Wait for the tests to complete
1. Click the View report button, which will open an HTML report file. All tests should complete with Success, with the exception of the 'Storage > Validate Microsoft MPIO-based disks' test. This fails as there is only one usable path. There are additional steps that need to be completed so that if that path fails, vSAN will assign a new I/O Owner Host and Windows will failover automatically to the newly available target.

2. Select **Create the cluster now using the validated nodes**

   Click **Finish**

**Create the Cluster**

In the next portion of the wizard, we are creating the Virtual IP that can be used to connect to the cluster. Any connections to the cluster will be via this IP/hostname, which allow a user to continue connecting even after a failover. A DNS entry for the cluster hostname and IP have already been created.

1. In the Cluster Name field, enter **wsfc-cluster**. (We do not need to enter the FQDN here as the wizard in only looking for the NetBIOS, or shortname, as the server is already joined to the domain)

2. In the Networks field, enter the following information (The two Windows servers already have statically assigned addresses of 192.168.110.101 / 192.168.130.101 and 192.168.110.102 / 192.168.130.102) This will serve as the Virtual IP of the cluster.

   192.168.110.0/24 : 192.168.110.103
   192.168.130.0/24 : 192.168.130.103

   Click **Next**
Create the Cluster

Review the details to create the cluster.

Click **Next**

Wait for the Cluster to be created

Create the Cluster
Revire the summary page. You can also View the report created by the wizard.

Click **Finish**

**Validate the cLuster**

1. In the left pane of the Failover Cluster Manager window, expand the `wsfc-cluster.corp.local` and then expand **Storage**.
2. Select **Disks**.
3. Note the Owner Node of the disks. This is the primary node of the cluster and is the server that will be connected to if a user connects to `wsfc-cluster.corp.local`.

Open the File Explorer on the Owner Node server and click **This PC**. You should see the C: drive and the CD-ROM drive, as well as the Data and Quorum drives for the cluster.

Perform the same operation on the other node and you should only see the C: and CD-ROM drives.

**Conclusion**

This completes the basic setup of a Windows Server Failover Cluster. Specific applications or services running on top of the WSFC would require additional steps, but
for the purposes of this lab, the current configuration will be sufficient to test and validate vSAN iSCSI configuration.
vSAN CLI Interfaces

ESXCLI Enhancements

VMware vSAN has several documented ESXCLI commands that can be used to explore & configure individual ESXi hosts.

In this lesson, we will provide some useful commands to use with vSAN. Feel free to follow along. Do note that if you run any commands outside the scope of this lesson, you could potentially have an adverse effect on the lab and may not be able to continue with any remaining modules or the remainder of this module. We will use some of these commands later in this module, too.

Launch PuTTY

Launch the PuTTY application from the Windows Taskbar.
Choose esx-01a.corp.local

1. Select the ESXi host called esx-01a.corp.local
2. Select Load
3. Select Open

ESXCLI vSAN Commands

```
[root@esx-01a -] esxcli vsan
Usage: esxcli vsan (cmd) [cmd options]
Available Namespaces:
  cluster            Commands for vSAN host cluster configuration
  datastore          Commands for vSAN datastore configuration
  debug              Commands for vSAN debugging
  health             Commands for vSAN Health
  iscsi              Commands for vSAN iSCSI target configuration
  network            Commands for vSAN host network configuration
  resync             Commands for vSAN resync configuration
  storage            Commands for vSAN physical storage configuration
  faultdomain        Commands for vSAN fault domain configuration
  maintenancemode    Commands for vSAN maintenance mode operation
  policy             Commands for vSAN storage policy configuration
  trace              Commands for vSAN trace configuration
```

```
By typing:

esxcli vsan

This will give you a list of all the possible esxcli commands related to vSAN, with a brief description for each.

**esxcli vsan cluster command**

1. To view details about the vSAN Cluster, like it's Health or whether it is a Master or Backup Node, you can type the following:

   esxcli vsan cluster get

Please note that the UUID typically used to reference the VSAN cluster is listed as the "Sub-Cluster UUID".

If you ever were to issue the corresponding "esxcli vsan cluster join" command you would furnish this value for the UUID.
To view networking details, you can execute this command:

```
esxcli vsan network list
```

Here we can see that the Network VmkNic is vmk3 and the Traffic Type on this VMKernel port is vsan.

By the way, if you run an esxcli vsan network list, multicast information will still be displayed even though it may not be used.
esxcli vsan storage command

To view the details on the physical storage devices on this host that are part of the vSAN Cluster, you can use this command:

```
esxcli vsan storage list
```

Please note that this command does NOT list the storage devices available in the ESXi host - it only reports those storage devices that have already been assigned to VSAN as part of VSAN Disk Group. If no disks are configured for vSAN on the ESXi host, then the output from this command will be blank.

We can tell a lot of information from this command.
1. Is the disk an SSD or spinning disk.
2. Is vSAN Dedupe and Compression enabled.
3. Is the disk used for Cache or Capacity.
4. What the On-disk format is.
5. Is vSAN Encryption enabled.

**esxcli vsan policy command**

To view the Policies in effect, such as how many failures the vSAN can tolerate, the command can be executed:

```
esxcli vsan policy getdefault
```

Notice that the policy may contain different capabilities for different vSAN object types - here this is reflected as specifying the additional capability of "forceProvisioning" exclusively for the vmswap object. This makes sense for vmswap object type since it is not a permanent attribute of the VM and will be recreated if the VM needs to migrate to another host in the cluster (vMotion, DRS, etc.)
esxcli vsan health command

The following two ESXCLI commands have been added to support vSAN Health Checks on an individual ESXi host:

- `vsan.health.cluster get`
- `vsan.health.cluster list`

1. To get a summary view of all vSAN Health Checks, you can run the following command:

```
esxcli vsan health cluster list
```

![Command Output](image.png)
esxcli vsan health command contd...

1. To check Host vSAN Health service installation

```bash
esxcli vsan health cluster get -t "ESXi vSAN Health service installation"
```

2. To check Hosts with no vSAN vmknic configured

```bash
esxcli vsan health cluster get -t "All hosts have a vSAN vmknic configured"
```
esxcli vsan cluster unicastagent command

The following new esxcli command will tell which hosts are using unicast (it does not list the host where the command is being run from however):

```
esxcli vsan cluster unicastagent list
```
PowerCLI vSAN Commands

PowerCLI Overview

VMware PowerCLI is a command-line and scripting tool built on Windows Powershell, and provides more than 500 cmdlets for managing and automating vSphere, vSAN, Site Recovery Manager, vRealize Operations Manager, vSphere Automation SDK, vCloud Director, vCloud Air, vSphere Update Manager and VMware Horizon environments.

In this lesson we will examine our Lab PowerCLI environment and perform a few vSphere Administrative Tasks.

Launch PowerCLI

PowerCLI has been pre-installed in the Lab.

1. Click the PowerShell Icon on the Windows taskbar
1. Type the following cmdlet name to retrieve our PowerCLI version information:

```
Get-PowerCLIVersion
```

2. You will notice that the get-powercliversion command is being deprecated, so let's run the **get-module** cmdlet.

```
Get-Module -ListAvailable -name VMware.PowerCLI
```

### Connect to vCenter

Type the following to connect to our Lab vCenter:

```
Connect-VIServer vcsa-01a.corp.local
```
The Connect-VIServer cmdlet can be used to connect and query across multiple vCenter instances.

**PowerCLI Cmdlets**

1. Retrieve available vCenter Datacenter(s):
   
   ```
   Get-Datacenter
   ```

2. Retrieve vCenter Cluster(s):
   
   ```
   Get-Cluster
   ```

We used the 'Connect-VIServer' cmdlet earlier. Cmdlets are small programs that are precompiled for your usage.

Let's use a few cmdlets to examine our vCenter environment by typing these commands (remember that you can use the Tab key to autocomplete if desired).

1. Retrieve available vCenter Datacenter(s):
   ```
   Get-Datacenter
   ```

2. Retrieve vCenter Cluster(s):
   ```
   Get-Cluster
   ```
3. Retrieve Virtual Machines:

Get-VM

4. Retrieve available vCenter Datastores:

Get-Datastore

**Cmdlets, cont.**

You can pipe commands together to create a pipeline.

A pipeline is a series of commands separated by the pipe operator |. Each command in the pipeline receives an object from the previous command, performs some operation on it, and then passes it to the next command in the pipeline. Objects are output from the pipeline as soon as they become available.

1. Type the following command to pipe the output of Get-VM to the Format-Table cmdlet and return only the Name and PowerState Columns:

```
Get-VM | Format-Table Name, PowerState
```

2. We can also pipe the result of Get-VM to the Where-Object cmdlet to filter on specific information (like Power state):
For the final step of this Lesson we will clone an existing VM using the New-VM cmdlet (this VM will be used in a later automation lesson on using Storage Policy Based Management).

1. Type the following command and monitor the clone progress (you can also simply highlight the entire command in your manual then drag and drop it into your PowerCLI window if you prefer):

   ```powershell
   ```

**PowerCLI vSAN Commands**

The previous version of PowerCLI had (6) vSAN specific cmdlets that could be utilized:

- Get-VsanDisk
- Get-VsanDiskGroup
- New-VsanDisk
- New-VsanDiskGroup
- Remove-VsanDisk
- Remove-VsanDiskGroup
### PowerCLI vSAN Commands

<table>
<thead>
<tr>
<th>Command Type</th>
<th>Name</th>
<th>Version</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cmdlet</td>
<td>Get-VsanClusterConfiguration</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-VsanDisk</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-VsanDiskGroup</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-VsanEvacuationPlan</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-VsanFaultDomain</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-VsanIscsiInitiatorGroup</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-VsanIscsiInitiatorGroupTargetAssociation</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-VsanIscsiLun</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-VsanIscsiTarget</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-VsanResyncingComponent</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-VsanRuntimeInfo</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-VsanSpaceUsage</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Get-VsanView</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>New-VsanDisk</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>New-VsanDiskGroup</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>New-VsanFaultDomain</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>New-VsanIscsiInitiatorGroup</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>New-VsanIscsiInitiatorGroupTargetAssociation</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>New-VsanIscsiLun</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>New-VsanIscsiTarget</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Remove-VsanDisk</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Remove-VsanDiskGroup</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Remove-VsanFaultDomain</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Remove-VsanIscsiInitiatorGroup</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Remove-VsanIscsiInitiatorGroupTargetAssociation</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Remove-VsanIscsiLun</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Remove-VsanIscsiTarget</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Repair-VsanObject</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Set-VsanClusterConfiguration</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Set-VsanFaultDomain</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Set-VsanIscsiInitiatorGroup</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Set-VsanIscsiLun</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Set-VsanIscsiTarget</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Start-VsanClusterDiskUpdate</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Start-VsanClusterRebalance</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Start-VsanEncryptionConfiguration</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Stop-VsanClusterRebalance</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Test-VsanClusterHealth</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Test-VsanNetworkPerformance</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Test-VsanStoragePerformance</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Test-VsanVMCreation</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
<tr>
<td>Cmdlet</td>
<td>Update-VsanHCLDatabase</td>
<td>10.1.0</td>
<td>VMware.VimAutomation.Storage</td>
</tr>
</tbody>
</table>

1. **Use** `Get-Command` **to view cmdlets containing 'vsan' in their name:**

Get-Command *vsan*
vSAN Configuration Information

1. To make things easier, let's create a Variable named $cluster and set it equal to the value of the Get-Cluster cmdlet:

```powershell
$cluster = Get-Cluster
```

2. Output the Variable contents:

```powershell
$cluster
```

3. Pass the $cluster variable to the new Get-VsanClusterConfiguration cmdlet:

```powershell
Get-VsanClusterConfiguration $cluster
```

Note that we can see a few high level properties of our vSAN Cluster (vSAN is enabled, Stretched Cluster is not, etc.)
Get-VsanClusterConfiguration

Let's see what additional information is available via this cmdlet.

1. Set a variable named `$vsanconfig` equal to the results of `Get-VsanClusterConfiguration` (you can up-arrow once then left-arrow over to insert the variable name):

   ```powershell
   $vsanConfig = Get-VsanClusterConfiguration $cluster
   ```

2. Pipe `$vsanConfig` into the `Get-Member` cmdlet to see all of the Methods and Properties that are available:

   ```powershell
   $vsanConfig | Get-Member
   ```
Get-VsanClusterConfiguration, cont.

You can directly view individual Properties by appending their name to your $vsanConfig variable.

1. For example, try one or more of these:

   - `$vsanConfig.HealthCheckEnabled`
   - `$vsanConfig.PerformanceServiceEnabled`
   - `$vsanConfig.VsanDiskClaimMode`

2. To view all of the Properties and their results you can simply pass the $vsanConfig variable to the Format-List cmdlet:
This test creates a very simple, tiny virtual machine on every ESXi host in the vSAN cluster.

If that creation succeeds, the virtual machine is deleted and it can be concluded that a lot of aspects of vSAN are fully operational (the management stack is operational on all hosts, the vSAN network is plumbed and is working, the creation, deletion and I/O to objects is working, etc.).

By performing this test, an administrator can reveal issues that the passive health checks may not be able to detect. By doing so systemically it is also very easy to isolate any particular faulty host and then take steps to remediate the underlying problem.

1. Create a $testVM variable and assign it to the result of our Test-VsanVMCreation cmdlet:

   ```powershell
   $testVM = Test-VsanVMCreation $cluster
   ```

2. Output the result of this test by typing the $testVM variable and pressing enter:

   ```powershell
   $testVM
   ```

Notice that the Test Results indicated, 'Passed'.
Test-VsanVMCreation, cont.

1. Examine the Properties that Test-VsanVMCreation is aware of by using the Get-Member cmdlet:

   ```powershell
   $testVM | Get-Member
   ```

2. Examine the HostResult property by appending this to your $testVM variable:

   ```powershell
   $testVM.HostResult
   ```

Notice that the Test Virtual Machine was successfully created on each vSphere Host.
Get-VsanSpaceUsage

Let's examine the Get-VsanSpaceUsage cmdlet in more detail.

1. Set a variable named $vsanUsage equal to the result of the Get-VsanSpaceUsage cmdlet:

```powershell
.vsanUsage = Get-VsanSpaceUsage
```

2. Output the result by typing the variable name:

```powershell
.vsanUsage
```

Note: The CapacityGB size may be different in your lab environment, depending on how many disks in each ESXi host that are consumed to create the vSAN Datastore.
Get-VsanSpaceUsage, cont.

Examine the Properties that are available to the Get-VsanSpaceUsage cmdlet:

```powershell
$vsanUsage | Get-Member
```

```vbnet
if ($vsanUsage.FreeSpaceGB -gt 50)
{ write-host -foregroundColor Yellow "You have plenty of disk remaining!" }
elseif ($vsanUsage.FreeSpaceGB -lt 50)
{ write-host -foregroundColor Yellow "Time to order more disk!"}
```

Enter this simple script to check the amount of disk free and respond accordingly.
Storage Policy Based Management

Storage Policy Based Management (SPBM) enables precise control of storage services. vSAN provides services such as availability level, striping for performance, and the ability to limit IOPS. Policies that contain one or more rules can be created using the vSphere Web Client and/or PowerCLI.

These policies are assigned to virtual machines and individual objects such as a virtual disk.

Storage policies can easily be changed and/or reassigned if application requirements change.

These changes are performed with no downtime and without the need to migrate (Storage vMotion) virtual machines from one location to another.
Virtual Machine Prep

Applying new Storage Policies could be very cumbersome if you had to apply them manually to individual Virtual Machines. In this section we will create a new Storage Policy and illustrate how easy it is to apply it to multiple Virtual Machines.

This new Storage Policy will set an IOPS Limit of 500 per VM -- this could be helpful if you wanted to prioritize certain VM's over others.

To prepare our Virtual Machines, please perform the following steps:

1. Create another VM in your environment

   ```powershell
   ```

2. Set a Variable named $vms equal to all Virtual Machines that start with the word 'PowerCLI', then confirm variable contents:

   ```powershell
   $vms = Get-VM -name PowerCLI*
   $vms
   ```

3. Power on each VM:

   ```powershell
   Start-VM $vms
   ```
Start-VM $vms

New-SpbmStoragePolicy

1. Create a new Storage Policy that sets an IOPS Limit of 500:

New-SpbmStoragePolicy -Name vSAN-IOPSlimit -RuleSet (New-SpbmRuleSet -Name "vSANIOPSlimit" -AllOfRules @((New-SpbmRule -Capability VSAN.iopslimit 500)))

2. View Storage Policies:

Get-SpbmStoragePolicy -requirement -namespace "VSAN" | Select Name, Description

Set-SpbmStoragePolicy

1. Apply the newly created Storage Policy to our multiple Virtual Machines:
foreach ( $vm in $vms ) { $vm, (Get-HardDisk -VM $vm) | Set-SpbmEntityConfiguration -StoragePolicy "vSAN-IOPSlimit" }

Note: This command may take a while to complete in our Lab environment. In the meantime, please feel free to continue on to our final section of this Lesson.

**Conclusion**

In this Module you have spent time learning about PowerCLI and how it can be used to monitor, manage and automate VMware vSAN.

We hope that this information has sparked ideas around how you can utilize PowerCLI in your own environments.

As you would expect, there is a wealth of additional information available to assist you in your PowerCLI with vSAN journey.
Conclusion

In this lesson we examined the benefits that vRealize Network Log Insight can provide in vSAN Environments. We also discussed vSAN 6.7 iSCSI enhancements and had you publish an iSCSi target via the vSAN Datastore. Lastly, for our power users out there, we illustrated various vSAN command line interfaces.

You've finished Module 5

Congratulations on completing Module 5.

If you are looking for additional information on topic:

- vRealize Operations and Log Insight in vSAN Environments
- vSAN 6.7 iSCSI Target Service
- Go to VMware Storage Hub for all things related to vSAN.

Proceed to the remaining module in this Hands On Lab.

- Module 6 - vSAN Encryption (30 minutes) (Intermediate)

Module 6 discusses vSAN security parameters such as FIPS 104-2 Validation and vSAN Data-at-rest Encryption.

How to End the Lab

If you would like to end your lab click on the END button.
Module 6 - vSAN 6.7
Security (30 Minutes)
Introduction

Business leaders need confidence that their data is well protected, but also need to keep their costs low. Traditionally, enterprises would need to purchase additional security, such as self-encrypting drives or third party security software. vSAN offers the industry’s first native software based, FIPS 140-2 validated Hyper-Converged Infrastructure (HCI) data-at-rest encryption. Built right into vSAN, vSAN encryption supports customers choice of standard drives (SSDs and HDDs), avoiding the limited options and pricing premium of self-encrypting drives (SEDs). Designed for compliance requirements, vSAN supports 2-factor authentication (SecurID and CAC), and offers the first DISA-approved STIG for HCI.
DISA STIG (FIPS 140-2) Validated

vSAN offered the first native HCI encryption solution for data-at-rest, and now with vSAN 6.7, vSAN Encryption is the first FIPS 140-2 validated software solution, meeting stringent US Federal Government requirements. vSAN Encryption delivers lower data protection costs and greater flexibility by being hardware agnostic and by offering simplified key management. This is also the first HCI solution with a DISA-approved STIG.

FIPS 140-2 Validation

vSAN takes an important step forward with improved security in vSphere 6.7, with FIPS 140-2 validation. Since vSAN is integrated into the hypervisor, it uses the kernel module used in vSphere, and as of vSphere 6.7, has achieved FIPS 140-2 validation. Organizations that require this level of validation can be confident that VMware vSphere, paired with VMware vSAN, will allow them to meet their security requirements.
vSAN Encryption

You can use data at rest encryption to protect data in your vSAN cluster.

vSAN can perform data at rest encryption. Data is encrypted after all other processing, such as deduplication, is performed. Data at rest encryption protects data on storage devices, in case a device removed from the cluster.

Using encryption on your vSAN cluster requires some preparation. After your environment is set up, you can enable encryption on your vSAN cluster.

vSAN encryption requires an external Key Management Server (KMS), the vCenter Server system, and your ESXi hosts. vCenter Server requests encryption keys from an external KMS. The KMS generates and stores the keys, and vCenter Server obtains the key IDs from the KMS and distributes them to the ESXi hosts.

vCenter Server does not store the KMS keys, but keeps a list of key IDs.

Lab Preparation

If you have completed the previous modules by completing the steps as outlined, then you can skip the next few steps to prepare your environment for this lesson.

Click here to go to the lesson.

If you have skipped to this module, we will use our Module Switcher PowerCLI Application to prepare the environment.

Module Switcher

Double-Click the Module Switcher Desktop Shortcut called HOL-1908 HCI
Module 6 Start

Click the **Module 6** Start button

Module 6 Progress

Monitor Progress until Complete.

- Press **Enter** to continue (and close the PowerCLI Window)

Lab Prep Complete

Your Lab has been successfully prepared for Module 6
Click Window Close to safely stop the Module Switcher

Please Note that you cannot 'go back' and take Modules prior to the one you are currently in unless you end the lab and start it over again

For example: If you Start Module 4, you cannot use the Module Switcher to Start Labs 1, 2 or 3).

Validate HyTrust KeyControl

![Image showing a browser with a security warning]

1. Open a New Chrome Browser Window or Tab and enter the following URL to connect to the HyTrust KeyControl interface:
2. Select **Advanced** (Not Shown)

3. Click **Proceed to 192.168.110.81 (unsafe)**

**Validate HyTrust KeyControl, cont.**

1. Use the following credentials to authenticate and click **Log In**

   - **User Name:** secroot
   - **Password:** VMware1!

**Change Password**

Password must be at least 8 characters long, including 1 digit, 1 uppercase character, 1 lowercase character, and 1 symbol.
Note: If you receive a System Recovery needed warning, please click [here](#) to resolve, otherwise:

1. Enter the following new password

   Password: !Password123

2. Click **Update Password**

**KMIP**

1. Select **KMIP**
2. Note that the State of the KMS is **Enabled**

We have confirmed the functional state of the HyTrust KeyControl KMS instance. Click [here](#) to begin enabling vSAN Encryption.
System Recovery Options

1. Open a New Chrome Tab and use the following URL to connect to the HyTrust KeyControl interface:

https://192.168.110.81

2. Use the following credentials to authenticate and click Log In

User Name: secroot
Password: VMware1!

Recover Admin Key

1. Click Browse
Open Dialog

1. Click Browse

Upload File

1. Click Upload File

Allow the process to complete (note that this may take a few minutes, thank you for your patience)!
Recovery Success

1. Click **Proceed**

HyTrust Login

1. Use the following credentials to authenticate and click **Log In**

User Name: **secroot**
Password: **VMware1!**
Change Password

Note: If you receive a System Recovery needed warning, please click [here](#) to resolve, otherwise:

1. Enter the following new password

   Password: !Password123

2. Click **Update Password**
1. Select **KMIP**
2. Note that the State of the KMS is **Enabled**

We have confirmed the functional state of the HyTrust KeyControl KMS instance and are now ready to configure vSAN Encryption.

### Configuring the Key Management Server

A Key Management Server (KMS) cluster provides the keys that you can use to encrypt the vSAN datastore.

Before you can encrypt the vSAN Datastore, you must set up a KMS cluster to support encryption. That task includes adding the KMS to vCenter Server and establishing trust with the KMS.
The vCenter Server provisions encryption keys from the KMS cluster.

The KMS must support the Key Management Interoperability Protocol (KMIP) 1.1 standard.

**Launch vSphere Client**

1. If Chrome is not already running, Click on the Chrome Icon on the Windows Quick Launch Task Bar.

**Login to vSphere Client**

1. On the vSphere Web Client login screen, select "Use Windows session authentication"
2. Click Login
Select Hosts and Clusters

Add Key Management Server settings

A Key Management Server (KMS) cluster provides the keys that you can use to encrypt the vSAN datastore.

Before you can encrypt the vSAN datastore, you must set up a KMS cluster to support encryption.
That task includes adding the KMS to vCenter Server and establishing trust with the KMS.

vCenter Server provisions encryption keys from the KMS cluster.

1. Select the vCenter Server called `vcsa-01a.corp.local`
2. Select `Configure`
3. Select `More > Key Management Servers`
4. Click `ADD`

**Add Key Management Server**

```
KMS cluster
New cluster name
KMS Cluster: Hytrust KMS Server
Make this the default cluster: enabled
Server name
Server address: 192.168.110.81
Server port: 5696
Proxy address
Proxy port
User name
Password
```

Enter the following information to create the KMS Cluster:

- **KMS Cluster:**
  - Cluster name: Hytrust KMS Server
  - Make this the default cluster: enabled
- **Server alias:** `kms-01a`
- **Server Address:** `192.168.110.81`
- **Server port:** `5696`

The remaining settings can be left blank.

Click `ADD`
Add Key Management Server

On the Trust Certificate dialog box.

Click **TRUST**

Add Key Management Server

1. Expand the *kms-01a* that you just added to see additional information.
2. Click **Make KMS TRUST VCENTER**
Add Key Management Server

Make KMS trust vCenter

1. Choose a method

2. Establish Trust

Choose a method

Choose a method to make the KMS trust the vCenter based on the KMS vendor's requirements. Once the trust is established, all replicas in the same KMS cluster will also trust the vCenter.

- vCenter Root CA Certificate
  Download the vCenter root certificate and upload it to the KMS. All certificates signed by this root certificate will be trusted by the KMS.

- vCenter Certificate
  Download the vCenter certificate and upload it to the KMS.

- KMS certificate and private key
  Upload the KMS certificate and private key to vCenter.

- New Certificate Signing Request (CSR)
  Submit the vCenter-generated CSR to the KMS then upload the new KMS-signed certificate to vCenter.

Select **KMS certificate and private key**

Click **NEXT**
Add Key Management Server

1. For the KMS Certificate, click **UPLOAD A FILE** and Browse to **KMIPvSphereCert.pem** on the Desktop and click **Open**
2. For the KMS Private Key, click **UPLOAD A FILE** and Browse to **KMIPvSphereCert.pem** on the Desktop and click **Open**

Click **ESTABLISH TRUST**
Verify Key Management Server

Verify that the HyTrust Key Management Server has been added.
Verify that the Connection Status is Green and the Certificates are valid.

Enabling vSAN Encryption

Since vSAN 6.6, we are introducing another option for native data-at-rest encryption, vSAN Encryption.

vSAN Encryption is the industry’s first native HCI encryption solution; it is built right into the vSAN software. With a couple of clicks, it can be enabled or disabled for all items on the vSAN datastore, with no additional steps.

Because it runs at the hypervisor level and not in the context of the virtual machine, it is virtual machine agnostic, like VM Encryption.

And because vSAN Encryption is hardware agnostic, there is no requirement to use specialized and more expensive Self-Encrypting Drives (SEDs), unlike the other HCI solutions that offer encryption.
Enabling vSAN Encryption

You can enable encryption by editing the configuration parameters of an existing vSAN cluster.

1. Select the Cluster called RegionA01-COMP01
2. Select Configure
3. Select vSAN > Services
4. Expand the Encryption service
5. Click EDIT

Turning on encryption is a simple matter of clicking a checkbox. Encryption can be enabled when vSAN is enabled or after and with or without virtual machines (VMs) residing on the datastore.

Note that a rolling disk reformat is required when encryption is enabled.

This can take a considerable amount of time – especially if large amounts of existing data must be migrated as the rolling reformat takes place.
Enabling vSAN Encryption is a one click operation.

1. Click to enable Encryption
2. Verify the KMS Server is selected (Hytrust KMS Server), if you have multiple KMS clusters in your environment, you can choose from here.
3. Select option to Allow Reduced Redundancy

Enabling vSAN Encryption has an option to Erase disk before use. Do not enable this option.

Click on the information button (i) for these options to get additional information on these options.

Click APPLY

The Erase disks before use option will significantly reduce the possibility of data leak and increase the attackers cost to reveal sensitive data. This option will also increase the cost of time to consume disks.
Monitor Recent Tasks

You can monitor the vSAN Encryption process from the Recent Tasks window.

To enable vSAN Encryption, the following operations take place.

- Data is migrated from each vSAN Disk Group
- That vSAN Disk Group is removed
- The vSAN Disk Group is recreated with Encryption enabled

This process is repeated for each of the Disk Groups in the vSAN Cluster.

Monitor Formatting Progress

1. You can also monitor the vSAN Encryption process from the Configure -> vSAN -> Disk Management screen
Enabling vSAN Encryption will take a little time. Each of the Disk Groups in the vSAN Cluster have to be removed and recreated.

**Enabling vSAN Encryption**

Once the rolling reformat of all the disk groups task has completed, Encryption of data at rest is enabled on the vSAN cluster.

vSAN encrypts all data added to the vSAN datastore.

You have the option to generate new encryption keys, in case a key expires or becomes compromised.

**vSAN Encryption Health Check**
There are vSAN Health Checks to verify that your vSAN Encryption is enabled and healthy.

1. Select the Cluster called RegionA01-COMP01
2. Select Monitor
3. Select vSAN > Health
4. Expand the Encryption health service

**vSAN Encryption Health Check**

1. Select **vCenter and all hosts are connected to Key Management Servers**

This vSAN Health Check verifies that the vCenter Server can connect to the Key Management Servers
1. Select **CPU AES-NI is enabled on hosts**

This check verifies whether ESXi hosts in the vSAN cluster have **CPU AES-NI** feature enabled.

Advanced Encryption Standard Instruction Set (or the Intel Advanced Encryption Standard New Instructions; AES-NI) is an extension to the x86 instruction set architecture for microprocessors from Intel and AMD. The purpose of the instruction set is to improve the speed of applications performing encryption and decryption using the Advanced Encryption Standard (AES).

**Conclusion**

With the addition of vSAN Encryption in vSAN 6.6 and with VM Encryption introduced in vSphere 6.5, native data-at-rest encryption can be easily accomplished on hyper-converged infrastructure (HCI) powered by vSAN storage or any other vSphere storage.

While vSAN Encryption and VM Encryption meet similar requirements, they do so a bit differently, each with use cases they excel at.

Most importantly, they provide customers choice for when deciding how to provide data-at-rest encryption for their vSphere workloads.
Conclusion

In this lesson we explored vSAN security parameters including DISA STIG (FIPS 104-2) Validation and vSAN Data-at-rest Encryption.

You've finished Module 6

Congratulations on completing Module 6.

If you are looking for additional information on topic:

- VMware Security Certification
- vSAN 6.7 Datasheet (including FIPS 140-2 Information)
- vSAN Encryption
- Go to VMware Storage Hub for all things related to vSAN.

How to End the Lab

If you would like to end your lab click on the END button.
Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit http://hol.vmware.com/ to continue your lab experience online.

Lab SKU: HOL-1908-01-HCI

Version: 20181116-042153