HOL-2534-01-VCF-L

Getting Started and Advanced Topics

vmware®

Table of contents

Lab Overview - HOL-2534-01-VCF-L - VMware vSAN - Getting Started and Advanced Topics

Lab Guidance

[2]

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 What's new with vSAN 8 such as file services and Encryption with Security then explore the vSAN environment including monitoring the health, capacity and performance of vSAN within vCenter and also via, built-in, Aria 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.

Lab Module List:

- Module 1 - vSAN SPBM and Availability (30 minutes) (Basic) Introduction to VMware vSAN's Express Storage Architecture. We will cover the power of Storage Based Policy Management (SPBM) and show you the availability of vSAN.
- Module 2 - Monitoring, Health, Capacity, and Performance (30 minutes) (Basic) Show you how to enable Aria Operations within vCenter Server. We will cover the vSAN Health Check and how you can monitor your vSAN environment.
- Module 3 - vSAN Encryption and Security (30 minutes) (Advanced) Introduction to vSAN Encryption. We will enable a Key Management Server and demonstrate how to configure vSAN Encryption.
- Module 4 - File services (30 minutes) (Basic) Introduction to vSAN's File Services capabilities. We will create both NFS and SMB file shares and mount them to their respective clients.
- Module 5 - Data Protection (30 minutes) (Advanced) Introduction to vSAN ESA's new data protection capabilities. We will cover creating protection groups and snapshot schedules.
- Module 6 - vSAN Stretched Cluster (30 minutes) (Advanced) Introduction to vSAN Stretched Clusters. We will convert an existing vSAN cluster into a stretched cluster. In addition, we will explore storage policies as well as Skyline Health checks with respect to stretched clusters.

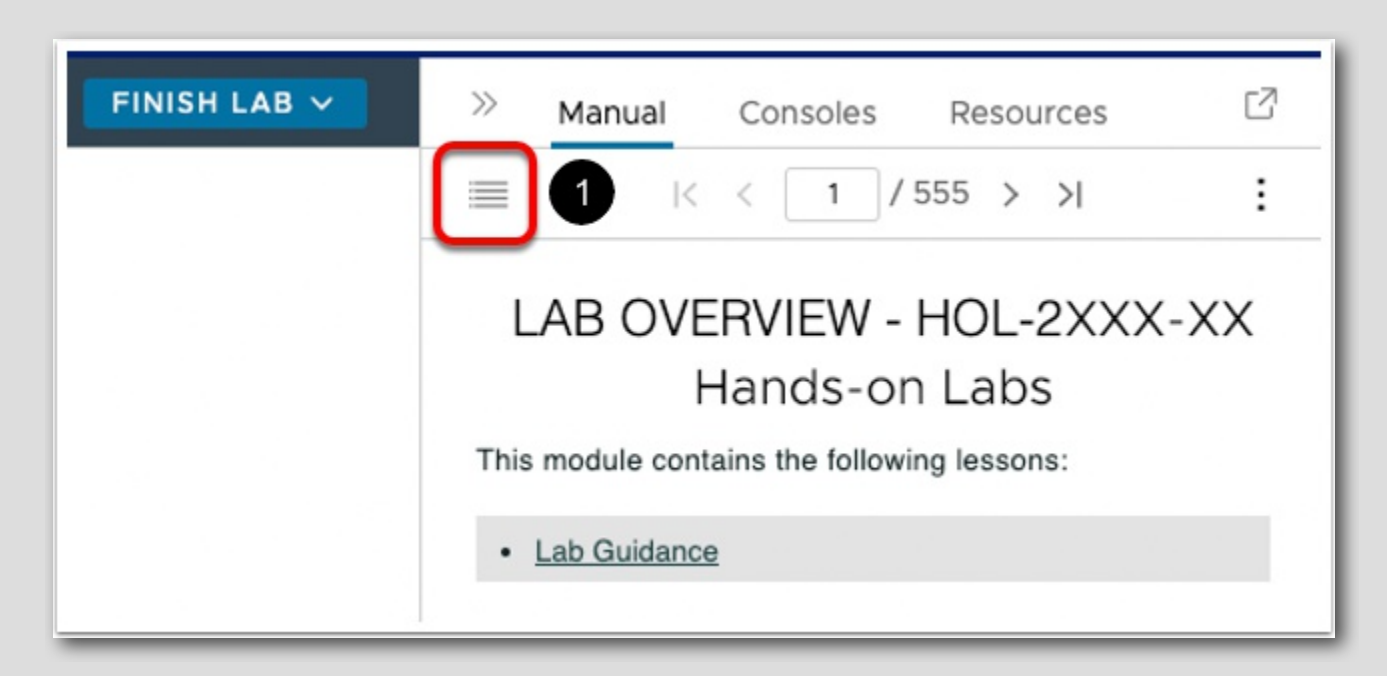
Lab Captains:

- Cristian Lamson, Solutions Architect, USA
- Jim LaFollette, Cloud Architect, USA

Principal:

- Peter Kieren, Enterprise Architect, Canada

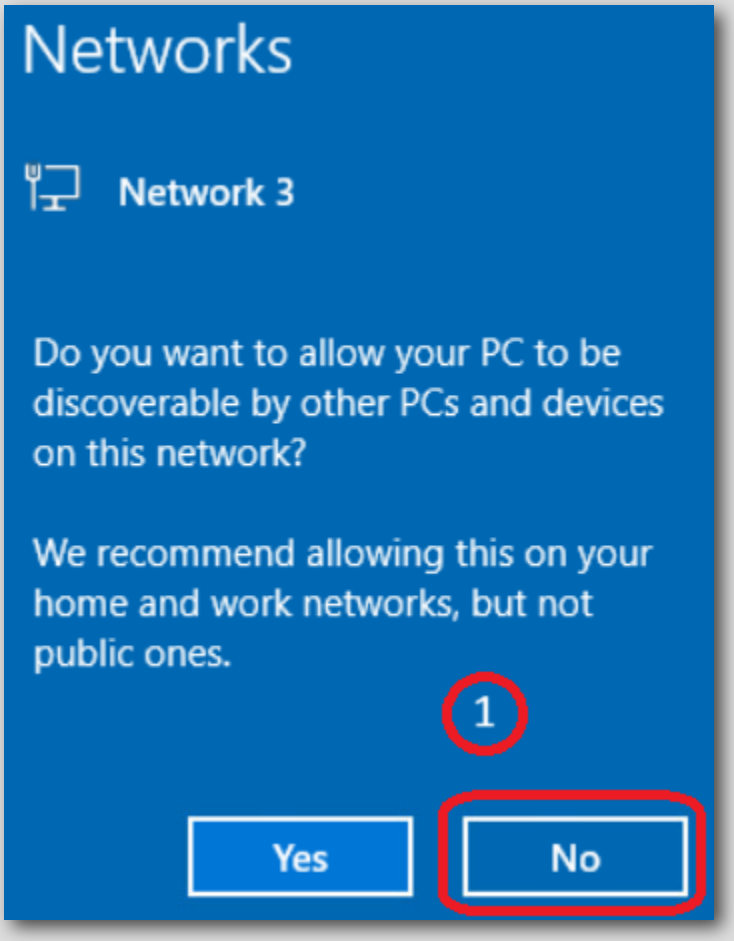
First time using Hands-on Labs? [3]

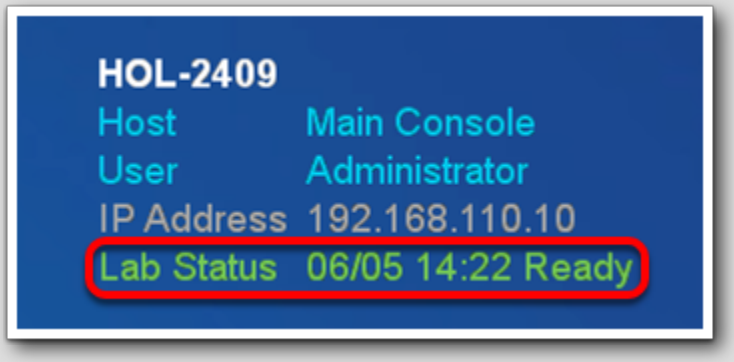


Welcome!

1. If this is your first time taking a lab navigate to the **Appendix** in the Table of Contents to review the interface and features before proceeding. For returning users, feel free to start your lab by clicking next in the manual.

You are ready....is your lab? [4]





PLEASE NOTE - There is a chance Windows will ask you if you want your "Network 3" to be discoverable - if you see this screen please click "No" and continue with your lab.

Please verify that your lab has 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.

Lab Description

[5]

Explore the components and capabilities within vSAN 8's Express Storage Architecture- VMware's market-leading HCI platform. This lab covers:

- Storage Policy-Based Management & Availability
- Performance and Capacity Monitoring & Management
- Data Encryption & Security
- File Services
- Data Protection
- Stretched Cluster

Module 1 - vSAN SPBM and Availability (30 minutes) Basic

Introduction [7]

vSAN delivers flash-optimized, secure shared storage solution 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 8 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 make it the most complete platform for virtual machines, whether running business-critical databases, virtual desktops or next-generation applications.

What's new in vSAN 8? [8]

Before we jump in the Lab, let's take a moment to review What's New with vSAN 8.

With vSAN 8, we are continuing to build on the robust features that make vSAN a high performing general-purpose infrastructure. vSAN 8 makes it easy for you to standardize on a single storage operational model with three new capabilities: integrated file services, enhanced cloud-native storage, and simpler lifecycle management. You can now unify block and file storage on hyper-converged infrastructure with a single control pane, which reduces costs and simplifies storage management.
Cloud-native applications also benefit from these updates, which include integrated file services, vSphere with Kubernetes support, and increased data services. Finally, vSAN 8 also simplifies HCI lifecycle management by reducing the number of tools required for Day 2 operations, while simultaneously increasing update reliability.

Product Enhancements

[9]

The most significant new capabilities and updates of vSAN 8 include:

- One Solution - Two Architectures

At a high level, the original storage architecture (OSA) of vSAN was a two-tier architecture designed to accommodate a wide ranging set of older storage devices, while the vSAN Express Storage Architecture (ESA) in vSAN 8 is a single-tier architecture optimized for high-performance NVMe based TLC flash devices for both on-premises environments, and for the public cloud hyper-scalers.

- vSAN Max

Built using the vSAN Express Storage Architecture, vSAN Max provides highly flexible disaggregated storage for vSphere. It provides the unique ability to provision a vSAN cluster to be used as shared storage for vSphere clusters. It is built using vSAN's Express Storage Architecture (ESA), and will most certainly introduce all new benefits to those who wish to have a three-tier architecture, but like the convenience and simplicity of vSAN.

- Enhanced Cloud-Native Storage

vSAN supports file-based persistent volumes for Kubernetes on vSAN datastore. Developers can dynamically create file shares for their applications and have multiple pods share data.

- Integrated File Services

In vSAN 8, integrated file services make it easier to provision and share files. Users can now provision a file share from their vSAN cluster, which can be accessed via NFS 4.1 and NFS 3 and SMB. A simple workflow reduces the amount of time it takes to stand up a file share.

- Simpler Lifecycle Management

Consistent operations with a unified Lifecycle Management tool. vSAN 8 provides a unified vSphere Lifecycle Manager tool (vLCM) for Day 2 operations for software and server hardware. vLCM delivers a single lifecycle workflow for the full HCI server stack: vSphere, vSAN, drivers and OEM server firmware. vLCM constantly monitors and automatically remediates compliance drift.

- Increased Visibility into vSAN Used Capacity

Replication objects are now visible in vSAN monitoring for customers using *VMware Site Recovery Manager* and *vSphere Replication*. The objects are labeled "vSphere Replicas" in the "Replication" category.

- Uninterrupted Application Run Time

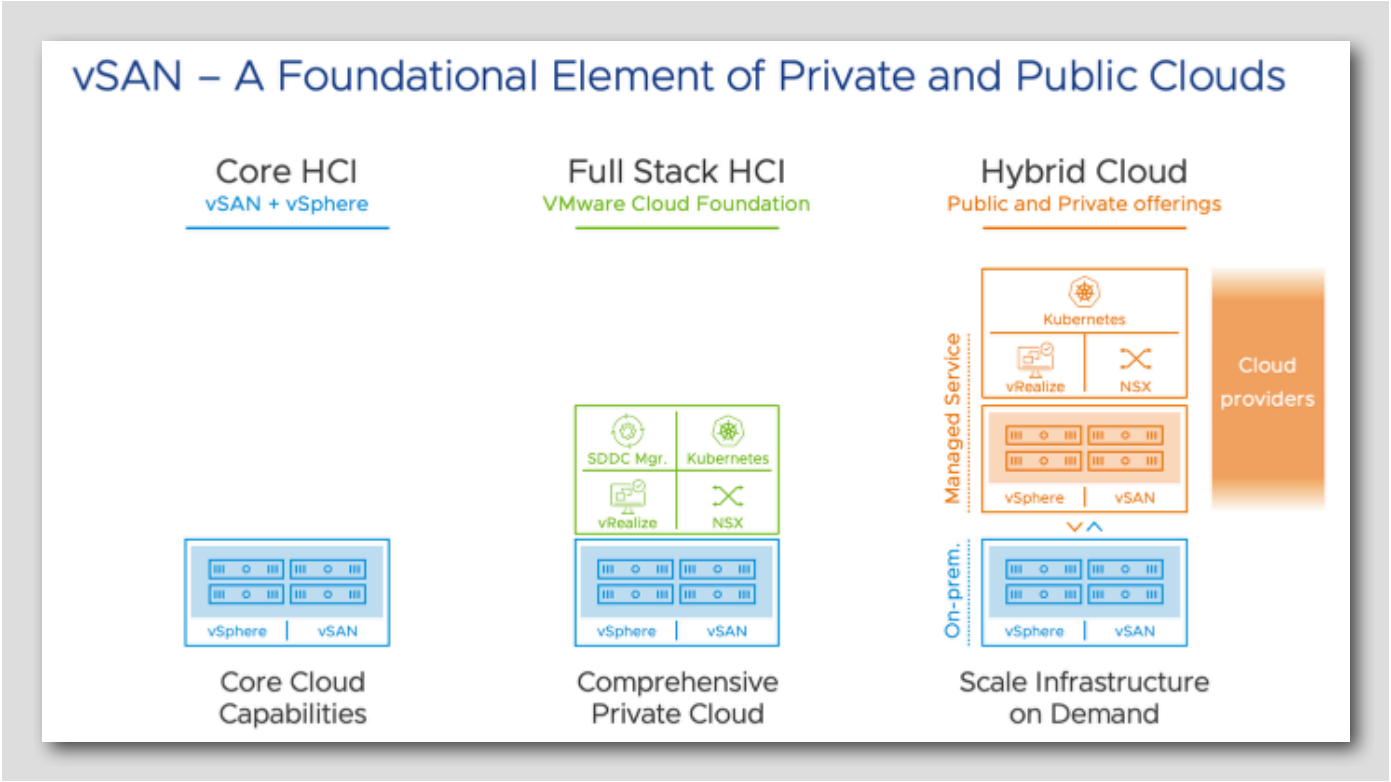
vSAN 8 enhances uptime in Stretched Clusters by introducing the ability to redirect VM I/O from one site to another in the event of a capacity imbalance. Once the disks at the first site have freed up capacity, customers can redirect I/O back to the original site without disruption.

- Automatic Policy Compliance for 2-Node vSAN Deployments

vSAN 8 keeps 2-node deployments in policy compliance by automating repair objects operations during witness replacement.

Why vSAN?

[10]



VMware's solution stack offers the levels of flexibility that is needed for today's rapidly changing needs. It's built off of a foundation of VMware vSphere, paired with vSAN. This provides the basis for a fully software defined storage and virtualization platform that removes dependencies from legacy solutions using physical hardware. Next is VMware Cloud Foundation, the integrated solution that provides the full stack of tools for an automated private cloud. And finally, there is VMware's Solutions for the Public Cloud. VMware is partnered with the industry-leading cloud providers that offer services based on VMware Cloud Foundation. This offers customers to build a hybrid cloud using public and private assets using a common substrate of management and tools for consistent infrastructure operations. The result is a complete solution regardless of where the topology sits on-prem or on the cloud.

Storage Policy Based Management

[11]

As an abstraction layer, Storage Policy Based Management (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.
- Bi-directional 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.

vSAN requires that the virtual machines deployed on the vSAN Datastore 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 Datastore.

Auto-Policy Management Capabilities with vSAN ESA

[12]

vSAN ESA 8.0 U1 introduces a way to ensure data using a default storage policy is stored in the most optimal, resilient way. The cluster service can be enabled by highlighting the cluster, clicking on Configure > vSAN Services > Storage, then clicking on "Edit" and enabling "Auto-Policy management." This feature has already been enabled in this lab.

When enabled, a new cluster-specific default storage policy will be created on the managing vCenter Server. This is created for a specific cluster and prevents imparting sub-optimal or incompatible settings for other vSAN clusters. It will create a policy using a syntax similar to: "**[Cluster Name]-Optimal Datastore Default Policy - RAID[x]**"

The policy settings the optimized storage policy uses are based on the **type of cluster**, the **number of hosts in a cluster**, and if the **Host Rebuild Reserve** (HRR) capacity management feature is enabled on the cluster.

vSAN Default Storage Policy Specifications

[13]

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.

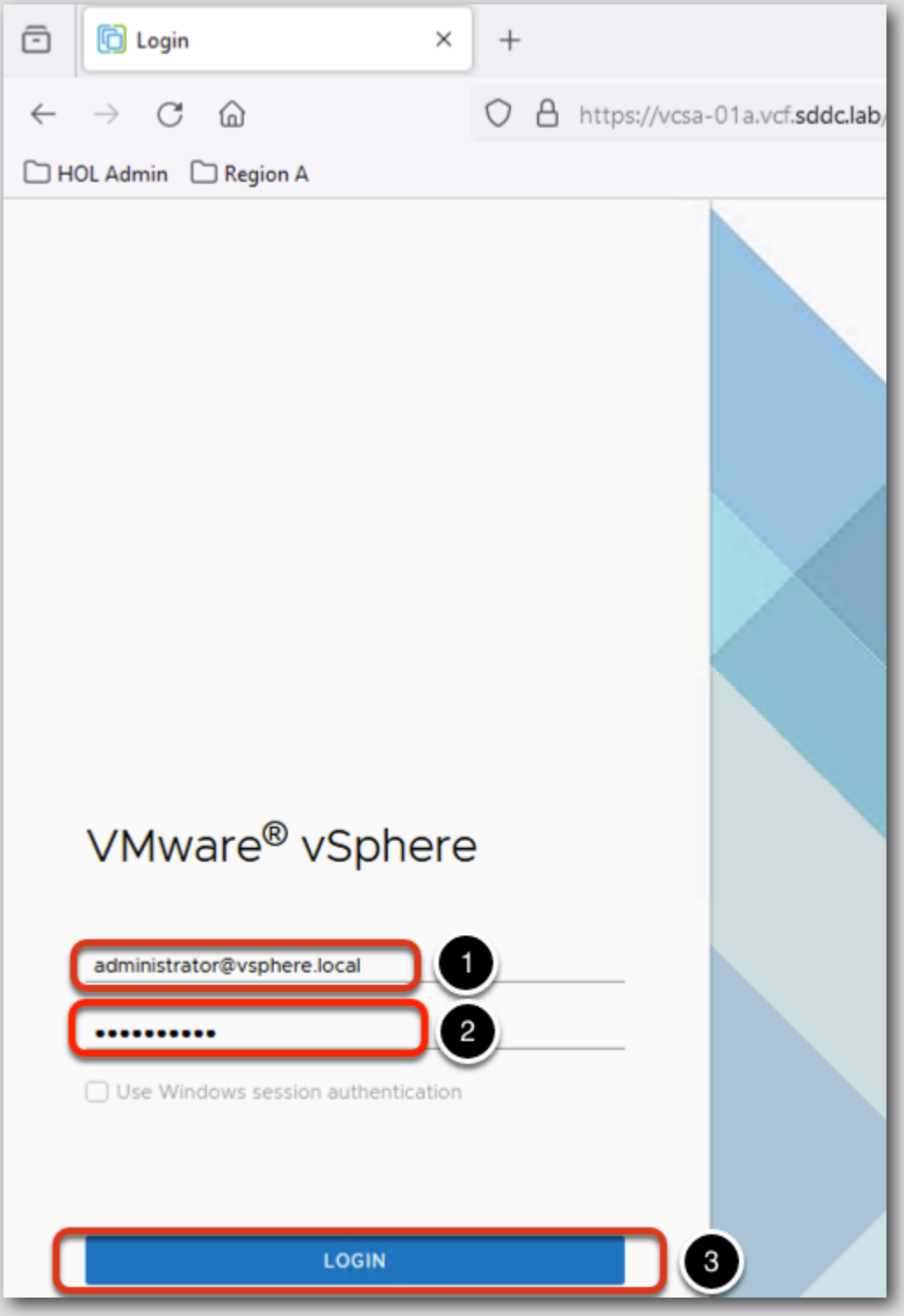
Open Firefox Browser from Windows Quick Launch Task Bar

[14]

1. Click on the **Firefox Icon** on the Windows Quick Launch Task Bar. You can skip this step if you're already in vSphere Client.

Login to vSphere Client

[15]

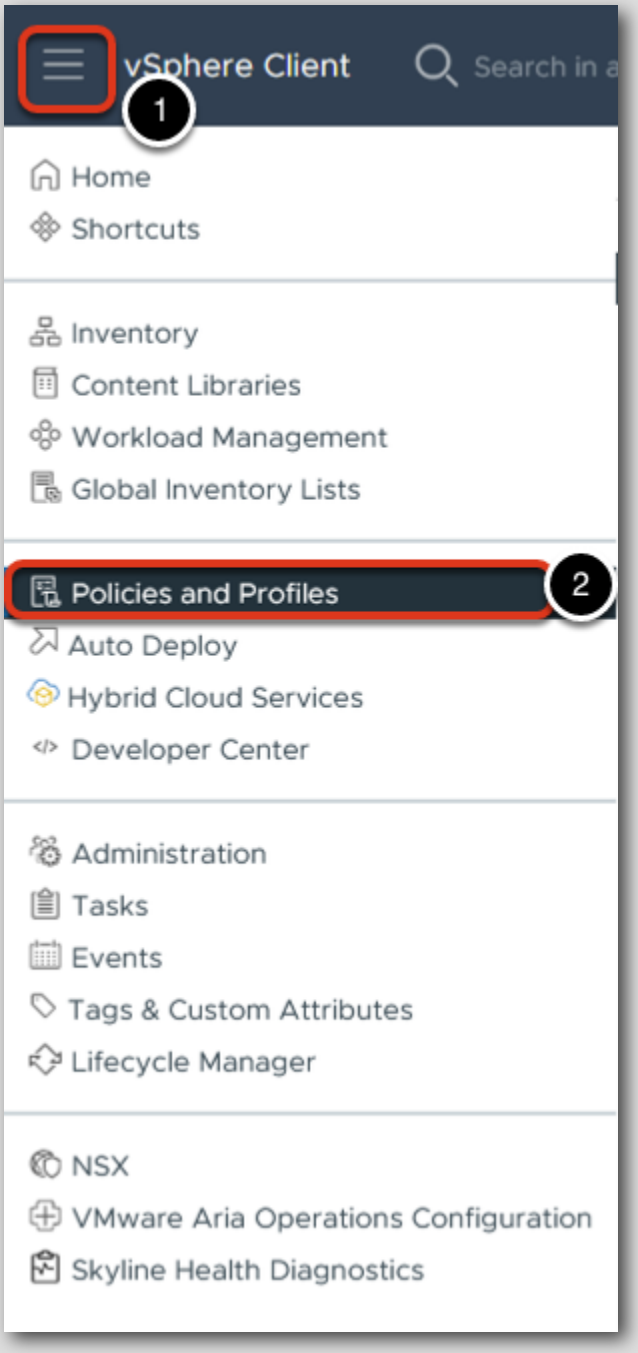

Login
https://vcsa-01a.vcf.sddc.lab/
HOL Admin
Region A
VMware® vSphere
administrator@vsphere.local
1
2
Use Windows session authentication
LOGIN
3

1. On the vSphere Client login screen, username: `administrator@vsphere.local`
2. Enter Password: `VMware123!`
3. Click **LOGIN**

You can skip this step if you're already in vSphere Client.

Examine the Default Storage Policy

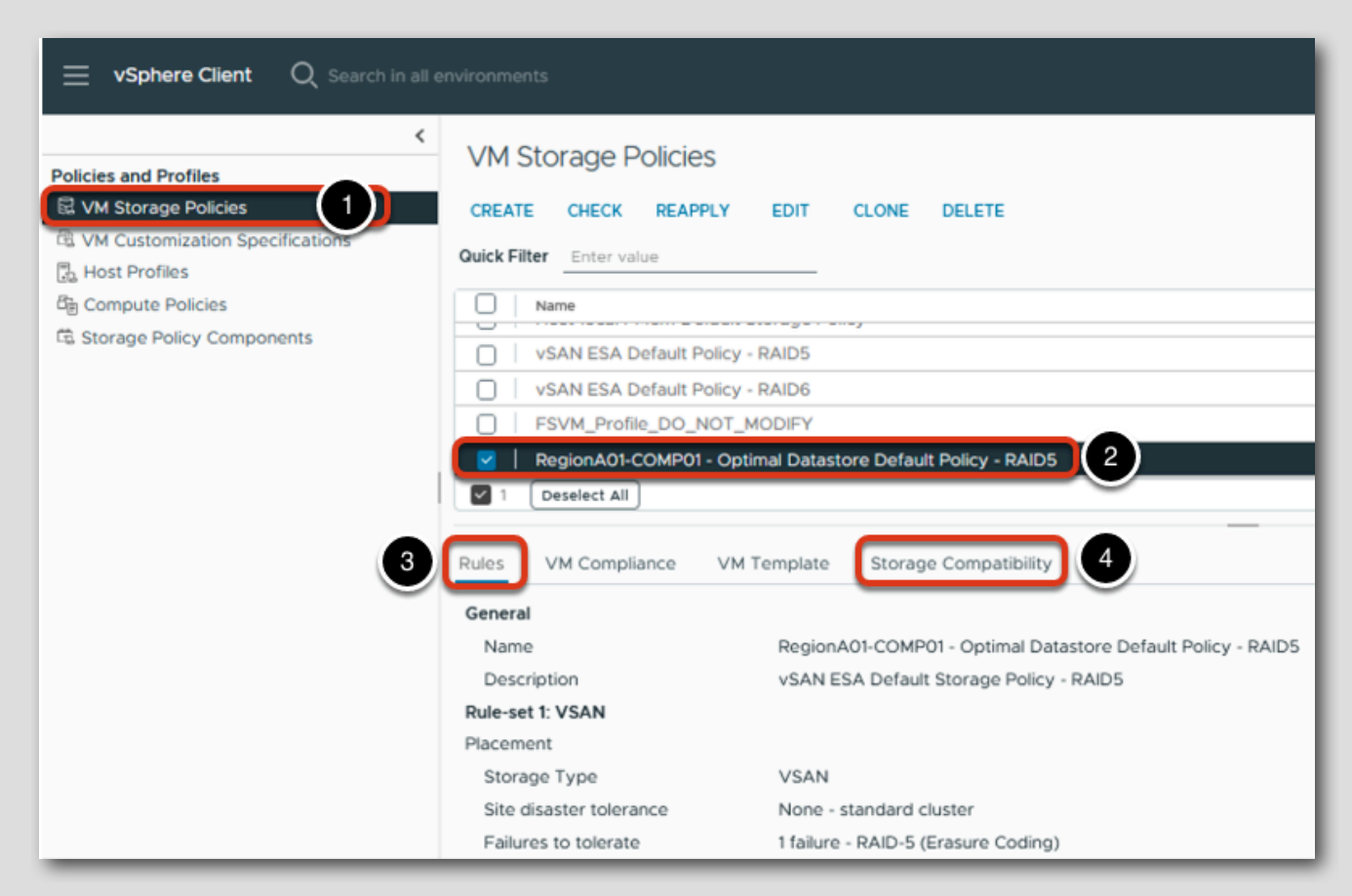
[16]



1. From the homepage, Click **Menu (3 Horizontal Lines)**of the vSphere Client
2. Select **Policies and Profiles**

Examine the Optimal Datastore Default Policy

[17]



1. Select **VM Storage Policies**
2. Scroll down and select the VM Storage Policy called **RegionA01-COMP01 - Optimal Datastore Default Policy - RAID5**
3. Select **Rules**

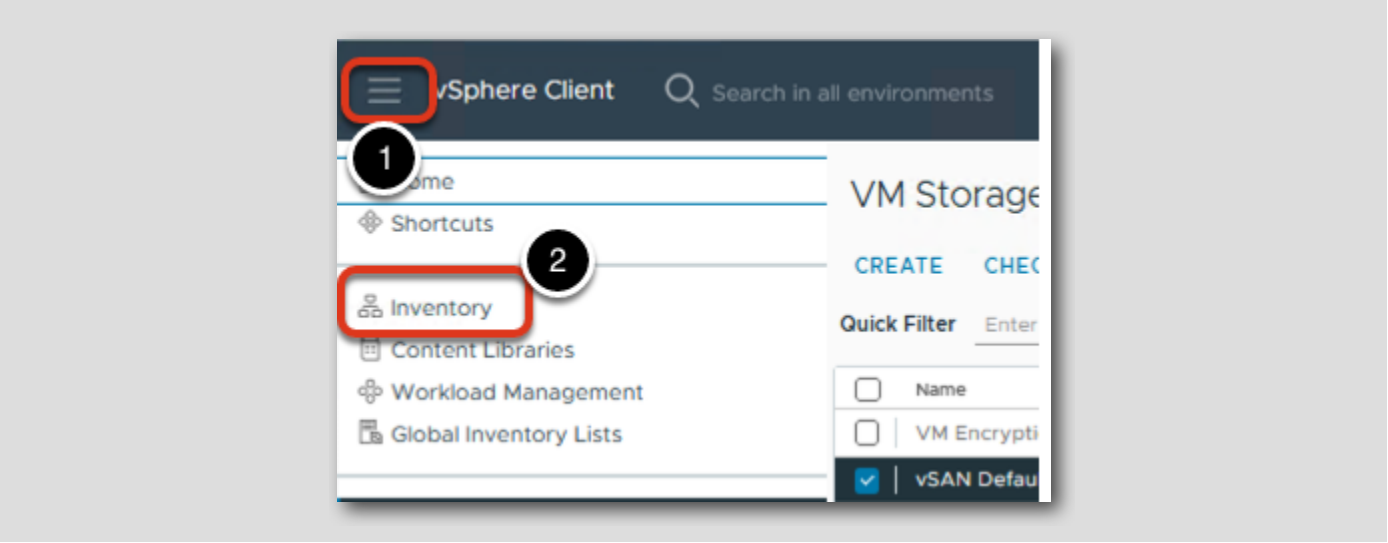
The default rules for the Storage Policy are displayed.

4. Select **Storage Compatibility**

Here we can see that the **vsanDatastore** is compatible with this storage policy (not pictured). If you're unable to see the compatible datastore listings, you may need to minimize the **Recent Tasks** bar by clicking the down arrow to the left of **Recent Tasks**.

Deploy VM with the Default Storage Policy

[18]



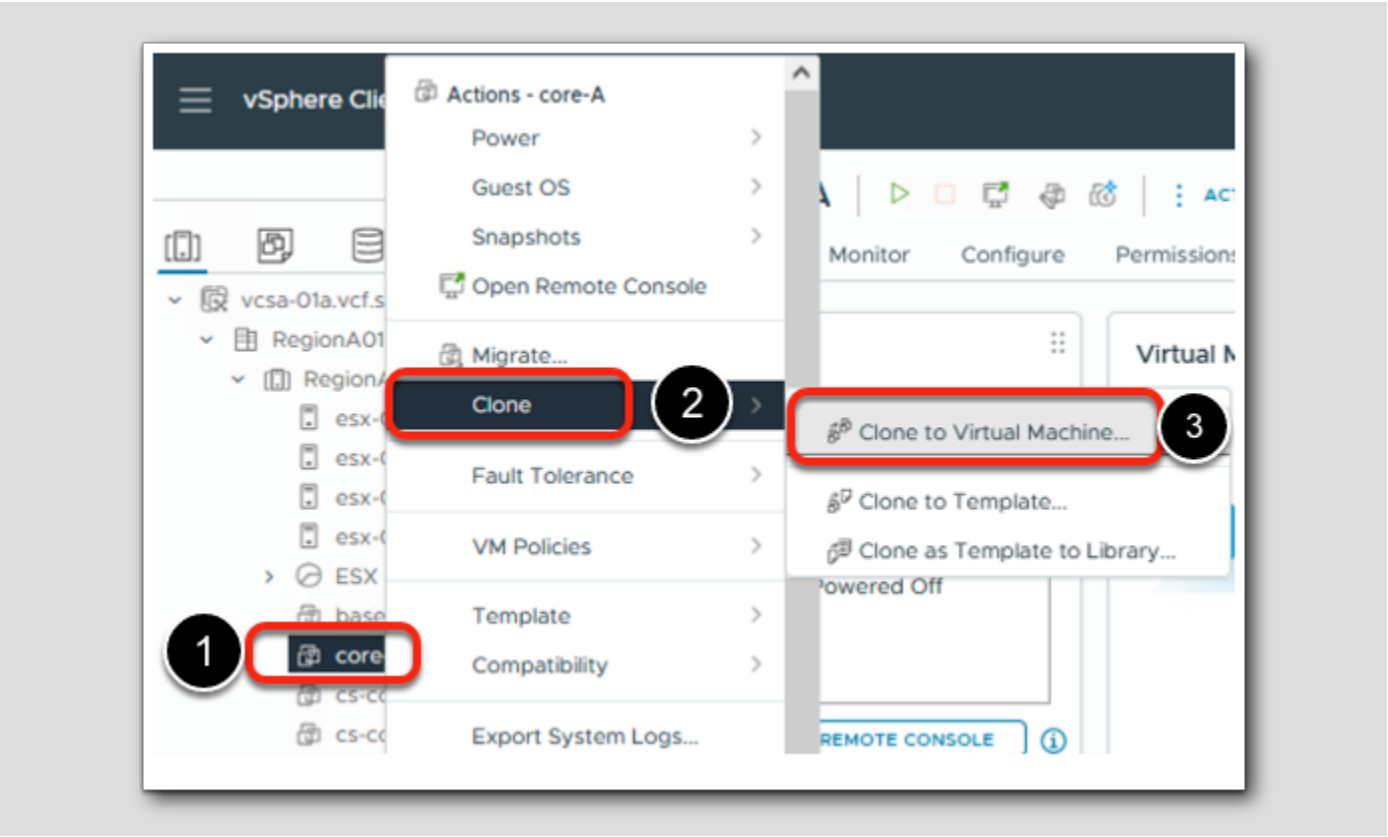
We will now clone a VM and apply the Default Storage Policy

1. Select **Menu** (3 Horizontal Lines)
2. Select **Inventory**

Deploy VM with Default Policy

[19]

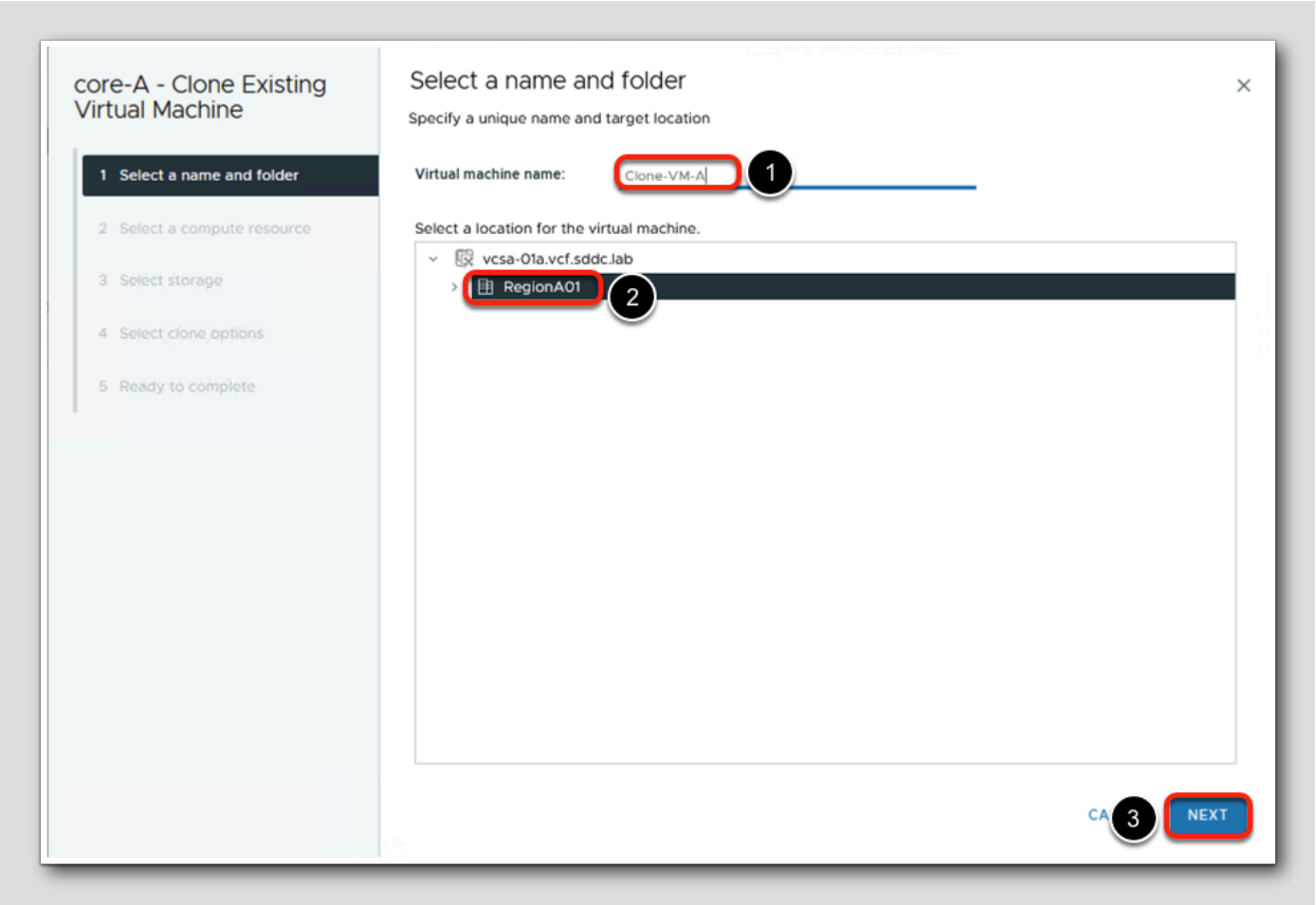
We will clone the VM called **core-A** (which currently resides on a Local VMFS datastore on an ESXi host) to the vSAN Datastore and apply the Default Storage Policy.



1. Expand the vSphere Cluster called **RegionA01-COMP01** and right click the VM called **core-A**
2. Select **Clone**
3. Select **Clone to Virtual Machine**

Deploy VM with Default Policy

[20]



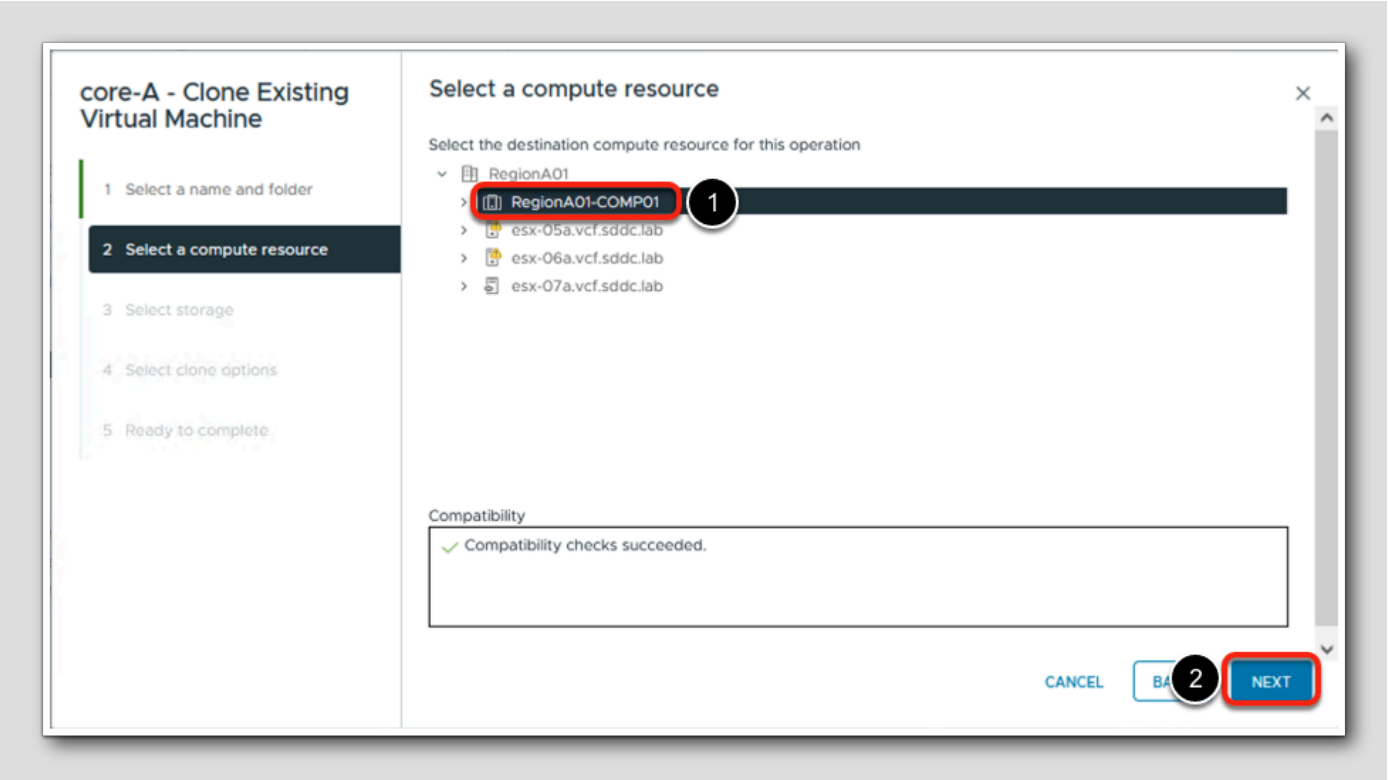
1. Give the Virtual Machine a name:

   ```
   Clone-VM-A
   ```

2. Select **vcsa-01a.vcf.sddc.lab** > **RegionA01**
3. Click **Next**

Deploy VM with Default Policy

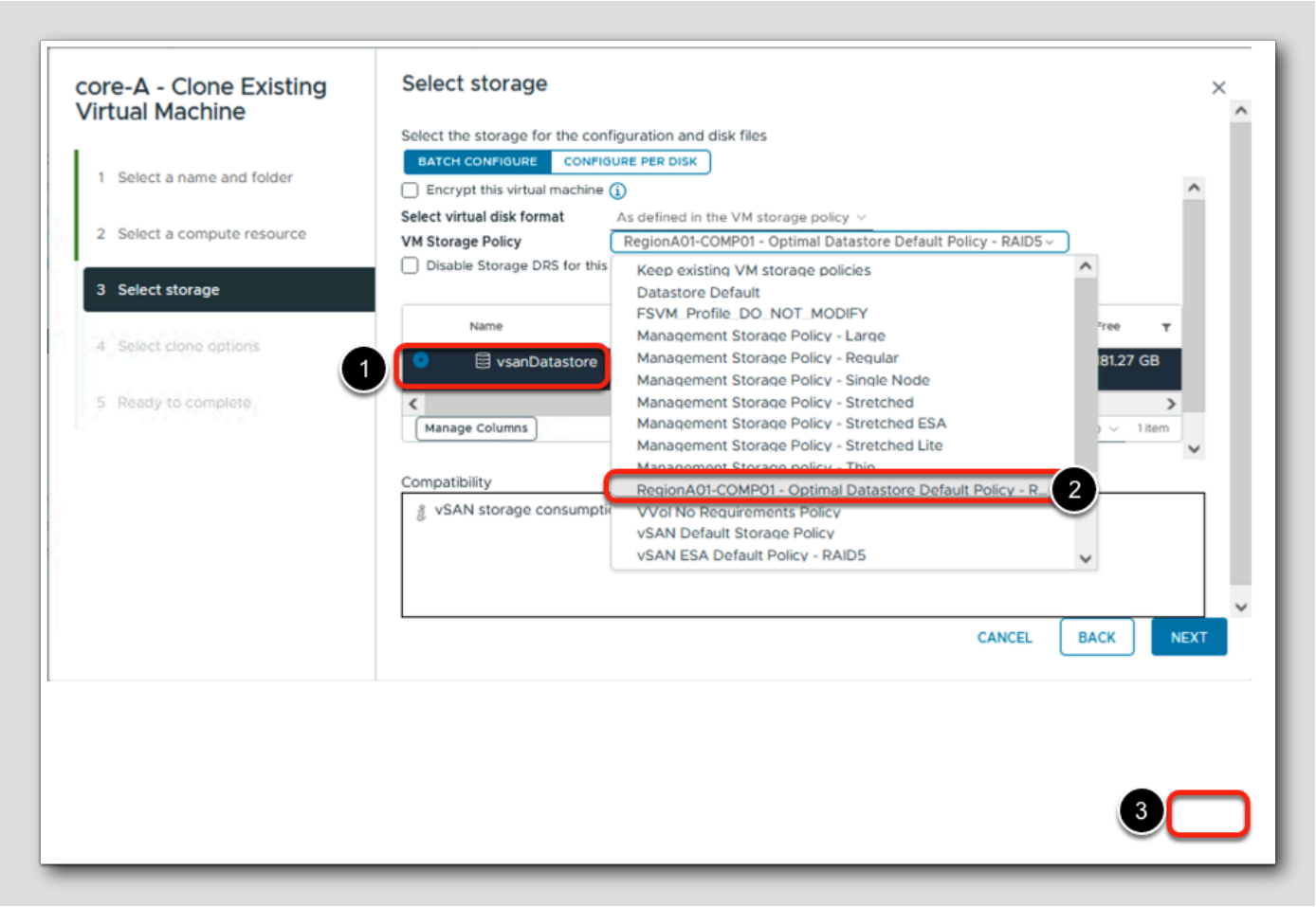
[21]



1. Select the cluster called RegionA01-COMP01
2. Click NEXT

Deploy VM with Default Policy

[22]



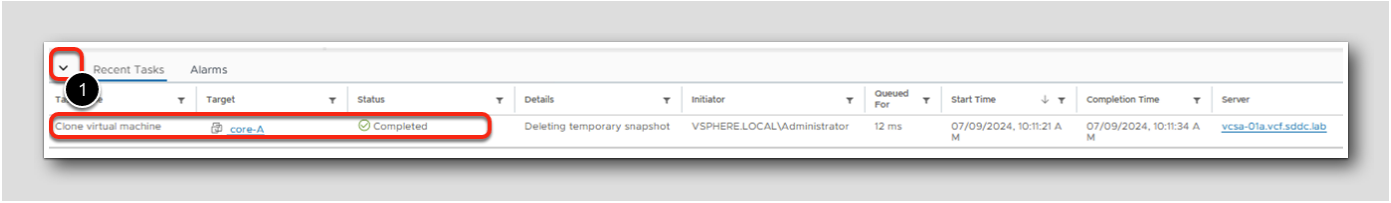
1. Click on **vsanDatastore**
2. For the VM Storage Policy dropdown, select **RegionA01-COMP01 - Optimal Datastore Default Policy - RAID 5** (part of the policy name may be cut off).

The resulting list of compatible datastores will be presented, in our case the vsanDatastore.

3. Click **NEXT**; then, click **NEXT** on the **Select clone options** (not picture); then, click **FINISH** (not picture)

Deploy VM with Default Policy

[23]

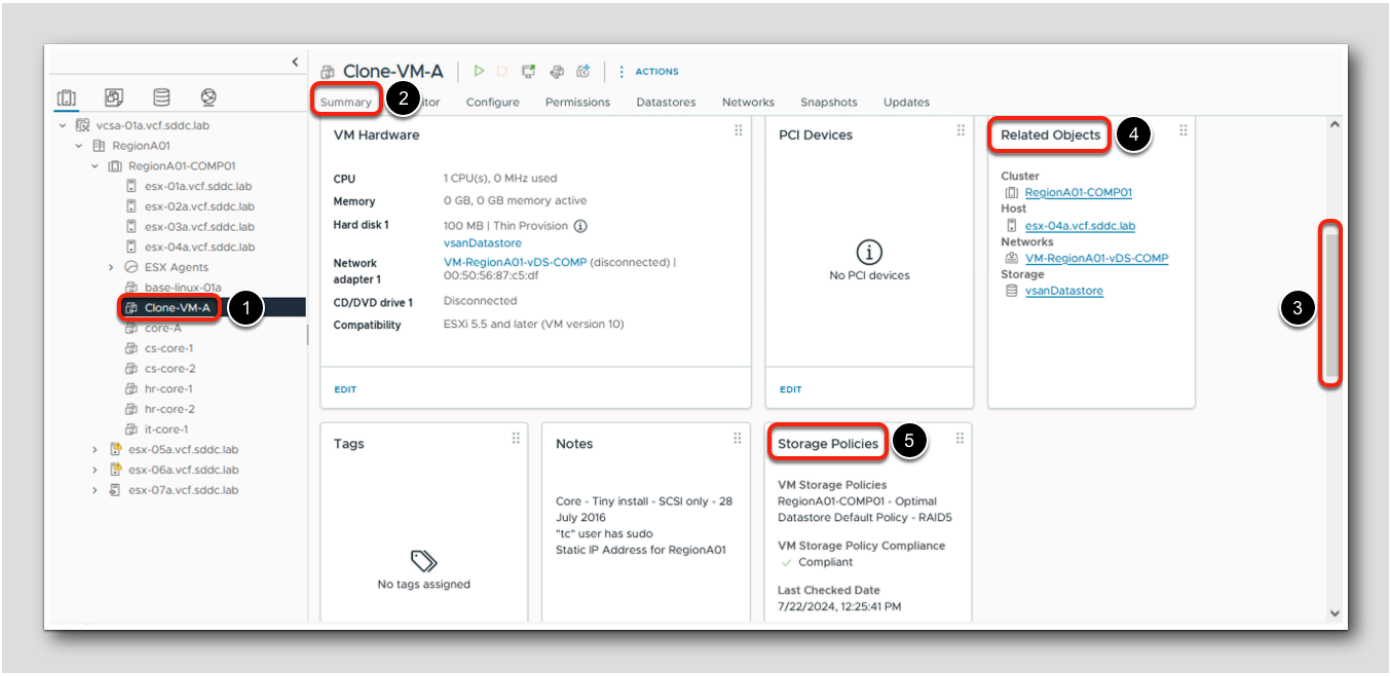


Wait for the Clone operation to complete.

1. Check the **Recent Tasks** for a status update on the Clone virtual machine task.

Verify VM has the Assigned Storage Policy

[24]



Once the clone operation has been completed:

1. Select the VM called **Clone-VM-A**
2. Select **Summary**
3. Scroll down
4. View **Related Objects**

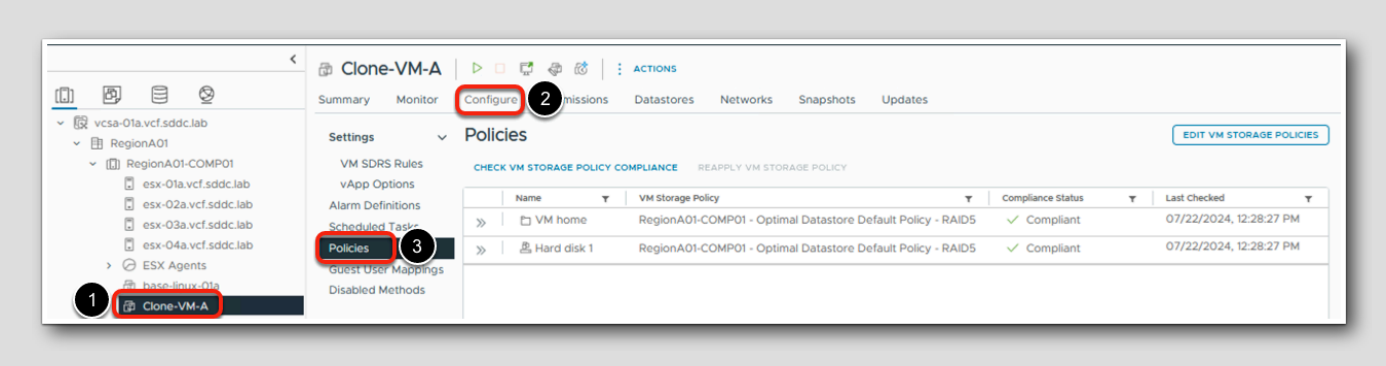
The VM is now residing on the **vsanDatastore**

5. Scroll down and View **Storage Policies**

Here we can see that the VM Storage Policy for this VM is set to **RegionA01-COMP01 - Optimal Datastore Default Policy - RAID5** and the policy is **Compliant**.

VM Disk Policies

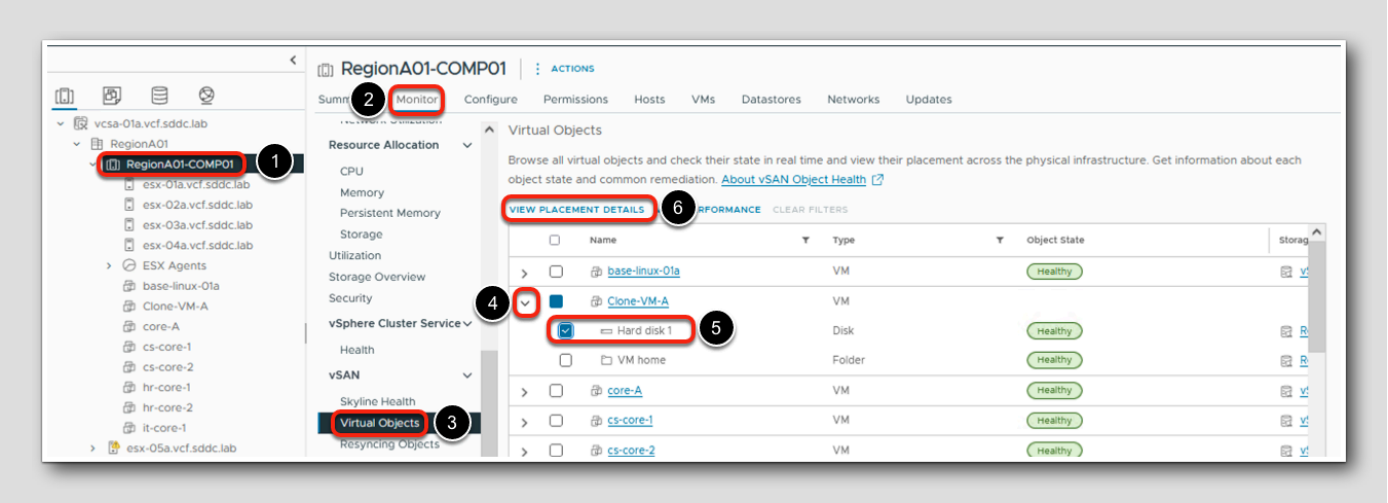
[25]



1. Select the VM called **Clone-VM-A**
2. Select **Configure**
3. Select **Policies**

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

VM Disk Policies



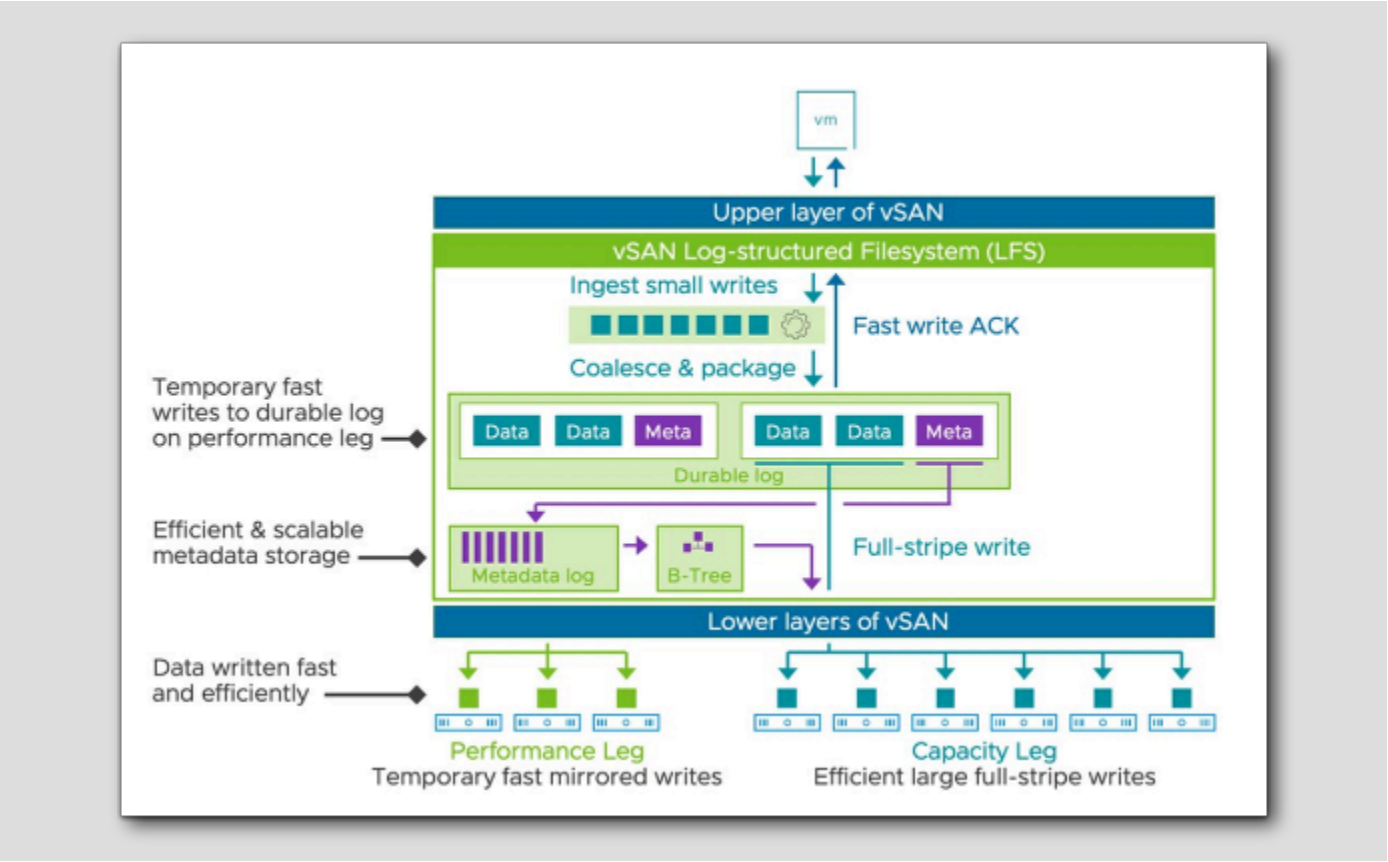
1. Select the **RegionA01-COMP01**
2. Select **Monitor**
3. Scroll down and select **vSAN** > **Virtual Objects**
4. Expand **Clone-VM-A**
5. Select **Hard disk 1**

Verify that the Object State is **Healthy** and **vSAN Default Storage Policy** is applied. You may need to scroll to the right to see the Storage Policy.

6. Click **View Placement Details**

vSAN ESA Log-Structured File System

[27]

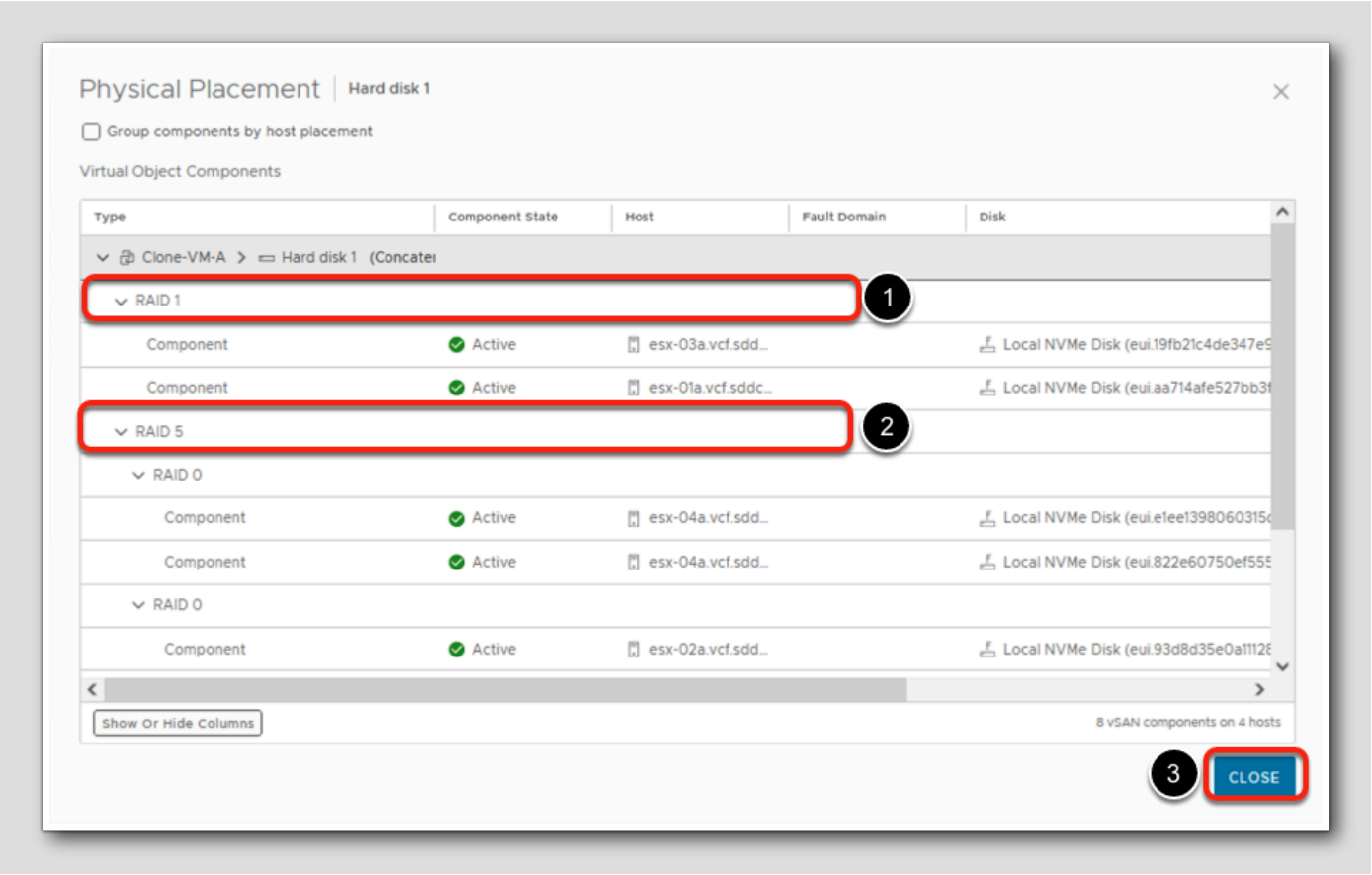


vSAN ESA uses a log-structured file system to reduce IO amplification and to maximize performance. First, data is written to the performance leg as a mirrored RAID 1 in order to provide a fast write acknowledgement. Then, vSAN will coalesce and package enough small writes in order to destage the data into a full- stripe write. This could be a RAID-1, however more often than not it will be either a RAID-5 or RAID-6 depending on the policy chosen.

Let's take a look at how a VM's components are spread across the cluster.

VM Disk Policies

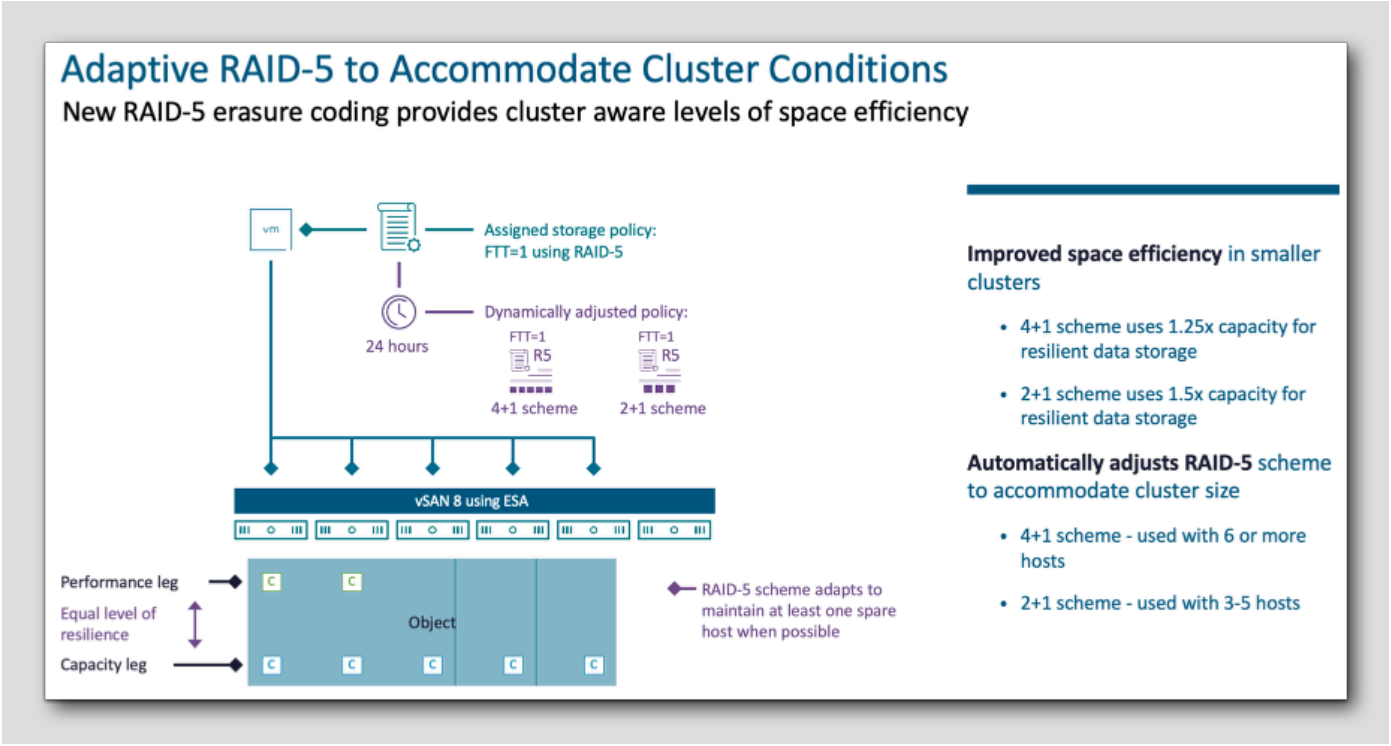
[28]



Here we can see the Component layout for the Hard Disk object.

1. The RAID 1 is the Performance Leg which is where we mirror the data across hosts to provide the fast write acknowledgement.
2. The RAID 5 is the Capacity Leg which is where the mirrored writes are coalesced and destaged. In this case, you'll notice that the data is striped across three hosts.
3. Click **CLOSE**

Scaling out the vSAN Environment



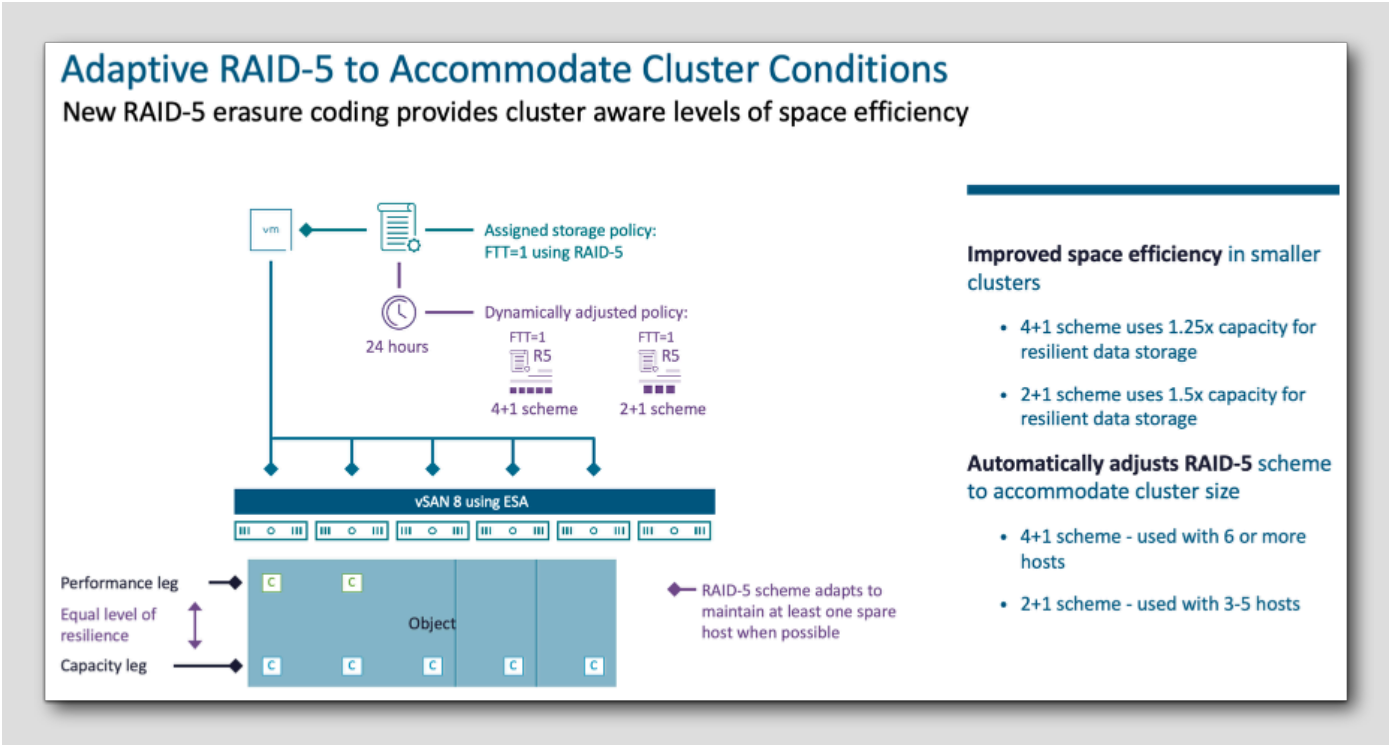
Note that there is a requirement on the number of hosts needed to implement RAID-5 or RAID-6 configurations on vSAN.

For RAID-5 utilizing the Original Storage Architecture (OSA), a minimum of 4 hosts are required; for RAID-6, a minimum of 6 hosts are required.

For vSAN's Express Storage Architecture (ESA), we now have an adaptive RAID-5 that can change its stripe scheme depending on the amount of hosts in the cluster:

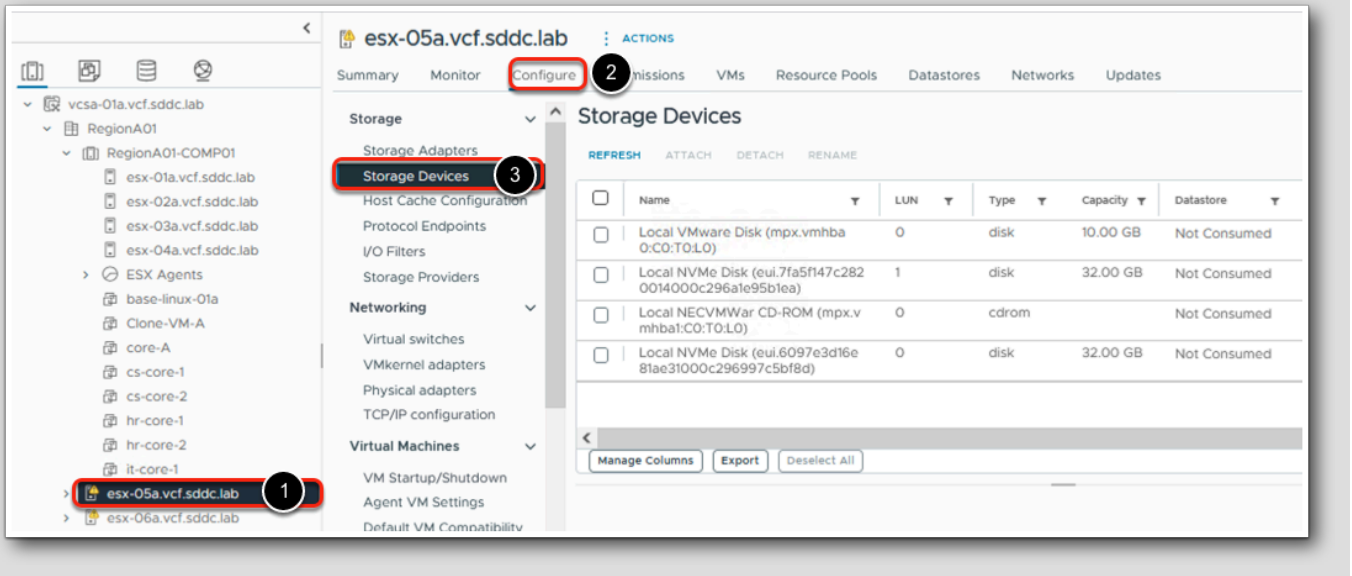
- For clusters containing 3-5 hosts, vSAN ESA will use a 2+1 scheme that uses 1.5x raw capacity.
- For clusters containing 6 or more hosts, vSAN ESA will use a 4+1 scheme that uses 1.25x raw capacity.
- In addition, this RAID 5 scheme will automatically adjust after 24 hours if the number of hosts in the cluster changes (whether due to adding a host or due to host failure).

A minimum of 6 hosts is still required for RAID-6 with ESA.



Lab Environment Review - Compute

[30]



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

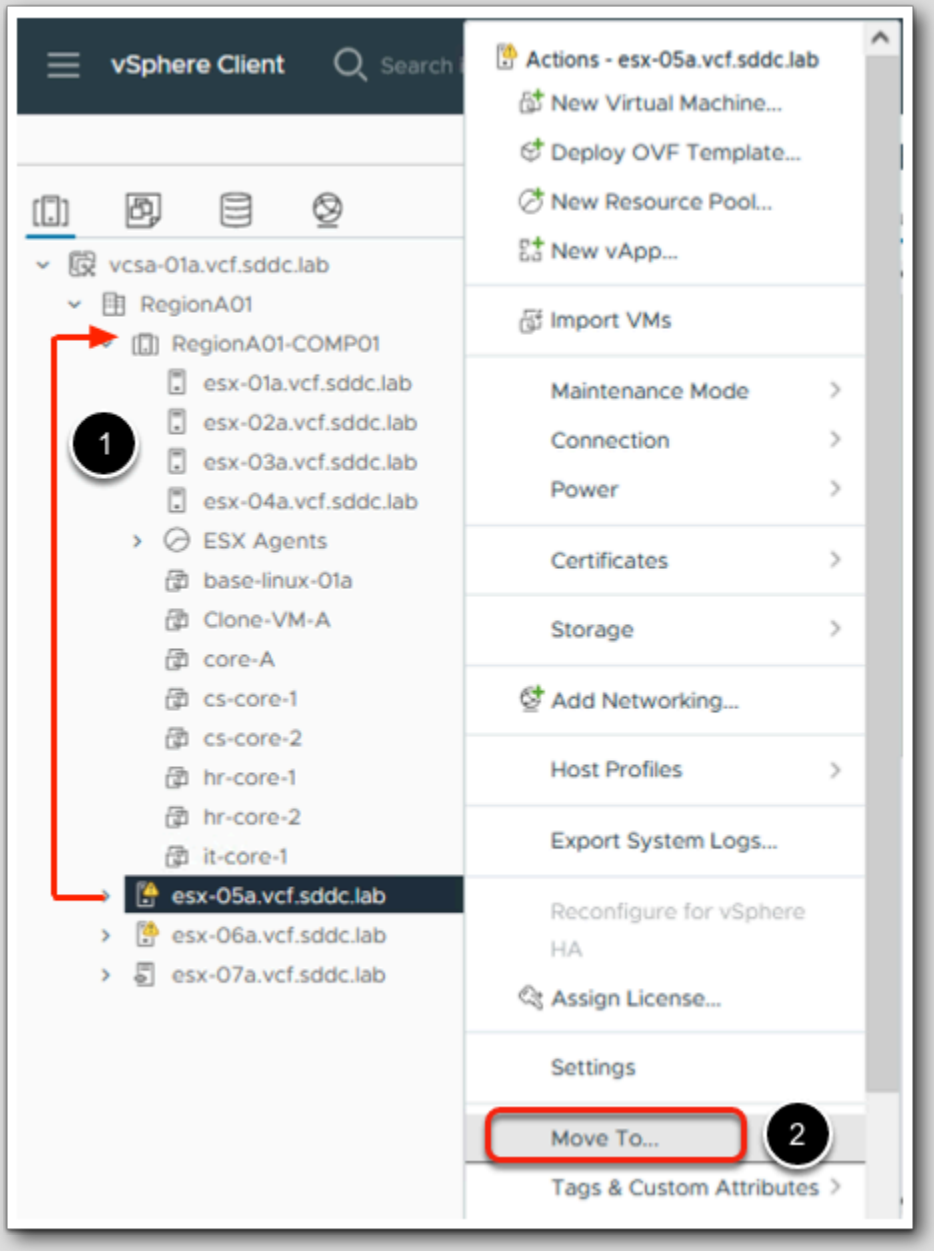
There are currently three hosts in the cluster, and there are additional hosts not in the cluster.

1. Select the ESXi host called **esx-05a.vcf.sddc.lab**
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.

Add Additional Node to Cluster

[31]

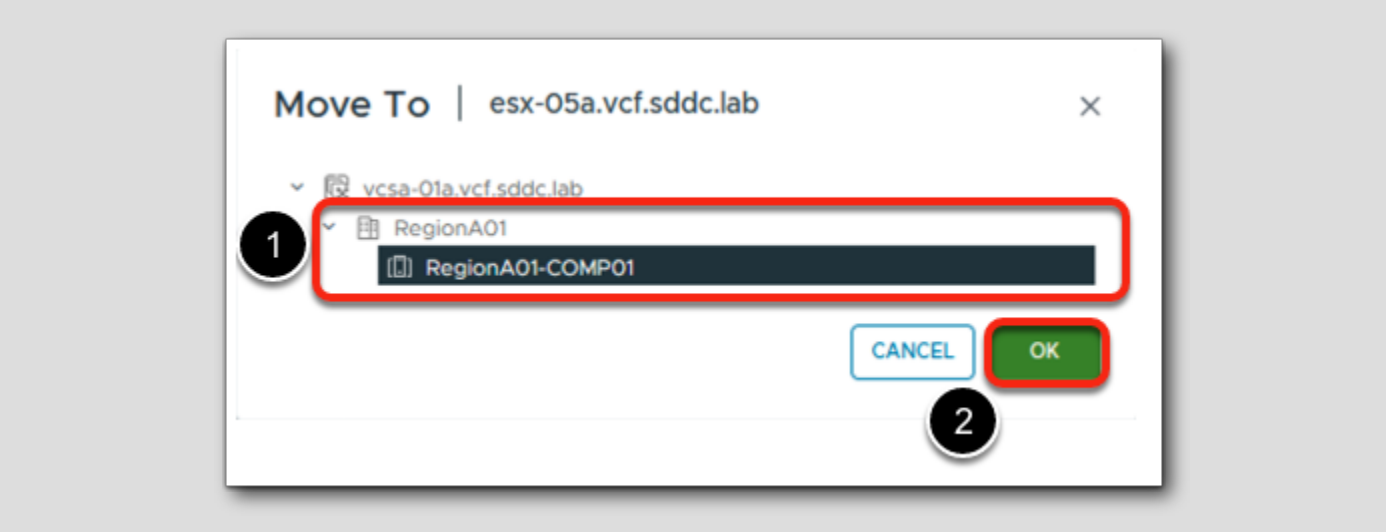


We are now going to add the **esx-05a.vcf.sddc.lab** to the vSAN Cluster. The server has already been configured with the vSAN vmkernel port for networking.

1. Drag and drop **esx-05a.vcf.sddc.lab** into **RegionA01-COMP01** cluster

If the Drag and Drop does not seem to be working for you,

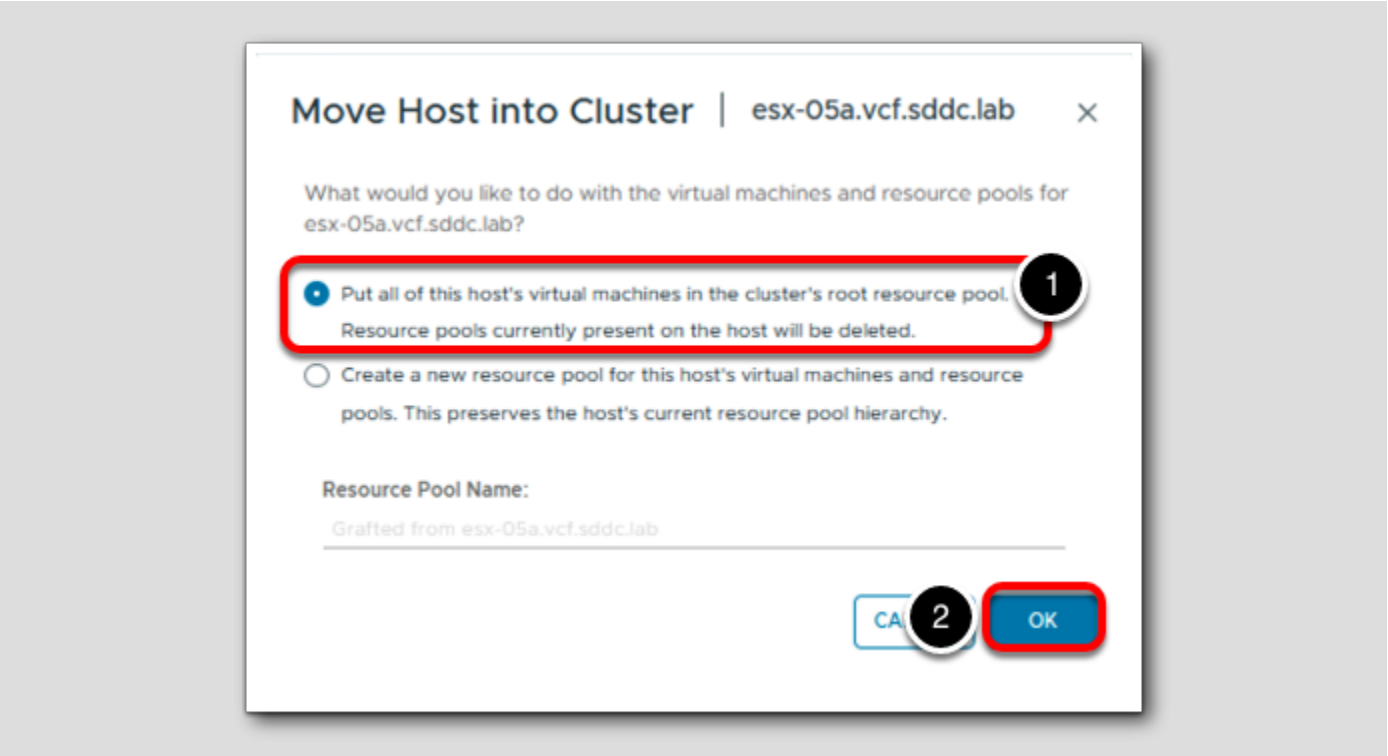
2. Right click the ESXi host called **esx-05a.vcf.sddc.lab** and select Move to ….



1. Expand **RegionA01** and select **RegionA01-COMP01**
2. Click **OK**

Move Host into Cluster

[32]

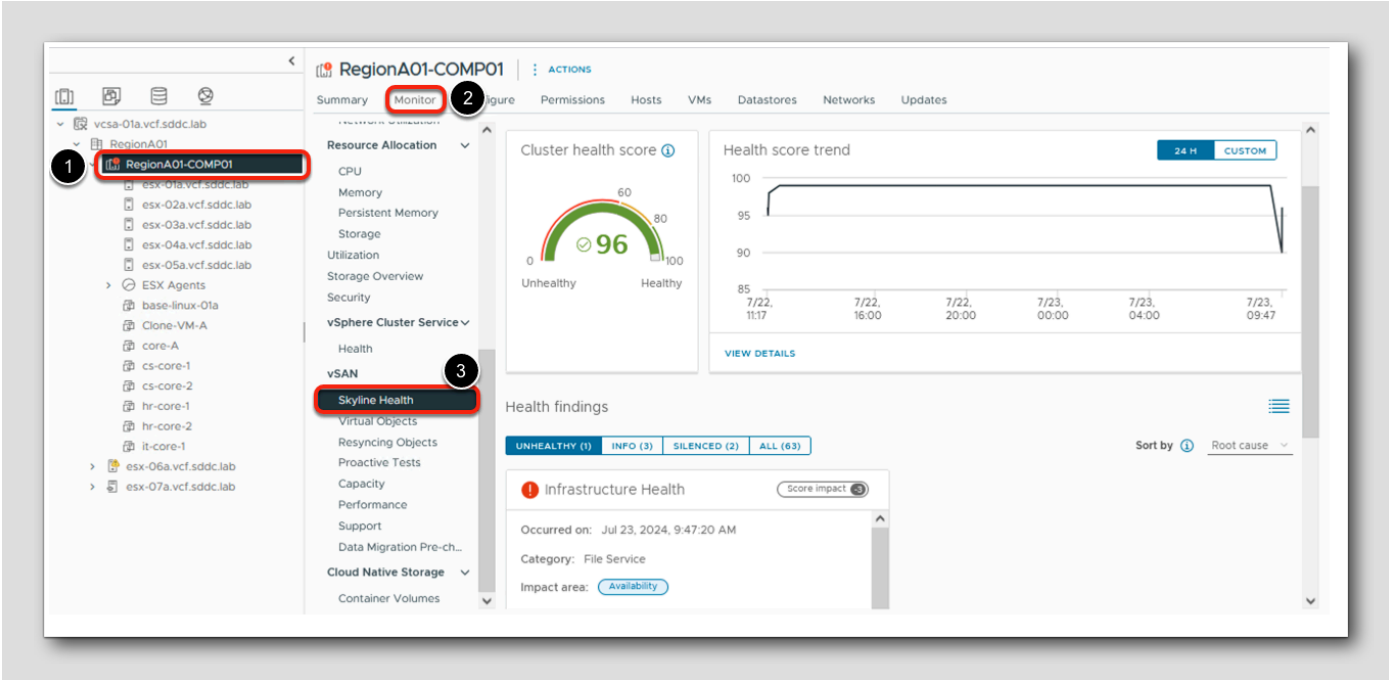


Confirming that we want to move host into the vSAN Cluster and resource pool.

1. Select **Put all of this host's virtual machines in the clusters.....**
2. Click **OK**

Checking Skyline Health

[33]



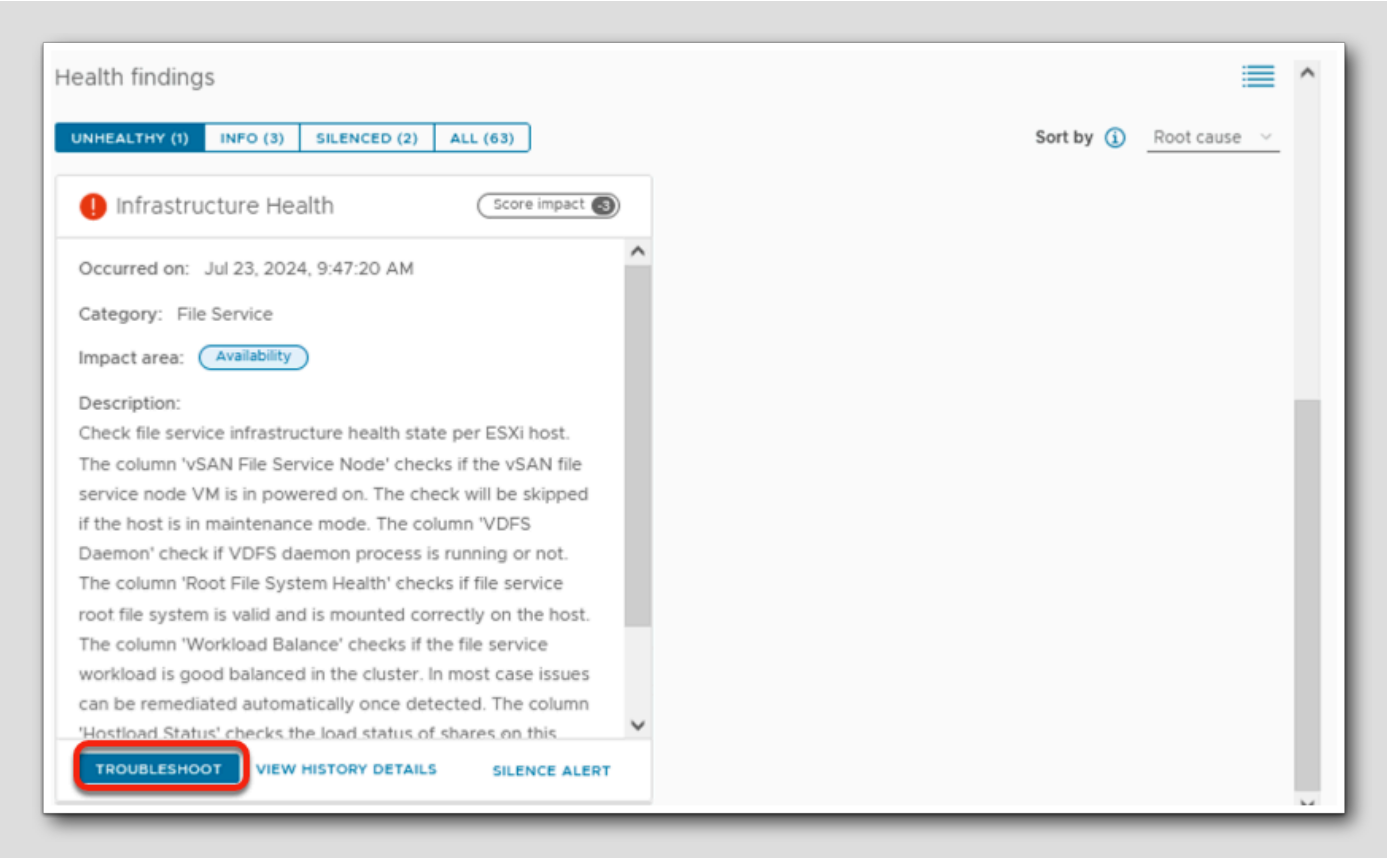
Let's check Skyline Health to see if there are any current issues with the vSAN cluster. You can use vSAN Skyline Health to monitor the status of cluster components, diagnose issues, and troubleshoot problems. The health findings cover hardware compatibility, network configuration and operation, advanced vSAN configuration options, storage device health, and virtual machine objects.

1. Click on the **RegionA01-COMP01** cluster
2. Click on the **Monitor** tab
3. Click on **vSAN > Skyline Health**

We now have Cluster Health Score and health score trend. Let's dig into why we have a score in the range of 94-96 out of 100.

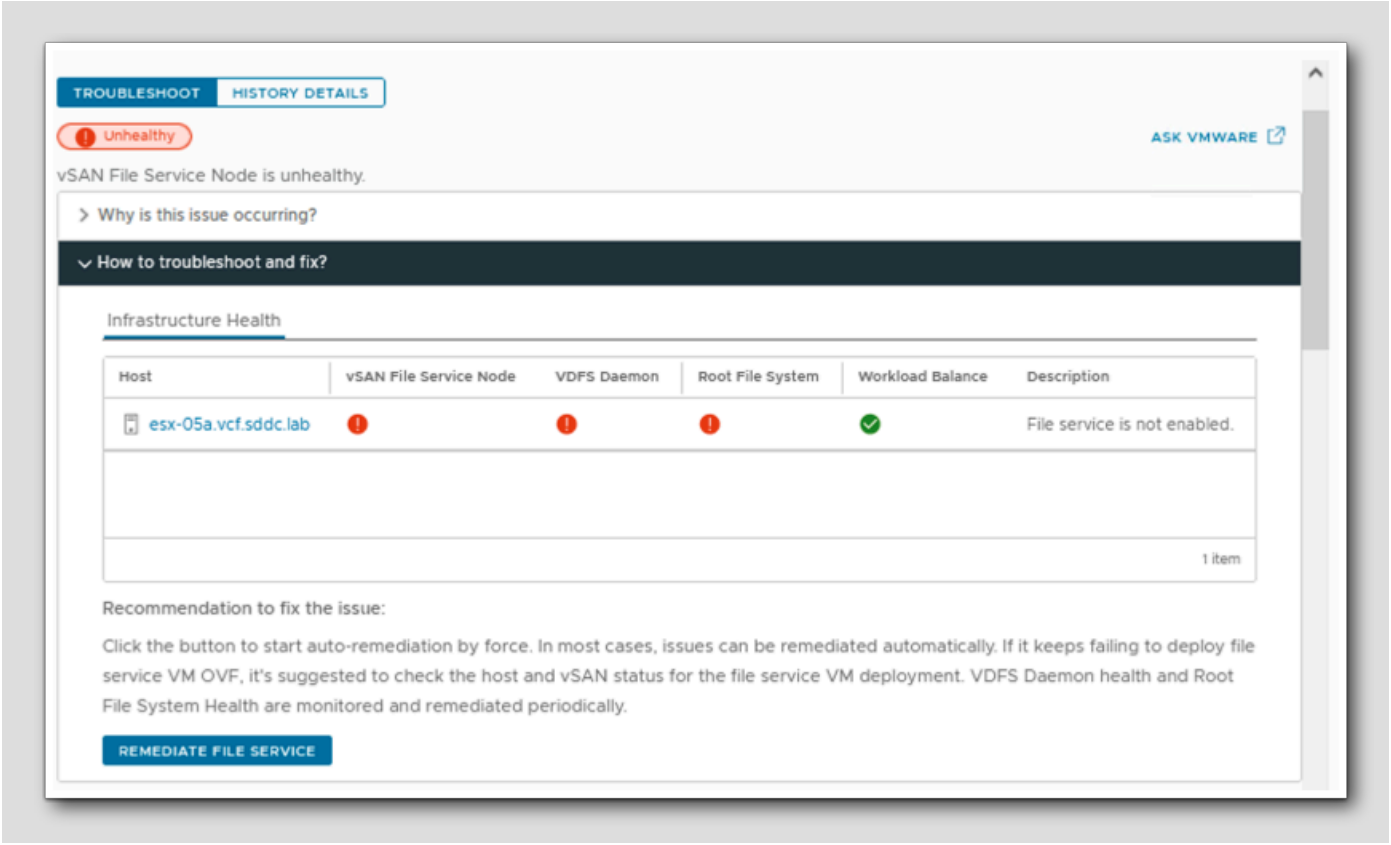
Checking Skyline Health

[34]



One of the first issues we see is that not all hosts have file services properly running. This is because the file services VM is in the process of being deployed on the **esx-05a.vcf.sddc.lab**. Let's go ahead and click **TROUBLESHOOT**.

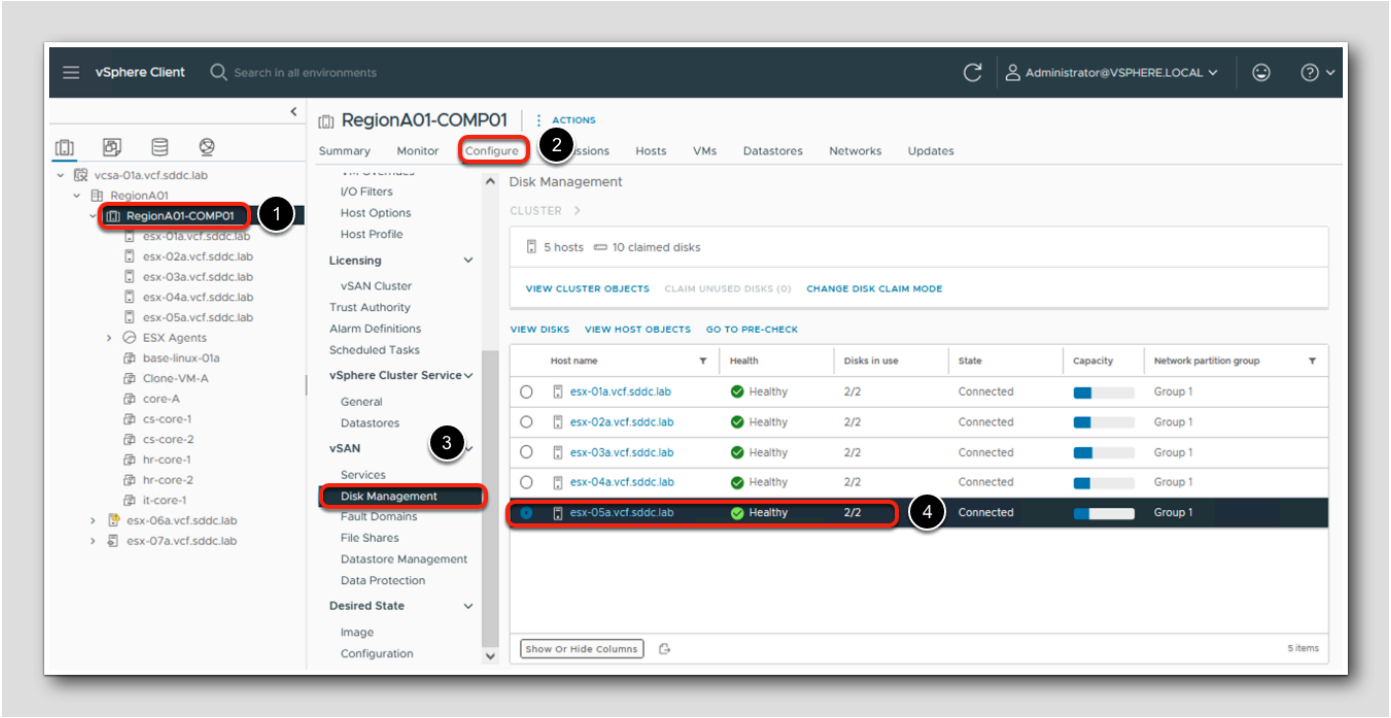
Troubleshooting File Services



4. Here, we can see that file services is not currently configured on the newest host that we added to the vSAN cluster. This is because the file services VM is currently being deployed. As stated in the Skyline recommendation, this issue can be remediated automatically and will be once the file servies VM is up and running.

Confirm Additional vSAN Capacity

[36]



Now that we have added an additional host to the vSAN datastore, let's confirm the additional drives are in use. With Express Storage Architecture, we no longer use disk groups and instead use the concept of a disk pool which consists of all of the drives contributing capacity to vSAN. In addition, vSAN ESA does allow for managed disk claim, which can automatically claim vSAN ESA-compatible drives. Since this is a nested environment, managed disk claim is not available, however we were able to recreate the experience in this lab. Let's confirm that **esx-05a.vcf.sddc.lab's** drives were claimed by the vSAN ESA datastore.

1. Select vSAN Cluster called **RegionA01-COMP01**
2. Select **Configure**
3. Select **vSAN > Disk Management**
4. Select **esx-05a.vcf.sddc.lab** (do not click host name hyperlink directly, click radio button beside the name

Here, we can see that the two drives from **esx-05a.vcf.sddc.lab** were added to the vSAN datastore and are currently in use.

Advanced Storage Based Policy Management

[37]

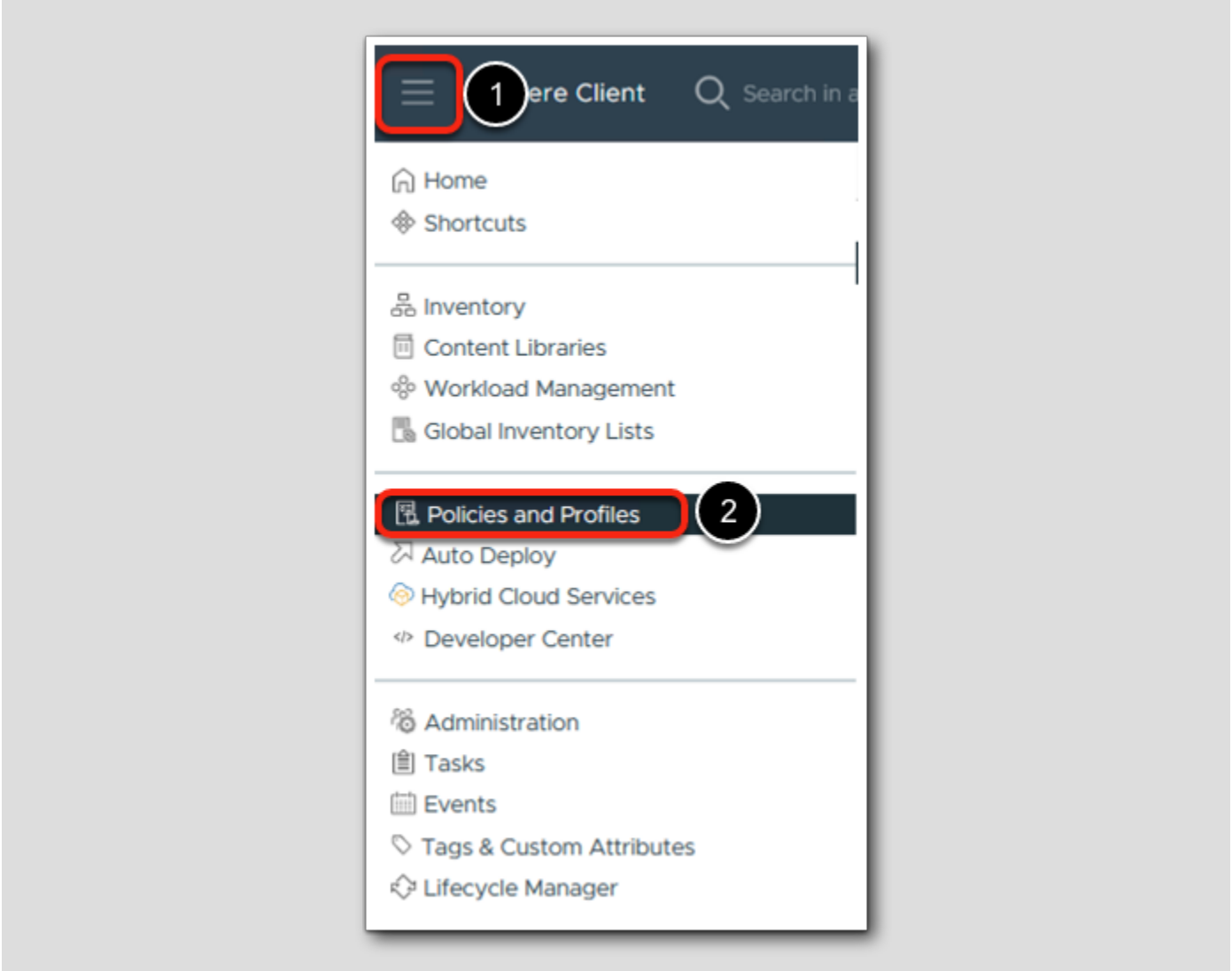
vSAN Express Storage Architecture provided the ability to change how compression is implemented. Compression now takes place in the upper layers of vSAN as it receives new writes (which means replica traffic is always compressed). In addition, compression is now toggled by storage policy and is enabled by default.

There may be times when compression needs to be disabled, such as when a VM is running an application that performs its own compression (e.g. databases). In this exercise, we will clone an existing storage policy, disable compression, then apply that policy to an

existing VM.

Clone a VM Storage Policy (Compression Disabled)

[38]

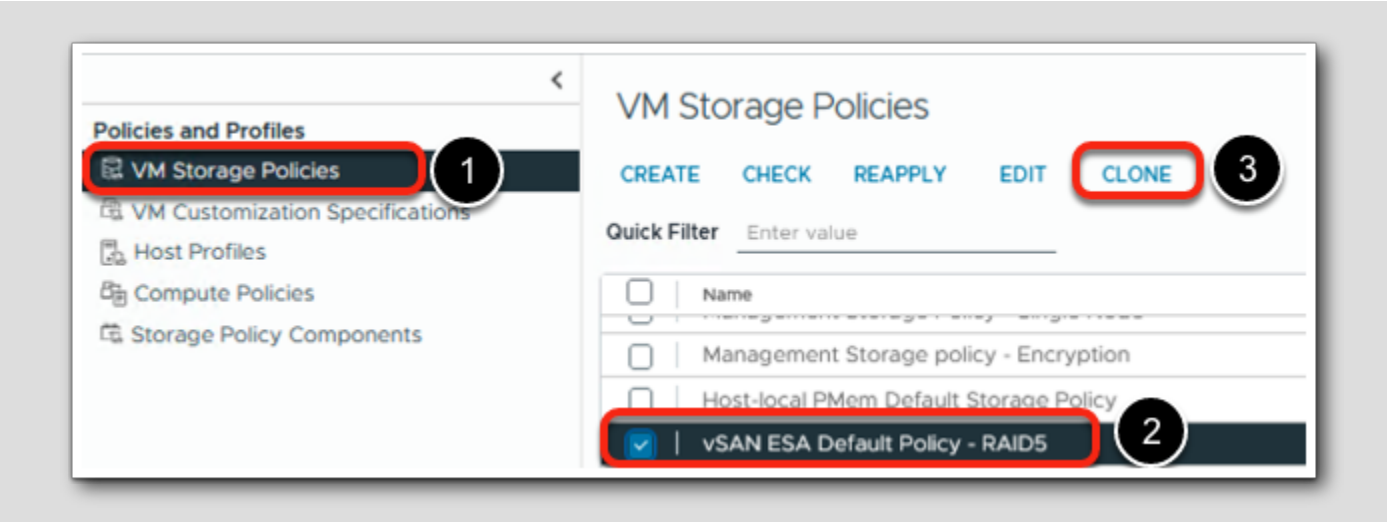


First, we need to clone an VM Storage Policy and modify that policy to disable compression.

1. From the **Menu** page of the vSphere Client
2. Select **Policies and Profiles**

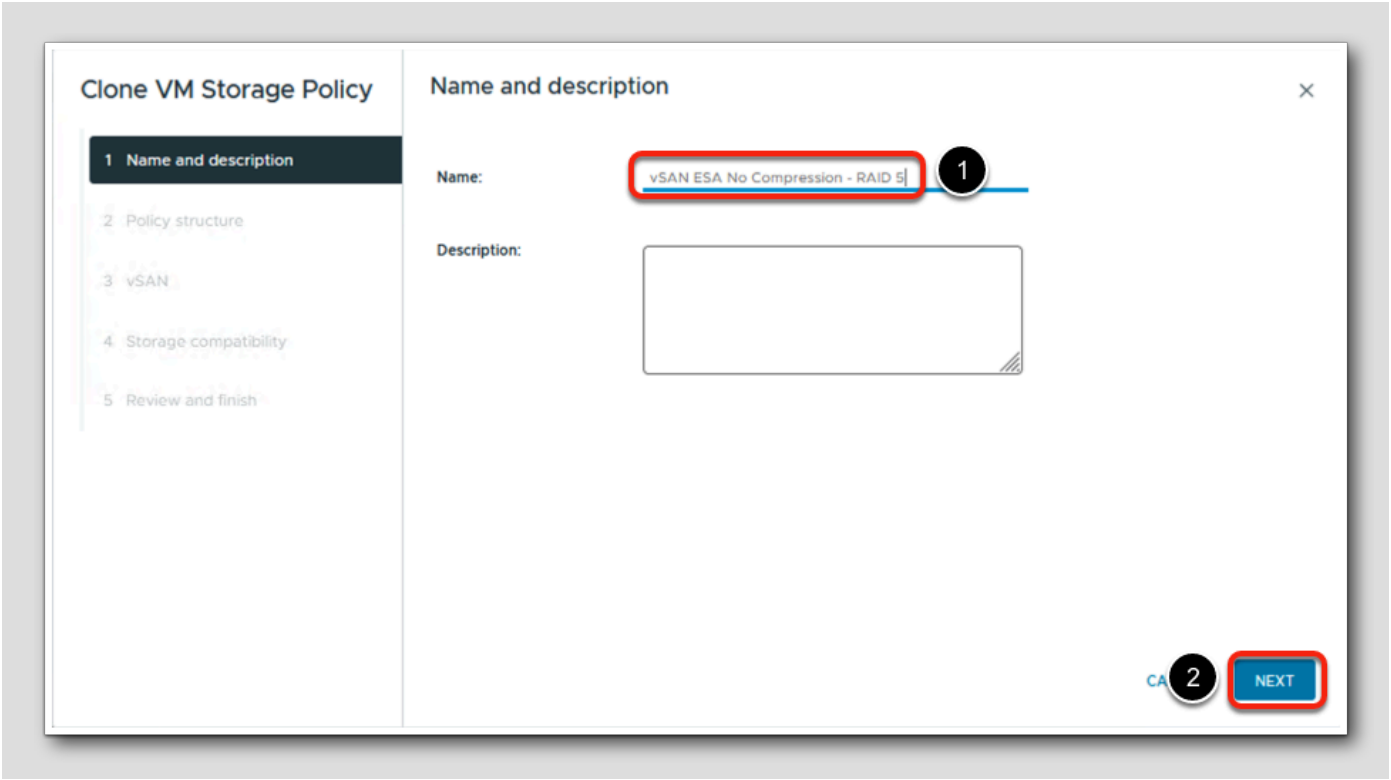
Clone a VM Storage Policy (Compression Disabled)

[39]



1. Select **VM Storage Policies**
2. Scroll down and check the box next to **vSAN ESA Default Policy - RAID5**
3. Click **CLONE**

Note: If you do not see the **CLONE** option, that means you have multiple storage policies selected. Be sure to uncheck any other policies so that **vSAN ESA Default Policy - RAID5** is the only one selected.



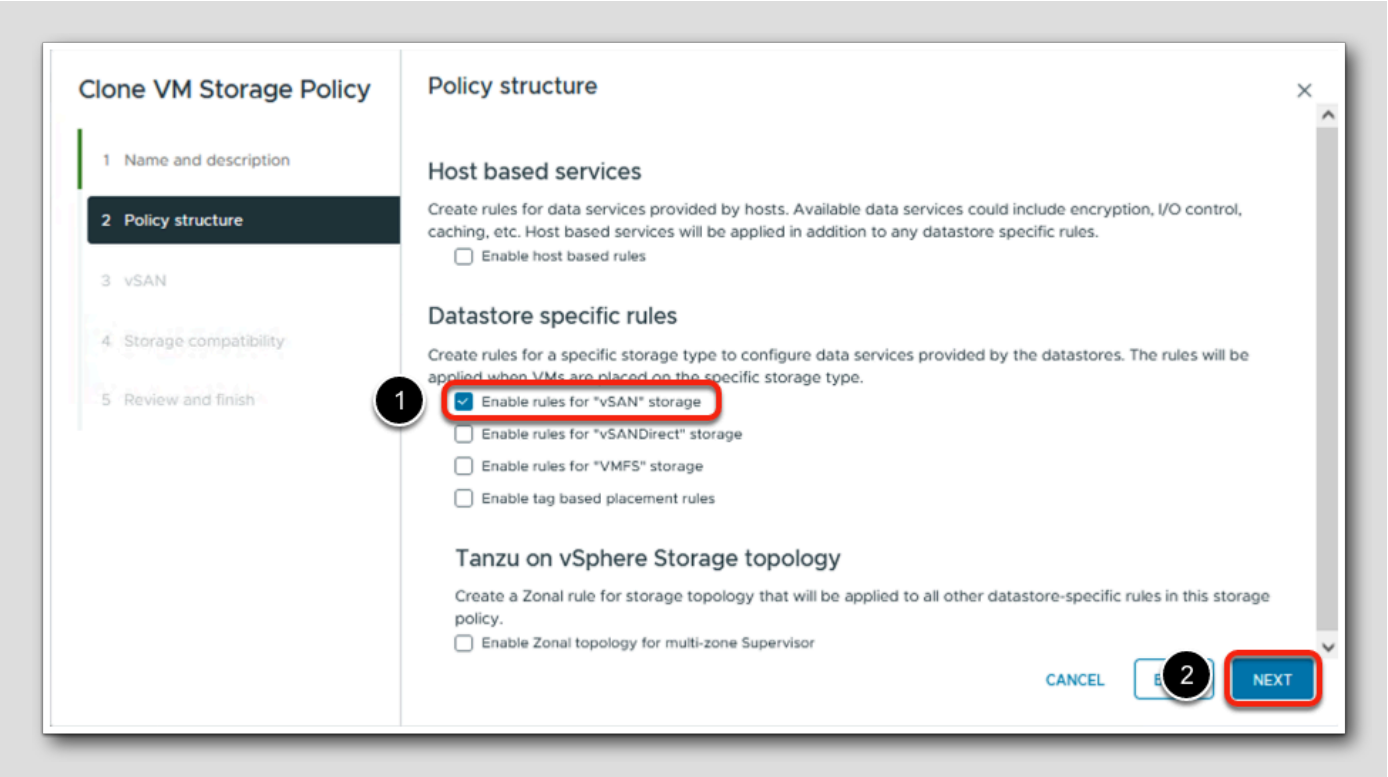
1. Create a new VM Storage Policy using the following name :

```
vSAN ESA No Compression - RAID 5
```

2. Click NEXT

Clone a VM Storage Policy (Compression Disabled)

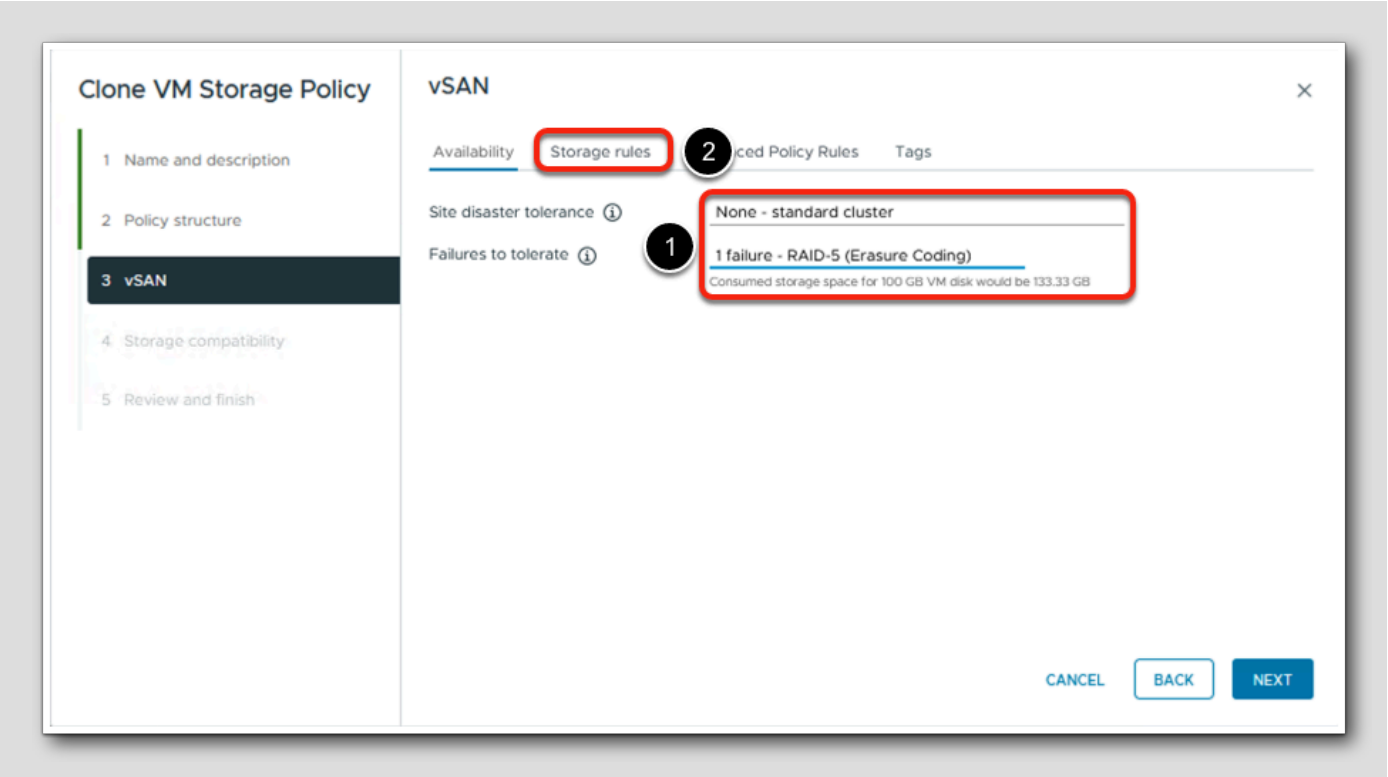
[40]



1. Make sure **Enable rules for "vSAN" storage** is checked
2. Click **NEXT**

Clone a VM Storage Policy (Compression Disabled)

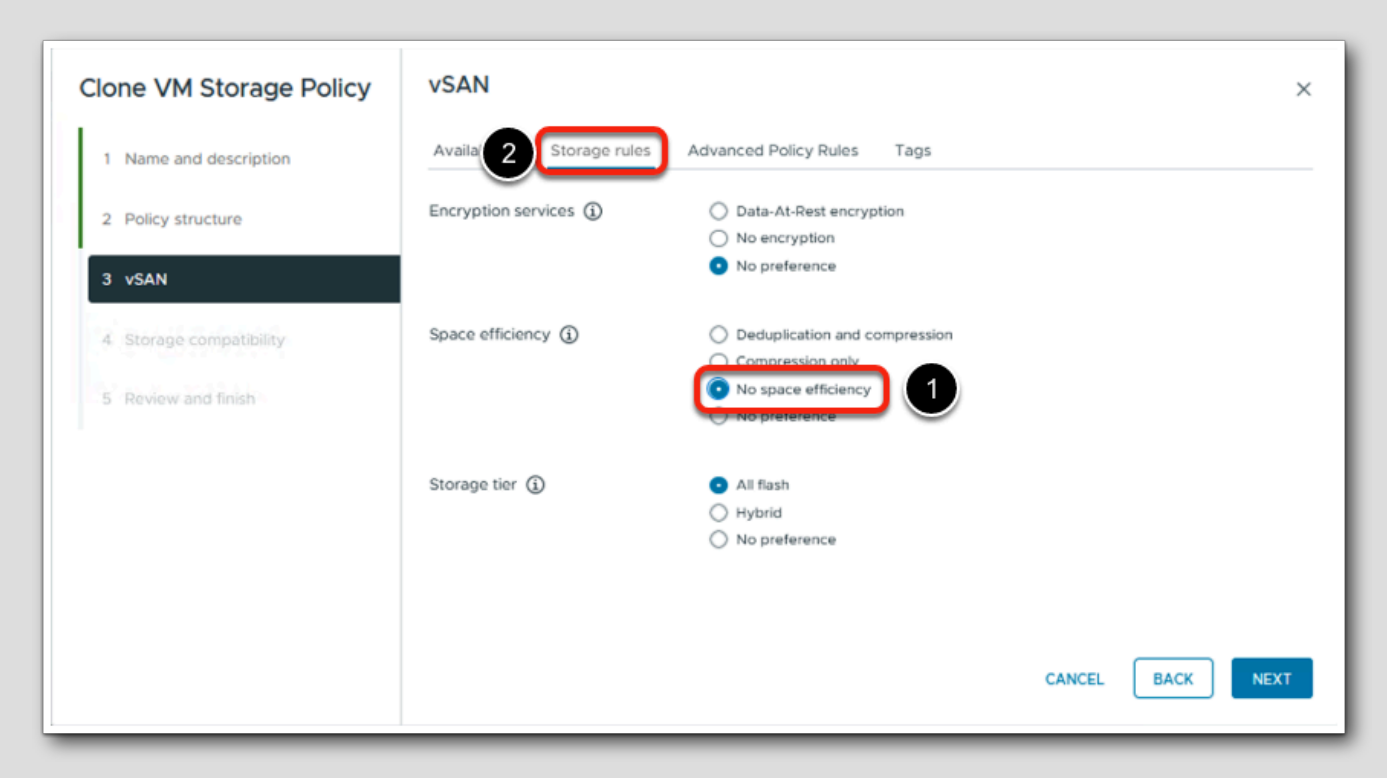
[41]



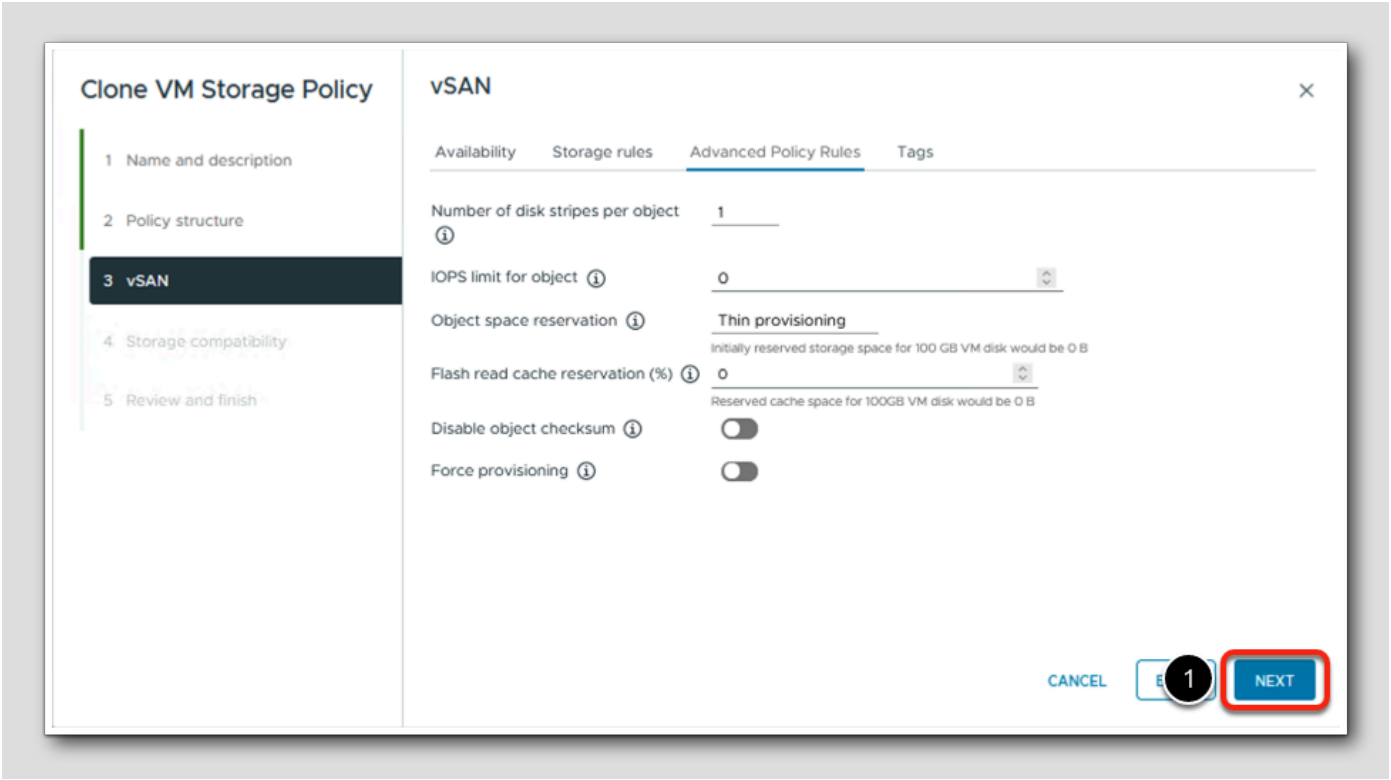
1. In the **Availability** tab, Select the following options :

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

2. Click **Storage rules**



1. In the **Storage rules** tab, Select **No space efficiency** for the Storage tier
2. Select **Advanced Policy Rules** tab

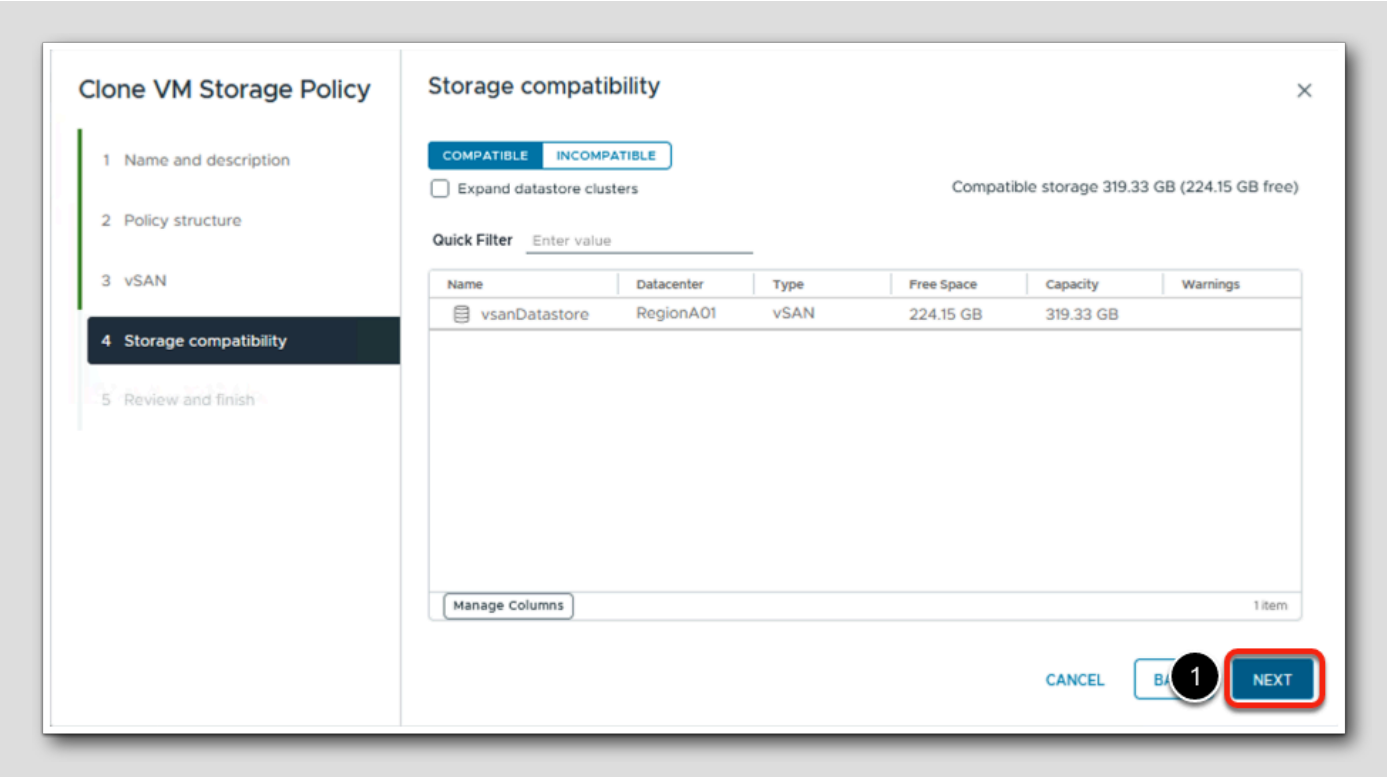


Review the options that are available here, but leave at the default settings.

1. Click NEXT

Clone a VM Storage Policy (Compression Disabled)

[42]

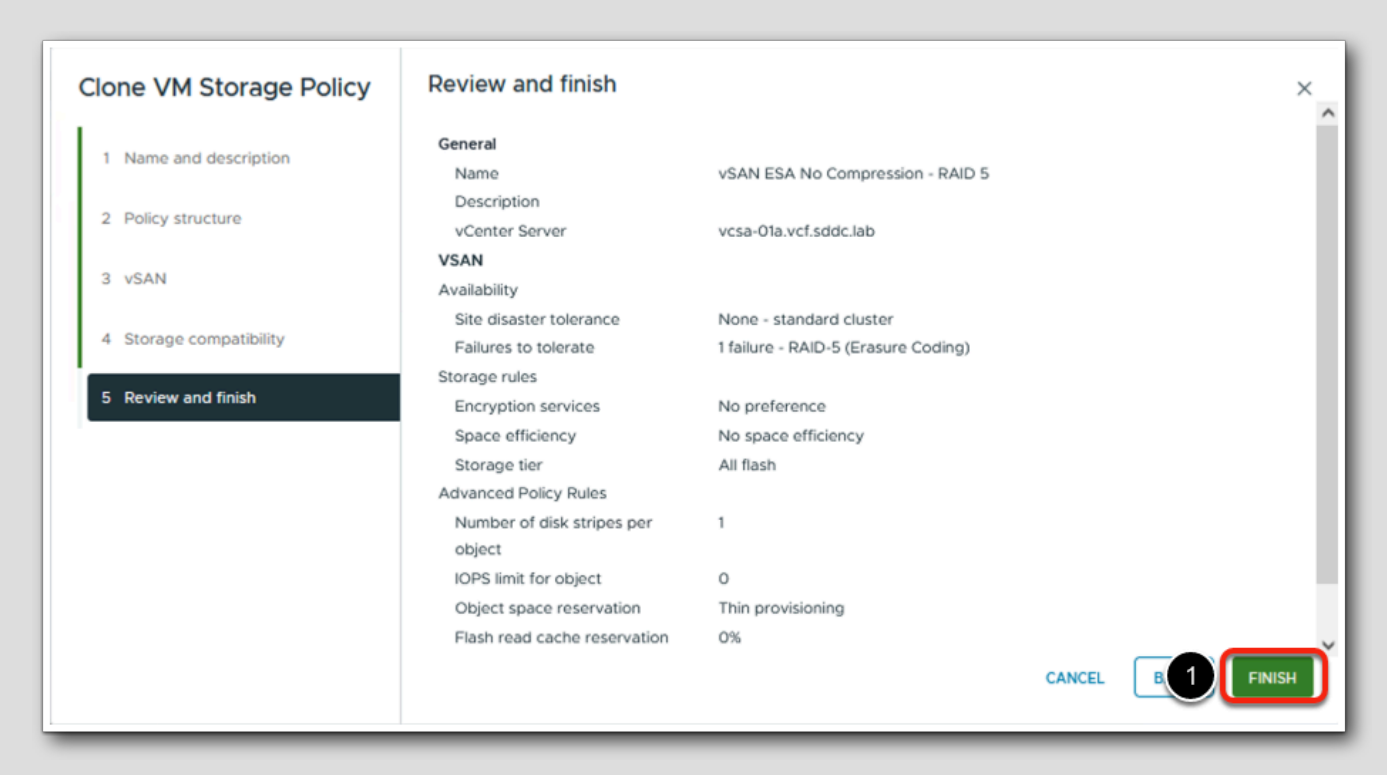


Verify that the **vsanDatastore** is compatible against the VM Storage Policy.

1. Click **NEXT**

Clone a VM Storage Policy (Compression Disabled)

[43]

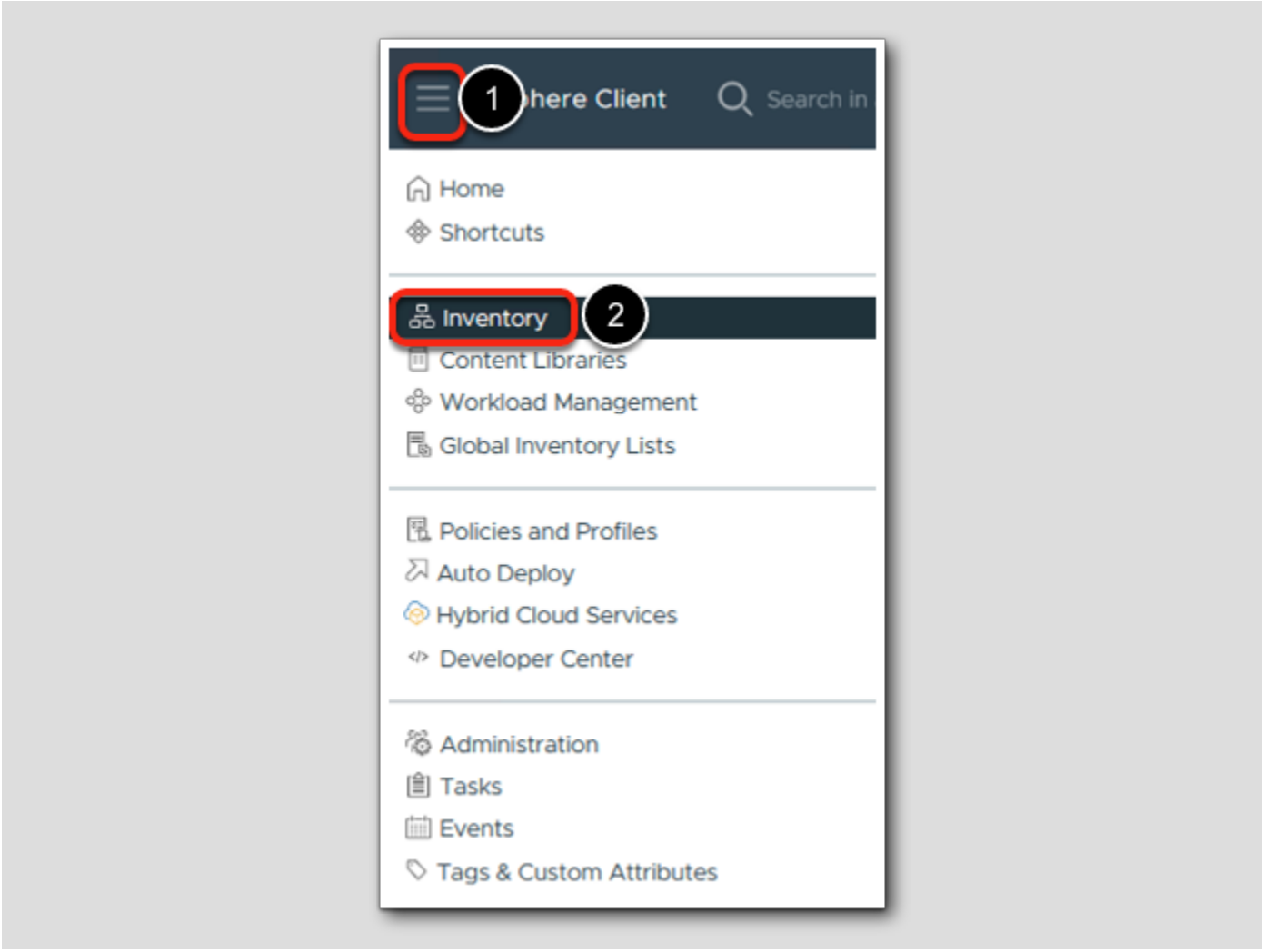


Here we can see the rules that make up our VM Storage Policy.

1. Review the settings and click **FINISH**

Assign VM Storage Policy to an existing VM

[44]

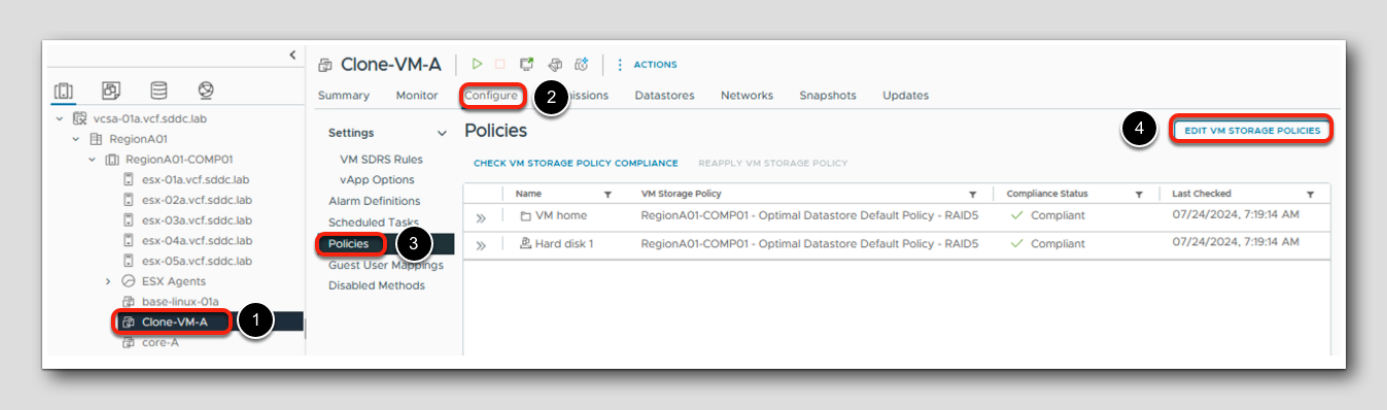


Now that we have created a new VM Storage Policy , let's assign that policy to an existing VM on the vSAN Datastore.

1. Select **Menu** on the vSphere Client
2. Select **Inventory**

Assign VM Storage Policy to an existing VM

[45]



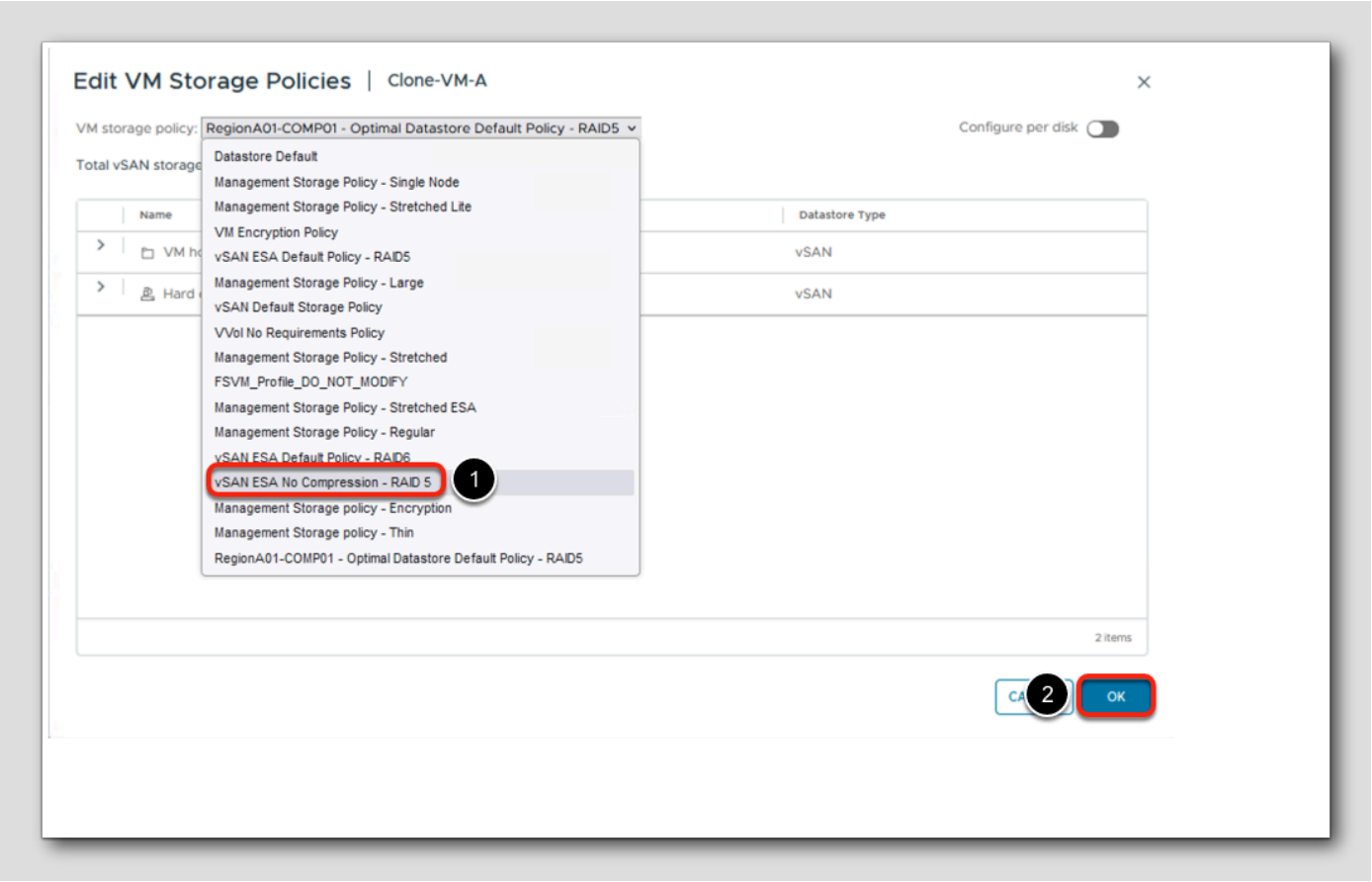
1. Select the VM called **Clone-VM-A**
2. Select **Configure**
3. Select **Policies**

Here we can see that the **RegionA01-COMP01 - Optimal Datastore Default Policy - RAID 5** is assigned to this VM.

4. Select **EDIT VM STORAGE POLICIES**

Assign VM Storage Policy to an existing VM

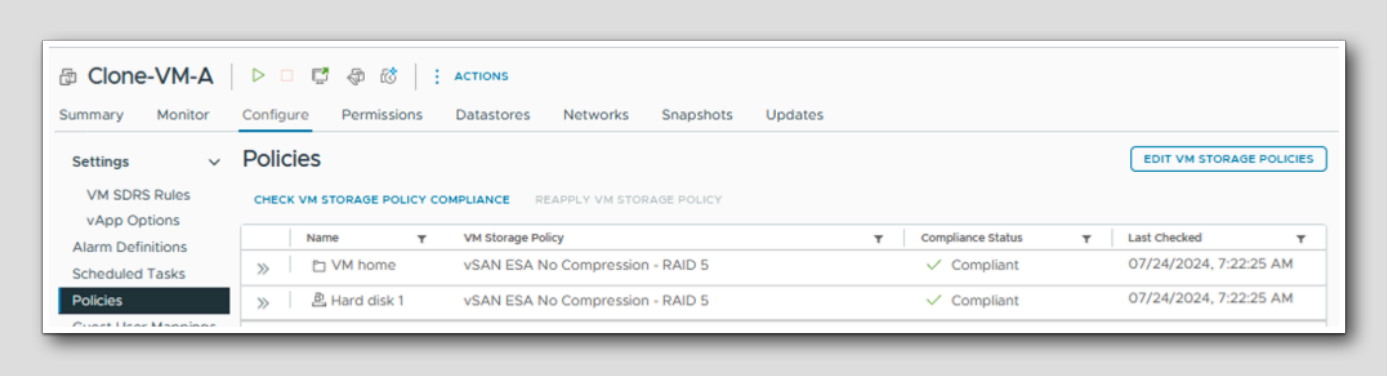
[46]



1. Change the VM storage Policy from the dropdown list to **vSAN ESA No Compression - RAID 5.**
2. Click **OK**

Assign VM Storage Policy to an existing VM

[47]



Verify that the VM Storage Policy has been changed and that the VM is compliant against the new storage Policy. You might have to hit the refresh button to see the change.

Reserved Capacity

[48]

We now have the ability to control the amount of capacity that is reserved for both rebuild operations and transient operations such as temporary capacity need to do policy change on an object.

By default, the Capacity Reserve feature is disabled, meaning all vSAN capacity is available for workloads. You can enable capacity reservations for internal cluster operations and host failure rebuilds. Reservations are soft-thresholds designed to prevent user-driven provisioning activity from interfering with internal operations, such as data rebuilds, rebalancing activity, or policy re-configurations. The capacity required to restore a host failure matches the total capacity of the largest host in the cluster and minimum of 4 hosts are required.

By enabling reserve capacity in advanced, vSAN prevents you from using the space to create workloads and intends to save the capacity available in a cluster.

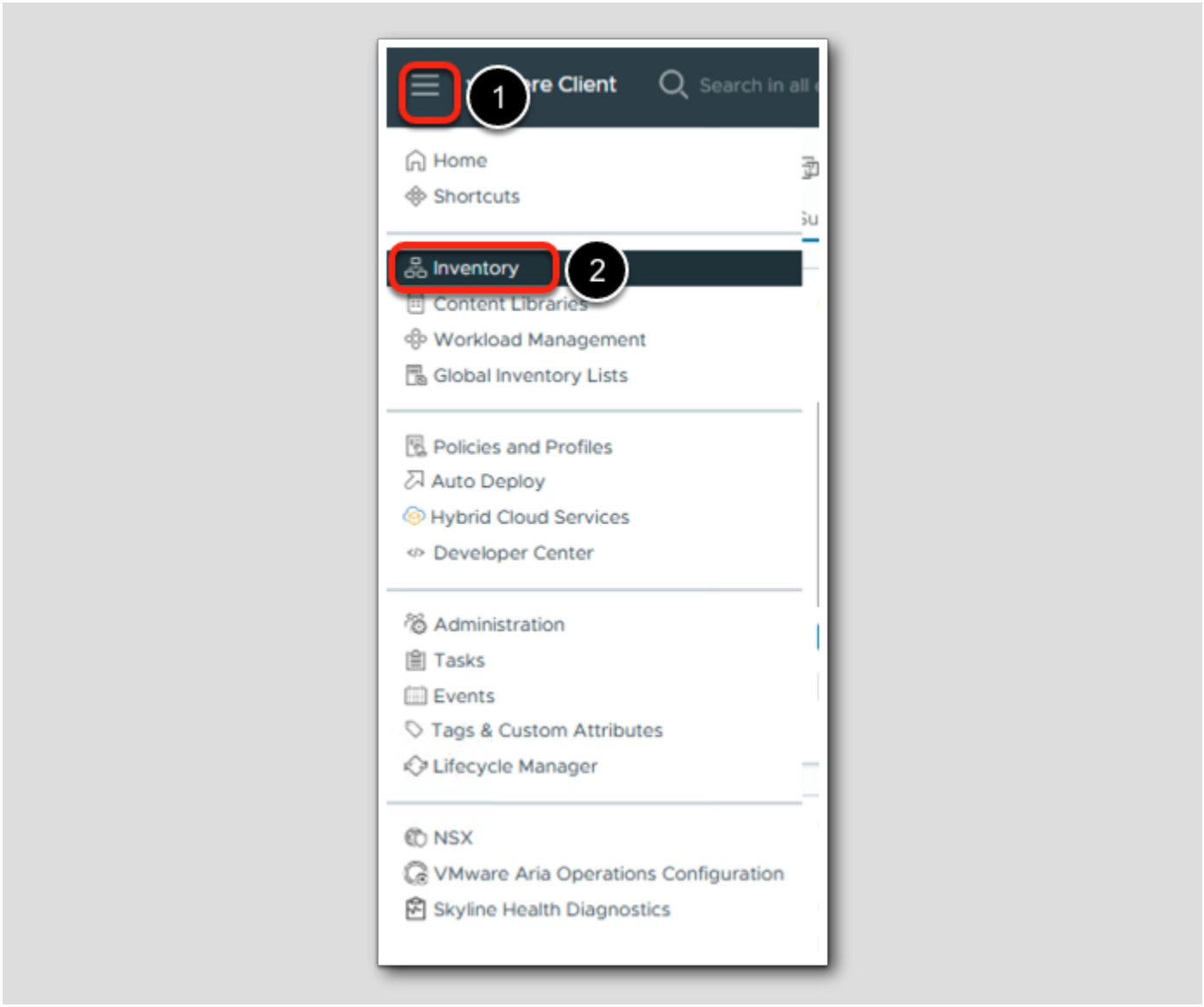
If there is enough free space in the vSAN cluster, you can enable the operations reserve and/or the host rebuild reserve.

- Operations Reserve - Reserved space in the cluster for vSAN internal operations.
- Host Rebuild Reserve - Reserved space for vSAN to be able to repair in case of a single host failure.

The reserved capacity is not supported on a stretched cluster, cluster with fault domains and nested fault domains, ROBO cluster, or the number of hosts in the cluster is less than four.

Configure Reserved Capacity

[49]

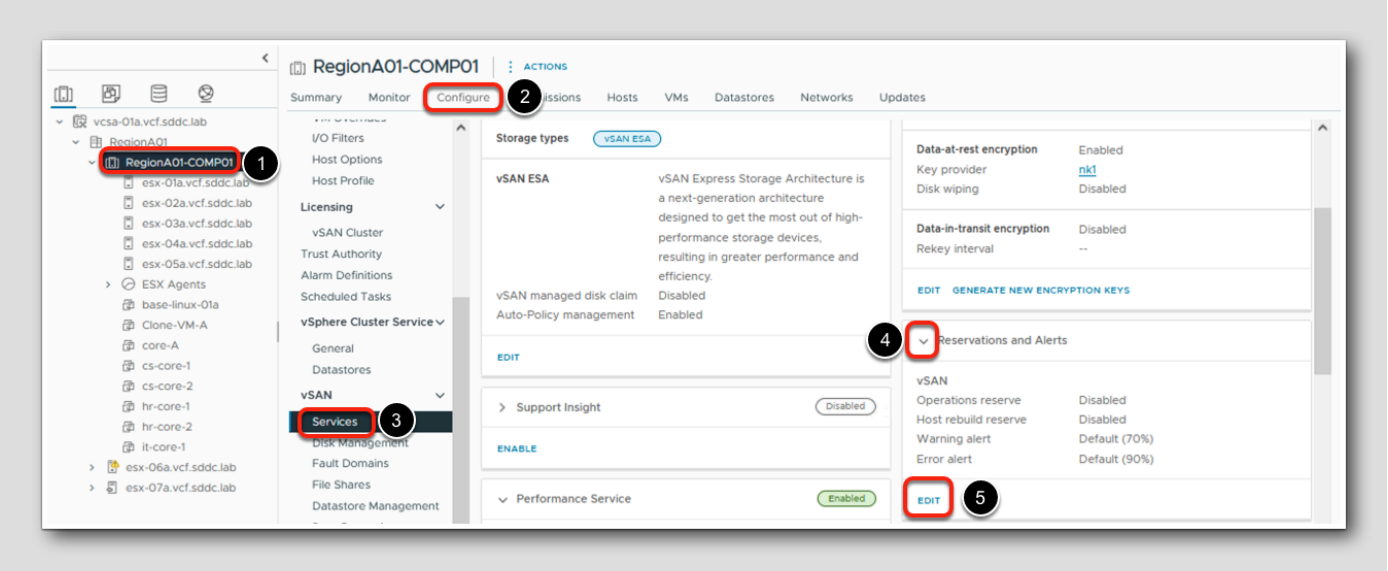


Now that we have 4 hosts in the cluster, we can start configuring the Reserve Capacity.

1. Select **Menu**
2. Select **Inventory**

Configure Reserve Capacity

[50]

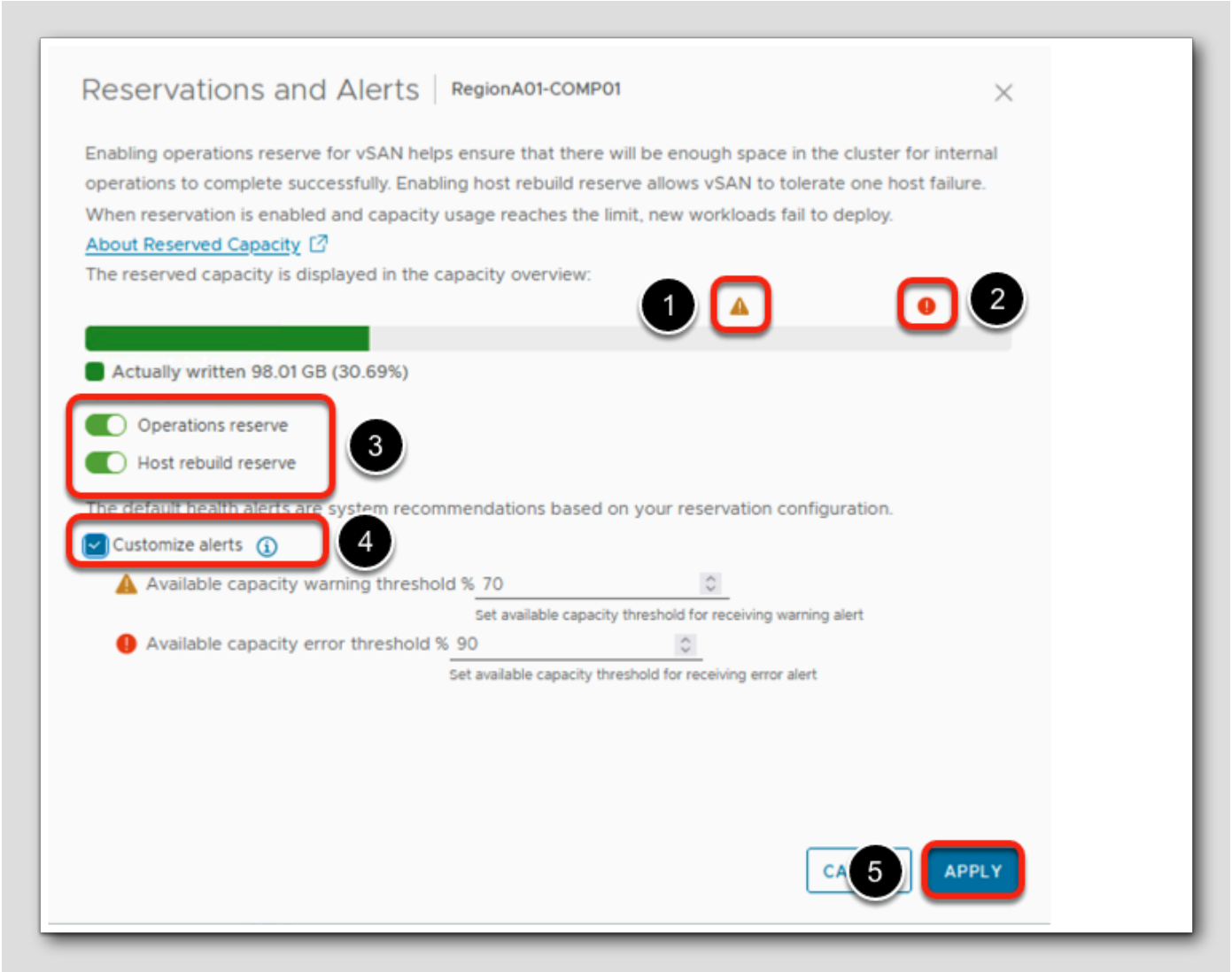


Once we edit the Enable Capacity reserve, you will be shown how much of the total vSAN datastore capacity (by default) is allocated to each reserve.

1. Navigate to the vSAN Cluster, **RegionA01-COMP01**
2. Select **Configure**
3. Select **vSAN > Services**
4. Scroll and expand **Reservations and Alerts**
5. Under the **Reservations and Alerts**, click **EDIT**

Enable Capacity Reserve

[51]



1. Hover onto the Warning Icon. You will see a warning notifications when the storage reaches 70%
2. Hover onto the Error Icon. You will see an error alert at 90% of storage consumption
3. Toggle on **Operations reserve** and **Host rebuild reserve** to be on
4. Select **Customize alerts**. You can set the warning and error alerts but we will keep it at default
5. Click on **APPLY**

Scale In vSAN environment

[52]

Here we will show you how to scale in your vSAN environment.

Since we already know that the minimum number of hosts to form a vSAN cluster is 3 hosts, there are a number of considerations when we want to scale down a vSAN Cluster.

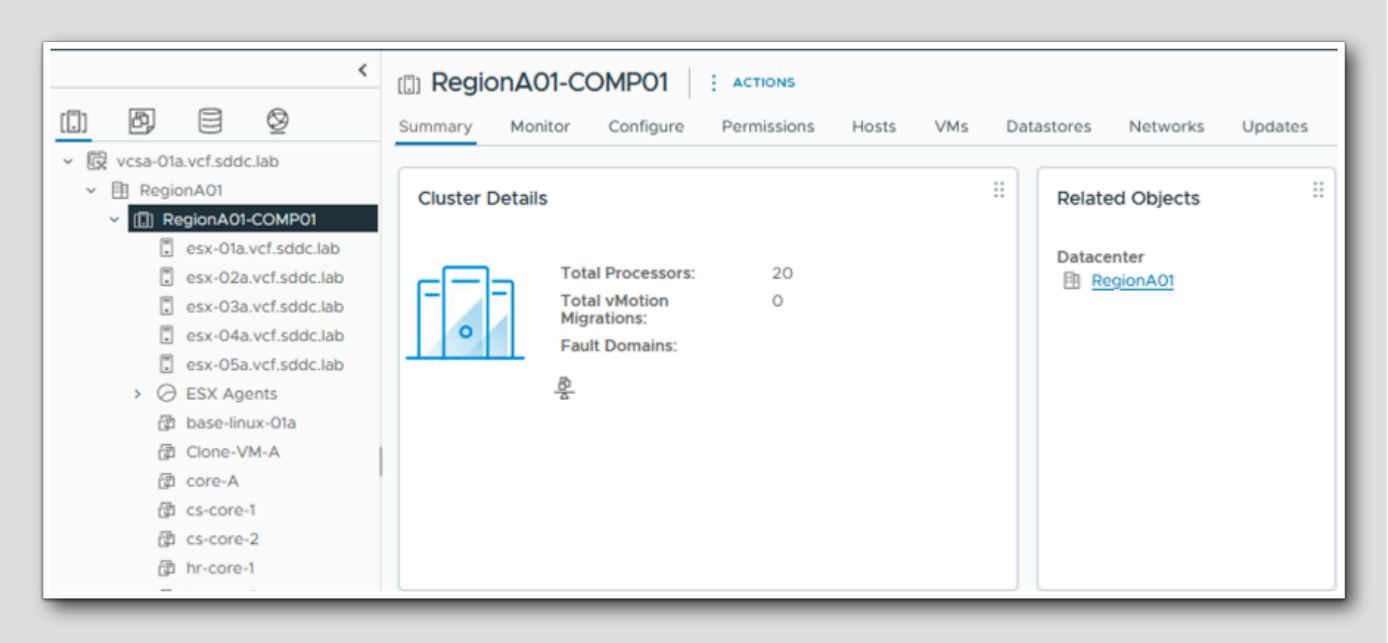
- Do I have enough Compute and storage capacity ?
- Will my VM Storage policies remain in a compliant state ?

Here is a high level overview of the steps required to scale down a vSAN Datastore.

- Run Data Migration Pre-Check to see which VMs will be impacted by removing a host.
- Remove vSAN disks from the Hosts that you will be removing from the vSAN Cluster
- Put the Hosts into Maintenance Mode and remove from the Cluster

vSAN environment review

[53]

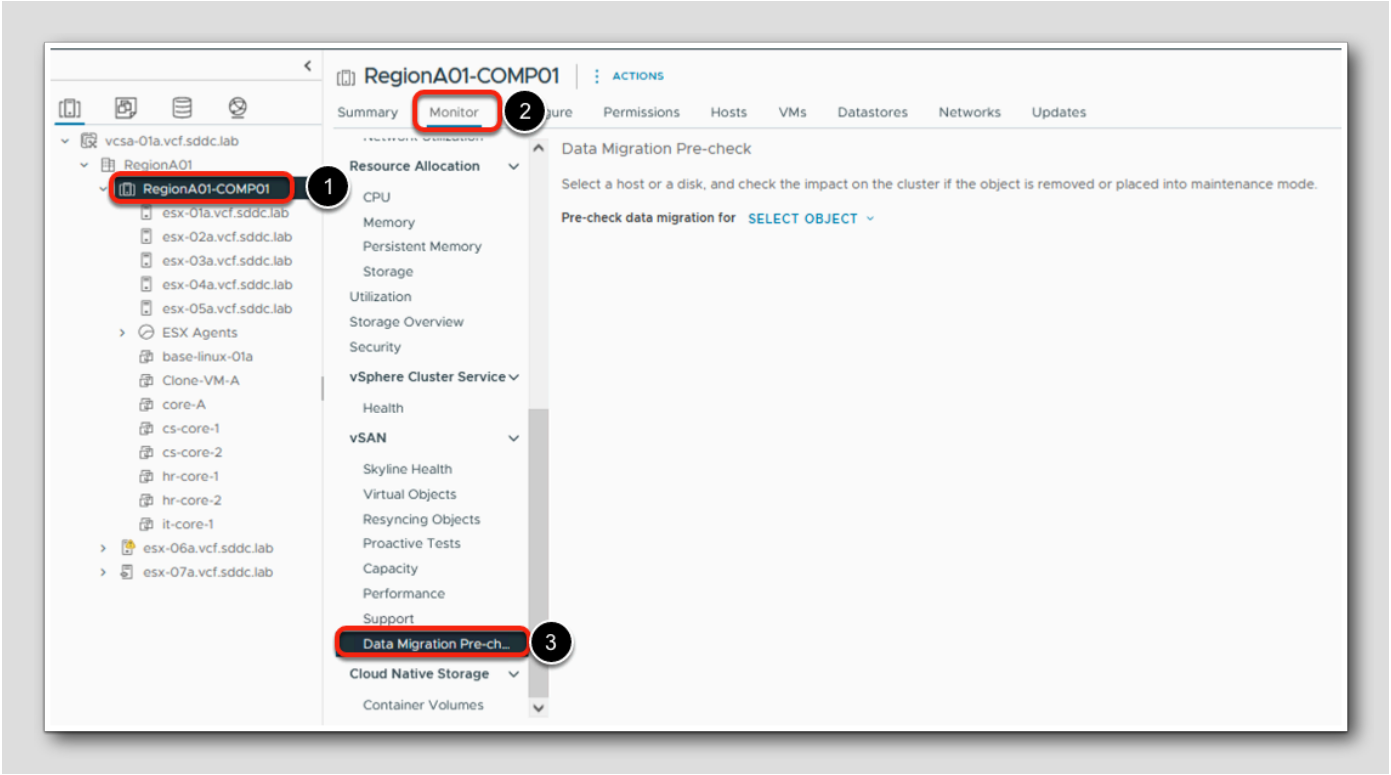


Let's review our current vSAN Cluster environment.

We have 5 ESXi hosts that make up out vSAN Cluster.

Run a Data Migration Pre-Check

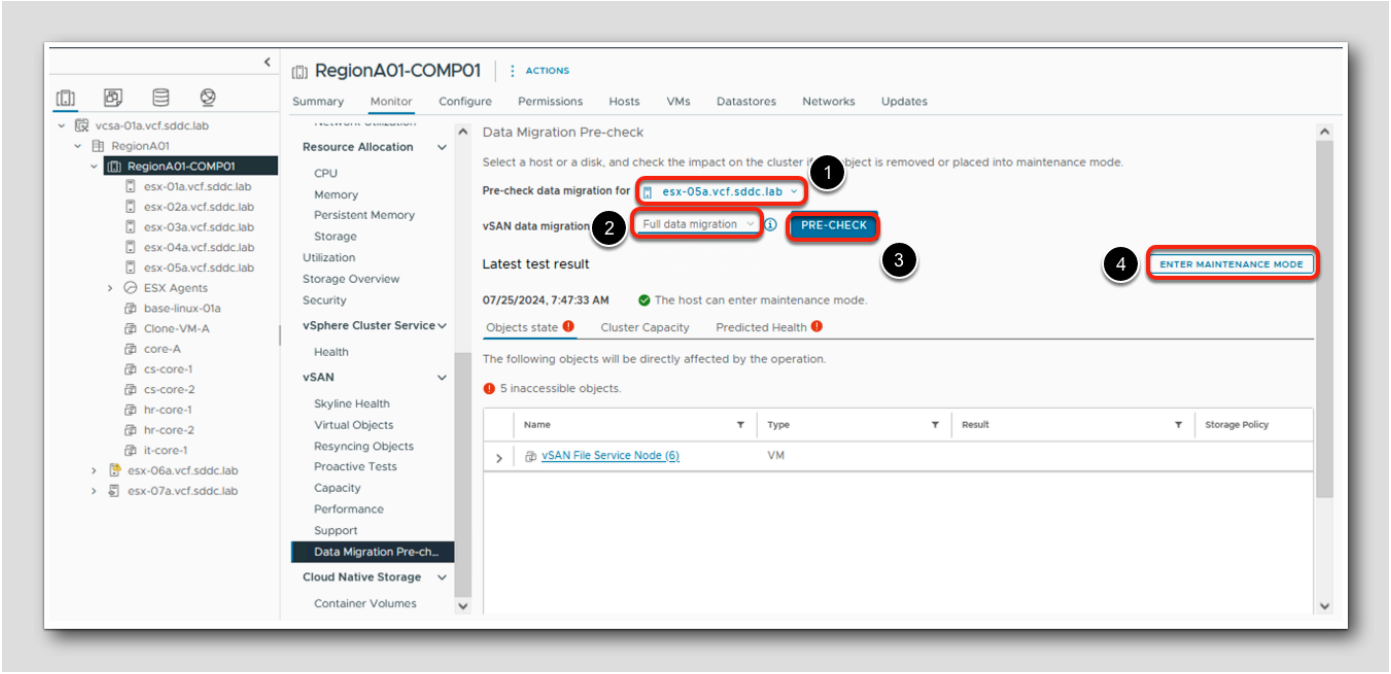
[54]



1. Select the **RegionA01-COMP01** cluster
2. Select **Monitor**
3. Scroll down and select **vSAN** > **Data Migration Pre-check**

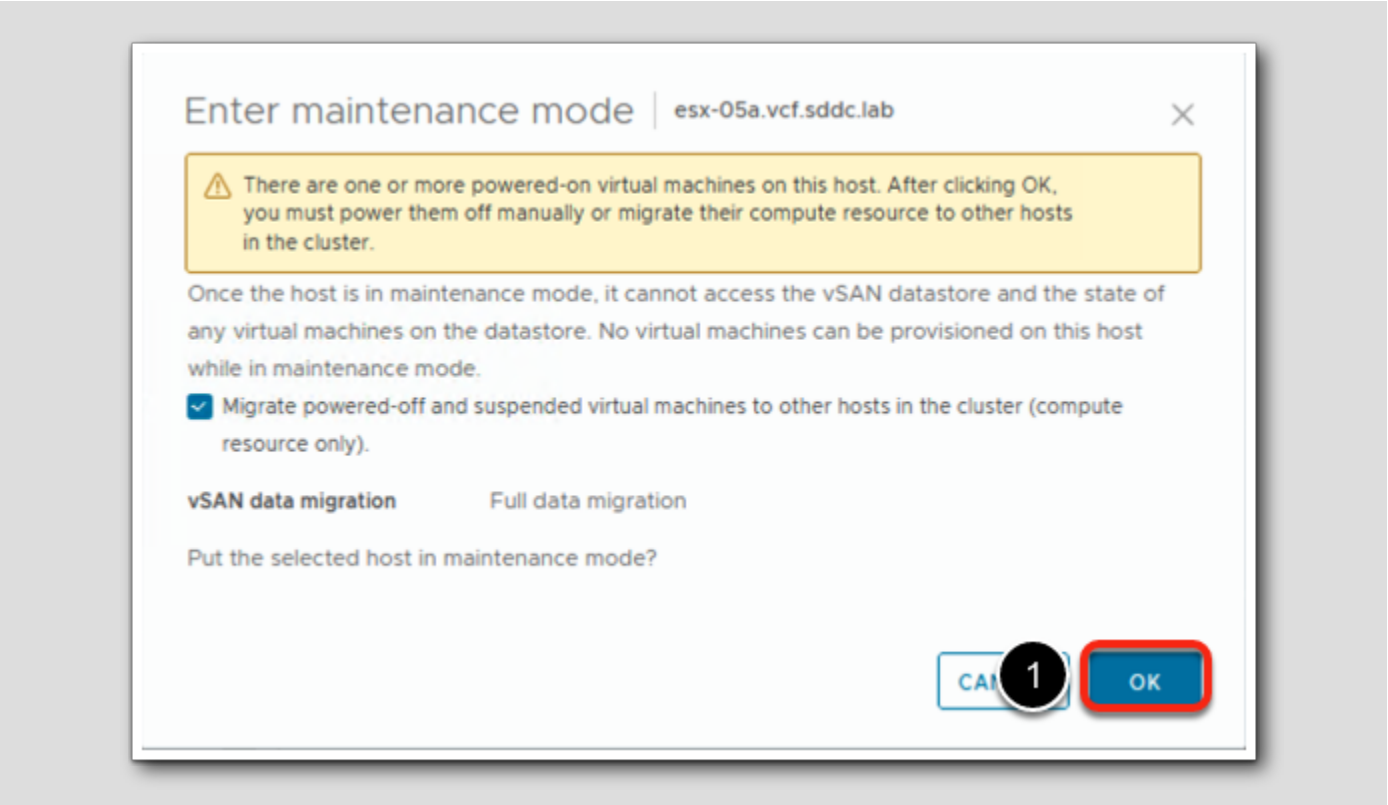
Run a Data Migration Pre-Check

[55]



1. Next to **Pre-check data migration for**, select **esx-05a.vcf.sddc.lab**
2. Next to **vSAN data migration**, select **Full data migration**
3. Click **PRE-CHECK**
    a. Here, we see that the vSAN File Service VM running on **esx-05a.vcf.sddc.lab** is the only VM that would be impacted. Once we put the host in maintenance mode and remove it from the cluster, that VM will be deleted since it's no longer needed.
4. Click **ENTER MAINTENANCE MODE**

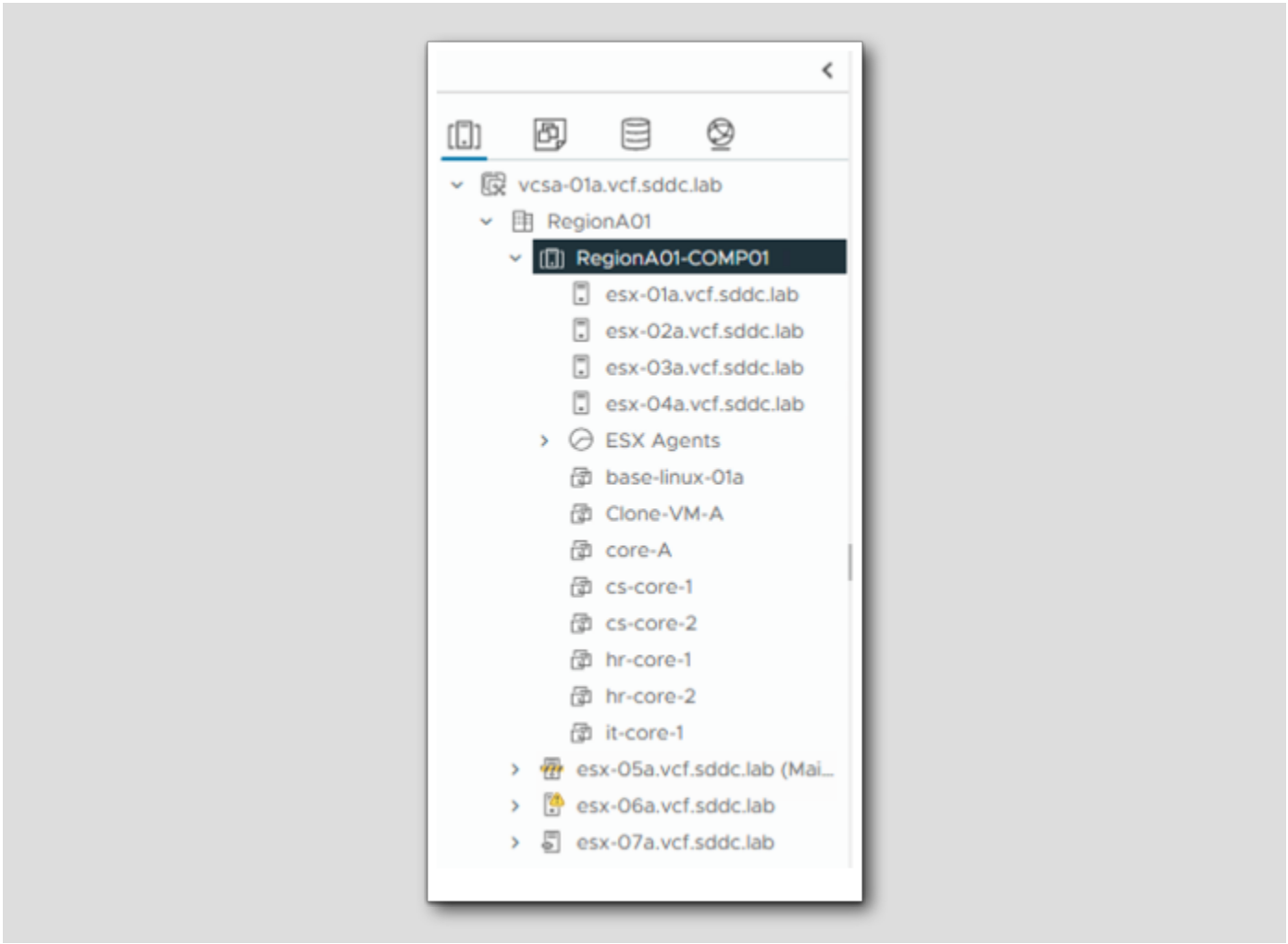
Place Host in Maintenance Mode



1. Leave everything by default and click **OK**

Move Host out of Cluster

[57]



Drag the ESXi host **esxi-05a.vcf.sddc.lab** and drop it on the Datacenter called **RegionA01**

The ESXi host will be removed from the cluster.

You can also right click the ESXi host and select **Move To..**

You have now scaled down your vSAN Cluster.

Conclusion

[58]

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.

You Finished Module 1

[59]

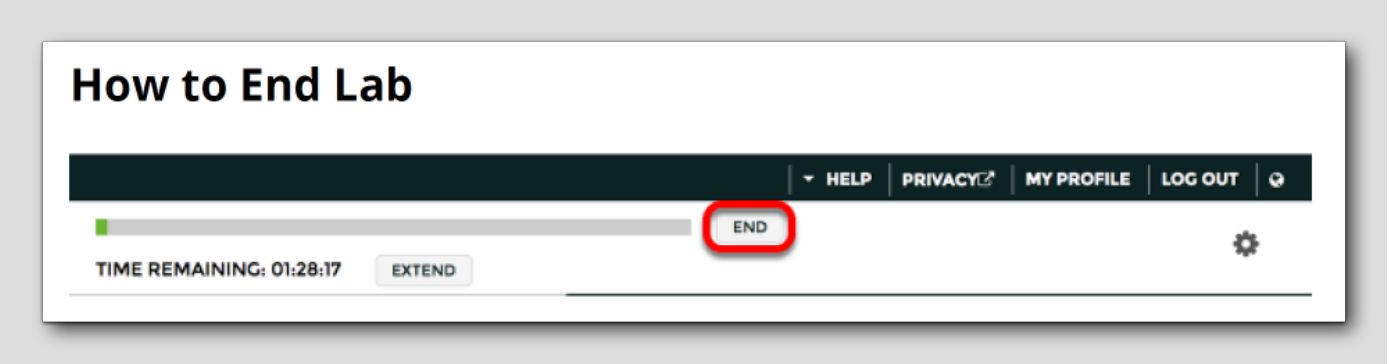
Congratulations on completing Module 1. You can EITHER continue to another module in this lab, or if you want to stop taking the lab you can end your session using the instructions below. Please do not end the lab if you plan to continue!

If you want to take another module, please use the links below:

- Module 2 - Monitoring, Health, Capacity, and Performance (30 minutes) (Basic) Show you how to enable Aria Operations within vCenter Server. We will cover the vSAN Health Check and how you can monitor your vSAN environment.
- Module 3 - vSAN Encryption and Security (30 minutes) (Advanced) Introduction to vSAN Encryption. We will enable a Key Management Server and demonstrate how to configure vSAN Encryption.
- Module 4 - File services (30 minutes) (Basic) Introduction to vSAN's File Services capabilities. We will create both NFS and SMB file shares and mount them to their respective clients.
- Module 5 - Data Protection (30 minutes) (Advanced) Introduction to vSAN ESA's new data protection capabilities. We will cover creating protection groups and snapshot schedules.
- Module 6 - vSAN Stretched Cluster (30 minutes) (Advanced) Introduction to vSAN Stretched Clusters. We will convert an existing vSAN cluster into a stretched cluster. In addition, we will explore storage policies as well as Skyline Health checks with respect to stretched clusters.

How to End Lab

[60]



To end your lab, click on the **END** button.

Module 2 - Monitoring, Health, Capacity and Performance (30 minutes) Basic

Introduction

[62]

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. Initially available with vSAN 7 and continuing with vSAN 8, vSAN 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.

vSAN Health Check Validation

[63]

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

[64]

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.

Open Firefox Browser from Windows Quick Launch Task Bar

[65]

1. Click on the **Firefox** on the Windows Quick Launch Task Bar.

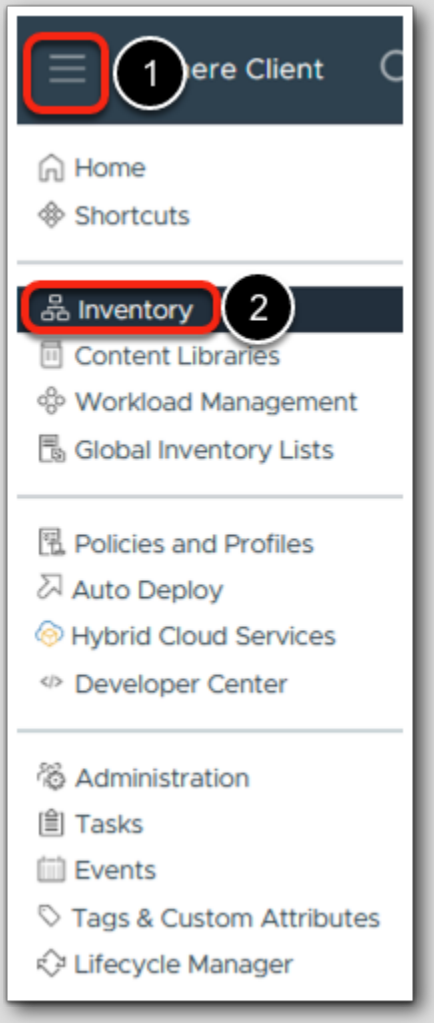
Login to vSphere Client

[66]

1. On the vSphere Client login screen, username: **administrator@vsphere.local**
2. Enter Password: **VMware123!**
3. Click **LOGIN**

Use Health Check to Verify vSAN Functionality

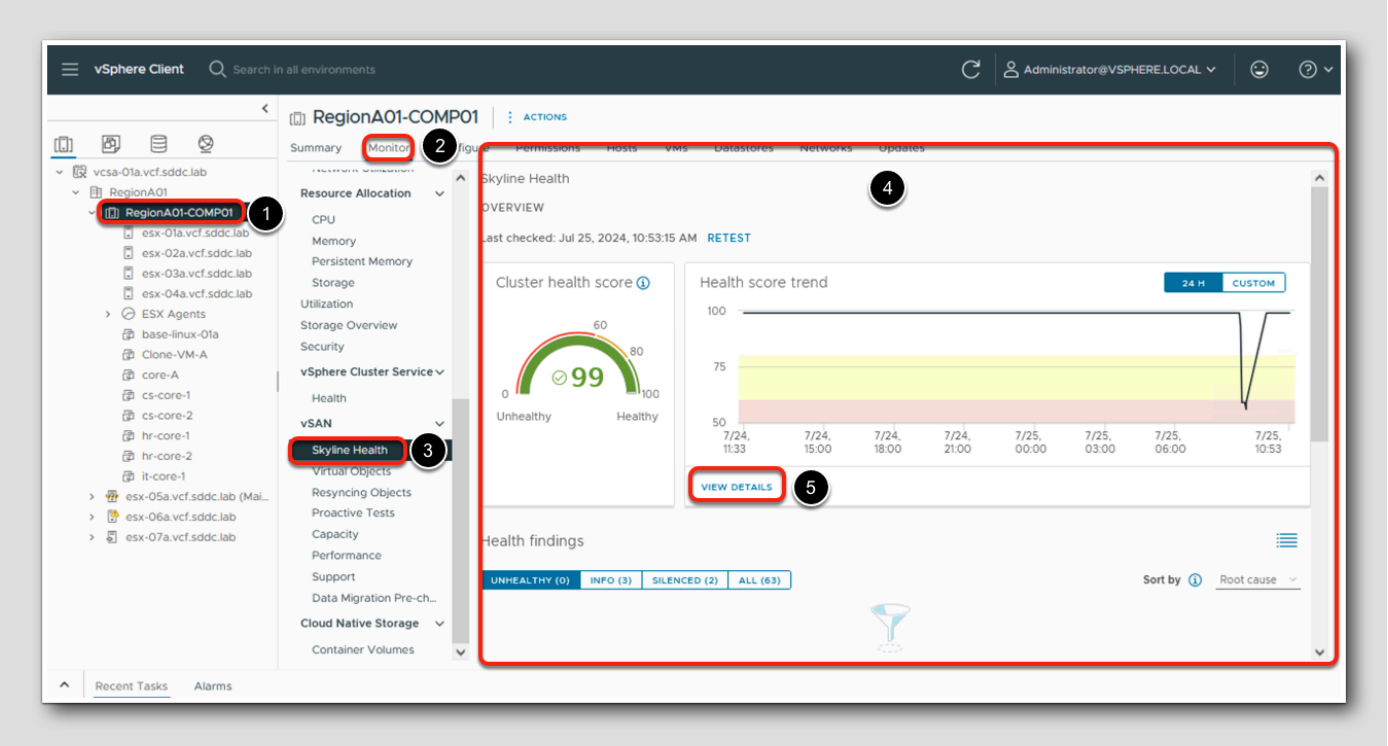
[67]



1. Select **Menu**
2. Select **Inventory**

Use Health Check to Verify vSAN Functionality

[68]



To run a vSAN Health Check,

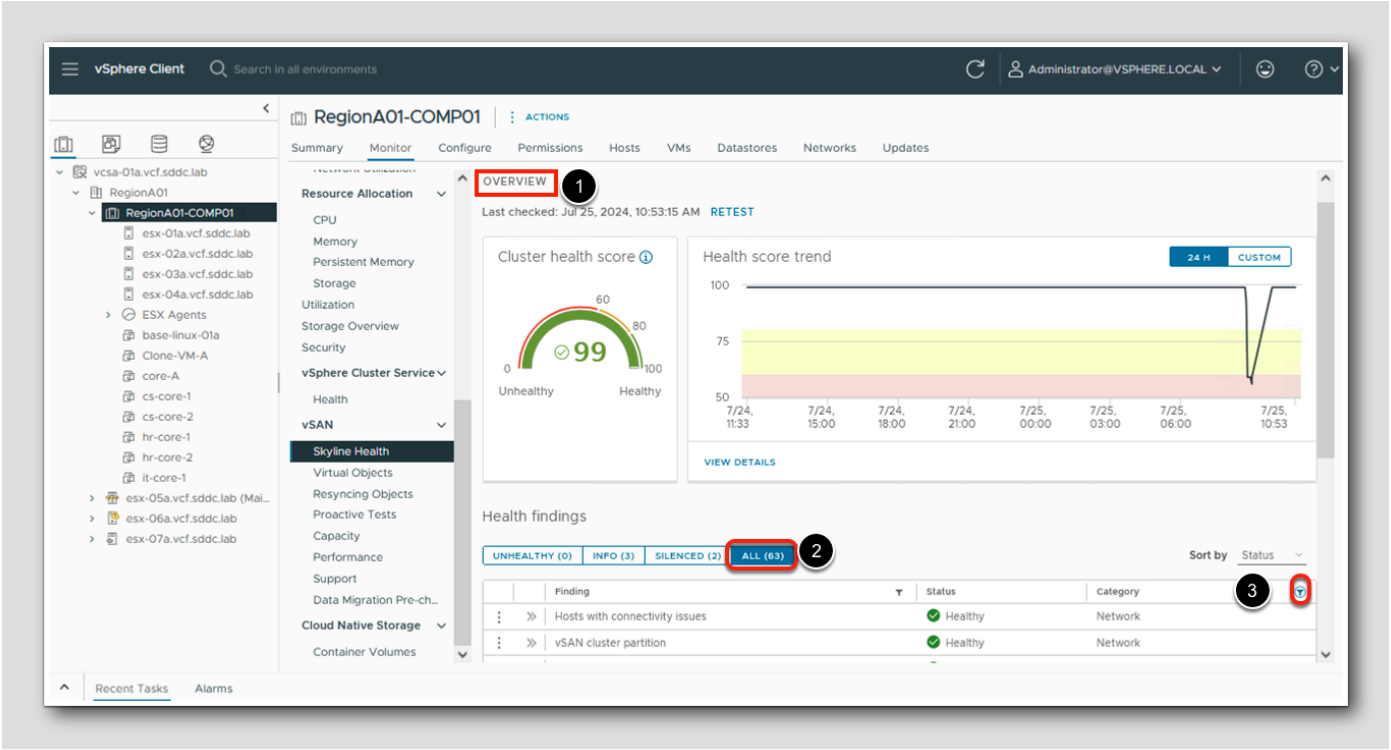
1. Select the vSAN Cluster, **RegionA01-COMP01**
2. Select **Monitor**
3. Select **vSAN > Skyline Health**
4. The Skyline Health overview will show you the current Cluster health score, the Health score trend, as well as health findings that outlines current issues in the vSAN environment.
5. Under Health score trend, click **VIEW DETAILS**.

You can view the history of the health of the vSAN Cluster and when an event was unhealthy.

Note there may be some health findings 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

[69]

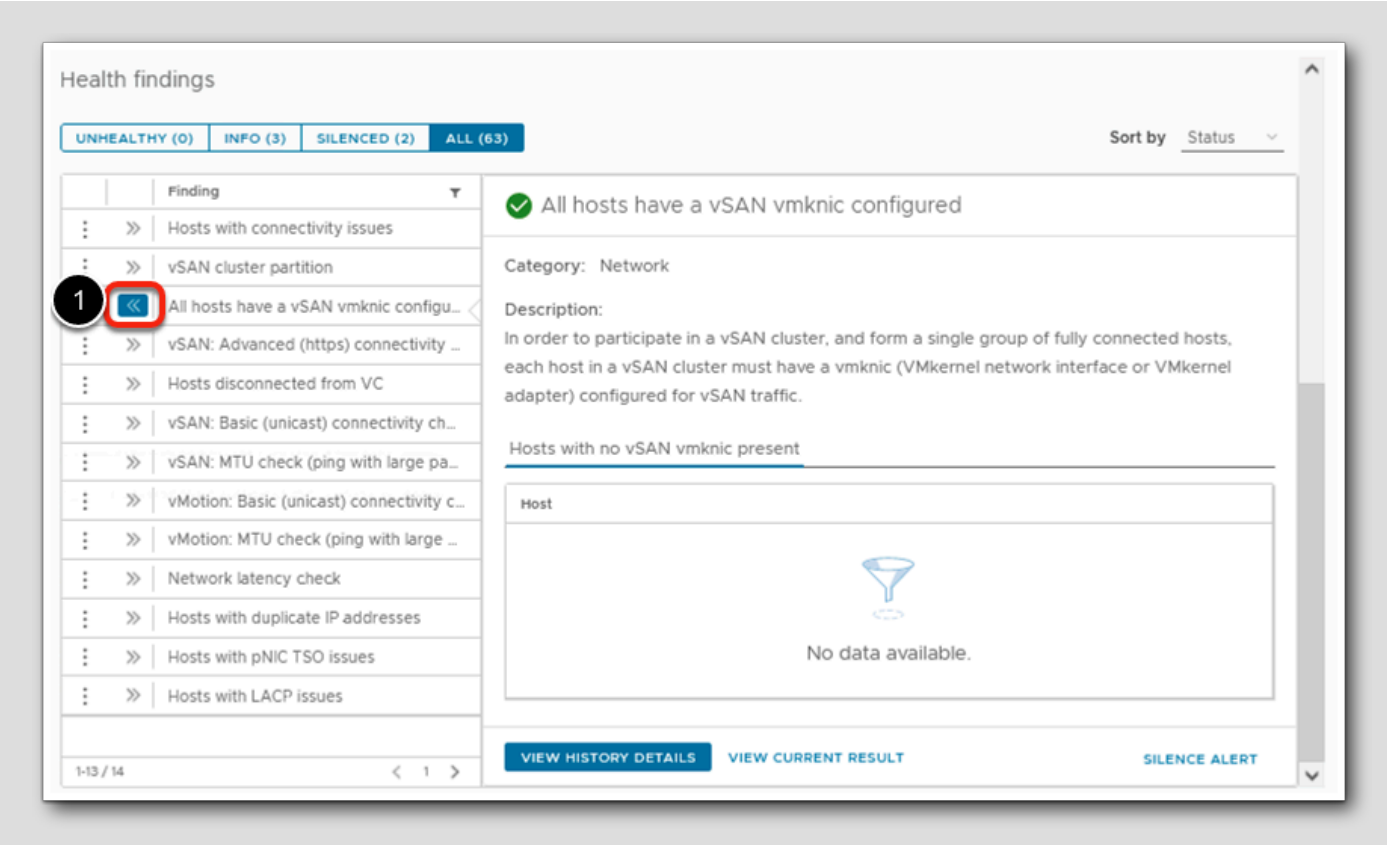


To see the individual tests that can be run from within a vSAN Health category.

1. Click back into **Overview**
2. Scroll down and click on **ALL**
3. Click the filter button in the **Category** column and check "**Network**"

Getting Detail on a Network Health Check

[70]



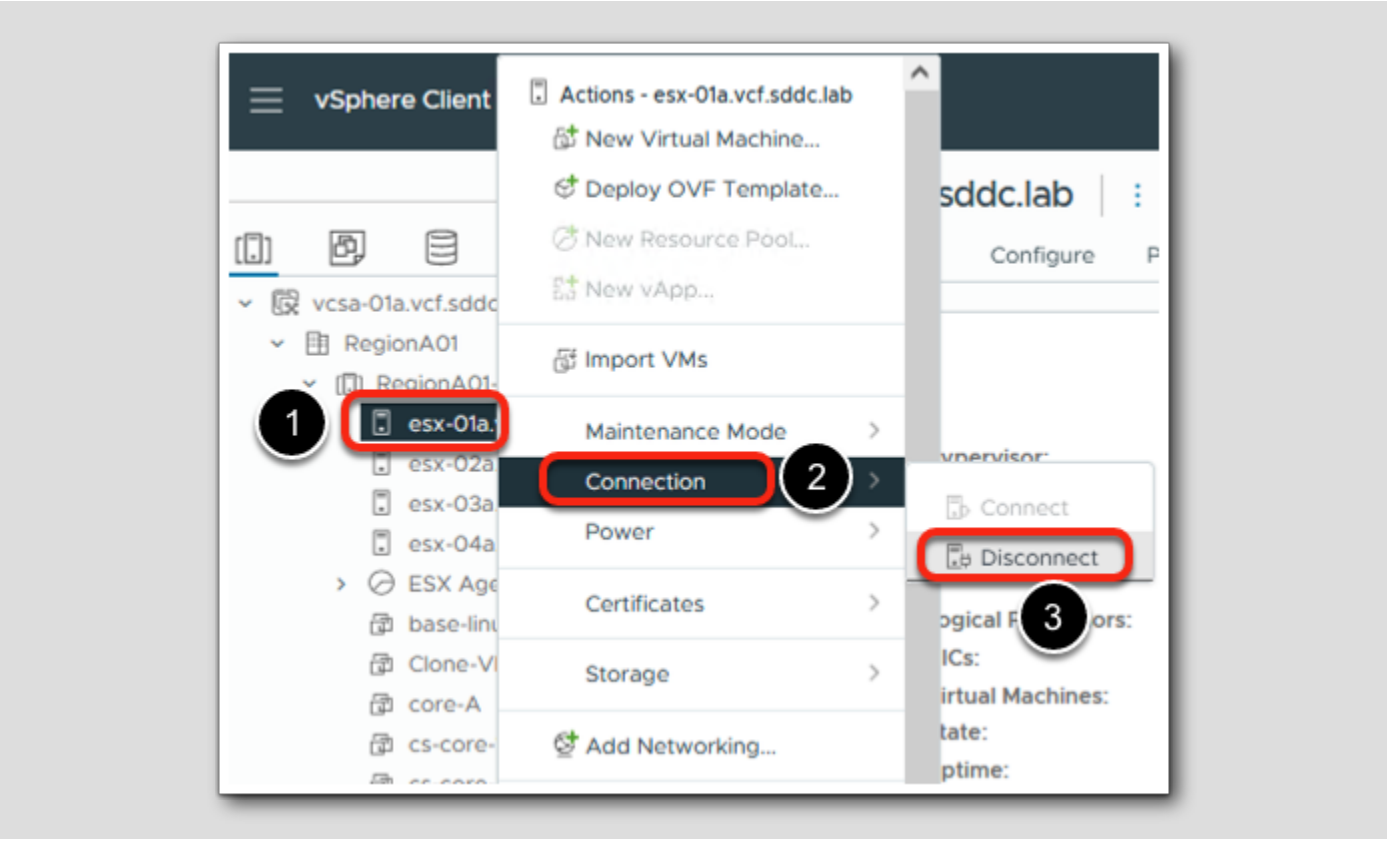
To get additional information on a Health Check item, select the appropriate check and examine the details pane on the right for information on how to resolve the issue.

1. Click the >> icon next to "All hosts have a vSAN vmknic configured"

Here we have the explanation of the health check that was performed as well as the green check showing that it passed the check.

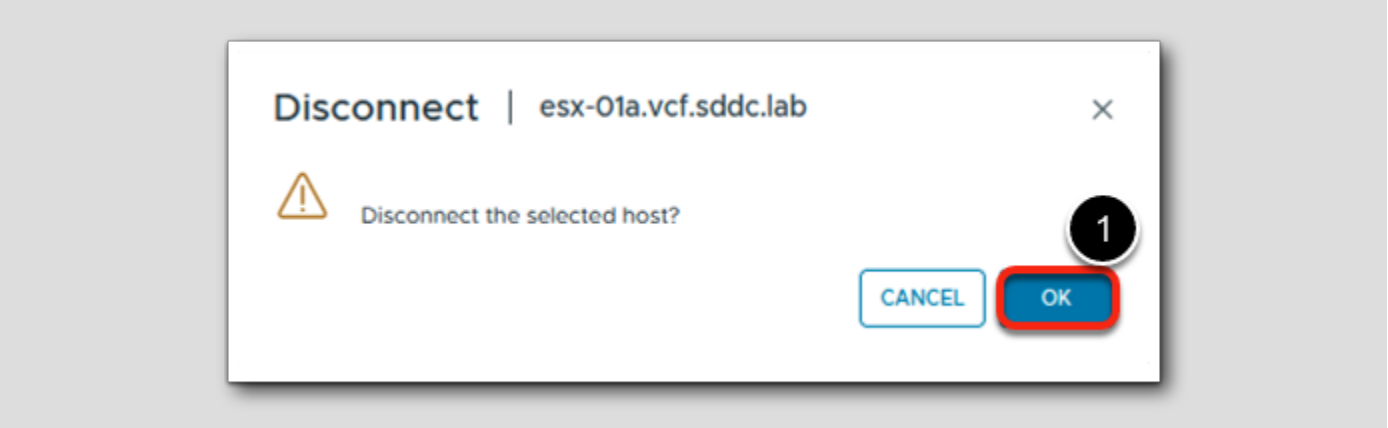
Inducing a vSAN Health Check Failure

[71]



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

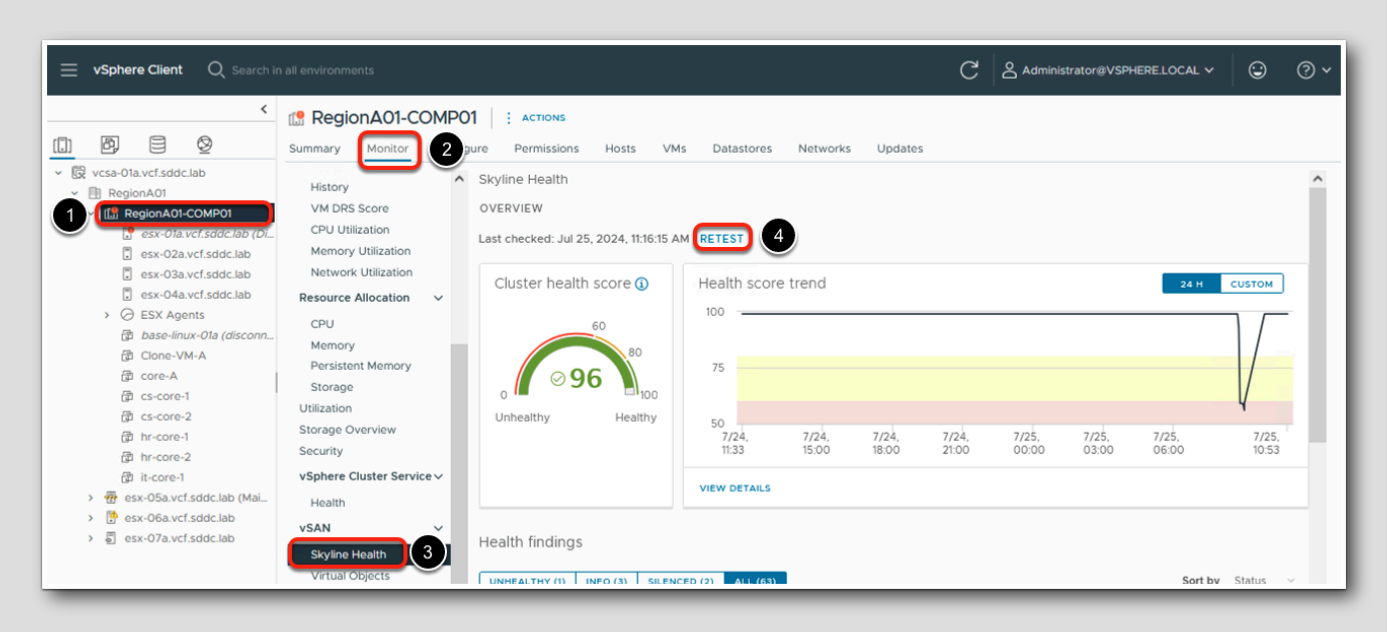
1. Right click the ESXi host called **esx-01a.vcf.sddc.lab**
2. Select **Connection**
3. Select **Disconnect**



1. Click **OK** to disconnect the selected host.

Inducing a vSAN Health Check Failure

[72]

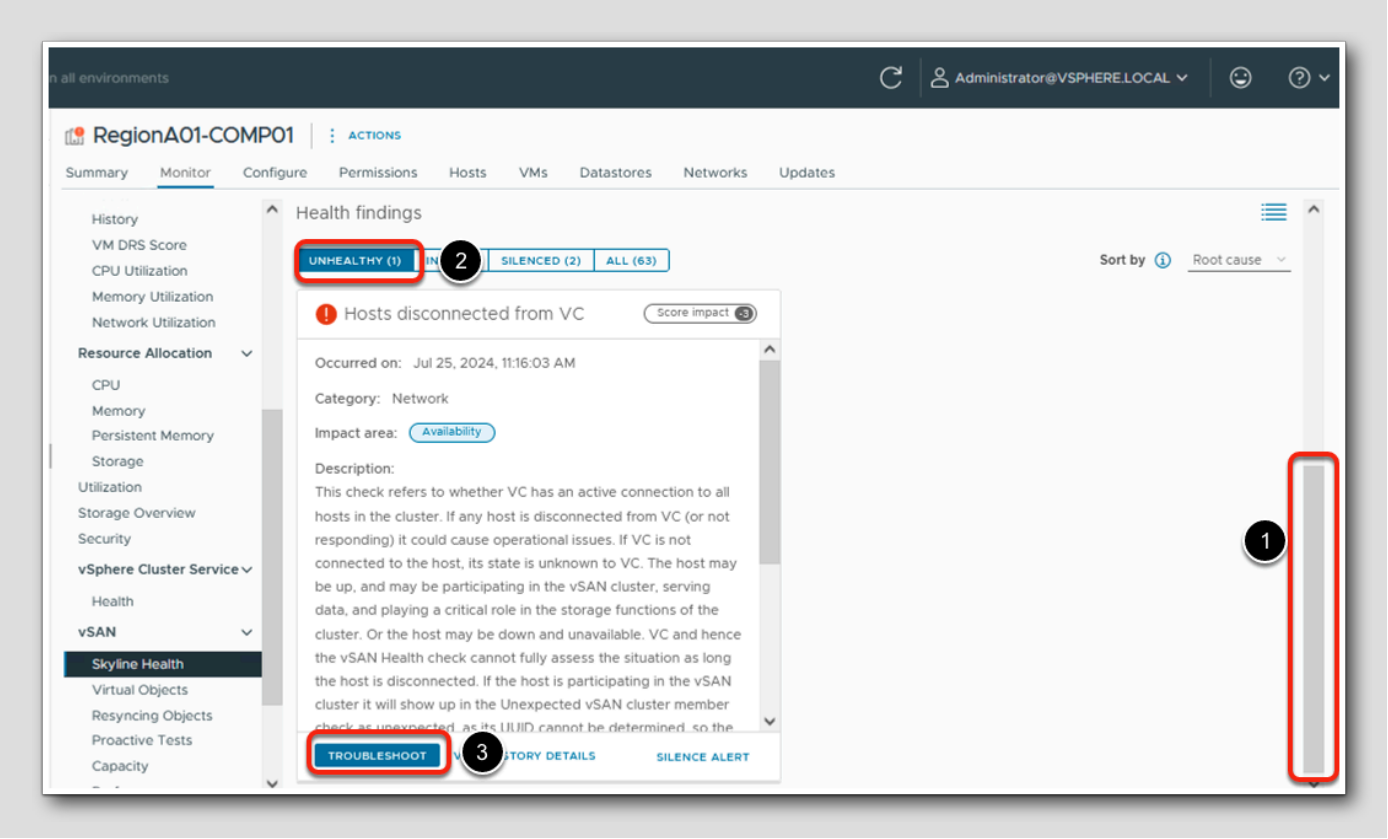


Let's return to the vSAN Health Check

1. Select the vSAN Cluster, **RegionA01-COMP01**
2. Select **Monitor**
3. Select **vSAN > Skyline Health**
4. Click the **RETEST** button.

Inducing a vSAN Health Check Failure

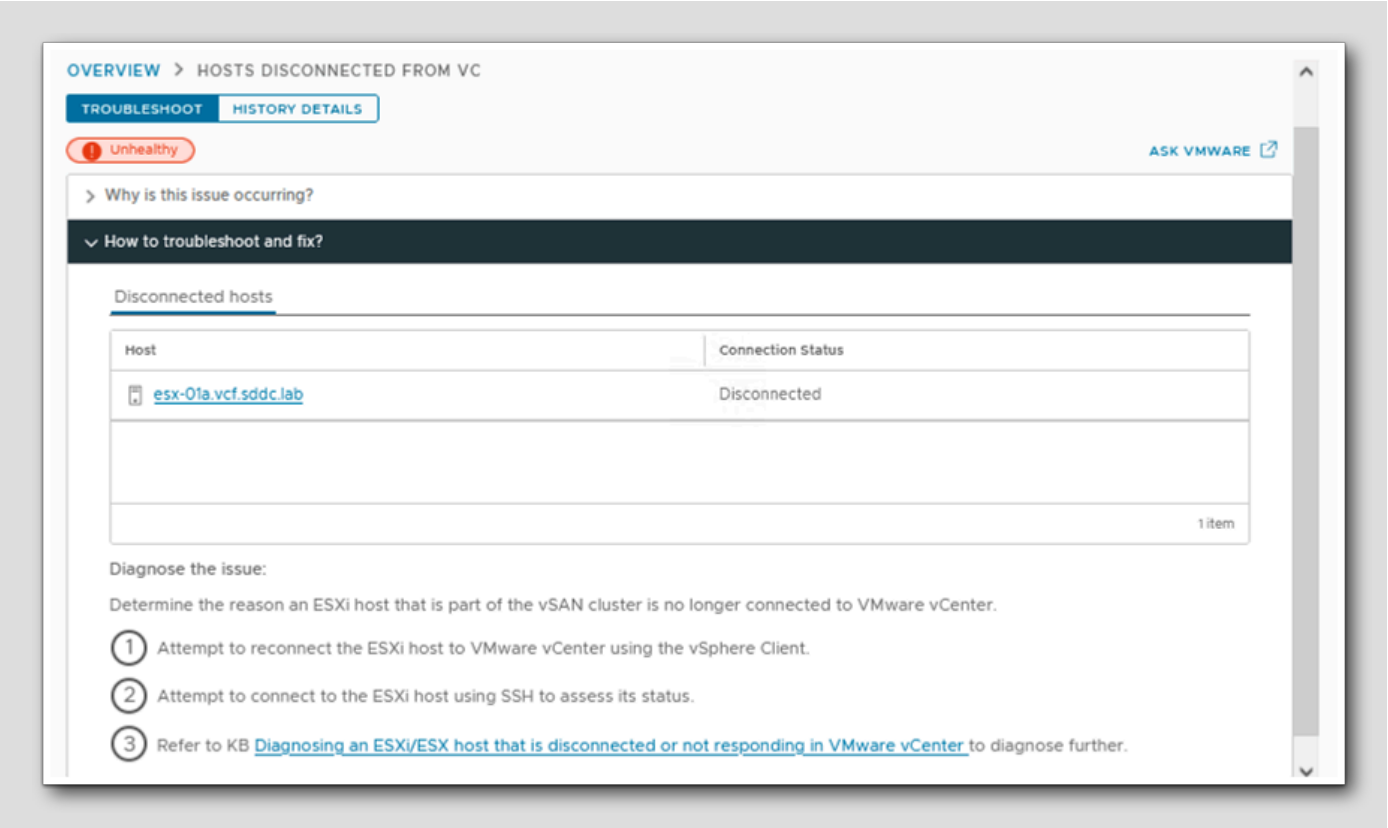
[73]



1. Scroll down to see the **Health findings** section.
2. Click on **UNHEALTHY (1)**
3. You will now see a Skyline Health alert that a host is disconnected from vCenter. Click on the **TROUBLESHOOT** button.

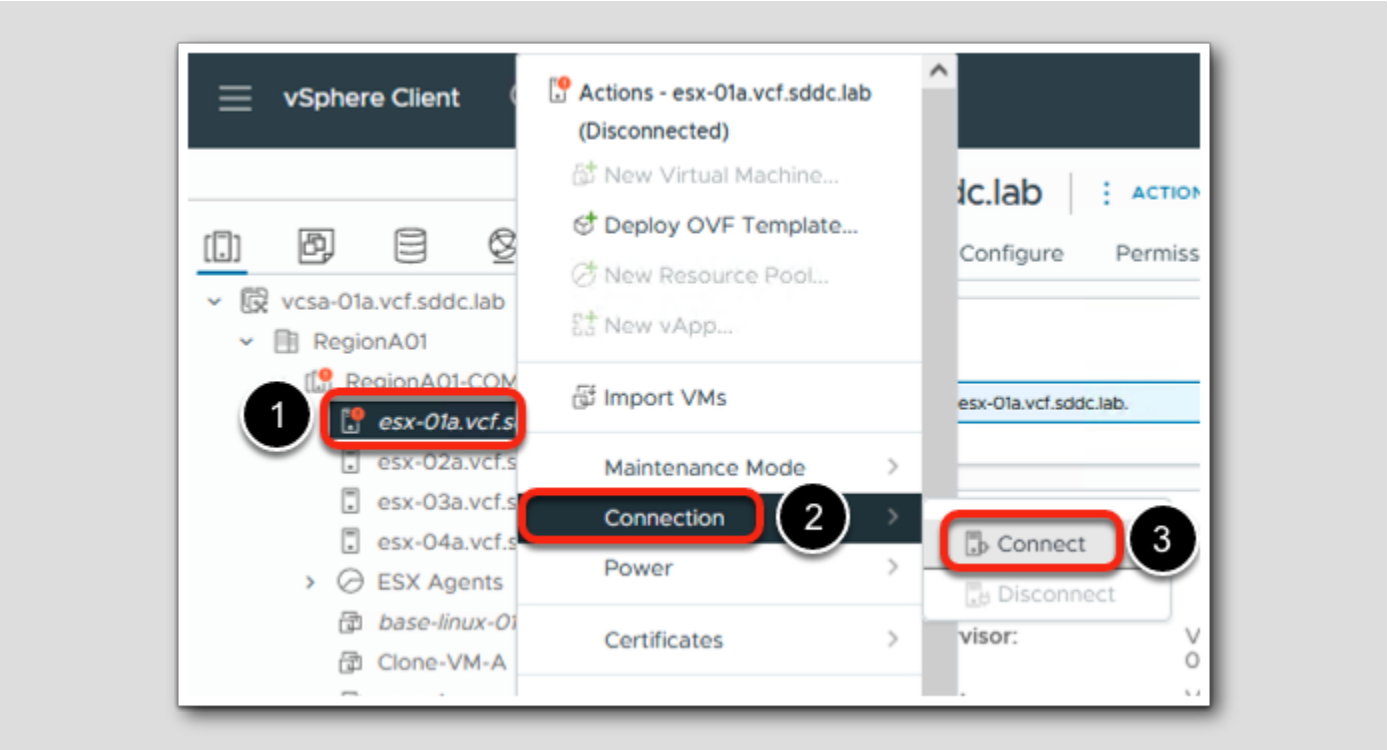
Inducing a vSAN Health Check Failure

[74]



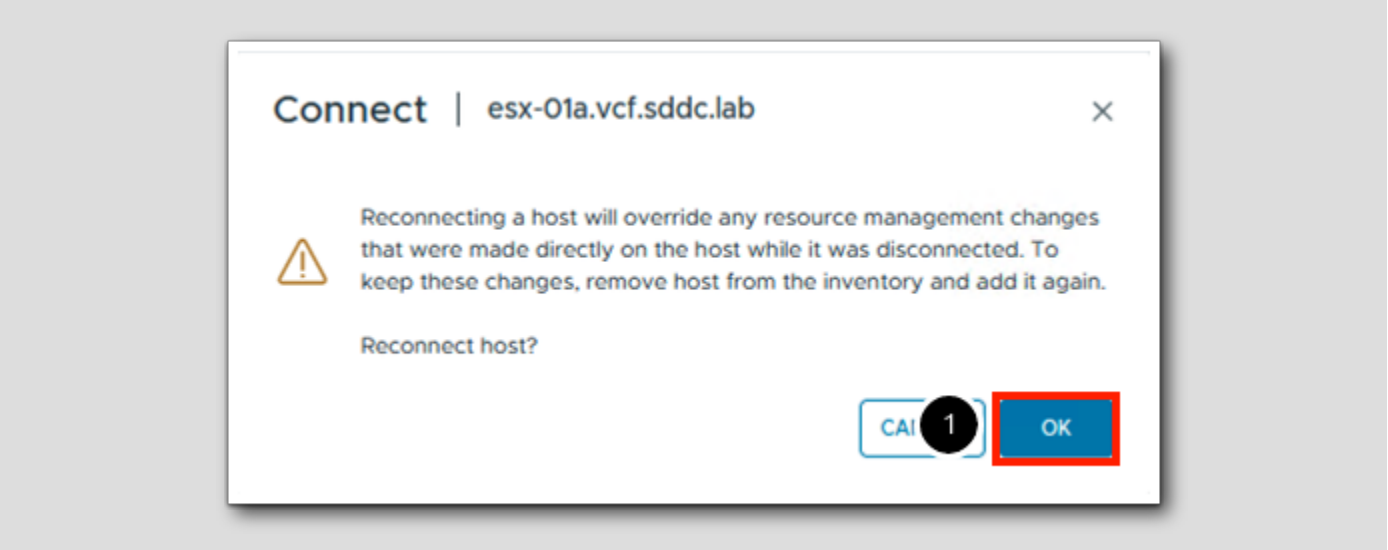
Here we can see that the ESXi host called **esx-01a.vcf.sddc.lab** is showing as **Disconnected** along with steps to take to fix the issue, including the link to a kb article to help further diagnose the issue.

Resolving a vSAN Health Check Failure



Let's resolve the vSAN Health Check failure.

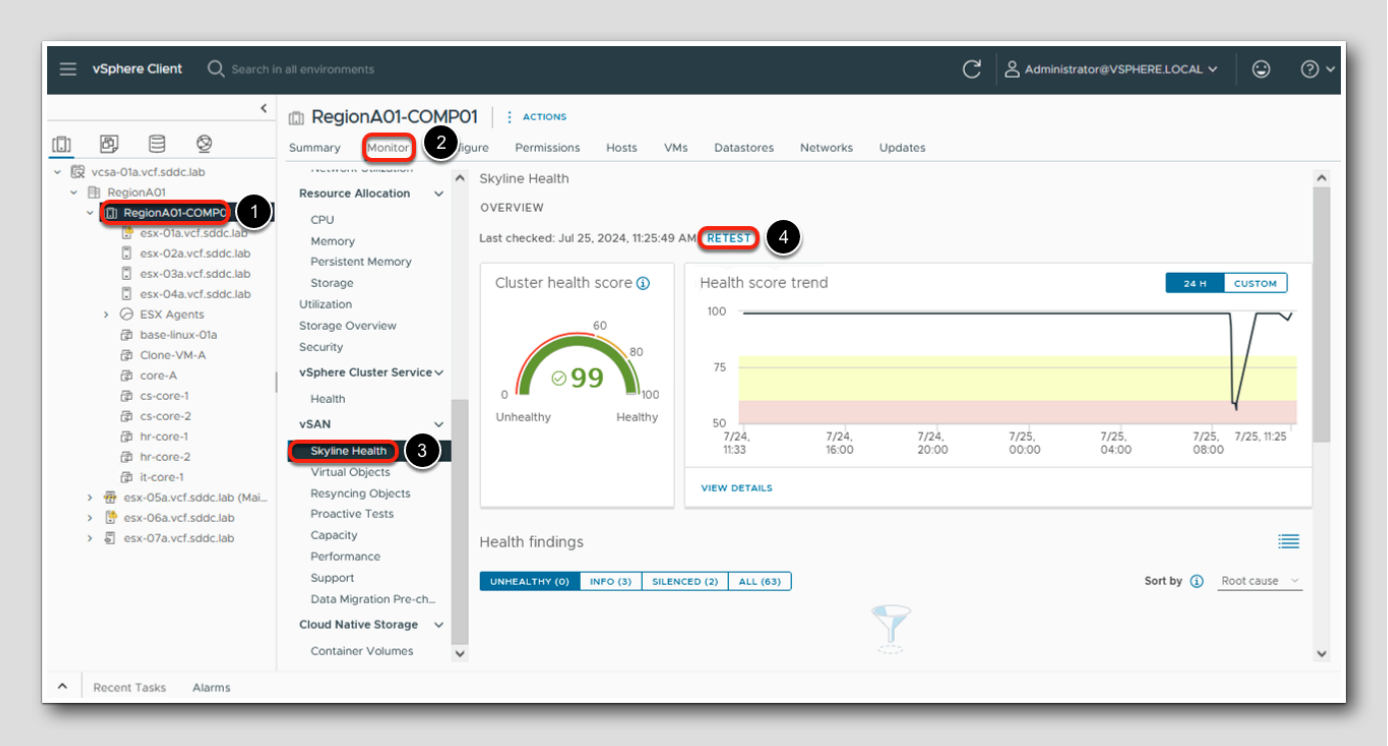
1. Right click the ESXi host called esx-01a.vcf.sddc.lab
2. Select Connection
3. Select Connect



1. Answer OK to reconnect the selected host.

Resolving a vSAN Health Check Failure

[76]



Let's return to the vSAN Health Check

1. Select the vSAN Cluster, **RegionA01-COMP01**
2. Select **Monitor**
3. Select **vSAN > Skyline Health**
4. Click **RETEST**
5. The **Hosts disconnect from VC** test has passed again as all the ESXi host in the vSAN Cluster are connected. In addition, the errors have now disappeared from the **UNHEALTHY** section.

Conclusion

[77]

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.

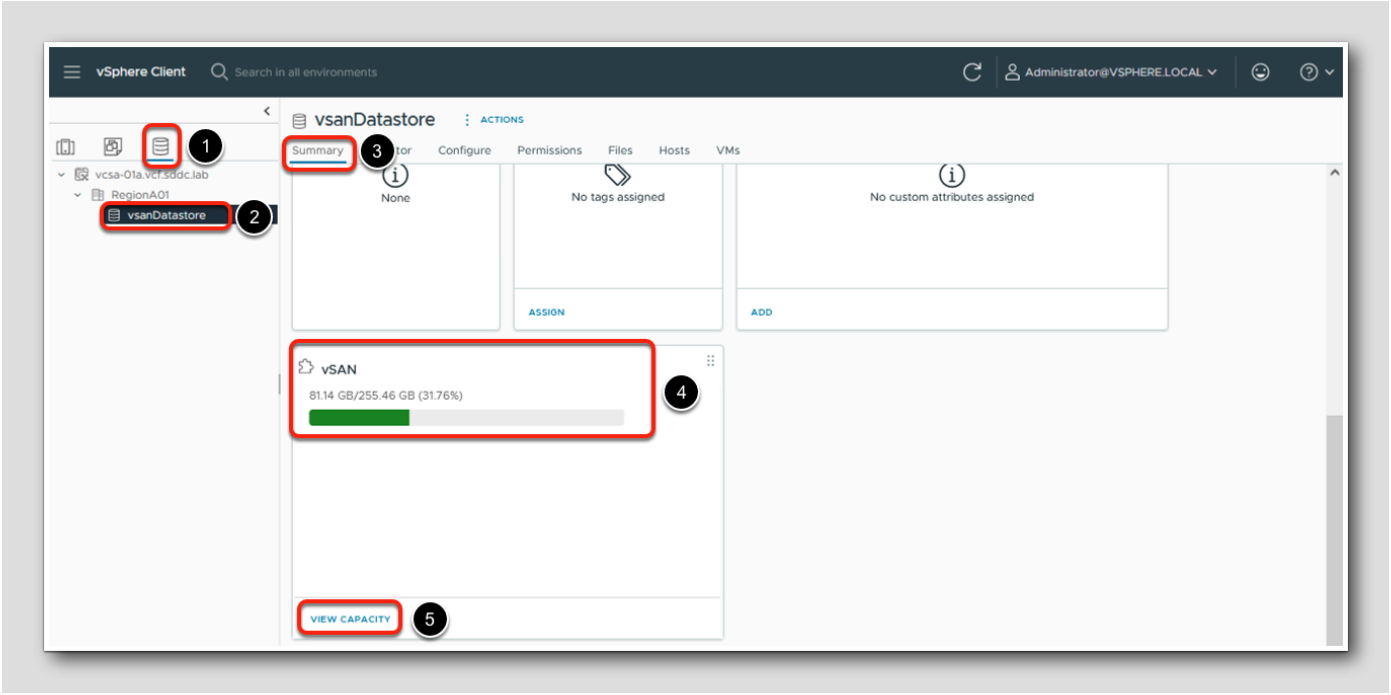
Monitoring vSAN Capacity

[78]

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

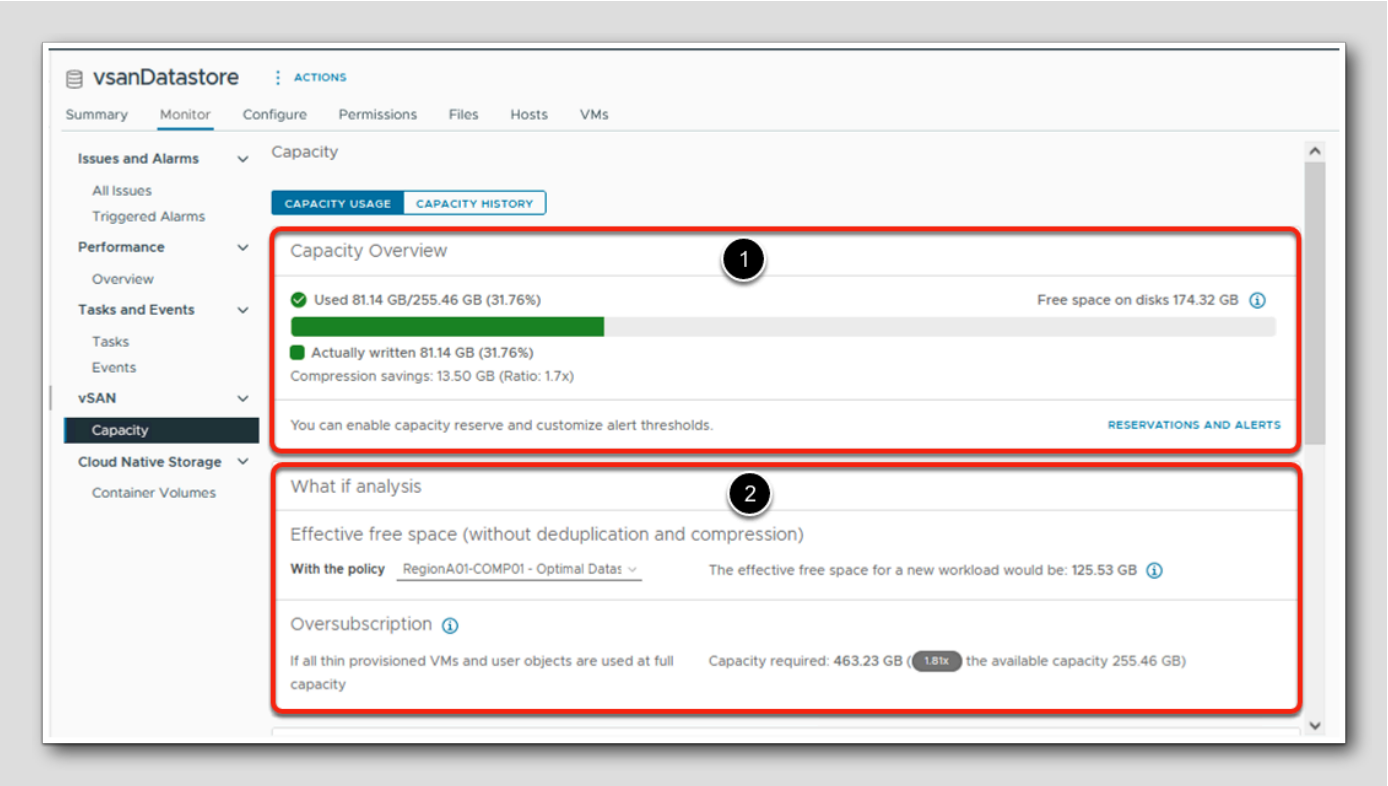
[79]



1. Select **Storage** Icon
2. Select **RegionA01** > **vsanDatastore**
3. Click **Summary**
4. Scroll down and note the amount of **Used** and **Free Capacity** Information
5. Click **VIEW CAPACITY**

Capacity Overview

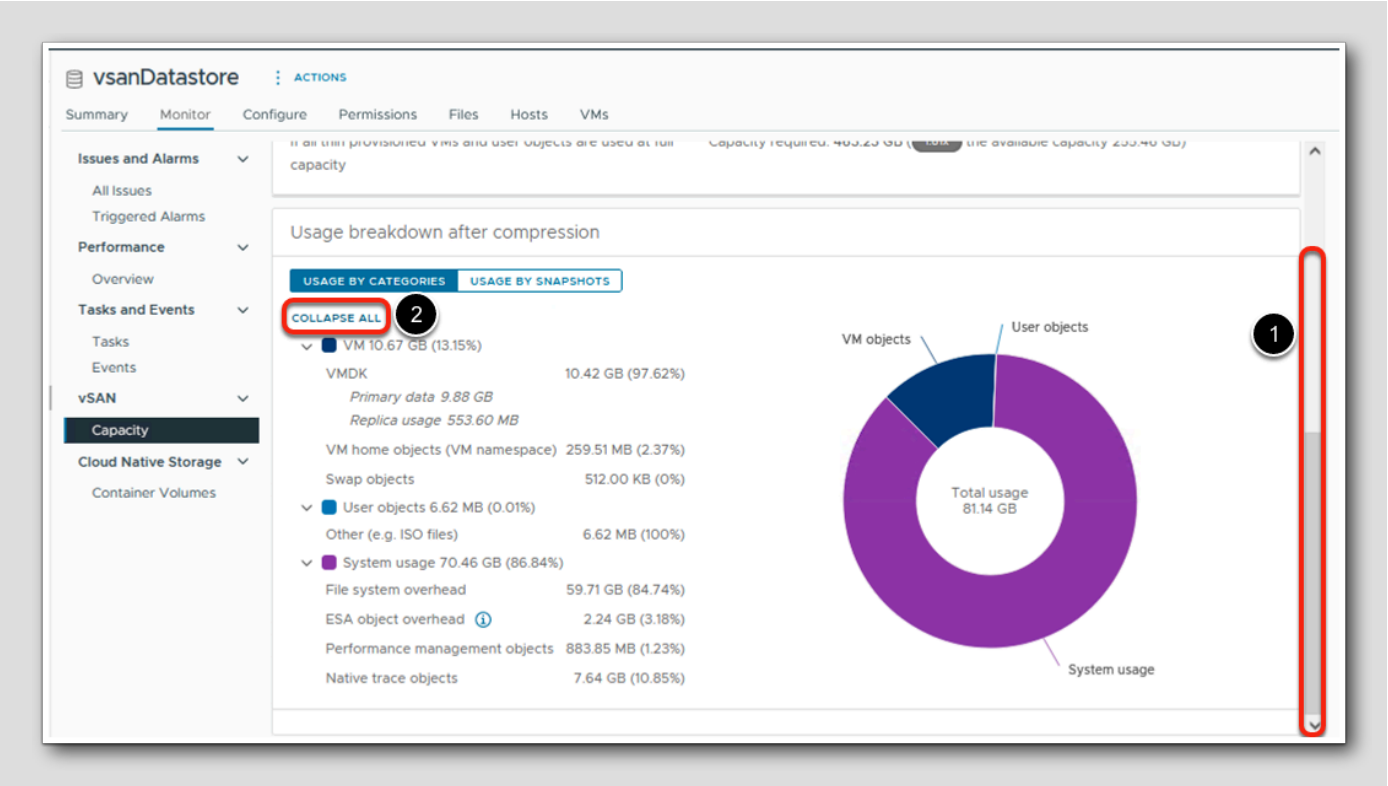
[80]



1. The Capacity Overview displays the storage capacity of the vSAN Datastore, including used space and free space.
2. The What if analysis will show the effective free space based on a chosen storage policy as well as the vSAN datastore is oversubscribed from a thin provisioning perspective.

Usage breakdown before dedupe and compression

[81]



1. Scroll Down to view the **Usage breakdown**
2. Click on **EXPAND ALL** (note - screenshot shows **COLLAPSE ALL** after **EXPAND ALL** is clicked)

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).

Monitoring vSAN Performance

[82]

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

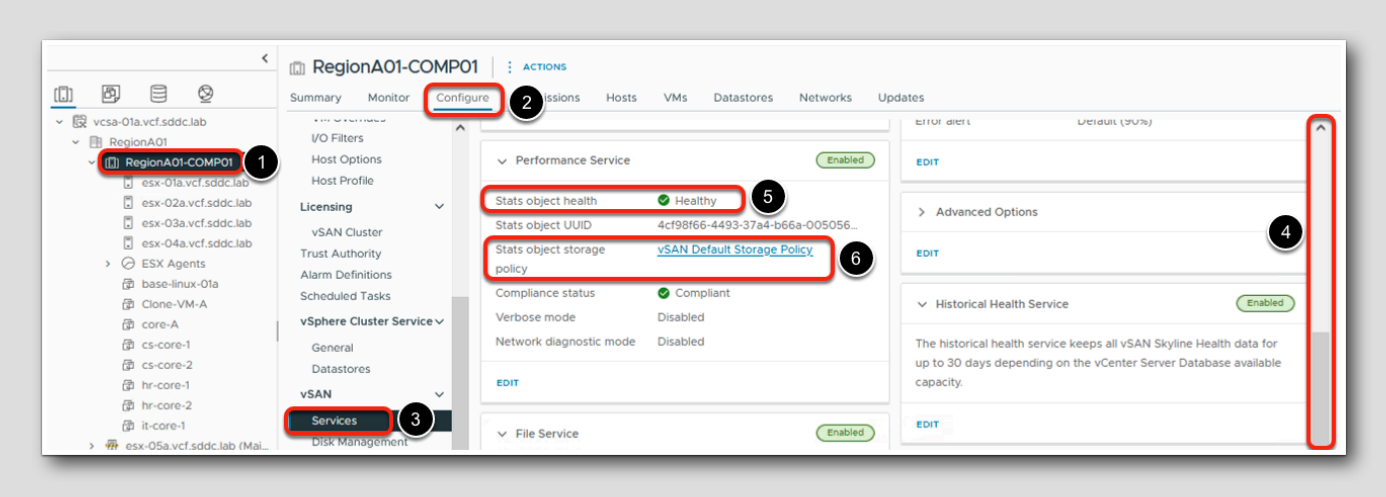
[83]

With vSAN 8, 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

[84]

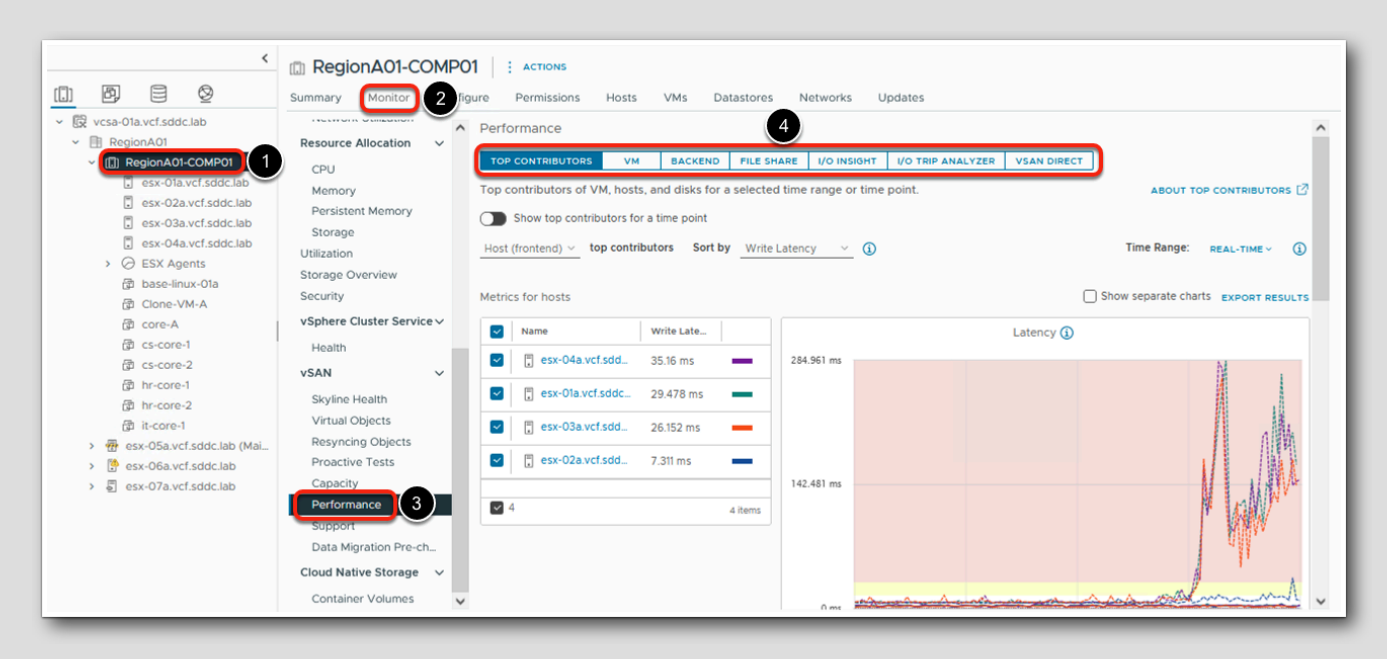


1. Select **RegionA01-COMP01**
2. Select **Configure**
3. Select **vSAN > Services**
4. Scroll down until you see **Performance Service.** Expand it, if necessary.
5. Note that the Performance Stats Database Object is reported as **Healthy**
6. Note that the Stats DB is using the **vSAN Default Storage 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

[85]



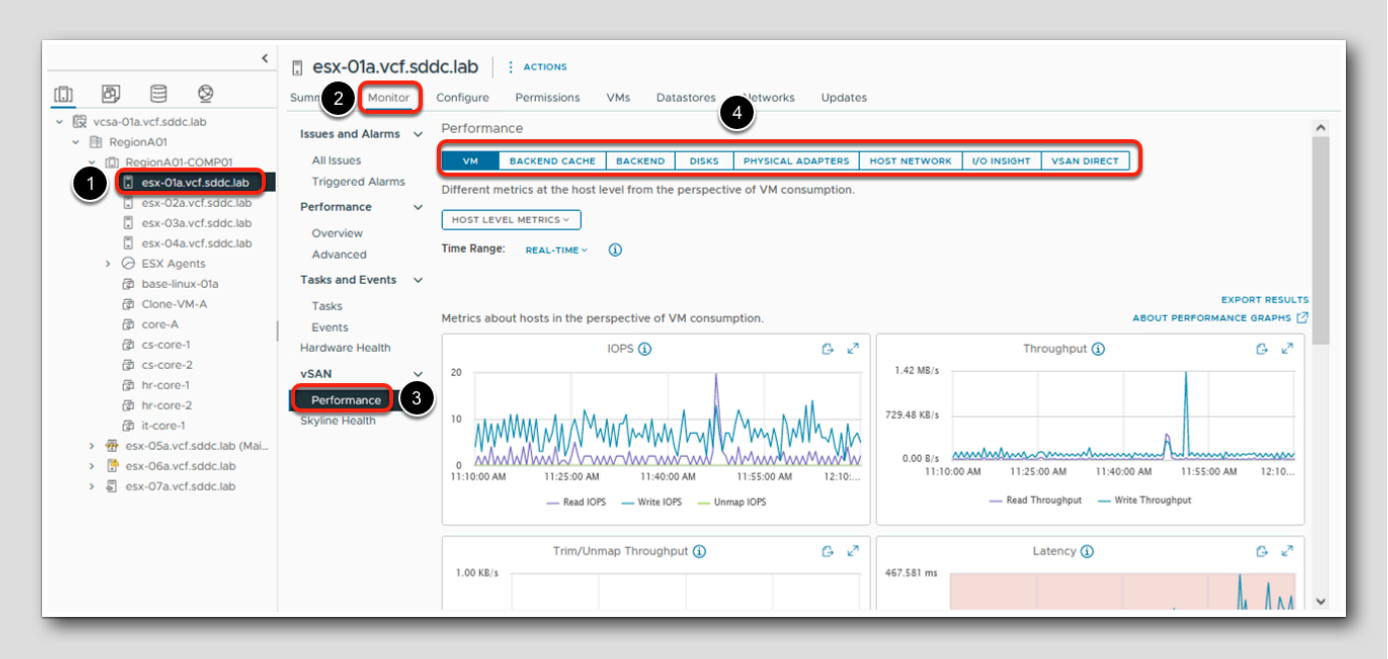
1. Select RegionA01-COMP01
2. Select Monitor
3. Select vSAN > Performance
4. Note that we can choose to view VM, Backend, File Share and IOInsight Performance views at the Cluster level (you can also customize the Time Range if desired).

Scroll-down to view the graphs of 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

[86]



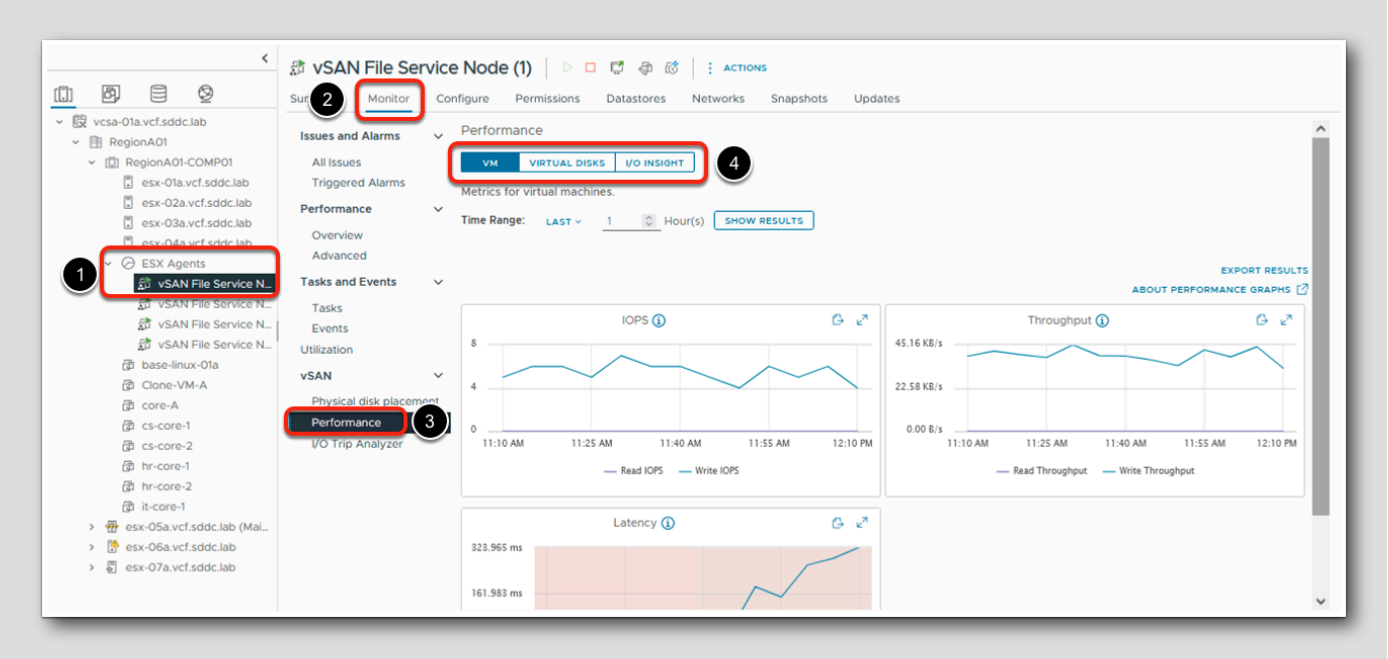
1. Select host, esx-01a.vcf.sddc.lab
2. Select Monitor
3. Select vSAN > Performance
4. Note that we can choose to view VM, Backend, Disks, Physical Adapters, Host Network and IOInsight Performance views at the Host level (you can also customize the Time Range if desired).

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

[87]



1. Open the **ESX Agents** resource pool and pick one of the file service VMs
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).

Scroll-down to view the various metrics that are collected (**IOPS, Throughput, Latency**, etc.)

Conclusion

[88]

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.

You Finished Module 2

[89]

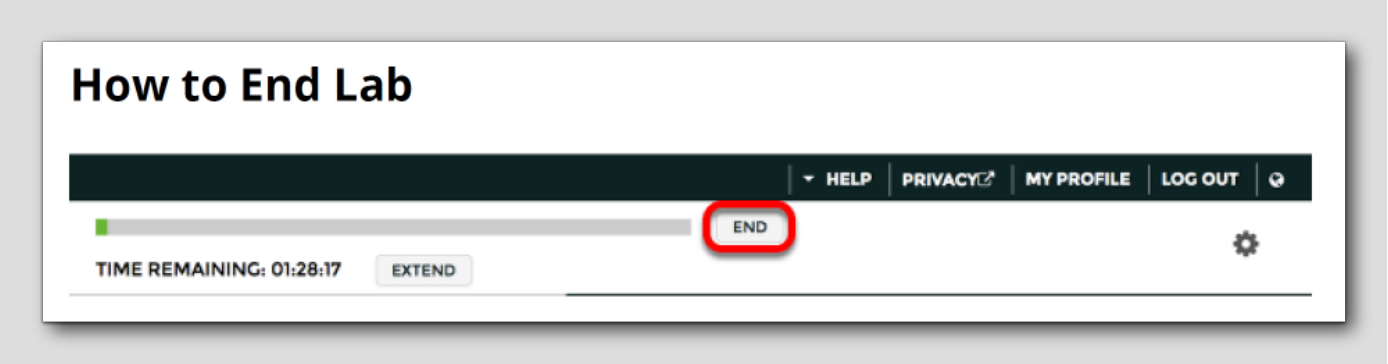
Congratulations on completing Module 2. You can EITHER continue to another module in this lab, or if you want to stop taking the lab you can end your session using the instructions below. Please do not end the lab if you plan to continue!

If you want to take another module, please use the links below:

- Module 1 - vSAN SPBM and Availability (30 minutes) (Basic) Introduction to VMware vSAN's Express Storage Architecture. We will cover the power of Storage Based Policy Management (SPBM) and show you the availability of vSAN.
- Module 3 - vSAN Encryption and Security (30 minutes) (Advanced) Introduction to vSAN Encryption. We will enable a Key Management Server and demonstrate how to configure vSAN Encryption.
- Module 4 - File services (30 minutes) (Basic) Introduction to vSAN's File Services capabilities. We will create both NFS and SMB file shares and mount them to their respective clients.
- Module 5 - Data Protection (30 minutes) (Advanced) Introduction to vSAN ESA's new data protection capabilities. We will cover creating protection groups and snapshot schedules.
- Module 6 - vSAN Stretched Cluster (30 minutes) (Advanced) Introduction to vSAN Stretched Clusters. We will convert an existing vSAN cluster into a stretched cluster. In addition, we will explore storage policies as well as Skyline Health checks with respect to stretched clusters.

How to End Lab

[90]



To end your lab, click on the **END** button.

Module 3 - vSAN Encryption and Security (30 minutes) Advanced

vSAN Encryption

[92]

vSAN Encryption Overview

You can encrypt data-in transit in your vSAN Cluster and encrypt data-at-rest in your vSAN datastore.

vSAN can encrypt data in transit across hosts in the vSAN cluster. Data-in-transit encryption protects data as it moves around the vSAN cluster.

vSAN can encrypt data at rest in the vSAN datastore. Data-at-rest encryption protects data on storage devices, in case a device is removed from the cluster.

vSAN Data-In Transit Encryption

- vSAN can encrypt data in transit, as it moves across hosts in your vSAN cluster.
- vSAN uses AES-256 bit encryption on data in transit.
- vSAN data-in-transit encryption is not related to data-at-rest-encryption. You can enable or disable each one separately.
- Forward secrecy is enforced for vSAN data-in-transit encryption.
- Traffic between data hosts and witness hosts is encrypted.
- File service data traffic between the VDFS proxy and client servers is encrypted.
- vSAN uses symmetric keys that are generated dynamically and shared between hosts. Hosts dynamically generate an encryption key when they establish a connection, and they use the key to encrypt all traffic between the hosts. You do not need a key management server to perform data-in-transit encryption.
- Each host is authenticated when it joins the cluster, ensuring connections only to trusted hosts are allowed. When a host is removed from the cluster, it is authentication certificate is removed.

vSAN Data-At-Rest Encryption

- vSAN can encrypt data at rest in your vSAN datastore.
- When you enable encryption, vSAN encrypts everything in the vSAN datastore. All files are encrypted, so all virtual machines and their corresponding data are protected. Only administrators with encryption privileges can perform encryption and decryption tasks.
- New with vSAN Express Storage Architecture, data-at-rest encryption now takes place in the upper layers of vSAN (just after compression) which will minimize both CPU cost and I/O amplification.
- vSAN uses encryption keys as follows:
    - vCenter Server requests an AES-256 Key Encryption Key (KEK) from the KMS.vCenter Serverstores only the ID of the KEK, but not the key itself
    - The ESXi host encrypts disk data using the industry standard AES-256 XTS mode. Each disk has a different randomly generated Data Encryption Key (DEK)

- Each ESXi host uses the KEK to encrypt its DEKs, and stores the encrypted DEKs on disk. The host does not store the KEK on disk. If a host reboots, it requests the KEK with the corresponding ID from the KMS. The host can then decrypt its DEKs as needed
- A host key is used to encrypt core dumps, not data. All hosts in the same cluster use the same host key. When collecting support bundles, a random key is generated to re-encrypt the core dumps. You can specify a password to encrypt the random key

Data-In-Transit Encryption [93]

vSAN can encrypt data-in-transit across hosts in the cluster. When you enable data-in-transit encryption, vSAN encrypts all data and metadata traffic between hosts.

vSAN data-in-transit encryption has the following characteristics:

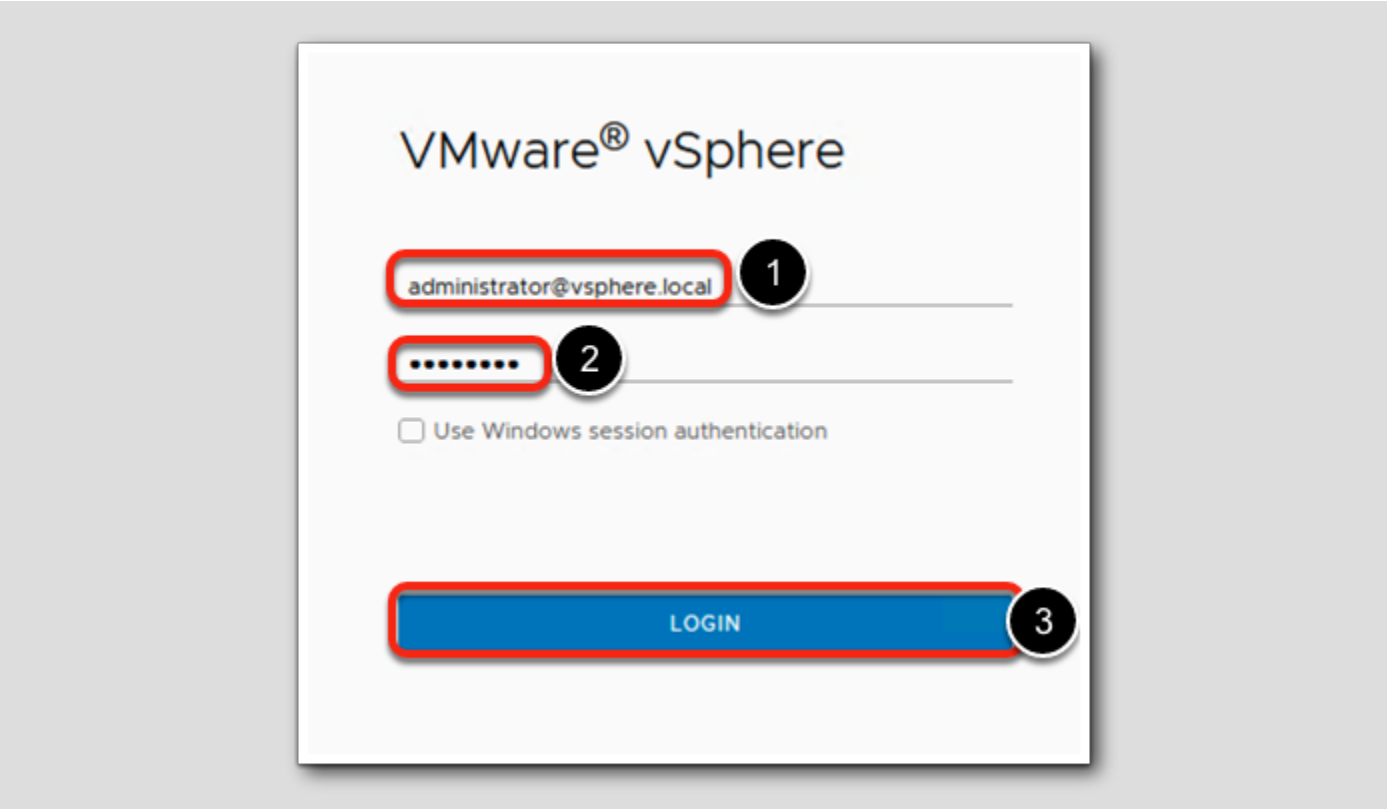
- vSAN uses AES-256 bit encryption on data in transit.
- vSAN data-in-transit encryption is not related to data-at-rest-encryption. You can enable or disable each one separately.
- Forward secrecy is enforced for vSAN data-in-transit encryption.
- Traffic between data hosts and witness hosts is encrypted.
- File service data traffic between the VDFS proxy and VDFS server is encrypted.
- vSAN file services inter-host connections are encrypted.

Open Firefox Browser from Windows Quick Launch Task Bar [94]

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

Login to vSphere Client

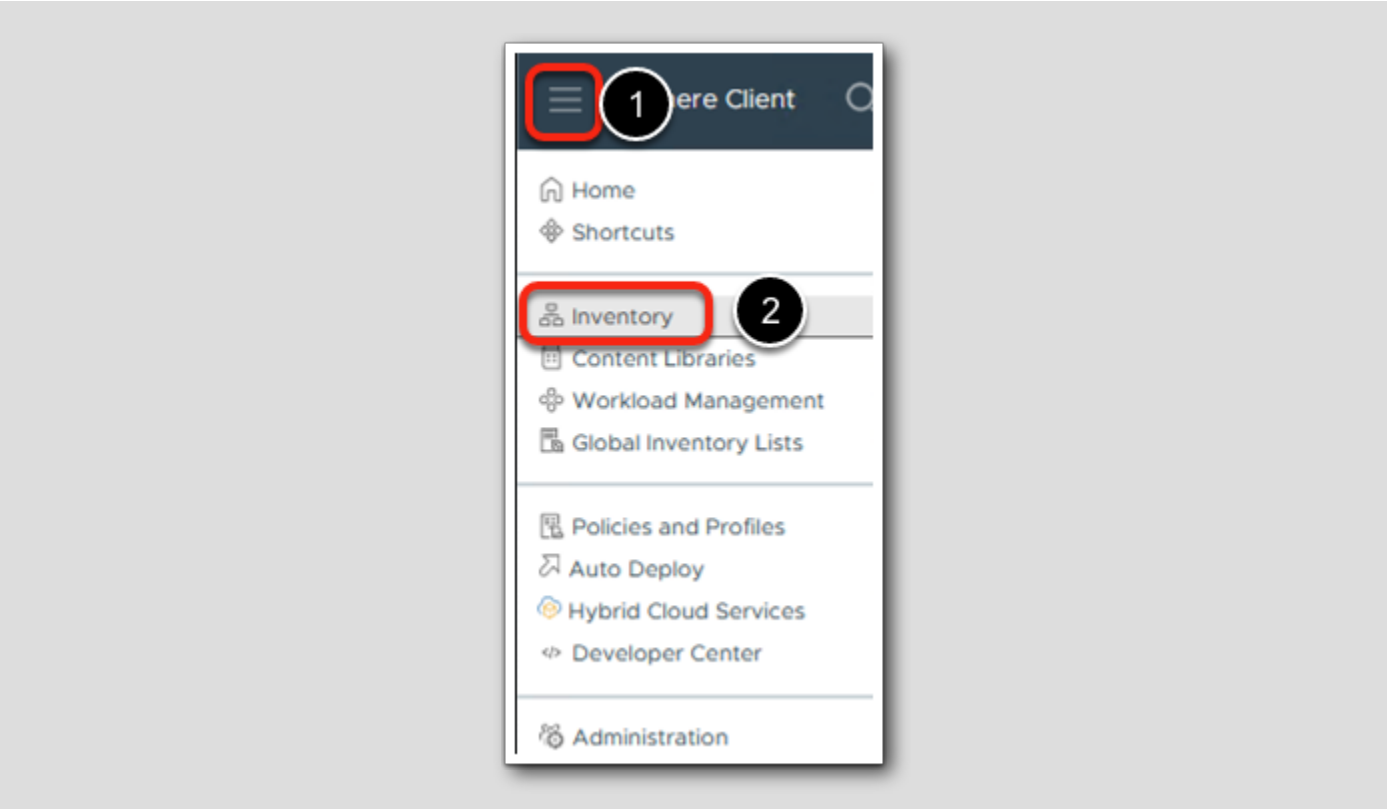
[95]



1. On the vSphere Client login screen, username: administrator@vsphere.local
2. Enter Password: VMware123!
3. Click **LOGIN**

Login to vSphere Client

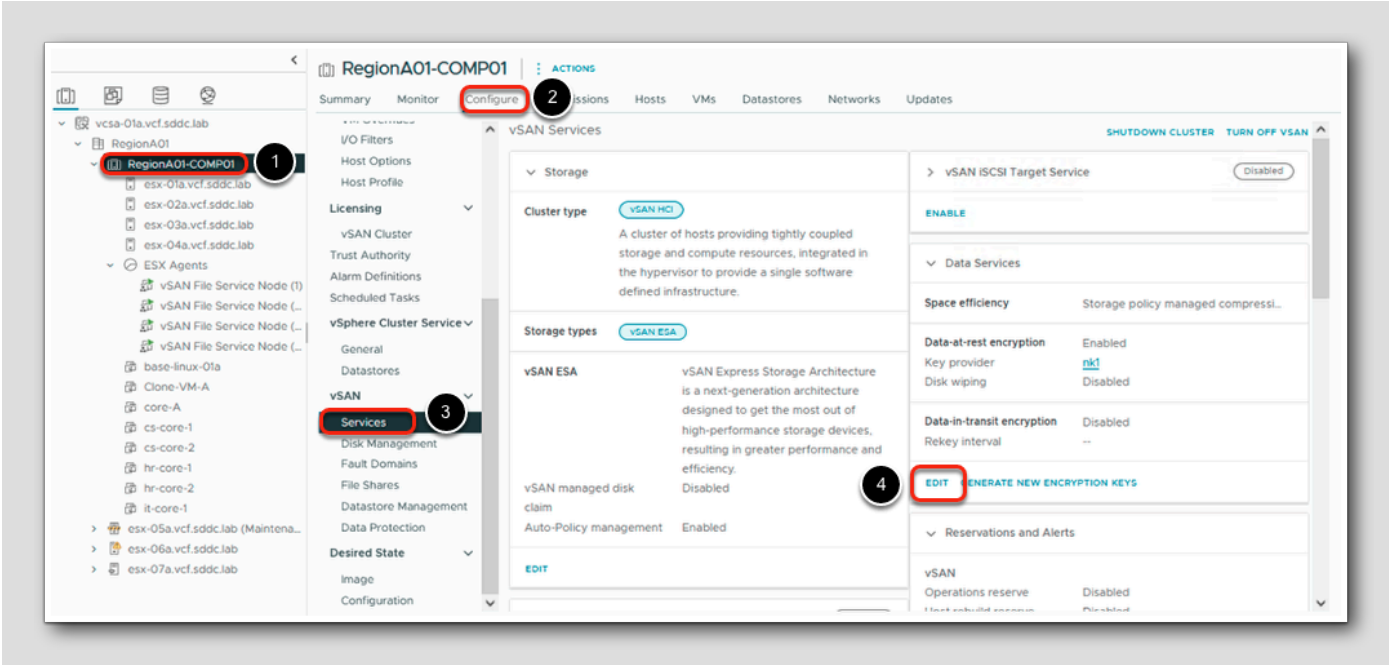
[96]



1. Click on the menu icon.
2. Click on **Inventory**

Enable Data-In-Transit Encryption

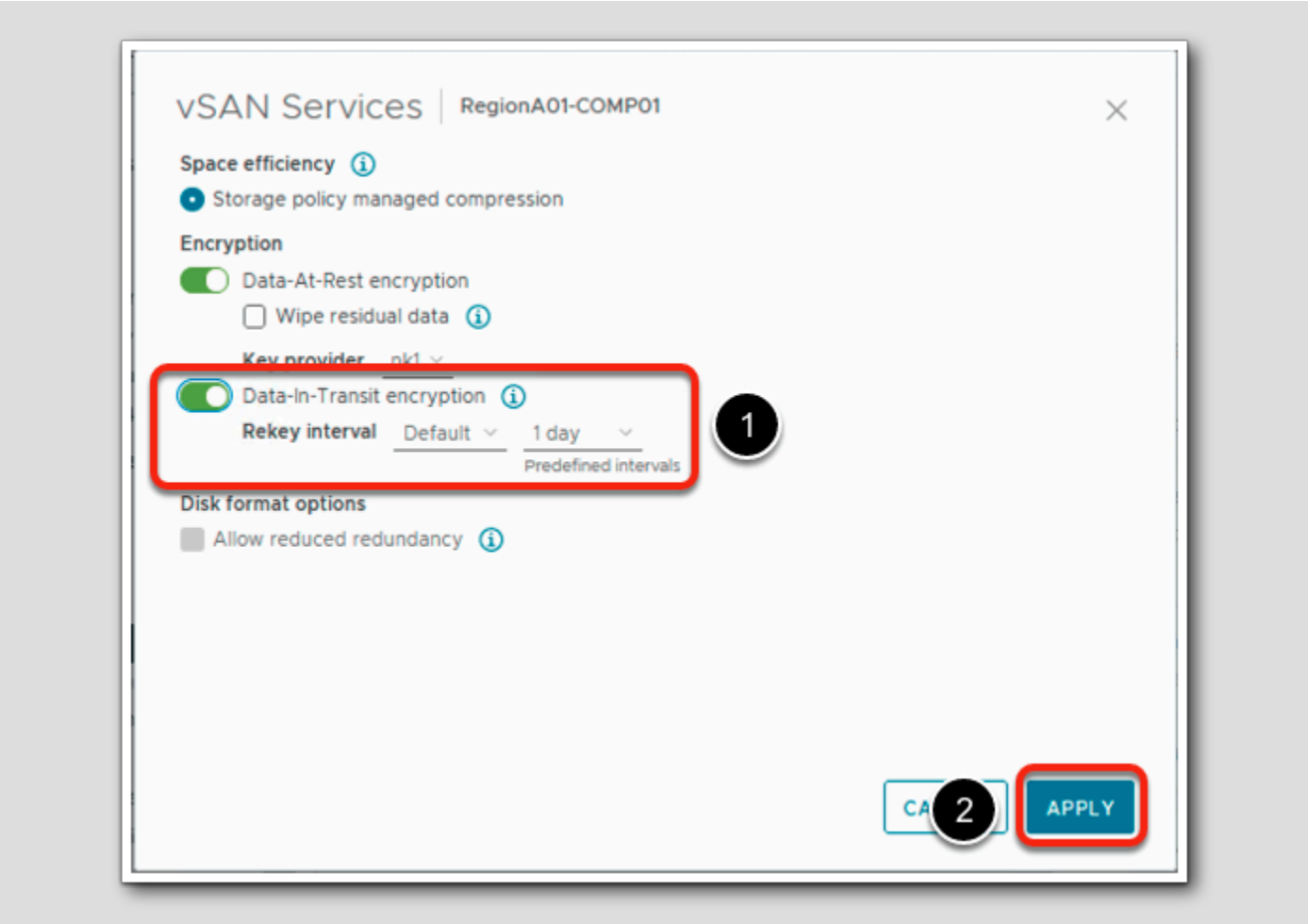
[97]



1. Select vSAN Cluster, **RegionA01-COMP01**
2. Click **Configure**
3. Select **vSAN > Services**
4. Expand **Data Services** and click **Edit** (You may need to scroll down the screen to find the Data Services tile)

Enable Data-In-Transit Encryption

[98]

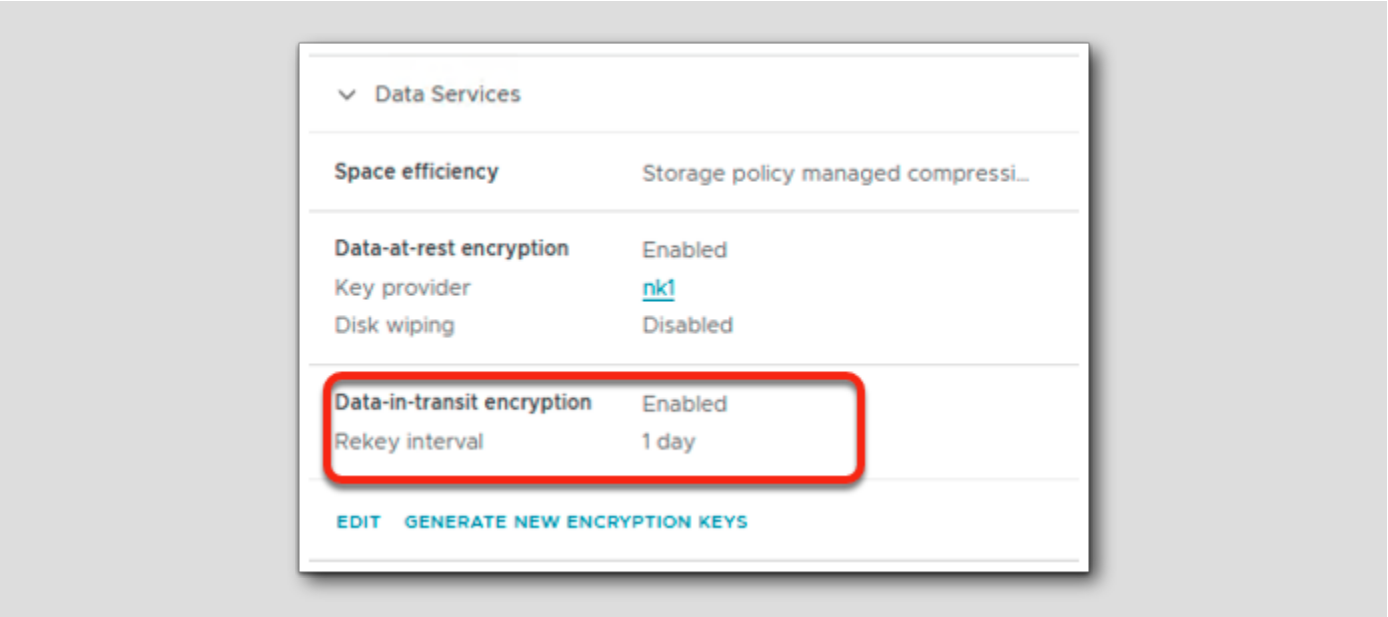


When you enable Data-In-Transit Encryption, rekey interval can be set. By default, it is set for 1 day but you can customize it as needed.

1. **Toggle** on Data-In-Transit encryption to be enable the service.
2. Click on **APPLY**

Enable Data-In-Transit Encryption

[99]



Verify **Data-in-Transit Encryption** is **Enabled**

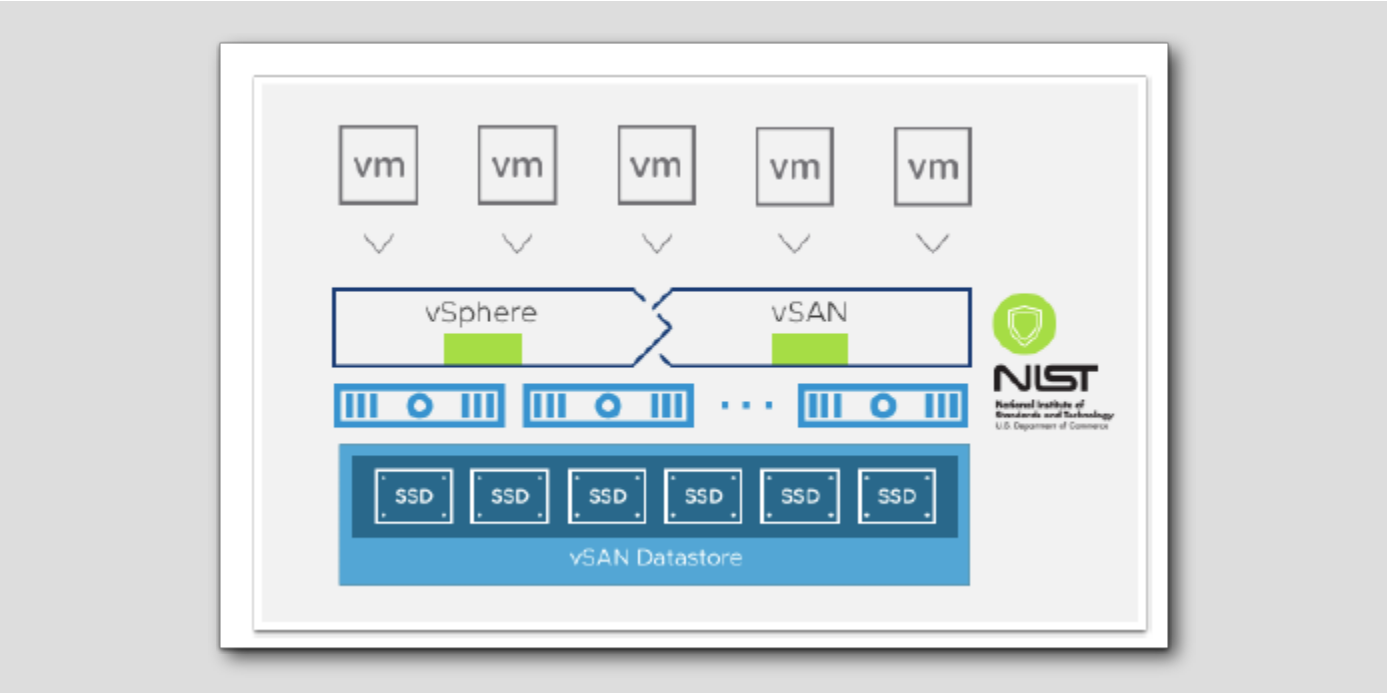
DISA STIG (FIPS 140-2) Validated

[100]

vSAN offered the first native HCI encryption solution for data-at-rest since 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

[101]



vSAN takes an important step forward with improved security since 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

[102]

vSAN can perform data at rest encryption. With vSAN Express Storage Architecture data is encrypted in the upper layers of vSAN to reduce both CPU cost and I/O amplification. 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.

Configuring the Key Management Server

[103]

A Key Management Server (KMS) cluster provides the keys that you can use to encrypt the vSAN datastore. This can be either an external KMS or you can utilize vSphere's Native Key Provider.

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.

In this lab, we have already encrypted the vSAN datastore, however we will create a new Native Key Provider and performa a shallow rekey of the datastore.

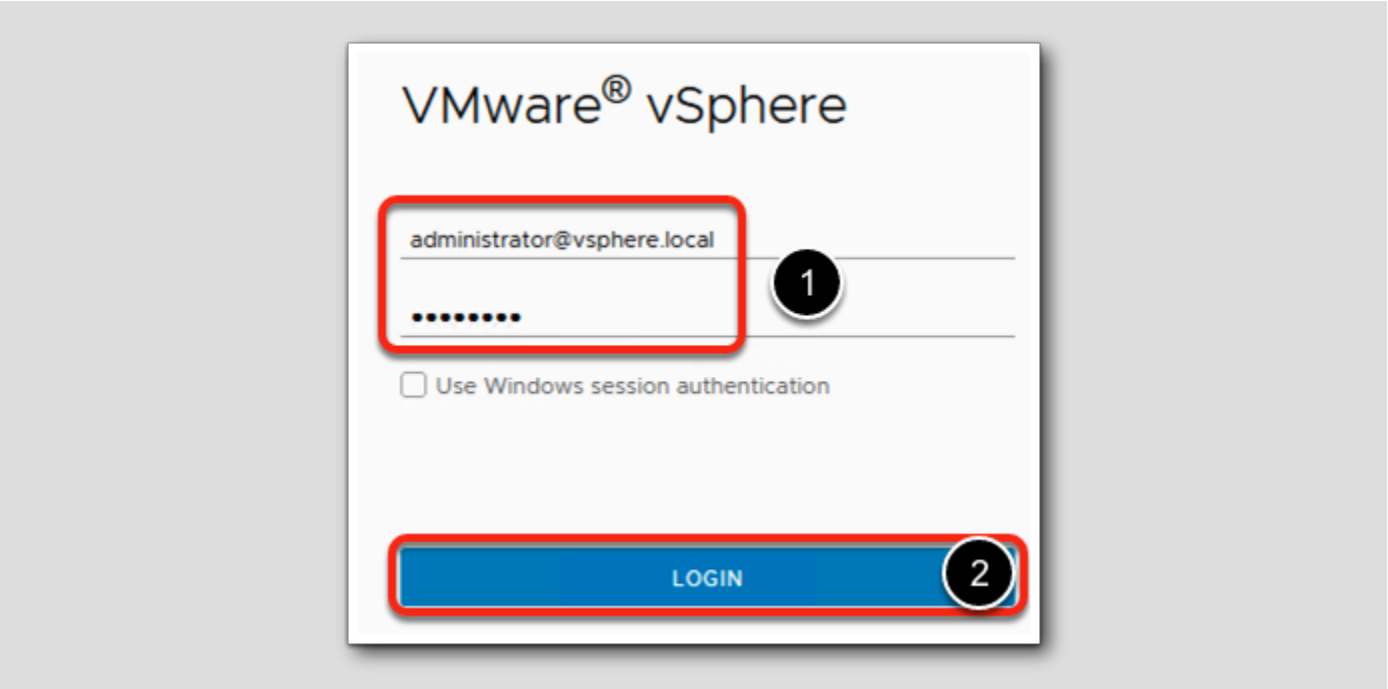
Launch vSphere Client

[104]

1. If Firefox is not already running, Click on the Firefox Icon on the Windows Quick Launch Task Bar.

Login to vSphere Client

[105]



1. On the vSphere Client login screen, enter the following :

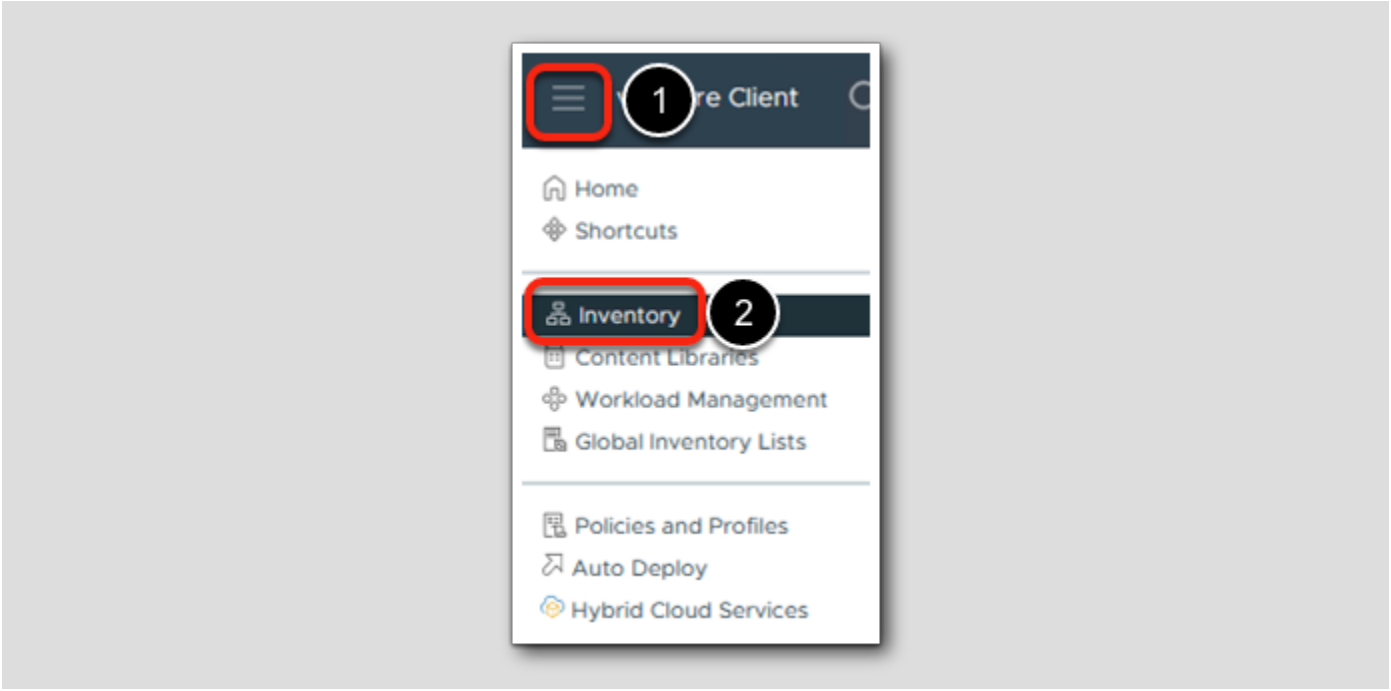
   Username : administrator@vsphere.local

   Password : VMware123!

2. Click **Login**

Select Inventory

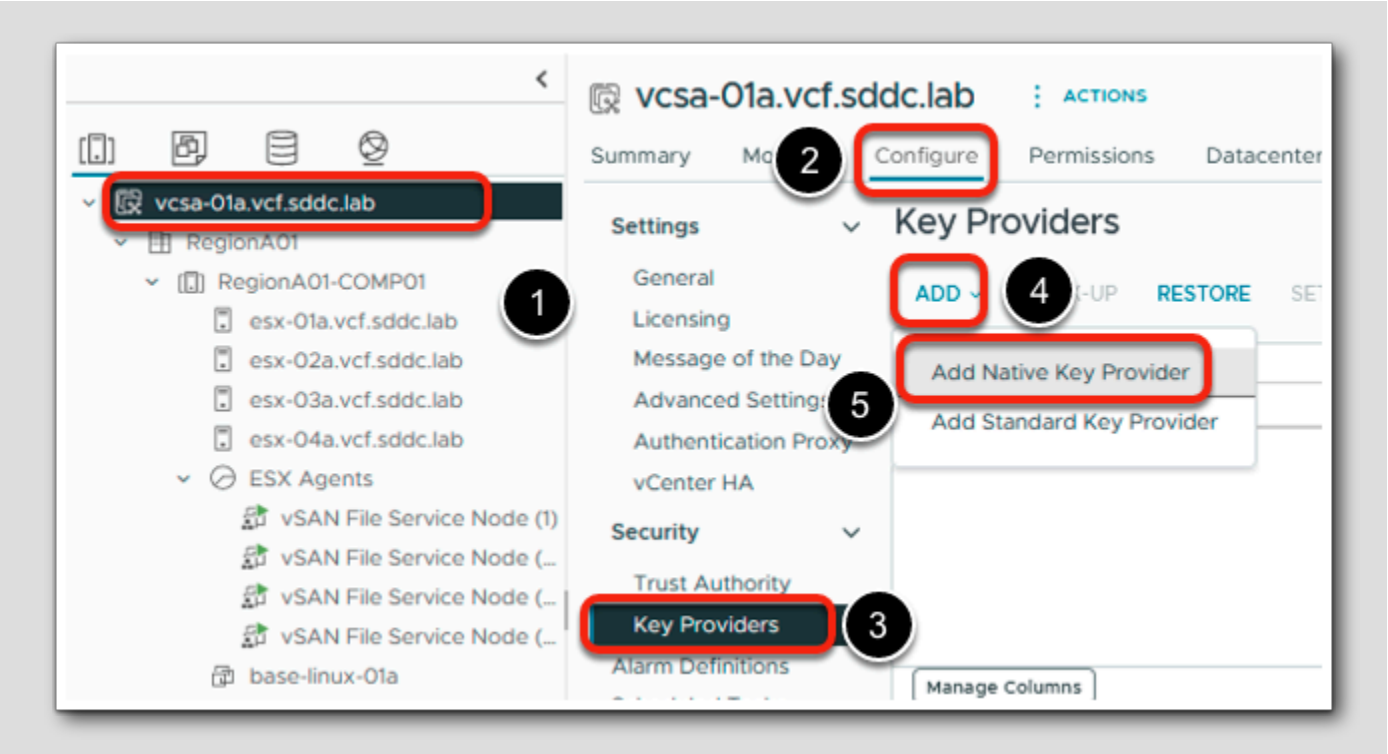
[106]



1. Click the **Menu** icon
2. Select **Inventory**

Add Key Management Server settings

[107]



A Key Management Server (KMS) cluster provides the keys that you can use to encrypt the vSAN datastore.

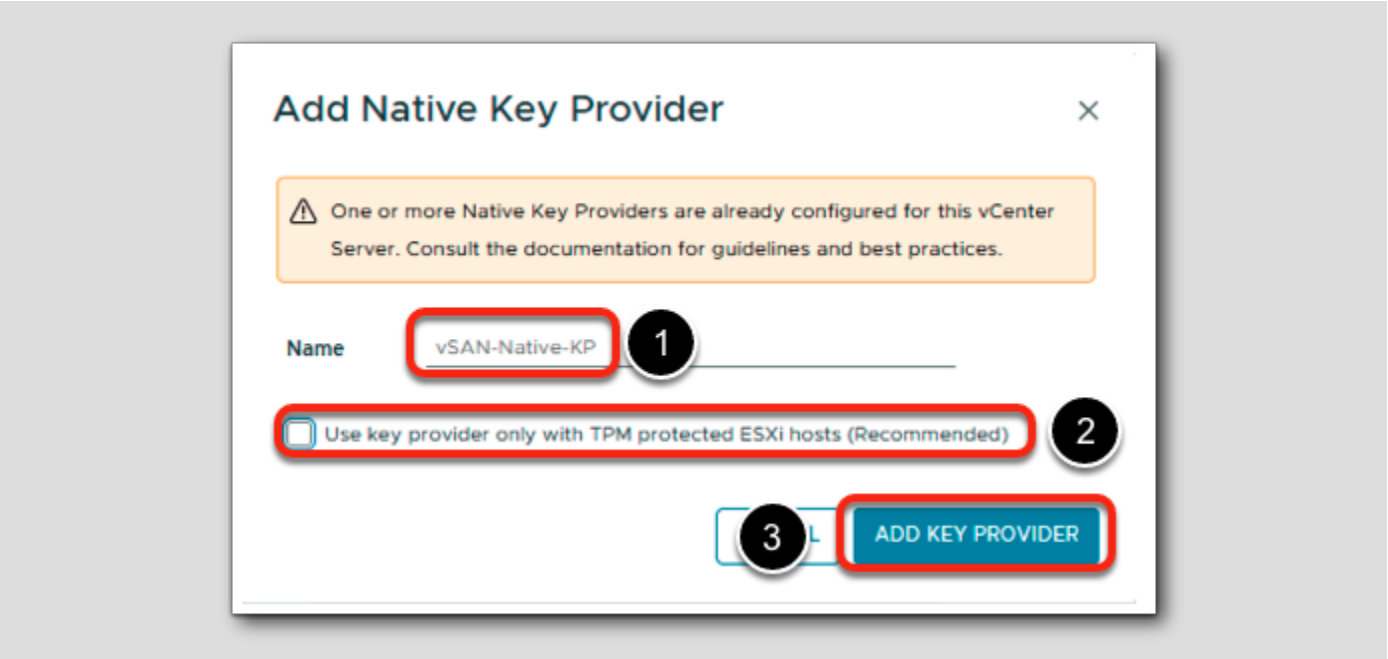
Before you can encrypt the vSAN datastore, you must add a Key Provider.

That task includes adding the Native Key Provider.

1. Select the vCenter Server called **vcsa-01a.vcf.sddc.lab**
2. Select **Configure**
3. Select **Security > Key Providers**
4. Click **ADD**
5. Select **Add Native Key Provider**

Add Key Management Server

[108]



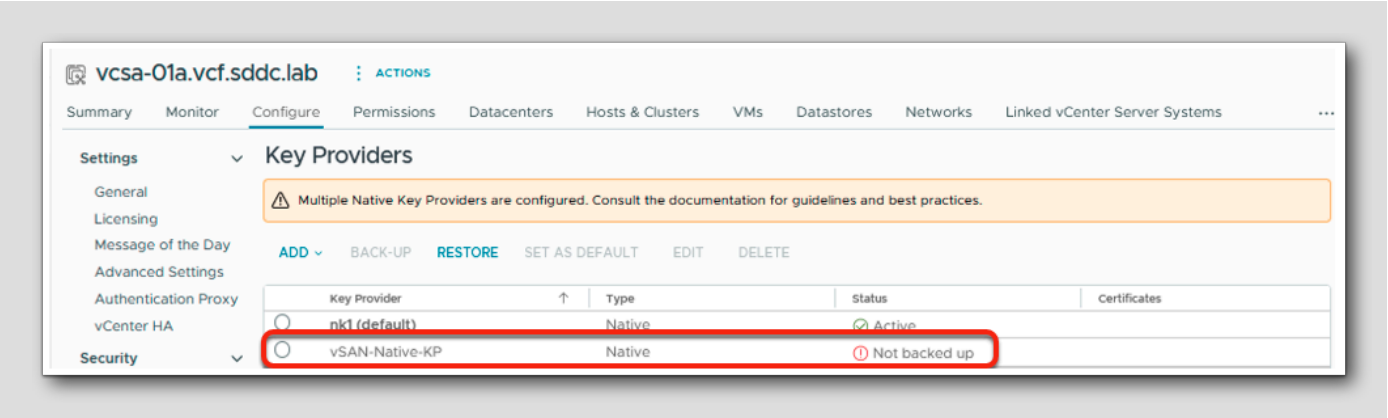
1. Enter the following information for the Native Key Provider:

- Name : `vSAN-Native-KP`

2. Since this is a nested environment, uncheck the "**Use key provider only with TPM...**" box
3. Click **ADD KEY PROVIDER**

Add Native Key Provider

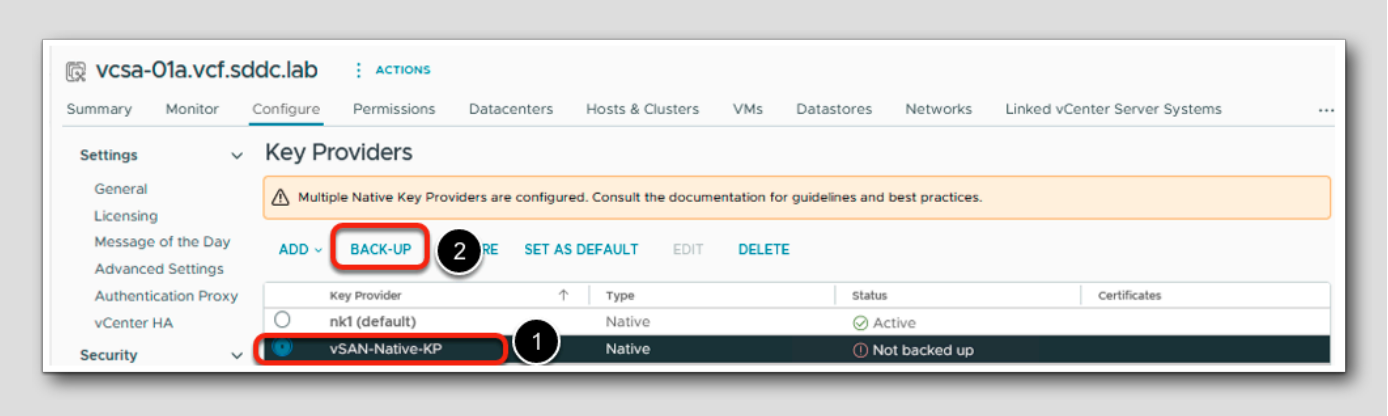
[109]



The Key Provider is added. We can see that the Type is **Native** and the Status is **Not backed up**.

Verify Key Management Server

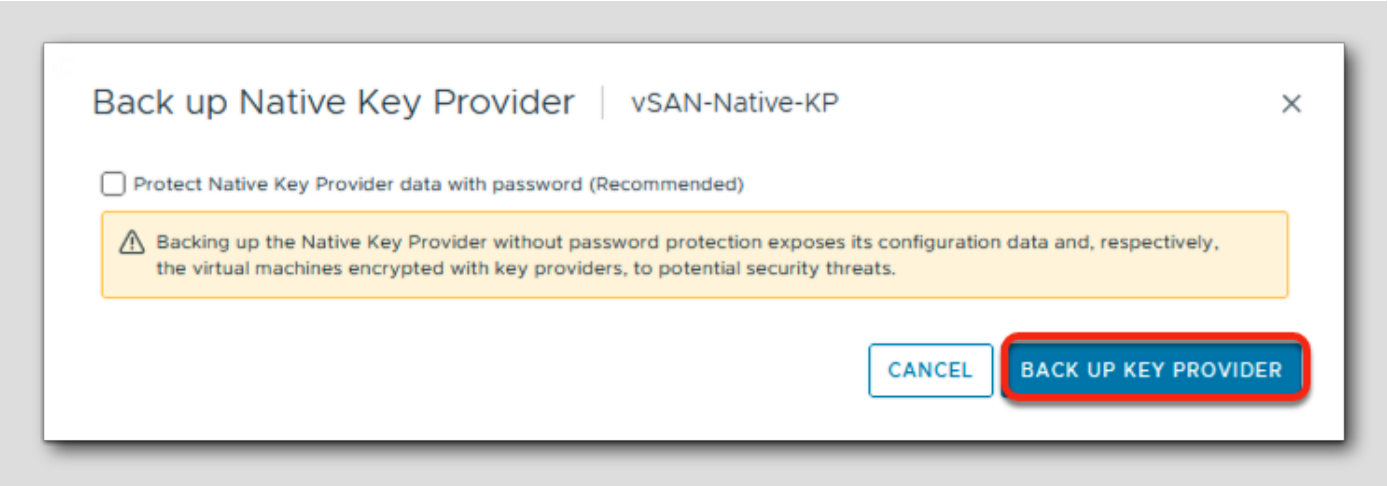
[110]



1. Select the Key Provider called **vSAN-Native-KP (default)**
2. Click **BACK-UP**

Verify Key Management Server

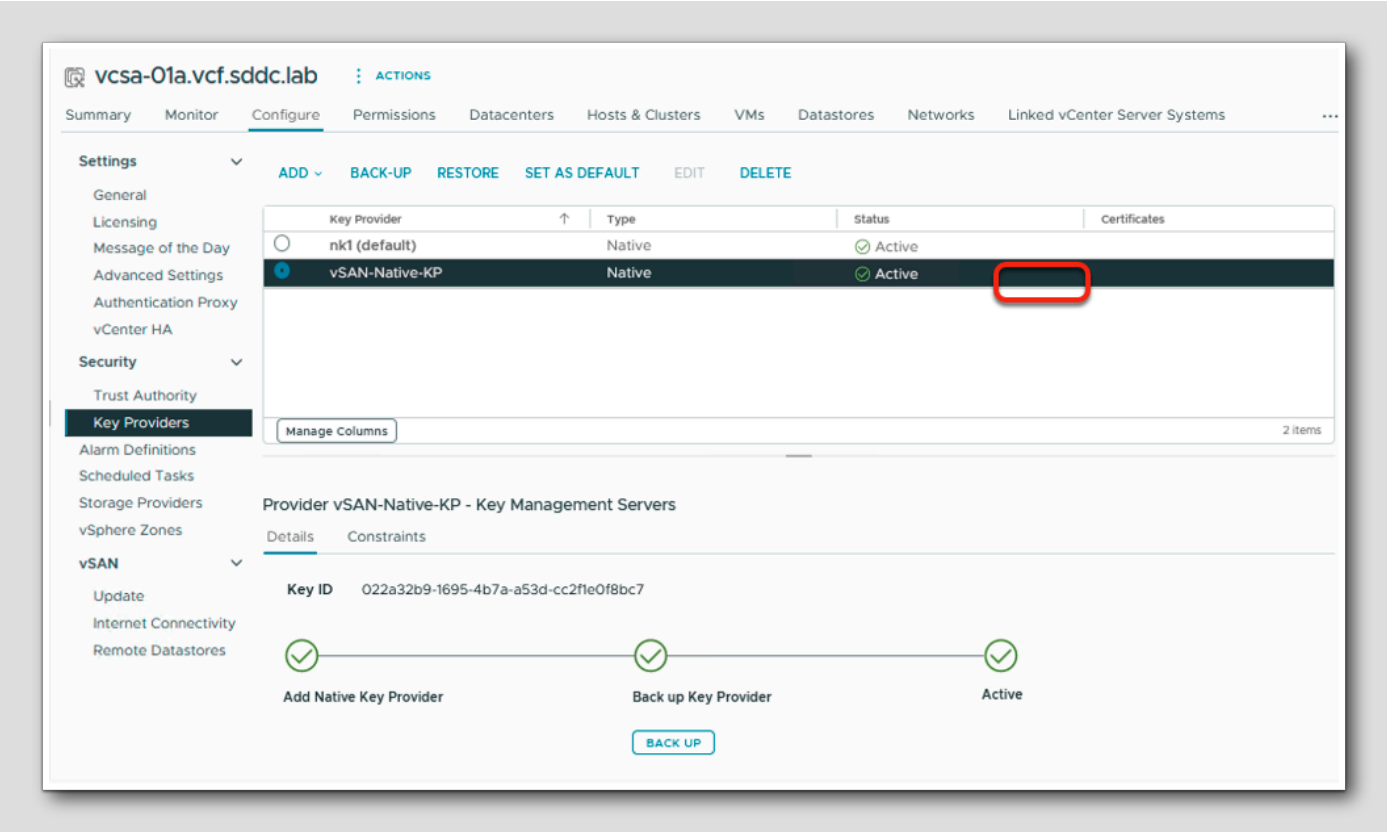
[111]



1. Click **BACK UP KEY PROVIDER**

Verify Key Management Server

[112]



1. Scroll down and verify that the Key Provider now shows a status of Active.

Enabling vSAN Encryption

[113]

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.

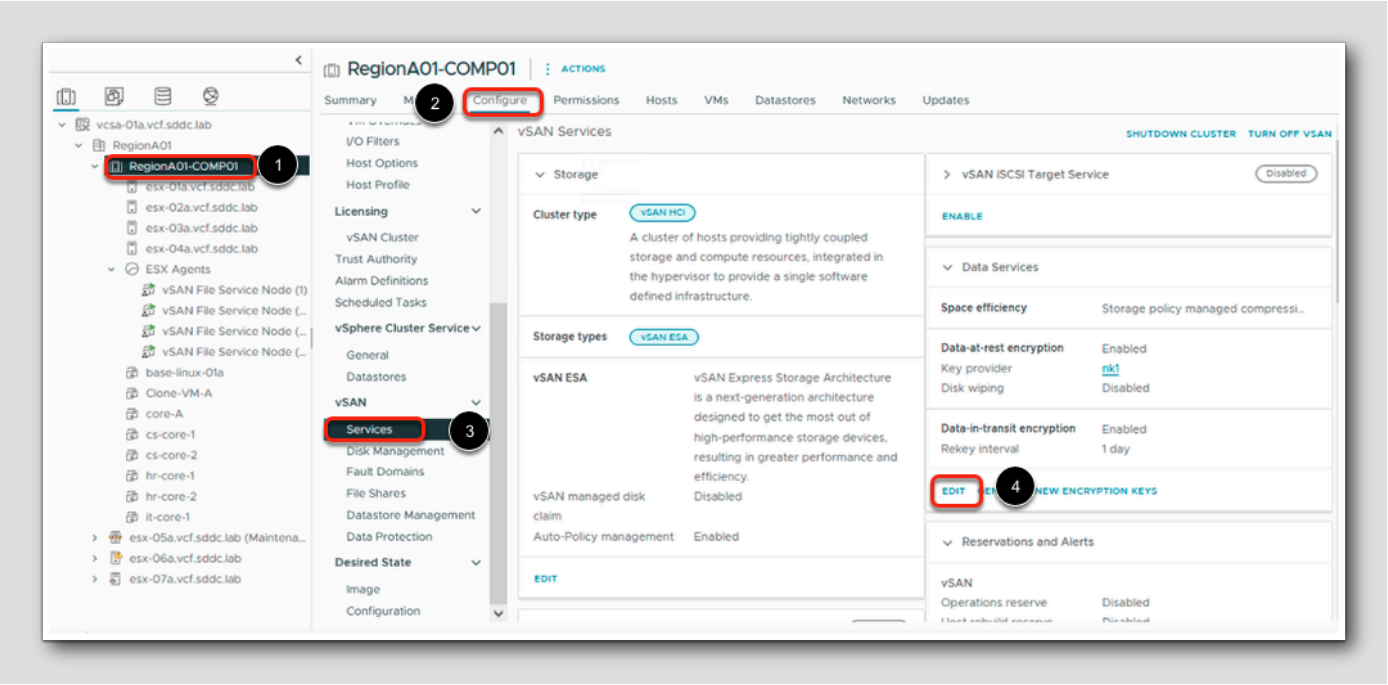
Because it runs at the hypervisor level and not in the context of the virtual machine, it is virtual machine agnostic, like VM Encryption.

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.

In this lab, data-at-rest encryption has already been enabled, however we will perform a shallow rekey which will cover the same steps as enabling data-at-rest encryption for the first time.

Enabling vSAN Encryption

[114]



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. Under Data Services, Click **EDIT** (You may need to scroll down the screen to find the Data Services tile)

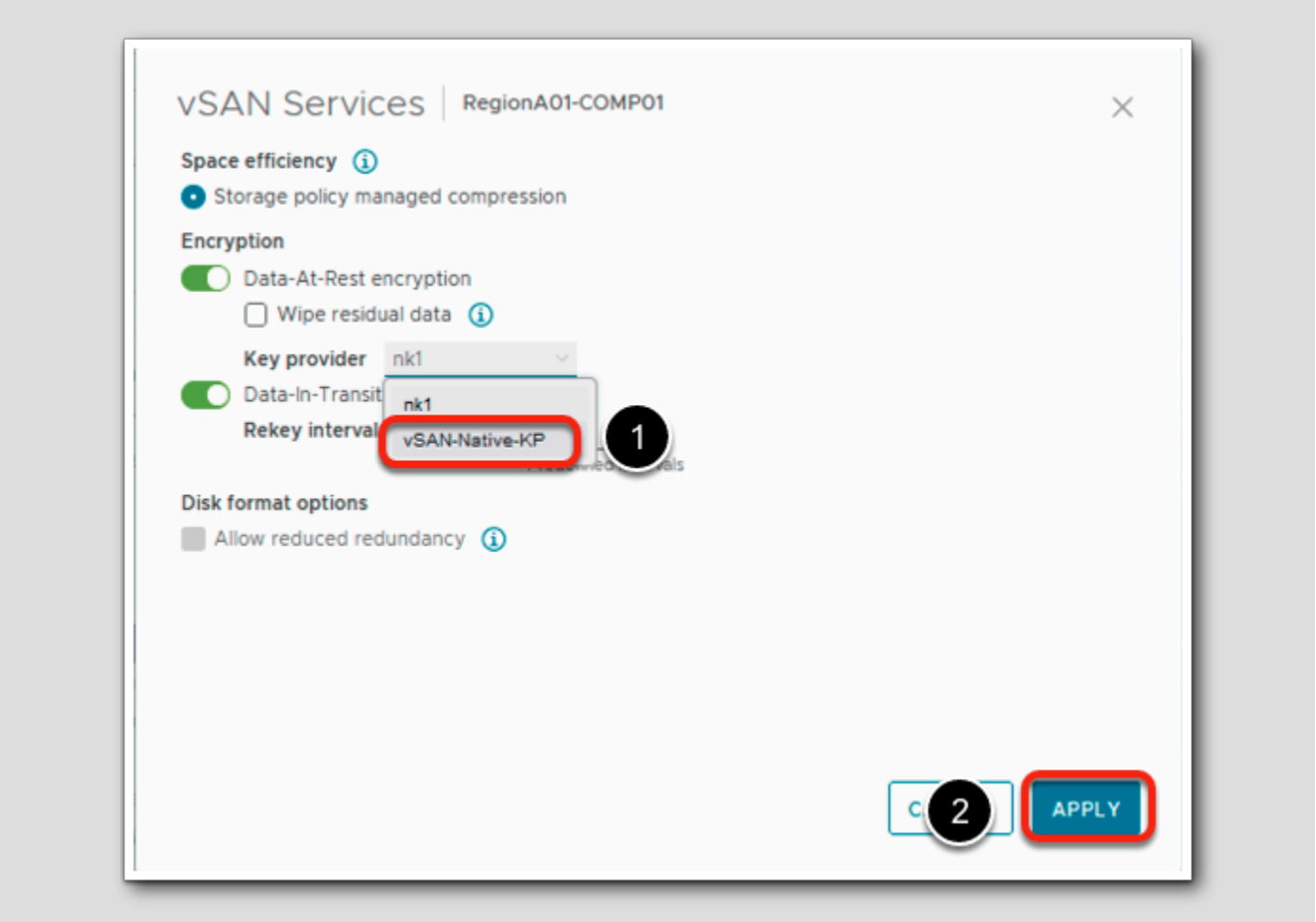
Turning on encryption is a simple matter of clicking a checkbox. Encryption can be enabled when vSAN is enabled or after and with or without virtual machines (VMs) residing on the vSAN datastore.

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

[115]



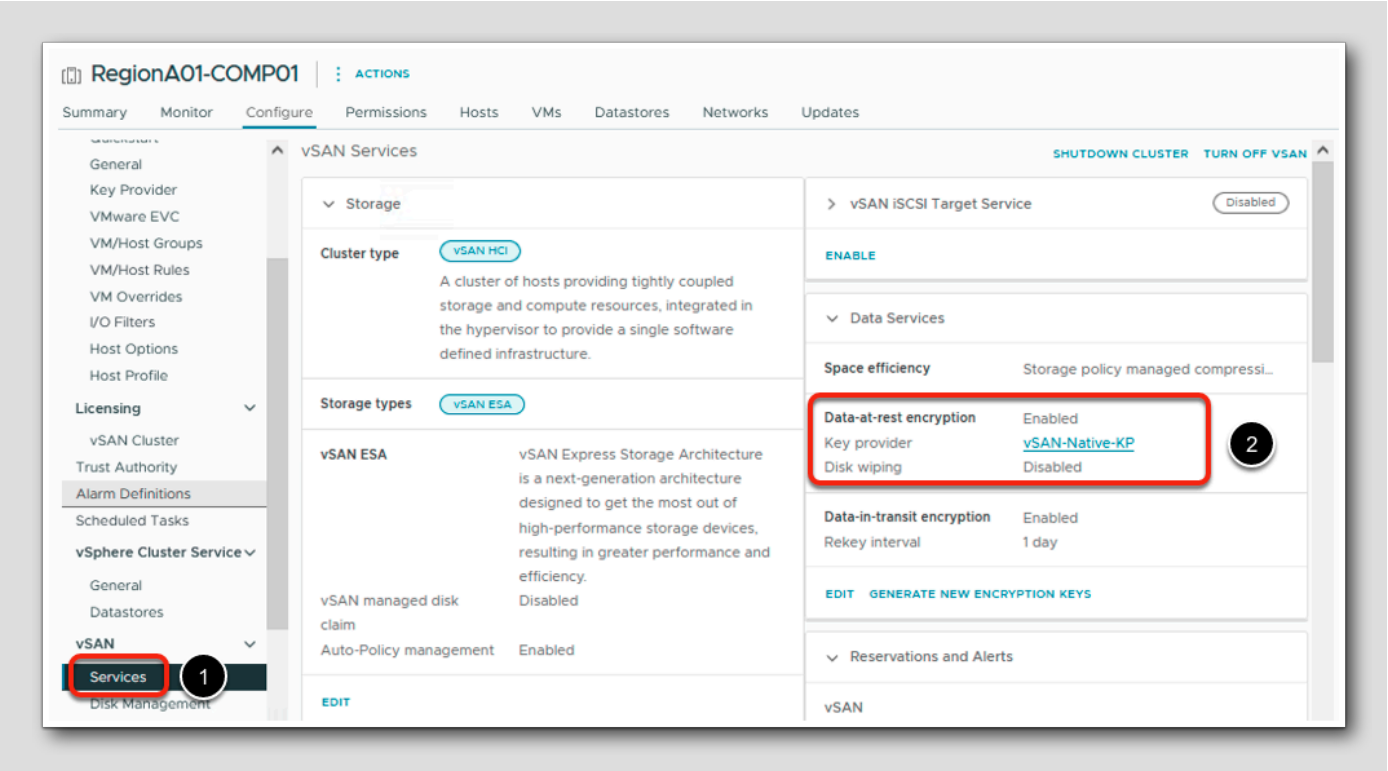
Enabling vSAN Encryption is a one click operation.

1. You'll see that **Data-at-rest Encryption is already toggled on**
2. Change the Key Provider from **nk1** to **vSAN-Native-KP**.
    a. Click on the information button **(i)** for these options to get additional information on these options.
3. Click **APPLY**

The Wipe residual data 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.

Enabling vSAN Encryption

[116]



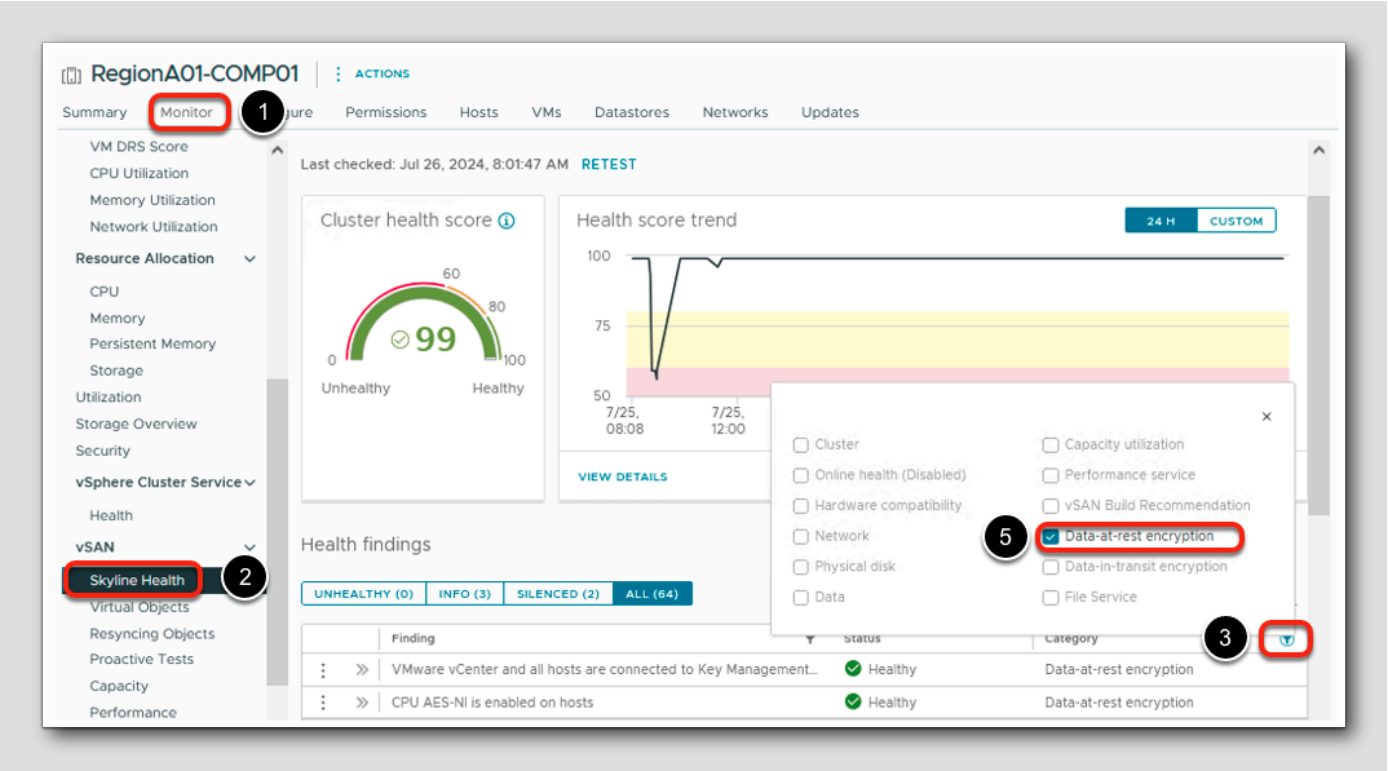
1. Select **vSAN** > **Services**
2. Expand **Data Services** and confirm that the Key provider is set to **vSAN-Native-KP**

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

[117]

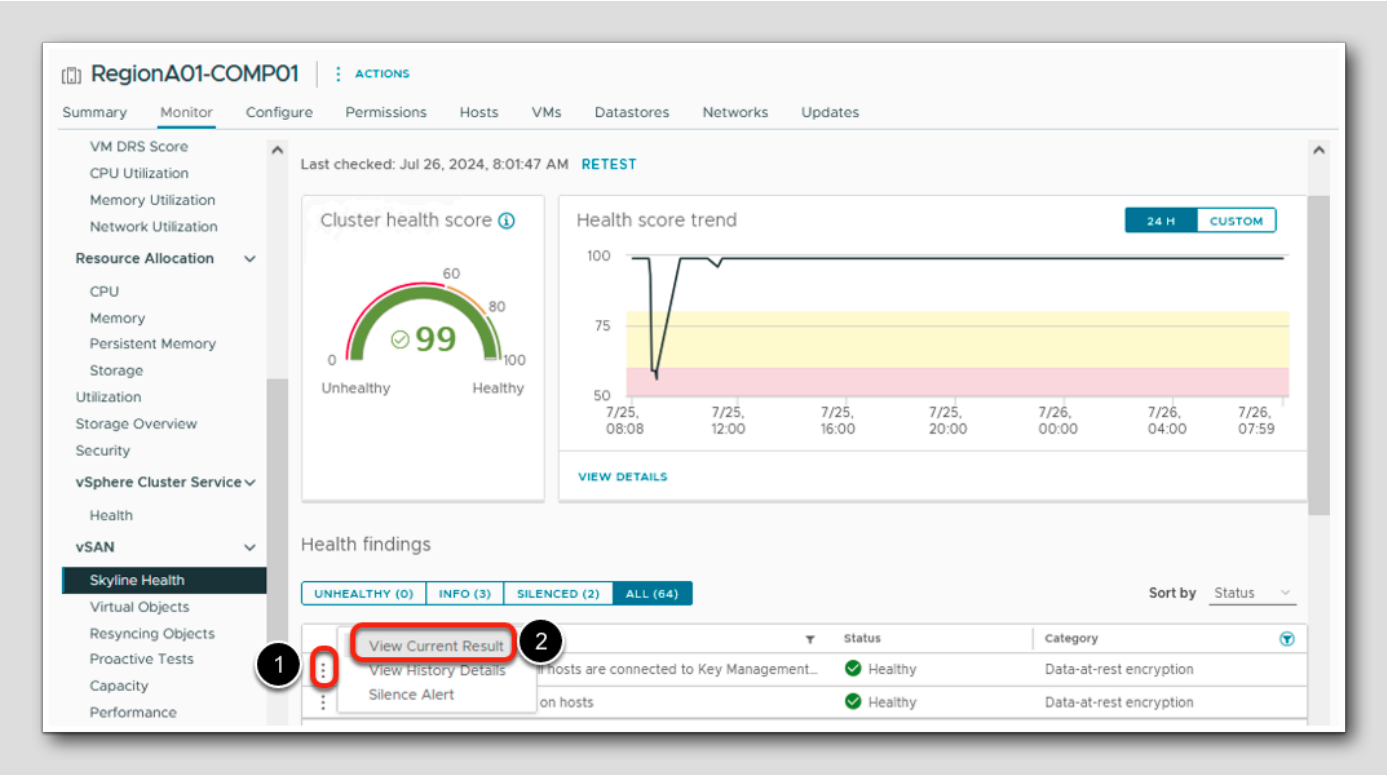


There are vSAN Health Checks to verify that your vSAN Encryption is enabled and healthy.

1. With the cluster **RegionA01-COMP01** selected, Select **Monitor**.
2. Select **vSAN > Skyline Health**
3. Scroll down and click on the filter icon next to the **Category** column
4. Check **Data-at-rest encryption**

There are 2 Health Checks associated with vSAN Encryption.

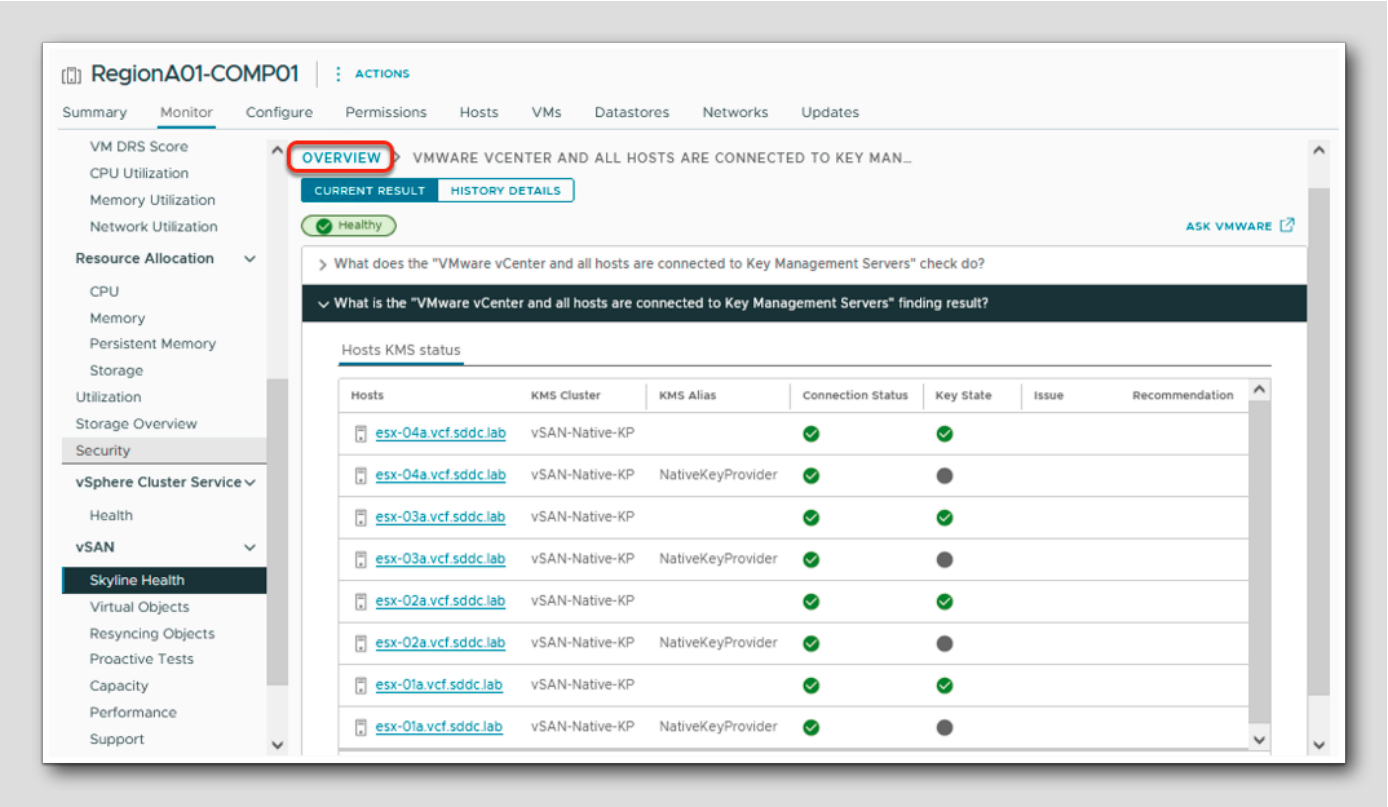
vSAN Encryption Health Check



1. Expand the **Finding** column and click the 3-dotted menu next to **vCenter and all hosts are connected to Key Management Servers**
2. Click **View Current Result**

vSAN Encryption Health Check

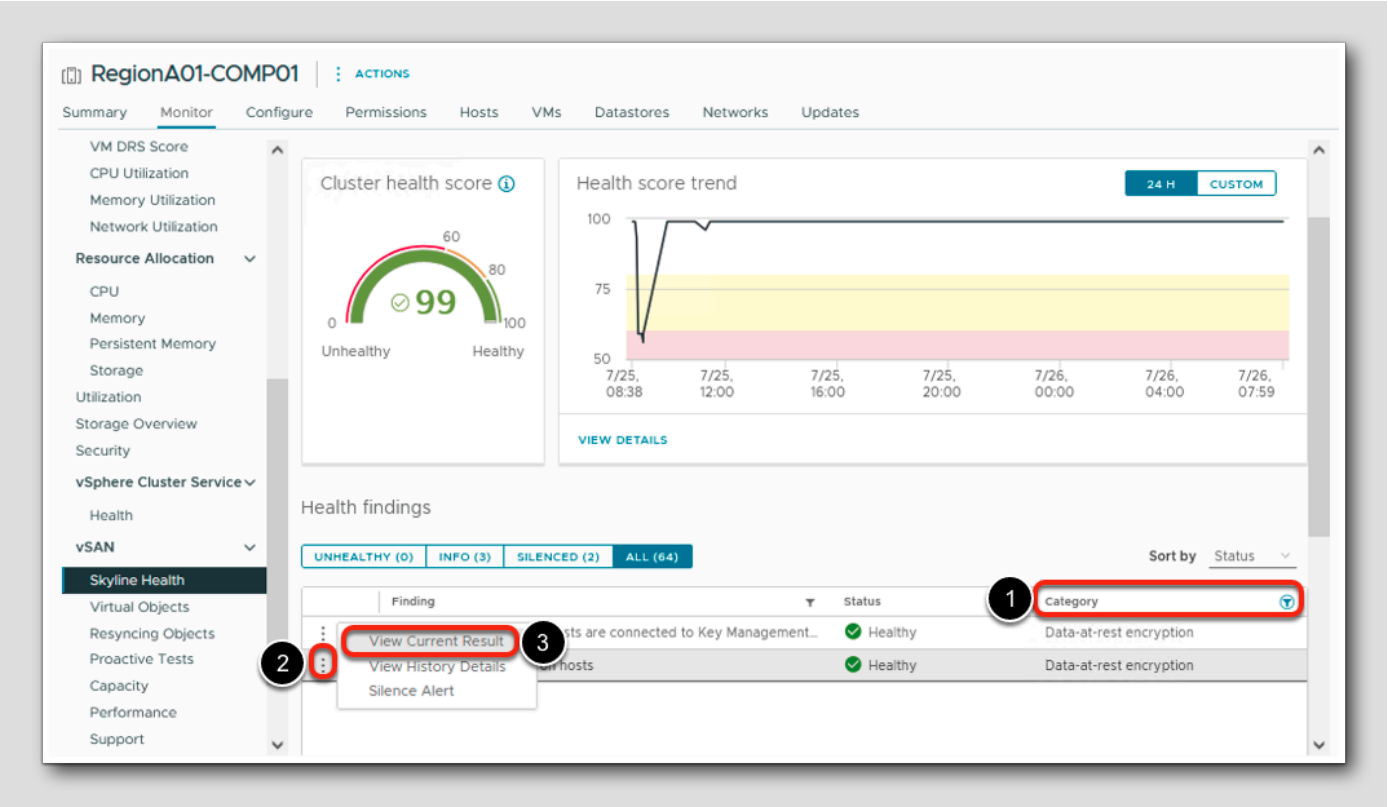
[119]



This vSAN Health Check verifies that the ESXi Key Provider Status and lists the Connection Status and Key State

After reviewing the information, click on **Overview**

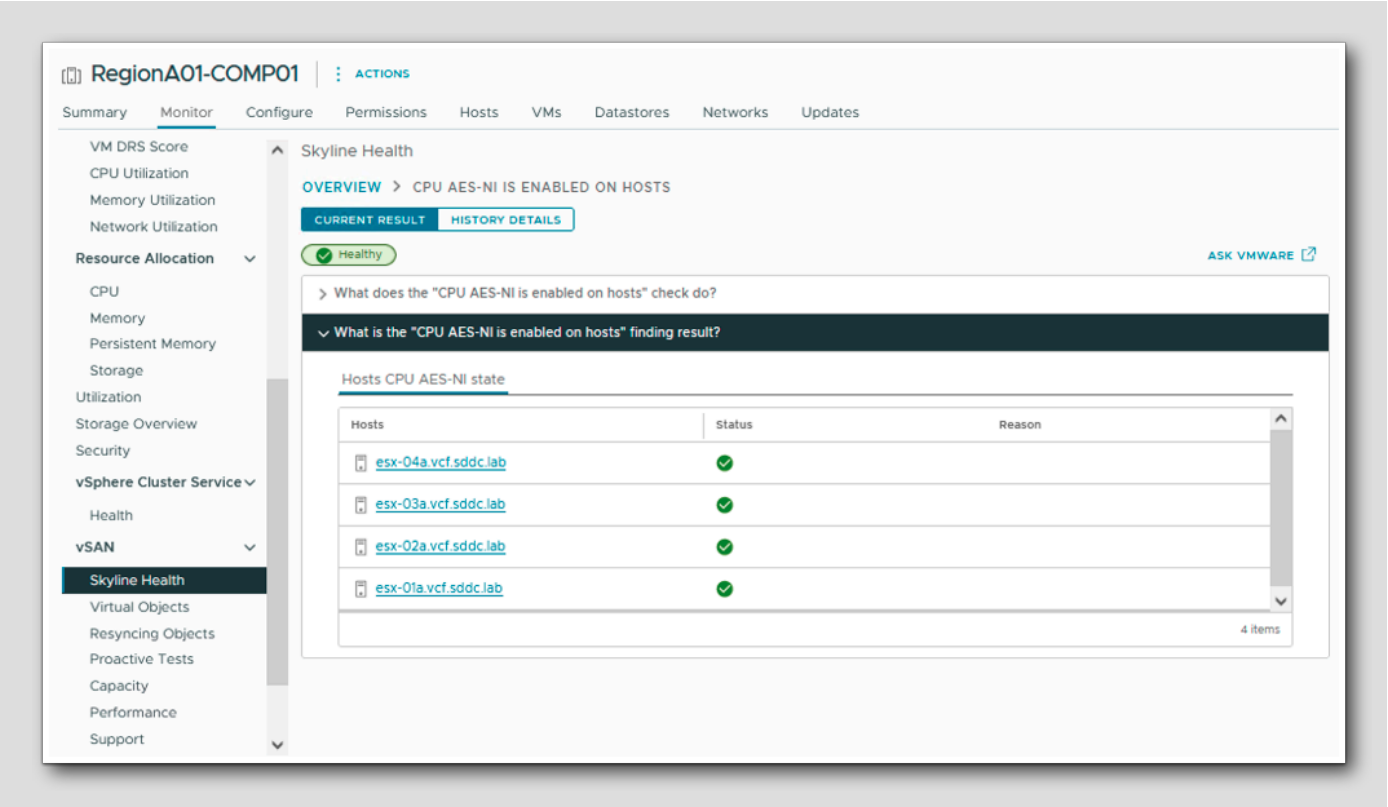
vSAN Encryption Health Check



1. Filter the **Category** column and select **Data-at-rest encryption.**
2. Click the three dots next to **CPU AES-NI is enabled on hosts**
3. Click **View Current Result**

vSAN Encryption Health Check

[121]



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

[122]

In this lesson we explored vSAN security parameters including DISA STIG (FIPS 104-2) Validation and vSAN Data-at-rest Encryption.

You Finished Module 3

[123]

Congratulations on completing Module 3.

If you are looking for additional information on topic:

- VMware Security Certification
- vSAN Datasheet (including FIPS 140-2 Information)
- vSAN Encryption
- Go to VMware Cloud Platform Tech Zone - vSAN for all things related to vSAN.

To take additional modules, please follow one of the links below:

- Module 1 - vSAN SPBM and Availability (30 minutes) (Basic) Introduction to VMware vSAN's Express Storage Architecture. We will cover the power of Storage Based Policy Management (SPBM) and show you the availability of vSAN.
- Module 2 - Monitoring, Health, Capacity, and Performance (30 minutes) (Basic) 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 4 - File services (30 minutes) (Basic) Introduction to vSAN's File Services capabilities. We will create both NFS and SMB file shares and mount them to their respective clients.
- Module 5 - Data Protection (30 minutes) (Advanced) Introduction to vSAN ESA's new data protection capabilities. We will cover creating protection groups and snapshot schedules.
- Module 6 - vSAN Stretched Cluster (30 minutes) (Advanced) Introduction to vSAN Stretched Clusters. We will convert an existing vSAN cluster into a stretched cluster. In addition, we will explore storage policies as well as Skyline Health checks with respect to stretched clusters.

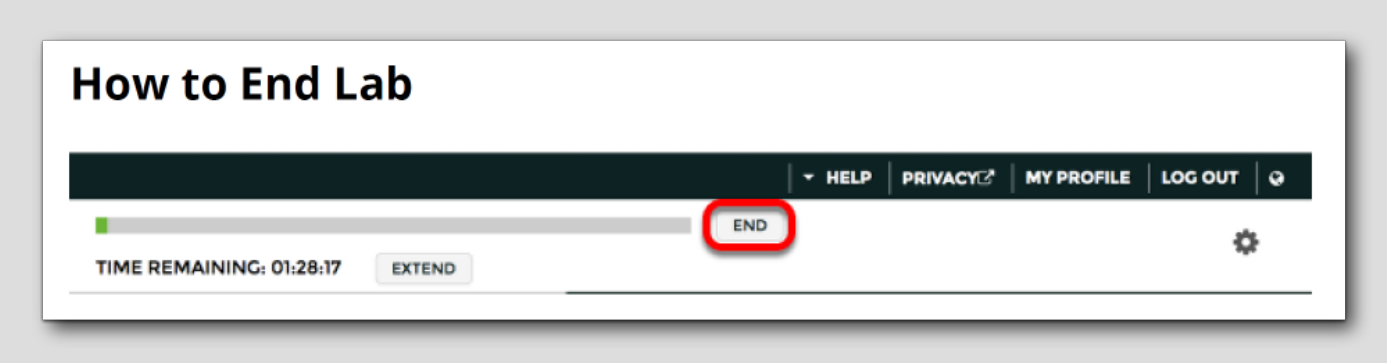
Test Your Skills

[124]

Now that you've completed this lab, try testing your skills with VMware Odyssey, our newest Hands-on Labs gamification program. We have taken Hands-on Labs to the next level by adding gamification elements to the labs you know and love. Experience the fully automated VMware Odyssey as you race against the clock to complete tasks and reach the highest ranking on the leaderboard. Try the vSAN Odyssey lab.

How to End Lab

[125]



If you would like to end your lab click on the END button.

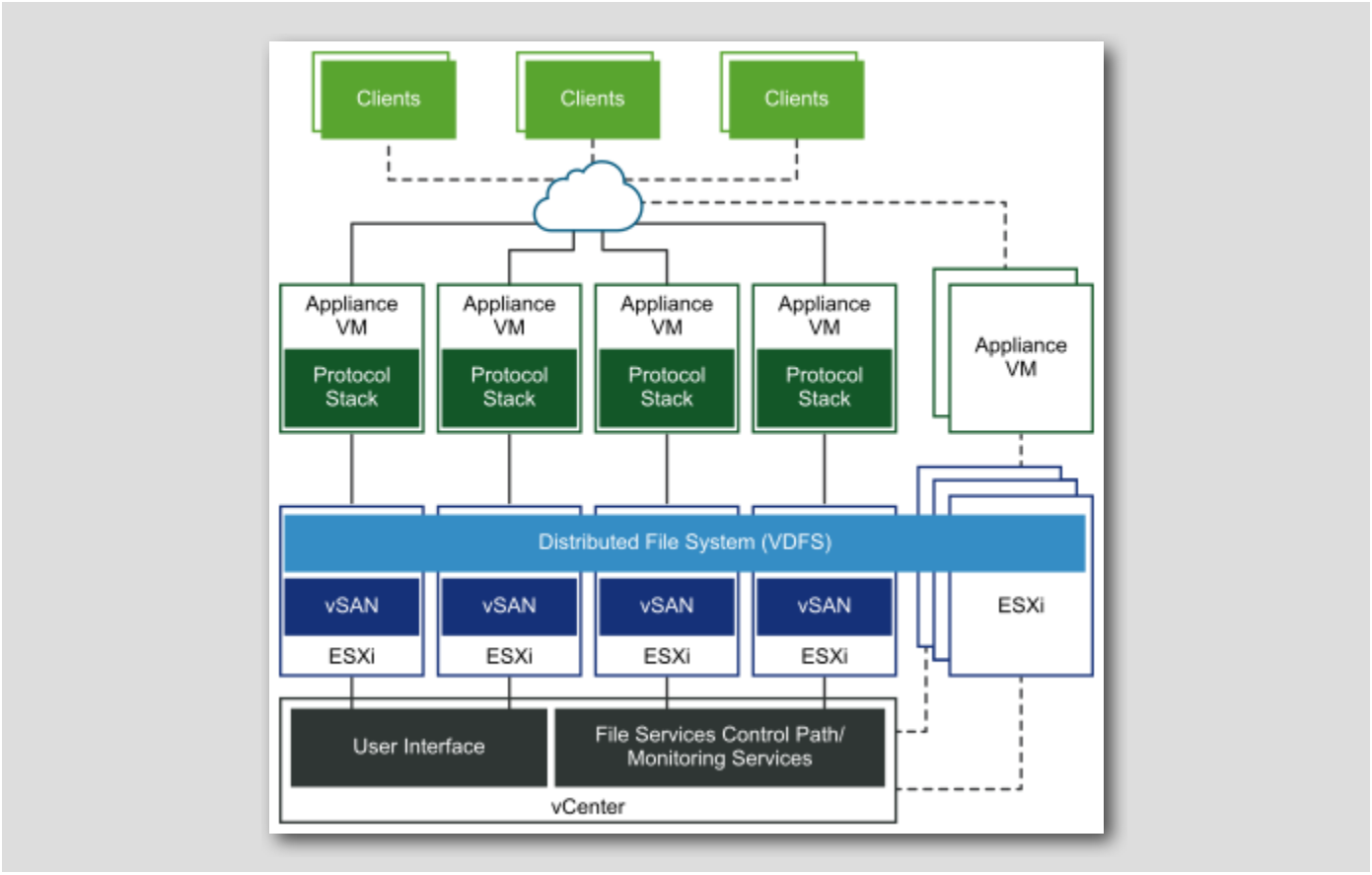
Module 4 - File Services (30 minutes) Basic

vSAN File Services Overview

[127]

The vSAN File Services are used to create file shares in the vSAN datastore that client workstations or VMs can access. The data stored in a file share can be accessed from any device that has access rights.

vSAN File Service is a layer that sits on top of vSAN to provide file shares. It currently supports SMB, NFSv3 and NFSv4.1 file shares. vSAN File Service comprises of vSAN Distributed File System (vDFS) which provides the underlying scalable filesystem by aggregating vSAN objects, a Storage Services Platform which provides resilient file server end points and a control plane for deployment, management and monitoring. File shares are integrated into the existing vSAN Storage Policy Based Management, and on a per-share basis. vSAN File Service brings in capability to host the file shares directly on the vSAN cluster.



When you configure the vSAN File Service, vSAN creates a single vDFS distributed file system for the cluster which will be used internally for management purposes. vSAN File Services is powered and managed by the vSphere platform that deploys a set of containers on each of the hosts. These containers act as the primary delivery vehicle to provision file services and are tightly integrated with the hypervisor.

A static IP address pool should be provided as an input while enabling the file service workflow. One of the IP addresses is designated as the primary IP address. The primary IP address can be used for accessing all the shares in the File Services cluster with the help of SMB and NFSv4.1 referrals. A file server is started for every IP address provided in the IP pool. However, the file shares are evenly distributed across all the file servers. To provide computing resources that help manage access requests, the number of IP addresses

must be equal to the number of hosts in the vSAN cluster. These IP addresses must have DNS forward and reverse lookup entries.

- Configure File Services

  You can configure the File Service, which enables you to create file shares on your vSAN datastore. You can enable vSAN Files Service only on a regular vSAN cluster. Currently the File Service is not supported on a vSAN Stretched Cluster.

- Create a File Share

  When the vSAN File Service is enabled, you can create one or more file shares on the vSAN datastore. vSAN File Service does not support using these file shares as NFS datastores on ESXi.

- View File Shares

  You can view the list of vSAN file shares.

- Access File Shares

  You can access a file share from a host client, using an operating system that communicates with NFS file systems. For RHEL-based Linux distributions, NFS 4.1 support is available in RHEL 7.3 and CentOS 7.3-1611 running kernel 3.10.0-514 or later. For Debian based Linux distributions, NFS 4.1 support is available in Linux kernel version 4.0.0 or later. All NFS clients must have unique hostnames for NFSv4.1 to work. You can use the Linux mount command with the Primary IP to mount a vSAN file share to the client.

  - Access NFS Kerberos File Share (A linux client accessing an NFS Kerberos share should have a valid Kerberos ticket.)
  - Access SMB File Share (You can access an SMB file share from a Window client.)

- Edit a File Share

  You can edit the settings of a vSAN file share.

- Delete a File Share

  You can delete a file share when you no longer need it.

- Upgrade File Share

  When you upgrade the File Service, the upgrade is performed on a rolling basis. During the upgrade, the file server containers running on the virtual machines which are undergoing upgrade fails over to other virtual machines. The file shares remain accessible during the upgrade. During the upgrade, you might experience some interruptions while accessing the file shares.

- Monitor Performance

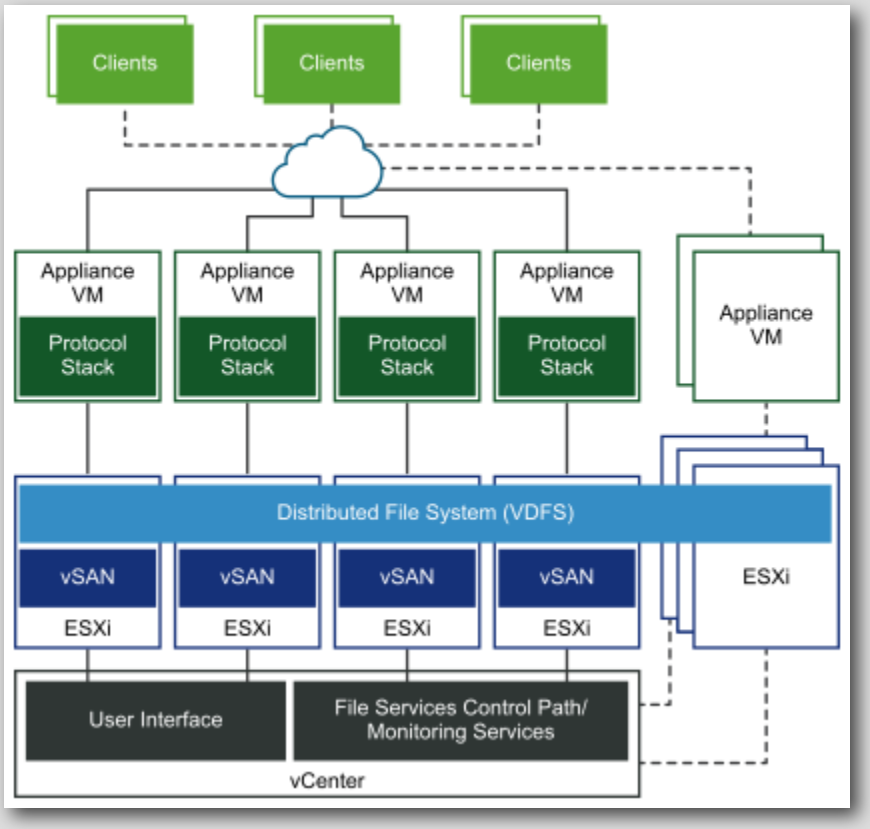
  You can monitor the performance of vSAN File Services.

- Monitor Capacity

  You can monitor the capacity for both native file shares and Cloud Native Storage managed file shares.

- Monitor Health

  You can monitor the health of both vSAN File Service and file share objects.



Enabling File Shares

[128]

To enable vSAN Files Services, we need to make sure we meet the network requirements:

- A static IP address to use as the single point of access to vSAN file shares. For best performance, the number of IP addresses must be equal to the number of hosts in the vSAN cluster.
- The static IP addresses should be part of the Forward lookup and Reverse lookup zones in the DNS server.
- All the static IP addresses should be from the same subnet.
- vSAN File services is supported on DVS version 6.6.0 or higher. Create a dedicated port group for vSAN File Service in the DVS.
- Promiscuous Mode and Forged Transmits are enabled as part of the vSAN File Services enablement process for provided network entity. If NSX based networks are being used, ensure that similar settings are configured for the provided network entity from the NSX admin console.

We have already ENABLED File Services in this lab.

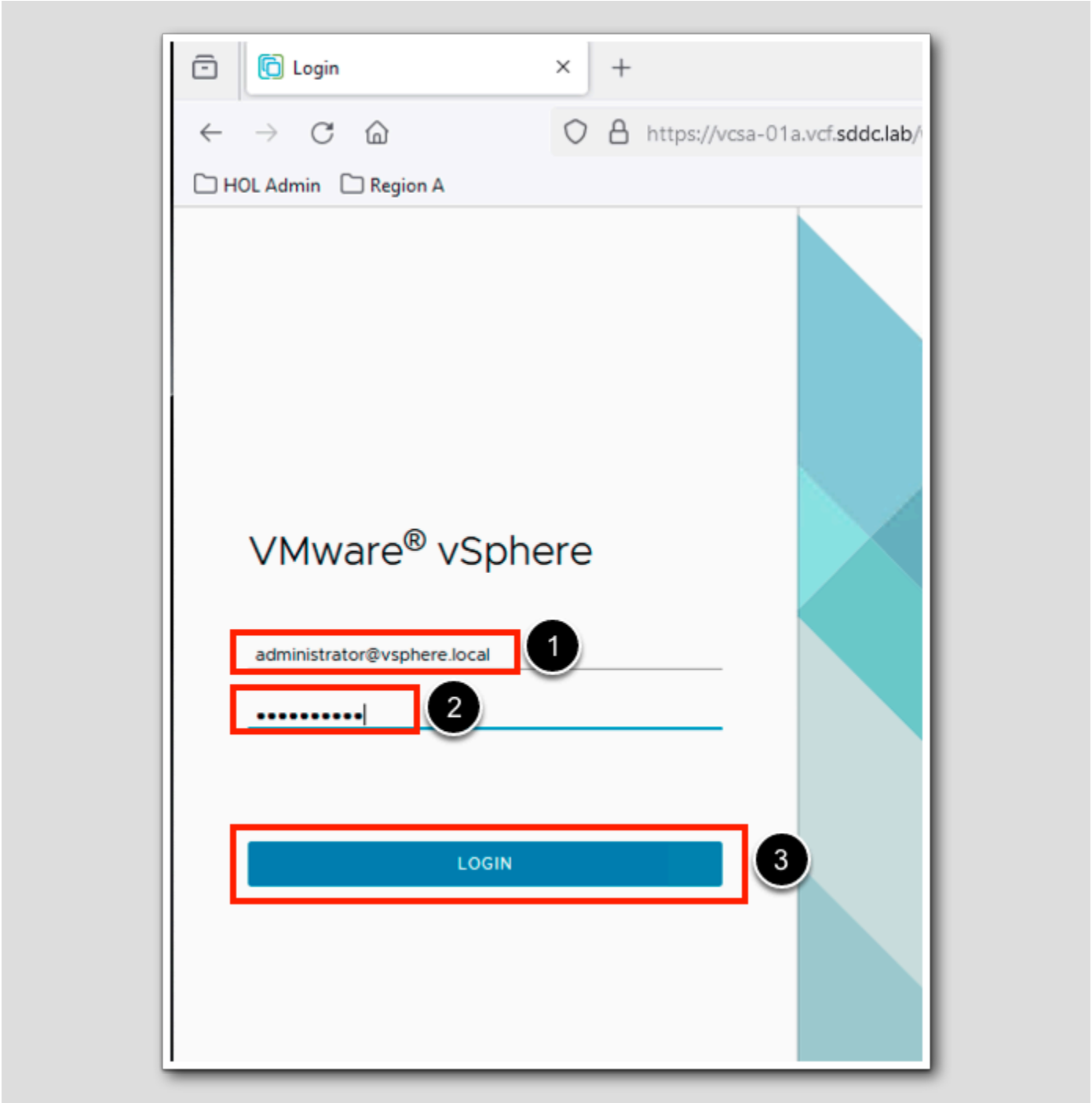
Open Firefox Browser from Windows Quick Launch Task Bar

[129]

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

Login to vSphere Client

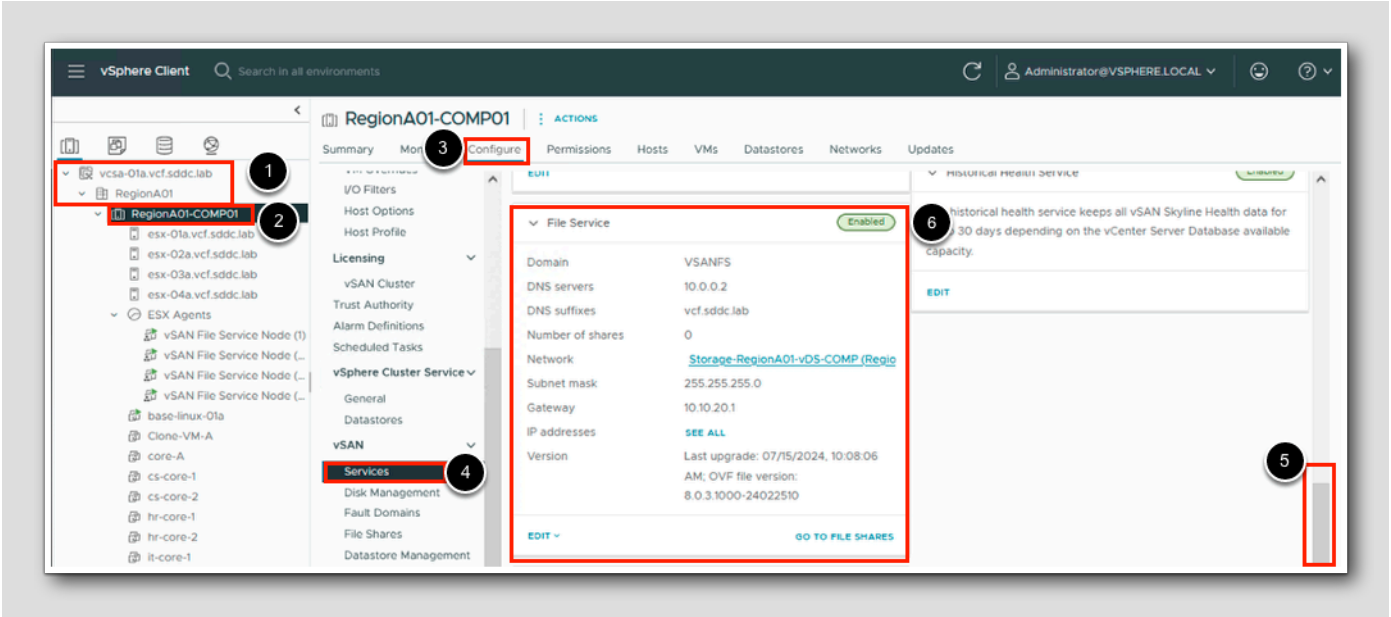
[130]



1. On the vSphere Client login screen, username: **administrator@vsphere.local**
2. Enter Password: **VMware123!**
3. Click **LOGIN**

Enable File Services

[131]



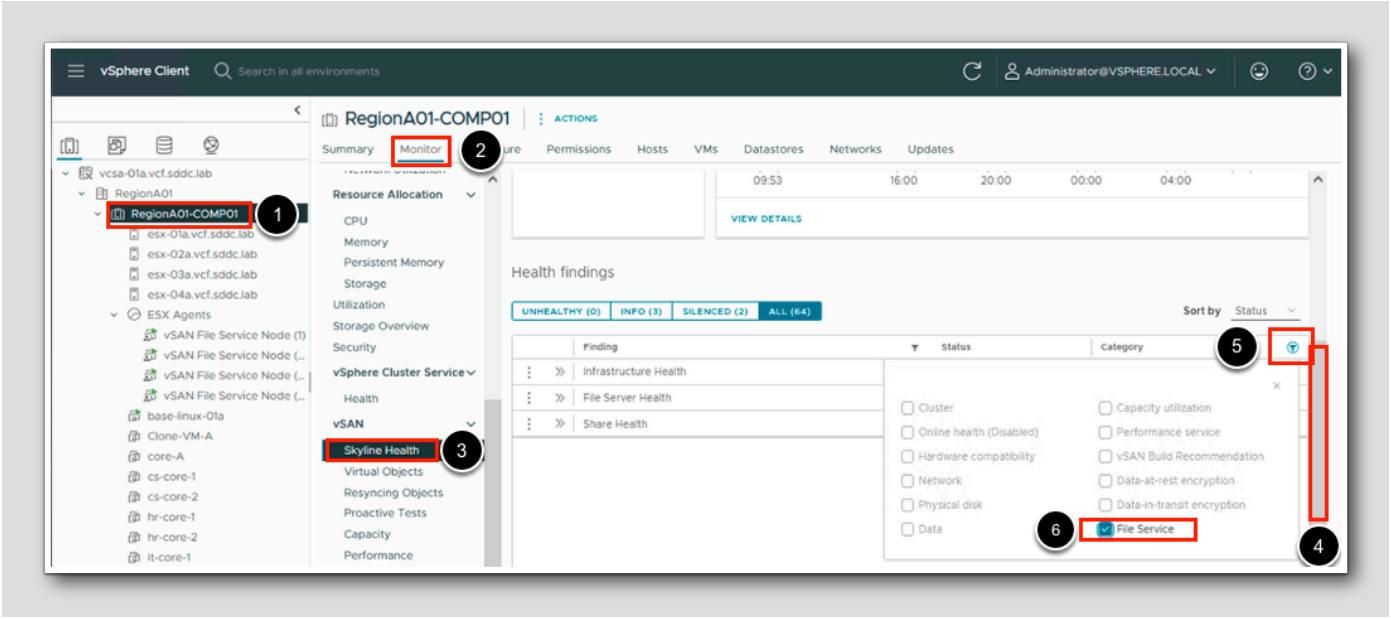
As we said, vSAN File Services is already ENABLED. Let's verify that vSAN File Services are enabled.

1. Expand **vcsa-01b.vcf.sddc.lab -> RegionA01**
2. Select vSAN Cluster, **RegionA01-COMP01**
3. Select **Configure**
4. Select **vSAN > Services**
5. Scroll down to find **File Service**
6. vSAN Services : **File Service = Enabled**

For the **Files Service**, you can see the network details of the file service

You can see the vSAN File Service Nodes were created. One for each vSAN node enabled and up to 100 file shares and 64 file servers with vSAN 8.0.

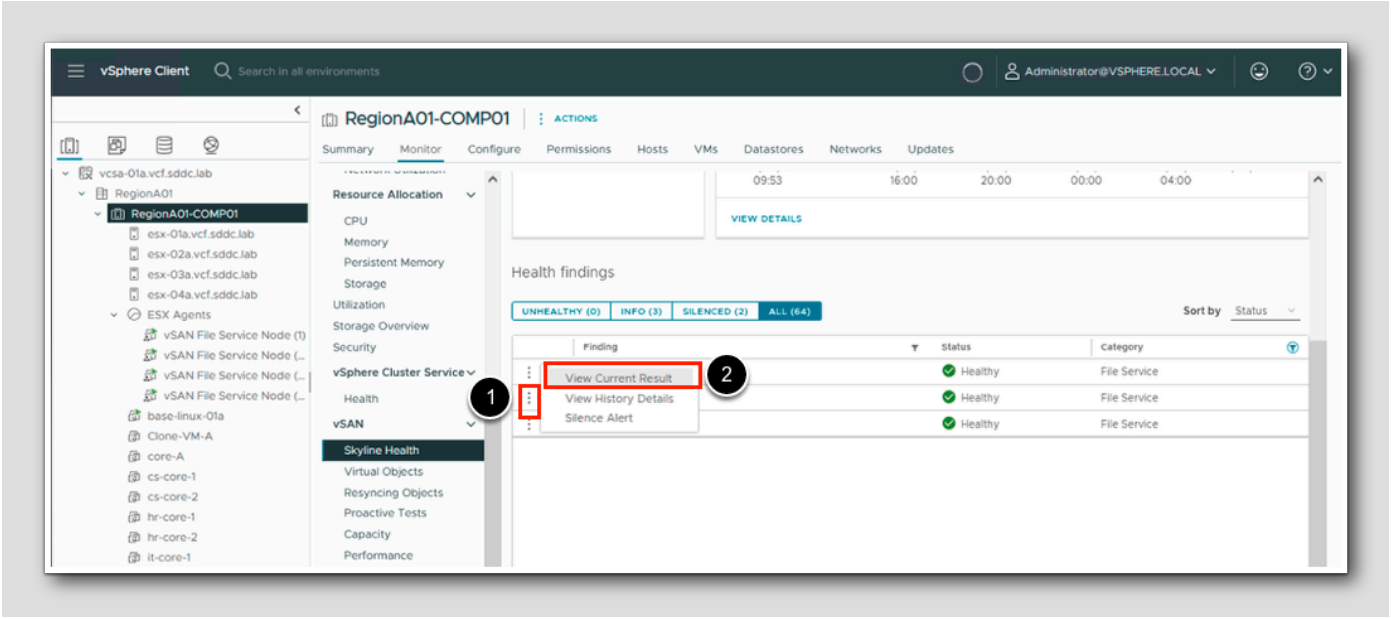
Health Check for File Server



1. Select vSAN Cluster, **RegionA01-COMP01**
2. Select **Monitor**
3. Select **vSAN > Skyline Health**
4. Scroll down to reveal controls for navigating across multiple pages of vSAN Skyline Health Findings
5. Click the filter icon on the **Category** column
6. Click **File Service**

Skyline Health

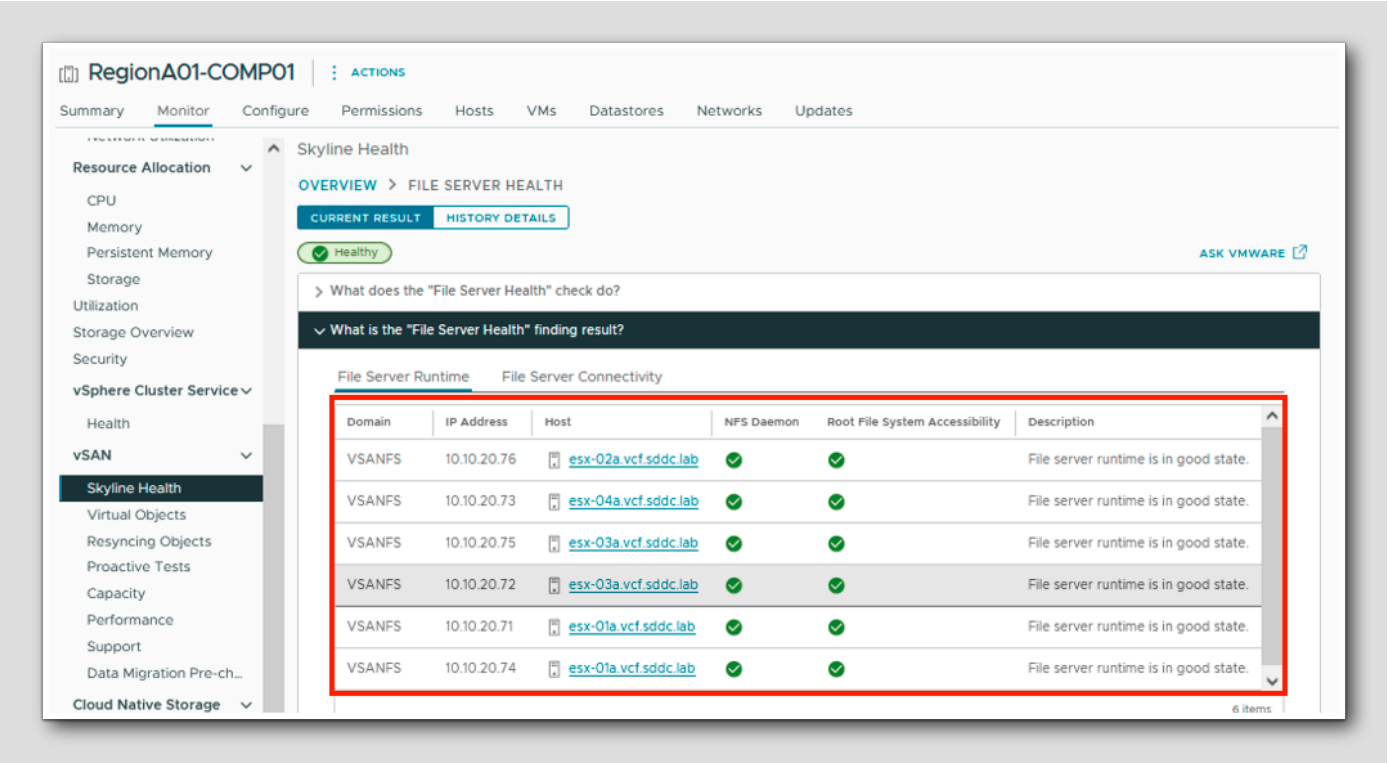
[133]



1. Click on the **three vertical dots** to the left of the File Server Health
2. Click **View Current Result** in the pop-up box

Observe the hosts

[134]



Here, you can see the hosts that are contributing into the File Servers Service - we can observe greater details on the services running in the file server nodes as well as their assigned IP addresses.

Creating NFS File Shares

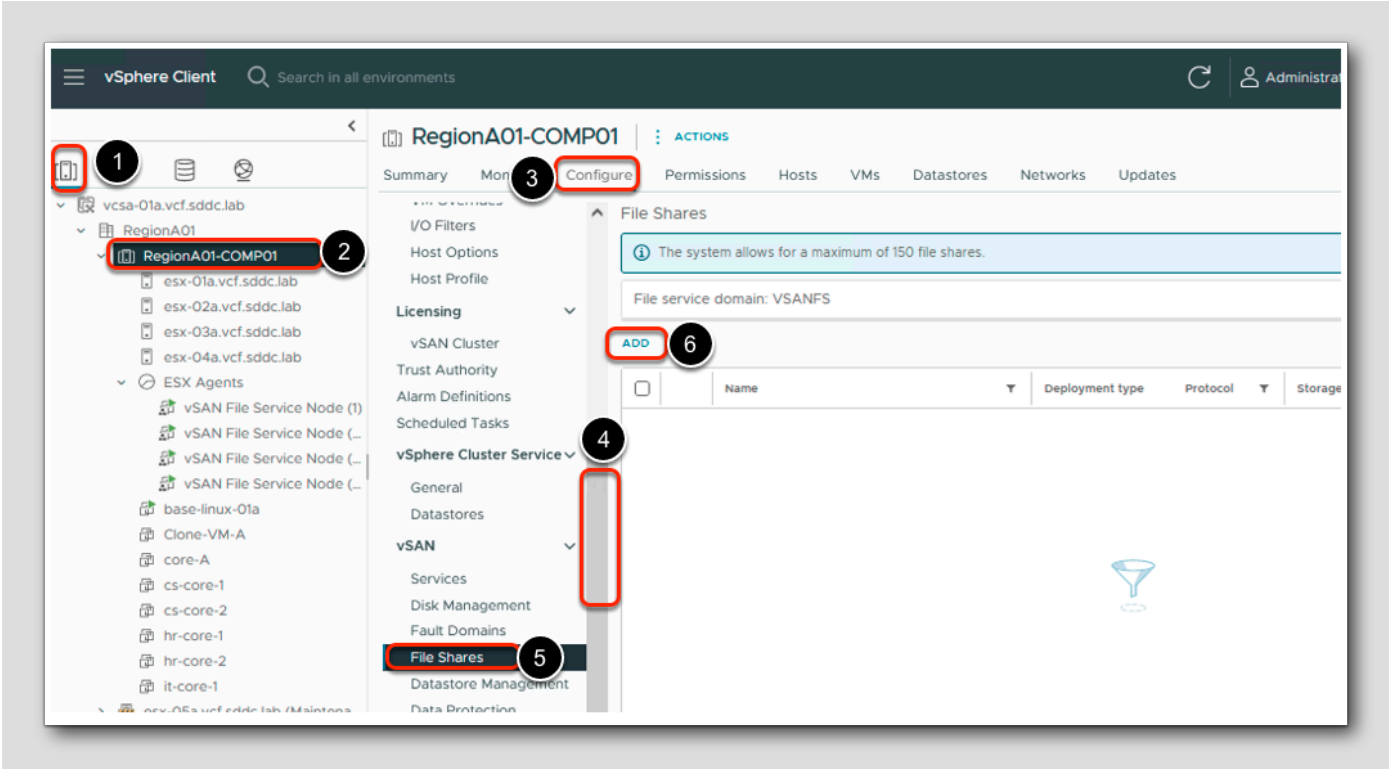
[135]

To create vSAN Files Services for NFS, consider the followings for share names and usages:

- Usernames with non-ascii characters can be used to access share data
- Share names can contain only English characters
- For pure NFSv4 type shares, the file and directories can only contain any UTF-8 compatible
- For pure NFSv3 and NFSv3+NFSv4 shares file and directories can contain only ASCII compatible strings

Create a File Share

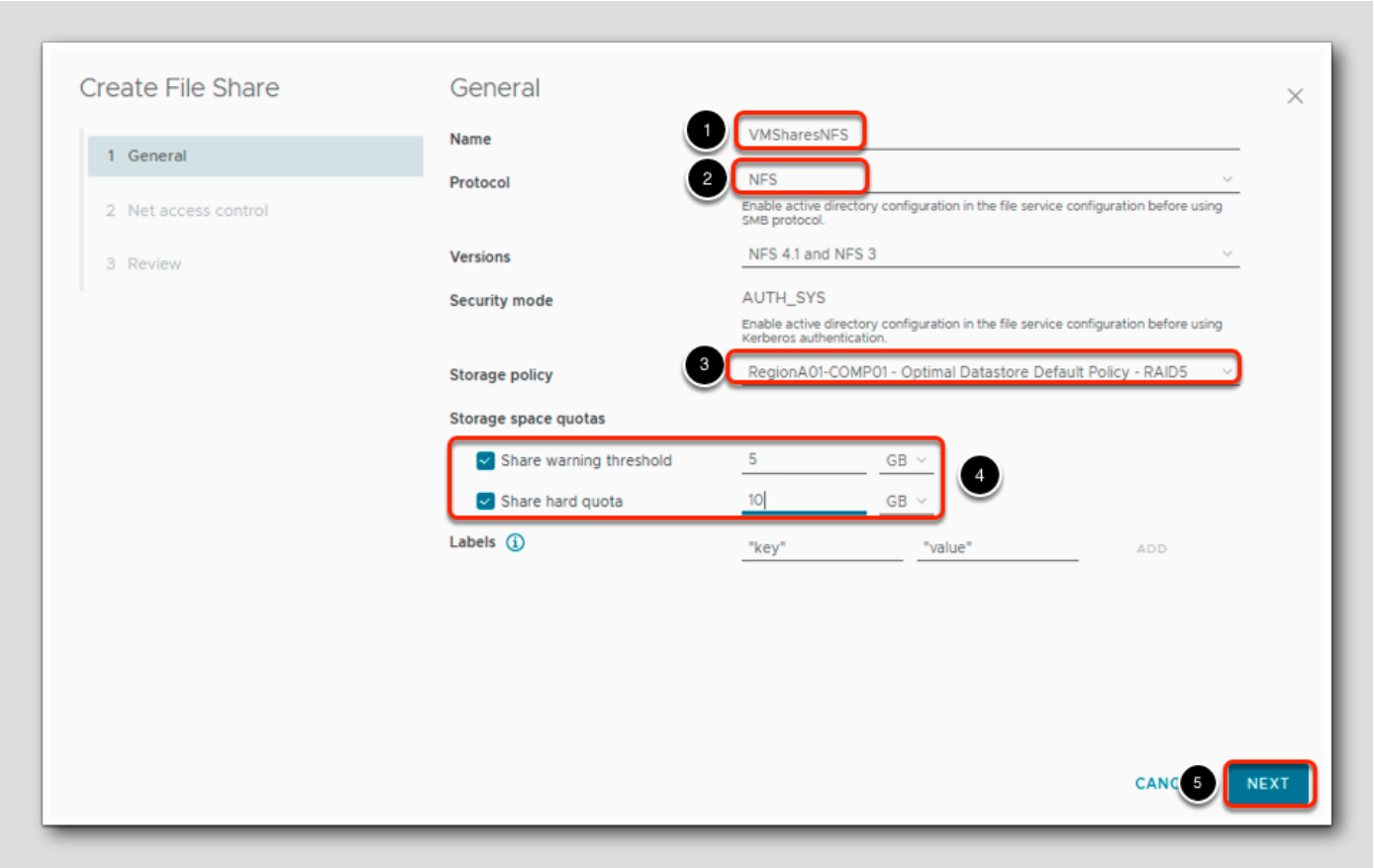
[136]



1. Select the **Hosts & Clusters icon**
2. Select the vSAN cluster, **RegionA01-COMP01**
3. Select **Configure**
4. Scroll down the slider to reveal **vSAN** configuration items
5. Select **vSAN > File Shares**
6. Click **ADD**

Create File Share

[137]

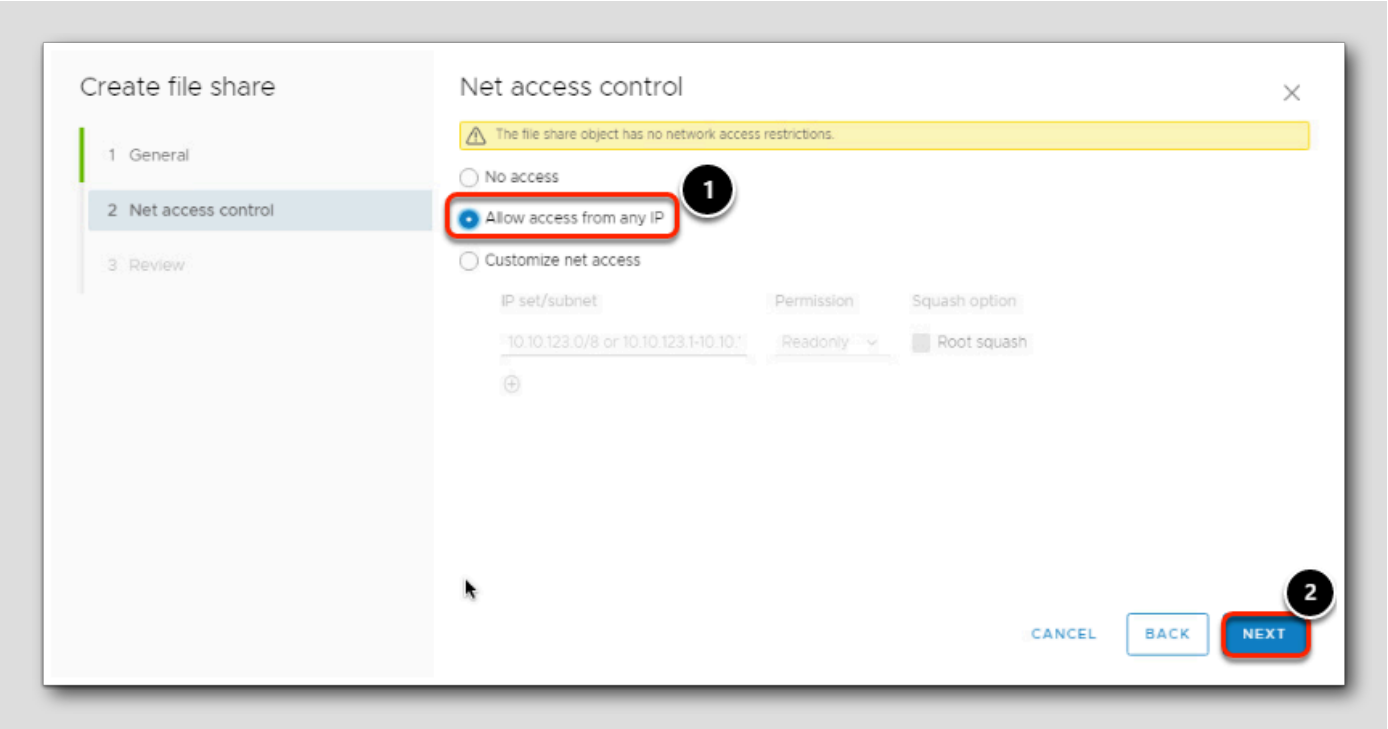


In the General page,

1. Enter the **Name** of the Shares: VMSharesNFS
2. Select **Versions**: NFS 4.1 and NFS 3
3. Select **Storage Policy**: RegionA01-COMP01 - Optimal Datastore Default Policy - RAID5
4. **Enabled Shared warning threshold and Enabled Share hard quota** and enter 5 GB and 10 GB respectively
5. Click **NEXT**

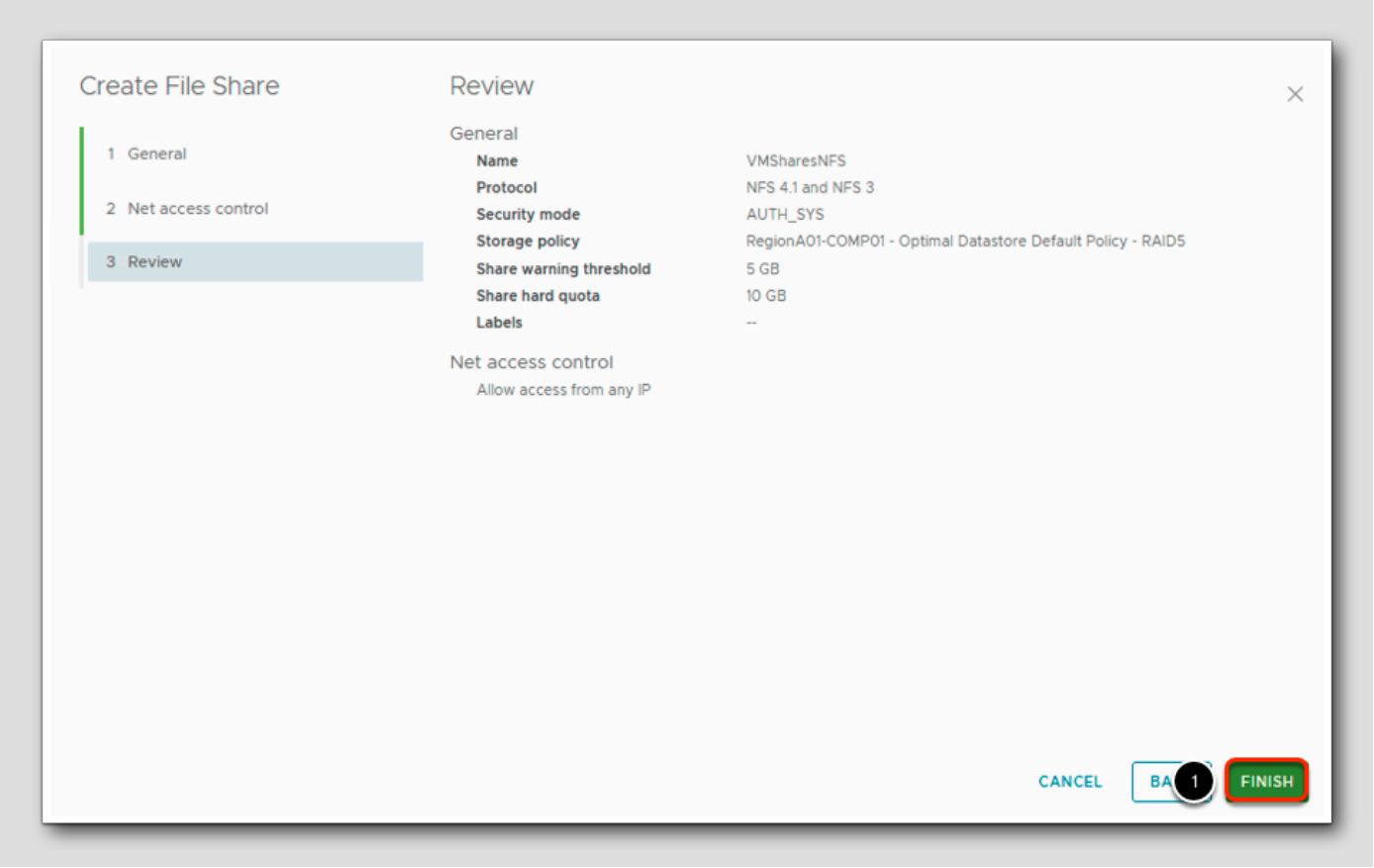
Create File Share

[138]



In the Net access control page,

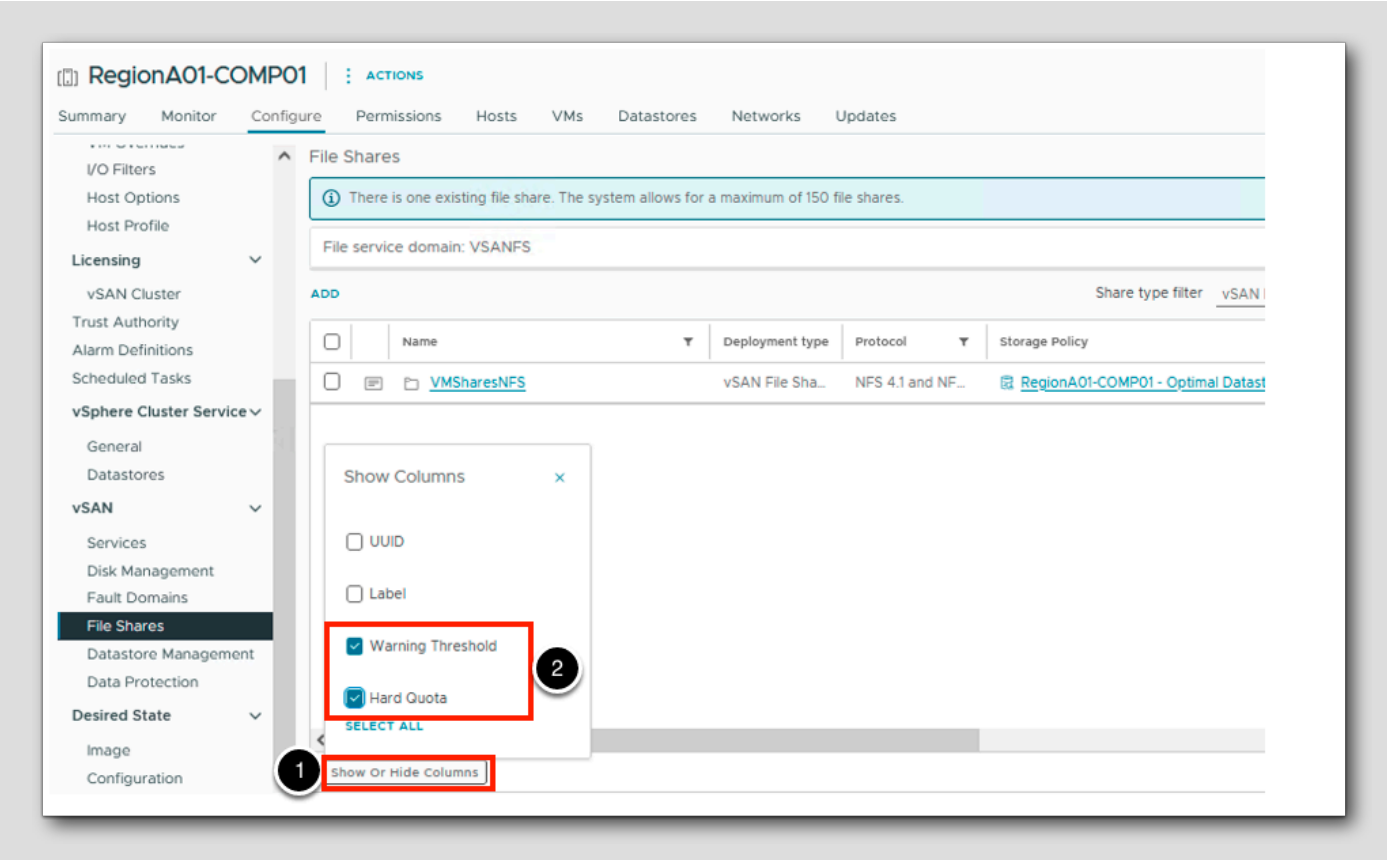
1. Select **Allow access from any IP**
2. Click **NEXT**



1. You can review what you enter then Click **FINISH**

Create File Share

[139]



You can view the list of vSAN file shares we just created called **VMSharesNFS** with the appropriate storage policy, Usage/Quota and Actual Usage

1. You can add additional columns by clicking the **Show or Hide Columns**
2. Select **Hard Quota** and **Warning Threshold**

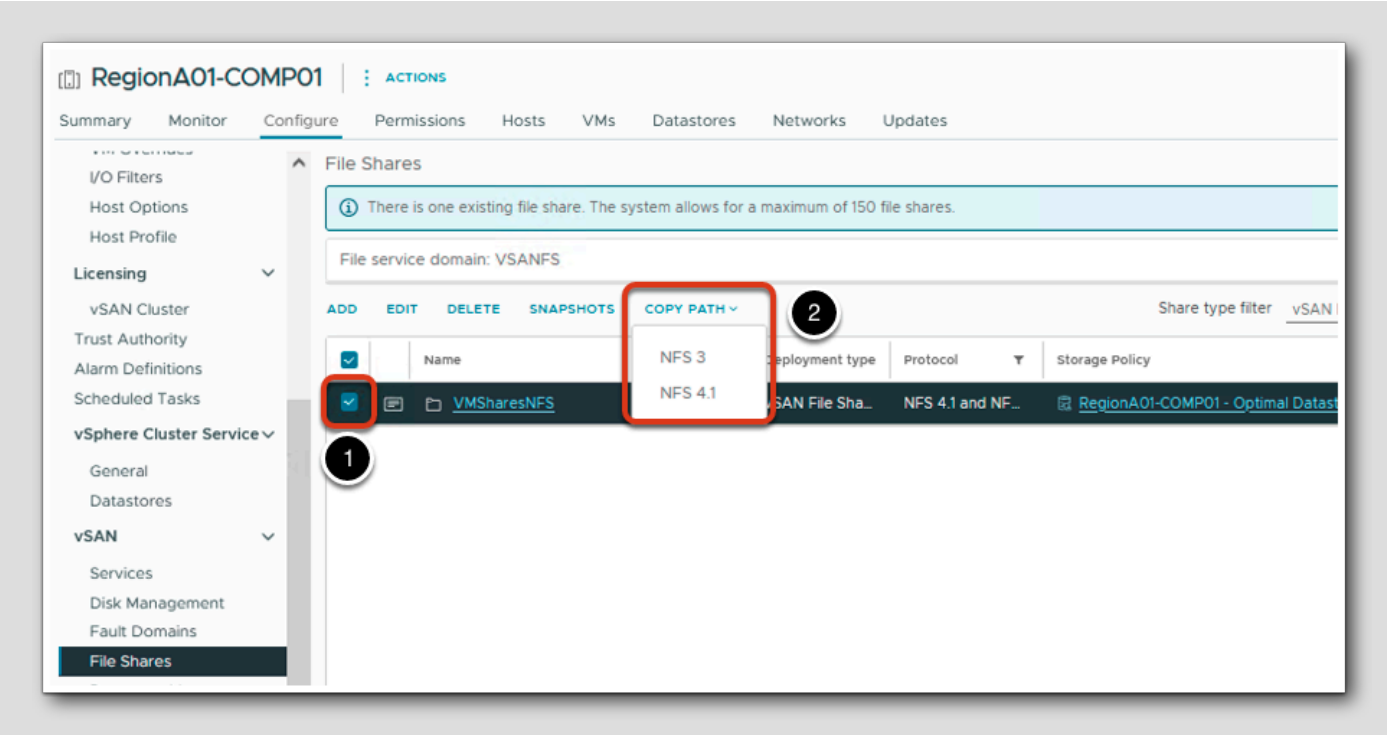
Mounting vSAN NFS File Shares to other Systems

[140]

You can access a file share from a host client, using an operating system that communicates with NFS file systems. For RHEL-based Linux distributions, NFS 4.1 support is available in RHEL 7.3 and CentOS 7.3-1611 running kernel 3.10.0-514 or later. For Debian based Linux distributions, NFS 4.1 support is available in Linux kernel version 4.0.0 or later. All NFS clients must have unique hostnames for NFSv4.1 to work. You can use the Linux mount command with the Primary IP to mount a vSAN file share to the client.

Mount File Service Shares

[141]



1. Check the box next to **VMShareNFS**
2. Click the **COPY PATH** drop down menu, you have the option to select either **NFSv3** or **NFSv4.1**

Examples of the connection string copied.

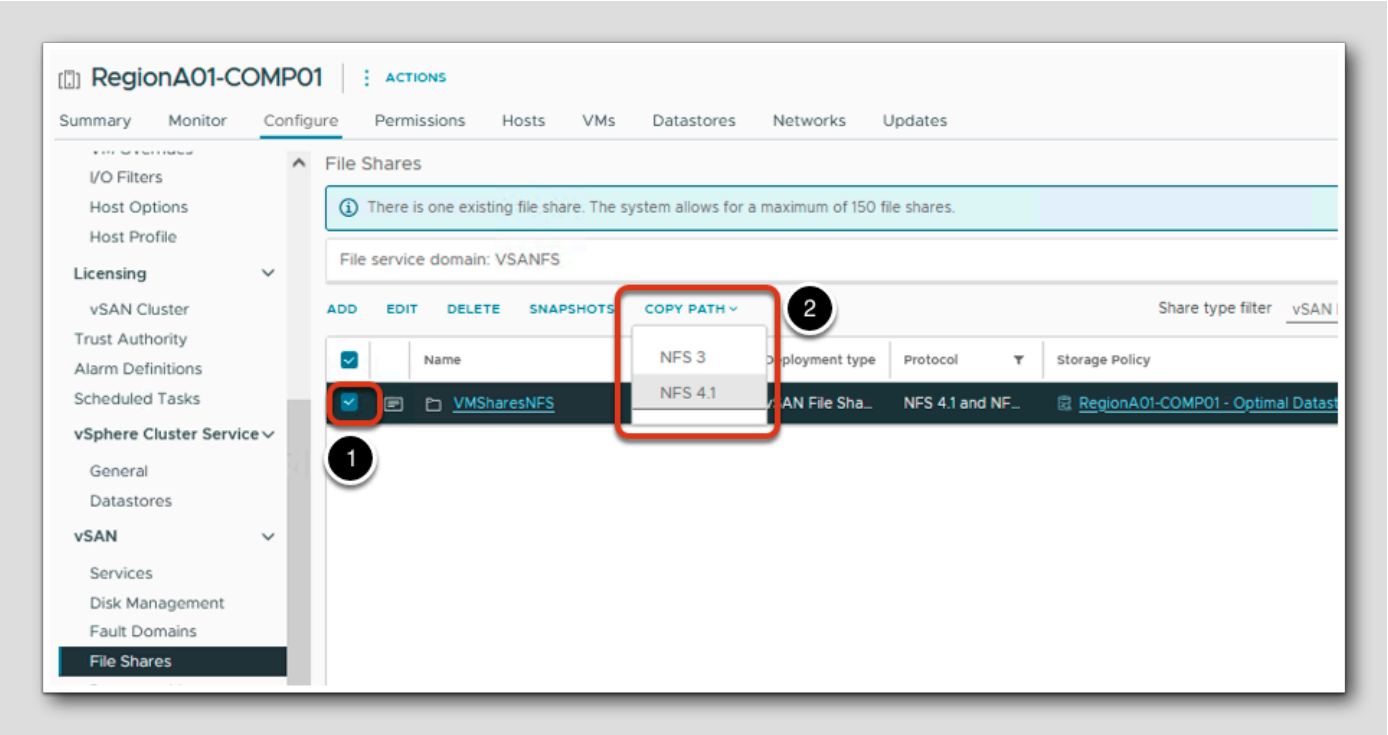
NFSv3: vsan-fs-06a.vcf.sddc.lab:/VMSharesNFS

NFSv4.1: vsan-fs-01a.vcf.sddc.lab:/vsanfs/VMSharesNFS

To mount this file share as NFS v4.1 and the NFSv4.1 referral mechanism, you need to include the root share (/vsanfs) in the mount path

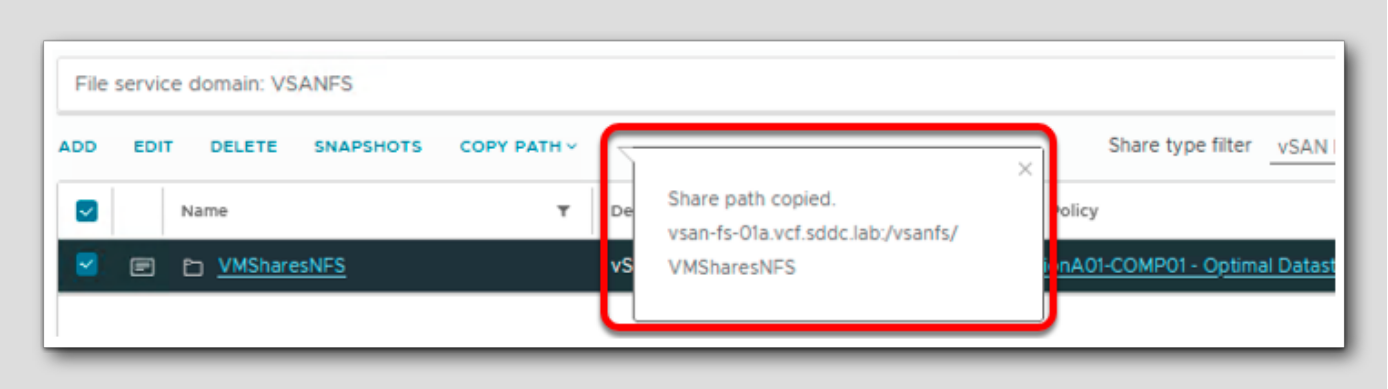
Mount File Service Shares

[142]



1. Check the box next to **VMShareNFS**
2. Select **COPY PATH**, then select **NFS 4.1**

We will use NFSv4.1 to mount the shares.



Note: Take note of the file share mount path as you will use this path in later steps.

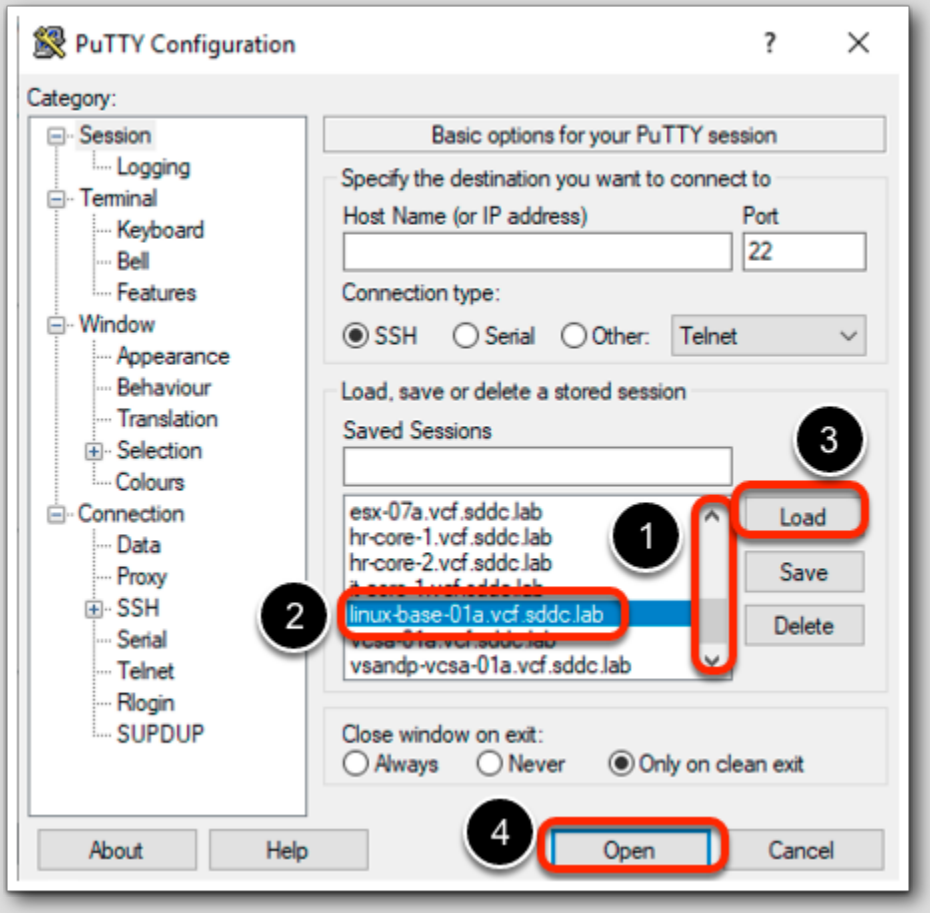
Launch PuTTy

[143]

1. Launch the **PuTTy** application from the Windows Taskbar

Connect to linux-base-01a.vcf.sddc.lab

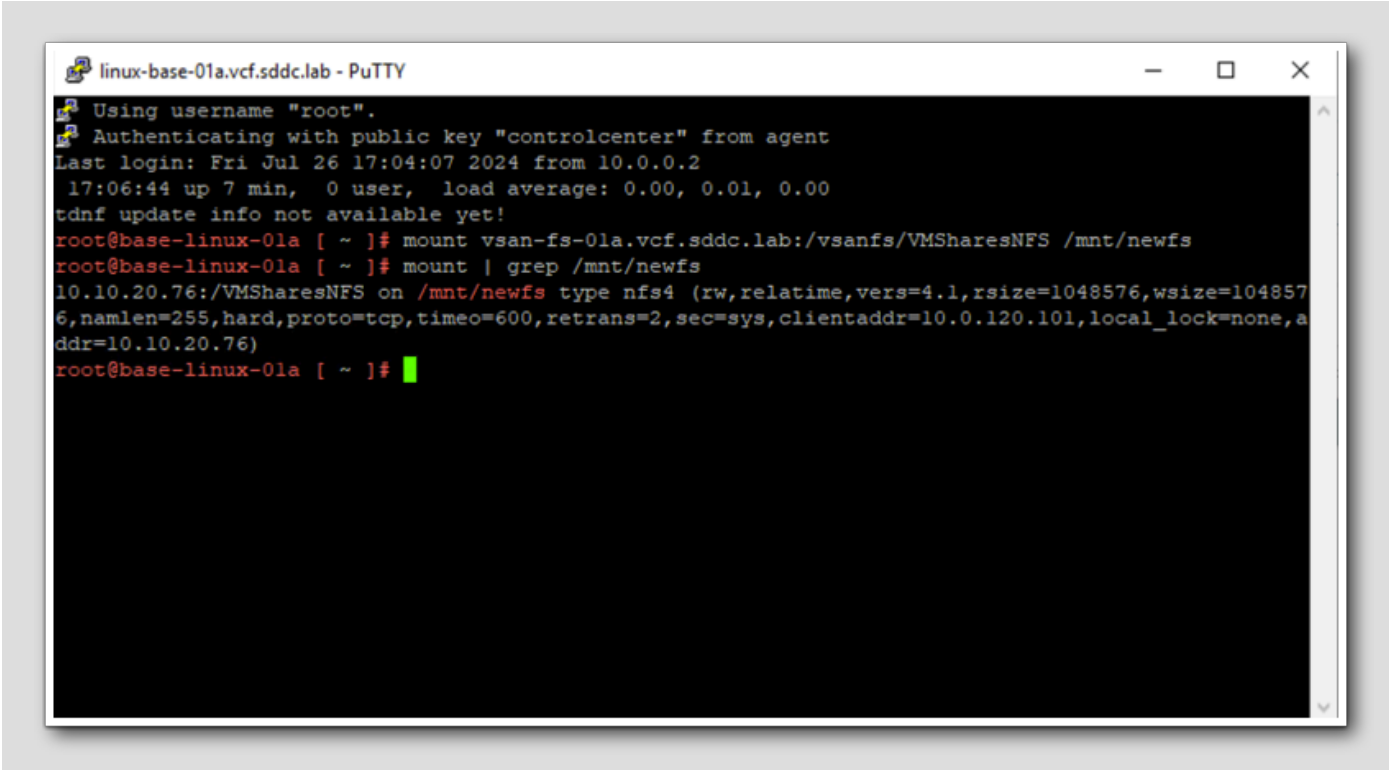
[144]



1. Scroll through list of Saved Sessions
2. Select linux-base-01a.vcf.sddc.lab
3. Load the session
4. Open the connection

Mount vSAN File Shares

[145]



On this VM, we have already created a directory, */mnt/newfs*, with which we will use to mount the file share.

Below is the command to mount the file share using NFS v4.1. NFS v4.1 is also the default mount version if no protocol is specified. In that case, the client will negotiate the mount protocol with the server and mount with the highest matching protocol, which for vSAN 8 Native File Services is NFS v4.1.

By typing:

- root@base-linux-01a[~]# `mount vsan-fs-01a.vcf.sddc.lab:/vsanfs/VMSharesNFS /mnt/newfs`
- root@base-linux-01a[~]# `mount | grep /mnt/newfs`

Note:

Above "mount" command referencing vsanfs-01a is an example only. vSAN file services shares could be located on a variation of vsanfs-0#a depending on your configuration. Refer to previous steps for complete path.

Mount vSAN FIle Shares

[146]

Let's write a file to the file share and confirmed it worked.

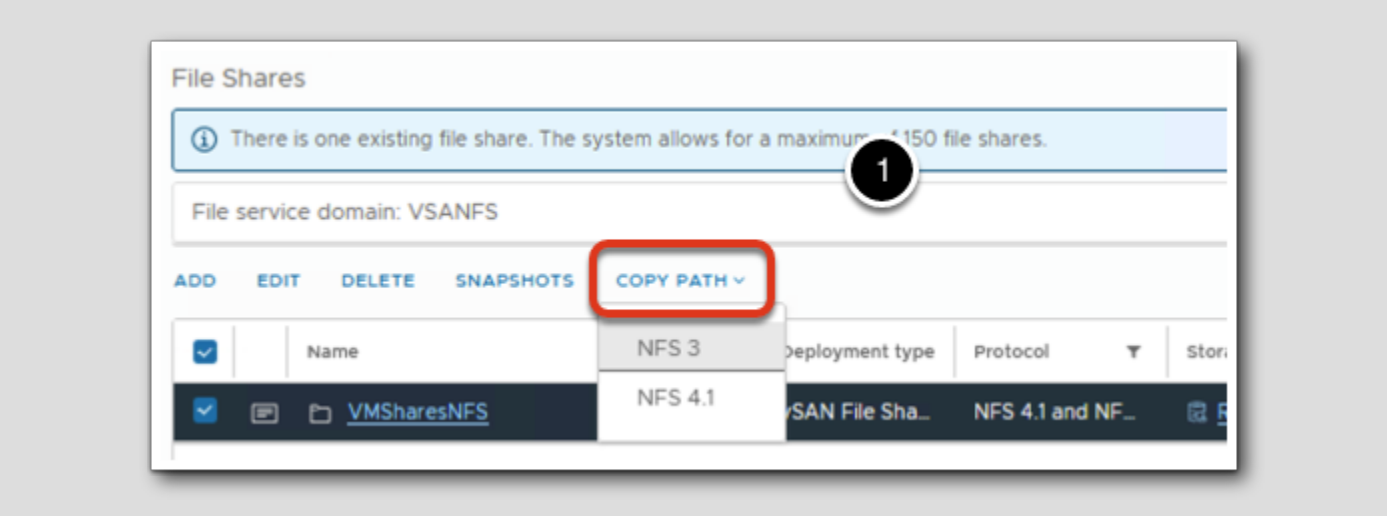
Type the following commands into Putty.

- root@base-linux-01a[~]# `cd /mnt/newfs`
- root@base-linux-01a[~]# `echo "NFS 4 Share" > newfs.txt`
- root@base-linux-01a[~]# `cat newfs.txt`

Mount vSAN FIle Shares (vSphere Client)

[147]

Return to the vSphere Client



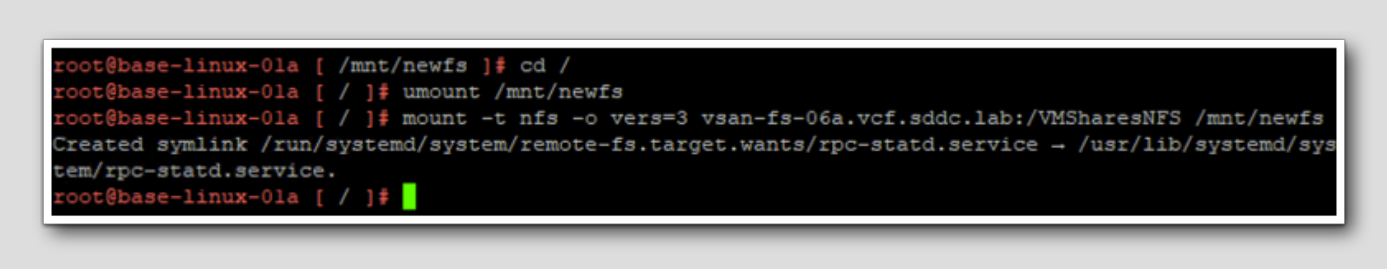
Let us mount to the NFSv3:

1. Select **COPY PATH**, then select **NFSv3**

Take notice of the new connection string. It might be different from what is in the picture since it is on a pool of IP

Mount vSAN File Shares

[148]



Switch back to the putty session for 'base-linux-01a' and run:

- root@base-linux-01a[~]# `cd /`
- root@base-linux-01a[~]# `umount /mnt/newfs`
- root@base-linux-01a[~]# `mount -t nfs -o vers=3 vsan-fs-06a.vcf.sddc.lab:/VMSharesNFS /mnt/newfs`

NOTE - Use the Connection Strings for NFSv3 that is display in your lab. Since it is on a pool of IP, it might be different from what is shown above in the manual.

The Above "mount" command referencing vsanfs-06a is an example only. vSAN file services shares could be located on a variation of vsan-fs-0#a

Mount NEWFS

[149]

1. Run the following commands:

- root@base-linux-01a[~]# `cd /mnt/newfs`
- root@base-linux-01a[~]# `cat newfs.txt`

You should see 'NFS 4 Share' as a return value

2. Now mount the following command:

- root@base-linux-01a[~]# `mount | grep /mnt/newfs`

You can see the /mnt/newfs is now mounted via NFSv3

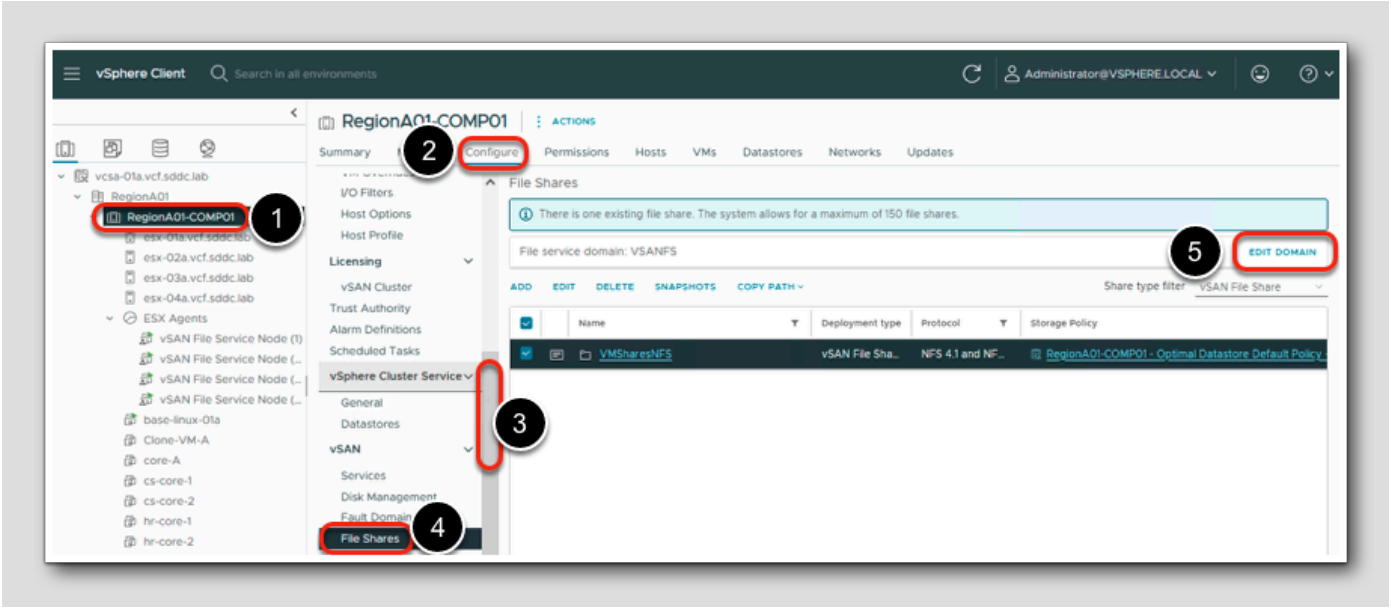
Creating SMB File Shares

[150]

If you are creating a SMB file share or an NFSv4.1 file share with Kerberos security, then ensure that you have configured vSAN File Service with AD domain credentials.

Enable AD Domain for File Share

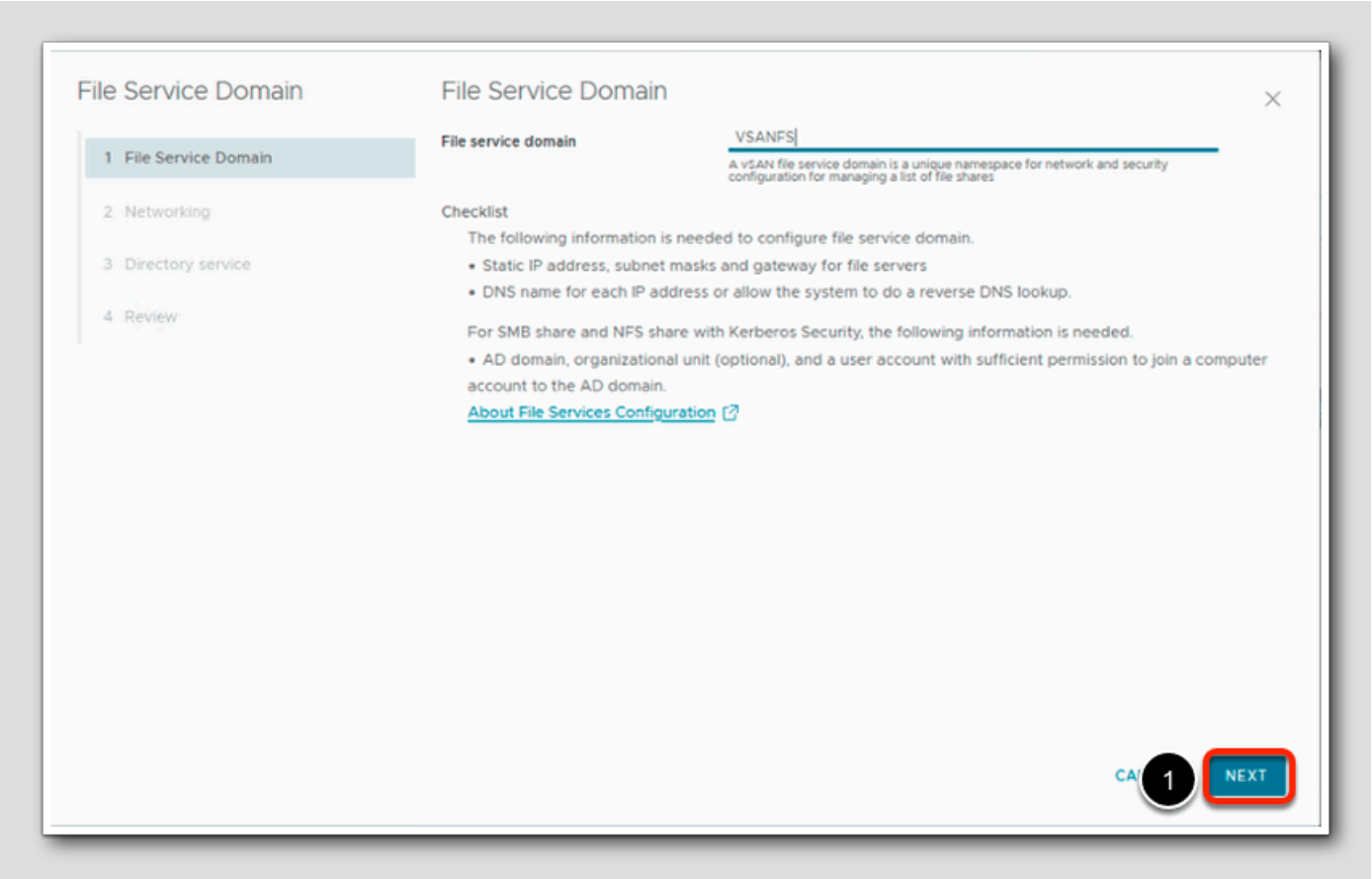
[151]



1. Select vSAN Cluster, **RegionA01-COMP01**
2. Select **Configure**
3. **Scroll down** to the list of configuration items
4. Select **vSAN > File Shares**
5. Click on **EDIT Domain** in the upper left corner of the File Shares panel

Edit File Share Domain

[152]

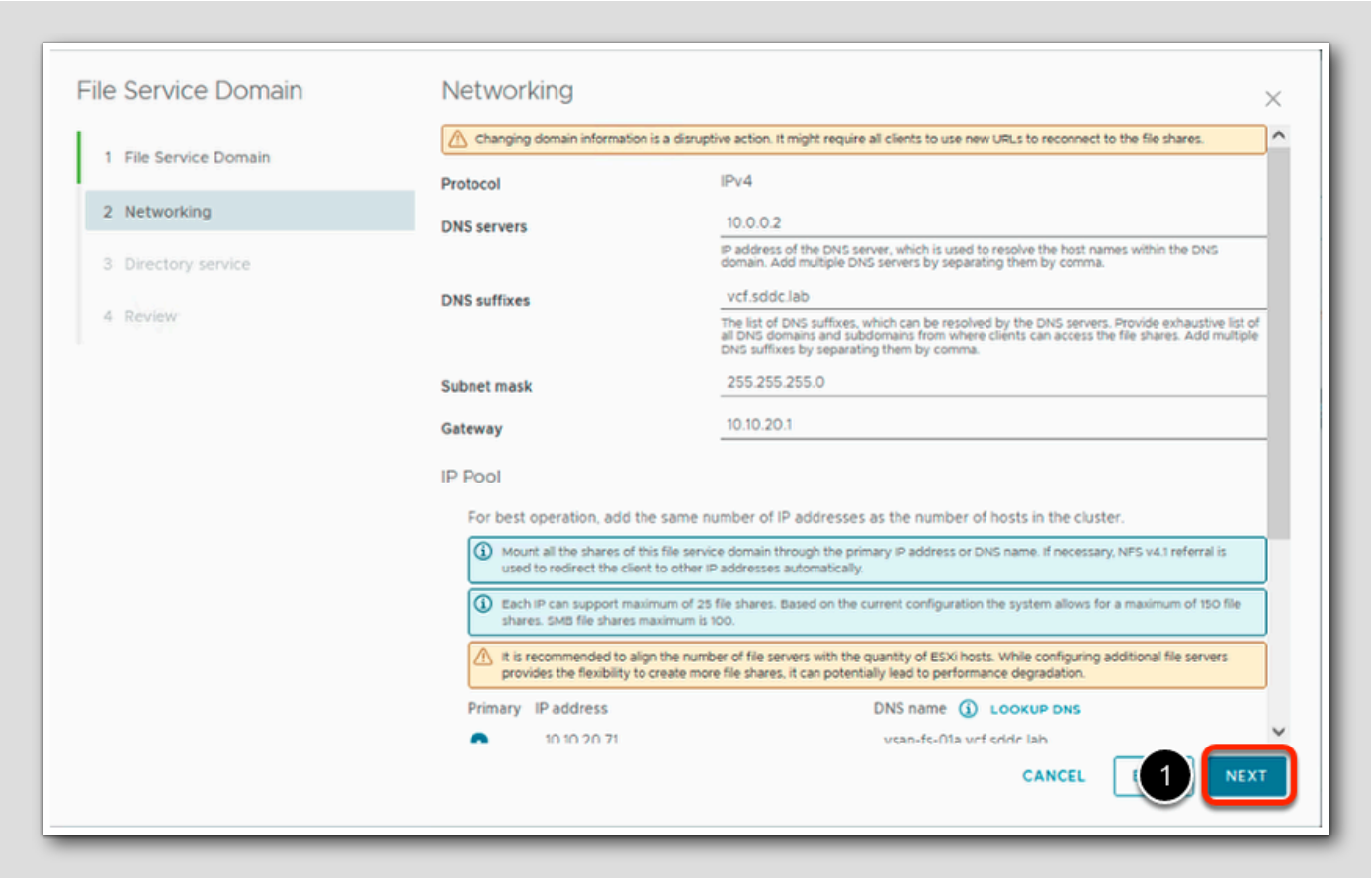


The vSAN File Service Domain is a construct used within VMware vSAN to manage the networking and security amongst the nodes of a vSAN cluster that supports File Services - don't confuse the vSAN file service domain name with the Microsoft Active Directory domain that used to integrate SMB file shares.

1. Click **Next** to advance the screen

Review the Networking Information

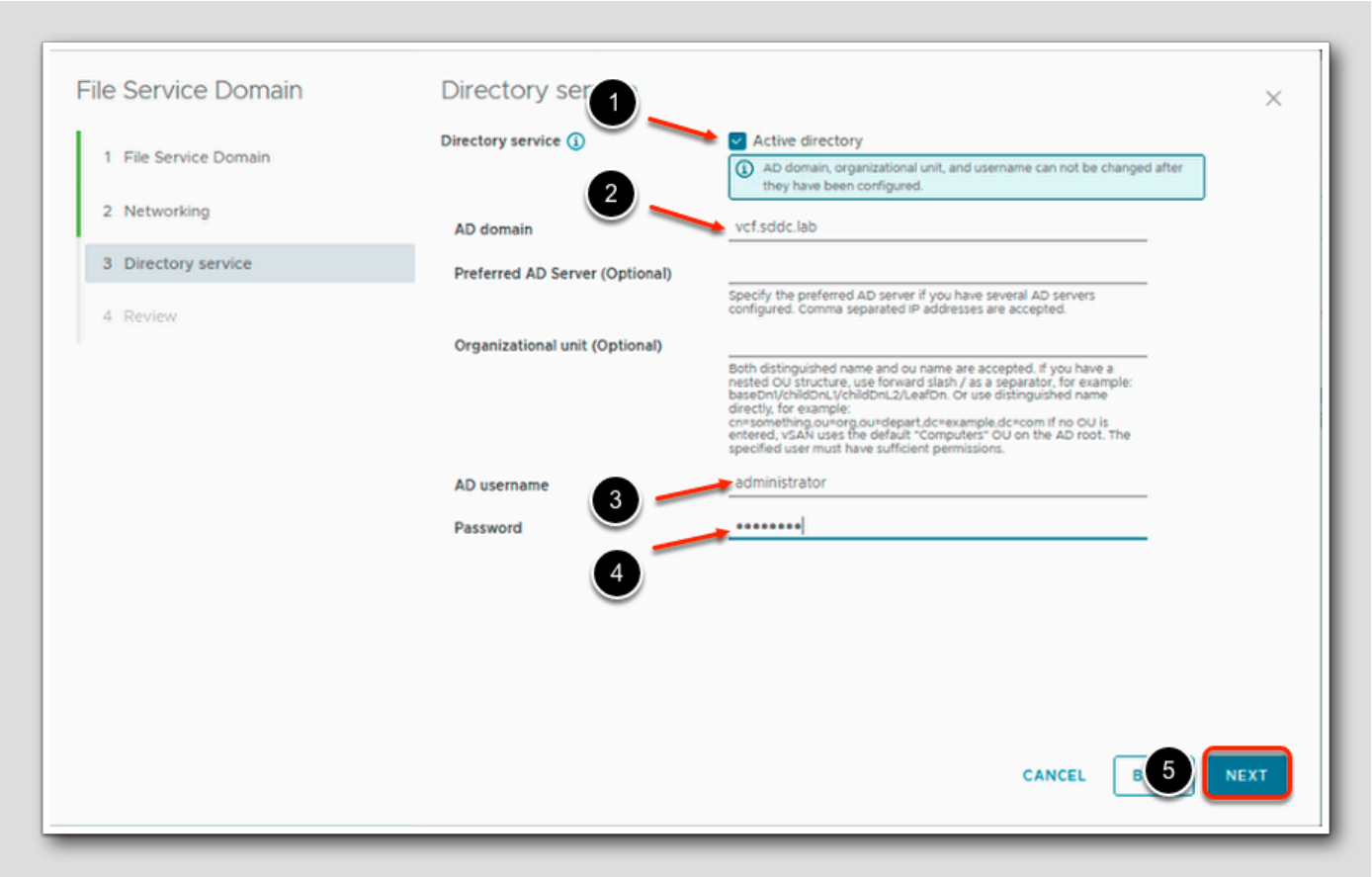
[153]



1. Click **Next** to advance the screen

Directory Service

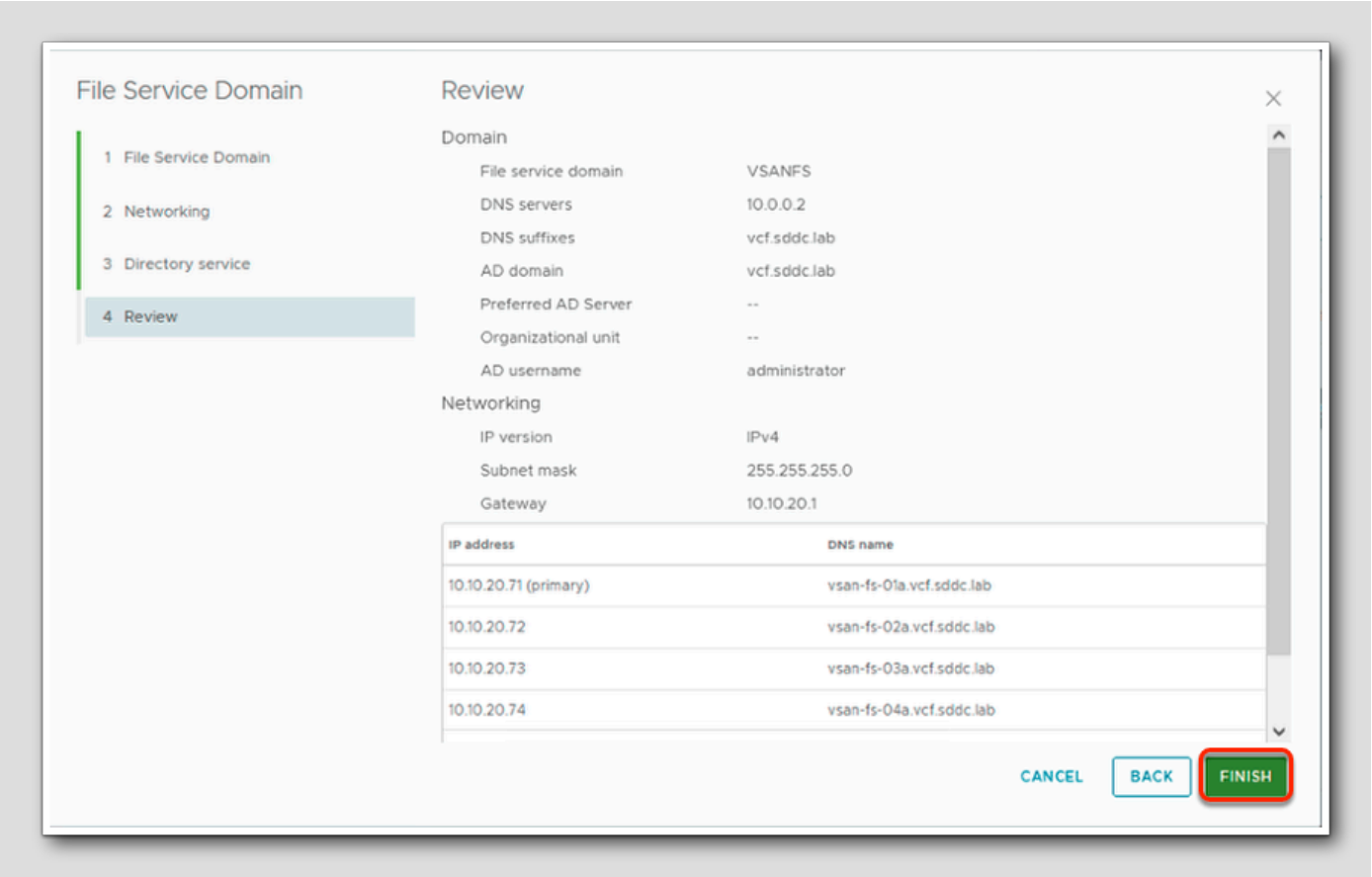
[154]



In this lab we've already enabled vSAN File Services & the appropriate DNS services for the NFS file shares but not the requisite Active Directory domain information to support SMB and Kerberos-authenticated NFS 4.1 shares. Let's perform the Active Directory Configuration ...

1. Check the box to enable **Active Directory**
2. Our AD domain is: **vcf.sddc.lab**
3. Our AD username: **administrator**
4. The password is: **VMware123!**
5. Click on **NEXT**

Review and Finish

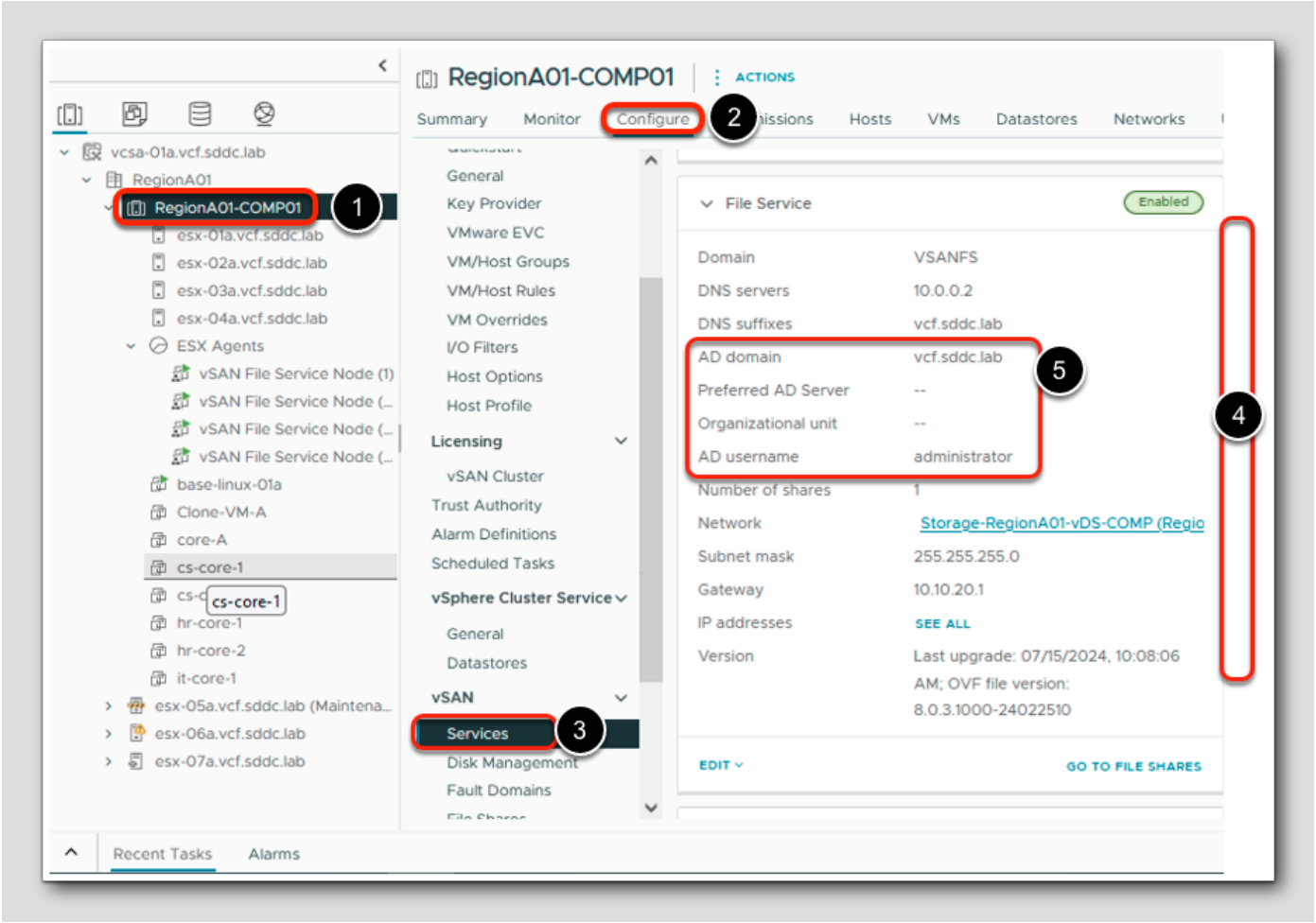


1. Click **FINISH** on the Review page

It will take a few minutes for the vSAN File Services to be reconfigured. This involves a restart of the vSAN File Services VM's.

File Service - AD Domain enabled

[156]

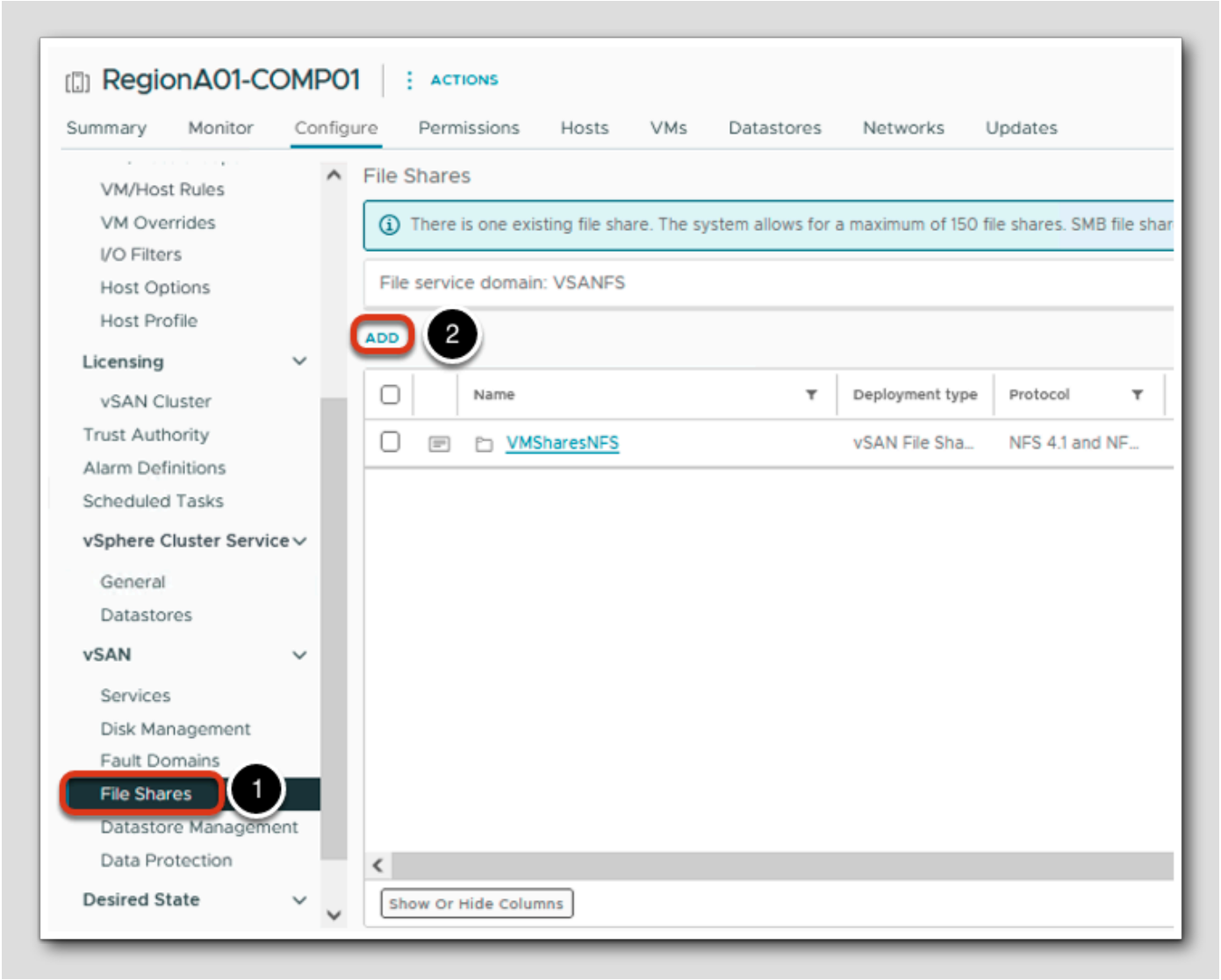


Monitor the enabling of the AD Domain via **Recent Tasks**. This should only take a couple of minutes. After the tasks are complete:

1. Click on cluster **RegionA01-COMP01**.
2. Click **Configure**.
3. Go to **vSAN > Services**
4. Scroll down until you see **File Services.**
5. You should see that **AD domain** and **AD username** are now a part of the **File Service** section.

Create SMB File Share

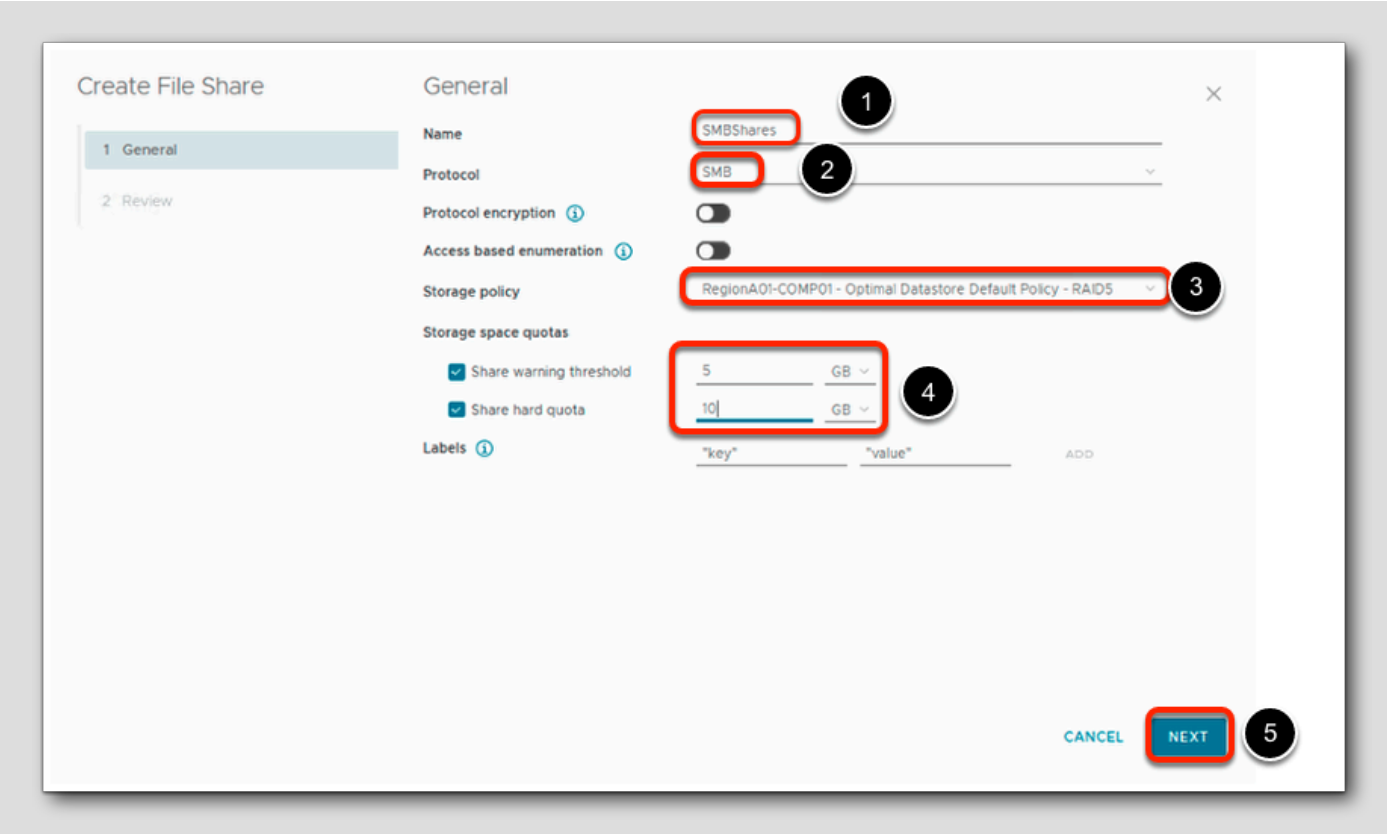
[157]



1. Select **vSAN** > **File Shares**
2. Click **ADD**

Create File Share - General

[158]



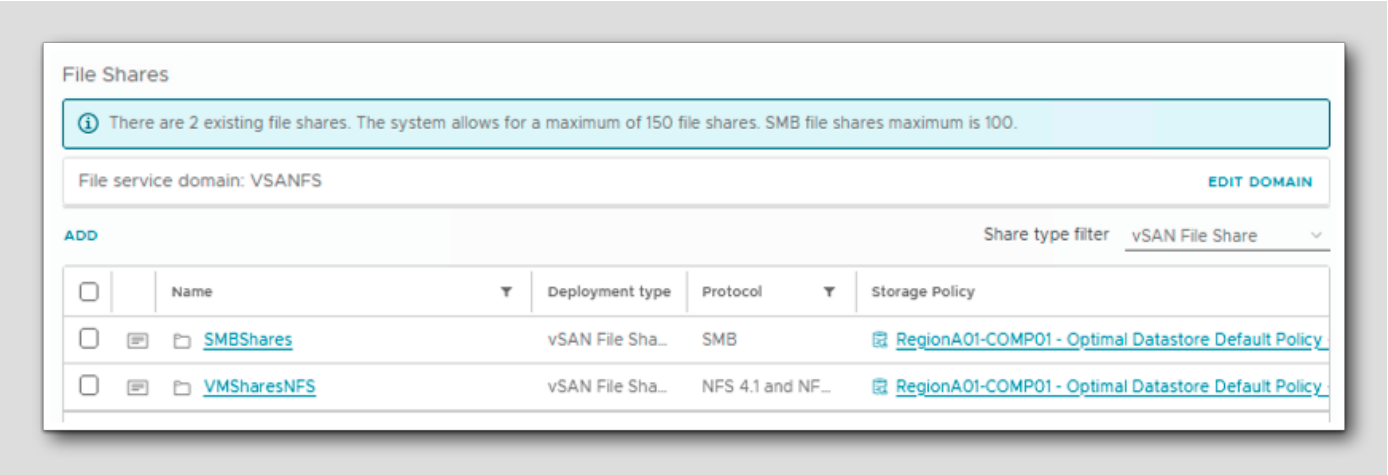
In the General page,

1. Enter the **Name** of the Shares: SMBShares
2. Select Protocol: **SMB**
3. Select Storage policy: **RegionA01-COMP01 - Optimal Datastore Default Policy - RAID5**
4. Enter the threshold and hard quota for the storage: **5 GB** threshold and **10 GB** for hard quota
5. Click **NEXT**

Click **FINISH** on the Review page

Create File Share

[159]

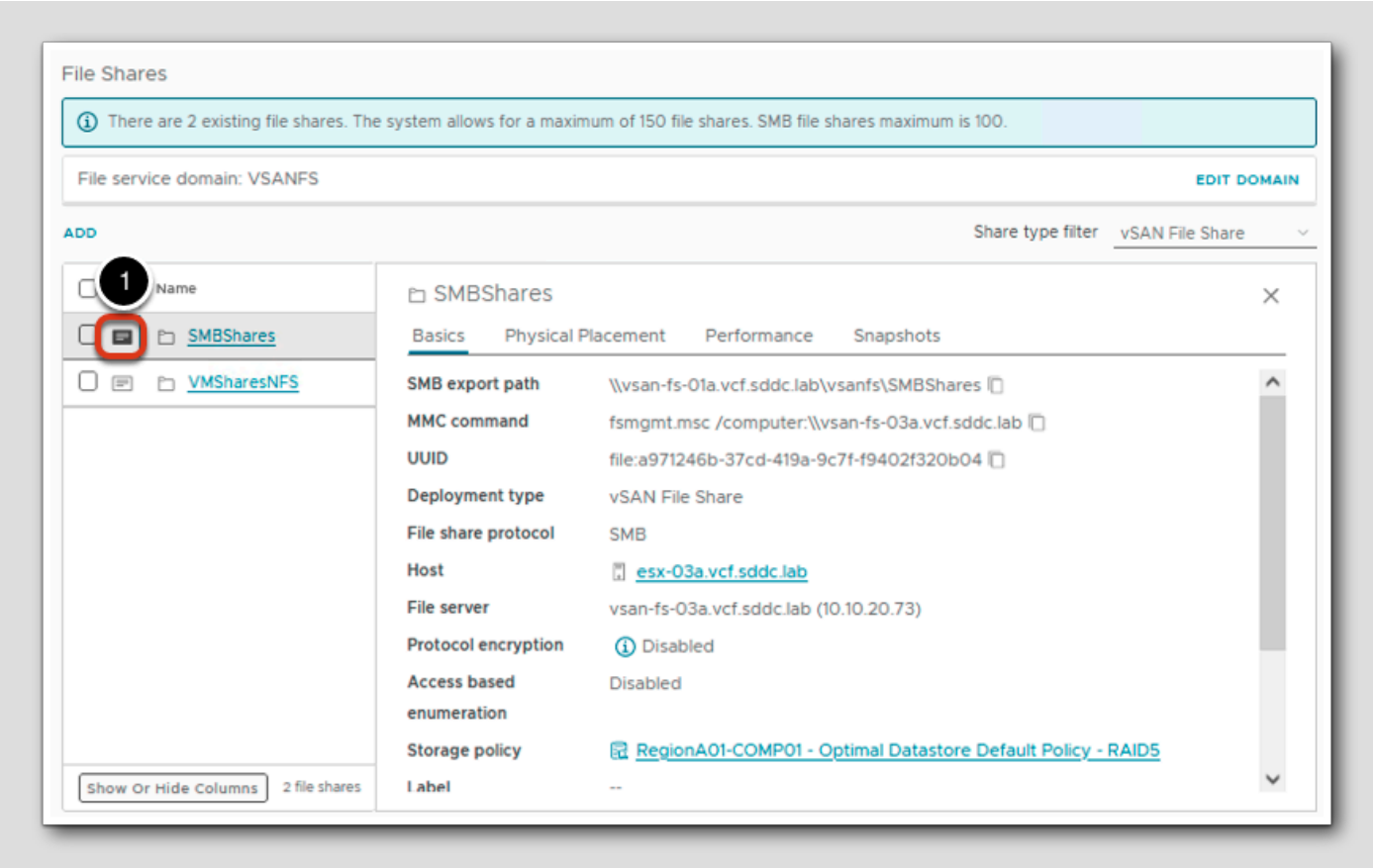


To view the list of vSAN file shares, navigate to the vSAN cluster and click **Configure** > **vSAN** > **File Shares**.

You can view the list of vSAN file shares we just created called **VMSharesNFS** for NFS and **SMBShares** for SMB with the appropriate storage policy, hard quota, usage over quota, actual usage, and so on.

View File Shares

[160]



1. Click on the button next to the **SMBShares**

You have the ability to review the physical placement of the SMB file share across the hosts and disks in the vSAN Cluster.

Also can view the **SMB export path** and the **MMC command**.

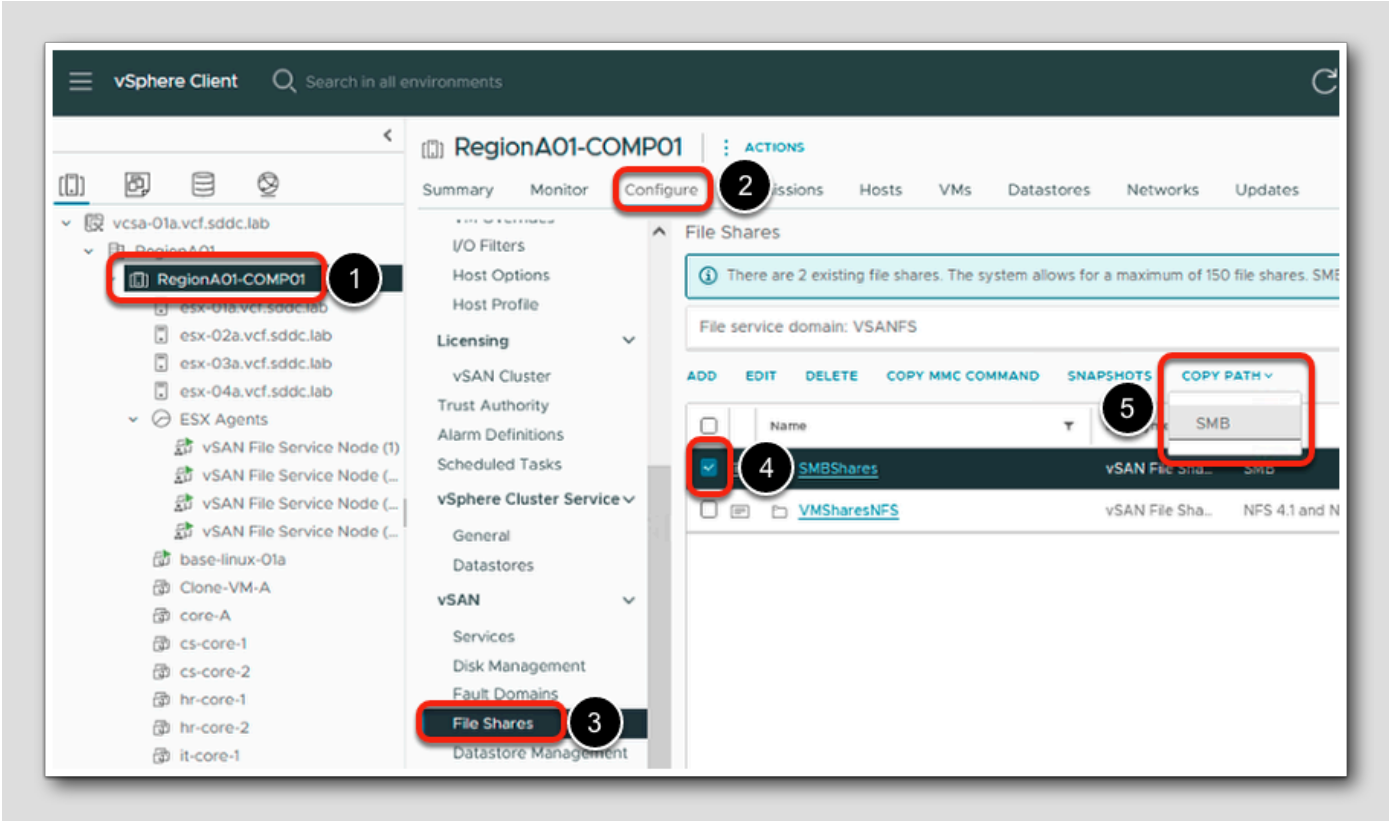
Client File Share Access

[161]

vSAN File Service supports SMB export path and shared folders snap-in for Microsoft Management Console (MMC) for managing SMB Shares on the vSAN Cluster.

Copy SMB Path

[162]



1. Select the **RegionA01-COMP01** cluster.
2. Click on the **Configure** tab.
3. Scroll down and select **vSAN > File Shares**
4. Check the box next to **SMBShares**.
5. Click on **COPY PATH** and then **SMB**.

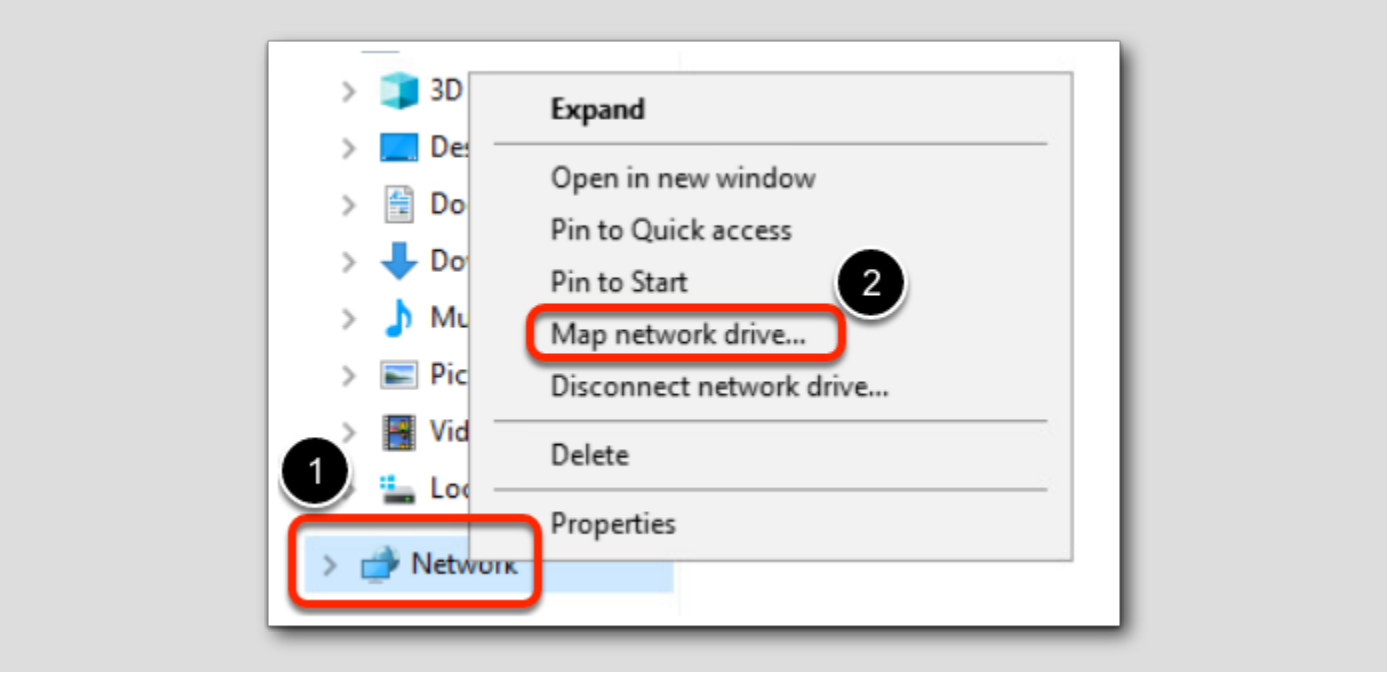
Client File Share Access

[163]

1. Launch **File Explorer** on the taskbar

Client File Shares Access via Network

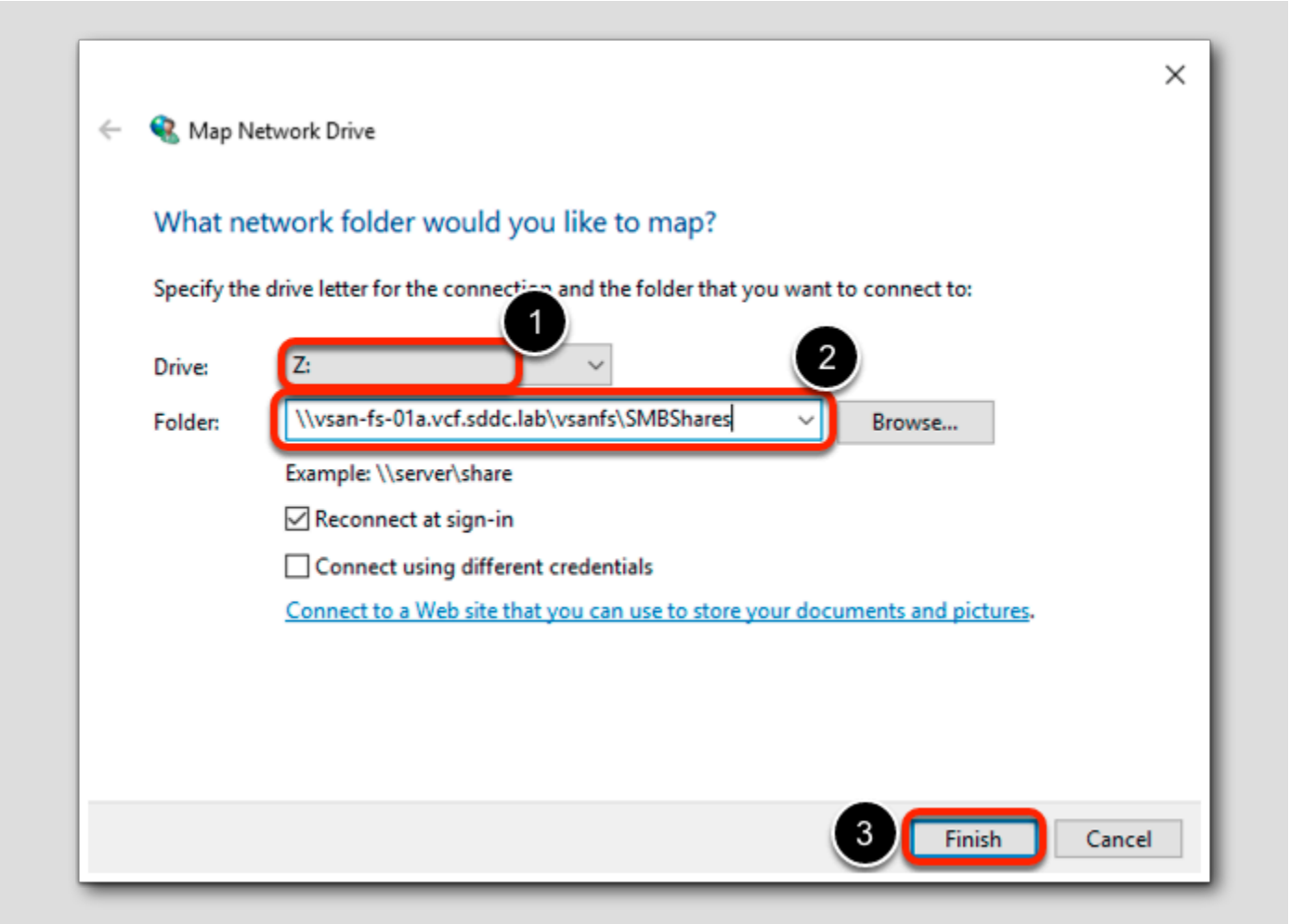
[164]



1. Right click **Network**
2. Select **Map network drive...**

Mapping Network Drive

[165]



1. Enter the Drive : Z:
2. Paste the SMB path next to **Folder**:

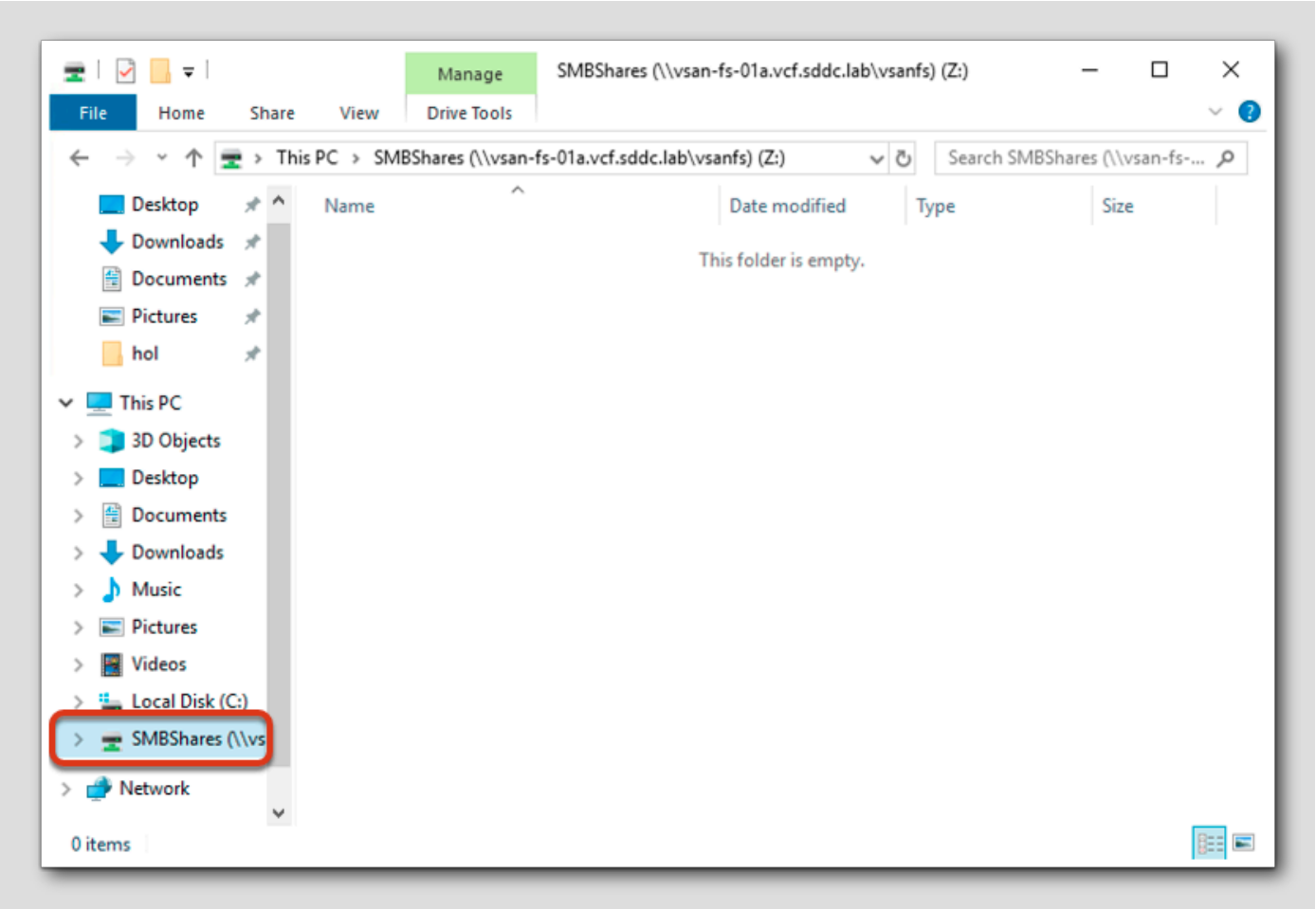
```
\\vsan-fs-01a.vcf.sddc.lab\vsanfs\SMBShares
```

This address may be slightly different so be sure to copy / paste from vCenter.

3. Click **Finish**

Mapping Network Drive

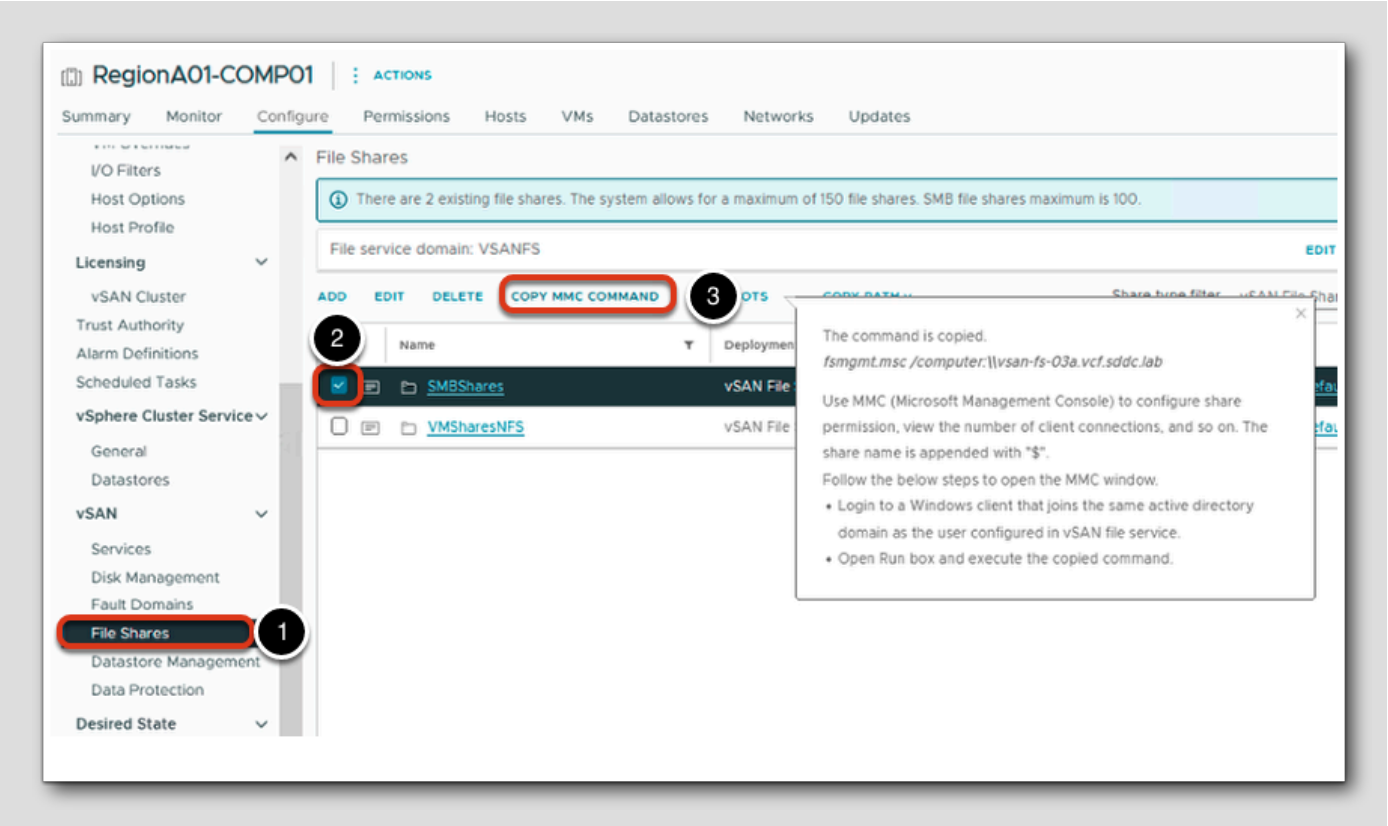
[166]



You can see **SMBShares** is mapped from the file explorer.

Create File Shares via Microsoft Management Console

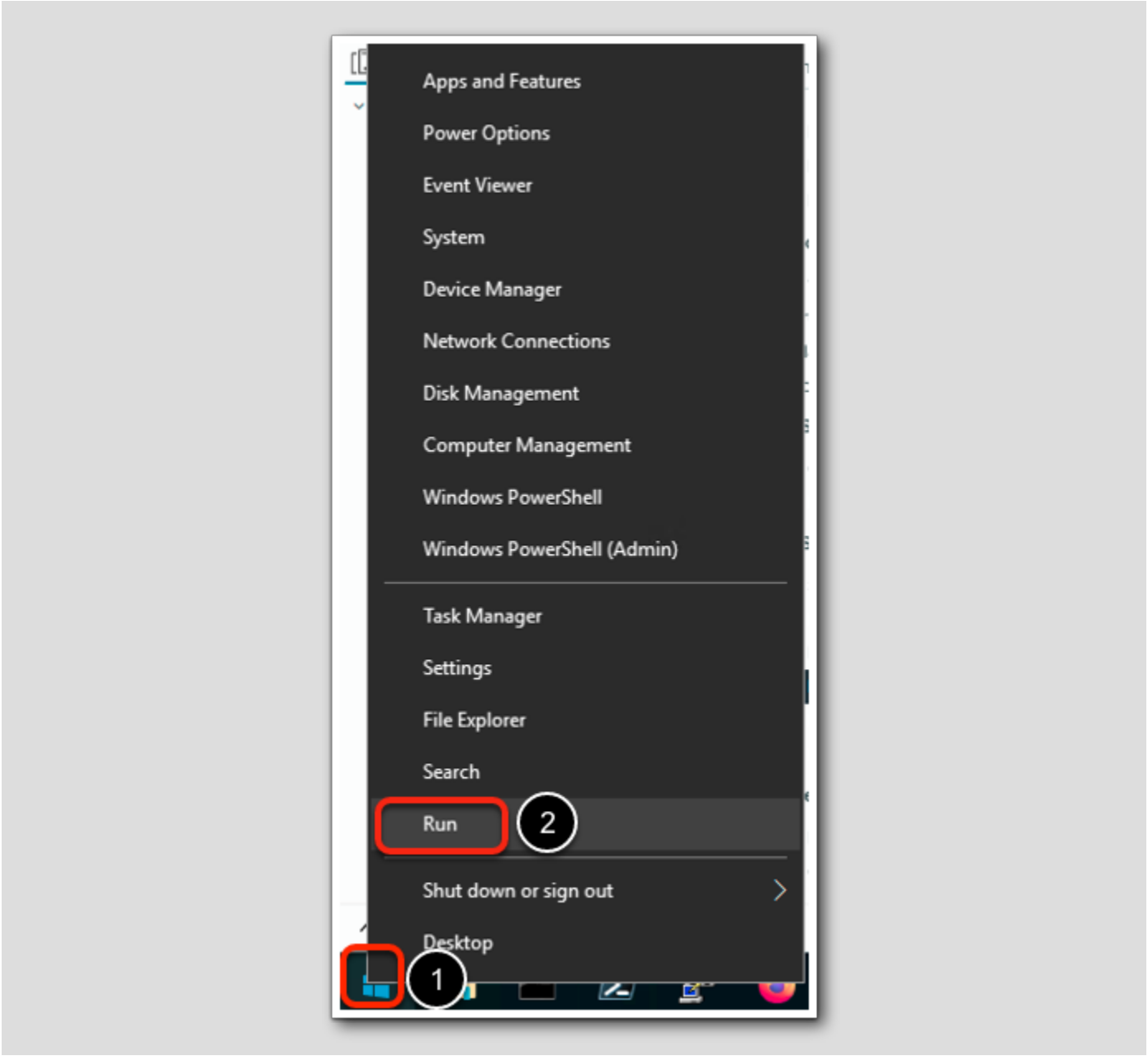
[167]



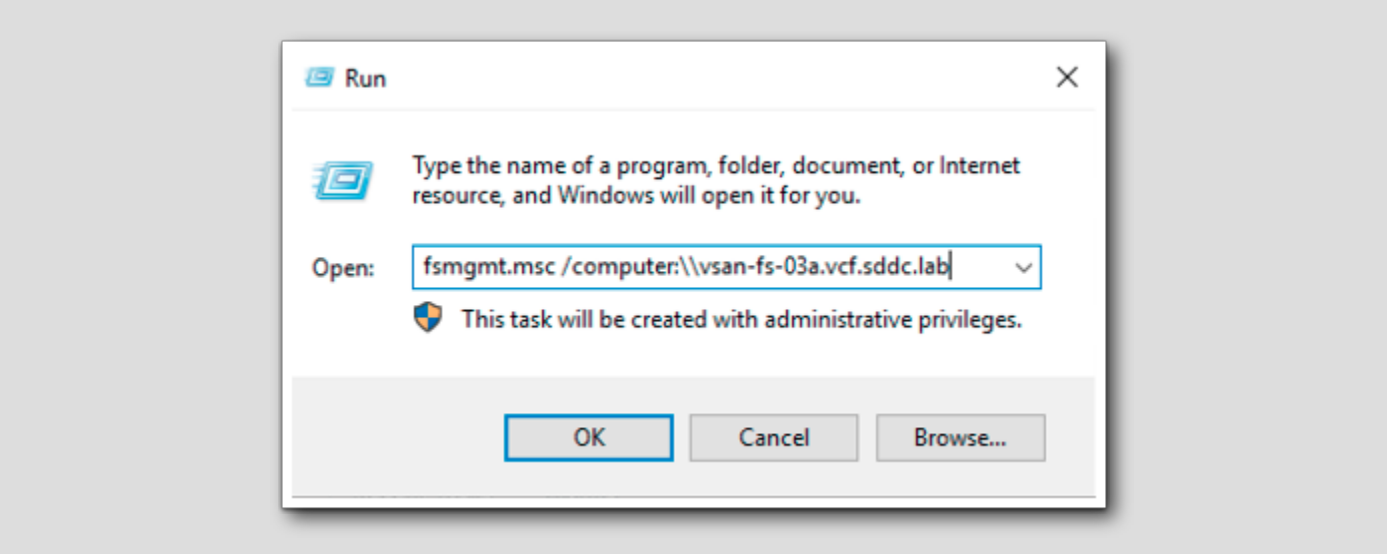
We will find the MMC command so we can use it to launch MMC.

1. Select **vSAN > File Shares**
2. Check mark on **SMBShares**
3. Click on **COPY MMC Command** to view the command string and details

Open the windows menu on your taskbar [168]



1. Right-click the **Start** button from the task bar
2. Select **Run**

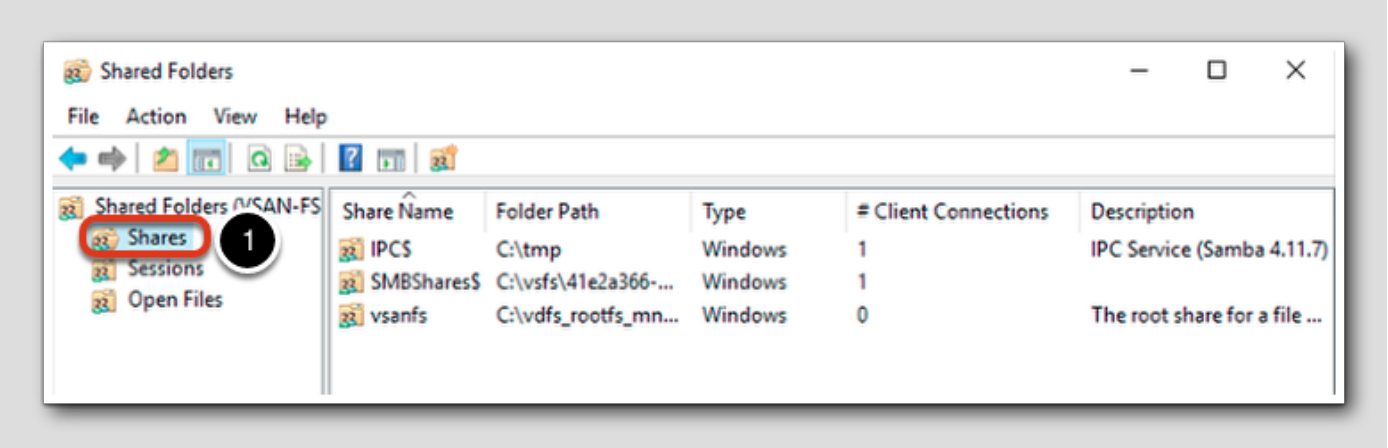


1. Paste the command from vCenter into the Run window and then click OK.

`fsmgmt.msc /computer:\\vsan-fs-03a.vcf.sddc.lab` (The address you paste might be different)

SMB Shares

[169]



1. Select **Shares**

You can see the SMB shares called **SMBShares**

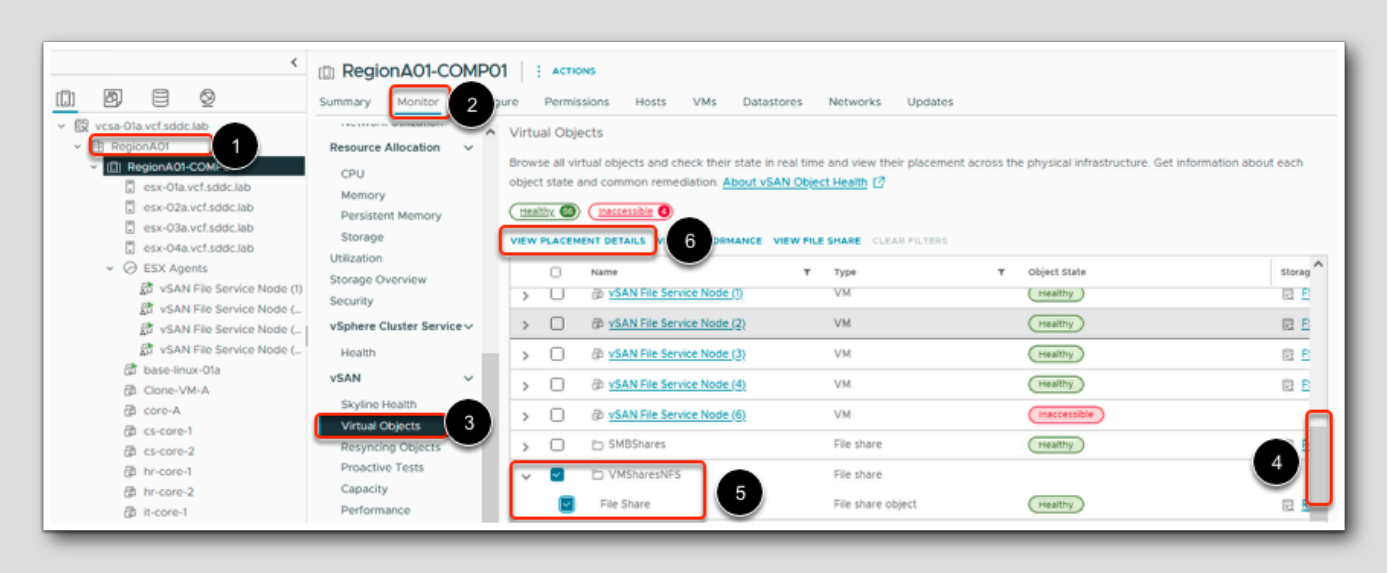
vSAN File Services Monitoring [170]

You can monitor the performance and capacity of vSAN file shares.

vSAN Object View and Health Integration [171]

Since the file share is instantiated on vSAN, you can see the file share from the file shares view and see the file share details in the Virtual Object View

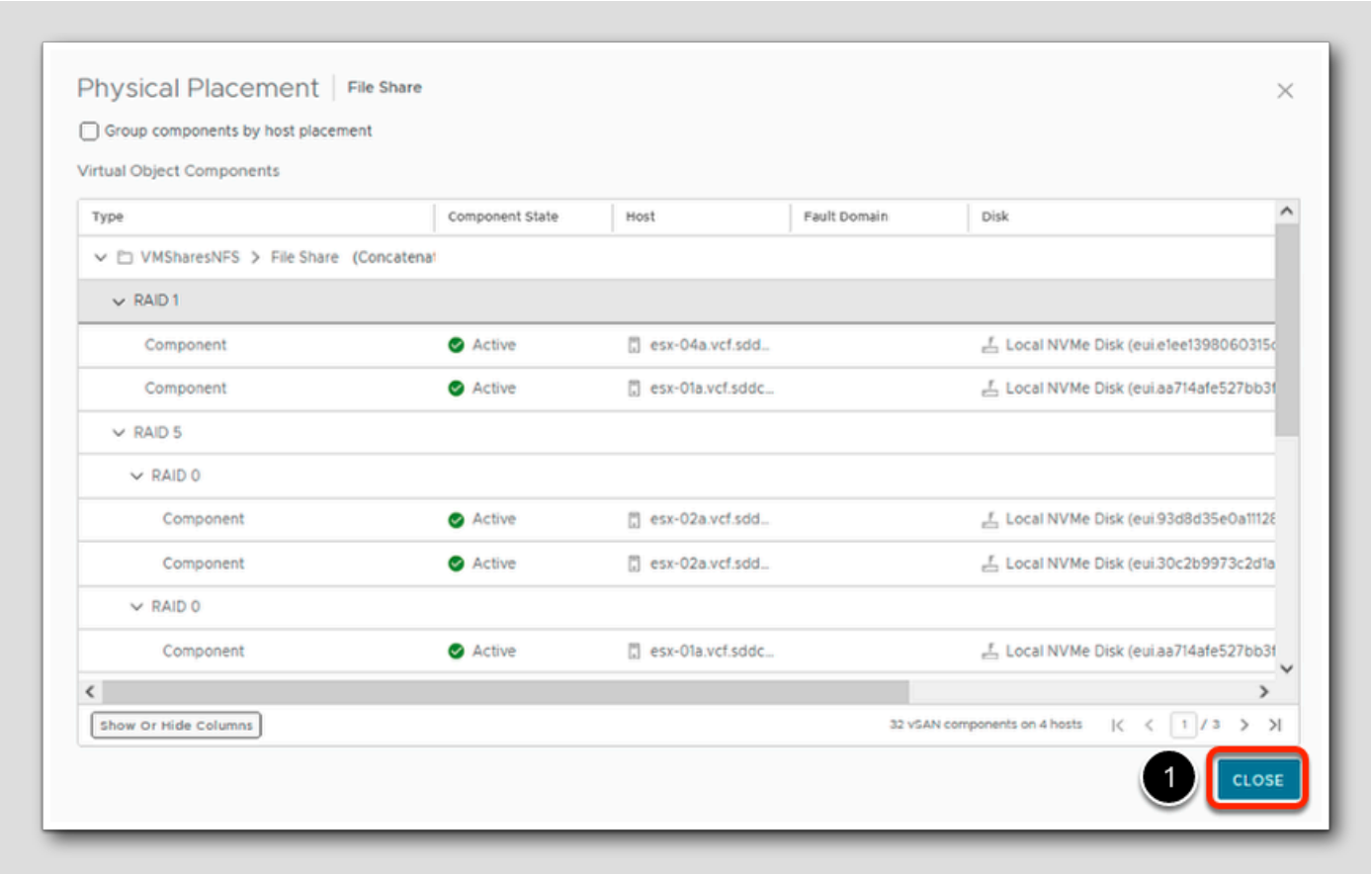
View Placement Details [172]



1. Select **RegionA01-COMP01**
2. Select **Monitor**
3. Select **vSAN > Virtual Objects**
4. **Scroll down**
5. Check mark **VMSharesNFS**
6. Select **VIEW PLACEMENT DETAILS**

Review Physical Placement

[173]

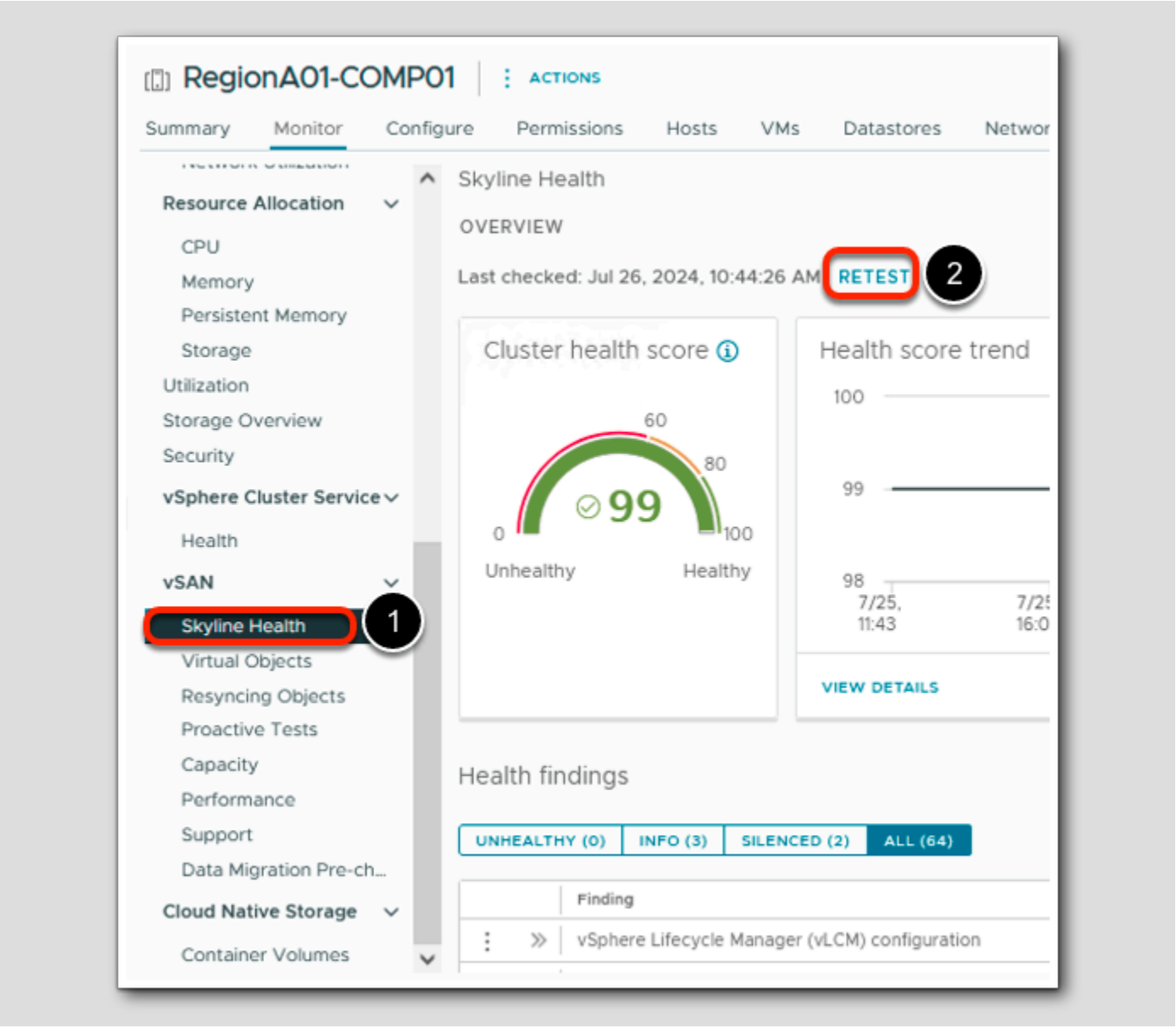


You can see layout of the underlying vSAN object to see which hosts and which physical storage devices are used for placing the components of the file share object.

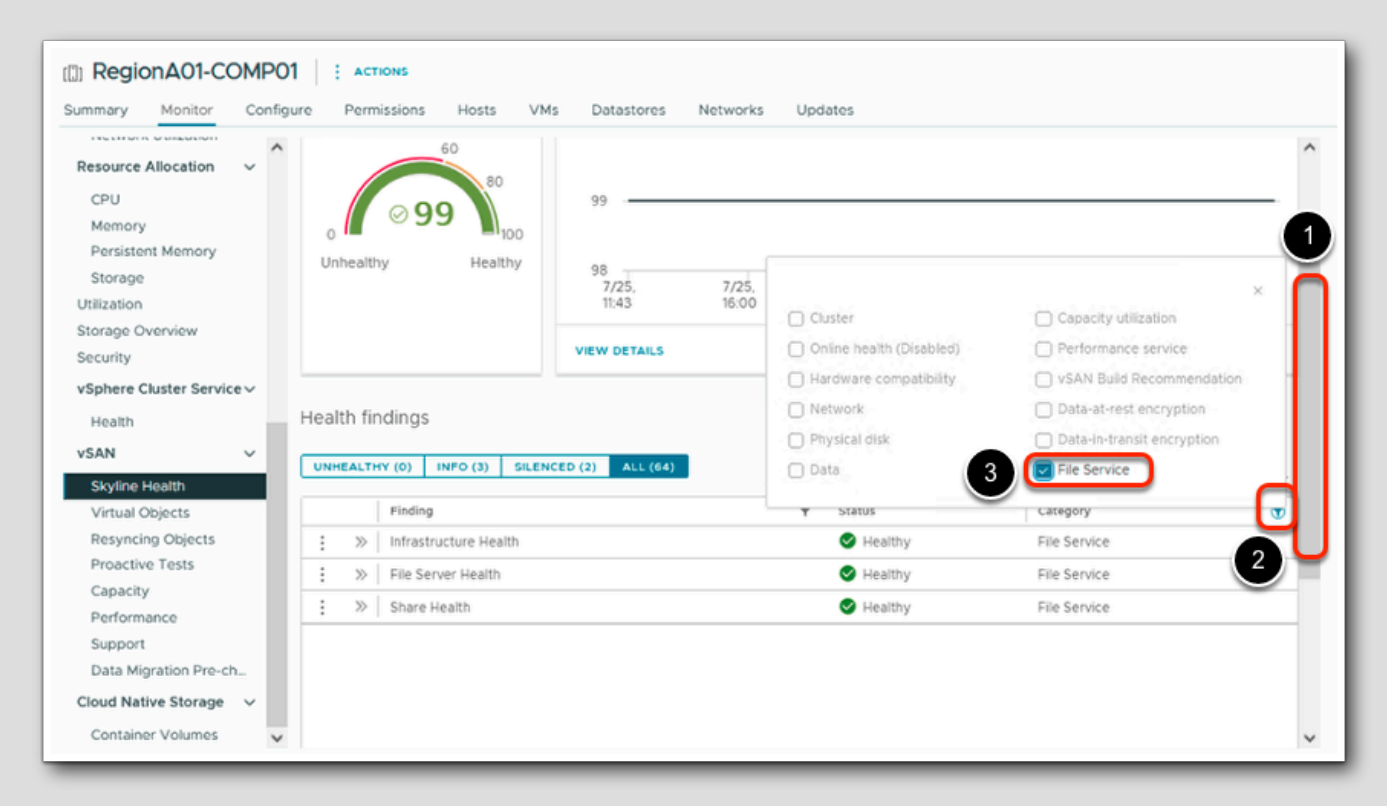
1. Click **CLOSE**

Skyline Health - File Service

[174]



1. Select **vSAN > Skyline Health**
2. Click the **RETEST** link (although the health check runs on a scheduled basis, since we just added a new service a few minutes ago we should force a retest before checking the health of our file shares in this lab exercise).



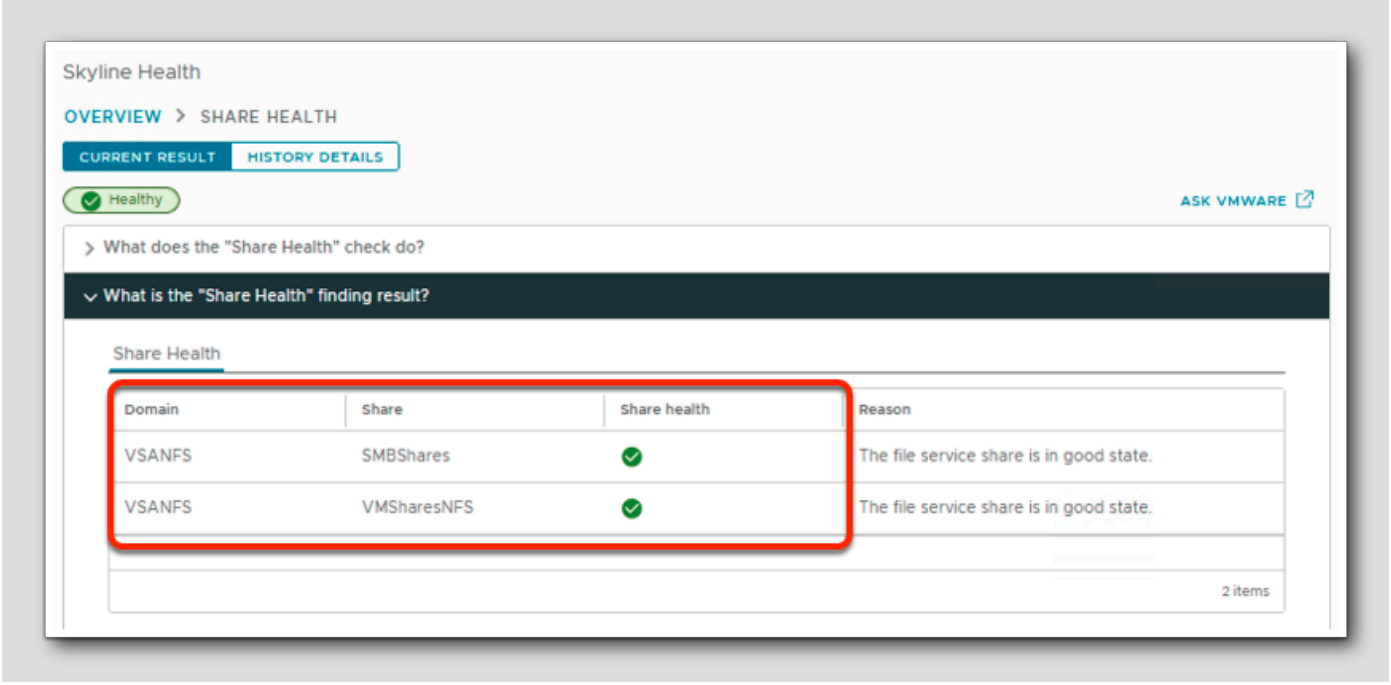
After the retest of the cluster health completes …

1. Scroll vertically downward to better see the *Health findings* area
2. Click the filter icon to filter on Category
3. Check the box next to File Service

Skyline Health - Share Health

[175]

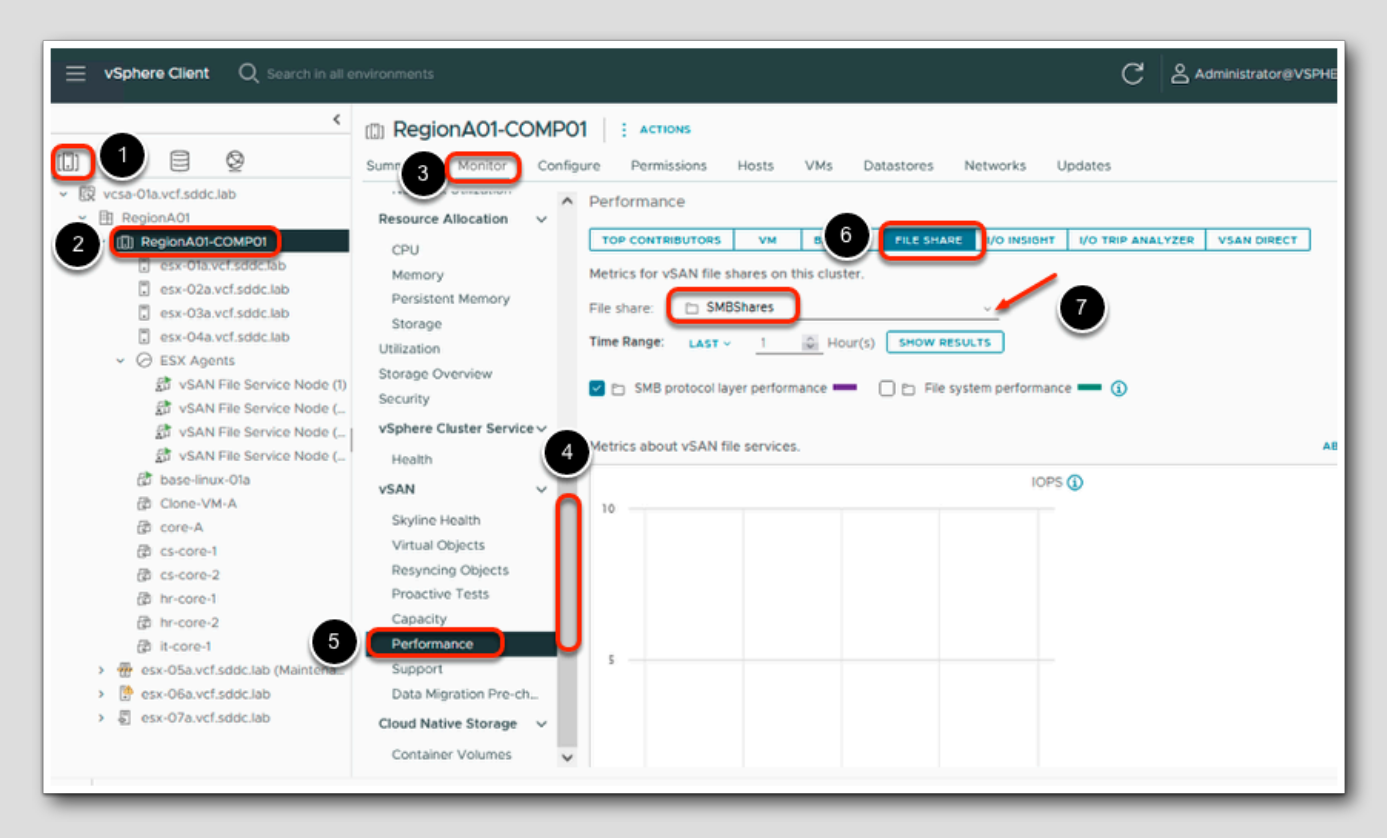
1. Click the three vertical dots on the **Share Health** finding
2. Select View Current Result from the popup dialog box



We observe that the both the file shares we created in the lab exercises are healthy.

Monitoring Performance

[176]



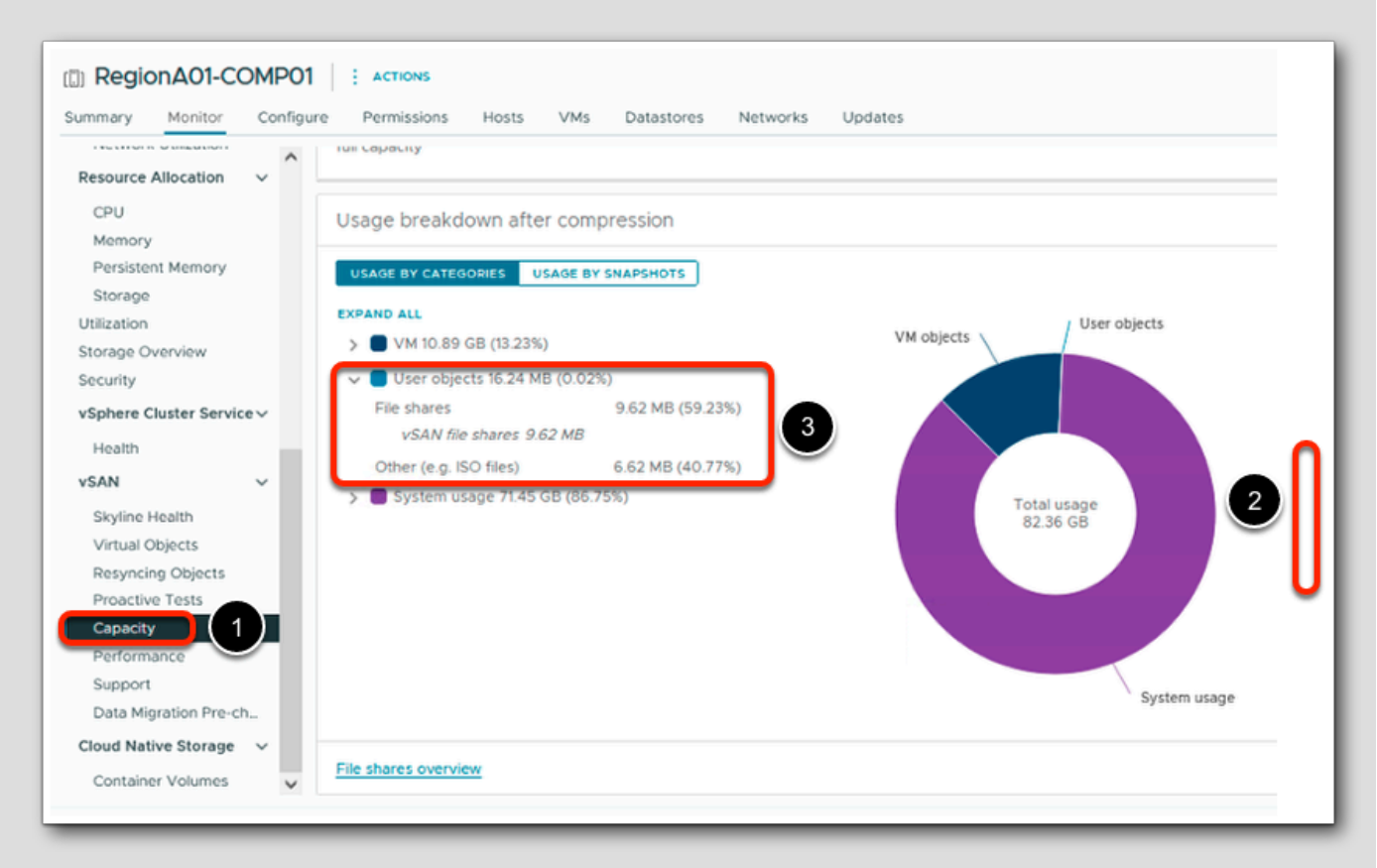
1. Select **Host and Cluster** Icon
2. Select **RegionA01-COMP01**
3. Select **Monitor**
4. Scroll vertically to reveal **vSAN**
5. Select **vSAN > Performance**
6. Select **FILE SHARE**
7. Click the "\/" and select SMBShares from the list of available vSAN file shares

You can browse the performance screens and you might see the latency and throughput spikes when we mount the shares and created a file.

Monitor Capacity

[177]

You can monitor the capacity for both native file shares and Cloud Native Storage (CNS)-managed file shares.



1. Click **Capacity**, under **vSAN**
2. **Scroll down**
3. Notice the **File Shares** usage breakdown for **vSAN file Shares**

Conclusion [178]

You Finished Module 4 [179]

Congratulations on completing Module 4.

To take additional modules, please follow one of the links below:

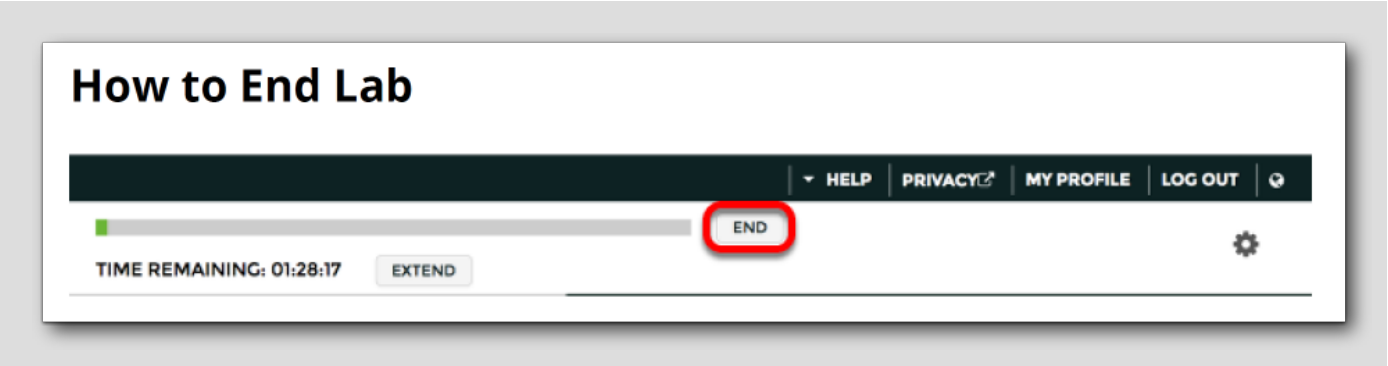
- Module 1 - vSAN SPBM and Availability (30 minutes) (Basic) Introduction to VMware vSAN's Express Storage Architecture. We will cover the power of Storage Based Policy Management (SPBM) and show you the availability of vSAN.
- Module 2 - Monitoring, Health, Capacity, and Performance (30 minutes) (Basic) 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 Encryption and Security (30 minutes) (Advanced) Introduction to vSAN Encryption. We will enable a Key Management Server and demonstrate how to configure vSAN Encryption.
- Module 5 - Data Protection (30 minutes) (Advanced) Introduction to vSAN ESA's new data protection capabilities. We will cover creating protection groups and snapshot schedules.
- Module 6 - vSAN Stretched Cluster (30 minutes) (Advanced) Introduction to vSAN Stretched Clusters. We will convert an existing vSAN cluster into a stretched cluster. In addition, we will explore storage policies as well as Skyline Health checks with respect to stretched clusters.

Test Your Skills [180]

Now that you've completed this lab, try testing your skills with VMware Odyssey, our newest Hands-on Labs gamification program. We have taken Hands-on Labs to the next level by adding gamification elements to the labs you know and love. Experience the fully automated VMware Odyssey as you race against the clock to complete tasks and reach the highest ranking on the leaderboard. Try the vSAN Odyssey lab.

How to End Lab

[181]



If you would like to end your lab click on the **END** button.

Module 5 - Data Protection

vSAN Data Protection - Introduction

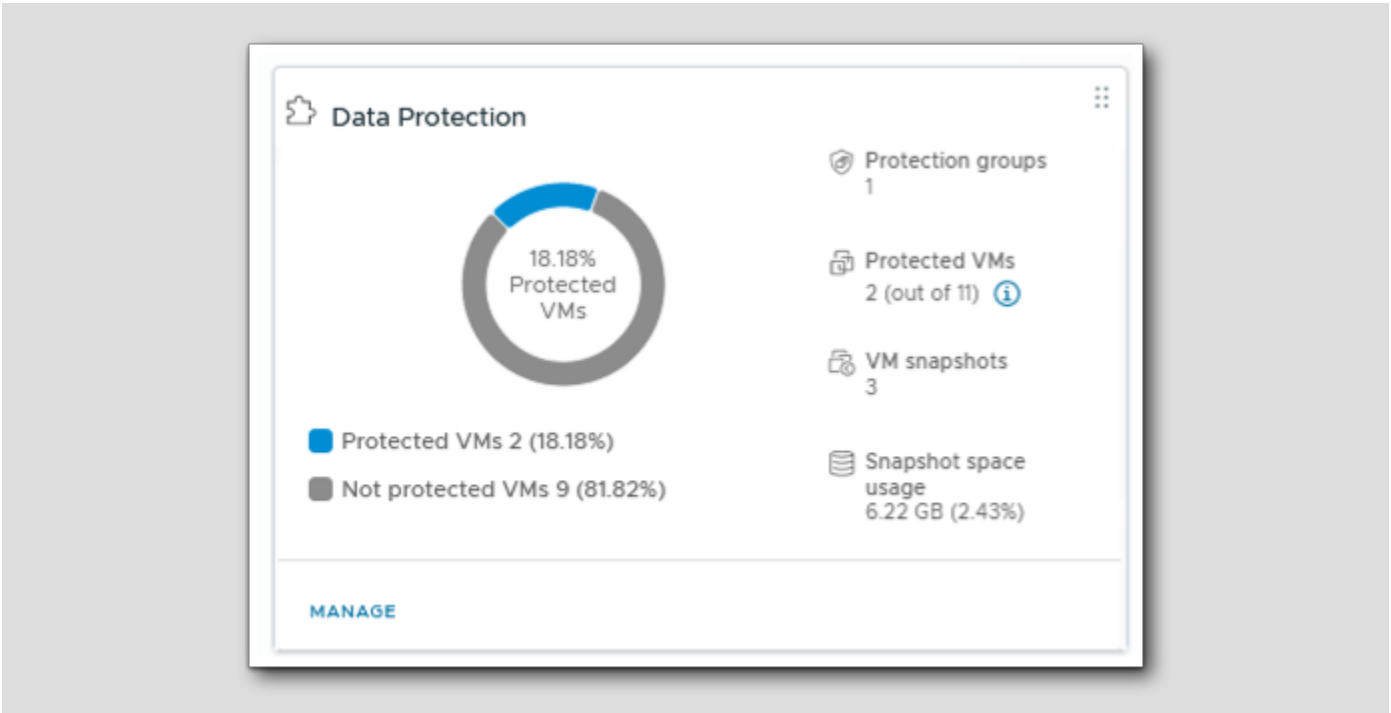
[183]

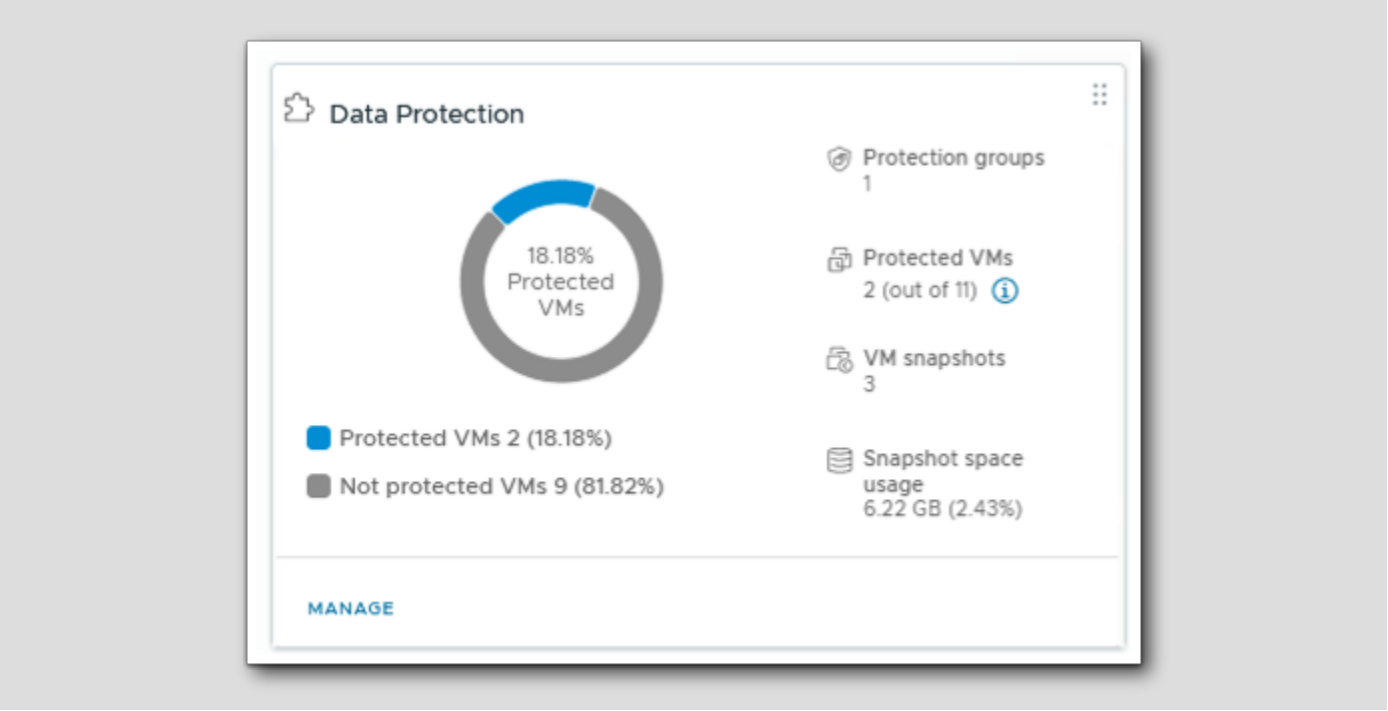
vSAN Data Protection - a newly-available feature introduced in vSAN 8.0 Update 3 - enables you to quickly recover VMs from operational failure or ransomware attacks, using native snapshots stored locally on the vSAN cluster.

vSAN Data Protection (DP) uses Policy-based "protection groups" to manage the schedule and retention period of applications and vms. vSAN DP can be used to recover VMs from accidental deletion and to quickly clone VMs for operational agility. vSAN Data Protection also integrates with VMware by Broadcom's separately-available VMware Live Cyber Recovery solution to streamline recovery from Ransomware events.

vSAN Data Protection is supported on vSAN HCI clusters powered by vSAN Express Storage Architecture (ESA). It uses native vSAN snapshots to capture the current state of your VMs. You can use vSAN snapshots to restore a VM to its previous state, or clone a VM for development and testing.

vSAN Data Protection requires the VMware Snapshot Service to manage vSAN snapshots. This service is provided by a VMware virtual appliance available for download from VMware by Broadcom's public website. Once the "SnapService" virtual appliance is installed and registered to the vCenter Service instance - as we've already done for this lab - vSAN data protection will appear in the vSphere Client.





vSAN ESA Snapshots

[184]

vSAN Express Storage Architecture offers integrated high-performance snapshots that preserve the state and data of a virtual machine at the time you take the snapshot. This local archive preserves the VM's data as it existed at that time. You can restore a VM to the state that existed when the snapshot was taken, or create a linked clone VM that matches the state preserved in the snapshot.

Taking a snapshot captures the VM state at a specific point in time. vSAN snapshots are not quiesced, and they capture the current running state of the VM.

Snapshots operate on individual virtual machines. Each VM requires a separate snapshot. You can take manual or scheduled snapshots of virtual machines by placing them in protection groups.

Each vSAN snapshot contains the state of the VM's namespace object and virtual disk objects. vSAN takes snapshots of VMs in protection groups at scheduled intervals. These vSAN snapshots are stored locally in the vSAN datastore.

vSAN Data Protection - User Interface

[185]

Let's use the vSphere Client to explore the user interface, protect & recover VMs and otherwise administer our environment. If you haven't already done so, please login to the vCenter Server using the Firefox browser as instructed below …

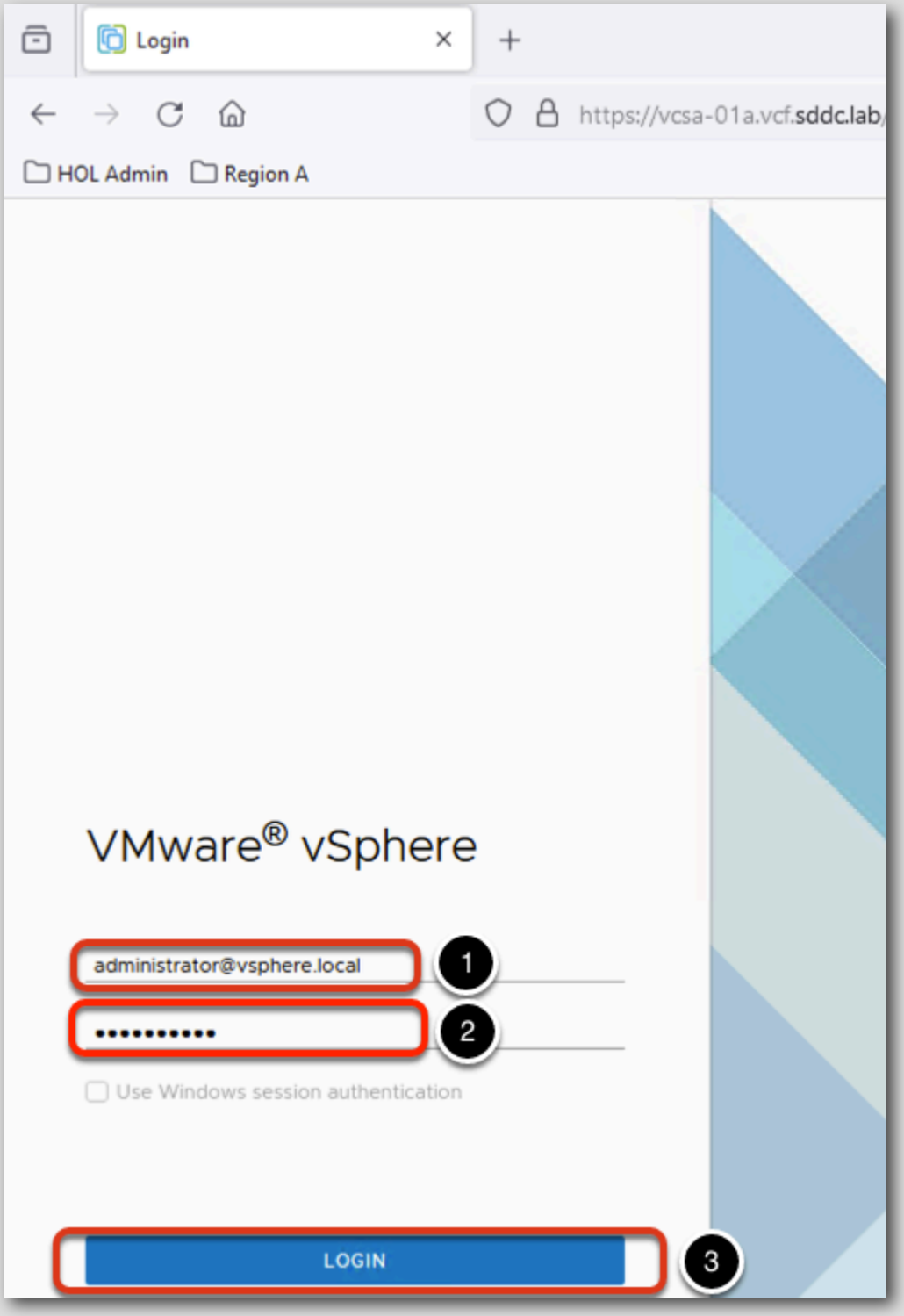
Open Firefox Browser from Windows Quick Launch Task Bar

[186]

1. Click on the **Firefox Icon** on the Windows Quick Launch Task Bar. You can skip this step if you're already in vSphere Client.

Login to vSphere Client

[187]

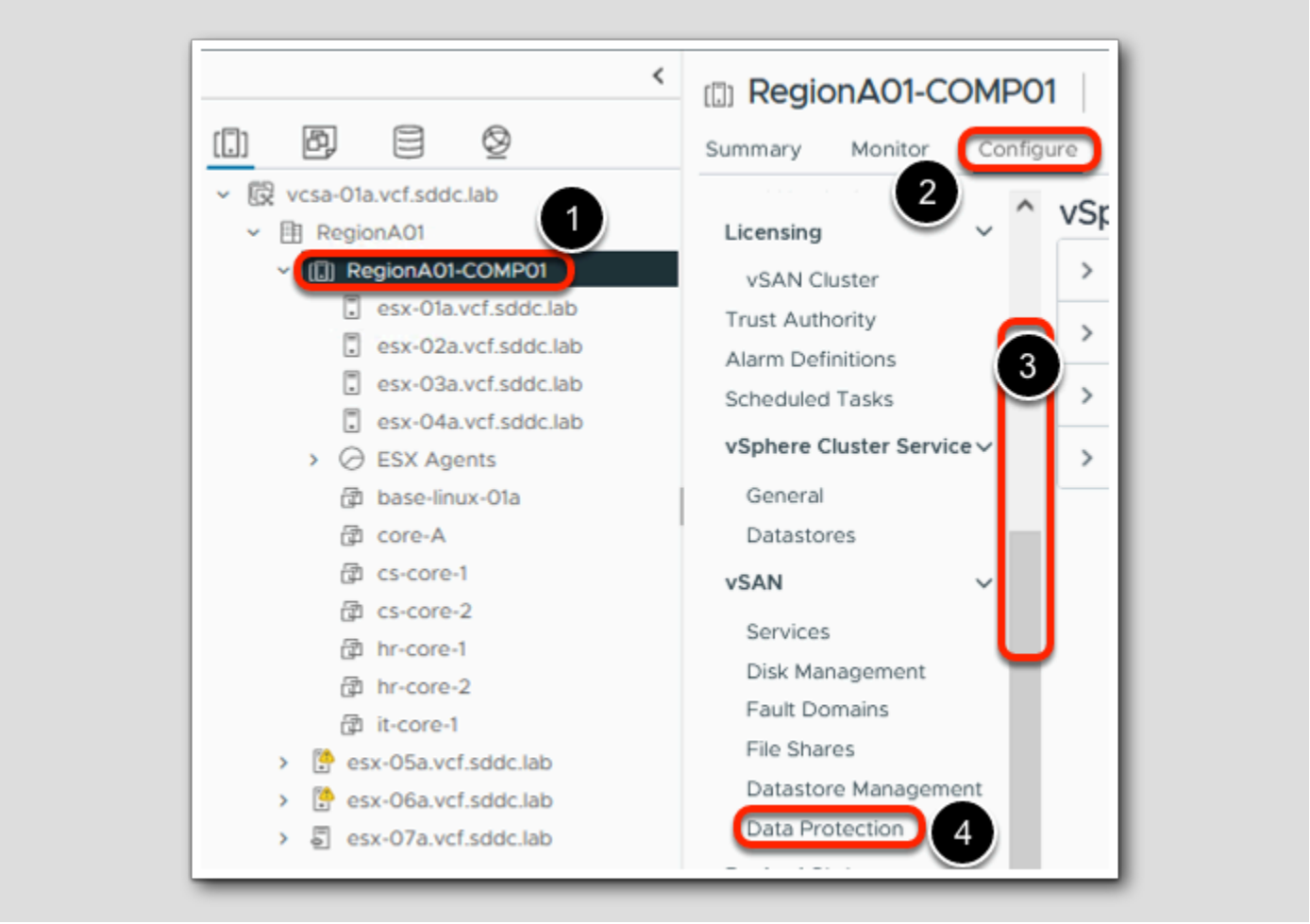

Login
https://vcsa-01a.vcf.sddc.lab/
HOL Admin
Region A
VMware® vSphere
administrator@vsphere.local
1
2
Use Windows session authentication
LOGIN
3

1. On the vSphere Client login screen, username: `administrator@vsphere.local`
2. Enter Password: `VMware123!`
3. Click **LOGIN**

You can skip this step if you're already in vSphere Client.

Navigate to vSAN Data Protection

[188]

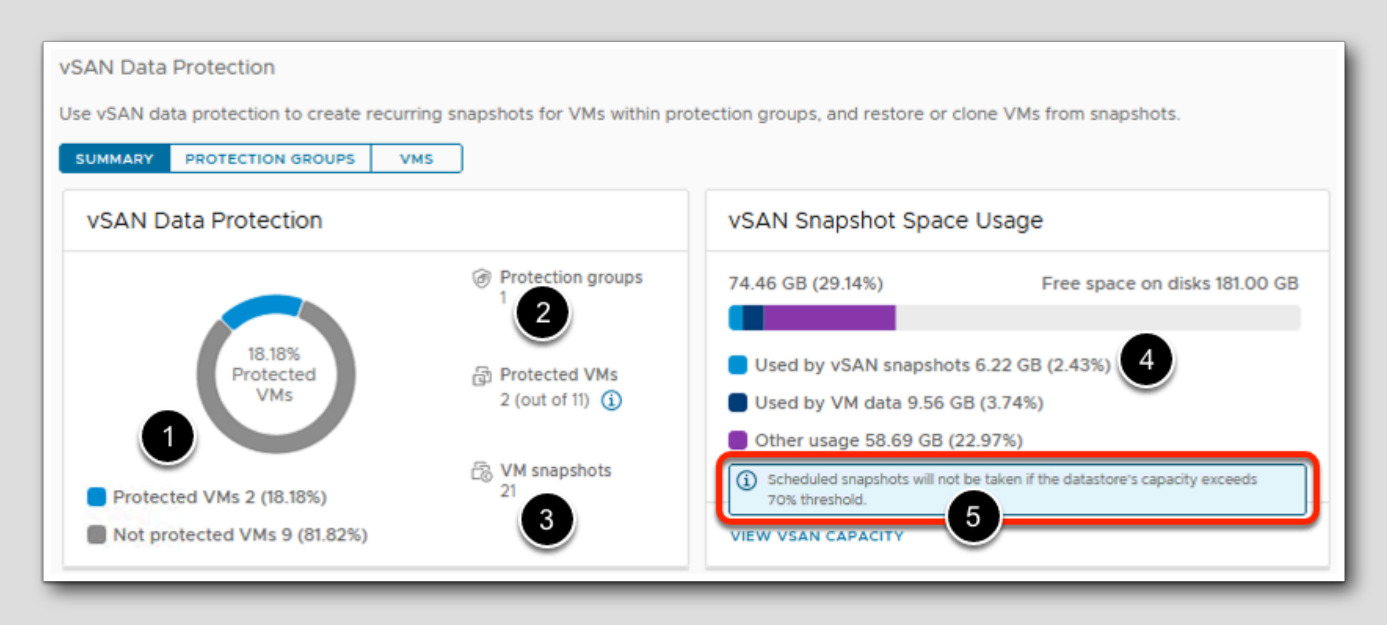


From the "Inventory" view of vSphere Client:

1. Select the **RegionA01-COMP01** vSAN cluster;
2. Select **Configure**;
3. **Scroll vertically** until you see **vSAN** configuration settings;
4. Select **Data Protection**.

Examine the vSAN Data Protection Summary Screen

[189]

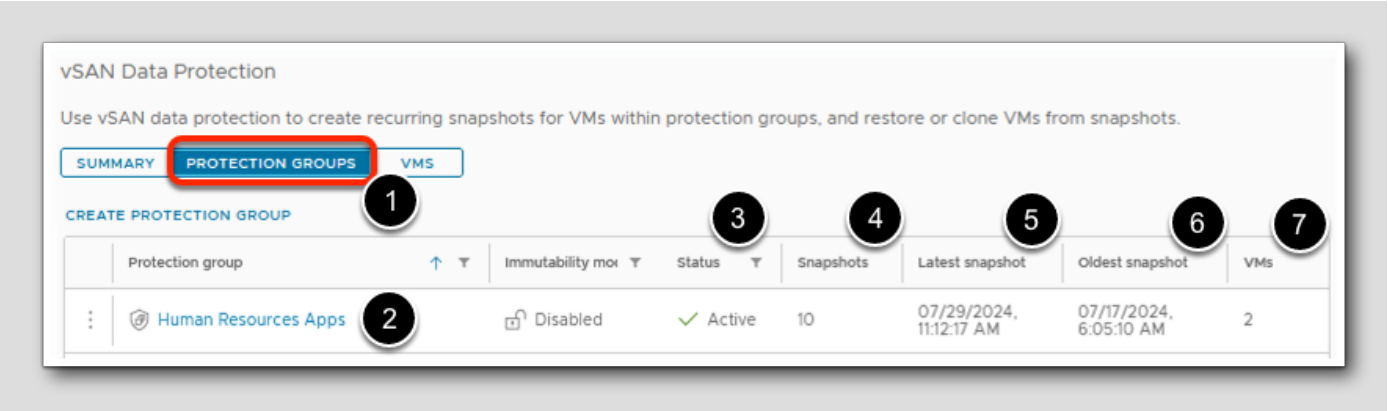


1. At this time in our lab only 2 out of 11 total VMs are included in Protection Groups;
2. There is only 1 defined Protection Group;
3. vSAN Data Protection is managing 21 total snapshots for protected VMs (*this number will vary depending from session to session - your number might be different depending on how long your lab session has been active*);
4. The amount of storage consumed by vSAN snapshots - both in a capacity (GB) and percentage of total vSAN datastore capacity; and
5. Reminder that scheduled snapshots will not be taken if the vSAN datastore's capacity exceeds 70% threshold - this behavior is a safety net to prevent vSAN DP snapshots from hindering normal operation of your vSAN datastore.

Protection Groups

[190]

Protection Groups are used to protect VMs by specifying the included VMs, configuring the snapshot frequency and specifying a retention period.

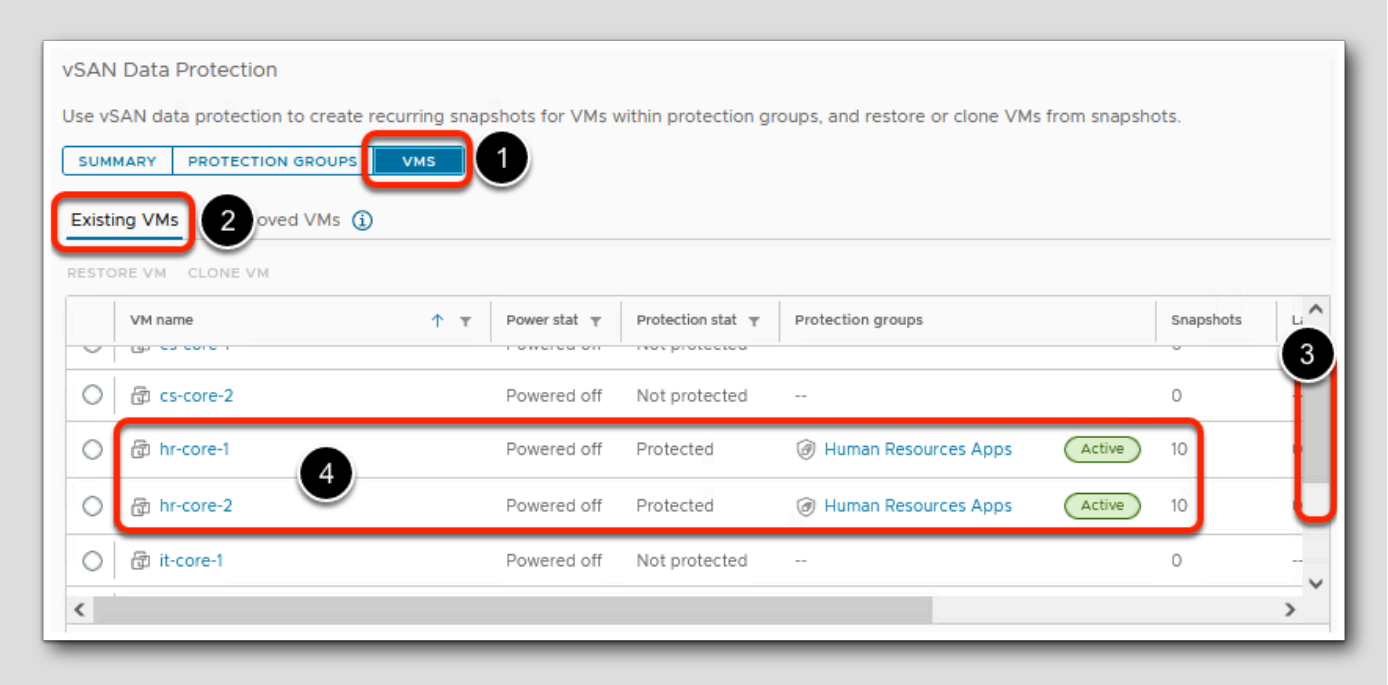


1. Select the **Protection Groups** section;
2. There is only one Protection Group defined - to protect the "Human Resources" (HR) Applications;
3. The *Human Resources Apps* Protection Group is "Active" so scheduled snapshots will be taken as configured;
4. There are currently 10 snapshots associated with this Protection Group (again this number will vary from lab session to lab session);
5. The most recent snapshot for this protection group was taken on July 29, 2024 at 11:12 AM (your lab will have different time stamp);
6. The oldest snapshot was taken on July 17th, 2024; and
7. There are currently 2 VMs associated with this protection group.

Existing VMs

[191]

The VMs stored on vSAN datastores and their protection group status is listed here. Protected VMs can be restored to an earlier state, or quickly cloned for other use-cases - we'll explore these activities later in this lab.

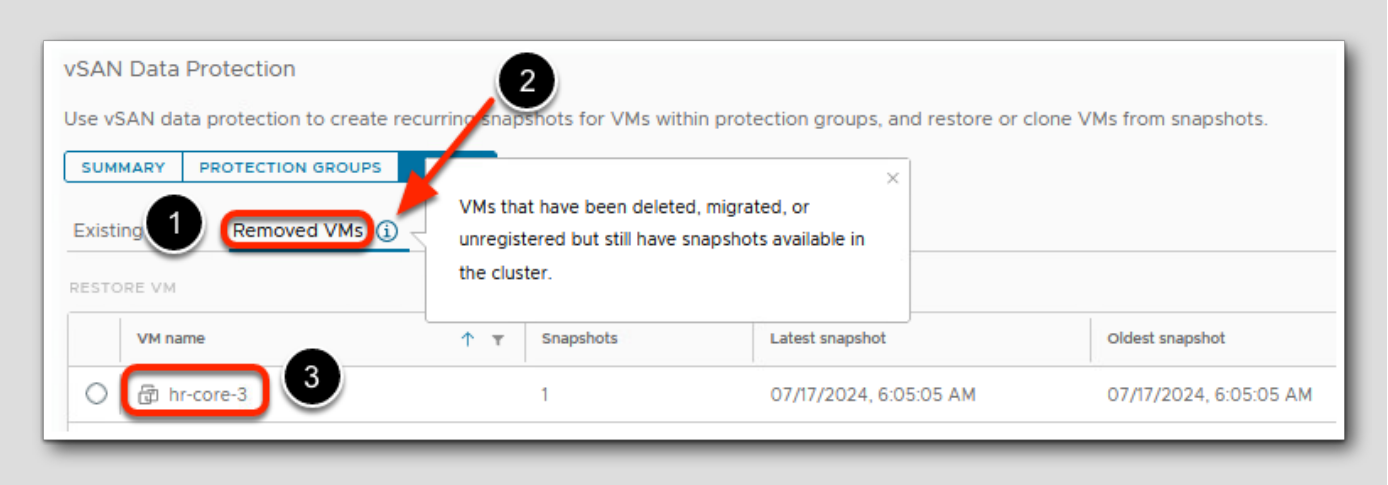


1. Select **VMs**;
2. Notice that we are looking at Existing VMs - these are VMs currently managed by vCenter Server;
3. Scroll Vertically to reveal the "**hr-core-1 & hr-core-2**" VMs;
4. Note that these two "HR" VMs are shown as **Protected** by the Human Resources Apps Protection Group, while the adjacent VMs (cs-core-2 & it-core-1) are not protected.

Removed VMs

[192]

VMs that were members of a protection group that have been deleted, migrated or unregistered from vCenter Server yet still have snapshots available will be listed here - these VMs can be restored as we'll see a bit later in the lab.

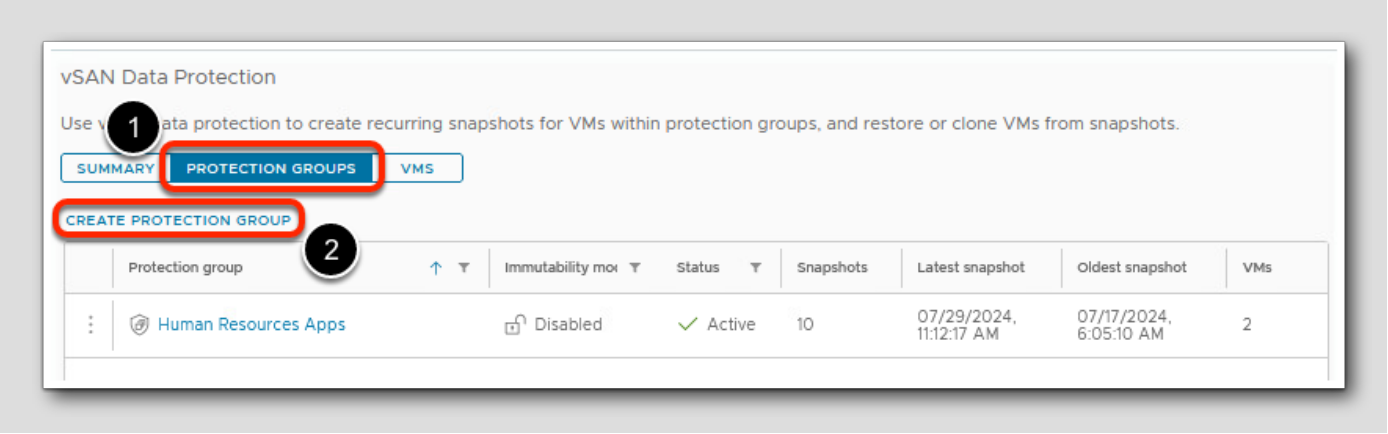


1. Select **Removed VMs**;
2. **Click** the little **(i)** icon to learn about what constitutes a removed VM; and
3. Notice that we do have a removed VM: **hr-core-3**. This VM was last protected on July 17th, 2024 and the snapshot is still available to restore this VM.

Customer Service Apps protection group

[193]

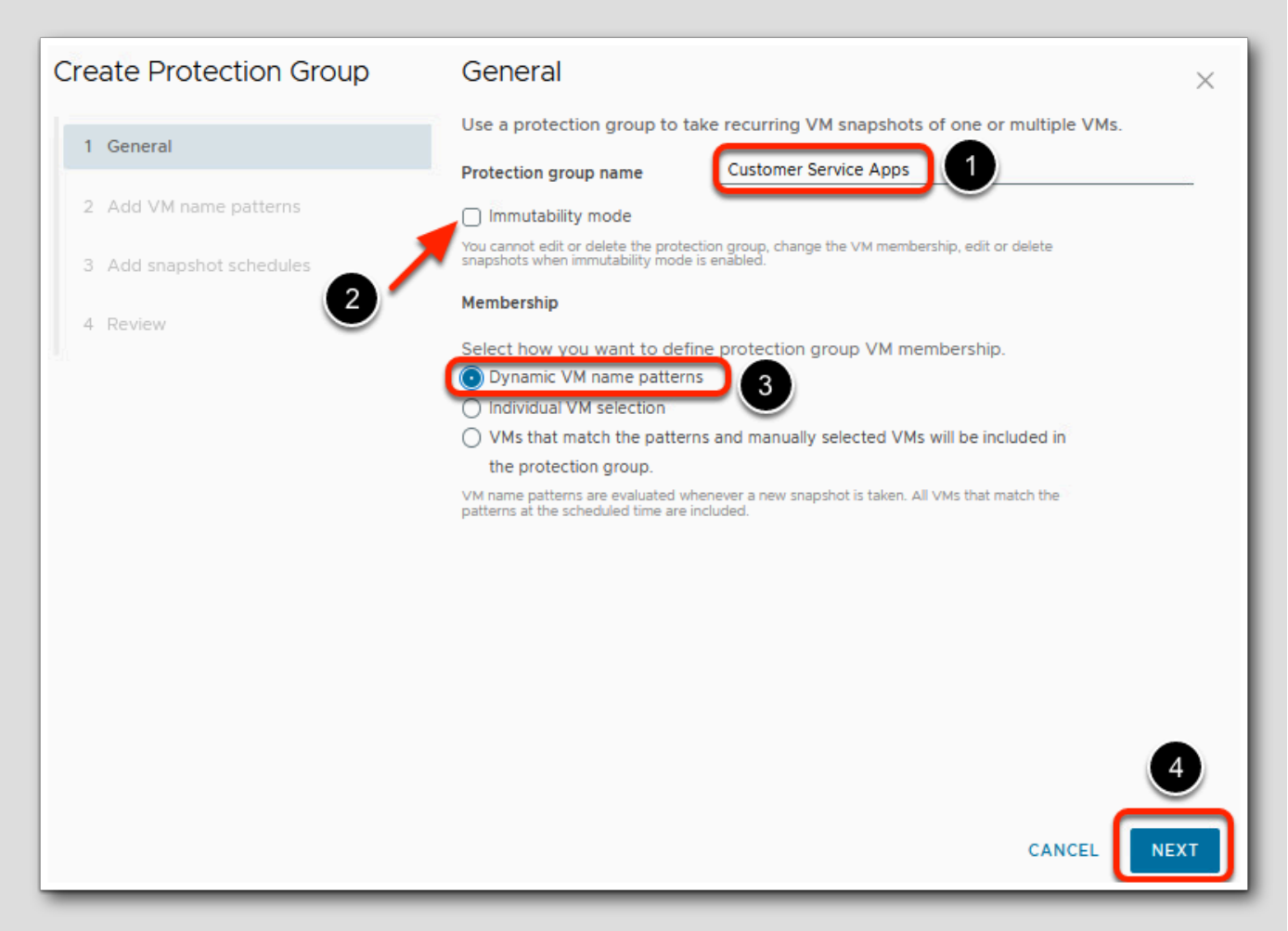
Let's create protection group to protect our customer service applications. In this lab our customer service (cs) application VMs begin with with the "cs" prefix ...



1. Select **Protection Groups**; then
2. Select **Create Protection Group**.

Create a Protection Group - General

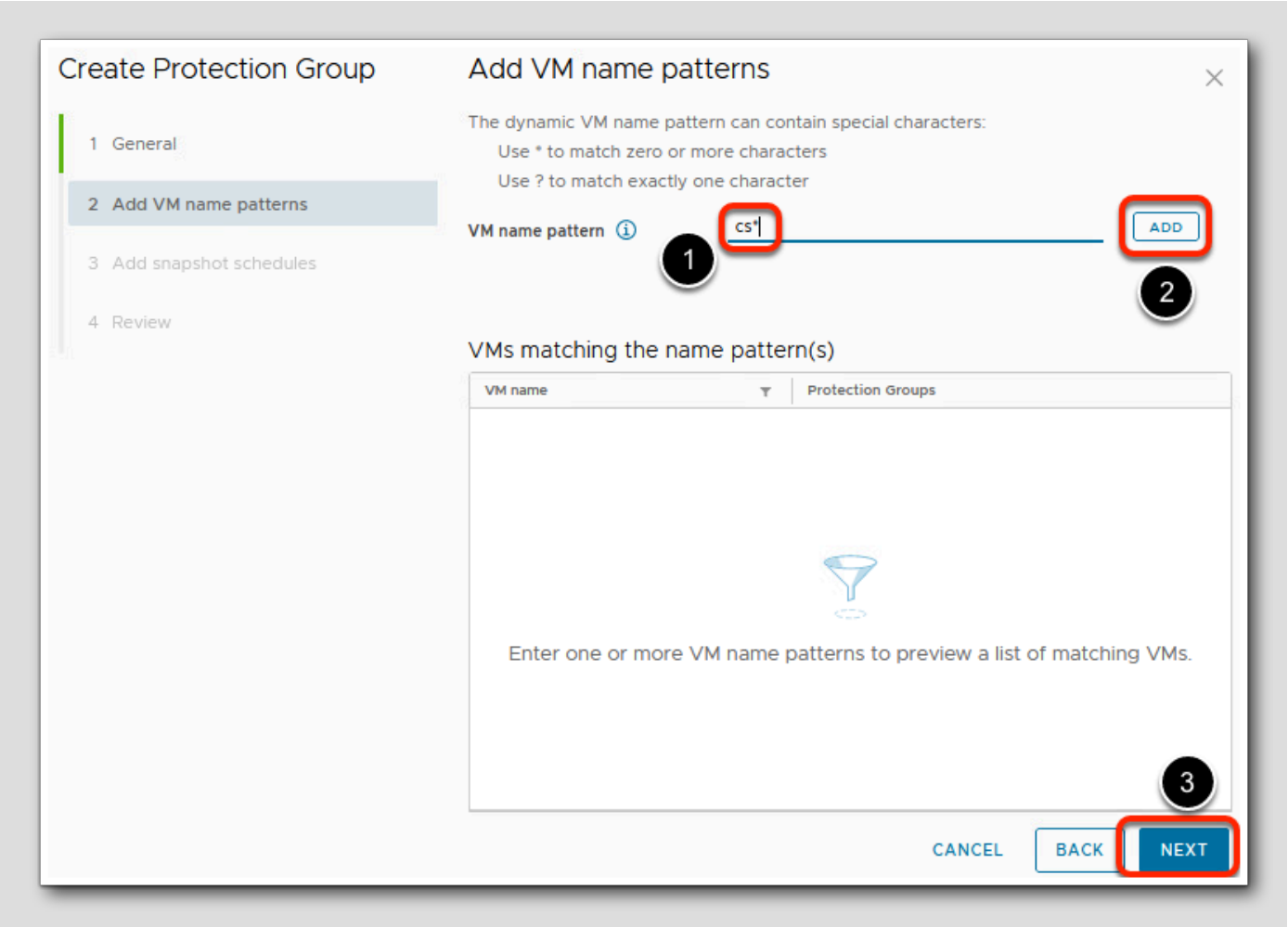
[194]



1. Type in the name **Customer Service Apps** for our new protection group;
2. Leave the Immutability Mode check box **unselected** - we will revisit Immutability mode later in this lab;
3. Select the **Dynamic VM name patterns** option to determine which VMs will be protected; and
4. Click **NEXT**.

Create Protection Group - Add VM name patterns

[195]

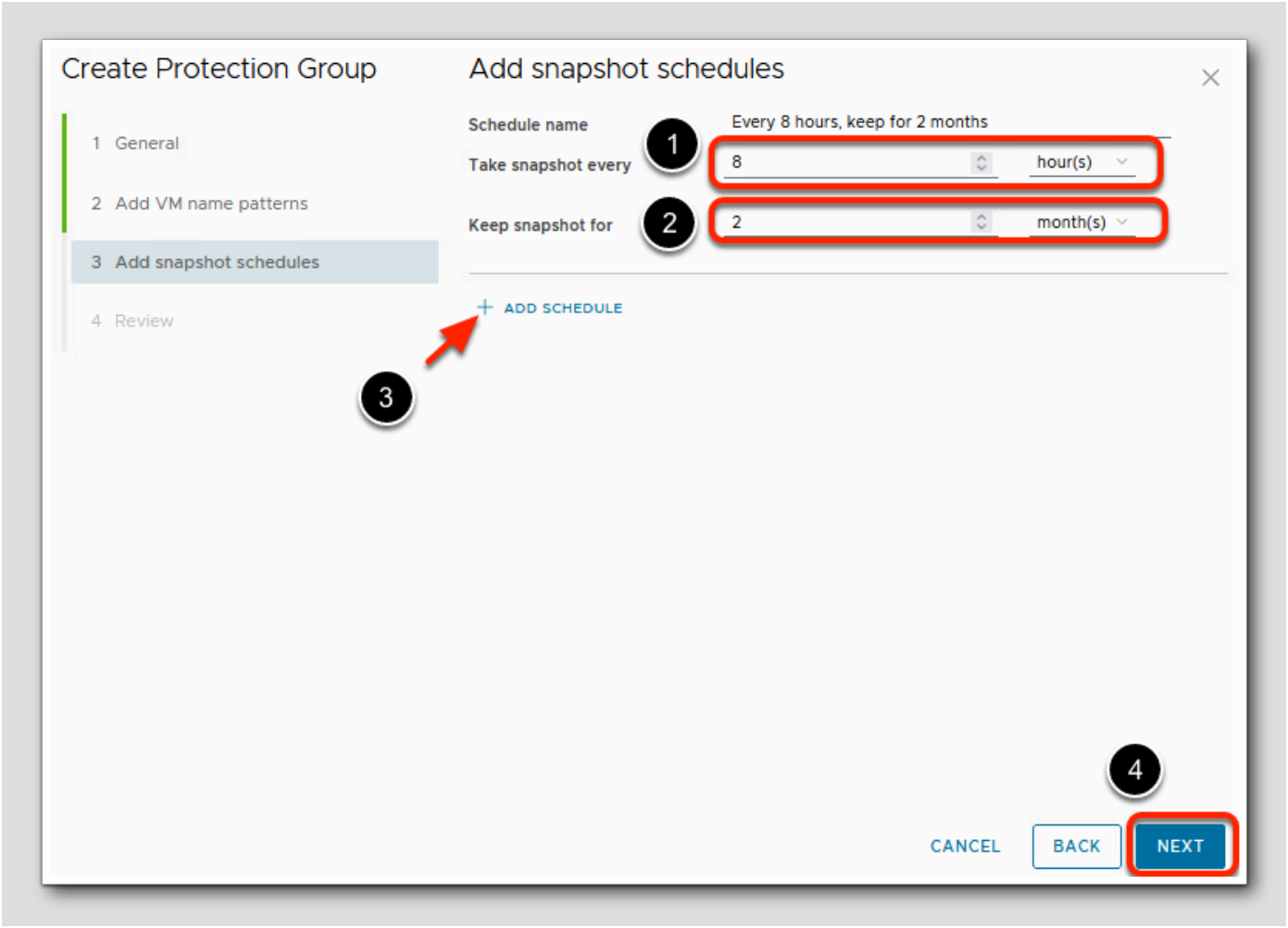


1. Type in **cs*** to define the dynamic naming pattern (all of our Customer Service application VMs use the naming convention cs-xxxx-y);
2. Click **Add** - notice that matching Customer Service Application VMs cs-core-1 & cs-core-2 will be listed as matching VMs (not reflected in screenshot);
3. Click **Next**.

Create Protection Group - Add snapshot schedules

[196]

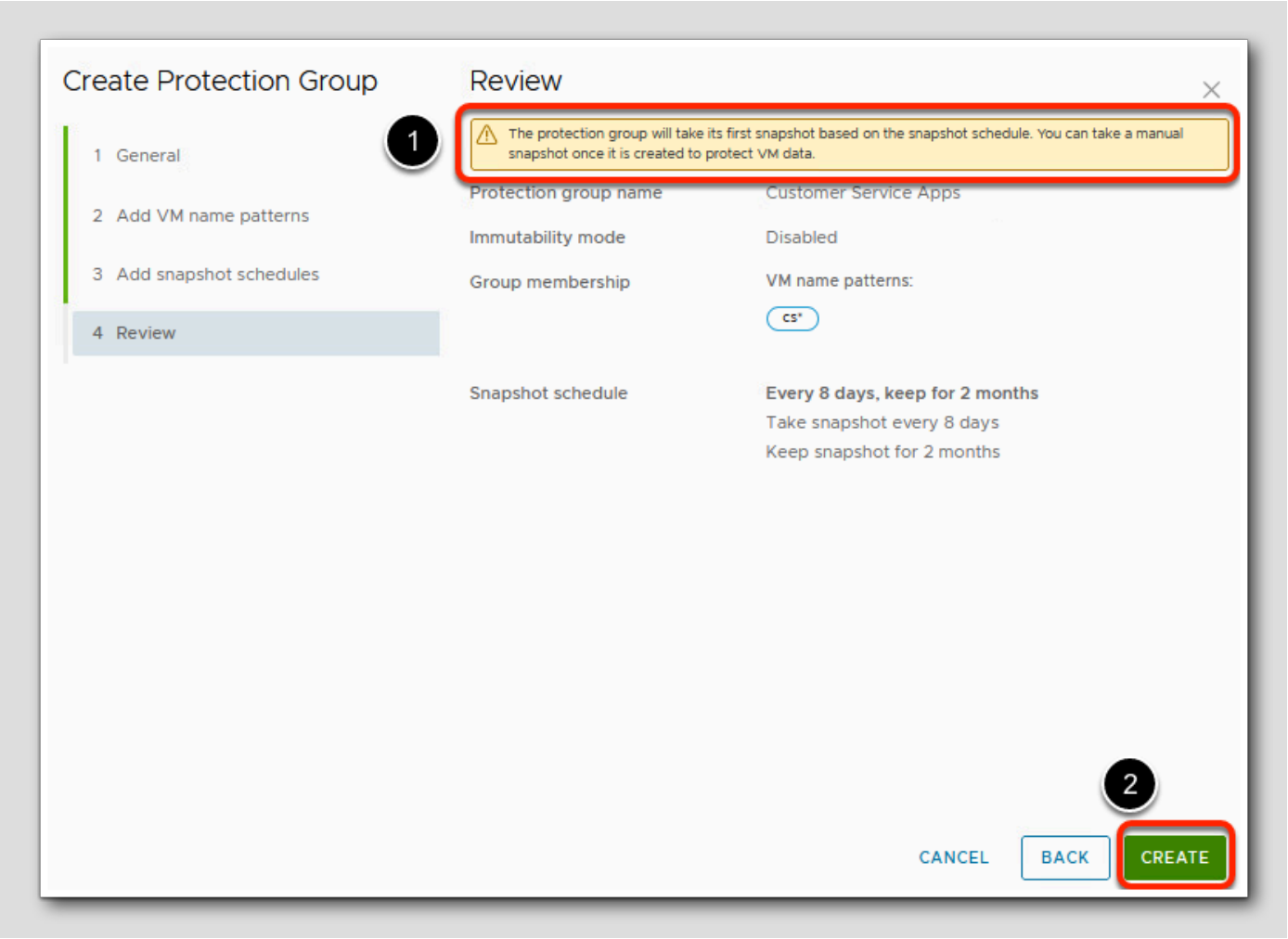
vSAN Express Storage Architecture snapshots scale to as many as 200 copies per object. When creating snapshot schedules keep this limit in mind - if your combination of snapshot frequency and retention period will exceed this limit, your protection group will need to edited before it can be created.



1. Configure our snapshot frequency (Take snapshot every …) to be every **8 hours**;
2. Configure our snapshot retention perion (Keep snapshot for …) to be **2 months**;
3. Note: *it is possible to configure multiple snapshot schedules for each protection group*, but we'll **just configure a single schedule for this lab**;
4. **Next**.

Create Protection Group - Review

[197]

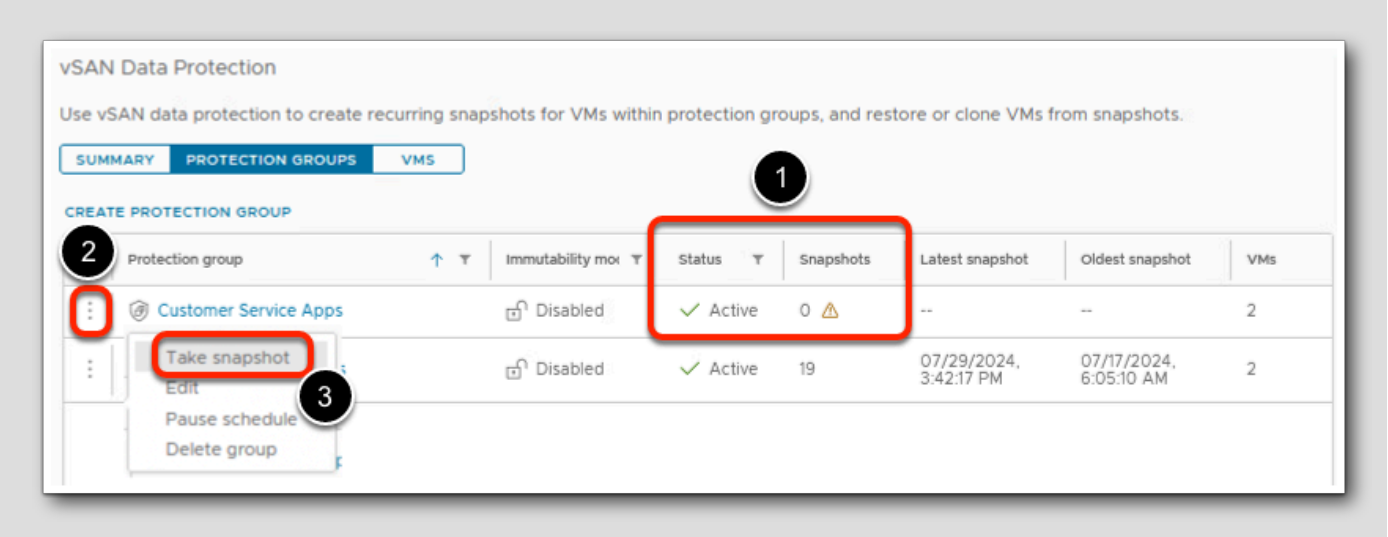


1. Notice that - unlike the common vSphere Client "snapshot" UI - *vSAN Data Protection snapshots are not created immediately*; instead **they are scheduled**. We are reminded that the vSAN Data Protection feature does allow us to create a manual snapshot if desired.
2. Click **Create**.

Take a Manual Snapshot of a Protection Group

[198]

As explained in the last step of creating our Customer Service Apps protection group we can create manual snapshot of a protection group - this will be helpful for our lab since you might not want to wait up to 8 hours for the scheduler to perform its work!

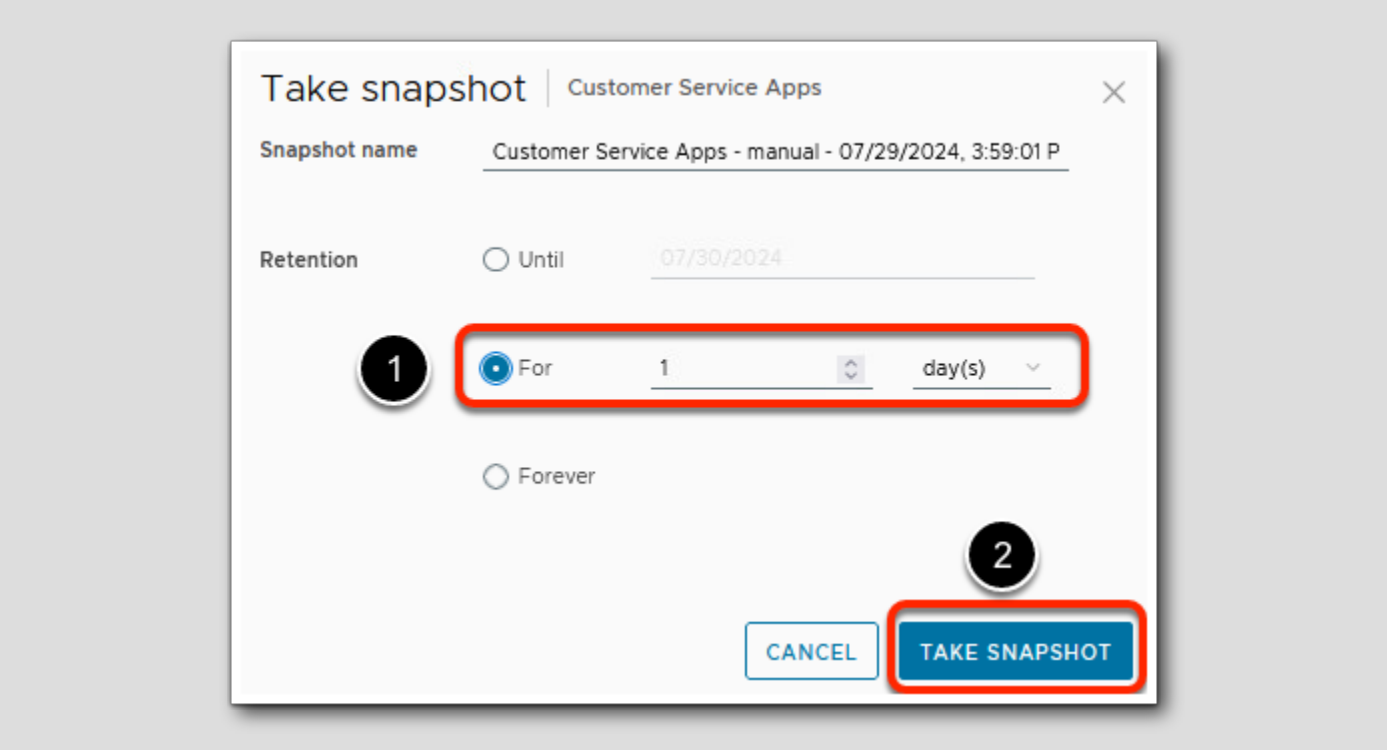


1. Notice that vSAN DP has marked our Customer Service Apps protection group with a *warning triangle* - that's because we have an Active protection group with **no snapshots** for the VMs in the protection group!
2. Click the **three vertical dots** to the left of our Customer Service Apps protection group;
3. Click the **Take Snapshot** option on the popup menu.

Take Snapshot - Name & Retention

[199]

You can name your snapshot - default is a descriptive reference to protection group and creation method with a time & date stamp. You can also choose to keep the snapshot until a specified future date, for a fixed period of time or forever.

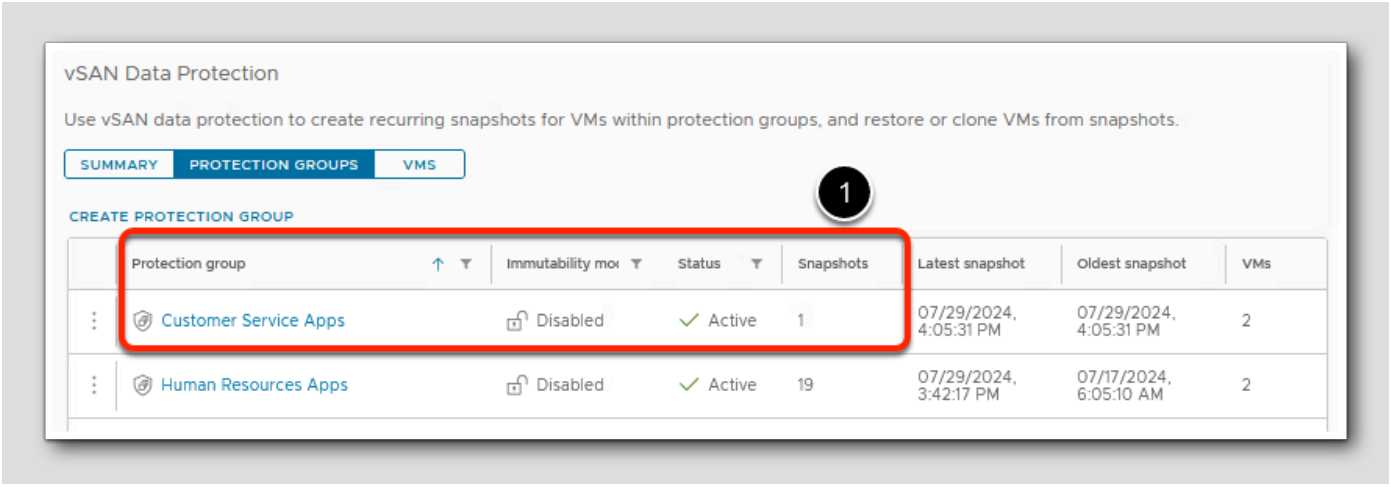


1. Select the option to retain the snapshot for **1 day**;
2. Click **Take Snapshot**.

Customer Service Protection Group - Status

[200]

Watch the recent task pane of the vSphere Client - you will see activity related to taking VM snapshots and updating the vSAN Data Protection service.

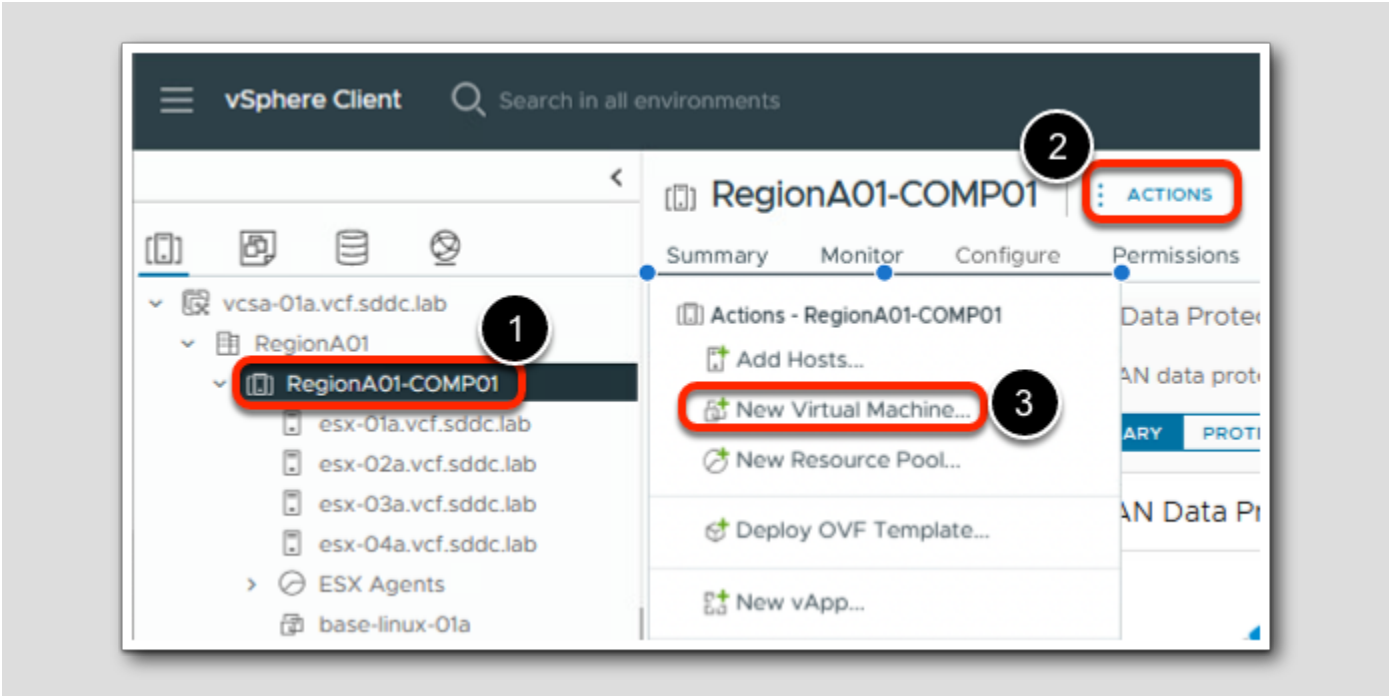


1. Notice that the warning triangle is cleared, and that we now have snapshot(s) for our two Customer Service VMs.

Create a new Customer Service VM

[201]

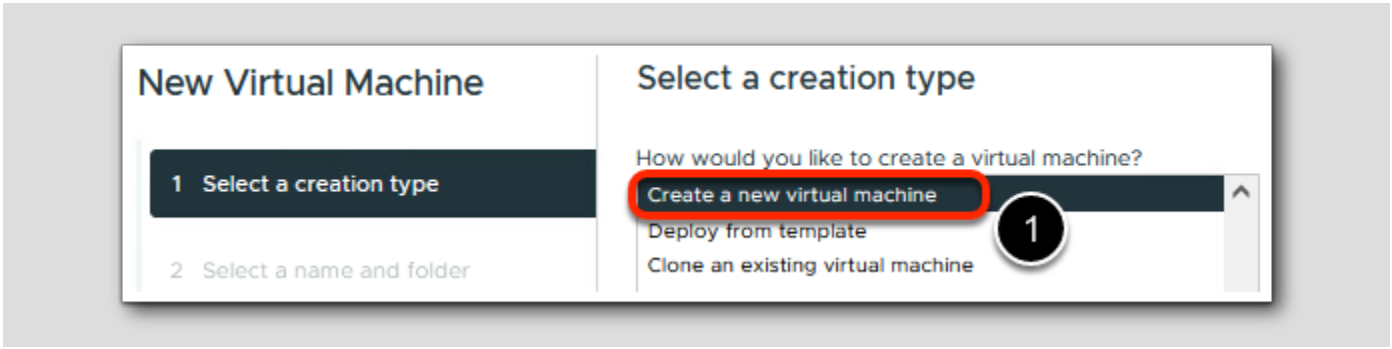
Since we created our Customer Service Apps protection group with a dynamic VM naming pattern setting, any new VMs added to vSAN datastores beginning with the prefix "cs" will automatically be included in the protection group.



2. Select our vSAN cluster **RegionA01-COMP01**
3. Select **Actions**
4. Select **New Virtual Machine**

New Virtual Machine - Select a creation type

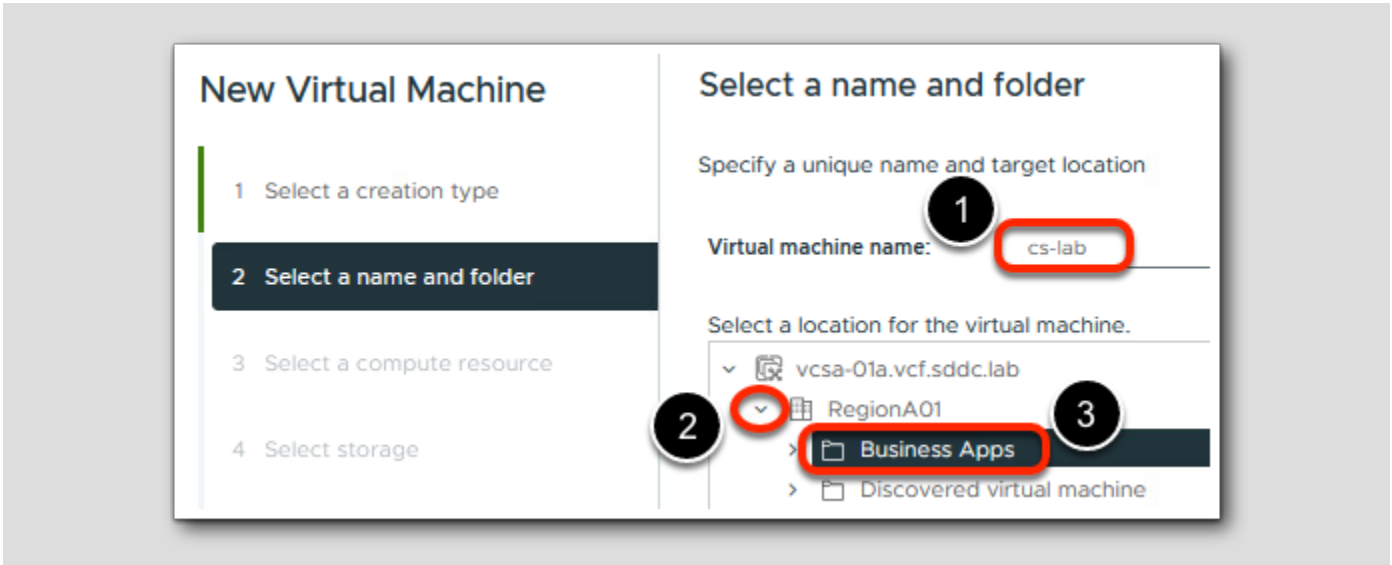
[202]



1. Choose the option to **Create a new virtual machine**
2. Click **Next** in lower right (not shown)

New Virtual Machine - Select a name and folder

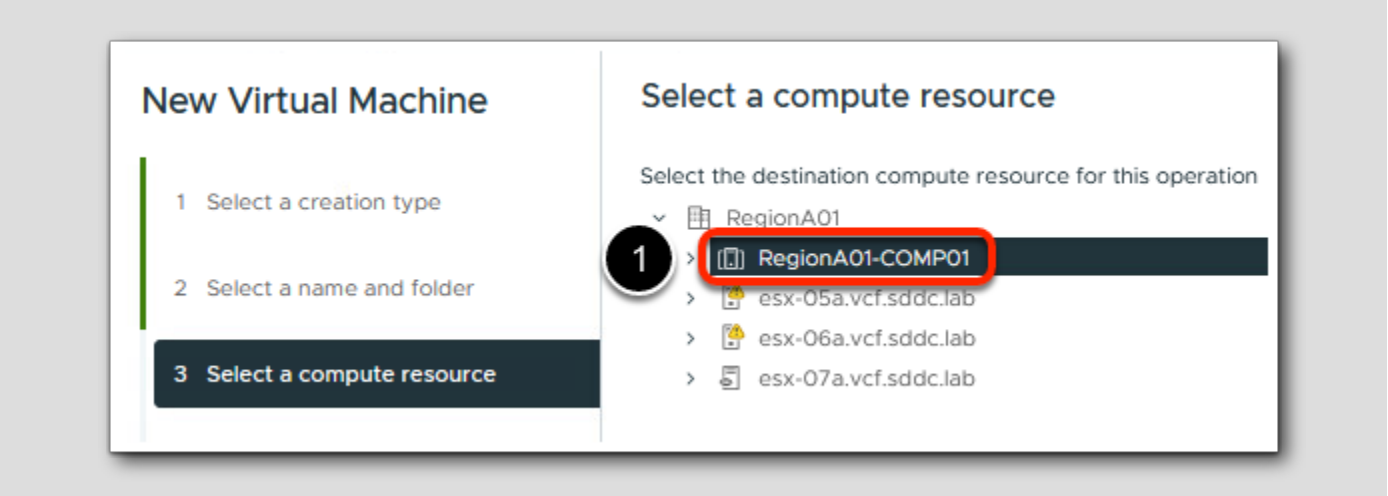
[203]



1. Type in the name **cs-lab** for our new VM;
2. **Expand** the list of RegionA01 folders;
3. Select the **Business Apps** folder;
4. Click **Next** in lower right (not shown).

New Virtual Machine - Select a compute resource

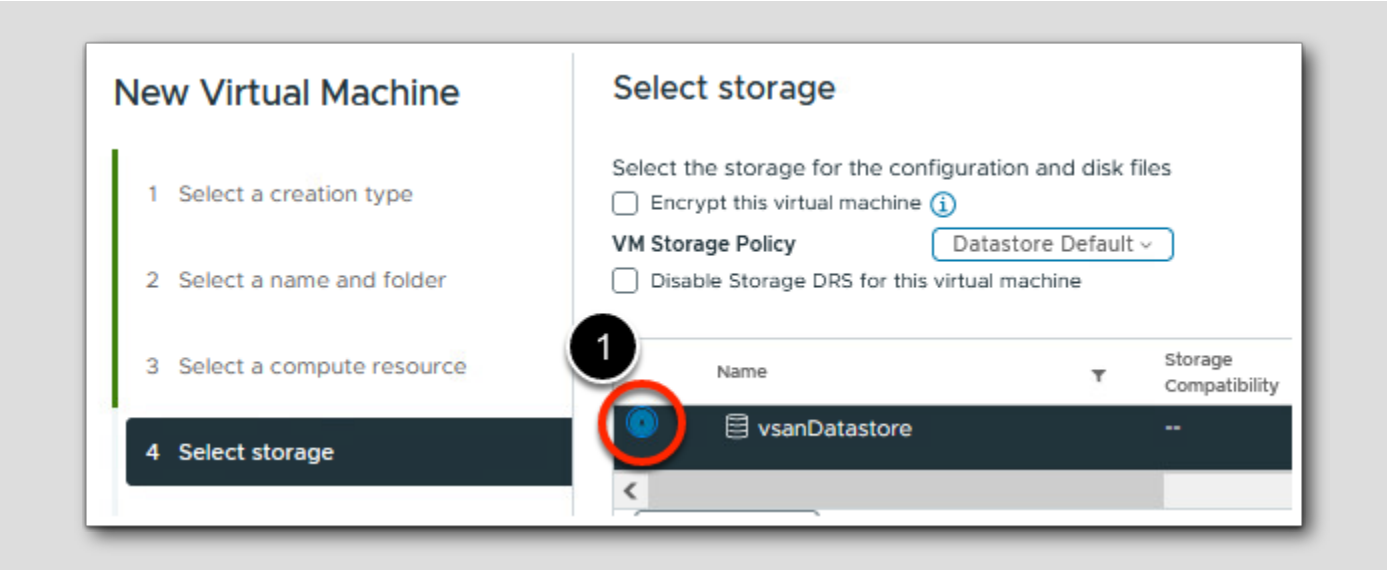
[204]



1. Select vSAN cluster **RegionA01-COMP01;**
2. Click **Next** in lower right (not shown).

New Virtual Machine - Select storage

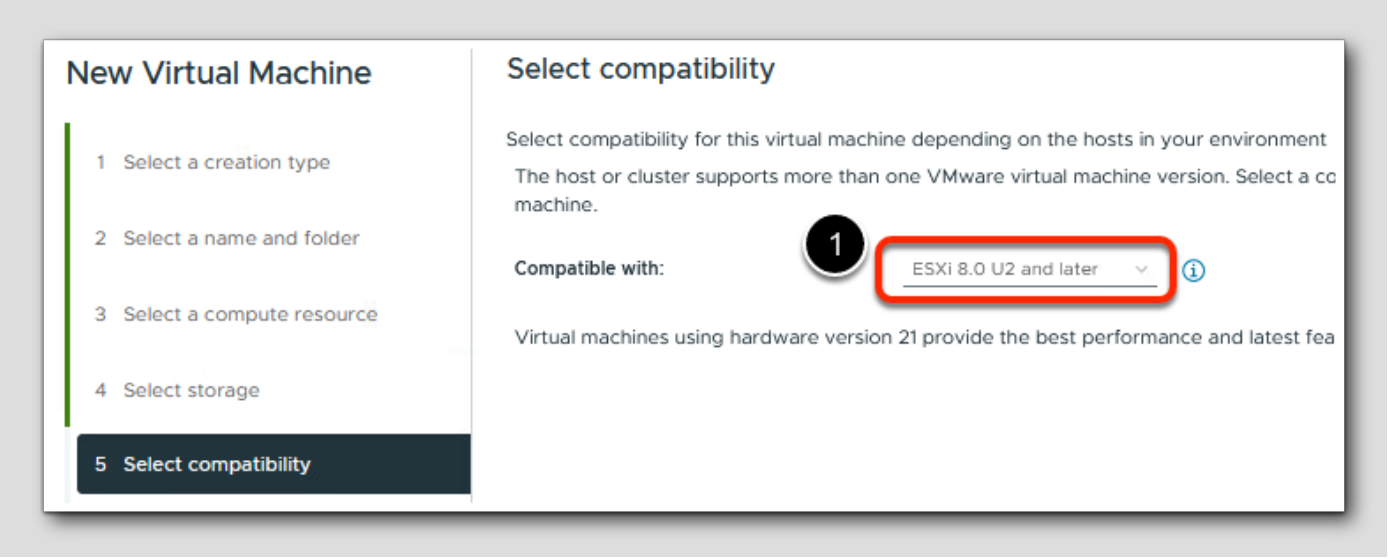
[205]



1. Select **vsanDatastore** to store the VM;
2. Click **Next** in lower right (not shown).

New Virtual Machine - Select compatibility

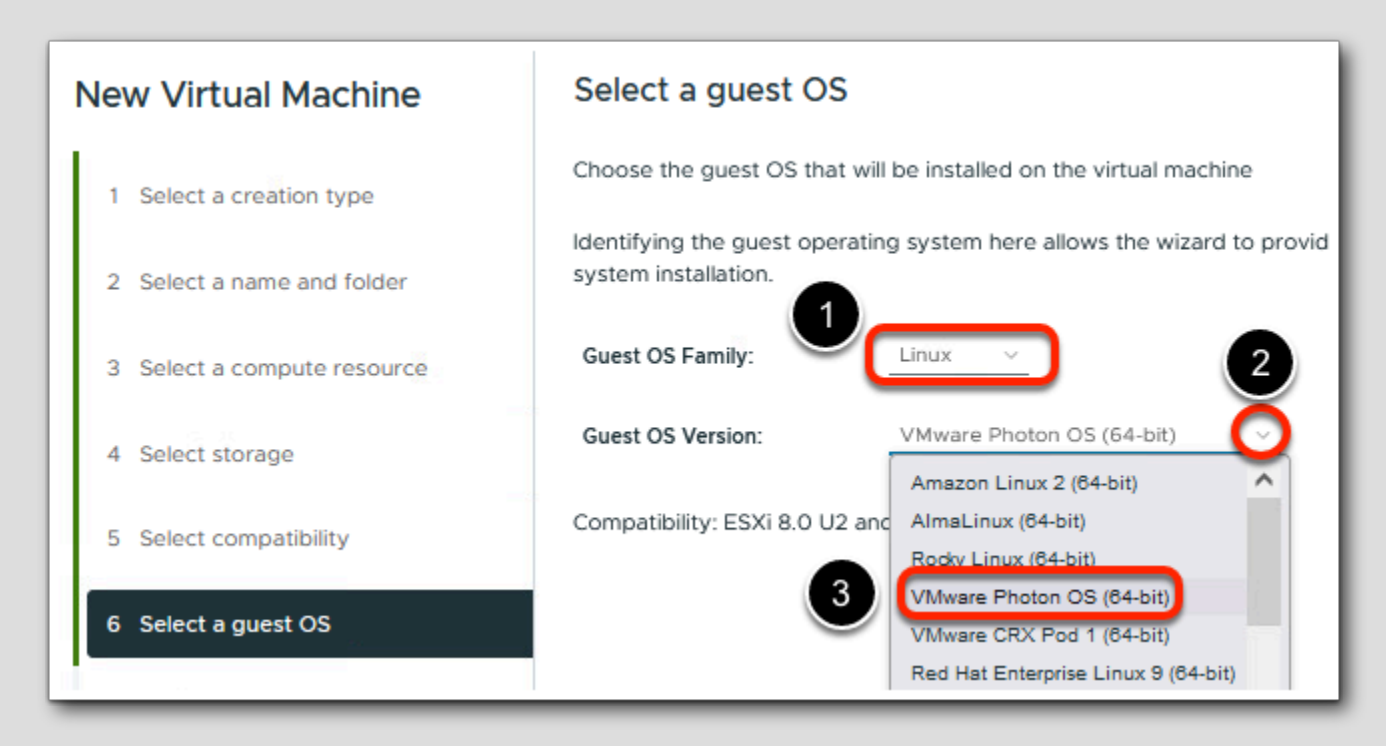
[206]



1. **Accept the default** compatibility of ESXi 8.0 U2 and later;
2. Click **Next** in lower right (not shown).

New Virtual Machine - Select a guest OS

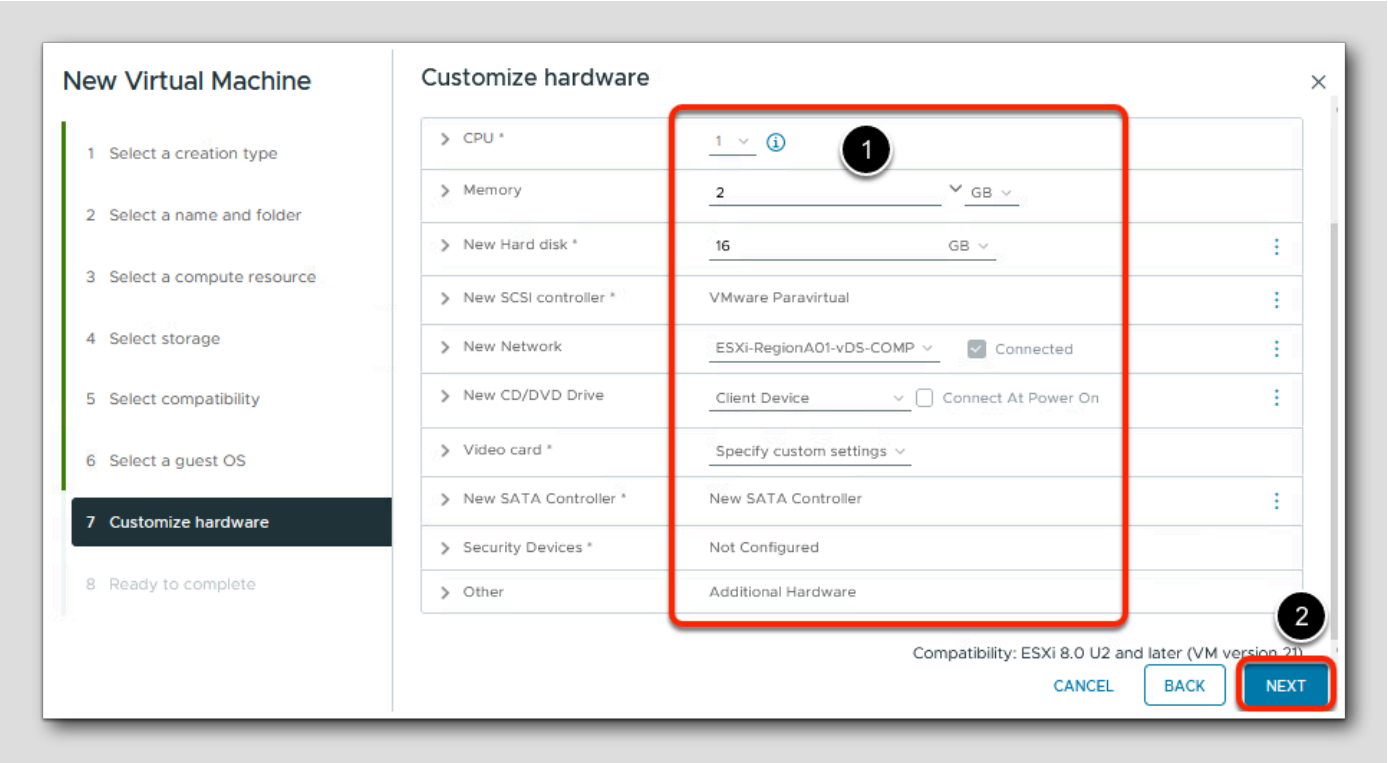
[207]



1. Select **Linux** for Guest OS Family;
2. Select the **drop down arrow** to expand the list of Linux versions;
3. Select **VMware Photon OS (64-bit)**;
4. Click **Next** in lower right (not shown).

New Virtual Machine - Customize hardware

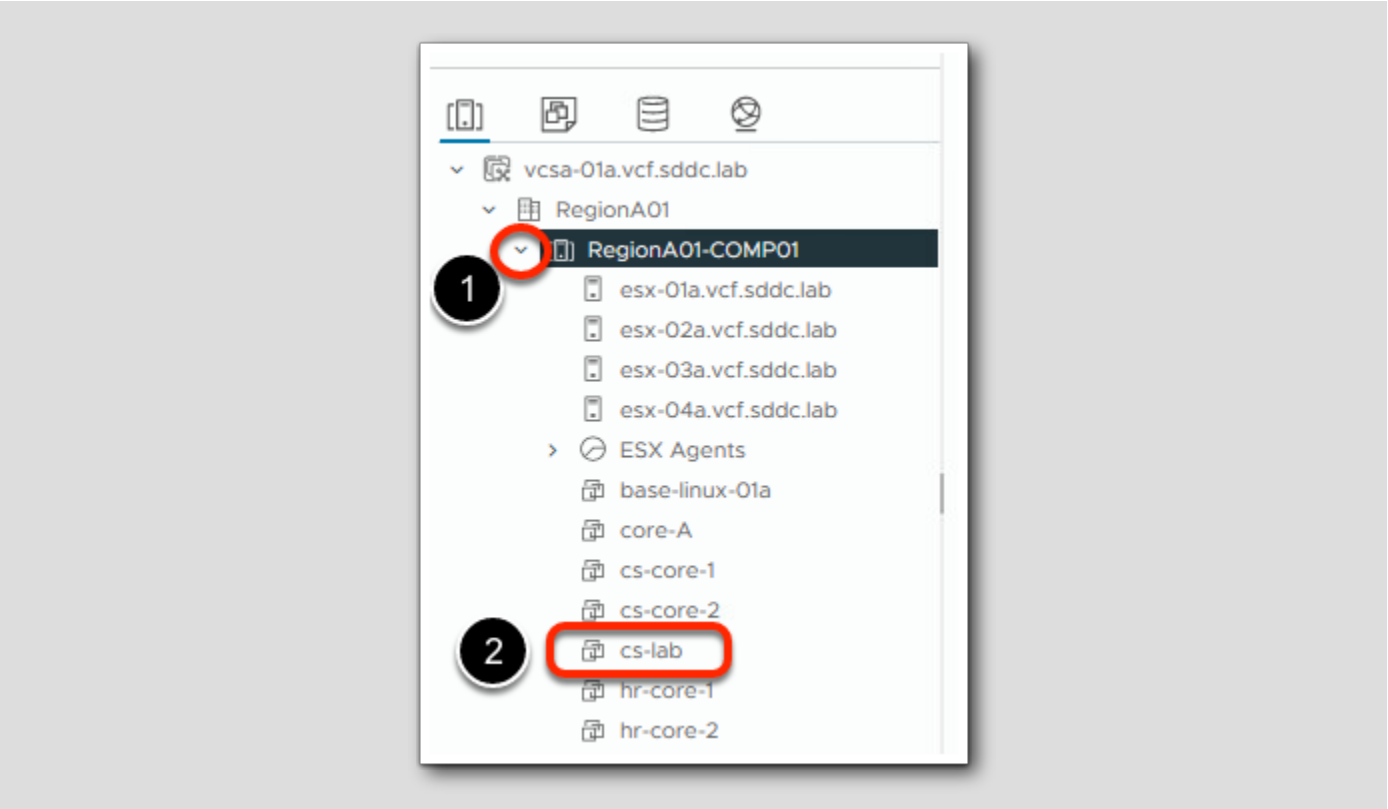
[208]



1. **Accept the defaults** for hardware - no changes needed;
2. Click **Next**.
3. Click Finish on the Ready to complete screen (not shown).

Check for newly created cs-lab VM

[209]

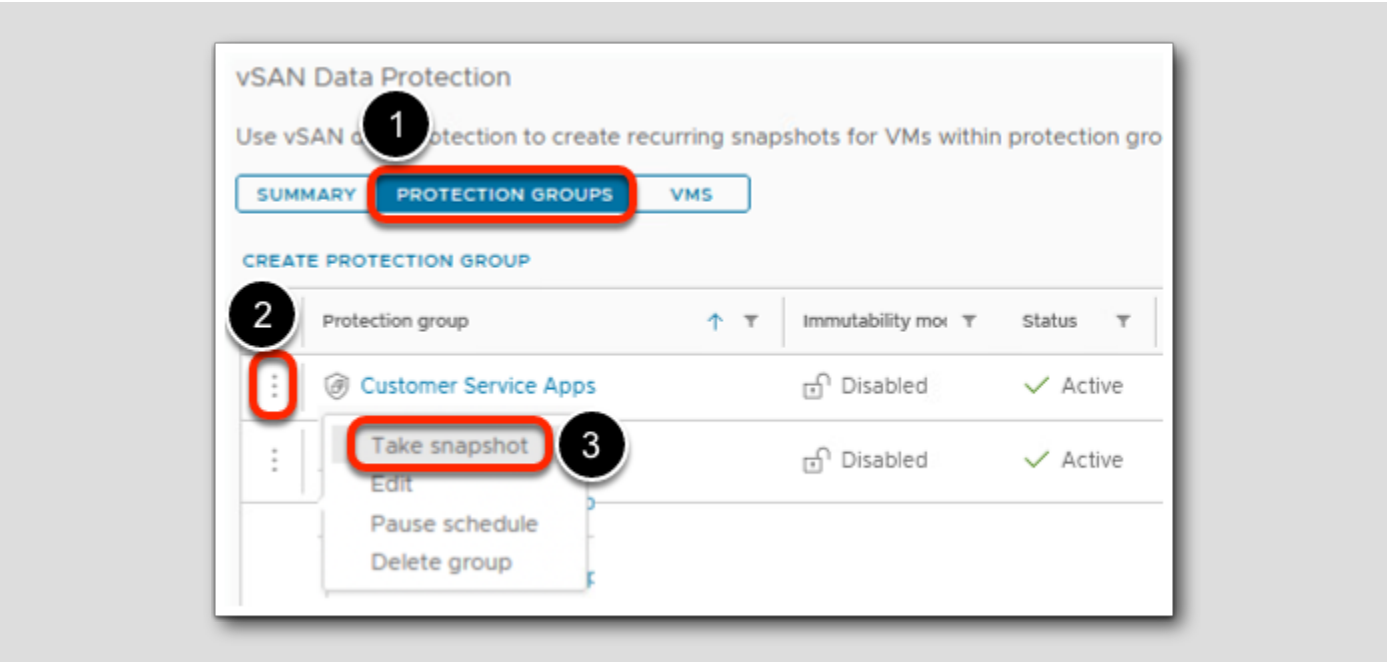


1. **Expand the list of VMs** running on the vSAN cluster RegionA01-COMP01 by clicking the **drop down arrow**;
2. Check that our new **cs-lab** VM has been created in the vSAN cluster and registered in vCenter inventory.

Take another protection group snapshot

[210]

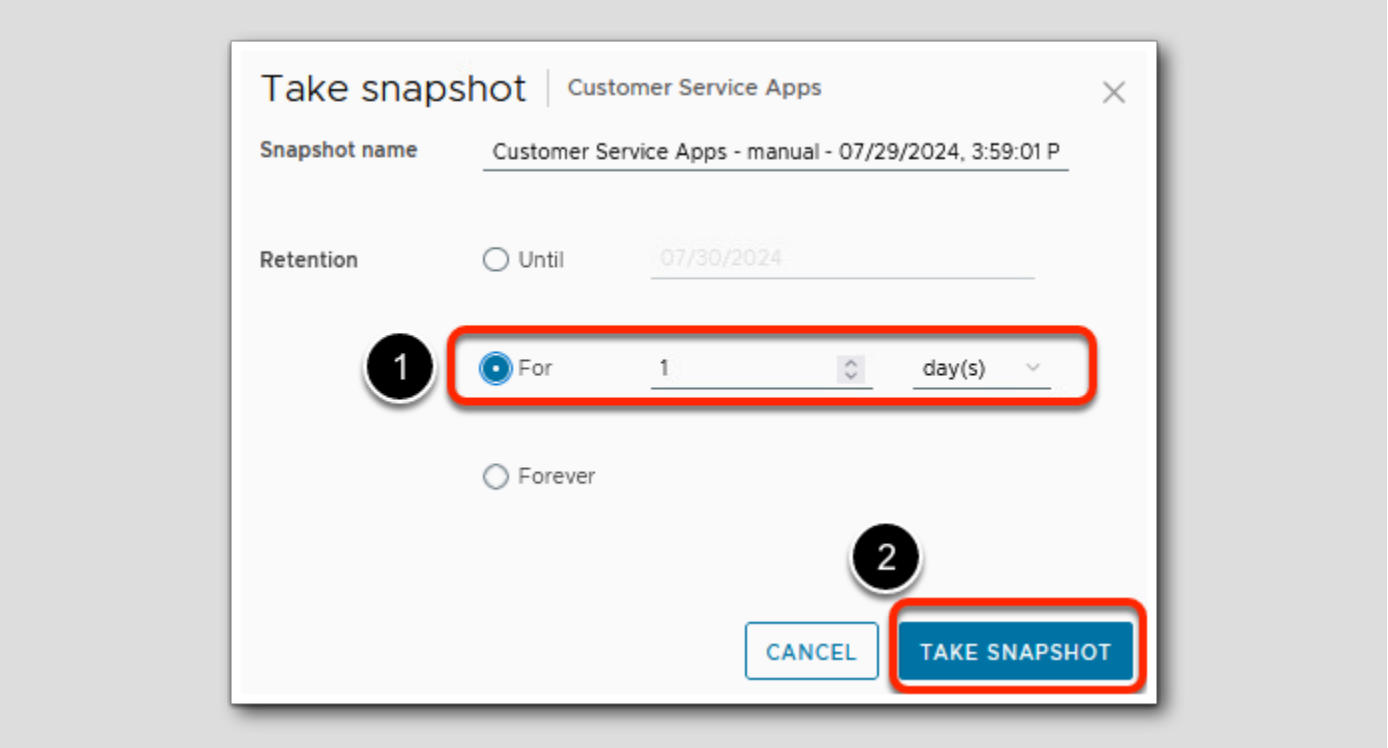
Our newly created VM has name that starts with "cs" so it will be included in the Customer Service Apps protection group automatically at the next scheduled snapshot interval. However we can take another manual snapshot to speed things up in our lab …



1. Select **Protection Groups**;
2. Select the **three vertical dots** to the left of Customer Service Apps;
3. Select **Take snapshot**.

Take snapshot - Customer Service Apps

[211]

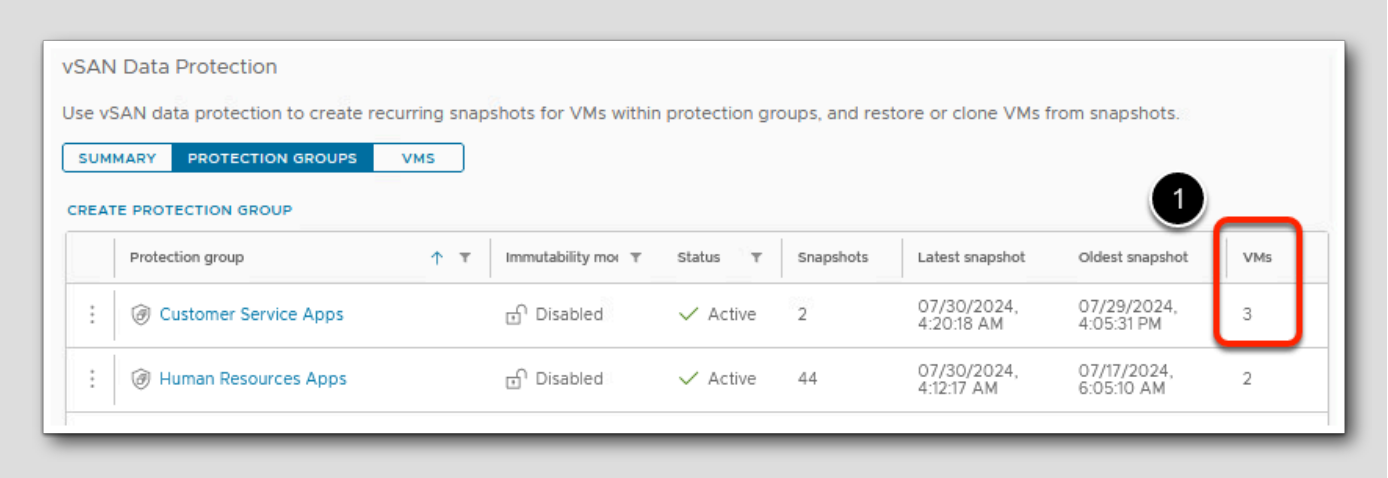


1. Specify a retention period of **For 1 day(s)**;
2. Select **Take Snapshot**.

Review Customer Service Apps protection group VM count

[212]

You can see snapshot activity in the Recent Task pane, and when it completes there will be updated status in the vSAN Data Protection screen …



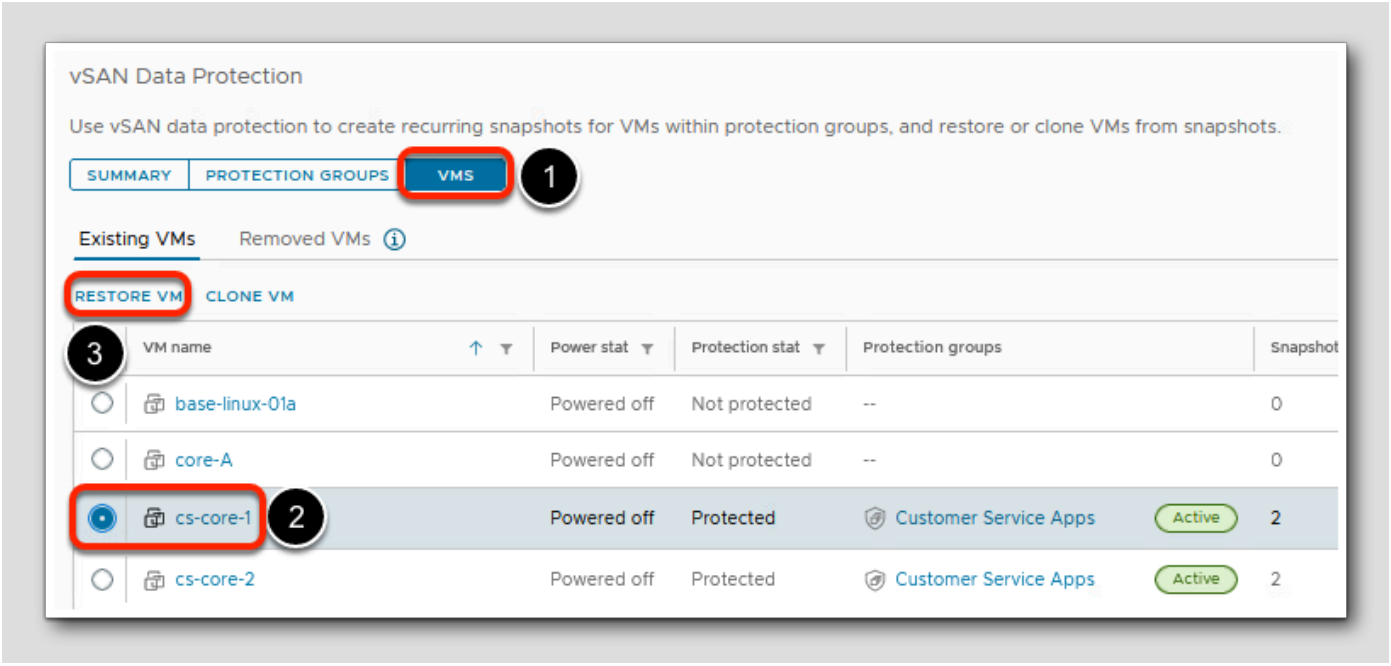
1. Notice that we now have THREE VMs protected; the original VMs cs-core-1 & cs-core-2 and your newly-created cs-lab VM. Recall that even though you added a new VM, no reconfiguration of the protection group was required since we used the dynamic naming option.

Recover VMs using vSAN Data Protection

[213]

vSAN Data Protection allows you to recover VMs that have available snapshots - whether they are existing VMs in the vCenter Inventory, or VMs that were protected at one point but are now missing from the vCenter - be it they were deleted or migrated somewhere else.

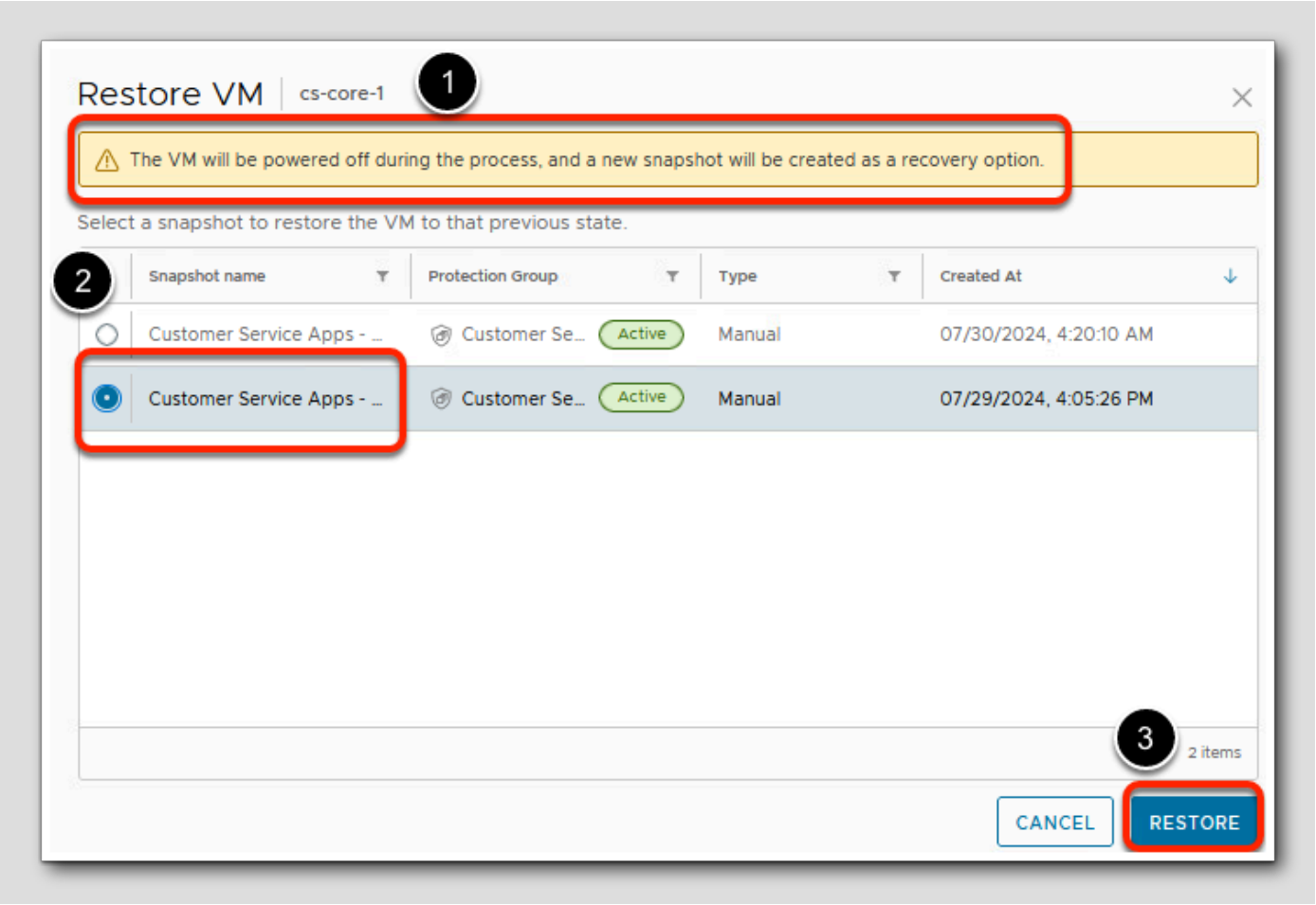
To prepare for the next exercise please check the that VM cs-core-1 is powered on, if it is powered-off, please power it on now and return to the vSAN Data Protection panel ...



1. Select **VMs** from the vSAN Data Protection panel;
2. Select the **cs-core-1** VM;
3. Select **Retore VM**.

Restore VM - cs-core-1

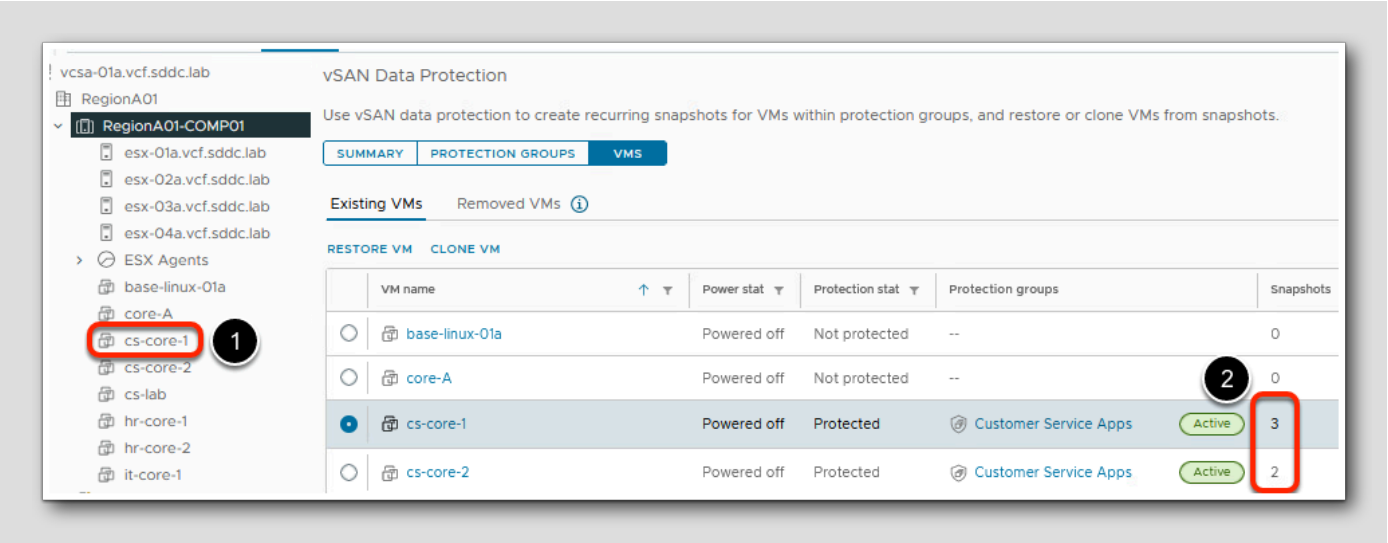
[214]



1. Notice that vSAN Data Protection warns us that the **VM will be powered-off**, and that a **new snapshot for the VM will be created** as new recovery option in case we later choose to roll forward (back to current state) after we restore the older image of the VM.
2. Select one of the **available snapshots**;
3. Select **Restore**.

Review Restored VM Status

[215]

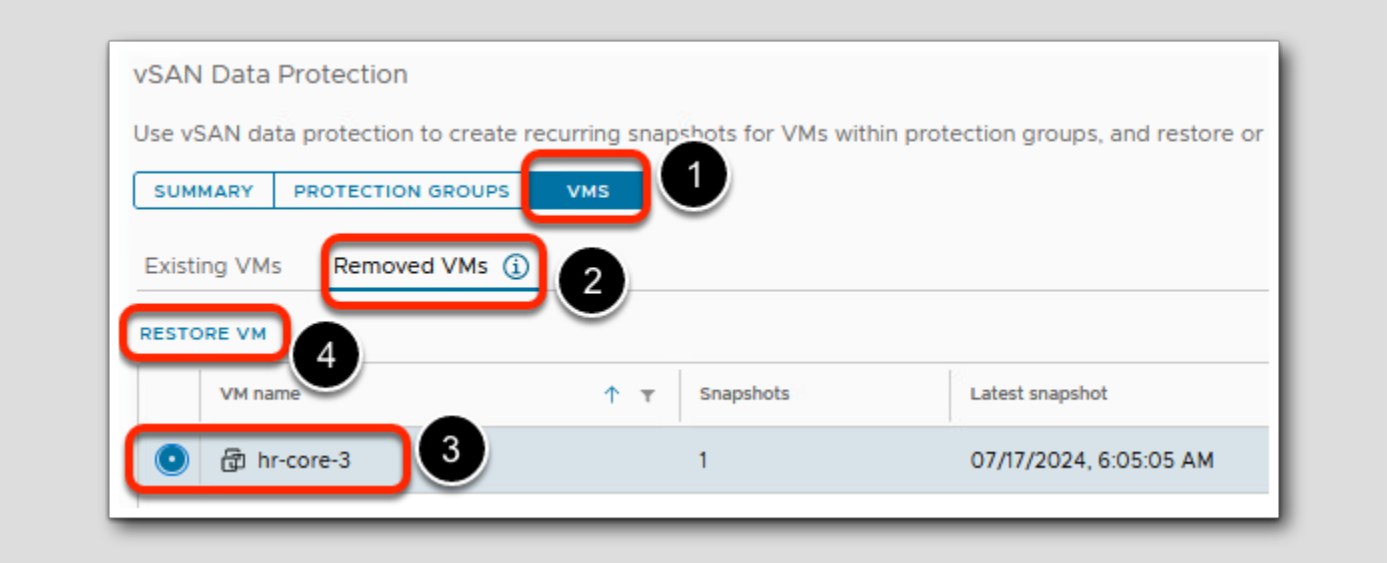


1. Notice that the VM cs-core-1 is now powered-off - just as we were warned;
2. Notice that there is now an additional snapshot for the cs-core-1 VM compared to the cs-core-2 VM - that's the additional snapshot created as part of the restore operation.

Recover a VM - Removed VMs

[216]

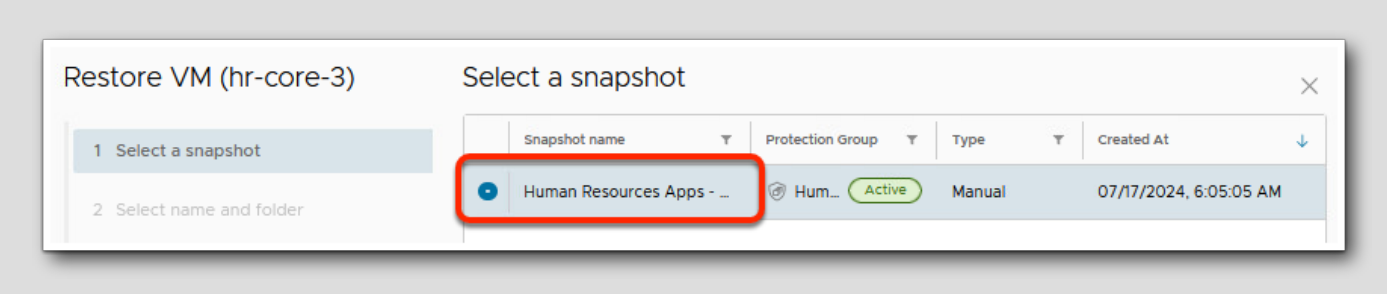
vSAN Data Protection also facilitates recovering VMs that were removed from the vCenter Inventory - as long as there remains a snapshot available for that VM. Remember that snapshots created for the protection groups have retention periods or dates - if the snapshot has "aged out" the VM will not be recoverable.



1. Select **VMs** in the vSAN Data Protection panel;
2. Select **Removed VMs**;
3. Select the VM **hr-core-3**;
4. Select **Restore VM**.

Restore VM (hr-core-3) - Select a Snapshot

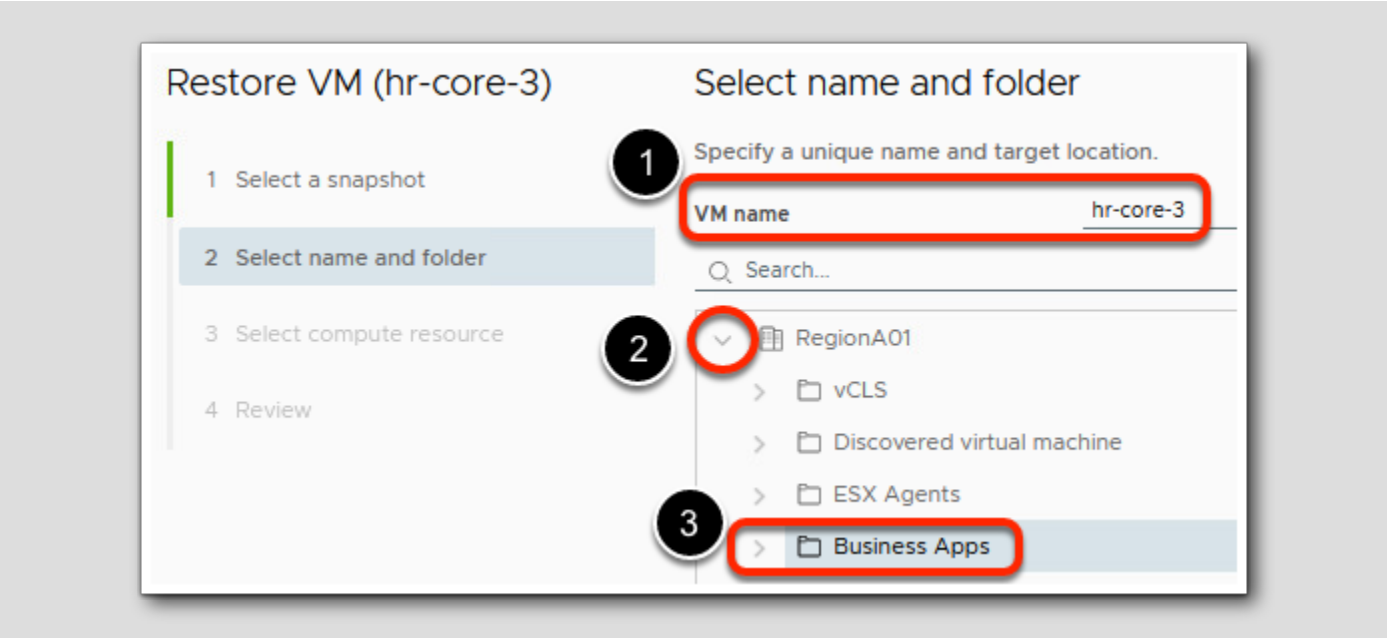
[217]



1. Select an available snapshot;
2. Click **Next** in lower right (not shown).

Restore VM (hr-core-3) - Select name and folder

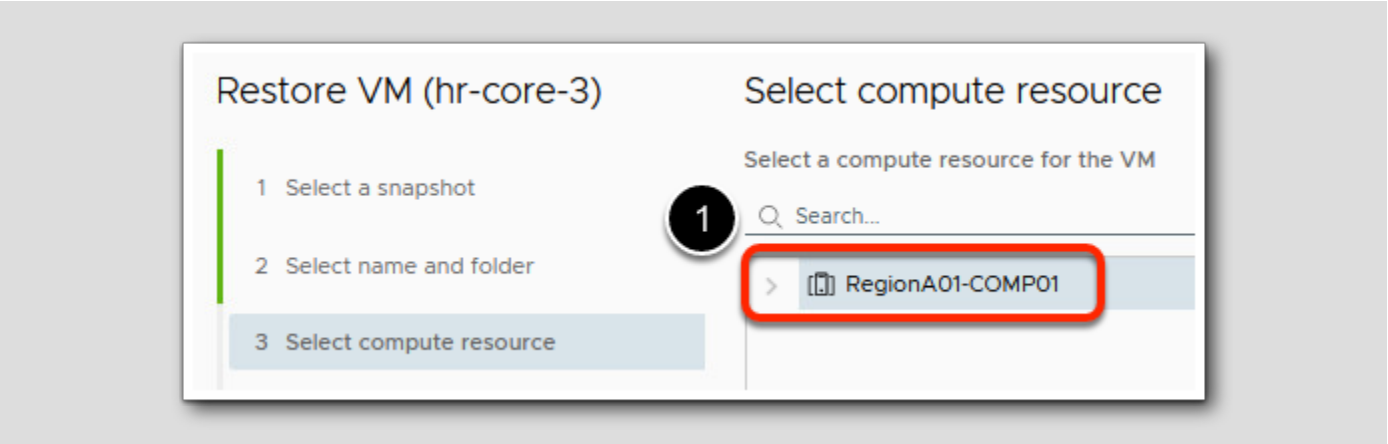
[218]



1. Accept the default - restore the VM using its original name hr-core-3;
2. **Expand** the list of RegionA01 folders;
3. Select the **Business Apps** folder;
4. Click **Next** in lower right (not shown).

Restore VM (hr-core-3) - Select compute resource

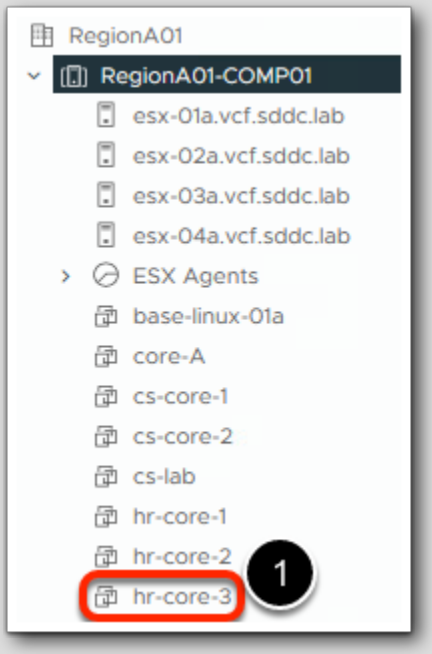
[219]



1. Accept the default - our vSAN cluster RegionA01-COMP01;
2. Click **Next** in lower right (not shown);
3. Click Restore on the next screen (not shown).

Review Recovered VM hr-core-3

[220]

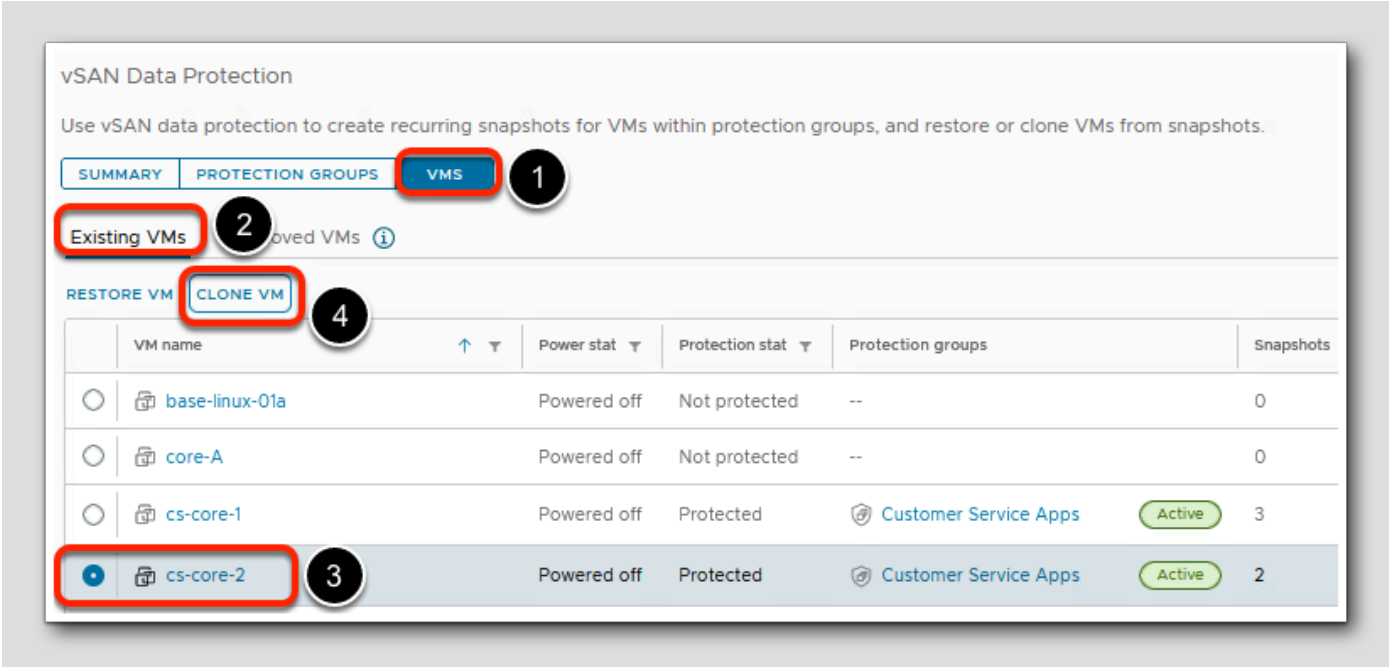


1. Note that vSAN Data Protection has recovered the previously-deleted VM hr-core-3 and placed it vCenter's inventory - ready to power-on and run. *Also note that since the VM retains its name starting with "hr" that it will be protected using the already-configured Human Resources Apps protection group for as long as it remains in the vSAN cluster.*

Clone a VM

[221]

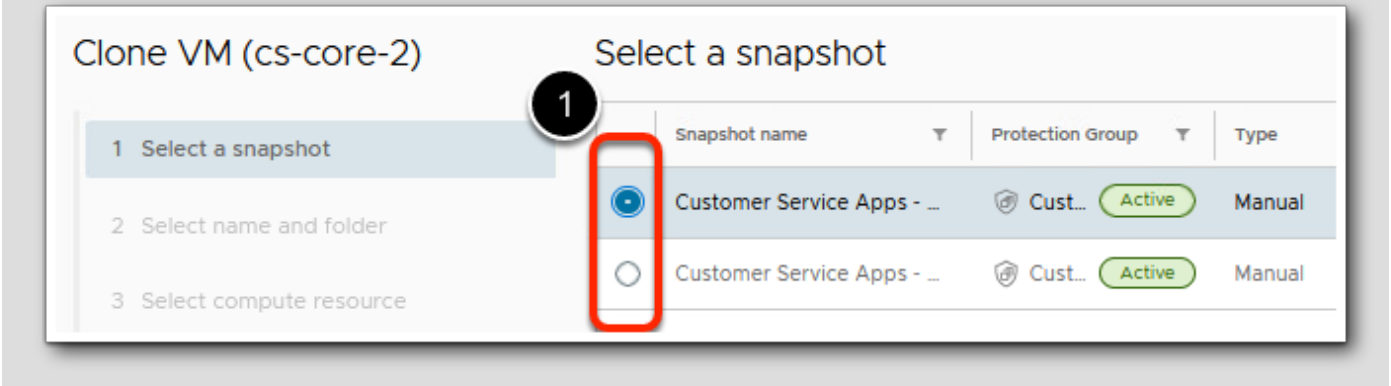
vSAN Data Protection provides the capability to quickly clone a VM from any existing VM assigned to a protection group. These clones are based on ESA snapshots and use a linked-clone architecture which offers quick creation and high performance, but they are best viewed as transient copies of the VM to be used for research or selected recovery of data located within the VM. The cloned-VMs produced by vSAN Data Protection are different from VMs created with vCenter's traditional "cloning" operations - and these clones are NOT candidates for protection by vSAN Data Protection.



1. Select **VMs** from the vSAN Data Protection panel;
2. Select **Existing VMs**;
3. Select the VM **cs-core-2**;
4. Select **Clone VM**.

Clone VM (cs-core-2) - Select a snapshot

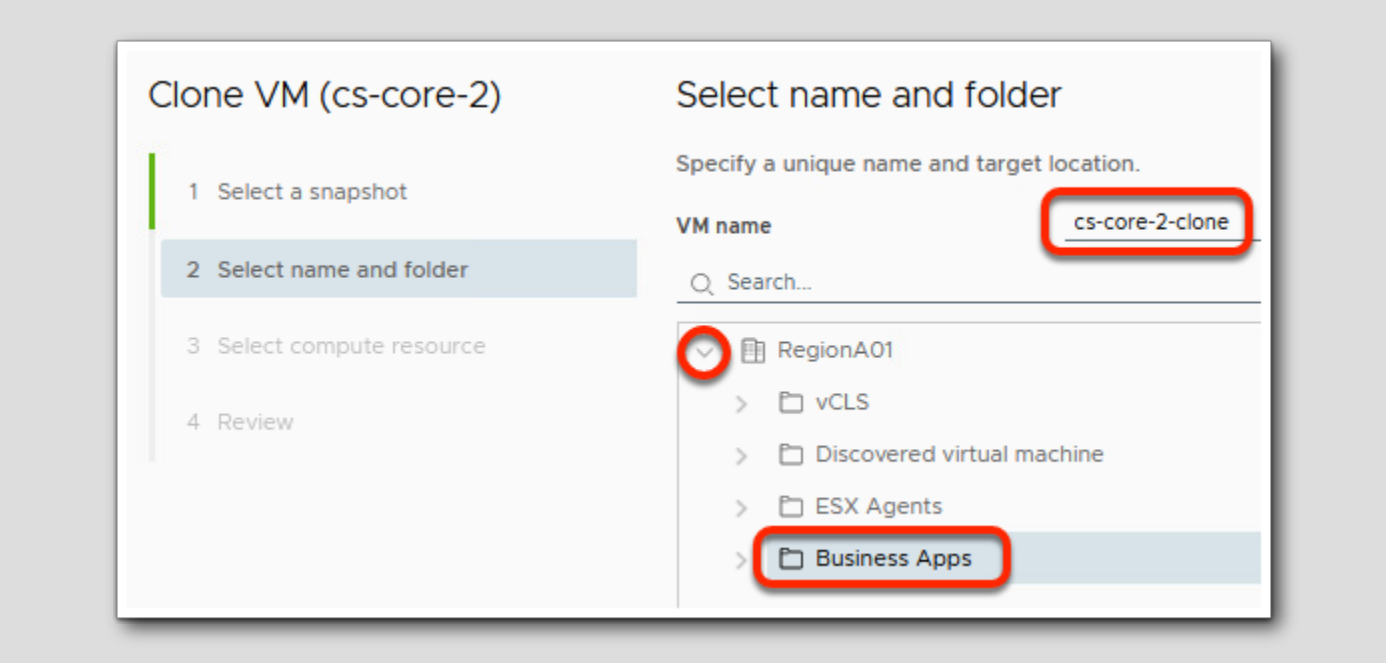
[222]



1. Select one of the available snapshots;
2. Click **Next** in lower right (not shown).

Clone VM (cs-core-2) - Select name and folder

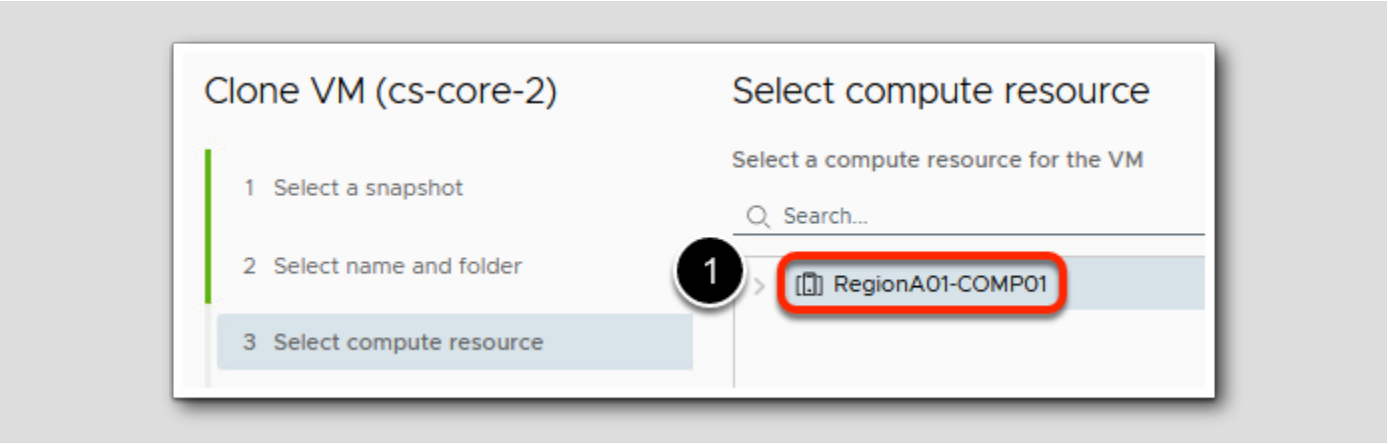
[223]



1. Accept the default - clone the VM using the name cs-core-2-clone;
2. **Expand** the list of RegionA01 folders;
3. Select the **Business Apps** folder;
4. Click **Next** in lower right (not shown).

Clone VM (cs-core-2) - Select compute resource

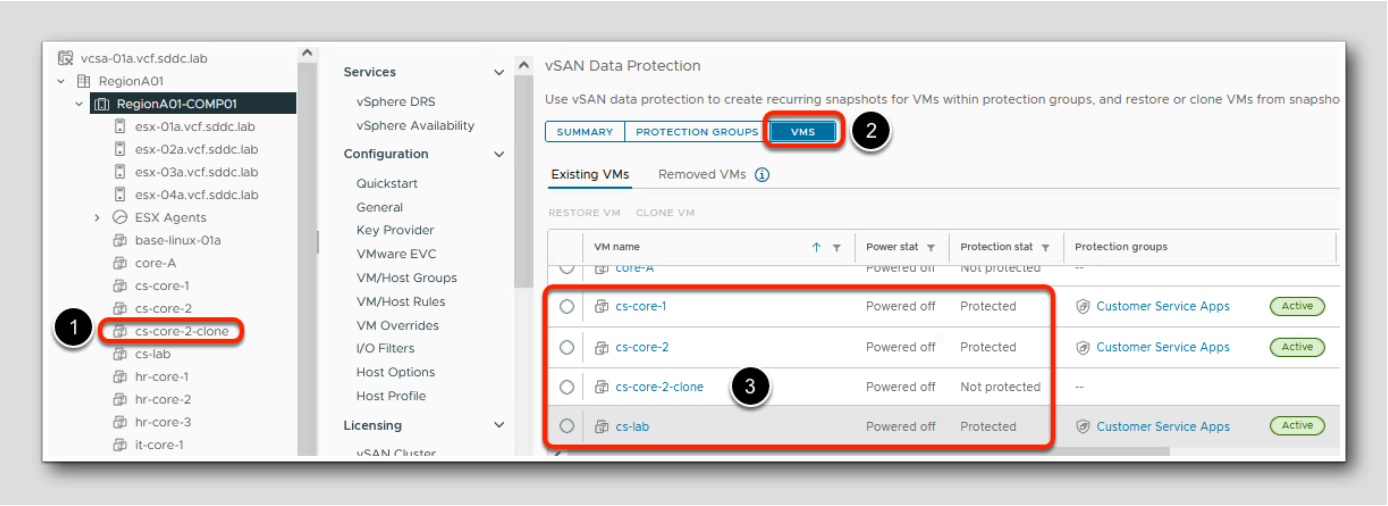
[224]



1. Accept the default location - our vSAN cluster Region-A01-COMP01
2. Click **Next** in lower right (not shown);
3. Click Clone on the next screen (not shown).

Review VM Cloning Results

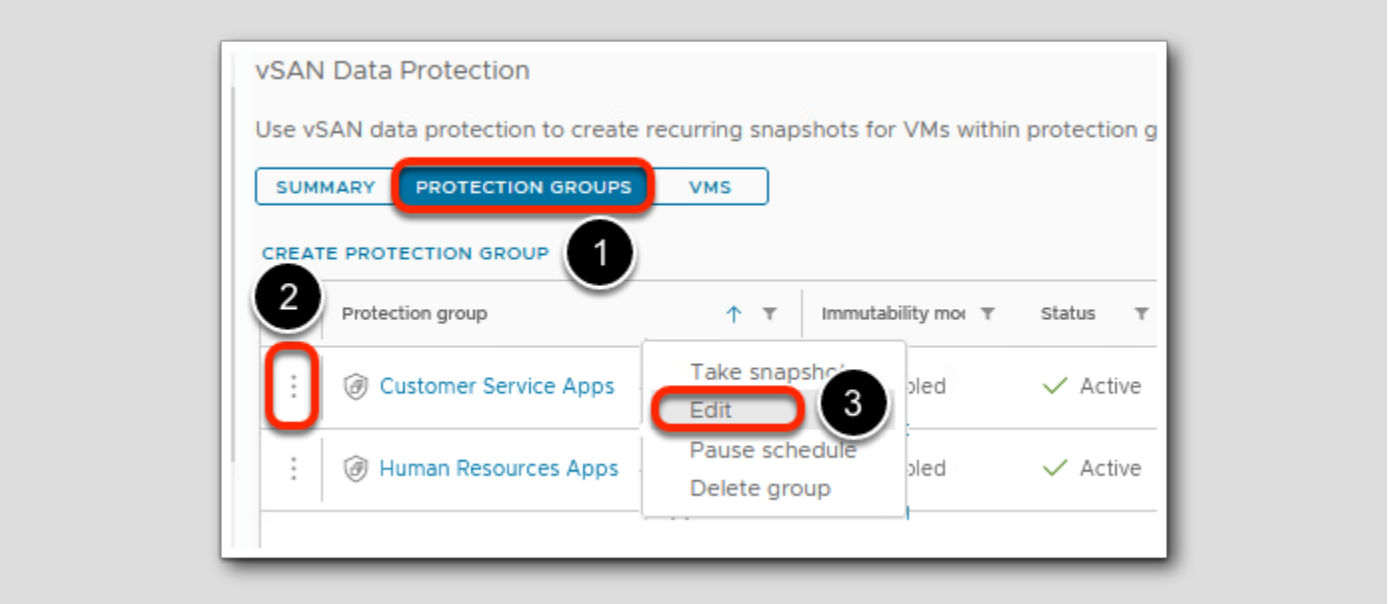
[225]



1. Notice that our cloned VM **cs-core-2-clone** now appears in the vCenter Inventory;
2. Select **VMs** in the vSAN Data Protection Panel;
3. Notice that **cs-core-2-clone** VM now appears with the status of *Not protected*.

Observe how cloned VMs are treated by vSAN Data Protection

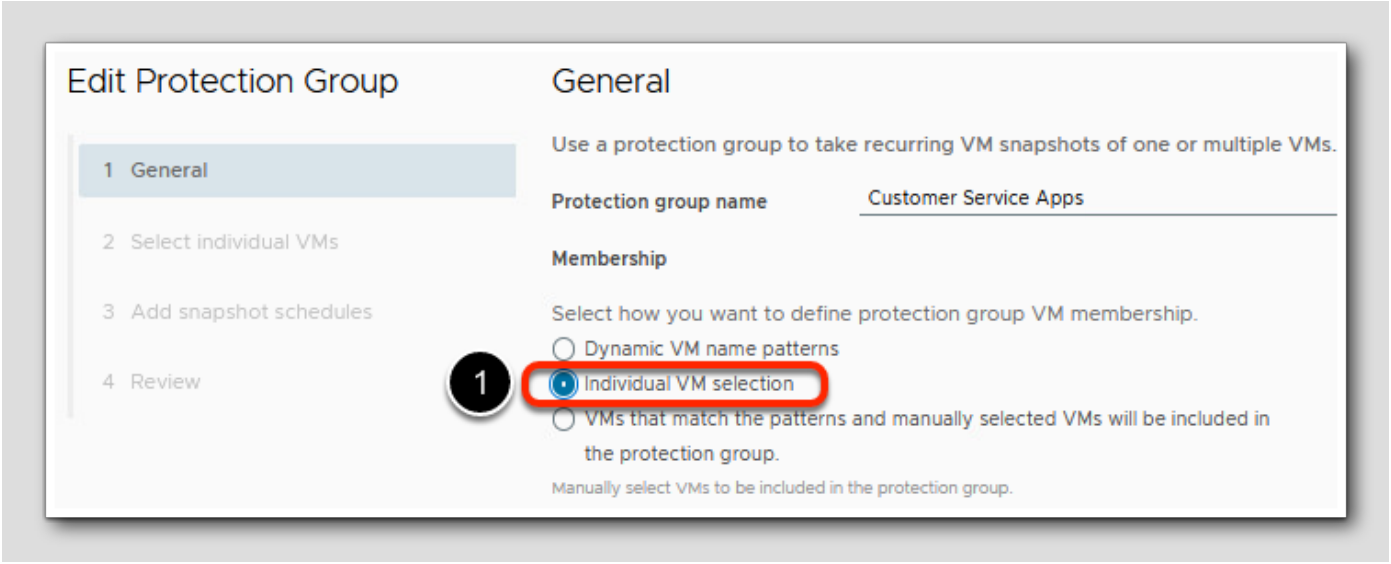
[226]



1. Select **Protection Groups** from the vSAN Data Protection panel;
2. Select the **three vertical dots** next to the **Customer Service Apps** protection group to call up the pop-up menu;
3. Select **Edit**.

Edit Protection Group - General

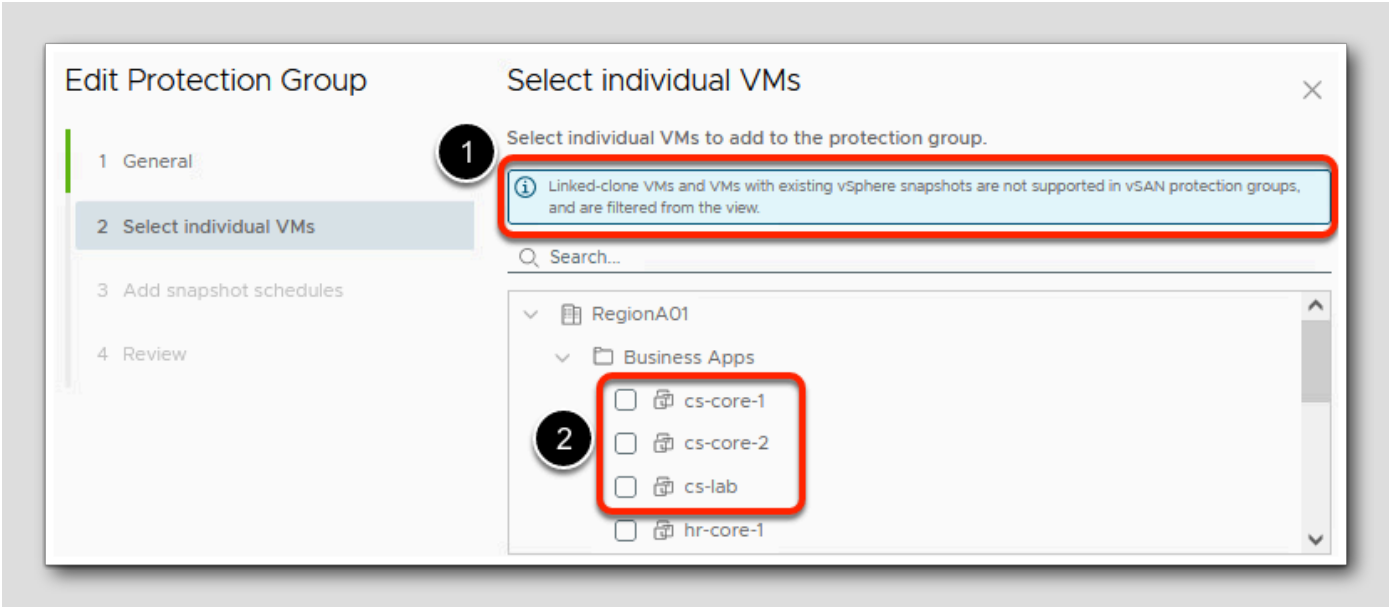
[227]



1. Select **Individual VM selection**;
2. Click **Next** in lower right (not shown).

Edit Protection Group - Select individual VMs

[228]

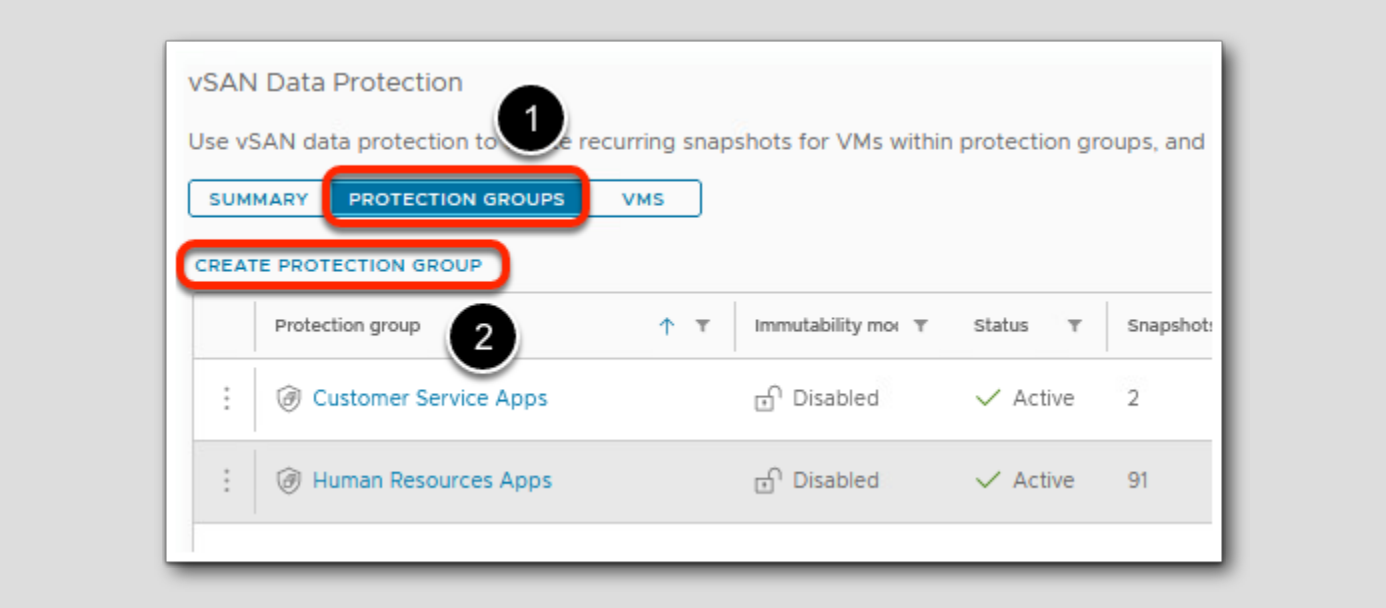


1. Notice that vSAN Data Protection advises users that **Linked-clone VMs are not supported** in vSAN protection groups; and
2. Notice that our **cs-core-2-clone VM has been filtered out** of the list of candidate VMs for inclusion in the protection group;
3. Click **Cancel** to stop editing the protection group (not shown).

Immutable Protection Groups

[229]

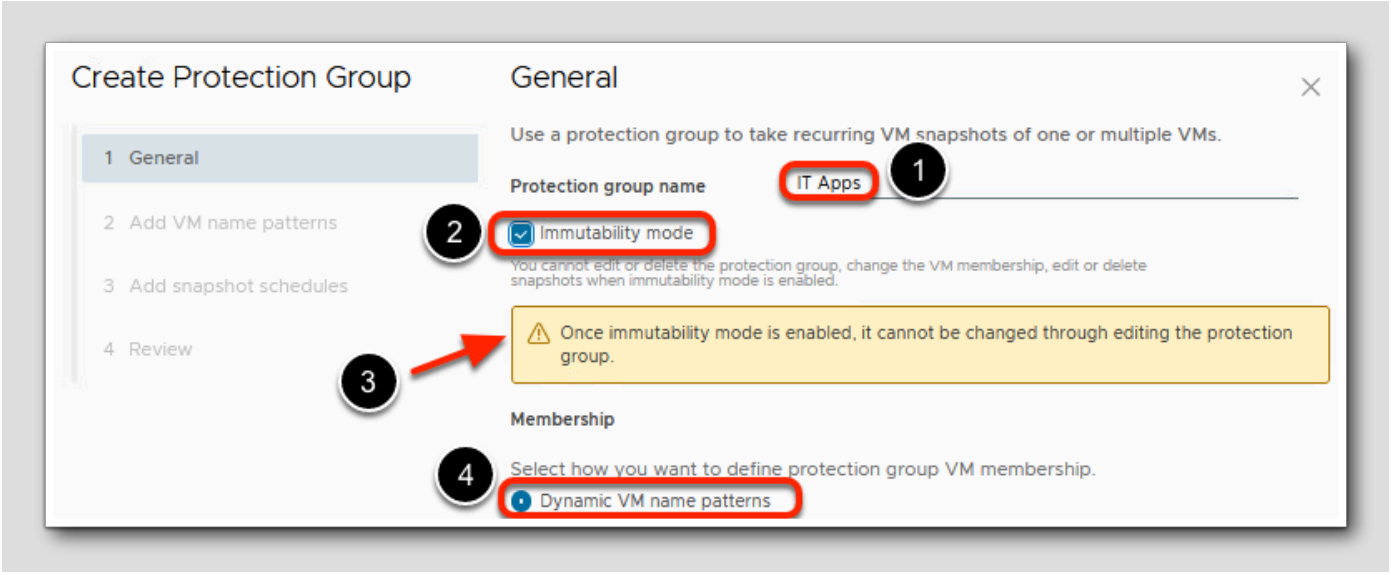
vSAN Data Protection offers the option to create *Immutable* protection groups. Immutable protection groups - once created - are not changeable or cancelable. The criteria for protected VMs - whether using dynamic naming inclusion, individual VM specifications or both - is fixed once the group is created. The same holds for the snapshot schedule(s) and retention period(s) - they can not be altered after initial configuration. And finally, the protection group can not be deleted. Immutable protection groups are designed to prevent "bad actors" from tampering with or deleting the protection plans.



1. Select **Protection Groups** from the vSAN Data Protection panel;
2. Select **Create Protection Group**.

Create Protection Group - Immutability mode General

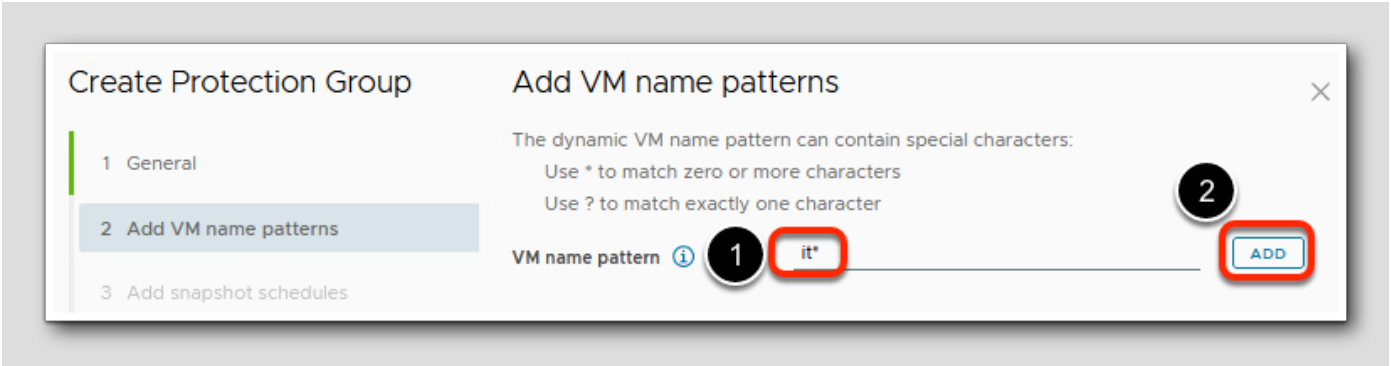
[230]



1. Type in the name **IT Apps** for our new Immutable protection group;
2. Check the box to enable **Immutability mode**;
3. Note the warning that this group will not be editable once created;
4. Select the option for **Dynamic VM name patterns**;
5. Click **Next** in lower right (not shown).

Create Protection Group - Immutability mode Add VMs

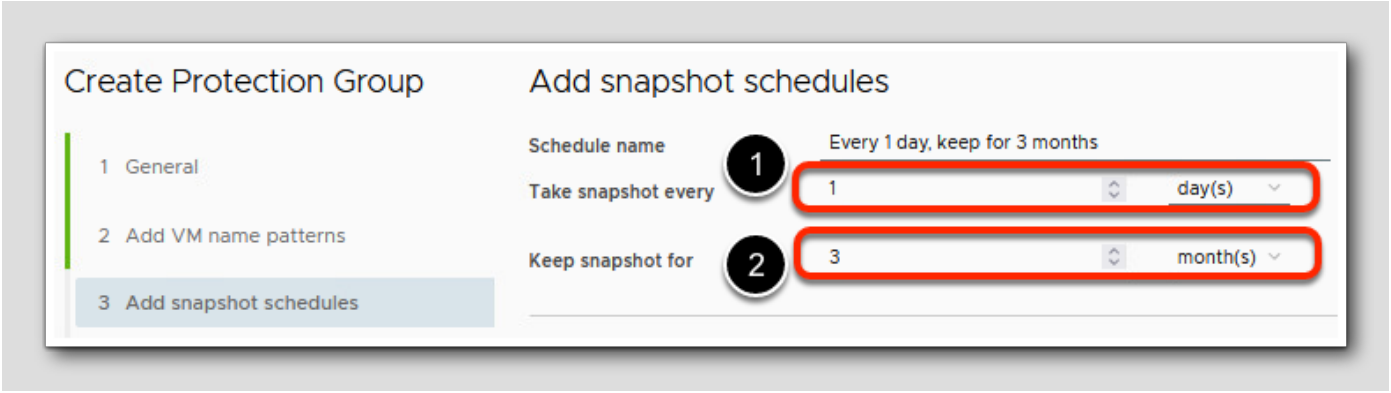
[231]



1. Our IT application VMs start with the prefix "it" - type in **it*** for our VM name pattern;
2. Select **Add** include that VMs starting with it;
3. Not that one existing VM matches this pattern - **it-core-1** (not shown);
4. Click **Next** in lower right (not shown).

Create Protection Group - Immutability mode Add schedule

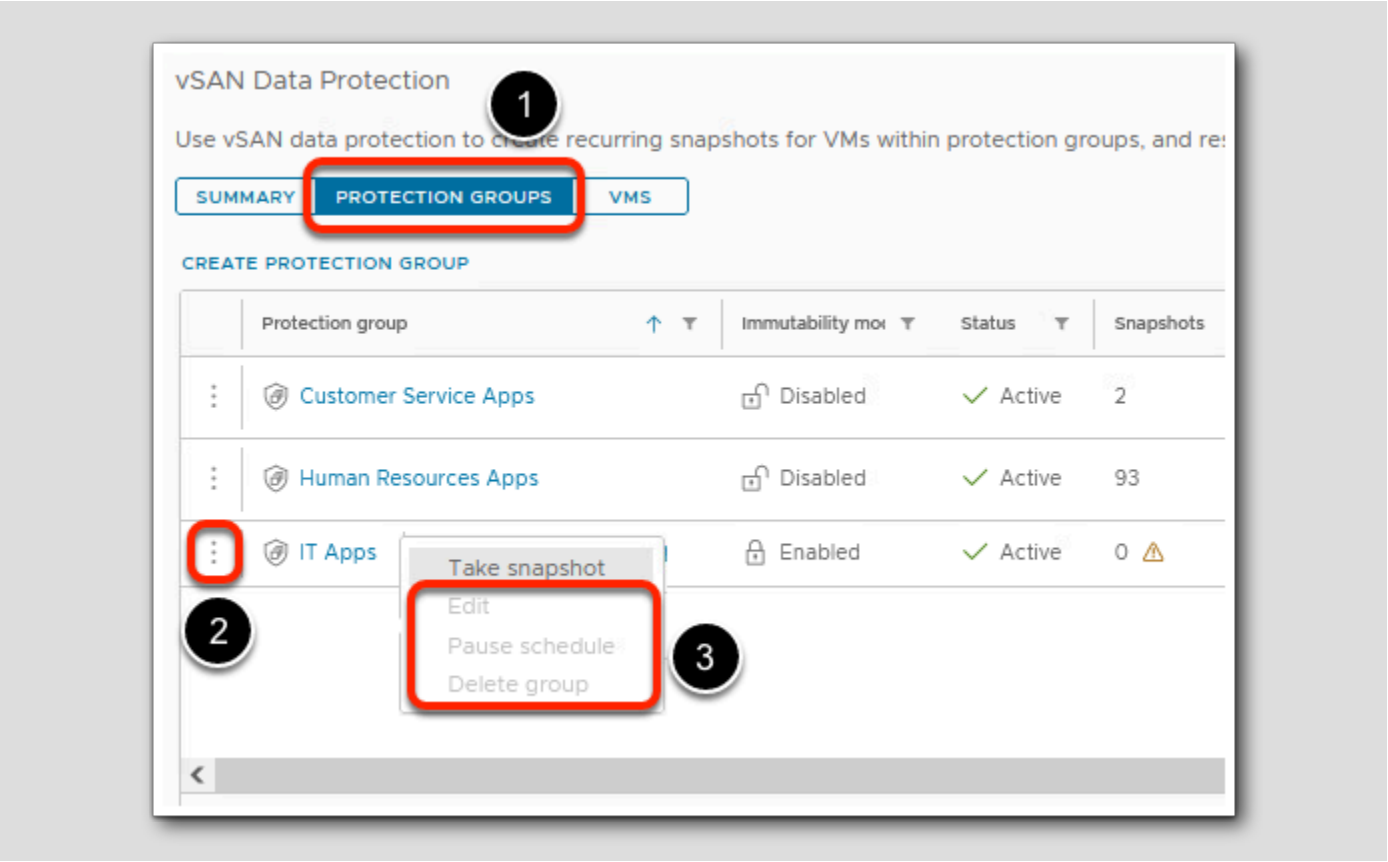
[232]



1. Configure the snapshot schedule (**Take snapshots every** ...) to every **1 day(s)**.
2. Configure the snapshot retention (**Keep snapshot for** ...) to be **3 month(s)**.
3. Click **Next** in lower right (not shown).
4. Click **Create** on the next screen (not shown).

Review Immutable Protection Group IT Apps

[233]



1. Select Protection Groups in the vSAN Data Protection panel;
2. Select the **three vertical dots** next to the **IT Apps** protection group to call up the pop-up menu;
3. Note that the options to **Edit, Pause or Delete** the IT Apps protection group has been **greyed-out (disabled)** - these capabilities are not allowed for Immutable protection groups.

Since we used a dynamic naming convention (VM names starting with "it") new IT VMs added to vSAN datastores will be automatically protected, and their snapshots will be retained for 3 months - even if the VMs are subsequently deleted.

Conclusion

[234]

This concludes our activities related to vSAN Data Protection - you can now proceed to the next module or end your lab.

Conclusion [235]

In this module, you were provided an overview of vSAN Data Protection and how to utilize these features to protect VM's running on the vSAN Datastore

You Finished Module 5 [236]

Congratulations on completing Module 5.

You can find more information on vSAN Data Protection in the following links:

https://core.vmware.com/resource/data-protection-vmware-vsan

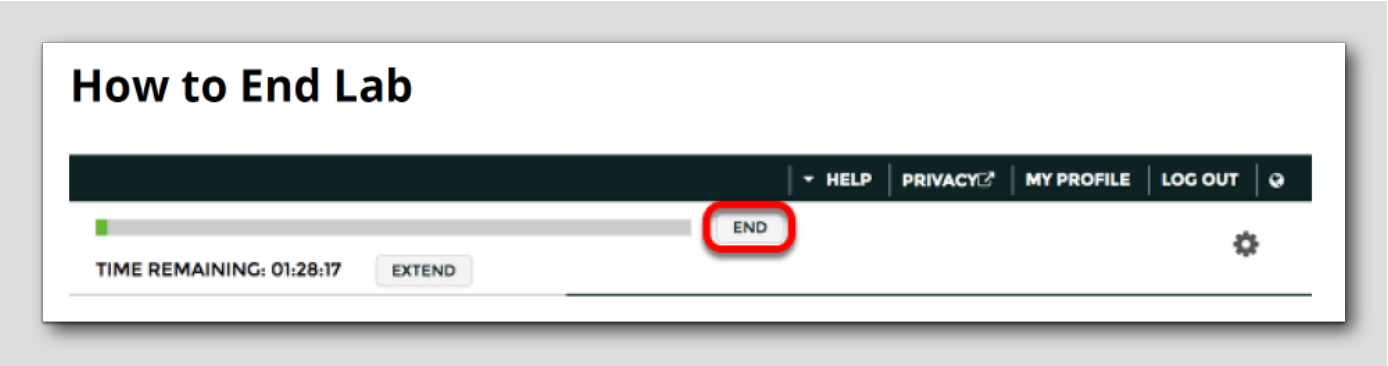
https://core.vmware.com/vmware?share=video3643&title=native-scalable-snapshots-in-the-vsan-express-storage-architecture

If you would like to continue with additional modules, please follow one of the links below:

- Module 1 - vSAN SPBM and Availability (30 minutes) (Basic) Introduction to VMware vSAN's Express Storage Architecture. We will cover the power of Storage Based Policy Management (SPBM) and show you the availability of vSAN.
- Module 2 - Monitoring, Health, Capacity, and Performance (30 minutes) (Basic) Show you how to enable Aria Operations within vCenter Server. We will cover the vSAN Health Check and how you can monitor your vSAN environment.
- Module 3 - vSAN Encryption and Security (30 minutes) (Advanced) Introduction to vSAN Encryption. We will enable a Key Management Server and demonstrate how to configure vSAN Encryption.
- Module 4 - File services (30 minutes) (Basic) Introduction to vSAN's File Services capabilities. We will create both NFS and SMB file shares and mount them to their respective clients.
- Module 6 - vSAN Stretched Cluster (30 minutes) (Advanced) Introduction to vSAN Stretched Clusters. We will convert an existing vSAN cluster into a stretched cluster. In addition, we will explore storage policies as well as Skyline Health checks with respect to stretched clusters.

How to End Lab

[237]



To end your lab, click on the **END** button.

Module 6 - vSAN Stretched Cluster (30 minutes) Advanced

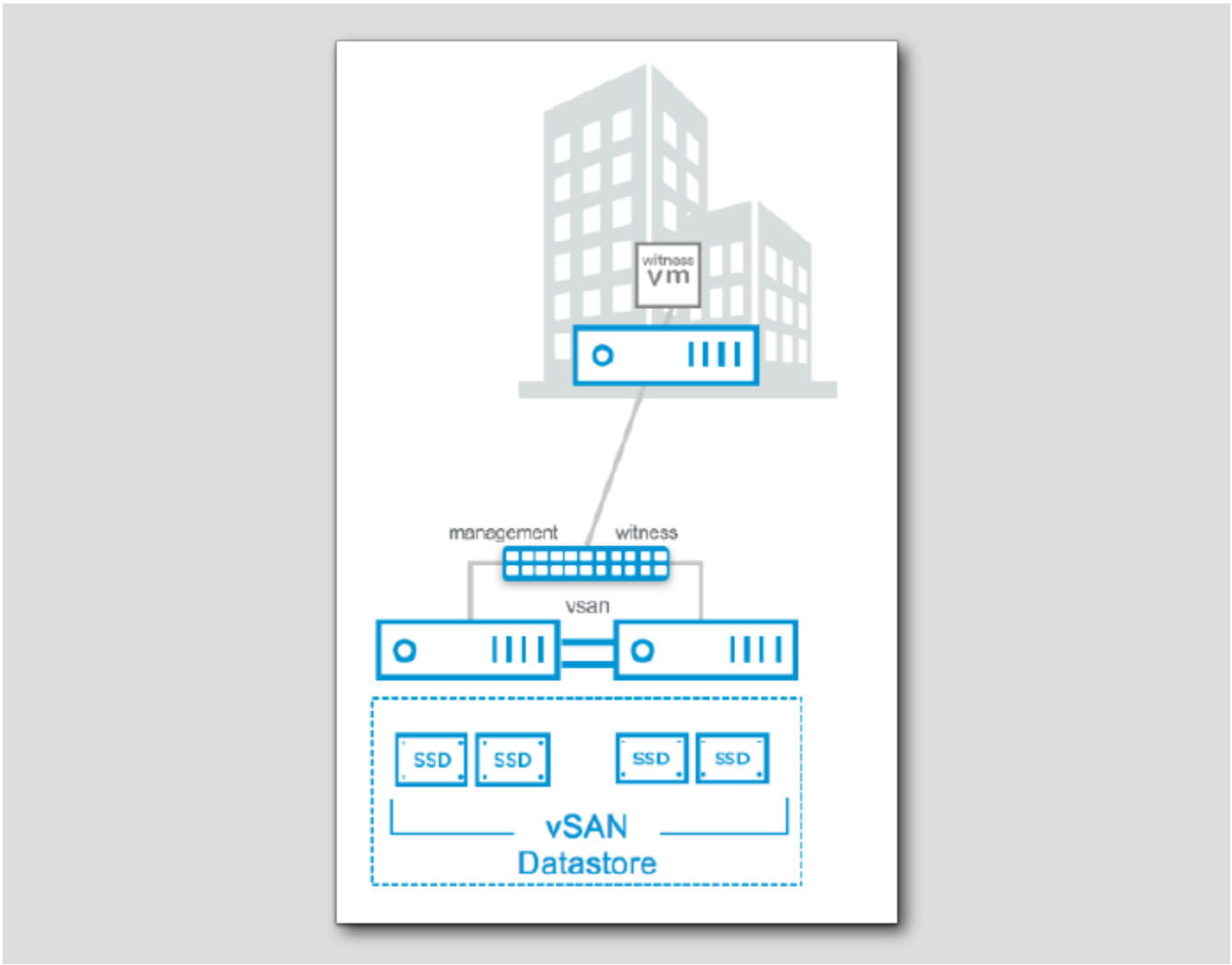
vSAN - Stretched Cluster Overview

[239]

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.

2-Node Direct Connect vSAN Cluster

[240]



vSAN 6.5 and later supports the use of network crossover cables in 2-node configurations. This is especially beneficial in use cases such as remote office and branch office (ROBO) deployments where it can be cost prohibitive to procure, deploy, and manage 10GbE networking equipment at each location. This configuration also reduces complexity and improves reliability. In the VMware Hands On Labs platform we aren't able to fully simulate this configuration, but the steps in this lab module show how to prepare a stretched cluster and separate the Witness VM traffic just as one would do in a direct-connect cluster.

What is a Preferred Domain/Preferred Site?

[241]

Preferred domain/preferred site is simply a directive for vSAN. The “Preferred” site is the site that vSAN wishes to remain running when there is a failure and the sites can no longer communicate. One might say that the “Preferred" site is the site expected to have the most reliability.

Since virtual machines can run on any of the two sites, if network connectivity is lost between site 1 and site 2, but both still have connectivity to the Witness, the preferred site is the one that survives and its components remains active, while the storage on the non-preferred site is marked as down and components on that site are marked as absent.

What is Read Locality?

[242]

Since virtual machines deployed on vSAN Stretched Cluster will have compute on one site, but a copy of the data on both sites, vSAN will use a read locality algorithm to read 100% from the data copy on the local site, i.e. same site where the compute resides. This is not the regular vSAN algorithm, which reads in a round-robin fashion across all replica copies of the data.

This new algorithm for vSAN Stretched Clusters will reduce the latency incurred on read operations.

If latency is less than 5ms and there is enough bandwidth between the sites, read locality could be disabled. However please note that disabling read locality means that the read algorithm reverts to the round robin mechanism, and for Virtual SAN Stretched Clusters, 50% of the read requests will be sent to the remote site. This is a significant consideration for sizing of the network bandwidth. Please refer to the sizing of the network bandwidth between the two main sites for more details.

The advanced parameter VSAN.DOMOwnerForceWarmCache can be enabled or disabled to change the behavior of read locality. This advanced parameter is hidden and is not visible in the Advanced System Settings vSphere web client. It is only available the CLI.

Read locality is enabled by default when vSAN Stretched Cluster is configured – it should only be disabled under the guidance of VMware’s Global Support Services organization, and only when extremely low latency is available across all sites.

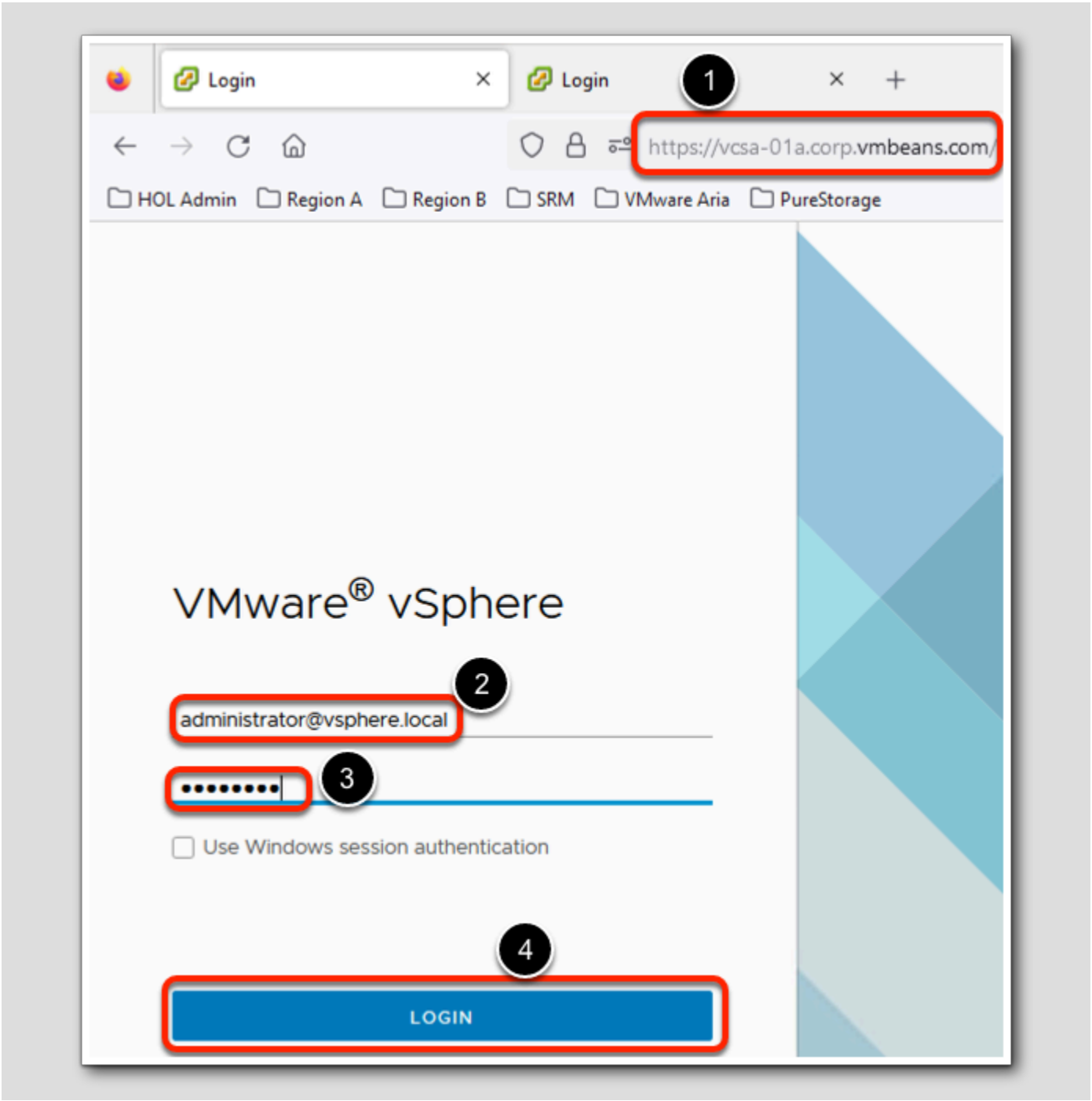
Open Firefox Browser from Windows Quick Launch Task Bar

[243]

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

Login to vSphere Client

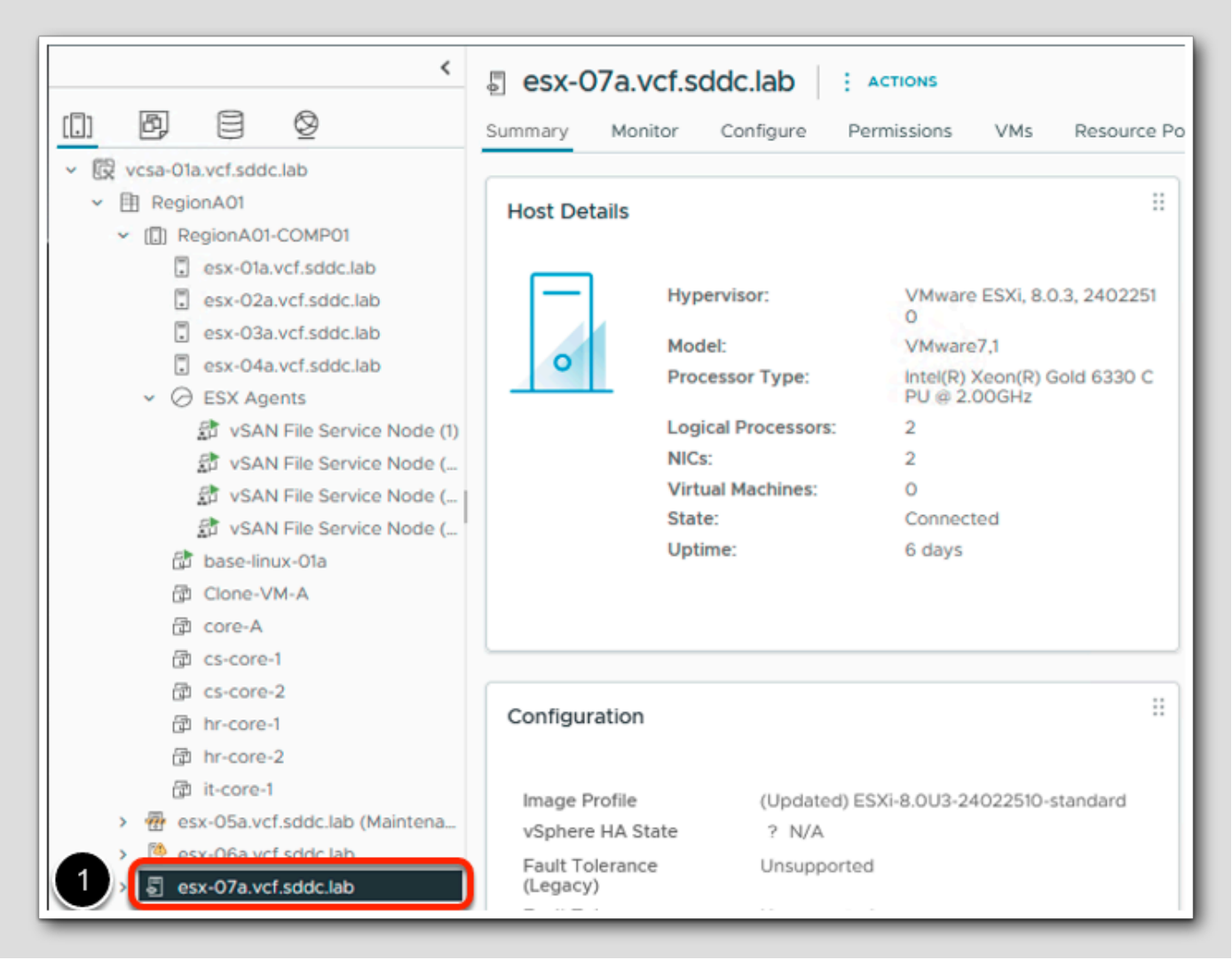
[244]



1. Check that you are logging in to vCenter Server: vcsa-01a.vcf.sddc.lab
2. On the vSphere Client login screen, username: administrator@vsphere.local
3. Enter Password: VMware1!
4. Click LOGIN

Witness Host must not be part of the vSAN Cluster

[245]



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. In our lab this host is called **esx-07a.vcf.sddc.lab**

Thus for a 1 (host) +1 (host) +1 (witness) configuration, there is one or more ESXi host at each site and one VSAN Witness host for the cluster.

Networking

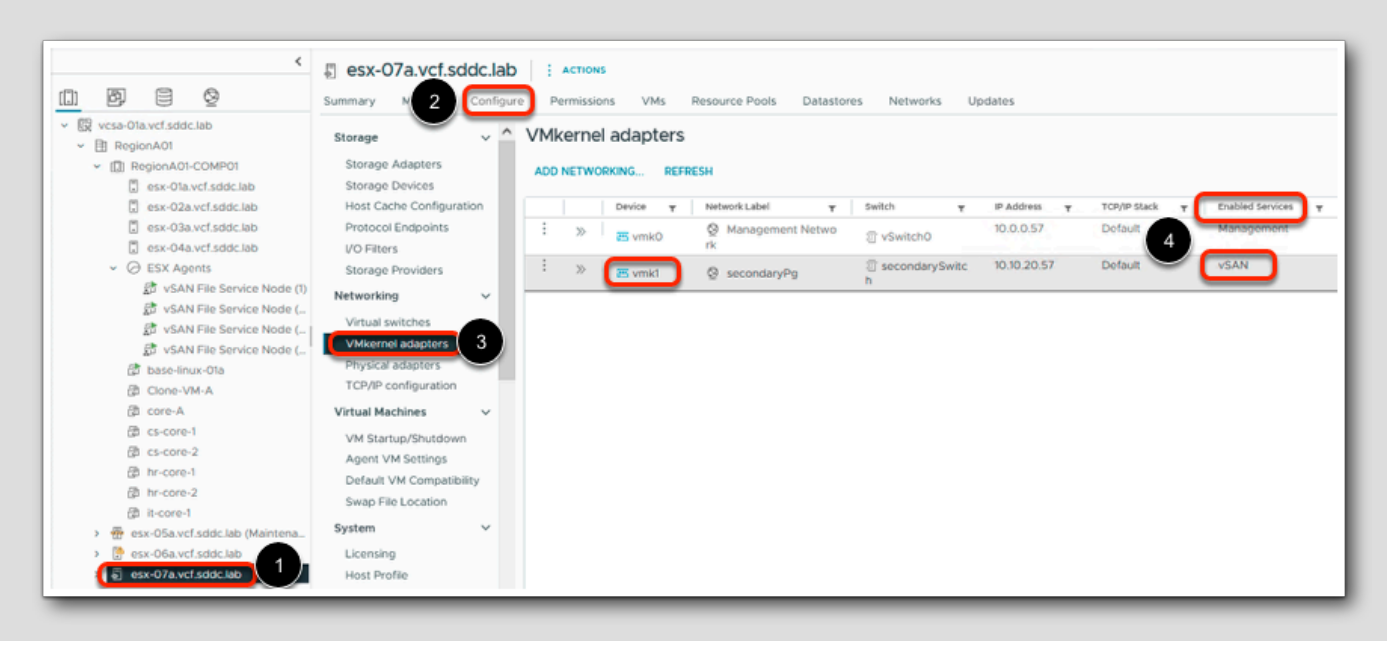
[246]

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 secondaryPG is attached to the other VSS. The Management VMkernel (vmk0) is used to communicate with the vCenter Server for appliance management. The secondaryPG 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 secondaryPg. 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, **esx-07a.vcf.sddc.lab**
2. Select **Configure**
3. Select **Networking > VMkernel adapters**
4. Validate that "**vSAN**" is an enabled service as depicted in the screenshot.

Default Gateways and Static Routes

[247]

The final step before a vSAN Stretched Cluster can be configured is to ensure there is connectivity among the hosts in each site and the Witness host. It is important to verify connectivity before attempting to configure vSAN Stretched Clusters.

When using vSAN 6.5 + (without a specified gateway), administrators must implement static routes. Static routes, as highlighted previously, tell the TCPIP stack to use a different path to reach a particular network. Now we can tell the TCPIP stack on the data hosts to use a different network path (instead of the default gateway) to reach the vSAN network on the witness host. Similarly, we can tell the witness host to use an alternate path to reach the vSAN network on the data hosts rather than via the default gateway.

Note once again that the vSAN network is a stretched L2 broadcast domain between the data sites as per VMware recommendations, but L3 is required to reach the vSAN network of the witness appliance. Therefore, static routes are needed between the data hosts and the witness host for the vSAN network, but they are not required for the data hosts on different sites to communicate to each other over the vSAN network.

In vSphere 6.5, a default gateway can be specified for each VMkernel interface and does not require static routes when specifying a default route for the vSAN tagged VMkernel interfaces.

The esxcli commands used to add a static route is:

```
esxcli network ip route ipv4 add -n <remote network> -g <gateway to use>
```

Other useful commands are esxcfg-route –n, which will display the network neighbors on various interfaces, and esxcli network ip route ipv4 list, to display gate ways for various networks. Make sure this step is repeated for all hosts.

Converting an existing vSAN Cluster to a Stretched Cluster

[248]

Converting an existing vSAN cluster to a stretched cluster is relatively simple. In this module, we will walk through the conversion steps.

Launch Firefox and the login to the vSphere Web Client

[249]

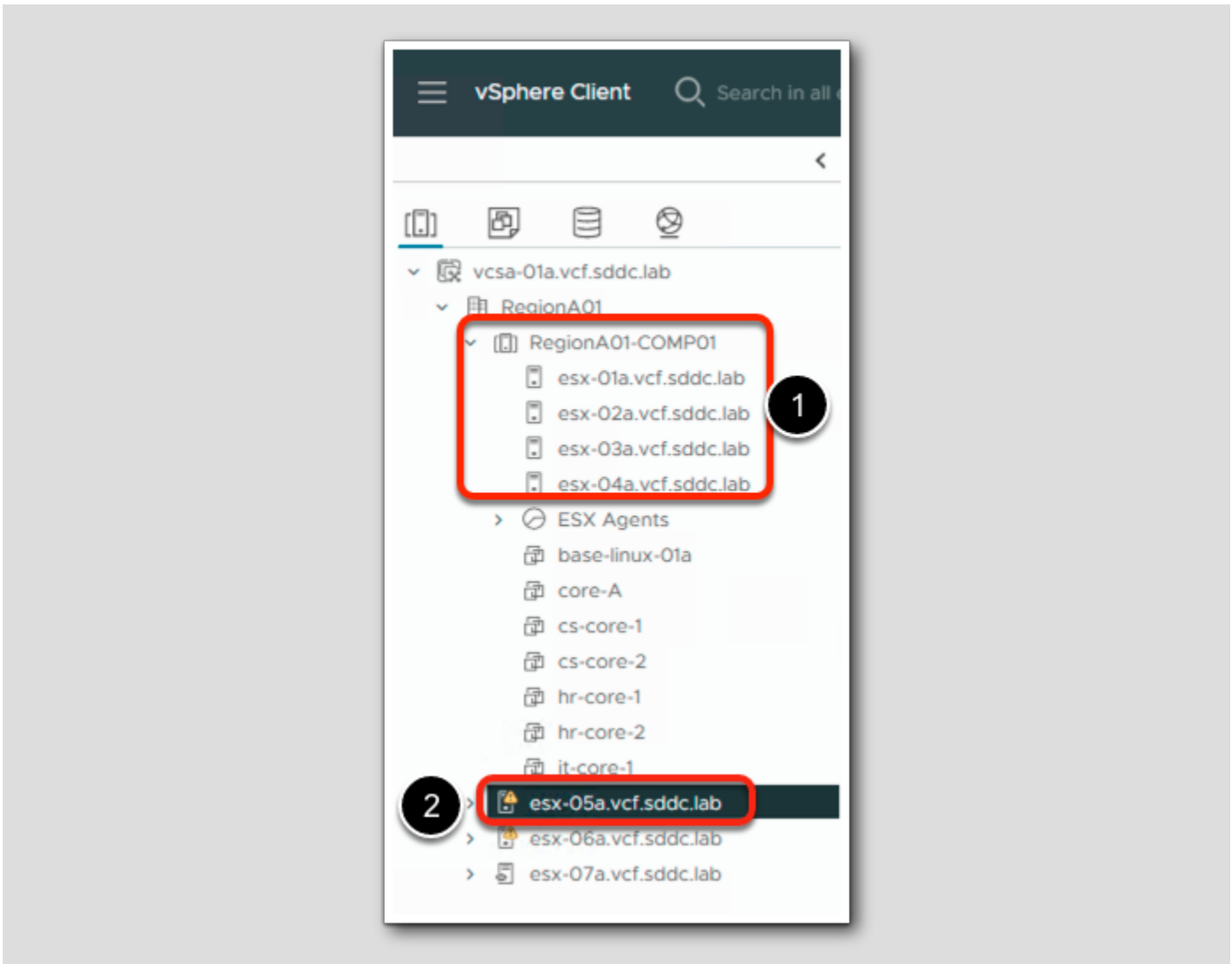
1. Select the Firefox icon in the Windows Task bar to launch the vSphere Web client

Log into vSphere Client [250]

1. Make sure that you are logging into vCenter Server: **vcsa-01a-vcf.sddc.lab**
2. Enter User ID: **administrator@vsphere.local**
3. Enter Password: **VMware123!**
4. Select **LOGIN**

Expand Inventory & review ESXi hosts

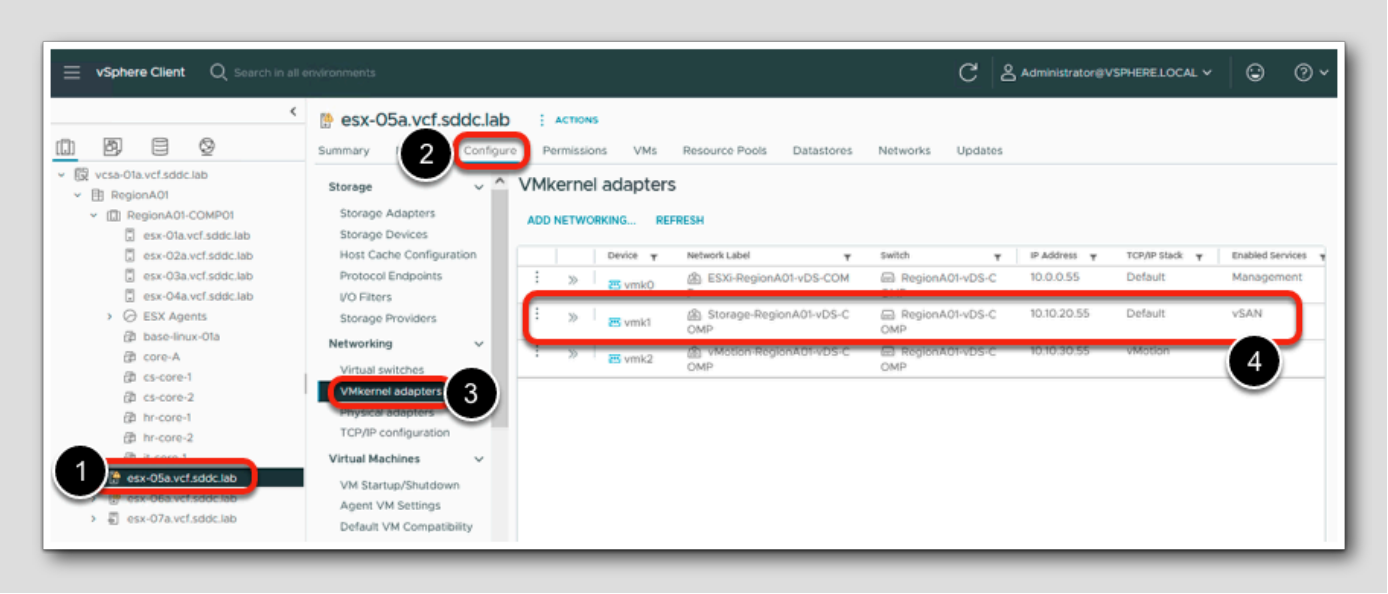
[251]



1. Note that we have an existing 3-node vSphere cluster already configured - RegionA01-COMP01 - which is comprised of hosts **esx-01a**, **esx-02a**, **esx-03a**, and **esx-04a**.
2. We have two hosts that we will add to the cluster: **esx-05a** & **esx-06a**.
    a. **esx-05a** may still be in maintenance mode due to a previous module. Go ahead and have that host exit out of maintenance mode.
3. Host **esx-07a** is a special type of host as shown by the small mark on the server icon - it is a vSAN witness host - a specialized virtual appliance used to support vSAN 2-Node and vSAN Stretch Cluster architectures.

Confirming Host Networking

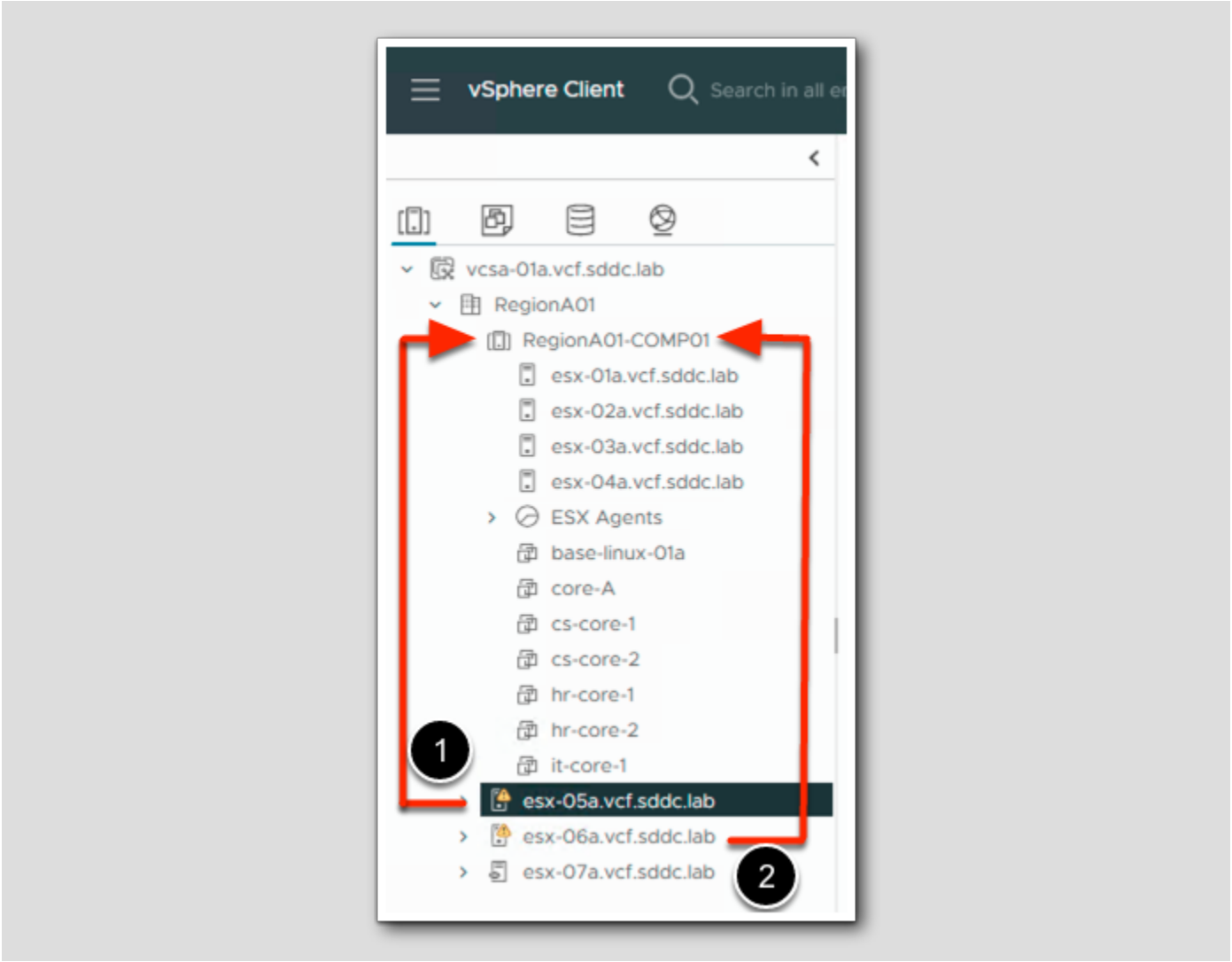
[252]



1. Click on **esx-05a.vcf.sddc.lab**
2. Click **Configure**
3. Select **VMkernel adapters**
4. Confirm there is a vSAN VMkernel adapter configured.
5. Repeat the step for **esx-06a.vcf.sddc.lab**

Add Hosts to vSAN Cluster

[253]

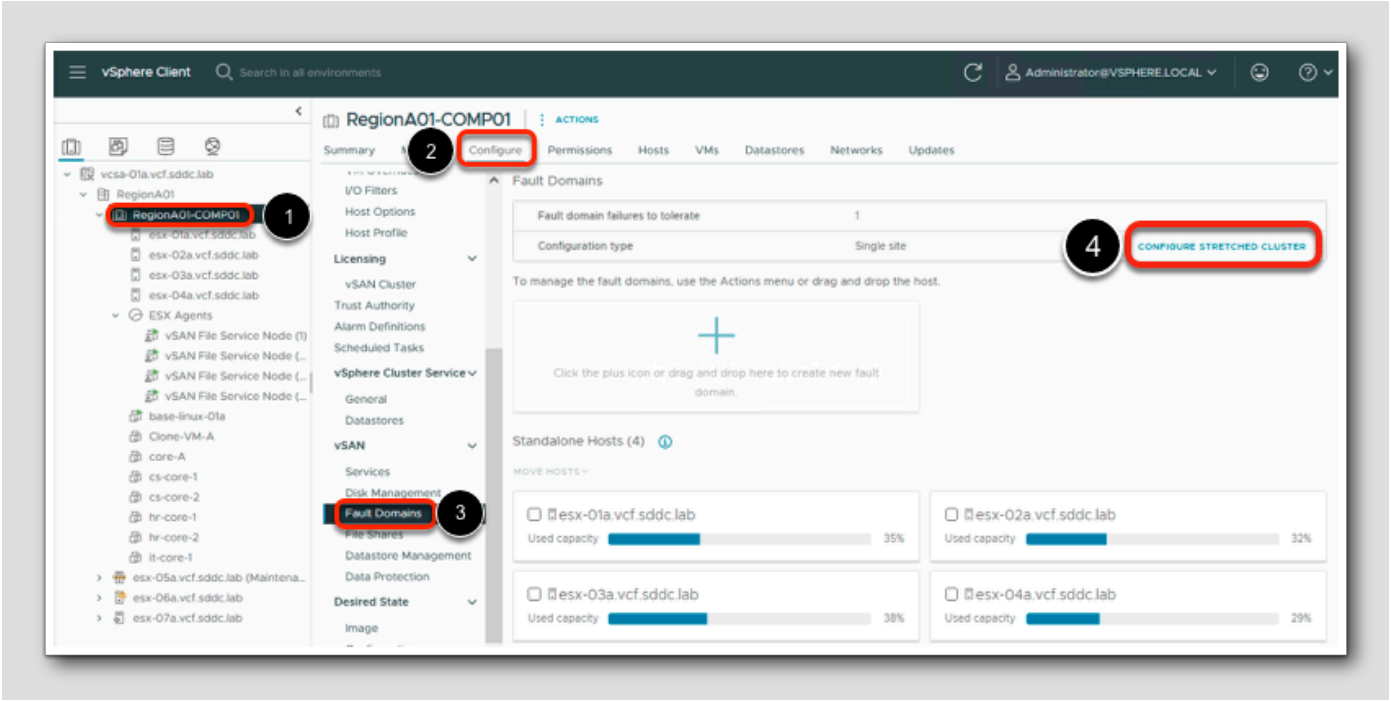


1. Drag host **esx-05a.vcf.sddc.lab** into **RegionA01-COMP01**
    a. There will be a dialog box that comes up. Leave it at default and click **OK**
2. Repeat step 1 and 1a for host **esx-06a.vcf.sddc.lab**

It may take a few minutes to add the hosts as new file service VMs will be provisioned. Once those tasks are complete, feel free to proceed to the next step.

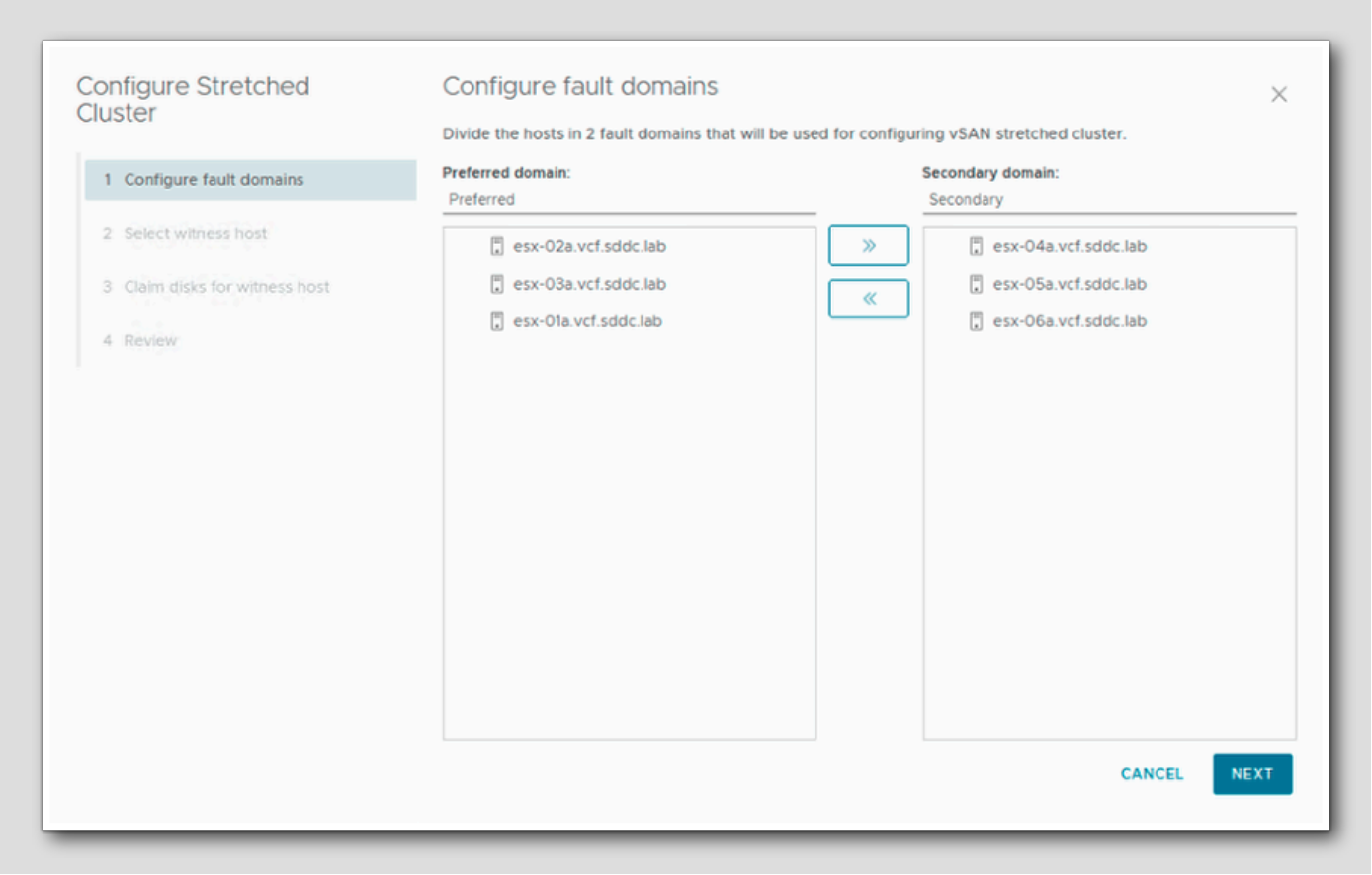
Reconfigure cluster RegionA01-COMP01

[254]



1. Select the cluster **RegionA01-COMP01**
2. Select **Configure**
3. Select **vSAN > Fault Domains**
4. Click **CONFIGURE STRETCHED CLUSTER**

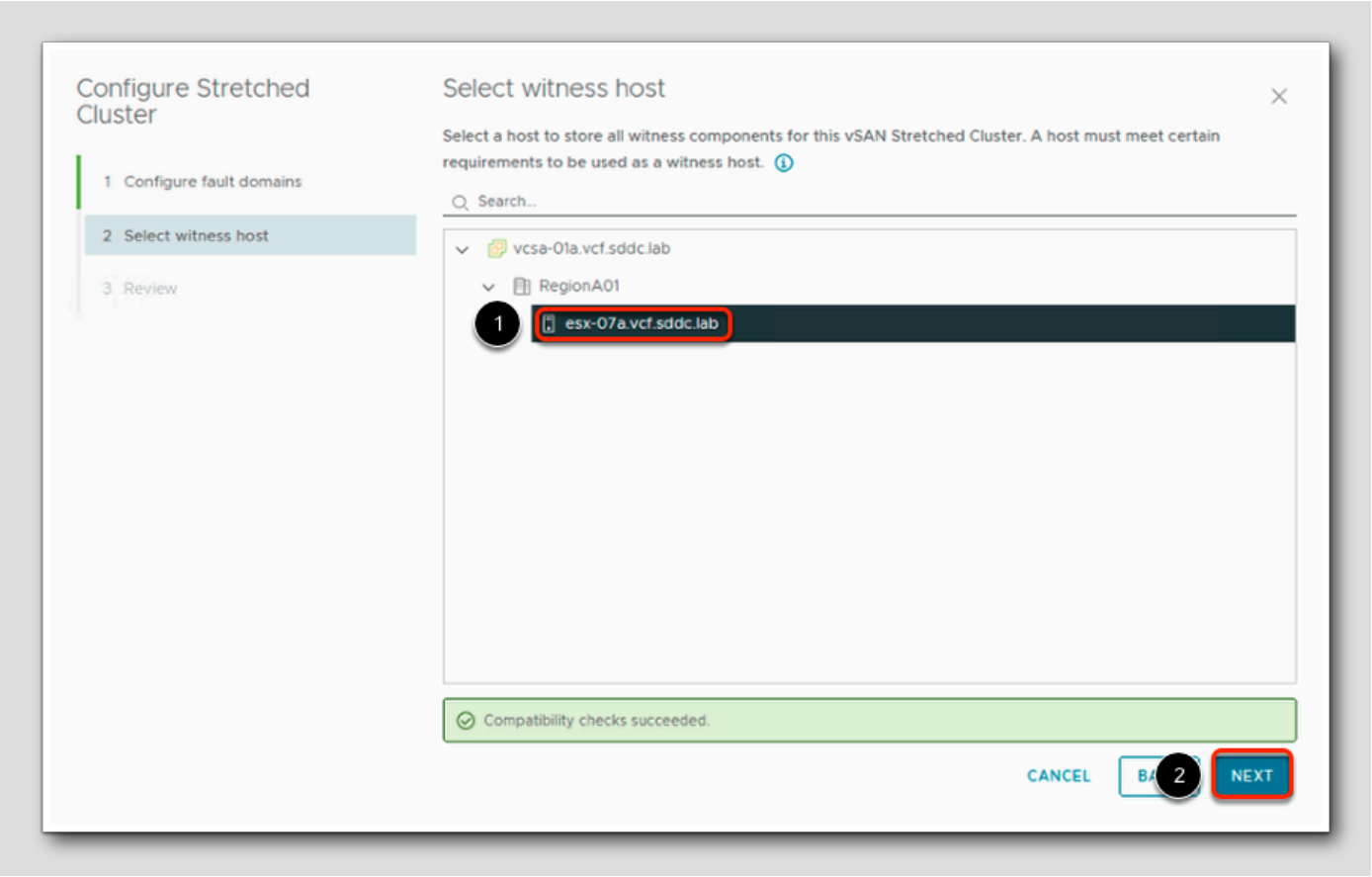
Configure a Stretched Cluster - Fault Domains



1. Click on the host **esx-04a.vcf.sddc.lab**
2. Click **>>** to move the host to the secondary domain.
3. Repeat steps 1 & 2 for host **esx-05a.vcf.sddc.lab & esx-06a.vcf.sddc.lab**
4. Confirm your screen matches the screenshot above.
5. Click **NEXT**.

Configure vSAN - Select witness host

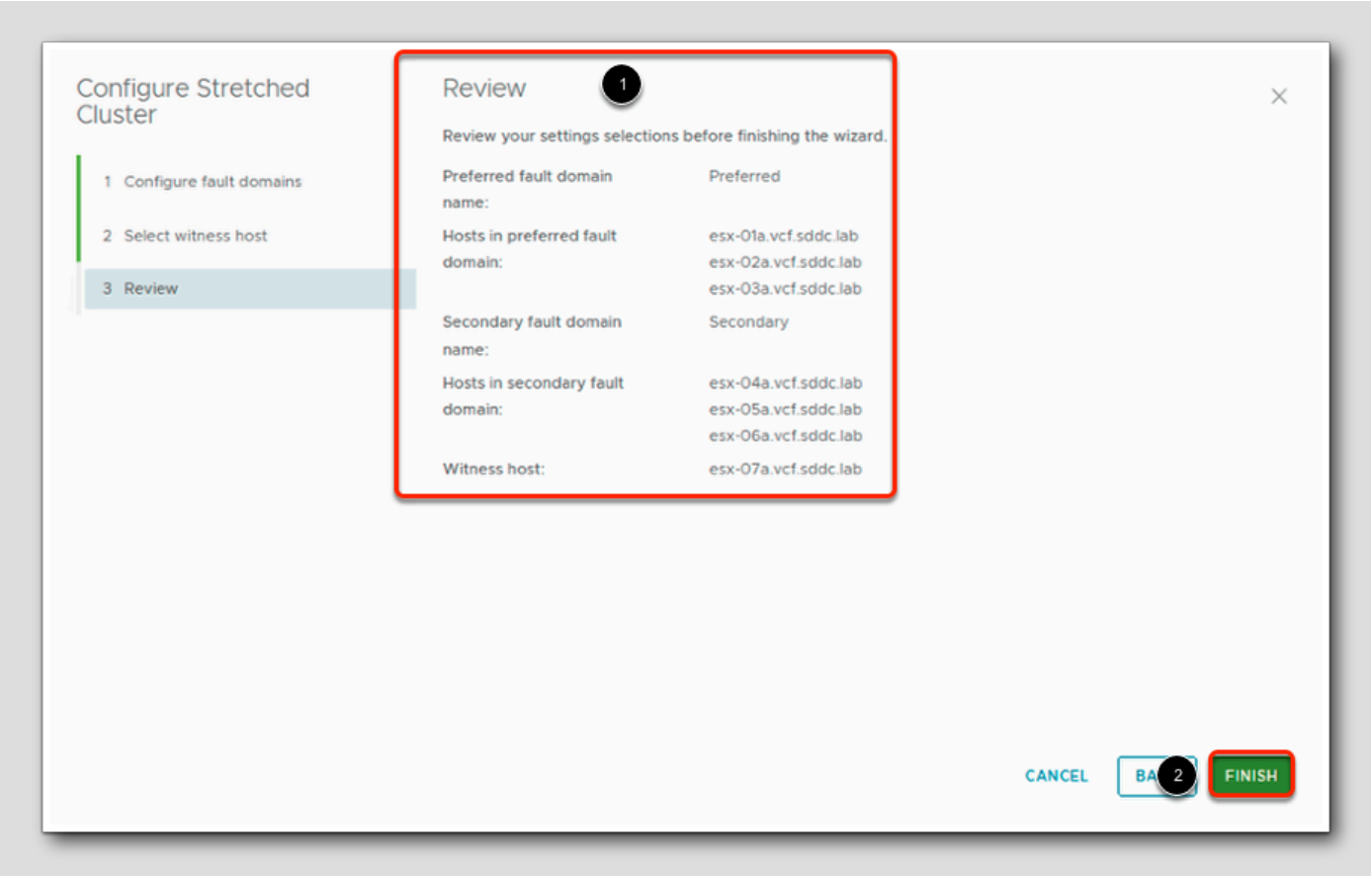
[256]



1. Expand the resource hierarchy and select **esx-07a.vcf.sddc.lab** as our vSAN witness host.
2. Notice that vSAN will run a compatibility check on the selected vSAN witness host to validate that it can be used with our cluster.
3. Select **NEXT**.

Configure a Stretched Cluster - Review

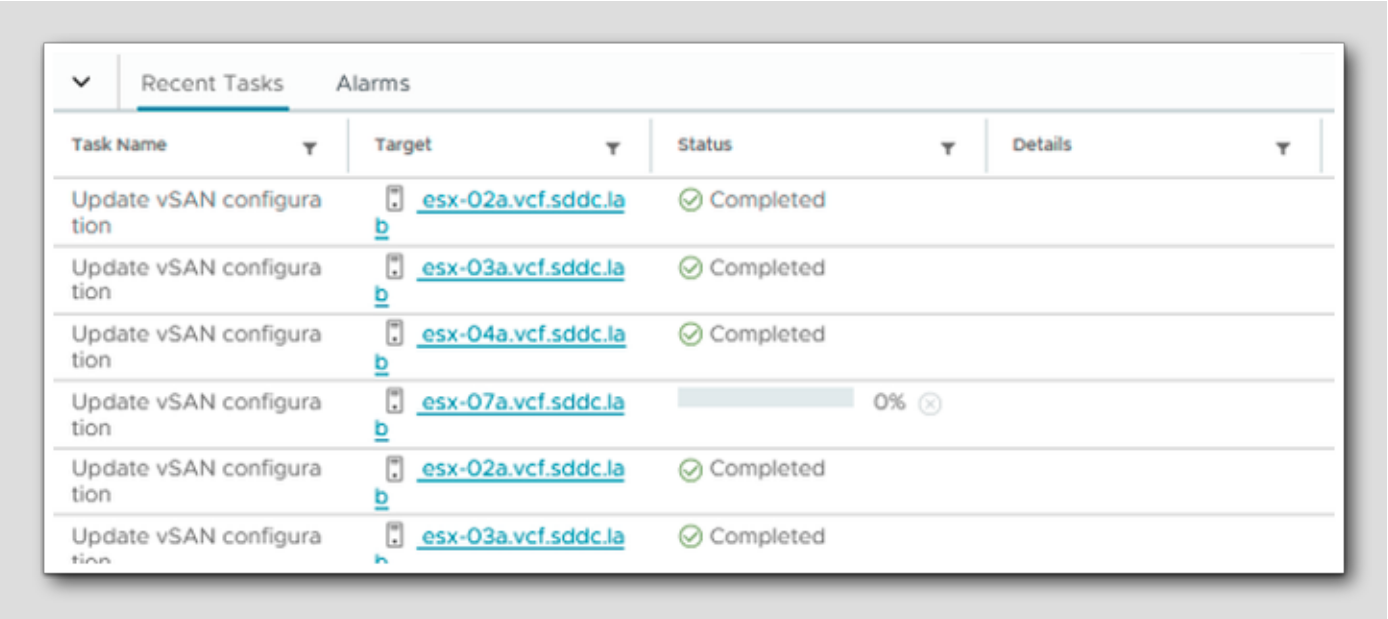
[257]



1. Notice that vSAN summarizes the configuration of the cluster it will create - and provides you an opportunity make corrections prior to converting to a stretched cluster.
2. Select **FINISH** to create the vSAN stretch cluster.

Monitor Recent Tasks pane in vCenter

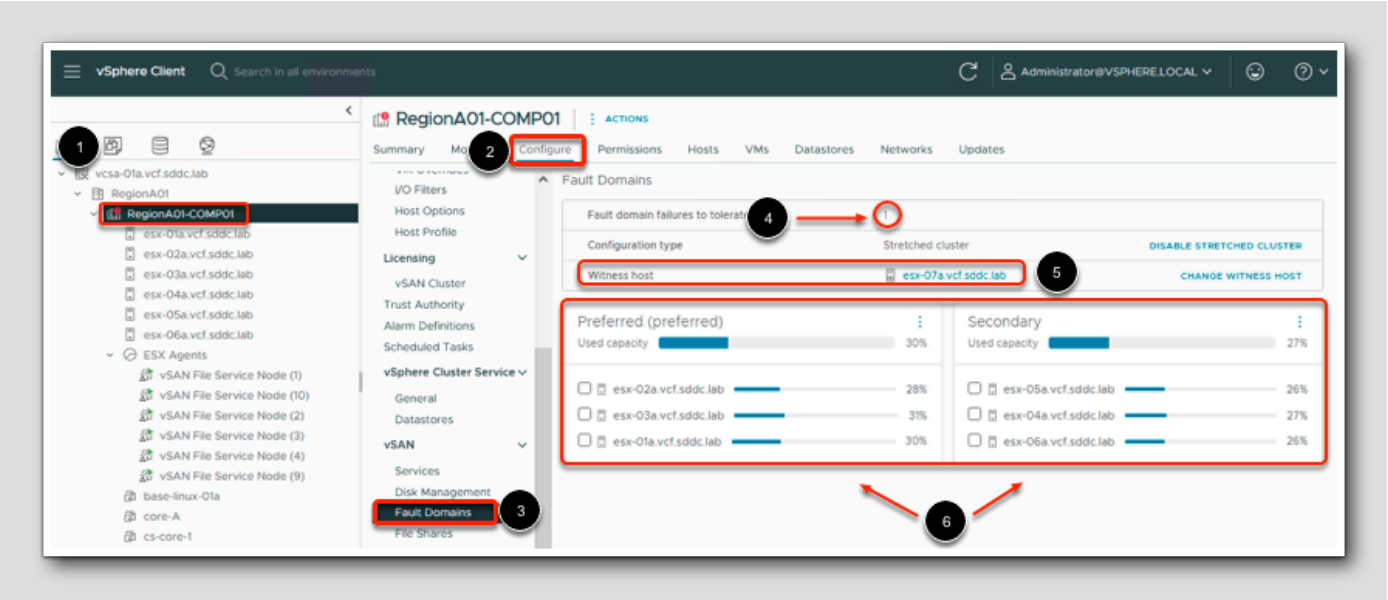
[258]



At this stage vSAN is forming a cluster and vCenter can be used to monitor the progress - once all the tasks are "Completed" it is safe to proceed to the next step.

Review Stretched Cluster Configuration

[259]



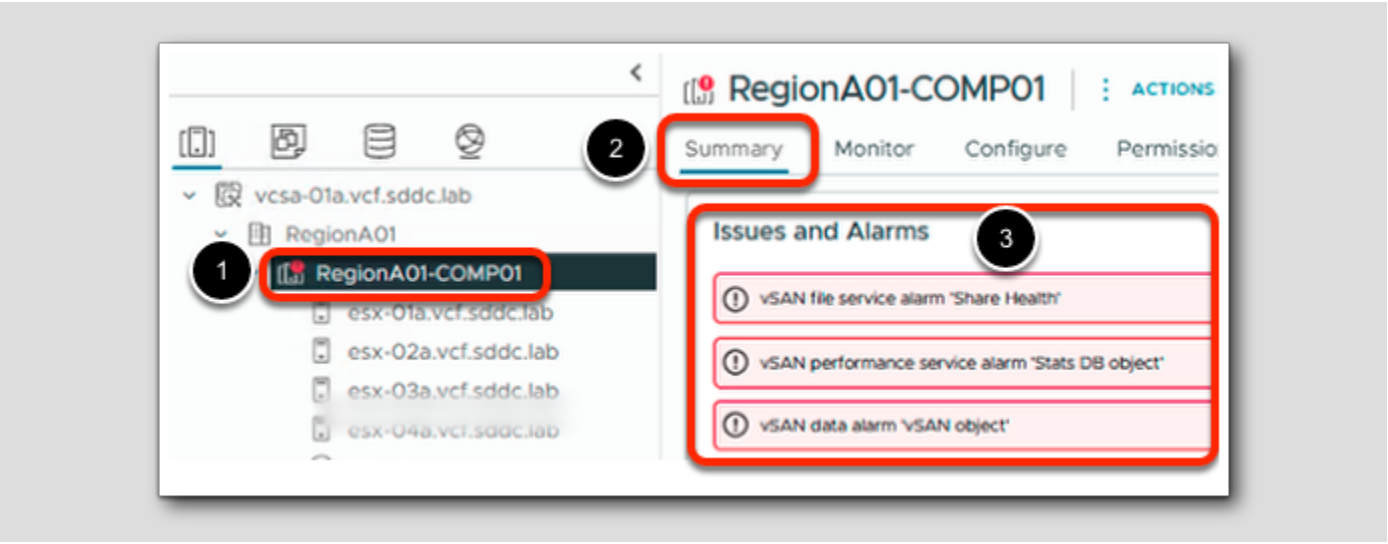
Lets now have a look at the **Fault Domains and Stretched Cluster** configuration.

1. Select **RegionA01-COMP01**
2. Select **Configure**
3. Select **vSAN > Fault Domains**
4. Fault domain failures to tolerate (FTT) is 1 - this means our cluster can tolerate the loss of either site (or the witness host) and still run the VMs in the cluster. Site Mirroring and FTT=1 is a prescribed architecture for vSAN stretch clusters. In larger vSAN stretch clusters of 6 nodes or more, administrators can optionally configure an additional level of protection for VMs to protect against failures within a site - these choices align with typical vSAN policies of RAID-1 (Mirroring), & RAID-5 & RAID-6 (Erasure Coding).
5. vSAN Stretched Cluster is **enabled** with the witness host **esx-07a.vcf.sddc.lab**
6. We can also see the **2 Fault Domains** that have been created and their respective ESXi hosts

Issues and Alarms

[260]

Since our lab runs in nested-vSphere environment, there are several warnings that vCenter will surface about the health of our vSAN cluster. In the scope of this lab, it is OK to ignore - or suppress - these warnings, but in any "live" vSAN cluster used to host actual workloads, you should use vSAN's Skyline Health service to research any warnings in greater detail.



1. Select RegionA01-COMP01
2. Select **Summary**
3. Review any listed **Issues and Alarms** and clear, if desired.

Conclusion

[261]

This concludes the lesson on converting to a vSAN 8.0 Update 3 for 6-node Stretched Cluster.

Monitoring a vSAN Stretched Cluster

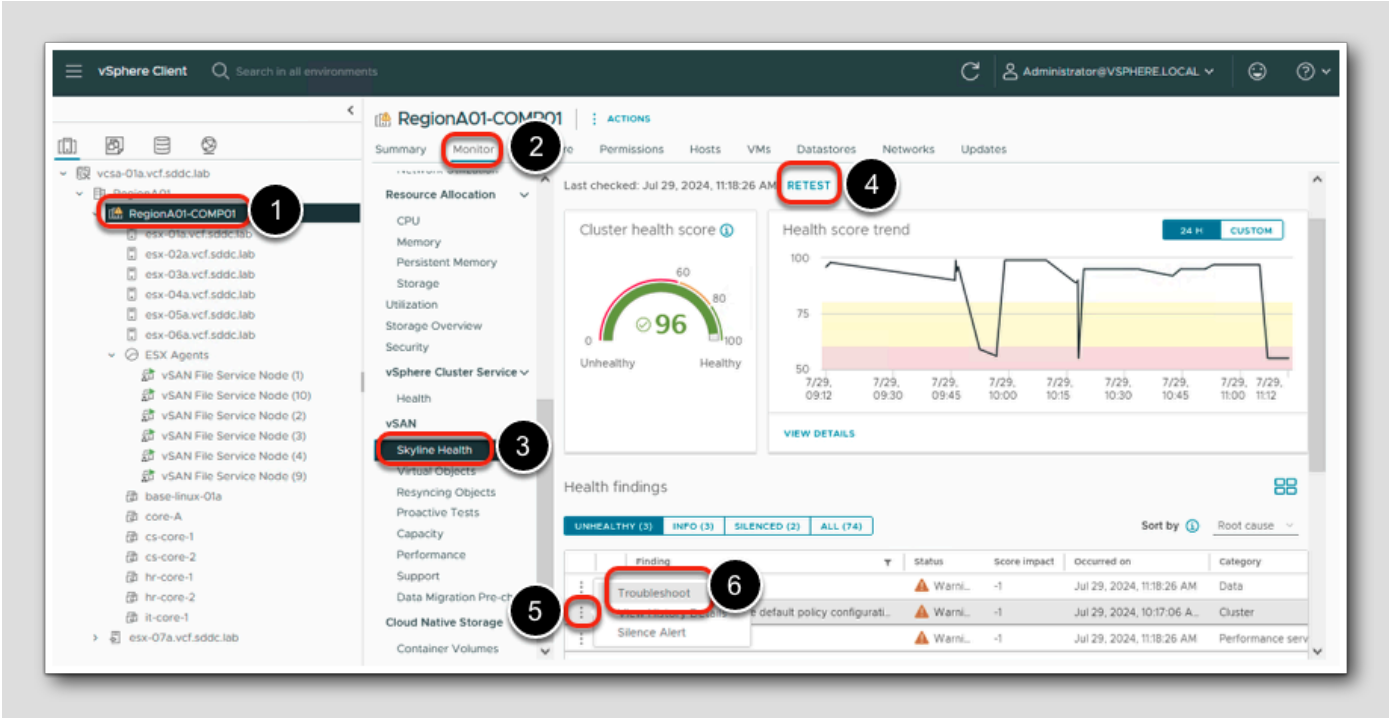
[262]

One of the ways to monitor your vSAN environment is to use the vSAN Skyline 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

[263]



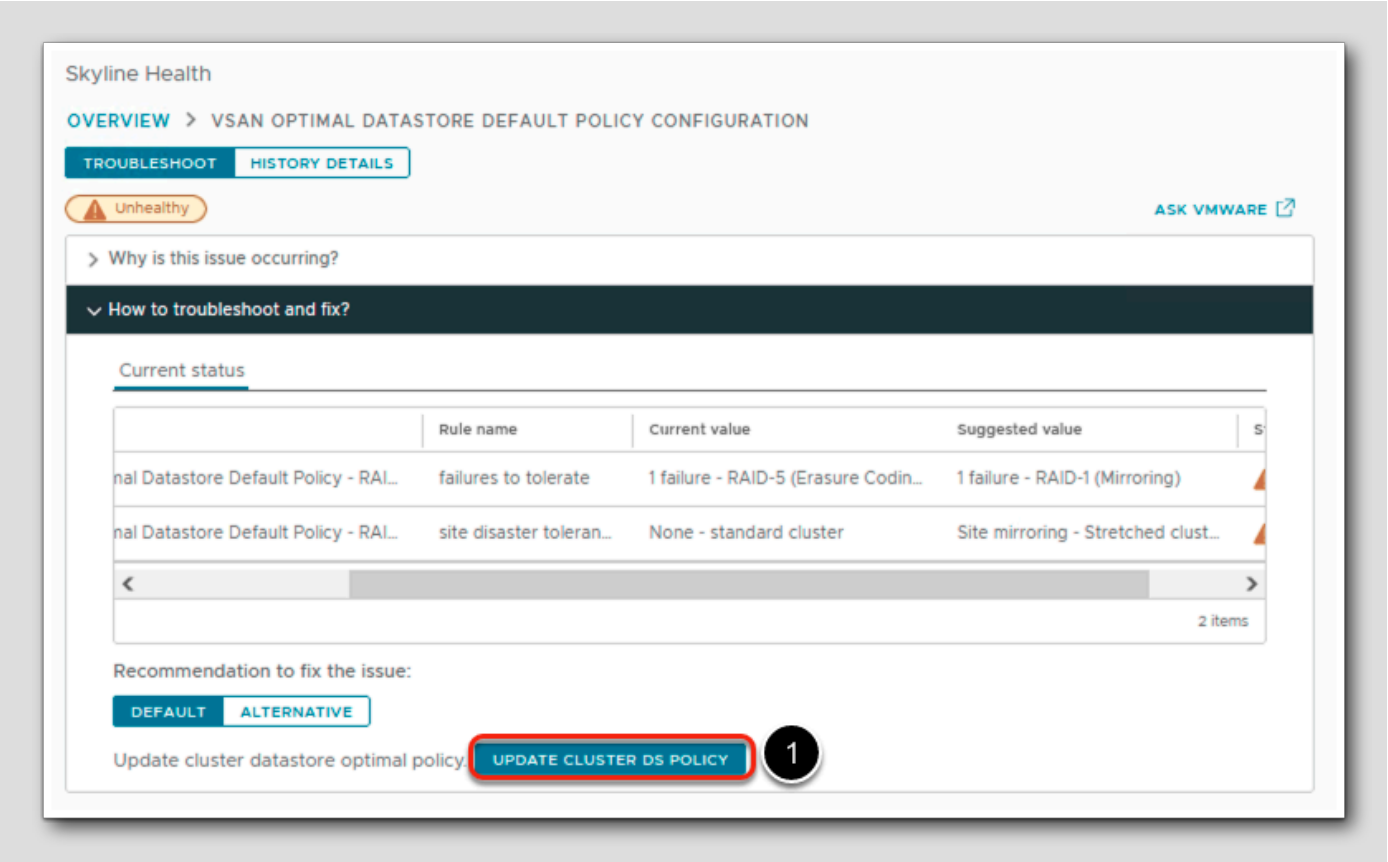
Let's run a **Skyline Health Check** and see what issues come up.

1. Select **RegionA01-COMP01**
2. Click **Monitor**
3. Select **vSAN > Skyline Health**
4. Click **RETEST**
5. Click on the three dots next to, **vSAN optimal datastore default policy configuration...**
6. Click **Troubleshoot**

To drill in deeper to the individual tests select the stack of "3 dots" in the left margin of the table, then choose View Current Result to see more information the health finding.

Changing the Datastore Default Policy

[264]



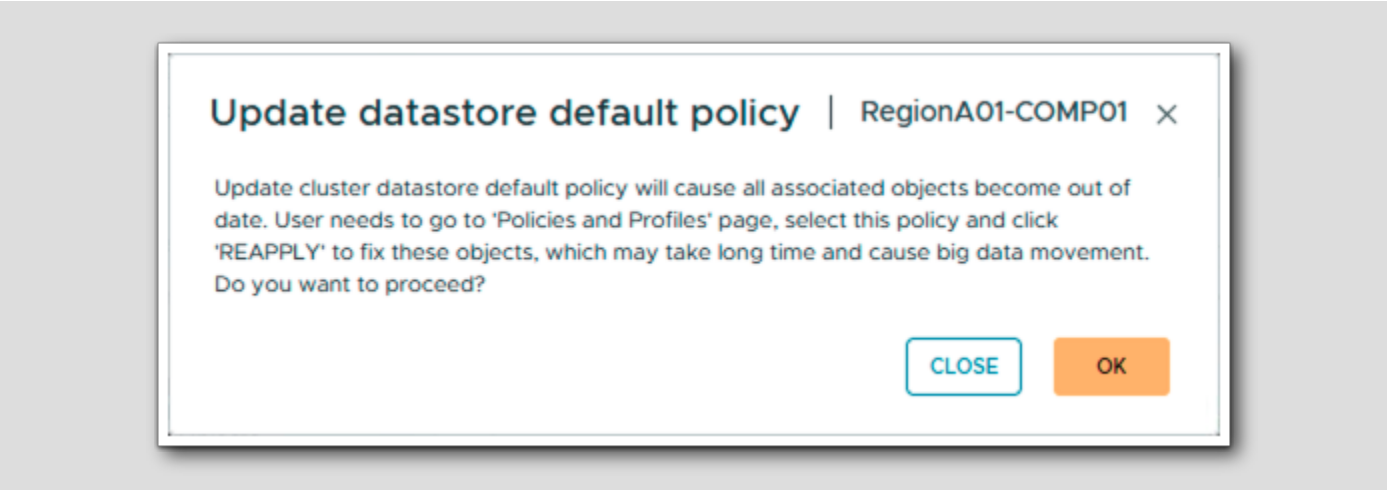
Here, you can see that since we made changes to the build of the cluster (mainly, converting to a stretch cluster with three hosts at each location), Skyline health has made some recommendations on changing some of the rules of the optimal storage policy:

- Changing from a standard cluster to a stretched cluster (with Site mirroring).
- Changing from a RAID 5 to a RAID 1 within each site.

1. Click **UPDATE Cluster DS Policy**

Changing the Datastore Default Policy

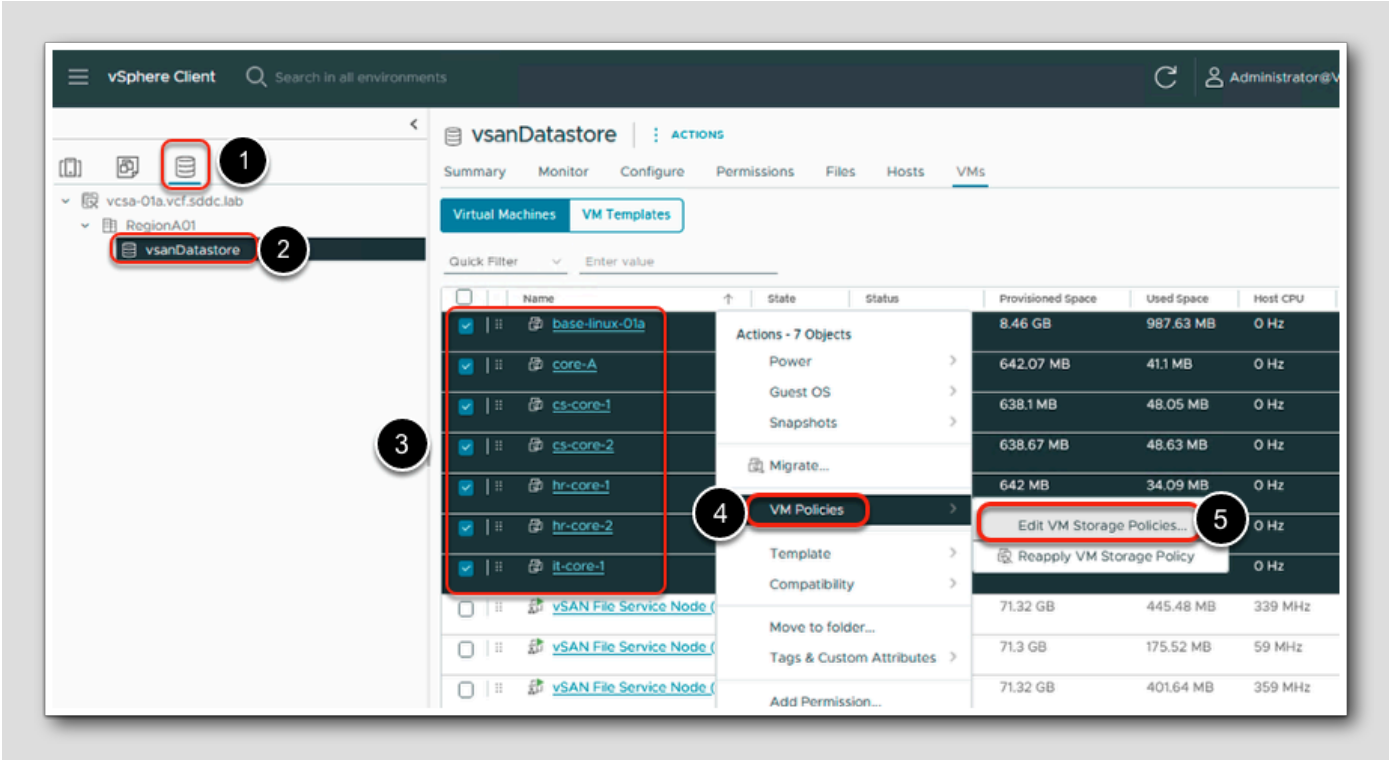
[265]



1. An **Update datastore default policy** dialog window will pop up. Click **OK**.
    a. Since we are changing the default policy, we would need to reapply the policy so that any VMs using the original policy adopt the new one. Since the VMs in this environment are using the default ESA RAID 5 policy, let's go ahead and manually change the policy to use the new Optimal Storage Policy.

Applying Updated Policy to Existing VMs

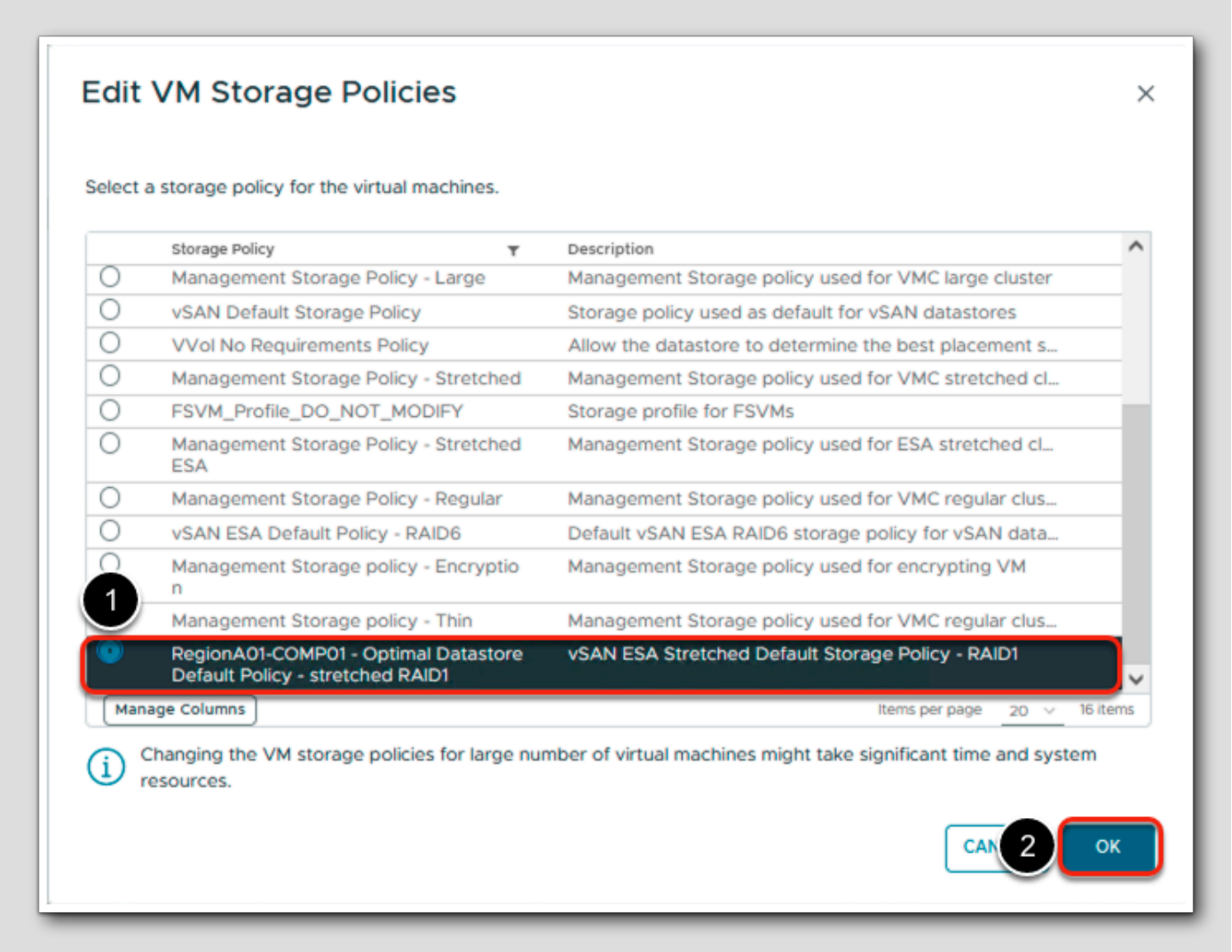
[266]



1. Click on the datastore icon
2. Select **RegionA01 > vsanDatastore**
3. Check the box next to the VMs highlighted in the screenshot. **Do not select any of the vSAN File Service VMs.**
4. Right click in the highlighted area and click on **VM Policies**.
5. Click on **Edit VM Storage Policies**.
6. A pop-up will show asking if you want to perform the action on the 7 objects. Click **YES**.

Applying Updated Policy to Existing VMs

[267]

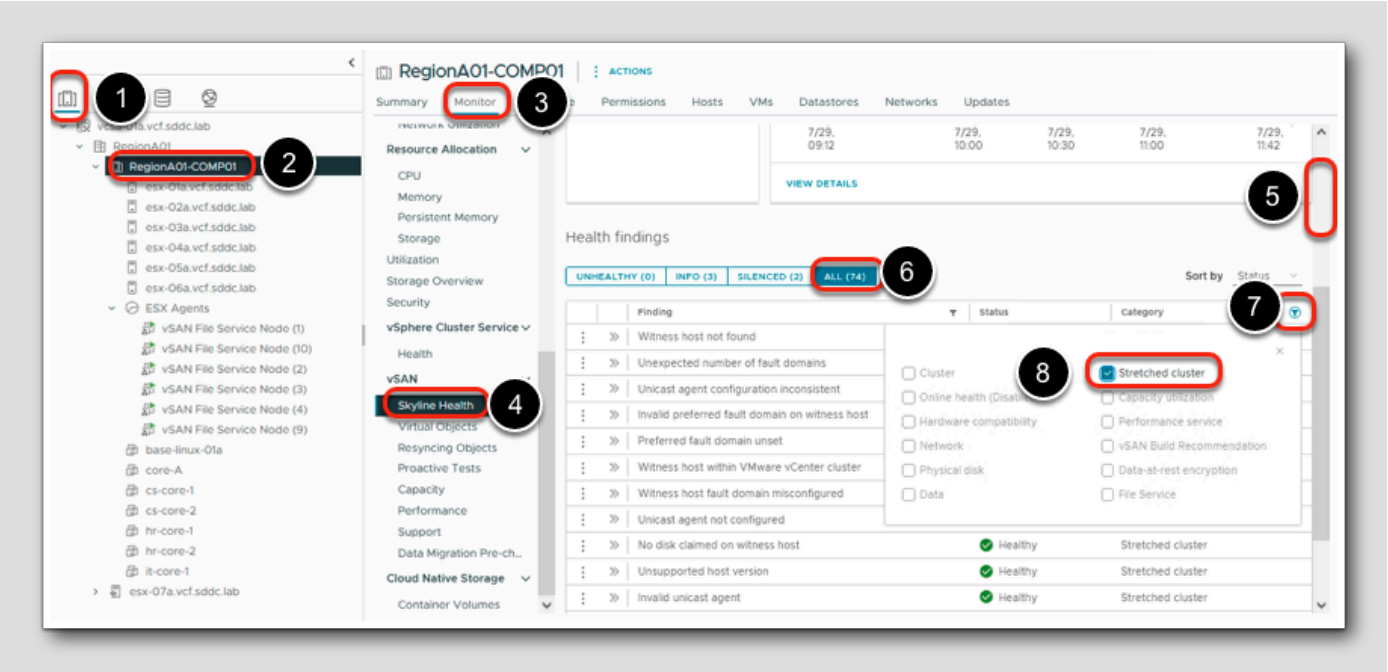


1. Scroll down and select **RegionA01-COMP01 - Optimal Datastore Default Policy - stretched RAID 1**
2. Click **OK**

This will convert the existing VMs to the new optimal storage policy and ensure availability across both sites as well as within each site.

Viewing Skyline Health Checks for Stretched Clusters

[268]



Now that we've applied the new optimal storage policy, let's go back to Skyline Health and see what other health checks related to stretched clusters are available.

1. Click on the clusters icon
2. Select **RegionA01-COMP01**
3. Click **Monitor**
4. Select **vSAN > Skyline Health**
5. Scroll down until you see **Health findings**
6. Click **ALL**
7. Click the filter icon
8. Check **Stretched cluster**.

Here, you can review the different types of health checks Skyline looks at for stretched clusters.

Conclusion

[269]

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.

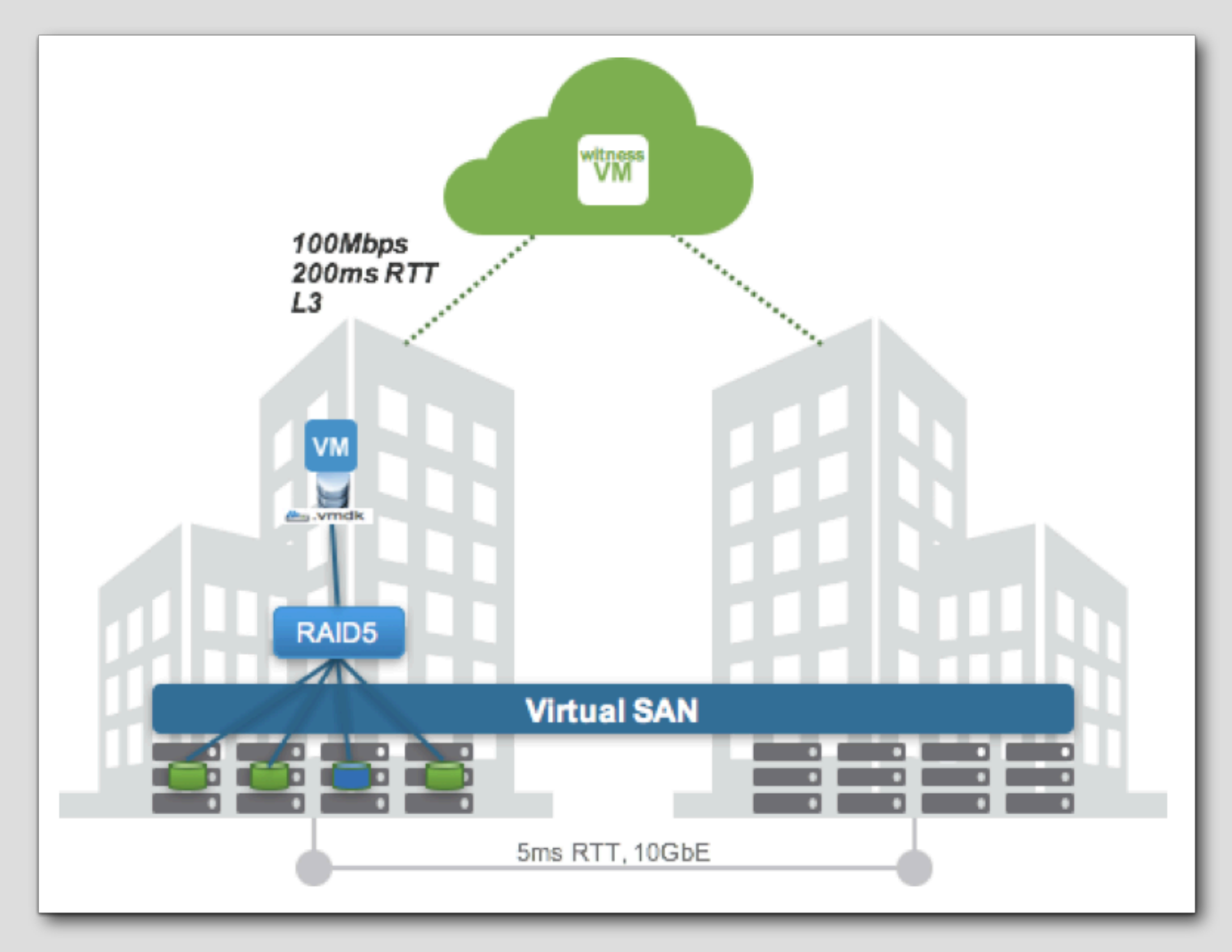
vSAN Site Affinity

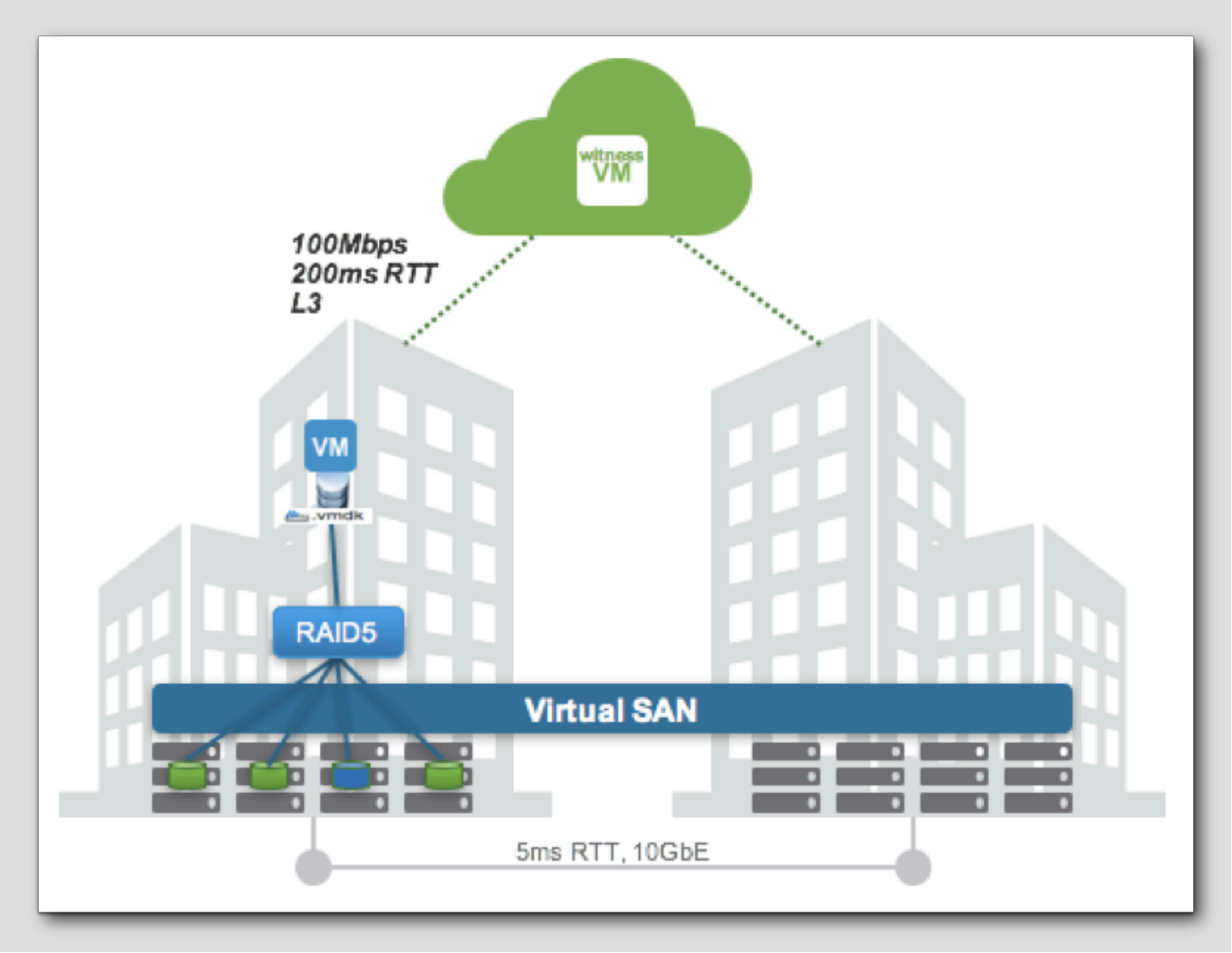
[270]

There are several workloads in a datacenter with inbuilt application level availability or redundancy.

However, typical production workloads require multi-site protection to enable better data redundancy.

How do we cater to workloads which do not require copies to be stored on different sites?





Introducing Local Affinity

[271]

With Local Affinity, customers can use policies to keep data on a single site. In this case Primary Failures to Tolerate (PFTT) = 0.

This ensures that objects are not replicated to the secondary site there by reducing the bandwidth required between sites.

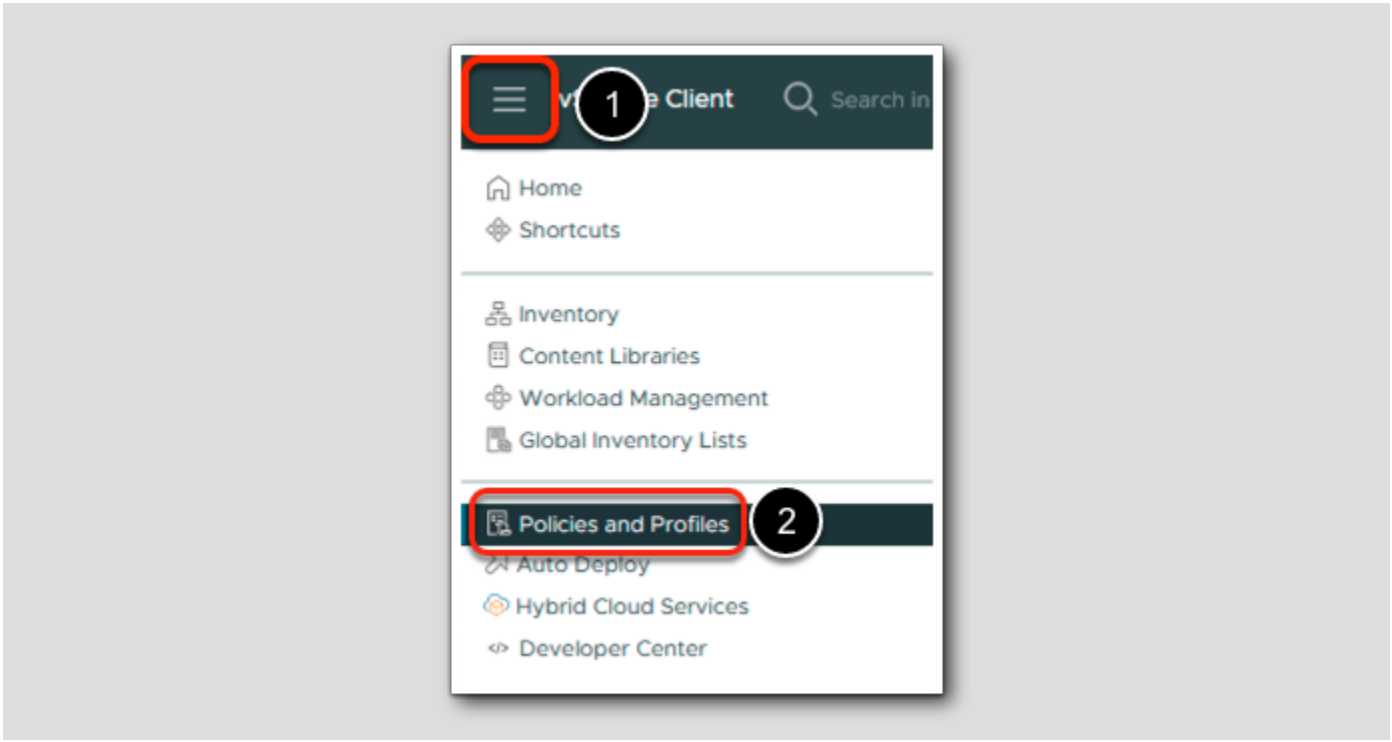
Additionally, by using Affinity rules, customers can set VM/VMDK assignments to specific hosts.

For example, to test local affinity, you can set PFTT = 0, SFTT = 2, FTM = RAID 5. The outcome of this test is that all IOs should be done locally and not on the secondary site. This way, you can seamlessly achieve host/disk protection for objects that do not require site protection.

A few housekeeping rules for local affinity:

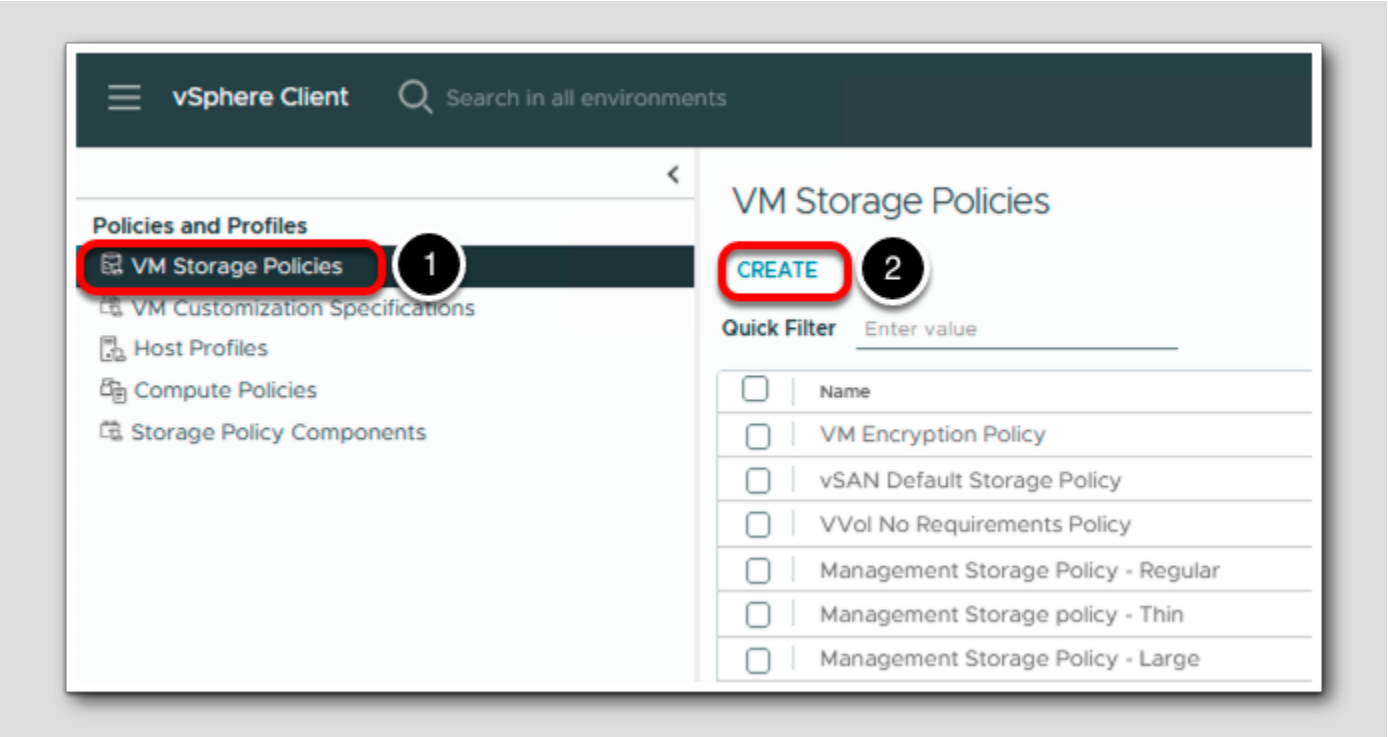
- Affinity will only be available when Stretched Clusters is enabled
- DRS/HA rules should be aligned with Data Locality
- RAID 0 / RAID 1 are supported for Hybrid and RAID 0 / RAID 1 / RAID 5 / RAID 6 are supported for All Flash

Storage Policy Based Management - Local Affinity [272]



1. Select **vSphere Client** menu at the top left of the screen.
2. Click on **Policies and Profiles**.

Storage Policy Based Management - Local Affinity

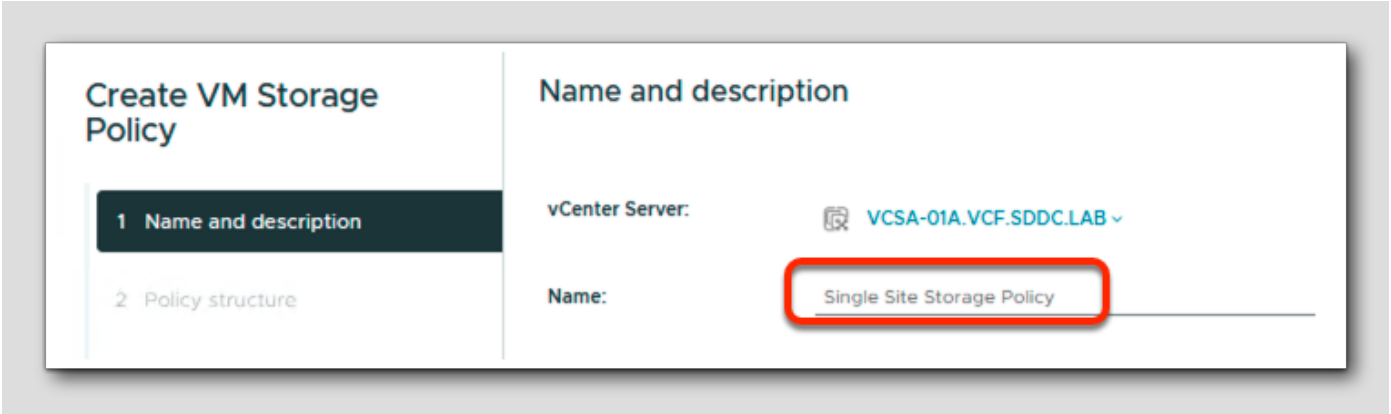


In this lesson, we will create a VM Storage Policy for **Local Affinity**.

1. Select **VM Storage Policies**
2. Select **CREATE**

Storage Policy Based Management - Local Affinity

[274]



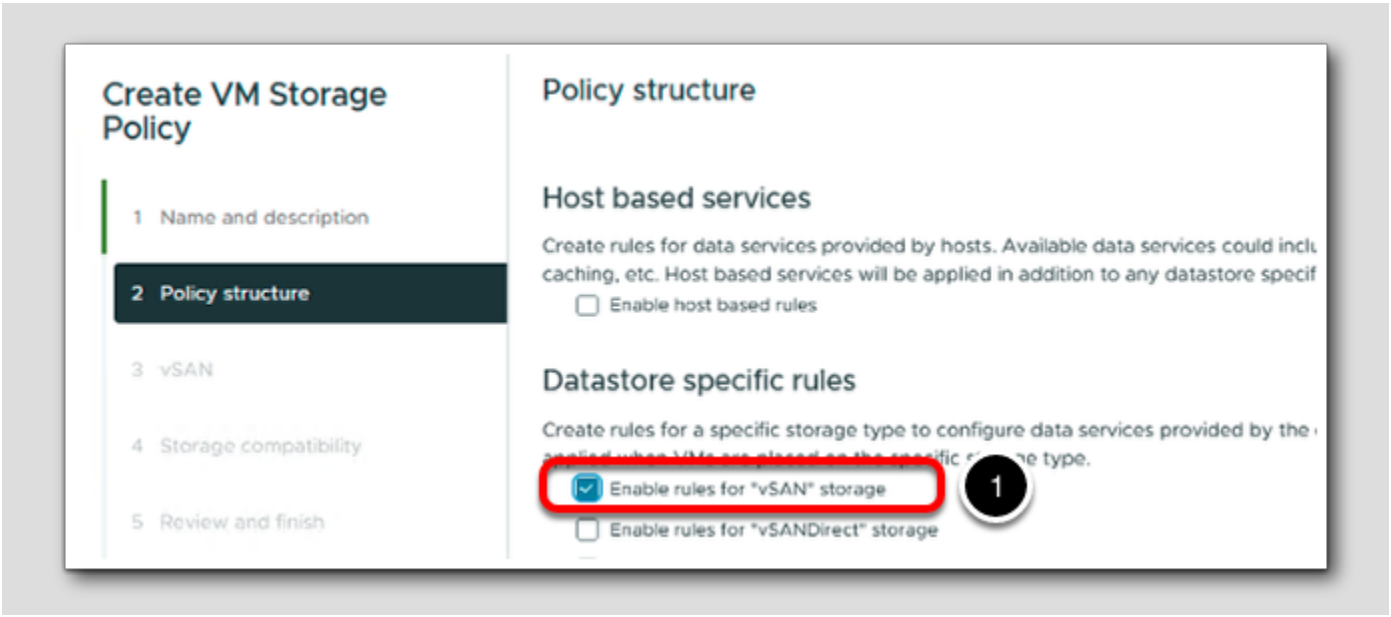
1. Enter a name for the VM Storage Policy

```
Single Site Storage Policy
```

2. Click NEXT (not pictured)

Storage Policy Based Management - Local Affinity

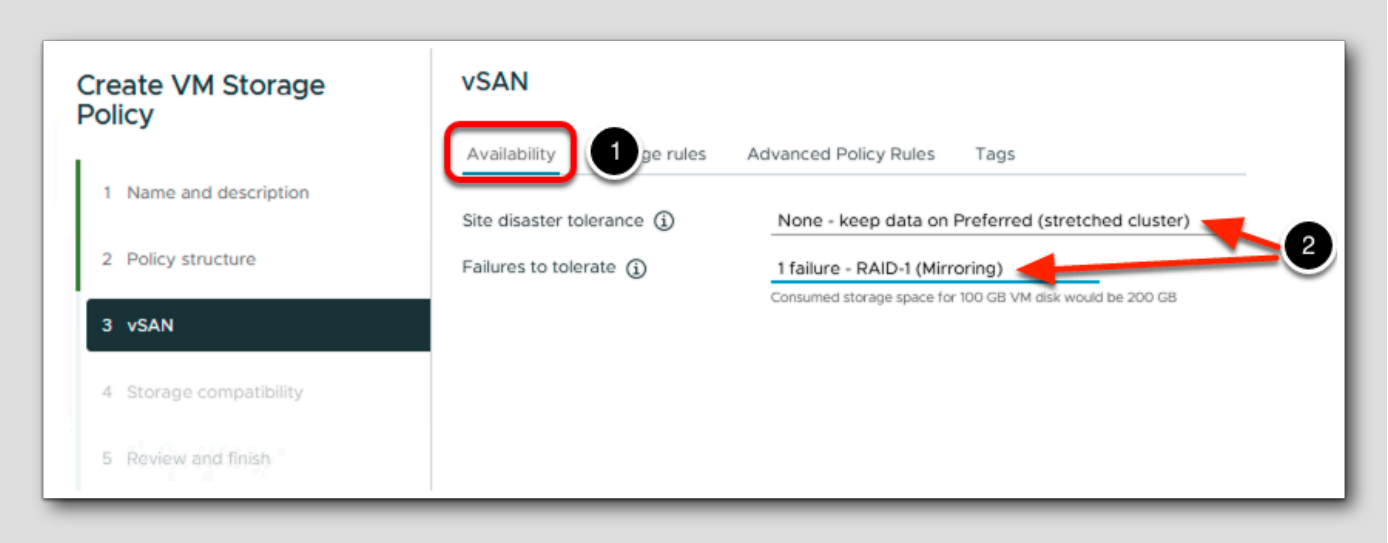
[275]



1. Select **Enable rules for "vSAN" storage**
2. Click **NEXT** (not pictured)

Storage Policy Based Management - Local Affinity

[276]



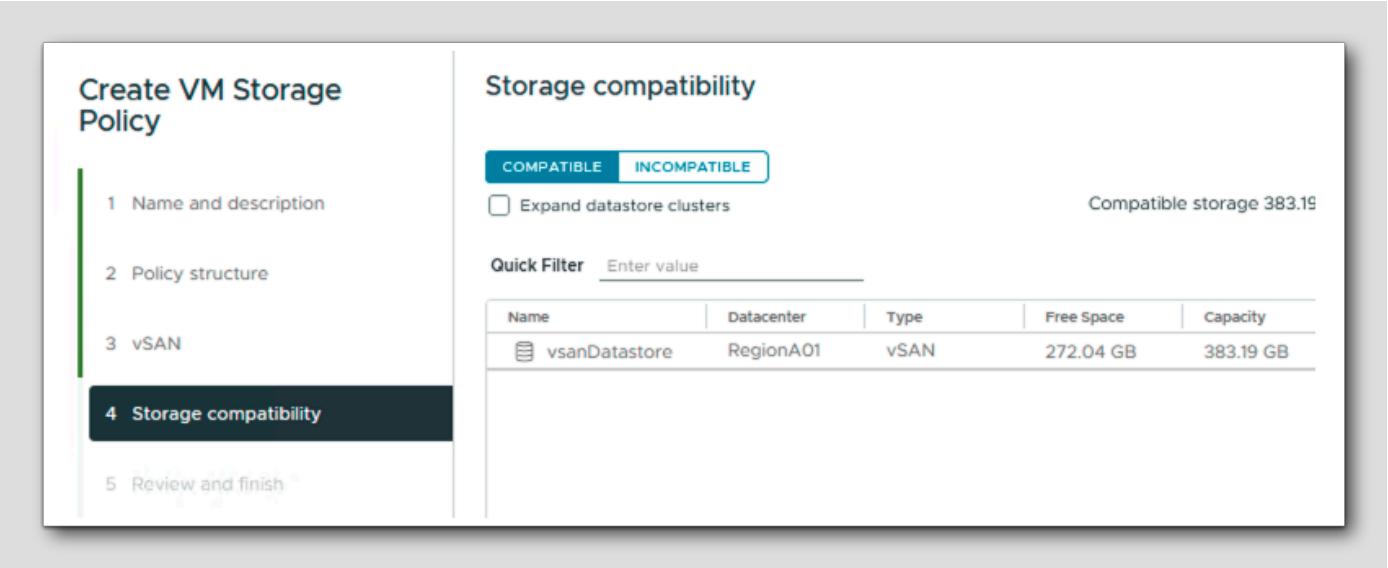
1. Select the following from the **Availability** tab.
2. Select the following options :

```
Site disaster tolerance : None - keep data on Preferred (stretched cluster)

Failures to tolerance : 1 failure - RAID-1 (Mirroring)
```

Storage Policy Based Management - Local Affinity

[277]



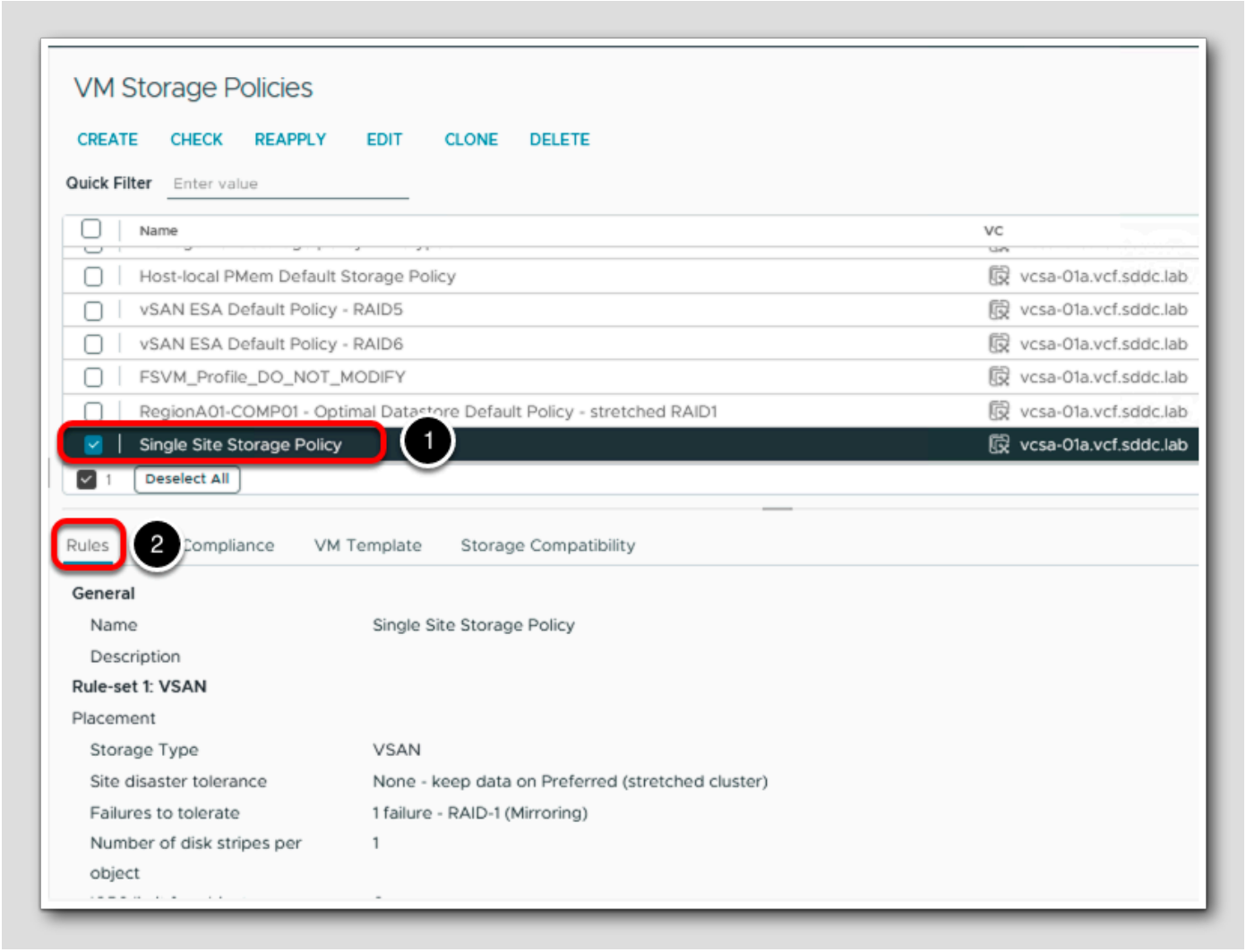
Verify that the **vsanDatastore** is Compatible

Click **NEXT** (not pictured)

At the Review and finish screen, click **FINISH**

Storage Policy Based Management - Local Affinity

[278]

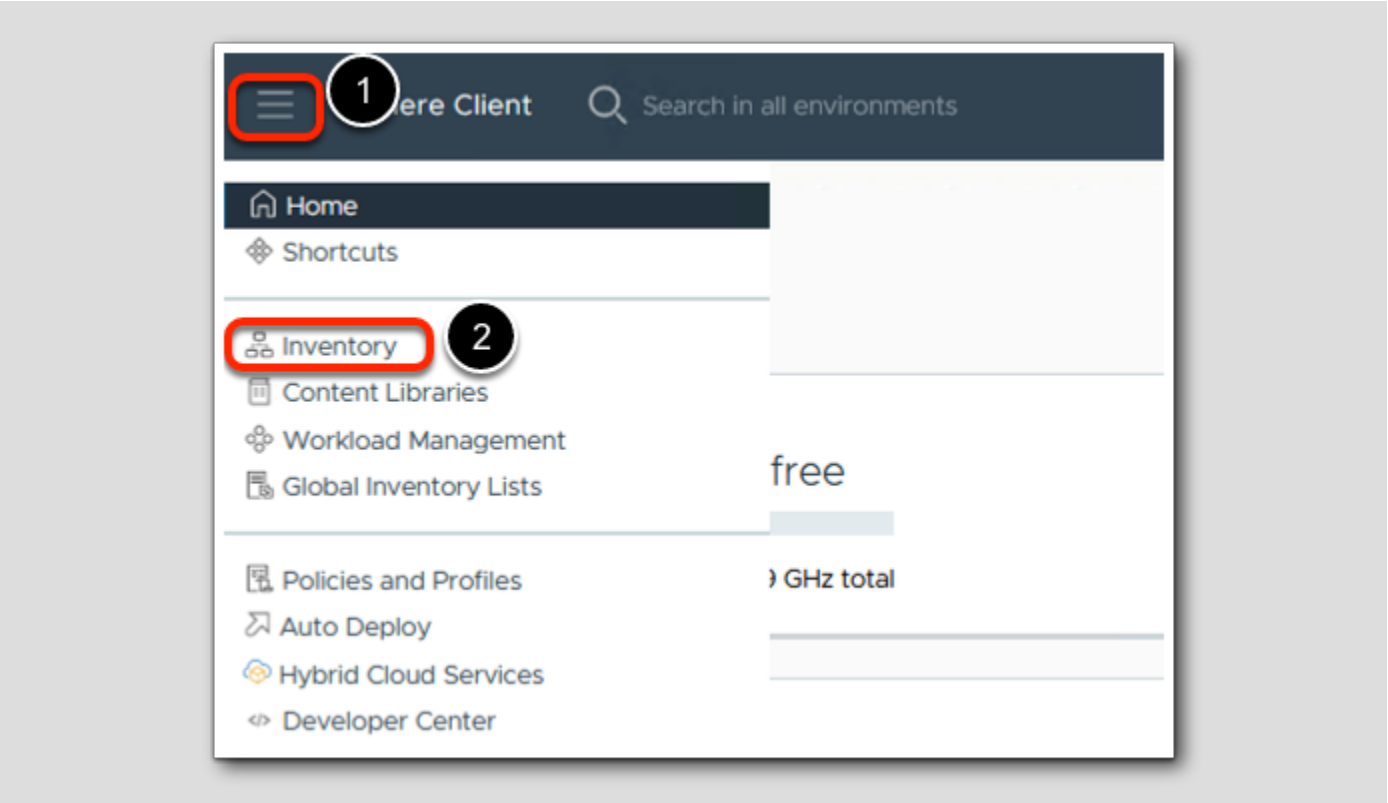


Verify the VM Storage Policy is created.

1. Scroll down and select the VM Storage Policy called **Single Site Storage Policy**
2. Review the Rules that you have created.

Create a VM with Local Affinity SPBM

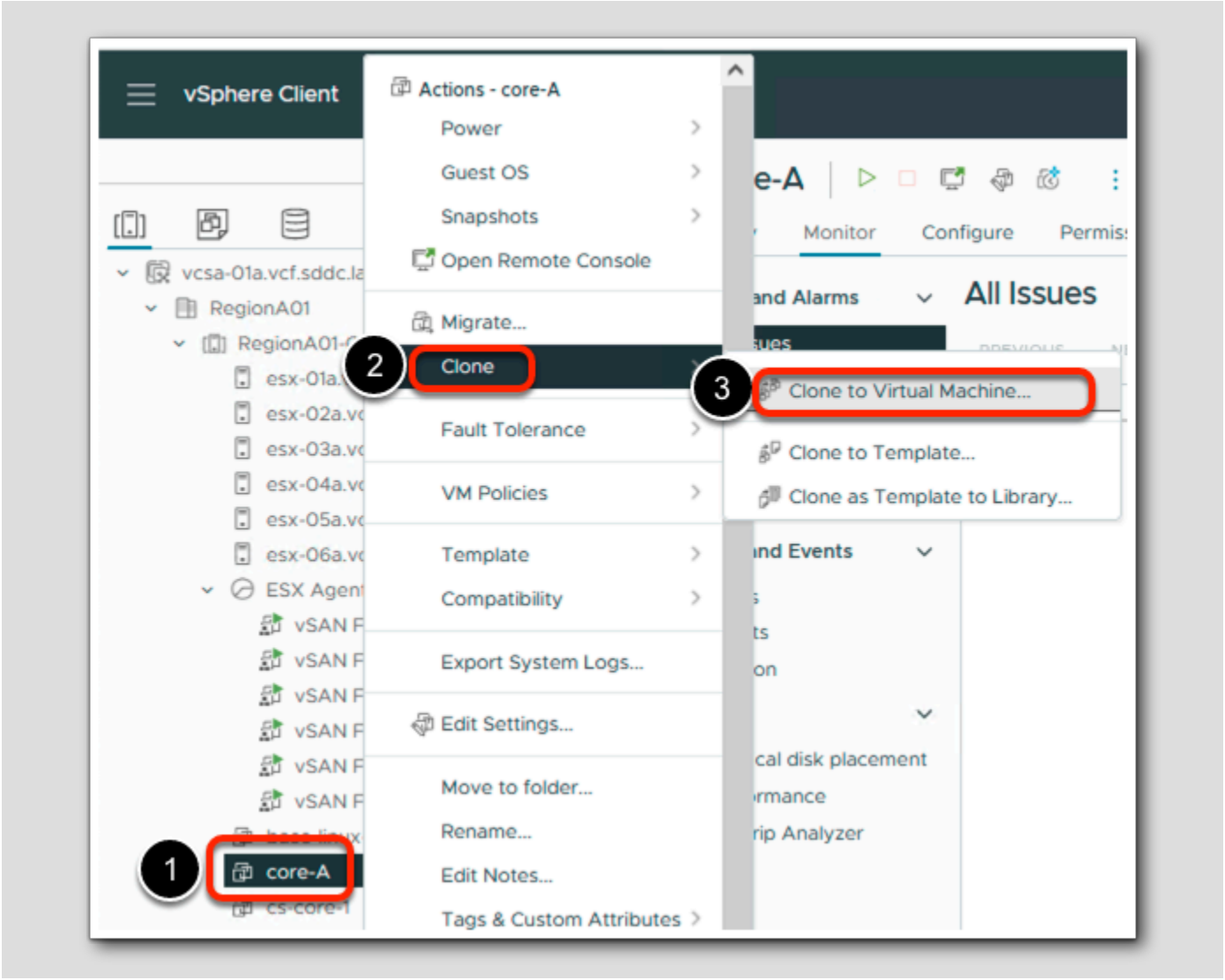
[279]



1. Click **Menu** (hamburger icon)
2. Select **Inventory**

Create a VM with Local Affinity SPBM

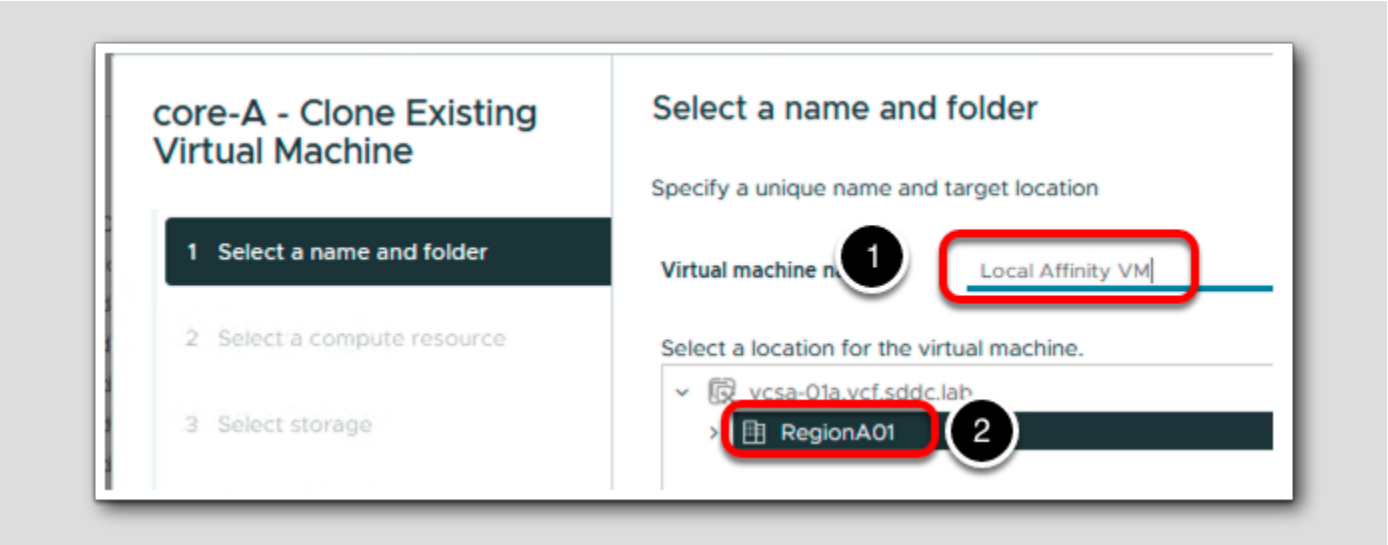
[280]



1. Right-click the VM called **core-A**
2. Select **Clone**
3. Select **Clone to Virtual Machine...**

Create a VM with Local Affinity SPBM

[281]



1. Give the VM a name, lets call it **Local Affinity VM**

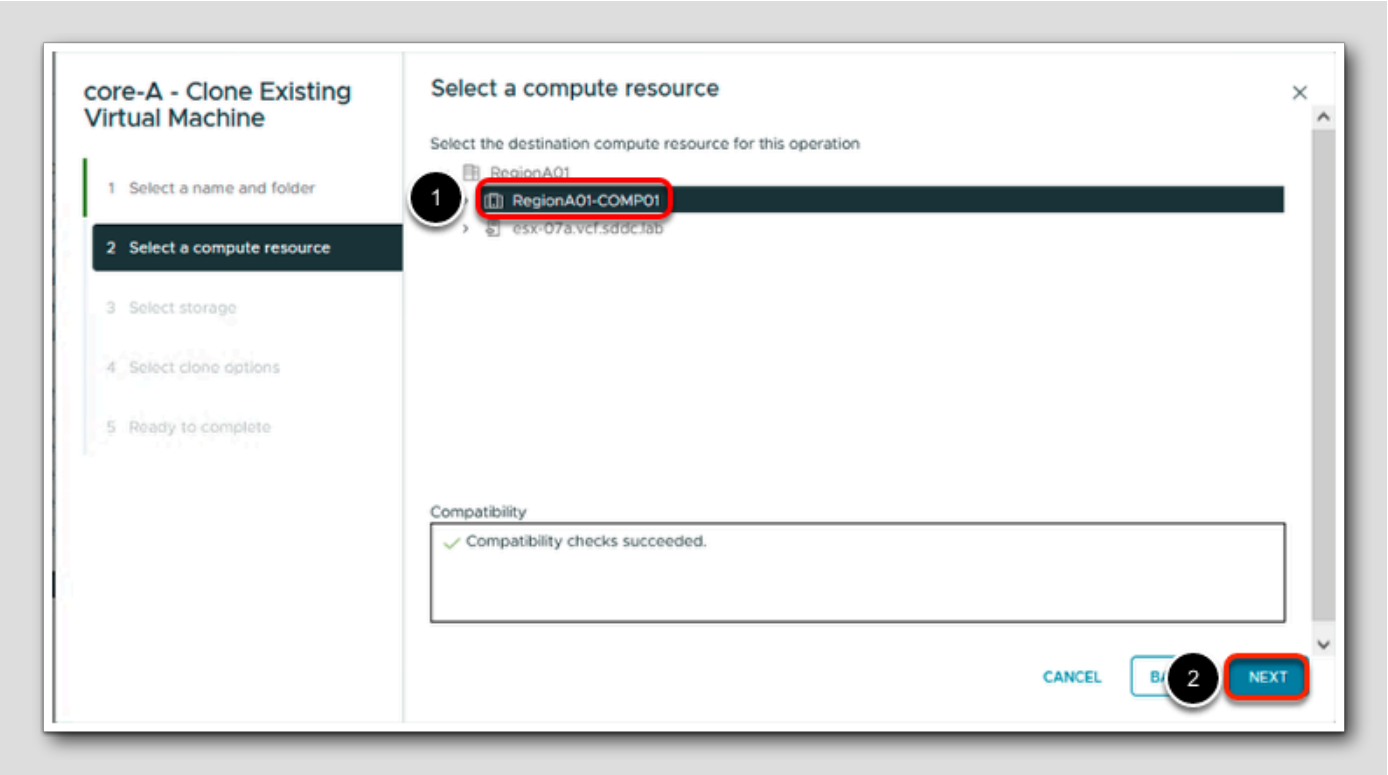
```
Local Affinity VM
```

2. Select the datacenter called **RegionA01**

Click **NEXT** (not pictured)

Create a VM with Local Affinity SPBM

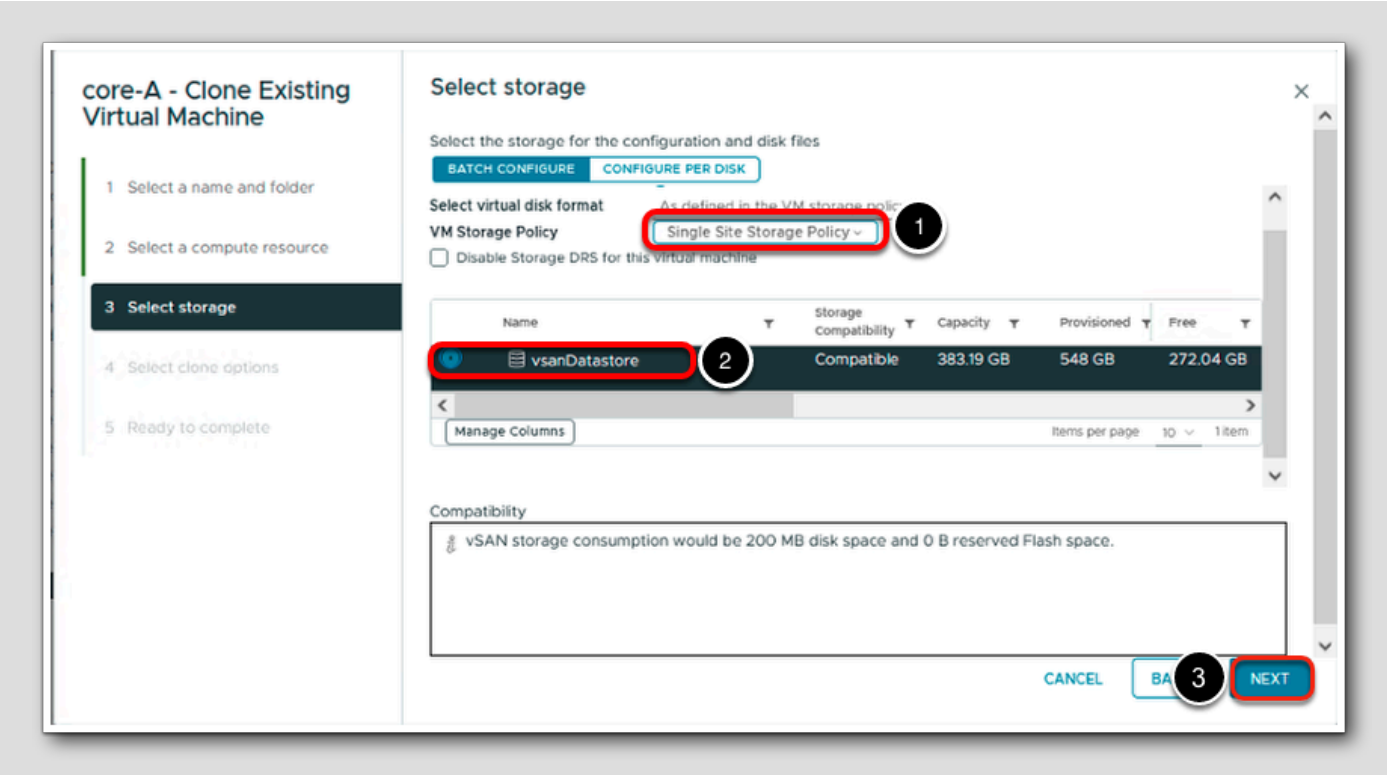
[282]



1. Select **RegionA01-COMP01**
2. Click **NEXT**

Create a VM with Local Affinity SPBM

[283]



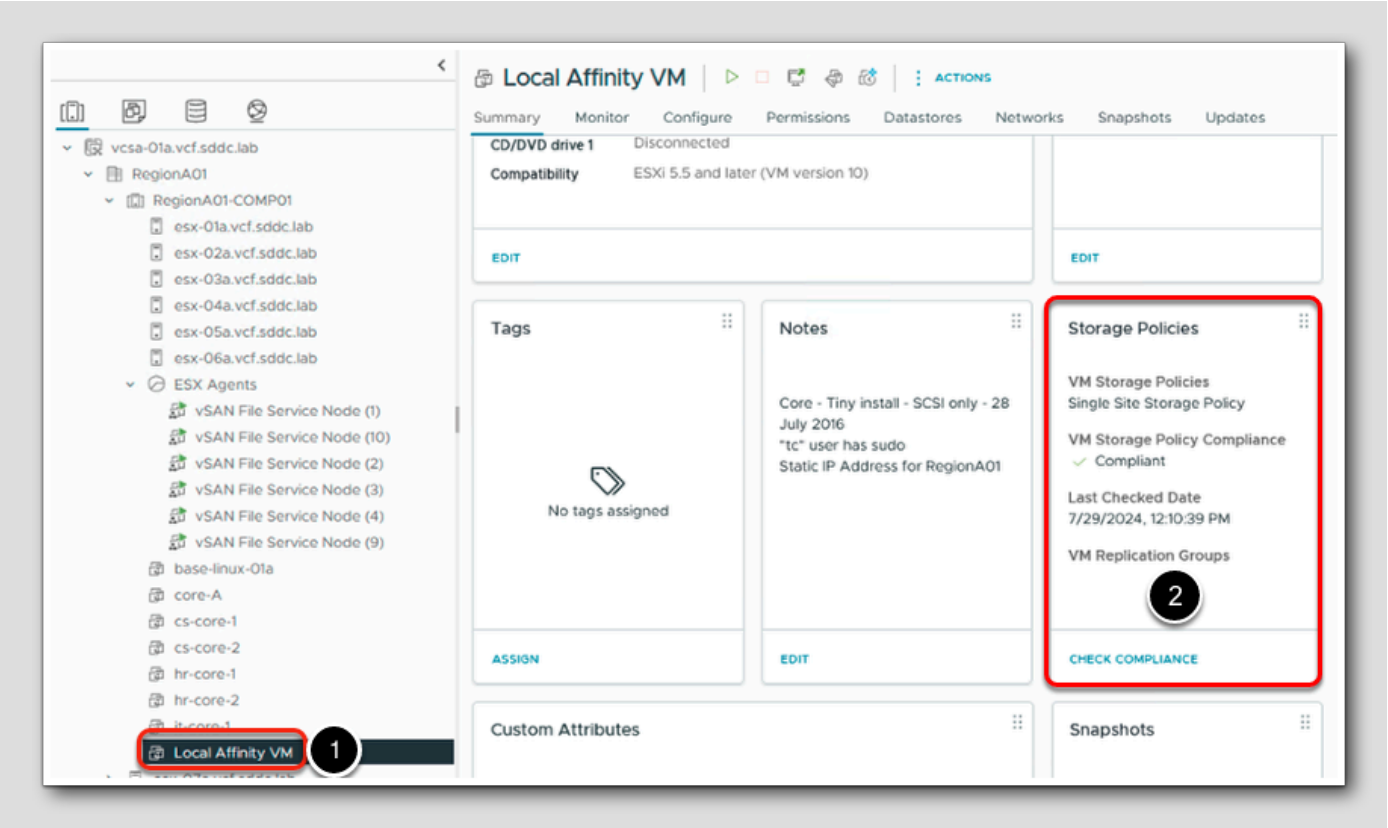
1. For the VM Storage policy, select **Single Site Storage Policy**
2. Select the **Stretched-vsanDatastore** which is compatible with this Storage Policy
3. Click **NEXT**

Click **NEXT** on the Clone options (not pictured)

At the **Ready to complete** click **FINISH** (not pictured)

Create a VM with Local Affinity SPBM

[284]

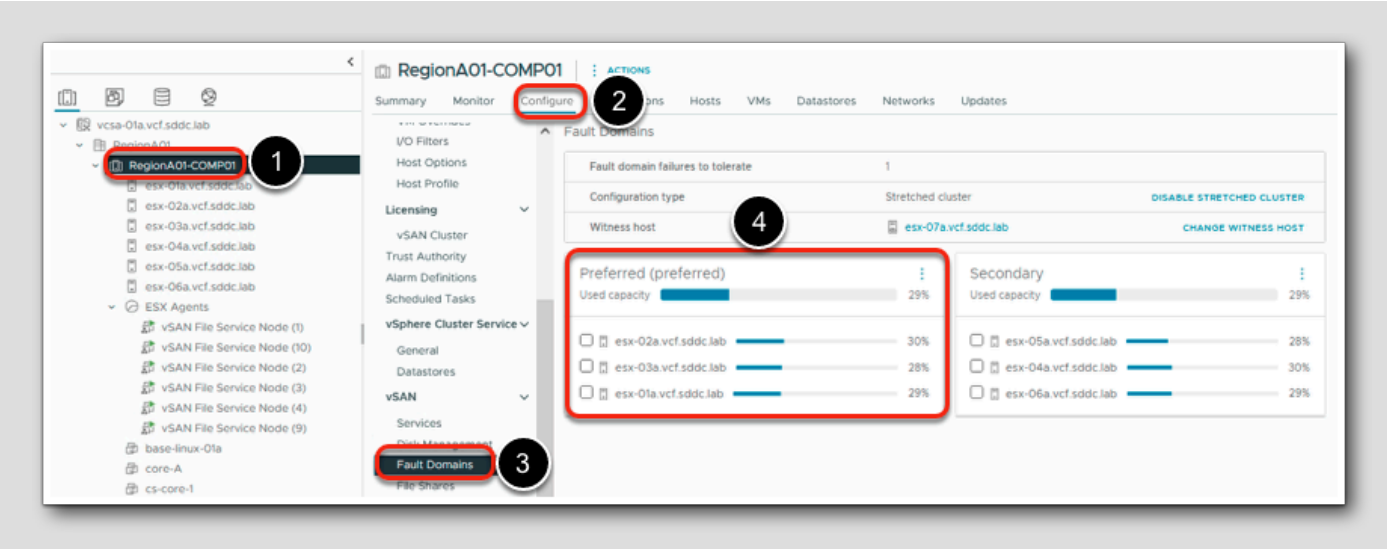


Verify that the Virtual Machine called **Local Affinity VM** has been created in the **Stretched-Cluster** in the Summary tab.

1. Once the cloning is complete, select **Local Affinity VM**
2. Verify that the VM Storage Policy called **Single Site Storage Policy** has been applied to the VM and the policy is **Compliant**.

vSAN Fault Domain

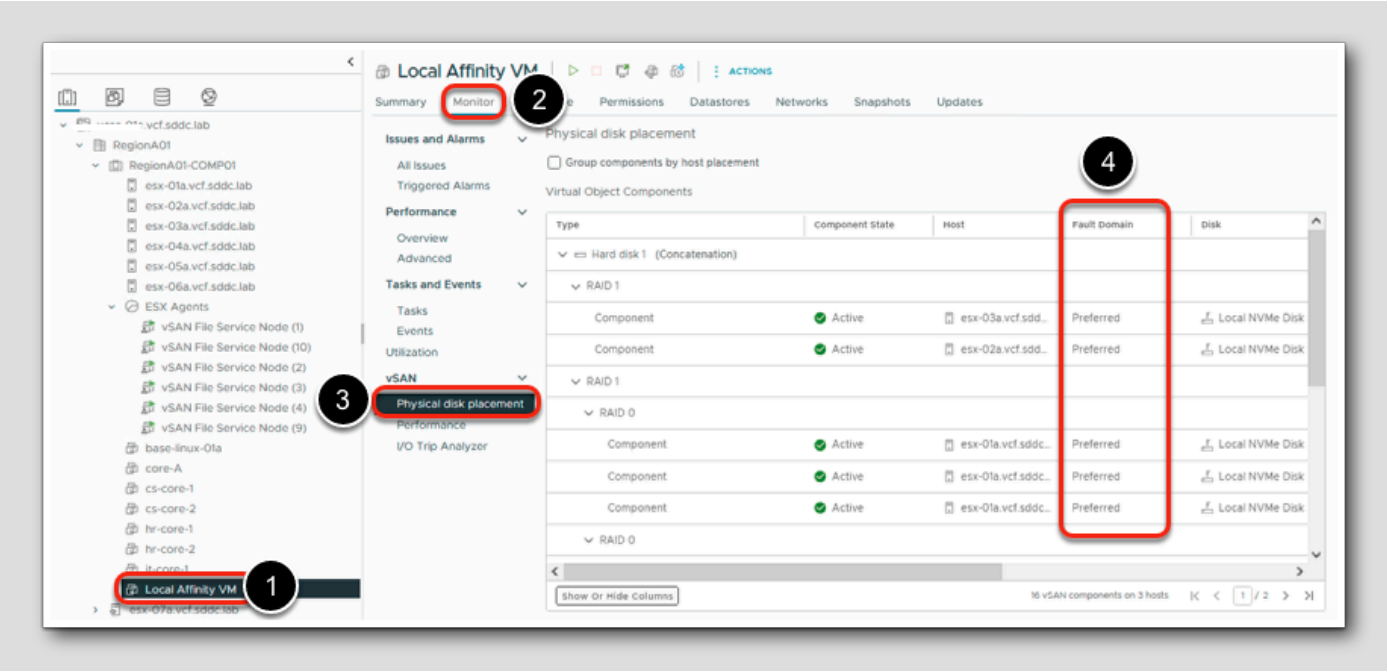
[285]



1. Select the cluster called **RegionA01-COMP01**
2. Select **Configure**
3. Select **vSAN > Fault Domains**
4. Note the Preferred fault domain and the ESXi hosts in the Preferred Fault Domain.

In the example shown here, the ESXi hosts called **esx-01a.vcf.sddc.lab, esx-02a.vcf.sddc.lab, and esx-03a.vcf.sddc.lab** are in the **Preferred fault domain**.

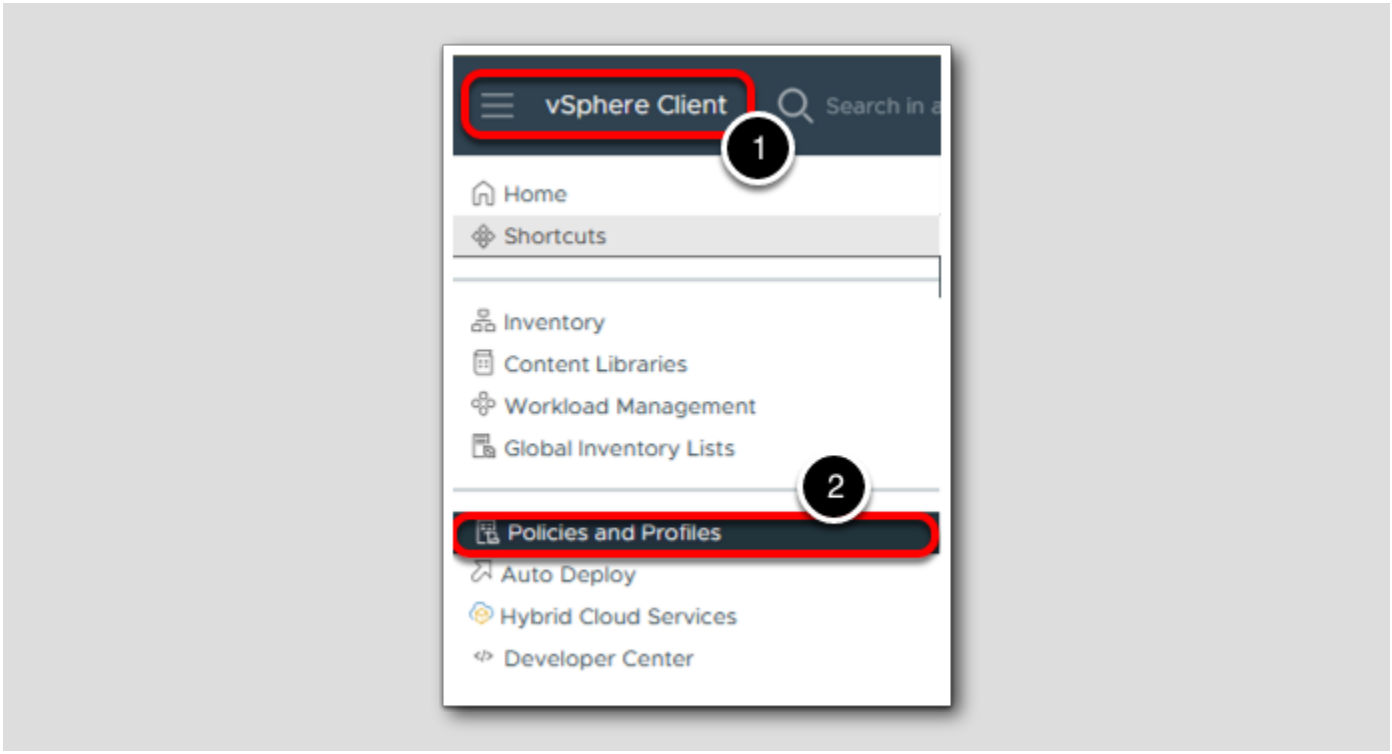
Policy Compliance



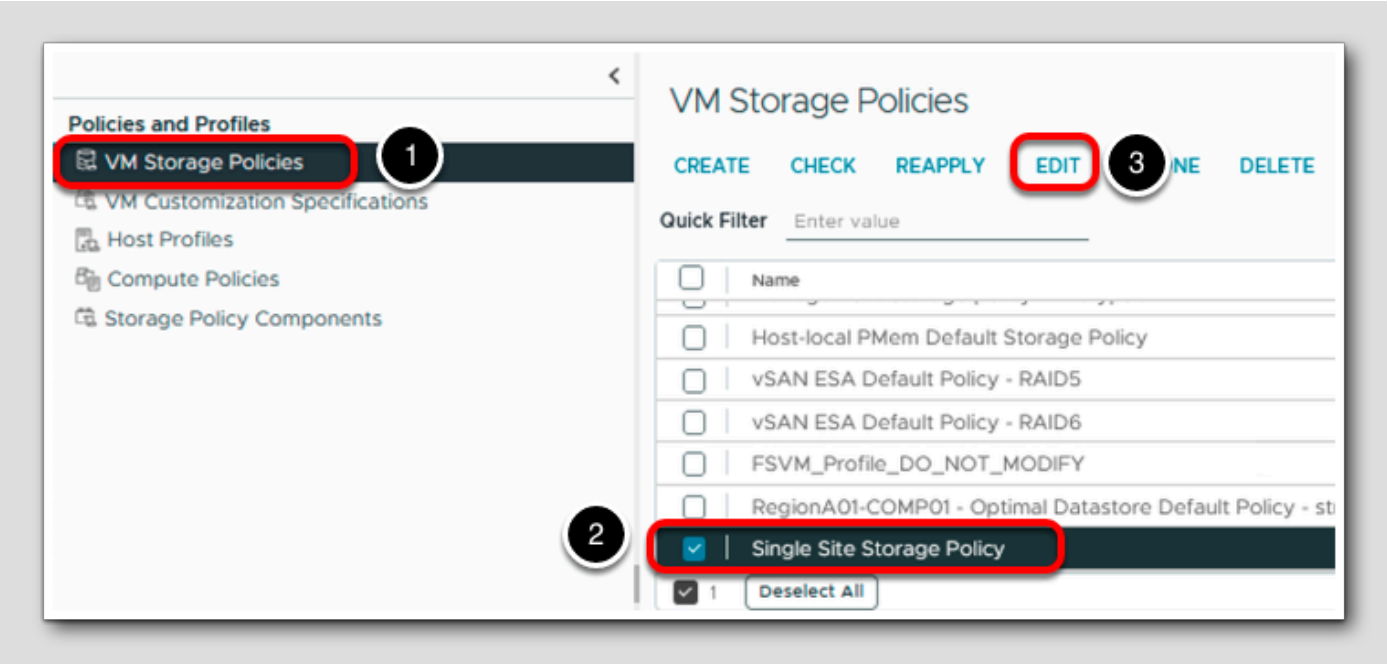
1. Select the VM called **Local Affinity VM**
2. Select **Monitor**
3. Select **vSAN > Physical disk placement**
4. Notice that the components have been placed on the **Preferred fault domain.**

Modify VM Storage Policy

[287]



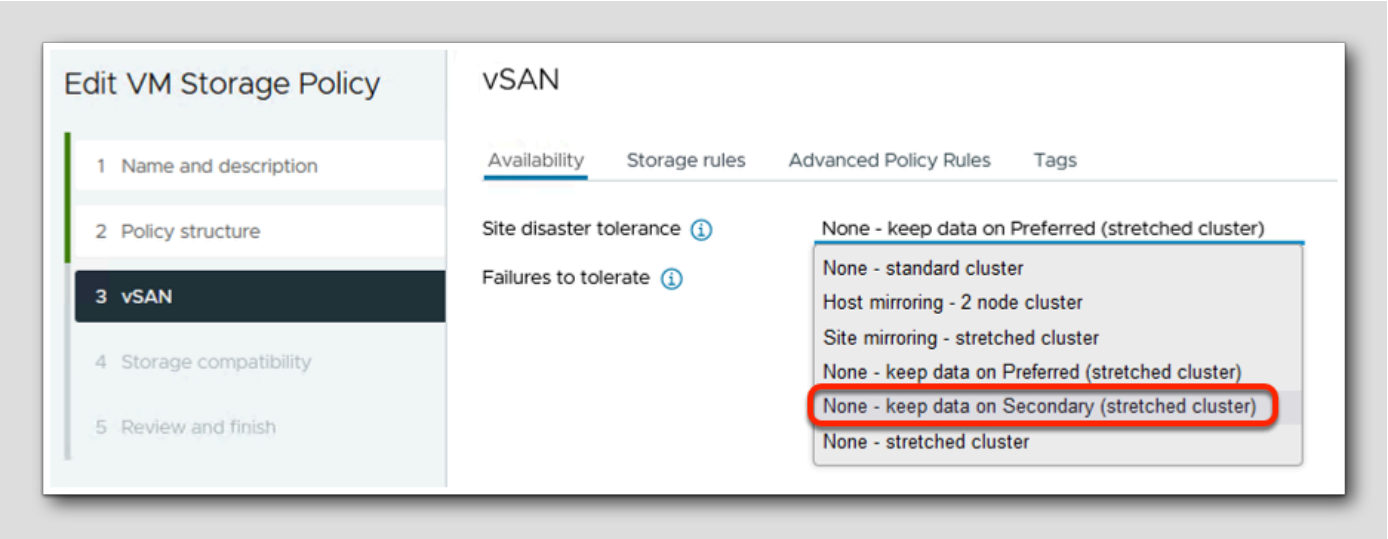
1. Click **Menu** of vSphere Client
2. Select **Policies and Profiles**



1. Select **VM Storage Policies**
2. Select **Single Site Storage Policy** (you may need to scroll down to see the policy)
3. Click **EDIT**

Modify VM Storage Policy

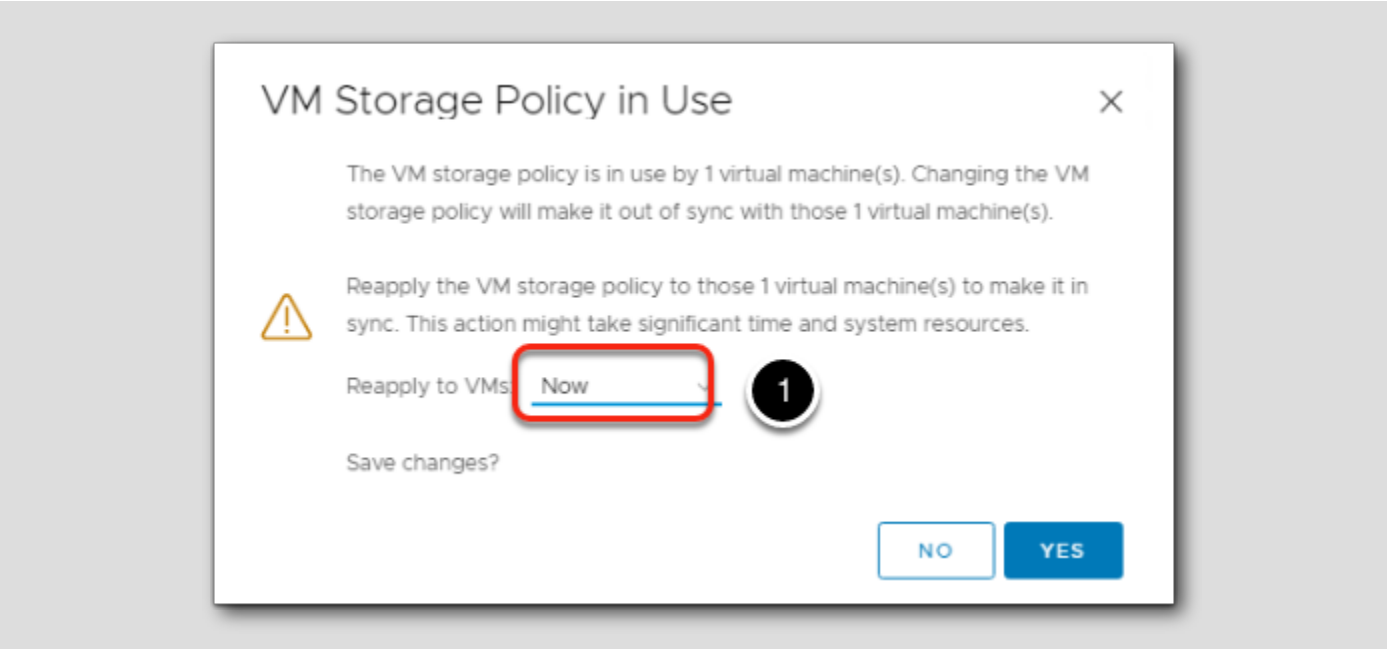
[288]



1. Click **NEXT** on Name and description (not pictured)
2. Click **NEXT** on Policy structure (not pictured)
3. On the vSAN Screen, for Site disaster tolerence, select **None - keep data on Secondary (stretched cluster)**
4. Click **NEXT** (not pictured)
5. Click **NEXT** (not pictured)
6. Click **FINISH** (not pictured)

Modify VM Storage Policy

[289]



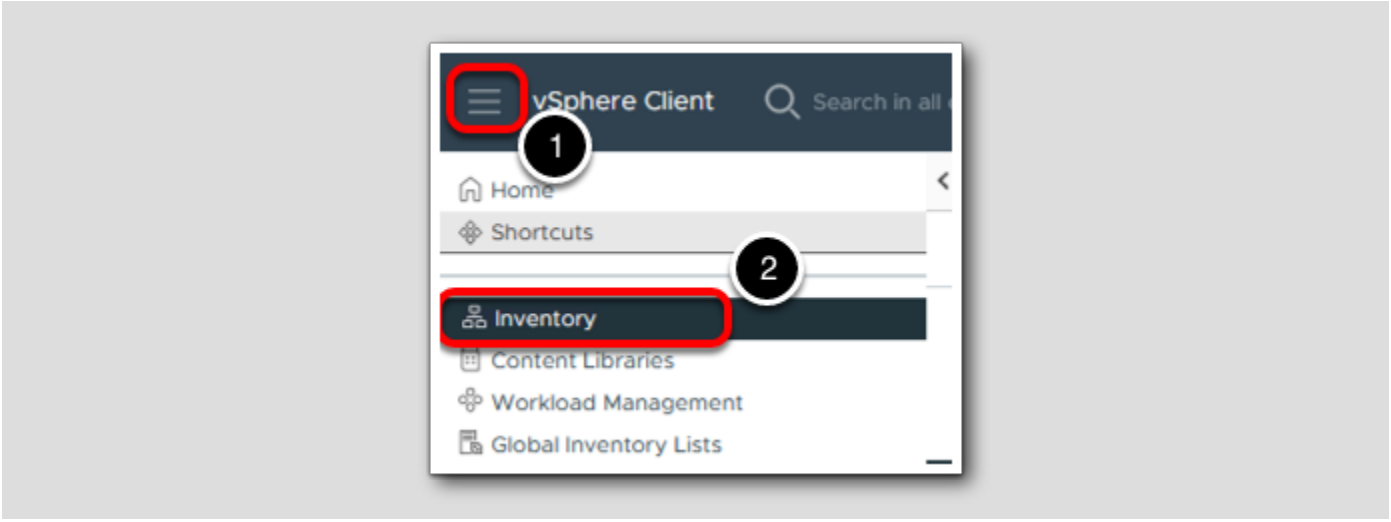
The VM storage Policy is already in use by some virtual machines. (optional page - depends if a VM is tied to this SPBM otherwise move to next step)

1. Change the **Reapply to VMs** to **Now**

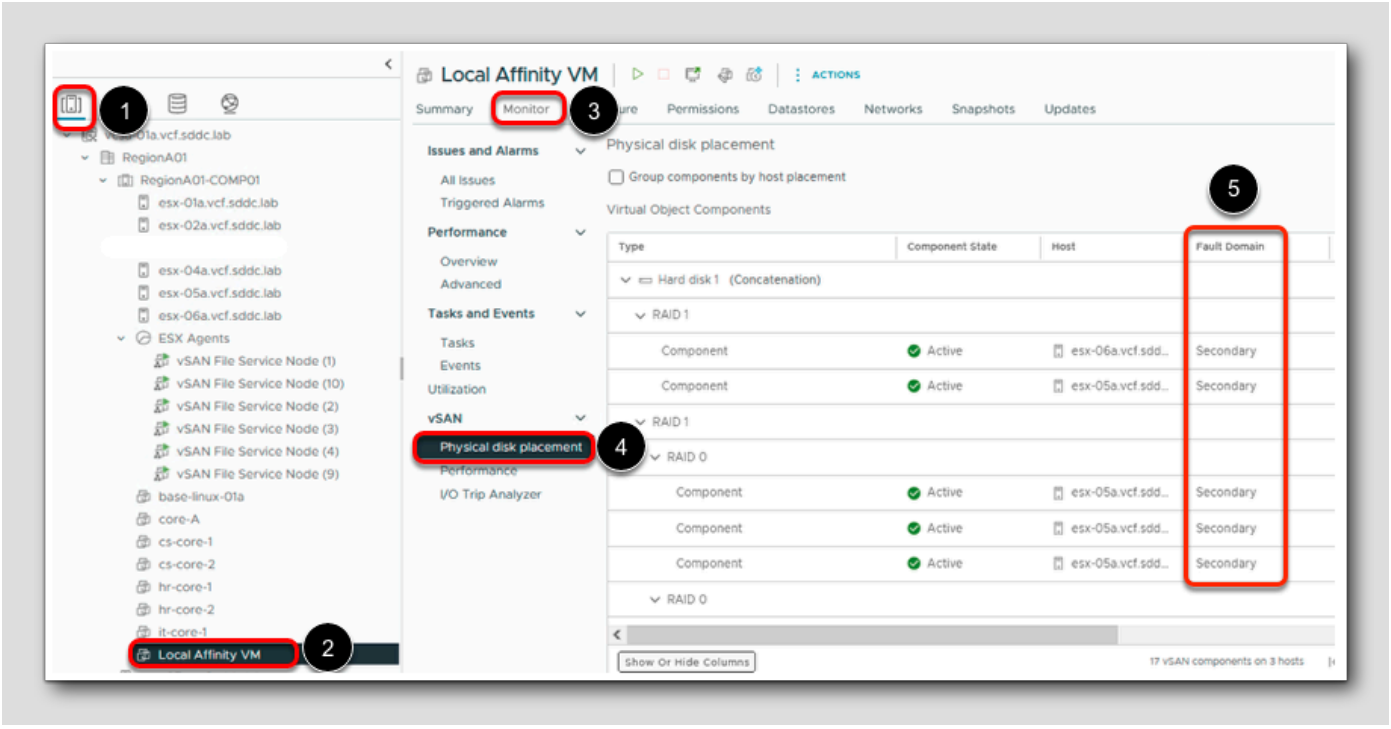
Click **YES** to save changes.

Verify VM Storage Policy

[290]



1. Click **Menu** of vSphere Client
2. Click **Inventory**



1. Select **Hosts and Clusters**
2. Select the VM called **Local Affinity VM**
3. Select **Monitor**
4. Select **vSAN > Physical disk placement**
5. Verify that the components are now on the **Secondary Fault Domain.**

Conclusion

[291]

In this lesson we looked at how to configure a vSAN Stretched Cluster. We gave you some background and some important features to understand before you configure your stretched vSAN Cluster environment.

Once of the features that we wanted to show here was the Witness and vSAN data separation. We showed you how to configure a Management VMKernel port for Witness traffic.

We then completed a vSAN Cluster Stretched Cluster configuration. In the end we showed you how to monitor the vSAN Health and how to run the vSAN Health Checks.

If you would like to take additional modules, please follow the links below:

- Module 1 - vSAN SPBM and Availability (30 minutes) (Basic) Introduction to VMware vSAN's Express Storage Architecture. We will cover the power of Storage Based Policy Management (SPBM) and show you the availability of vSAN.
- Module 2 - Monitoring, Health, Capacity, and Performance (30 minutes) (Basic) Show you how to enable Aria Operations within vCenter Server. We will cover the vSAN Health Check and how you can monitor your vSAN environment.
- Module 3 - vSAN Encryption and Security (30 minutes) (Advanced) Introduction to vSAN Encryption. We will enable a Key Management Server and demonstrate how to configure vSAN Encryption.
- Module 4 - File services (30 minutes) (Basic) Introduction to vSAN's File Services capabilities. We will create both NFS and SMB file shares and mount them to their respective clients.
- Module 5 - Data Protection (30 minutes) (Advanced) Introduction to vSAN ESA's new data protection capabilities. We will cover creating protection groups and snapshot schedules.

You've finished Module 3

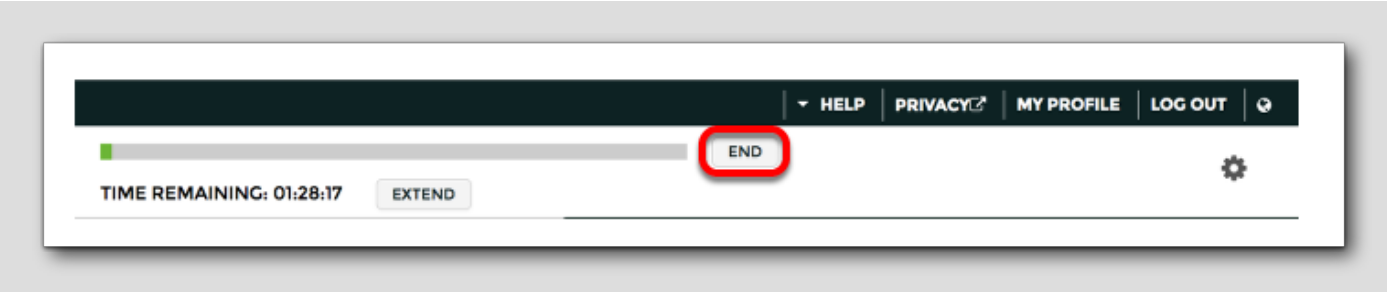
[292]

Additional information is available here on vSAN Clusters and vSAN Stretched Clusters :

- *VMware Blogs*
- *VMware vSAN*
- *vSAN on Youtube*

How to End Lab

[293]



If you would like to end your lab click on the **END** button.

Appendix

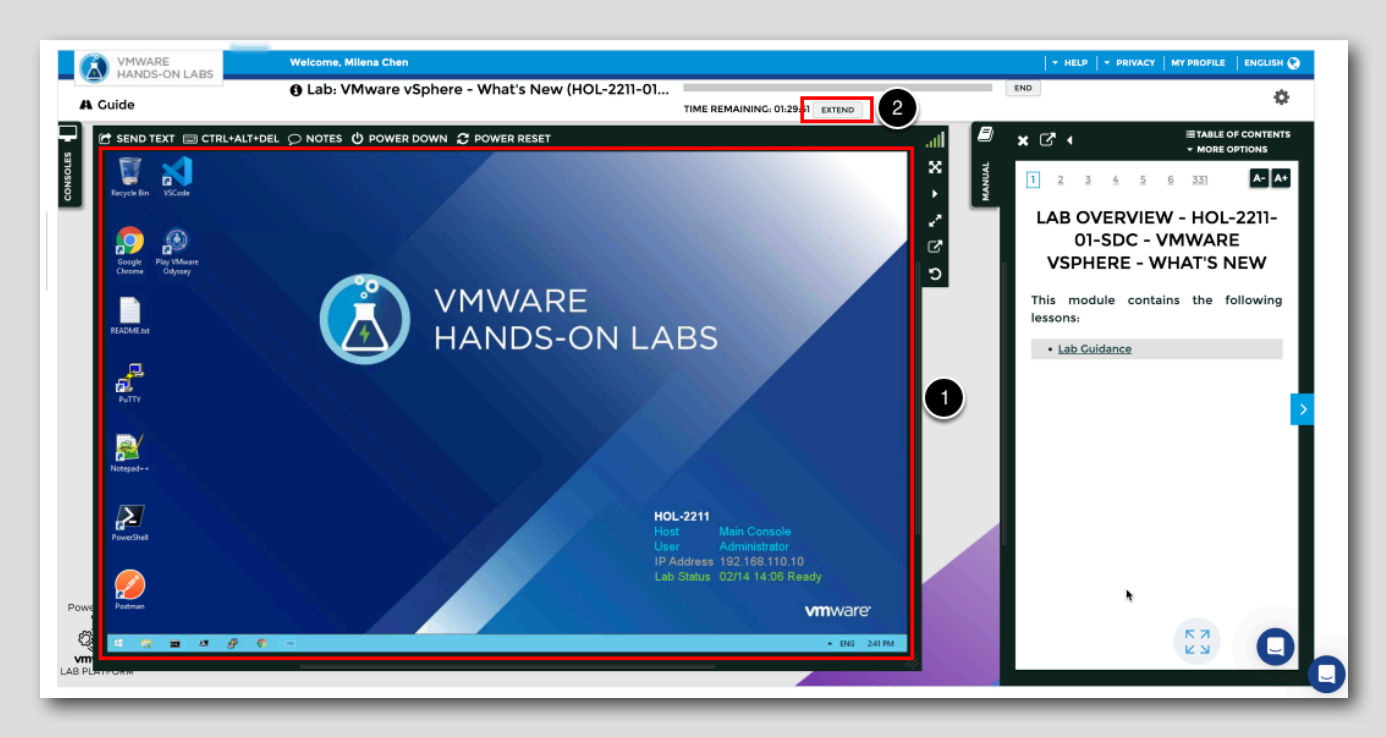
Hands-on Labs Interface

[295]

Welcome to Hands-on Labs! This overview of the interface and features will help you to get started quickly. Click next in the manual to explore the Main Console or use the Table of Contents to return to the Lab Overview page or another module.

Location of the Main Console

[296]



1. The area in the large RED box contains the Main Console. The Lab Manual is on the tab to the right of the Main Console.
2. Your lab starts with a timer. The lab cannot be saved and will end when the timer expires. Click the **EXTEND** button to increase the time allowed. The amount of time you can extend will depend on the lab.

Alternate Methods of Keyboard Data Entry

[297]

In this lab you will input text into the Main Console. Besides directly typing in the console, two alternate methods make it easier to enter complex data.

Click and Drag Lab Manual Content Into Console Active Window

[298]

https://www.youtube.com/watch?v=xS07n6GzGuo

You can 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

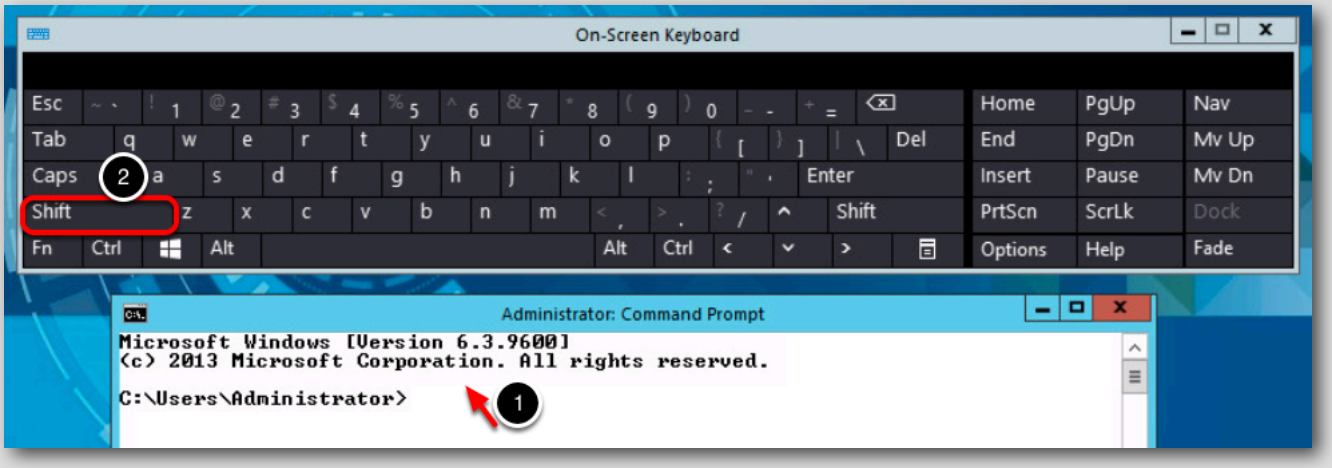
[299]

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

[300]

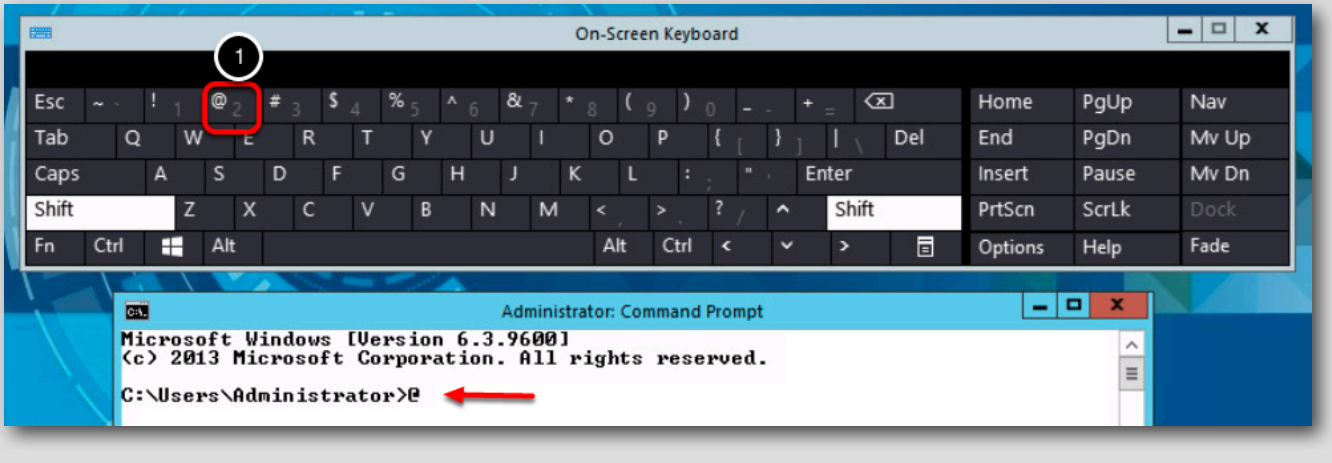


For example, to enter the "@" sign used in email addresses you can use the Online Keyboard. The "@" sign is Shift-2 on US keyboard layouts.

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

Click on the @ key

[301]



1. Click on the "@" key.

Notice the @ sign entered in the active console window.

Return to Lab Guidance

[302]

Use the Table of Contents to return to the Lab Overview page or another module.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.
 Lab SKU: HOL-2534-01-VCF-L Version: 20241105-121750