VMware Virtualization

NetApp Solutions

NetApp
September 22, 2024

Table of Contents

NetApp Solutions for Virtualization with VMware by Broadcom

VMware vSphere with ONTAP

ONTAP has been a leading storage solution for VMware vSphere environments for almost two decades and continues to add innovative capabilities to simplify management while reducing costs. This document introduces the ONTAP solution for vSphere, including the latest product information and best practices, to streamline deployment, reduce risk, and simplify management.

For more information, visit VMware vSphere with ONTAP

VMware vSphere Foundation

NFS v3 Reference Guide for vSphere 8

VMware vSphere Foundation (VVF) is an enterprise-grade platform capable of delivering various virtualized workloads. Core to vSphere are VMware vCenter, the ESXi hypervisor, networking components, and various resource services. When combined with ONTAP, VMware-powered virtualized infrastructures exhibit remarkable flexibility, scalability, and capability.

Using NFS v3 with vSphere 8 and ONTAP Storage Systems

This document provides information on storage options available for VMware Cloud vSphere Foundation using the NetApp All-Flash Arrays. Supported storage options are covered with specific instruction for deploying NFS datastores. Additionally, VMware Live Site Recovery for Disaster Recovery of NFS datastores is demonstrated. Finally, NetApp's Autonomous Ransomware Protection for NFS storage is reviewed.

Use Cases

Use cases covered in this documentation:

- Storage options for customers seeking uniform environments across both private and public clouds.
- Deployment of virtual infrastructure for workloads.
- Scalable storage solution tailored to meet evolving needs, even when not aligned directly with compute resource requirements.
- Protect VMs and datastores using the SnapCenter Plug-in for VMware vSphere.
- Use of VMware Live Site Recovery for Disaster Recovery of NFS datastores.
- Ransomware detection strategy, including multiple layers of protection at ESXi host and guest VM levels.

Audience

This solution is intended for the following people:

- Solution architects looking for more flexible storage options for VMware environments that are designed to maximize TCO.

- Solution architects looking for VVF storage options that provide data protection and disaster recovery options with the major cloud providers.
- Storage administrators wanting specific instruction on how to configure VVF with NFS storage.
- Storage administrators wanting specific instruction on how to protect VMs and datastores residing on ONTAP storage.

Technology Overview

The NFS v3 VVF Reference Guide for vSphere 8 is comprised of the following major components:

VMware vSphere Foundation

A central component of vSphere Foundation, VMware vCenter is a centralized management platform for providing configuration, control and administration of vSphere environments. vCenter acts as the base for managing virtualized infrastructures, allowing administrators to deploy, monitor and manage VMs, containers, and ESXi hosts within the virtual environment.

The VVF solution supports both native Kubernetes and virtual machine-based workloads. Key components include:

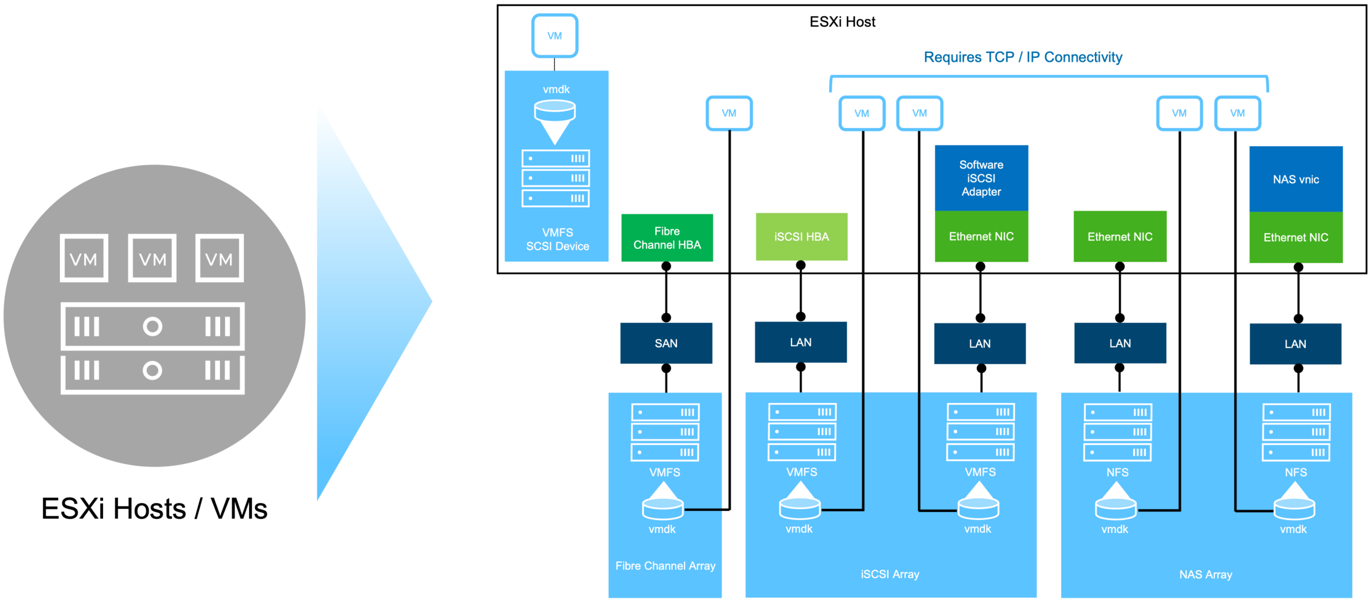
- VMware vSphere
- VMware vSAN
- Aria Standard
- VMware Tanzu Kubernetes Grid Service for vSphere
- vSphere Distributed Switch

For more information on VVF included components, refer to architecture and planning, refer to VMware vSphere Product Live Comparison.

VVF Storage Options

Central to a successful and powerful virtual environment is storage. Storage whether through VMware datastores or guest-connected use cases, unlocks the capabilities of your workloads as you can pick the best price per GB that delivers the most value while also reducing underutilization. ONTAP has been a leading storage solution for VMware vSphere environments for almost two decades and continues to add innovative capabilities to simplify management while reducing costs.

VMware storage options are typically organized as traditional storage and software defined storage offerings. Traditional storage models include local and networked storage while software-defined storage models include vSAN and VMware Virtual Volumes (vVols).



Refer to Introduction to Storage in vSphere Environment for more information on supported storage types for VMware vSphere Foundation.

NetApp ONTAP

There are numerous compelling reasons why tens of thousands of customers have chosen ONTAP as their primary storage solution for vSphere. These include the following:

1. **Unified Storage System:** ONTAP offers a unified storage system that supports both SAN and NAS protocols. This versatility allows for seamless integration of various storage technologies within a single solution.
2. **Robust Data Protection:** ONTAP provides robust data protection capabilities through space-efficient snapshots. These snapshots enable efficient backup and recovery processes, ensuring the safety and integrity of application data.
3. **Comprehensive Management Tools:** ONTAP offers a wealth of tools designed to assist in managing application data effectively. These tools streamline storage management tasks, enhancing operational efficiency and simplifying administration.
4. **Storage efficiency:** ONTAP includes several storage efficiency features, enabled by default, designed to optimized storage utilization, reduce costs and enhance overall system performance.

Using ONTAP with VMware affords great flexibility when it comes to given application needs. The following protocols are supported as VMware datastore with using ONTAP:
* FCP
* FCoE
* NVMe/FC
* NVMe/TCP
* iSCSI
* NFS v3
* NFS v4.1

Using a storage system separate from the hypervisor allows you to offload many functions and maximize your investment in vSphere host systems. This approach not only makes sure your host resources are focused on application workloads, but it also avoids random performance effects on applications from storage operations.

Using ONTAP together with vSphere is a great combination that lets you reduce host hardware and VMware software expenses. You can also protect your data at lower cost with consistent high performance. Because virtualized workloads are mobile, you can explore different approaches using Storage vMotion to move VMs across VMFS, NFS, or vVols datastores, all on the same storage system.

NetApp All-Flash Arrays

NetApp AFF (All Flash FAS) is a product line of all-flash storage arrays. It is designed to deliver high-performance, low-latency storage solutions for enterprise workloads. The AFF series combines the benefits of flash technology with NetApp's data management capabilities, providing organizations with a powerful and efficient storage platform.

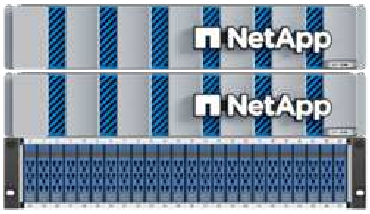
The AFF lineup is comprised of both A-Series and C-Series models.

The NetApp A-Series all-NVMe flash arrays are designed for high-performance workloads, offering ultra-low latency and high resiliency, making them suitable for mission-critical applications.

AFF A70

AFF A90

AFF A1K



C-Series QLC flash arrays are aimed at higher-capacity use cases, delivering the speed of flash with the economy of hybrid flash.

AFF C250

AFF C400

AFF C800

Storage Protocol Support

The AFF support all standard protocols used for virtualization, both datastores and guest connected storage, including NFS, SMB, iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), NVME over fabrics and S3. Customers are free to choose what works best for their workloads and applications.

NFS - NetApp AFF provides support for NFS, allowing for file-based access of VMware datastores. NFS-connected datastores from many ESXi hosts, far exceeds the limits imposed on VMFS file systems. Using NFS with vSphere provides some ease of use and storage efficiency visibility benefits. ONTAP includes file access features available for the NFS protocol. You can enable an NFS server and export volumes or qtrees.

For design guidance on NFS configurations, refer to the NAS storage management documentation.

iSCSI - NetApp AFF provides robust support for iSCSI, allowing block-level access to storage devices over IP networks. It offers seamless integration with iSCSI initiators, enabling efficient provisioning and management of iSCSI LUNs. ONTAP's advanced features, such as multi-pathing, CHAP authentication, and ALUA support.

For design guidance on iSCSI configurations refer to the SAN Configuration reference documentation.

Fibre Channel - NetApp AFF offers comprehensive support for Fibre Channel (FC), a high-speed network technology commonly used in storage area networks (SANs). ONTAP seamlessly integrates with FC infrastructure, providing reliable and efficient block-level access to storage devices. It offers features like zoning, multi-pathing, and fabric login (FLOGI) to optimize performance, enhance security, and ensure seamless connectivity in FC environments.

For design guidance on Fibre Channel configurations refer to the SAN Configuration reference documentation.

NVMe over Fabrics - NetApp ONTAP support NVMe over fabrics. NVMe/FC enables the use of NVMe storage devices over Fibre Channel infrastructure, and NVMe/TCP over storage IP networks.

For design guidance on NVMe refer to NVMe configuration, support and limitations.

Active-active technology

NetApp All-Flash Arrays allows for active-active paths through both controllers, eliminating the need for the host operating system to wait for an active path to fail before activating the alternative path. This means that the host can utilize all available paths on all controllers, ensuring active paths are always present regardless of whether the system is in a steady state or undergoing a controller failover operation.

For more information, see Data Protection and disaster recovery documentation.

Storage guarantees

NetApp offers a unique set of storage guarantees with NetApp All-flash Arrays. The unique benefits include:

Storage efficiency guarantee: Achieve high performance while minimizing storage cost with the Storage Efficiency Guarantee. 4:1 for SAN workloads.
Ransomware recovery guarantee: Guaranteed data recovery in the event of a ransomware attack.

For detailed information see the NetApp AFF landing page.

NetApp ONTAP Tools for VMware vSphere

A powerful component of vCenter is the ability to integrate plug-ins or extensions that further enhance its functionality and provide additional features and capabilities. These plug-ins extend the management capabilities of vCenter and allow administrators to integrate 3rd party solutions, tools and services into their vSphere environment.

NetApp ONTAP tools for VMware is a comprehensive suite of tools designed to facilitate virtual machine lifecycle management within VMware environments via its vCenter Plug-in architecture. These tools seamlessly integrate with the VMware ecosystem, enabling efficient datastore provisioning and delivering essential protection for virtual machines. With ONTAP Tools for VMware vSphere, administrators can effortlessly manage storage lifecycle management tasks.

Comprehensive ONTAP tools 10 resources can be found ONTAP tools for VMware vSphere Documentation Resources.

View the ONTAP tools 10 deployment solution at Use ONTAP tools 10 to configure NFS datastores for vSphere 8

NetApp NFS Plug-in for VMware VAAI

The NetApp NFS Plug-in for VAAI (vStorage APIs for Array Integration) enhances storage operations by offloading certain tasks to the NetApp storage system, resulting in improved performance and efficiency. This includes operations such as full copy, block zeroing, and hardware-assisted locking. Additionally, the VAAI plugin optimizes storage utilization by reducing the amount of data transferred over the network during virtual machine provisioning and cloning operations.

The NetApp NFS Plug-in for VAAI can be downloaded from the NetApp support site and is uploaded and installed on ESXi hosts using ONTAP tools for VMware vSphere.

Refer to NetApp NFS Plug-in for VMware VAAI Documentation for more information.

SnapCenter Plug-in for VMware vSphere

The SnapCenter Plug-in for VMware vSphere (SCV) is a software solution from NetApp that offers comprehensive data protection for VMware vSphere environments. It is designed to simplify and streamline the process of protecting and managing virtual machines (VMs) and datastores. SCV uses storage based snapshot and replication to secondary arrays to meet lower recovery time objectives.

The SnapCenter Plug-in for VMware vSphere provides the following capabilities in a unified interface, integrated with the vSphere client:

Policy-Based Snapshots - SnapCenter allows you to define policies for creating and managing application-consistent snapshots of virtual machines (VMs) in VMware vSphere.

Automation - Automated snapshot creation and management based on defined policies help ensure consistent and efficient data protection.

VM-Level Protection - Granular protection at the VM level allows for efficient management and recovery of individual virtual machines.

Storage Efficiency Features - Integration with NetApp storage technologies provides storage efficiency features like deduplication and compression for snapshots, minimizing storage requirements.

The SnapCenter Plug-in orchestrates the quiescing of virtual machines in conjunction with hardware-based snapshots on NetApp storage arrays. SnapMirror technology is utilized to replicate copies of backups to secondary storage systems including in the cloud.

For more information refer to the SnapCenter Plug-in for VMware vSphere documentation.

BlueXP integration enables 3-2-1 backup strategies that extend copies of data to object storage in the cloud.

For more information on 3-2-1 backup strategies with BlueXP visit 3-2-1 Data Protection for VMware with SnapCenter Plug-in and BlueXP backup and recovery for VMs.

For step-by-step deployment instructions for the SnapCenter Plug-in, refer to the solution Use SnapCenter Plug-in for VMware vSphere to protect VMs on VCF Workload Domains.

Storage considerations

Leveraging ONTAP NFS datastores with VMware vSphere yields a high-performing, easy-to-manage, and scalable environment that provides VM-to-datastore ratios unattainable with block-based storage protocols. This architecture can result in a tenfold increase in datastore density, accompanied by a corresponding reduction in the number of datastores.

nConnect for NFS: Another benefit of using NFS is the ability to leverage the **nConnect** feature. nConnect enables multiple TCP connections for NFS v3 datastore volumes, thereby achieving higher throughput. This helps increase parallelism and for NFS datastores. Customers deploying datastores with NFS version 3 can increase the number of connections to the NFS server, maximizing the utilization of high-speed network interface cards.

For detailed information on nConnect, refer to NFS nConnect Feature with VMware and NetApp.

Session trunking for NFS: Starting from ONTAP 9.14.1, clients using NFSv4.1 can leverage session trunking to establish multiple connections to various LIFs on the NFS server. This enables faster data transfer and enhances resilience by utilizing multipathing. Trunking proves particularly beneficial when exporting FlexVol volumes to clients that support trunking, such as VMware and Linux clients, or when using NFS over RDMA, TCP, or pNFS protocols.

Refer to NFS trunking overview for more information.

FlexVol volumes: NetApp recommends using **FlexVol** volumes for most NFS datastores. While larger datastores can enhance storage efficiency and operational benefits, it is advisable to consider using at least four datastores (FlexVol volumes) to store VMs on a single ONTAP controller. Typically, administrators deploy datastores backed by FlexVol volumes with capacities ranging from 4TB to 8TB. This size strikes a good balance between performance, ease of management, and data protection. Administrators can start small and scale the datastore as needed (up to a maximum of 100TB). Smaller datastores facilitate faster recovery from backups or disasters and can be swiftly moved across the cluster. This approach allows for maximum performance utilization of hardware resources and enables datastores with different recovery policies.

FlexGroup volumes: For scenarios requiring a large datastore, NetApp recommends the use of **FlexGroup** volumes. FlexGroup volumes have virtually no capacity or file count constraints, enabling administrators to easily provision a massive single namespace. Using FlexGroup volumes does not entail additional maintenance or management overhead. Multiple datastores are not necessary for performance with FlexGroup volumes, as they scale inherently. By utilizing ONTAP and FlexGroup volumes with VMware vSphere, you can establish simple and scalable datastores that leverage the full power of the entire ONTAP cluster..

Ransomware protection

NetApp ONTAP data management software features a comprehensive suite of integrated technologies to help you protect, detect, and recover from ransomware attacks. The
NetApp SnapLock Compliance feature built into ONTAP prevents the deletion of data stored in an enabled volume using WORM (write once, read many) technology with
advanced data retention. After the retention period is established and the Snapshot copy is locked, not even a storage administrator with full system privileges or a member of the NetApp Support team can delete the Snapshot copy. But, more importantly, a hacker with compromised credentials can’t delete the data.

NetApp guarantees that we will be able to recover your protected NetApp® Snapshot™ copies on eligible arrays, and if we can’t, we will compensate your organization.

More information about the Ransomware Recovery Guarantee, see: Ransomeware Recovery Guarantee.

Refer to the Autonomous Ransomware Protection overview for more in depth information.

See the the full solution at the NetApps Solutions documentation center: Autonomous Ransomware Protection for NFS Storage

Disaster recovery considerations

NetApp provides the most secure storage on the planet. NetApp can help protect data and application infrastructure, move data between on-premises storage and cloud, and help ensure data availability across clouds. ONTAP comes with powerful data protection and security technologies that help protect customers from disasters by proactively detecting threats and quickly recovering data and applications.

VMware Live Site Recovery, formerly known as VMware Site Recovery Manager, offers streamlined, policy-based automation for protecting virtual machines within the vSphere web client. This solution leverages NetApp's advanced data management technologies through the Storage Replication Adapter as part of ONTAP Tools for VMware. By harnessing the capabilities of NetApp SnapMirror for array-based replication, VMware environments can benefit from one of ONTAP's most reliable and mature technologies. SnapMirror ensures secure and highly efficient data transfers by copying only the changed file system blocks, rather than entire VMs or datastores. Moreover, these blocks take advantage of space-saving techniques like deduplication, compression, and compaction. With the introduction of version-independent SnapMirror in modern ONTAP systems, you gain flexibility in selecting your source and destination clusters. SnapMirror has truly emerged as a powerful tool for disaster recovery, and when combined with Live Site Recovery, it offers enhanced scalability, performance, and cost savings compared to local storage alternatives.

For more information refer to the Overview of VMware Site Recovery Manager.

See the the full solution at the NetApps Solutions documentation center: Autonomous Ransomware Protection for NFS Storage

BlueXP DRaaS (Disaster Recovery as a Service) for NFS is a cost-effective disaster recovery solution designed for VMware workloads running on on-premises ONTAP systems with NFS datastores. It leverages NetApp SnapMirror replication to protect against site outages and data corruption events, such as ransomware attacks. Integrated with the NetApp BlueXP console, this service enables easy management and automated discovery of VMware vCenters and ONTAP storage. Organizations can create and test disaster recovery plans, achieving a Recovery Point Objective (RPO) of up to 5 minutes through block-level replication. BlueXP DRaaS utilizes ONTAP's FlexClone technology for space-efficient testing without impacting production resources. The service orchestrates failover and failback processes, allowing protected virtual machines to be brought up on the designated disaster recovery site with minimal effort. Compared to other well-known alternatives, BlueXP DRaaS offers these capabilities at a fraction of the cost, making it an efficient solution for organizations to set up, test, and execute disaster recovery operations for their VMware environments using ONTAP storage systems.

See the the full solution at the NetApps Solutions documentation center: DR using BlueXP DRaaS for NFS Datastores

Solutions Overview

Solutions covered in this documentation:

- **NFS nConnect feature with NetApp and VMware**. Click **here** for deployment steps.
  - **Use ONTAP tools 10 to configure NFS datastores for vSphere 8**. Click **here** for deployment steps.
  - **Deploy and use the SnapCenter Plug-in for VMware vSphere to protect and restore VMs**. Click **here** for deployment steps.
  - **Disaster recovery of NFS Datastores with VMware Site Recovery Manager**. Click **here** for deployment steps.
  - **Autonomous Ransomware Protection for NFS storage**. Click **here** for deployment steps.

NFS nConnect feature with NetApp and VMware

Starting with VMware vSphere 8.0 U1 (as Tech-preview), the nconnect feature enables multiple TCP connections for NFS v3 datastore volumes to achieve more throughput.

Customers using NFS datastore can now increase the number of connections to NFS server thus maximizing the utilization of high speed network interface cards.

> The feature is generally available for NFS v3 with 8.0 U2, Refer storage section on Release notes of VMware vSphere 8.0 Update 2. NFS v4.1 support is added with vSphere 8.0 U3. for more info, check vSphere 8.0 Update 3 Release Notes

Use cases

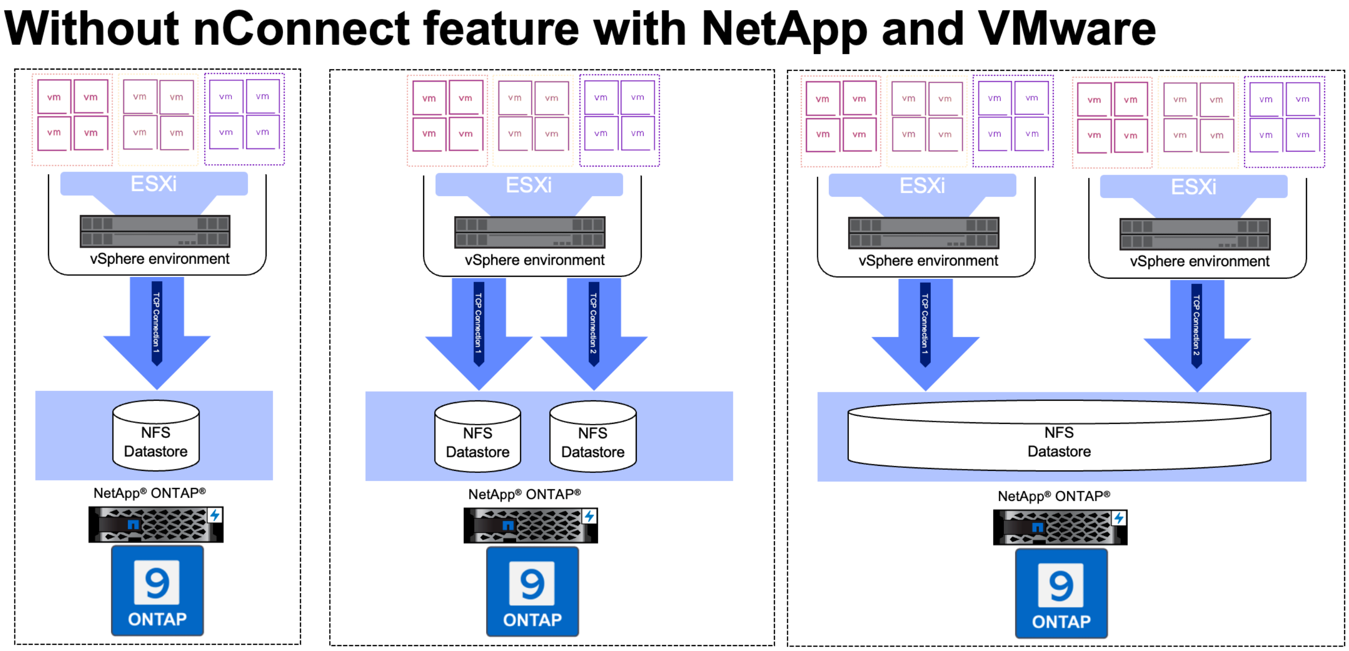
- Host more virtual machines per NFS datastore on the same host.
- Boost NFS datastore performance.
- Provide an option to offer service at a higher tier for VM and Container based applications.

Technical details

The purpose of nconnect is to provide multiple TCP connections per NFS datastore on a vSphere host. This helps increase parallelism and performance for NFS datastores. In ONTAP, when an NFS mount is established, a Connection ID (CID) iscreated. That CID provides up to 128 concurrent in-flight operations. When that number is exceeded by the client, ONTAP enacts a form of flow control until it can free up some available resources as other operations complete. These pauses usually are only a few microseconds, but over the course of millions of operations, those can add up and create performance issues. Nconnect can take the 128 limit and multiply it by the number of nconnect sessions on the client, which provides more concurrent operations per CID and can potentially add performance benefits. For additional details, please refer NFS best practice and implementation guide

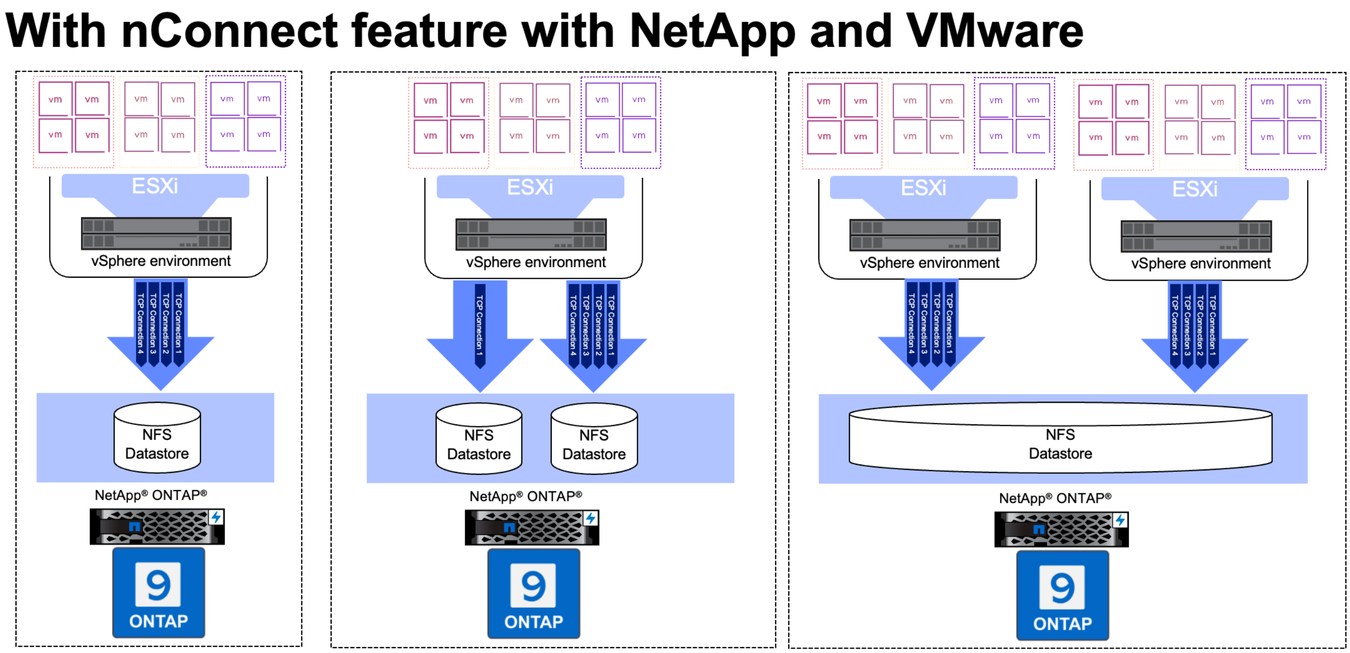
Default NFS Datastore

To address the performance limitations of single connection of NFS datastore, additional datastores are mounted or additional hosts are added to increase the connection.



With nConnect NFS Datastore

Once the NFS datastore is created using ONTAP Tools or with other options, the number of connection per NFS datastore can be modified using vSphere CLI, PowerCLI, govc tool or other API options. To avoid performance concerns along with vMotion, keep the number of connections same for the NFS datastore on all vSphere hosts that are part of the vSphere Cluster.



Pre-requisite

To utilize the nconnect feature, the following dependencies should be met.

ONTAP Version	vSphere Version	Comments
9.8 or above	8 Update 1	Tech preview with option to increase number of connections.
9.8 or above	8 Update 2	Generally available with option to increase and decrease the number of connections.
9.8 or above	8 Update 3	NFS 4.1 and multi-path support.

Update number of connection to NFS Datastore

A single TCP connection is used when a NFS datastore is created with ONTAP Tools or with vCenter. To increase the number of connections, vSphere CLI can be used. The reference command is shown below.

```
# Increase the number of connections while creating the NFS v3 datastore.
esxcli storage nfs add -H <NFS_Server_FQDN_or_IP> -v <datastore_name> -s <remote_share> -c <number_of_connections>
# To specify the number of connections while mounting the NFS 4.1 datastore.
esxcli storage nfs41 add -H <NFS_Server_FQDN_or_IP> -v <datastore_name> -s <remote_share> -c <number_of_connections>
# To utilize specific VMkernel adapters while mounting, use the -I switch
esxcli storage nfs41 add -I <NFS_Server_FQDN_or_IP>:vmk1 -I <NFS_Server_FQDN_or_IP>:vmk2 -v <datastore_name> -s <remote_share> -c <number_of_connections>
# To increase or decrease the number of connections for existing NFSv3 datastore.
esxcli storage nfs param set -v <datastore_name> -c <number_of_connections>
# For NFSv4.1 datastore
esxcli storage nfs41 param set -v <datastore_name> -c <number_of_connections>
# To set VMkernel adapter for an existing NFS 4.1 datastore
esxcli storage nfs41 param set -I <NFS_Server_FQDN_or_IP>:vmk2 -v <datastore_name> -c <number_of_connections>
```

or use PowerCLI similar to shown below

```
$datastoreSys = Get-View (Get-VMHost host01.vsphere.local).ExtensionData.ConfigManager.DatastoreSystem
$nfsSpec = New-Object VMware.Vim.HostNasVolumeSpec
$nfsSpec.RemoteHost = "nfs_server.ontap.local"
$nfsSpec.RemotePath = "/DS01"
$nfsSpec.LocalPath = "DS01"
$nfsSpec.AccessMode = "readWrite"
$nfsSpec.Type = "NFS"
$nfsSpec.Connections = 4
$datastoreSys.CreateNasDatastore($nfsSpec)
```

Here is the example of increasing the number of connection with govc tool.

```
$env.GOVC_URL = 'vcenter.vsphere.local'
$env.GOVC_USERNAME = 'administrator@vsphere.local'
$env.GOVC_PASSWORD = 'XXXXXXXXX'
$env.GOVC_Datastore = 'DS01'
# $env.GOVC_INSECURE = 1
$env.GOVC_HOST = 'host01.vsphere.local'
# Increase number of connections while creating the datastore.
govc host.esxcli storage nfs add -H nfs_server.ontap.local -v DS01 -s
/DS01 -c 2
# For NFS 4.1, replace nfs with nfs41
govc host.esxcli storage nfs41 add -H <NFS_Server_FQDN_or_IP> -v
<datastore_name> -s <remote_share> -c <number_of_connections>
# To utilize specific VMkernel adapters while mounting, use the -I switch
govc host.esxcli storage nfs41 add -I <NFS_Server_FQDN_or_IP>:vmk1 -I
<NFS_Server_FQDN_or_IP>:vmk2 -v <datastore_name> -s <remote_share> -c
<number_of_connections>
# To increase or decrease the connections for existing datastore.
govc host.esxcli storage nfs param set -v DS01 -c 4
# For NFSv4.1 datastore
govc host.esxcli storage nfs41 param set -v <datastore_name> -c
<number_of_connections>
# View the connection info
govc host.esxcli storage nfs list
```

Refer VMware KB article 91497 for more information.

Design considerations

The maximum number of connections supported on ONTAP is depended on storage platform model. Look for exec_ctx on NFS best practice and implementation guide for more information.

As the number of connections per NFSv3 datastore is increased, the number of NFS datastores that can be mounted on that vSphere host decreases. The total number of connections supported per vSphere host is 256. Check VMware KB article 91481 for datastore limts per vSphere host.

> vVol datastore does not support nConnect feature. But, protocol endpoints counts towards the connection limit. A protocol endpoint is created for each data lif of SVM when vVol datastore is created.

Use ONTAP tools 10 to configure NFS datastores for vSphere 8

ONTAP tools for VMware vSphere 10 features a next-generation architecture that enables native high availability and scalability for the VASA Provider (supporting iSCSI and NFS vVols). This simplifies the management of multiple VMware vCenter servers and ONTAP clusters.

In this scenario we will demonstrate how to deploy and use ONTAP tools for VMware vSphere 10 and configure an NFS datastore for vSphere 8.

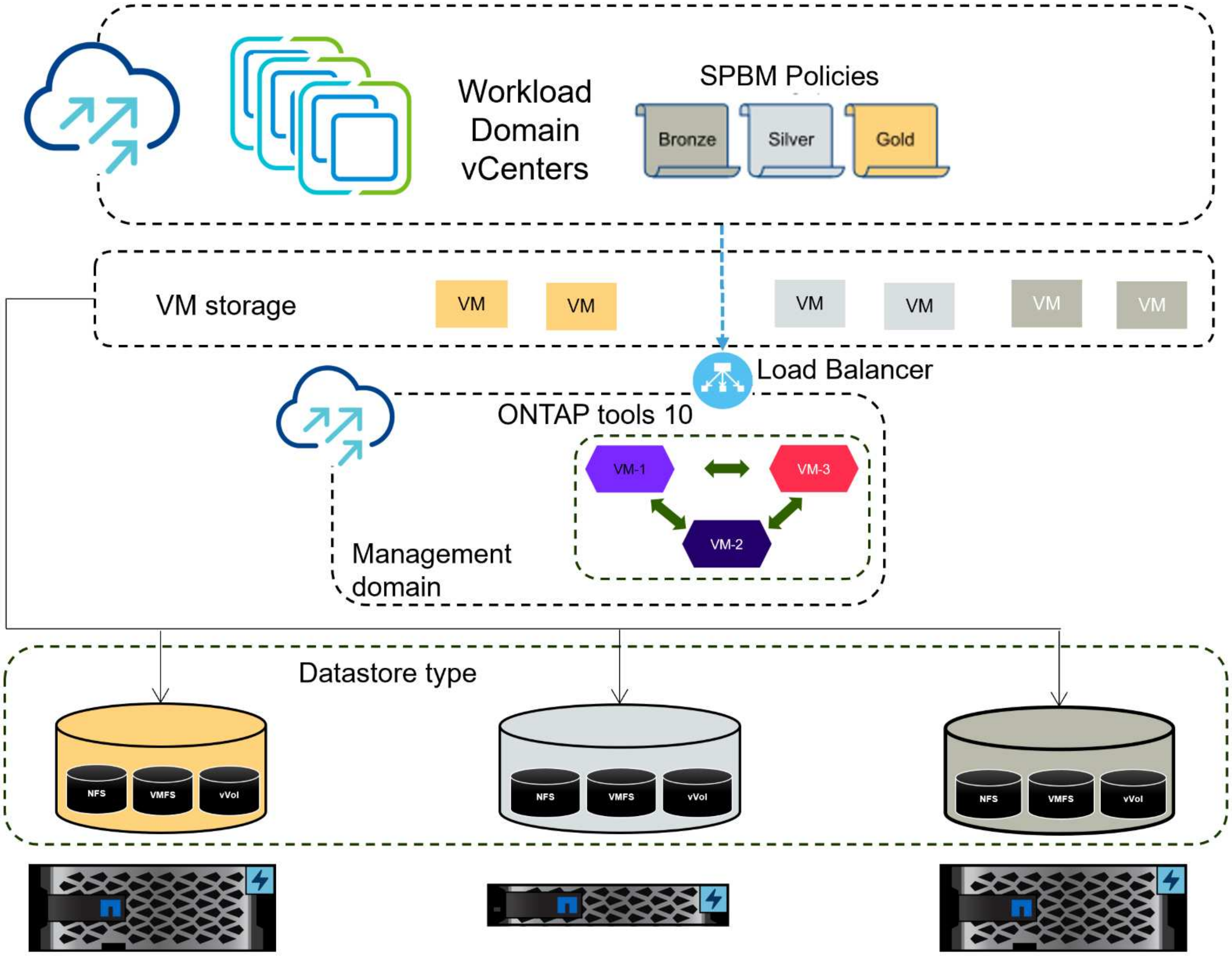
Solution Overview

This scenario covers the following high level steps:

- Create a storage virtual machine (SVM) with logical interfaces (LIFs) for NFS traffic.
- Create a distributed port group for the NFS network on the vSphere 8 cluster.
- Create a vmkernel adapter for NFS on the ESXi hosts in the vSphere 8 cluster.
- Deploy ONTAP tools 10 and register with the vSphere 8 cluster.
- Create a new NFS datastore on the vSphere 8 cluster.

Architecture

The following diagram shows the architectural components of an ONTAP tools for VMware vSphere 10 implementation.



Prerequisites

This solution requires the following components and configurations:

- An ONTAP AFF storage system with physical data ports on ethernet switches dedicated to storage traffic.
- vSphere 8 cluster deployment is complete and the vSphere client is accessible.
- ONTAP tools for VMware vSphere 10 OVA template has been downloaded from the NetApp support site.

NetApp recommends a redundant network designs for NFS, providing fault tolerance for storage systems, switches, networks adapters and host systems. It is common to deploy NFS with a single subnet or multiple subnets depending on the architectural requirements.

Refer to Best Practices For Running NFS with VMware vSphere for detailed information specific to VMware vSphere.

For network guidance on using ONTAP with VMware vSphere refer to the Network configuration - NFS section of the NetApp enterprise applications documentation.

Comprehensive ONTAP tools 10 resources can be found ONTAP tools for VMware vSphere Documentation Resources.

Deployment Steps

To deploy ONTAP tools 10 and use it to create an NFS datastore on the VCF management domain, complete the following steps:

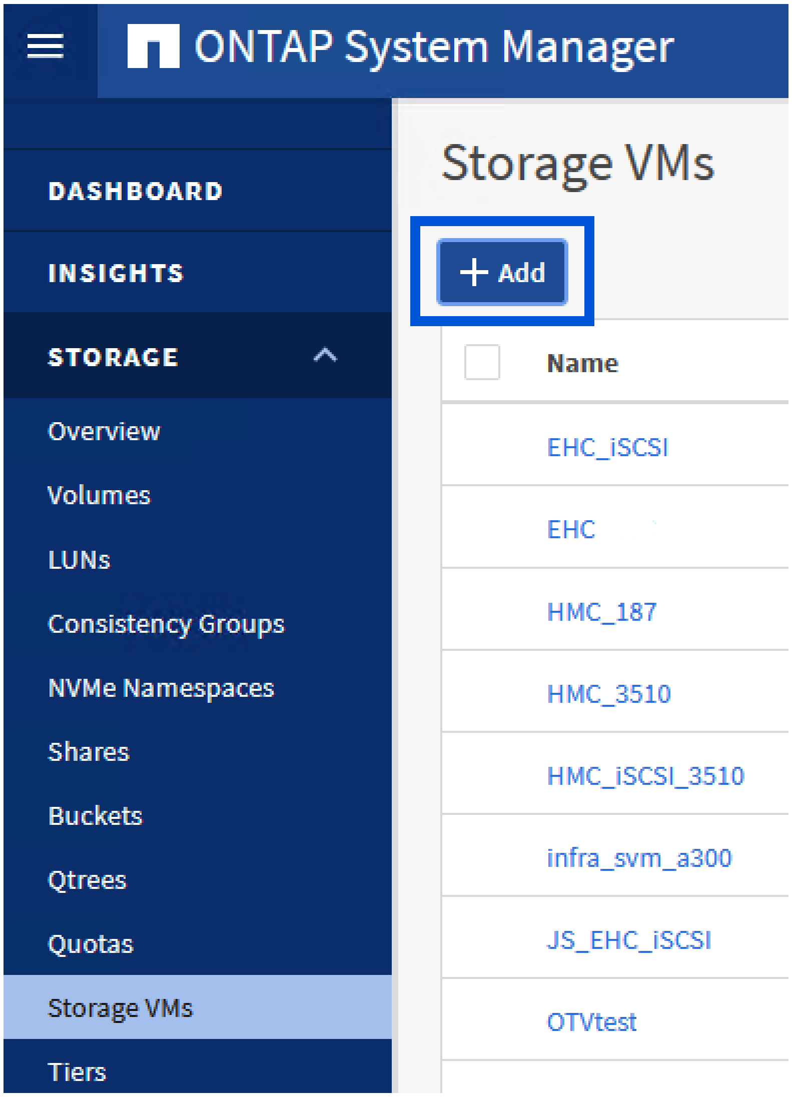
Create SVM and LIFs on ONTAP storage system

The following step is performed in ONTAP System Manager.

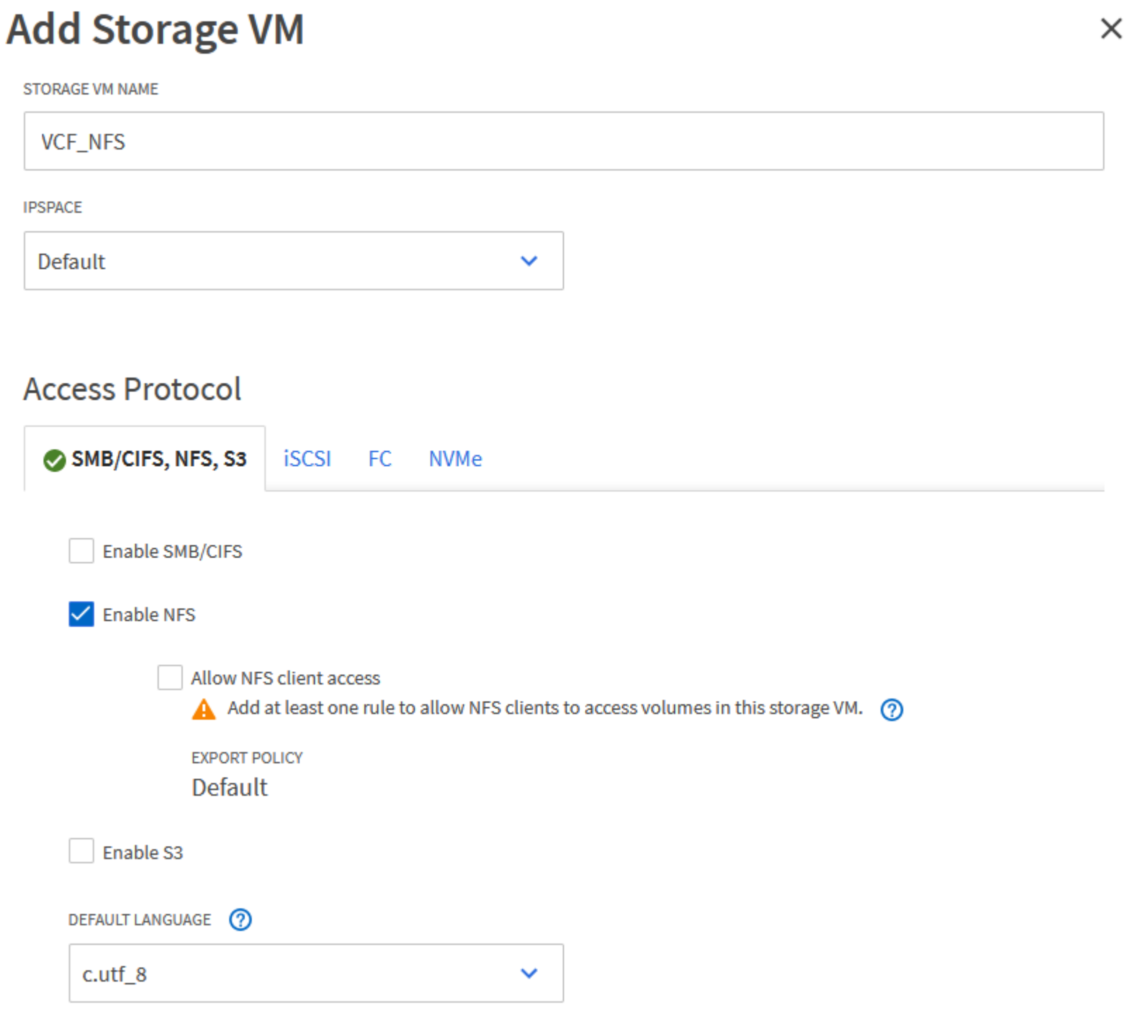
Create the storage VM and LIFs

Complete the following steps to create an SVM together with multiple LIFs for NFS traffic.

1. From ONTAP System Manager navigate to **Storage VMs** in the left-hand menu and click on **+ Add** to start.



2. In the **Add Storage VM** wizard provide a **Name** for the SVM, select the **IP Space** and then, under **Access Protocol**, click on the **SMB/CIFS, NFS, S3** tab and check the box to **Enable NFS**.



Add Storage VM

STORAGE VM NAME

VCF_NFS

IPSPACE

Default

Access Protocol

□ Enable SMB/CIFS

☑ Enable NFS

□ Allow NFS client access

⚠ Add at least one rule to allow NFS clients to access volumes in this storage VM.

EXPORT POLICY

Default

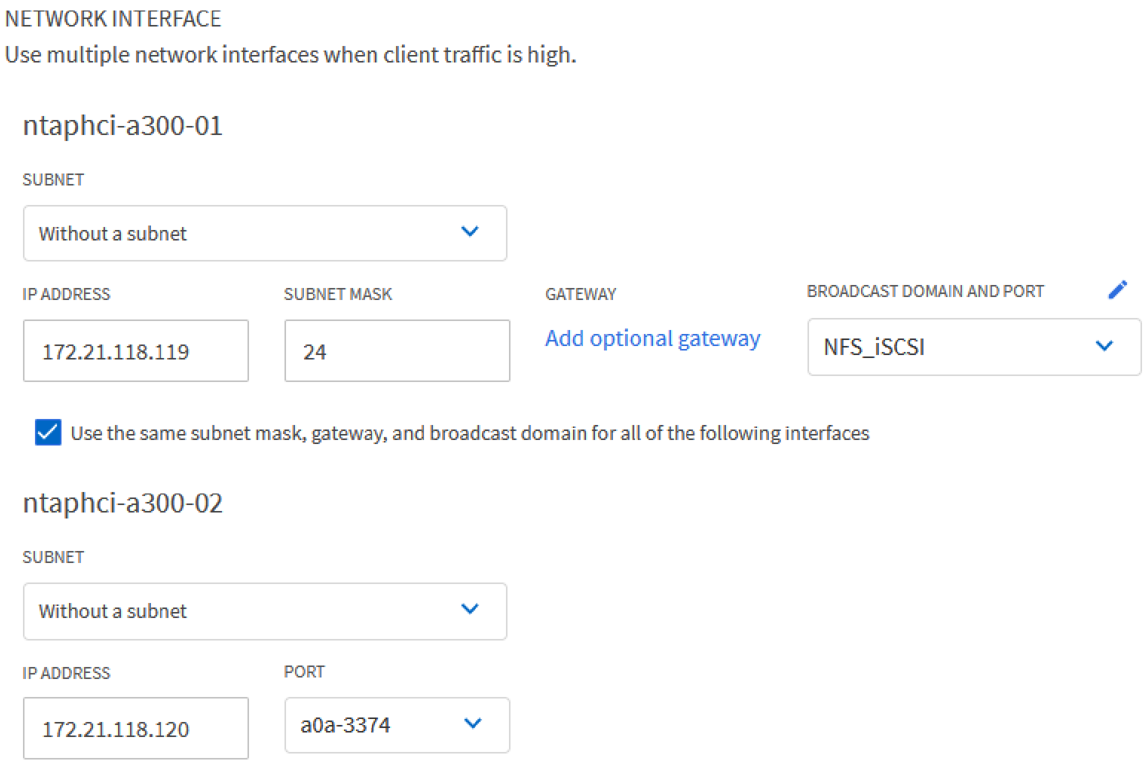
□ Enable S3

DEFAULT LANGUAGE

c.utf_8

It is not necessary to check the **Allow NFS client access** button here as Ontap tools for VMware vSphere will be used to automate the datastore deployment process. This includes providing client access for the ESXi hosts.

3. In the **Network Interface** section fill in the **IP address**, **Subnet Mask**, and **Broadcast Domain and Port** for the first LIF. For subsequent LIFs the checkbox may be enabled to use common settings across all remaining LIFs or use separate settings.



NETWORK INTERFACE
Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET: Without a subnet

IP ADDRESS	SUBNET MASK	GATEWAY	BROADCAST DOMAIN AND PORT
172.21.118.119	24	Add optional gateway	NFS_iSCSI

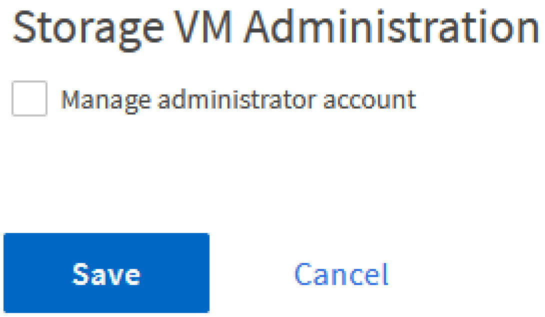
☑ Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

ntaphci-a300-02

SUBNET: Without a subnet

IP ADDRESS	PORT
172.21.118.120	a0a-3374

4. Choose whether to enable the Storage VM Administration account (for multi-tenancy environments) and click on **Save** to create the SVM.



Storage VM Administration

□ Manage administrator account

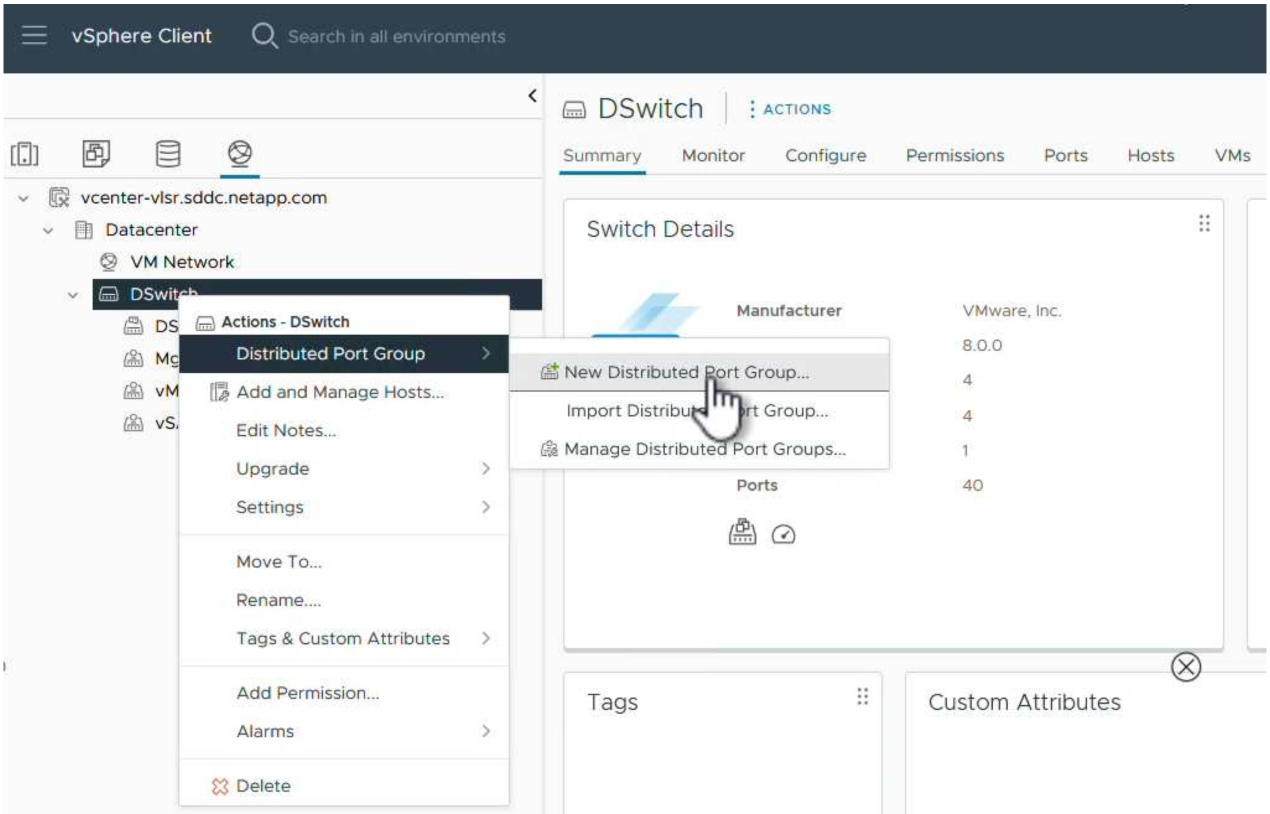
Set up networking for NFS on ESXi hosts

The following steps are performed on the VI Workload Domain cluster using the vSphere client. In this case vCenter Single Sign-On is being used so the vSphere client is common across the management and workload domains.

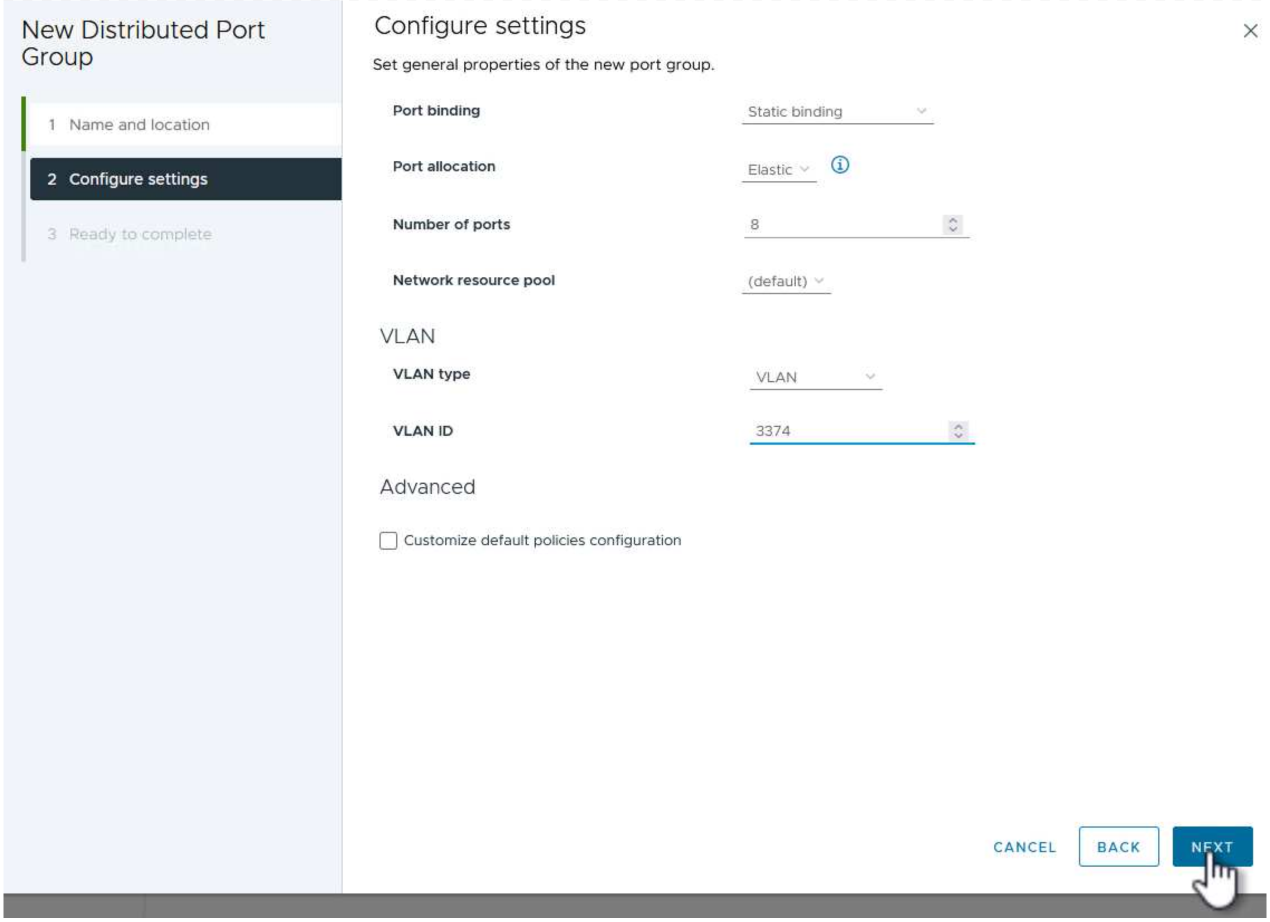
Create a Distributed Port Group for NFS traffic

Complete the following to create a new distributed port group for the network to carry NFS traffic:

1. From the vSphere client , navigate to **Inventory > Networking** for the workload domain. Navigate to the existing Distributed Switch and choose the action to create **New Distributed Port Group…**.



2. In the **New Distributed Port Group** wizard fill in a name for the new port group and click on **Next** to continue.
3. On the **Configure settings** page fill out all settings. If VLANs are being used be sure to provide the correct VLAN ID. Click on **Next** to continue.



New Distributed Port Group

1 Name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding	Static binding
Port allocation	Elastic
Number of ports	8
Network resource pool	(default)

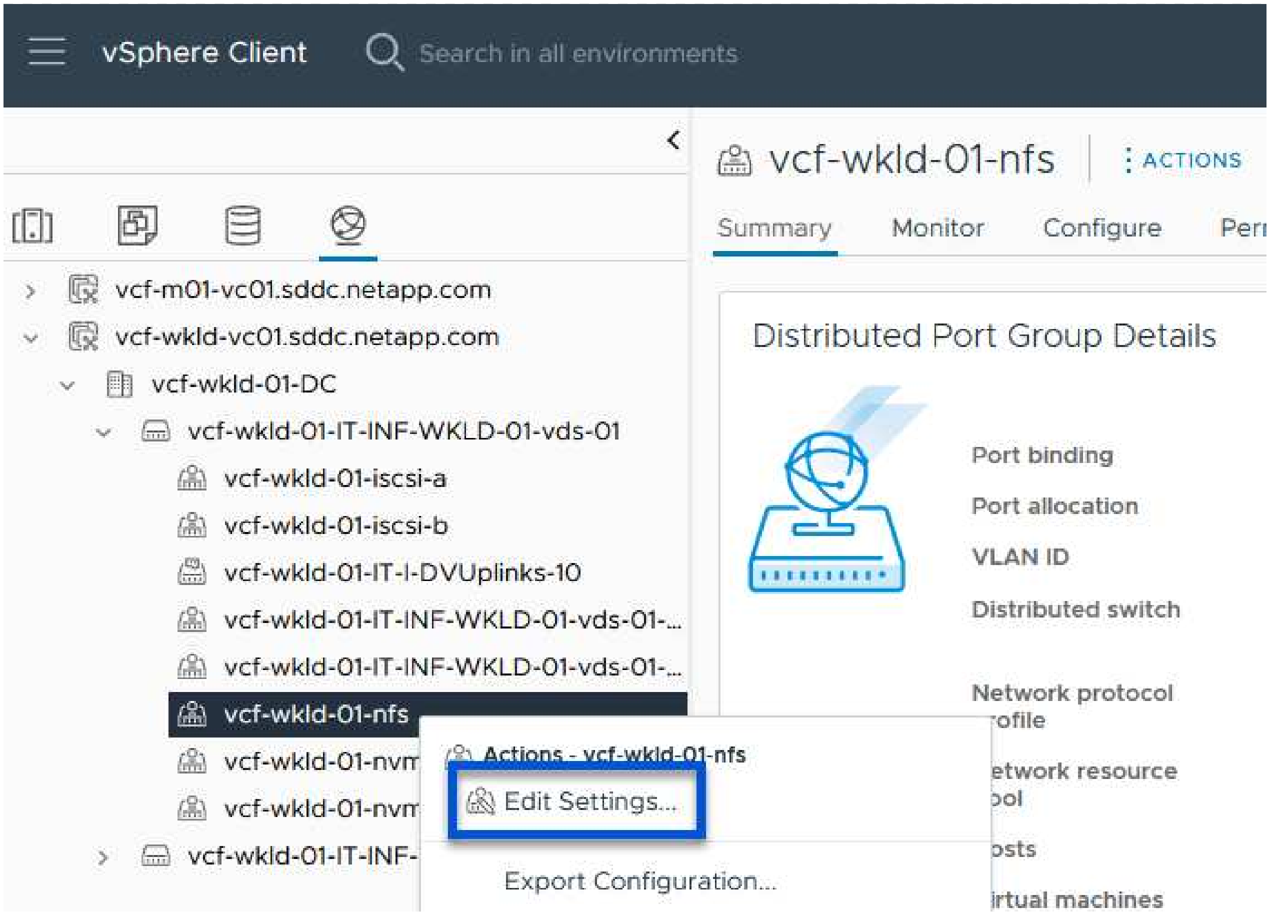
VLAN

VLAN type	VLAN
VLAN ID	3374

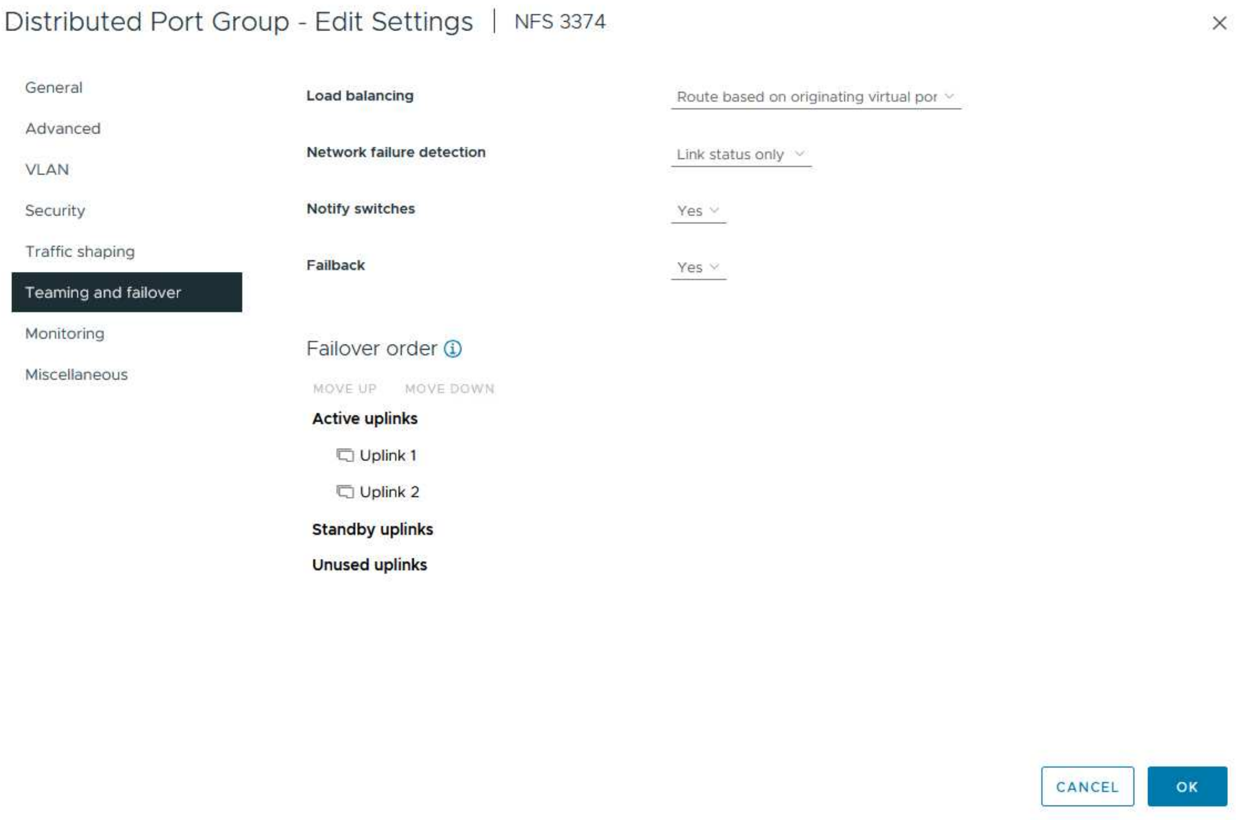
Advanced

□ Customize default policies configuration

4. On the **Ready to complete** page, review the changes and click on **Finish** to create the new distributed port group.
5. Once the port group has been created, navigate to the port group and select the action to **Edit settings…**.



6. On the **Distributed Port Group - Edit Settings** page, navigate to **Teaming and failover** in the left-hand menu. Enable teaming for the Uplinks to be used for NFS traffic by ensuring they are together in the **Active uplinks** area. Move any unused uplinks down to **Unused uplinks**.



Distributed Port Group - Edit Settings | NFS 3374

Load balancing: Route based on originating virtual por

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

Failover order

Active uplinks
- Uplink 1
- Uplink 2

Standby uplinks

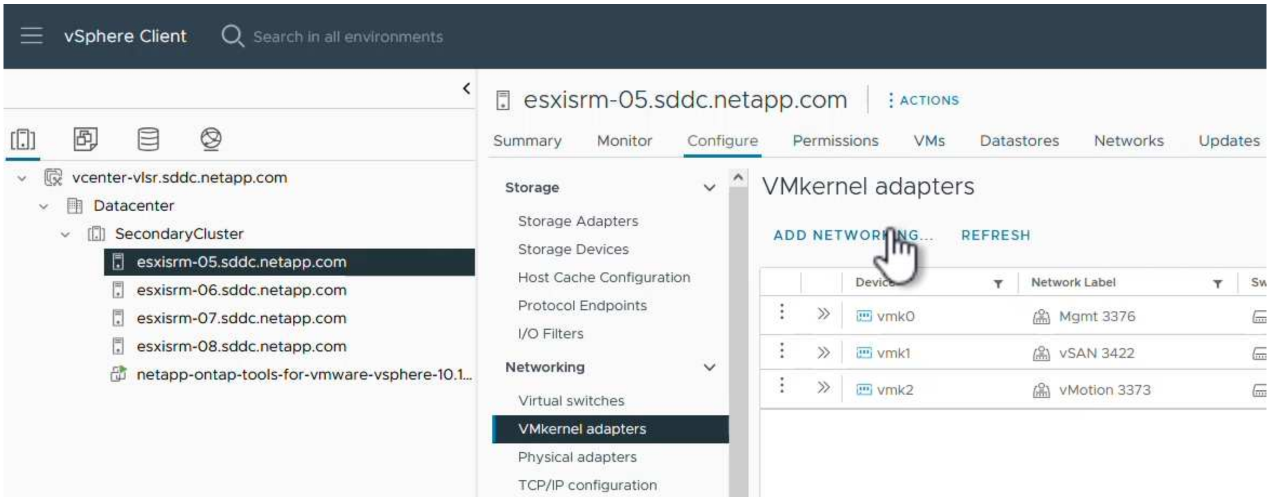
Unused uplinks

7. Repeat this process for each ESXi host in the cluster.

Create a VMkernel adapter on each ESXi host

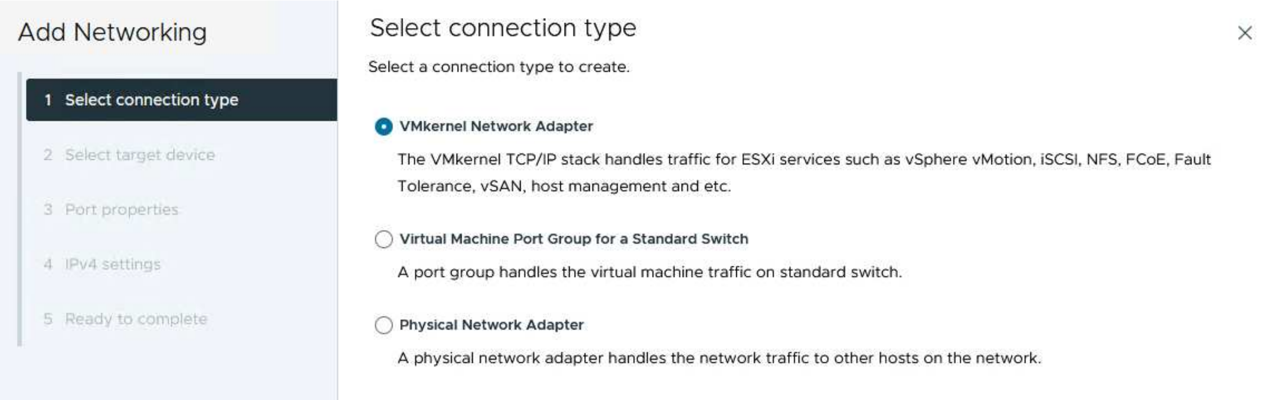
Repeat this process on each ESXi host in the workload domain.

1. From the vSphere client navigate to one of the ESXi hosts in the workload domain inventory. From the **Configure** tab select **VMkernel adapters** and click on **Add Networking…** to start.



Device	Network Label
vmk0	Mgmt 3376
vmk1	vSAN 3422
vmk2	vMotion 3373

2. On the **Select connection type** window choose **VMkernel Network Adapter** and click on **Next** to continue.



Select connection type

Select a connection type to create.

● VMkernel Network Adapter

The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.

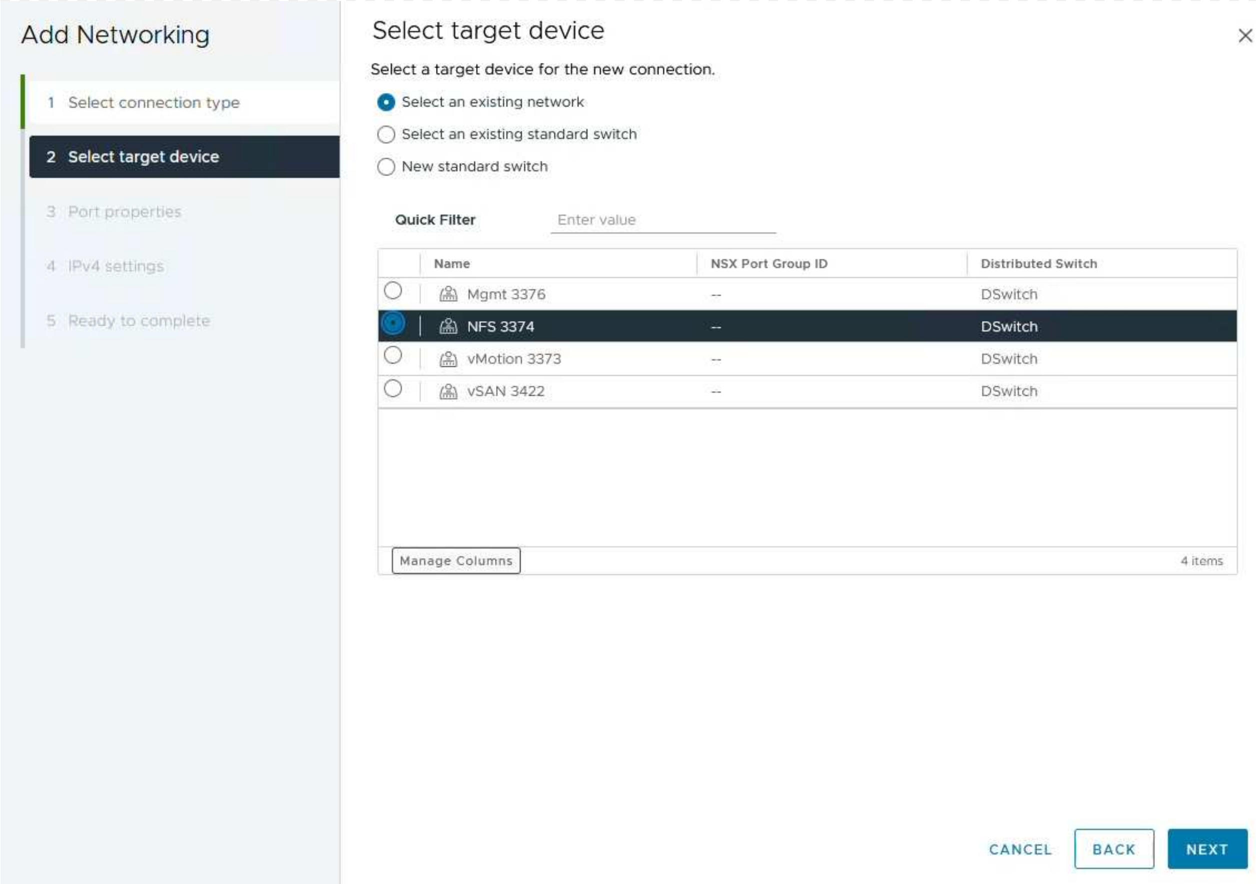
○ Virtual Machine Port Group for a Standard Switch

A port group handles the virtual machine traffic on standard switch.

○ Physical Network Adapter

A physical network adapter handles the network traffic to other hosts on the network.

3. On the **Select target device** page, choose one of the distributed port groups for NFS that was created previously.



Select target device

Select a target device for the new connection.

● Select an existing network

○ Select an existing standard switch

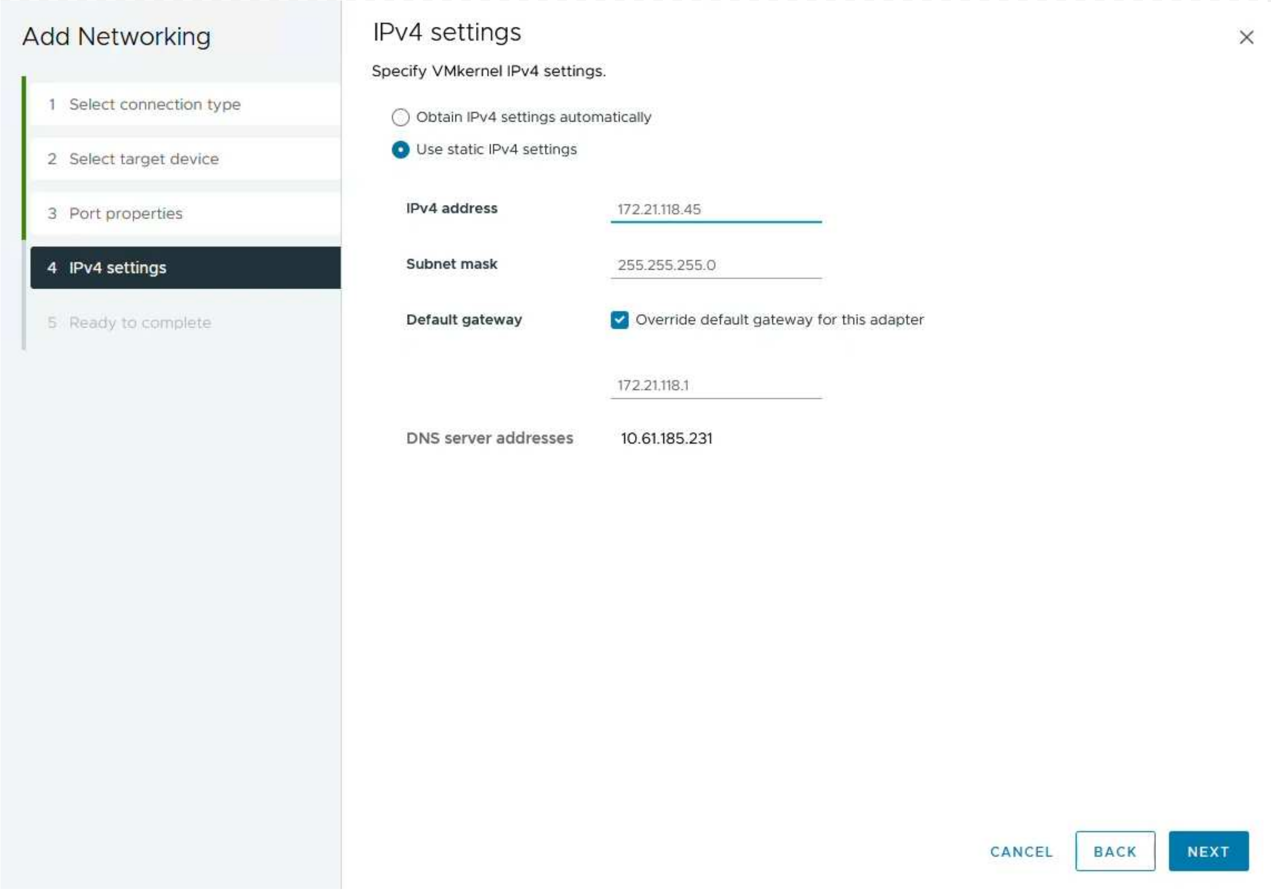
○ New standard switch

Quick Filter Enter value

	Name	NSX Port Group ID	Distributed Switch
○	Mgmt 3376	--	DSwitch
●	NFS 3374	--	DSwitch
○	vMotion 3373	--	DSwitch
○	vSAN 3422	--	DSwitch

Manage Columns 4 items

4. On the **Port properties** page keep the defaults (no enabled services) and click on **Next** to continue.
5. On the **IPv4 settings** page fill in the **IP address**, **Subnet mask**, and provide a new Gateway IP address (only if required). Click on **Next** to continue.



Add Networking

1 Select connection type
2 Select target device
3 Port properties
4 IPv4 settings
5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

○ Obtain IPv4 settings automatically

● Use static IPv4 settings

IPv4 address: 172.21.118.45

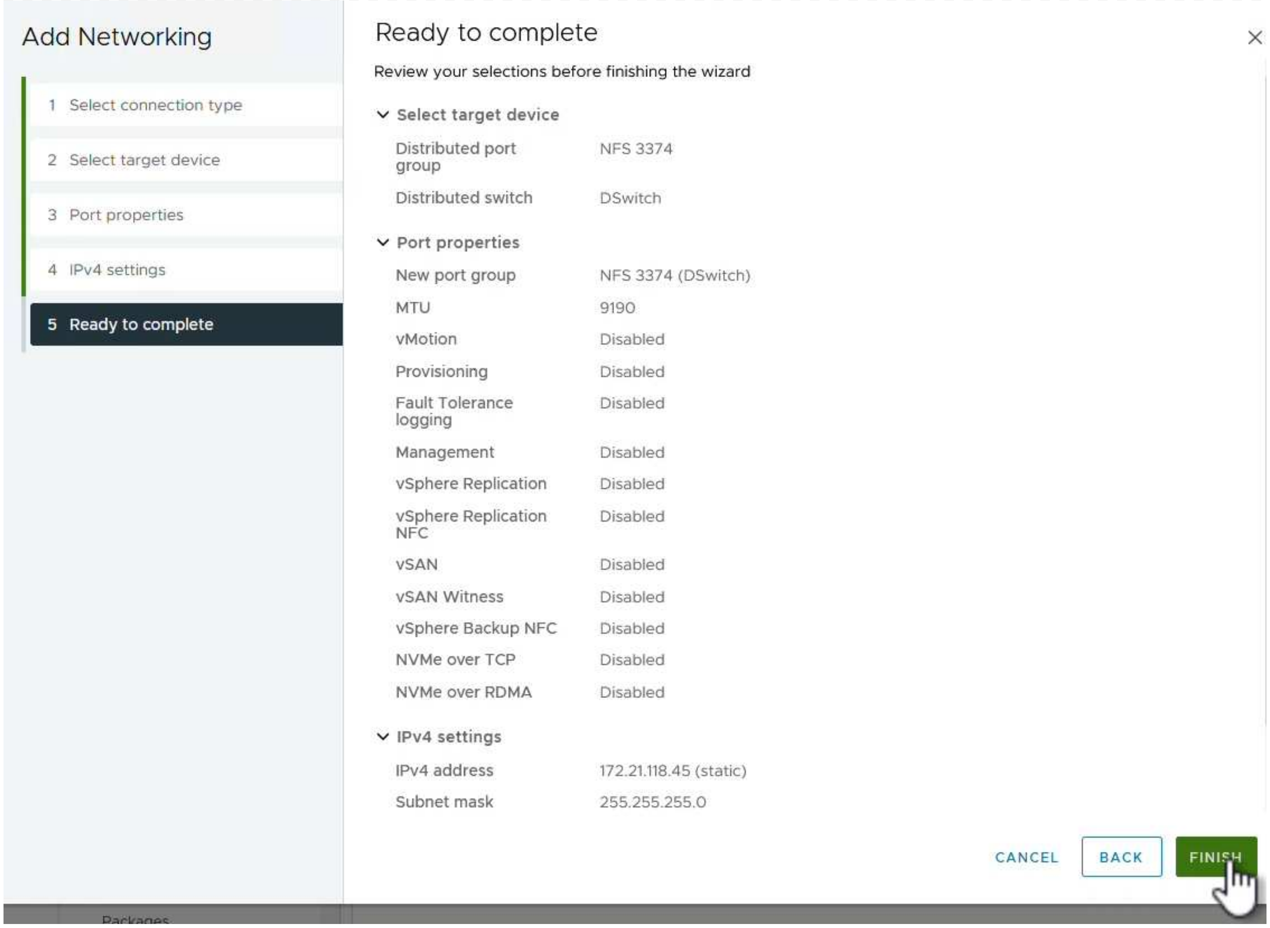
Subnet mask: 255.255.255.0

Default gateway: ☑ Override default gateway for this adapter

172.21.118.1

DNS server addresses: 10.61.185.231

6. Review the your selections on the **Ready to complete** page and click on **Finish** to create the VMkernel adapter.



Ready to complete

Review your selections before finishing the wizard

Select target device

Distributed port group	NFS 3374
Distributed switch	DSwitch

Port properties

New port group	NFS 3374 (DSwitch)
MTU	9190
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Disabled
NVMe over RDMA	Disabled

IPv4 settings

IPv4 address	172.21.118.45 (static)
Subnet mask	255.255.255.0

Deploy and use ONTAP tools 10 to configure storage

The following steps are performed on vSphere 8 cluster using the vSphere client and involve deploying OTV, configuring ONTAP tools Manager, and creating a vVols NFS datastore.

For the full documentation on deploying and using ONTAP tools for VMware vSphere 10 refer to Prepare to deploy ONTAP tools for VMware vSphere.

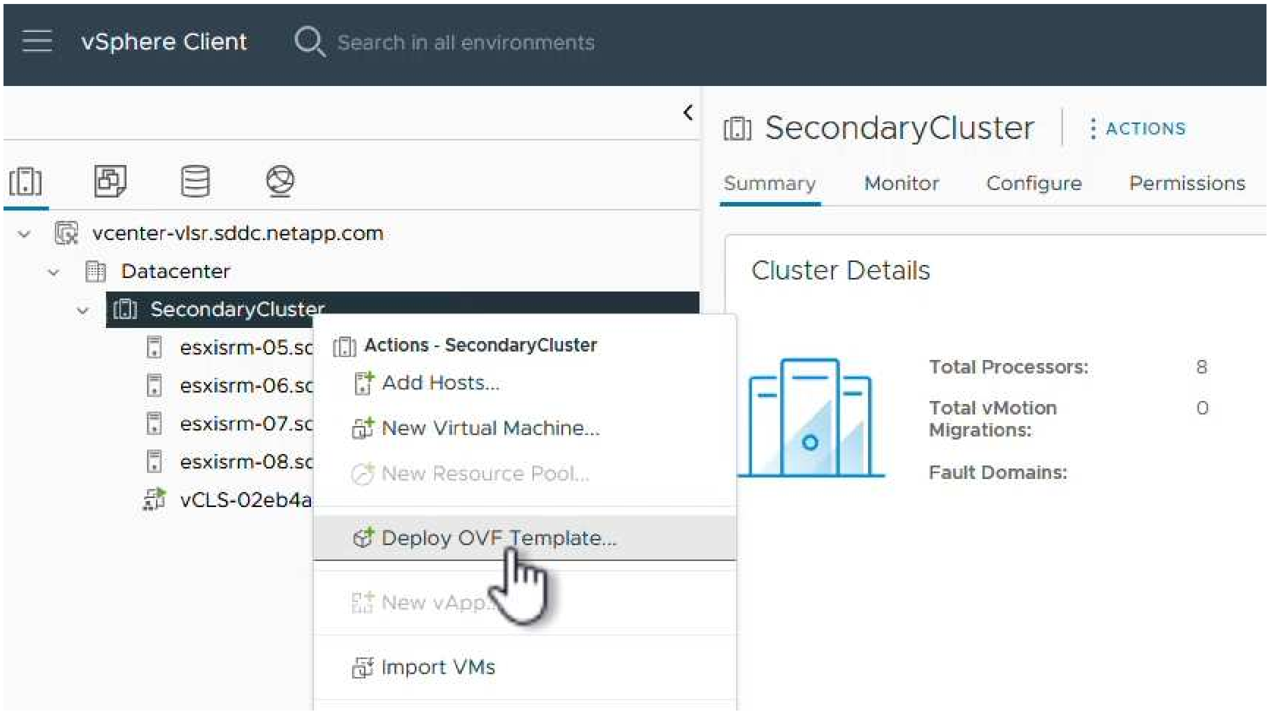
Deploy ONTAP tools for VMware vSphere 10

ONTAP tools for VMware vSphere 10 is deployed as a VM appliance and provides an integrated vCenter UI for managing ONTAP storage. ONTAP tools 10 features a new global management portal for managing connections to multiple vCenter servers and ONTAP storage backends.

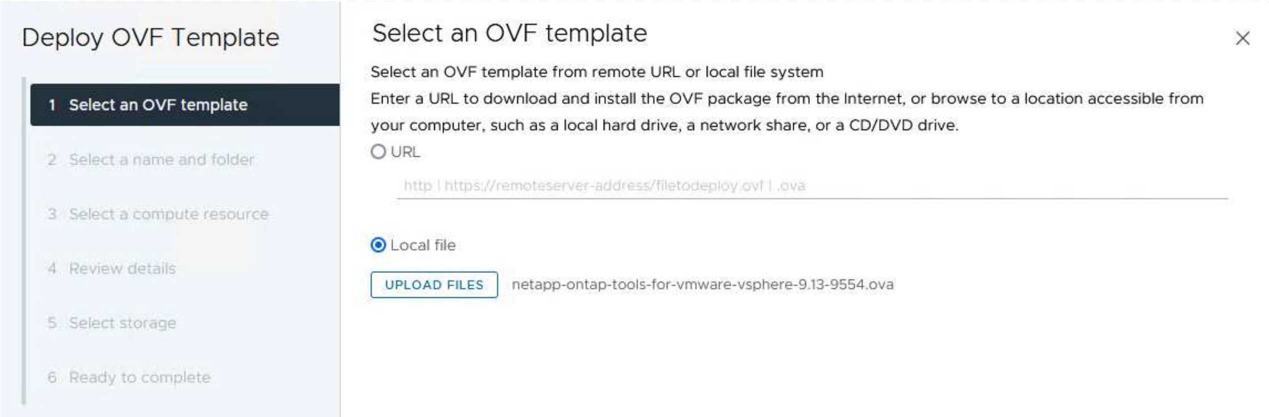
> In a non-HA deployment scenario, three available IP addresses are required. One IP address is allocated for the load balancer, another for the Kubernetes control plane, and the remaining one for the node. In an HA deployment, two additional IP addresses are necessary for the second and third nodes, in addition to the initial three. Prior to assignment, the host names should be associated to the IP addresses in DNS. It is important that all five IP addresses are on the same VLAN, which is chosen for the deployment.

Complete the following to Deploy ONTAP tools for VMware vSphere:

1. Obtain the ONTAP tools OVA image from the NetApp Support site and download to a local folder.
2. Log into the vCenter appliance for the vSphere 8 cluster.
3. From the vCenter appliance interface right-click on the management cluster and select **Deploy OVF Template…**



4. In the **Deploy OVF Template** wizard click the **Local file** radio button and select the ONTAP tools OVA file downloaded in the previous step.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

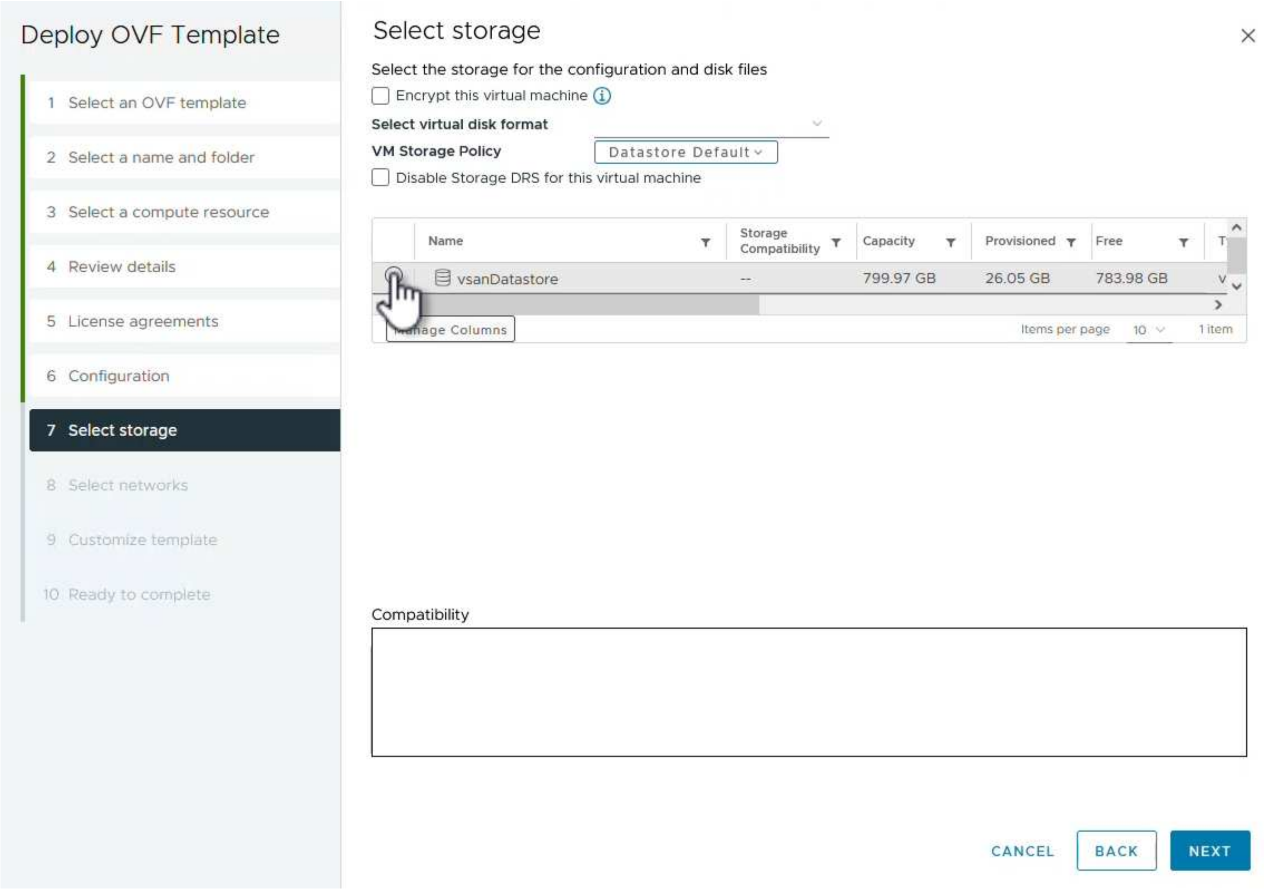
○ URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

● Local file

UPLOAD FILES netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. For steps 2 through 5 of the wizard select a name and folder for the VM, select the compute resource, review the details, and accept the license agreement.
6. For the storage location of the configuration and disk files, select a local datastore or vSAN datastore.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine

Select virtual disk format

VM Storage Policy: Datastore Default

□ Disable Storage DRS for this virtual machine

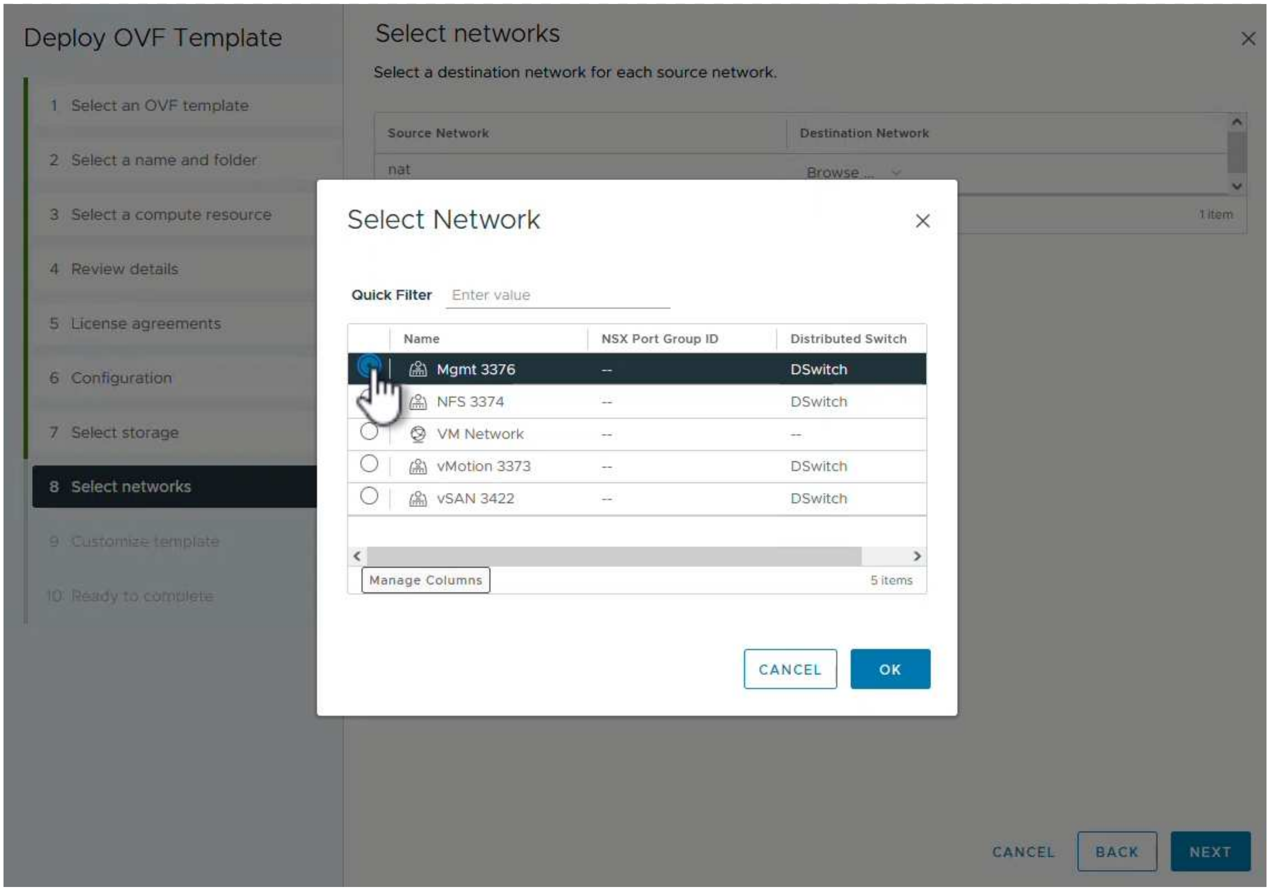
	Name	Storage Compatibility	Capacity	Provisioned	Free	T
○	vsanDatastore	--	799.97 GB	26.05 GB	783.98 GB	V

Manage Columns — Items per page 10 — 1 item

Compatibility

CANCEL BACK NEXT

7. On the Select network page select the network used for management traffic.



Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	Browse ...

1 item

Select Network

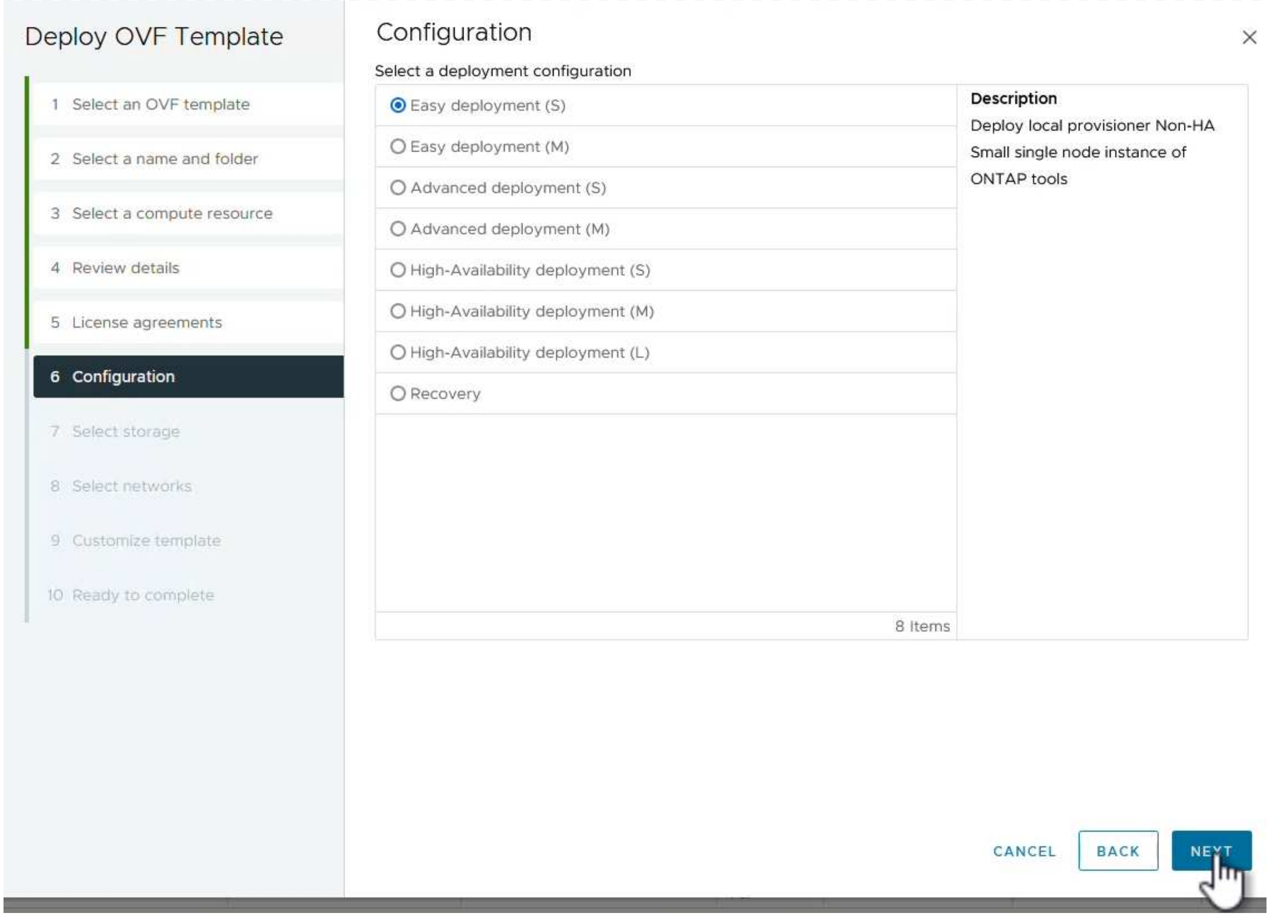
Quick Filter: Enter value

	Name	NSX Port Group ID	Distributed Switch
●	Mgmt 3376	--	DSwitch
○	NFS 3374	--	DSwitch
○	VM Network	--	--
○	vMotion 3373	--	DSwitch
○	vSAN 3422	--	DSwitch

5 items

8. On the Configuration page select the deployment configuration to be used. In this scenario the easy deployment method is used.

   ONTAP Tools 10 features multiple deployment configurations including high-availability deployments using multiple nodes. For documentation on all deployment configurations, refer to Prepare to deploy ONTAP tools for VMware vSphere.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Configuration

Select a deployment configuration

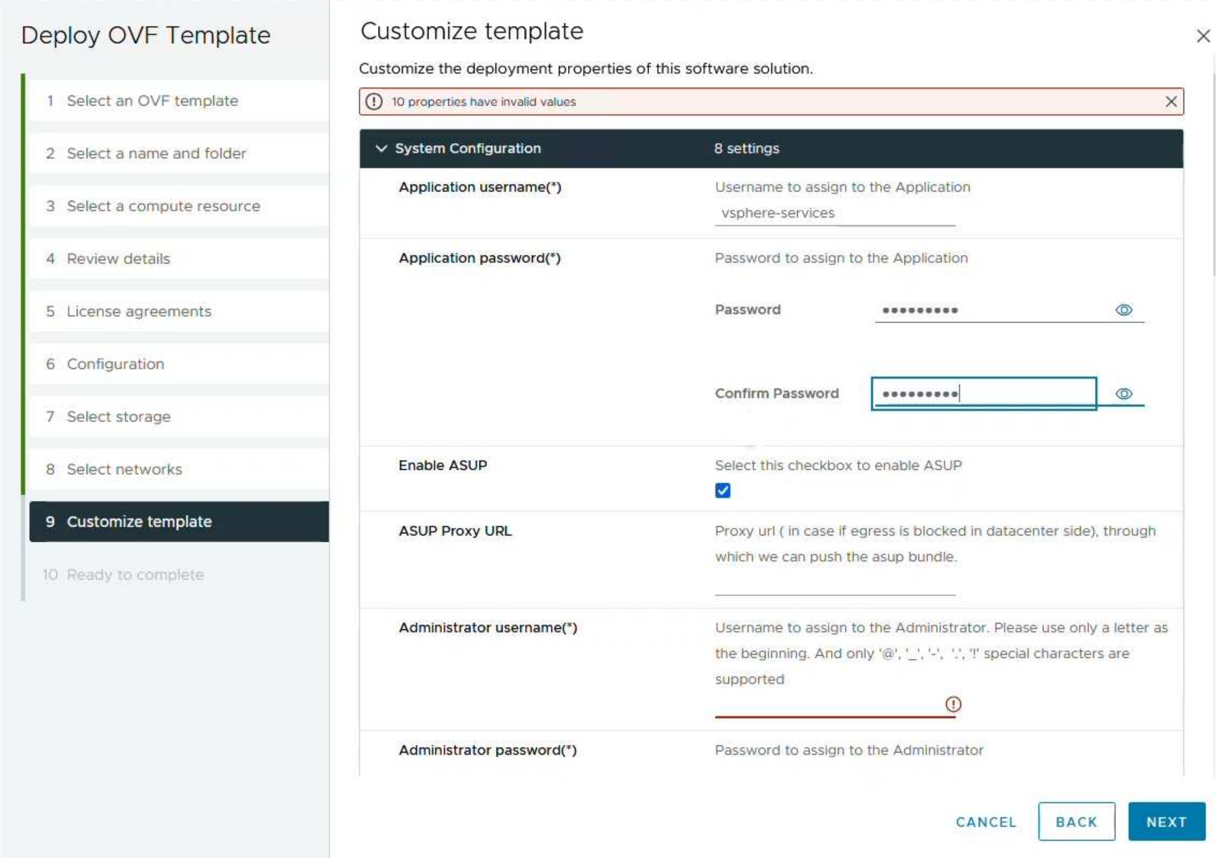
- ● Easy deployment (S)
- ○ Easy deployment (M)
- ○ Advanced deployment (S)
- ○ Advanced deployment (M)
- ○ High-Availability deployment (S)
- ○ High-Availability deployment (M)
- ○ High-Availability deployment (L)
- ○ Recovery

8 Items

Description
Deploy local provisioner Non-HA Small single node instance of ONTAP tools

9. On the Customize template page fill out all required information:
    - Application username to be used to register the VASA provider and SRA in the vCenter Server.
    - Enable ASUP for automated support.
    - ASUP Proxy URL if required.
    - Administrator username and password.
    - NTP servers.
    - Maintenance user password to access management functions from the console.
    - Load Balancer IP.
    - Virtual IP for K8s control plane.
    - Primary VM to select the current VM as the primary (for HA configurations).
    - Hostname for the VM
    - Provide the required network properties fields.

    Click on **Next** to continue.



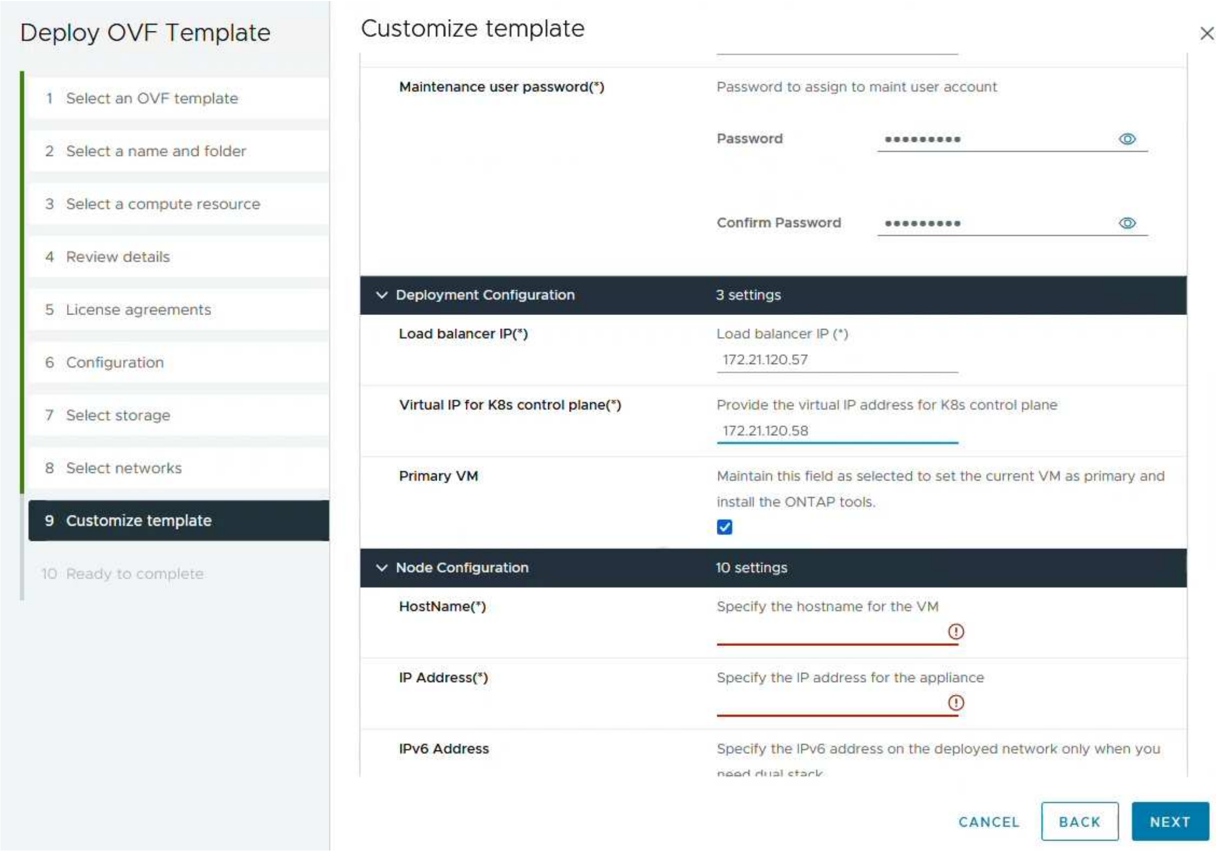
Customize template

Customize the deployment properties of this software solution.

ⓘ 10 properties have invalid values

System Configuration — 8 settings

Application username(*)	Username to assign to the Application vsphere-services
Application password(*)	Password to assign to the Application Password ●●●●●●●●● Confirm Password ●●●●●●●●●
Enable ASUP	Select this checkbox to enable ASUP ☑
ASUP Proxy URL	Proxy url (in case if egress is blocked in datacenter side), through which we can push the asup bundle.
Administrator username(*)	Username to assign to the Administrator. Please use only a letter as the beginning. And only '@', '_', '-', '.', '!' special characters are supported ⓘ
Administrator password(*)	Password to assign to the Administrator



Customize template

Maintenance user password(*)	Password to assign to maint user account Password ●●●●●●●●● Confirm Password ●●●●●●●●●

Deployment Configuration — 3 settings

Load balancer IP(*)	Load balancer IP (*) 172.21.120.57
Virtual IP for K8s control plane(*)	Provide the virtual IP address for K8s control plane 172.21.120.58
Primary VM	Maintain this field as selected to set the current VM as primary and install the ONTAP tools. ☑

Node Configuration — 10 settings

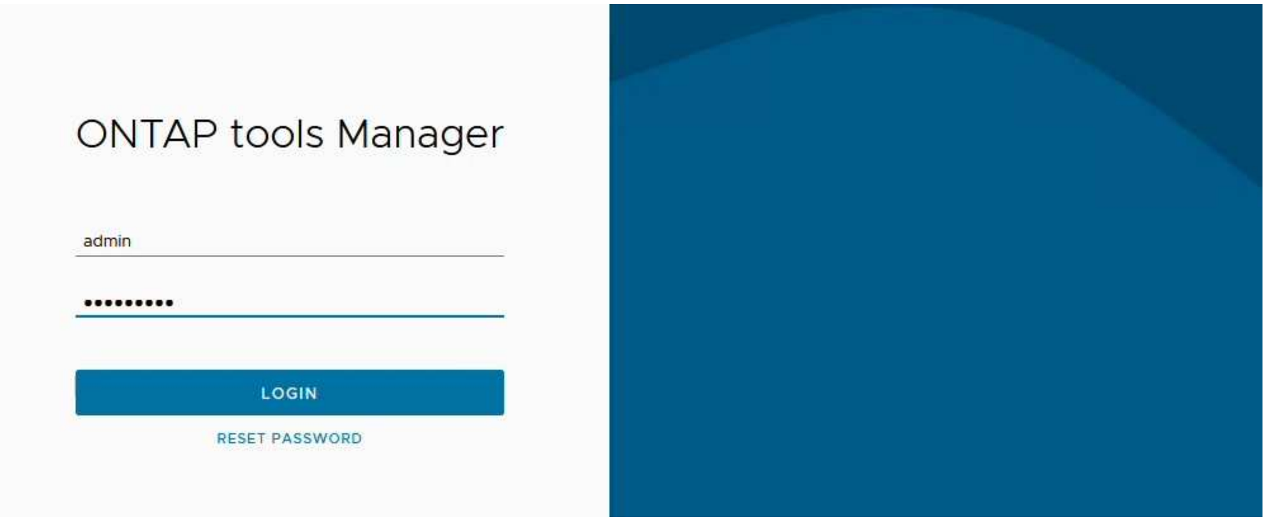
HostName(*)	Specify the hostname for the VM ⓘ
IP Address(*)	Specify the IP address for the appliance ⓘ
IPv6 Address	Specify the IPv6 address on the deployed network only when you need dual stack

10. Review all information on the Ready to complete page and the click Finish to begin deploying the ONTAP tools appliance.

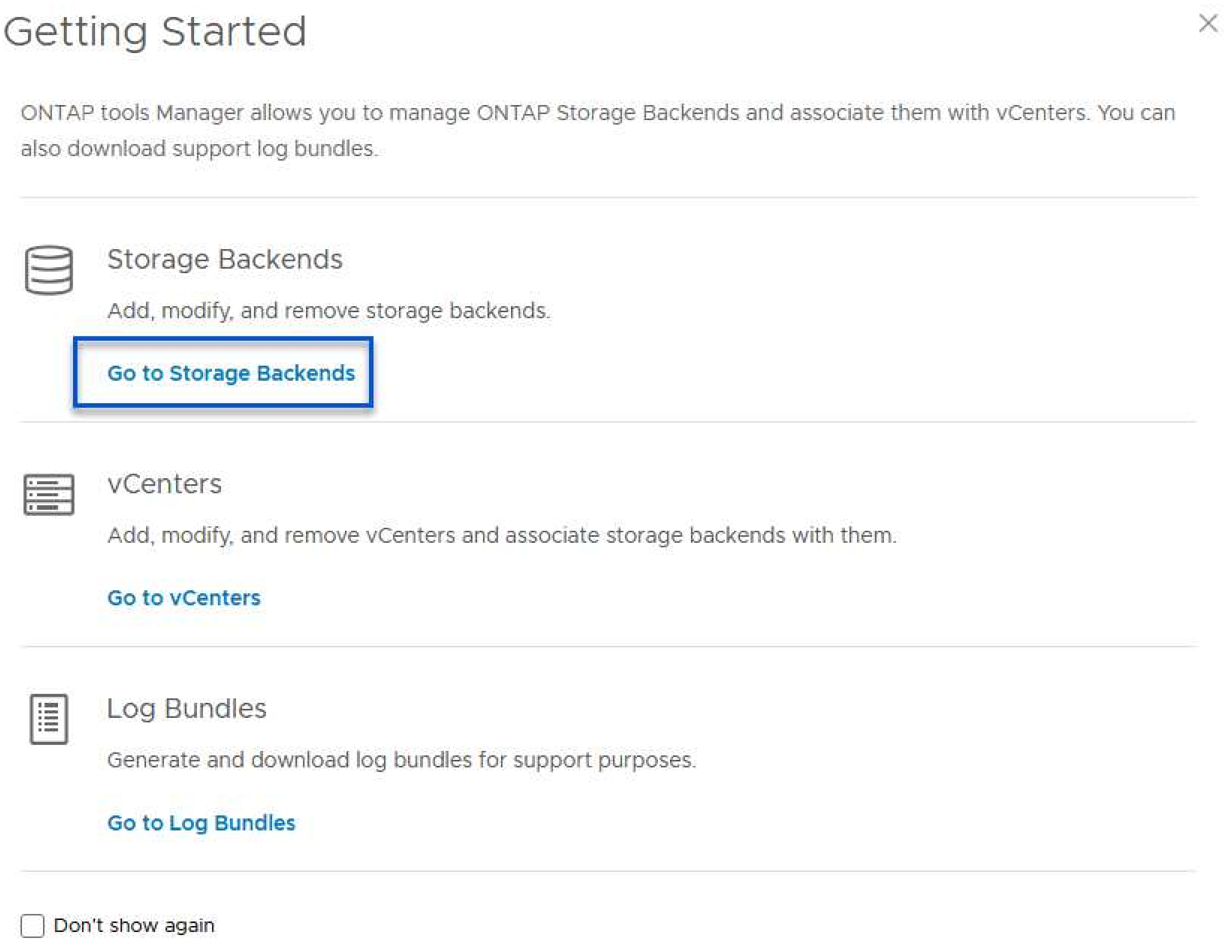
Connect Storage Backend and vCenter Server to ONTAP tools 10.

ONTAP tools manager is used to configure global settings for ONTAP Tools 10.

1. Access ONTAP tools Manager by navigating to https://loadBalanceIP:8443/virtualization/ui/ in a web browser and logging in with the administrative credentials provided during deployment.



2. On the **Getting Started** page click on **Go to Storage Backends**.



Getting Started

ONTAP tools Manager allows you to manage ONTAP Storage Backends and associate them with vCenters. You can also download support log bundles.

Storage Backends

Add, modify, and remove storage backends.

Go to Storage Backends

vCenters

Add, modify, and remove vCenters and associate storage backends with them.

Go to vCenters

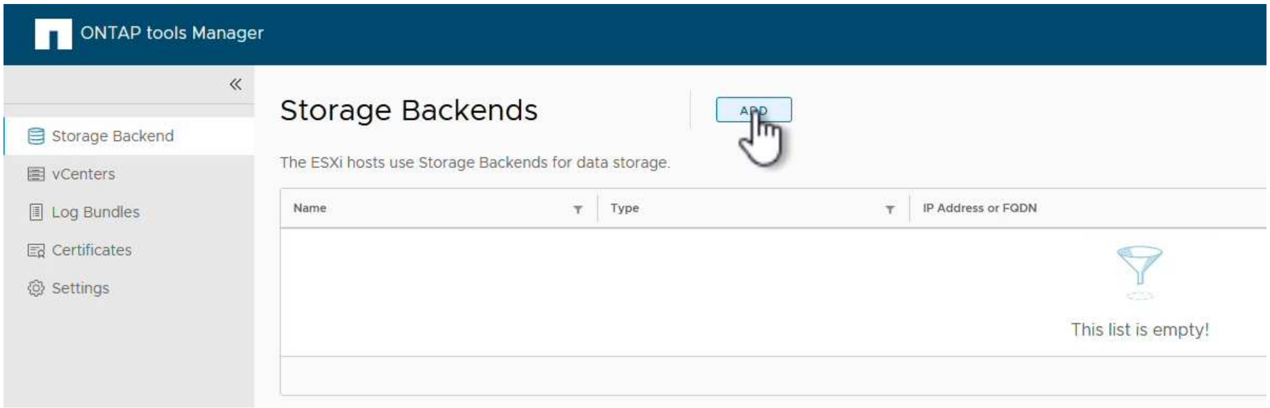
Log Bundles

Generate and download log bundles for support purposes.

Go to Log Bundles

□ Don't show again

3. On the **Storage Backends** page, click on **ADD** to fill in the credentials of an ONTAP storage system to be registered with ONTAP tools 10.



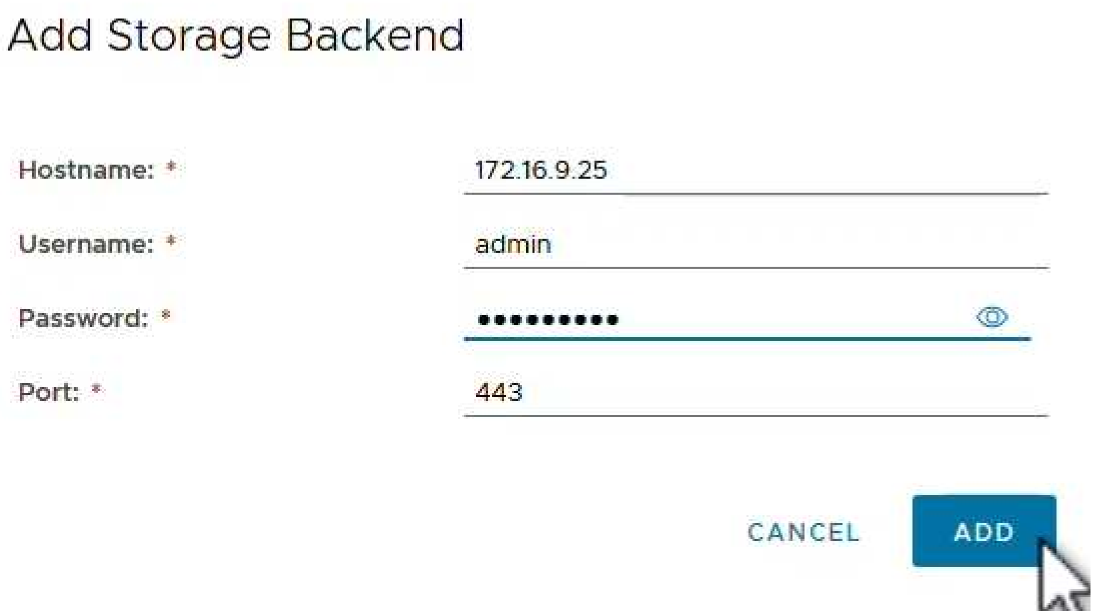
Storage Backends

The ESXi hosts use Storage Backends for data storage.

Name	Type	IP Address or FQDN

This list is empty!

4. On the **Add Storage Backend** box, fill out the credentials for the ONTAP storage system.



Add Storage Backend

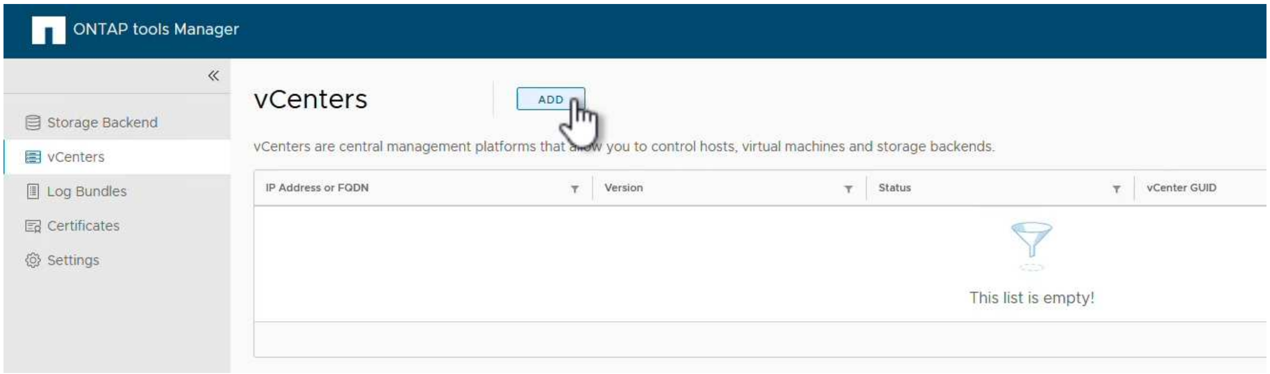
Hostname: * 172.16.9.25

Username: * admin

Password: * ••••••••••

Port: * 443

5. In the left hand menu click on **vCenters**, and then on on **ADD** to fill in the credentials of a vCenter server to be registered with ONTAP tools 10.



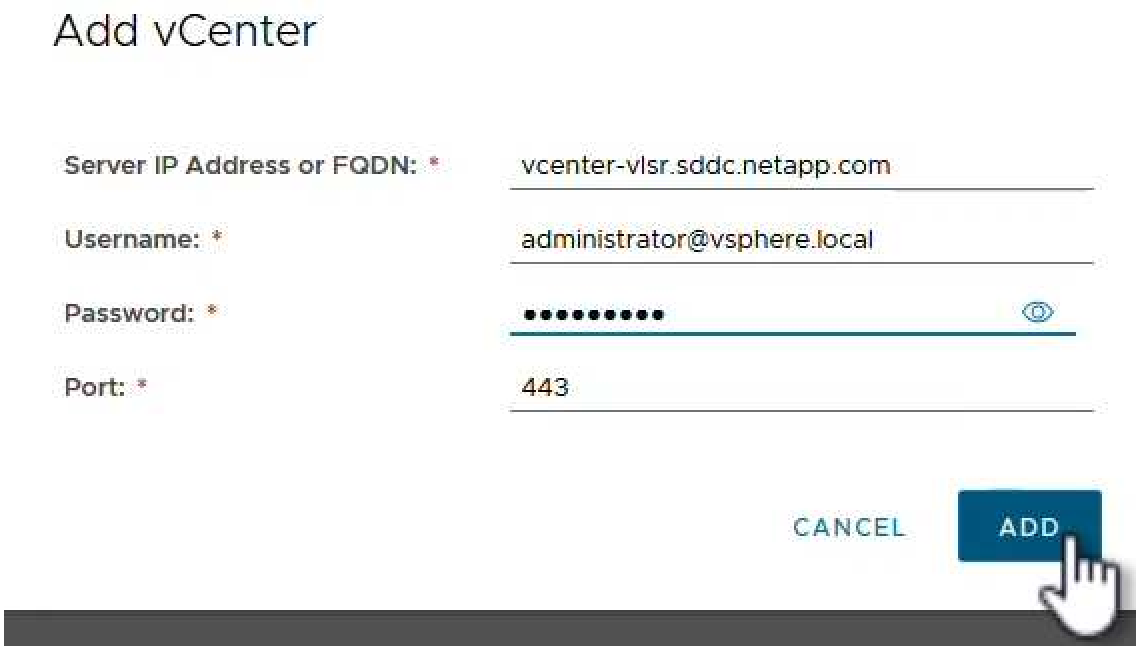
vCenters

vCenters are central management platforms that allow you to control hosts, virtual machines and storage backends.

IP Address or FQDN	Version	Status	vCenter GUID

This list is empty!

6. On the **Add vCenter** box, fill out the credentials for the ONTAP storage system.


Add vCenter

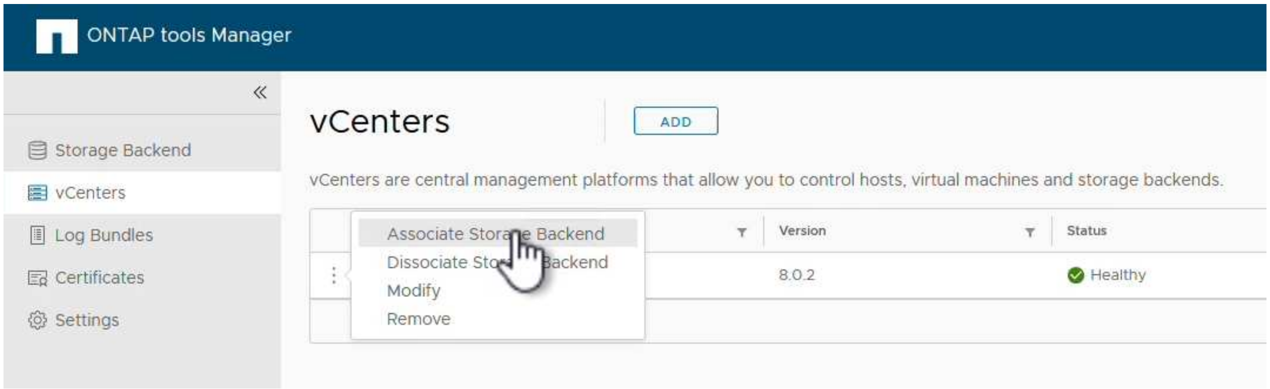
Server IP Address or FQDN: * vcenter-vlsr.sddc.netapp.com

Username: * administrator@vsphere.local

Password: * ●●●●●●●●●●

Port: * 443

7. From the vertical three-dot menu for the newly discovered vCenter server, select **Associate Storage Backend**.

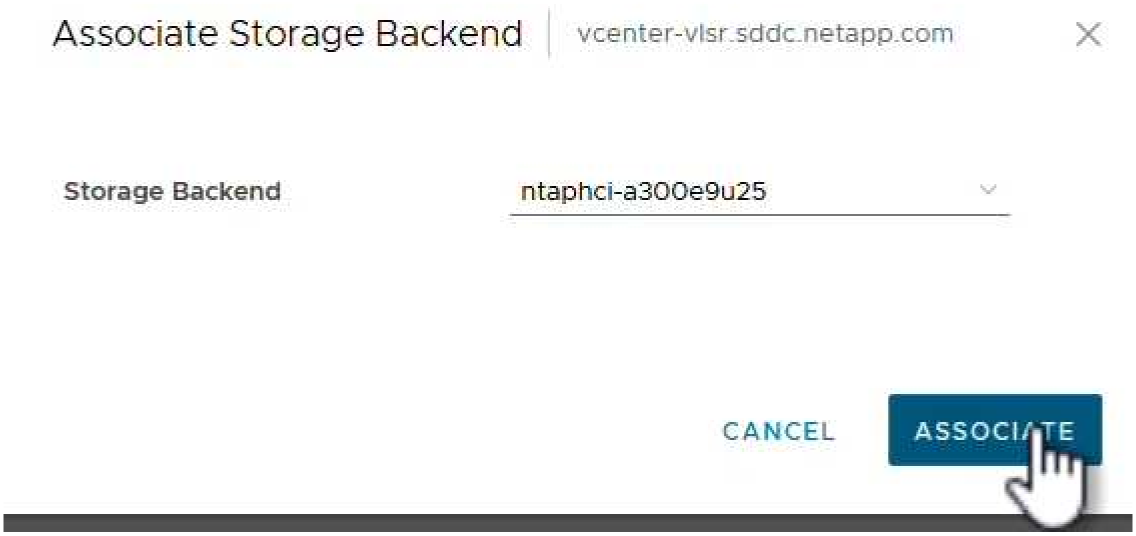


vCenters

vCenters are central management platforms that allow you to control hosts, virtual machines and storage backends.

Version	Status
8.0.2	Healthy

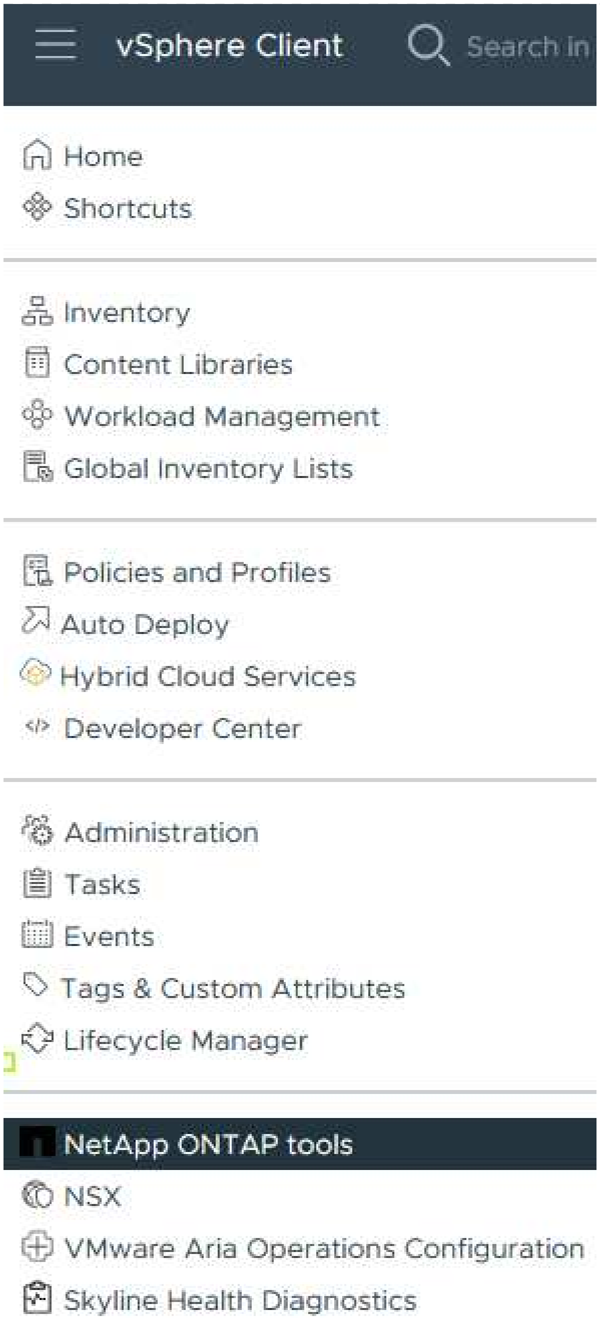
8. On the **Associate Storage Backend** box, select the ONTAP storage system to associated with the vCenter server and click on **Associate** to complete the action.



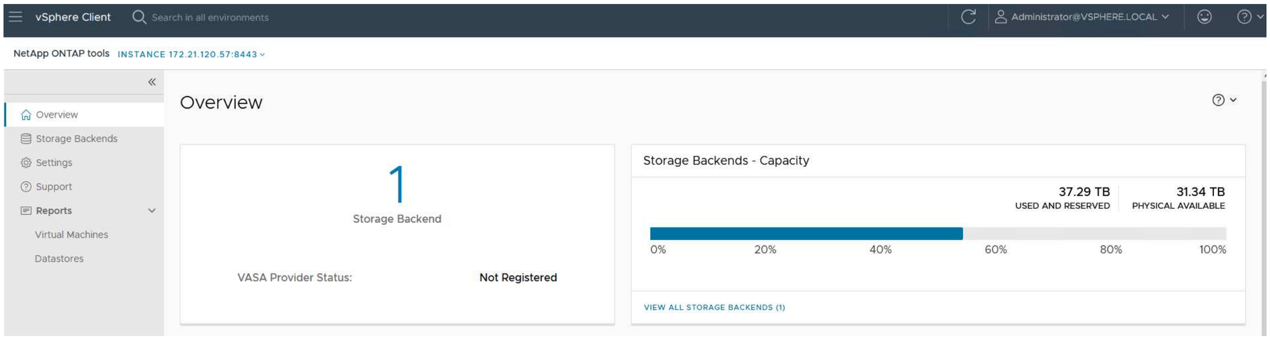
Associate Storage Backend | vcenter-vlsr.sddc.netapp.com

Storage Backend: ntaphci-a300e9u25

9. To verify the installation, log into the vSphere client and select **NetApp ONTAP tools** from the left hand menu.



10. From the ONTAP tools dashboard you should see that a Storage Backend was associated with the vCenter Server.



1 Storage Backend

VASA Provider Status: Not Registered

Storage Backends - Capacity

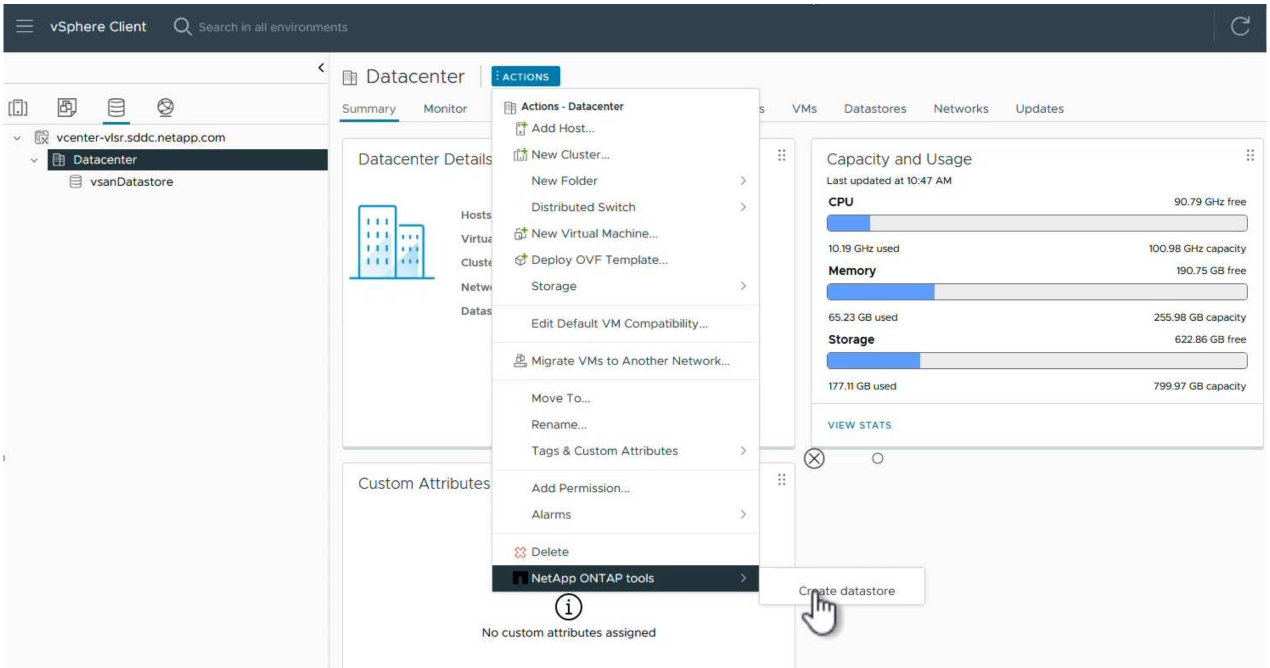
37.29 TB USED AND RESERVED

31.34 TB PHYSICAL AVAILABLE

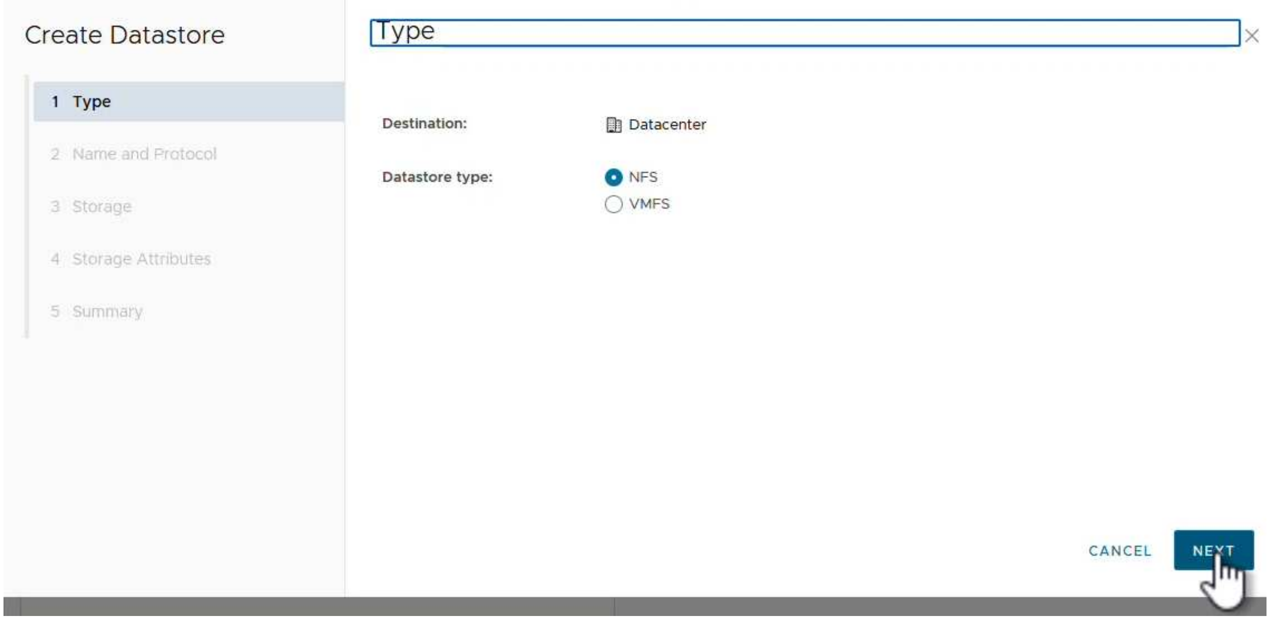
Create an NFS datastore using ONTAP tools 10

Complete the following steps to deploy an ONTAP datastore, running on NFS, using ONTAP tools 10.

1. In the vSphere client, navigate to the storage inventory. From the **ACTIONS** menu, select **NetApp ONTAP tools > Create datastore**.



2. On the **Type** page of the Create Datastore wizard, click on the NFS radio button and then on **Next** to continue.

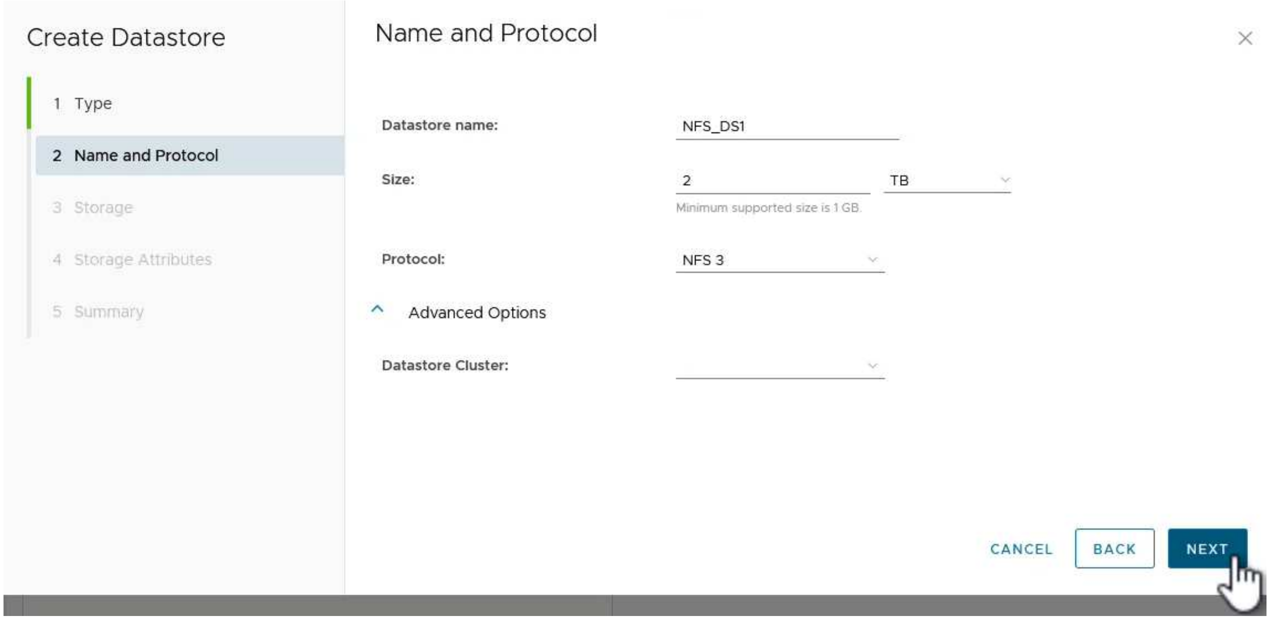


Destination: Datacenter

Datastore type: ● NFS ○ VMFS

3. On the **Name and Protocol** page, fill out the name, size and protocol for the datastore. Click on **Next**

to continue.


Create Datastore

1 Type

2 Name and Protocol

3 Storage

4 Storage Attributes

5 Summary

Name and Protocol

Datastore name: NFS_DS1

Size: 2 TB

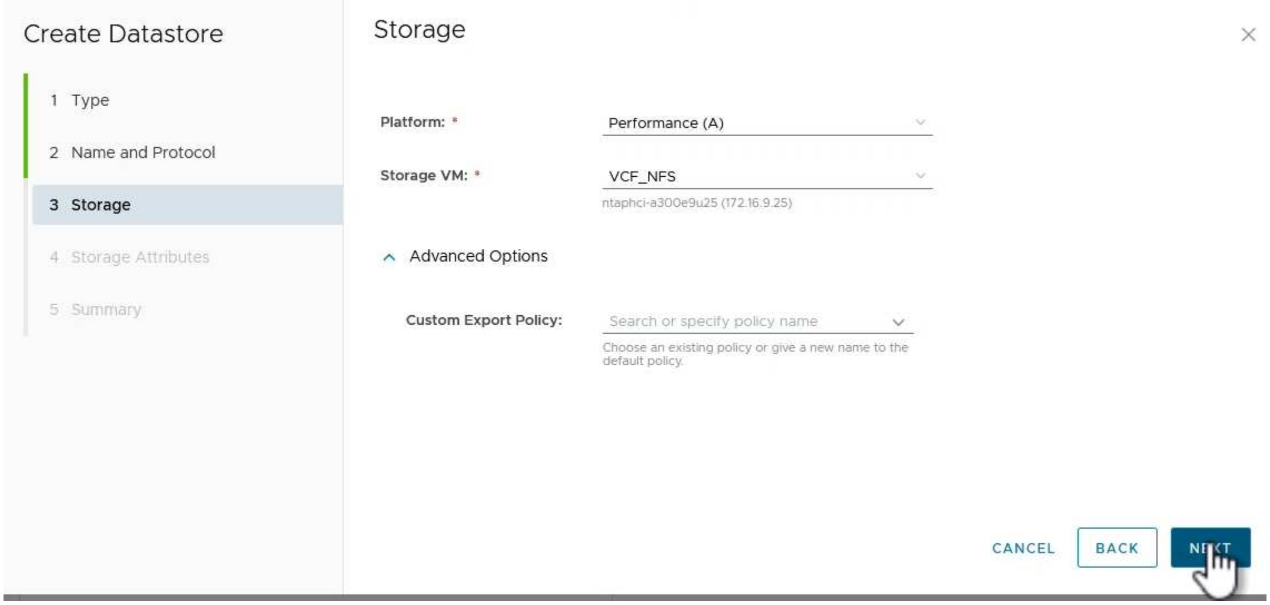
Minimum supported size is 1 GB.

Protocol: NFS 3

Advanced Options

Datastore Cluster:

4. On the **Storage** page select a Platform (filters storage system by type) and a storage VM for the volume. Optionally, select a custom export policy. Click on **Next** to continue.


Create Datastore

1 Type

2 Name and Protocol

3 Storage

4 Storage Attributes

5 Summary

Storage

Platform: * Performance (A)

Storage VM: * VCF_NFS

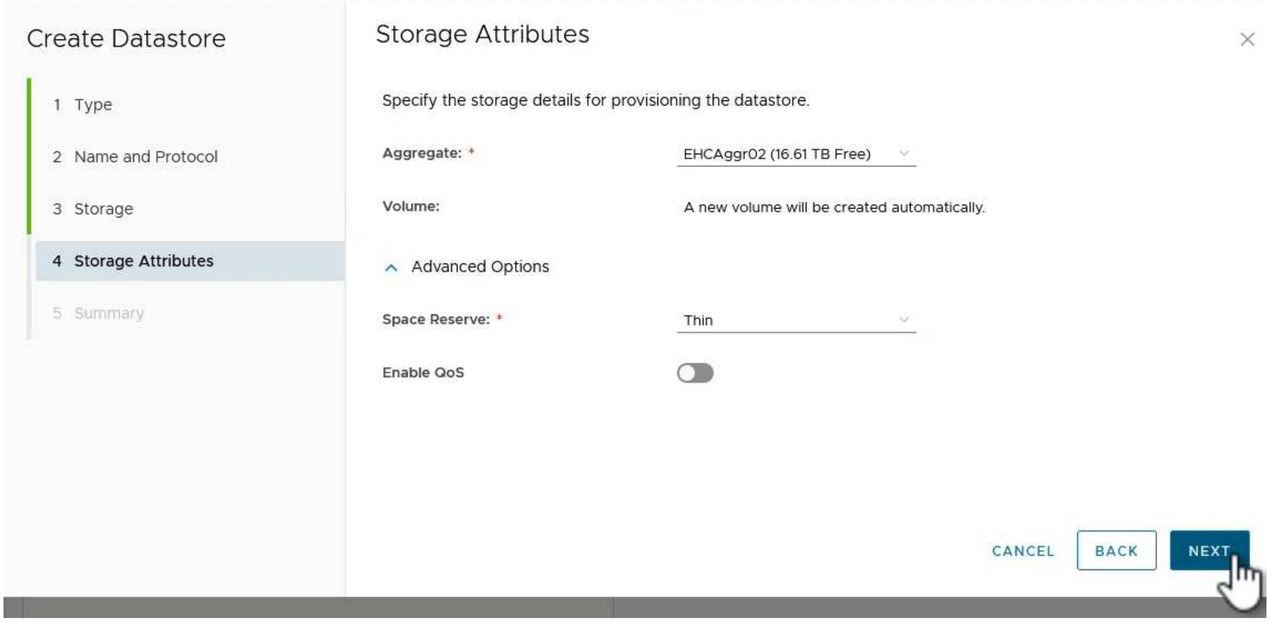
ntaphci-a300e9u25 (172.16.9.25)

Advanced Options

Custom Export Policy: Search or specify policy name

Choose an existing policy or give a new name to the default policy.

5. On the **Storage attributes** page select the storage aggregate to use, and optionally, advanced options such as space reservation and quality of service. Click on **Next** to continue.



Create Datastore

Storage Attributes

Specify the storage details for provisioning the datastore.

Aggregate: * EHCAggr02 (16.61 TB Free)

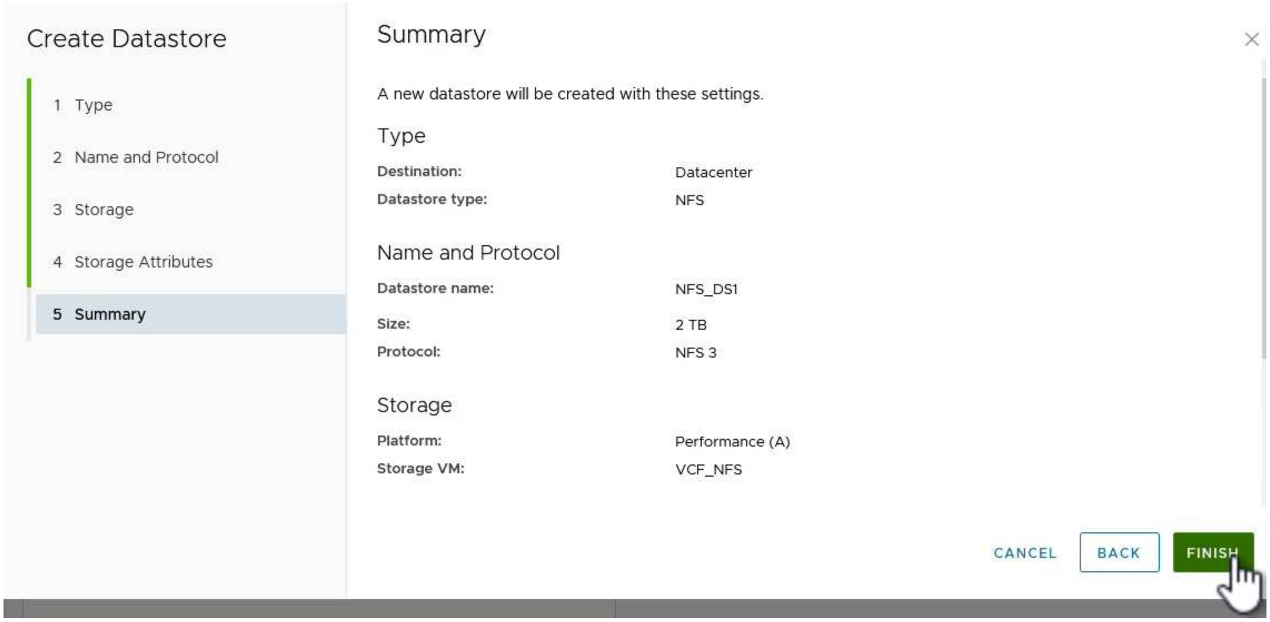
Volume: A new volume will be created automatically.

Advanced Options

Space Reserve: * Thin

Enable QoS

6. Finally, review the **Summary** and click on Finish to begin creating the NFS datastore.



Create Datastore

Summary

A new datastore will be created with these settings.

Type

Destination: Datacenter

Datastore type: NFS

Name and Protocol

Datastore name: NFS_DS1

Size: 2 TB

Protocol: NFS 3

Storage

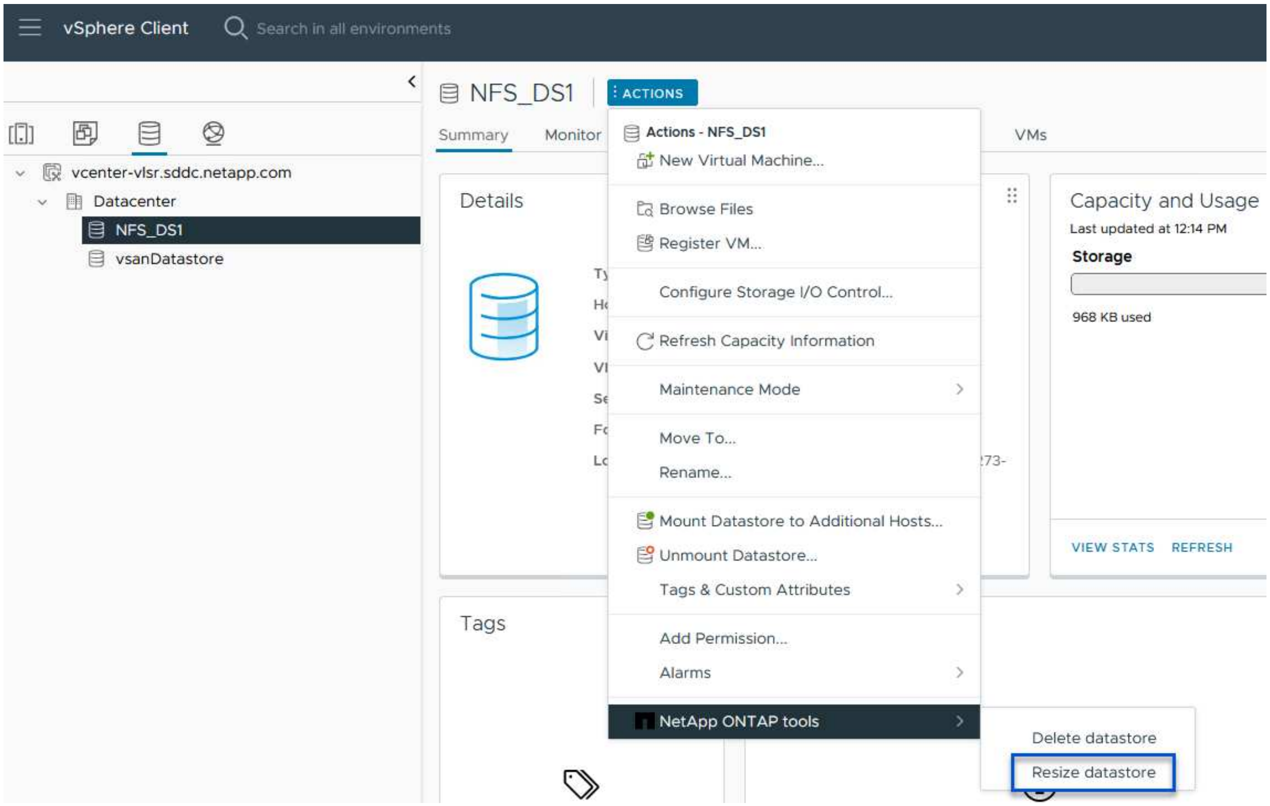
Platform: Performance (A)

Storage VM: VCF_NFS

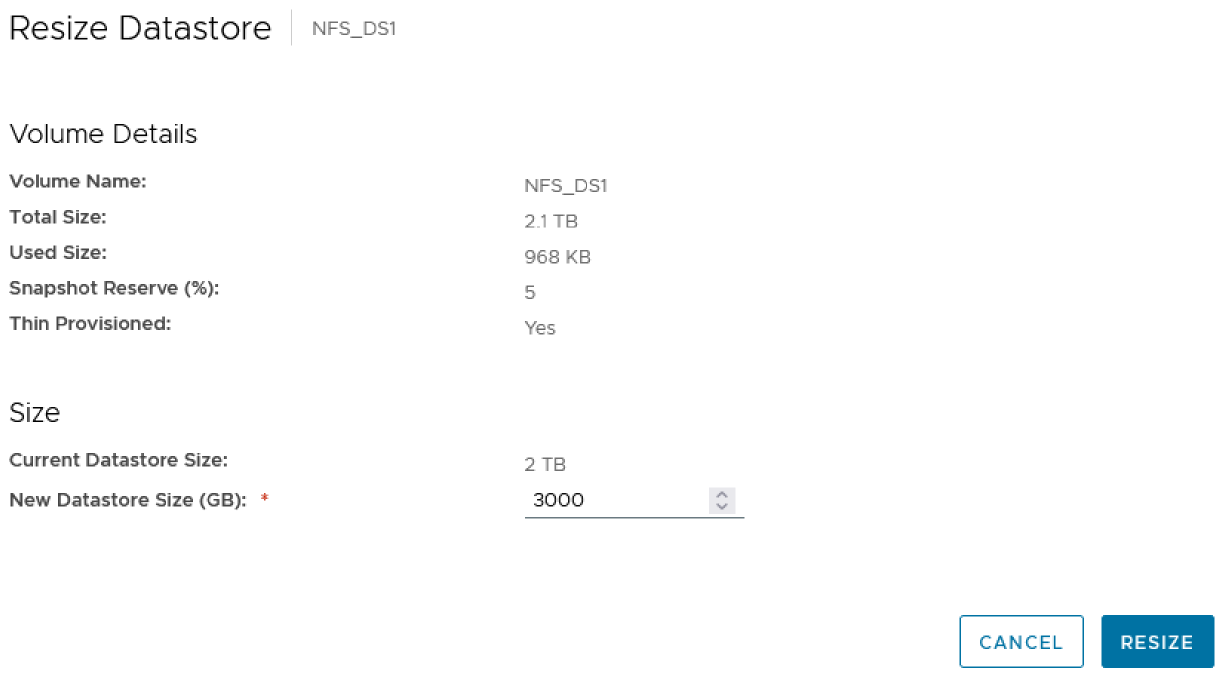
Resize an NFS datastore using ONTAP tools 10

Complete the following steps to resize an existing NFS datastore using ONTAP tools 10.

1. In the vSphere client, navigate to the storage inventory. From the **ACTIONS** menu, select **NetApp ONTAP tools > Resize datastore**.



2. On the **Resize Datastore** wizard, fill in the new size of the datastore in GB and click on **Resize** to continue.



Resize Datastore | NFS_DS1

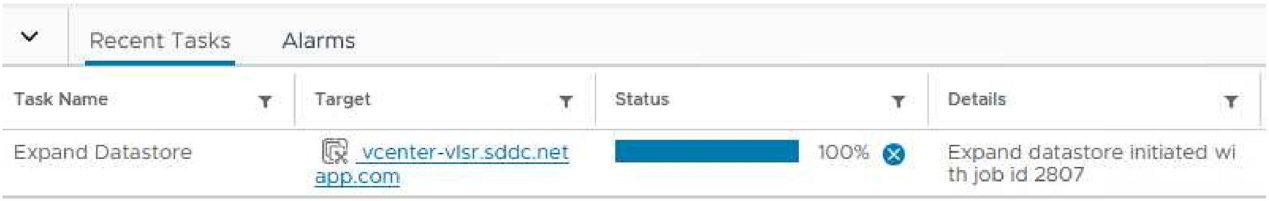
Volume Details

Volume Name:	NFS_DS1
Total Size:	2.1 TB
Used Size:	968 KB
Snapshot Reserve (%):	5
Thin Provisioned:	Yes

Size

Current Datastore Size:	2 TB
New Datastore Size (GB): *	3000

3. Monitor the progress of the resize job in the **Recent Tasks** pane.



Task Name	Target	Status	Details
Expand Datastore	vcenter-vlsr.sddc.netapp.com	100%	Expand datastore initiated with job id 2807

Additional information

For a complete listing of ONTAP tools for VMware vSphere 10 resources refer to ONTAP tools for VMware vSphere Documentation Resources.

For more information on configuring ONTAP storage systems refer to the ONTAP 10 Documentation center.

Use VMware Site Recovery Manager for Disaster Recovery of NFS datastores

The utilization of ONTAP tools for VMware vSphere 10 and the Site Replication Adapter (SRA) in conjunction with VMware Site Recovery Manager (SRM) brings significant value to disaster recovery efforts. ONTAP tools 10 provide robust storage capabilities, including native high availability and scalability for the VASA Provider, supporting iSCSI and NFS vVols. This ensures data availability and simplifies the management of multiple VMware vCenter servers and ONTAP clusters. By using the SRA with VMware Site Recovery Manager, organizations can achieve seamless replication and failover of virtual machines and data between sites, enabling efficient disaster recovery processes. The combination of ONTAP tools and the SRA empowers businesses to protect critical workloads, minimize downtime, and maintain business continuity in the face of unforeseen events or disasters.

ONTAP tools 10 simplifies storage management and efficiency features, enhances availability, and reduces storage costs and operational overhead, whether you are using SAN or NAS. It uses best practices for provisioning datastores and optimizes ESXi host settings for NFS and block storage environments. For all these benefits, NetApp recommends this plug-in when using vSphere with systems running ONTAP software.

The SRA is used together with SRM to manage the replication of VM data between production and disaster recovery sites for traditional VMFS and NFS datastores and also for the nondisruptive testing of DR replicas. It helps automate the tasks of discovery, recovery, and reprotection.

In this scenario we will demonstrate how to deploy and use VMWare Site Recovery manager to protect datastores and run both a test and final failover to a secondary site. Reprotection and failback are also discussed.

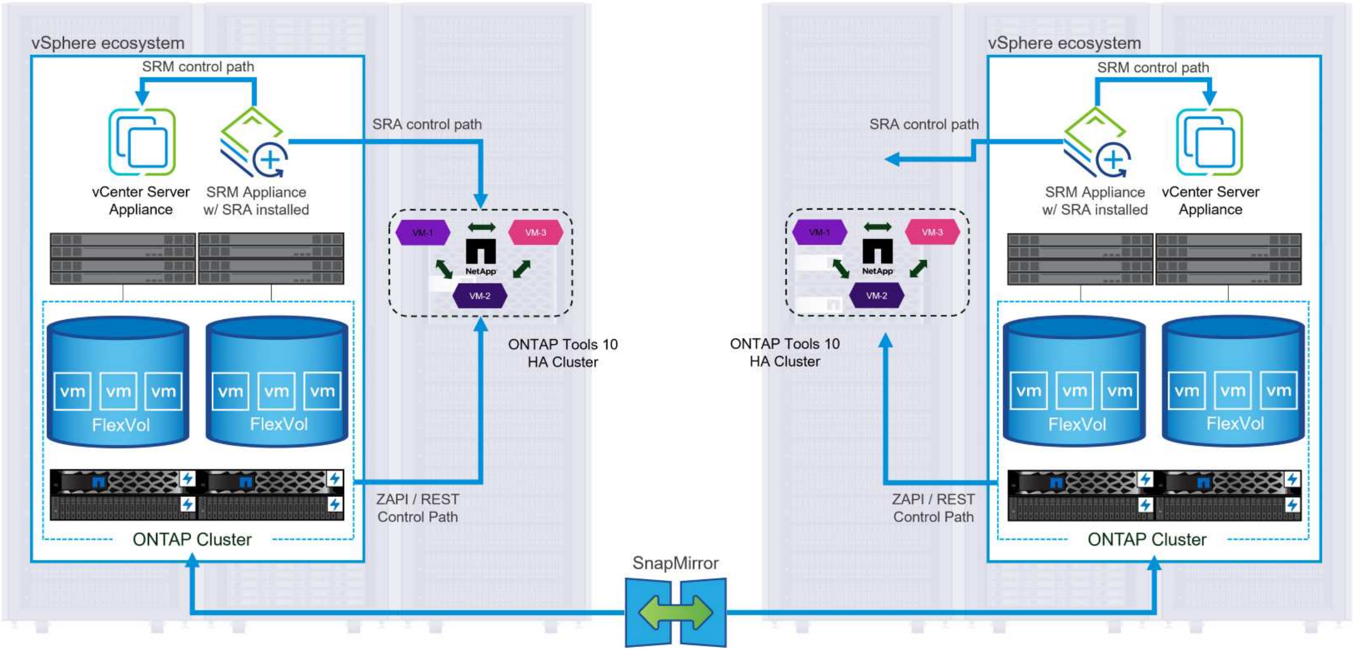
Scenario Overview

This scenario covers the following high level steps:

- Configure SRM with vCenter servers at primary and secondary sites.
- Install the SRA adapter for ONTAP tools for VMware vSphere 10 and register with vCenters.
- Create SnapMirror relationships between source and destination ONTAP storage systems
- Configure Site Recovery for SRM.
- Conduct test and final failover.
- Discuss reprotection and failback.

Architecture

The following diagram shows a typical VMware Site Recovery architecture with ONTAP tools for VMware vSphere 10 configured in a 3-node high availability configuration.



Prerequisites

This scenario requires the following components and configurations:

- vSphere 8 clusters installed at both the primary and secondary locations with suitable networking for communications between environments.
- ONTAP storage systems at both the primary and secondary locations, with physical data ports on ethernet switches dedicated to NFS storage traffic.
- ONTAP tools for VMware vSphere 10 is installed and has both vCenter servers registered.
- VMware Site Replication Manager appliances have been installed for the primary and secondary sites.
    - Inventory mappings (network, folder, resource, storage policy) have been configured for SRM.

NetApp recommends a redundant network designs for NFS, providing fault tolerance for storage systems, switches, networks adapters and host systems. It is common to deploy NFS with a single subnet or multiple subnets depending on the architectural requirements.

Refer to Best Practices For Running NFS with VMware vSphere for detailed information specific to VMware vSphere.

For network guidance on using ONTAP with VMware vSphere refer to the Network configuration - NFS section of the NetApp enterprise applications documentation.

For NetApp documentation on using ONTAP storage with VMware SRM refer to VMware Site Recovery Manager with ONTAP

Deployment Steps

The following sections outline the deployment steps to implement and test a VMware Site Recovery Manager configuration with ONTAP storage system.

Create SnapMirror relationship between ONTAP storage systems

A SnapMirror relationship must be established between the source and destination ONTAP storage systems, for the datastore volumes to be protected.

Refer to ONTAP documentation starting HERE for complete information on creating SnapMirror relationships for ONTAP volumes.

Step-by-step instructions are outline in the following document, located HERE. These steps outline how to create cluster peer and SVM peer relationships and then SnapMirror relationships for each volume. These steps can be performed in ONTAP System Manager or using the ONTAP CLI.

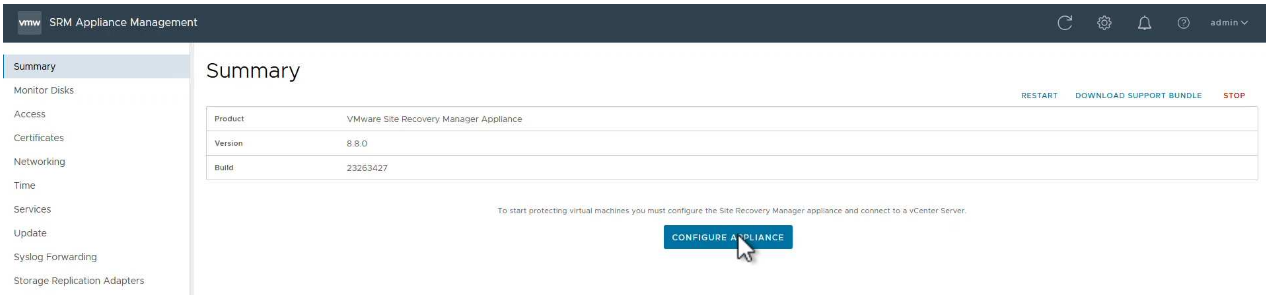
Configure the SRM appliance

Complete the following steps to configure the SRM appliance and SRA adapter.

Connect the SRM appliance for primary and secondary sites

The following steps must be completed for both the primary and secondary sites.

1. In a web browser, navigate to `https://<SRM_appliance_IP>:5480` and log in. Click on **Configure Appliance** to get started.

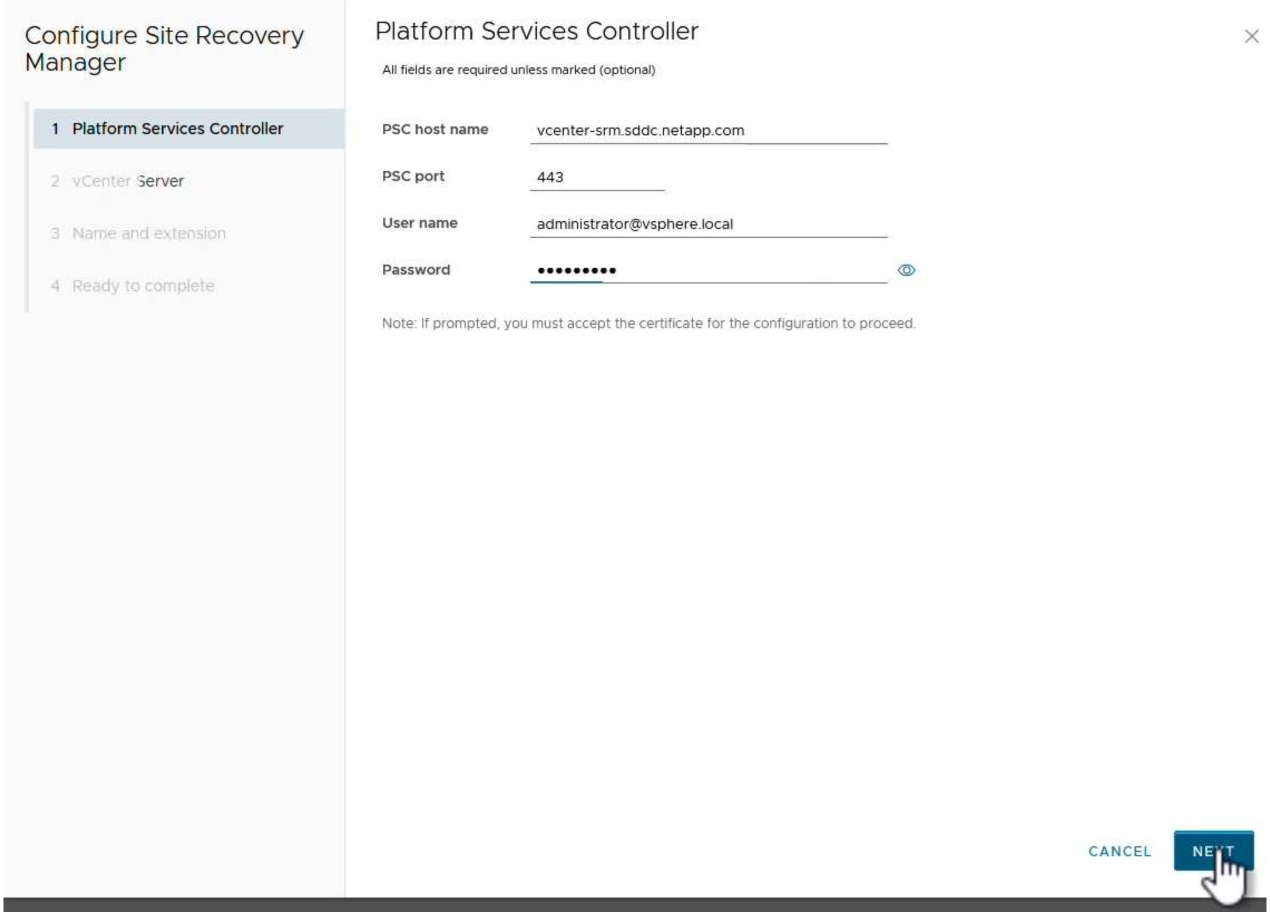


Summary

Product	VMware Site Recovery Manager Appliance
Version	8.8.0
Build	23263427

To start protecting virtual machines you must configure the Site Recovery Manager appliance and connect to a vCenter Server.

2. On the **Platform Services Controller** page of the Configure Site Recovery Manager wizard, fill in the credentials of the vCenter server to which SRM will be registered. Click on **Next** to continue.



Platform Services Controller

All fields are required unless marked (optional)

PSC host name: vcenter-srm.sddc.netapp.com

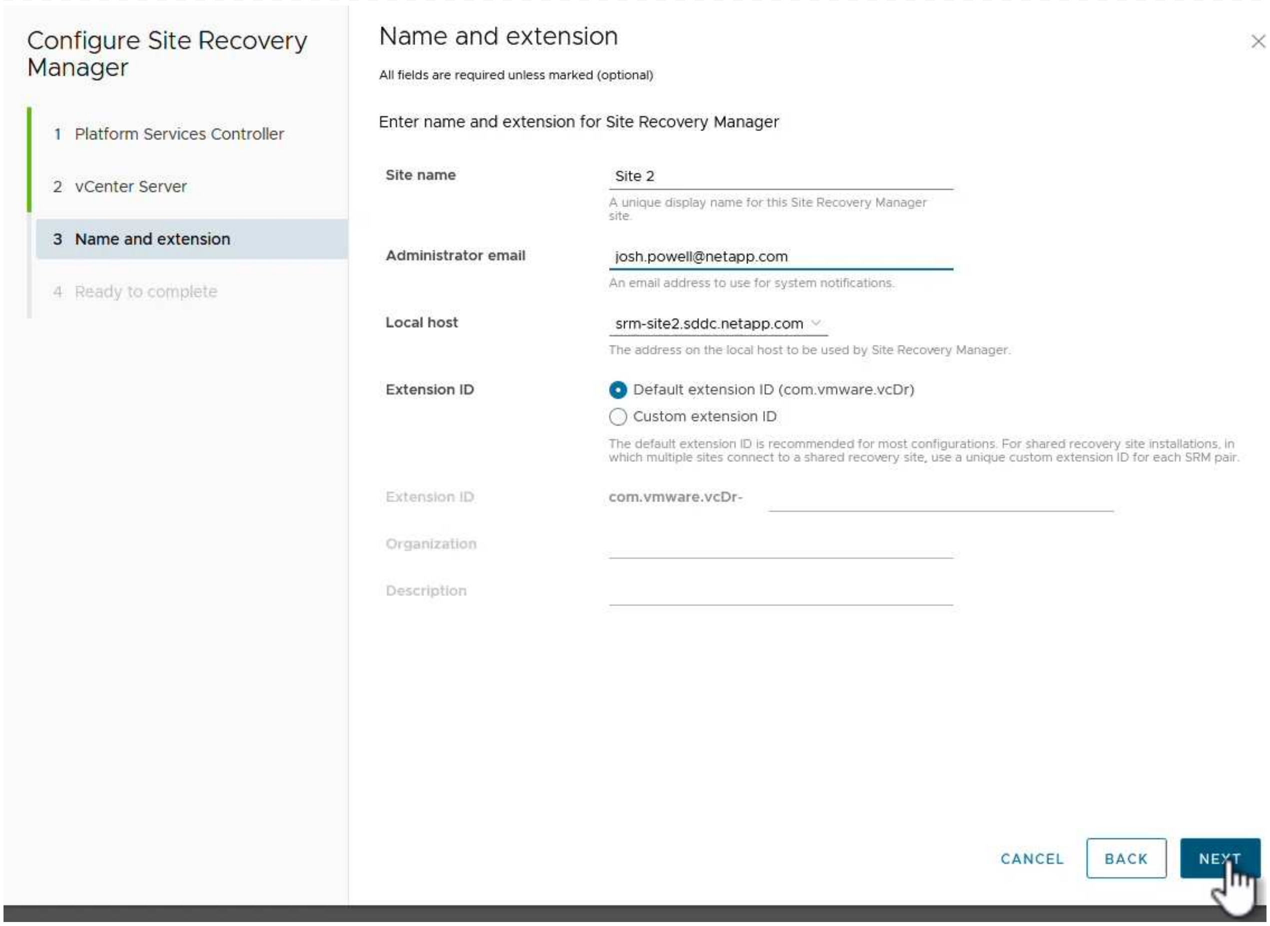
PSC port: 443

User name: administrator@vsphere.local

Password: ••••••••••

Note: If prompted, you must accept the certificate for the configuration to proceed.

3. On the **vCenter Server** page, view the connected vServer and click on **Next** to continue.
4. On the **Name and extension** page, fill in a name for the SRM site, an administrators email address, and the local host to be used by SRM. Click on **Next** to continue.


Configure Site Recovery Manager

1 Platform Services Controller

2 vCenter Server

3 Name and extension

4 Ready to complete

Name and extension

All fields are required unless marked (optional)

Enter name and extension for Site Recovery Manager

Site name: Site 2

A unique display name for this Site Recovery Manager site.

Administrator email: josh.powell@netapp.com

An email address to use for system notifications.

Local host: srm-site2.sddc.netapp.com

The address on the local host to be used by Site Recovery Manager.

Extension ID:

● Default extension ID (com.vmware.vcDr)

○ Custom extension ID

The default extension ID is recommended for most configurations. For shared recovery site installations, in which multiple sites connect to a shared recovery site, use a unique custom extension ID for each SRM pair.

Extension ID: com.vmware.vcDr-

Organization

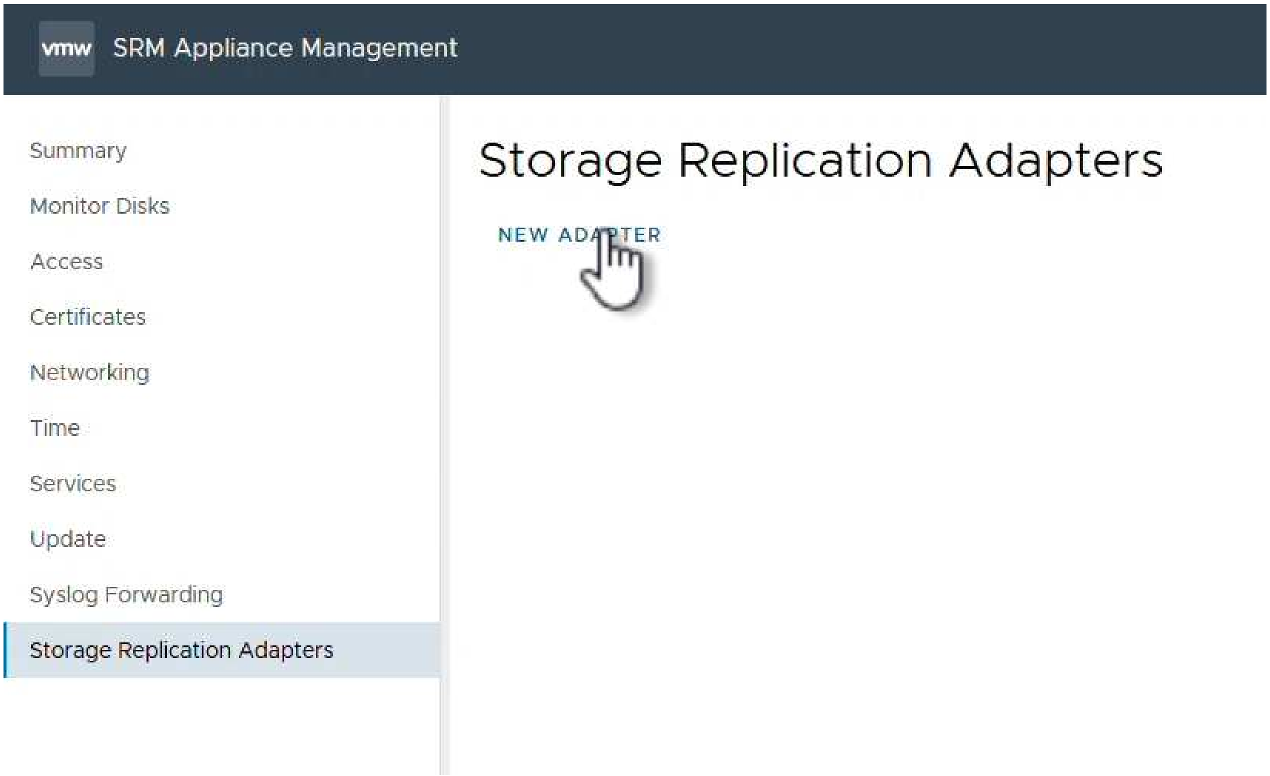
Description

5. On the **Ready to complete** page review the summary of changes

Configure SRA on the SRM appliance

Complete the following steps to configure the SRA on the SRM appliance:

1. Download the SRA for ONTAP tools 10 at the NetApp support site and save the tar.gz file to a local folder.
2. From the SRM management appliance click on **Storage Replication Adapters** in the left hand menu and then on **New Adapter**.



3. Follow the steps outlined on the ONTAP tools 10 documentation site at Configure SRA on the SRM appliance. Once complete, the SRA can communicate with SRA using the provided IP address and credentials of the vCenter server.

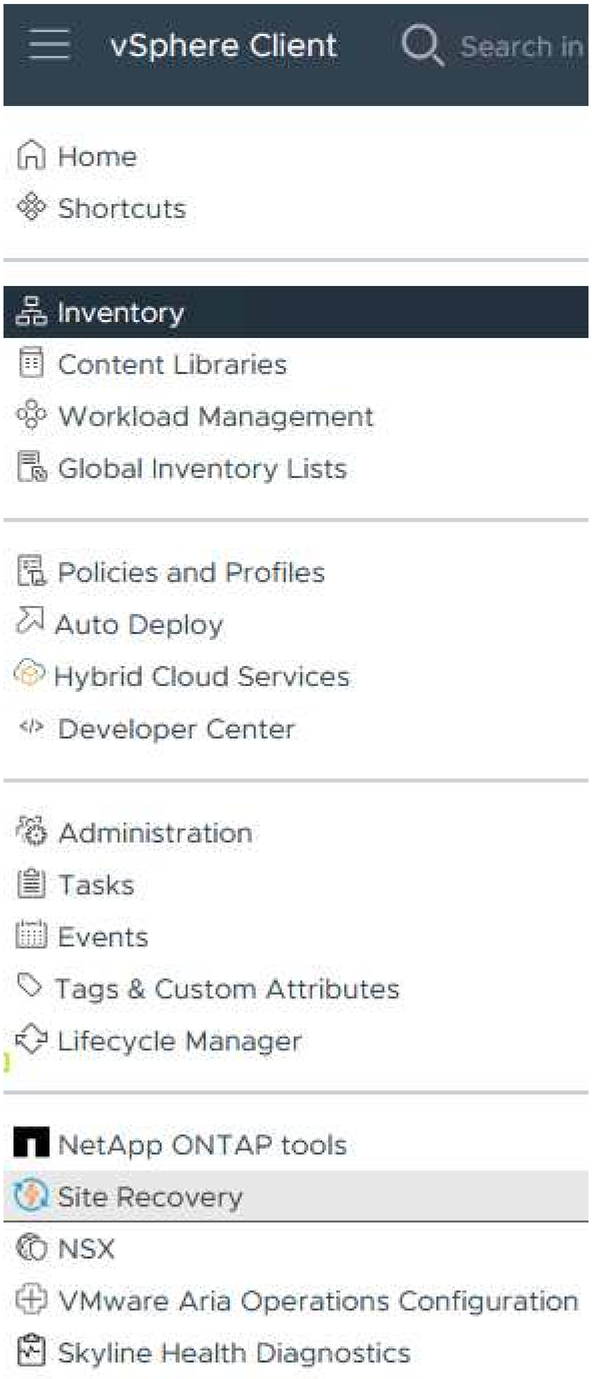
Configure Site Recovery for SRM

Complete the following steps to configure Site Pairing, create Protection Groups,

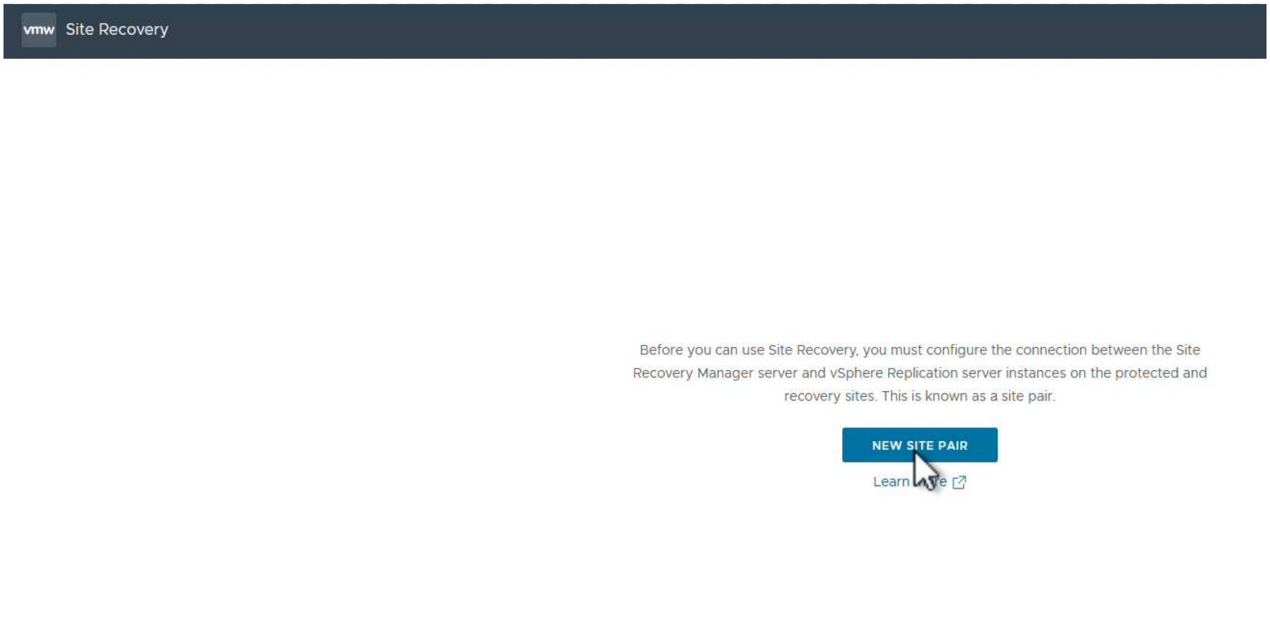
Configure Site Pairing for SRM

The following step is completed in the vCenter client of the primary site.

1. In the vSphere client click on **Site Recovery** in the left hand menu. A new browser windows opens to the SRM management UI on the primary site.

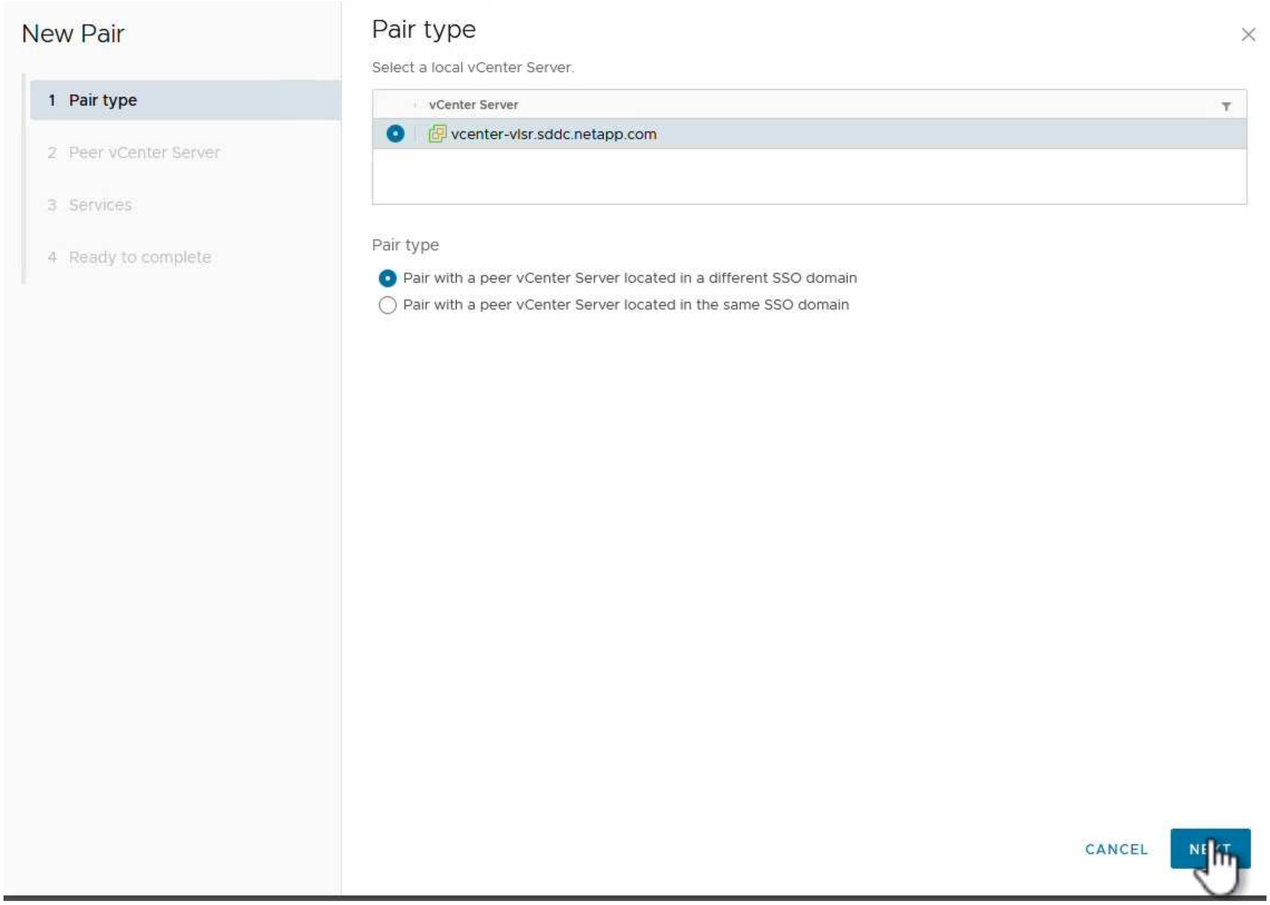


2. On the **Site Recovery** page, click on **NEW SITE PAIR**.



Before you can use Site Recovery, you must configure the connection between the Site Recovery Manager server and vSphere Replication server instances on the protected and recovery sites. This is known as a site pair.

3. On the **Pair type** page of the **New Pair wizard**, verify that the local vCenter server is selected and select the **Pair type**. Click on **Next** to continue.



Pair type

Select a local vCenter Server.

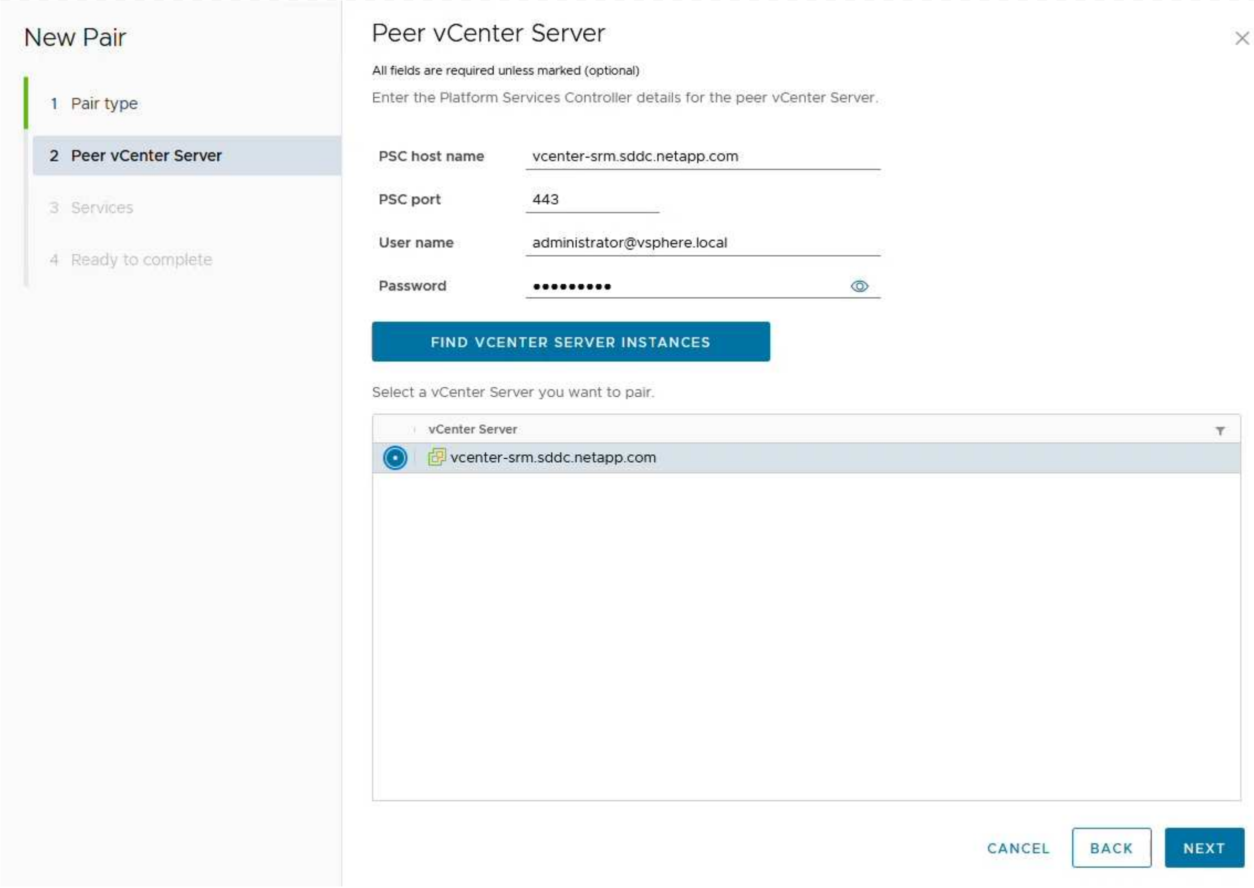
	vCenter Server
●	vcenter-vlsr.sddc.netapp.com

Pair type

● Pair with a peer vCenter Server located in a different SSO domain

○ Pair with a peer vCenter Server located in the same SSO domain

4. On the **Peer vCenter** page fill out the credentials of the vCenter at the secondary site and click on **Find vCenter Instances**. Verify the the vCenter instance has been discovered and click on **Next** to continue.



Peer vCenter Server

All fields are required unless marked (optional)

Enter the Platform Services Controller details for the peer vCenter Server.

PSC host name: vcenter-srm.sddc.netapp.com

PSC port: 443

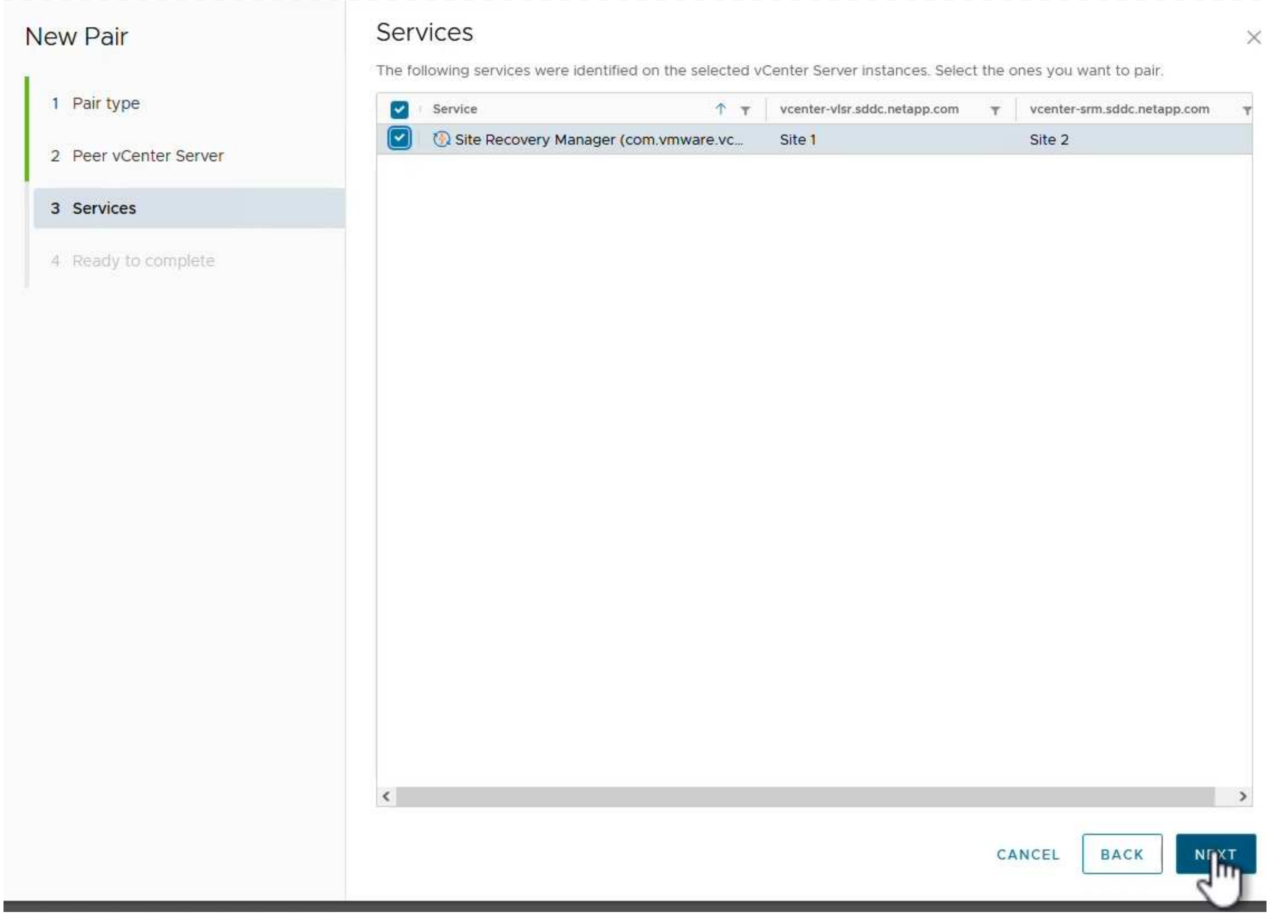
User name: administrator@vsphere.local

Password: ••••••••••

Select a vCenter Server you want to pair.

	vCenter Server
●	vcenter-srm.sddc.netapp.com

5. On the **Services** page, check the box next the proposed site pairing. Click on **Next** to continue.



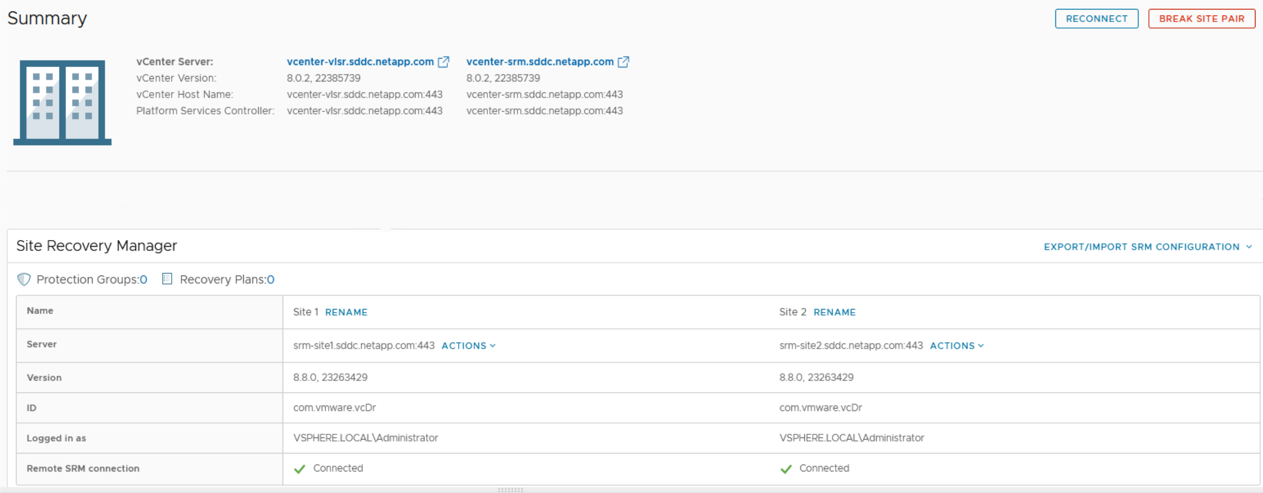
Services

The following services were identified on the selected vCenter Server instances. Select the ones you want to pair.

☑ Service	vcenter-vlsr.sddc.netapp.com	vcenter-srm.sddc.netapp.com
☑ Site Recovery Manager (com.vmware.vc...	Site 1	Site 2

6. On the **Ready to complete** page, review the proposed configuration and then click on the **Finish** button to create the Site Pairing

7. The new Site Pair and its summary can be viewed on the Summary page.



Summary

vCenter Server:	vcenter-vlsr.sddc.netapp.com	vcenter-srm.sddc.netapp.com
vCenter Version:	8.0.2, 22385739	8.0.2, 22385739
vCenter Host Name:	vcenter-vlsr.sddc.netapp.com:443	vcenter-srm.sddc.netapp.com:443
Platform Services Controller:	vcenter-vlsr.sddc.netapp.com:443	vcenter-srm.sddc.netapp.com:443

Site Recovery Manager

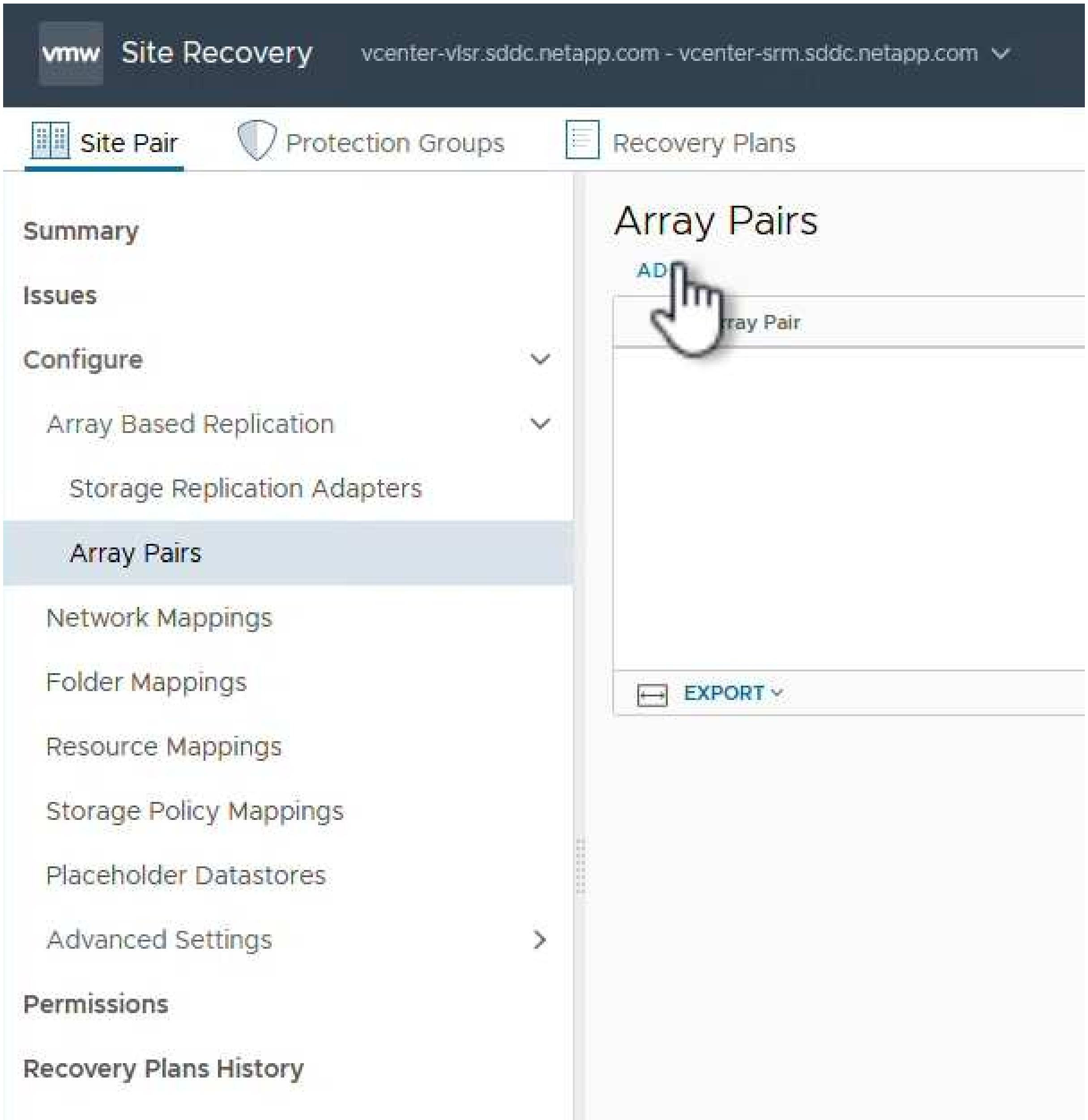
Protection Groups:0 Recovery Plans:0

Name	Site 1 RENAME	Site 2 RENAME
Server	srm-site1.sddc.netapp.com:443 ACTIONS	srm-site2.sddc.netapp.com:443 ACTIONS
Version	8.8.0, 23263429	8.8.0, 23263429
ID	com.vmware.vcDr	com.vmware.vcDr
Logged in as	VSPHERE.LOCAL\Administrator	VSPHERE.LOCAL\Administrator
Remote SRM connection	✓ Connected	✓ Connected

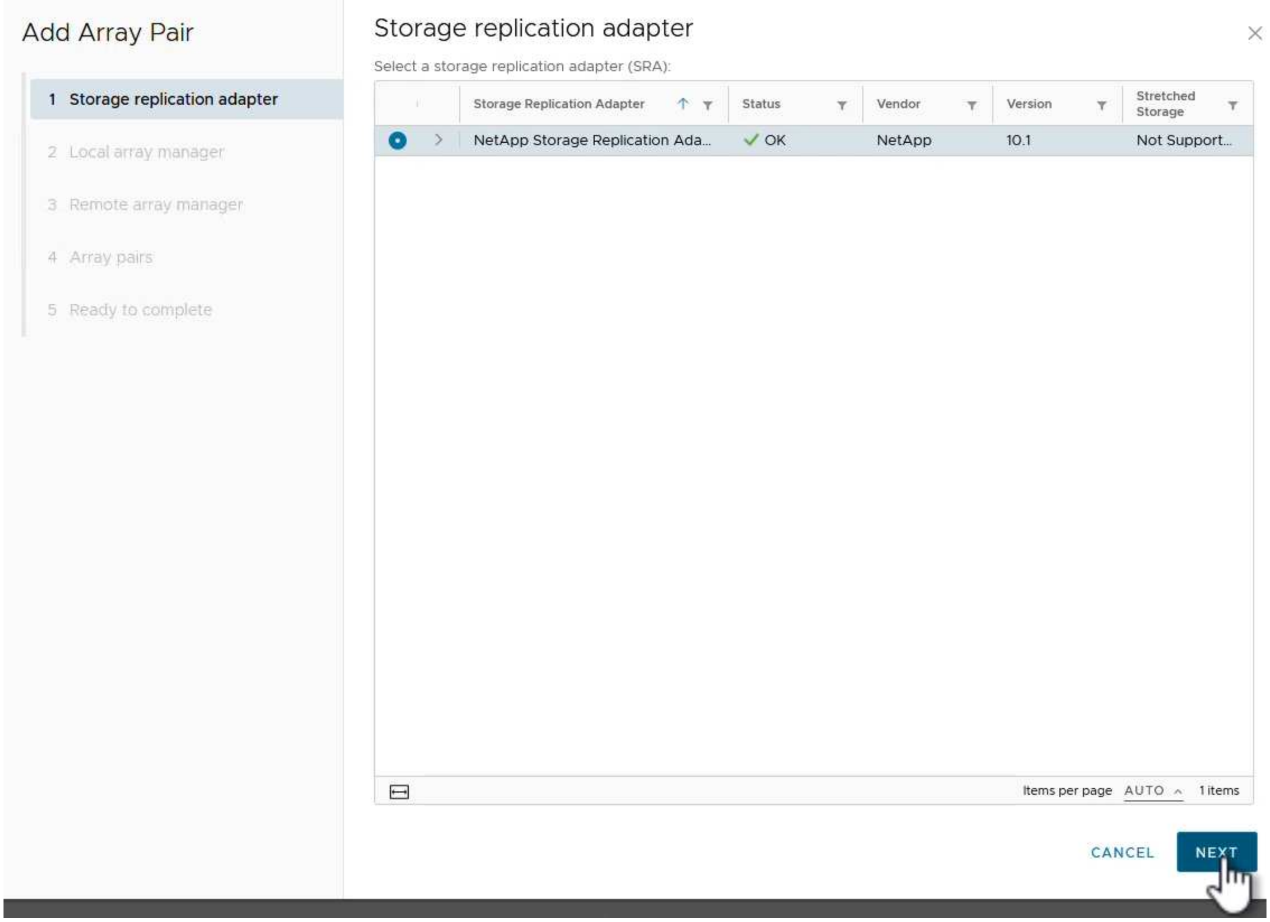
Add an Array Pair for SRM

The following step is completed in the Site Recovery interface of the primary site.

1. In the Site Recovery interface navigate to **Configure > Array Based Replication > Array Pairs** in the left hand menu. Click on **ADD** to get started.



2. On the **Storage replication adapter** page of the **Add Array Pair** wizard, verify the SRA adapter is present for the primary site and click on **Next** to continue.



Add Array Pair

1 Storage replication adapter
2 Local array manager
3 Remote array manager
4 Array pairs
5 Ready to complete

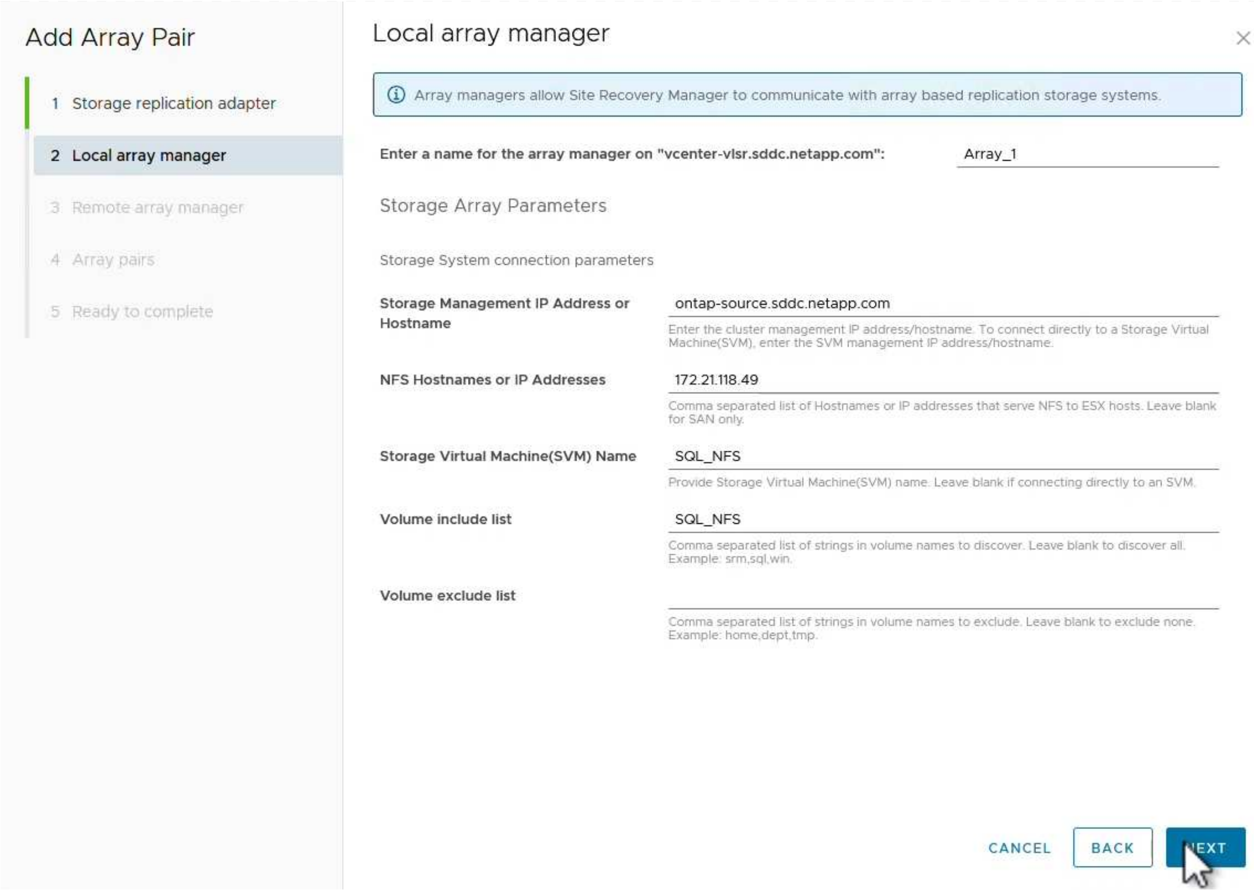
Storage replication adapter

Select a storage replication adapter (SRA):

	Storage Replication Adapter	Status	Vendor	Version	Stretched Storage
●	NetApp Storage Replication Ada...	✓ OK	NetApp	10.1	Not Support...

Items per page AUTO 1 items

3. On the **Local array manager** page, enter a name for the array at the primary site, the FQDN of the storage system, the SVM IP addresses serving NFS, and optionally, the names of specific volumes to be discovered. Click on **Next** to continue.



Local array manager

Array managers allow Site Recovery Manager to communicate with array based replication storage systems.

Enter a name for the array manager on "vcenter-vlsr.sddc.netapp.com": Array_1

Storage Array Parameters

Storage System connection parameters

Storage Management IP Address or Hostname: ontap-source.sddc.netapp.com
Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.

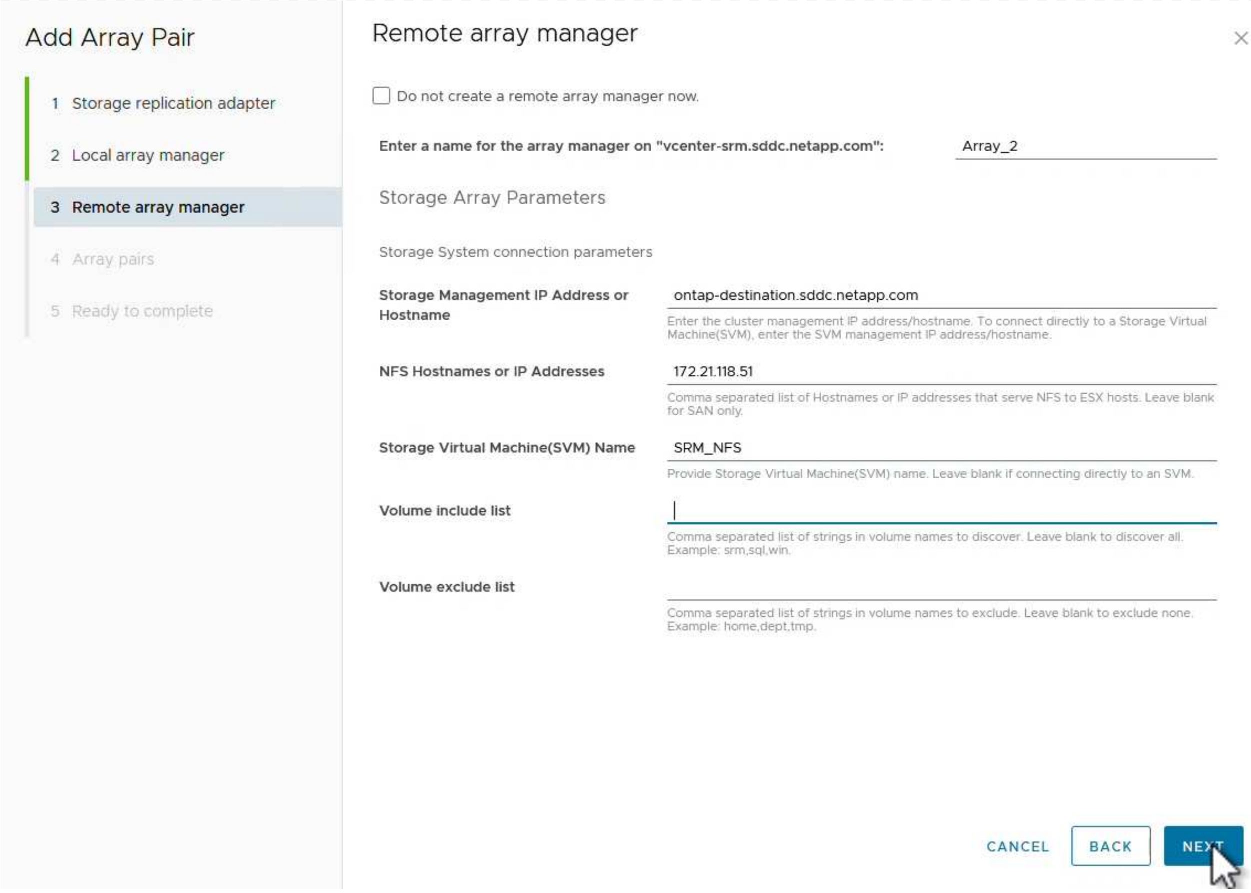
NFS Hostnames or IP Addresses: 172.21.118.49
Comma separated list of Hostnames or IP addresses that serve NFS to ESX hosts. Leave blank for SAN only.

Storage Virtual Machine(SVM) Name: SQL_NFS
Provide Storage Virtual Machine(SVM) name. Leave blank if connecting directly to an SVM.

Volume include list: SQL_NFS
Comma separated list of strings in volume names to discover. Leave blank to discover all. Example: srm,sql,win.

Volume exclude list:
Comma separated list of strings in volume names to exclude. Leave blank to exclude none. Example: home,dept,tmp.

4. On the **Remote array manager** fill out the same information as the last step for the ONTAP storage system at the secondary site.



Remote array manager

□ Do not create a remote array manager now.

Enter a name for the array manager on "vcenter-srm.sddc.netapp.com": Array_2

Storage Array Parameters

Storage System connection parameters

Storage Management IP Address or Hostname: ontap-destination.sddc.netapp.com

Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.

NFS Hostnames or IP Addresses: 172.21.118.51

Comma separated list of Hostnames or IP addresses that serve NFS to ESX hosts. Leave blank for SAN only.

Storage Virtual Machine(SVM) Name: SRM_NFS

Provide Storage Virtual Machine(SVM) name. Leave blank if connecting directly to an SVM.

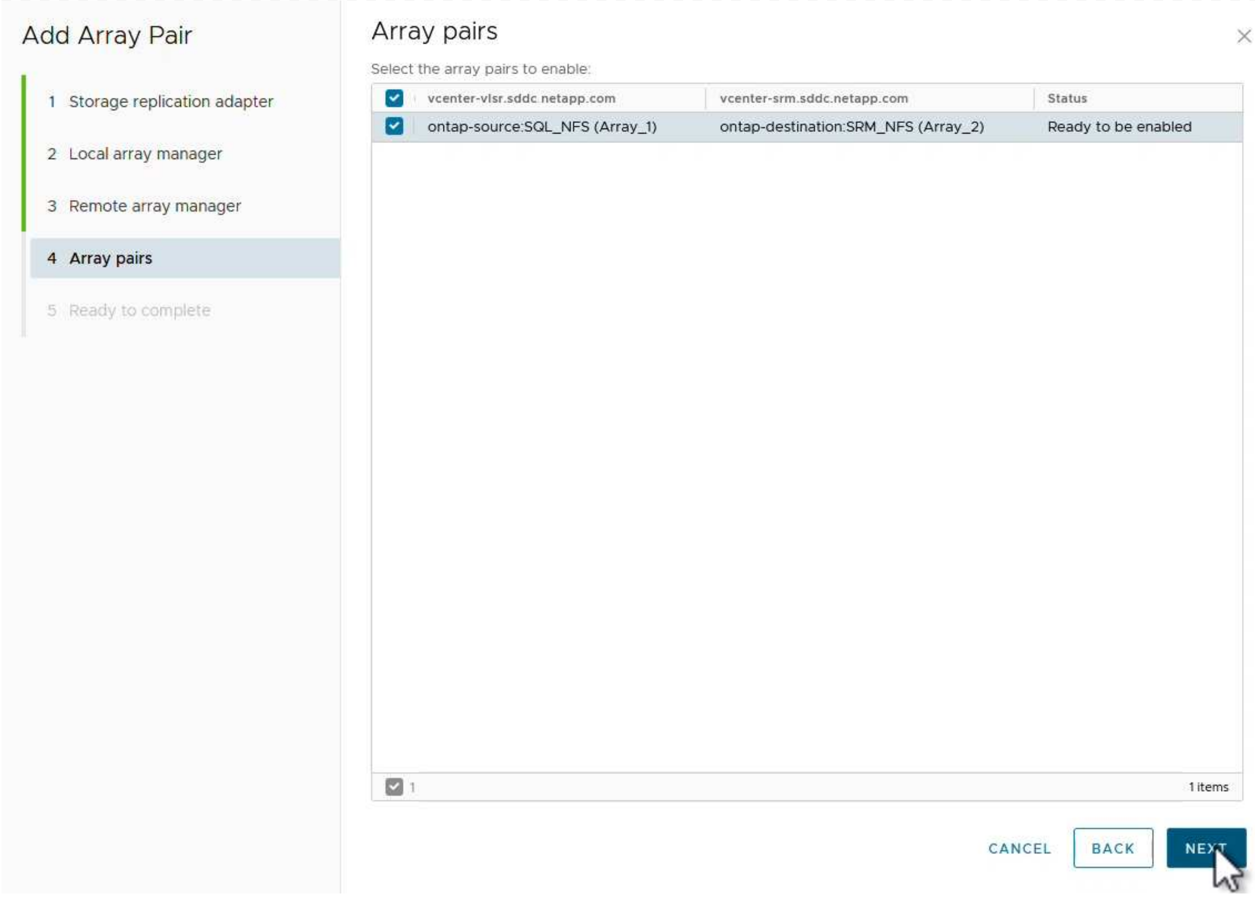
Volume include list:

Comma separated list of strings in volume names to discover. Leave blank to discover all. Example: srm,sql,win.

Volume exclude list:

Comma separated list of strings in volume names to exclude. Leave blank to exclude none. Example: home,dept,tmp.

5. On the **Array pairs** page, select the array pairs to enable and click on **Next** to continue.



Select the array pairs to enable:

☑	vcenter-vlsr.sddc.netapp.com	vcenter-srm.sddc.netapp.com	Status
☑	ontap-source:SQL_NFS (Array_1)	ontap-destination:SRM_NFS (Array_2)	Ready to be enabled

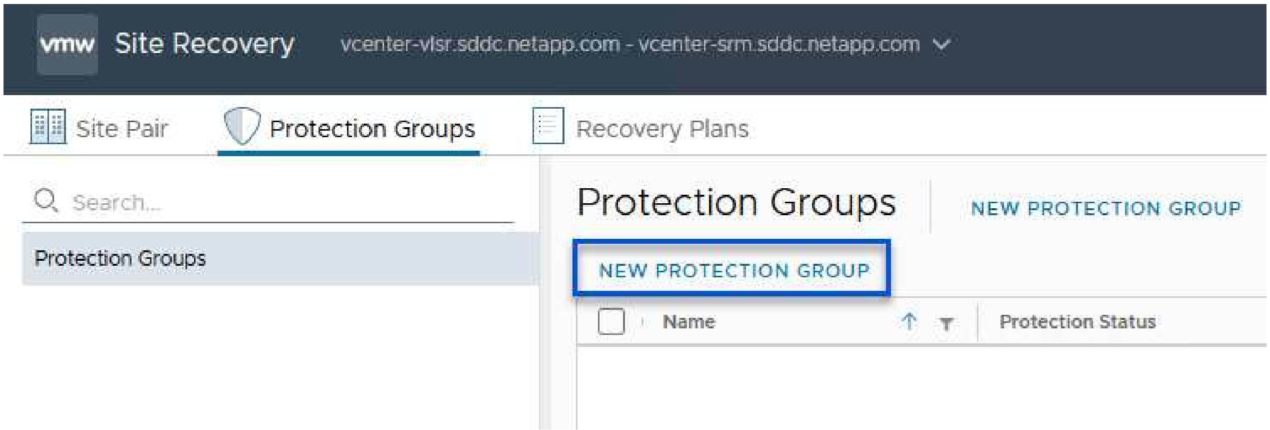
☑ 1 1 items

6. Review the information on the **Ready to complete** page and click on **Finish** to create the array pair.

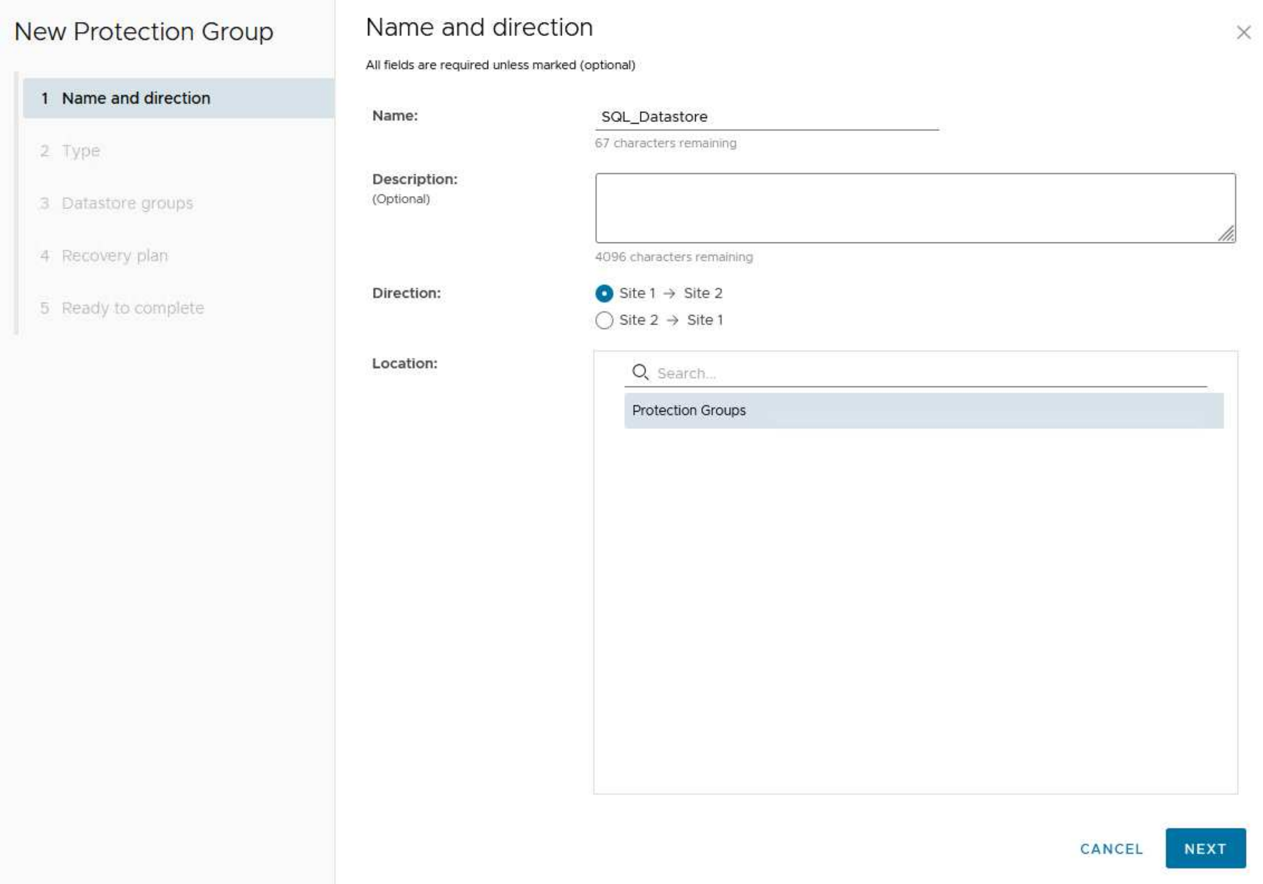
Configure Protection Groups for SRM

The following step is completed in the Site Recovery interface of the primary site.

1. In the Site Recovery interface click on the **Protection Groups** tab and then on **New Protection Group** to get started.



2. On the **Name and direction** page of the **New Protection Group** wizard, provide a name for the group and choose the site direction for protection of the data.



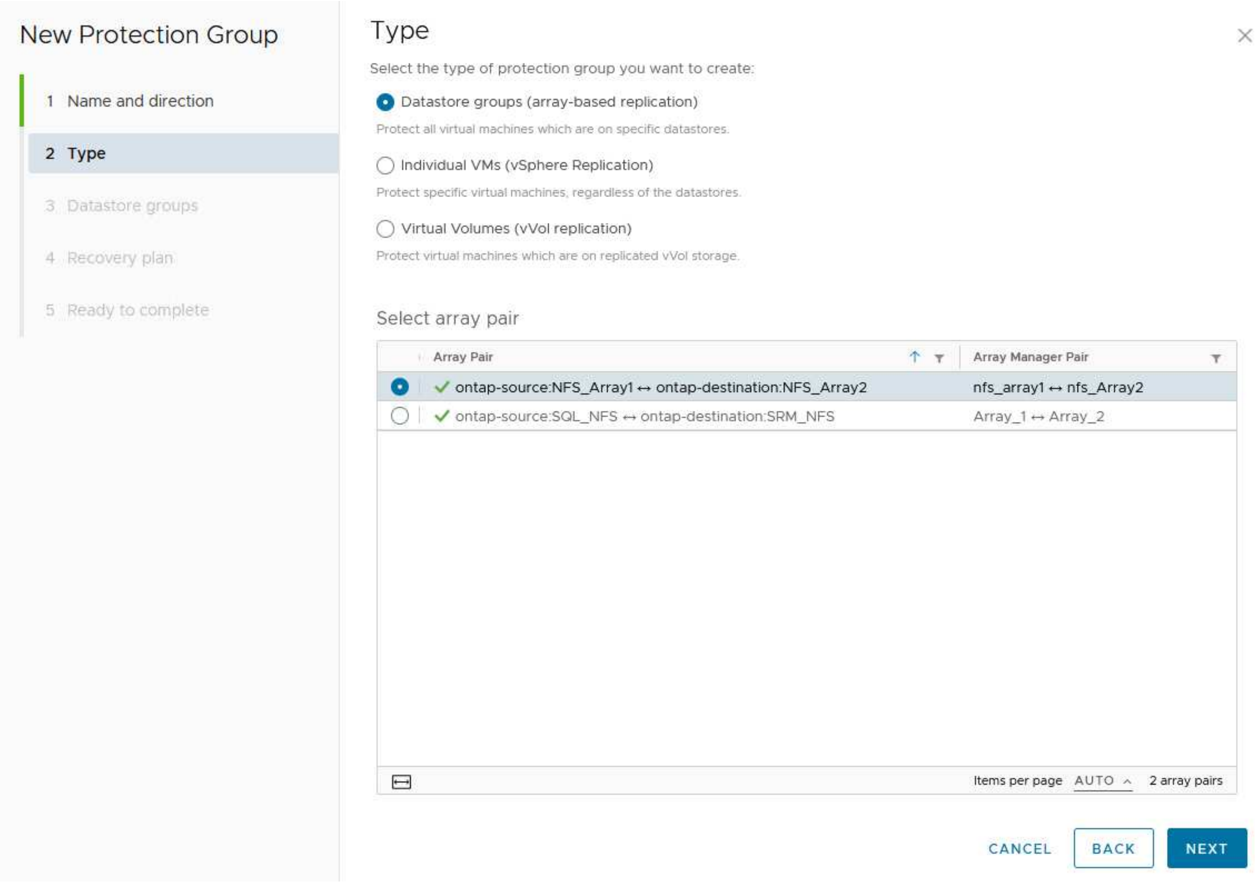
Name: SQL_Datastore
67 characters remaining

Description: (Optional)
4096 characters remaining

Direction:
● Site 1 → Site 2
○ Site 2 → Site 1

Location:

3. On the **Type** page select the protection group type (datastore, VM, or vVol) and select the array pair. Click on **Next** to continue.



New Protection Group

1 Name and direction

2 Type

3 Datastore groups

4 Recovery plan

5 Ready to complete

Type

Select the type of protection group you want to create:

● Datastore groups (array-based replication)

Protect all virtual machines which are on specific datastores.

○ Individual VMs (vSphere Replication)

Protect specific virtual machines, regardless of the datastores.

○ Virtual Volumes (vVol replication)

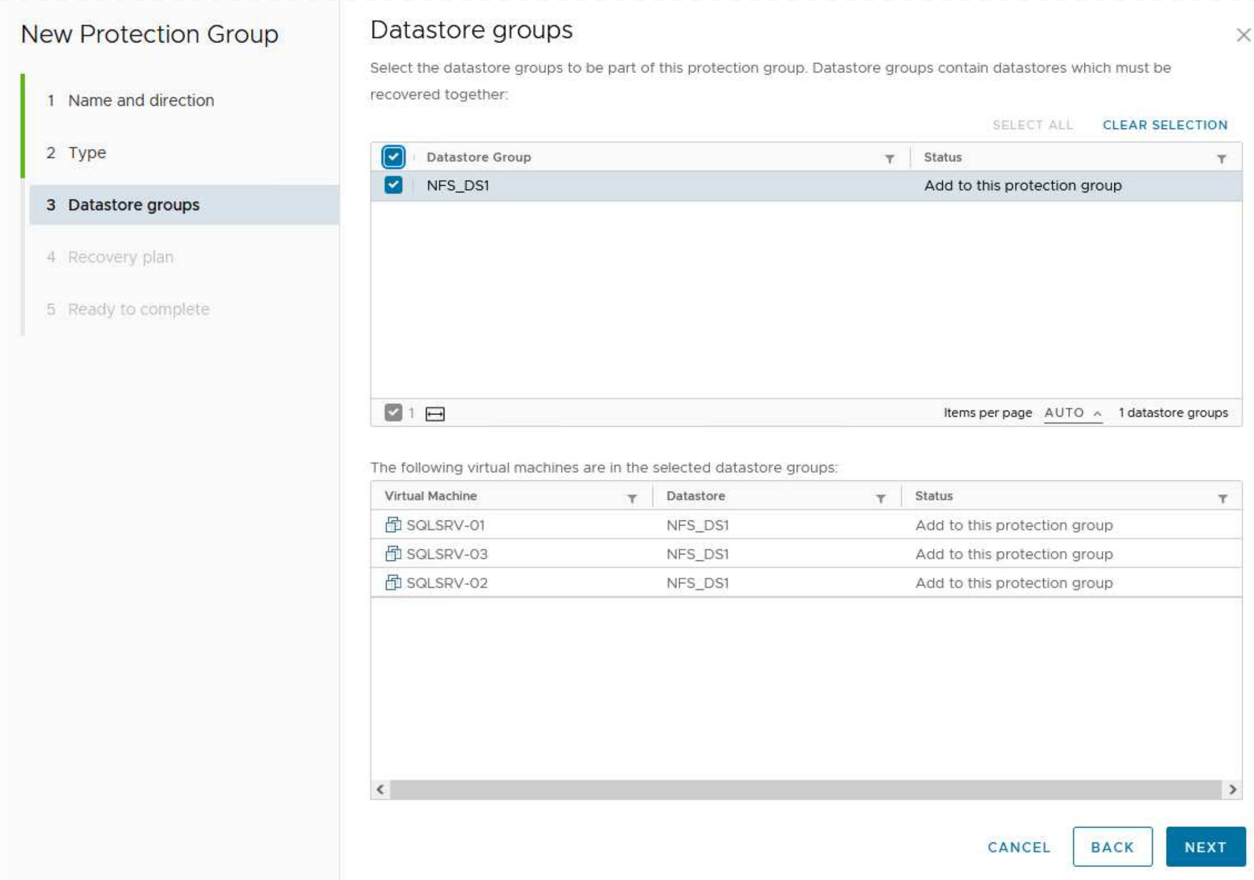
Protect virtual machines which are on replicated vVol storage.

Select array pair

	Array Pair	Array Manager Pair
●	✓ ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2	nfs_array1 ↔ nfs_Array2
○	✓ ontap-source:SQL_NFS ↔ ontap-destination:SRM_NFS	Array_1 ↔ Array_2

Items per page AUTO 2 array pairs

4. On the **Datastore groups** page, select the datastores to include in the protection group. VMs currently residing on the datastore are displayed for each datastore selected. Click on **Next** to continue.



New Protection Group

1 Name and direction

2 Type

3 Datastore groups

4 Recovery plan

5 Ready to complete

Datastore groups

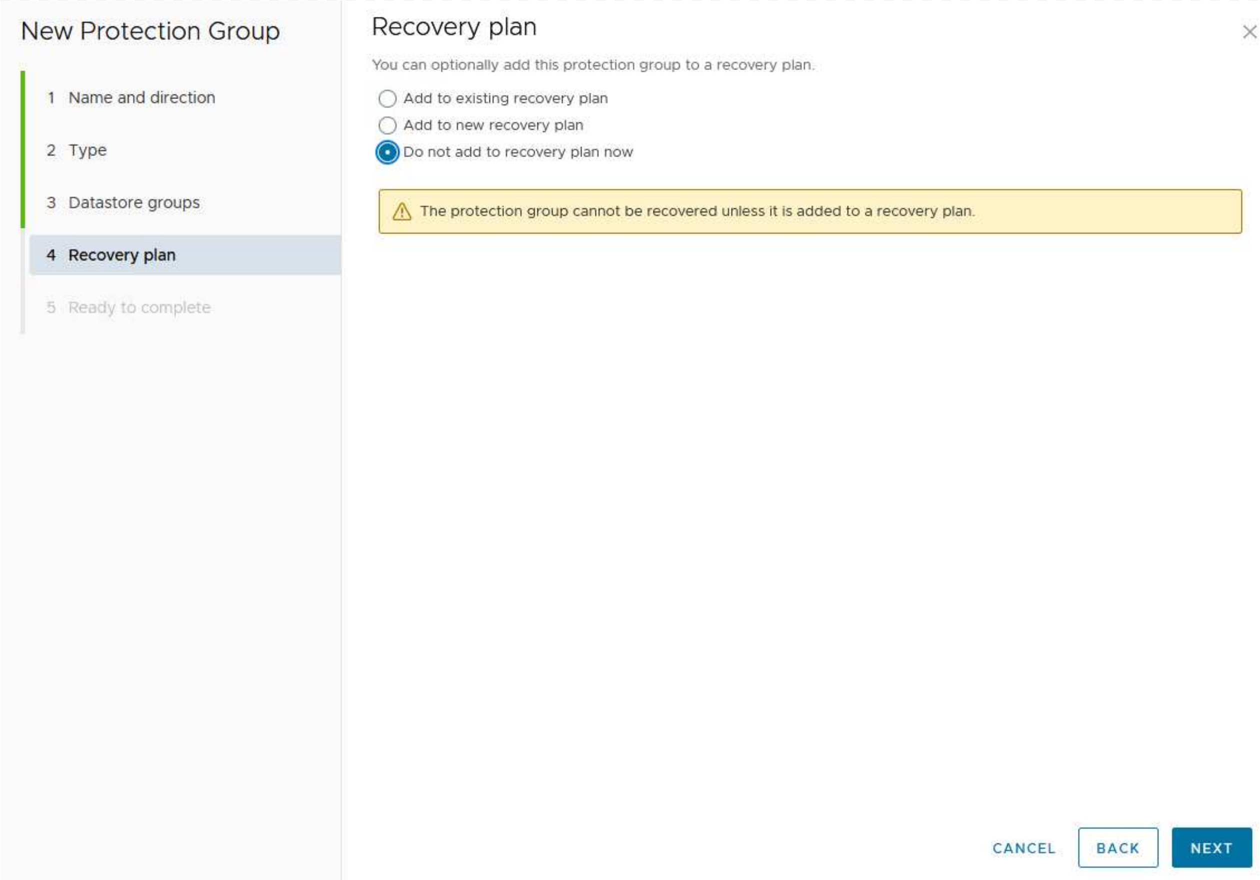
Select the datastore groups to be part of this protection group. Datastore groups contain datastores which must be recovered together:

☑	Datastore Group	Status
☑	NFS_DS1	Add to this protection group

The following virtual machines are in the selected datastore groups:

Virtual Machine	Datastore	Status
SQLSRV-01	NFS_DS1	Add to this protection group
SQLSRV-03	NFS_DS1	Add to this protection group
SQLSRV-02	NFS_DS1	Add to this protection group

5. On the **Recovery plan** page, optionally choose to add the protection group to a recovery plan. In this case, the recovery plan is not yet created so **Do not add to recovery plan** is selected. Click on **Next** to continue.



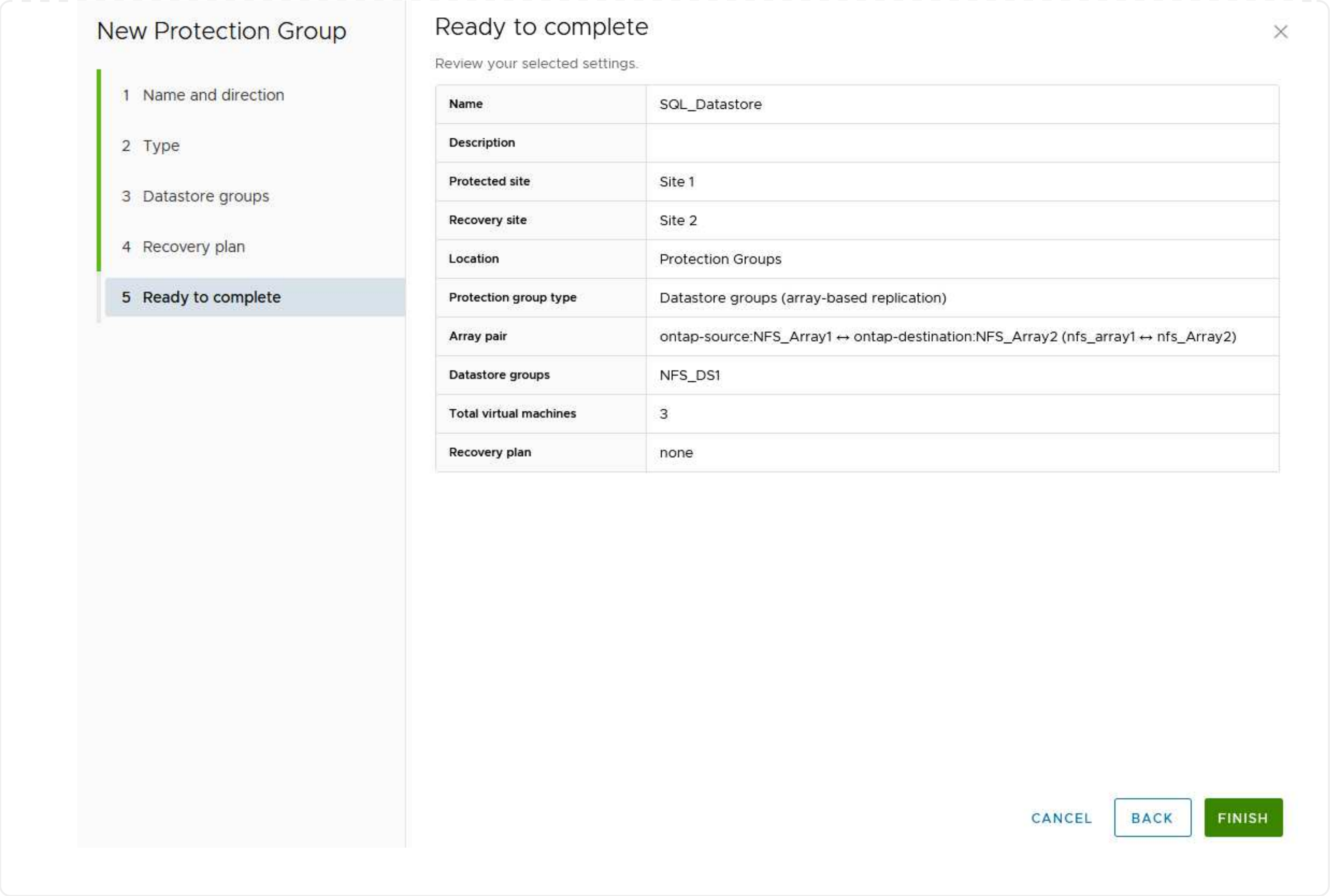
Recovery plan

You can optionally add this protection group to a recovery plan.

○ Add to existing recovery plan
○ Add to new recovery plan
● Do not add to recovery plan now

⚠ The protection group cannot be recovered unless it is added to a recovery plan.

6. On the **Ready to complete** page, review the new protection group parameters and click on **Finish** to create the group.



Ready to complete

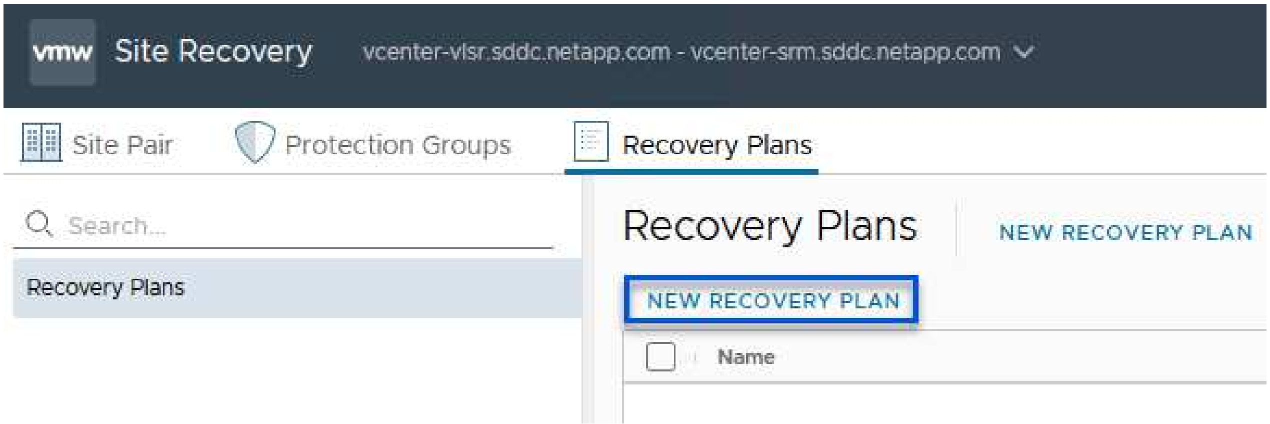
Review your selected settings.

Name	SQL_Datastore
Description	
Protected site	Site 1
Recovery site	Site 2
Location	Protection Groups
Protection group type	Datastore groups (array-based replication)
Array pair	ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2 (nfs_array1 ↔ nfs_Array2)
Datastore groups	NFS_DS1
Total virtual machines	3
Recovery plan	none

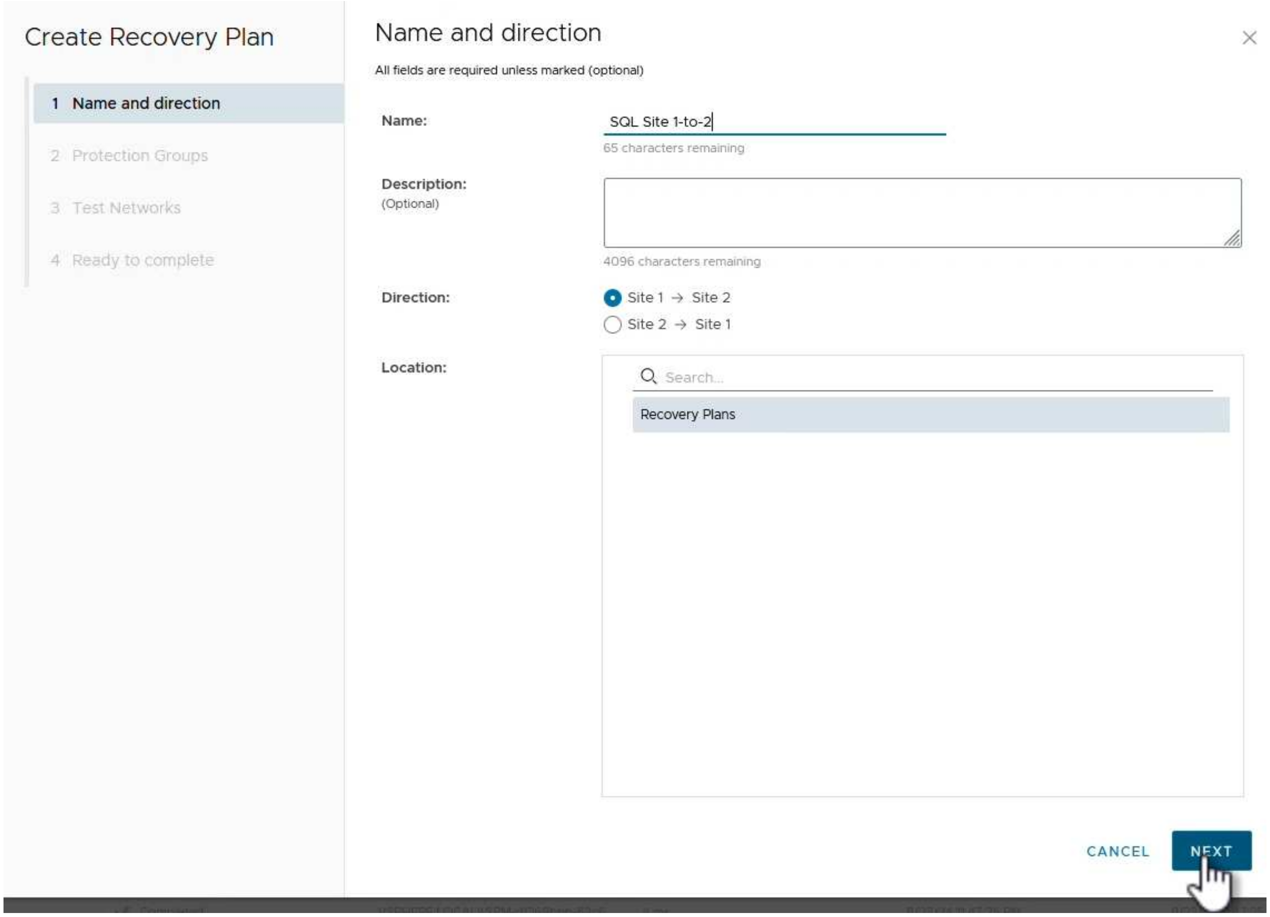
Configure Recovery Plan for SRM

The following step is completed in the Site Recovery interface of the primary site.

1. In the Site Recovery interface click on the **Recovery plan** tab and then on **New Recovery Plan** to get started.



2. On the **Name and direction** page of the **Create Recovery Plan** wizard, provide a name for the recovery plan and choose the direction between source and destination sites. Click on **Next** to continue.



All fields are required unless marked (optional)

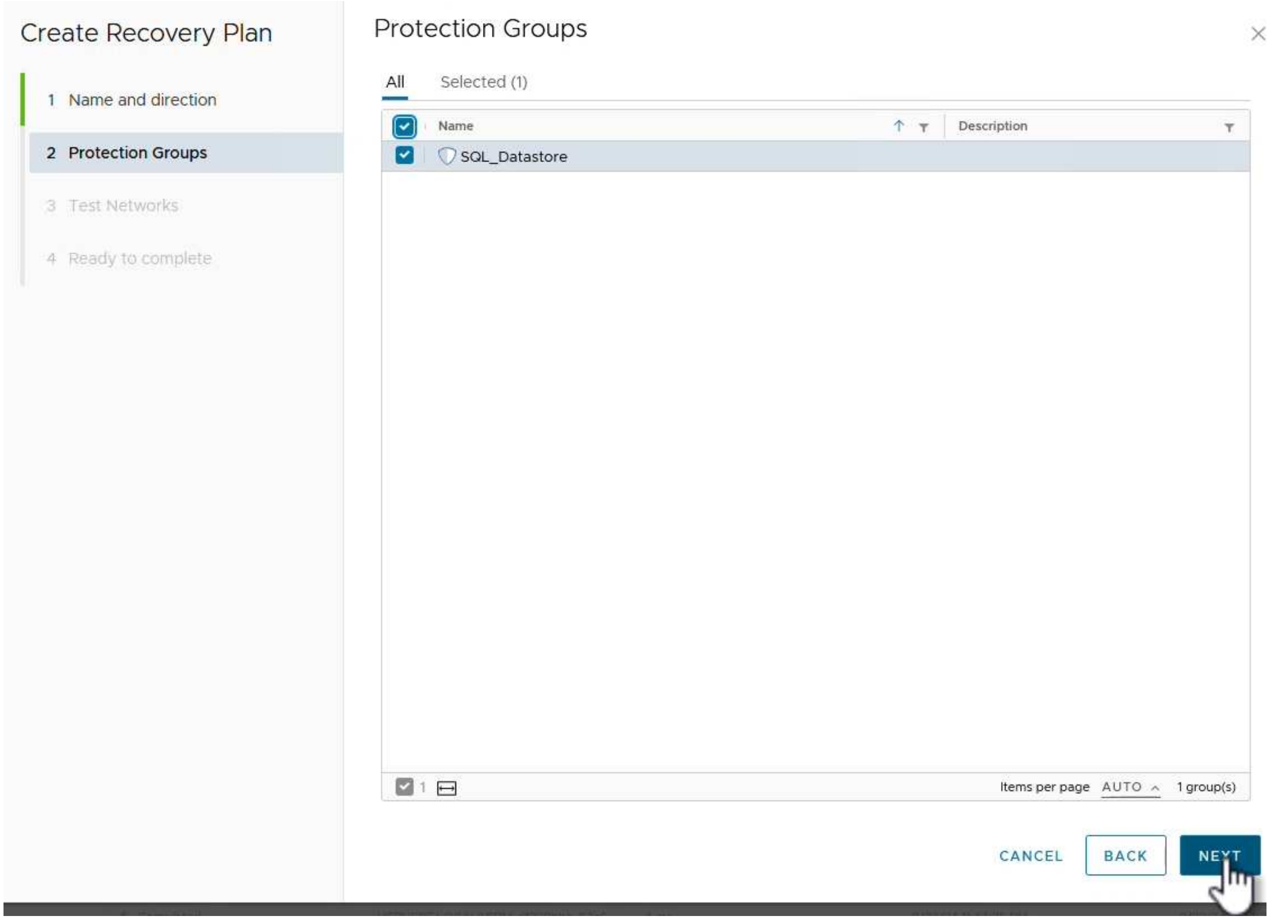
Name: SQL Site 1-to-2
65 characters remaining

Description: (Optional)
4096 characters remaining

Direction:
● Site 1 → Site 2
○ Site 2 → Site 1

Location: Recovery Plans

3. On the **Protection groups** page, select the previously created protection groups to include in the recovery plan. Click on **Next** to continue.



Create Recovery Plan

1 Name and direction
2 Protection Groups
3 Test Networks
4 Ready to complete

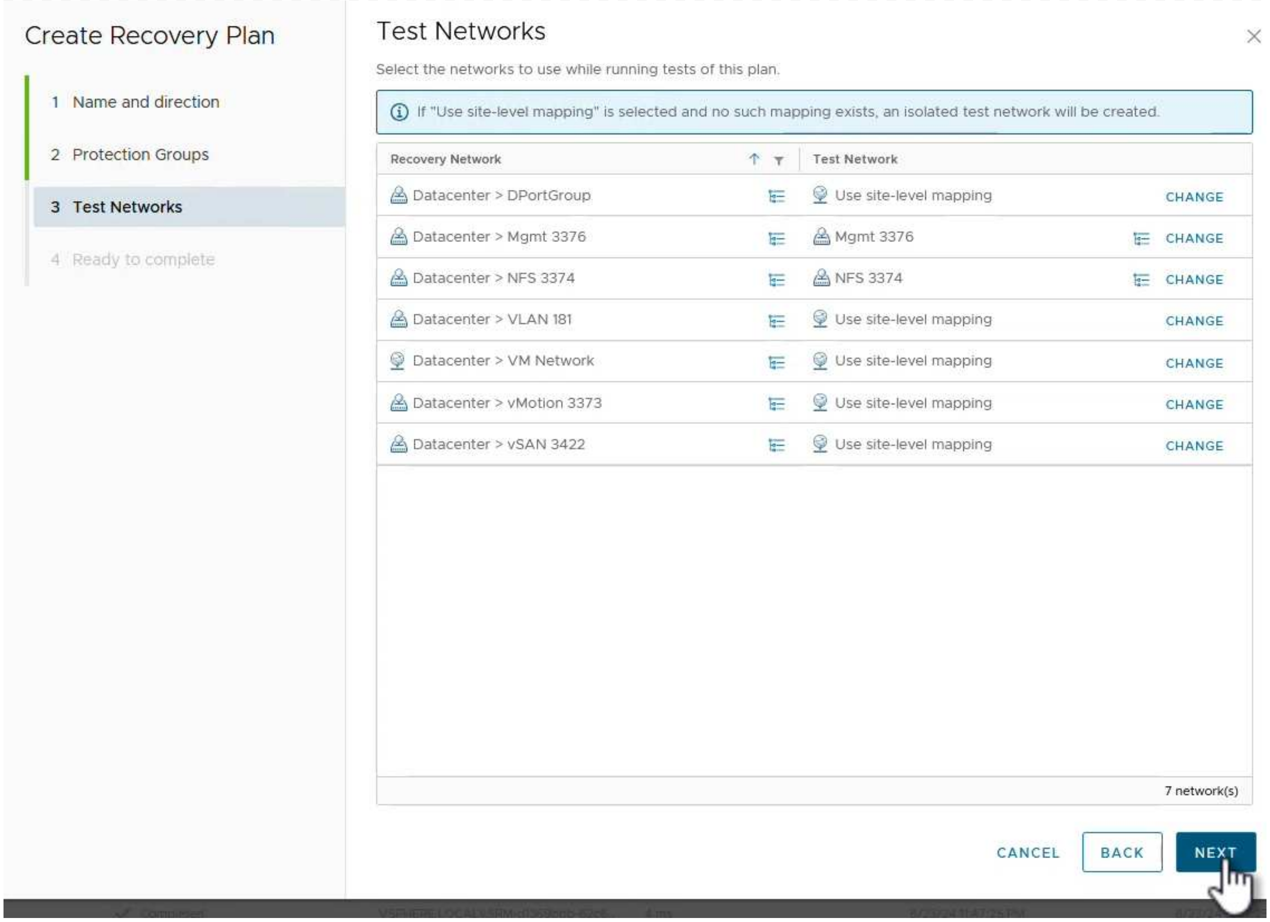
Protection Groups

All | Selected (1)

☑	Name	Description
☑	SQL_Datastore	

Items per page AUTO 1 group(s)

4. On the **Test Networks** configure specific networks that will be used during the test of the plan. If no mapping exists or if no network is selected, an isolated test network will be created. Click on **Next** to continue.



Create Recovery Plan

1 Name and direction

2 Protection Groups

3 Test Networks

4 Ready to complete

Test Networks

Select the networks to use while running tests of this plan.

ⓘ If "Use site-level mapping" is selected and no such mapping exists, an isolated test network will be created.

Recovery Network	Test Network	
Datacenter > DPortGroup	Use site-level mapping	CHANGE
Datacenter > Mgmt 3376	Mgmt 3376	CHANGE
Datacenter > NFS 3374	NFS 3374	CHANGE
Datacenter > VLAN 181	Use site-level mapping	CHANGE
Datacenter > VM Network	Use site-level mapping	CHANGE
Datacenter > vMotion 3373	Use site-level mapping	CHANGE
Datacenter > vSAN 3422	Use site-level mapping	CHANGE

7 network(s)

5. On the **Ready to complete** page, review the chosen parameters and then click on **Finish** to create the recovery plan.

Disaster recovery operations with SRM

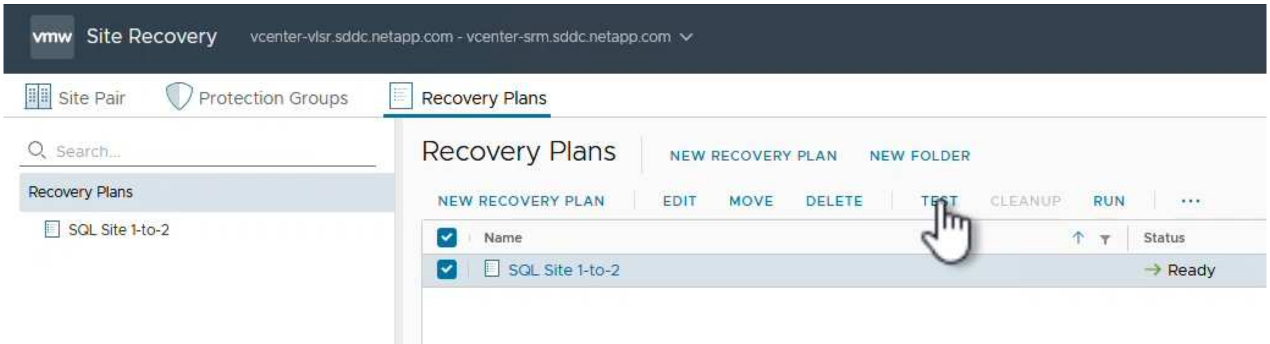
In this section various functions of using disaster recovery with SRM will be covered including, testing failover, performing failover, performing reprotection and failback.

Refer to Operational best practices for more information on using ONTAP storage with SRM disaster recovery operations.

Testing failover with SRM

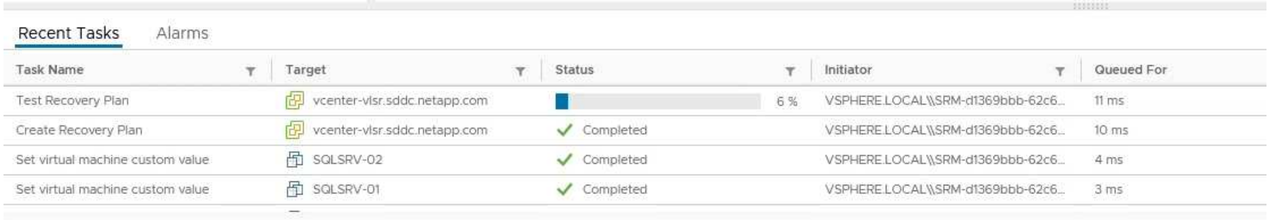
The following step is completed in the Site Recovery interface.

1. In the Site Recovery interface click on the **Recovery plan** tab and then select a recovery plan. Click on the **Test** button to begin testing failover to the secondary site.



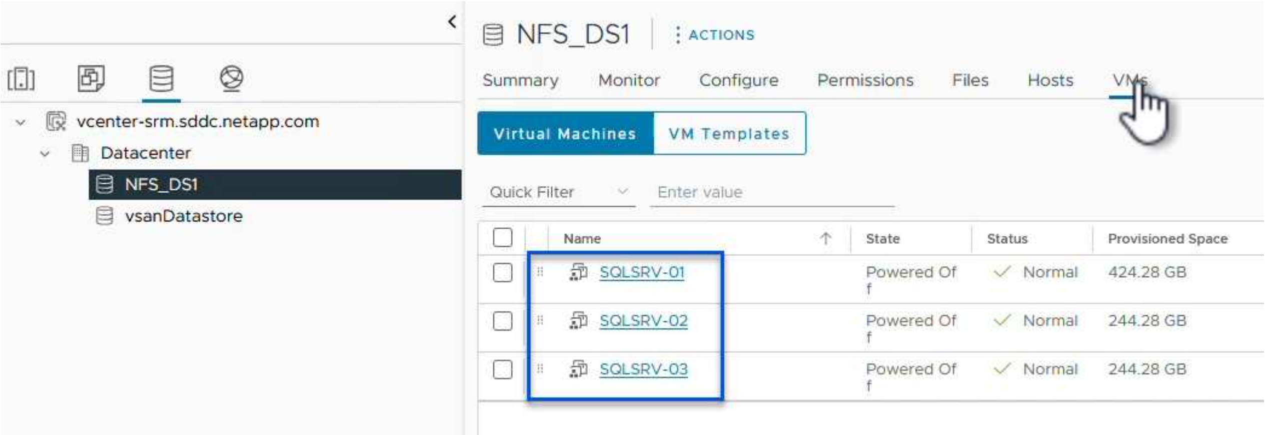
☑	Name	Status
☑	SQL Site 1-to-2	→ Ready

2. You can view the progress of the test from the Site Recovery task pane as well the vCenter task pane.



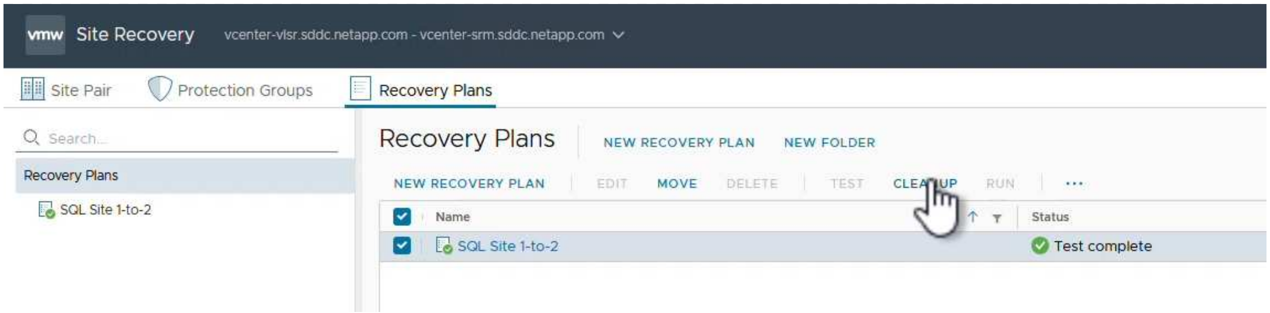
Task Name	Target	Status	Initiator	Queued For
Test Recovery Plan	vcenter-vlsr.sddc.netapp.com	6 %	VSPHERE.LOCAL\\SRM-d1369bbb-62c6...	11 ms
Create Recovery Plan	vcenter-vlsr.sddc.netapp.com	✓ Completed	VSPHERE.LOCAL\\SRM-d1369bbb-62c6...	10 ms
Set virtual machine custom value	SQLSRV-02	✓ Completed	VSPHERE.LOCAL\\SRM-d1369bbb-62c6...	4 ms
Set virtual machine custom value	SQLSRV-01	✓ Completed	VSPHERE.LOCAL\\SRM-d1369bbb-62c6...	3 ms

3. SRM sends commands via the SRA to the secondary ONTAP storage system. A FlexClone of the most recent snapshot is created and mounted at the secondary vSphere cluster. The newly mounted datastore can be viewed in the storage inventory.



□	Name	State	Status	Provisioned Space
□	SQLSRV-01	Powered Off	✓ Normal	424.28 GB
□	SQLSRV-02	Powered Off	✓ Normal	244.28 GB
□	SQLSRV-03	Powered Off	✓ Normal	244.28 GB

4. Once the test has completed, click on **Cleanup** to unmount the datastore and revert back to the original environment.

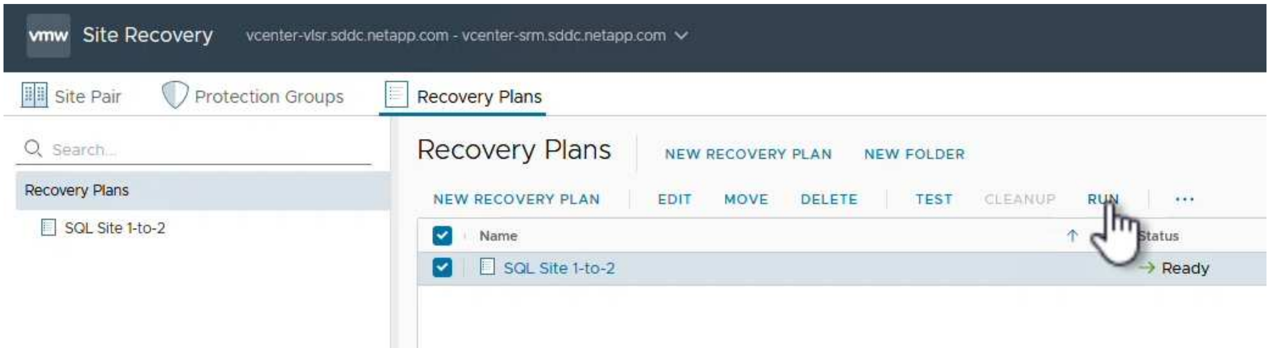


Name	Status
SQL Site 1-to-2	Test complete

Run Recovery Plan with SRM

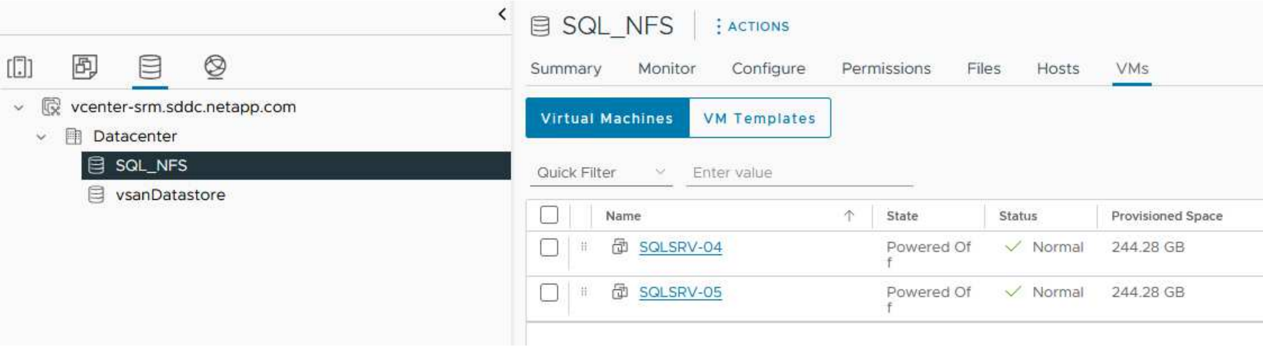
Perform a full recovery and failover to the secondary site.

1. In the Site Recovery interface click on the **Recovery plan** tab and then select a recovery plan. Click on the **Run** button to begin failover to the secondary site.



Name	Status
SQL Site 1-to-2	Ready

2. Once the failover is complete you can see the datastore mounted and the VMs registered at the secondary site.



Name	State	Status	Provisioned Space
SQLSRV-04	Powered Of f	Normal	244.28 GB
SQLSRV-05	Powered Of f	Normal	244.28 GB

Additional functions are possible in SRM once a failover has completed.

Reprotection: Once the recovery process is complete, the previously designated recovery site assumes the role of the new production site. However, it’s important to note that the SnapMirror replication is disrupted during the recovery operation, leaving the new production site vulnerable to future disasters. To ensure continued protection, it is recommended to establish new protection for the new production site by replicating it to another site. In cases where the original production site remains functional, the VMware administrator can repurpose it as a new recovery site, effectively reversing the direction of protection. It’s crucial to highlight that re-protection is only feasible in non-catastrophic failures, necessitating the eventual recoverability of the original vCenter Servers, ESXi servers, SRM servers, and their respective databases. If these components are unavailable, the creation of a new protection group and a new recovery plan becomes necessary.

Failback: A failback operation is a reverse failover, returning operations to the original site. It’s crucial to ensure that the original site has regained functionality before initiating the failback process. To ensure a smooth failback, it’s recommended to conduct a test failover after completing the reprotection process and before executing the final failback. This practice serves as a verification step, confirming that the systems at the original site are fully capable of handling the operation. By following this approach, you can minimize risks and ensure a more reliable transition back to the original production environment.

Additional information

For NetApp documentation on using ONTAP storage with VMware SRM refer to VMware Site Recovery Manager with ONTAP

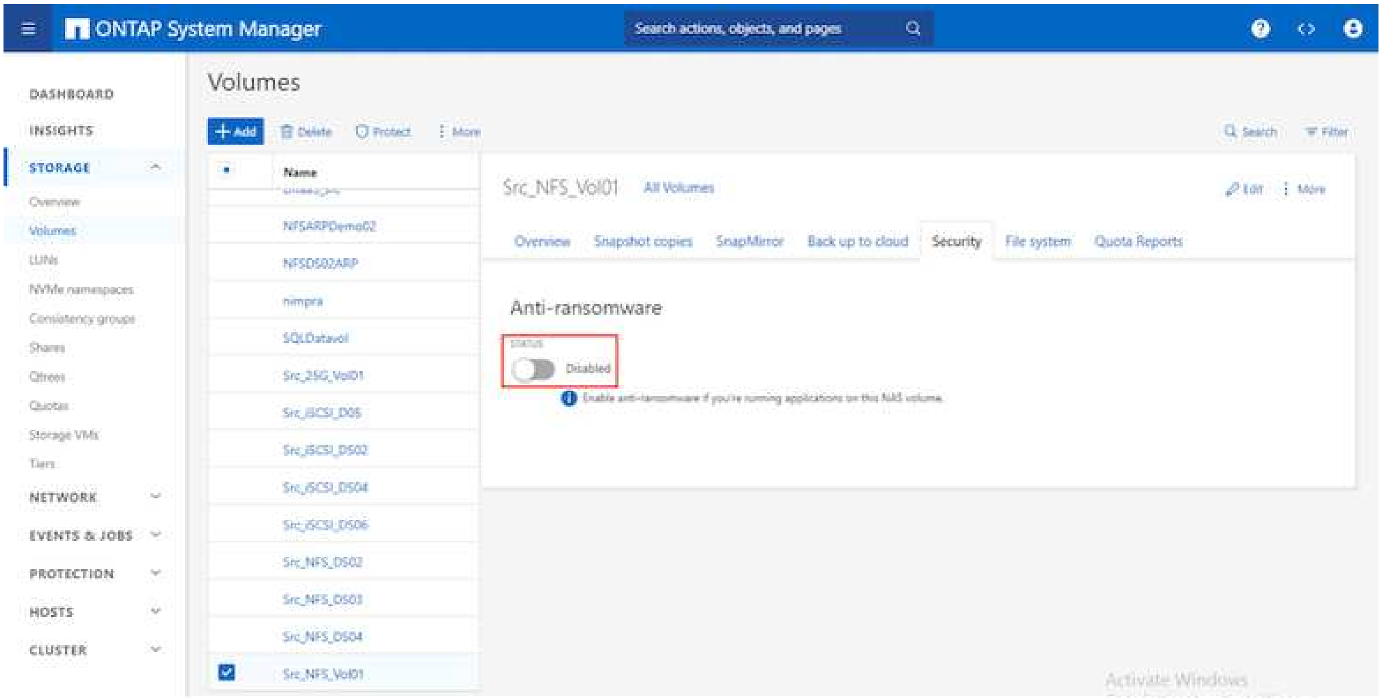
For information on configuring ONTAP storage systems refer to the ONTAP 9 Documentation center.

For information on configuring VCF refer to VMware Cloud Foundation Documentation.

Autonomous Ransomware Protection for NFS Storage

Detecting ransomware as early as possible is crucial in preventing its spread and avoiding costly downtime. An effective ransomware detection strategy must incorporate multiple layers of protection at ESXi host and guest VM levels. While multiple security measures are implemented to create a comprehensive defense against ransomware attacks, ONTAP enables adding more layers of protection to the overall defense approach. To name a few capabilities, it starts with Snapshots, Autonomous Ransomware Protection, tamperproof snapshots and so on.

Let’s look at how the above-mentioned capabilities work with VMware to protect and recover the data against ransomware. To protect vSphere and guest VMs against attacks, it is essential to take several measures including segmenting, utilizing EDR/XDR/SIEM for endpoints and installing security updates and adhering to the appropriate hardening guidelines. Each virtual machine residing on a datastore also hosts a standard operating system. Ensure enterprise server anti-malware product suites are installed and regularly updated on them which is an essential component of multi-layered ransomware protection strategy. Along with this, enable Autonomous Ransomware Protection (ARP) on the NFS volume powering the datastore. ARP leverages built-in onbox ML that looks at volume workload activity plus data entropy to automatically detect ransomware. ARP is configurable through the ONTAP built-in management interface or system Manager and is enabled on a per-volume basis.



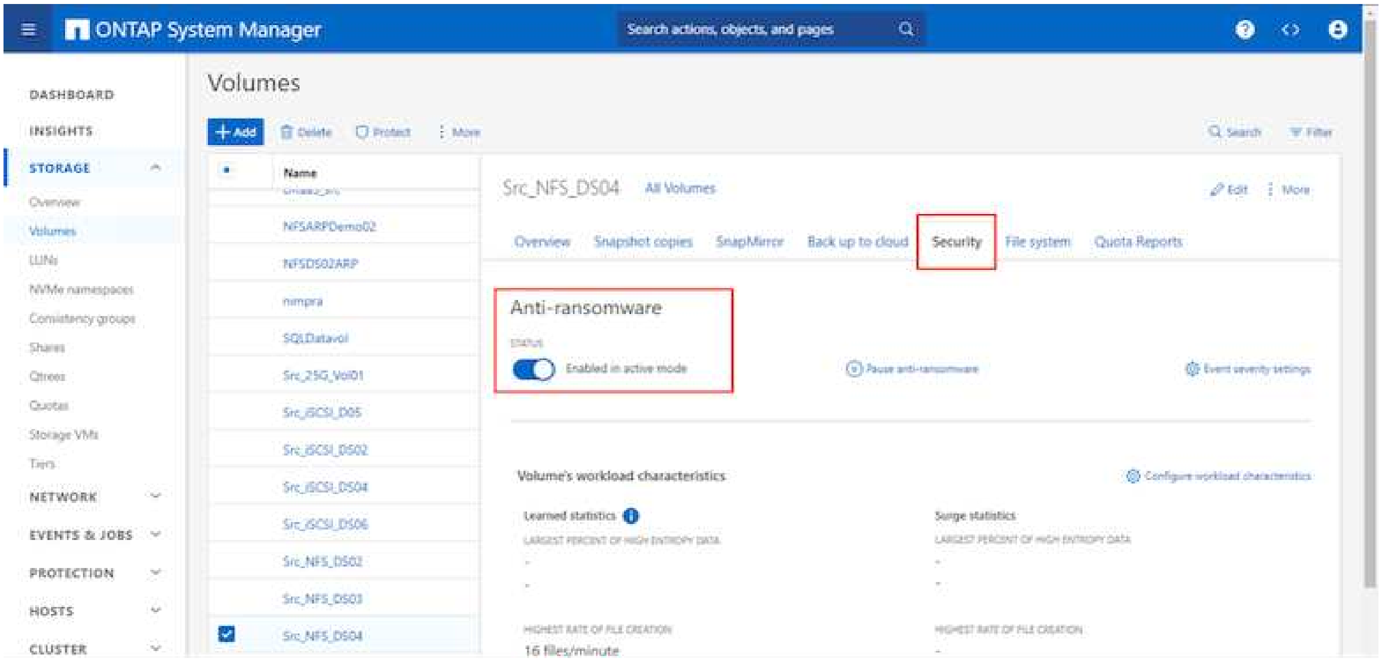
STATUS Disabled

Enable anti-ransomware if you're running applications on this NAS volume.

With the new NetApp ARP/AI, which is currently in tech preview, there is no need for a learning mode. Instead, it can go straight to active mode with its AI-powered ransomware detection capability.

With ONTAP One, all these feature sets are completely free. Access NetApp's robust suite of data protection, security and all the features that ONTAP offers without worrying about licensing barriers.

Once in active mode, it starts looking for the abnormal volume activity that might potentially be ransomware. If abnormal activity is detected, an automatic Snapshot copy is immediately taken, which provides a restoration point as close as possible to the file infection. ARP can detect changes in VM specific file extensions on an NFS volume located outside of the VM when a new extension is added to the encrypted volume or a file's extension is modified.



Anti-ransomware

STATUS

Enabled in active mode

Volume's workload characteristics

Learned statistics

LARGEST PERCENT OF HIGH ENTROPY DATA
-
-

HIGHEST RATE OF FILE CREATION
16 files/minute

Surge statistics

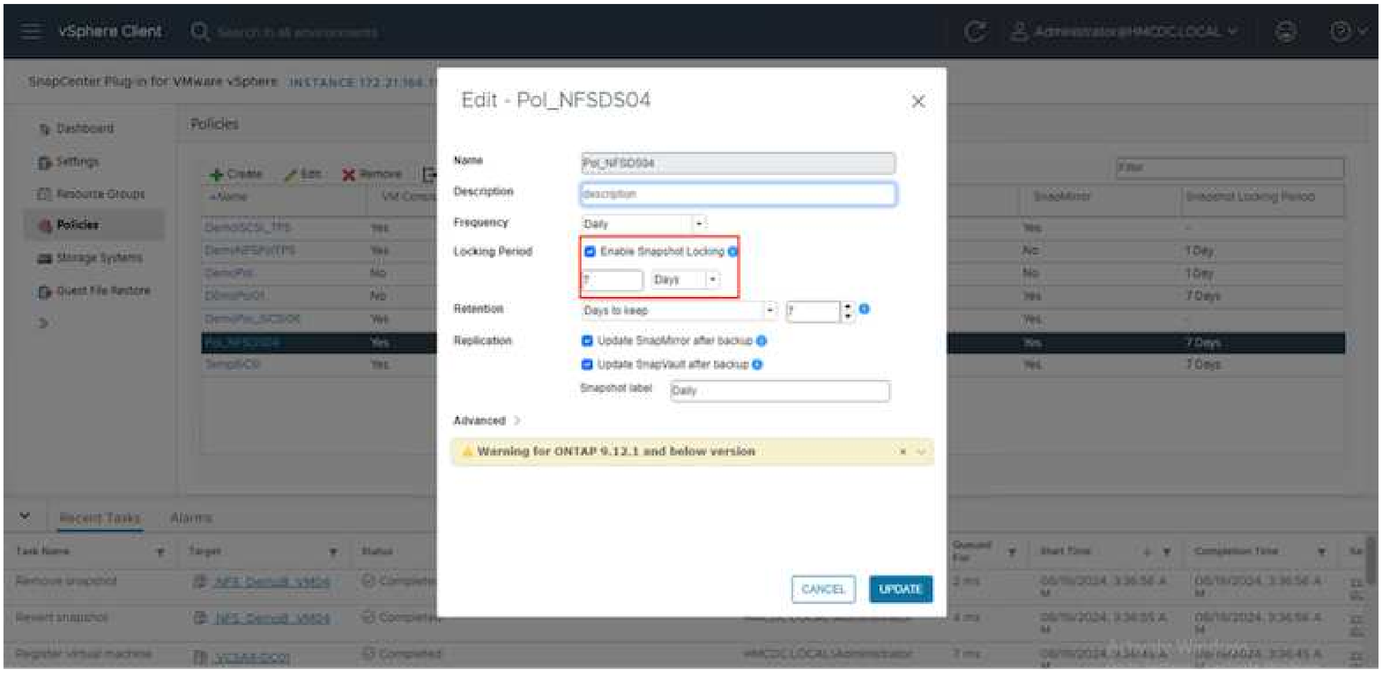
LARGEST PERCENT OF HIGH ENTROPY DATA
-
-

HIGHEST RATE OF FILE CREATION
-

If a ransomware attack targets the virtual machine (VM) and alter files within the VM without making changes outside the VM, the Advanced Ransomware Protection (ARP) will still detect the threat if the default entropy of the VM is low, for example, for file types like .txt, .docx, or .mp4 files. Even though ARP creates a protective snapshot in this scenario, it does not generate a threat alert because the file extensions outside of the VM have not been tampered with. In such scenarios, the initial layers of defense would identify the anomaly, however ARP helps in creating a snapshot based on the entropy.

For detailed information, refer to “ARP and Virtual machines” section in ARP usecases and considerations.

Moving from files to backup data, ransomware attacks are now increasingly targeting backups and snapshot recovery points by trying to delete them before starting to encrypt files. However, with ONTAP, this can be prevented by creating tamperproof snapshots on primary or secondary systems with NetApp Snapshot™ copy locking.



Edit - Pol_NFSDS04

Name: Pol_NFSDS04

Description: description

Frequency: Daily

Locking Period: ☑ Enable Snapshot Locking

7 Days

Retention: Days to keep 7

Replication: ☑ Update SnapMirror after backup

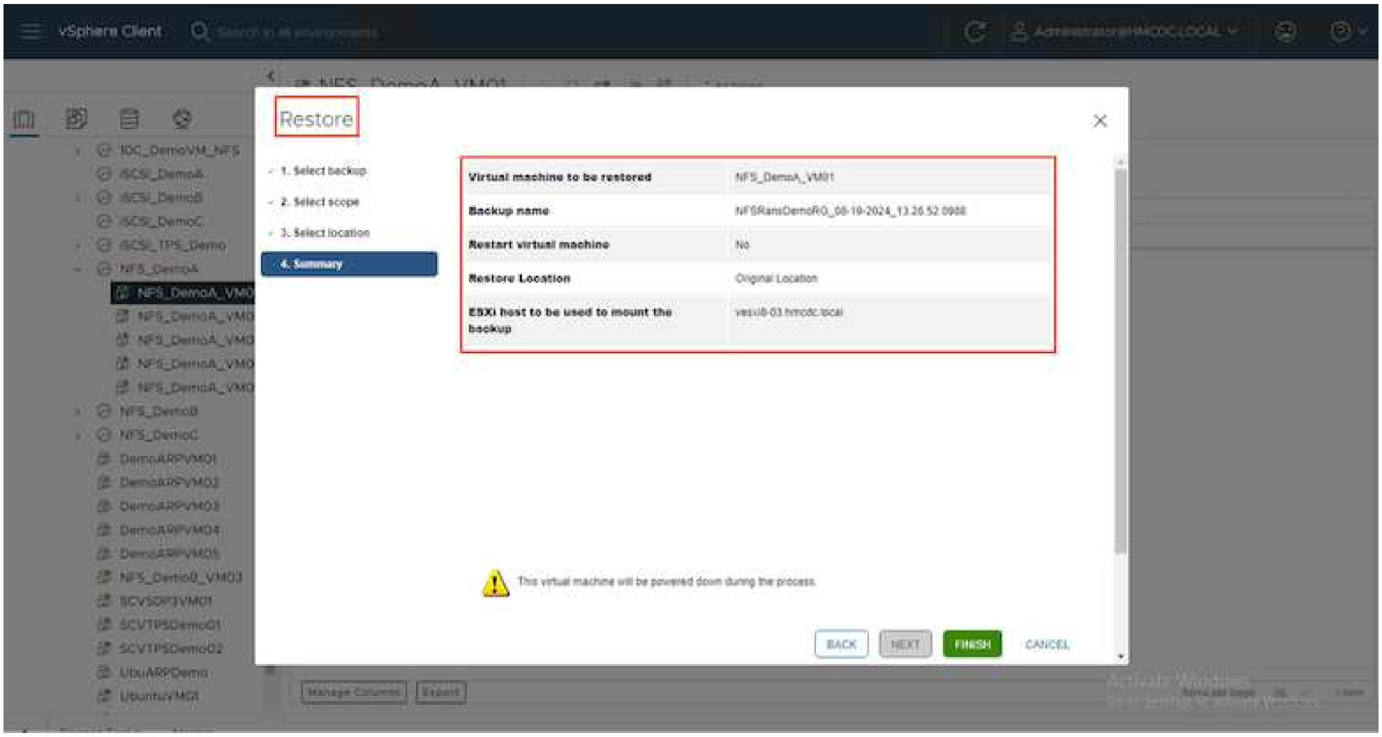
☑ Update SnapVault after backup

Snapshot label: Daily

Advanced >

Warning for ONTAP 9.12.1 and below version

These Snapshot copies can’t be deleted or changed by ransomware attackers or rogue administrators, so they’re available even after an attack. If the datastore or specific virtual machines are affected, SnapCenter can recover virtual machine data in seconds, minimizing organization’s downtime.



Restore

- 1. Select backup
- 2. Select scope
- 3. Select location
- 4. Summary

Virtual machine to be restored	NFS_DemoA_VM01
Backup name	NFSRansDemoRG_08-19-2024_13.26.52.0908
Restart virtual machine	No
Restore Location	Original Location
ESXi host to be used to mount the backup	vesxi8-03.hmcdc.local

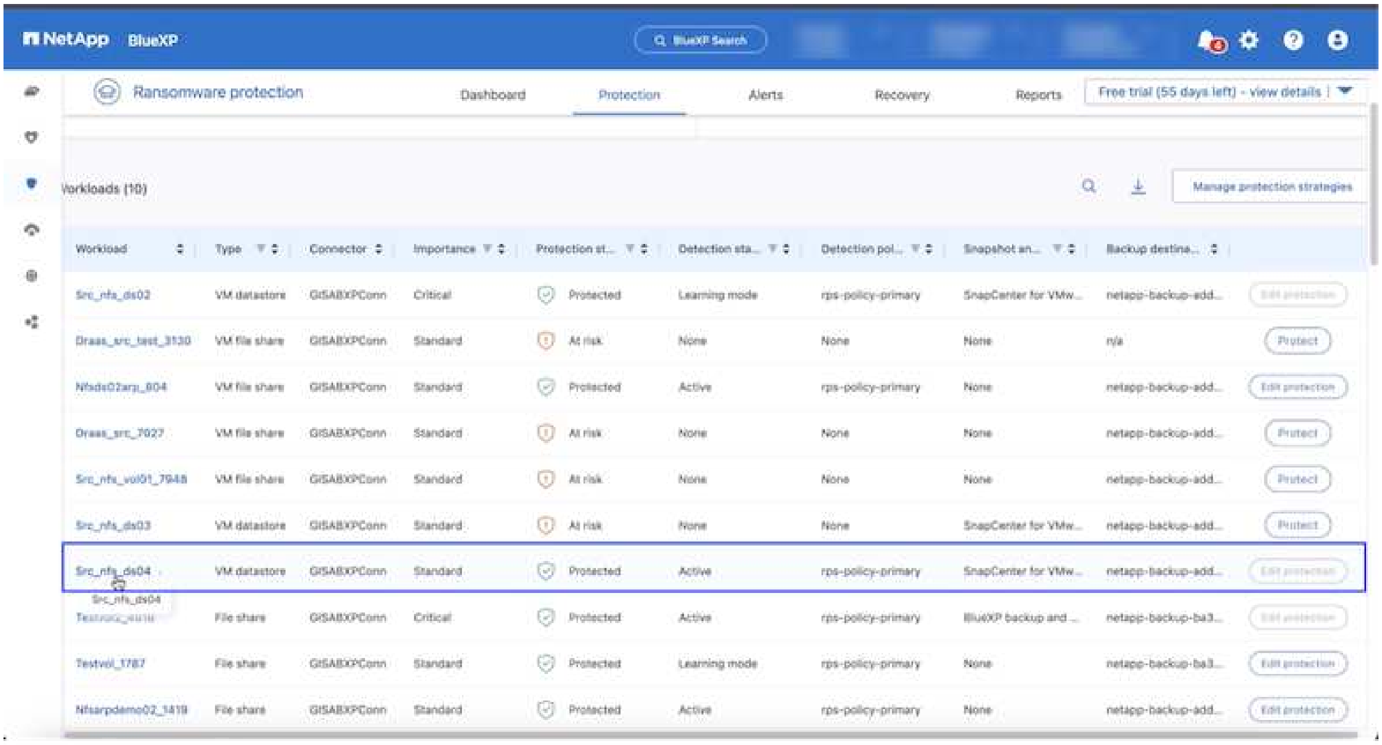
This virtual machine will be powered down during the process.

The above demonstrates how ONTAP storage adds an additional layer to the existing techniques, enhancing futureproofing of the environment.

For additional information, view guidance for NetApp solutions for ransomware.

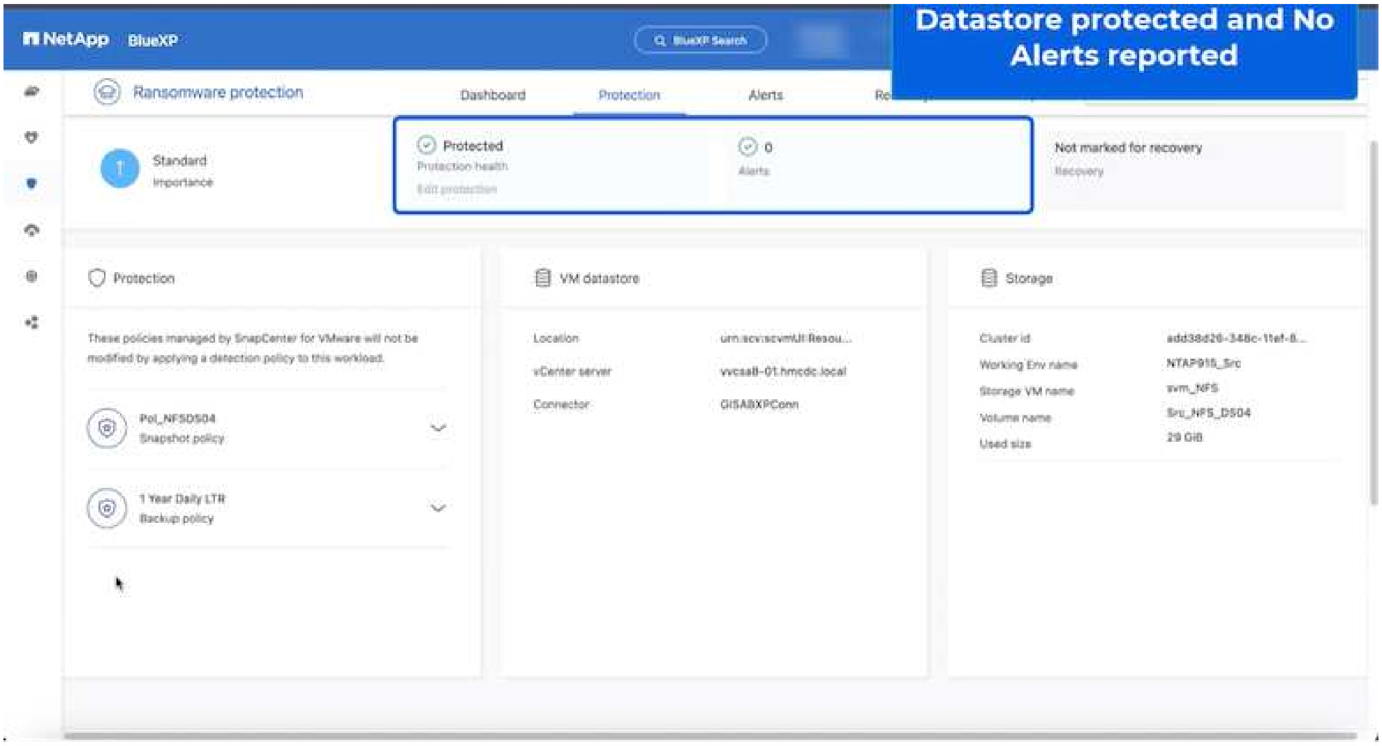
Now if all these needs to be orchestrated and integrated with SIEM tools, then offtap service like BlueXP ransomware protection can be used. It is a service designed to safeguard data from ransomware. This service offers protection for application-based workloads such as Oracle, MySQL, VM datastores, and file shares on on-premises NFS storage.

In this example, NFS datastore “Src_NFS_DS04” is protected using BlueXP ransomware protection.



Workloads (10)

Workload	Type	Connector	Importance	Protection st...	Detection sta...	Detection pol...	Snapshot an...	Backup destina...	
Src_nfs_ds02	VM datastore	GISABXPConn	Critical	Protected	Learning mode	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	Edit protection
Draas_src_test_3130	VM file share	GISABXPConn	Standard	At risk	None	None	None	n/a	Protect
Nfsds02arp_804	VM file share	GISABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	Edit protection
Draas_src_7027	VM file share	GISABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	Protect
Src_nfs_vol01_7948	VM file share	GISABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	Protect
Src_nfs_ds03	VM datastore	GISABXPConn	Standard	At risk	None	None	SnapCenter for VMw...	netapp-backup-add...	Protect
Src_nfs_ds04	VM datastore	GISABXPConn	Standard	Protected	Active	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	Edit protection
Testvol[illegible]	File share	GISABXPConn	Critical	Protected	Active	rps-policy-primary	BlueXP backup and ...	netapp-backup-ba3...	Edit protection
Testvol_1787	File share	GISABXPConn	Standard	Protected	Learning mode	rps-policy-primary	None	netapp-backup-ba3...	Edit protection
Nfsarpdemo02_1419	File share	GISABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	Edit protection



Datastore protected and No Alerts reported

Standard
Importance

Protected
Protection health
Edit protection

0
Alerts

Not marked for recovery
Recovery

Protection

These policies managed by SnapCenter for VMware will not be modified by applying a detection policy to this workload.

Pol_NFSDS04
Snapshot policy

1 Year Daily LTR
Backup policy

VM datastore

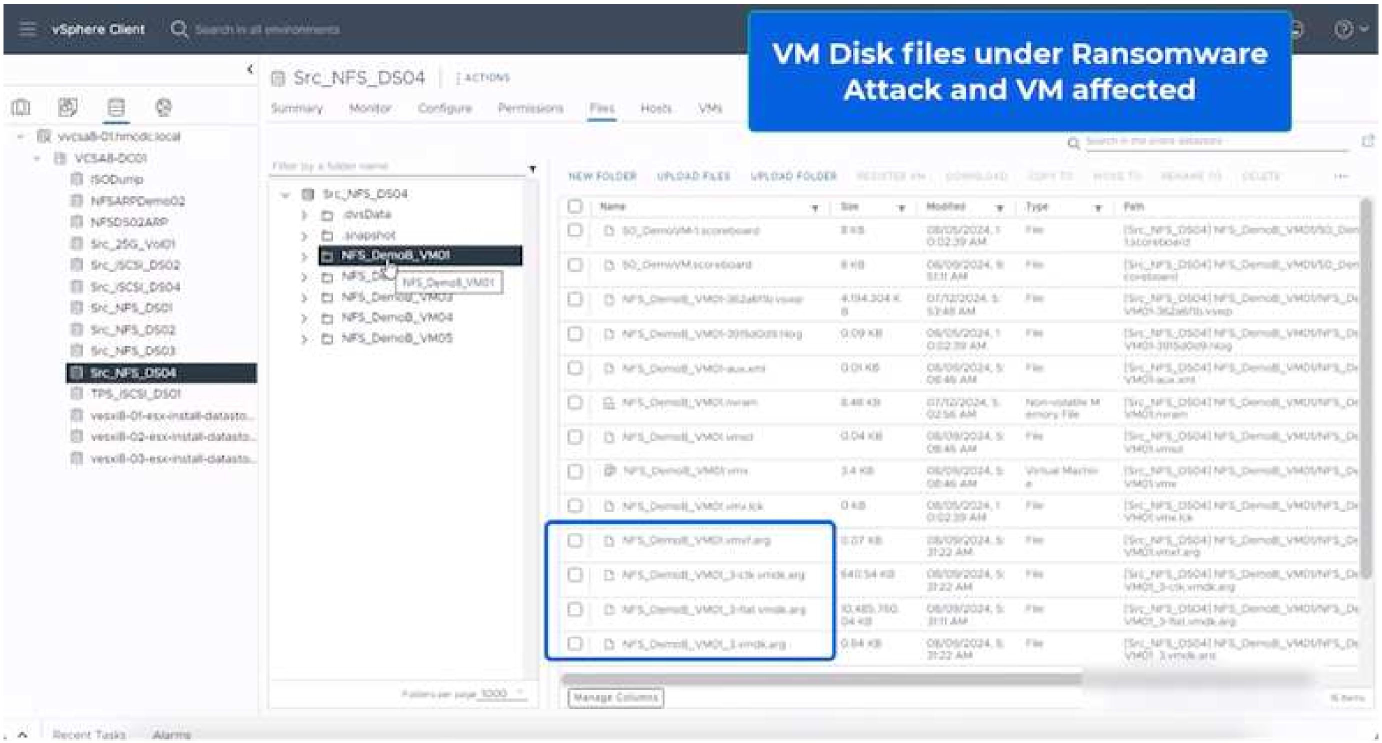
Location	urn:scv:scvmUI:Resou...
vCenter server	vvcsa8-01.hmcdc.local
Connector	GISABXPConn

Storage

Cluster id	add38d26-348c-11ef-8...
Working Env name	NTAP915_Src
Storage VM name	svm_NFS
Volume name	Src_NFS_DS04
Used size	29 GiB

For detailed information on to configure BlueXP ransomware protection, refer to Setup BlueXP ransomware protection and Configure BlueXP ransomware protection settings.

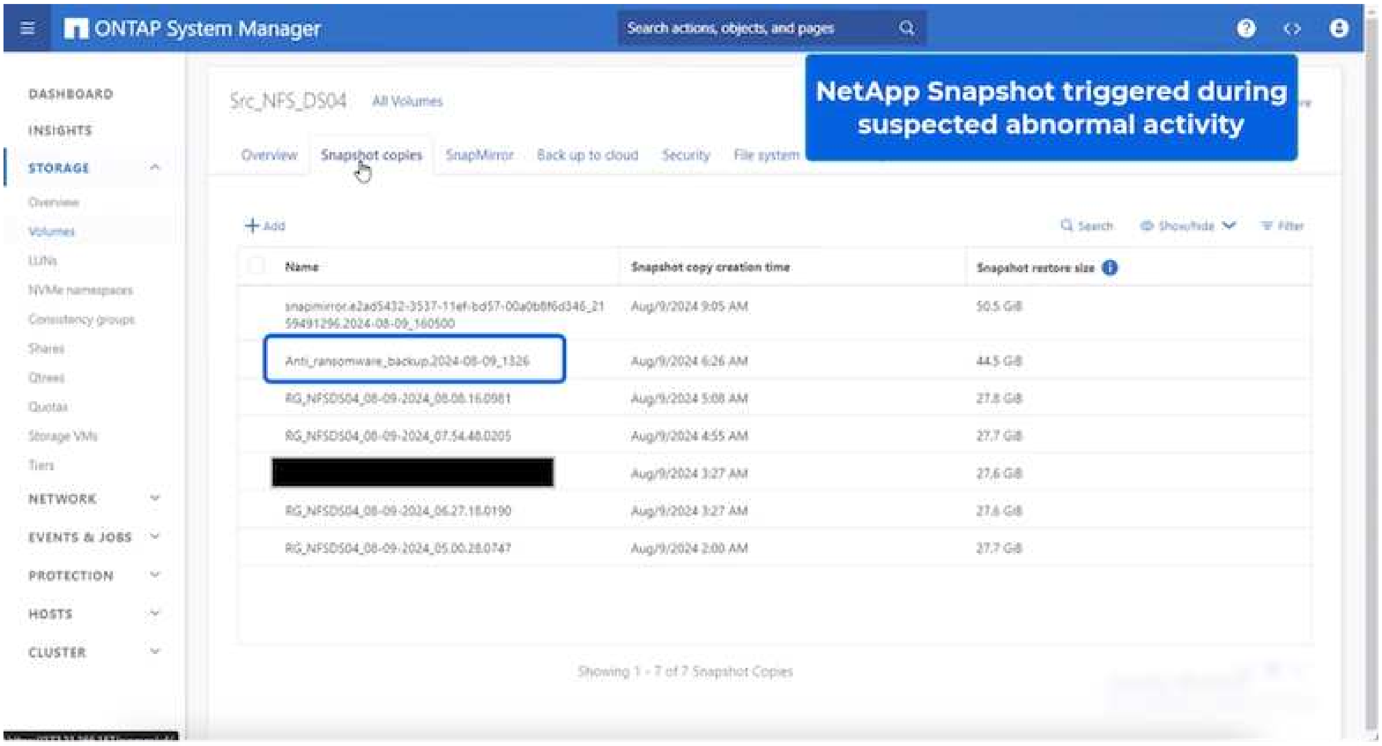
It’s time to walk through this with an example. In this walkthrough, the datastore “Src_NFS_DS04” is affected.



VM Disk files under Ransomware Attack and VM affected

Name	Size	Modified	Type	Path
SO_DemoVM-1.scoreboard	8 KB	08/05/2024, 10:02:39 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/SO_Dem 1.scoreboard
SO_DemoVM.scoreboard	8 KB	08/09/2024, 9:51:11 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/SO_Dem coreboard
NFS_DemoB_VM01-362a6f1b.vswp	4,194,304 KB	07/12/2024, 5:53:48 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01-362a6f1b.vswp
NFS_DemoB_VM01-2015d0d9.hlog	0.09 KB	08/05/2024, 10:02:39 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01-2015d0d9.hlog
NFS_DemoB_VM01-aux.xml	0.01 KB	08/09/2024, 5:08:46 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01-aux.xml
NFS_DemoB_VM01.nvram	8.48 KB	07/12/2024, 5:02:56 AM	Non-volatile Memory File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01.nvram
NFS_DemoB_VM01.vmsd	0.04 KB	08/09/2024, 5:08:46 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01.vmsd
NFS_DemoB_VM01.vmx	3.4 KB	08/09/2024, 5:08:46 AM	Virtual Machine	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01.vmx
NFS_DemoB_VM01.vmx.lck	0 KB	08/05/2024, 10:02:39 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01.vmx.lck
NFS_DemoB_VM01.vmxf.arg	0.07 KB	08/09/2024, 5:31:22 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01.vmxf.arg
NFS_DemoB_VM01_3-ctk.vmdk.arg	640.54 KB	08/09/2024, 5:31:22 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01_3-ctk.vmdk.arg
NFS_DemoB_VM01_3-flat.vmdk.arg	10,485,760.04 KB	08/09/2024, 5:31:11 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01_3-flat.vmdk.arg
NFS_DemoB_VM01_3.vmdk.arg	0.64 KB	08/09/2024, 5:31:22 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01_3.vmdk.arg

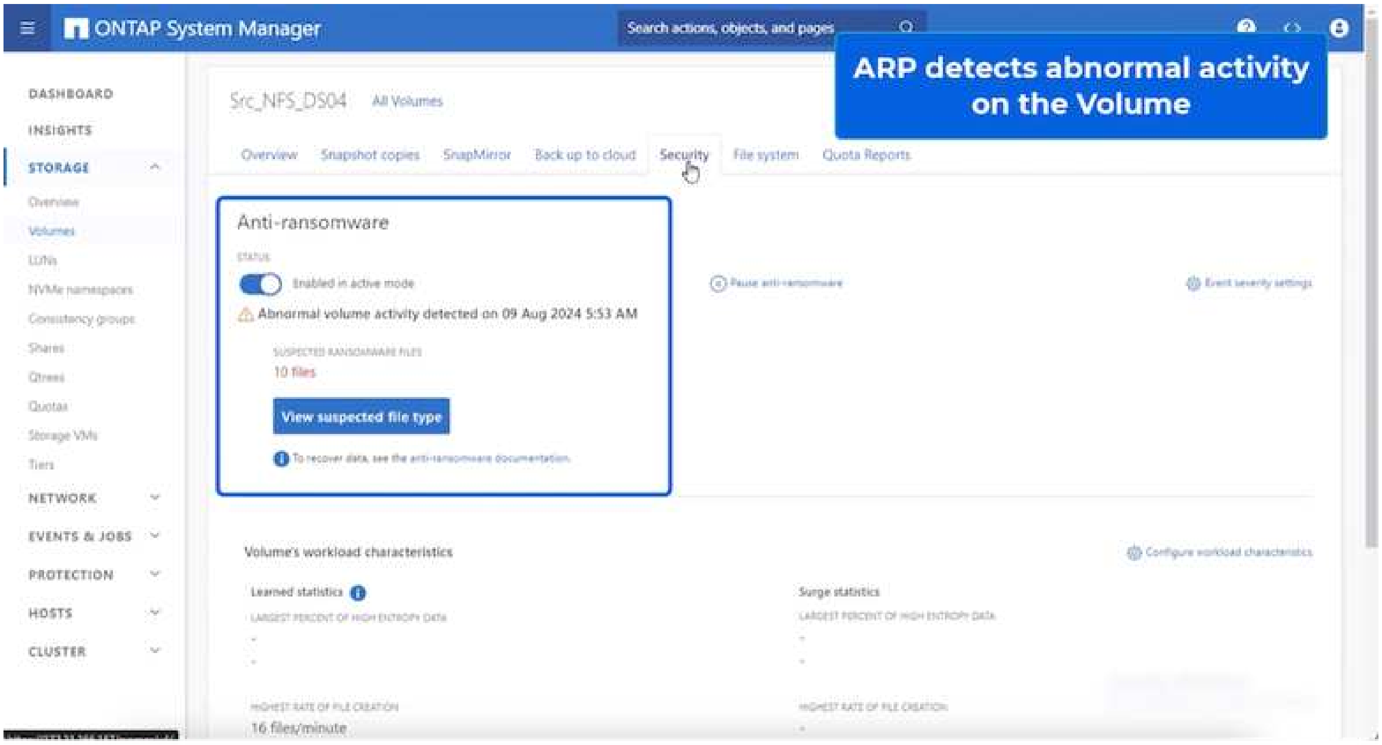
ARP immediately triggered a snapshot on the volume upon detection.



NetApp Snapshot triggered during suspected abnormal activity

Name	Snapshot copy creation time	Snapshot restore size
snapmirror.e2ad5432-3537-11ef-bd57-00a0b8f6d346_2159491296.2024-08-09_160500	Aug/9/2024 9:05 AM	50.5 GB
Anti_ransomware_backup.2024-08-09_1326	Aug/9/2024 6:26 AM	44.5 GB
RG_NFSDS04_08-09-2024_08.08.16.0981	Aug/9/2024 5:08 AM	27.8 GB
RG_NFSDS04_08-09-2024_07.54.48.0205	Aug/9/2024 4:55 AM	27.7 GB
[redacted]	Aug/9/2024 3:27 AM	27.6 GB
RG_NFSDS04_08-09-2024_06.27.18.0190	Aug/9/2024 3:27 AM	27.6 GB
RG_NFSDS04_08-09-2024_05.00.28.0747	Aug/9/2024 2:00 AM	27.7 GB

Showing 1 - 7 of 7 Snapshot Copies



ARP detects abnormal activity on the Volume

Anti-ransomware

STATUS

Enabled in active mode

⚠ Abnormal volume activity detected on 09 Aug 2024 5:53 AM

SUSPECTED RANSOMWARE FILES

10 files

To recover data, see the anti-ransomware documentation.

Volume's workload characteristics

Learned statistics

LARGEST PERCENT OF HIGH ENTROPY DATA

HIGHEST RATE OF FILE CREATION

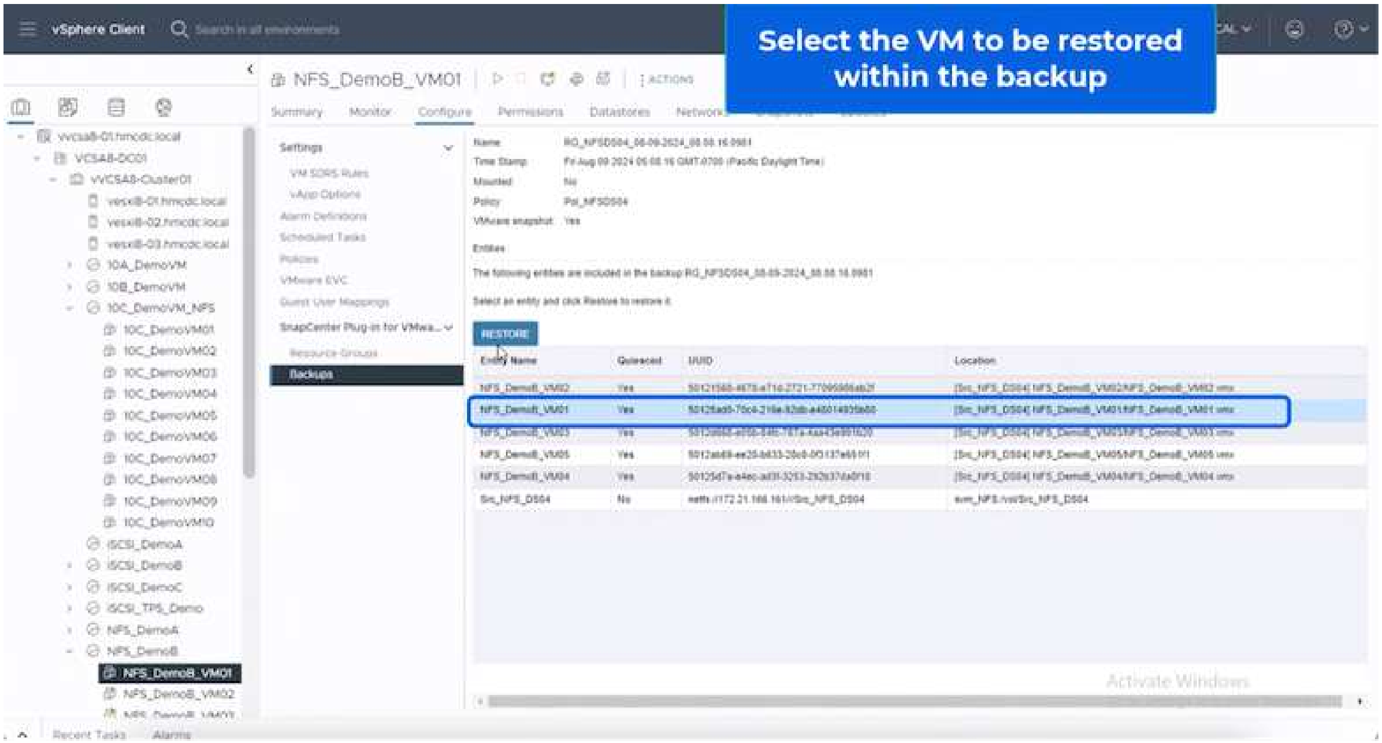
16 files/minute

Surge statistics

LARGEST PERCENT OF HIGH ENTROPY DATA

HIGHEST RATE OF FILE CREATION

Once the forensic analysis is complete, then the restores can be done quickly and seamlessly using SnapCenter or BlueXP ransomware protection. With SnapCenter, go to the affected virtual machines and select the appropriate snapshot to restore.



Select the VM to be restored within the backup

Name RG_NFSDS04_08-09-2024_05.08.16.0981

Time Stamp Fri Aug 09 2024 05:08:16 GMT-0700 (Pacific Daylight Time)

Mounted No

Policy Pol_NFSDS04

VMware snapshot Yes

Entities

The following entities are included in the backup RG_NFSDS04_08-09-2024_05.08.16.0981

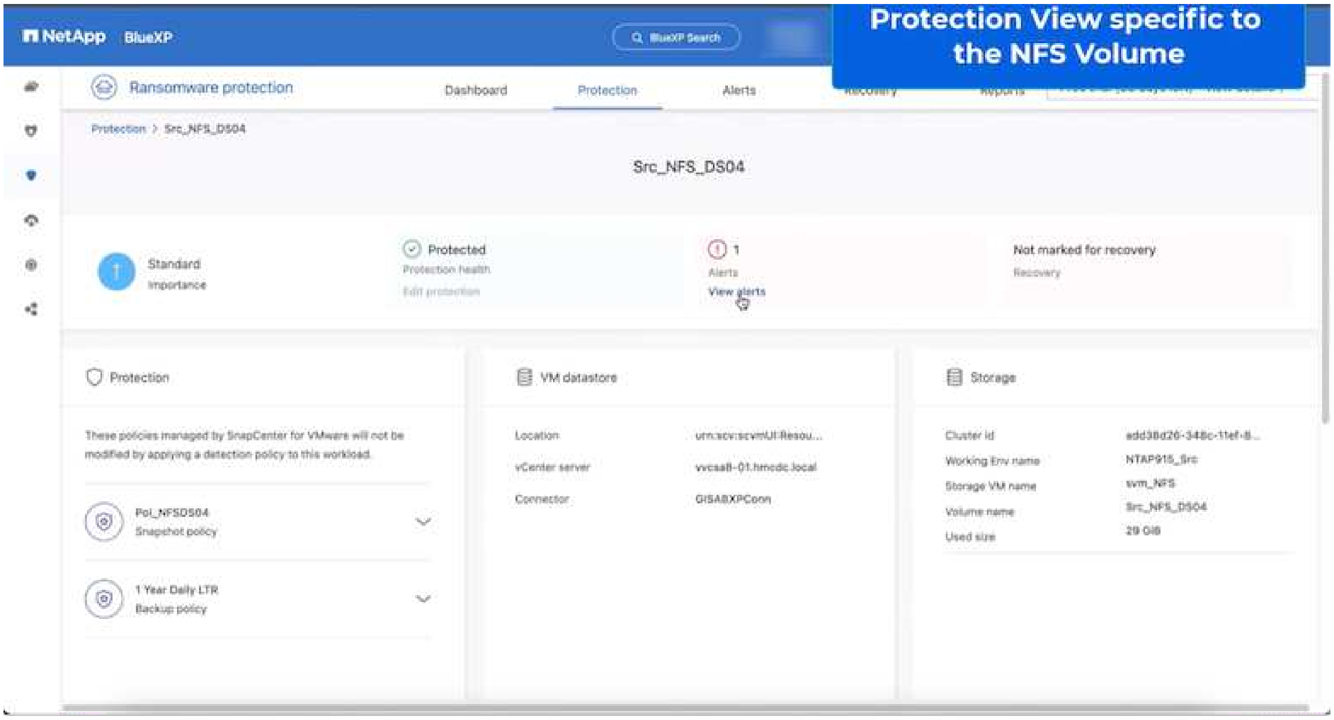
Select an entity and click Restore to restore it.

Entity Name	Quiesced	UUID	Location
NFS_DemoB_VM02	Yes	50121568-4678-a716-2721-77095866ab2f	[Src_NFS_DS04] NFS_DemoB_VM02/NFS_DemoB_VM02.vmx
NFS_DemoB_VM01	Yes	50126ad5-70c4-216a-82db-a40014935a80	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_DemoB_VM01.vmx
NFS_DemoB_VM03	Yes	5012d868-e050-84fc-787a-4aa43e801620	[Src_NFS_DS04] NFS_DemoB_VM03/NFS_DemoB_VM03.vmx
NFS_DemoB_VM05	Yes	5012ab69-ee25-b633-28c6-05137e65f1f1	[Src_NFS_DS04] NFS_DemoB_VM05/NFS_DemoB_VM05.vmx
NFS_DemoB_VM04	Yes	50125d7a-a4ec-ad31-3253-282b37da0f18	[Src_NFS_DS04] NFS_DemoB_VM04/NFS_DemoB_VM04.vmx
Src_NFS_DS04	No	netfs://172.21.166.161//Src_NFS_DS04	svm_NFS:/vol/Src_NFS_DS04

This section looks at how BlueXP ransomware protection orchestrates recovery from a ransomware incident wherein the VM files are encrypted.

> ⓘ If the VM is managed by SnapCenter, BlueXP ransomware protection restores the VM back to its previous state using the VM-consistent process.

1. Access BlueXP ransomware protection and an alert appears on the BlueXP ransomware protection Dashboard.
2. Click on the alert to review the incidents on that specific volume for the generated alert


Protection View specific to the NFS Volume

Src_NFS_DS04

Standard
Importance

Protected
Protection health

1
Alerts

Not marked for recovery
Recovery

Protection

These policies managed by SnapCenter for VMware will not be modified by applying a detection policy to this workload.

Pol_NFSDS04
Snapshot policy

1 Year Daily LTR
Backup policy

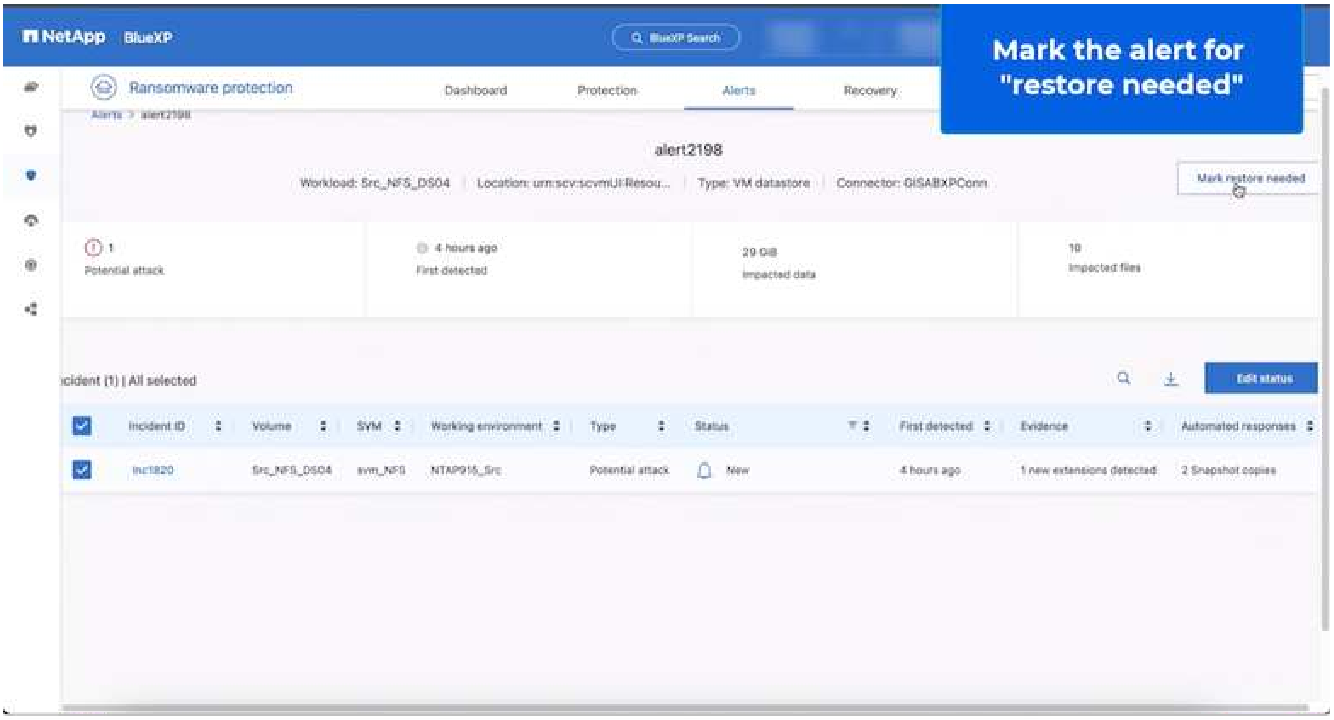
VM datastore

Location	urn:scv:scvmUI:Resou...
vCenter server	vvcsa8-01.hmcdc.local
Connector	GISABXPConn

Storage

Cluster id	add38d26-348c-11ef-8...
Working Env name	NTAP915_Src
Storage VM name	svm_NFS
Volume name	Src_NFS_DS04
Used size	29 GiB

3. Mark the ransomware incident as ready for recovery (after incidents are neutralized) by selecting “Mark restore needed”


Mark the alert for "restore needed"

alert2198

Workload: Src_NFS_DS04 | Location: urn:scv:scvmUI:Resou... | Type: VM datastore | Connector: GISABXPConn

1
Potential attack

4 hours ago
First detected

29 GiB
Impacted data

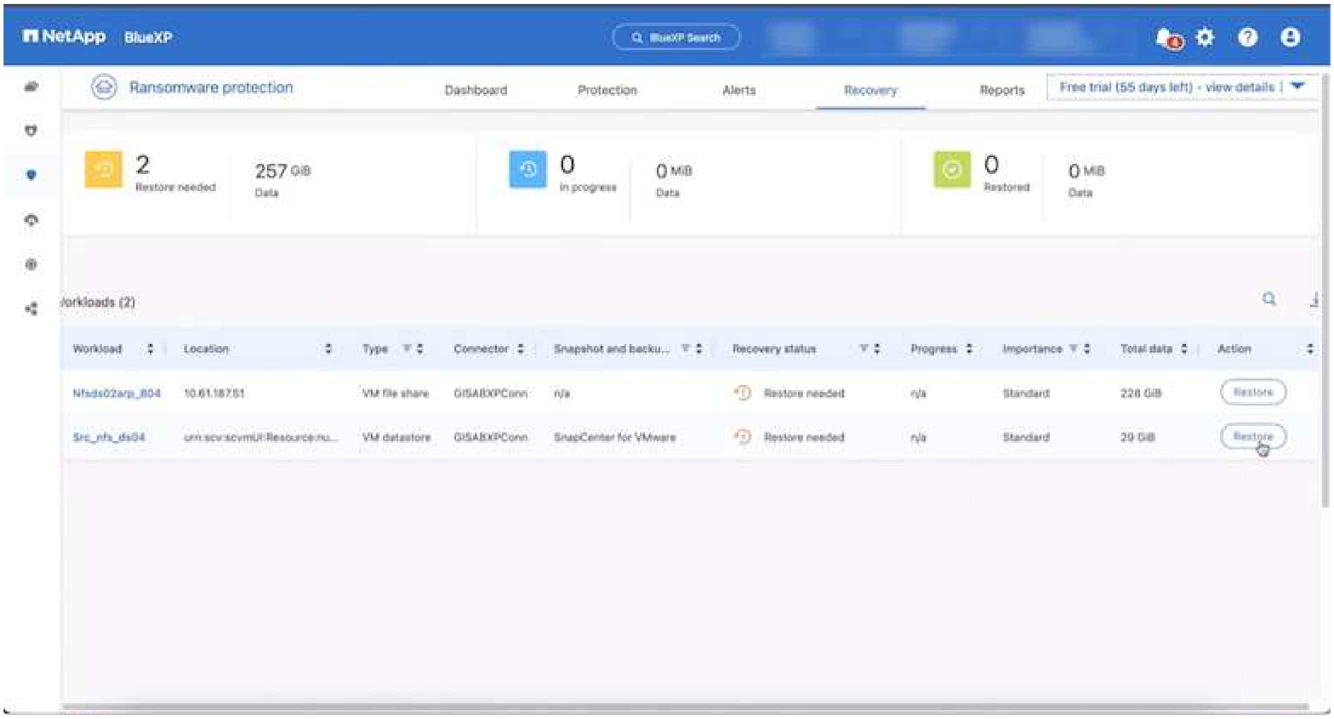
10
Impacted files

ıcident (1) | All selected

☑	Incident ID	Volume	SVM	Working environment	Type	Status	First detected	Evidence	Automated responses
☑	inc1820	Src_NFS_DS04	svm_NFS	NTAP915_Src	Potential attack	New	4 hours ago	1 new extensions detected	2 Snapshot copies

ⓘ The alert can be dismissed if the incident turns out to be false positive.

4. Got to Recovery tab and review the workload information in the Recovery page and select the datastore volume that is in the “Restore needed” state and select Restore.

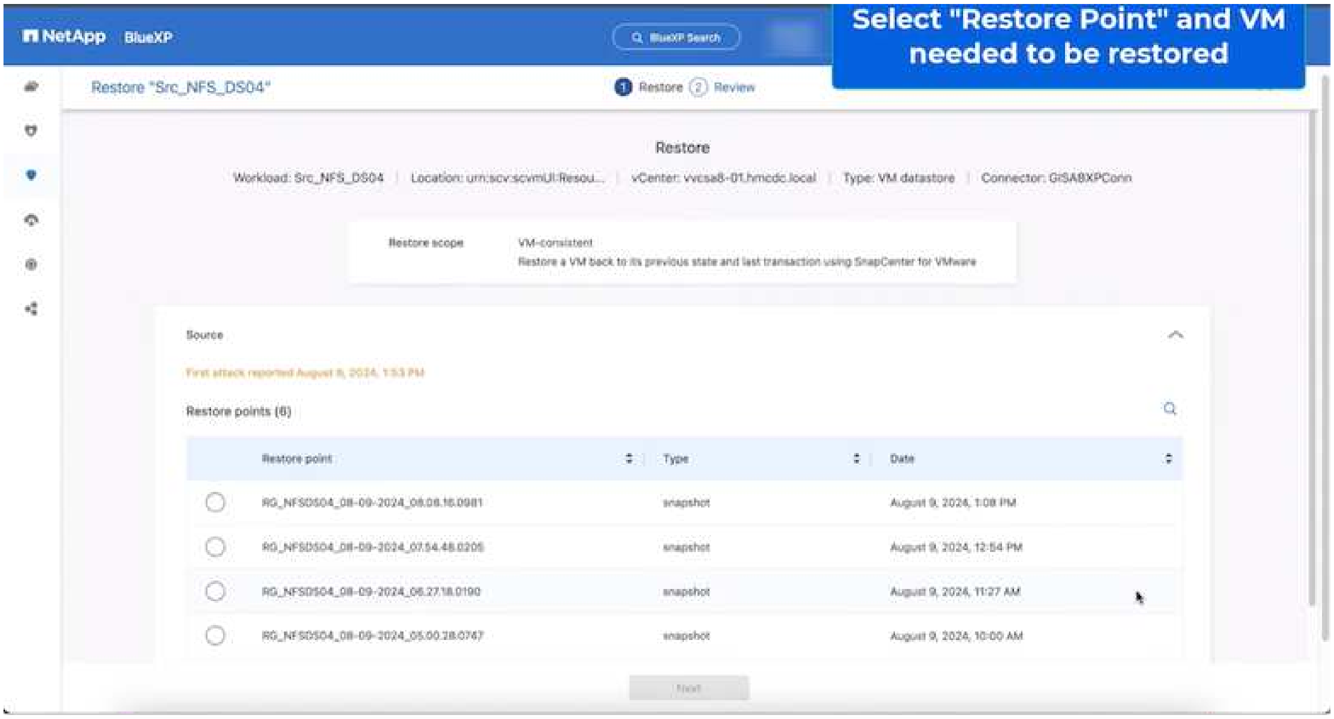


2 Restore needed | 257 GiB Data
0 In progress | 0 MiB Data
0 Restored | 0 MiB Data

Workloads (2)

Workload	Location	Type	Connector	Snapshot and backu...	Recovery status	Progress	Importance	Total data	Action
Nfsds02arp_804	10.61.187.51	VM file share	GISABXPConn	n/a	Restore needed	n/a	Standard	228 GiB	Restore
Src_nfs_ds04	urn:scv:scvmUI:Resource:nu...	VM datastore	GISABXPConn	SnapCenter for VMware	Restore needed	n/a	Standard	29 GiB	Restore

5. In this case, the restore scope is "By VM" (for SnapCenter for VMs, the restore scope is "By VM")



Restore "Src_NFS_DS04"

Restore

Workload: Src_NFS_DS04 | Location: urn:scv:scvmUI:Resou... | vCenter: vvcsa8-01.hmcdc.local | Type: VM datastore | Connector: GISABXPConn

Restore scope: VM-consistent
Restore a VM back to its previous state and last transaction using SnapCenter for VMware

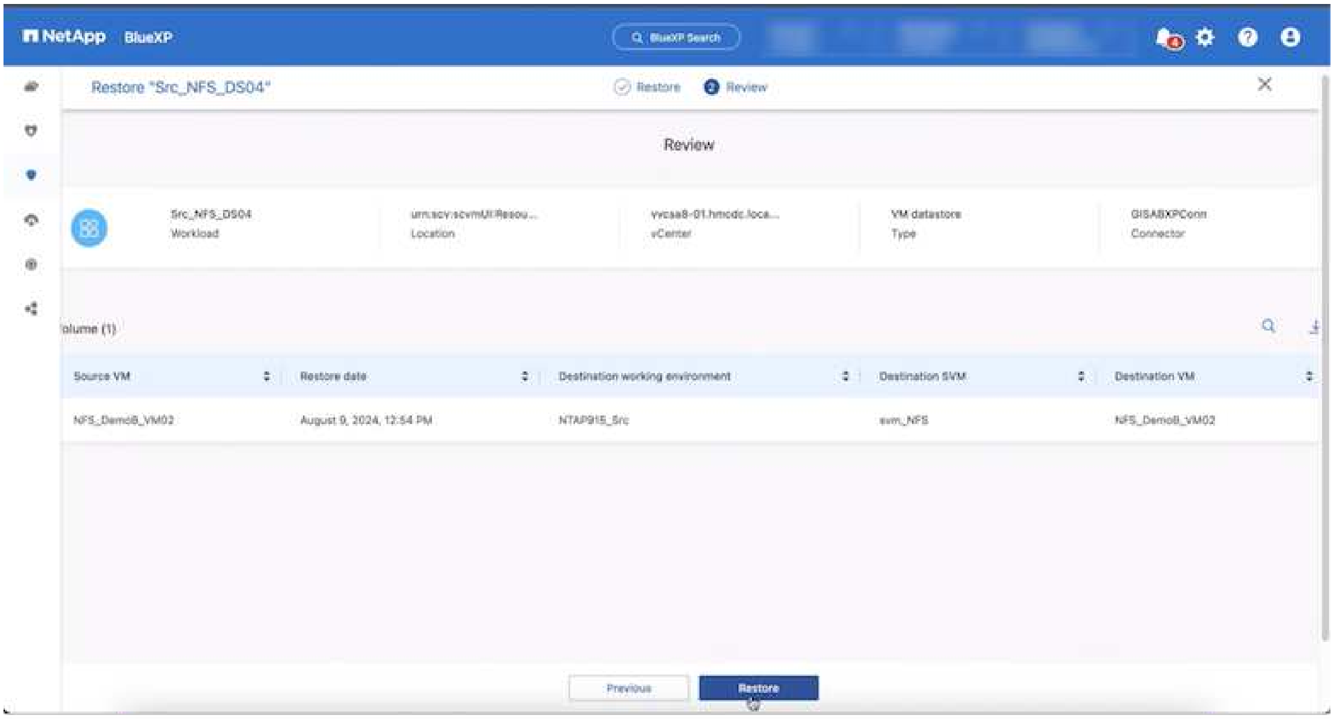
Source

First attack reported August 9, 2024, 1:53 PM

Restore points (6)

	Restore point	Type	Date
○	RG_NFSDS04_08-09-2024_08.08.16.0981	snapshot	August 9, 2024, 1:08 PM
○	RG_NFSDS04_08-09-2024_07.54.48.0205	snapshot	August 9, 2024, 12:54 PM
○	RG_NFSDS04_08-09-2024_06.27.18.0190	snapshot	August 9, 2024, 11:27 AM
○	RG_NFSDS04_08-09-2024_05.00.28.0747	snapshot	August 9, 2024, 10:00 AM

6. Choose the restore point to use to restore the data and select Destination and click on Restore.



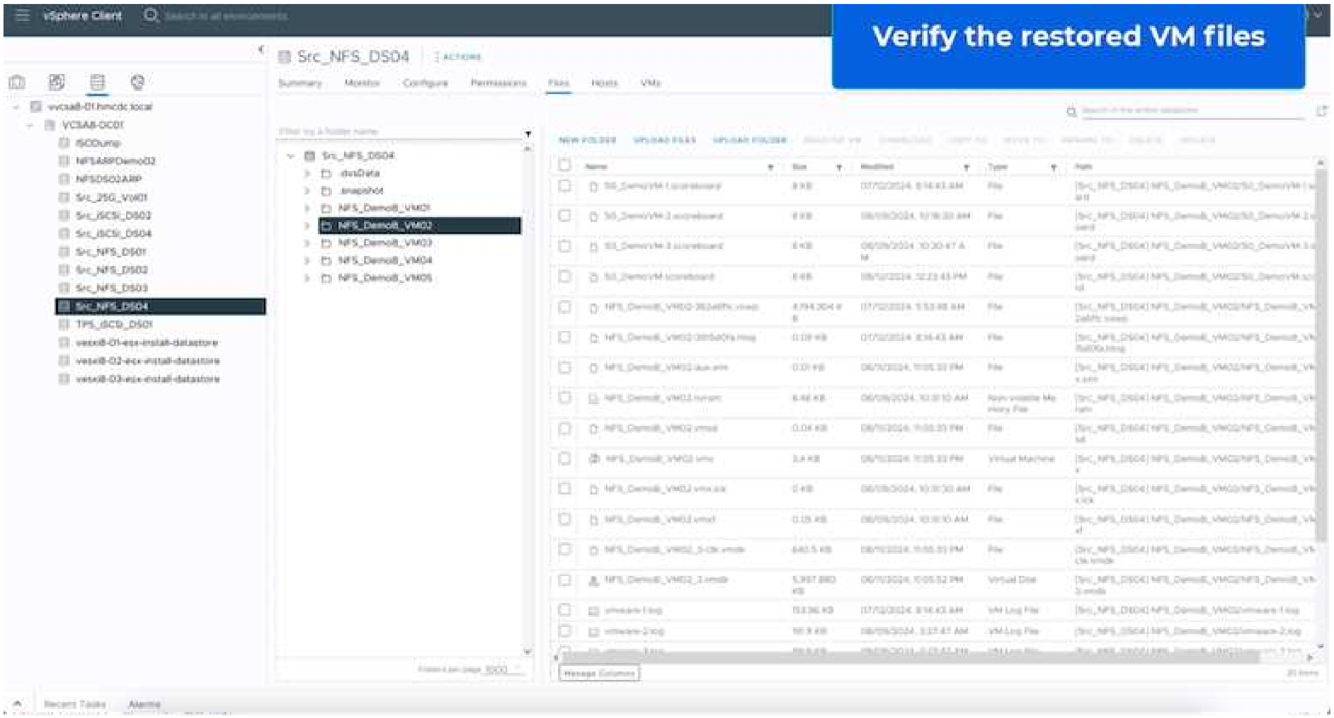
Review

Src_NFS_DS04 Workload | urn:scv:scvmUI:Resou... Location | vvcsa8-01.hmcdc.loca... vCenter | VM datastore Type | GISABXPConn Connector

olume (1)

Source VM	Restore date	Destination working environment	Destination SVM	Destination VM
NFS_DemoB_VM02	August 9, 2024, 12:54 PM	NTAP915_Src	svm_NFS	NFS_DemoB_VM02

7. From the top menu, select Recovery to review the workload on the Recovery page where the status of the operation moves through the states. Once restore is complete, the VM files are restored as shown below.



The recovery can be performed from SnapCenter for VMware or SnapCenter plugin depending on the application.

The NetApp solution provides various effective tools for visibility, detection, and remediation, helping you to spot ransomware early, prevent this spread, and recover quickly, if necessary, to avoid costly downtime. Traditional layered defense solutions remain prevalent, as do third parties and partner solutions for visibility and detection. Effective remediation remains a crucial part of the response to any threat.

VMware Virtual Volumes with ONTAP

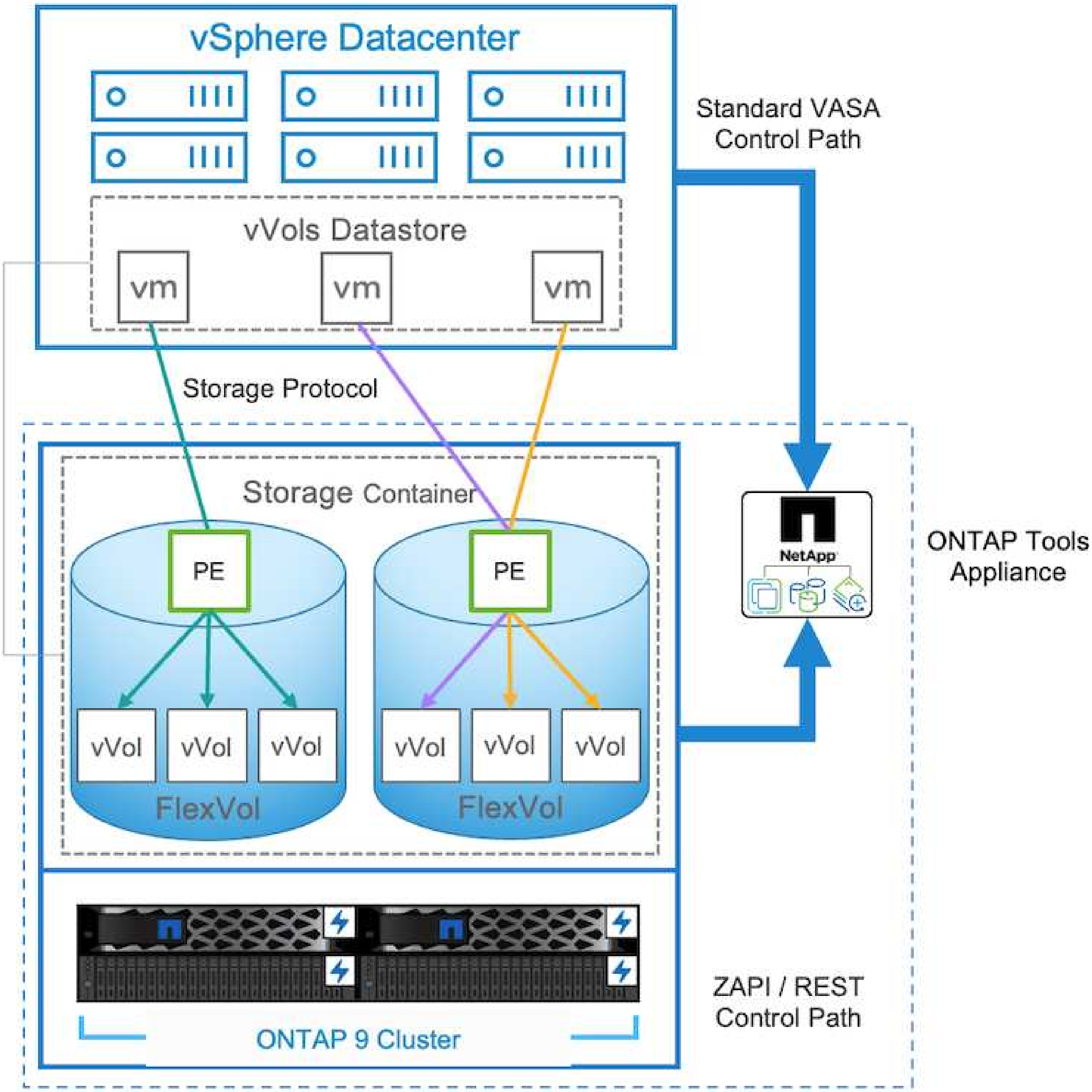
VMware Virtual Volumes (vVols) enables application-specific requirements to drive storage provisioning decisions while
leveraging the rich set of capabilities provided by storage arrays. The vSphere API for Storage Awareness (VASA) make it easy for a VM administrator to use whatever storage capabilities are needed to provision VMs without having to interact with their storage team. Prior to VASA, VM administrators could define VM storage policies, but had to work with their storage administrators to identify appropriate datastores, often by using documentation or naming conventions. With VASA, vCenter administrators with the appropriate permissions can define a range of storage capabilities which vCenter users can then use to provision VMs. The mapping between VM storage policy and datastore storage capability profile allows vCenter to display a list of compatible datastores for selection, as well as enabling other technologies like Aria (formerly known as vRealize) Automation or Tanzu Kubernetes Grid to automatically select storage from an assigned policy. This approach is known as storage policy based management. While storage capability profiles and policies may also be used with traditional datastores, our focus here is on vVols datastores. The VASA provider for ONTAP is included as part of ONTAP tools for VMware vSphere.

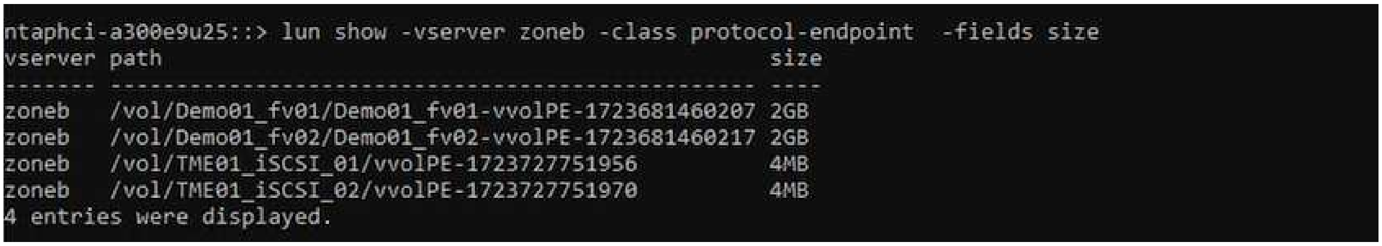
The advantages of having VASA Provider out of Storage Array, includes:

- Single Instance can manage multiple Storage Arrays.
- Release cycle doesn’t have to depend on Storage OS release.
- Resources on Storage Array is much expensive.

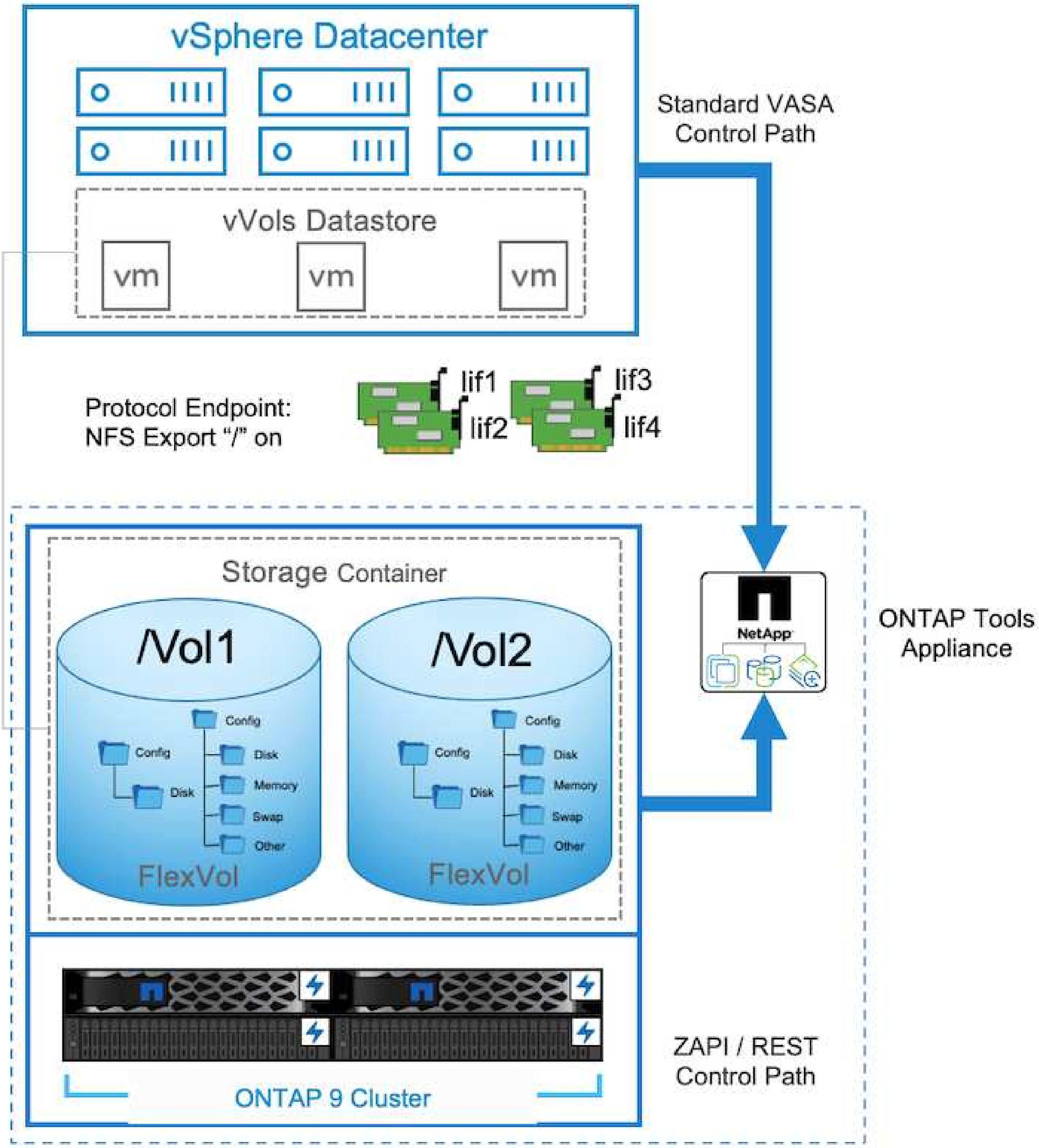
Each vVol datastore is backed by Storage Container which is a logical entry in VASA provider to define the storage capacity. The Storage container with ONTAP tools is constructed with ONTAP volumes. The Storage Container can be expanded by adding ONTAP volumes within same SVM.

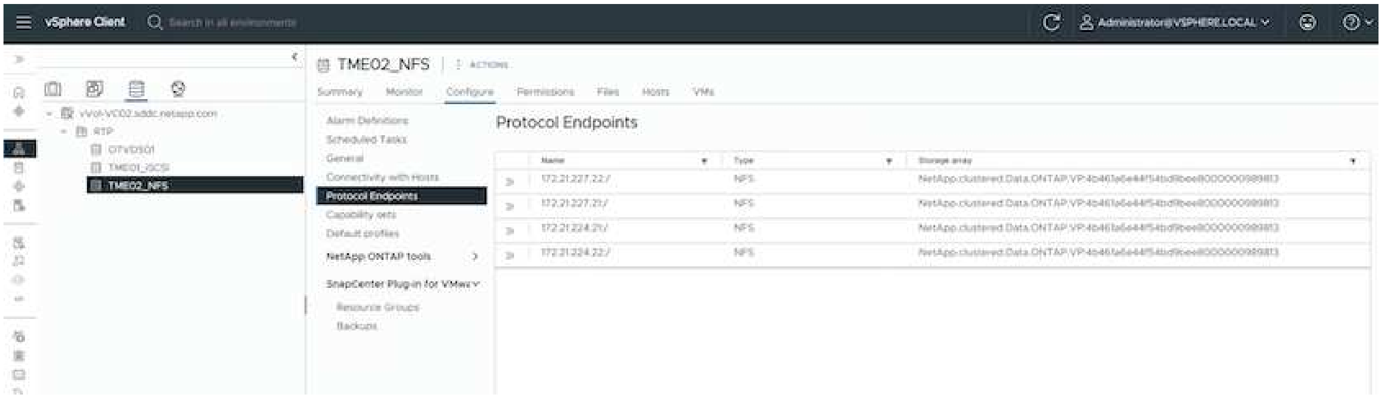
The Protocol Endpoint (PE) is mostly managed by ONTAP tools. In case of iSCSI based vVols, one PE is created for every ONTAP volume that is part of that storage container or vVol datastore. The PE for iSCSI is a small sized LUN (4MiB for 9.x and 2GiB for 10.x) that is presented to vSphere host and multipathing policies are applied to the PE.




```
ntaphci-a300e9u25::> lun show -vserver zoneb -class protocol-endpoint  -fields size
vserver path                                                  size
------- ----------------------------------------------------- ----
zoneb   /vol/Demo01_fv01/Demo01_fv01-vvolPE-1723681460207 2GB
zoneb   /vol/Demo01_fv02/Demo01_fv02-vvolPE-1723681460217 2GB
zoneb   /vol/TME01_iSCSI_01/vvolPE-1723727751956          4MB
zoneb   /vol/TME01_iSCSI_02/vvolPE-1723727751970          4MB
4 entries were displayed.
```

For NFS, one PE is created for root filesystem export with every NFS data lif on SVM on which the storage container or vVol datastore resides.





Protocol Endpoints

Name	Type	Storage array
172.21.227.22:/	NFS	NetApp-clustered-Data-ONTAP-VP:4b461a6e44f54bd9bee8000000989813
172.21.227.21:/	NFS	NetApp-clustered-Data-ONTAP-VP:4b461a6e44f54bd9bee8000000989813
172.21.224.21:/	NFS	NetApp-clustered-Data-ONTAP-VP:4b461a6e44f54bd9bee8000000989813
172.21.224.22:/	NFS	NetApp-clustered-Data-ONTAP-VP:4b461a6e44f54bd9bee8000000989813

ONTAP tools manages the lifecycle of PE and also for vSphere host communication with vSphere cluster expansion and shrinkage. ONTAP tools API is available to integrate with existing automation tool.

Currently, ONTAP tools for VMware vSphere is available with two releases.

ONTAP tools 9.x

- When vVol support for NVMe/FC is required
- US Federal or EU regulatory requirements
- More use cases integrated with SnapCenter Plug-in for VMware vSphere

ONTAP tools 10.x

- High Availablity
- Multi-tenancy
- Large Scale
- SnapMirror active sync support for VMFS datastore
- Upcoming integration for certain use cases with SnapCenter Plug-in for VMware vSphere

Why vVols?

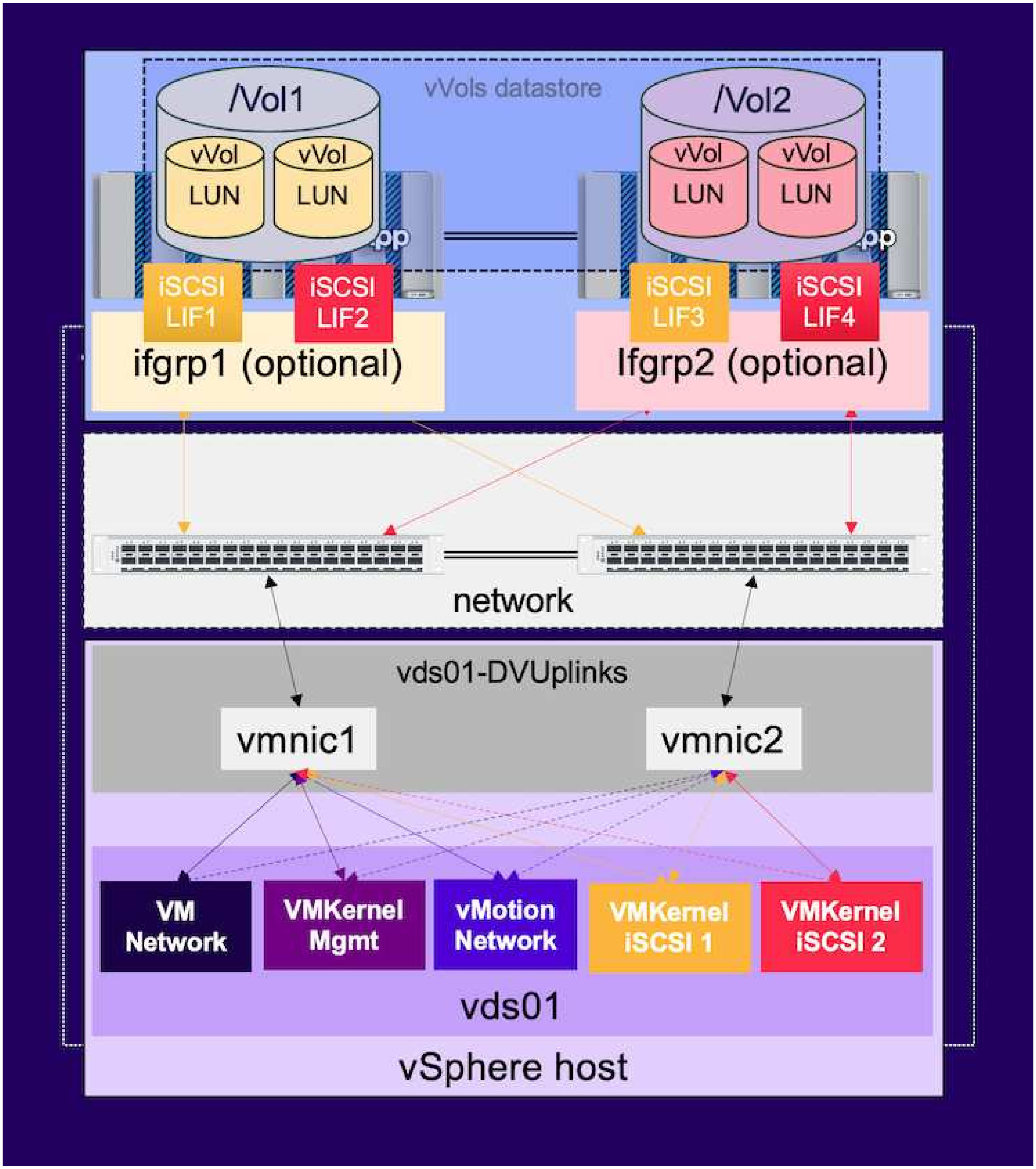
VMware Virtual Volumes (vVols) provides the following benefits:

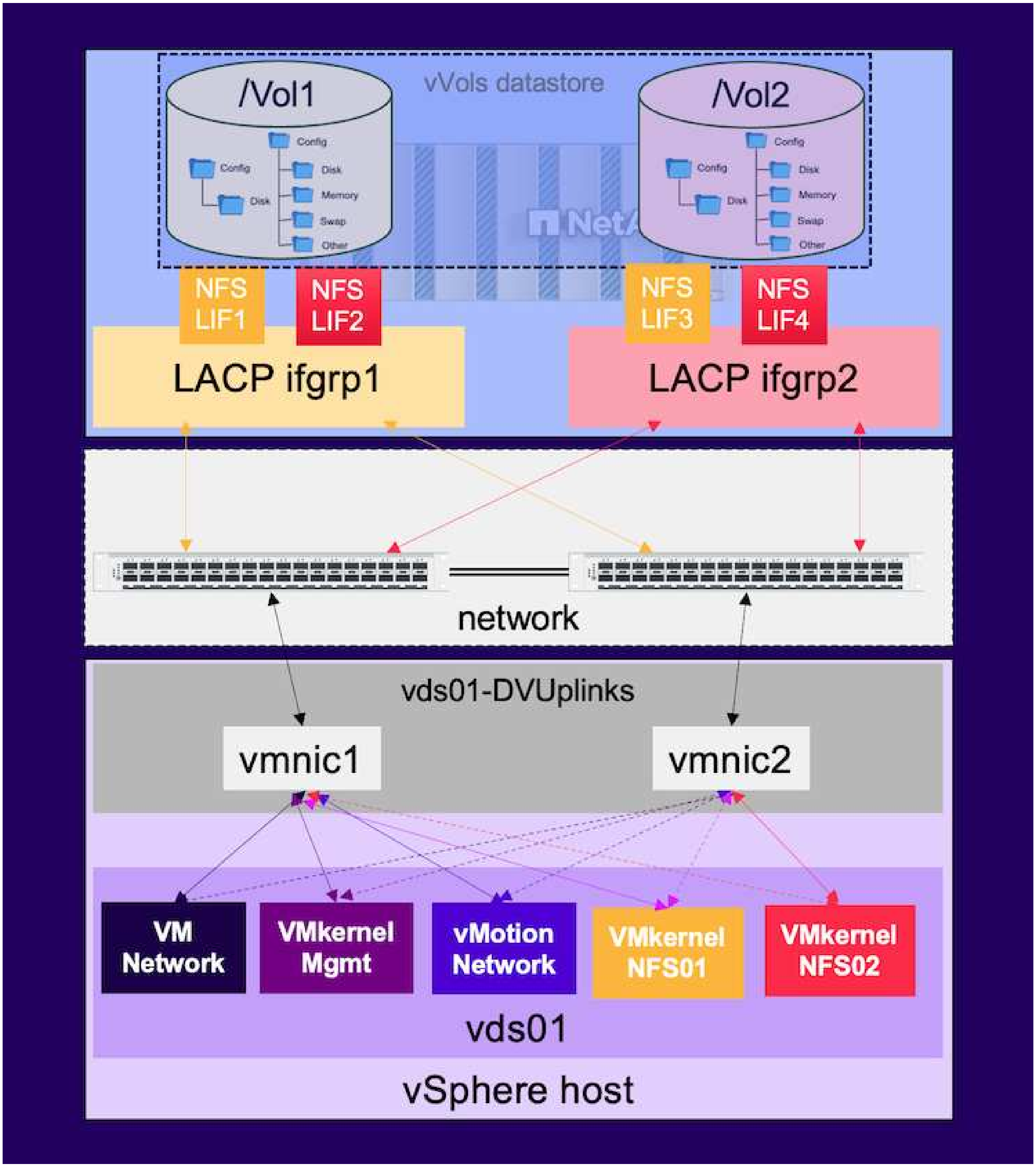
- Simplified provisioning (No need to worry about Maximum LUN limits per vSphere host or need to create the NFS exports for each volume)
- Minimizes the number of iSCSI/FC paths (For block SCSI based vVol)
- Snapshots, Clones & other Storage operations are typically offloaded to storage array and performs much faster.
- Simplified data migrations for the VMs (No need to coordinate with other VM owners in same LUN)
- QoS policies applied at VM disk level rather than volume level.
- Operational simplicity (Storage vendors provide their differenciated features in VASA provider)
- Supports large scale of VMs.
- vVol replication support to migrate between vCenters.
- Storage Administrators has option to monitor at VM disk level.

Connectivity options

Dual fabric environment is typically recommended for the storage networks to address the high availability, performance and fault tolerance. The vVols are supported with iSCSI, FC, NFSv3 and NVMe/FC.
NOTE: Refer Interoperability Matrix Tool (IMT) for supported ONTAP Tool version

The connectivity option remains consistent with VMFS datastore or NFS datastore options.
A sample reference vSphere network is shown below for iSCSI and NFS.





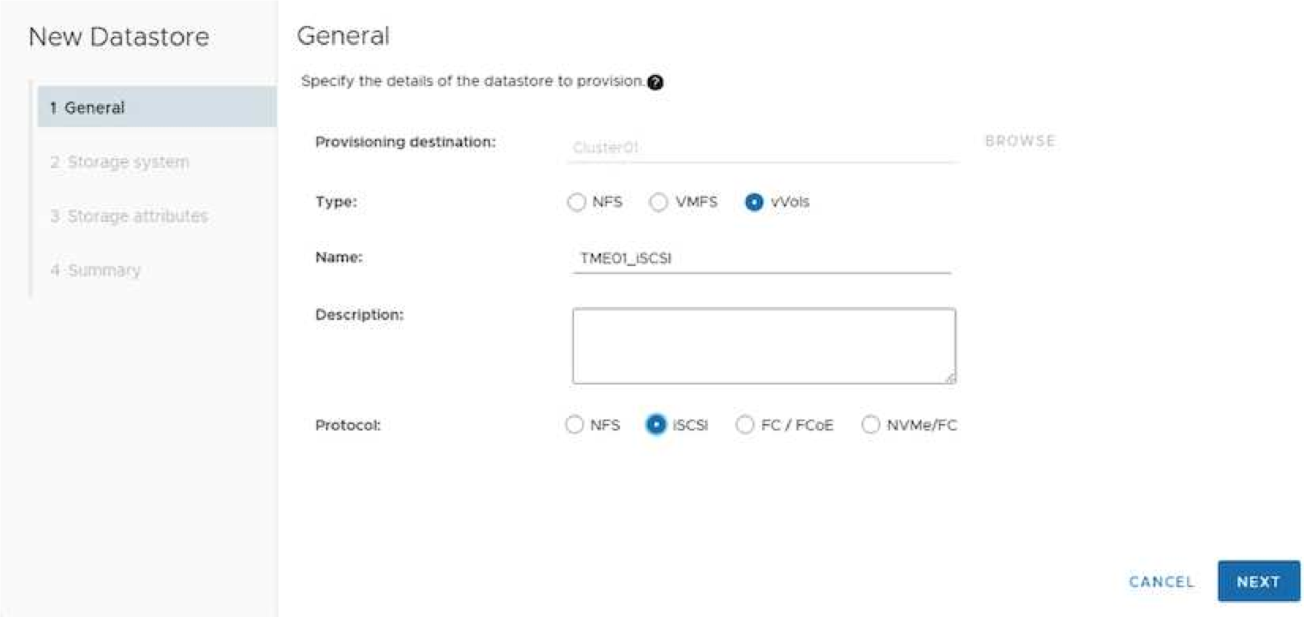
Provisioning using ONTAP tools for VMware vSphere

The vVol datastore can be provisioned similar to VMFS or NFS datastore using ONTAP tools. If ONTAP tools plug-in is not available on vSphere client UI, refer the How to get started section below.

With ONTAP tools 9.13

1. Right click on vSphere cluster or host and select Provision Datastore under NetApp ONTAP tools.

2. Keep the type as vVols, provide name for the datastore and select the desired protocol



Specify the details of the datastore to provision.

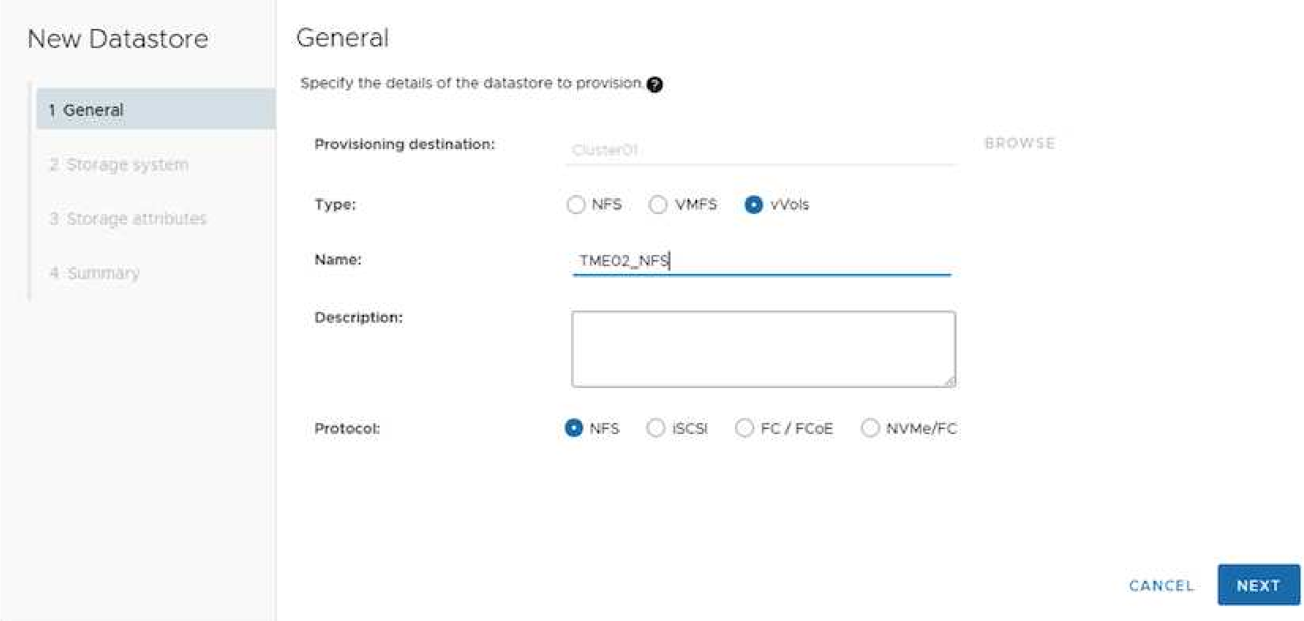
Provisioning destination: Cluster01

Type: ○ NFS ○ VMFS ● vVols

Name: TME01_iSCSI

Description:

Protocol: ○ NFS ● iSCSI ○ FC / FCoE ○ NVMe/FC



Specify the details of the datastore to provision.

Provisioning destination: Cluster01

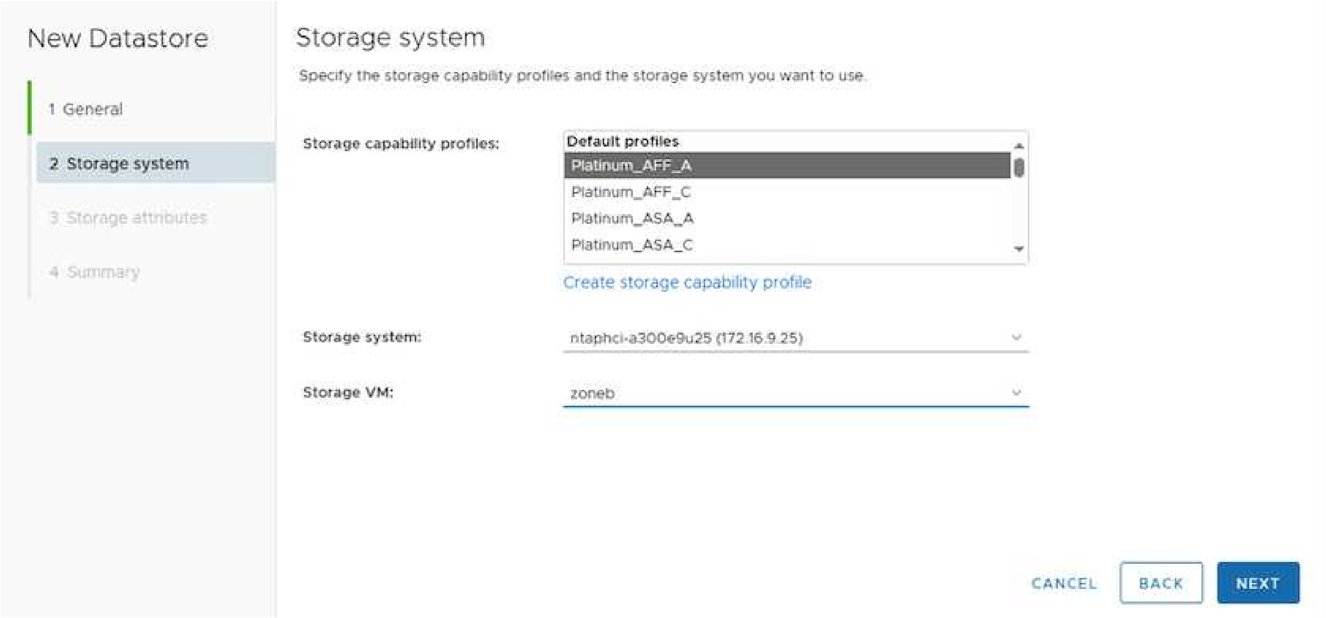
Type: ○ NFS ○ VMFS ● vVols

Name: TME02_NFS

Description:

Protocol: ● NFS ○ iSCSI ○ FC / FCoE ○ NVMe/FC

3. Select the desired storage capability profile, pick the storage system and SVM.



New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles:

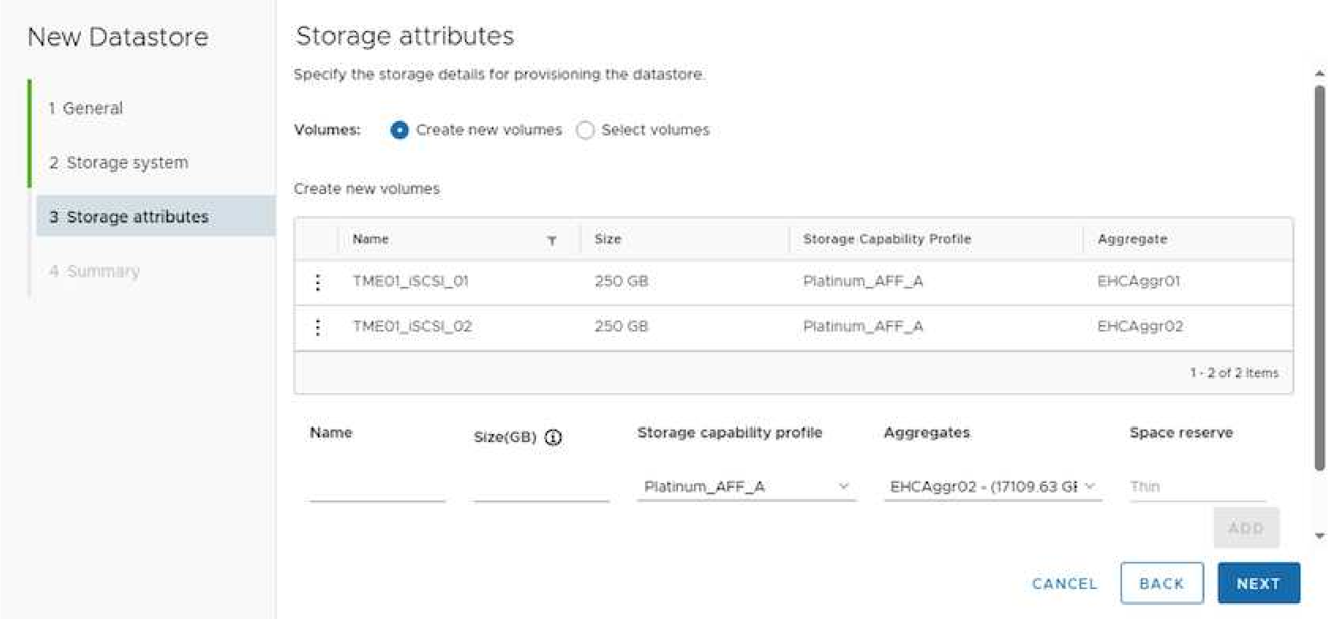
Default profiles
- Platinum_AFF_A
- Platinum_AFF_C
- Platinum_ASA_A
- Platinum_ASA_C

Create storage capability profile

Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: zoneb

4. Create new ONTAP volumes or select existing one for the vVol datastore.



New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: ● Create new volumes ○ Select volumes

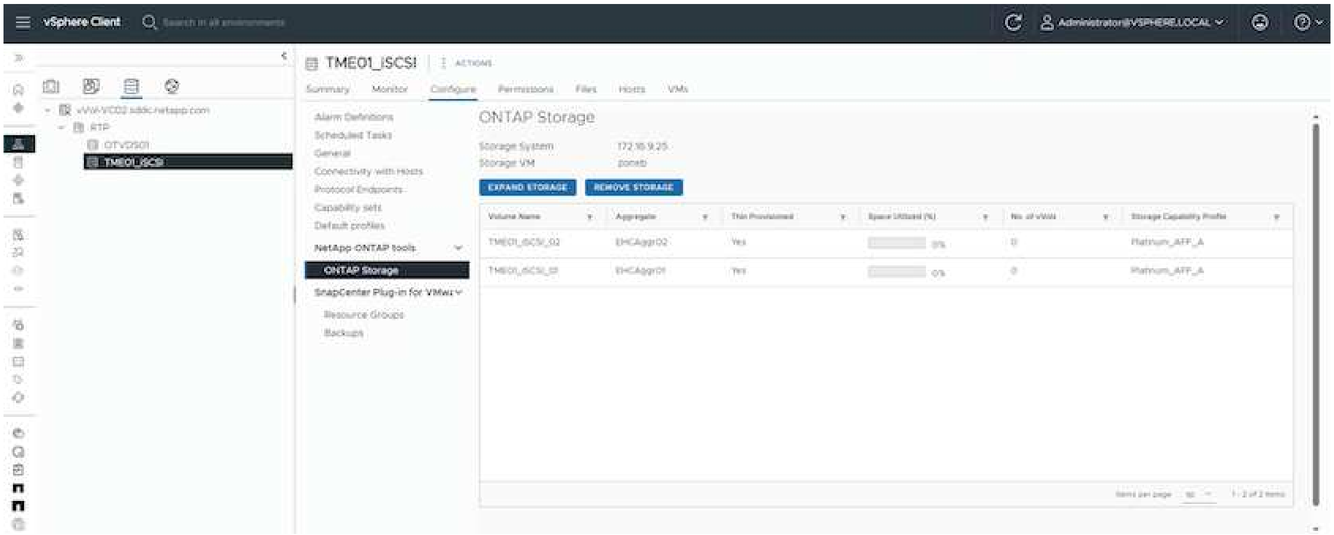
Create new volumes

	Name	Size	Storage Capability Profile	Aggregate
⋮	TME01_iSCSI_01	250 GB	Platinum_AFF_A	EHCAggr01
⋮	TME01_iSCSI_02	250 GB	Platinum_AFF_A	EHCAggr02

1 - 2 of 2 items

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
		Platinum_AFF_A	EHCAggr02 - (17109.63 GI	Thin

ONTAP volumes can be viewed or change later from the datastore option.



TME01_iSCSI

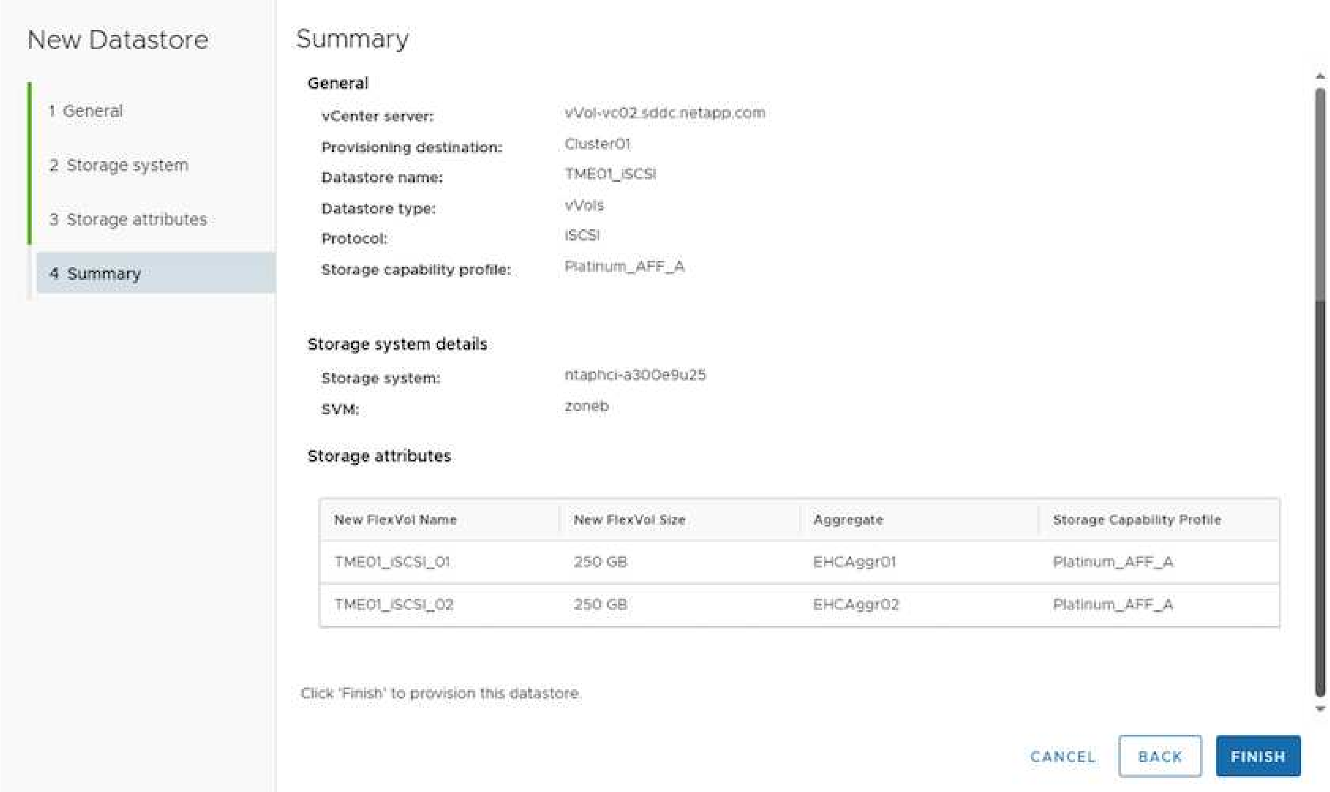
ONTAP Storage

Storage System: 172.16.9.25

Storage VM: zoneb

Volume Name	Aggregate	Thin Provisioned	Space Utilized (%)	No. of vVols	Storage Capability Profile
TME01_iSCSI_02	EHCAggr02	Yes	0%	0	Platinum_AFF_A
TME01_iSCSI_01	EHCAggr01	Yes	0%	0	Platinum_AFF_A

5. Review the summary and click on Finish to create the vVol datastore.



Summary

General

vCenter server:	vVol-vc02.sddc.netapp.com
Provisioning destination:	Cluster01
Datastore name:	TME01_iSCSI
Datastore type:	vVols
Protocol:	iSCSI
Storage capability profile:	Platinum_AFF_A

Storage system details

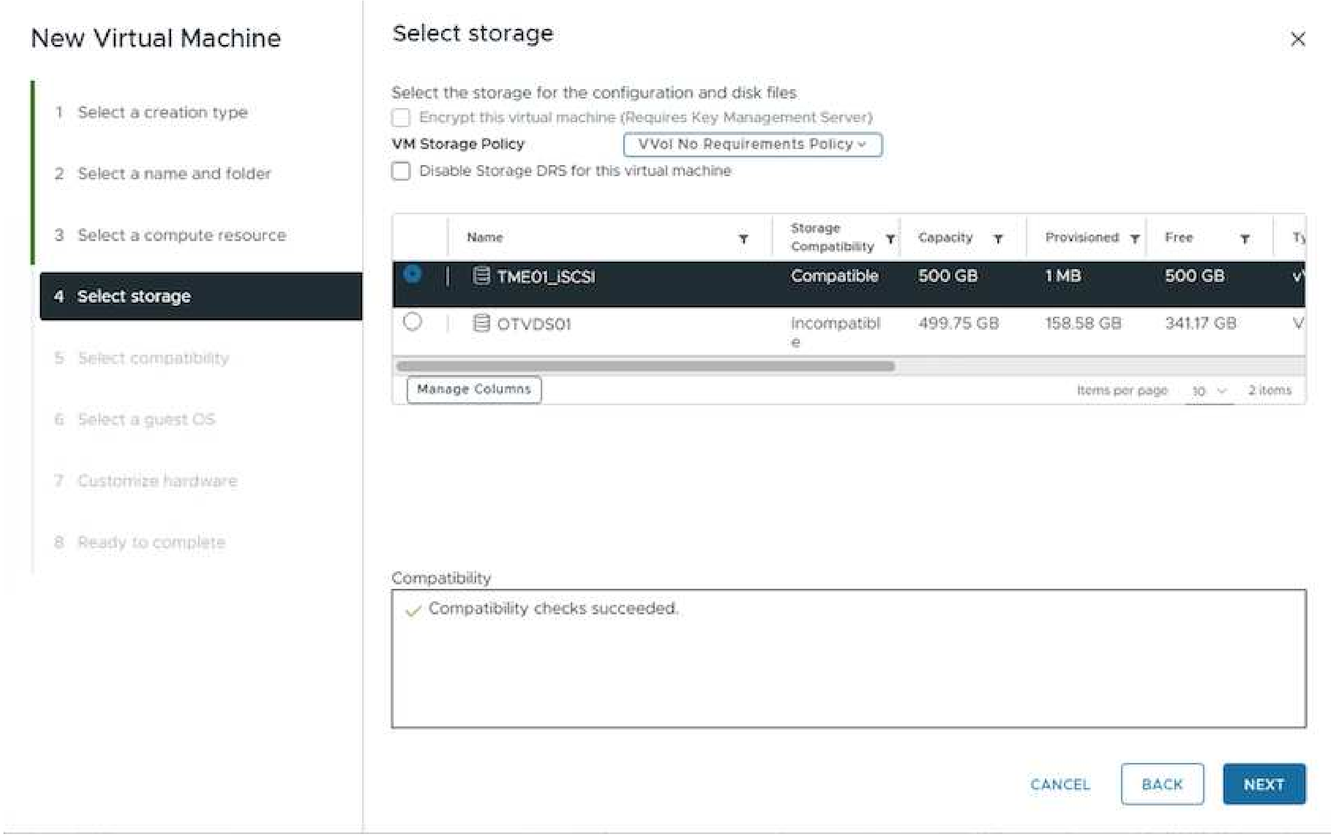
Storage system:	ntaphci-a300e9u25
SVM:	zoneb

Storage attributes

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile
TME01_iSCSI_01	250 GB	EHCAggr01	Platinum_AFF_A
TME01_iSCSI_02	250 GB	EHCAggr02	Platinum_AFF_A

Click 'Finish' to provision this datastore.

6. Once vVol datastore is created, it can be consumed like any other datastore. Here is an example of assigning datastore based on VM storage policy to a VM that is getting created.



New Virtual Machine

1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

VM Storage Policy: VVol No Requirements Policy

□ Disable Storage DRS for this virtual machine

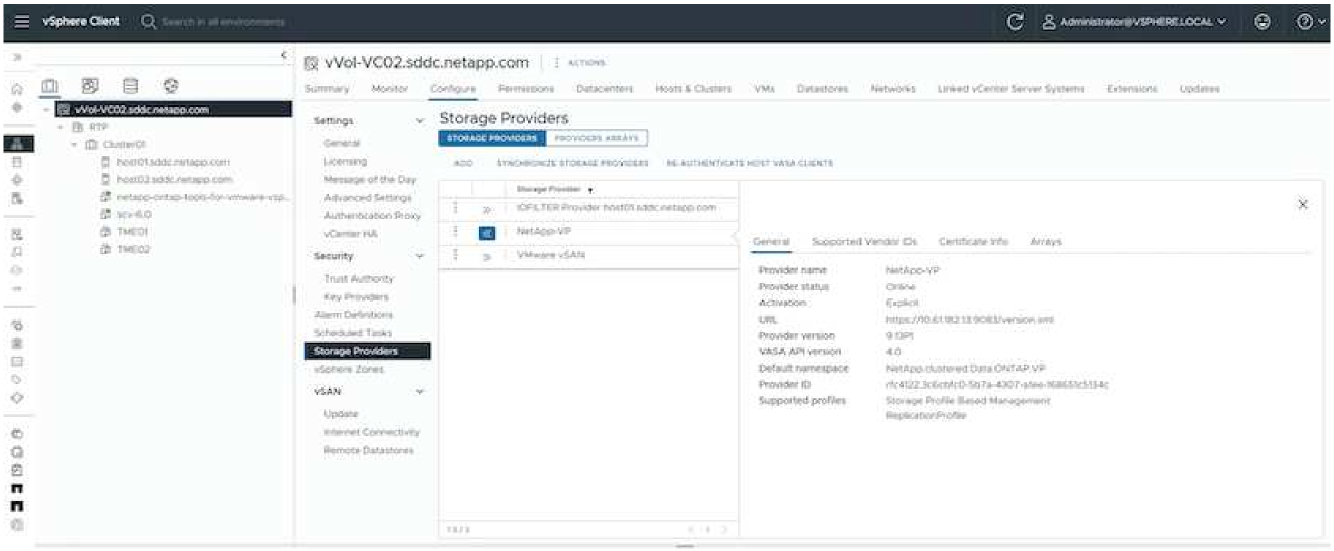
	Name	Storage Compatibility	Capacity	Provisioned	Free	Ty
●	TME01_iSCSI	Compatible	500 GB	1 MB	500 GB	v
○	OTVDS01	Incompatible	499.75 GB	158.58 GB	341.17 GB	V

Manage Columns — Items per page 10 — 2 items

Compatibility

✓ Compatibility checks succeeded.

7. vVol details can be retrieved using web based CLI interface. The URL of the portal is same as VASA provider URL without the file name version.xml.



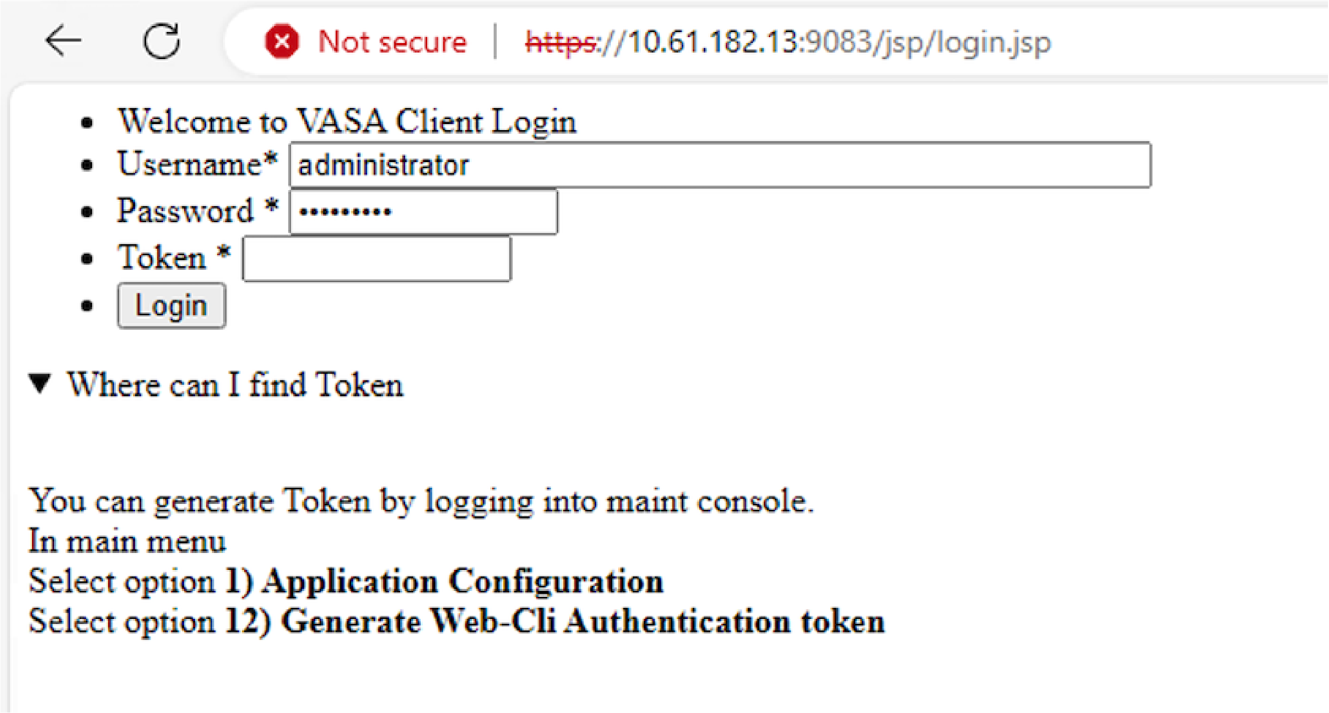
vVol-VC02.sddc.netapp.com

Storage Providers

Storage Provider
IOFILTER Provider host01.sddc.netapp.com
NetApp-VP
VMware vSAN

Provider name	NetApp-VP
Provider status	Online
Activation	Explicit
URL	https://10.61.182.13:9083/version.xml
Provider version	9.13P1
VASA API version	4.0
Default namespace	NetApp.clustered.Data.ONTAP.VP
Provider ID	rfc4122.3c6cbfc0-5b7a-4307-a1ee-168651c5134c
Supported profiles	Storage Profile Based Management ReplicationProfile

The credential should match the info used during provision of ONTAP tools

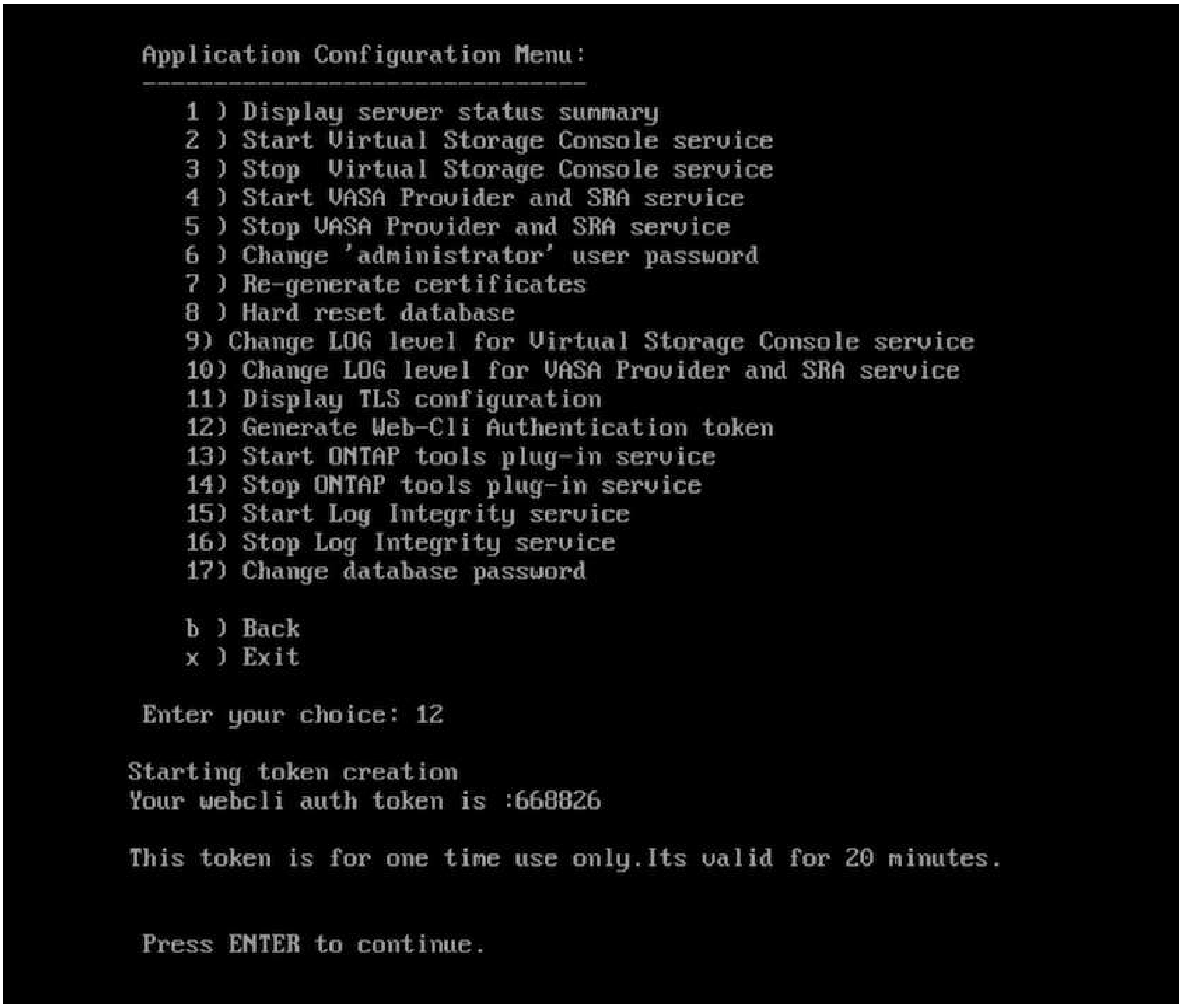


- Welcome to VASA Client Login
- Username* administrator
- Password * ••••••••••
- Token *
- Login

▼ Where can I find Token

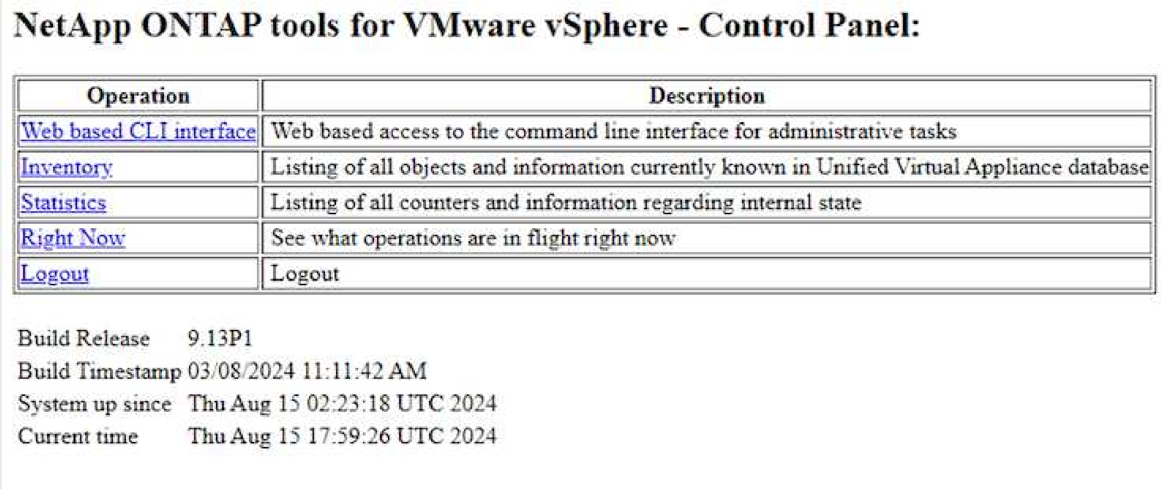
You can generate Token by logging into maint console.
In main menu
Select option **1) Application Configuration**
Select option **12) Generate Web-Cli Authentication token**

or use updated password with ONTAP tools maintenance console.



```
Application Configuration Menu:
--------------------------------

   1 ) Display server status summary
   2 ) Start Virtual Storage Console service
   3 ) Stop  Virtual Storage Console service
   4 ) Start VASA Provider and SRA service
   5 ) Stop VASA Provider and SRA service
   6 ) Change 'administrator' user password
   7 ) Re-generate certificates
   8 ) Hard reset database
   9) Change LOG level for Virtual Storage Console service
   10) Change LOG level for VASA Provider and SRA service
   11) Display TLS configuration
   12) Generate Web-Cli Authentication token
   13) Start ONTAP tools plug-in service
   14) Stop ONTAP tools plug-in service
   15) Start Log Integrity service
   16) Stop Log Integrity service
   17) Change database password

   b ) Back
   x ) Exit

Enter your choice: 12

Starting token creation
Your webcli auth token is :668826

This token is for one time use only.Its valid for 20 minutes.


Press ENTER to continue.
```

Select Web based CLI interface.

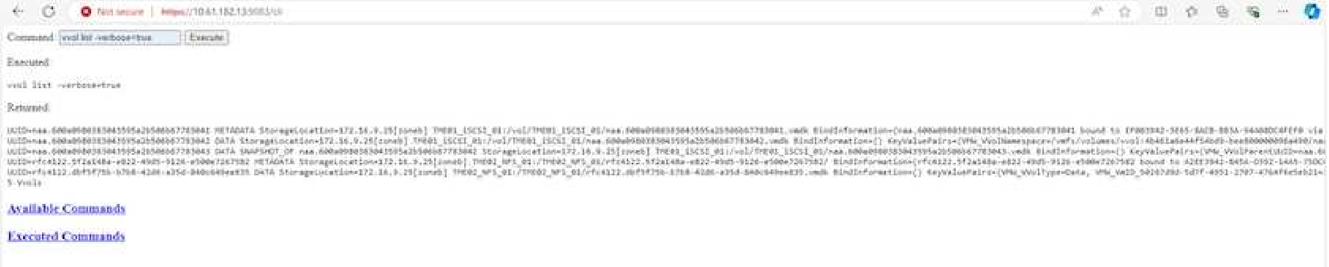


NetApp ONTAP tools for VMware vSphere - Control Panel:

Operation	Description
Web based CLI interface	Web based access to the command line interface for administrative tasks
Inventory	Listing of all objects and information currently known in Unified Virtual Appliance database
Statistics	Listing of all counters and information regarding internal state
Right Now	See what operations are in flight right now
Logout	Logout

Build Release	9.13P1
Build Timestamp	03/08/2024 11:11:42 AM
System up since	Thu Aug 15 02:23:18 UTC 2024
Current time	Thu Aug 15 17:59:26 UTC 2024

Type the desired command from the Available command list. To list the vVol details along with underlying storage info, try vvol list -verbose=true



Command: vvol list -verbose=true Execute

Executed:

```
vvol list -verbose=true
```

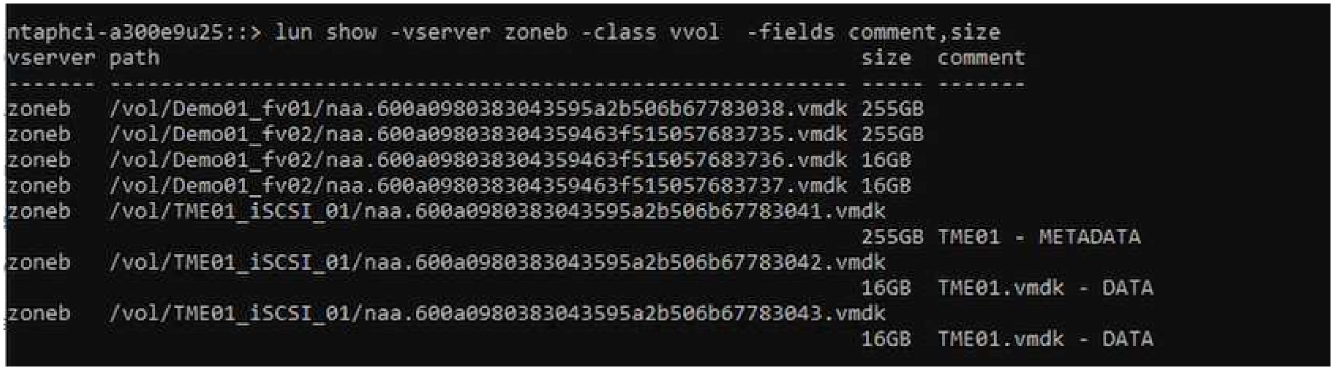
Returned:

```
UUID=naa.600a0980383043595a2b506b67783041 METADATA StorageLocation=172.16.9.25[zoneb] TME01_iSCSI_01:/vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783041.vmdk BindInformation={naa.600a0980383043595a2b506b67783041 bound to [illegible] via
UUID=naa.600a0980383043595a2b506b67783042 DATA StorageLocation=172.16.9.25[zoneb] TME01_iSCSI_01:/vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783042.vmdk BindInformation={} KeyValuePairs={VMW_VVolNamespace=/vmfs/volumes/vvol:4b461a6a44f54bd5-bea0000000006a490/na
UUID=naa.600a0980383043595a2b506b67783043 DATA SNAPSHOT_OF naa.600a0980383043595a2b506b67783042 StorageLocation=172.16.9.25[zoneb] TME01_iSCSI_01:/vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783043.vmdk BindInformation={} KeyValuePairs={VMW_VVolParentUUID=naa.60
UUID=rfc4122.5f2a148a-e822-49d5-9126-e500e7267582 METADATA StorageLocation=172.16.9.25[zoneb] TME02_NFS_01:/TME02_NFS_01/rfc4122.5f2a148a-e822-49d5-9126-e500e7267582/ BindInformation={rfc4122.5f2a148a-e822-49d5-9126-e500e7267582 bound to [illegible]
UUID=rfc4122.dbf5f756-b768-42d6-a35d-840c640ea835 DATA StorageLocation=172.16.9.25[zoneb] TME02_NFS_01:/TME02_NFS_01/rfc4122.dbf5f756-b768-42d6-a35d-840c640ea835.vmdk BindInformation={} KeyValuePairs={VMW_VVolType=Data, VMW_VmID_50267d92-5d7f-4951-2797-476df6e5eb21=
5 Vvols
```

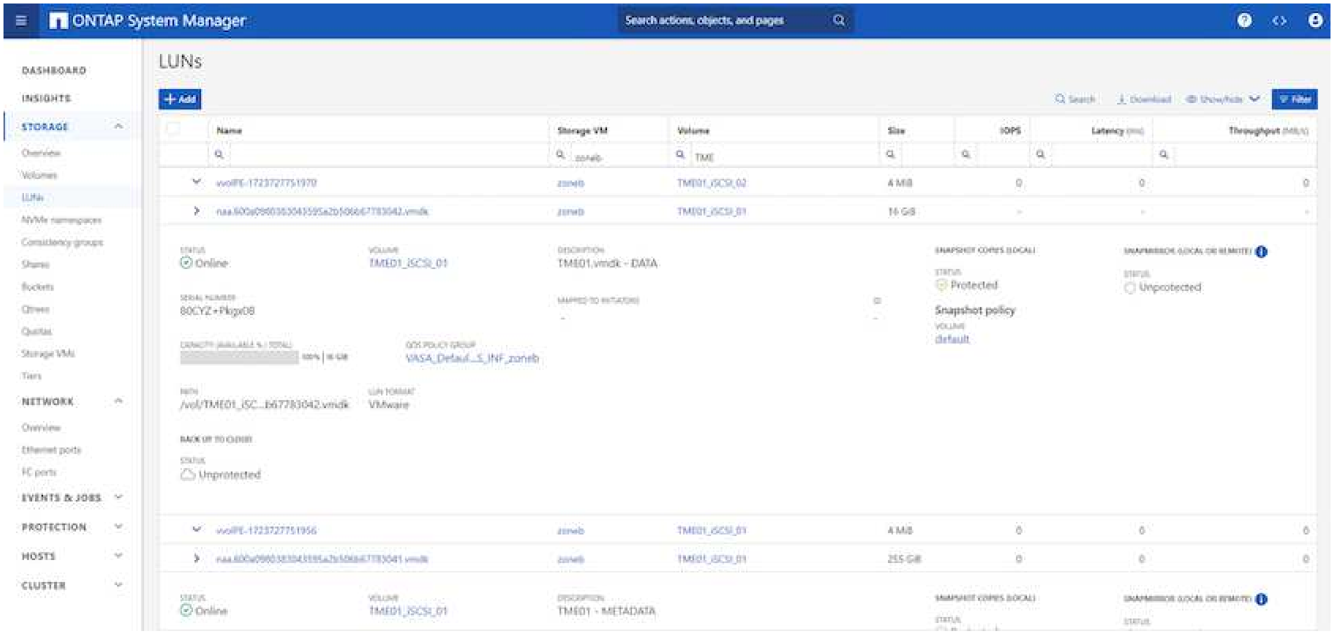
Available Commands

Executed Commands

For LUN based, the ONTAP cli or System Manager can also be used.



```
ntaphci-a300e9u25::> lun show -vserver zoneb -class vvol  -fields comment,size
vserver path                                                         size  comment
------- ------------------------------------------------------------ ----- -------
zoneb   /vol/Demo01_fv01/naa.600a0980383043595a2b506b67783038.vmdk 255GB
zoneb   /vol/Demo01_fv02/naa.600a098038304359463f515057683735.vmdk 255GB
zoneb   /vol/Demo01_fv02/naa.600a098038304359463f515057683736.vmdk 16GB
zoneb   /vol/Demo01_fv02/naa.600a098038304359463f515057683737.vmdk 16GB
zoneb   /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783041.vmdk
                                                                   255GB TME01 - METADATA
zoneb   /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783042.vmdk
                                                                   16GB  TME01.vmdk - DATA
zoneb   /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783043.vmdk
                                                                   16GB  TME01.vmdk - DATA
```



LUNs

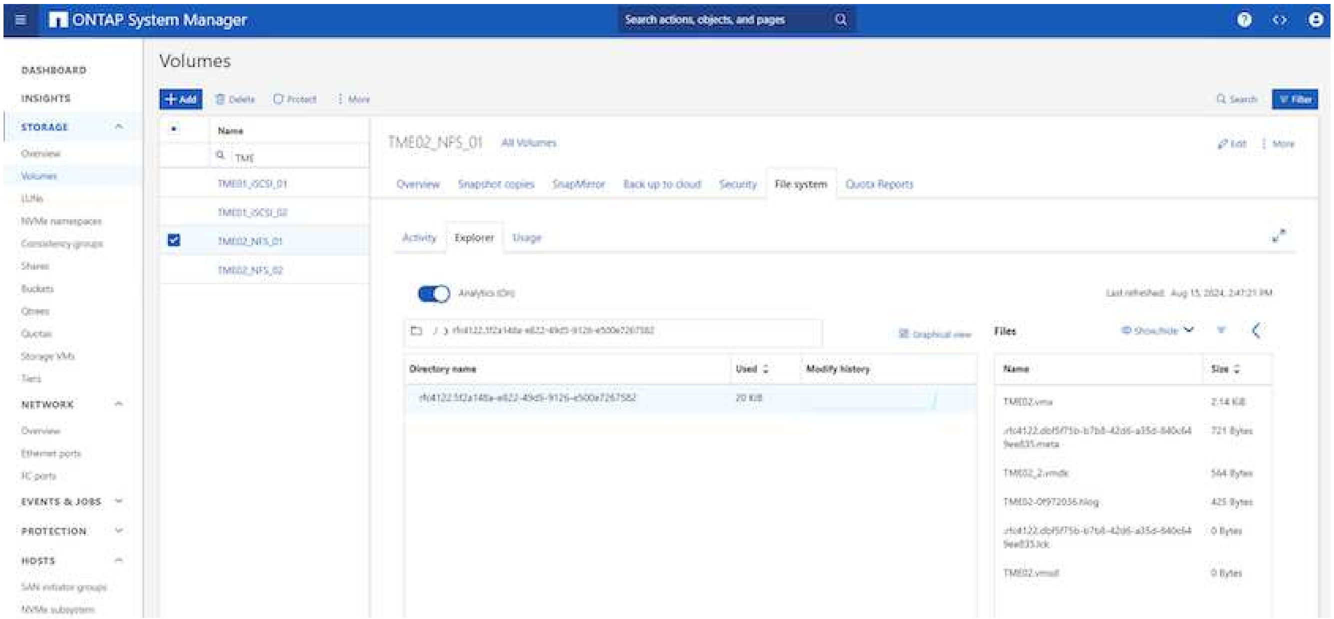
Name	Storage VM	Volume	Size	IOPS	Latency (ms)	Throughput (MB/s)
	zoneb	TME				
vvolPE-1723727751970	zoneb	TME01_iSCSI_02	4 MiB	0	0	0
naa.600a0980383043595a2b506b67783042.vmdk	zoneb	TME01_iSCSI_01	16 GiB	-	-	-

STATUS: Online
VOLUME: TME01_iSCSI_01
DESCRIPTION: TME01.vmdk - DATA
SERIAL NUMBER: 80CYZ+Pkgx08
MAPPED TO INITIATORS: -
ID: -
CAPACITY (AVAILABLE % / TOTAL): 100% | 16 GiB
QOS POLICY GROUP: VASA_Defaul..._S_INF_zoneb
PATH: /vol/TME01_iSC...b67783042.vmdk
LUN FORMAT: VMware
BACK UP TO CLOUD
STATUS: Unprotected
SNAPSHOT COPIES (LOCAL)
STATUS: Protected
Snapshot policy
VOLUME: default
SNAPMIRROR (LOCAL OR REMOTE)
STATUS: Unprotected

Name	Storage VM	Volume	Size	IOPS	Latency (ms)	Throughput (MB/s)
vvolPE-1723727751956	zoneb	TME01_iSCSI_01	4 MiB	0	0	0
naa.600a0980383043595a2b506b67783041.vmdk	zoneb	TME01_iSCSI_01	255 GiB	0	0	0

STATUS: Online
VOLUME: TME01_iSCSI_01
DESCRIPTION: TME01 - METADATA
SNAPSHOT COPIES (LOCAL)
STATUS
SNAPMIRROR (LOCAL OR REMOTE)
STATUS

For NFS based, the System Manager can be used to browse the datastore.



Last refreshed: Aug 15, 2024, 2:47:21 PM

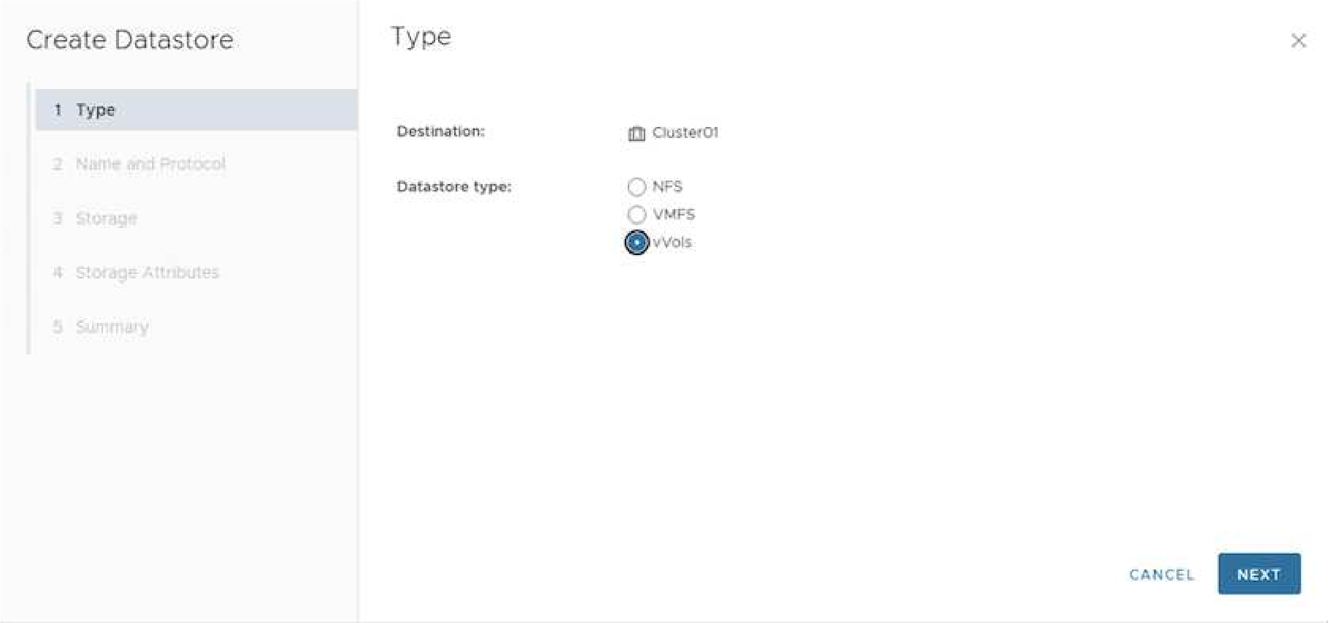
/ > rfc4122.5f2a148a-e822-49d5-9126-e500e7267582

Directory name	Used	Modify history
rfc4122.5f2a148a-e822-49d5-9126-e500e7267582	20 KiB	

Name	Size
TME02.vmx	2.14 KiB
.rfc4122.dbf5f75b-b7b8-42d6-a35d-840c649ee835.meta	721 Bytes
TME02_2.vmdk	564 Bytes
TME02-0f972036.hlog	425 Bytes
.rfc4122.dbf5f75b-b7b8-42d6-a35d-840c649ee835.lck	0 Bytes
TME02.vmsd	0 Bytes

With ONTAP tools 10.1

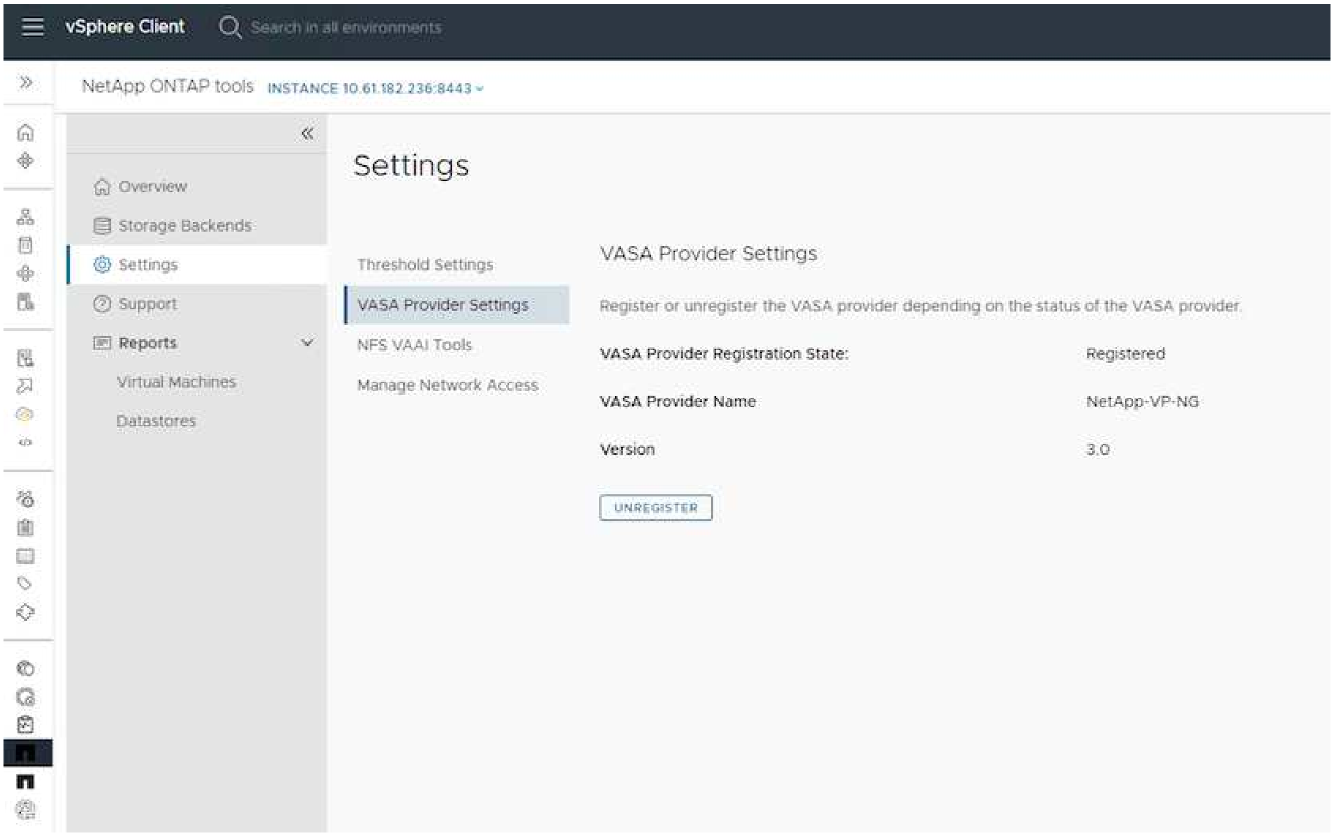
1. Right click on vSphere cluster or host and select Create Datastore (10.1) under NetApp ONTAP tools.
2. Select the datastore type as vVols.



Destination: Cluster01

Datastore type:
○ NFS
○ VMFS
● vVols

If vVols option is not available, ensure the VASA provider is registered.



Settings

VASA Provider Settings

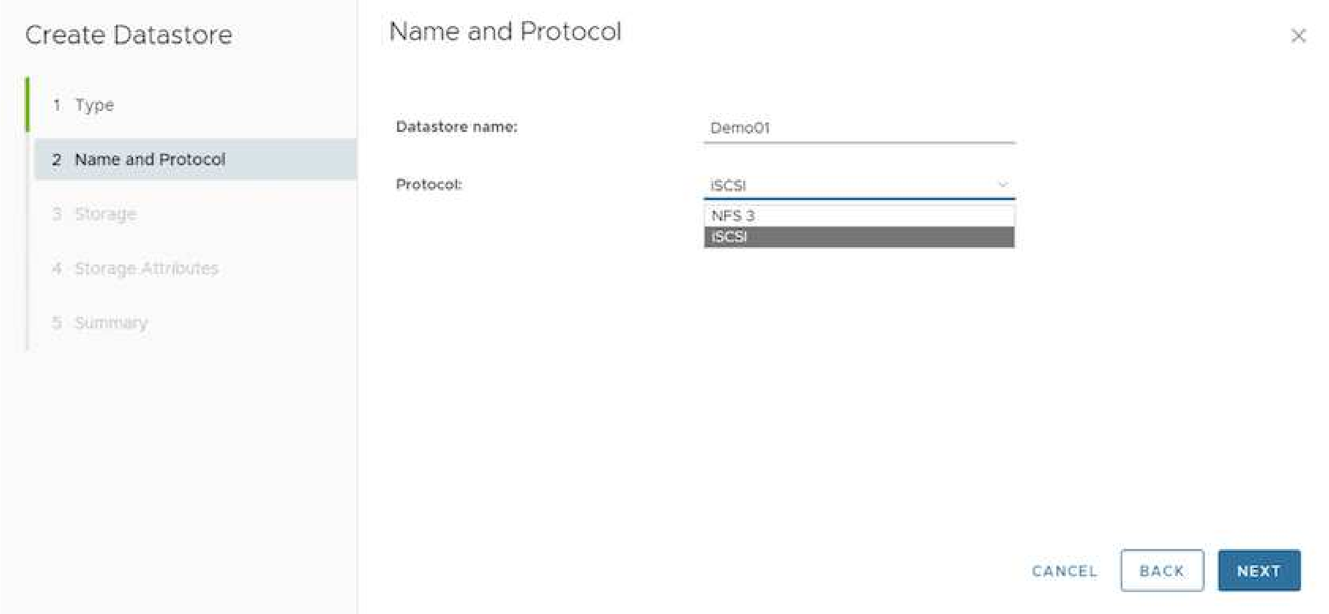
Register or unregister the VASA provider depending on the status of the VASA provider.

VASA Provider Registration State: Registered

VASA Provider Name: NetApp-VP-NG

Version: 3.0

3. Provide the vVol datastore name and select the transport protocol.

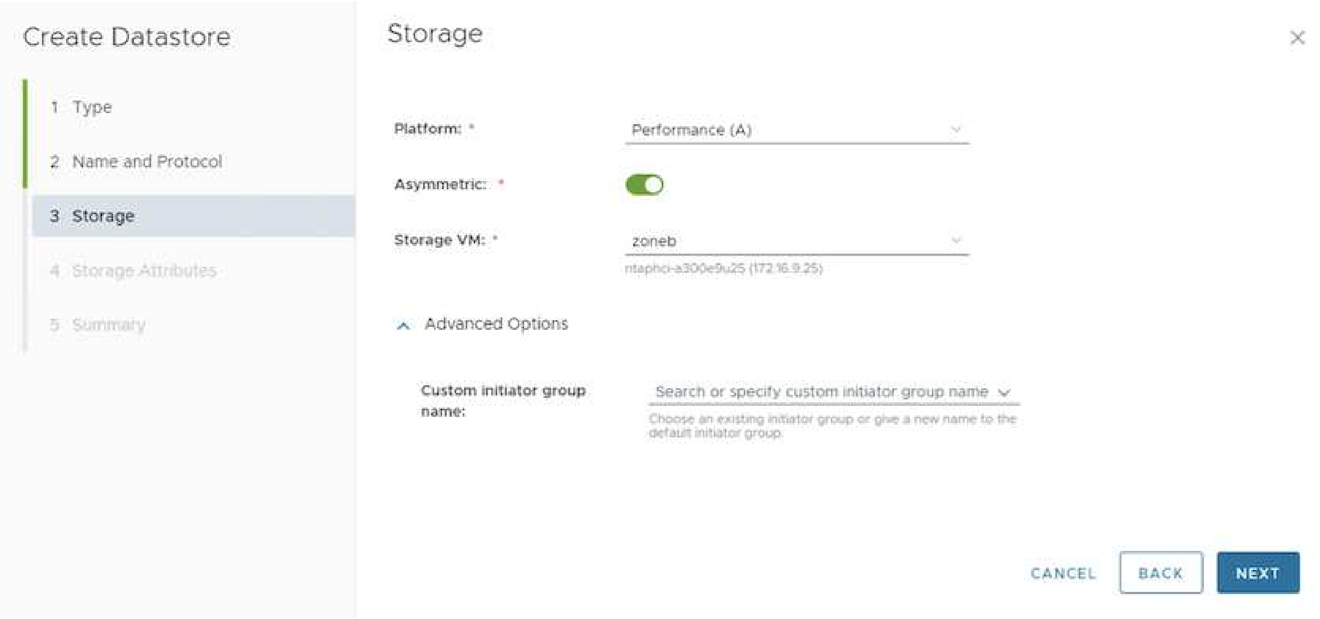


Name and Protocol

Datastore name: Demo01

Protocol: iSCSI

4. Select platform and Storage VM.



Storage

Platform: * Performance (A)

Asymmetric: *

Storage VM: * zoneb

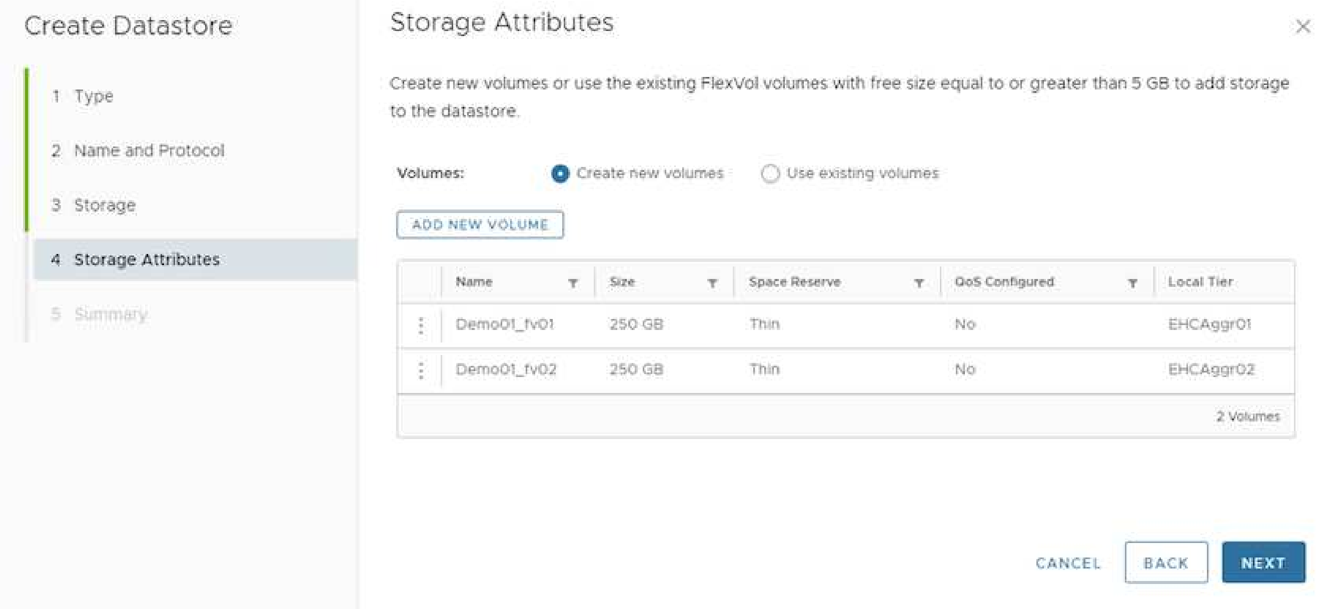
ntaphci-a300e9u25 (172.16.9.25)

Advanced Options

Custom initiator group name: Search or specify custom initiator group name

Choose an existing initiator group or give a new name to the default initiator group.

5. Create or use existing ONTAP volumes for the vVol datastore.



Storage Attributes

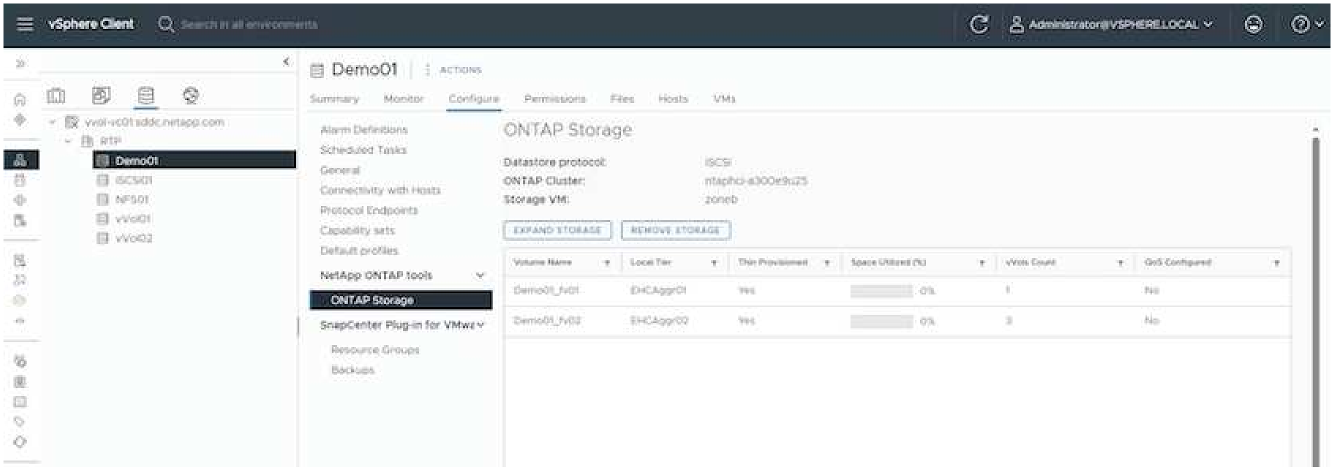
Create new volumes or use the existing FlexVol volumes with free size equal to or greater than 5 GB to add storage to the datastore.

Volumes: ● Create new volumes ○ Use existing volumes

Name	Size	Space Reserve	QoS Configured	Local Tier
Demo01_fv01	250 GB	Thin	No	EHCAggr01
Demo01_fv02	250 GB	Thin	No	EHCAggr02

2 Volumes

ONTAP volumes can be viewed or updated later from the datastore configuration.



Demo01

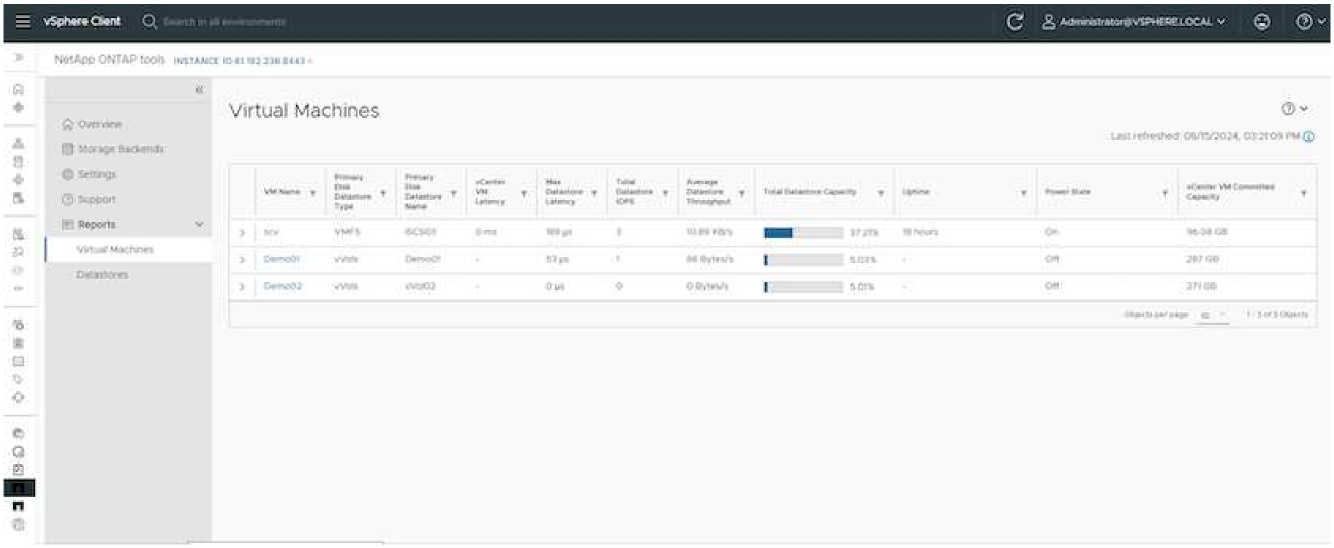
ONTAP Storage

Datastore protocol: iSCSI
ONTAP Cluster: ntaphci-a300e9u25
Storage VM: zoneb

Volume Name	Local Tier	Thin Provisioned	Space Utilized (%)	vVols Count	QoS Configured
Demo01_fv01	EHCAggr01	Yes	0%	1	No
Demo01_fv02	EHCAggr02	Yes	0%	3	No

6. After vVol datastore is provisioned, it can be consumed similar to any other datastore.

7. ONTAP tools provide the VM and Datastore report.

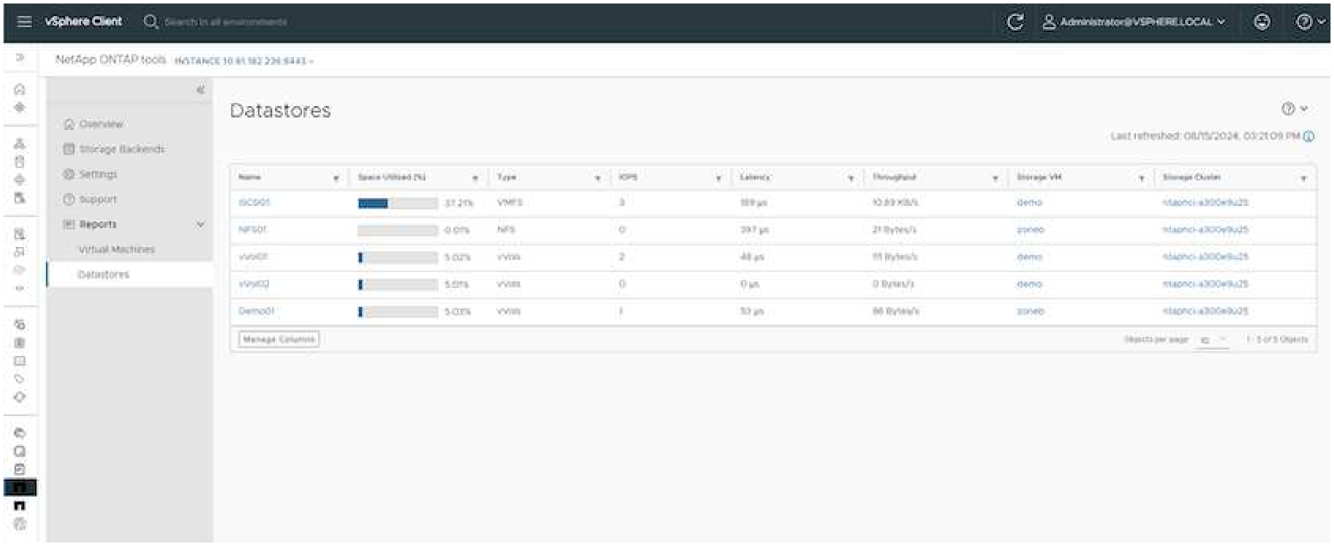

vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
NetApp ONTAP tools INSTANCE 10.61.182.236:8443
Overview
Storage Backends
Settings
Support
Reports
Virtual Machines
Datastores

Virtual Machines

Last refreshed: 08/15/2024, 03:21:09 PM

	VM Name	Primary Disk Datastore Type	Primary Disk Datastore Name	vCenter VM Latency	Max Datastore Latency	Total Datastore IOPS	Average Datastore Throughput	Total Datastore Capacity	Uptime	Power State	vCenter VM Committed Capacity
>	scv	VMFS	iSCSI01	0 ms	189 µs	3	10.89 KB/s	37.21%	19 hours	On	96.08 GB
>	Demo01	vVols	Demo01	-	53 µs	1	86 Bytes/s	5.03%	-	Off	287 GB
>	Demo02	vVols	vVol02	-	0 µs	0	0 Bytes/s	5.01%	-	Off	271 GB

Objects per page 10 1 - 3 of 3 Objects



Datastores

Last refreshed: 08/15/2024, 03:21:09 PM

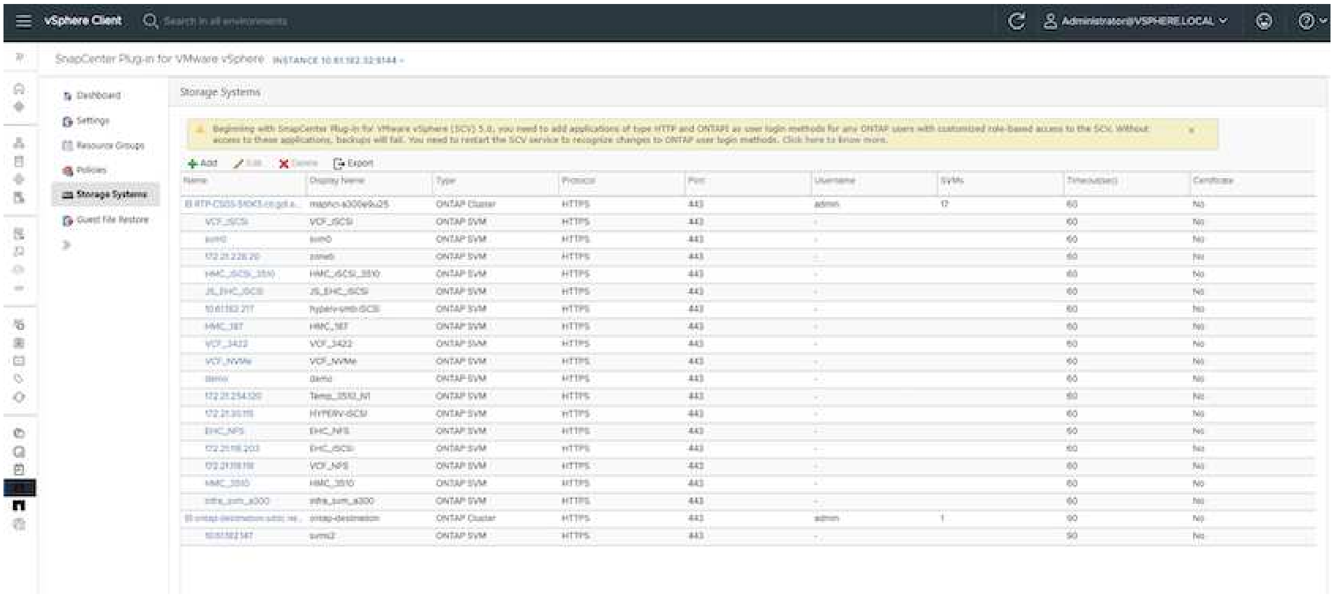
Name	Space Utilized (%)	Type	IOPS	Latency	Throughput	Storage VM	Storage Cluster
iSCSI01	37.21%	VMFS	3	189 µs	10.89 KB/s	demo	ntaphci-a300e9u25
NFS01	0.01%	NFS	0	397 µs	21 Bytes/s	zoneb	ntaphci-a300e9u25
vVol01	5.02%	vVols	2	48 µs	111 Bytes/s	demo	ntaphci-a300e9u25
vVol02	5.01%	vVols	0	0 µs	0 Bytes/s	demo	ntaphci-a300e9u25
Demo01	5.03%	vVols	1	53 µs	86 Bytes/s	zoneb	ntaphci-a300e9u25

Objects per page 10 1 - 5 of 5 Objects

Data Protection of VMs on vVol datastore

Overview of data protection of VMs on vVol datastore can be found at protecting vVols.

1. Register the Storage system hosting the vVol datastore and any replication partners.

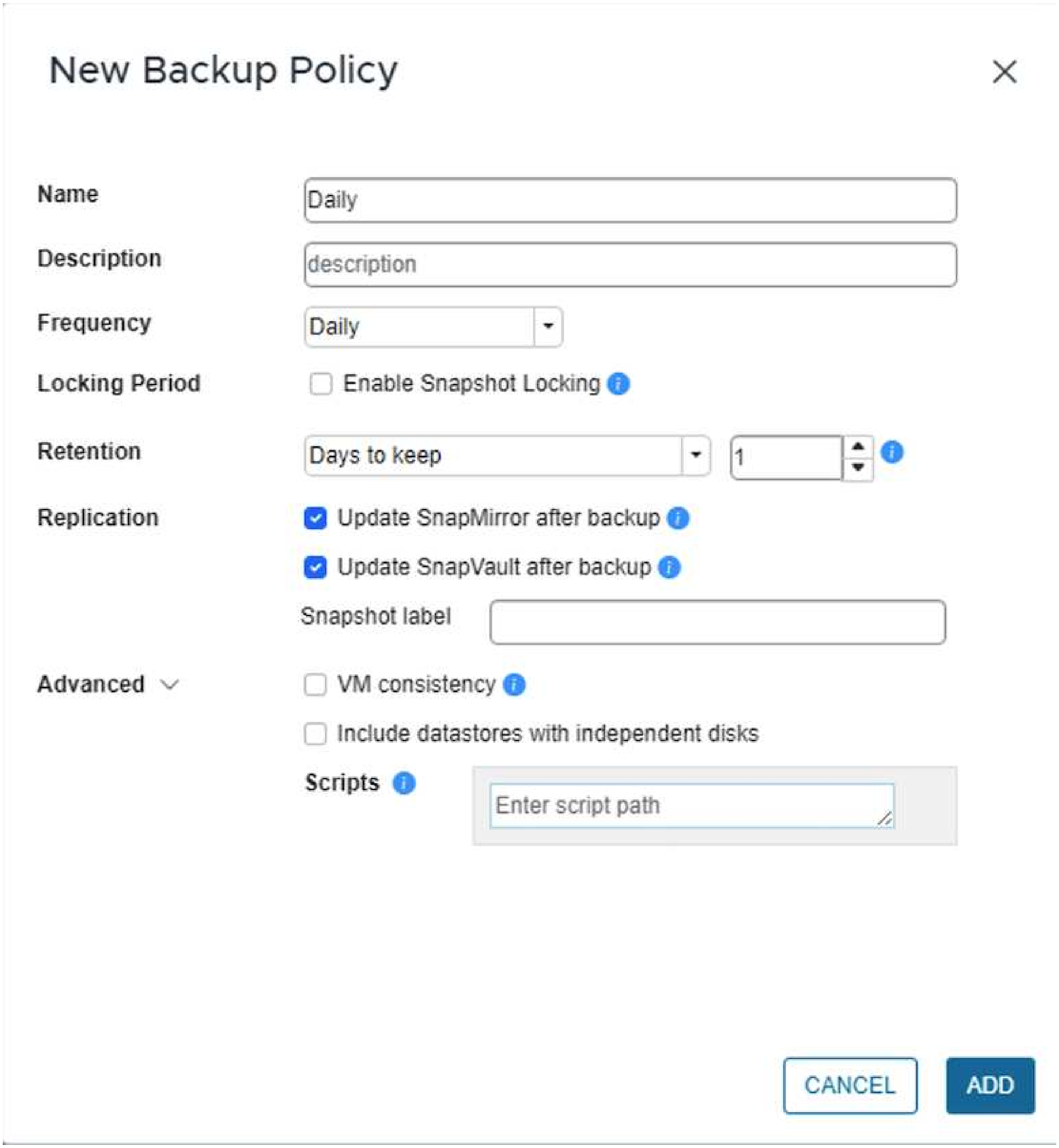

vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
SnapCenter Plug-in for VMware vSphere
INSTANCE 10.61.182.32:8144
Dashboard
Settings
Resource Groups
Policies
Storage Systems
Guest File Restore
Add
Edit
Delete
Export

Storage Systems

Beginning with SnapCenter Plug-in for VMware vSphere (SCV) 5.0, you need to add applications of type HTTP and ONTAPI as user login methods for any ONTAP users with customized role-based access to the SCV. Without access to these applications, backups will fail. You need to restart the SCV service to recognize changes to ONTAP user login methods. Click here to know more.

Name	Display Name	Type	Protocol	Port	Username	SVMs	Timeout(sec)	Certificate
RTP-C505-510K3.rtr.gdl.e...	maphci-a300e9u25	ONTAP Cluster	HTTPS	443	admin	17	60	No
VCF_iSCSI	VCF_iSCSI	ONTAP SVM	HTTPS	443	-		60	No
svm0	svm0	ONTAP SVM	HTTPS	443	-		60	No
172.21.228.20	zoneb	ONTAP SVM	HTTPS	443	-		60	No
HMC_iSCSI_3510	HMC_iSCSI_3510	ONTAP SVM	HTTPS	443	-		60	No
JS_EHC_iSCSI	JS_EHC_iSCSI	ONTAP SVM	HTTPS	443	-		60	No
10.61.182.217	hyperv-smb-iSCSI	ONTAP SVM	HTTPS	443	-		60	No
HMC_187	HMC_187	ONTAP SVM	HTTPS	443	-		60	No
VCF_3422	VCF_3422	ONTAP SVM	HTTPS	443	-		60	No
VCF_NVMe	VCF_NVMe	ONTAP SVM	HTTPS	443	-		60	No
demo	demo	ONTAP SVM	HTTPS	443	-		60	No
172.21.254.120	Temp_3510_N1	ONTAP SVM	HTTPS	443	-		60	No
172.21.20.115	HYPERV-iSCSI	ONTAP SVM	HTTPS	443	-		60	No
EHC_NFS	EHC_NFS	ONTAP SVM	HTTPS	443	-		60	No
172.21.118.203	EHC_iSCSI	ONTAP SVM	HTTPS	443	-		60	No
172.21.118.118	VCF_NFS	ONTAP SVM	HTTPS	443	-		60	No
HMC_3510	HMC_3510	ONTAP SVM	HTTPS	443	-		60	No
infra_svm_a300	infra_svm_a300	ONTAP SVM	HTTPS	443	-		60	No
ontap-destination.sddc.ne...	ontap-destination	ONTAP Cluster	HTTPS	443	admin	1	90	No
10.61.182.147	svm2	ONTAP SVM	HTTPS	443	-		90	No

2. Create a policy with required attributes.



New Backup Policy

Name: Daily

Description: description

Frequency: Daily

Locking Period: □ Enable Snapshot Locking

Retention: Days to keep 1

Replication: ☑ Update SnapMirror after backup

☑ Update SnapVault after backup

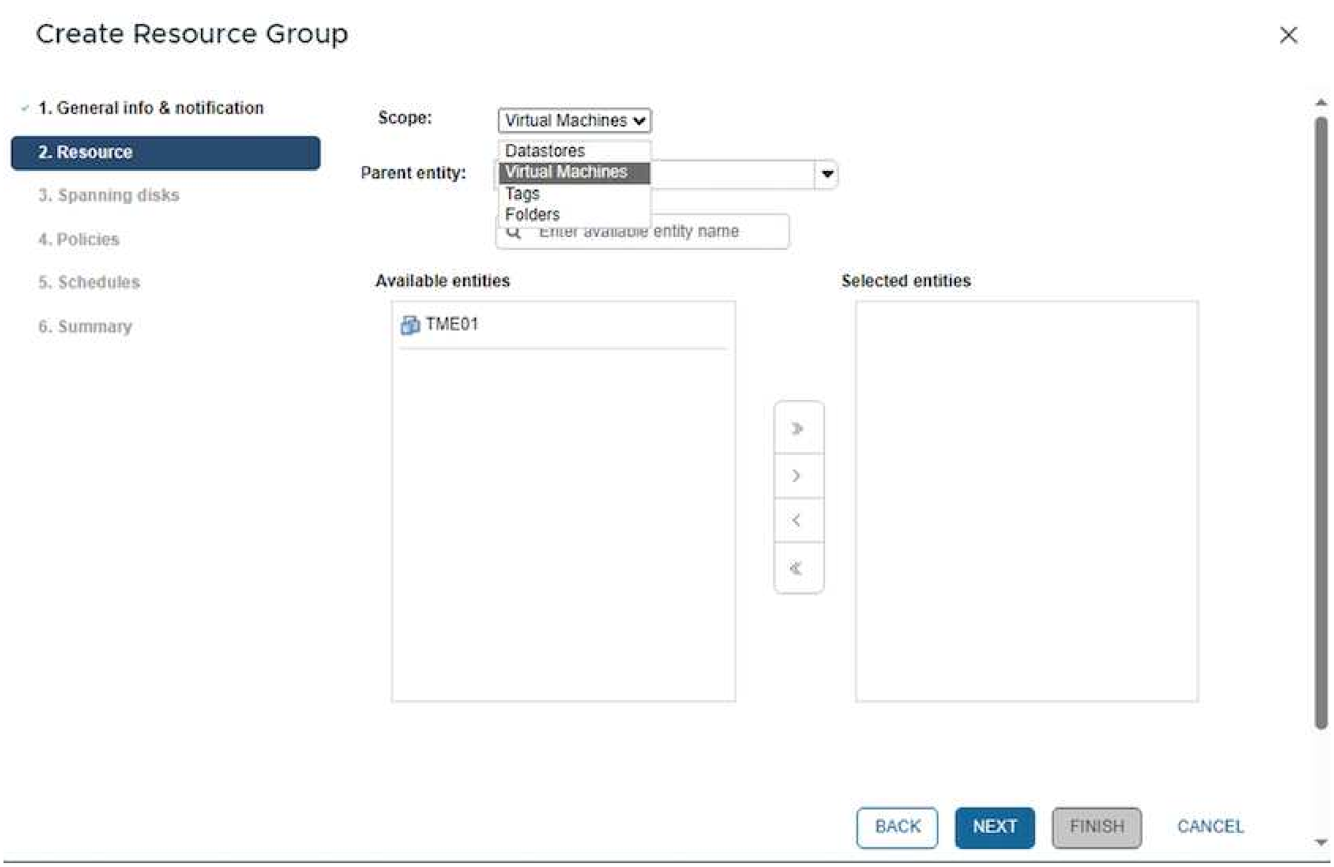
Snapshot label:

Advanced: □ VM consistency

□ Include datastores with independent disks

Scripts: Enter script path

3. Create a resource group and associate to policy (or Policies.)



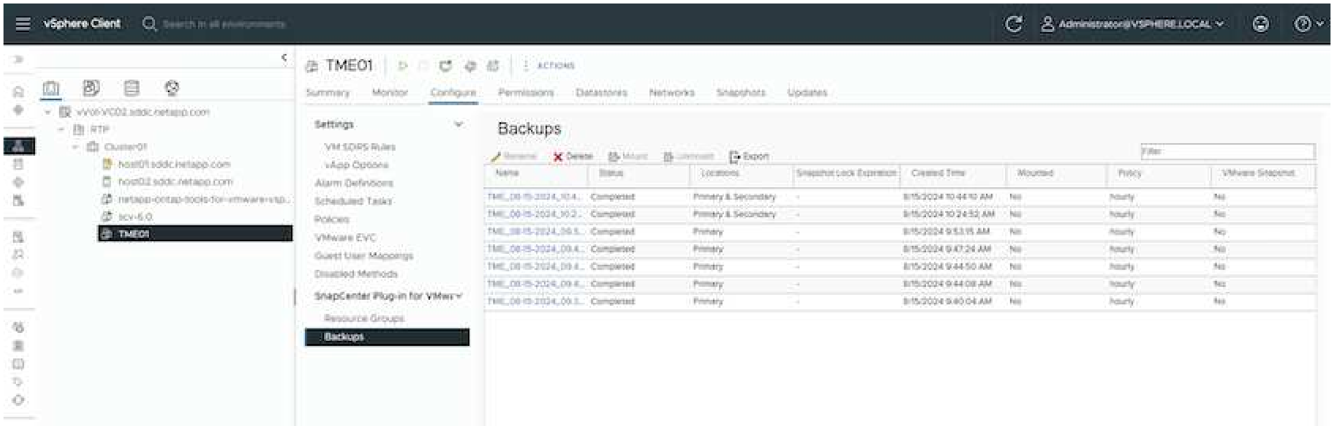
Scope: Virtual Machines

Parent entity:

TME01

NOTE: For vVol datastore, need to protect with VM, tag or folder. vVol datastore can't be included in the resource group.

4. Specific VM backup status can be viewed from its configure tab.



TME01

Backups

Name	Status	Locations	Snapshot Lock Expiration	Created Time	Mounted	Policy	VMware Snapshot
TME_08-15-2024_10.4...	Completed	Primary & Secondary	-	8/15/2024 10:44:10 AM	No	hourly	No
TME_08-15-2024_10.2...	Completed	Primary & Secondary	-	8/15/2024 10:24:52 AM	No	hourly	No
TME_08-15-2024_09.5...	Completed	Primary	-	8/15/2024 9:53:15 AM	No	hourly	No
TME_08-15-2024_09.4...	Completed	Primary	-	8/15/2024 9:47:24 AM	No	hourly	No
TME_08-15-2024_09.4...	Completed	Primary	-	8/15/2024 9:44:50 AM	No	hourly	No
TME_08-15-2024_09.4...	Completed	Primary	-	8/15/2024 9:44:08 AM	No	hourly	No
TME_08-15-2024_09.3...	Completed	Primary	-	8/15/2024 9:40:04 AM	No	hourly	No

5. VM can be restored from its primary or secondary location.

Refer SnapCenter plug-in documentation for additional use cases.

VM migration from traditional datastores to vVol datastore

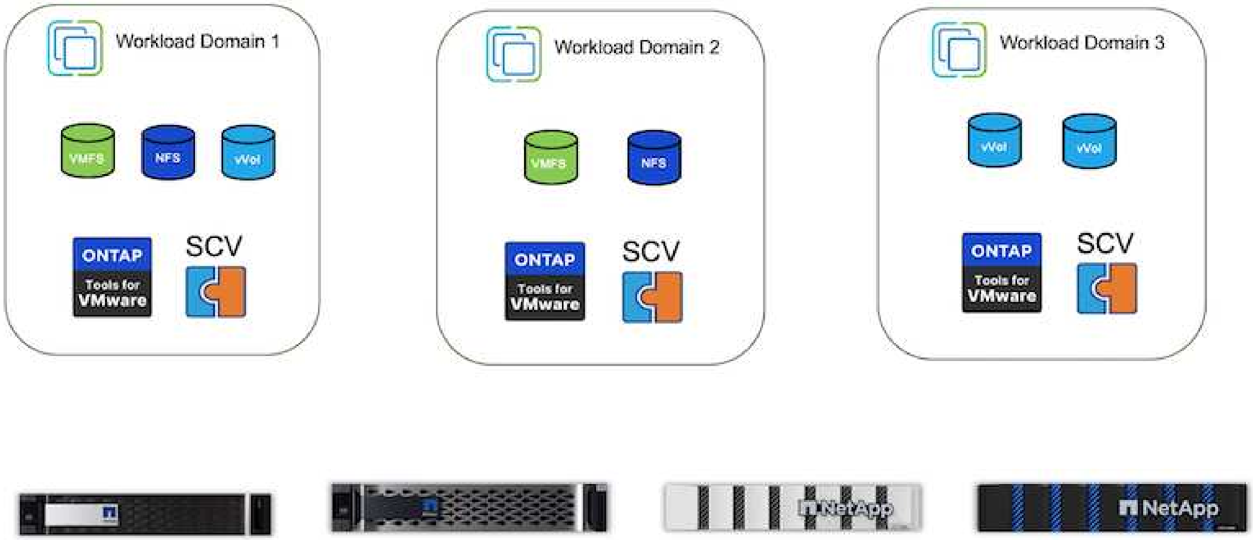
To migrate VMs from other datastores to a vVol datastore, various options are available based on the scenario. It can vary from a simple storage vMotion operation to migration using HCX. Refer migrate vms to ONTAP datastore for more details.

VM migration between vVol datastores

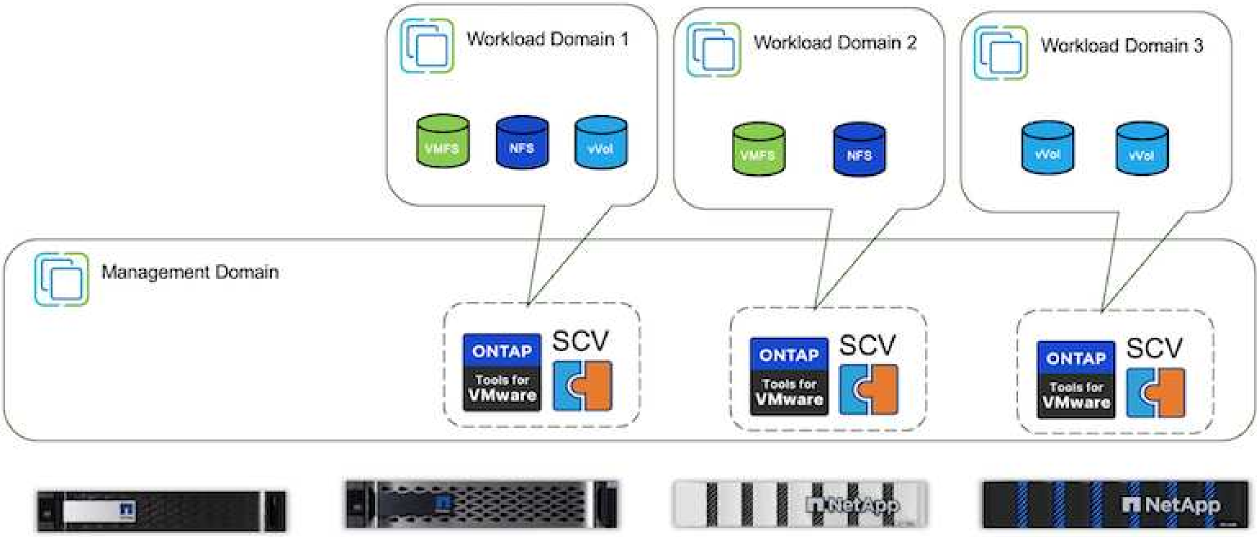
For bulk migration of VMs between vVol datastores, please do check migrate vms to ONTAP datastore.

Sample Reference architecture

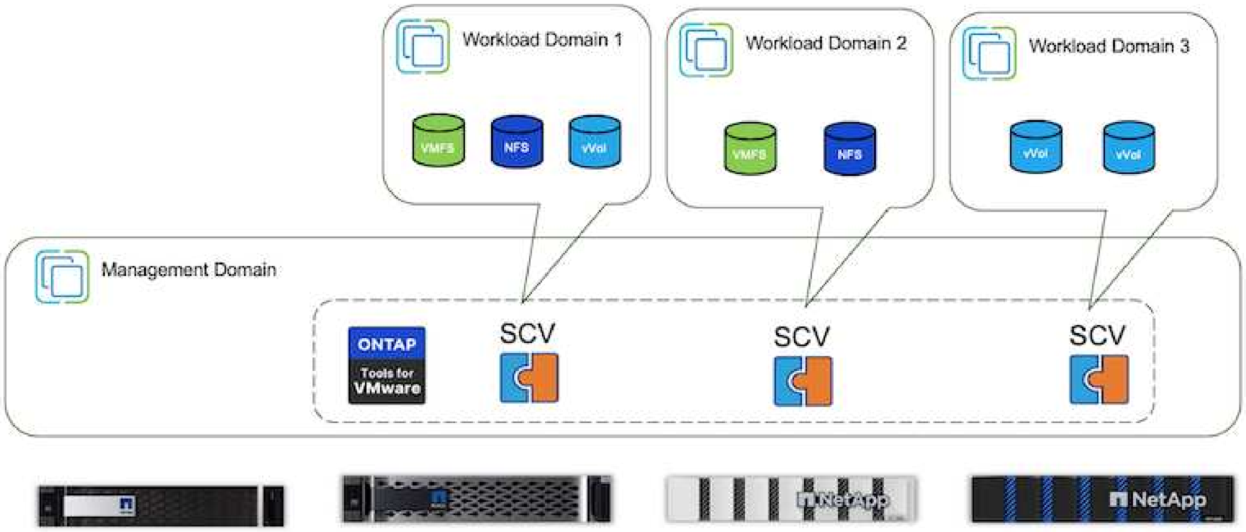
ONTAP tools for VMware vSphere and SCV can be installed on same vCenter it is managing or on different vCenter server. It is better to avoid to host on vVol datastore it is managing.



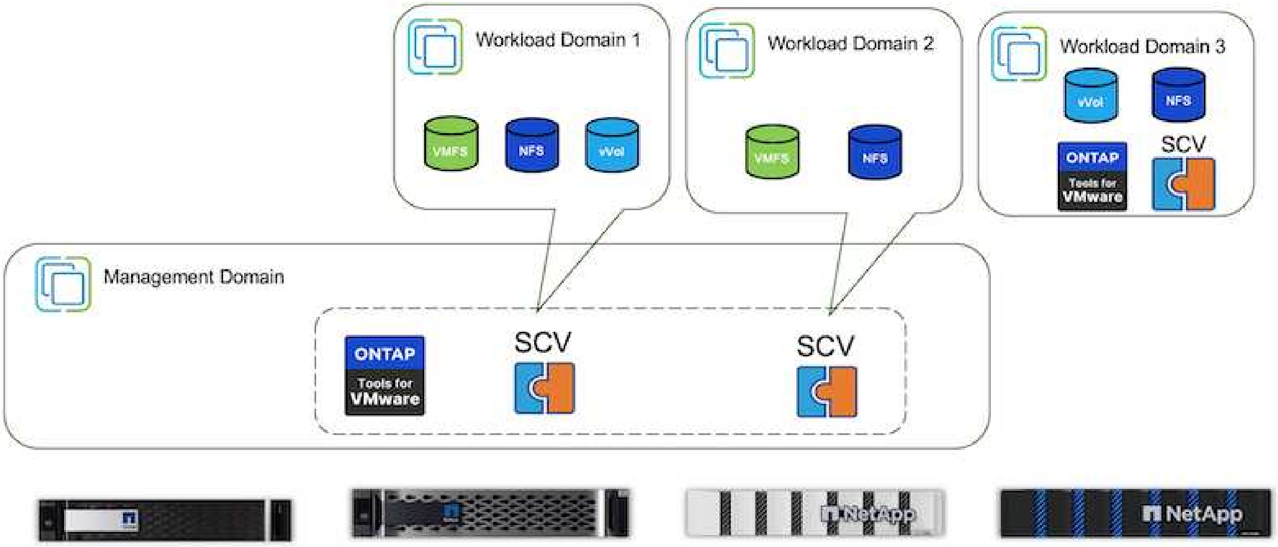
As many customers host their vCenter servers on different one rather than it is managing, similar approach is adviced for ONTAP tools & SCV too.



With ONTAP tools 10.x, a single instance can manage multiple vCenter environments. The storage systems are registered globally with cluster credentials and SVMs are assigned to each tenant vCenter servers.



Mix of dedicated and shared model is also supported.



How to get started

If ONTAP tools is not installed on your environment, please download from NetApp Support Site and follow the instructions available at using vVols with ONTAP.

Deployment Guide for VMFS

NetApp's storage solutions and offerings empower customers to fully capitalize on the advantages of a virtualized infrastructure. With NetApp solutions, customers can efficiently implement comprehensive data management software ensuring automation, efficiency, data protection and security capabilities to effectively meet demanding performance requirements. Combining ONTAP software with VMware vSphere allows to reduce host hardware and VMware licensing expenses, make sure data is protected at lower cost, and provide consistent high performance.

Introduction

Virtualized workloads are mobile. Therefore, administrators use VMware Storage vMotion to move VMs across VMware Virtual Machine File System (VMFS), NFS, or vVols datastores, all residing on the same storage system and thus explore different storage approaches if using an All-Flash System or use the latest ASA models with SAN innovation for higher cost efficiency.

The key message here is that migrating to ONTAP improves customer experience and application performance while offering the flexibility to migrate data and applications between FCP, iSCSI, NVMe/FC and NVMe/TCP. For enterprises deeply invested in VMware vSphere, using ONTAP storage is a cost-effective option given the current market conditions, one that presents a unique opportunity. Enterprises today face new imperatives that a modern SAN approach can address simply and quickly. Here are some of the ways existing and new NetApp customers are adding value with ONTAP.

- Cost efficiency - Integrated storage efficiency allows ONTAP to significantly reduce storage costs. NetApp ASA systems can run all storage efficiency capabilities in production with no performance impact. NetApp makes it simple to plan for these efficiency benefits with the most effective guarantee available.
- Data Protection - SnapCenter software using snapshots provides advanced VM and application-level data protection for various enterprise applications deployed in a VM configuration.
- Security - Use Snapshot copies to protect against malware and ransomware. Enhance protection by making Snapshot copies immutable using Snapshot locking and NetApp SnapLock® software.
- Cloud - ONTAP provides a wide range of hybrid cloud options that enable enterprises to combine public and private clouds, offering flexibility and reducing infrastructure management overhead. Supplemental datastore support based on ONTAP offerings allow for the use of VMware Cloud on Azure, AWS and Google for TCO optimized deployment, data protection, and business continuity while avoiding vendor lock-in.
- Flexibility - ONTAP is well-equipped to meet the rapidly changing needs of modern organizations. With ONTAP One, all these capabilities come standard with an ONTAP system at no extra cost.

Rightsize and optimize

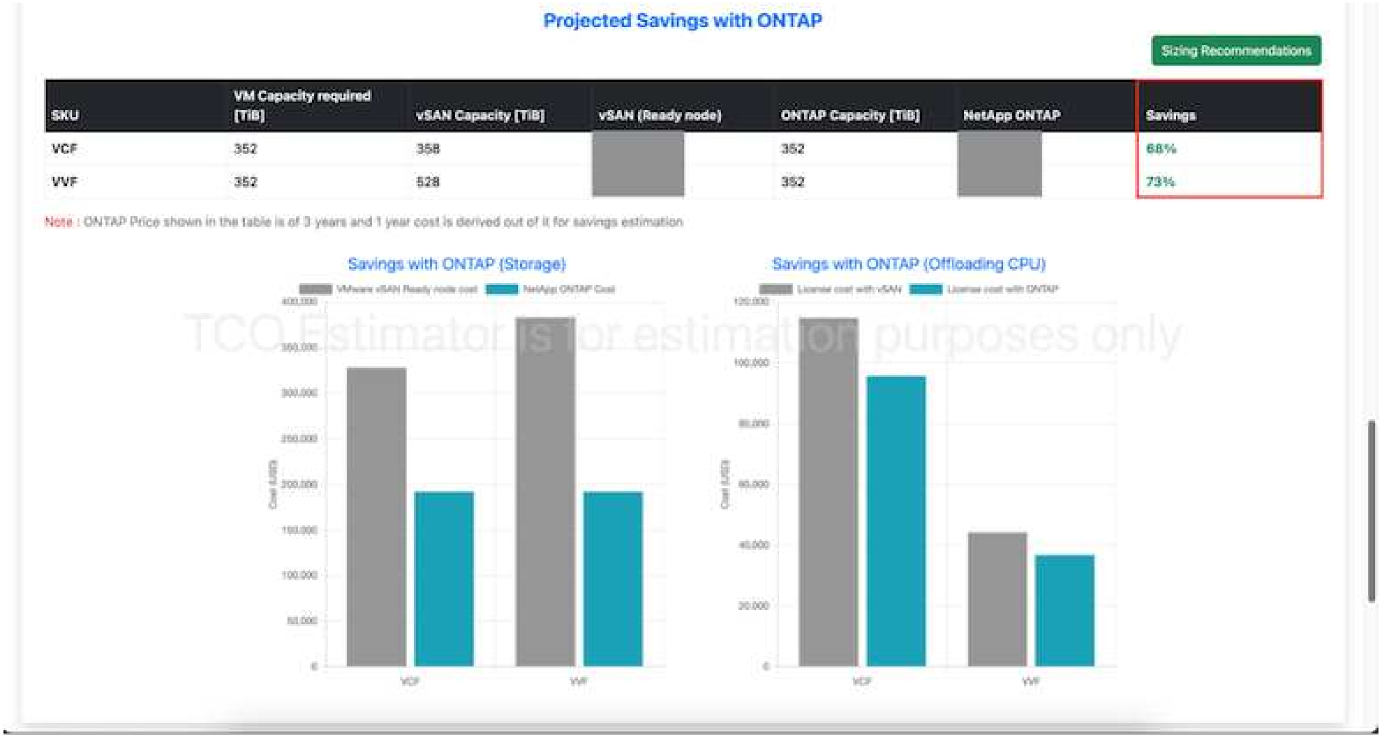
With impending licensing changes, organizations are proactively addressing the potential increase in Total Cost of Ownership (TCO). They are strategically optimizing their VMware infrastructure through aggressive resource management and right-sizing to enhance resource utilization and streamline capacity planning. Through the effective use of specialized tools, organizations can efficiently identify and reclaim wasted resources, subsequently reducing core counts and overall licensing expenses. It’s important to highlight that many organizations are already integrating these practices into their cloud assessments, demonstrating how these processes and tools effectively mitigate cost concerns in on-premises environments and eliminate unnecessary migration expenses to alternative hypervisors.

TCO Estimator

NetApp has created a simple TCO estimator which would act as the stepping stone in starting this optimisation journey. The TCO estimator uses RVtools or manual input methods to easily project how many hosts are required for the given deployment and calculate the savings to optimize the deployment using NetApp ONTAP storage systems. Keep in mind, this is the stepping stone.

> ⓘ The TCO estimator is only accessible to NetApp field teams and partners. Work with NetApp account teams to assess your existing environment.

Here is a screenshot from the TCO estimator.



Projected Savings with ONTAP

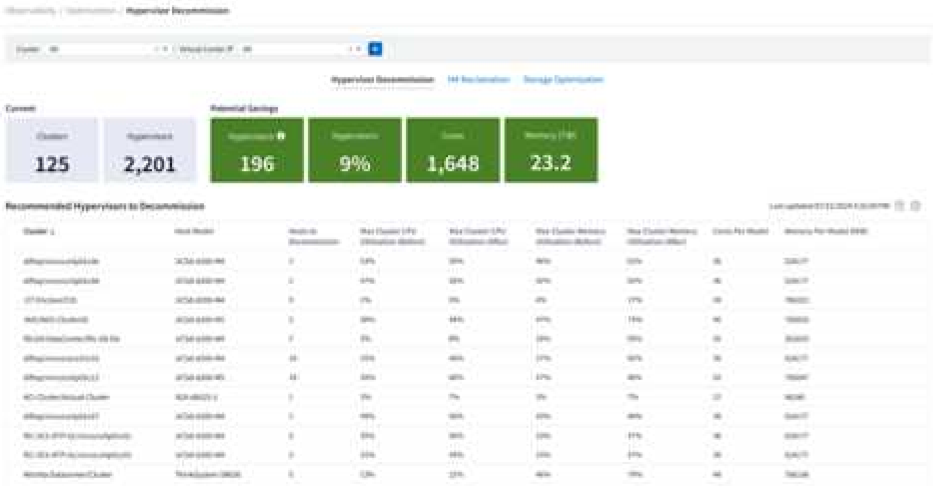
SKU	VM Capacity required [TiB]	vSAN Capacity [TiB]	vSAN (Ready node)	ONTAP Capacity [TiB]	NetApp ONTAP	Savings
VCF	352	358	[redacted]	352	[redacted]	68%
VVF	352	528	[redacted]	352	[redacted]	73%

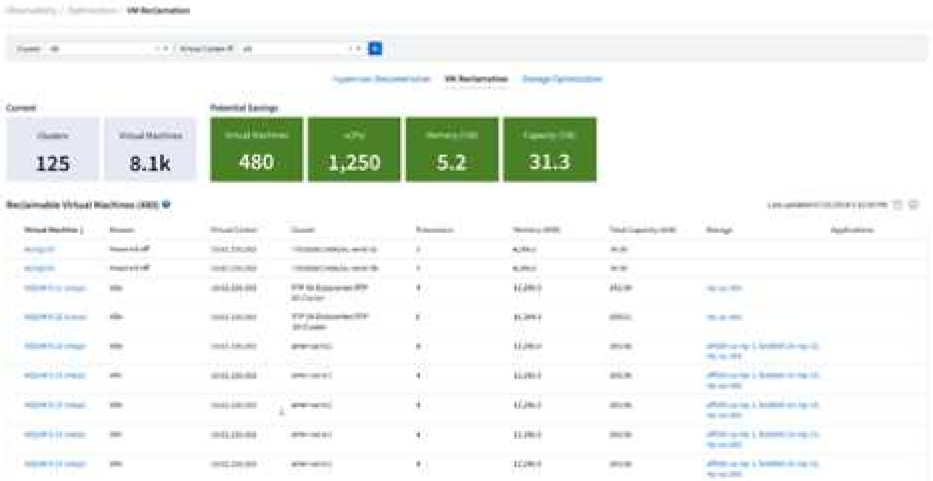
Note : ONTAP Price shown in the table is of 3 years and 1 year cost is derived out of it for savings estimation

Cloud Insights

Once the estimator shows the savings possible (which will be the case for any given organisation), then it's time to dive deep into analysing the workload IO profiles across virtual machines using real-time metrics. For this, NetApp provides Cloud Insights. By providing detailed analysis and recommendations for VM reclamation, Cloud Insights can help businesses make informed decisions about optimizing their VM environment. It can identify where resources can be reclaimed or hosts decommissioned with minimal impact on production, helping businesses navigate the changes brought about by Broadcom's acquisition of VMware in a thoughtful, strategic manner. In other words, Cloud Insight help businesses take the emotion out of the decision. Instead of reacting to the changes with panic or frustration, they can use the insights provided by Cloud Insights tool to make rational, strategic decisions that balance cost optimization with operational efficiency and productivity.

Below are the screenshots from Cloud Insights.





Conduct regular assessments to pinpoint underutilized resources, increase virtual machine density, and utilization within VMware clusters to control rising costs associated with new subscription licenses. Consider reducing the number of cores per CPU to 16 for new server purchases to align with changes in VMware licensing models.

With NetApp, right-size your virtualized environments and introduce cost-effective flash storage performance along with simplified data management and ransomware solutions to ensure organisations are prepared for new subscription model while optimizing the IT resources that are currently in place.

NetApp ONTAP Tools for VMware vSphere

To further enhance and simplify VMware integration, NetApp offers several offtap tools that can be used with NetApp ONTAP and VMware vSphere to efficiently manage virtualized environments. This section will focus on the ONTAP tools for VMware. ONTAP tools for VMware vSphere 10 provide a comprehensive set of tools for virtual machine lifecycle management, simplifying storage management, enhancing efficiency features, improving availability, and reducing storage costs and operational overhead. These tools seamlessly integrate with the VMware ecosystem, facilitating datastore provisioning and offering basic protection for virtual machines. The 10.x release of ONTAP tools for VMware vSphere comprises horizontally scalable, event-driven microservices deployed as an Open Virtual Appliance (OVA), following best practices for provisioning datastores and optimizing ESXi host settings for both block and NFS storage environments. Considering these benefits, OTV is recommended as a best practice to use with systems running ONTAP software.

Getting Started

Before deploying and configuring ONTAP tools for VMware, ensure the pre-requisites are met. Once done, deploy a single node configuration.

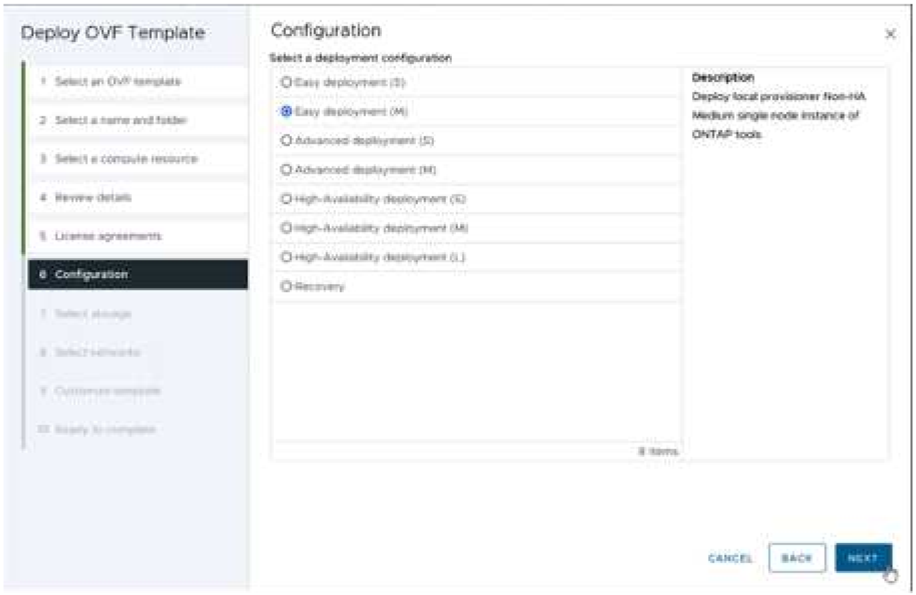
Three IP addresses are required for deployment - one IP address for load balancer, one IP address for the Kubernetes control plane and one for the node.

Steps

1. Log in to the vSphere server.
2. Navigate to the cluster or the host where you want to deploy the OVA.
3. Right-click the required location and select Deploy OVF template.
    a. Enter the URL for the .ova file or browse to the folder where the .ova file is saved, and then select Next.

4. Select a name, folder, cluster / host for the virtual machine and select Next.
5. In the Configuration window, select Easy deployment(S), Easy deployment(M), or Advanced deployment(S) or Advanced deployment(M) configuration.

> The easy deployment option is used in this walkthrough.



Configuration

Select a deployment configuration

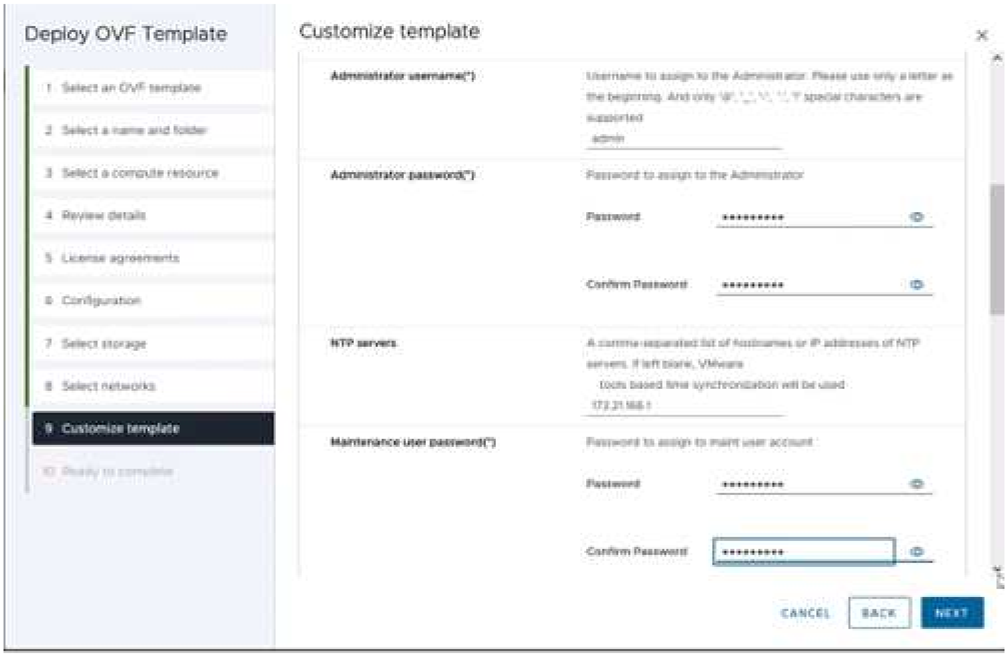
- ○ Easy deployment (S)
- ● Easy deployment (M)
- ○ Advanced deployment (S)
- ○ Advanced deployment (M)
- ○ High-Availability deployment (S)
- ○ High-Availability deployment (M)
- ○ High-Availability deployment (L)
- ○ Recovery

8 items

Description

Deploy local provisioner Non-HA Medium single node instance of ONTAP tools

6. Choose the datastore to deploy the OVA and the source and destination network. Once done, select Next.
7. It’s time to customize template > system configuration window.



Customize template

Administrator username(*)

Username to assign to the Administrator. Please use only a letter as the beginning. And only '@', '_', '-', '.', '!' special characters are supported

admin

Administrator password(*)

Password to assign to the Administrator

Password ••••••••••

Confirm Password ••••••••••

NTP servers

A comma-separated list of hostnames or IP addresses of NTP servers. If left blank, VMware tools based time synchronization will be used

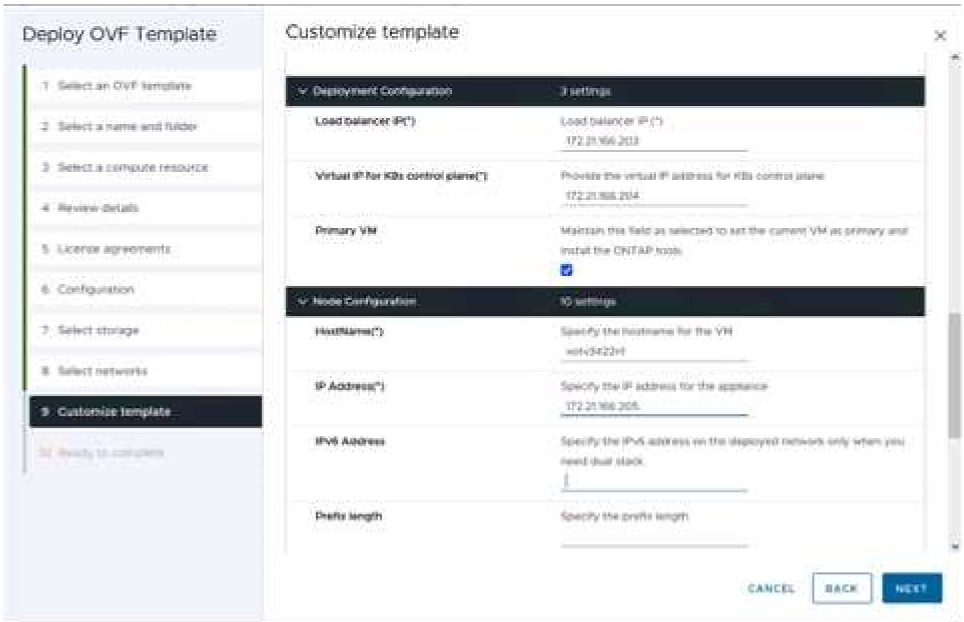
172.21.166.1

Maintenance user password(*)

Password to assign to maint user account

Password ••••••••••

Confirm Password ••••••••••



Customize template

∨ Deployment Configuration — 3 settings

Load balancer IP(*) — Load balancer IP (*): 172.21.166.203

Virtual IP for K8s control plane(*) — Provide the virtual IP address for K8s control plane: 172.21.166.204

Primary VM — Maintain this field as selected to set the current VM as primary and install the ONTAP tools. ☑

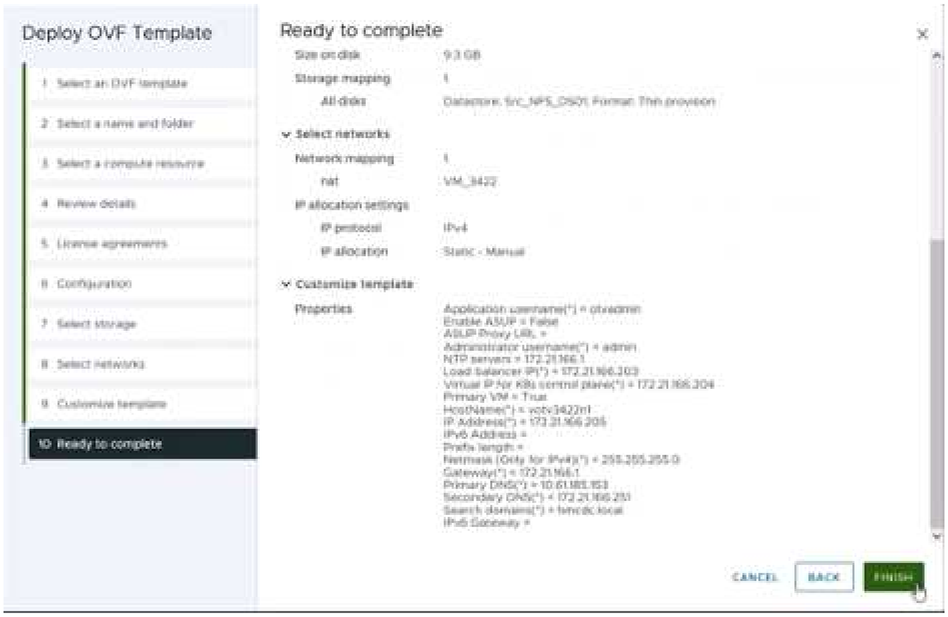
∨ Node Configuration — 10 settings

HostName(*) — Specify the hostname for the VM: votv3422n1

IP Address(*) — Specify the IP address for the appliance: 172.21.166.205

IPv6 Address — Specify the IPv6 address on the deployed network only when you need dual stack.

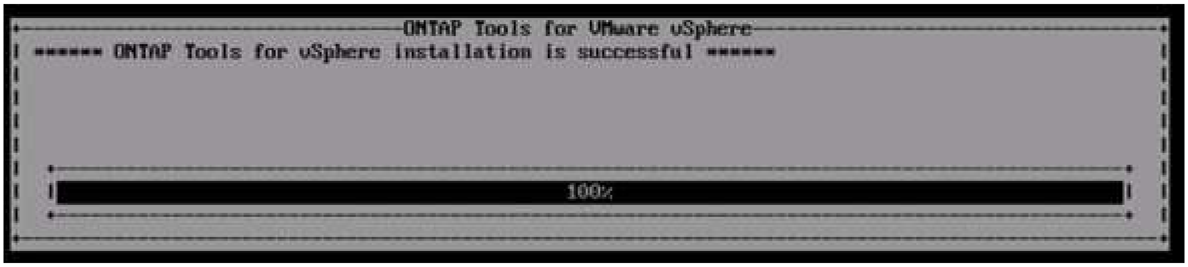
Prefix length — Specify the prefix length

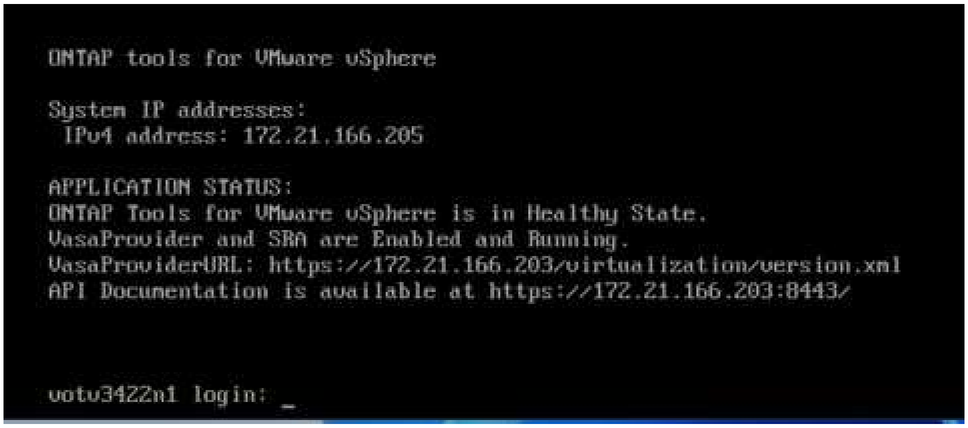


Ready to complete

Size on disk	9.3 GB
Storage mapping	1
All disks	Datastore: Src_NFS_DS01; Format: Thin provision
∨ Select networks	
Network mapping	1
nat	VM_3422
IP allocation settings	
IP protocol	IPv4
IP allocation	Static - Manual
∨ Customize template	
Properties	Application username(*) = otvadmin Enable ASUP = False ASUP Proxy URL = Administrator username(*) = admin NTP servers = 172.21.166.1 Load Balancer IP(*) = 172.21.166.203 Virtual IP for K8s control plane(*) = 172.21.166.204 Primary VM = True HostName(*) = votv3422n1 IP Address(*) = 173.21.166.205 IPv6 Address = Prefix length = Netmask (Only for IPv4)(*) = 255.255.255.0 Gateway(*) = 172.21.166.1 Primary DNS(*) = 10.61.185.153 Secondary DNS(*) = 172.21.166.251 Search domains(*) = hmcdc.local IPv6 Gateway =

After successful installation, the web console shows the state of ONTAP tools for VMware vSphere.


```
+-----------------------ONTAP Tools for VMware vSphere-----------------------+
| ****** ONTAP Tools for vSphere installation is successful ******           |
|                                                                            |
|    +-------------------------------------------------------------------+   |
|    |                               100%                                |   |
|    +-------------------------------------------------------------------+   |
+----------------------------------------------------------------------------+
```

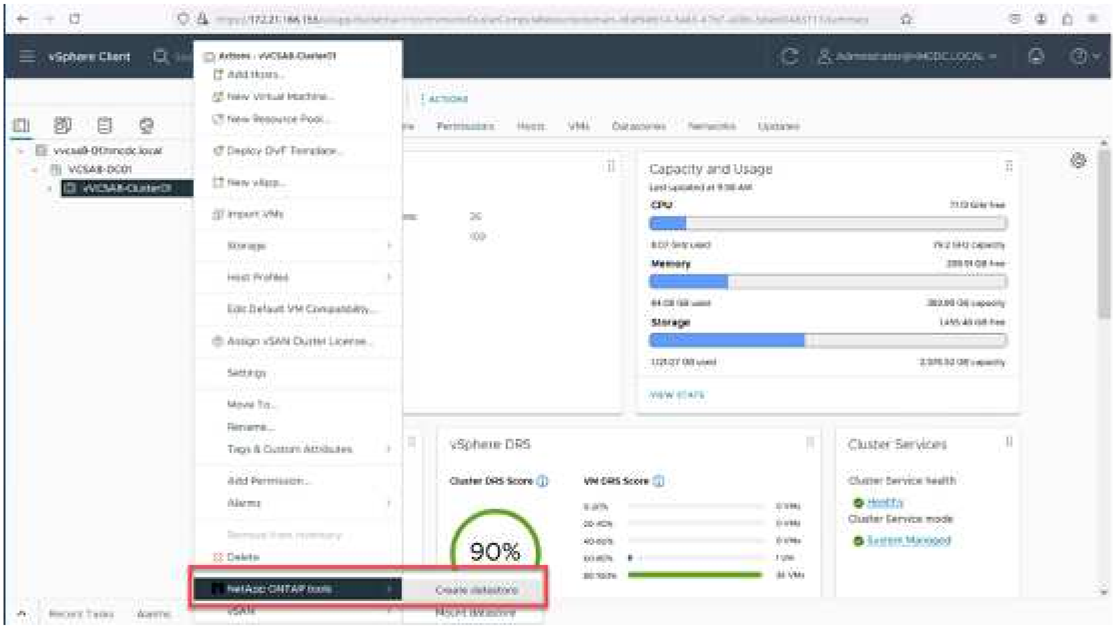


```
ONTAP tools for VMware vSphere

System IP addresses:
 IPv4 address: 172.21.166.205

APPLICATION STATUS:
ONTAP Tools for VMware vSphere is in Healthy State.
VasaProvider and SRA are Enabled and Running.
VasaProviderURL: https://172.21.166.203/virtualization/version.xml
API Documentation is available at https://172.21.166.203:8443/


votv3422n1 login: _
```

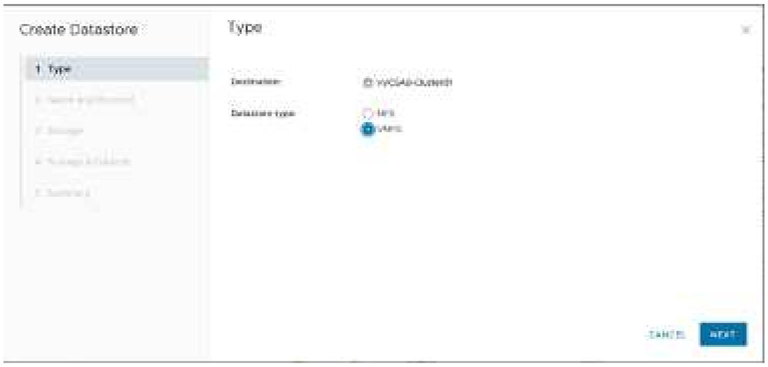
The datastore creation wizard supports provisioning of VMFS, NFS and vVols datastores.

It’s time to provision ISCSI based VMFS datastores for this walkthrough.

1. Log in to the vSphere client using https://vcenterip/ui
2. Right-click a Host or a Host Cluster or a Datastore, and then select NetApp ONTAP tools > Create Datastore.



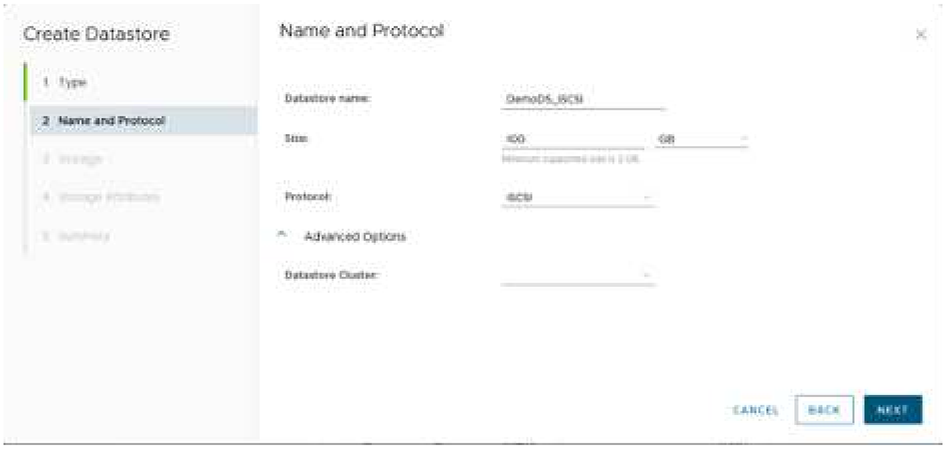
3. In the Type pane, select VMFS in Datastore Type.



Destination: vVCSA8-Cluster01

Datastore type: ○ NFS ● VMFS

4. In the Name and Protocol pane, enter the datastore name, size, and protocol information. In the Advanced options section of the pane, select the Datastore cluster if you want to add this datastore to.



Name and Protocol

Datastore name: DemoDS_iSCSI

Size: 100 GB

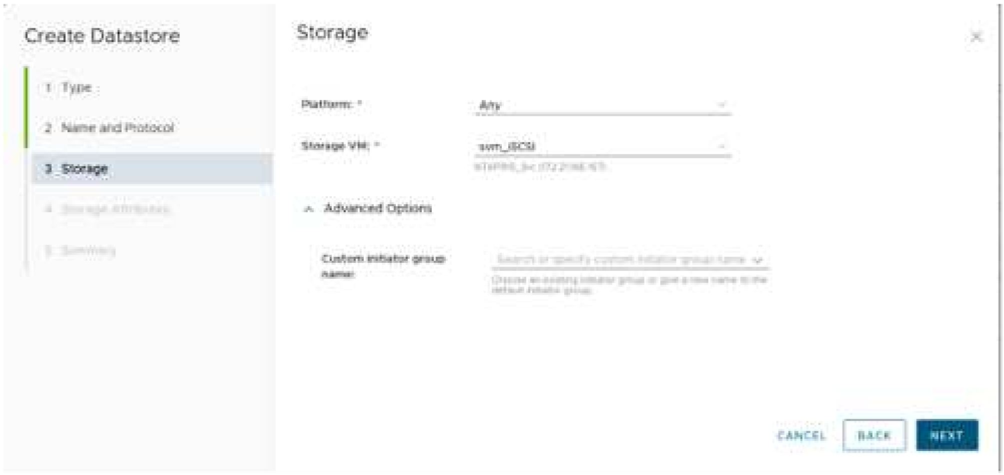
Minimum supported size is 1 GB

Protocol: iSCSI

Advanced Options

Datastore Cluster:

5. Select Platform and storage VM in the Storage pane. Provide the Custom initiator group name in the Advanced options section of the pane (optional). You can either choose an existing igroup for the datastore or create a new igroup with a custom name.



Storage

Platform: * Any

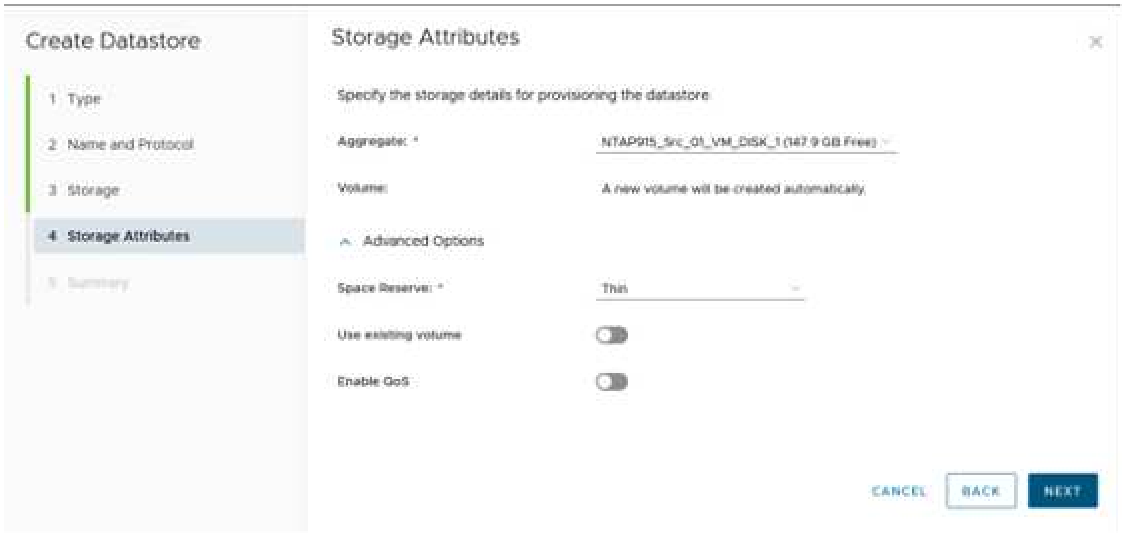
Storage VM: * svm_iSCSI

Advanced Options

Custom initiator group name: Search or specify custom initiator group name

Choose an existing initiator group or give a new name to the default initiator group.

6. From the storage attributes pane, select Aggregate from the drop-down menu. Select Space Reserve, volume option, and Enable QoS options as required from the Advanced options section.



Storage Attributes

Specify the storage details for provisioning the datastore

Aggregate: * NTAP915_Src_01_VM_DISK_1 (147.9 GB Free)

Volume: A new volume will be created automatically.

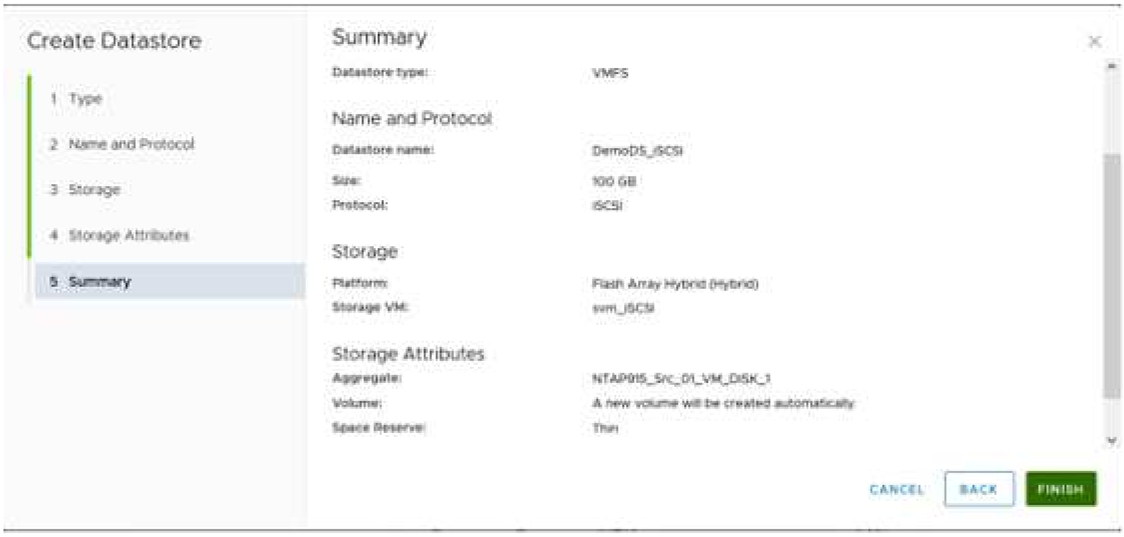
Advanced Options

Space Reserve: * Thin

Use existing volume

Enable QoS

7. Review the datastore details in the Summary pane and click Finish. The VMFS datastore is created and mounted on all the hosts.



Summary

Datastore type: VMFS

Name and Protocol

Datastore name: DemoDS_iSCSI
Size: 100 GB
Protocol: iSCSI

Storage

Platform: Flash Array Hybrid (Hybrid)
Storage VM: svm_iSCSI

Storage Attributes

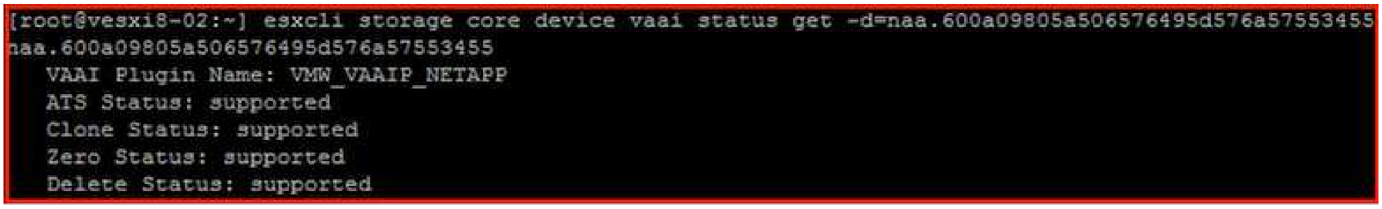
Aggregate: NTAP915_Src_01_VM_DISK_1
Volume: A new volume will be created automatically
Space Reserve: Thin

Refer to these links for vVol, FC, NVMe/TCP datastore provisioning.

VAAI Offloading

VAAI primitives are used in routine vSphere operations such as creating, cloning, migrating, starting, and stopping VMs. These operations can be executed through the vSphere client for simplicity or from the command line for scripting or to get more accurate timing. VAAI for SAN is natively supported by ESX. VAAI is always enabled on supported NetApp storage systems and provides native support for the following VAAI operations on SAN storage:

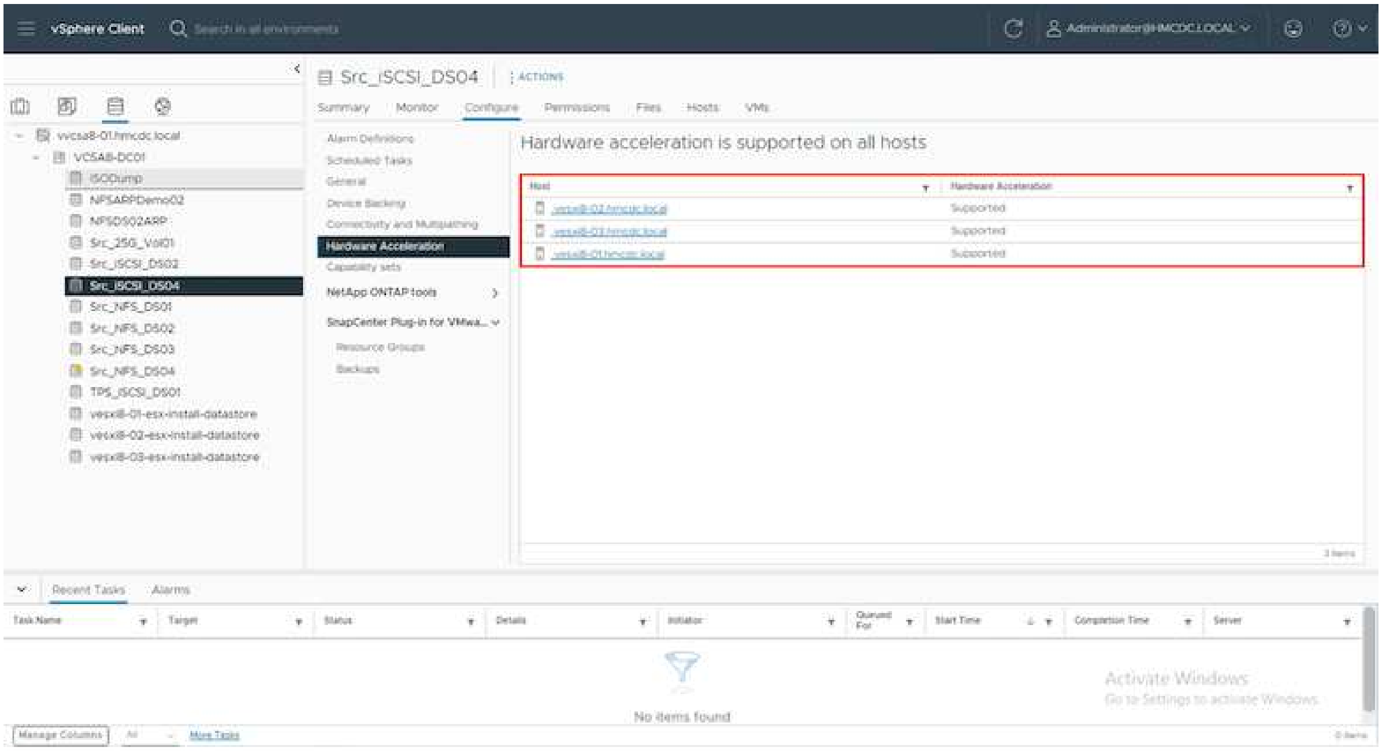
- Copy offload
- Atomic Test & Set (ATS) locking
- Write Same
- Out-of-space condition handling
- Space reclamation



```
[root@vesxi8-02:~] esxcli storage core device vaai status get -d=naa.600a09805a506576495d576a57553455
naa.600a09805a506576495d576a57553455
   VAAI Plugin Name: VMW_VAAIP_NETAPP
   ATS Status: supported
   Clone Status: supported
   Zero Status: supported
   Delete Status: supported
```

ⓘ Ensure that HardwareAcceleratedMove is enabled via the ESX advanced configuration options.

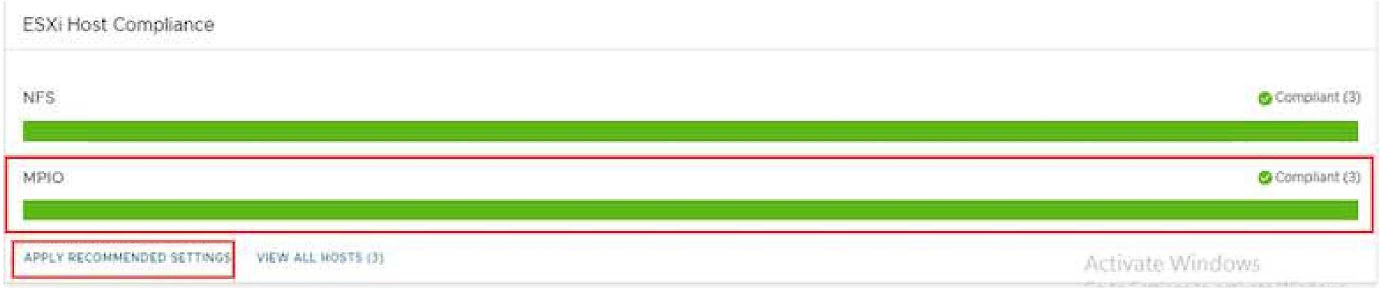
ⓘ Ensure that the LUN has "space-allocation" enabled. If not enabled, enable the option and rescan all HBAs.



Hardware acceleration is supported on all hosts

Host	Hardware Acceleration
vesxi8-02.hmcdc.local	Supported
vesxi8-03.hmcdc.local	Supported
vesxi8-01.hmcdc.local	Supported

> These values are easily set using ONTAP tools for VMware vSphere. From the Overview dashboard, go to ESXi Host compliance card and Select Apply Recommended Settings option. In the Apply recommended host settings window, select the hosts and click Next to apply NetApp recommended host settings.

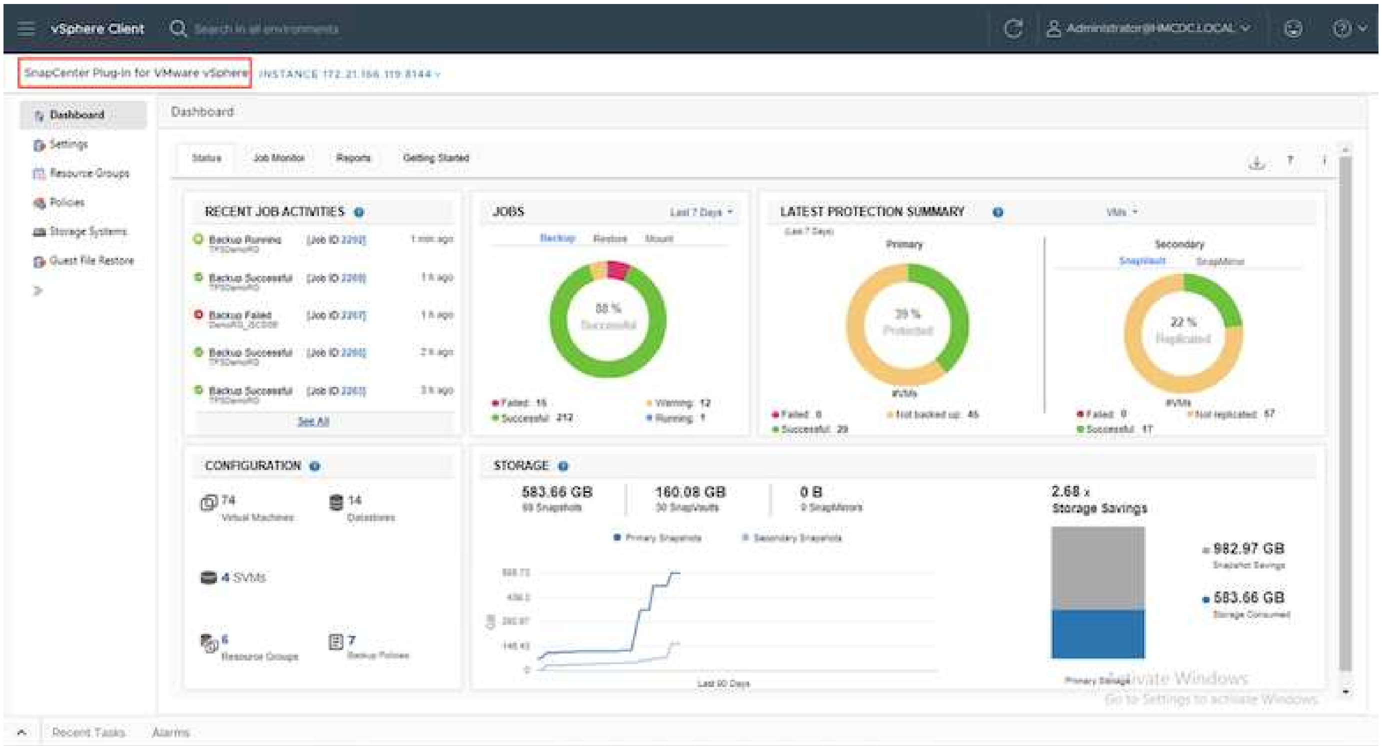

ESXi Host Compliance

NFS	Compliant (3)
MPIO	Compliant (3)

View detailed guidance for Recommended ESXi host and other ONTAP settings.

Data Protection

Efficiently backing up VMs on VMFS datastore and rapidly recovering them are amongst the key advantages of ONTAP for vSphere. By integrating with vCenter, NetApp SnapCenter® software offers a wide range of backup and recovery features for VMs. It provides fast, space-efficient, crash-consistent, and VM-consistent backup and restore operations for VMs, Datastores, and VMDKs. It also works with SnapCenter Server to support application-based backup and restore operations in VMware environments using SnapCenter application-specific plug-ins. Leveraging Snapshot copies allows to make quick copies of the VM or datastore without any impact on performance and use NetApp SnapMirror® or NetApp SnapVault® technology for long-term, off-site data protection.



The workflow is simple. Add primary storage systems and SVMs (and Secondary if SnapMirror/SnapVault is required).

High level steps for deployment and configuration:

1. Download SnapCenter for VMware Plug-in OVA
2. Log in with the vSphere Client credentials
3. Deploy OVF Template to start the VMware deploy wizard and complete the installation
4. To access the plug-in, select SnapCenter Plug-in for VMware vSphere from the Menu
5. Add Storage
6. Create backup policies
7. Create resource groups
8. Backup resource groups
9. Restore Entire virtual machine or particular virtual disk

Setting up SnapCenter Plug-in for VMware for VMs

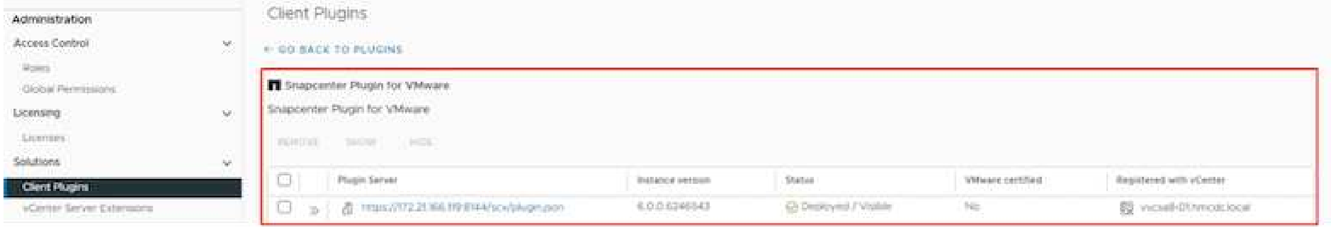
To protect VMs and iSCSI datastores hosting them, SnapCenter Plug-in for VMware must be deployed. It’s a simple OVF import.

The steps to deploy is as follows:

1. Download the Open Virtual Appliance (OVA) from NetApp Support Site.
2. Log in to the vCenter.
3. Within vCenter, right-click any inventory object such as a data center, folder, cluster, or host and select Deploy OVF template.
4. Select the right settings including storage, network and customise the template to update the vCenter and

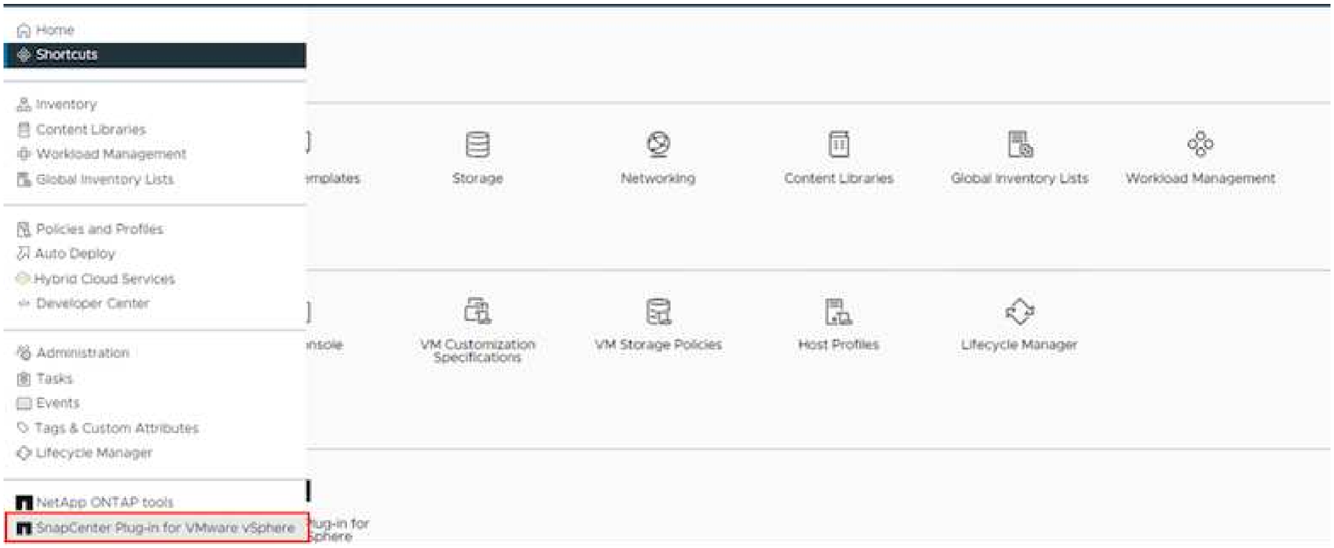
its credentials. Once reviewed, click Finish.

5. Wait for the OVF import and deployment tasks to complete.
6. Once SnapCenter Plug-in for VMware is successfully deployed, it will be registered within vCenter. The same can be verified by accessing Administration > Client Plugins



	Plugin Server	Instance version	Status	VMware certified	Registered with vCenter
□	https://172.21.166.119:8144/scv/plugin.json	6.0.0.6246543	Deployed / Visible	No	vxcsa8-01.nmcdc.local

7. To access the plug-in, navigation to the left sidecar of the vCenter web client page, select SnapCenter Plug-in for VMware.



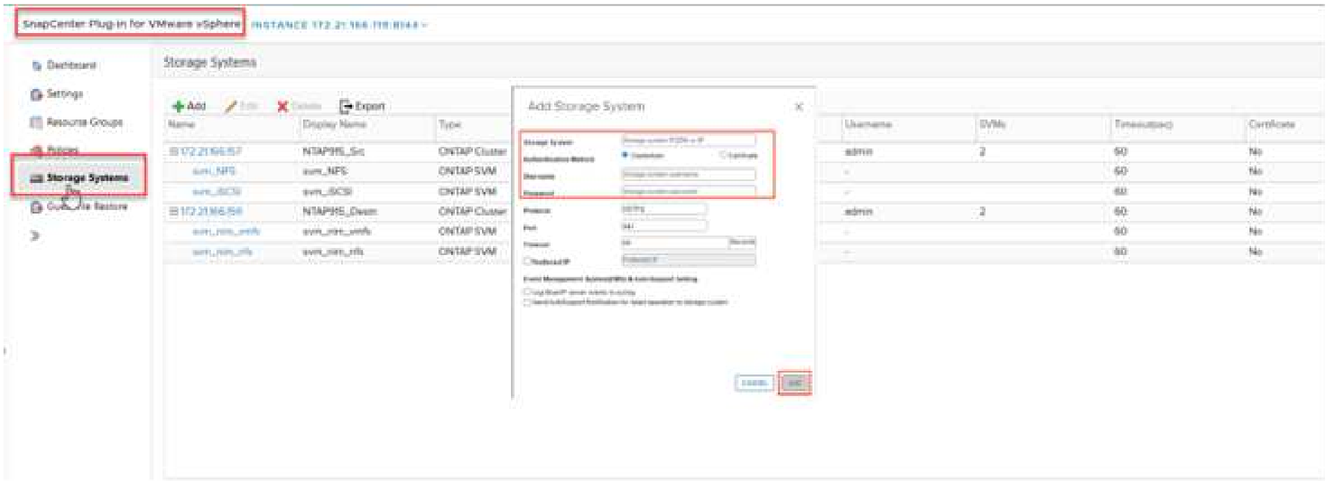
Add storage, create policy and resource group

Adding storage system

Next step is to add the storage system. Cluster management endpoint or Storage virtual machine (SVM) administration endpoint IP should be added as a storage system to backup or restore VMs. Adding storage enables SnapCenter Plug-in for VMware to recognize and manage backup and restore operations in vCenter.

The process is straight forward.

1. From the left navigation, select SnapCenter Plug-in for VMware.
2. Select Storage Systems.
3. Select Add to add the “storage” details.
4. Use Credentials as the Authentication method and enter the username & its password and then click Add to save the settings.



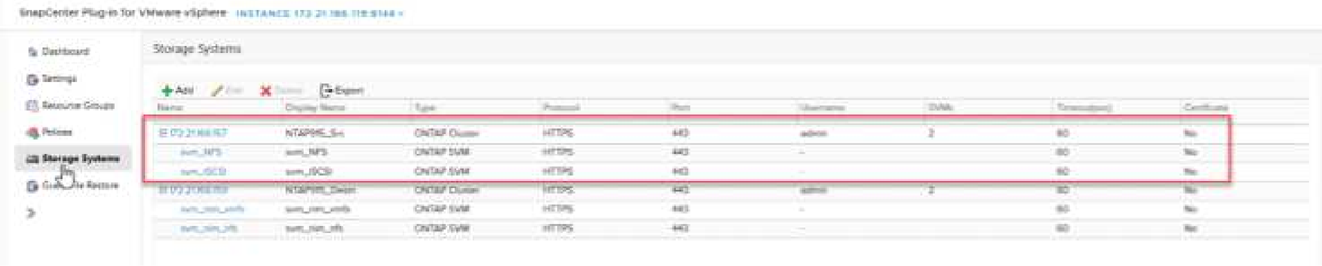
SnapCenter Plug-in for VMware vSphere INSTANCE 172.21.166.119:8144

Storage Systems

Name	Display Name	Type	Username	SVMs	Timeout(sec)	Certificate
⊟ 172.21.166.157	NTAP915_Src	ONTAP Cluster	admin	2	60	No
svm_NFS	svm_NFS	ONTAP SVM	-		60	No
svm_iSCSI	svm_iSCSI	ONTAP SVM	-		60	No
⊟ 172.21.166.158	NTAP915_Destn	ONTAP Cluster	admin	2	60	No
svm_nim_vmfs	svm_nim_vmfs	ONTAP SVM	-		60	No
svm_nim_nfs	svm_nim_nfs	ONTAP SVM	-		60	No

Add Storage System

Storage System: Storage system FQDN or IP
Authentication Method: ● Credentials ○ Certificate
Username: Storage system username
Password: Storage system password
Protocol: HTTPS
Port: 443
Timeout: 60 Seconds
□ Preferred IP: Preferred IP
Event Management System(EMS) & AutoSupport Setting
□ Log SnapCenter server events to syslog
□ Send AutoSupport Notification for failed operation to storage system



SnapCenter Plug-in for VMware vSphere INSTANCE 172.21.166.119:8144

Storage Systems

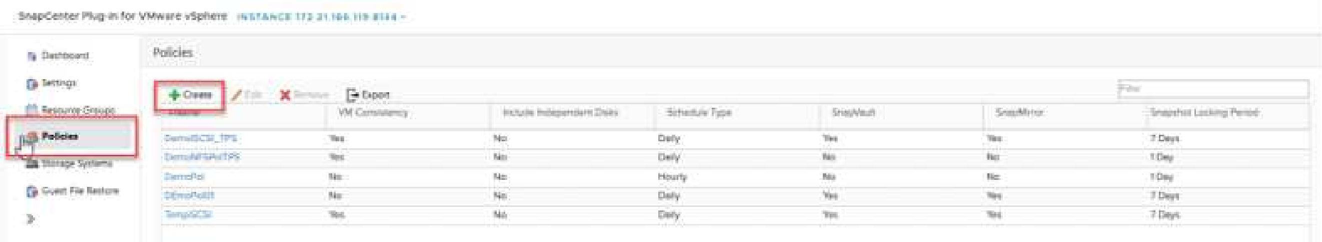
Name	Display Name	Type	Protocol	Port	Username	SVMs	Timeout(sec)	Certificate
⊟ 172.21.166.157	NTAP915_Src	ONTAP Cluster	HTTPS	443	admin	2	60	No
svm_NFS	svm_NFS	ONTAP SVM	HTTPS	443	-		60	No
svm_iSCSI	svm_iSCSI	ONTAP SVM	HTTPS	443	-		60	No
⊟ 172.21.166.158	NTAP915_Destn	ONTAP Cluster	HTTPS	443	admin	2	60	No
svm_nim_vmfs	svm_nim_vmfs	ONTAP SVM	HTTPS	443	-		60	No
svm_nim_nfs	svm_nim_nfs	ONTAP SVM	HTTPS	443	-		60	No

Create backup policy

A comprehensive backup strategy includes factors like when, what to back up and how long to keep backups. Snapshots can be trigged on an hourly or daily basis to back up entire datastores. This approach not only captures the datastores but also enables to back up and restore the VMs and VMDKs within those data stores.

Before backing up the VMs and datastores, a backup policy and resource group must be created. A backup policy includes settings such as the schedule and retention policy. Follow the below steps to create a backup policy.

1. In the left Navigator pane of SnapCenter Plug-in for VMware, click Policies.
2. On the Policies page, click Create to start the wizard.



SnapCenter Plug-in for VMware vSphere INSTANCE 172.21.166.119:8144

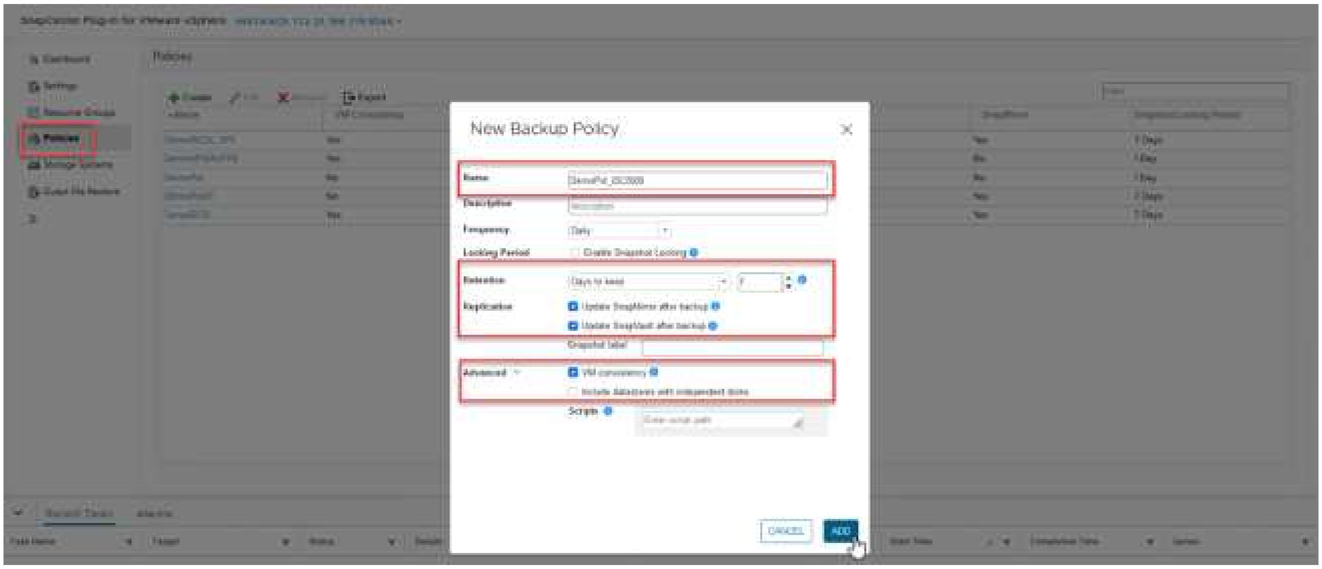
Policies

Name	VM Consistency	Include Independent Disks	Schedule Type	SnapVault	SnapMirror	Snapshot Locking Period
DemoiSCSI_TPS	Yes	No	Daily	Yes	Yes	7 Days
DemoNFSPolTPS	Yes	No	Daily	No	No	1 Day
DemoPol	No	No	Hourly	No	No	1 Day
DEmoPol01	No	No	Daily	Yes	Yes	7 Days
TempiSCSI	Yes	No	Daily	Yes	Yes	7 Days

3. On the New Backup Policy page, enter the policy name.
4. Specify the retention, frequency settings and replication.

> To replicate Snapshot copies to a mirror or vault secondary storage system, the relationships must be configured beforehand.

To enable VM-consistent backups, VMware tools must be installed and running. When VM consistency box is checked, the VMs are first quiesced, then VMware performs a VM consistent snapshot (excluding memory), and then SnapCenter Plug-in for VMware performs its backup operation, and then VM operations are resumed.


New Backup Policy

Name: DemoPol_iSCSI00
Description
Frequency: Daily
Locking Period: ☐ Enable Snapshot Locking
Retention: Days to keep 7
Replication: ☑ Update SnapMirror after backup
☑ Update SnapVault after backup
Snapshot label
Advanced: ☑ VM consistency
☐ Include datastores with independent disks
Scripts: Enter script path

Once the policy is created, next step is to create the resource group which will define the appropriate iSCSI datastores and VMs that should be backed up. After resource group is created, it’s time for triggering backups.

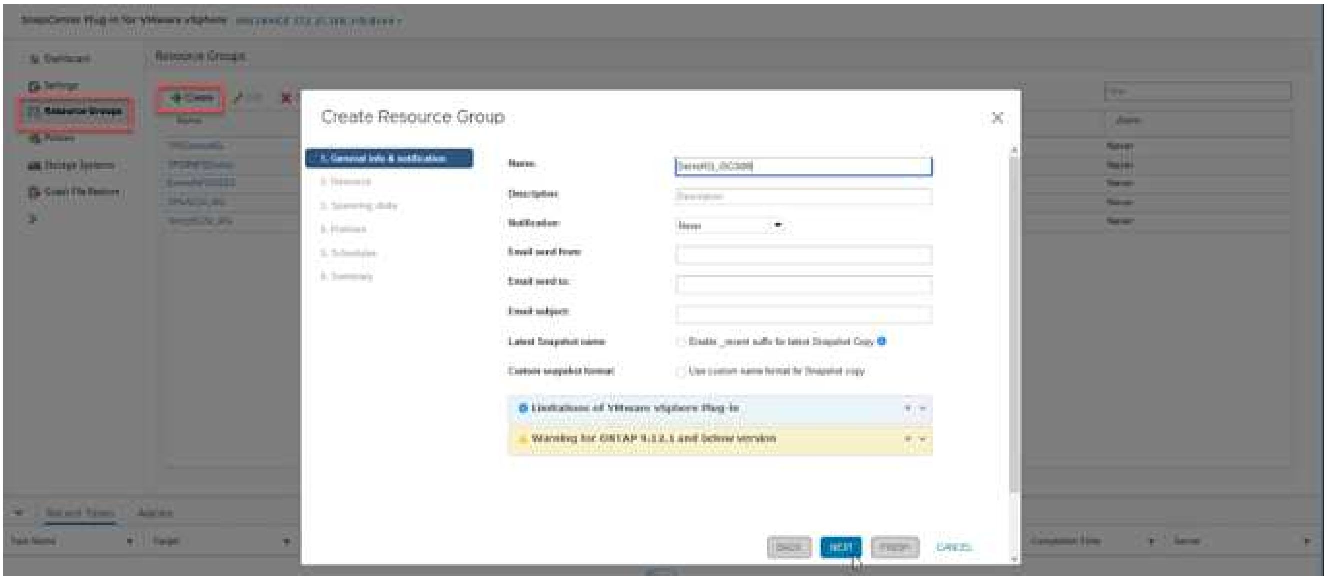
Create Resource group

A resource group is the container for VMs and datastores that needs to be protected. The resources can be added or removed to resource groups at anytime.

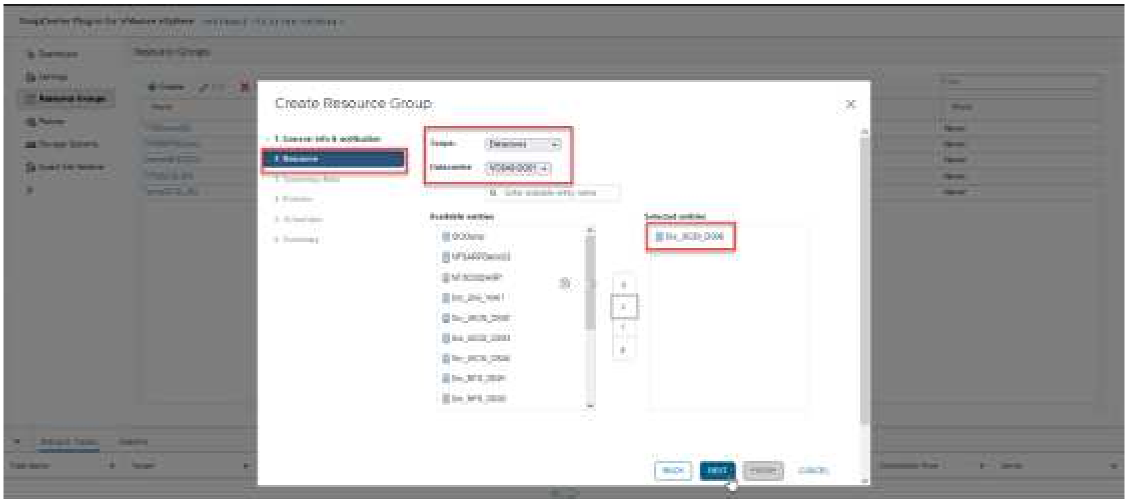
Follow the below steps to create a resource group.

1. In the left Navigator pane of SnapCenter Plug-in for VMware, click Resource Groups.
2. On the Resource Groups page, click Create to start the wizard.

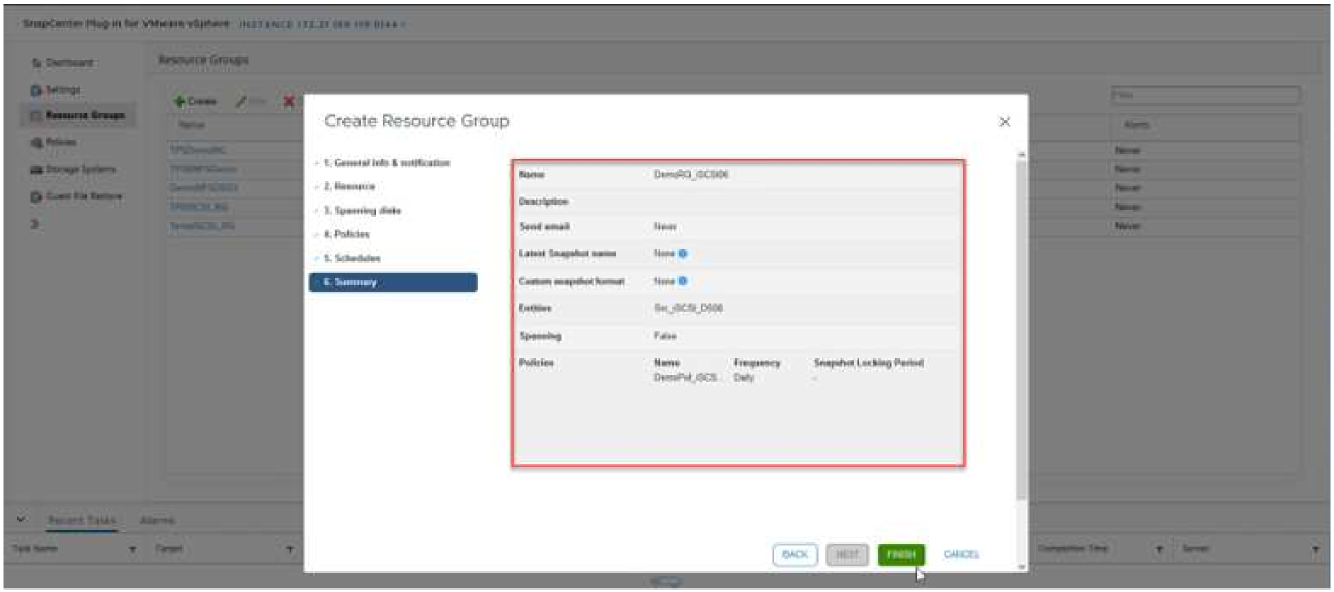
   Another option to create resource group is by selecting the individual VM or datastore and creating a resource group respectively.



3. On the Resources page, select the scope (virtual machines or datastores) and the datacenter.



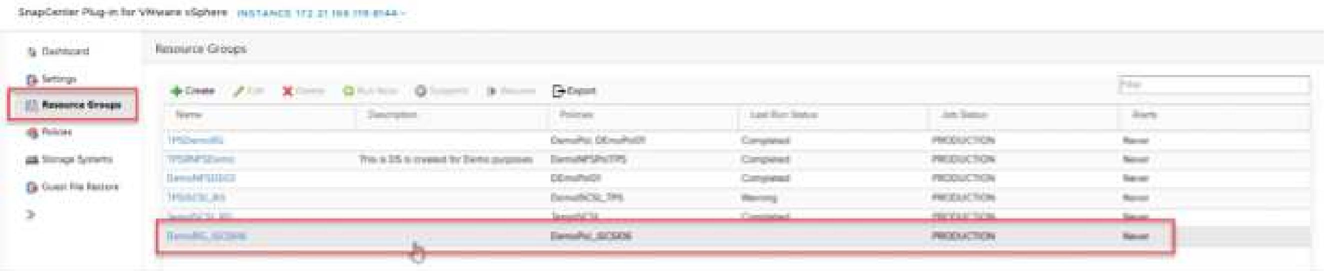
4. On the Spanning disks page, select an option for Virtual Machines with multiple VMDKs across multiple datastores
5. Next step is to associate a backup policy. Select an existing policy or create a new backup policy.
6. On the Schedules page, configure the backup schedule for each selected policy.



Name	DemoRG_iSCSI06
Description	
Send email	Never
Latest Snapshot name	None
Custom snapshot format	None
Entities	Src_iSCSI_DS06
Spanning	False
Policies	Name: DemoPol_iSCSI... Frequency: Daily Snapshot Locking Period: -

7. Once the appropriate selections are made, click Finish.

   This will create new resource group and add to the resource group list.

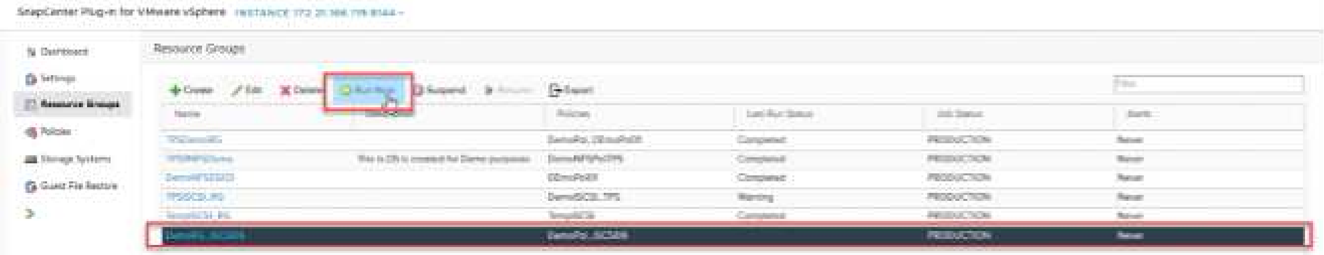


Name	Description	Policies	Last Run Status	Job Status	Alerts
TPSDemoRG		DemoPol, DEmoPol01	Completed	PRODUCTION	Never
TPSNFSDemo	This is DS is created for Demo purposes	DemoNFSPolTPS	Completed	PRODUCTION	Never
DemoNFSDS03		DEmoPol01	Completed	PRODUCTION	Never
TPSiSCSI_RG		DemoiSCSI_TPS	Warning	PRODUCTION	Never
TempiSCSI_RG		TempiSCSI	Completed	PRODUCTION	Never
DemoRG_iSCSI06		DemoPol_iSCSI06		PRODUCTION	Never

Back up resource groups

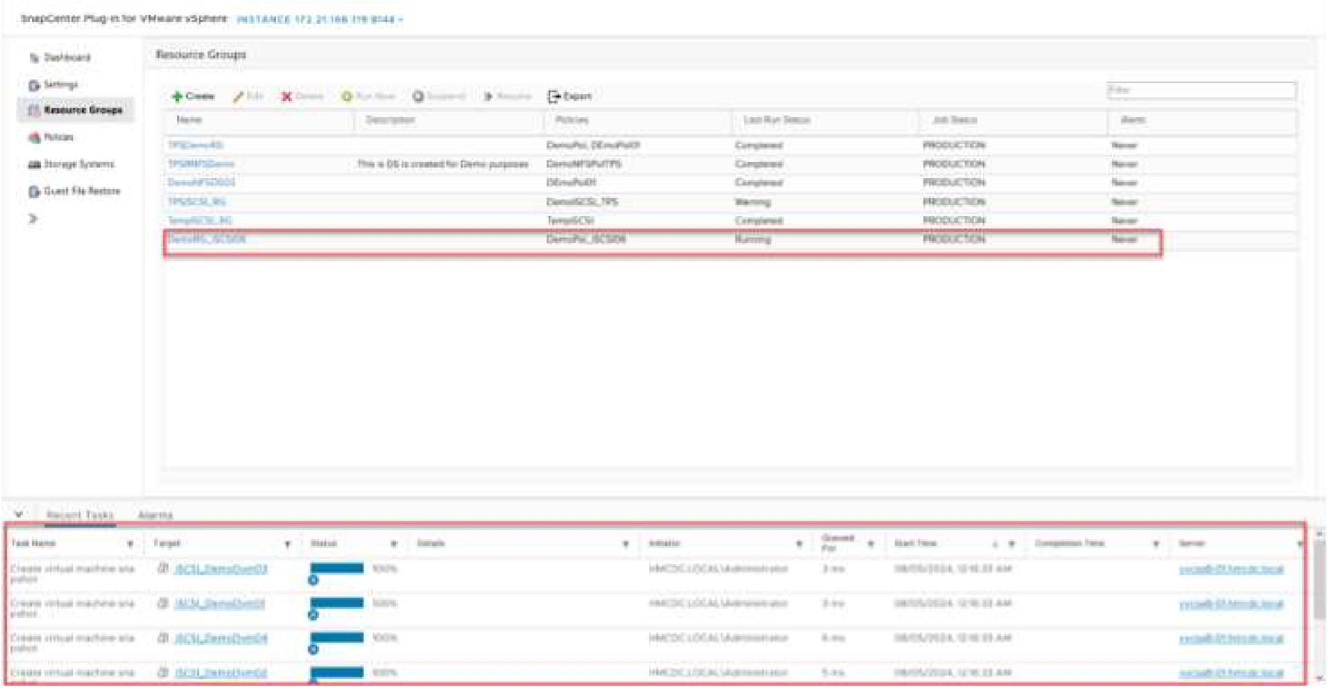
Now it’s time to trigger a backup. The backup operations are performed on all the resources defined in a resource group. If a resource group has a policy attached and a schedule configured, backups occur automatically according to the schedule.

1. In the left navigation of the vCenter web client page, select SnapCenter Plug-in for VMware > Resource Groups, then select the designated resource group. Select Run Now to start the ad-hoc backup.



Name	Description	Policies	Last Run Status	Job Status	Alerts
TPSDemoRG		DemoPol, DEmoPol01	Completed	PRODUCTION	Never
TPSNFSDemo	This is DS is created for Demo purposes	DemoNFSPolTPS	Completed	PRODUCTION	Never
DemoNFSDS03		DEmoPol01	Completed	PRODUCTION	Never
TPSiSCSI_RG		DemoiSCSI_TPS	Warning	PRODUCTION	Never
TempiSCSI_RG		TempiSCSI	Completed	PRODUCTION	Never
DemoRG_iSCSI06		DemoPol_iSCSI06		PRODUCTION	Never

2. If the resource group has multiple policies configured, select the policy for the backup operation in the Backup Now dialog box.
3. Select OK to initiate the backup.



SnapCenter Plug-in for VMware vSphere INSTANCE 172.21.166.119:8144

Resource Groups

Name	Description	Policies	Last Run Status	Job Status	Alarm
TPSDemoRG		DemoPol, DEmoPol01	Completed	PRODUCTION	Never
TPSNFSDemo	This is DS is created for Demo purposes	DemoNFSPolTPS	Completed	PRODUCTION	Never
DemoNFSDS03		DEmoPol01	Completed	PRODUCTION	Never
TPSiSCSI_RG		DemoiSCSI_TPS	Warning	PRODUCTION	Never
TempiSCSI_RG		TempiSCSI	Completed	PRODUCTION	Never
DemoRG_iSCSI06		DemoPol_iSCSI06	Running	PRODUCTION	Never

Recent Tasks

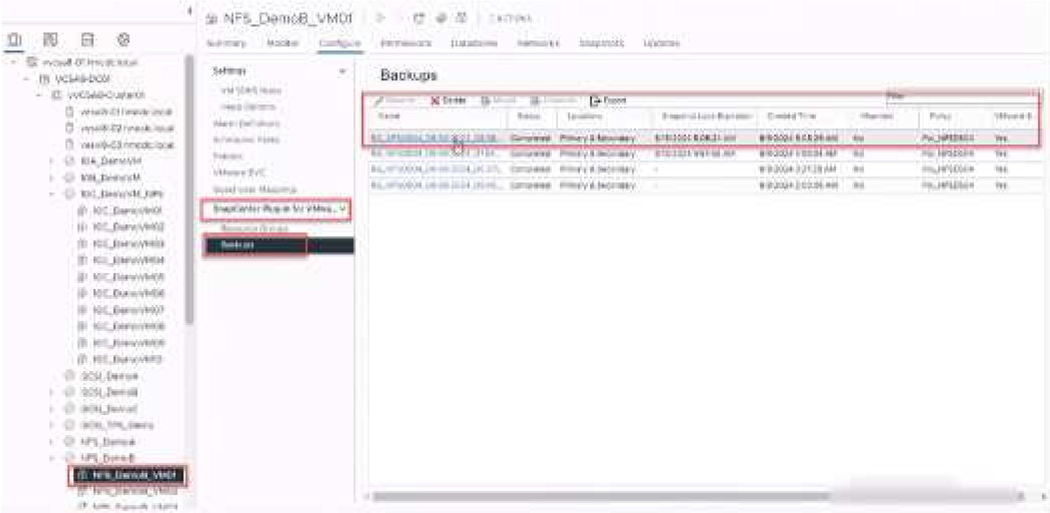
Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Create virtual machine via [illegible]	iSCSI_DemoOvm03	100%		HMCDC.LOCAL\Administrator	3 ms	08/05/2024, 12:16:33 AM		[illegible]
Create virtual machine via [illegible]	iSCSI_DemoOvm01	100%		HMCDC.LOCAL\Administrator	3 ms	08/05/2024, 12:16:33 AM		[illegible]
Create virtual machine via [illegible]	iSCSI_DemoOvm04	100%		HMCDC.LOCAL\Administrator	6 ms	08/05/2024, 12:16:33 AM		[illegible]
Create virtual machine via [illegible]	iSCSI_DemoOvm02	100%		HMCDC.LOCAL\Administrator	5 ms	08/05/2024, 12:16:33 AM		[illegible]

Monitor the operation progress by selecting Recent Tasks at the bottom of the window or on the dashboard Job Monitor for more details.

Restore VMs from backup

SnapCenter Plug-in for VMware enables to restore virtual machines (VMs) to the vCenter. While restoring a VM, it can be restored to the original datastore mounted on the original ESXi host which will overwrite the existing content with the backup copy that is selected or a deleted/renamed VM can be restored from a backup copy (operation overwrites the data in the original virtual disks). To perform restore, follow the below steps:

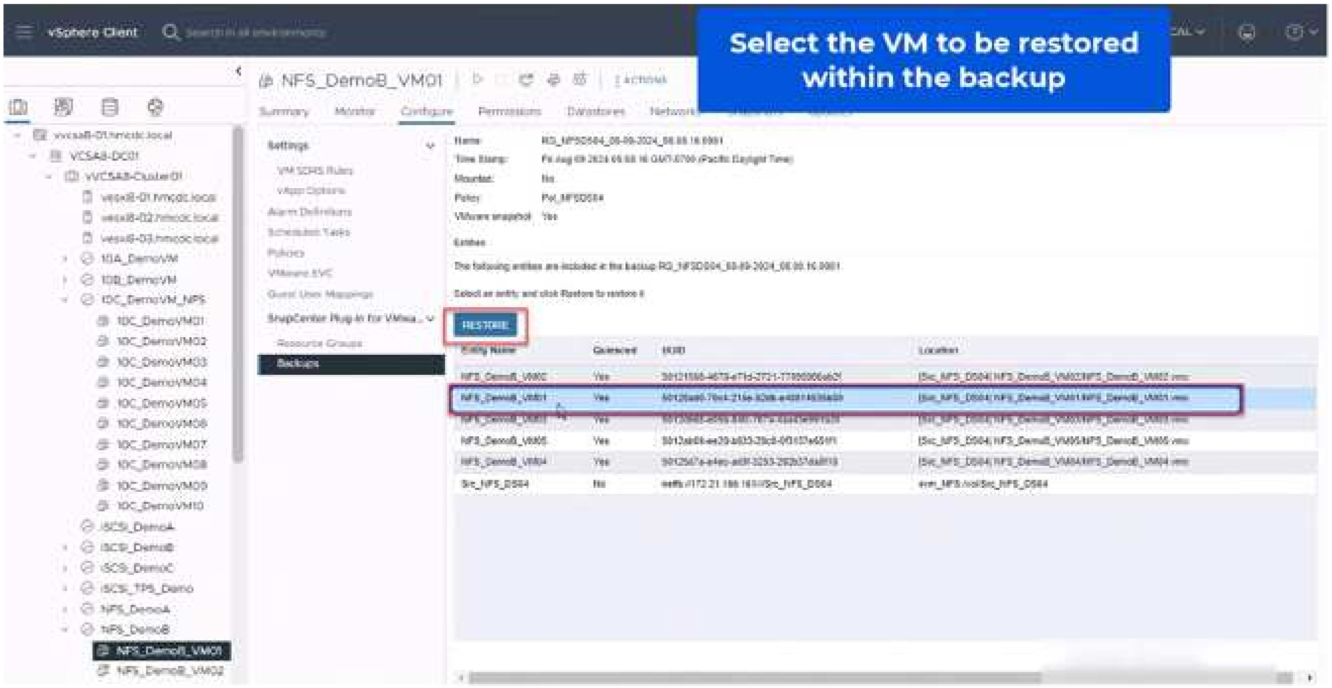
1. In the VMware vSphere web client GUI, select Menu in the toolbar. Select Inventory and then Virtual Machines and Templates.
2. In the left navigation, Select the Virtual Machine, then select Configure tab, Select Backups under SnapCenter Plug-in for VMware. Click on the backup job from which the VM needs to be restored.



NFS_DemoB_VM01

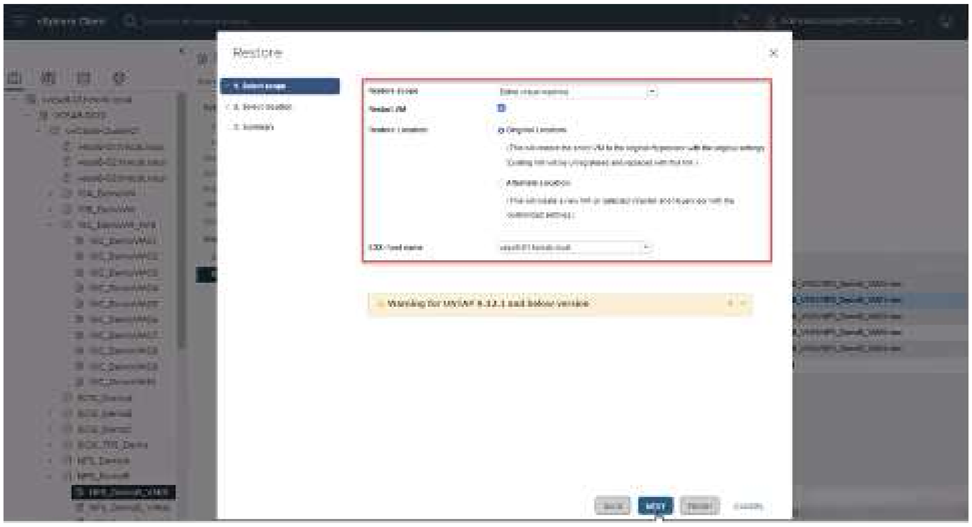
Backups

3. Select the VM that needs to be restored from the backup.

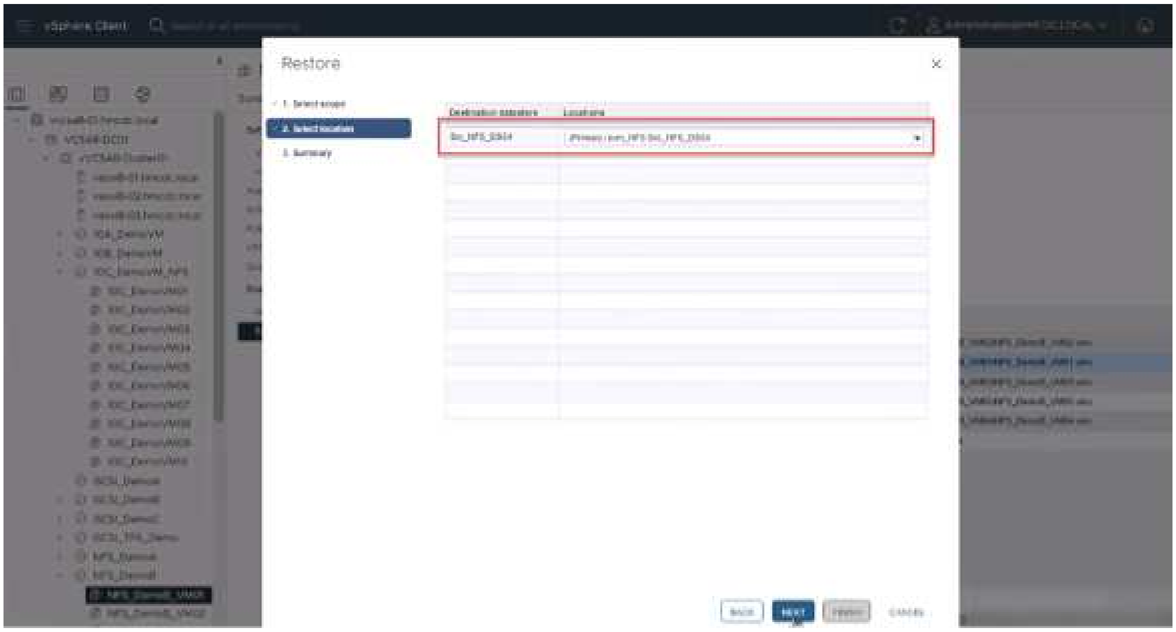


Select the VM to be restored within the backup

4. On the Select Scope page, select Entire Virtual Machine in the Restore scope field, then select Restore location, and then enter the destination ESXi information where the backup should be mounted. Enable Restart VM checkbox if the VM needs to be powered on after the restore operation.

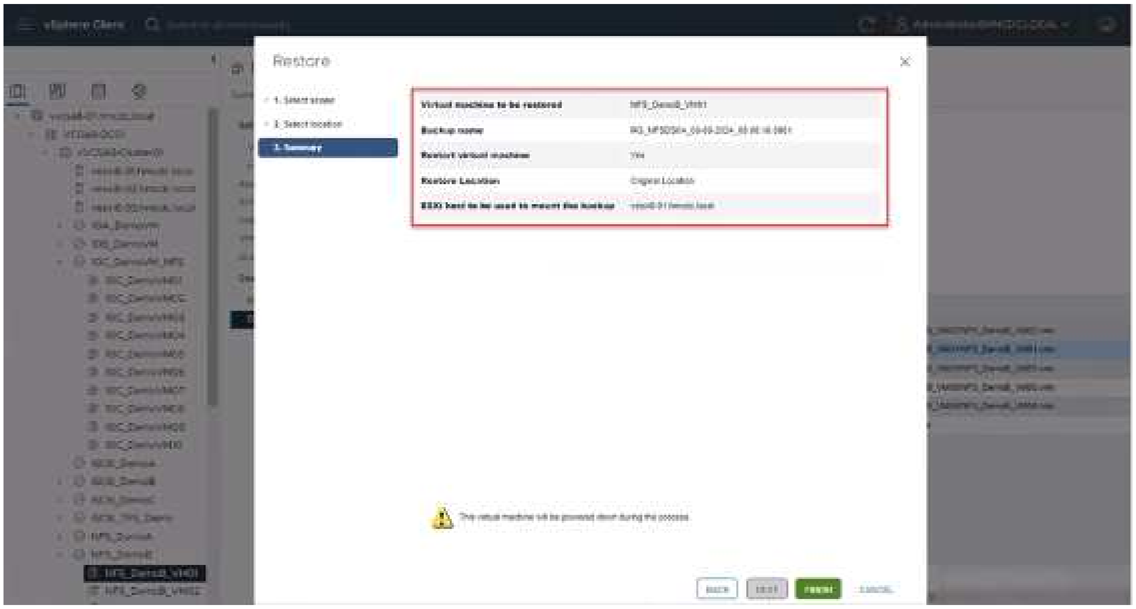


5. On the Select Location page, select the location for the primary location.



Destination datastore	Locations
Src_NFS_DS04	(Primary) svm_NFS:Src_NFS_DS04

6. Review the Summary page and then select Finish.



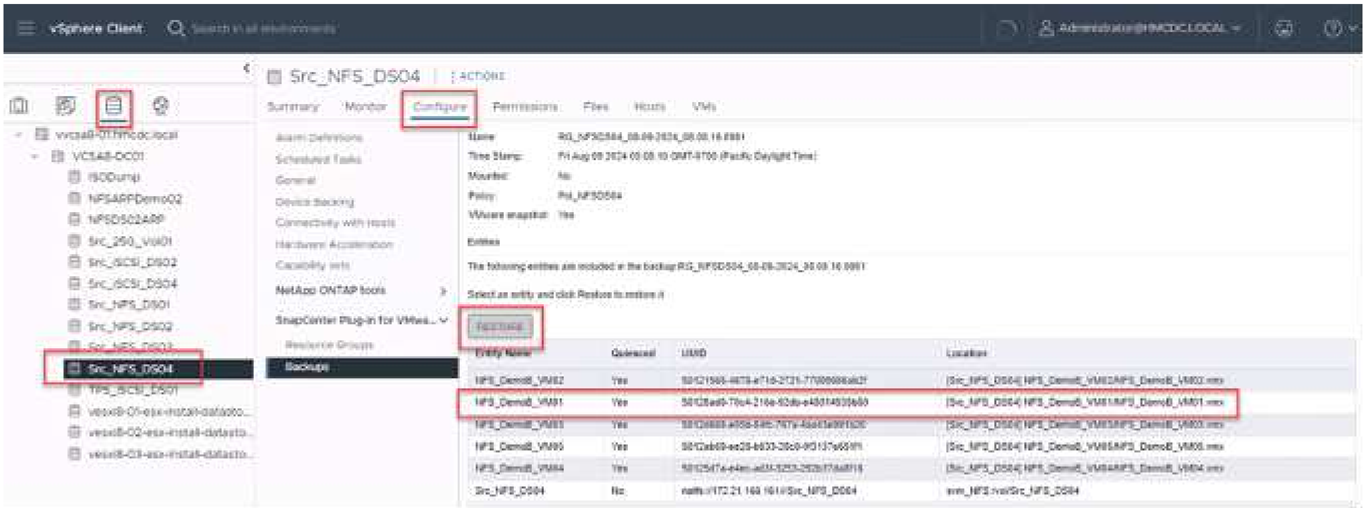
Virtual machine to be restored	NFS_DemoB_VM01
Backup name	RG_NFSDS04_03-09-2024_05.05.18.0861
Restart virtual machine	Yes
Restore Location	Original Location
ESXi host to be used to mount the backup	esxi8-01.hmcdc.local

This virtual machine will be powered down during the process.

Monitor the operation progress by selecting Recent Tasks at the bottom of the screen.

Although the VMs are restored, they're not automatically added to their former resource groups. Therefore, add the restored VMs to the appropriate resource groups manually if protection of those VMs is required.

Now what if the original VM was deleted. It's a simple task with SnapCenter Plug-in for VMware. The restore operation for a deleted VM can be performed from the datastore level. Go to respective Datastore > Configure > Backups and select the deleted VM and select Restore.



Name: RG_NFSDS04_08-09-2024_08.08.16.0981

Time Stamp: Fri Aug 09 2024 08:08:10 GMT-0700 (Pacific Daylight Time)

Mounted: No

Policy: Pol_NFSDS04

VMware snapshot: Yes

Entities

The following entities are included in the backup:RG_NFSDS04_08-09-2024_08.08.16.0981

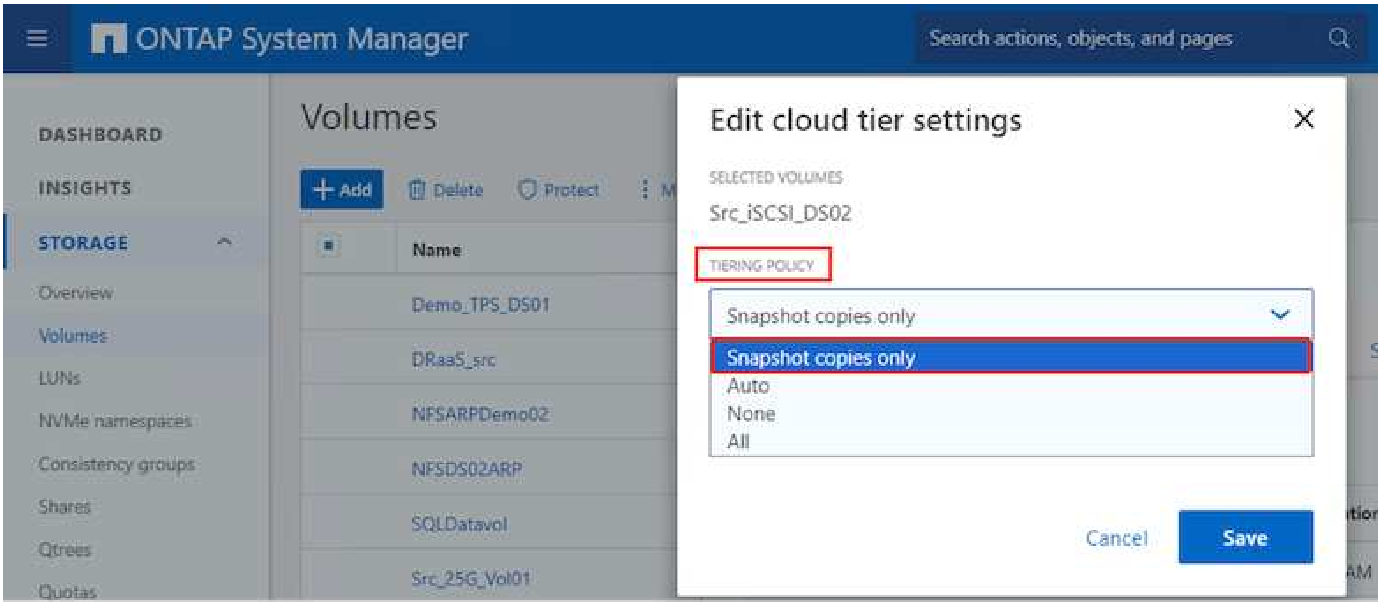
Select an entity and click Restore to restore it

Entity Name	Quiesced	UUID	Location
NFS_DemoB_VM02	Yes	[illegible]	[Src_NFS_DS04] NFS_DemoB_VM02/NFS_DemoB_VM02.vmx
NFS_DemoB_VM01	Yes	[illegible]	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_DemoB_VM01.vmx
NFS_DemoB_VM03	Yes	[illegible]	[Src_NFS_DS04] NFS_DemoB_VM03/NFS_DemoB_VM03.vmx
NFS_DemoB_VM05	Yes	[illegible]	[Src_NFS_DS04] NFS_DemoB_VM05/NFS_DemoB_VM05.vmx
NFS_DemoB_VM04	Yes	[illegible]	[Src_NFS_DS04] NFS_DemoB_VM04/NFS_DemoB_VM04.vmx
Src_NFS_DS04	No	netfs://172.21.169.161//Src_NFS_DS04	svm_NFS:/vol/Src_NFS_DS04

To summarize, when using ONTAP ASA storage to optimise TCO for a VMware deployment, use SnapCenter Plug-in for VMware as a simple and efficient method for backing up VMs. It enables to back up and restore VMs in a seamless and fast manner as snapshot backups take literally seconds to complete.

Refer to this solution guide and product documentation to learn about Snapcenter configuration, backup, restore from primary or secondary storage system or even from backups stored on object storage for long term retention.

To reduce storage costs, FabricPool volume tiering can be enabled to automatically move data for snapshot copies to a lower-cost storage tier. Snapshot copies typically use over 10% of allocated storage. While important for data protection and disaster recovery, these point-in-time copies are seldom used and are not an efficient use of high-performance storage. With the "Snapshot-Only" policy for FabricPool, you can easily free up space on high-performance storage. When this policy is enabled, inactive snapshot copy blocks in the volume that are not being used by the active file system are moved to the object tier and once read, the Snapshot copy is moved to the local tier to recover a VM or entire datastore. This object tier can be in the form of a private cloud (such as NetApp StorageGRID) or a public cloud (such as AWS or Azure).



Edit cloud tier settings

SELECTED VOLUMES
Src_iSCSI_DS02

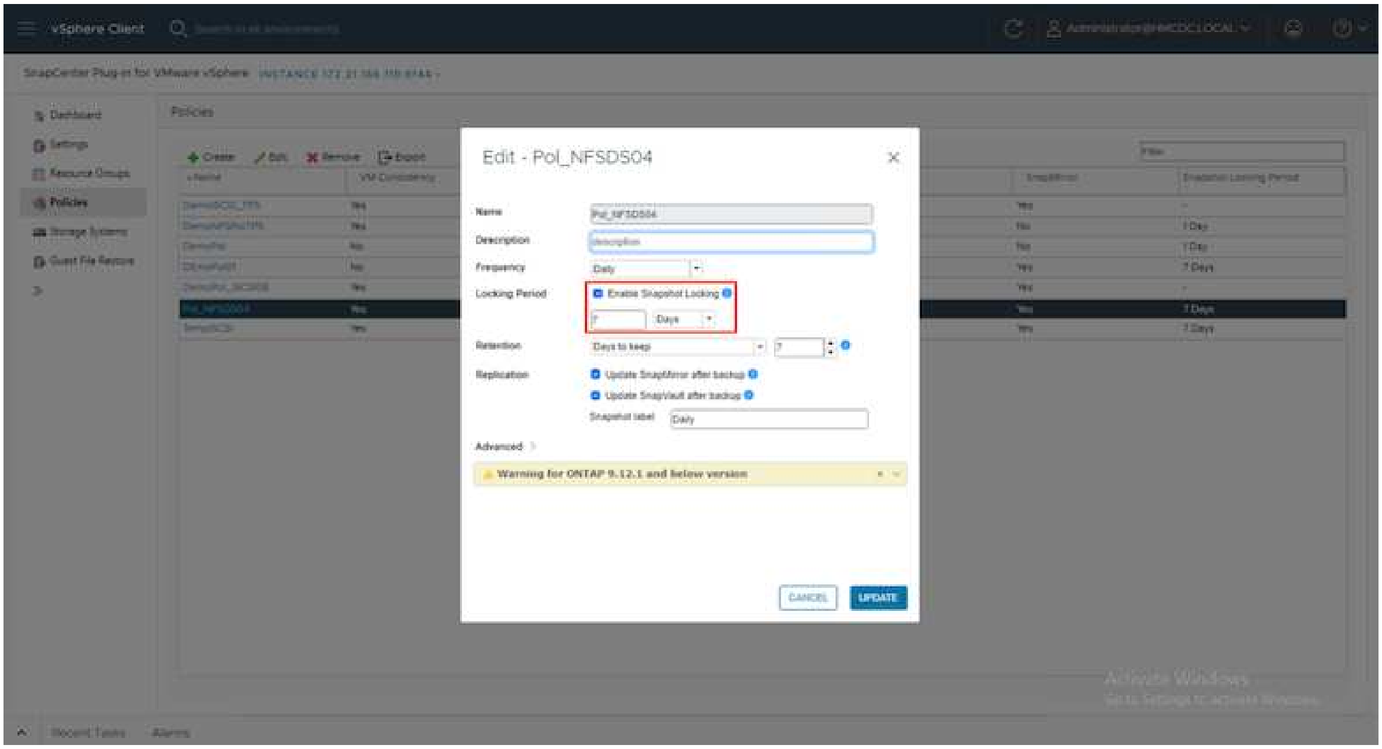
TIERING POLICY
Snapshot copies only

View detailed guidance for VMware vSphere with ONTAP.

Ransomware Protection

One of the most effective ways for ransomware attack protection is by implementing multi-layered security measures. Each virtual machine residing on a datastore hosts a standard operating system. Ensure enterprise server anti-malware product suites are installed and regularly updated on them which is an essential component of multi-layered ransomware protection strategy. Along with this, implement data protection leveraging NetApp snapshot technology to ensure rapid and reliable recovery from a ransomware attack.

Ransomware attacks are increasingly targeting backups and snapshot recovery points by trying to delete them before starting to encrypt files. However, with ONTAP this can be prevented by creating tamperproof snapshots on primary or secondary systems with NetApp Snapshot™ copy locking in ONTAP. These Snapshot copies can't be deleted or changed by ransomware attackers or rogue administrators, so they're available even after an attack. You can recover virtual machine data in seconds, minimizing organization's downtime. Plus, you have the flexibility to choose the Snapshot schedule and lock duration that are right for your organization.


Edit - Pol_NFSDS04

Name: Pol_NFSDS04
Description: description
Frequency: Daily
Locking Period: ☑ Enable Snapshot Locking — 7 Days
Retention: Days to keep — 7
Replication: ☑ Update SnapMirror after backup
☑ Update SnapVault after backup
Snapshot label: Daily

Warning for ONTAP 9.12.1 and below version

As part of adding multiple layered approach, there is also a native built-in ONTAP solution for protecting unauthorized deletion of backup Snapshot copies. It is known as multiadmin verification or MAV which is available in ONTAP 9.11.1 and later. The ideal approach will be to use queries for MAV specific operations.

To learn more about MAV and how to configure its protection capabilities see the Multi-admin verification overview.

Migration

Many IT organizations are adopting a hybrid cloud-first approach as they undergo a transformation phase. Customers are assessing their current IT infrastructure and moving their workloads to the cloud based on this assessment and discovery. The reasons for migrating to the cloud vary and can include factors such as elasticity and burst, data center exit, data center consolidation, end-of-life scenarios, mergers, acquisitions, and more. Each organization's migration reasoning depends on their specific business priorities with cost optimization being the highest priority. Selecting the right cloud storage is crucial when moving to the hybrid cloud, as it unleashes the power of cloud deployment and elasticity.

By integrating with 1P services powered by NetApp on each hyperscalar, organizations can realize a vSphere-based cloud solution with a simple migration approach, with no re-platforming, no IP changes, and no architectural changes. Additionally, this optimization enables you to scale the storage footprint while keeping the host count to least amount required in vSphere, but no change to the storage hierarchy, security, or files made available.

- View detailed guidance for Migrate Workloads to FSx for ONTAP datastore.
- View detailed guidance for Migrate workloads to Azure NetApp Files datastore.
- View detailed guidance for Migrate workloads to Google Cloud NetApp Volumes datastore.

Disaster Recovery

Disaster Recovery between on-premises sites

For more details, please visit DR using BlueXP DRaaS for VMFS Datastores

Disaster Recovery between on-premises and VMware Cloud in any hyperscalar

For those customers looking to use VMware Cloud on any hyperscalar as the disaster recovery target, ONTAP storage powered datastores (Azure NetApp Files, FSx for ONTAP, Google Cloud NetApp volumes) can be used to replicate data from on-premises using any validated third-party solution that provides VM replication capability. By adding ONTAP storage powered datastores, it will enable cost optimised disaster recovery on the destination with fewer amount of ESXi hosts. This also enables to decommission secondary site in the on-premises environment thus enabling significant cost savings.

- View detailed guidance for Disaster Recovery to FSx for ONTAP datastore.
- View detailed guidance for Disaster Recovery to Azure NetApp Files datastore.
- View detailed guidance for Disaster Recovery to Google Cloud NetApp Volumes datastore.

Conclusion

This solution demonstrates the optimal approach to using the ONTAP SAN technologies and Offtap tools to provide essential IT services for businesses both now and in the future. These advantages are particularly beneficial for virtualized environments running VMware vSphere in a SAN setup. With the flexibility and scalability of the NetApp storage systems, organizations can establish a foundation for updating and adjusting their infrastructure, allowing them to meet changing business needs over time. This system can handle current workloads and enhance infrastructure efficiency, thereby reducing operational costs and preparing for future workloads.

NetApp All-Flash SAN Array with VMware vSphere 8

For nearly two decades, NetApp ONTAP software has established itself as a premier storage solution for VMware vSphere environments, continually introducing innovative features that simplify management and decrease costs. NetApp is an established leader in the development of NAS and unified storage platforms that offer a wide range of protocol and connectivity support. Alongside this market segment, there are many customers who prefer the simplicity and cost benefits of block-based SAN storage platforms that are focused on doing one job well. NetApp's All-Flash SAN Array (ASA) delivers on that promise with simplicity at scale and with consistent management and automation features for all applications and cloud providers.

Author: Josh Powell - NetApp Solutions Engineering

Solution Overview

Purpose of This Document

In this document we will cover the unique value of using NetApp ASA storage systems with VMware vSphere and provide a technology overview of the NetApp All-Flash SAN Array. In addition, we will look at additional tools for simplifying storage provisioning, data protection, and monitoring of your VMware and ONTAP datacenter.

Deployment sections of this document cover creating vVol datastores with ONTAP Tools for VMware vSphere, and observability for the modern datacenter with NetApp Cloud Insights.

Technology Overview

This solution includes innovative technologies from VMware and NetApp.

VMware vSphere 8.0

VMware vSphere is a virtualization platform that transforms physical resources into pools of compute, network and storage which can be used to satisfy customers' workload and application requirements. The main components of VMware vSphere include:

- **ESXi** - VMware's hypervisor which enables the abstraction of compute processors, memory, network and other resources and makes them available to virtual machines and container workloads.
- **vCenter** - VMware vCenter is a centralized management platform for interacting with compute resources, networking and storage as part of a virtual infrastructure. vCenter plays a crucial role in simplifying the administration of virtualized infrastructure.

New Improvements in vSphere 8.0

vSphere 8.0 introduces some new improvements including, but not limited to:

Scalability - vSphere 8.0 supports the latest Intel and AMD CPUs and has extended limits for vGPU devices, ESXi hosts, VMs per cluster, and VM DirectPath I/O devices.

Distributed Services Engine - Network offloading with NSX to Data Processing Units (DPUs).

Enhanced Device Efficiency - vSphere 8.0 boosts device management capabilities with features like device groups and Device Virtualization Extensions (DVX).

Improved Security - The inclusion of an SSH timeout and TPM Provision Policy strengthens the security framework.

Integration with Hybrid Cloud Services - This feature facilitates seamless transition between on-premises and cloud workloads.

Integrated Kubernetes Runtime - With the inclusion of Tanzu, vSphere 8.0 simplifies container orchestration.

For more information refer to the blog, What's New in vSphere 8?.

VMware Virtual Volumes (vVols)

vVols are a revolutionary new approach to storage management in vSphere clusters, providing simplified management and more granular control of storage resources. In a vVols datastore each virtual disk is a vVol and becomes a native LUN object on the storage system. The integration of the storage system and vSphere takes place through the **VMware API's for Storage Awareness (VASA)** provider and allows the storage system to be aware of the VM data and manage it accordingly. Storage policies, defined in the vCenter Client are used to allocate and manage storage resources.

vVols are a simplified approach to storage management and are preferred in some use cases.

For more information on vVols see the vVols Getting Started Guide.

NVMe over Fabrics

With the release of vSphere 8.0, NVMe is now supported end-to-end with full support for vVols with NVMe-TCP and NVMe-FC.

For detailed information on using NVMe with vSphere refer to About VMware NVMe Storage in the vSphere Storage documentation.

NetApp ONTAP

NetApp ONTAP software has been a leading storage solution for VMware vSphere environments for almost two decades and continues to add innovative capabilities to simplify management while reducing costs. Using ONTAP together with vSphere is a great combination that lets you reduce host hardware and VMware software expenses. You can also protect your data at lower cost with consistent high performance while taking advantage of native storage efficiencies.

Base ONTAP Features

NetApp Snapshot copies: Snapshot copies of a VM or datastore, ensuring no performance impact upon the creation or utilization of a Snapshot. These replicas can serve as restoration points for VMs or as a simple data safeguard. These array-based snapshots are different than VMware (consistency) snapshots. The most straightforward method to generate an ONTAP Snapshot copy is through the SnapCenter Plug-In for VMware vSphere, backing up VMs and datastores.

- **Storage Efficiency** - ONTAP provides real-time and background deduplication and compression, zero-block deduplication, and data compaction.
- **Volume and LUN move** - Allows non-disruptive movement of volumes and LUNs supporting vSphere datastores and vVols within the ONTAP cluster to balance performance and capacity or support non-disruptive maintenance and upgrades.
- **Relocation of Volume and LUN** - ONTAP allows non-disruptive movement of volumes and LUNs that host vSphere datastores and vVols within the ONTAP cluster. This aids in balancing performance and capacity, and allows for non-disruptive upgrades.
- **Quality of Service** - QoS is a feature that enables the management of performance on an individual LUN, volume, or file. It can be used to limit an aggressive VM or to ensure that a critical VM receives sufficient performance resources.
- **Encryption** - NetApp Volume Encryption and NetApp Aggregate Encryption. These options provide a straightforward software-based approach to encrypting data at rest, ensuring its protection.
- **Fabric Pool** - This feature tiers less frequently accessed data to a separate object store, freeing up

valuable flash storage. By operating at the block level, it efficiently identifies and tiers colder data, helping to optimize storage resources and reduce costs.

- **Automation** - Simplifies storage and data management tasks by utilizing ONTAP REST APIs for automation, and leveraging Ansible modules for seamless configuration management of ONTAP systems. Ansible modules offer a convenient solution for efficiently managing the configurations of ONTAP systems. The combination of these powerful tools enables the streamlining of workflows and enhancement of the overall management of storage infrastructure.

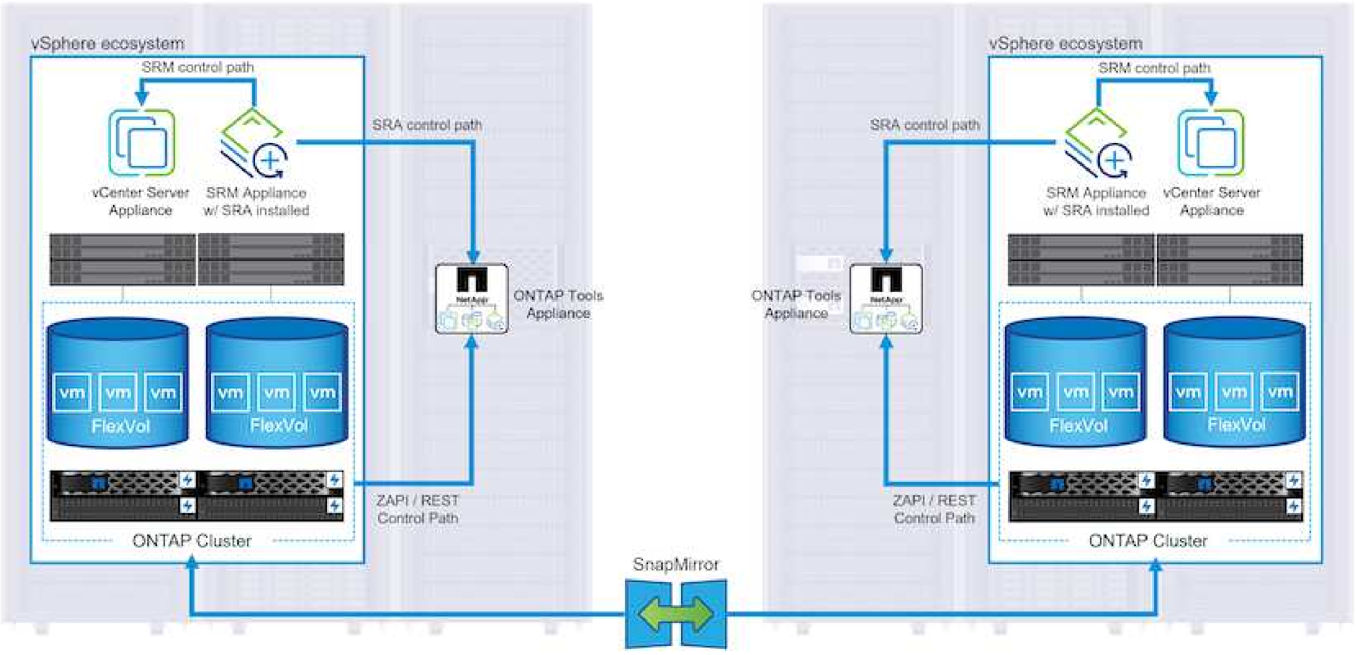
ONTAP Disaster Recovery Features

NetApp ONTAP provides robust disaster recovery solutions for VMware environments. These solutions leverage SnapMirror replication technologies between primary and secondary storage systems to allow failover and quick recovery in the case of failure.

Storage Replication Adapter:
The NetApp Storage Replication Adapter (SRA) is a software component that provides integration between NetApp storage systems and VMware Site Recovery Manager (SRM). It facilitates replication of virtual machine (VM) data across NetApp storage arrays, delivering robust data protection and disaster recovery capabilities. The SRA uses SnapMirror and SnapVault to achieve the replication of VM data across disparate storage systems or geographical locations.

The adapter provides asynchronous replication at the storage virtual machine (SVM) level using SnapMirror technology and extends support for both VMFS in SAN storage environments (iSCSI and FC) and NFS in NAS storage environments.

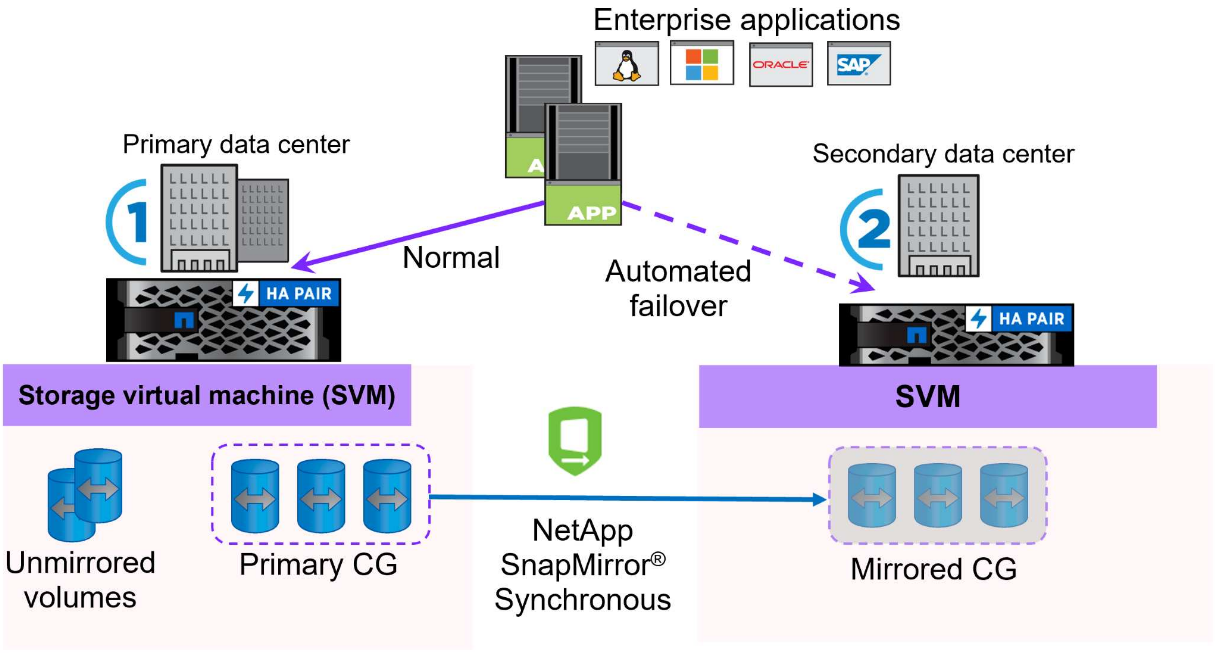
The NetApp SRA is installed as part of ONTAP Tools for VMware vSphere.



For information on the NetApp Storage Replication Adapter for SRM refer to VMware Site Recovery Manager with NetApp ONTAP.

SnapMirror Business Continuity:
SnapMirror is a NetApp data replication technology that provides synchronous replication of data between storage systems. It allows for the creation of multiple copies of data at different locations, providing the ability to recover data in case of a disaster or data loss event. SnapMirror provides flexibility in terms of replication

frequency and allows for the creation of point-in-time copies of data for backup and recovery purposes. SM-BC replicates data at the Consistency Group level.

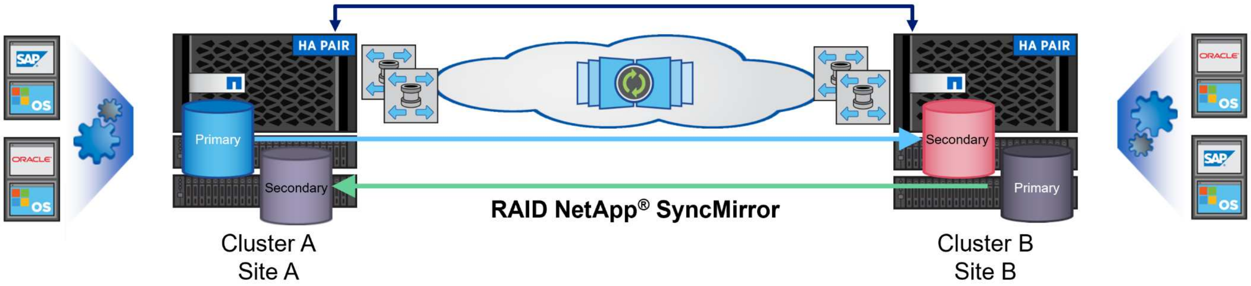


For more information refer to SnapMirror Business Continuity overview.

NetApp MetroCluster:
NetApp MetroCluster is a high-availability and disaster recovery solution that provides synchronous data replication between two geographically dispersed NetApp storage systems. It is designed to ensure continuous data availability and protection in the event of a site-wide failure.

MetroCluster uses SyncMirror to synchronously replicate data just above the RAID level. SyncMirror is designed to efficiently transition between synchronous and asynchronous modes. This allows the primary storage cluster to continue operating in a non-replicated state in situations where the secondary site becomes temporarily inaccessible. SyncMirror will also replicate back to a RPO = 0 state when connectivity is restored.

MetroCluster can operate over IP based networks or using fibre channel.



For detailed information on MetroCluster architecture and configuration refer to the MetroCluster documentation site.

ONTAP One Licensing Model

ONTAP One is a comprehensive licensing model that provides access to all features of ONTAP without requiring additional licenses. This includes data protection, disaster recovery, high availability, cloud integration, storage efficiency, performance, and security. Customers with NetApp storage systems licensed with Flash, Core plus Data Protection, or Premium are entitled to ONTAP One licensing, ensuring they can maximize the use of their storage systems.

ONTAP One licensing includes all of the following features:

NVMeoF – Enables the use of NVMe over Fabrics for front end client IO, both NVMe/FC and NVMe/TCP.

FlexClone – Enables rapid creation of space efficient cloning of data based on snapshots.

S3 – Enables the S3 protocol for front end client IO.

SnapRestore – Enables rapid recovery of data from snapshots.

Autonomous Ransomware Protection - Enables the automatic protection of NAS file shares when abnormal filesystem activity is detected.

Multi Tenant Key Manager - Enables the ability to have multiple key managers for different tenants on the system.

SnapLock – Enables the protection of data from modification, deletion or corruption on the system.

SnapMirror Cloud – Enables the replication of system volumes to object targets.

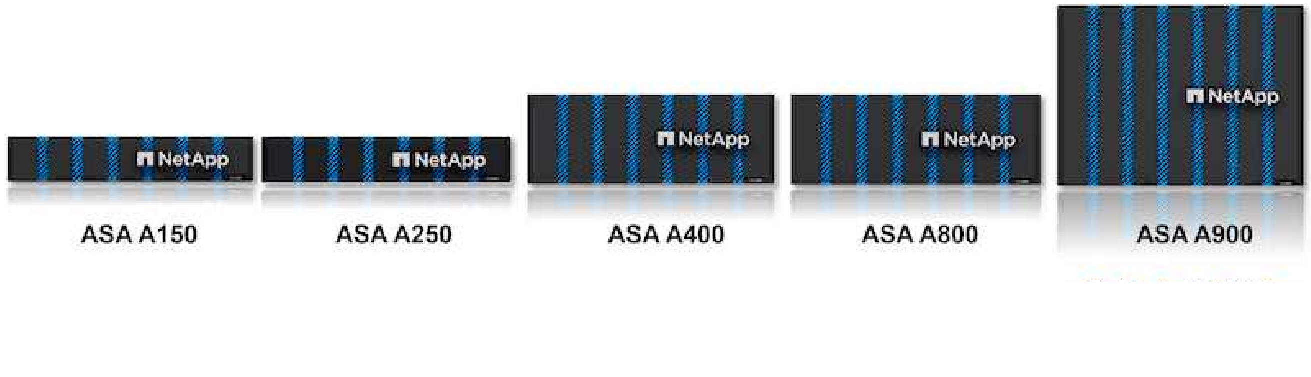
S3 SnapMirror – Enables the replication of ONTAP S3 objects to alternate S3 compatible targets.

NetApp All-Flash SAN Array

The NetApp All-Flash SAN Array (ASA) is a high-performance storage solution designed to meet the demanding requirements of modern data centers. It combines the speed and reliability of flash storage with NetApp’s advanced data management features to deliver exceptional performance, scalability, and data protection.

The ASA lineup is comprised of both A-Series and C-Series models.

The NetApp A-Series all-NVMe flash arrays are designed for high-performance workloads, offering ultra-low latency and high resiliency, making them suitable for mission-critical applications.



C-Series QLC flash arrays are aimed at higher-capacity use cases, delivering the speed of flash with the economy of hybrid flash.

For detailed information see the NetApp ASA landing page.

NetApp ASA features

The NetApp All-Flash SAN Array includes the following features:

Performance - The All-Flash SAN Array leverages solid-state drives (SSDs), with an end-to-end NVMe architecture, to provide lightning-fast performance, significantly reducing latency and improving application response times. It delivers consistent high IOPS and low latency, making it suitable for latency-sensitive workloads such as databases, virtualization, and analytics.

Scalability - NetApp All-Flash SAN Arrays are built with a scale-out architecture, allowing organizations to seamlessly scale their storage infrastructure as their needs grow. With the ability to add additional storage nodes, organizations can expand capacity and performance without disruption, ensuring that their storage can keep up with increasing data demands.

Data Management - NetApp's Data ONTAP operating system powers the All-Flash SAN Array, providing a comprehensive suite of data management features. These include thin provisioning, deduplication, compression, and data compaction, which optimize storage utilization and reduce costs. Advanced data protection features like snapshots, replication, and encryption ensure the integrity and security of stored data.

Integration and Flexibility - The All-Flash SAN Array integrates with NetApp's broader ecosystem, enabling seamless integration with other NetApp storage solutions, such as hybrid cloud deployments with NetApp Cloud Volumes ONTAP. It also supports industry-standard protocols like Fibre Channel (FC) and iSCSI, enabling easy integration into existing SAN infrastructures.

Analytics and Automation - NetApp's management software, including NetApp Cloud Insights, provides comprehensive monitoring, analytics, and automation capabilities. These tools enable administrators to gain insights into their storage environment, optimize performance, and automate routine tasks, simplifying storage management and improving operational efficiency.

Data Protection and Business Continuity - The All-Flash SAN Array offers built-in data protection features such as point-in-time snapshots, replication, and disaster recovery capabilities. These features ensure data availability and facilitate rapid recovery in the event of data loss or system failures.

Protocol Support

The ASA supports all standard SAN protocols including, iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), and NVME over fabrics.

iSCSI - NetApp ASA provides robust support for iSCSI, allowing block-level access to storage devices over IP networks. It offers seamless integration with iSCSI initiators, enabling efficient provisioning and management of iSCSI LUNs. ONTAP's advanced features, such as multi-pathing, CHAP authentication, and ALUA support.

For design guidance on iSCSI configurations refer to .

Fibre Channel - NetApp ASA offers comprehensive support for Fibre Channel (FC), a high-speed network technology commonly used in storage area networks (SANs). ONTAP seamlessly integrates with FC infrastructure, providing reliable and efficient block-level access to storage devices. It offers features like zoning, multi-pathing, and fabric login (FLOGI) to optimize performance, enhance security, and ensure seamless connectivity in FC environments.

For design guidance on Fibre Channel configurations refer to the SAN Configuration reference documentation.

NVMe over Fabrics - NetApp ONTAP and ASA support NVMe over fabrics. NVMe/FC enables the use of NVMe storage devices over Fibre Channel infrastructure, and NVMe/TCP over storage IP networks.

For design guidance on NVMe refer to NVMe configuration, support and limitations.

Active-active technology

NetApp All-Flash SAN Arrays allows for active-active paths through both controllers, eliminating the need for the host operating system to wait for an active path to fail before activating the alternative path. This means that the host can utilize all available paths on all controllers, ensuring active paths are always present regardless of whether the system is in a steady state or undergoing a controller failover operation.

Furthermore, the NetApp ASA offers a distinctive feature that greatly enhances the speed of SAN failover. Each controller continuously replicates essential LUN metadata to its partner. As a result, each controller is prepared to take over data serving responsibilities in the event of a sudden failure of its partner. This readiness is possible because the controller already possesses the necessary information to start utilizing the drives that were previously managed by the failed controller.

With active-active pathing, both planned and unplanned takeovers have IO resumption times of 2-3 seconds.

For more information see TR-4968, NetApp All-SAS Array – Data Availability and Integrity with the NetApp ASA.

Storage guarantees

NetApp offers a unique set of storage guarantees with NetApp All-flash SAN Arrays. The unique benefits include:

Storage efficiency guarantee: Achieve high performance while minimizing storage cost with the Storage Efficiency Guarantee. 4:1 for SAN workloads.

6 Nines (99.9999%) data availability guarantee: Guarantees remediation for unplanned downtime in excess of 31.56 seconds per year.

Ransomware recovery guarantee: Guaranteed data recovery in the event of a ransomware attack.

See the NetApp ASA product portal for more information.

NetApp Plug-ins for VMware vSphere

NetApp storage services are tightly integrated with VMware vSphere through the use of the following plug-ins:

ONTAP Tools for VMware vSphere

The ONTAP Tools for VMware allows administrators to manage NetApp storage directly from within the vSphere Client. ONTAP Tools allows you to deploy and manage datastores, as well as provision vVol datastores.
ONTAP Tools allows mapping of datastores to storage capability profiles which determine a set of storage system attributes. This allows the creation of datastores with specific attributes such as storage performance and QoS.

ONTAP Tools includes the following components:

Virtual Storage Console (VSC): The VSC includes the interface integrated with the vSphere client where you can add storage controllers, provision datastores, monitor performance of datastores, and view and update ESXi host settings.

VASA Provider: The VMware vSphere APIs for Storage Awareness (VASA) Provider for ONTAP send information about storage used by VMware vSphere to the vCenter Server, enabling provisioning of VMware Virtual Volumes (vVols) datastores, creation and use of storage capability profiles, compliance verification, and performance monitoring.

Storage Replication Adapter (SRA): When enabled and used with VMware Site Recovery Manager (SRM), SRA facilitates the recovery of vCenter Server datastores and virtual machines in the event of a failure, allowing configuration of protected sites and recovery sites for disaster recovery.

For more information on NetApp ONTAP tools for VMware see ONTAP tools for VMware vSphere Documentation.

SnapCenter Plug-in for VMware vSphere

The SnapCenter Plug-in for VMware vSphere (SCV) is a software solution from NetApp that offers comprehensive data protection for VMware vSphere environments. It is designed to simplify and streamline the process of protecting and managing virtual machines (VMs) and datastores.

The SnapCenter Plug-in for VMware vSphere provides the following capabilities in a unified interface, integrated with the vSphere client:

Policy-Based Snapshots - SnapCenter allows you to define policies for creating and managing application-consistent snapshots of virtual machines (VMs) in VMware vSphere.

Automation - Automated snapshot creation and management based on defined policies help ensure consistent and efficient data protection.

VM-Level Protection - Granular protection at the VM level allows for efficient management and recovery of individual virtual machines.

Storage Efficiency Features - Integration with NetApp storage technologies provides storage efficiency features like deduplication and compression for snapshots, minimizing storage requirements.

The SnapCenter Plug-in orchestrates the quiescing of virtual machines in conjunction with hardware-based snapshots on NetApp storage arrays. SnapMirror technology is utilized to replicate copies of backups to secondary storage systems including in the cloud.

For more information refer to the SnapCenter Plug-in for VMware vSphere documentation.

BlueXP integration enables 3-2-1 backup strategies that extend copies of data to object storage in the cloud.

For more information on 3-2-1 backup strategies with BlueXP visit 3-2-1 Data Protection for VMware with SnapCenter Plug-in and BlueXP backup and recovery for VMs.

NetApp Cloud Insights

NetApp Cloud Insights simplifies observation of on-prem and cloud infrastructure and provides analytics and troubleshooting capabilities to help solve complex problems. Cloud Insights works by collecting data from a data center environment and sending that data to the cloud. This is done with locally installed software called an Acquisition Unit and with specific collectors enabled for the assets in the data center.

The assets in Cloud Insights can be tagged with annotations that provide a method of organizing and classifying data. Dashboard can be created using a wide variety of widgets for displaying the data and Metric Queries can be created for detailed tabular views of data.

Cloud Insights comes with a large number of ready-made dashboards that help to zero in on specific types of problem areas and categories of data.

Cloud Insights is a heterogeneous tool designed to collect data from a wide range of devices. However, there is a library of templates, called ONTAP Essentials, that makes it easy for NetApp customers to get started quickly.

For detailed information on how to get started with Cloud Insights refer to the NetApp BlueXP and Cloud Insights landing page.

NetApp All-Flash SAN Array with VMware vSphere 8

The ONTAP Tools for VMware allows administrators to manage NetApp storage directly from within the vSphere Client. ONTAP Tools allows you to deploy and manage datastores, as well as provision vVol datastores.
ONTAP Tools allows mapping of datastores to storage capability profiles which determine a set of storage system attributes. This allows the creation of datastores with specific attributes such as storage performance and QoS.

Author: Josh Powell - NetApp Solutions Engineering

ONTAP Tools includes the following components:

Virtual Storage Console (VSC): The VSC includes the interface integrated with the vSphere client where you can add storage controllers, provision datastores, monitor performance of datastores, and view and update ESXi host settings.

VASA Provider: The VMware vSphere APIs for Storage Awareness (VASA) Provider for ONTAP send information about storage used by VMware vSphere to the vCenter Server, enabling provisioning of VMware Virtual Volumes (vVols) datastores, creation and use of storage capability profiles, compliance verification, and performance monitoring.

Storage Replication Adapter (SRA): When enabled and used with VMware Site Recovery Manager (SRM), SRA facilitates the recovery of vCenter Server datastores and virtual machines in the event of a failure, allowing configuration of protected sites and recovery sites for disaster recovery.

For more information on NetApp ONTAP tools for VMware see ONTAP tools for VMware vSphere Documentation.

Solution Deployment Overview

In this solution we will demonstrate the use of the ONTAP Tools for VMware vSphere to provision a VMware Virtual Volumes (vVol) datastores and create a virtual machine on a vVol datastore.

In a vVols datastore each virtual disk is a vVol and becomes a native LUN object on the storage system. The integration of the storage system and vSphere takes place through the VMware API's for Storage Awareness (VASA) provider (installed with ONTAP Tools) and allows the storage system to be aware of the VM data and manage it accordingly. Storage policies, defined in the vCenter Client are used to allocate and manage storage resources.

For detailed information on vVols with ONTAP refer to Virtual Volumes vVols) with ONTAP.

This solution covers the following high level steps:

1. Add a storage system in ONTAP Tools.
2. Create a storage capability profile in ONTAP Tools.
3. Create a vVols datastore in ONTAP Tools.
4. Create a VM storage policy in the vSphere client.
5. Create a new virtual machine on the vVol datastore.

Prerequisites

The following components were used in this solution:

1. NetApp All-Flash SAN Array A400 with ONTAP 9.13.
2. iSCSI SVM created on the ASA with network connectivity to the ESXi hosts.
3. ONTAP Tools for VMware vSphere 9.13 (VASA provider enabled by default).
4. vSphere 8.0 cluster (vCenter appliance, and ESXi hosts).

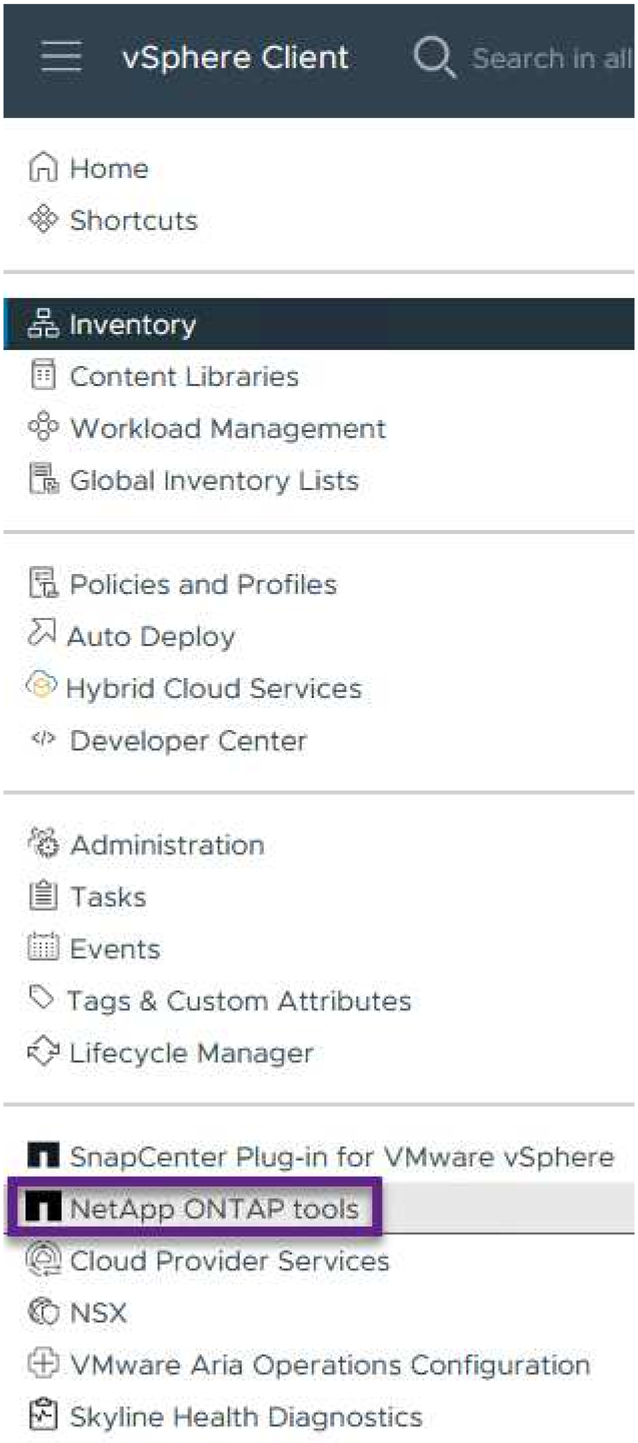
Solution Deployment

Create a vVols datastore in ONTAP Tools

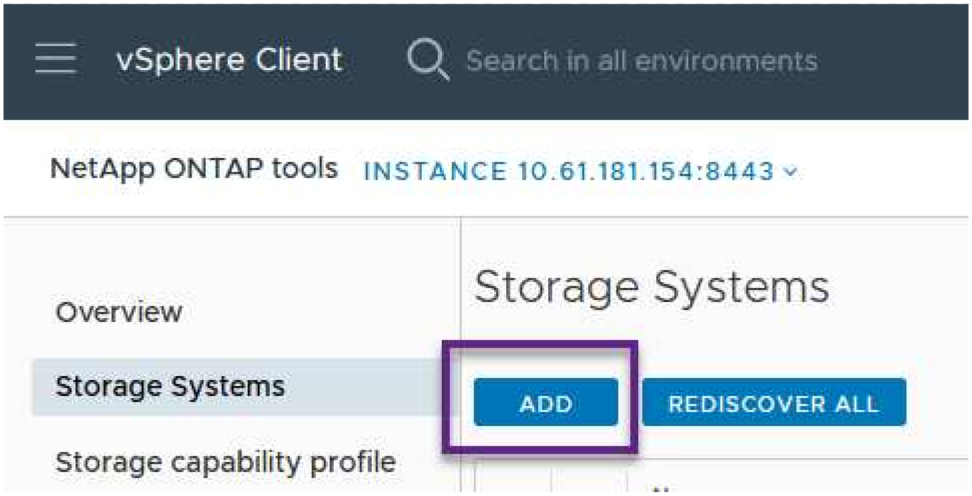
To create a vVols datastore in ONTAP Tools complete the following steps:

Add a storage system to ONTAP Tools.

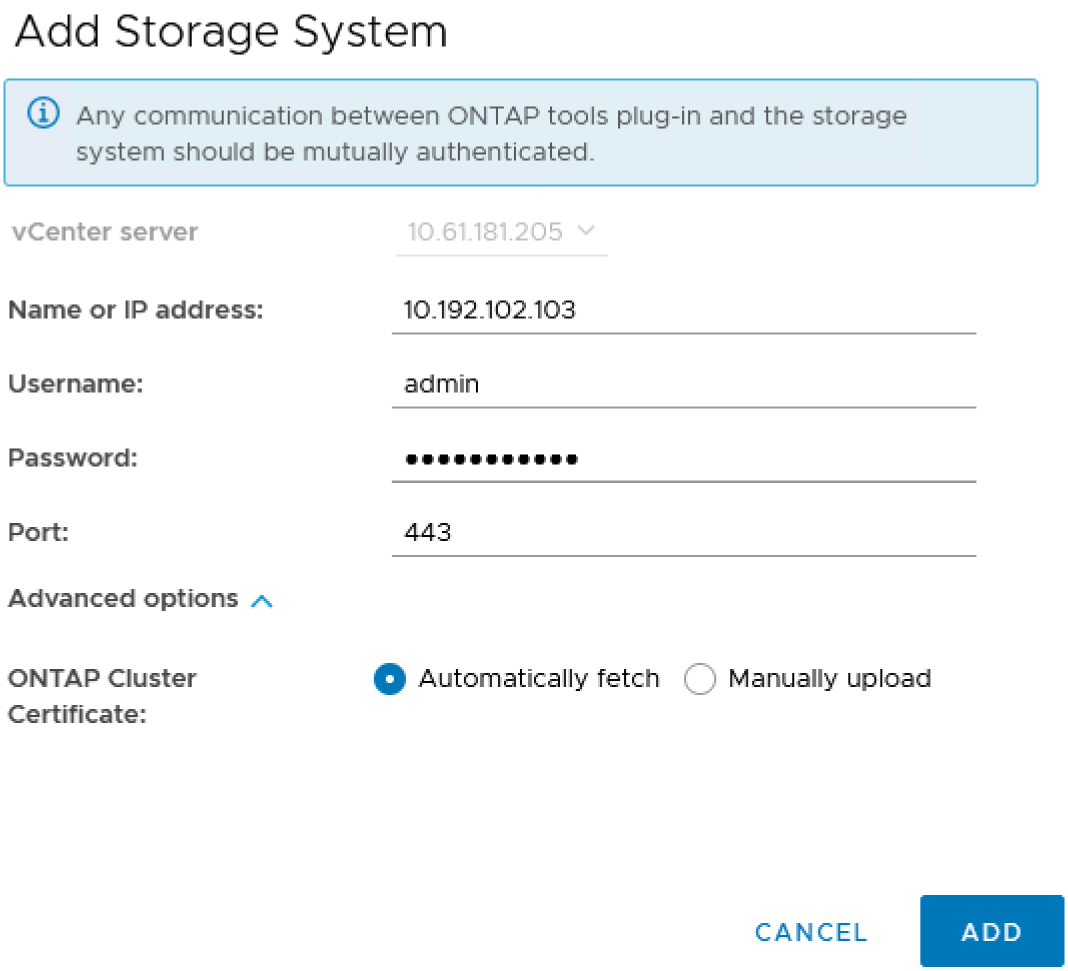
1. Access NetApp ONTAP Tools by selecting it from the main menu in the vSphere client.



2. In ONTAP Tools select **Storage Systems** from the left hand menu and then press **Add**.



3. Fill out the IP Address, credentials of the storage system and the port number. Click on **Add** to start the discovery process.



Add Storage System

Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server: 10.61.181.205

Name or IP address: 10.192.102.103

Username: admin

Password: ●●●●●●●●●●●●

Port: 443

Advanced options

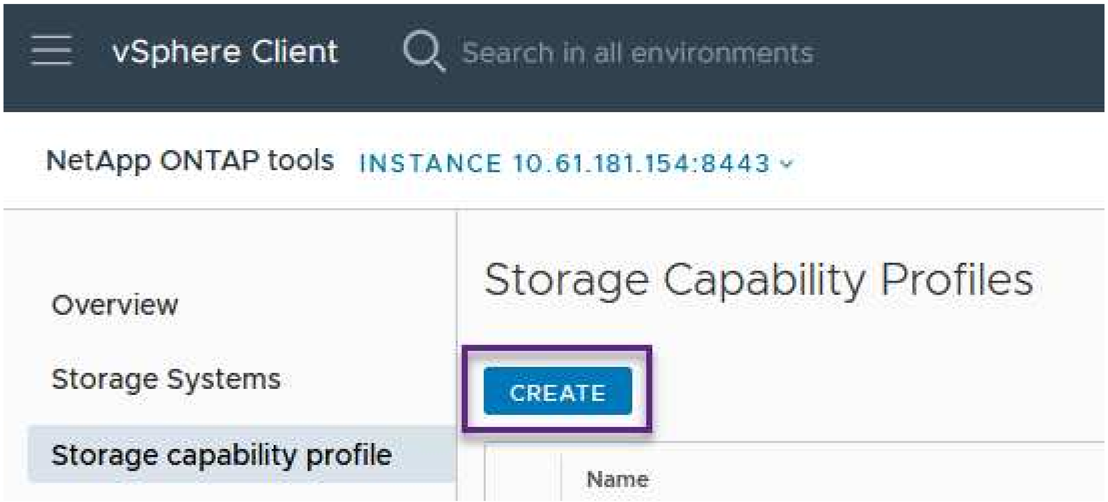
ONTAP Cluster Certificate: ● Automatically fetch ○ Manually upload

Create a storage capability profile in ONTAP Tools

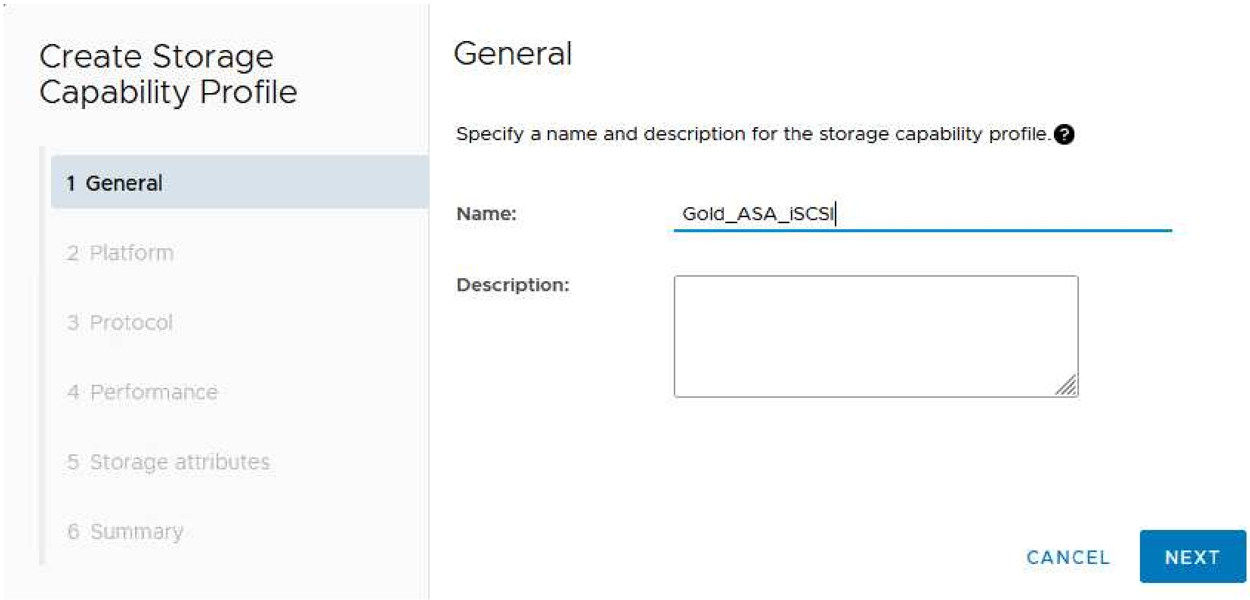
Storage capability profiles describe the features provided by a storage array or storage system. They include quality of service definitions and are used to select storage systems that meet the parameters defined in the profile.

To create a storage capability profile in ONTAP Tools complete the following steps:

1. In ONTAP Tools select **Storage capability profile** from the left hand menu and then press **Create**.


vSphere Client
Search in all environments
NetApp ONTAP tools
INSTANCE 10.61.181.154:8443
Overview
Storage Systems
Storage capability profile
Storage Capability Profiles
CREATE
Name

2. In the **Create Storage Capability profile** wizard provide a name and description of the profile and click on **Next**.

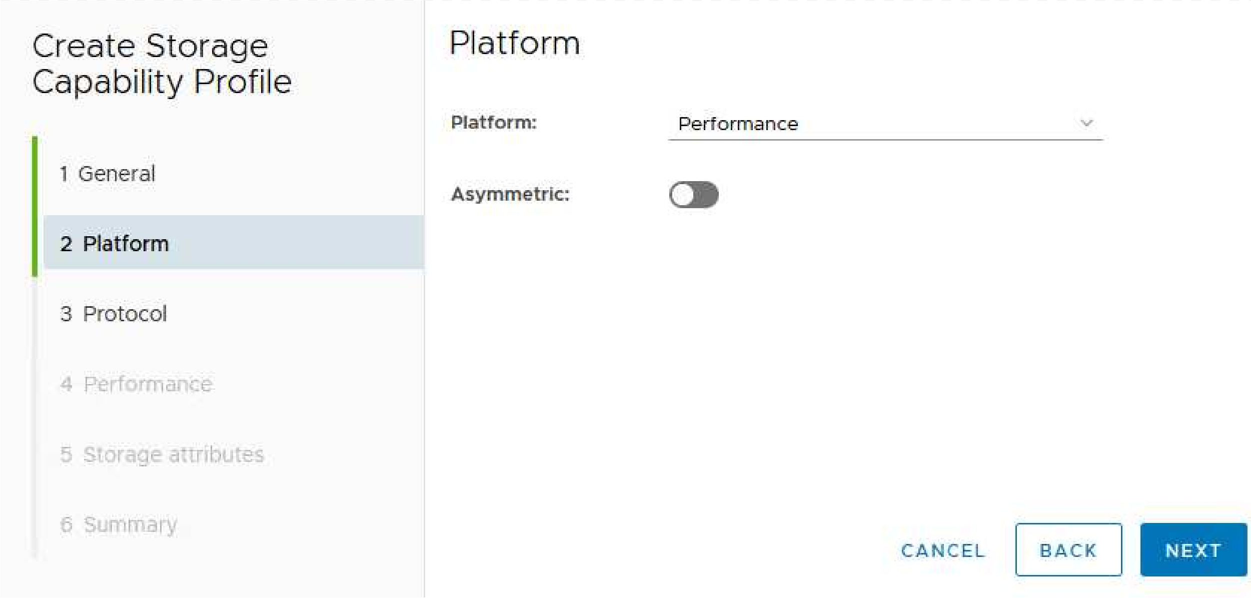


Specify a name and description for the storage capability profile.

Name: Gold_ASA_iSCSI

Description:

3. Select the platform type and to specify the storage system is to be an All-Flash SAN Array set **Asymmetric** to false.



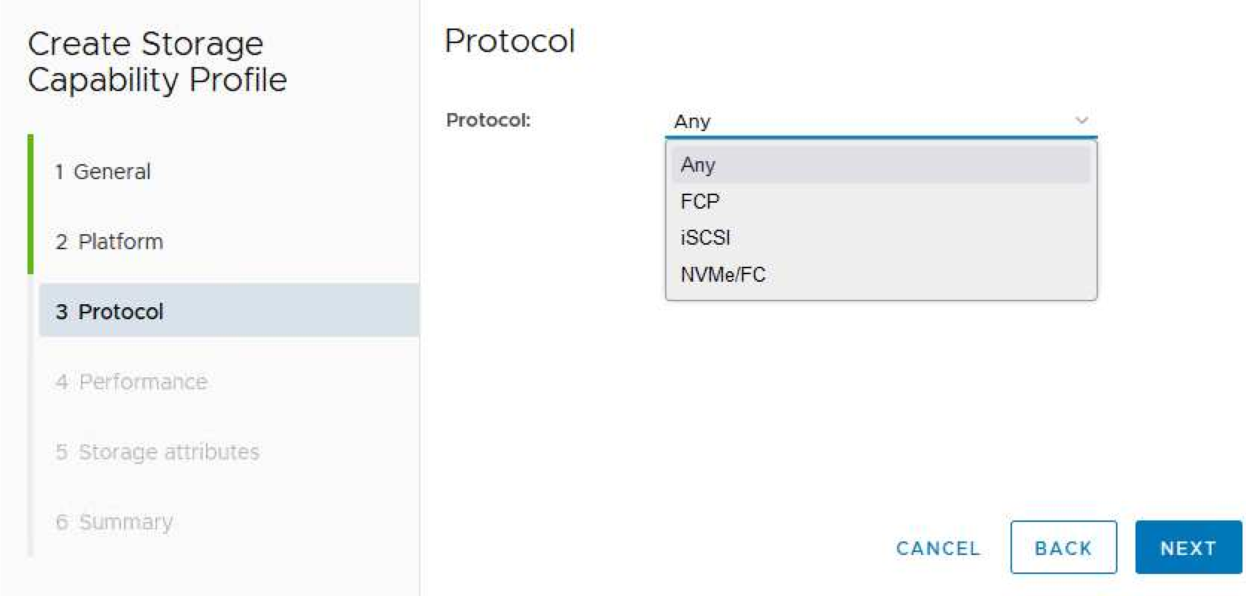
Create Storage Capability Profile

Platform

Platform: Performance

Asymmetric:

4. Next, select choice of protocol or **Any** to allow all possible protocols. Click **Next** to continue.

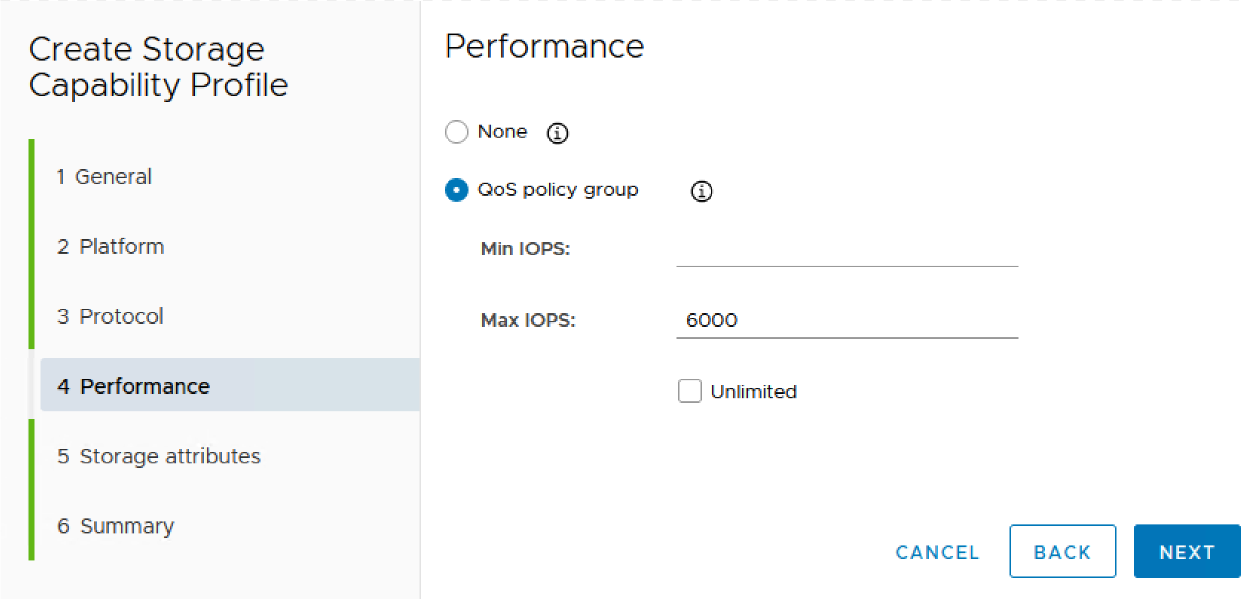


Create Storage Capability Profile

Protocol

Protocol: Any

5. The **performance** page allows setting of quality of service in form of minimum and maximum IOPs allowed.


Create Storage Capability Profile

1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary

Performance

○ None ⓘ

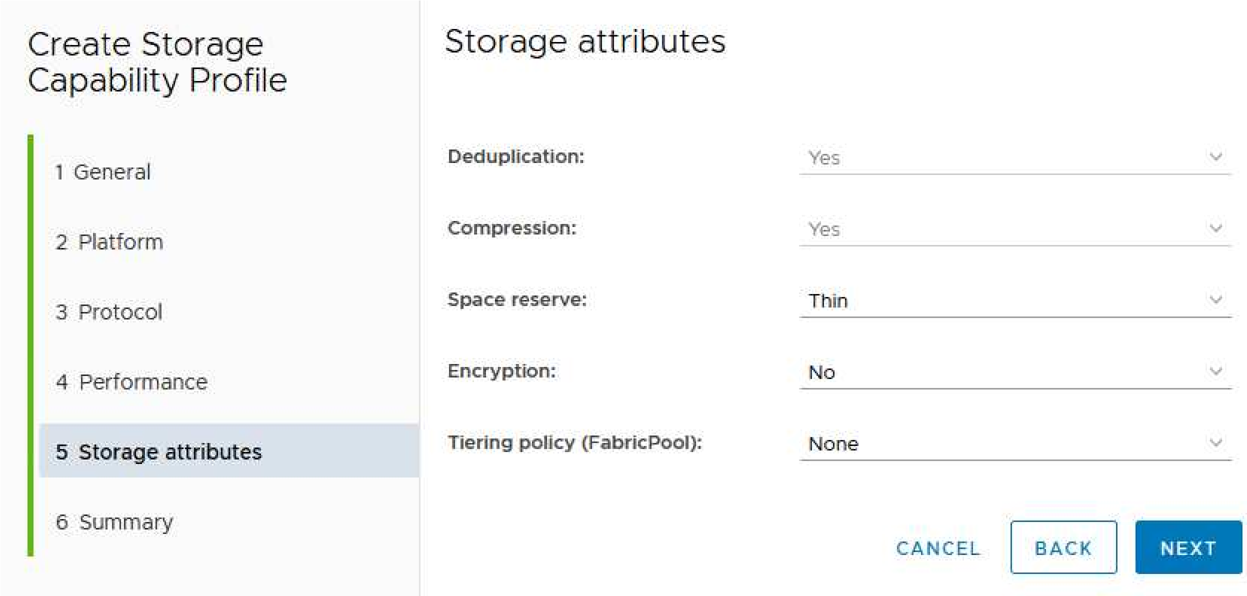
● QoS policy group ⓘ

Min IOPS:

Max IOPS: 6000

□ Unlimited

6. Complete the **storage attributes** page selecting storage efficiency, space reservation, encryption and any tiering policy as needed.


Create Storage Capability Profile

1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary

Storage attributes

Deduplication: Yes

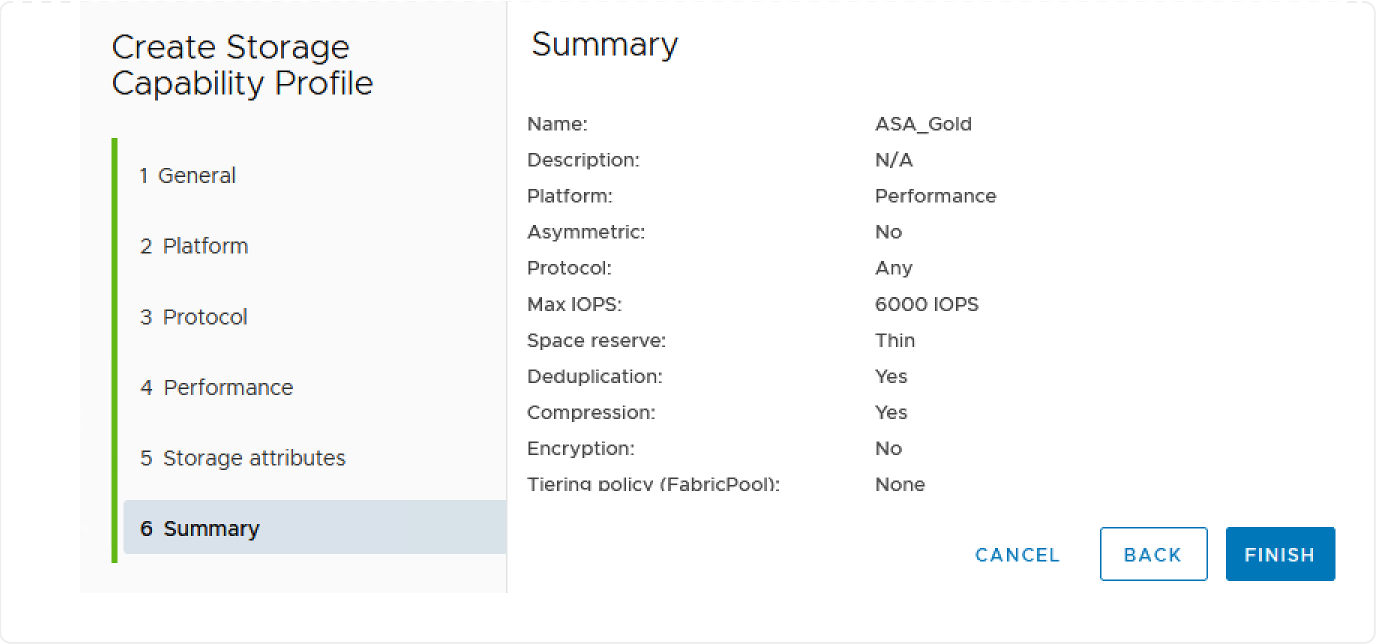
Compression: Yes

Space reserve: Thin

Encryption: No

Tiering policy (FabricPool): None

7. Finally, review the summary and click on Finish to create the profile.



Create Storage Capability Profile

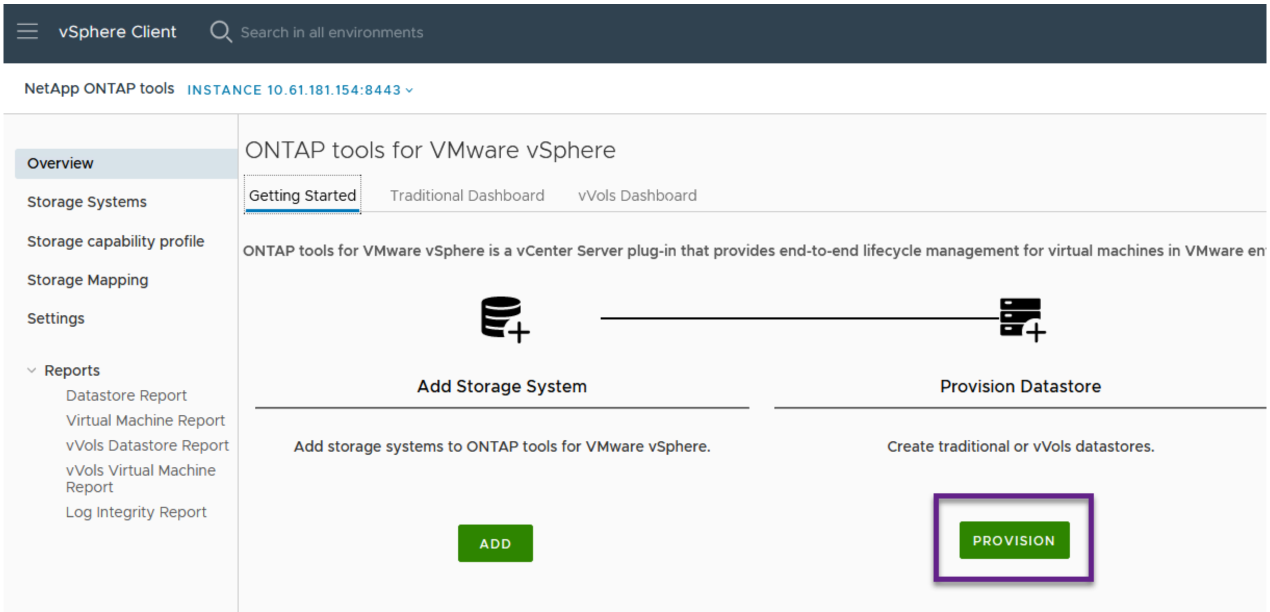
Summary

Name:	ASA_Gold
Description:	N/A
Platform:	Performance
Asymmetric:	No
Protocol:	Any
Max IOPS:	6000 IOPS
Space reserve:	Thin
Deduplication:	Yes
Compression:	Yes
Encryption:	No
Tiering policy (FabricPool):	None

Create a vVols datastore in ONTAP Tools

To create a vVols datastore in ONTAP Tools complete the following steps:

1. In ONTAP Tools select **Overview** and from the **Getting Started** tab click on **Provision** to start the wizard.

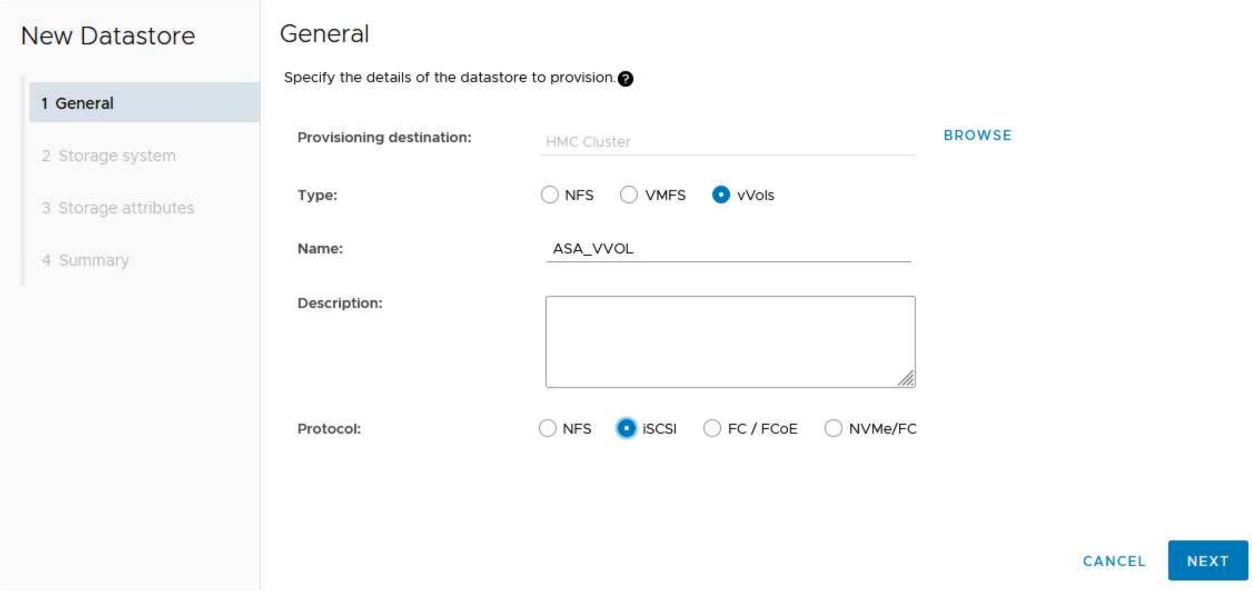


ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware en

Add storage systems to ONTAP tools for VMware vSphere.

Create traditional or vVols datastores.

2. On the **General** page of the New Datastore wizard select the vSphere datacenter or cluster destination. Select **vVols** as the dastatore type, fill out a name for the datastore, and select the protocol.



Specify the details of the datastore to provision.

Provisioning destination: HMC Cluster

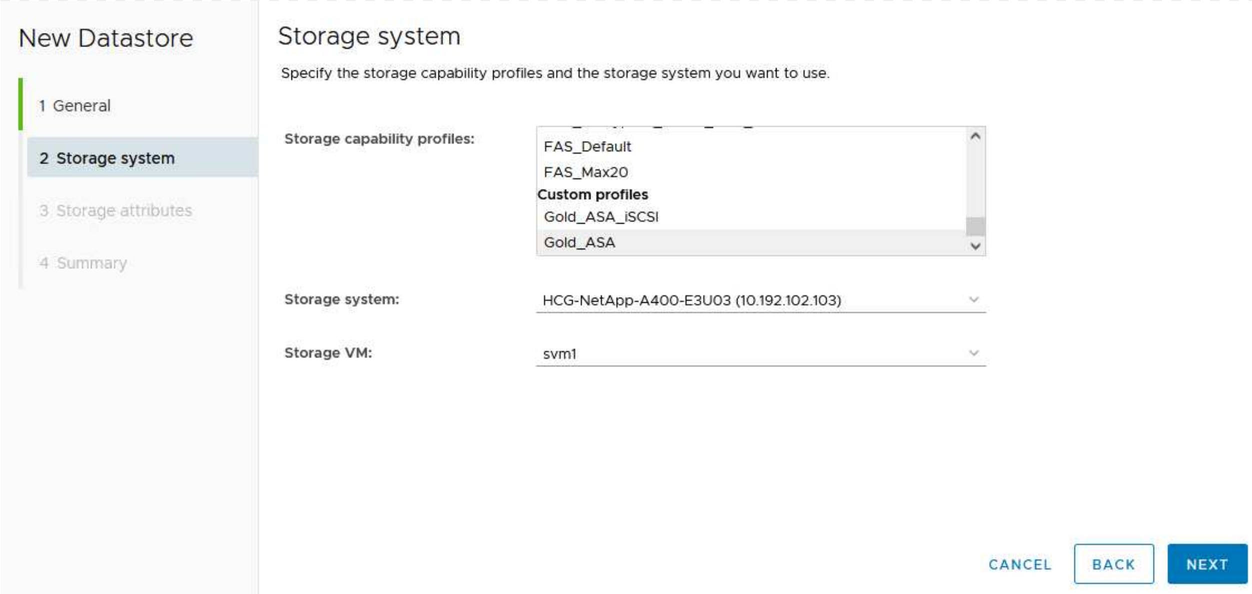
Type: ○ NFS ○ VMFS ● vVols

Name: ASA_VVOL

Description:

Protocol: ○ NFS ● iSCSI ○ FC / FCoE ○ NVMe/FC

3. On the **Storage system** page select the select a storage capability profile, the storage system and SVM. Click on **Next** to continue.



Storage system

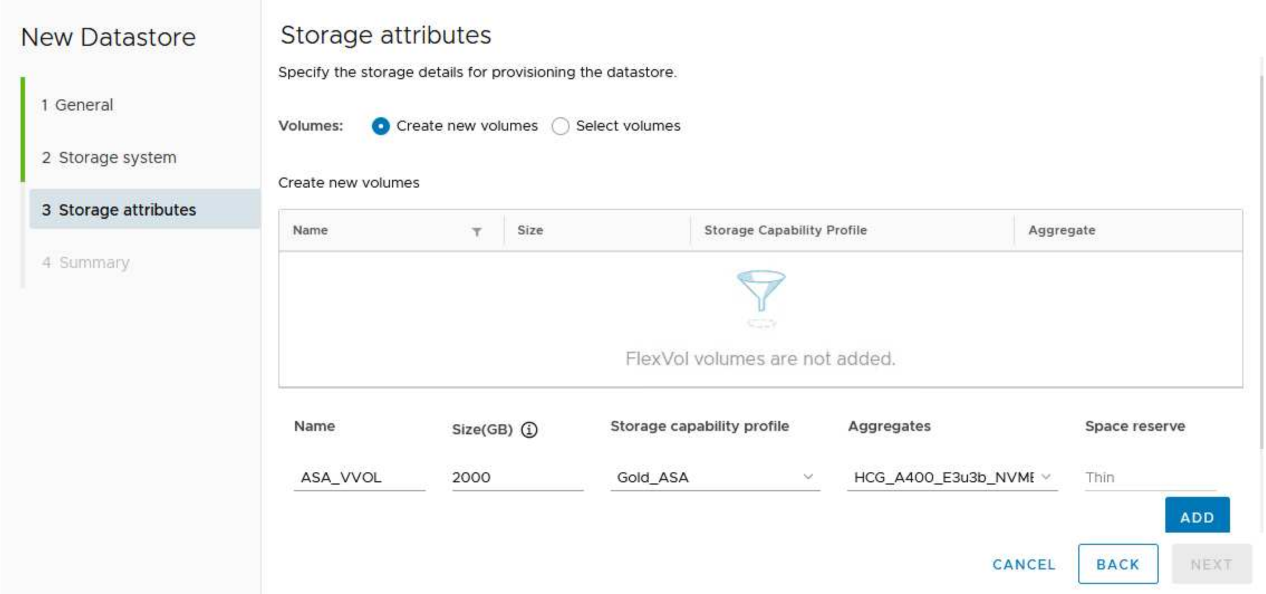
Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles: FAS_Default, FAS_Max20, Custom profiles, Gold_ASA_iSCSI, Gold_ASA

Storage system: HCG-NetApp-A400-E3U03 (10.192.102.103)

Storage VM: svm1

4. On the **Storage attributes** page select to create a new volume for the datastore and fill out the storage attributes of the volume to be created. Click on **Add** to create the volume and then **Next** to continue.



Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: ● Create new volumes ○ Select volumes

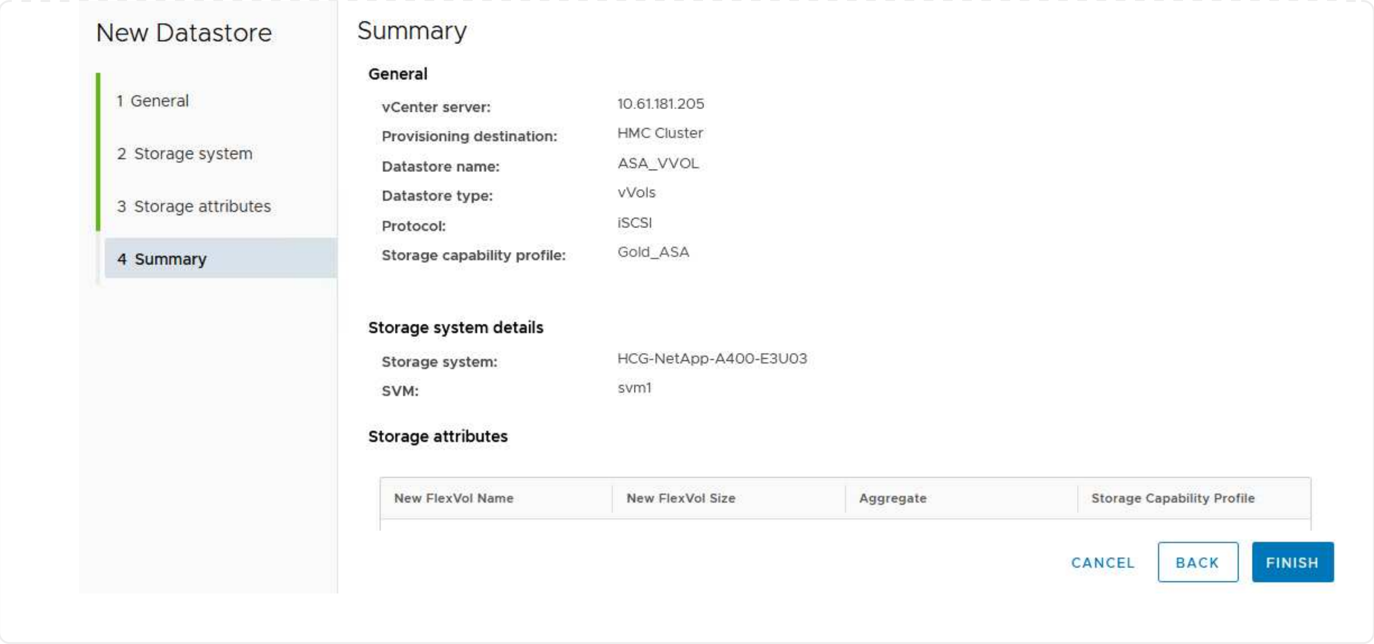
Create new volumes

Name	Size	Storage Capability Profile	Aggregate

FlexVol volumes are not added.

Name	Size(GB)	Storage capability profile	Aggregates	Space reserve
ASA_VVOL	2000	Gold_ASA	HCG_A400_E3u3b_NVME	Thin

5. Finally, review the summary and click on **Finish** to start the vVol datastore creation process.



Summary

General

vCenter server: 10.61.181.205
Provisioning destination: HMC Cluster
Datastore name: ASA_VVOL
Datastore type: vVols
Protocol: iSCSI
Storage capability profile: Gold_ASA

Storage system details

Storage system: HCG-NetApp-A400-E3U03
SVM: svm1

Storage attributes

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile

Create a VM storage policy in the vSphere client

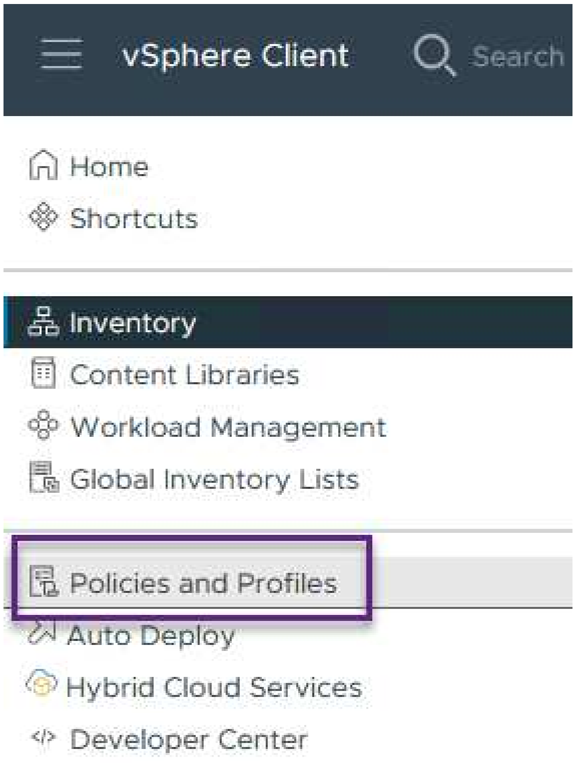
A VM storage policy is a set of rules and requirements that define how virtual machine (VM) data should be stored and managed. It specifies the desired storage characteristics, such as performance, availability, and data services, for a particular VM.

In this case, the task involves creating a VM storage policy to specify that a virtual machine will be generated on vVol datastores and to establish a one-to-one mapping with the previously generated storage capability profile.

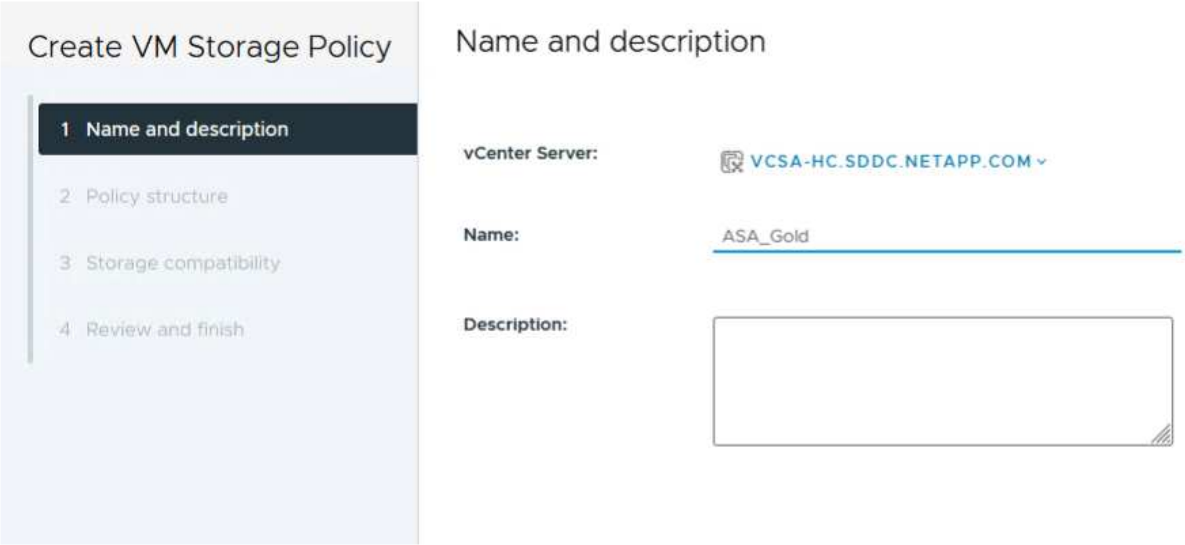
Create a VM storage policy

To create a VM storage policy complete the following steps:

1. From the vSphere clients main menu select **Policies and Profiles**.



2. In the **Create VM Storage Policy** wizard, first fill out a name and description for the policy and click on **Next** to continue.



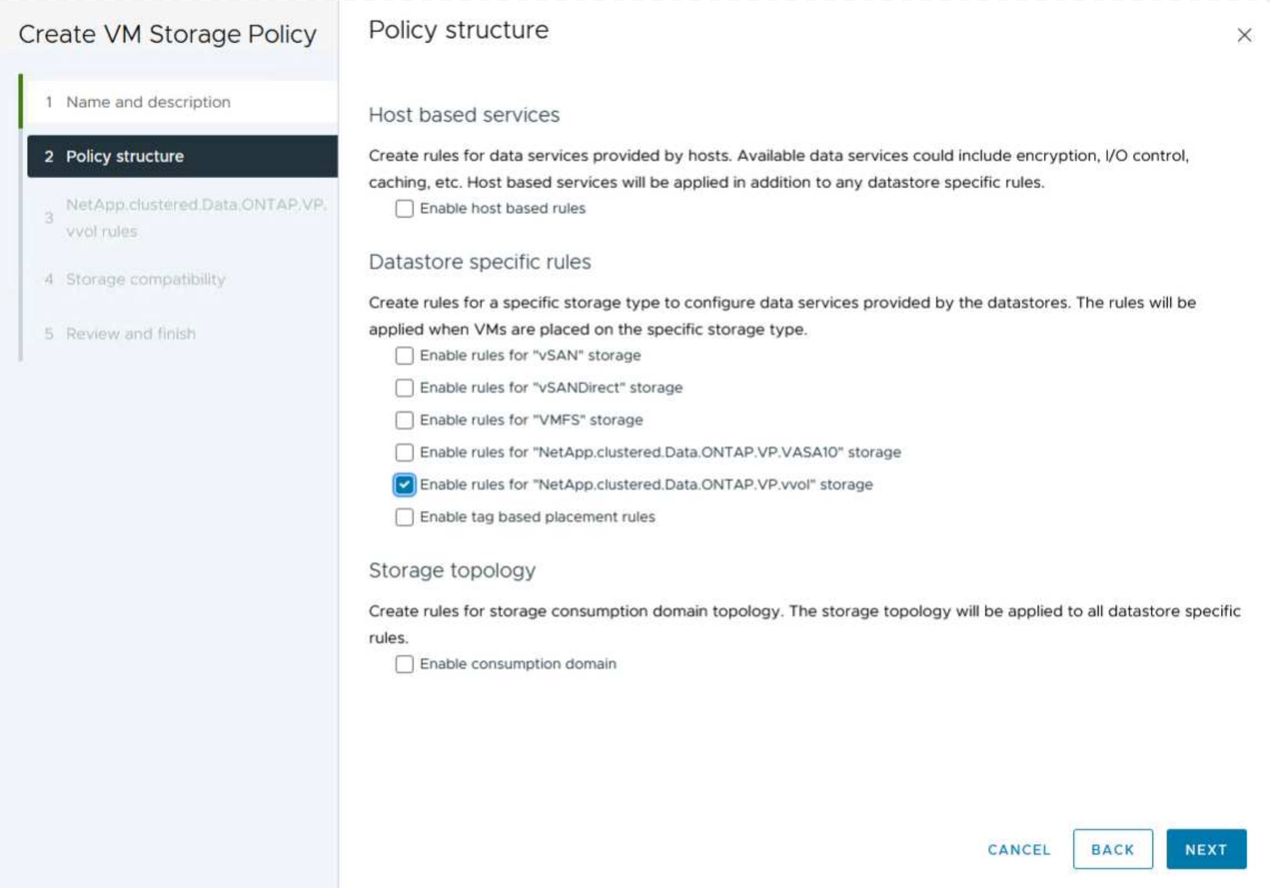
Name and description

vCenter Server: VCSA-HC.SDDC.NETAPP.COM

Name: ASA_Gold

Description:

3. On the **Policy structure** page select to enable rules for NetApp clustered data ontap vVol storage and click on **Next**.



Create VM Storage Policy

1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish

Policy structure

Host based services

Create rules for data services provided by hosts. Available data services could include encryption, I/O control, caching, etc. Host based services will be applied in addition to any datastore specific rules.

□ Enable host based rules

Datastore specific rules

Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.

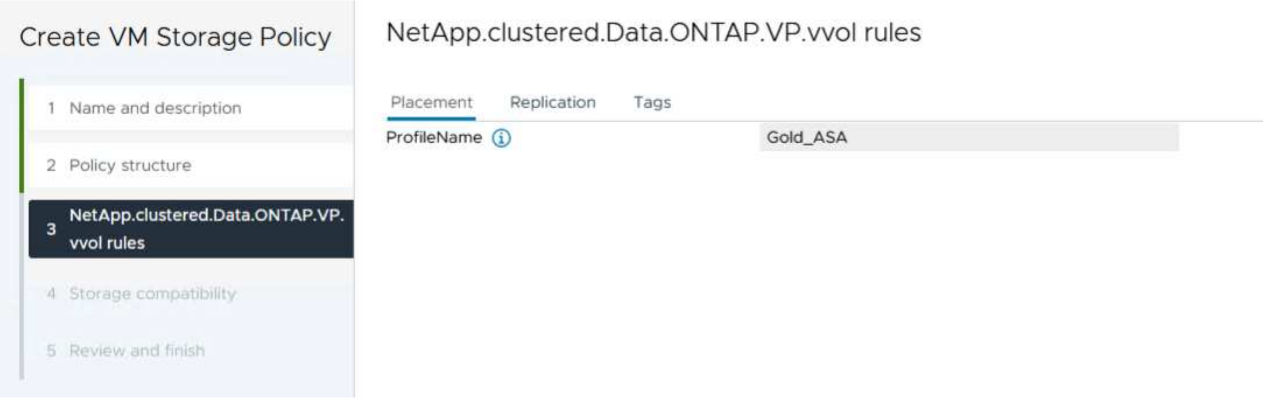
□ Enable rules for "vSAN" storage
□ Enable rules for "vSANDirect" storage
□ Enable rules for "VMFS" storage
□ Enable rules for "NetApp.clustered.Data.ONTAP.VP.VASA10" storage
☑ Enable rules for "NetApp.clustered.Data.ONTAP.VP.vvol" storage
□ Enable tag based placement rules

Storage topology

Create rules for storage consumption domain topology. The storage topology will be applied to all datastore specific rules.

□ Enable consumption domain

4. On the next page specific to the policy structure chosen, select the storage capability profile that describes the storage system(s) to be used in the VM storage policy. Click on **Next** to continue.



Create VM Storage Policy

1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish

NetApp.clustered.Data.ONTAP.VP.vvol rules

ProfileName: Gold_ASA

5. On the **Storage compatibility** page, review the list of vSAN datastores that match this policy and click **Next**.
6. Finally, review the policy to be implemented and click on **Finish** to create the policy.

Create a VM storage policy in the vSphere client

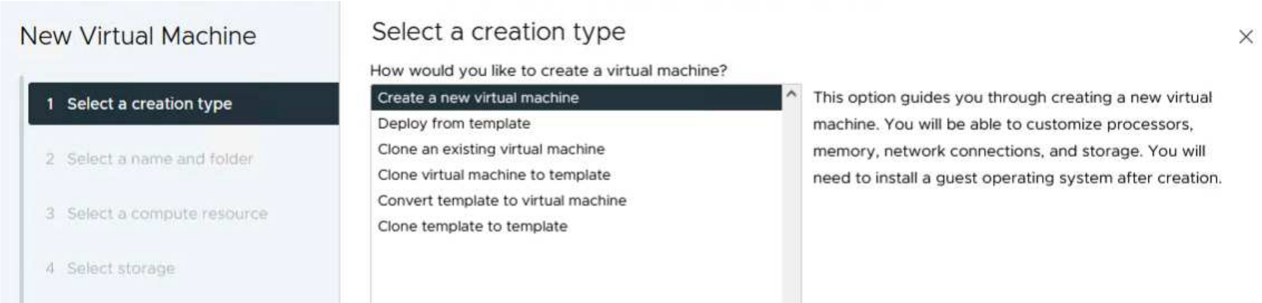
A VM storage policy is a set of rules and requirements that define how virtual machine (VM) data should be stored and managed. It specifies the desired storage characteristics, such as performance, availability, and data services, for a particular VM.

In this case, the task involves creating a VM storage policy to specify that a virtual machine will be generated on vVol datastores and to establish a one-to-one mapping with the previously generated storage capability profile.

Create a virtual machine on a vVol datastore

The final step is to create a virtual machine using the VM storage policies previously created:

1. From the **New Virtual Machine** wizard select **Create a new virtual machine** and select **Next** to continue.



New Virtual Machine

1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage

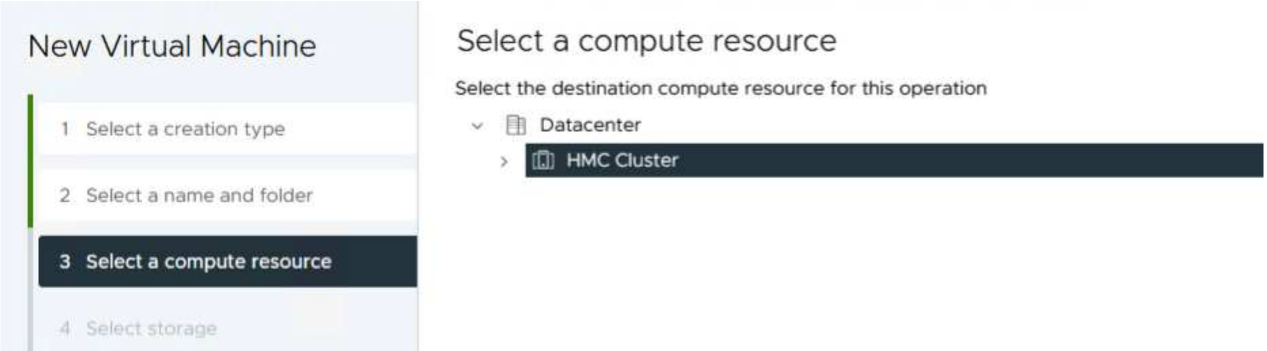
Select a creation type

How would you like to create a virtual machine?

- Create a new virtual machine
- Deploy from template
- Clone an existing virtual machine
- Clone virtual machine to template
- Convert template to virtual machine
- Clone template to template

This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.

2. Fill in a name and select a location for the virtual machine and click on **Next**.
3. On the **Select a compute resource** page select a destination and click on **Next**.



New Virtual Machine

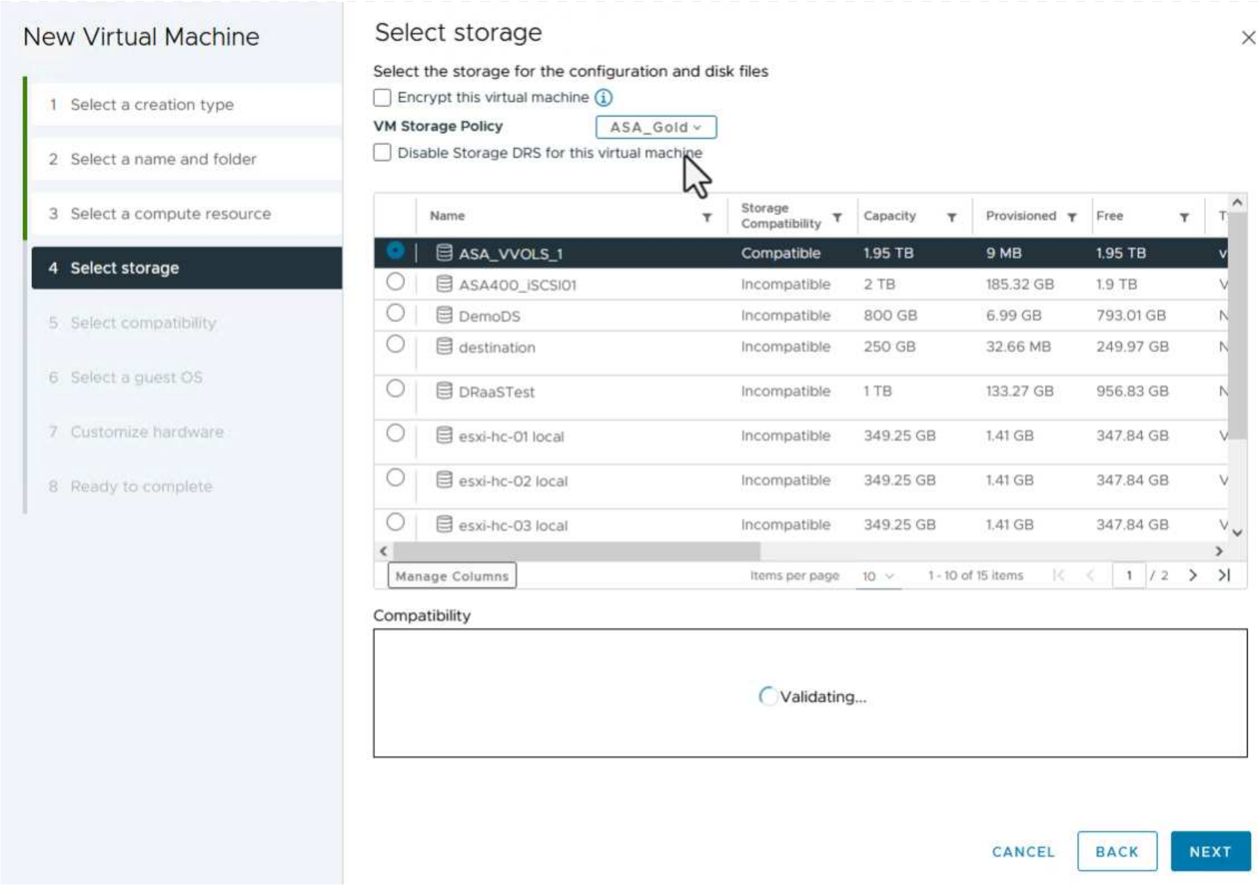
1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage

Select a compute resource

Select the destination compute resource for this operation

- Datacenter
  - HMC Cluster

4. On the **Select storage** page select a VM Storage Policy and the vVols datastore that will be the destination for the VM. Click on **Next**.



New Virtual Machine

1 Select a creation type

2 Select a name and folder

3 Select a compute resource

4 Select storage

5 Select compatibility

6 Select a guest OS

7 Customize hardware

8 Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine

VM Storage Policy: ASA_Gold

☐ Disable Storage DRS for this virtual machine

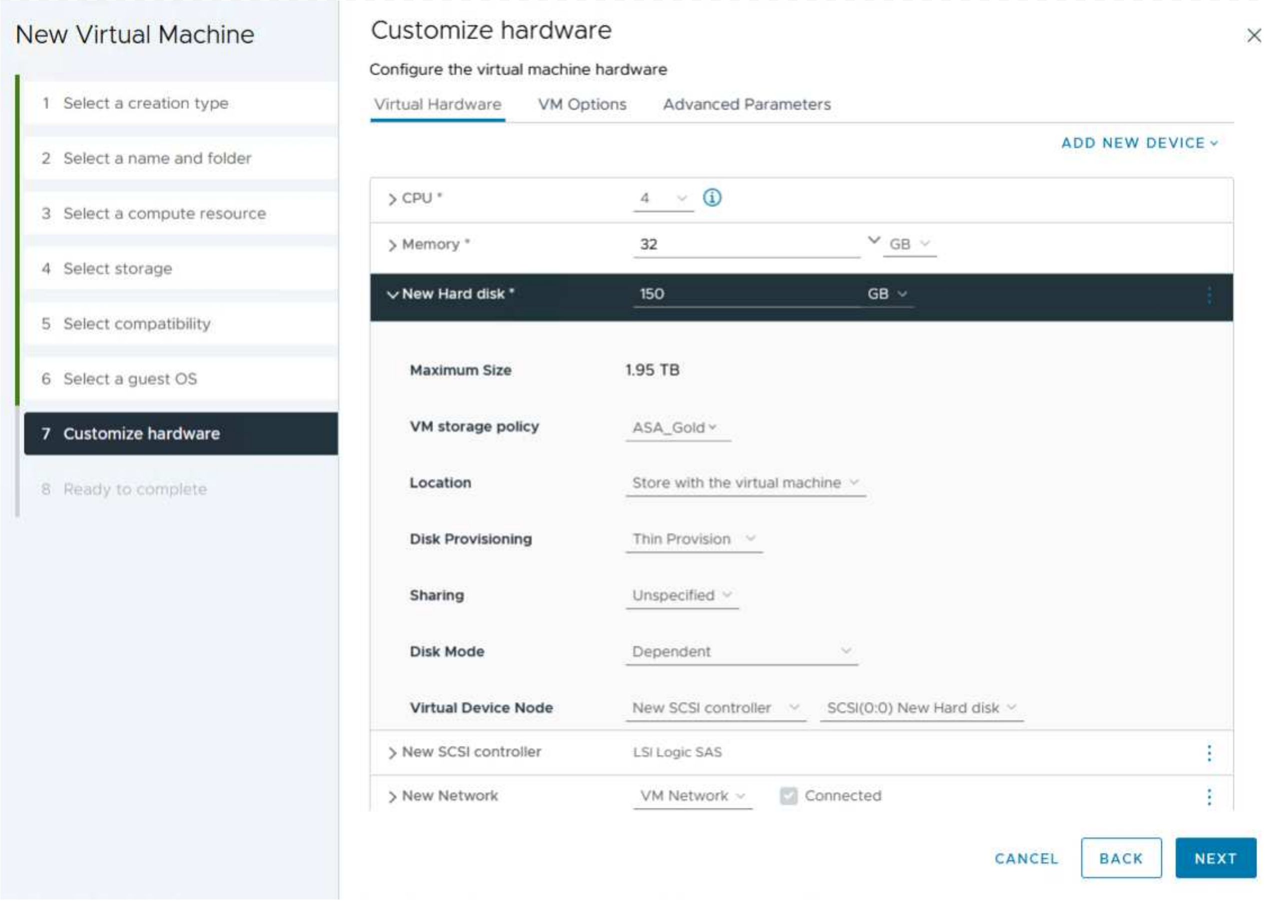
	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	ASA_VVOLS_1	Compatible	1.95 TB	9 MB	1.95 TB	v
○	ASA400_iSCSI01	Incompatible	2 TB	185.32 GB	1.9 TB	V
○	DemoDS	Incompatible	800 GB	6.99 GB	793.01 GB	N
○	destination	Incompatible	250 GB	32.66 MB	249.97 GB	N
○	DRaaSTest	Incompatible	1 TB	133.27 GB	956.83 GB	N
○	esxi-hc-01 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	V
○	esxi-hc-02 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	V
○	esxi-hc-03 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	V

Manage Columns   Items per page 10   1 - 10 of 15 items   1 / 2

Compatibility

Validating...

5. On the **Select compatibility** page choose the vSphere version(s) that the VM will be compatible with.
6. Select the guest OS family and version for the new VM and click on **Next**.
7. Fill out the **Customize hardware** page. Note that a separate VM storage policy can be selected for each hard disk (VMDK file).



Customize hardware

Configure the virtual machine hardware

CPU *: 4

Memory *: 32 GB

New Hard disk *: 150 GB

Maximum Size: 1.95 TB

VM storage policy: ASA_Gold

Location: Store with the virtual machine

Disk Provisioning: Thin Provision

Sharing: Unspecified

Disk Mode: Dependent

Virtual Device Node: New SCSI controller, SCSI(0:0) New Hard disk

New SCSI controller: LSI Logic SAS

New Network: VM Network ☑ Connected

8. Finally, review the summary page and click on **Finish** to create the VM.

In summary, NetApp ONTAP Tools automates the process of creating vVol datastores on ONTAP storage systems. Storage capability profiles define not only the storage systems to be used for datastore creation but also dictate QoS policies that can be implemented on an individual VMDK basis. vVols provide a simplified storage management paradigm and tight integration between NetApp and VMware make this a practical solution for streamlined, efficient, and granular control over virtualized environments.

NetApp All-Flash SAN Array with VMware vSphere 8

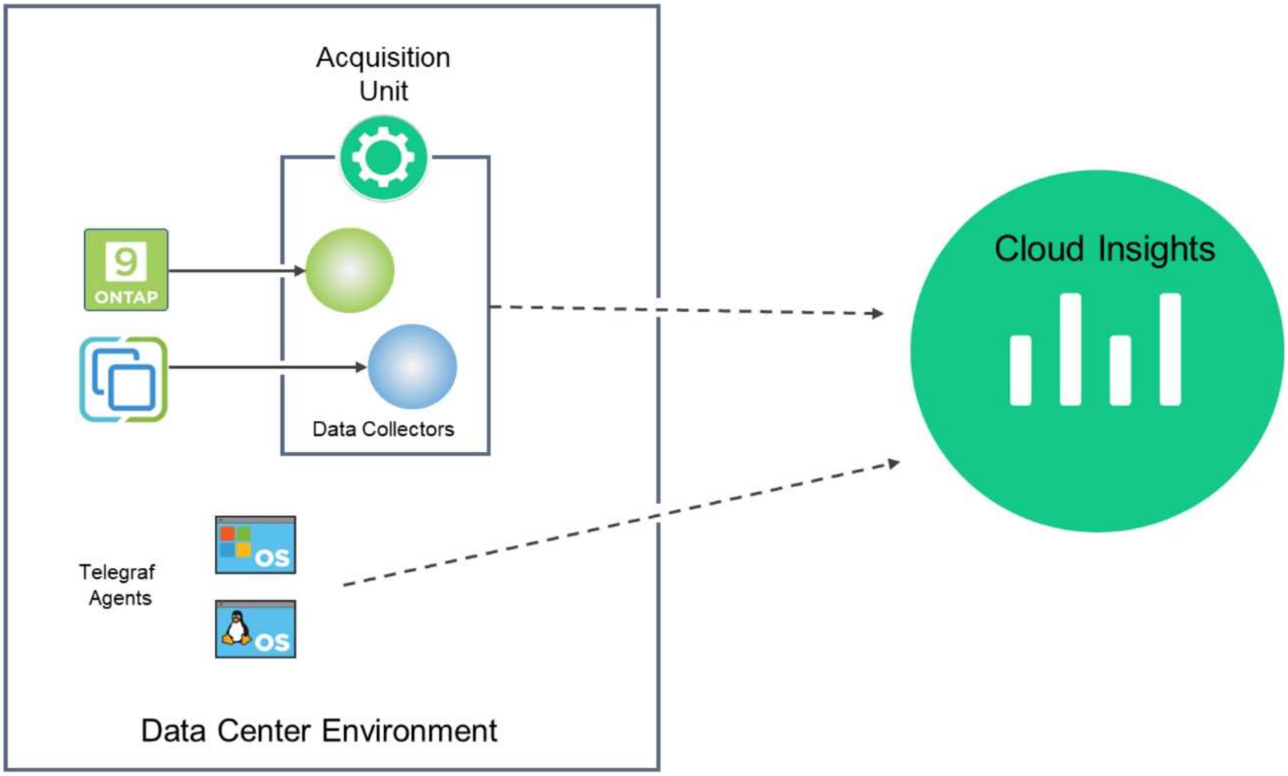
NetApp Cloud Insights is a cloud-based infrastructure monitoring and analytics platform designed to provide comprehensive visibility and insights into the performance, health, and costs of IT infrastructures, both on-premises and in the cloud. Key features of NetApp Cloud Insights include real-time monitoring, customizable dashboards, predictive analytics, and cost optimization tools, allowing organizations to effectively manage and optimize their on-premises and cloud environments.

Author: Josh Powell - NetApp Solutions Engineering

Monitoring On-Premises Storage with NetApp Cloud Insights

NetApp Cloud Insights operates through Acquisition Unit software, which is set up with data collectors for assets such as VMware vSphere and NetApp ONTAP storage systems. These collectors gather data and transmit it to Cloud Insights. The platform then utilizes a variety of dashboards, widgets, and metric queries to organize the data into insightful analyses for users to interpret.

Cloud Insights architecture diagram:



Solution Deployment Overview

This solution provides an introduction to monitoring on-premises VMware vSphere and ONTAP storage systems using NetApp Cloud Insights.

This list provides the high level steps covered in this solution:

1. Configure Data Collector for a vSphere cluster.
2. Configure Data Collector for an ONTAP storage system.
3. Use Annotation Rules to tag assets.
4. Explore and correlate assets.
5. Use a Top VM Latency dashboard to isolate noisy neighbors.
6. Identify opportunities to rightsize VMs.
7. Use queries to isolate and sort metrics.

Prerequisites

This solution uses the following components:

1. NetApp All-Flash SAN Array A400 with ONTAP 9.13.
2. VMware vSphere 8.0 cluster.
3. NetApp Cloud Insights account.

4. NetApp Cloud Insights Acqusition Unit software installed on a local VM with network connectivity to assets for data collection.

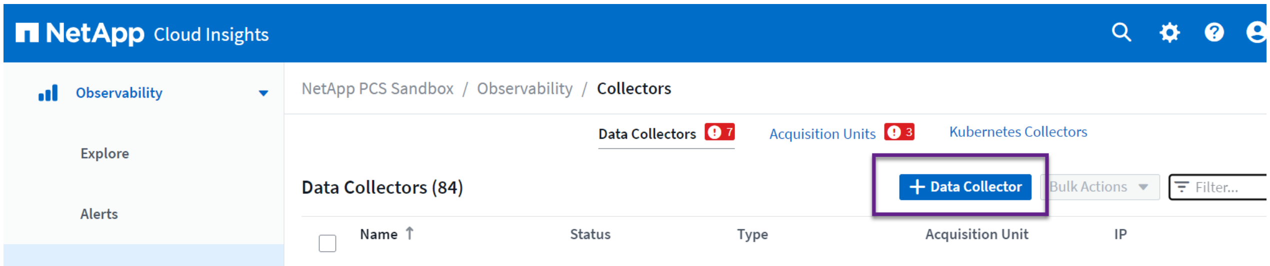
Solution Deployment

Configure Data Collectors

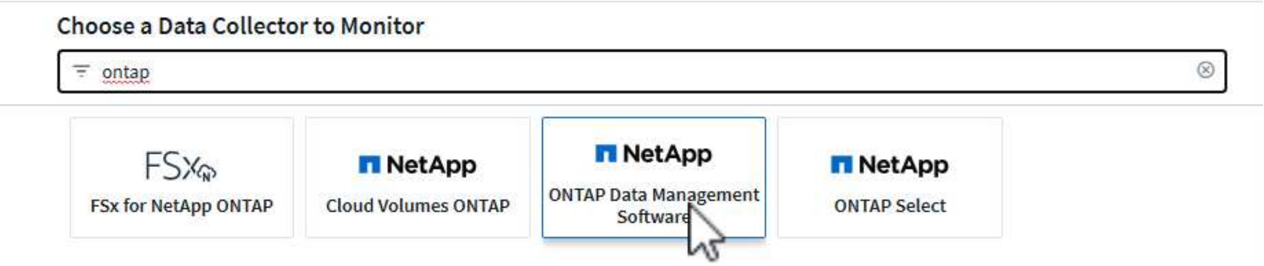
To configure Data Collectors for VMware vSphere and ONTAP storage systems complete the following steps:

Add a Data Collector for an ONTAP storage systems

1. Once logged into Cloud Insights, navigate to **Observability > Collectors > Data Collectors** and press the button to install a new Data Collector.

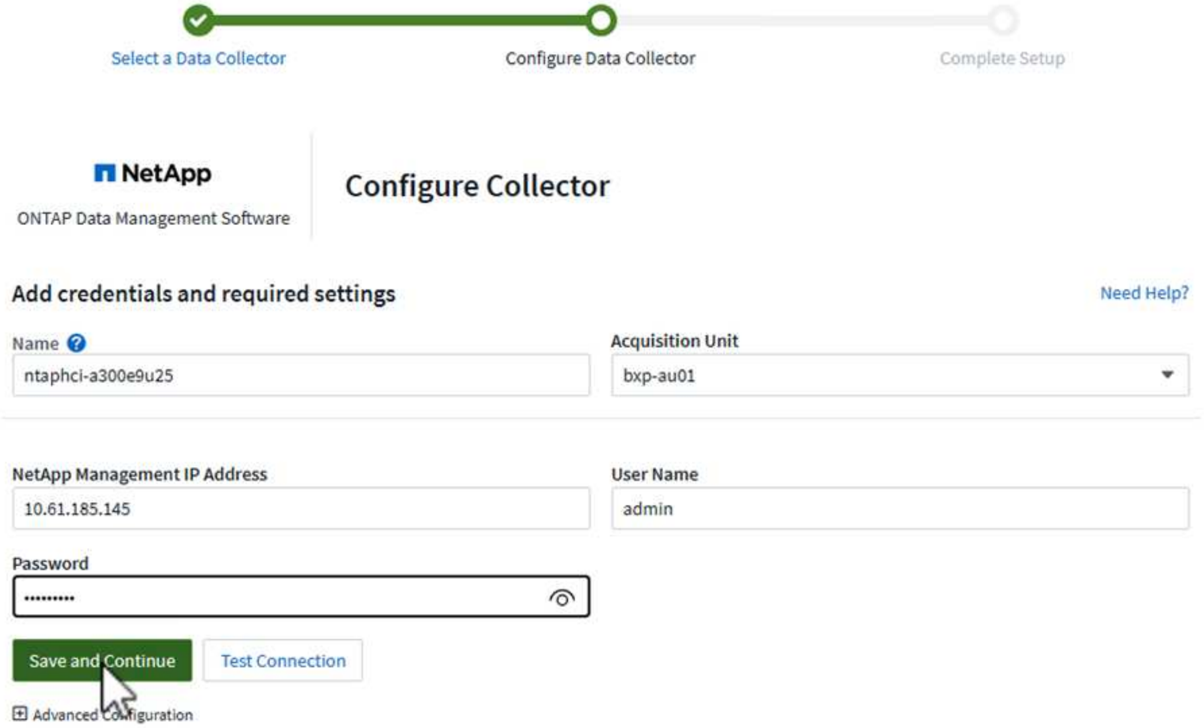


2. From here search for **ONTAP** and click on **ONTAP Data Management Software**.



ontap

3. On the **Configure Collector** page fill out a name for the collector, specify the correct **Acquisition Unit** and provide the credentials for the ONTAP storage system. Click on **Save and Continue** and then **Complete Setup** at the bottom of the page to complete the configuration.



Name: ntaphci-a300e9u25

Acquisition Unit: bxp-au01

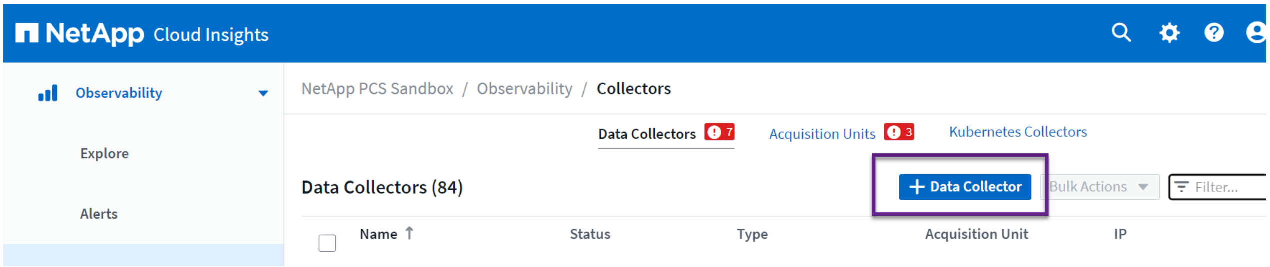
NetApp Management IP Address: 10.61.185.145

User Name: admin

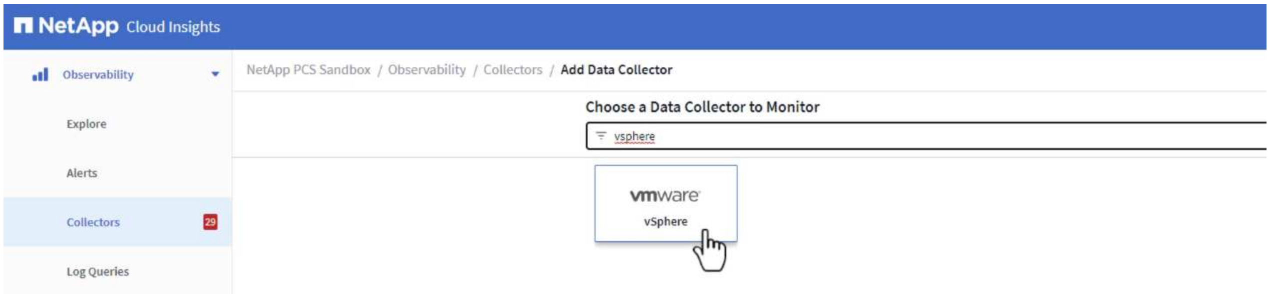
Password: •••••••••

Add a Data Collector for a VMware vSphere cluster

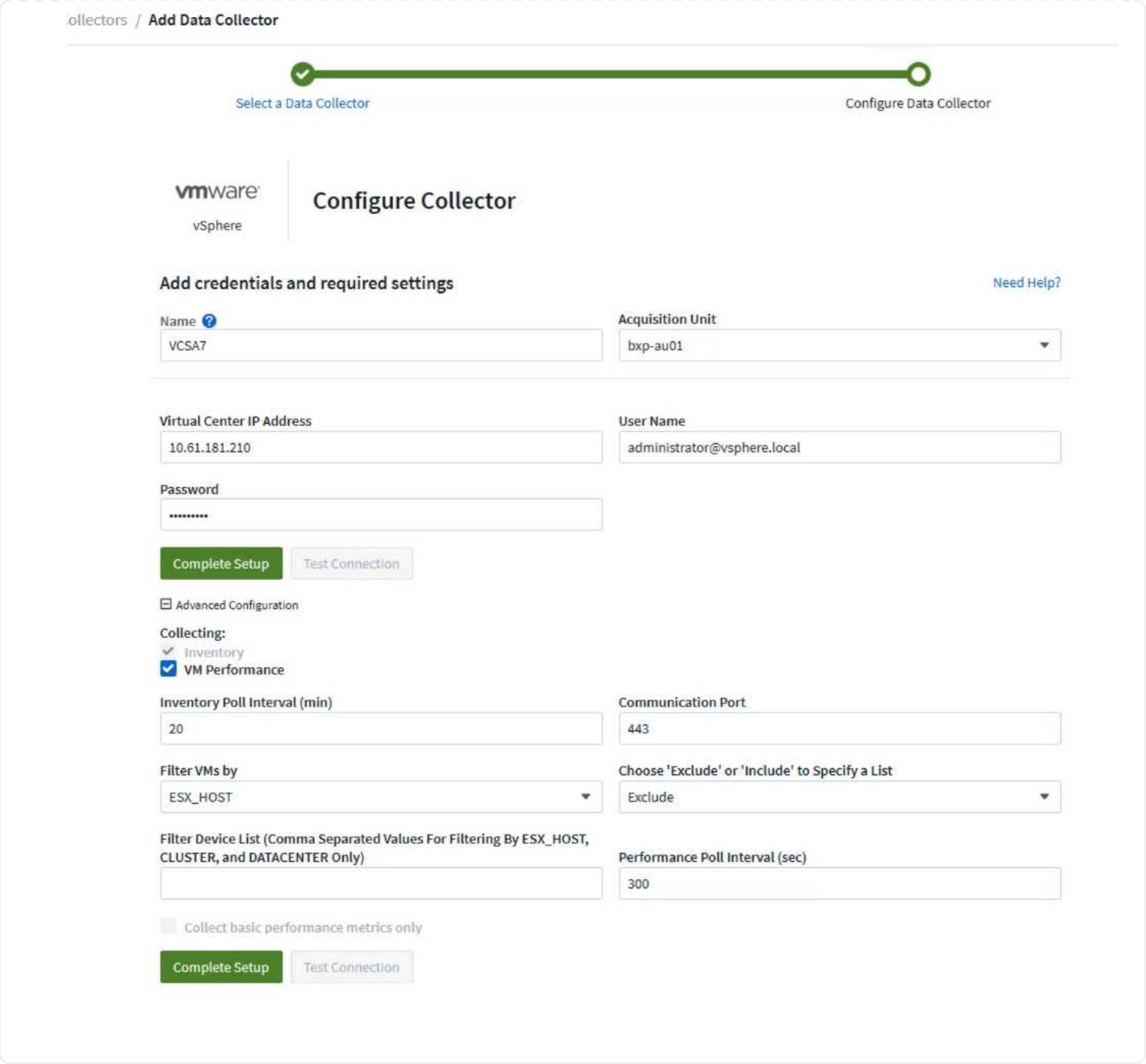
1. Once again, navigate to **Observability > Collectors > Data Collectors** and press the button to install a new Data Collector.



2. From here search for **vSphere** and click on **VMware vSphere**.


NetApp Cloud Insights
Observability
Explore
Alerts
Collectors 29
Log Queries
NetApp PCS Sandbox / Observability / Collectors / Add Data Collector
Choose a Data Collector to Monitor
vsphere
vmware
vSphere

3. On the **Configure Collector** page fill out a name for the collector, specify the correct **Acquisition Unit** and provide the credentials for the vCenter server. Click on **Save and Continue** and then **Complete Setup** at the bottom of the page to complete the configuration.



Configure Collector

Add credentials and required settings

Name: VCSA7	Acquisition Unit: bxp-au01
Virtual Center IP Address: 10.61.181.210	User Name: administrator@vsphere.local
Password: •••••••••	

Collecting:
☑ Inventory
☑ VM Performance

Inventory Poll Interval (min): 20	Communication Port: 443
Filter VMs by: ESX_HOST	Choose 'Exclude' or 'Include' to Specify a List: Exclude
Filter Device List (Comma Separated Values For Filtering By ESX_HOST, CLUSTER, and DATACENTER Only):	Performance Poll Interval (sec): 300

☐ Collect basic performance metrics only

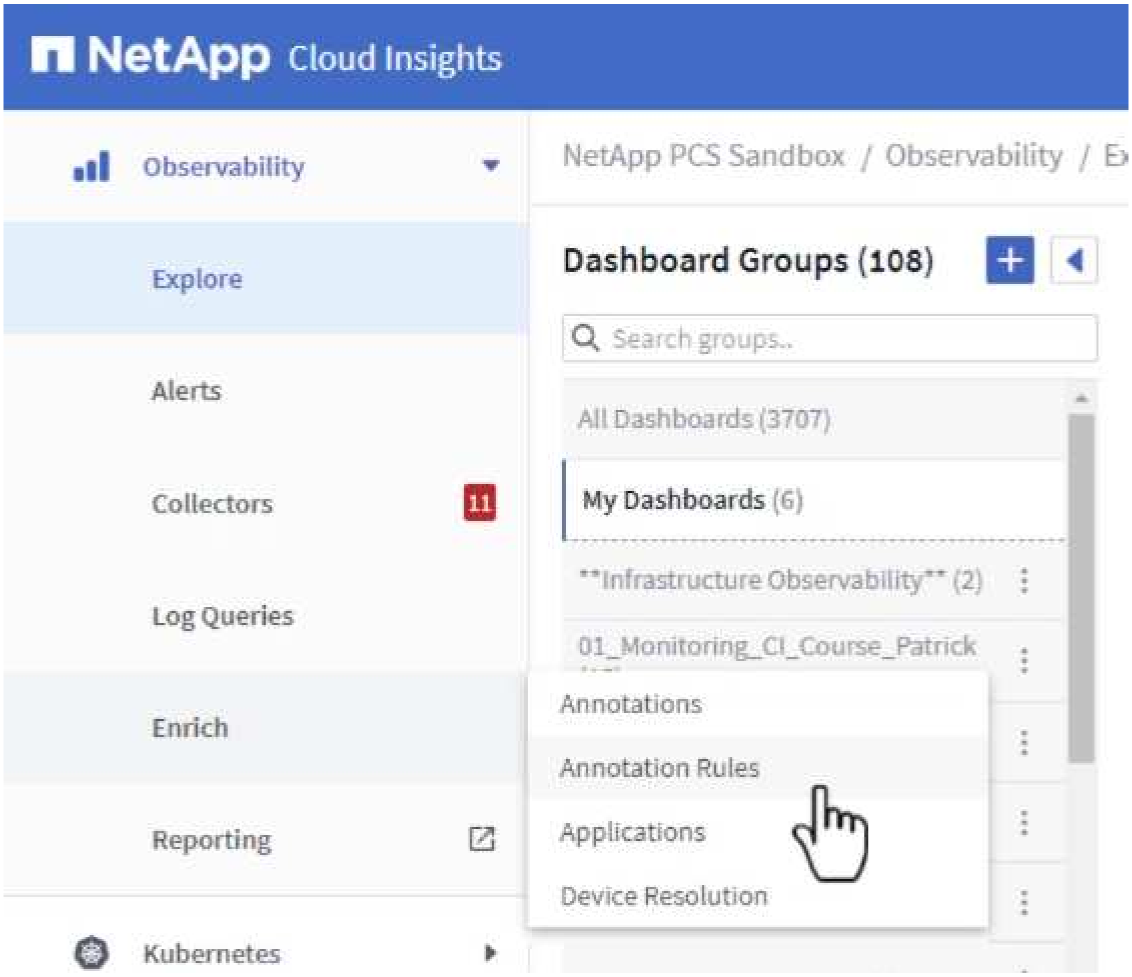
Add Annotations to assets

Annotations are a useful method of tagging assets so that they can be filtered and otherwise identified in the various views and metric queries available in Cloud Insights.

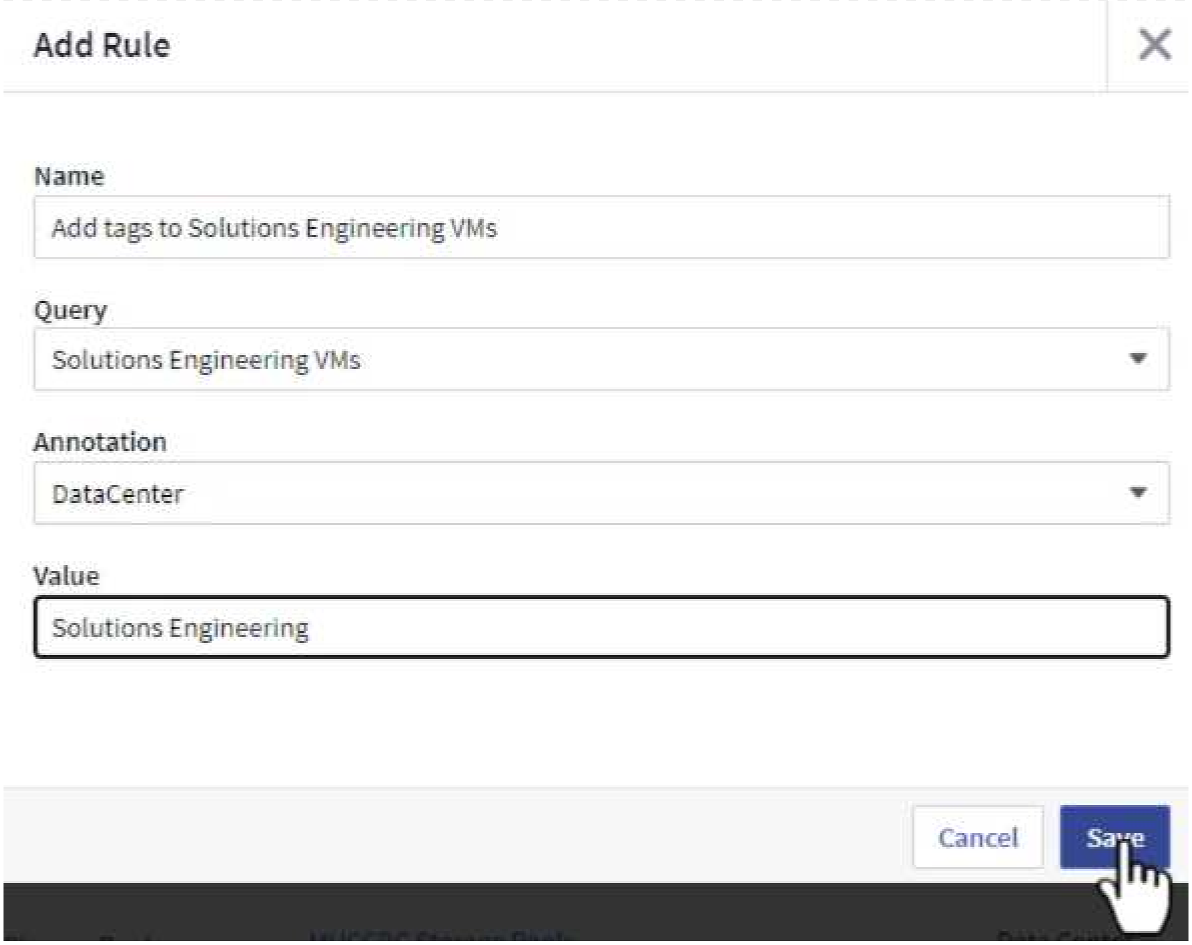
In this section, annotations will be added to virtual machine assets for filtering by **Data Center**.

Use Annotation Rules to tag assets

1. In the left-hand menu, navigate to **Observability > Enrich > Annotation Rules** and click on the **+ Rule** button in the upper right to add a new rule.



2. In the **Add Rule** dialog box fill in a name for the rule, locate a query to which the rule will be applied, the annotation field affected, and the value to be populated.



Add Rule

Name

Add tags to Solutions Engineering VMs

Query

Solutions Engineering VMs

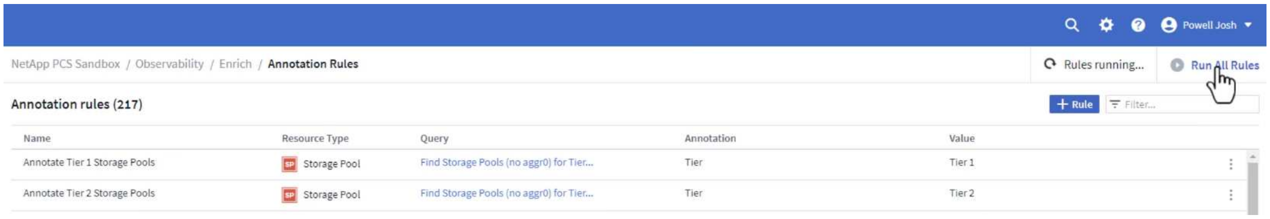
Annotation

DataCenter

Value

Solutions Engineering

3. Finally, in the upper right hand corner of the **Annotation Rules** page click on **Run All Rules** to run the rule and apply the annotation to the assets.



Powell Josh
NetApp PCS Sandbox / Observability / Enrich / Annotation Rules
Rules running...
Run All Rules
+ Rule
Filter...

Annotation rules (217)

Name	Resource Type	Query	Annotation	Value
Annotate Tier 1 Storage Pools	SP Storage Pool	Find Storage Pools (no aggr0) for Tier...	Tier	Tier 1
Annotate Tier 2 Storage Pools	SP Storage Pool	Find Storage Pools (no aggr0) for Tier...	Tier	Tier 2

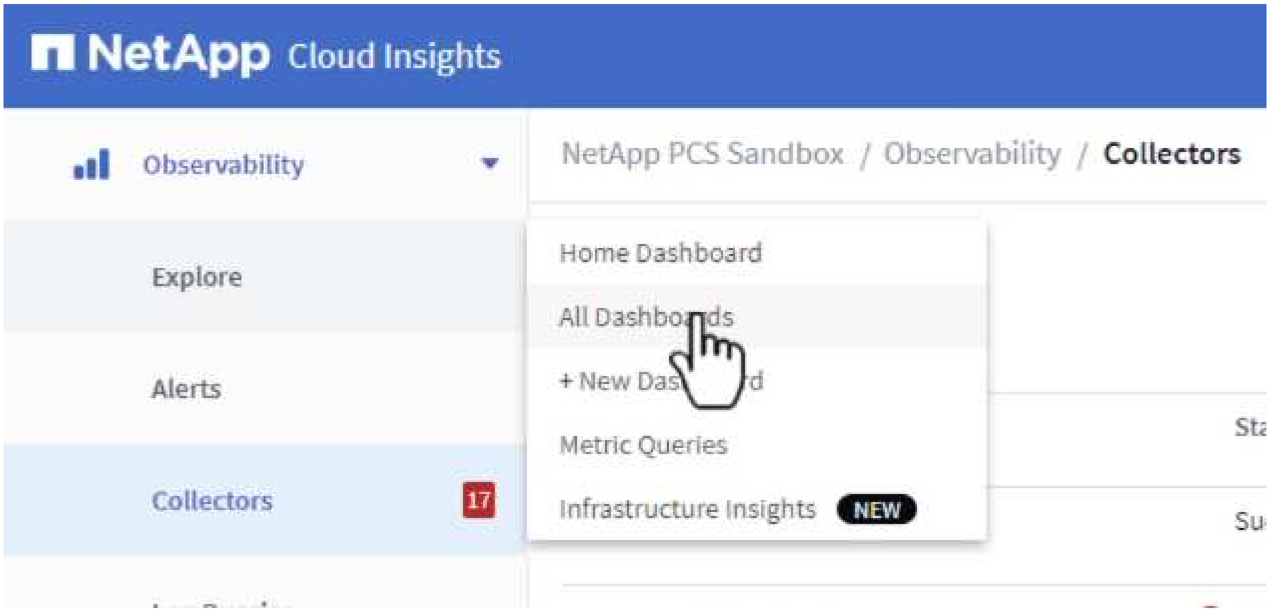
Explore and correlate assets

Cloud Insights draws logical conclusions about the assets that are running together on your storage systems and vsphere clusters.

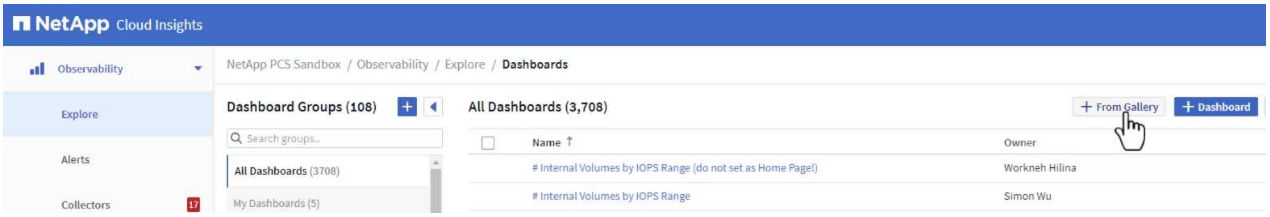
This sections illustrates how to use dashboards to correlate assets.

Correlating assets from a storage performance Dashboard

1. In the left-hand menu, navigate to **Observability > Explore > All Dashboards**.

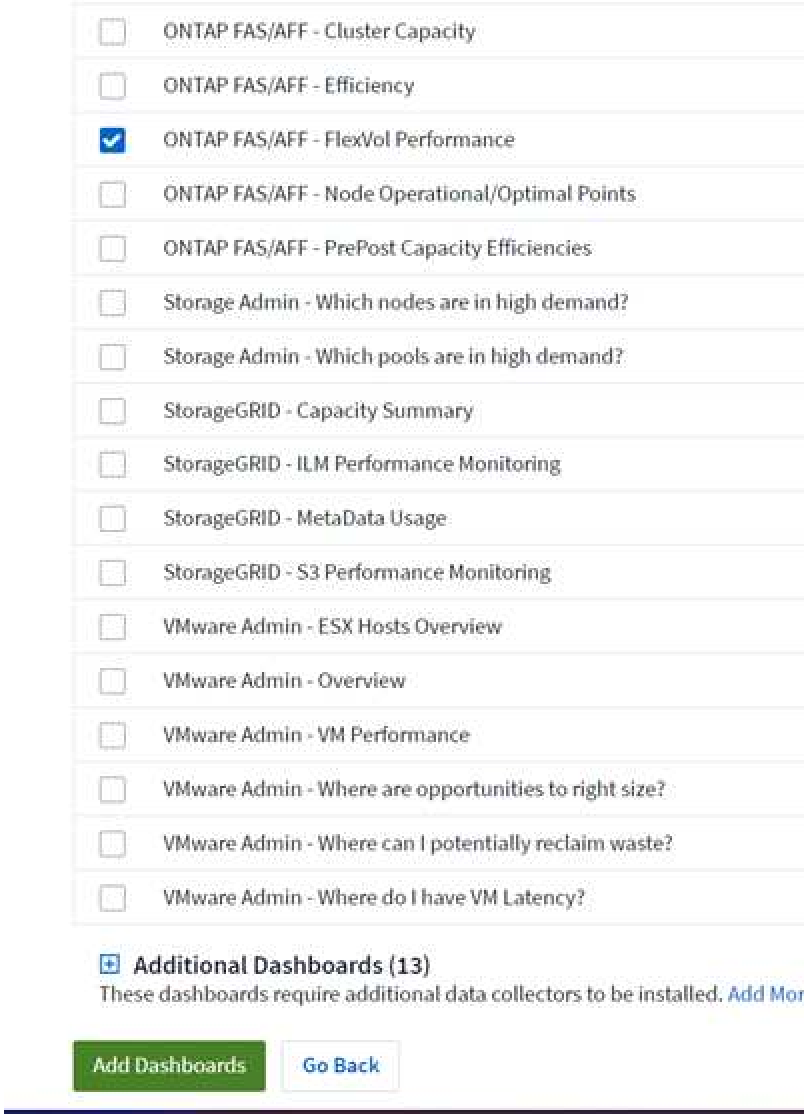


2. Click on the **+ From Gallery** button to view a list of ready-made dashboards that can be imported.



□	Name ↑	Owner
	# Internal Volumes by IOPS Range (do not set as Home Page!)	Workneh Hilina
	# Internal Volumes by IOPS Range	Simon Wu

3. Choose a dashboard for FlexVol performance from the list and click on the **Add Dashboards** button at the bottom of the page.



☐ ONTAP FAS/AFF - Cluster Capacity

☐ ONTAP FAS/AFF - Efficiency

☑ ONTAP FAS/AFF - FlexVol Performance

☐ ONTAP FAS/AFF - Node Operational/Optimal Points

☐ ONTAP FAS/AFF - PrePost Capacity Efficiencies

☐ Storage Admin - Which nodes are in high demand?

☐ Storage Admin - Which pools are in high demand?

☐ StorageGRID - Capacity Summary

☐ StorageGRID - ILM Performance Monitoring

☐ StorageGRID - MetaData Usage

☐ StorageGRID - S3 Performance Monitoring

☐ VMware Admin - ESX Hosts Overview

☐ VMware Admin - Overview

☐ VMware Admin - VM Performance

☐ VMware Admin - Where are opportunities to right size?

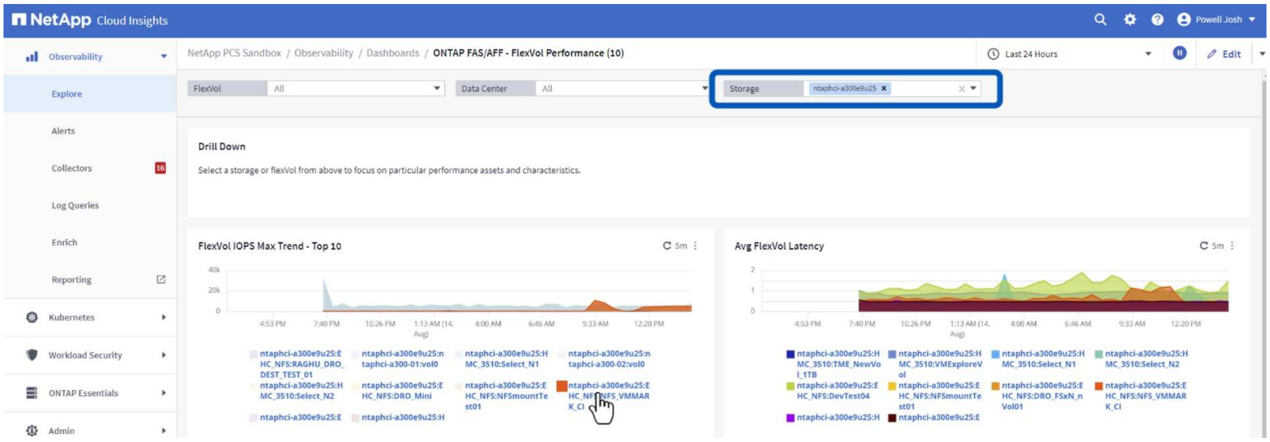
☐ VMware Admin - Where can I potentially reclaim waste?

☐ VMware Admin - Where do I have VM Latency?

⊞ Additional Dashboards (13)

These dashboards require additional data collectors to be installed. Add Mor

4. Once imported, open the dashboard. From here you can see various widgets with detailed performance data. Add a filter to view a single storage system and select a storage volume to drill into it’s details.

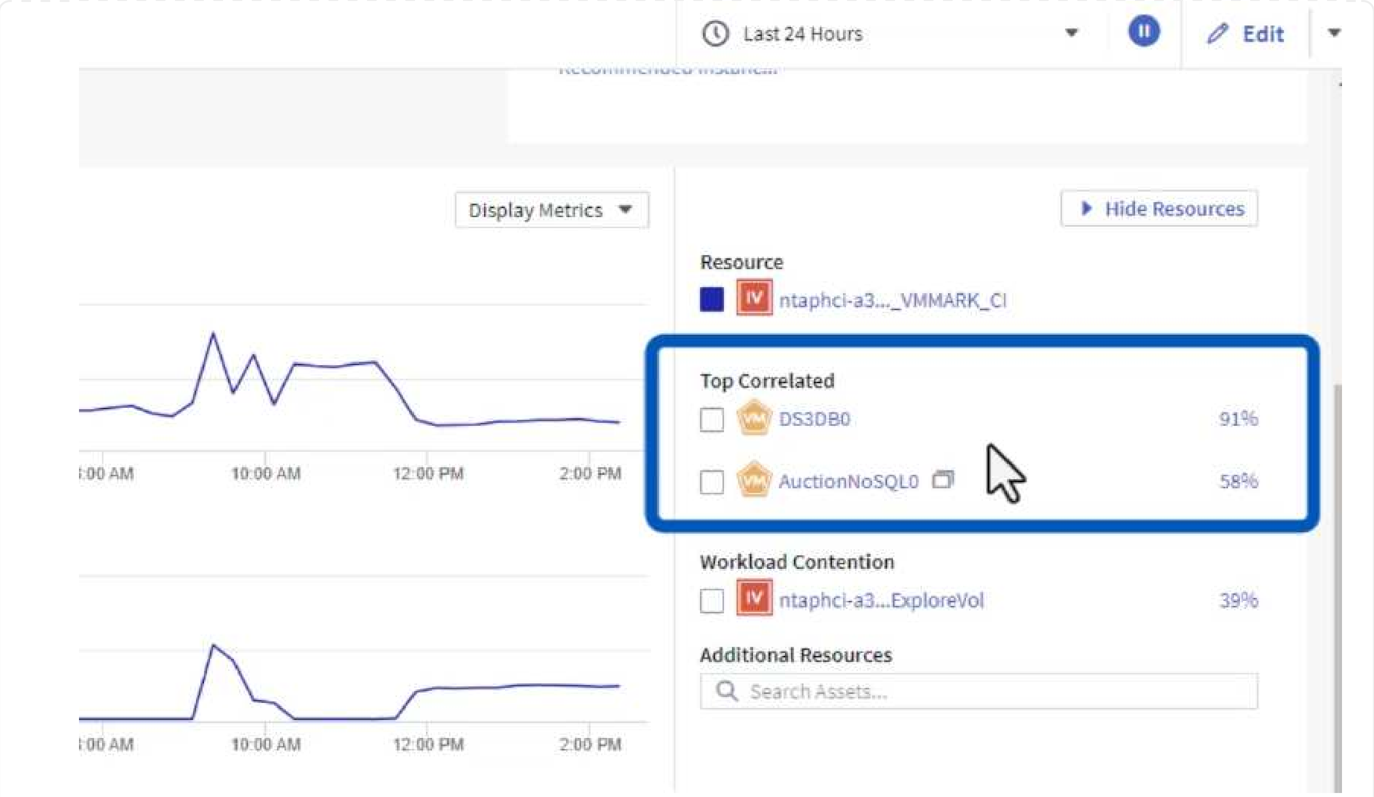


NetApp Cloud Insights
Powell Josh
Observability
Explore
Alerts
Collectors
16
Log Queries
Enrich
Reporting
Kubernetes
Workload Security
ONTAP Essentials
Admin
NetApp PCS Sandbox / Observability / Dashboards / ONTAP FAS/AFF - FlexVol Performance (10)
Last 24 Hours
Edit
FlexVol
All
Data Center
All
Storage
ntaphci-a300e9u25
FlexVol IOPS Max Trend - Top 10
5m
40k
20k
0
4:53 PM
7:40 PM
10:26 PM
1:13 AM (14. Aug)
4:00 AM
6:46 AM
9:33 AM
12:20 PM
ntaphci-a300e9u25:EHC_NFS:RAGHU_DRO_DEST_TEST_01
ntaphci-a300e9u25:ntaphci-a300-01:vol0
ntaphci-a300e9u25:HMC_3510:Select_N1
ntaphci-a300e9u25:ntaphci-a300-02:vol0
ntaphci-a300e9u25:HMC_3510:Select_N2
ntaphci-a300e9u25:EHC_NFS:DRO_Mini
ntaphci-a300e9u25:EHC_NFS:NFSmountTest01
ntaphci-a300e9u25:EHC_NFS:NFS_VMMARK_CI
ntaphci-a300e9u25:E
ntaphci-a300e9u25:H
Avg FlexVol Latency
5m
2
1
0
4:53 PM
7:40 PM
10:26 PM
1:13 AM (14. Aug)
4:00 AM
6:46 AM
9:33 AM
12:20 PM
ntaphci-a300e9u25:HMC_3510:TME_NewVol_1TB
ntaphci-a300e9u25:HMC_3510:VMExploreVol
ntaphci-a300e9u25:HMC_3510:Select_N1
ntaphci-a300e9u25:HMC_3510:Select_N2
ntaphci-a300e9u25:EHC_NFS:DevTest04
ntaphci-a300e9u25:EHC_NFS:NFSmountTest01
ntaphci-a300e9u25:EHC_NFS:DRO_FSxN_nVol01
ntaphci-a300e9u25:EHC_NFS:NFS_VMMARK_CI
ntaphci-a300e9u25:H
ntaphci-a300e9u25:E

Drill Down

Select a storage or flexVol from above to focus on particular performance assets and characteristics.

5. From this view you can see various metrics related to this storage volume and the top utilized and correlated virtual machines running on the volume.



Resource

IV ntaphci-a3..._VMMARK_CI

Top Correlated

□ VM DS3DB0	91%
□ VM AuctionNoSQL0	58%

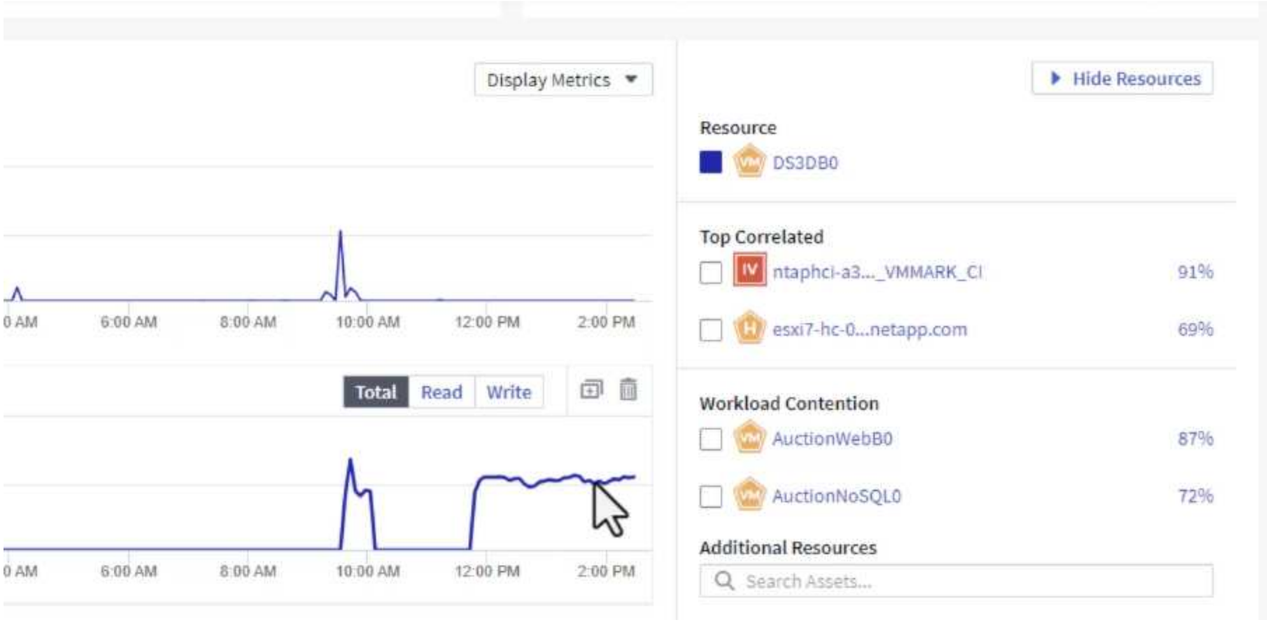
Workload Contention

□ IV ntaphci-a3...ExploreVol	39%

Additional Resources

Search Assets...

6. Clicking on the VM with the highest utilization drills into the metrics for that VM to view any potential issues.



Resource

VM DS3DB0

Top Correlated

□ IV ntaphci-a3..._VMMARK_CI	91%
□ H esxi7-hc-0...netapp.com	69%

Workload Contention

□ VM AuctionWebB0	87%
□ VM AuctionNoSQL0	72%

Additional Resources

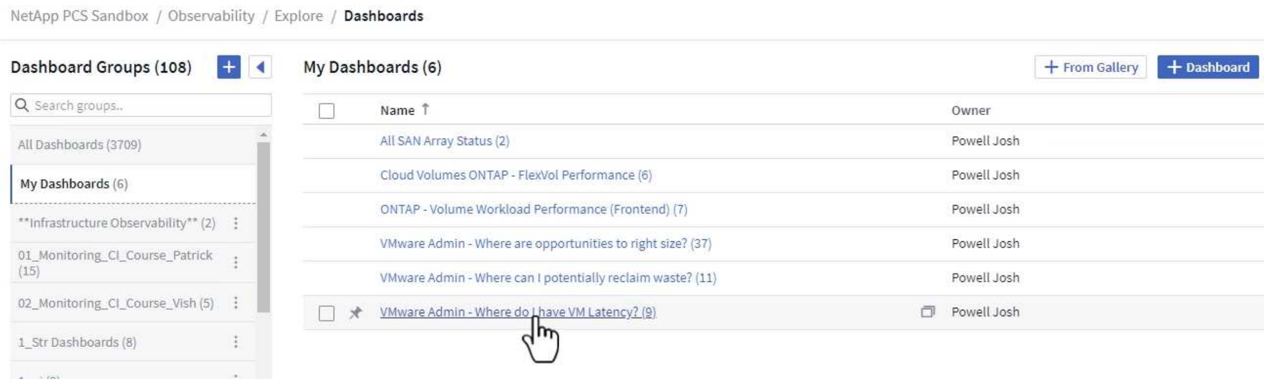
Search Assets...

Use Cloud Insights to identify noisy neighbors

Cloud Insights features dashboards that can easily isolate peer VMs that are negatively impacting other VMs running on the same storage volume.

Use a Top VM Latency dashboard to isolate noisy neighbors

1. In this example access a dashboard available in the **Gallery** called **VMware Admin - Where do I have VM Latency?**



NetApp PCS Sandbox / Observability / Explore / **Dashboards**

Dashboard Groups (108)

Search groups..

All Dashboards (3709)

My Dashboards (6)

Infrastructure Observability (2)

01_Monitoring_CI_Course_Patrick (15)

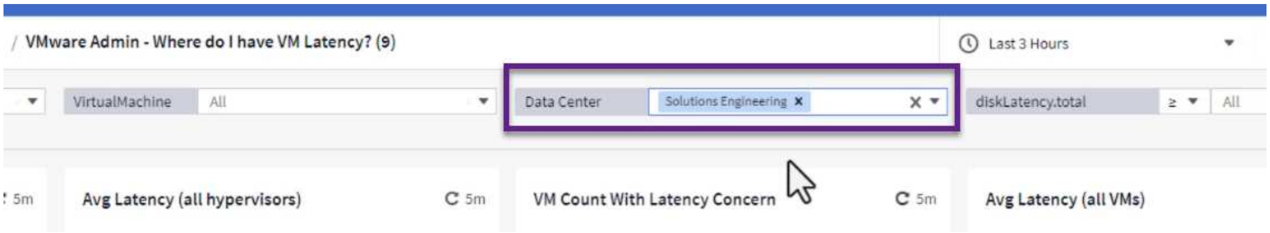
02_Monitoring_CI_Course_Vish (5)

1_Str Dashboards (8)

My Dashboards (6)

Name ↑	Owner
All SAN Array Status (2)	Powell Josh
Cloud Volumes ONTAP - FlexVol Performance (6)	Powell Josh
ONTAP - Volume Workload Performance (Frontend) (7)	Powell Josh
VMware Admin - Where are opportunities to right size? (37)	Powell Josh
VMware Admin - Where can I potentially reclaim waste? (11)	Powell Josh
VMware Admin - Where do I have VM Latency? (9)	Powell Josh

2. Next, filter by the **Data Center** annotation created in a previous step to view a subset of assets.



/ VMware Admin - Where do I have VM Latency? (9)

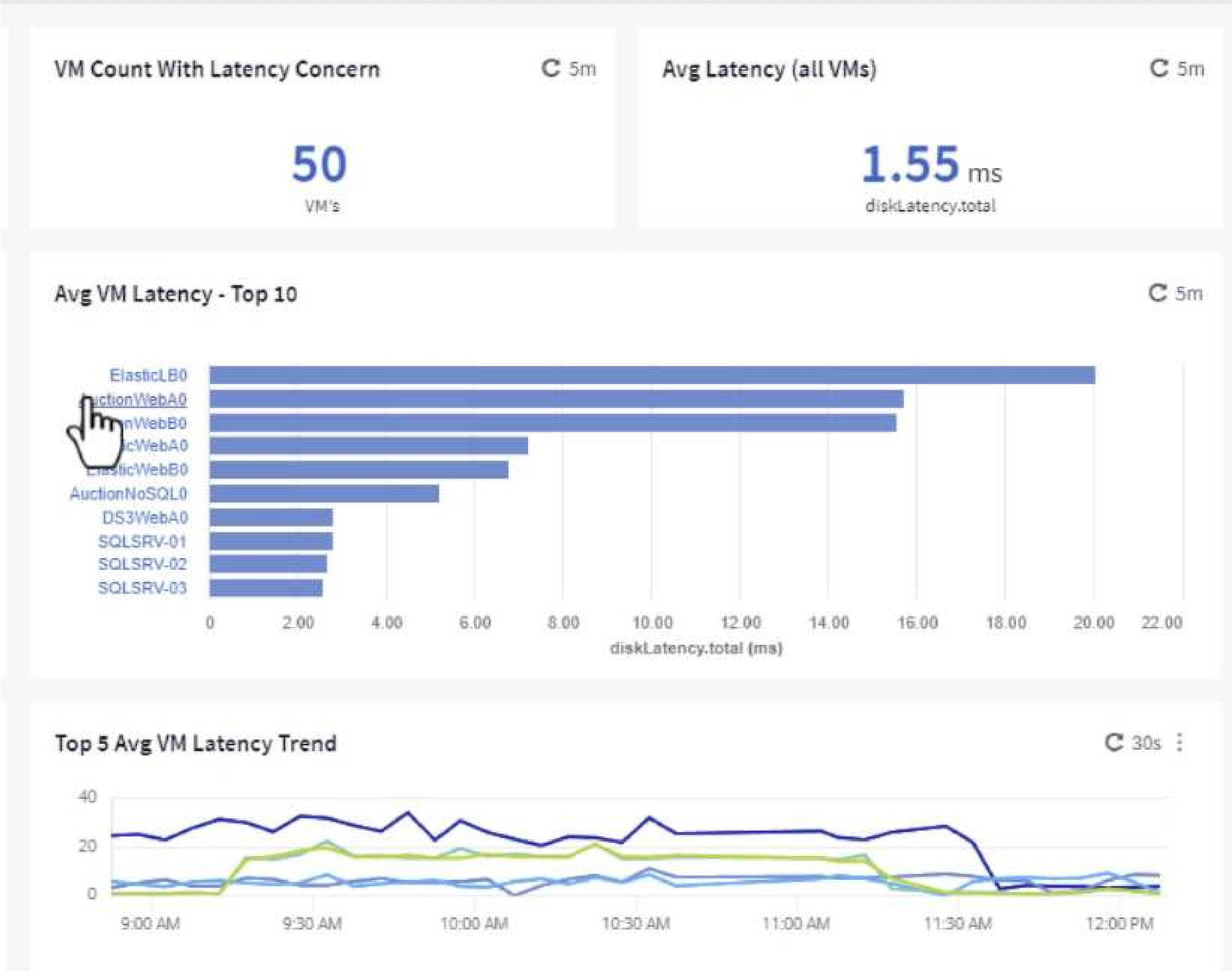
Last 3 Hours

VirtualMachine: All

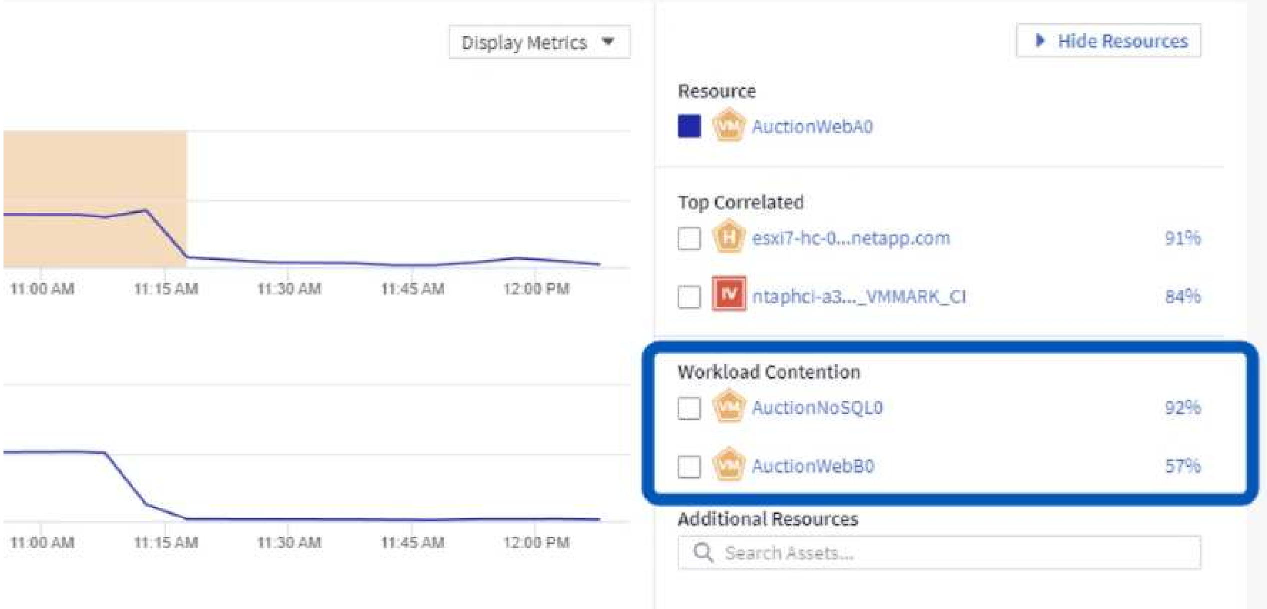
Data Center: Solutions Engineering

diskLatency.total ≥ All

3. This dashboard shows a list of the top 10 VMs by average latency. From here click on the VM of concern to drill into its details.



4. The VMs potentially causing workload contention are listed and available. Drill into these VMs performance metrics to investigate any potential issues.

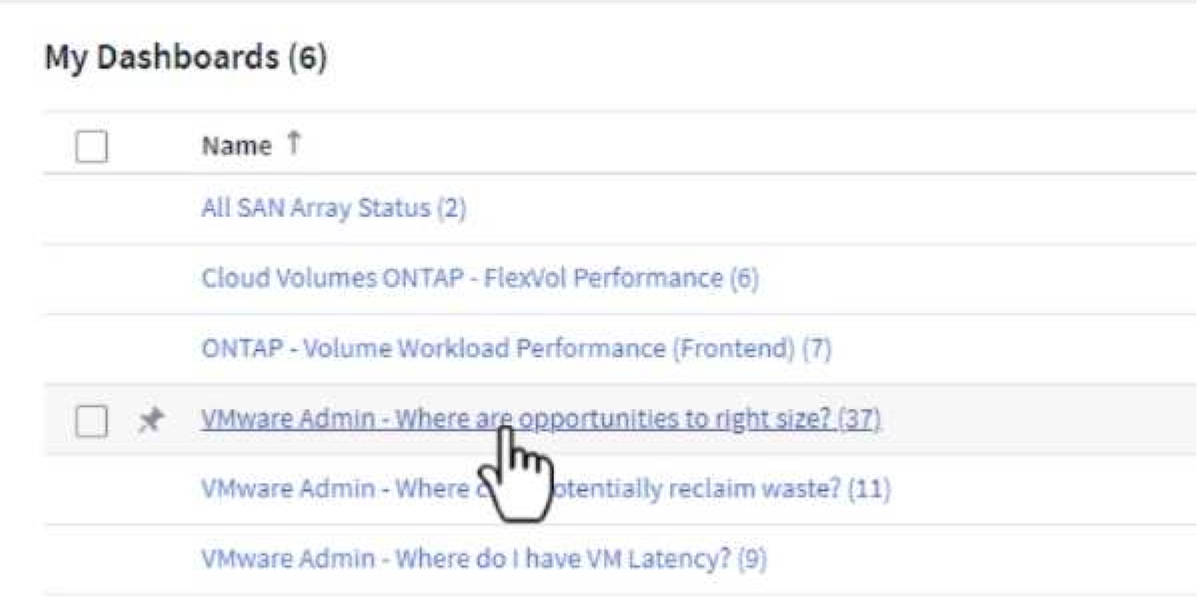


View over and under utilized resources in Cloud Insights

By matching VM resources to actual workload requirements, resource utilization can be optimized, leading to cost savings on infrastructure and cloud services. Data in Cloud Insights can be customized to easily display over or under utilized VMs.

Identify opportunities to right size VMs

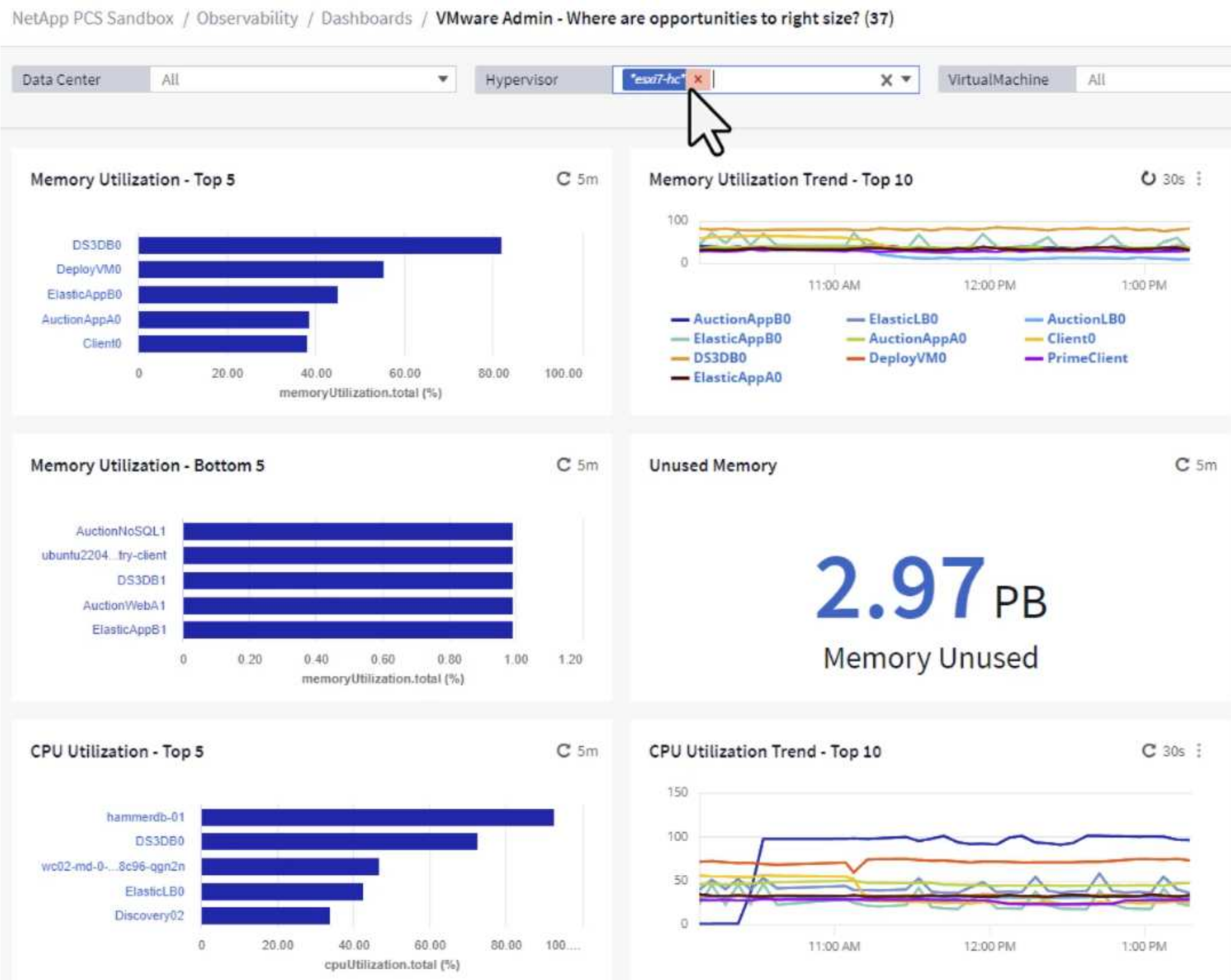
1. In this example access a dashboard available in the **Gallery** called **VMware Admin - Where are opportunities to right size?**



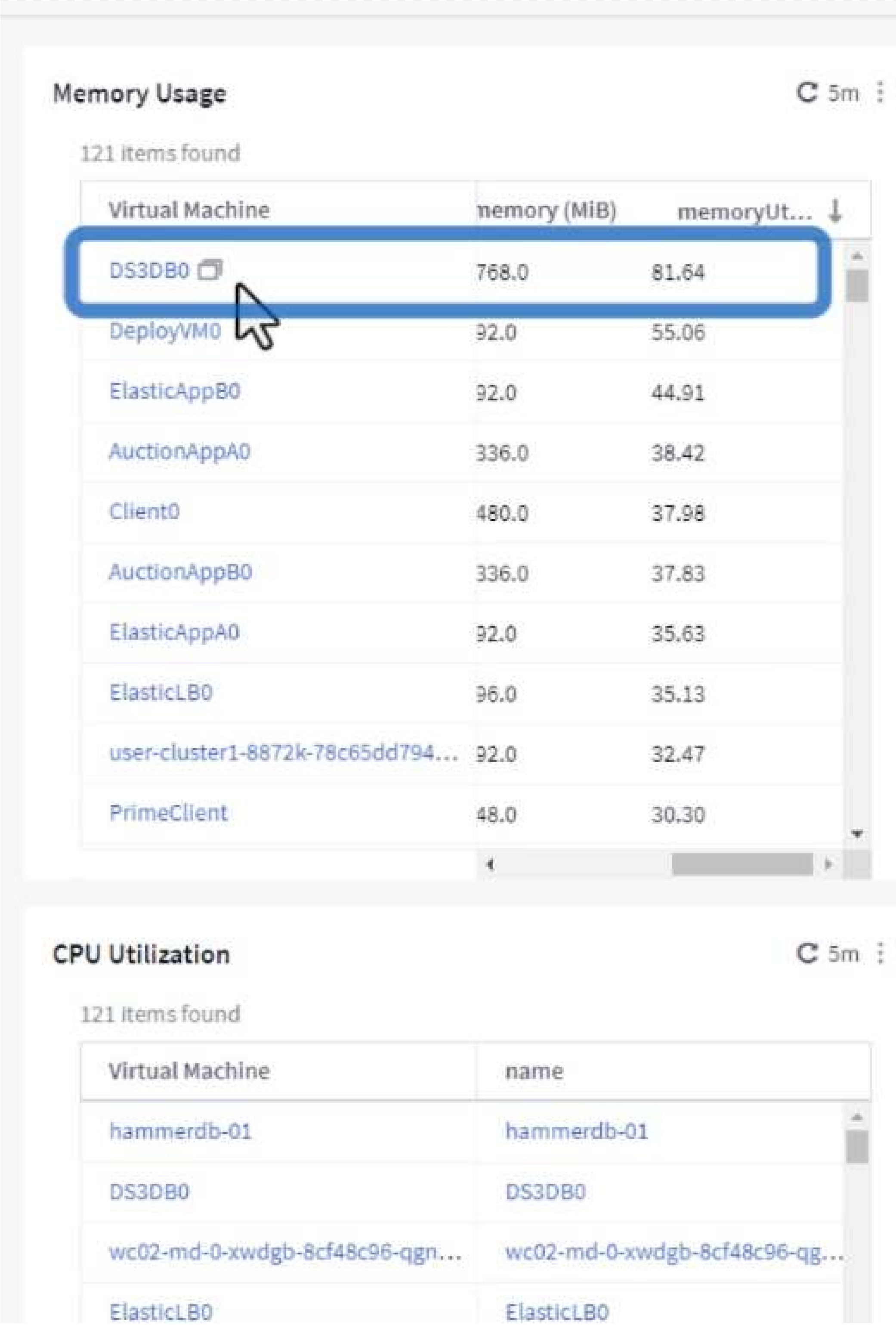
My Dashboards (6)

□		Name ↑
		All SAN Array Status (2)
		Cloud Volumes ONTAP - FlexVol Performance (6)
		ONTAP - Volume Workload Performance (Frontend) (7)
□		VMware Admin - Where are opportunities to right size? (37)
		VMware Admin - Where c[illegible] otentially reclaim waste? (11)
		VMware Admin - Where do I have VM Latency? (9)

2. First filter by all of the ESXi hosts in the cluster. You can then see ranking of the top and bottom VMs by memory and CPU utilization.



3. Tables allow sorting and provide more detail based on the columns of data chosen.



Memory Usage

121 items found

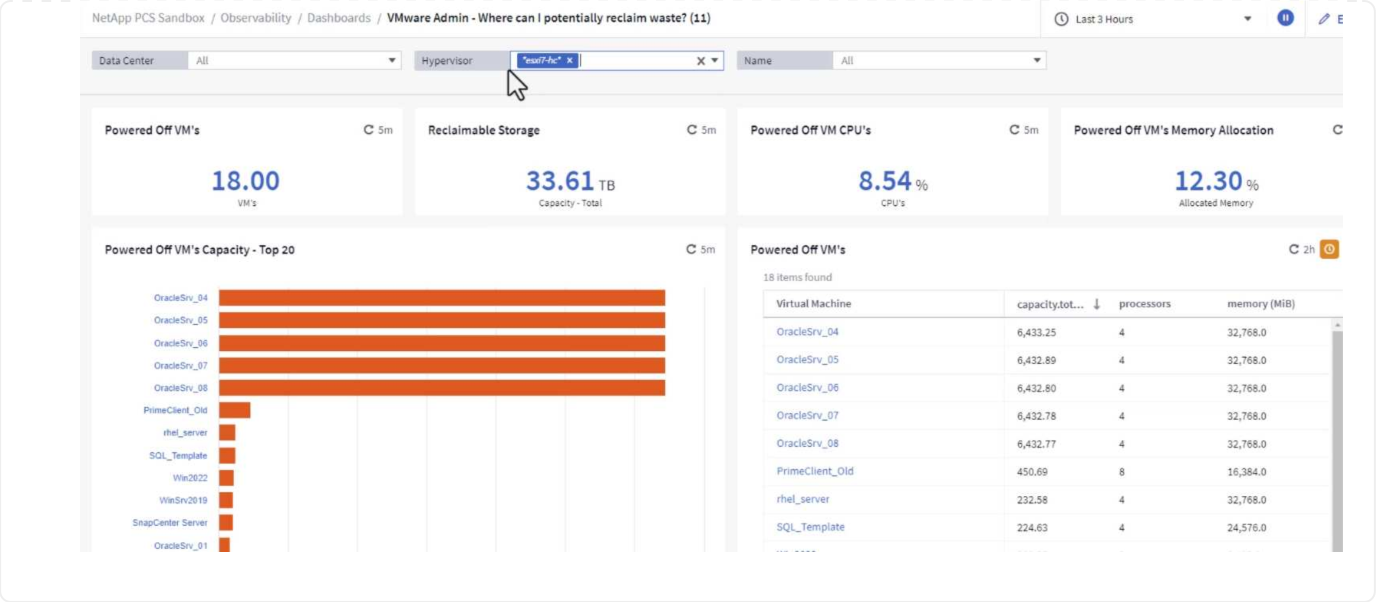
Virtual Machine	nemory (MiB)	memoryUt...
DS3DB0	768.0	81.64
DeployVM0	92.0	55.06
ElasticAppB0	92.0	44.91
AuctionAppA0	336.0	38.42
Client0	480.0	37.98
AuctionAppB0	336.0	37.83
ElasticAppA0	92.0	35.63
ElasticLB0	96.0	35.13
user-cluster1-8872k-78c65dd794...	92.0	32.47
PrimeClient	48.0	30.30

CPU Utilization

121 items found

Virtual Machine	name
hammerdb-01	hammerdb-01
DS3DB0	DS3DB0
wc02-md-0-xwdgb-8cf48c96-qgn...	wc02-md-0-xwdgb-8cf48c96-qg...
ElasticLB0	ElasticLB0

4. Another dashboard called **VMware Admin - Where can I potentially reclaim waste?** shows powered off VM’s sorted by their capacity use.



Data Center: All

Hypervisor: *esxi7-hc*

Name: All

Powered Off VM's — 18.00 VM's

Reclaimable Storage — 33.61 TB Capacity - Total

Powered Off VM CPU's — 8.54 % CPU's

Powered Off VM's Memory Allocation — 12.30 % Allocated Memory

Powered Off VM's

18 items found

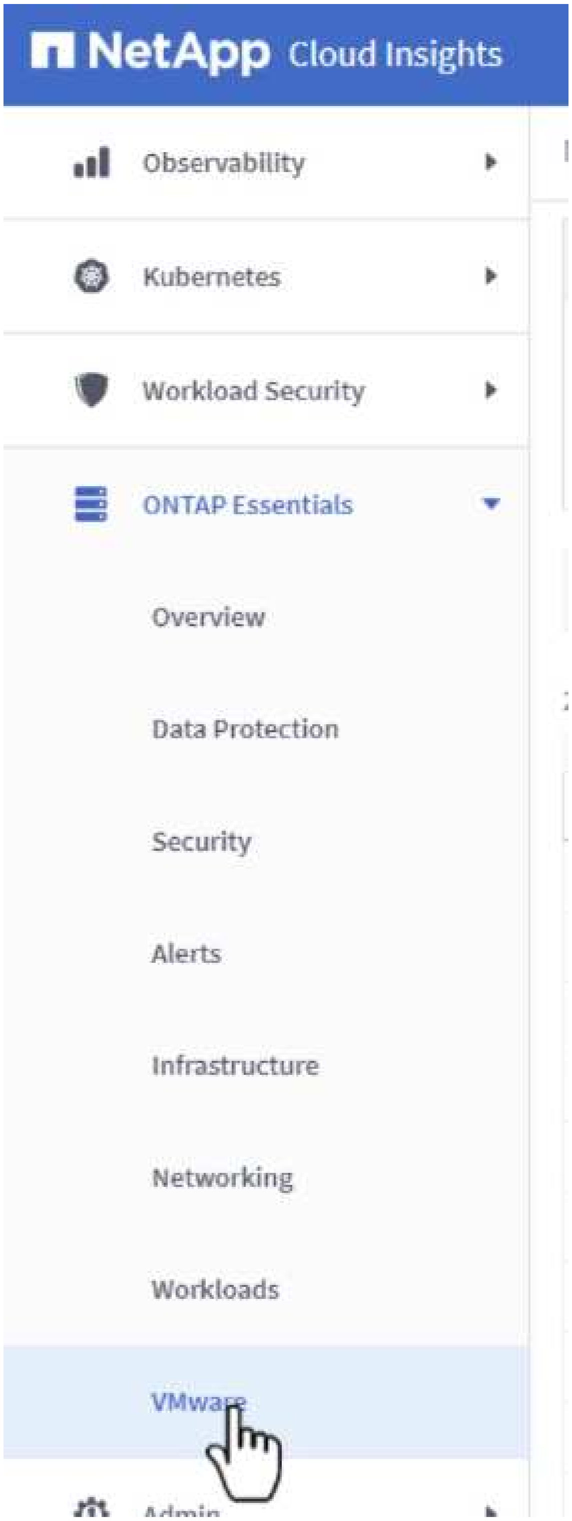
Virtual Machine	capacity.tot... ↓	processors	memory (MiB)
OracleSrv_04	6,433.25	4	32,768.0
OracleSrv_05	6,432.89	4	32,768.0
OracleSrv_06	6,432.80	4	32,768.0
OracleSrv_07	6,432.78	4	32,768.0
OracleSrv_08	6,432.77	4	32,768.0
PrimeClient_Old	450.69	8	16,384.0
rhel_server	232.58	4	32,768.0
SQL_Template	224.63	4	24,576.0

Use queries to isolate and sort metrics

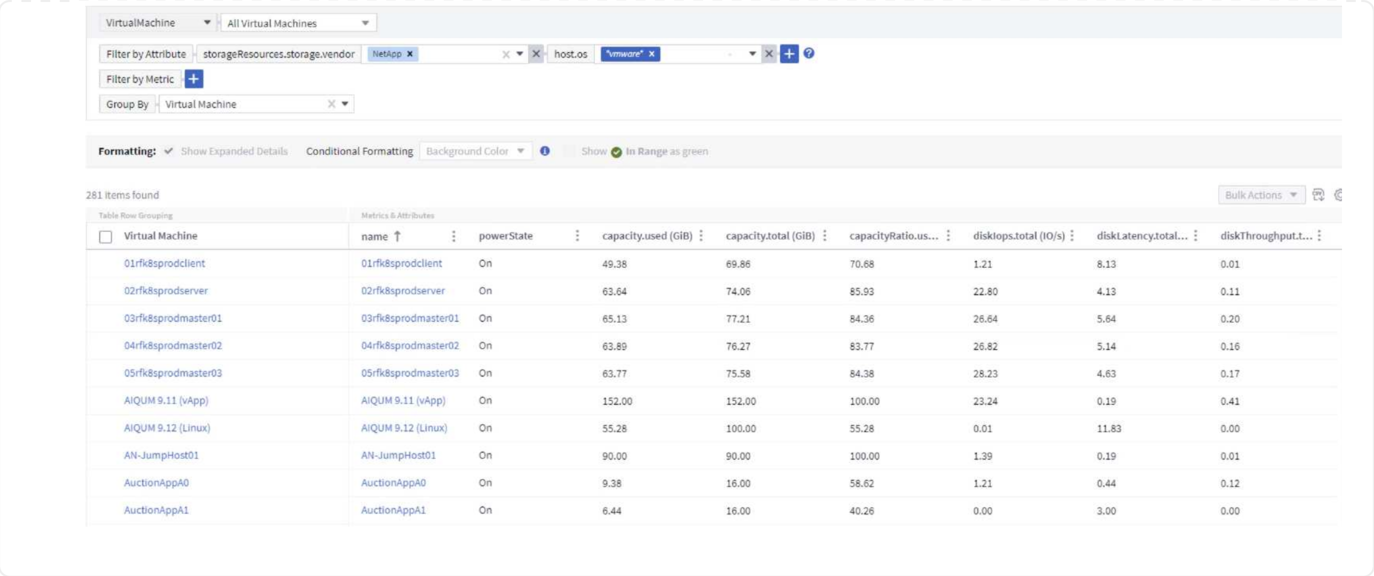
The amount of data captured by Cloud Insights is quite comprehensive. Metric queries provide a powerful way to sort and organize large amounts of data in useful ways.

View a detailed VMware query under ONTAP Essentials

1. Navigate to **ONTAP Essentials > VMware** to access a comprehensive VMware metric query.



2. In this view you are presented with multiple options for filtering and grouping the data at the top. All columns of data are customizable and additional columns can be easily added.



Filter by Attribute: storageResources.storage.vendor NetApp; host.os *vmware*

Group By: Virtual Machine

Formatting: ✓ Show Expanded Details | Conditional Formatting: Background Color | Show ● In Range as green

281 items found

Virtual Machine	name	powerState	capacity.used (GiB)	capacity.total (GiB)	capacityRatio.us...	diskIops.total (IO/s)	diskLatency.total...	diskThroughput.t...
01rfk8sprodclient	01rfk8sprodclient	On	49.38	69.86	70.68	1.21	8.13	0.01
02rfk8sprodserver	02rfk8sprodserver	On	63.64	74.06	85.93	22.80	4.13	0.11
03rfk8sprodmaster01	03rfk8sprodmaster01	On	65.13	77.21	84.36	26.64	5.64	0.20
04rfk8sprodmaster02	04rfk8sprodmaster02	On	63.89	76.27	83.77	26.82	5.14	0.16
05rfk8sprodmaster03	05rfk8sprodmaster03	On	63.77	75.58	84.38	28.23	4.63	0.17
AIQUM 9.11 (vApp)	AIQUM 9.11 (vApp)	On	152.00	152.00	100.00	23.24	0.19	0.41
AIQUM 9.12 (Linux)	AIQUM 9.12 (Linux)	On	55.28	100.00	55.28	0.01	11.83	0.00
AN-JumpHost01	AN-JumpHost01	On	90.00	90.00	100.00	1.39	0.19	0.01
AuctionAppA0	AuctionAppA0	On	9.38	16.00	58.62	1.21	0.44	0.12
AuctionAppA1	AuctionAppA1	On	6.44	16.00	40.26	0.00	3.00	0.00

Conclusion

This solution was designed as a primer to learn how to get started with NetApp Cloud Insights and show some of the powerful capabilities that this observability solution can provide. There are hundreds of dashboards and metric queries built into the product which makes it easy to get going immediately. The full version of Cloud Insights is available as a 30-day trial and the basic version is available free to NetApp customers.

Additional Information

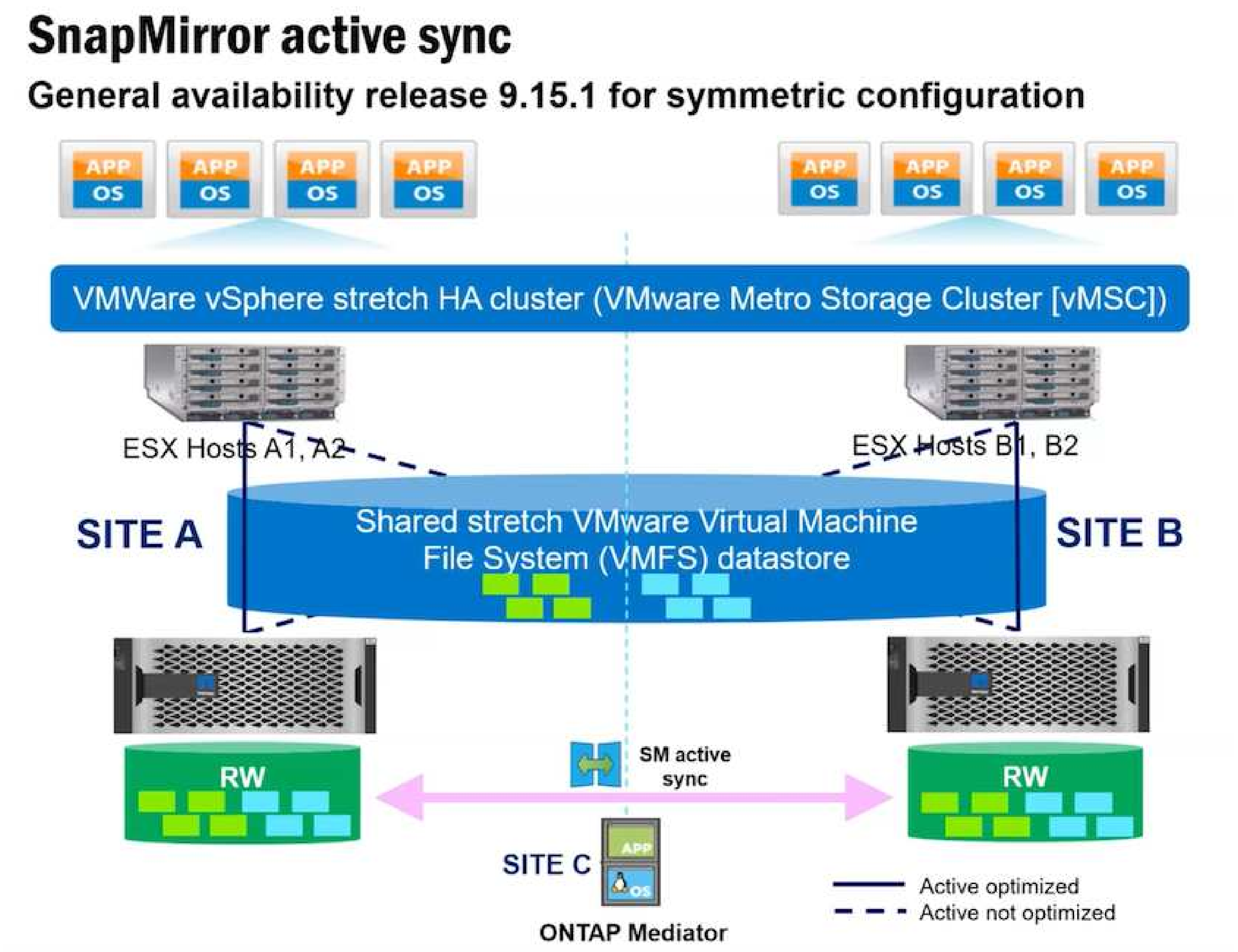
To learn more about the technologies presented in this solution refer to the following additional information.

- NetApp BlueXP and Cloud Insights landing page
- NetApp Cloud Insights documentation

VMware vSphere Metro Storage Cluster with SnapMirror active sync

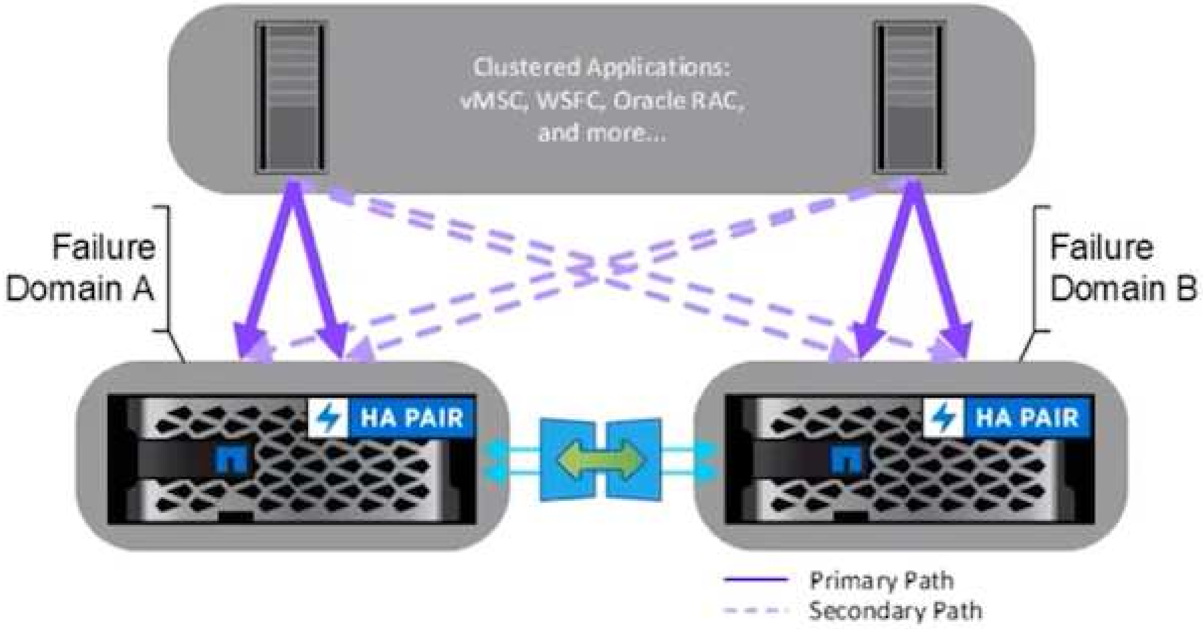
VMware vSphere Metro Storage Cluster (vMSC) is a stretched cluster solution across different fault domains to provide
* Workload mobility across availability zones or sites.
* downtime avoidance
* disaster avoidance
* fast recovery

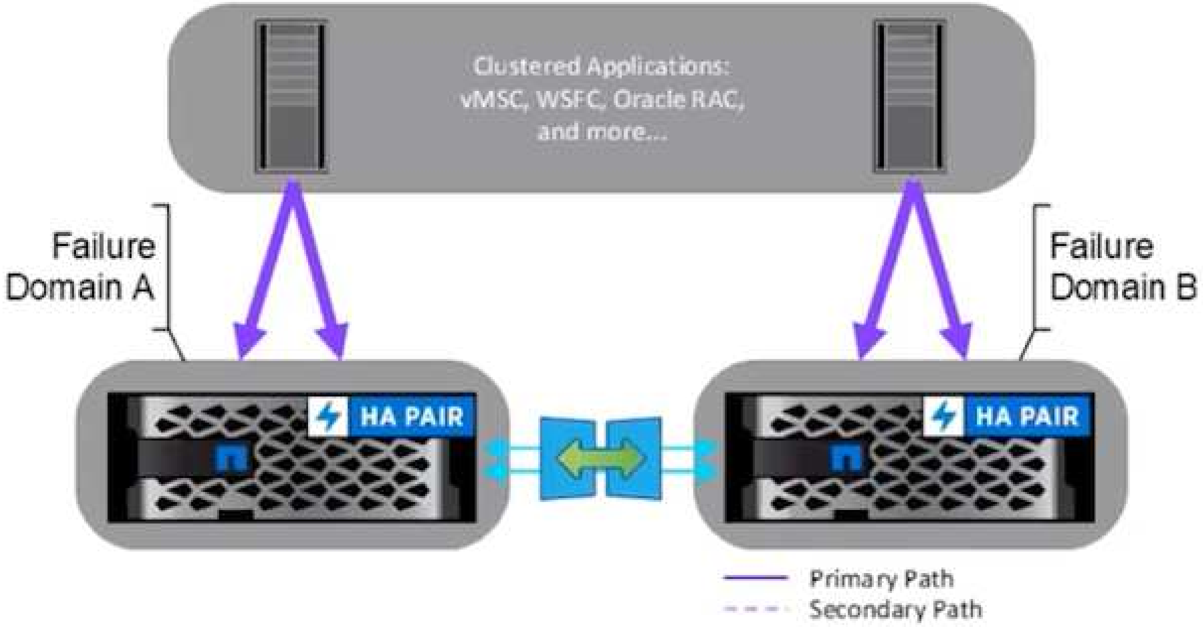
This document provides the vMSC implementation details with SnapMirror active sync (SM-as) utilizing System Manager and ONTAP Tools. Further, it shows how the VM can be protected by replicating to third site and manage with SnapCenter Plugin for VMware vSphere.


SnapMirror active sync
General availability release 9.15.1 for symmetric configuration
APP
OS
VMWare vSphere stretch HA cluster (VMware Metro Storage Cluster [vMSC])
ESX Hosts A1, A2
ESX Hosts B1, B2
SITE A
SITE B
Shared stretch VMware Virtual Machine File System (VMFS) datastore
RW
RW
SM active sync
SITE C
APP
OS
ONTAP Mediator
Active optimized
Active not optimized

SnapMirror active sync supports ASA, AFF and FAS storage arrays. It is recommended to use same type (Performance/Capacity models) on both fault domains. Currently, only block protocols like FC and iSCSI are supported. For further support guidelines, refer Interoperability Matrix Tool and Hardware Universe

vMSC supports two different deployment models named Uniform host access and Non-uniform host access. In Uniform host access configuration, every host on the cluster has access to LUN on both fault domains. It is typically used in different availability zones in same datacenter.





In Non-Uniform host access configuration, host has access only to local fault domain. It is typically used in different sites where running multiple cables across the fault domains are restrictive option.

In Non-Uniform host access mode, the VMs will be restarted in other fault domain by vSphere HA. Application availability will be impacted based on its design. Non-Uniform host access mode is supported only with ONTAP 9.15 onwards.

Prerequisites

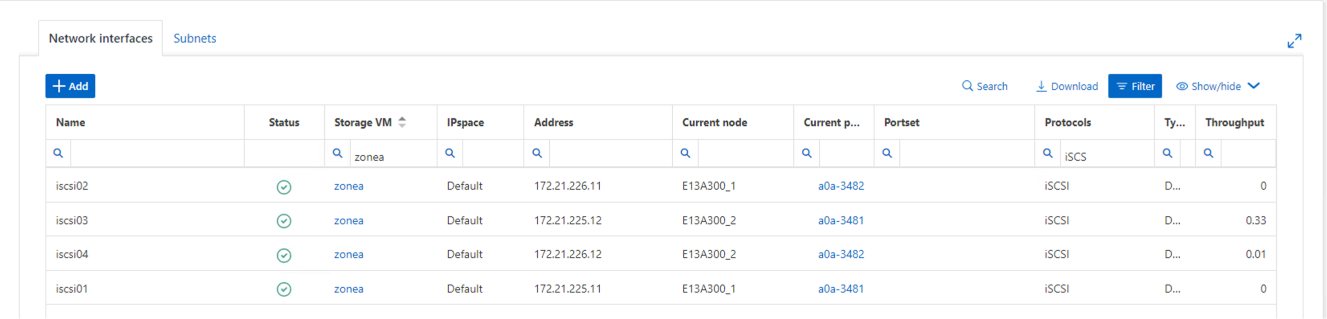
- VMware vSphere hosts deployed with dual storage fabric (Two HBAs or Dual VLAN for iSCSI) per host.
- Storage Arrays are deployed with link aggregation for data ports (for iSCSI).
- Storage VM and LIFs are available
- Inter-Cluster latency round trip time must be less than 10 milliseconds.
- ONTAP Mediator VM is deployed on different fault domain
- Cluster Peer relationship is established
- SVM Peer relationship is established
- ONTAP Mediator registered to ONTAP cluster

If using self-signed certificate, the CA certificate can be retrieved from the <installation path>/ontap_mediator/server_config/ca.crt on mediator VM.

vMSC non-uniform host access with ONTAP System Manager UI.

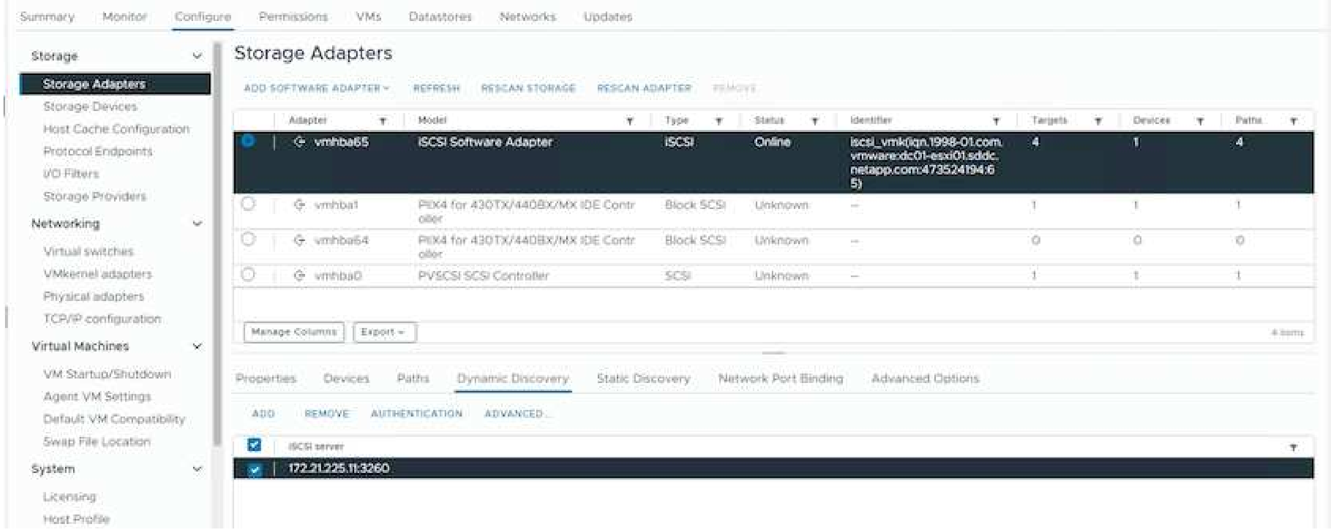
Note: ONTAP Tools 10.2 or above can be used to provision stretched datastore with non-uniform host access mode without switching multiple user interfaces. This section is just for reference if ONTAP Tools is not used.

1. Note down one of the iSCSI data lif IP address from the local fault domain storage array.



Name	Status	Storage VM	IPspace	Address	Current node	Current p...	Portset	Protocols	Ty...	Throughput
		zonea						iSCS		
iscsi02	✓	zonea	Default	172.21.226.11	E13A300_1	a0a-3482		iSCSI	D...	0
iscsi03	✓	zonea	Default	172.21.225.12	E13A300_2	a0a-3481		iSCSI	D...	0.33
iscsi04	✓	zonea	Default	172.21.226.12	E13A300_2	a0a-3482		iSCSI	D...	0.01
iscsi01	✓	zonea	Default	172.21.225.11	E13A300_1	a0a-3481		iSCSI	D...	0

2. On vSphere host iSCSI Storage Adapter, add that iSCSI IP under the Dynamic Discovery tab.



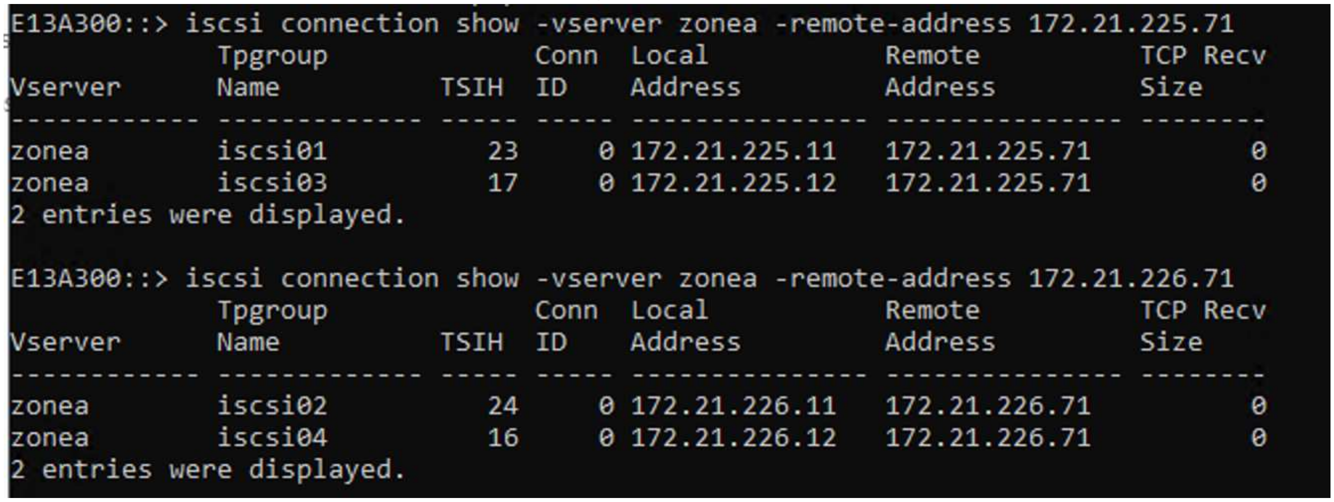
Storage Adapters

	Adapter	Model	Type	Status	Identifier	Targets	Devices	Paths
●	vmhba65	iSCSI Software Adapter	iSCSI	Online	iscsi_vmk(iqn.1998-01.com.vmware:dc01-esxi01.sddc.netapp.com:473524194:65)	4	1	4
○	vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	1	1	1
○	vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	0	0	0
○	vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	1	1	1

☑	iSCSI server
☑	172.21.225.11:3260

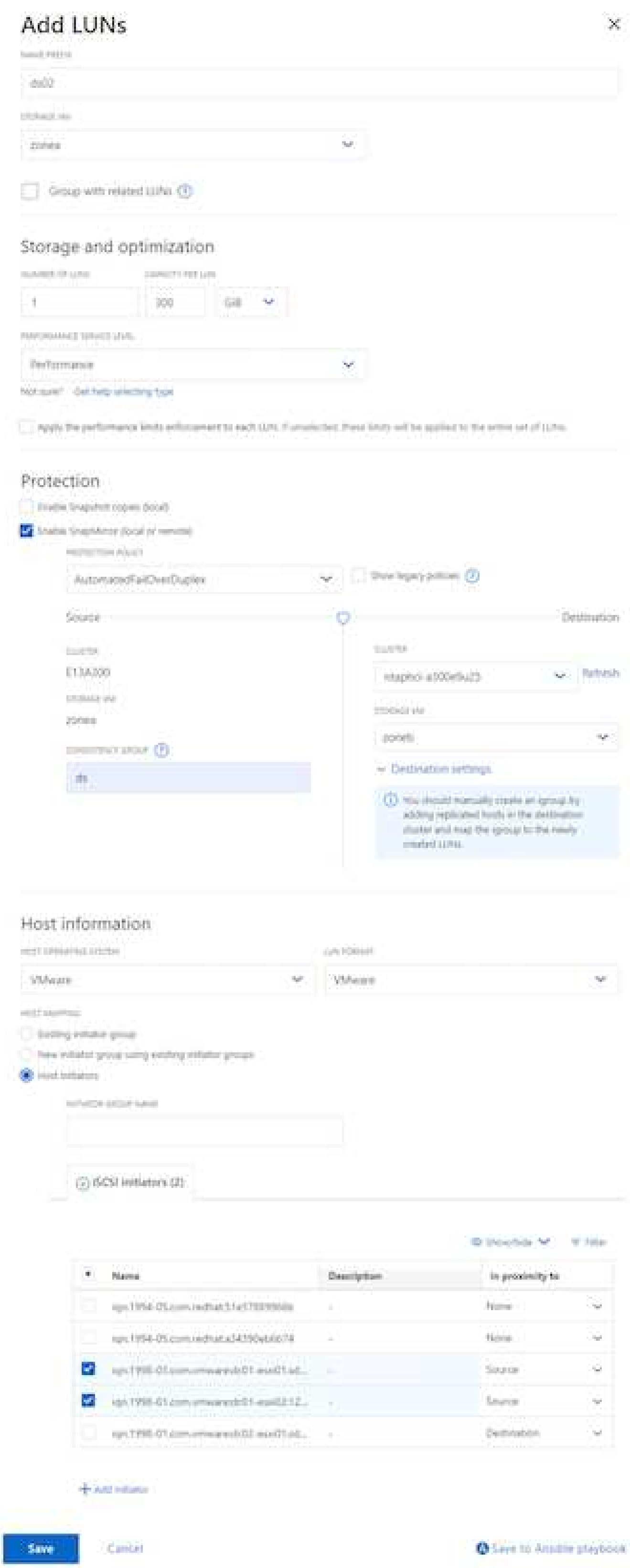
> For Uniform access mode, need to provide the source and target fault domain iSCSI data lif address.

3. Repeat the above step on vSphere hosts for the other fault domain adding its local iSCSI data lif IP on Dynamic Discovery tab.
4. With proper network connectivity, four iSCSI connection should exist per vSphere host that has two iSCSI VMKernel nics and two iSCSI data lifs per storage controller.



```
E13A300::> iscsi connection show -vserver zonea -remote-address 172.21.225.71
             Tpgroup              Conn  Local           Remote          TCP Recv
Vserver      Name            TSIH ID    Address         Address         Size
------------ ------------- ----- ----- --------------- --------------- --------
zonea        iscsi01           23     0 172.21.225.11   172.21.225.71          0
zonea        iscsi03           17     0 172.21.225.12   172.21.225.71          0
2 entries were displayed.

E13A300::> iscsi connection show -vserver zonea -remote-address 172.21.226.71
             Tpgroup              Conn  Local           Remote          TCP Recv
Vserver      Name            TSIH ID    Address         Address         Size
------------ ------------- ----- ----- --------------- --------------- --------
zonea        iscsi02           24     0 172.21.226.11   172.21.226.71          0
zonea        iscsi04           16     0 172.21.226.12   172.21.226.71          0
2 entries were displayed.
```

5. Create LUN using ONTAP System Manager, setup SnapMirror with replication policy AutomatedFailOverDuplex, pick the host initiators and set host proximity.



Add LUNs

NAME PREFIX
ds02

STORAGE VM
zonea

□ Group with related LUNs

Storage and optimization

NUMBER OF LUNS: 1
CAPACITY PER LUN: 300 GiB

PERFORMANCE SERVICE LEVEL
Performance

Not sure? Get help selecting type

□ Apply the performance limits enforcement to each LUN. If unselected, these limits will be applied to the entire set of LUNs.

Protection

□ Enable Snapshot copies (local)

☑ Enable SnapMirror (local or remote)

PROTECTION POLICY
AutomatedFailOverDuplex

□ Show legacy policies

Source

CLUSTER
E13A300

STORAGE VM
zonea

CONSISTENCY GROUP
ds

Destination

CLUSTER
ntaphci-a300e9u25

Refresh

STORAGE VM
zoneb

Destination settings

You should manually create an igroup by adding replicated hosts in the destination cluster and map the igroup to the newly created LUNs.

Host information

HOST OPERATING SYSTEM: VMware
LUN FORMAT: VMware

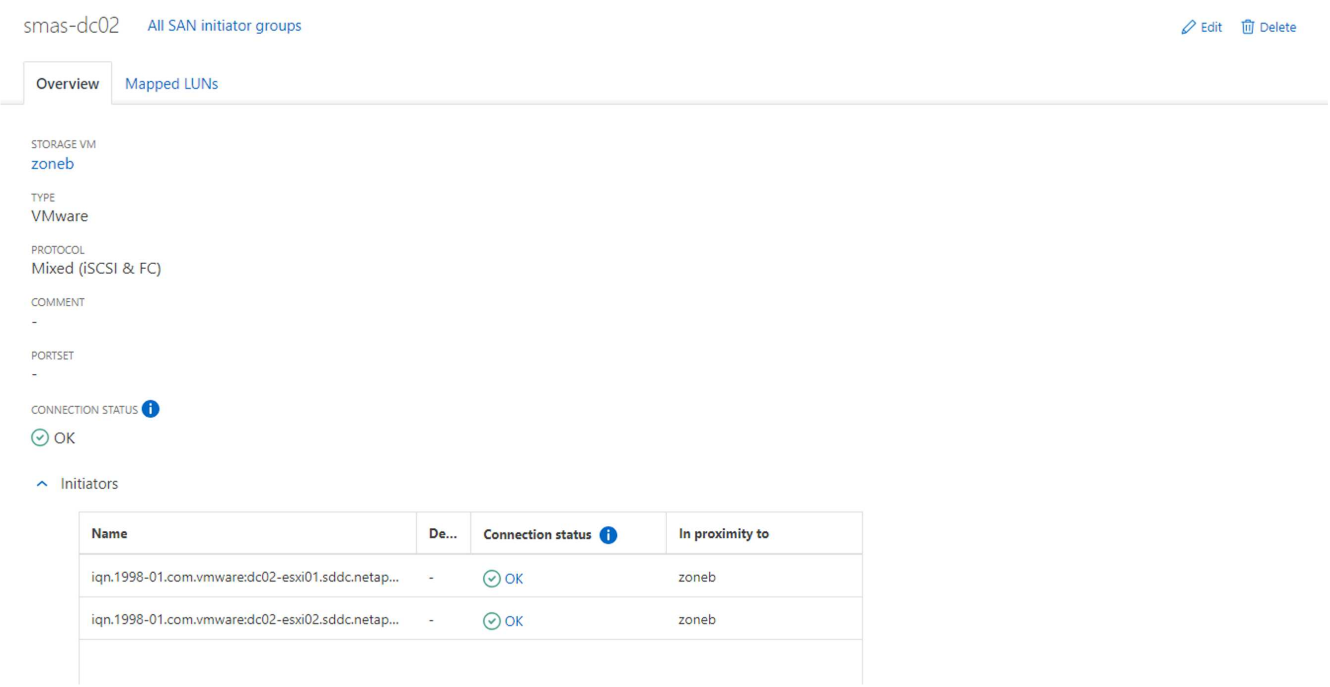
HOST MAPPING
○ Existing initiator group
○ New initiator group using existing initiator groups
● Host initiators

INITIATOR GROUP NAME

iSCSI initiators (2)

	Name	Description	In proximity to
□	iqn.1994-05.com.redhat:51a5780998b6	-	None
□	iqn.1994-05.com.redhat:a34390ebb674	-	None
☑	iqn.1998-01.com.vmware:sb01-esxi01.sd...	-	Source
☑	iqn.1998-01.com.vmware:sb01-esxi02.12...	-	Source
□	iqn.1998-01.com.vmware:sb02-esxi01.sd...	-	Destination

6. On other fault domain storage array, create the SAN initiator group with its vSphere host initiators and set host proximity.



smas-dc02 All SAN initiator groups

STORAGE VM
zoneb

TYPE
VMware

PROTOCOL
Mixed (iSCSI & FC)

COMMENT
-

PORTSET
-

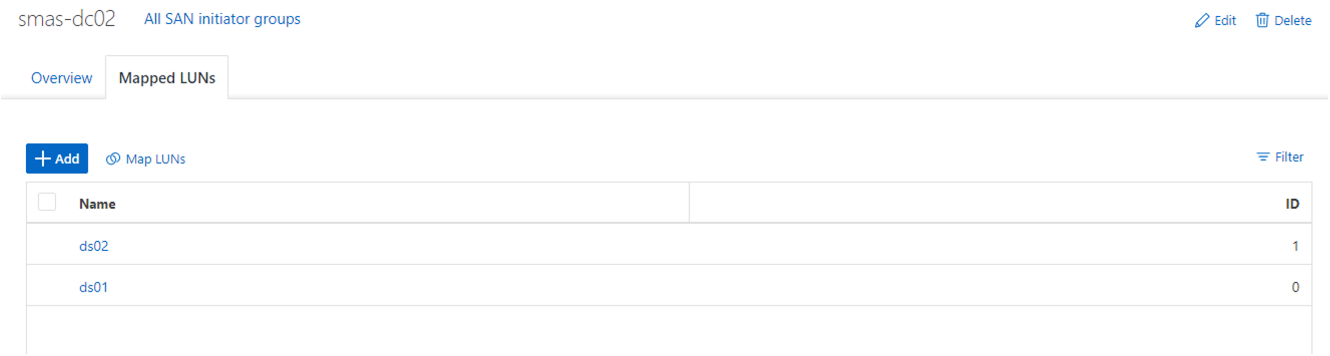
CONNECTION STATUS
OK

Initiators

Name	De...	Connection status	In proximity to
iqn.1998-01.com.vmware:dc02-esxi01.sddc.netap...	-	OK	zoneb
iqn.1998-01.com.vmware:dc02-esxi02.sddc.netap...	-	OK	zoneb

For Uniform access mode, the igroup can be replicated from source fault domain.

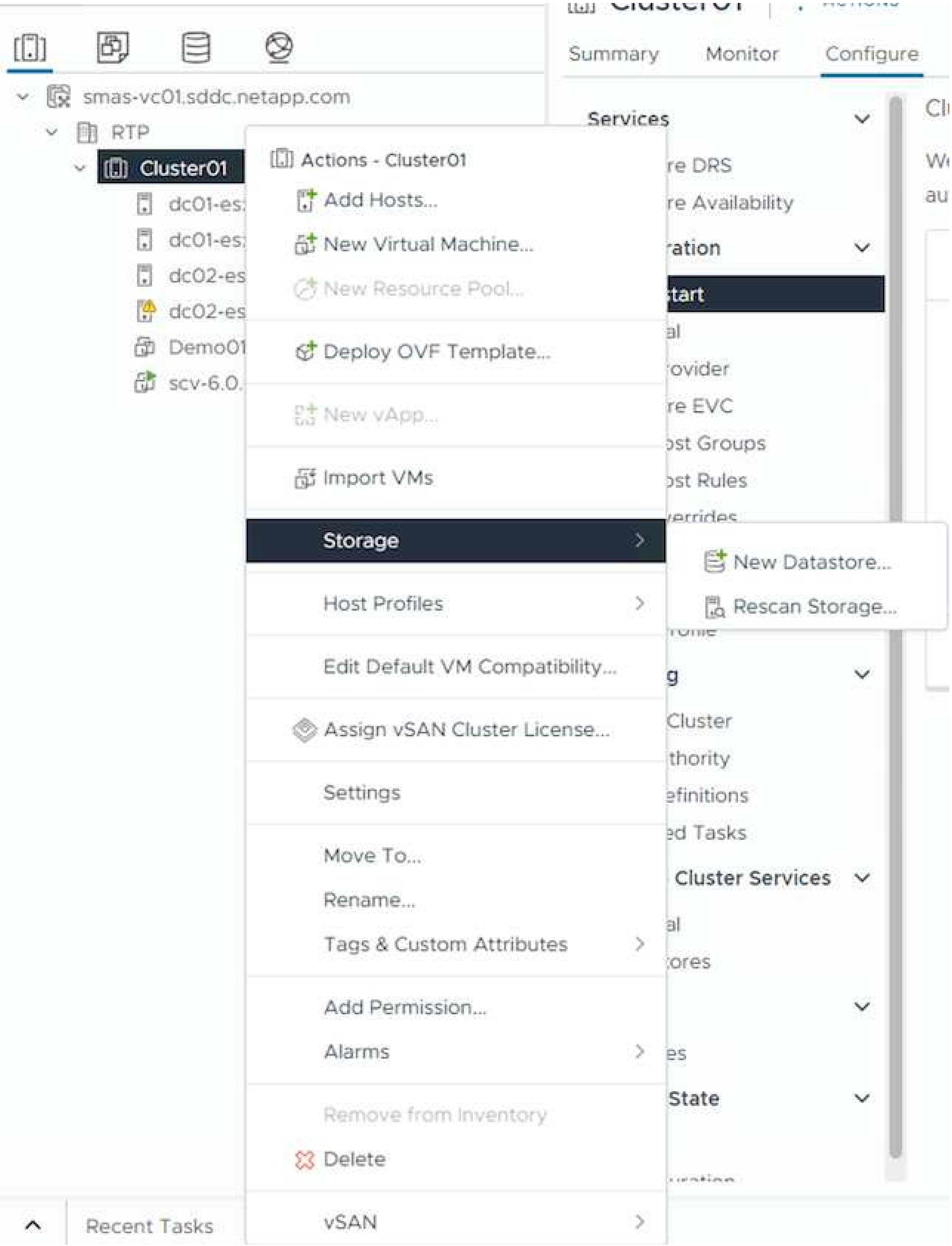
7. Map the replicated LUN with same mapping ID as in source fault domain.



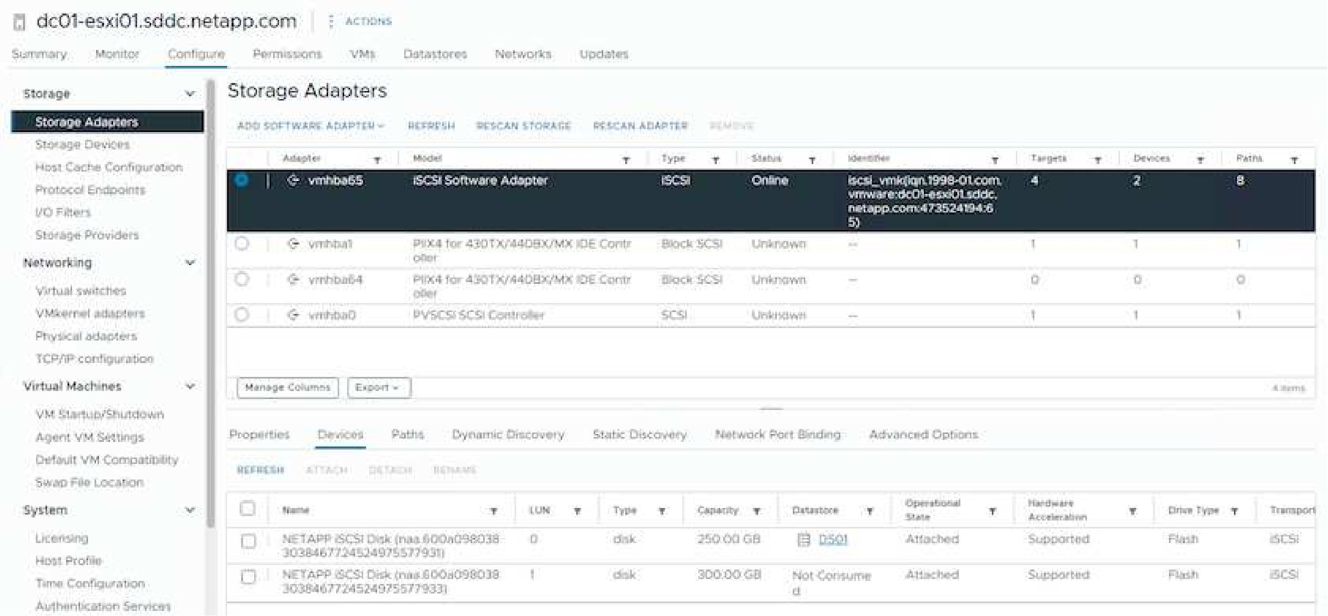
smas-dc02 All SAN initiator groups

Name	ID
ds02	1
ds01	0

8. On vCenter, right click on vSphere Cluster and select Rescan Storage option.



9. On one of the vSphere host in the cluster, check the newly created device shows up with datastore showing Not Consumed.

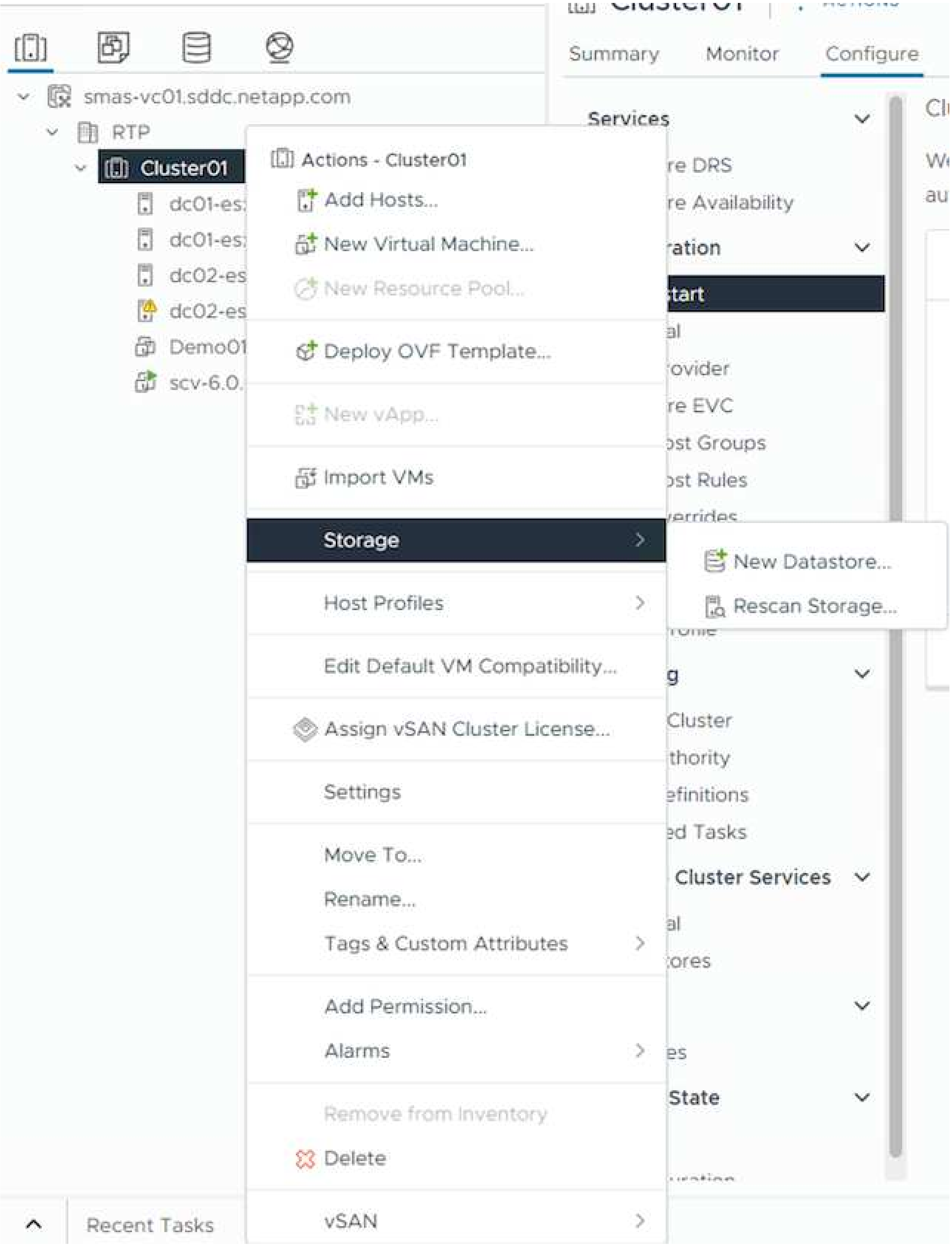


Storage Adapters

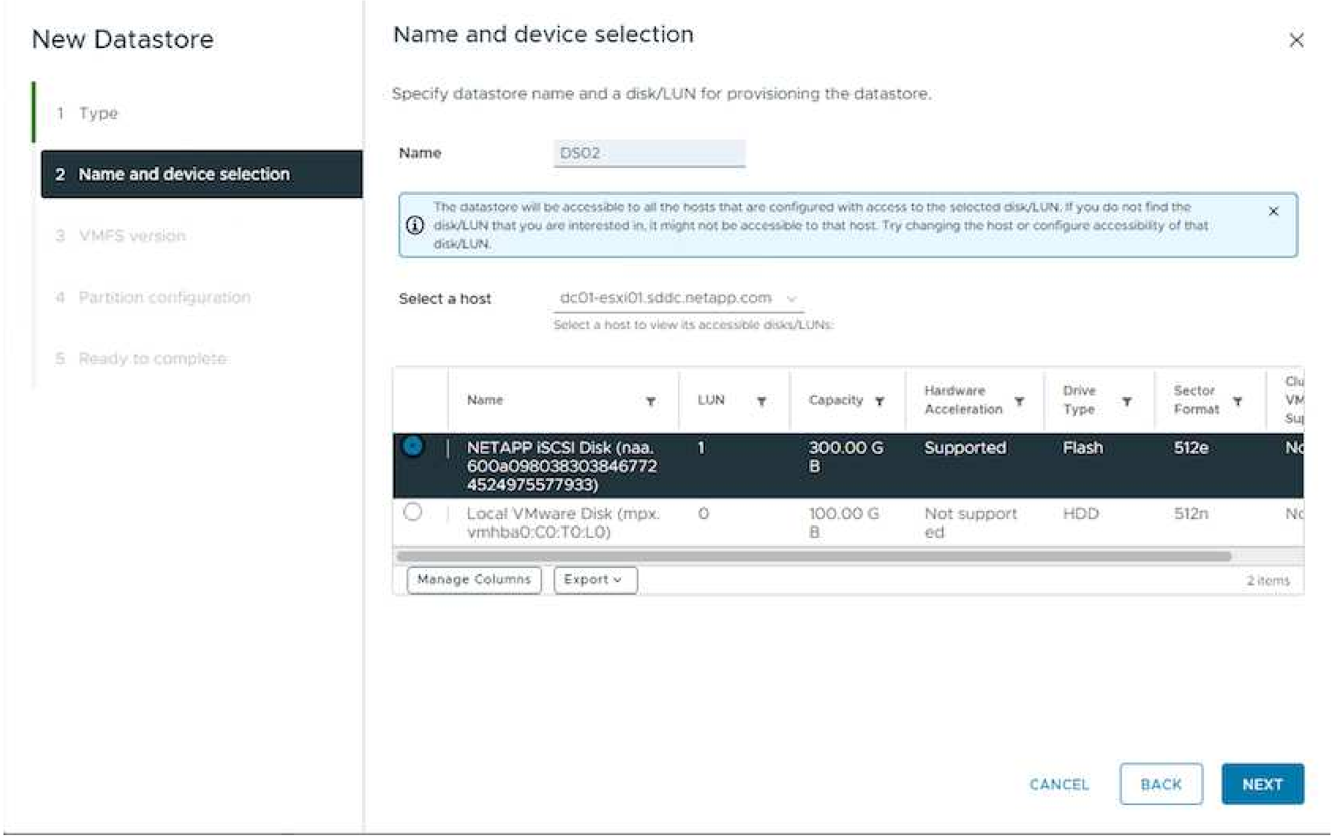
	Adapter	Model	Type	Status	Identifier	Targets	Devices	Paths
●	vmhba65	iSCSI Software Adapter	iSCSI	Online	iscsi_vmk(iqn.1998-01.com.vmware:dc01-esxi01.sddc.netapp.com:473524194:65)	4	2	8
○	vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	1	1	1
○	vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	0	0	0
○	vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	1	1	1

□	Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type	Transport
□	NETAPP iSCSI Disk (naa.600a098038303846772452497557793 1)	0	disk	250.00 GB	DS01	Attached	Supported	Flash	iSCSI
□	NETAPP iSCSI Disk (naa.600a098038303846772452497557793 3)	1	disk	300.00 GB	Not Consumed	Attached	Supported	Flash	iSCSI

10. On vCenter, right click on vSphere Cluster and select New Datastore option.



11. On Wizard, remember to provide the datastore name and select the device with right capacity & device id.



New Datastore

1 Type

2 Name and device selection

3 VMFS version

4 Partition configuration

5 Ready to complete

Name and device selection

Specify datastore name and a disk/LUN for provisioning the datastore.

Name: DS02

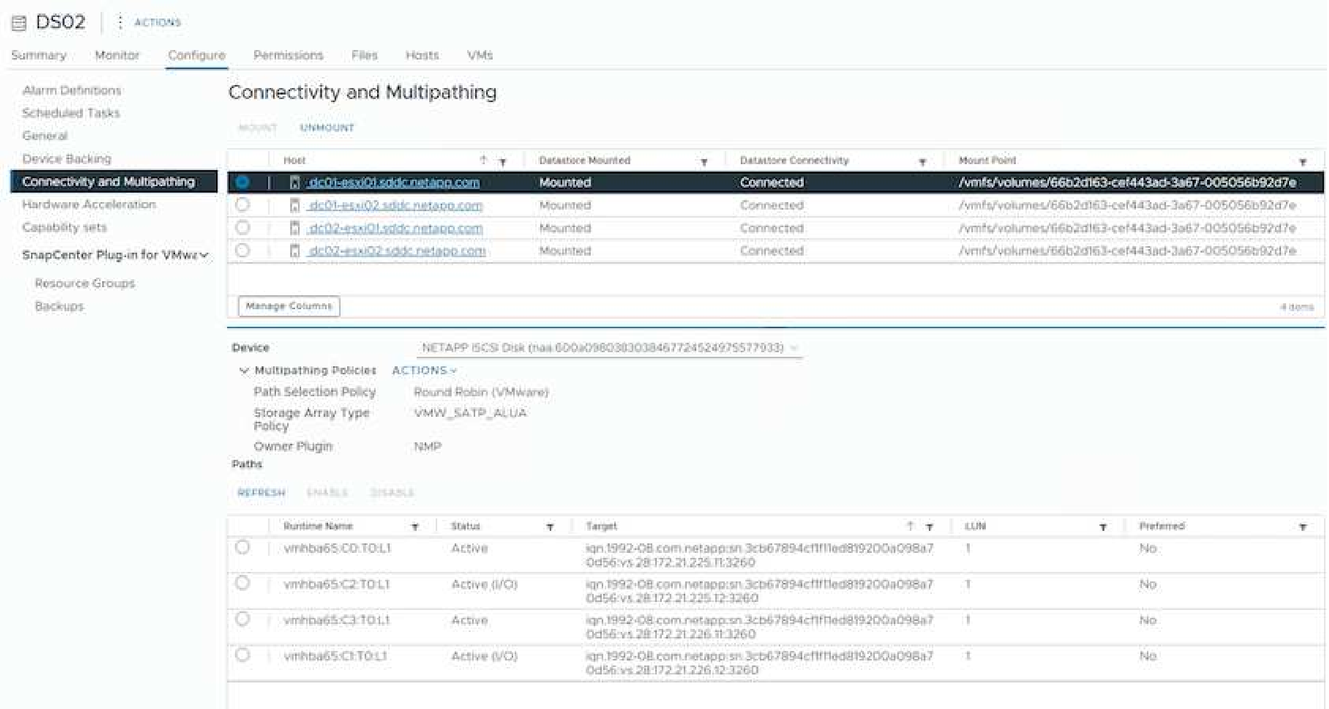
The datastore will be accessible to all the hosts that are configured with access to the selected disk/LUN. If you do not find the disk/LUN that you are interested in, it might not be accessible to that host. Try changing the host or configure accessibility of that disk/LUN.

Select a host: dc01-esxi01.sddc.netapp.com

Select a host to view its accessible disks/LUNs:

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format	Clu VM Su
●	NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)	1	300.00 GB	Supported	Flash	512e	No
○	Local VMware Disk (mpx.vmhba0:C0:T0:L0)	0	100.00 GB	Not supported	HDD	512n	No

12. Verify the datastore is mounted on all hosts on cluster across both fault domains.



Connectivity and Multipathing

	Host	Datastore Mounted	Datastore Connectivity	Mount Point
●	dc01-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
○	dc01-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
○	dc02-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
○	dc02-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e

Device: NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)

Multipathing Policies

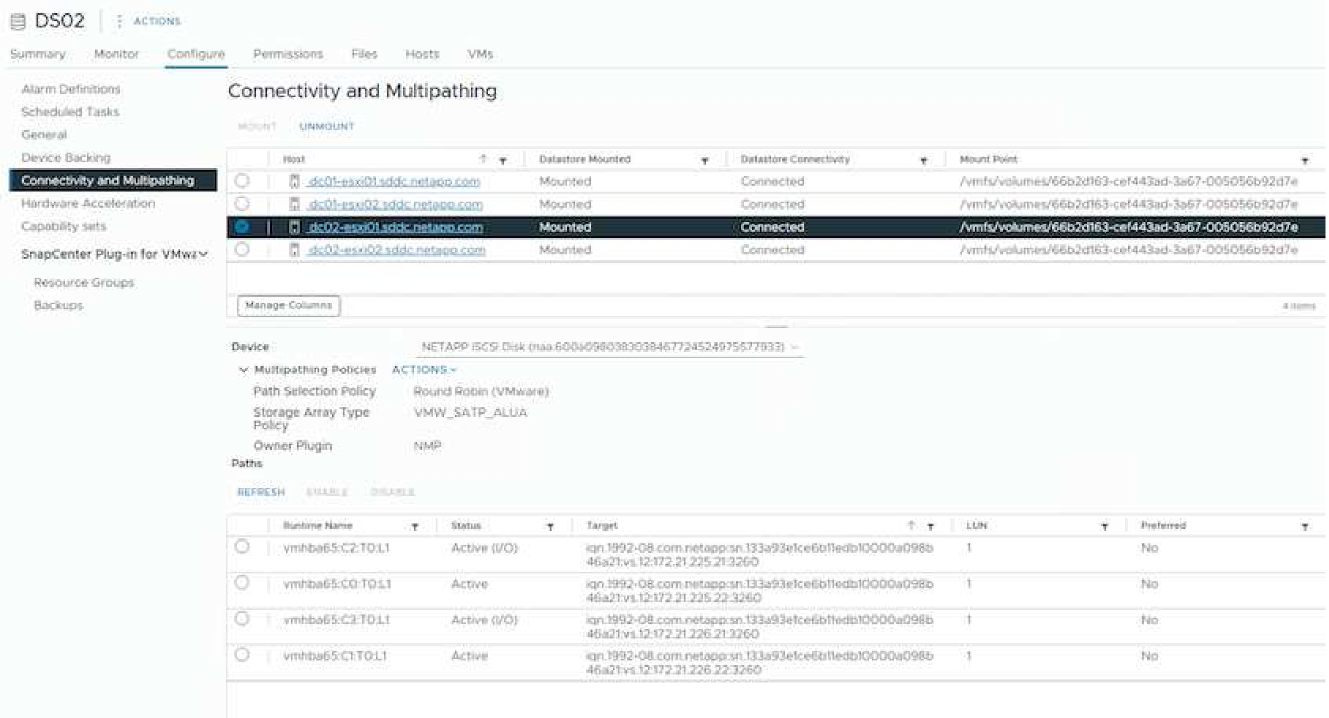
Path Selection Policy: Round Robin (VMware)

Storage Array Type Policy: VMW_SATP_ALUA

Owner Plugin: NMP

Paths

	Runtime Name	Status	Target	LUN	Preferred
○	vmhba65:C0:T0:L1	Active	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.225.11:3260	1	No
○	vmhba65:C2:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.225.12:3260	1	No
○	vmhba65:C3:T0:L1	Active	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.226.11:3260	1	No
○	vmhba65:C1:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.226.12:3260	1	No



DS02 ⋮ ACTIONS

Connectivity and Multipathing

MOUNT UNMOUNT

	Host	Datastore Mounted	Datastore Connectivity	Mount Point
○	dc01-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
○	dc01-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
●	dc02-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
○	dc02-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e

Manage Columns 4 items

Device NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)

Multipathing Policies ACTIONS

Path Selection Policy Round Robin (VMware)

Storage Array Type Policy VMW_SATP_ALUA

Owner Plugin NMP

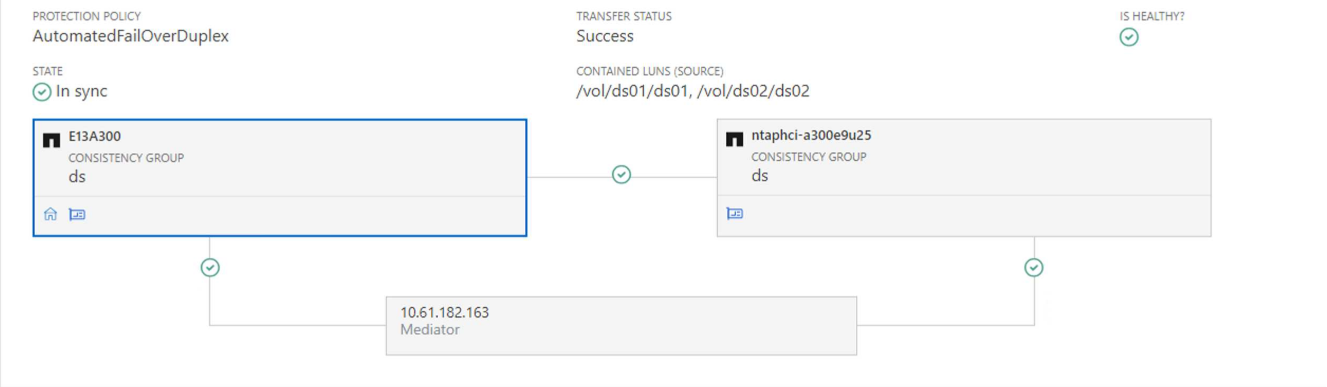
Paths

REFRESH ENABLE DISABLE

	Runtime Name	Status	Target	LUN	Preferred
○	vmhba65:C2:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.225.21:3260	1	No
○	vmhba65:C0:T0:L1	Active	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.225.22:3260	1	No
○	vmhba65:C3:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.226.21:3260	1	No
○	vmhba65:C1:T0:L1	Active	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.226.22:3260	1	No

> ⓘ The above screenshots shows Active I/O on single controller since we used AFF. For ASA, it will have Active IO on all paths.

13. When additional datastores are added, need to remember to expand the existing Consistency Group to have it consistent across the vSphere cluster.



PROTECTION POLICY
AutomatedFailOverDuplex

TRANSFER STATUS
Success

IS HEALTHY?
✓

STATE
✓ In sync

CONTAINED LUNS (SOURCE)
/vol/ds01/ds01, /vol/ds02/ds02

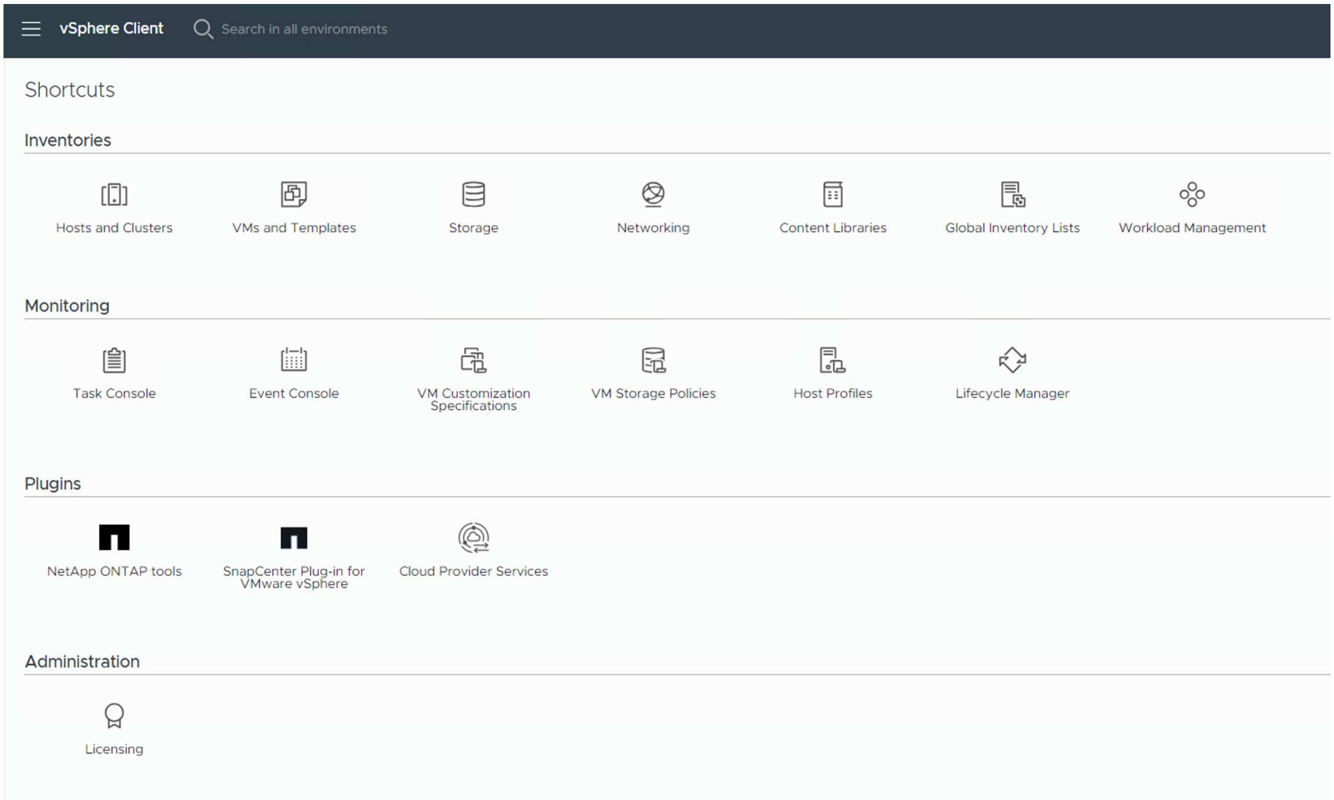
E13A300
CONSISTENCY GROUP
ds

ntaphci-a300e9u25
CONSISTENCY GROUP
ds

10.61.182.163
Mediator

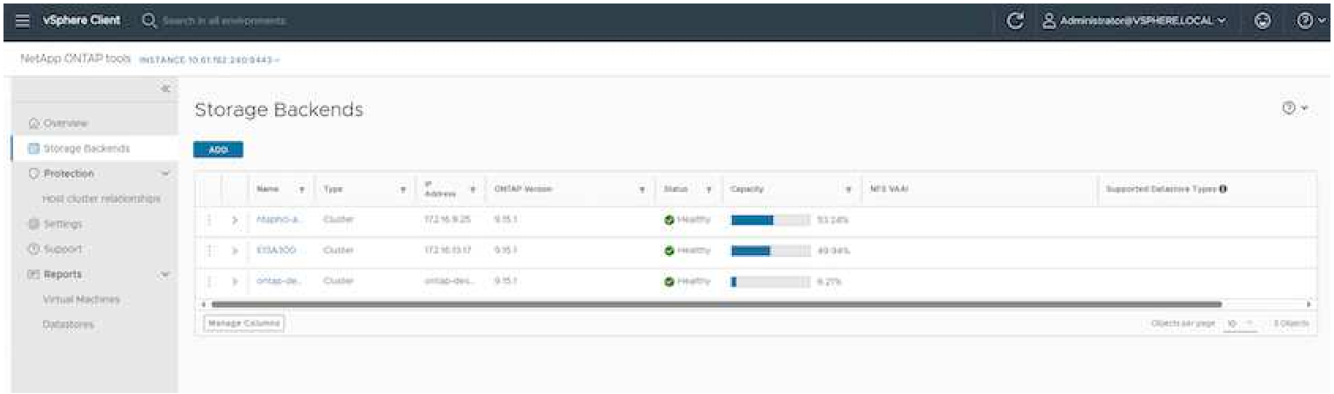
vMSC uniform host access mode with ONTAP Tools.

1. Ensure NetApp ONTAP Tools is deployed and registered to vCenter.



If not, follow ONTAP Tools deployment and Add a vCenter server instance

2. Ensure ONTAP Storage systems are registered to ONTAP Tools. This includes both fault domain storage systems and third one for Asynchronous remote replication to use for VM protection with SnapCenter Plugin for VMware vSphere.

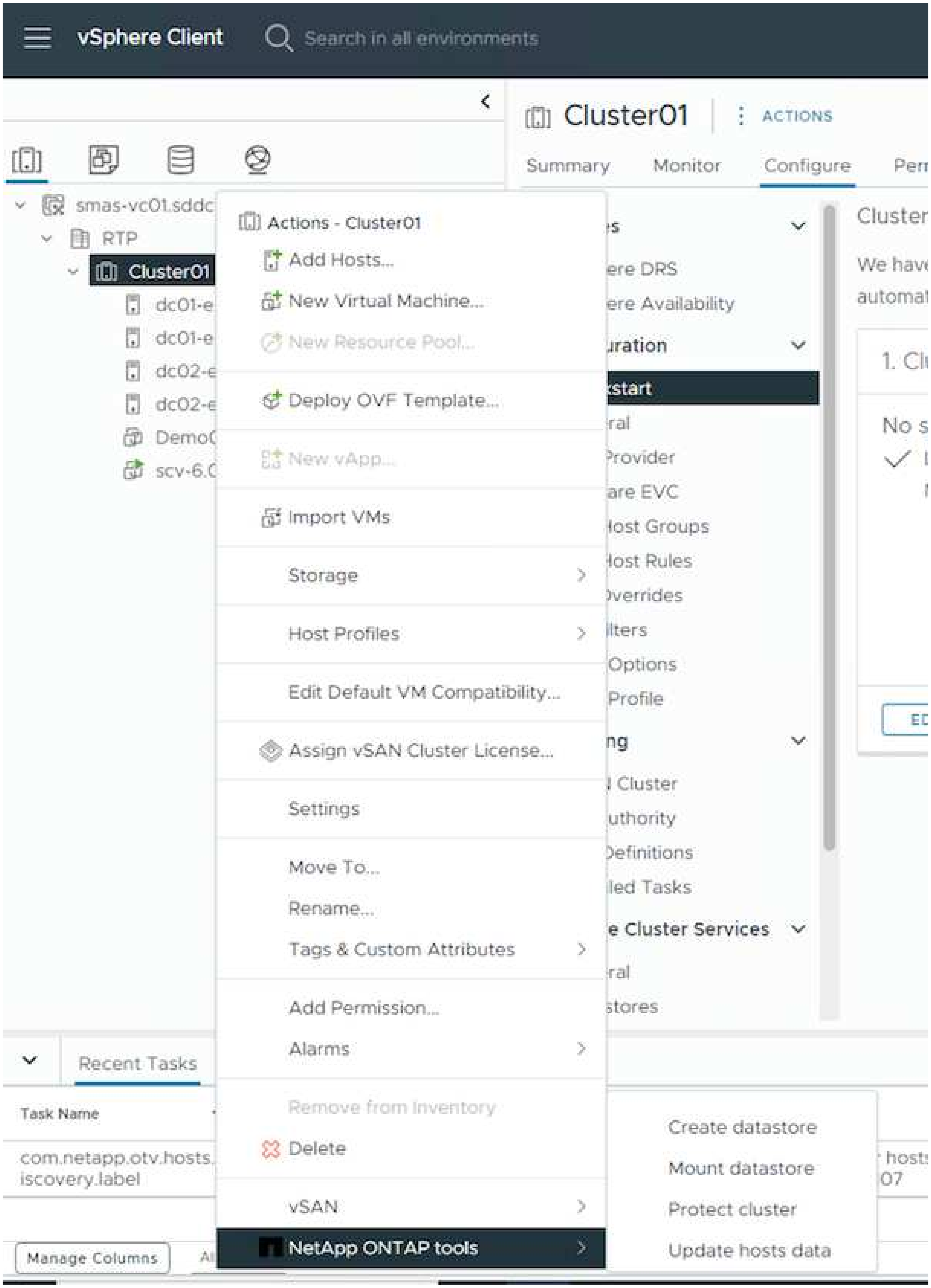


Storage Backends

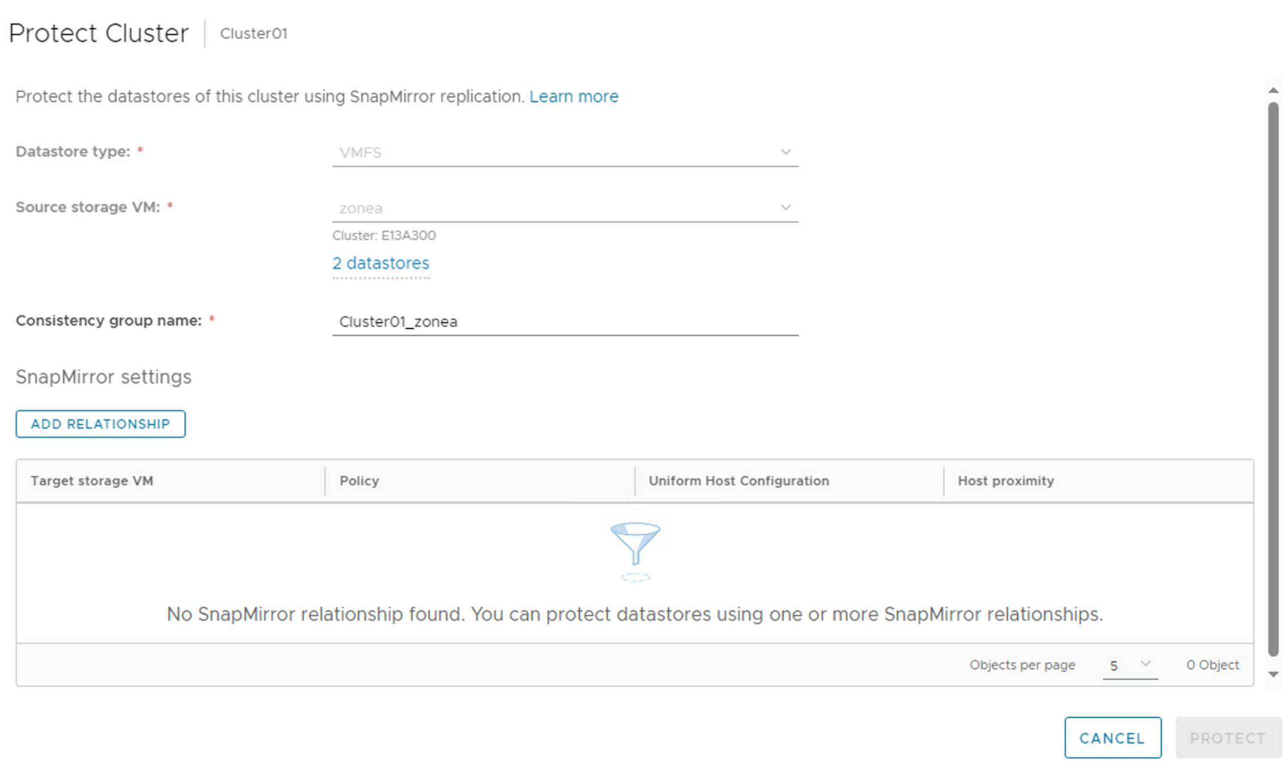
Name	Type	IP Address	ONTAP Version	Status	Capacity	NFS VAAI	Supported Datastore Types
HApho-a...	Cluster	172.16.9.25	9.15.1	Healthy	53.24%		
E13A300	Cluster	172.16.13.17	9.15.1	Healthy	40.94%		
ontap-de...	Cluster	ontap-des...	9.15.1	Healthy	6.27%		

If not, follow Add storage backend using vSphere client UI

3. Update hosts data to sync with ONTAP Tools and then, create a datastore.



4. To enable SM-as, right click on vSphere cluster and pick Protect cluster on NetApp ONTAP Tools (refer above screenshot)
5. It will show existing datastores for that cluster along with SVM details. The default CG name is <vSphere Cluster name>_<SVM name>. Click on Add Relationship button.


Protect Cluster | Cluster01

Protect the datastores of this cluster using SnapMirror replication. Learn more

Datastore type: * VMFS

Source storage VM: * zonea

Cluster: E13A300

2 datastores

Consistency group name: * Cluster01_zonea

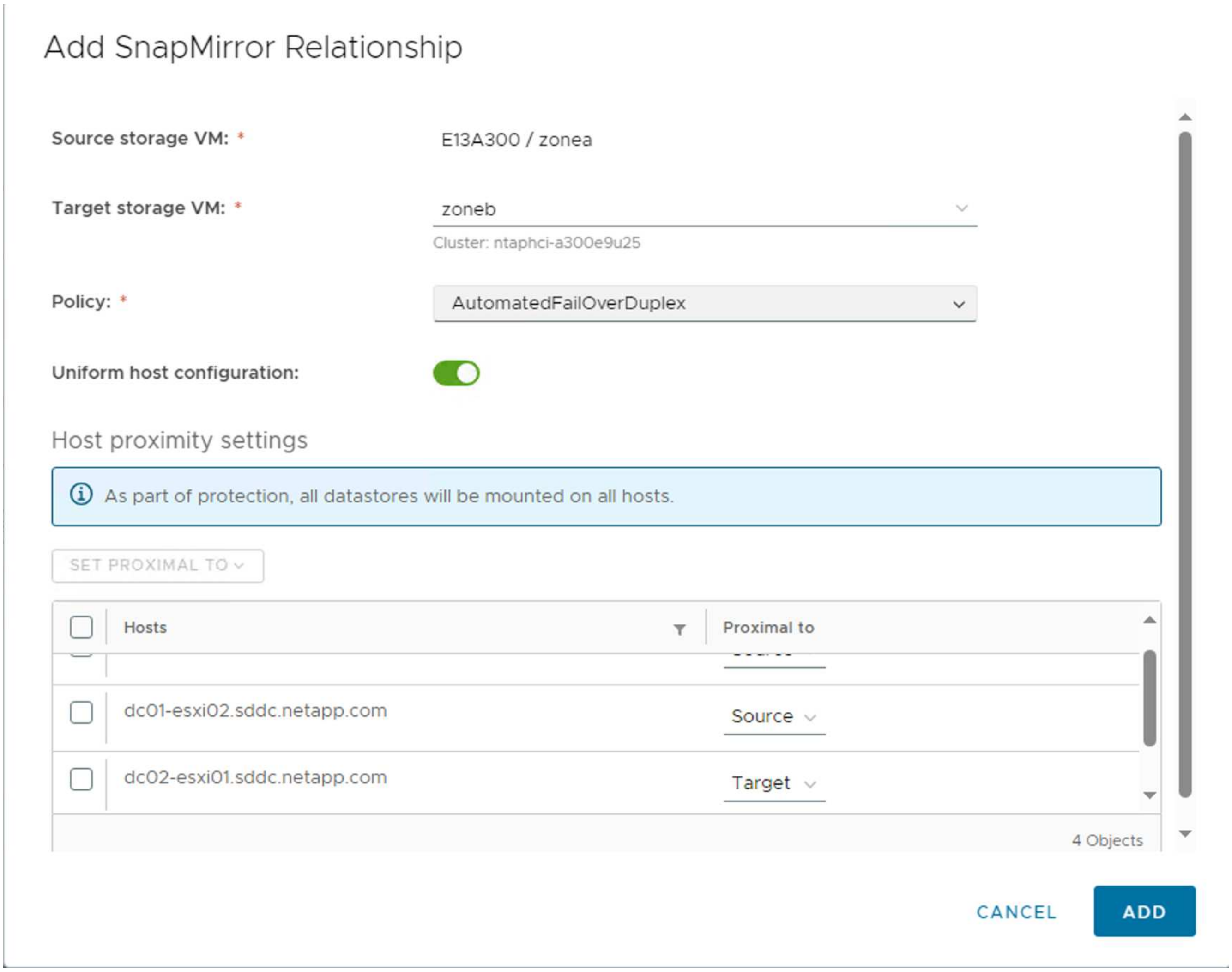
SnapMirror settings

Target storage VM	Policy	Uniform Host Configuration	Host proximity

No SnapMirror relationship found. You can protect datastores using one or more SnapMirror relationships.

Objects per page 5 0 Object

6. Pick the target SVM and set the policy to AutomatedFailOverDuplex for SM-as. There is a toggle switch for Uniform host configuration. Set the proximity for each host.



Add SnapMirror Relationship

Source storage VM: * E13A300 / zonea

Target storage VM: * zoneb

Cluster: ntaphci-a300e9u25

Policy: * AutomatedFailOverDuplex

Uniform host configuration: ●

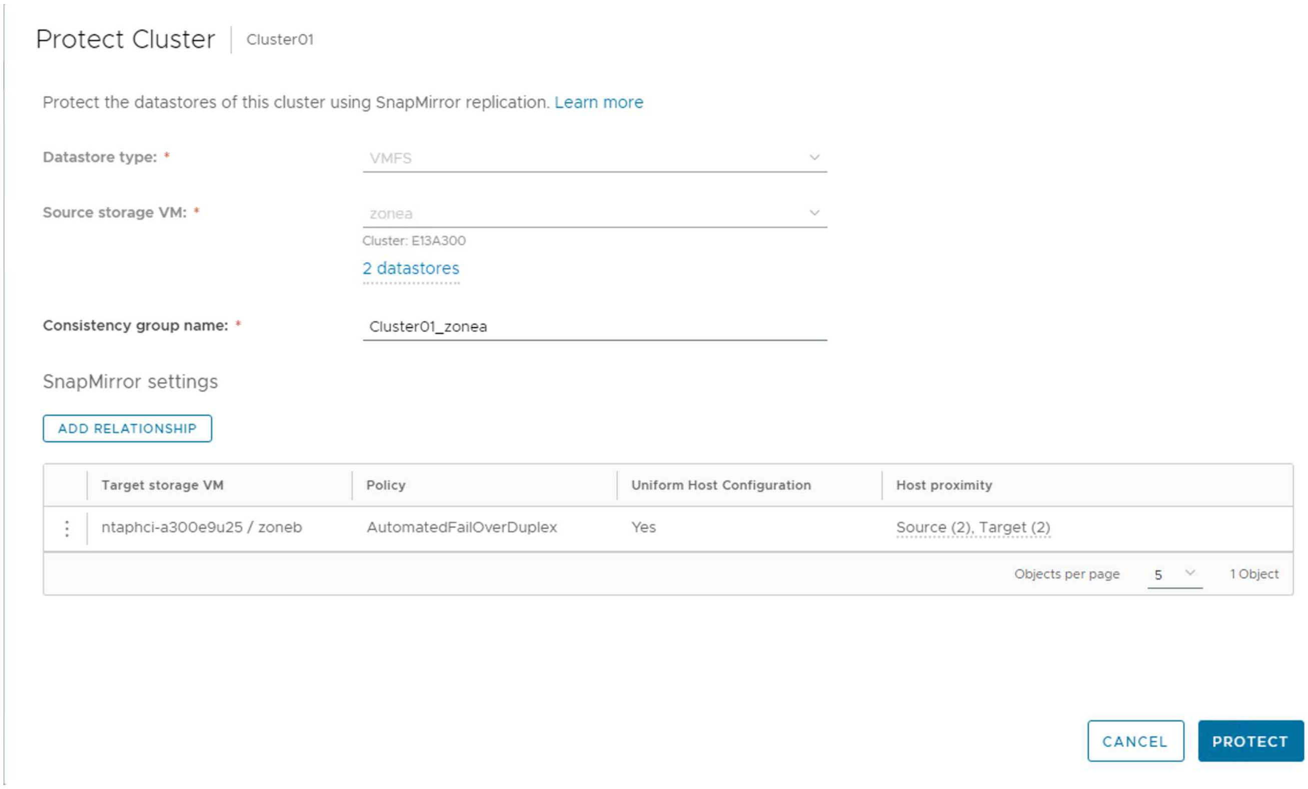
Host proximity settings

ⓘ As part of protection, all datastores will be mounted on all hosts.

□	Hosts	Proximal to
□	dc01-esxi02.sddc.netapp.com	Source
□	dc02-esxi01.sddc.netapp.com	Target

4 Objects

7. Verify the host promity info and other details. Add another relationship to third site with replication policy of Asynchronous if required. Then, click on Protect.



Protect Cluster | Cluster01

Protect the datastores of this cluster using SnapMirror replication. Learn more

Datastore type: * VMFS

Source storage VM: * zonea
Cluster: E13A300
2 datastores

Consistency group name: * Cluster01_zonea

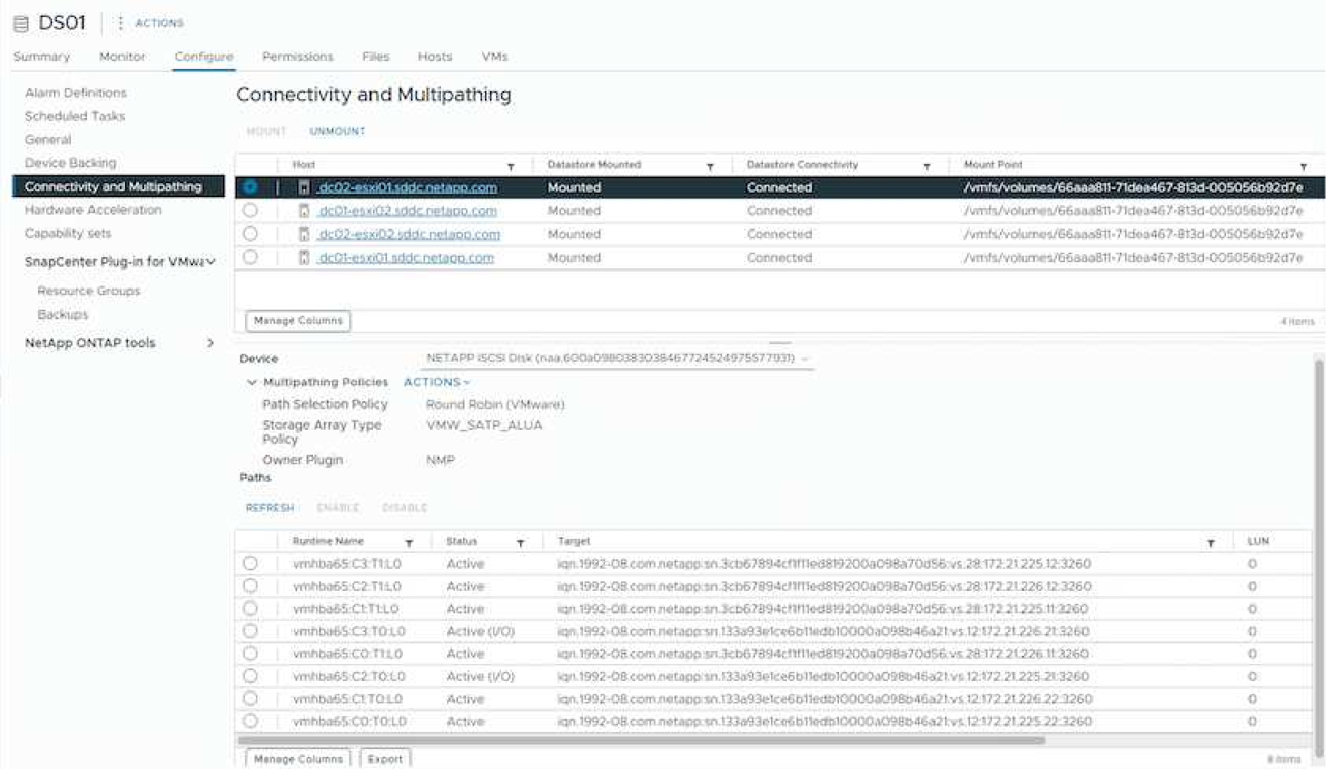
SnapMirror settings

	Target storage VM	Policy	Uniform Host Configuration	Host proximity
⋮	ntaphci-a300e9u25 / zoneb	AutomatedFailOverDuplex	Yes	Source (2), Target (2)

Objects per page 5 1 Object

NOTE: If plan to use SnapCenter Plug-in for VMware vSphere 6.0, the replication needs to be setup at volume level rather than at Consistency Group level.

8. With Uniform host access, the host has iSCSI connection to both fault domain storage arrays.



Connectivity and Multipathing

	Host	Datastore Mounted	Datastore Connectivity	Mount Point
●	dc02-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e
○	dc01-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e
○	dc02-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e
○	dc01-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e

Device NETAPP iSCSI Disk (naa.600a0980383038467724524975577931)

Multipathing Policies ACTIONS

Path Selection Policy Round Robin (VMware)

Storage Array Type Policy VMW_SATP_ALUA

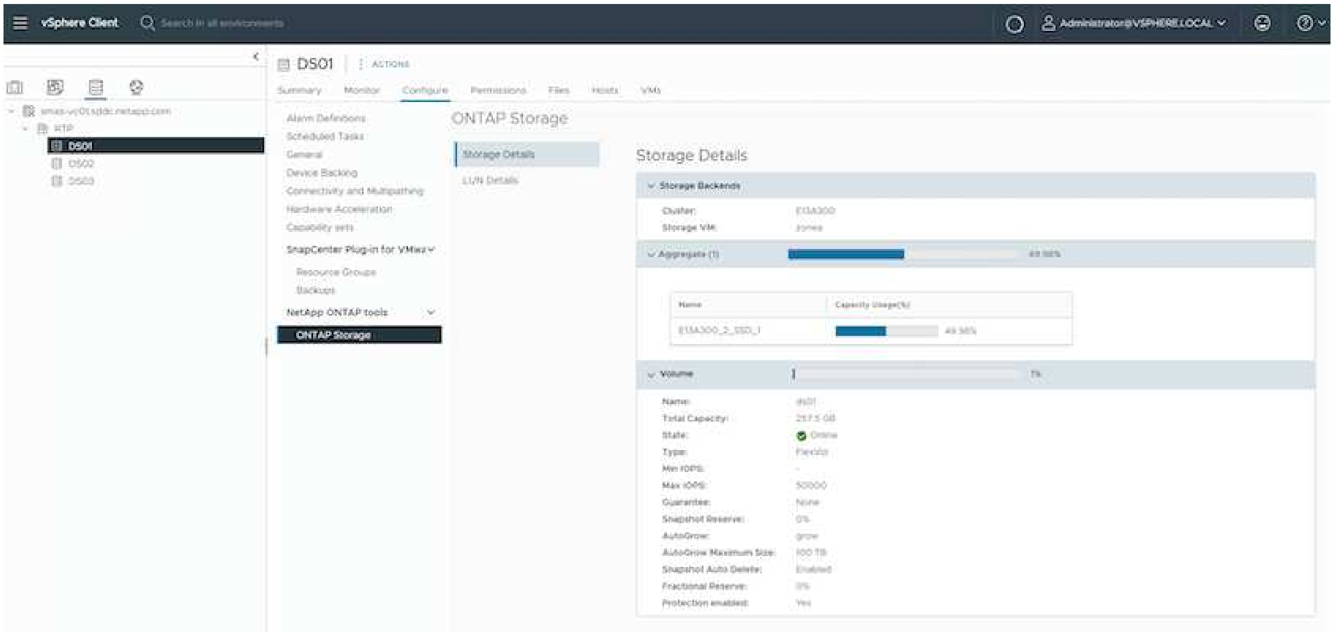
Owner Plugin NMP

Paths

	Runtime Name	Status	Target	LUN
○	vmhba65:C3:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.225.12:3260	0
○	vmhba65:C2:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.226.12:3260	0
○	vmhba65:C1:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.225.11:3260	0
○	vmhba65:C3:T0:L0	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.226.21:3260	0
○	vmhba65:C0:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.226.11:3260	0
○	vmhba65:C2:T0:L0	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.225.21:3260	0
○	vmhba65:C1:T0:L0	Active	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.226.22:3260	0
○	vmhba65:C0:T0:L0	Active	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.225.22:3260	0

NOTE: The above screenshot is from AFF. If ASA, ACTIVE I/O should be in all paths with proper network connections.

9. ONTAP Tools plugin also indicates the volume is protected or not.



Storage Details

Storage Backends

Cluster: E13A300
Storage VM: zonea

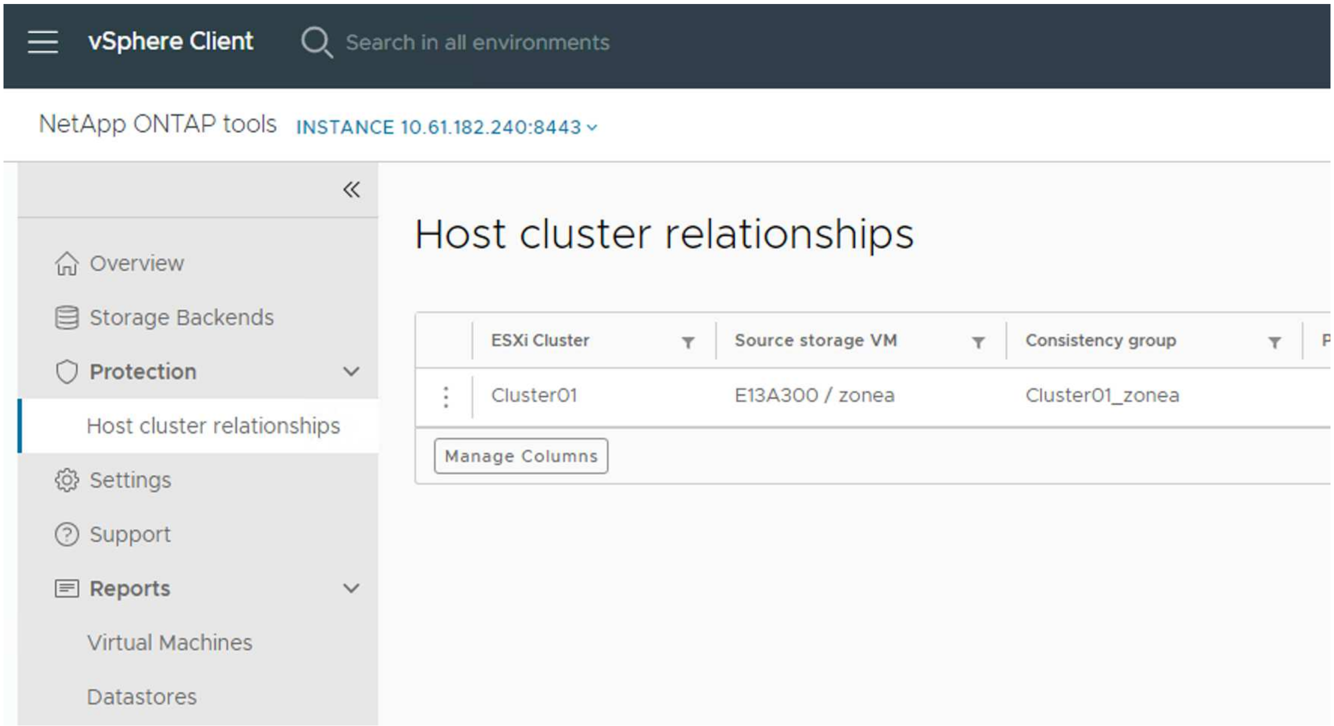
Aggregate (1) 49.98%

Name	Capacity Usage(%)
E13A300_2_SSD_1	49.98%

Volume 1%

Name: ds01
Total Capacity: 217.5 GB
State: Online
Type: FlexVol
Min IOPS: -
Max IOPS: 50000
Guarantee: None
Snapshot Reserve: 0%
AutoGrow: grow
AutoGrow Maximum Size: 100 TB
Snapshot Auto Delete: Enabled
Fractional Reserve: 0%
Protection enabled: Yes

10. For more details and to update the host proximity info, Host cluster relationships option under the ONTAP Tools can be utilized.

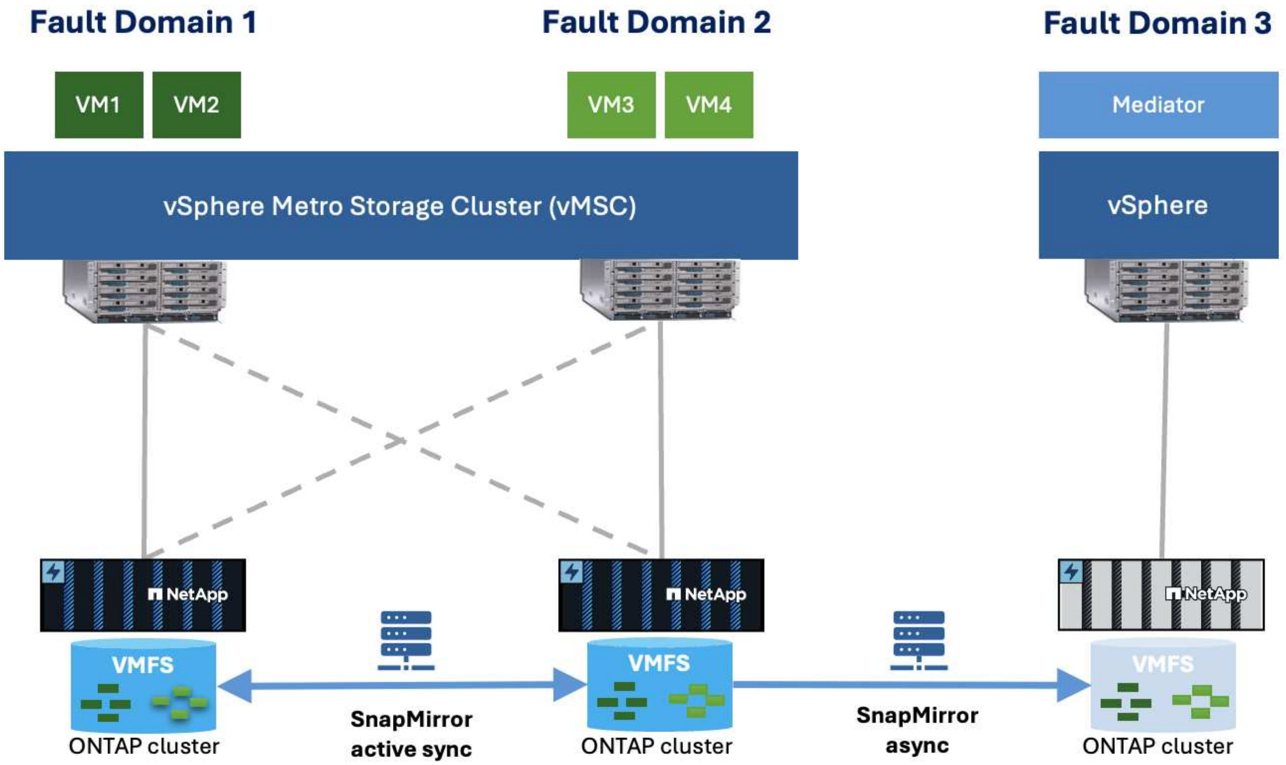


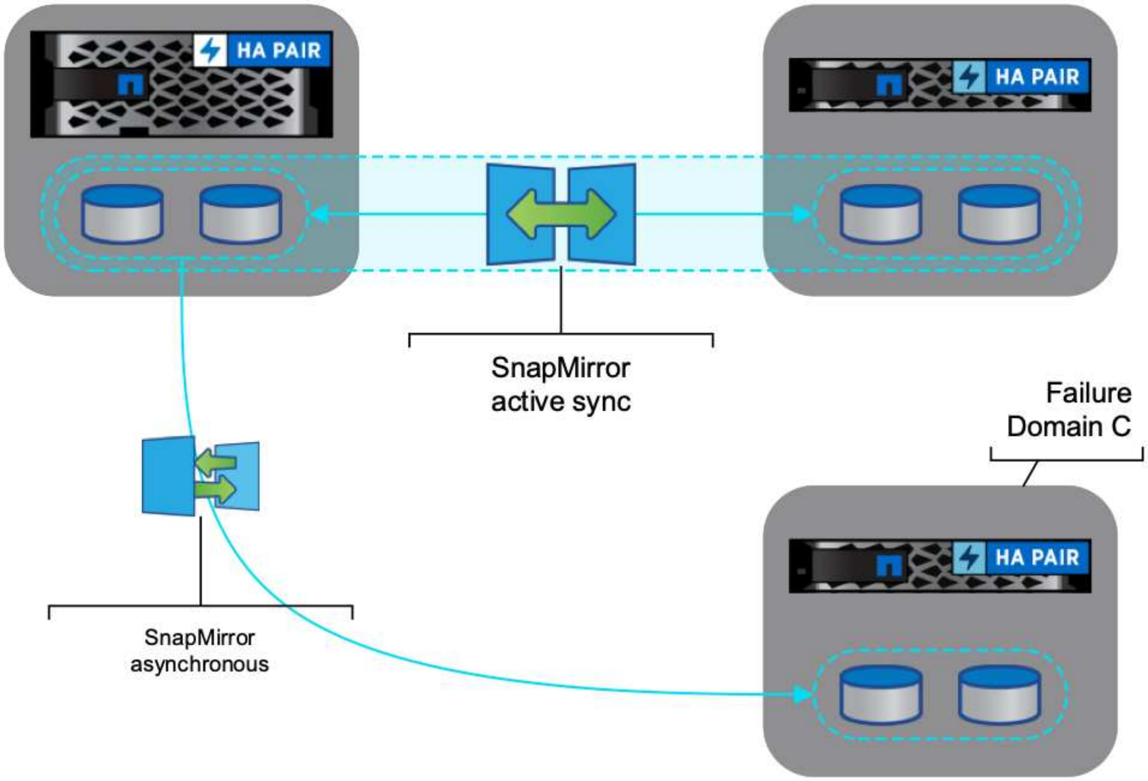
Host cluster relationships

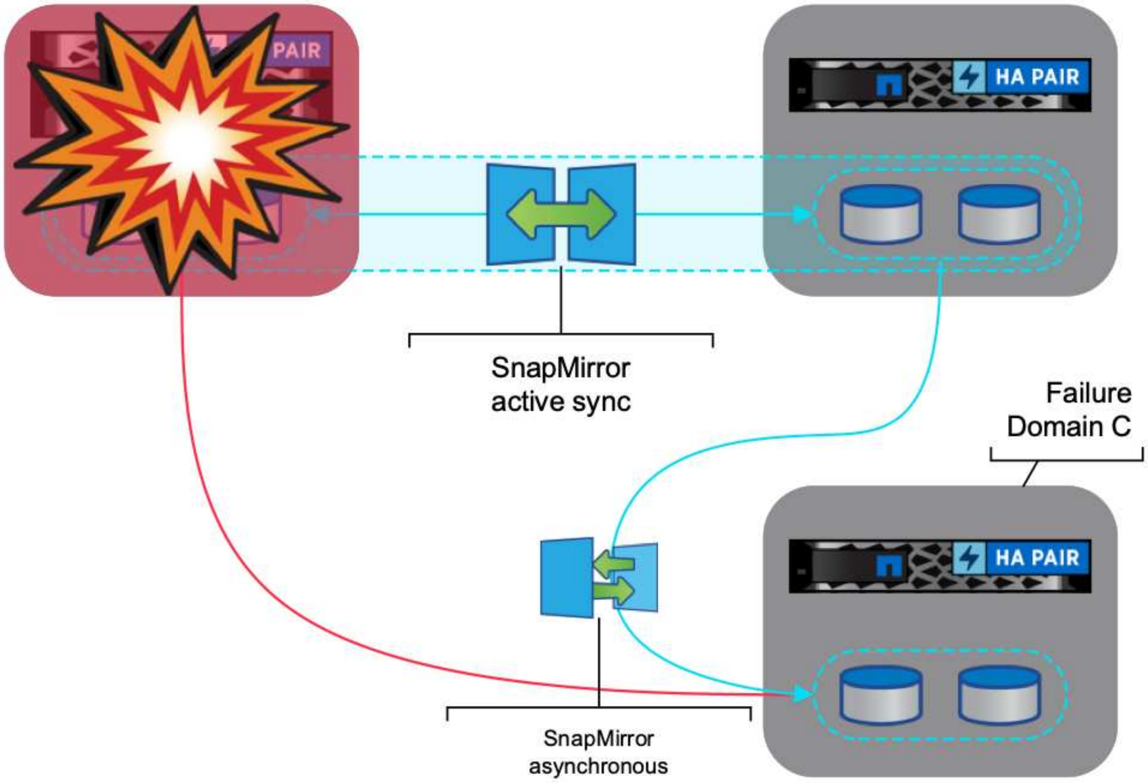
ESXi Cluster	Source storage VM	Consistency group	P
Cluster01	E13A300 / zonea	Cluster01_zonea	

VM protection with SnapCenter plug-in for VMware vSphere.

SnapCenter Plug-in for VMware vSphere (SCV) 6.0 or above supports SnapMirror active sync and also in combination with SnapMirror Async to replicate to third fault domain.

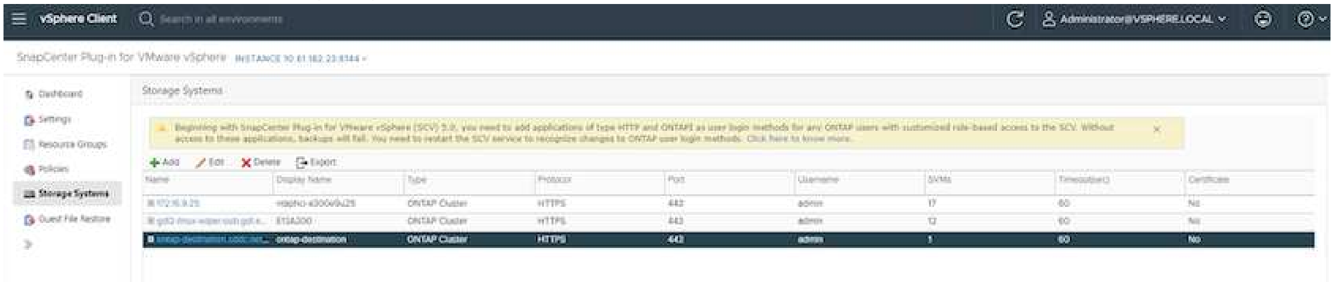

Fault Domain 1
Fault Domain 2
Fault Domain 3
VM1
VM2
VM3
VM4
Mediator
vSphere Metro Storage Cluster (vMSC)
vSphere
NetApp
NetApp
NetApp
VMFS
VMFS
VMFS
ONTAP cluster
SnapMirror active sync
ONTAP cluster
SnapMirror async
ONTAP cluster


HA PAIR
HA PAIR
SnapMirror active sync
Failure Domain C
HA PAIR
SnapMirror asynchronous


PAIR
HA PAIR
SnapMirror active sync
Failure Domain C
HA PAIR
SnapMirror asynchronous

Supported use-cases include:
* Backup and Restore the VM or Datastore from either of fault domains with SnapMirror active sync.
* Restore resources from third fault domain.

1. Add all the ONTAP Storage Systems planned to use in SCV.

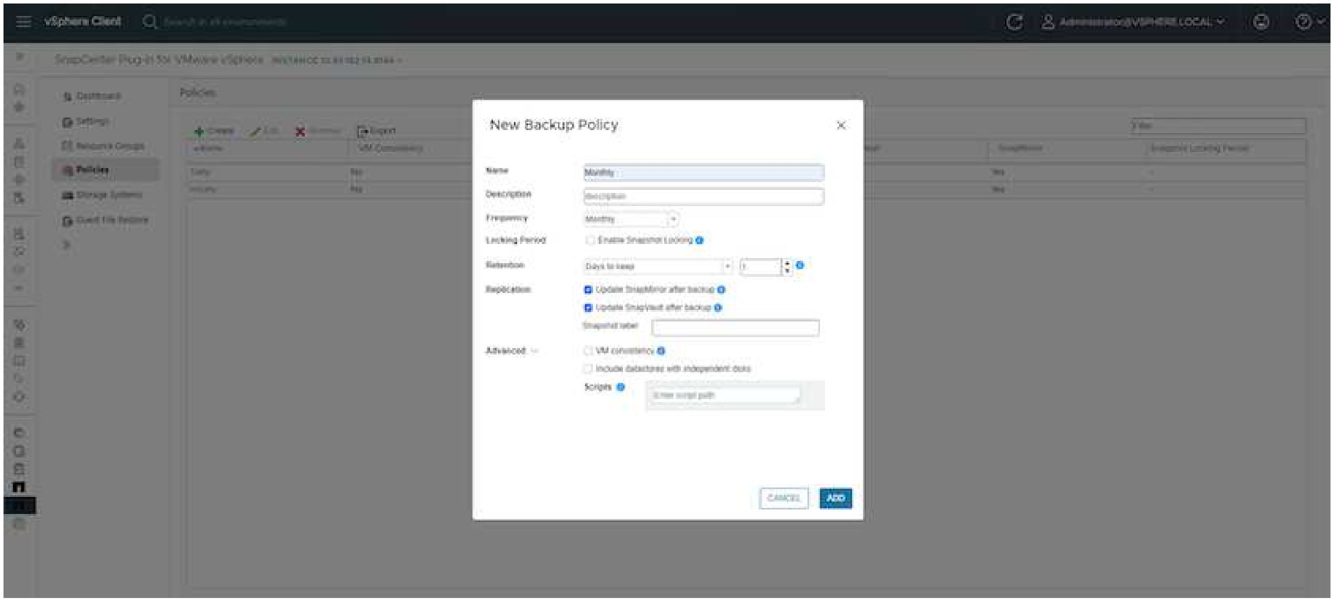


Storage Systems

Beginning with SnapCenter Plug-in for VMware vSphere (SCV) 5.0, you need to add applications of type HTTP and ONTAPI as user login methods for any ONTAP users with customized role-based access to the SCV. Without access to these applications, backups will fail. You need to restart the SCV service to recognize changes to ONTAP user login methods. Click here to know more.

Name	Display Name	Type	Protocol	Port	Username	SVMs	Timeout(sec)	Certificate
172.16.9.25	[illegible]	ONTAP Cluster	HTTPS	443	admin	17	60	No
[illegible]	[illegible]	ONTAP Cluster	HTTPS	443	admin	12	60	No
[illegible]	ontap-destination	ONTAP Cluster	HTTPS	443	admin	1	60	No

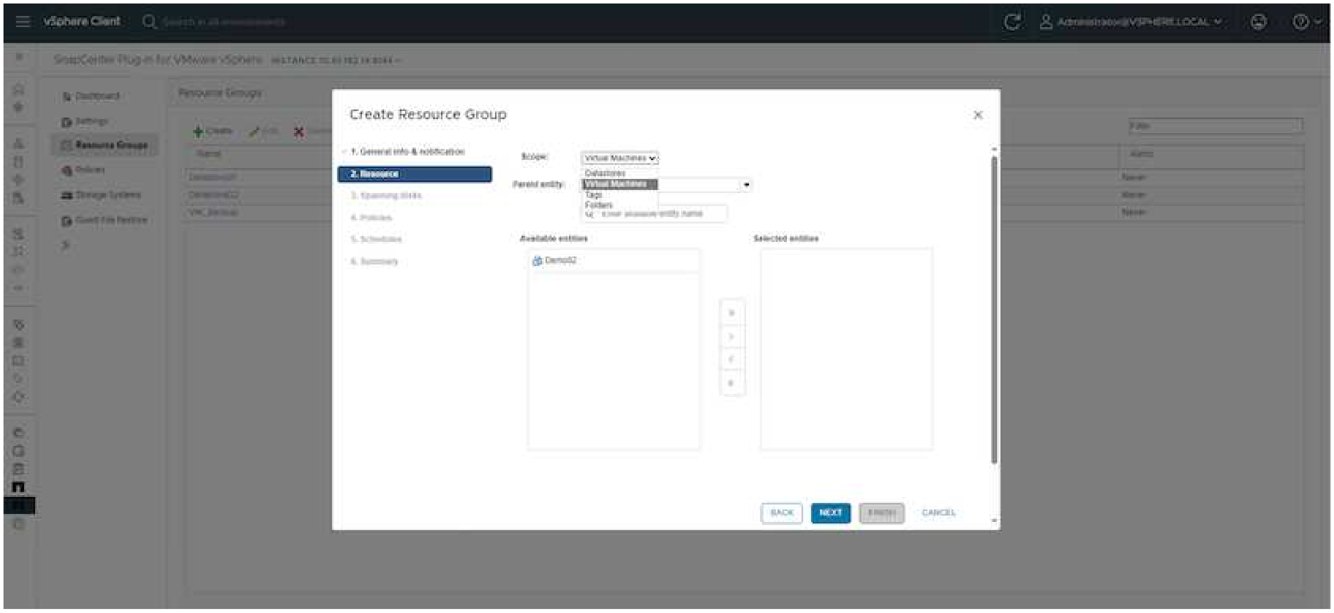
2. Create Policy. Ensure Update SnapMirror after backup is checked for SM-as and also Update SnapVault after backup for Async replication to third fault domain.



New Backup Policy

Name: Monthly
Description: description
Frequency: Monthly
Locking Period: □ Enable Snapshot Locking
Retention: Days to keep 1
Replication: ☑ Update SnapMirror after backup
☑ Update SnapVault after backup
Snapshot label:
Advanced: □ VM consistency
□ Include datastores with independent disks
Scripts: Enter script path

3. Create Resource Group with desiered items that need to be protected, associate to policy and schedule.

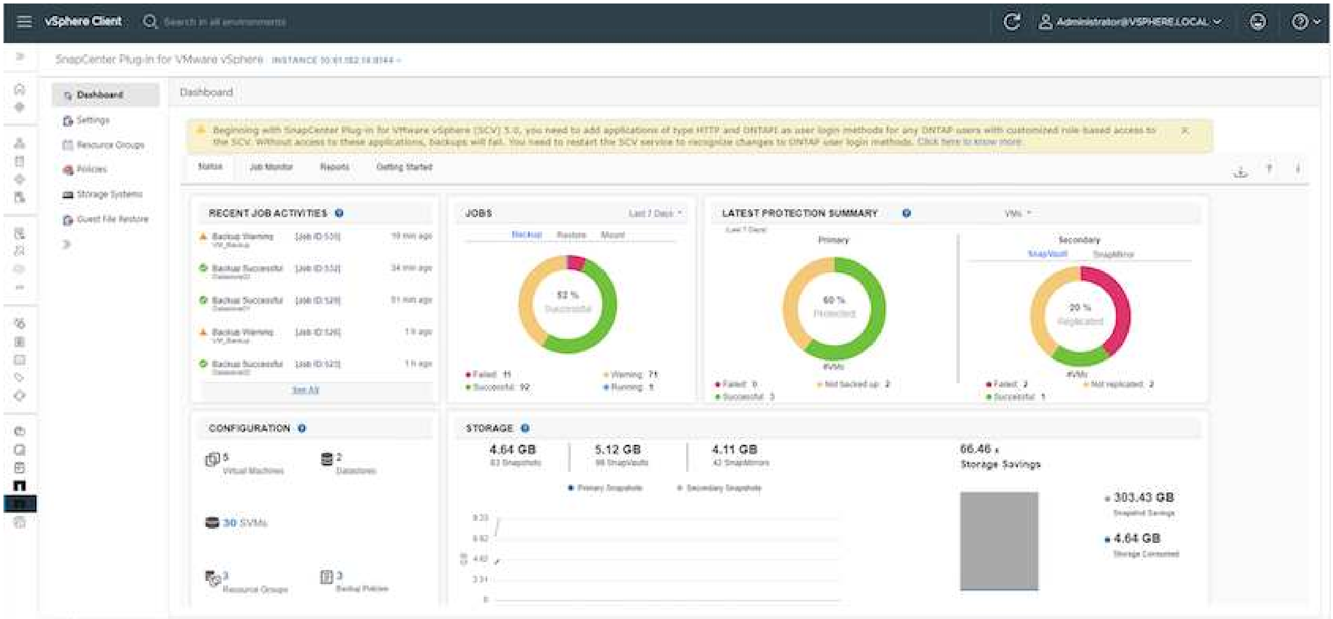


Create Resource Group

Scope: Virtual Machines
Parent entity: Virtual Machines
Available entities: Demo02
Selected entities

NOTE: Snapshot name ending with _recent is not supported with SM-as.

4. Backups occur at scheduled time based on Policy associated to Resource Group. Jobs can be monitored from the Dashboard job monitor or from the backup info on those resources.



Beginning with SnapCenter Plug-in for VMware vSphere (SCV) 5.0, you need to add applications of type HTTP and ONTAP as user login methods for any ONTAP users with customized role-based access to the SCV. Without access to these applications, backups will fail. You need to restart the SCV service to recognize changes to ONTAP user login methods. Click here to know more.

Recent job activities:

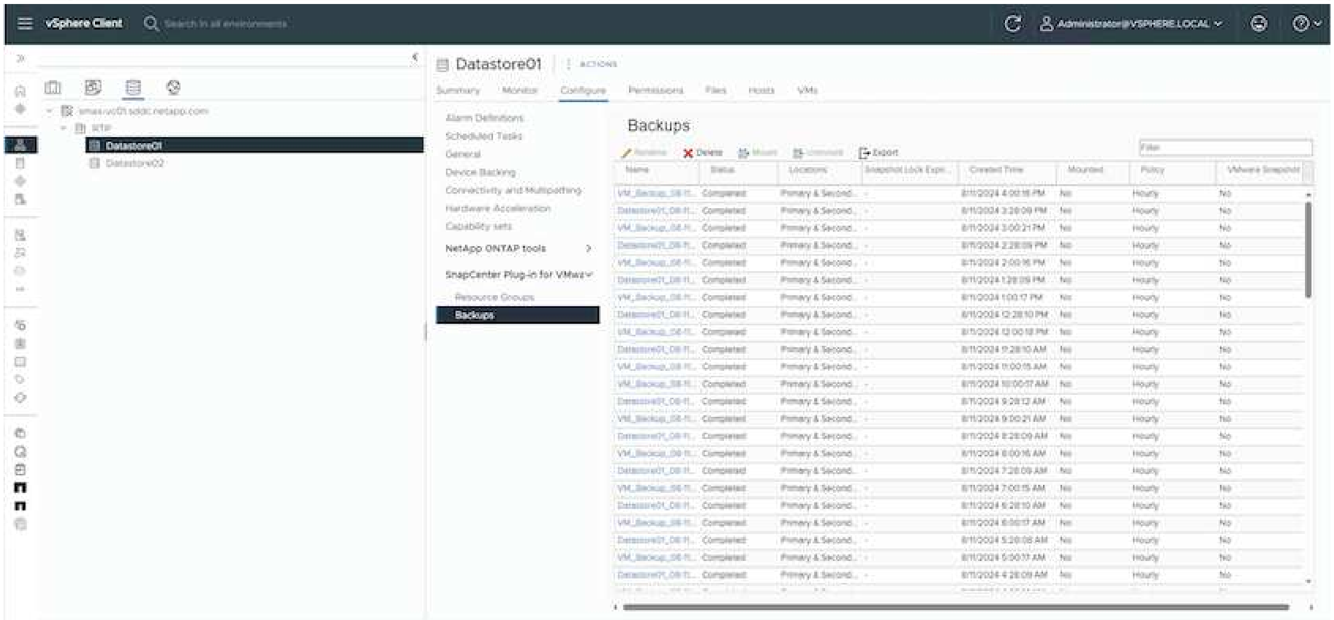
- Backup Warning VM_Backup [Job ID:530] 10 min ago
- Backup Successful Datastore01 [Job ID:532] 34 min ago
- Backup Successful Datastore01 [Job ID:529] 51 min ago
- Backup Warning VM_Backup [Job ID:526] 1 h ago
- Backup Successful Datastore01 [Job ID:523] 1 h ago

Jobs: Failed 11, Successful 92, Warning 71, Running 1

Latest protection summary – Primary: Failed 0, Successful 3, Not backed up 2; Secondary: Failed 2, Successful 1, Not replicated 2

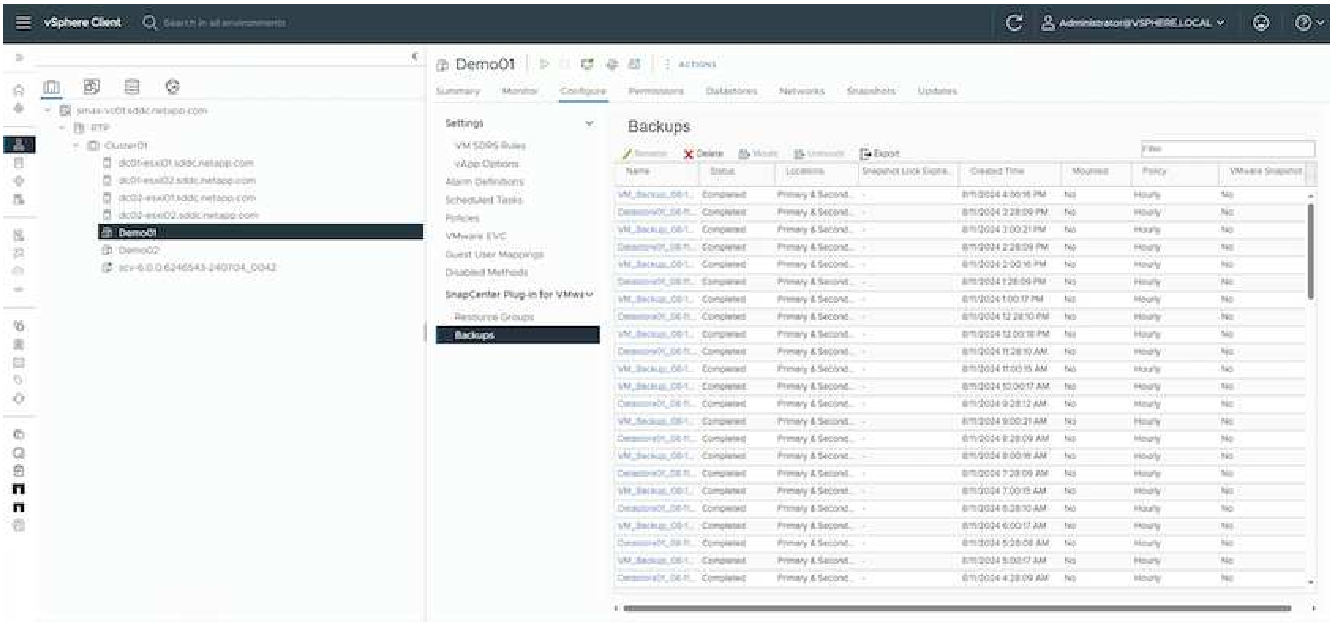
Configuration: 5 Virtual Machines, 2 Datastores, 30 SVMs, 3 Resource Groups, 3 Backup Policies

Storage: 4.64 GB 83 Snapshots | 5.12 GB 98 SnapVaults | 4.11 GB 42 SnapMirrors | 66.46 x Storage Savings | 303.43 GB Snapshot Savings | 4.64 GB Storage Consumed



Backups

Name	Status	Locations	Snapshot Lock Expi...	Created Time	Mounted	Policy	VMware Snapshot
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 4:00:16 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 3:28:09 PM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 3:00:21 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 2:28:09 PM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 2:00:16 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 1:28:09 PM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 1:00:17 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 12:28:10 PM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 12:00:18 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 11:28:10 AM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 11:00:15 AM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 10:00:17 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 9:28:12 AM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 9:00:21 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 8:28:09 AM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 8:00:16 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 7:28:09 AM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 7:00:15 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 6:28:10 AM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 6:00:17 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 5:28:08 AM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 5:00:17 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 4:28:09 AM	No	Hourly	No



Demo01

Settings: VM SDRS Rules, vApp Options, Alarm Definitions, Scheduled Tasks, Policies, VMware EVC, Guest User Mappings, Disabled Methods

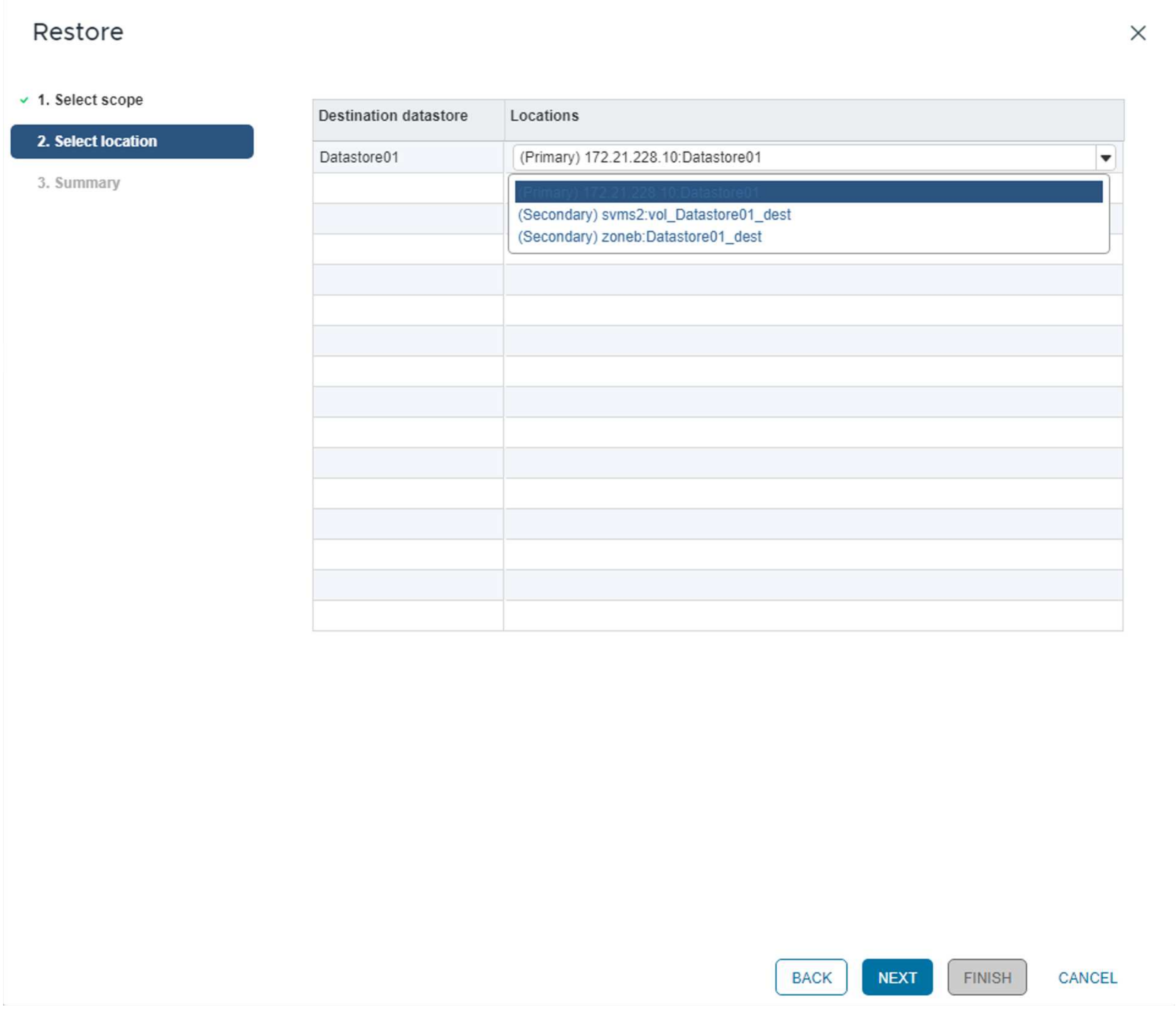
SnapCenter Plug-in for VMware: Resource Groups, Backups

Backups

Name	Status	Locations	Snapshot Lock Expira...	Created Time	Mounted	Policy	VMware Snapshot
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 4:00:16 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 3:28:09 PM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 3:00:21 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 2:28:09 PM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 2:00:16 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 1:28:09 PM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 1:00:17 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 12:28:10 PM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 12:00:18 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 11:28:10 AM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 11:00:15 AM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 10:00:17 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 9:28:12 AM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 9:00:21 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 8:28:09 AM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 8:00:18 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 7:28:09 AM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 7:00:15 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 6:28:10 AM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 6:00:17 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 5:28:08 AM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 5:00:17 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 4:28:09 AM	No	Hourly	No

vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
smas-vc01.sddc.netapp.com
RTP
Cluster01
dc01-esxi01.sddc.netapp.com
dc01-esxi02.sddc.netapp.com
dc02-esxi01.sddc.netapp.com
dc02-esxi02.sddc.netapp.com
Demo01
Demo02
scv-6.0.0.6246543-240704_0042
ACTIONS
Summary
Monitor
Configure
Permissions
Datastores
Networks
Snapshots
Updates
Rename
Delete
Mount
Unmount
Export
Filter

5. VMs can be restored to same or alternate vCenter from the SVM on Primary fault domain or from one of the secondary locations.



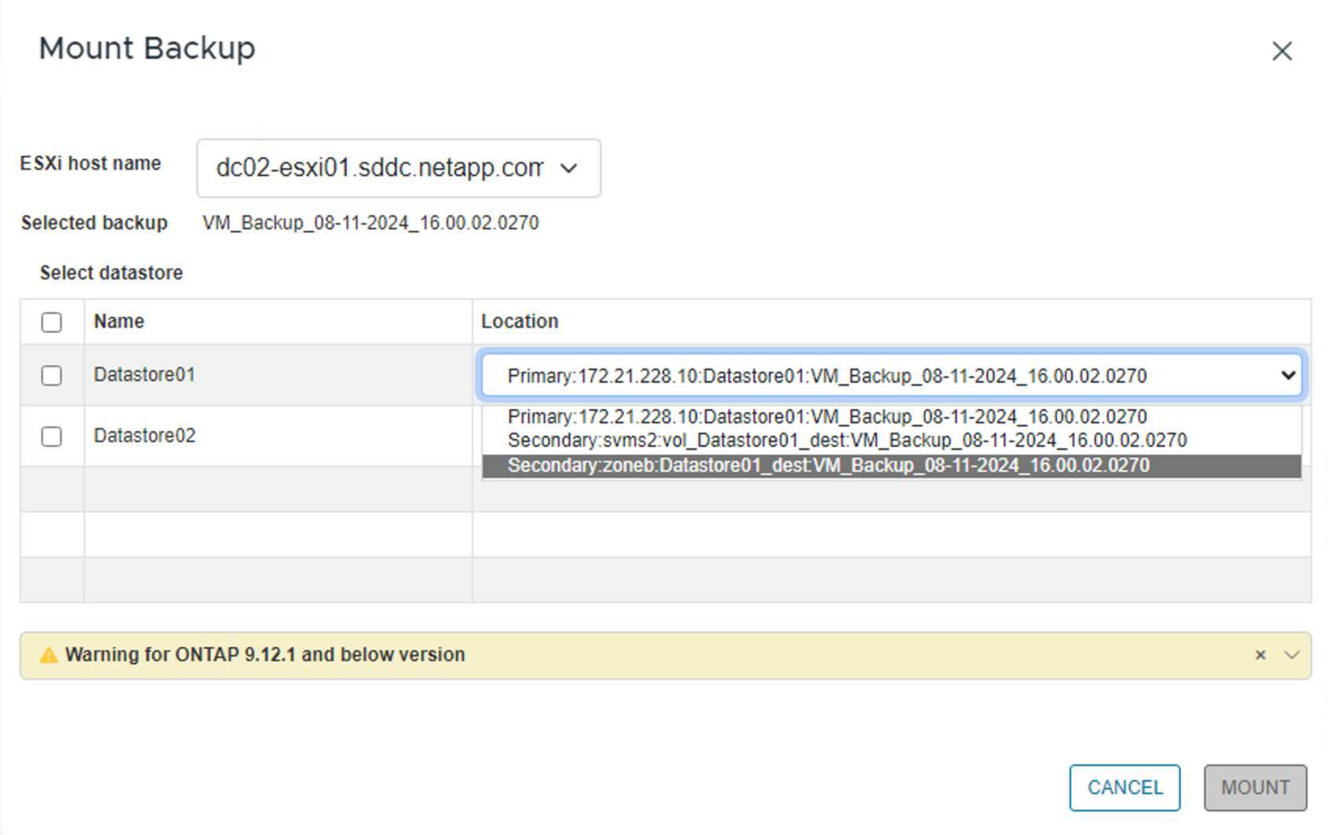
Restore

1. Select scope
2. Select location
3. Summary

Destination datastore	Locations
Datastore01	(Primary) 172.21.228.10:Datastore01

(Primary) 172.21.228.10:Datastore01
(Secondary) svms2:vol_Datastore01_dest
(Secondary) zoneb:Datastore01_dest

6. Similar option is also available for Datastore mount operation.



Mount Backup

ESXi host name: dc02-esxi01.sddc.netapp.com

Selected backup: VM_Backup_08-11-2024_16.00.02.0270

Select datastore

□	Name	Location
□	Datastore01	Primary:172.21.228.10:Datastore01:VM_Backup_08-11-2024_16.00.02.0270
□	Datastore02	

Primary:172.21.228.10:Datastore01:VM_Backup_08-11-2024_16.00.02.0270
Secondary:svms2:vol_Datastore01_dest:VM_Backup_08-11-2024_16.00.02.0270
Secondary:zoneb:Datastore01_dest:VM_Backup_08-11-2024_16.00.02.0270

Warning for ONTAP 9.12.1 and below version

For assistance with additional operations with SCV, refer SnapCenter Plug-in for VMware vSphere documentation

VMware Cloud Foundation

VMware Cloud Foundation

VMware Cloud Foundation (VCF) is a set of technologies that provides a straightforward path to accessing a hybrid cloud experience. Within the VCF solution, support is provided for both native Kubernetes and virtual machine based workloads. Essential services like VMware vSphere, VMware vSAN, VMware NSX-T Data Center, and VMware vRealize Cloud Management are integral components of the VCF package. When combined, these services establish a software-defined infrastructure capable of managing compute, storage, networking, security, and cloud management. This collective infrastructure provides a hybrid experience, wherein the VCF framework extends the environment from onsite data center to Amazon Web Services (AWS), Azure, and Google Cloud.

Documentation resources

For detailed information on NetApp offerings for VMware Cloud Foundation, refer to the following four (4) part blog series:

- NetApp and VMware Cloud Foundation made easy Part 1: Getting started
- NetApp and VMware Cloud Foundation made easy Part 2: VCF and ONTAP principal storage

- NetApp and VMware Cloud Foundation made easy Part 3: VCF and Element principal storage
- NetApp and VMware Cloud Foundation made easy - Part 4: ONTAP Tools for VMware and supplemental storage

VMware Cloud Foundation with NetApp All-Flash SAN Arrays

- VCF with NetApp ASA arrays, Introduction and Technology Overview
- Use Ontap Tools to deploy iSCSI datastores in a VCF management domain
- Use Ontap Tools to deploy vVols (iSCSI) datastores in a VI workload domain
- Configure NVMe over TCP datastores for use in a VI workload domain
- Deploy and use the SnapCenter Plug-in for VMware vSphere to protect and restore VMs in a VI workload domain

VMware Cloud Foundation with NetApp All-Flash AFF Arrays

- VCF with NetApp AFF arrays, Introduction and Technology Overview
- Use ONTAP with NFS as principal storage for VI workload domains
- Use ONTAP Tools to deploy NFS datastores in a VI workload domain

NetApp FlexPod solutions for VMware Cloud Foundation

- Expanding FlexPod hybrid cloud with VMware Cloud Foundation
- FlexPod as a Workload Domain for VMware Cloud Foundation
- FlexPod as a Workload Domain for VMware Cloud Foundation Design Guide

VMware Cloud Foundation with NetApp All-Flash SAN Arrays

VMware Cloud Foundation (VCF) is an integrated software defined data center (SDDC) platform that provides a complete stack of software-defined infrastructure for running enterprise applications in a hybrid cloud environment. It combines compute, storage, networking, and management capabilities into a unified platform, offering a consistent operational experience across private and public clouds.

Author: Josh Powell

This document provides information on storage options available for VMware Cloud Foundation using the NetApp All-Flash SAN Array. Supported storage options are covered with specific instruction for deploying iSCSI datastores as supplemental storage for management domains and both vVol (iSCSI) and NVMe/TCP datastores as supplemental datastores for workload domains. Also covered is data protection of VMs and datastores using SnapCenter for VMware vSphere.

Use Cases

Use cases covered in this documentation:

- Storage options for customers seeking uniform environments across both private and public clouds.
- Automated solution for deploying virtual infrastructure for workload domains.
- Scalable storage solution tailored to meet evolving needs, even when not aligned directly with compute

resource requirements.

- Deploy supplemental storage to management and VI workload domains using ONTAP Tools for VMware vSphere.
- Protect VMs and datastores using the SnapCenter Plug-in for VMware vSphere.

Audience

This solution is intended for the following people:

- Solution architects looking for more flexible storage options for VMware environments that are designed to maximize TCO.
- Solution architects looking for VCF storage options that provide data protection and disaster recovery options with the major cloud providers.
- Storage administrators wanting specific instruction on how to configure VCF with principal and supplemental storage.
- Storage administrators wanting specific instruction on how to protect VMs and datastores residing on ONTAP storage.

Technology Overview

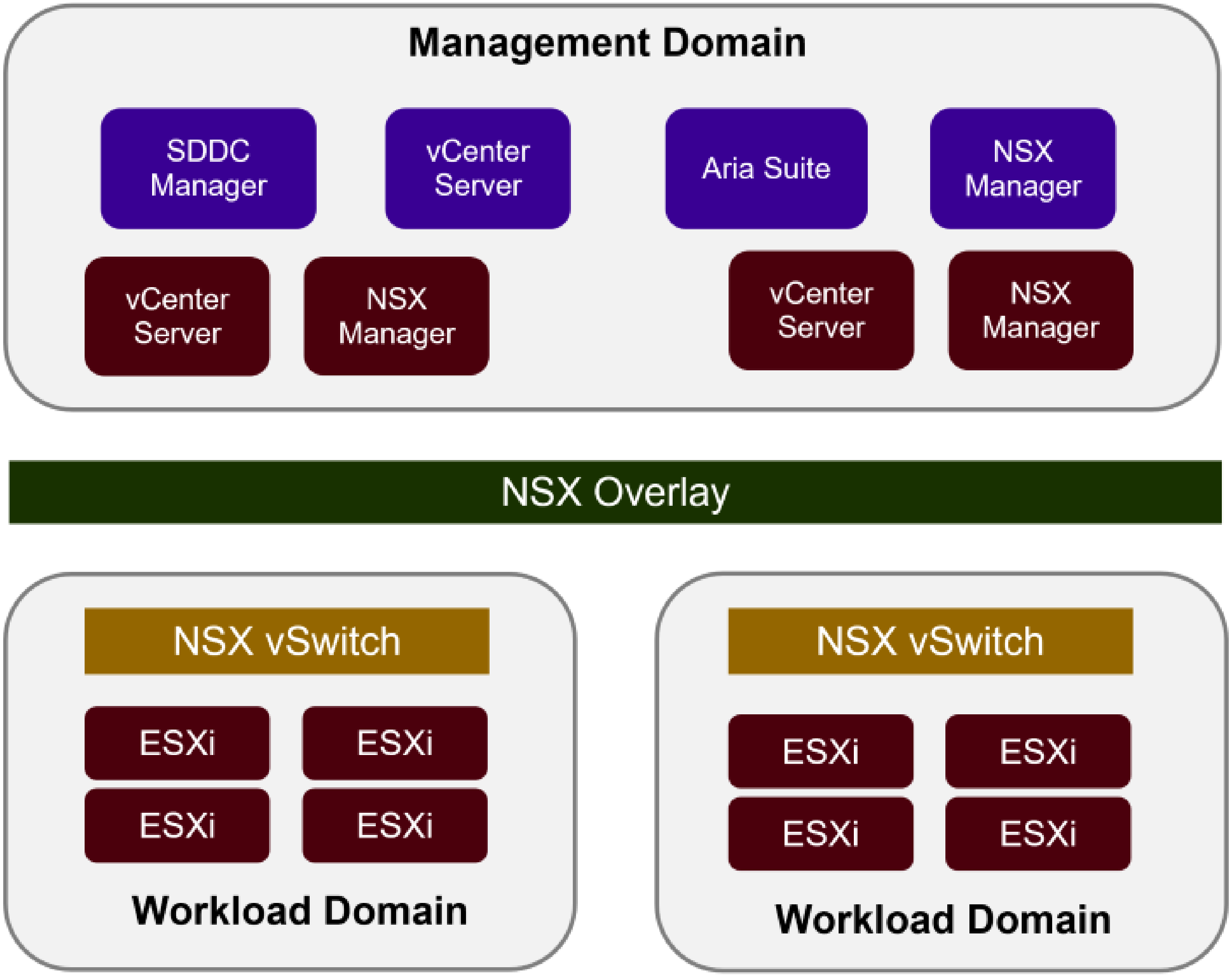
The VCF with NetApp ASA solution is comprised of the following major components:

VMware Cloud Foundation

VMware Cloud Foundation extends VMware’s vSphere hypervisor offerings by combining key components such as SDDC Manager, vSphere, vSAN, NSX, and VMware Aria Suite to create a software-defined datacenter.

The VCF solution supports both native Kubernetes and virtual machine-based workloads. Key services such as VMware vSphere, VMware vSAN, VMware NSX-T Data Center, and VMware Aria Cloud Management are integral components of the VCF package. When combined, these services establish a software-defined infrastructure capable of efficiently managing compute, storage, networking, security, and cloud management.

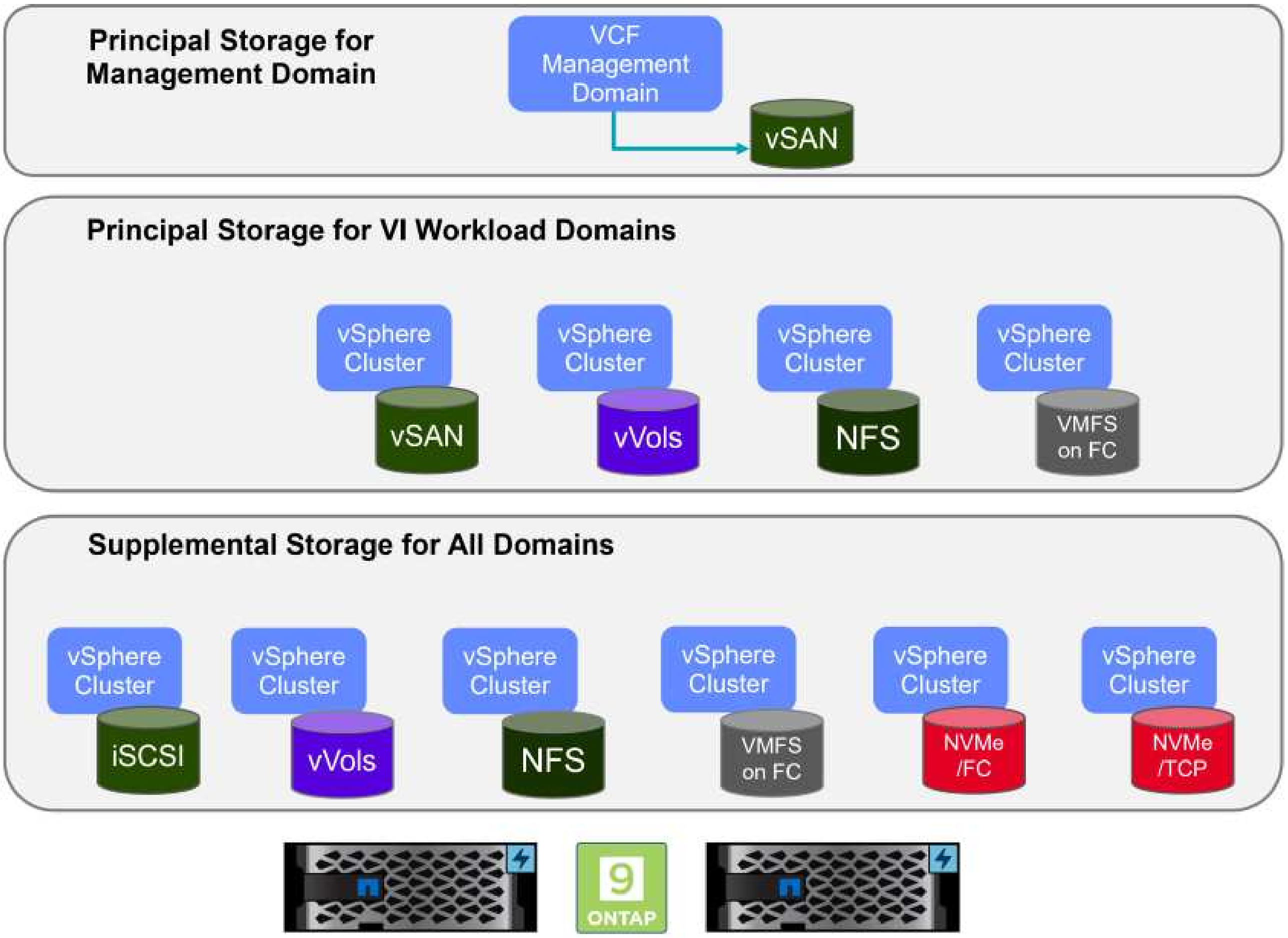
VCF is comprised of a single management domain and up to 24 VI workload domains that each represent a unit of application-ready infrastructure. A workload domain is comprised of one or more vSphere clusters managed by a single vCenter instance.



For more information on VCF architecture and planning, refer to Architecture Models and Workload Domain Types in VMware Cloud Foundation.

VCF Storage Options

VMware divides storage options for VCF into **principal** and **supplemental** storage. The VCF management domain must use vSAN as its principal storage. However, there are many supplemental storage options for the management domain and both principal and supplemental storage options available for VI workload domains.



Principal Storage for Workload Domains
Principal storage refers to any type of storage that can be directly connected to a VI workload domain during the setup process within SDDC Manager. Principal storage is deployed with SDDC manager as part of cluster creation orchestration and is the first datastore configured for a workload domain. It includes vSAN, vVols (VMFS), NFS and VMFS on Fibre Channel.

Supplemental Storage for Management and Workload Domains
Supplemental storage is the storage type that can be added to the management or workload domains at any time after the cluster has been created. Supplemental storage represents the widest range of supported storage options, all of which are supported on NetApp ASA arrays. Supplemental storage can be deployed using ONTAP Tools for VMware vSphere for most storage protocol types.

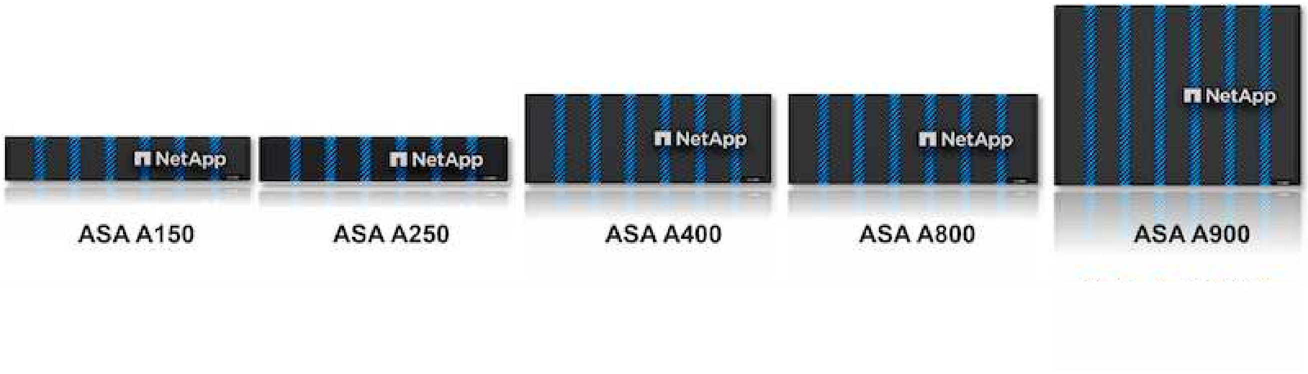
Additional documentation resources for VMware Cloud Foundation:
* VMware Cloud Foundation Documentation
* Supported Storage Types for VMware Cloud Foundation
* Managing Storage in VMware Cloud Foundation

NetApp All-Flash SAN Arrays

The NetApp All-Flash SAN Array (ASA) is a high-performance storage solution designed to meet the demanding requirements of modern data centers. It combines the speed and reliability of flash storage with NetApp's advanced data management features to deliver exceptional performance, scalability, and data protection.

The ASA lineup is comprised of both A-Series and C-Series models.

The NetApp A-Series all-NVMe flash arrays are designed for high-performance workloads, offering ultra-low latency and high resiliency, making them suitable for mission-critical applications.



C-Series QLC flash arrays are aimed at higher-capacity use cases, delivering the speed of flash with the economy of hybrid flash.

For detailed information see the NetApp ASA landing page.

Storage Protocol Support

The ASA supports all standard SAN protocols including, iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), and NVME over fabrics.

iSCSI - NetApp ASA provides robust support for iSCSI, allowing block-level access to storage devices over IP networks. It offers seamless integration with iSCSI initiators, enabling efficient provisioning and management of iSCSI LUNs. ONTAP’s advanced features, such as multi-pathing, CHAP authentication, and ALUA support.

For design guidance on iSCSI configurations refer to the SAN Configuration reference documentation.

Fibre Channel - NetApp ASA offers comprehensive support for Fibre Channel (FC), a high-speed network technology commonly used in storage area networks (SANs). ONTAP seamlessly integrates with FC infrastructure, providing reliable and efficient block-level access to storage devices. It offers features like zoning, multi-pathing, and fabric login (FLOGI) to optimize performance, enhance security, and ensure seamless connectivity in FC environments.

For design guidance on Fibre Channel configurations refer to the SAN Configuration reference documentation.

NVMe over Fabrics - NetApp ONTAP and ASA support NVMe over fabrics. NVMe/FC enables the use of NVMe storage devices over Fibre Channel infrastructure, and NVMe/TCP over storage IP networks.

For design guidance on NVMe refer to NVMe configuration, support and limitations

Active-active technology

NetApp All-Flash SAN Arrays allows for active-active paths through both controllers, eliminating the need for the host operating system to wait for an active path to fail before activating the alternative path. This means that the host can utilize all available paths on all controllers, ensuring active paths are always present regardless of whether the system is in a steady state or undergoing a controller failover operation.

Furthermore, the NetApp ASA offers a distinctive feature that greatly enhances the speed of SAN failover. Each controller continuously replicates essential LUN metadata to its partner. As a result, each controller is prepared to take over data serving responsibilities in the event of a sudden failure of its partner. This readiness is possible because the controller already possesses the necessary information to start utilizing the drives that were previously managed by the failed controller.

With active-active pathing, both planned and unplanned takeovers have IO resumption times of 2-3 seconds.

For more information see TR-4968, NetApp All-SAS Array – Data Availability and Integrity with the NetApp ASA.

Storage guarantees

NetApp offers a unique set of storage guarantees with NetApp All-flash SAN Arrays. The unique benefits include:

Storage efficiency guarantee: Achieve high performance while minimizing storage cost with the Storage Efficiency Guarantee. 4:1 for SAN workloads.

6 Nines (99.9999%) data availability guarantee: Guarantees remediation for unplanned downtime in excess of 31.56 seconds per year.

Ransomware recovery guarantee: Guaranteed data recovery in the event of a ransomware attack.

See the NetApp ASA product portal for more information.

NetApp ONTAP Tools for VMware vSphere

ONTAP Tools for VMware vSphere allows administrators to manage NetApp storage directly from within the vSphere Client. ONTAP Tools allows you to deploy and manage datastores, as well as provision vVol datastores.

ONTAP Tools allows mapping of datastores to storage capability profiles which determine a set of storage system attributes. This allows the creation of datastores with specific attributes such as storage performance and QoS.

ONTAP Tools also includes a **VMware vSphere APIs for Storage Awareness (VASA) Provider** for ONTAP storage systems, which enables the provisioning of VMware Virtual Volumes (vVols) datastores, creation and use of storage capability profiles, compliance verification, and performance monitoring.

For more information on NetApp ONTAP tools see the ONTAP tools for VMware vSphere Documentation page.

SnapCenter Plug-in for VMware vSphere

The SnapCenter Plug-in for VMware vSphere (SCV) is a software solution from NetApp that offers comprehensive data protection for VMware vSphere environments. It is designed to simplify and streamline the process of protecting and managing virtual machines (VMs) and datastores. SCV uses storage based snapshot and replication to secondary arrays to meet lower recovery time objectives.

The SnapCenter Plug-in for VMware vSphere provides the following capabilities in a unified interface, integrated with the vSphere client:

Policy-Based Snapshots - SnapCenter allows you to define policies for creating and managing application-consistent snapshots of virtual machines (VMs) in VMware vSphere.

Automation - Automated snapshot creation and management based on defined policies help ensure consistent and efficient data protection.

VM-Level Protection - Granular protection at the VM level allows for efficient management and recovery of individual virtual machines.

Storage Efficiency Features - Integration with NetApp storage technologies provides storage efficiency features like deduplication and compression for snapshots, minimizing storage requirements.

The SnapCenter Plug-in orchestrates the quiescing of virtual machines in conjunction with hardware-based snapshots on NetApp storage arrays. SnapMirror technology is utilized to replicate copies of backups to secondary storage systems including in the cloud.

For more information refer to the SnapCenter Plug-in for VMware vSphere documentation.

BlueXP integration enables 3-2-1 backup strategies that extend copies of data to object storage in the cloud.

For more information on 3-2-1 backup strategies with BlueXP visit 3-2-1 Data Protection for VMware with SnapCenter Plug-in and BlueXP backup and recovery for VMs.

Solution Overview

The scenarios presented in this documentation will demonstrate how to use ONTAP storage systems as supplemental storage for management and workload domains. In addition, the SnapCenter Plug-in for VMware vSphere is used to protect VMs and datastores.

Scenarios covered in this documentation:

- **Use Ontap Tools to deploy iSCSI datastores in a VCF management domain**. Click **here** for deployment steps.
- **Use Ontap Tools to deploy vVols (iSCSI) datastores in a VI workload domain**. Click **here** for deployment steps.
- **Configure NVMe over TCP datastores for use in a VI workload domain**. Click **here** for deployment steps.
- **Deploy and use the SnapCenter Plug-in for VMware vSphere to protect and restore VMs in a VI workload domain**. Click **here** for deployment steps.

Use ONTAP Tools to configure supplemental storage for VCF Management Domains

In this scenario we will demonstrate how to deploy and use ONTAP Tools for VMware vSphere (OTV) to configure an iSCSI datastore for a VCF management domain.

Author: Josh Powell

Scenario Overview

This scenario covers the following high level steps:

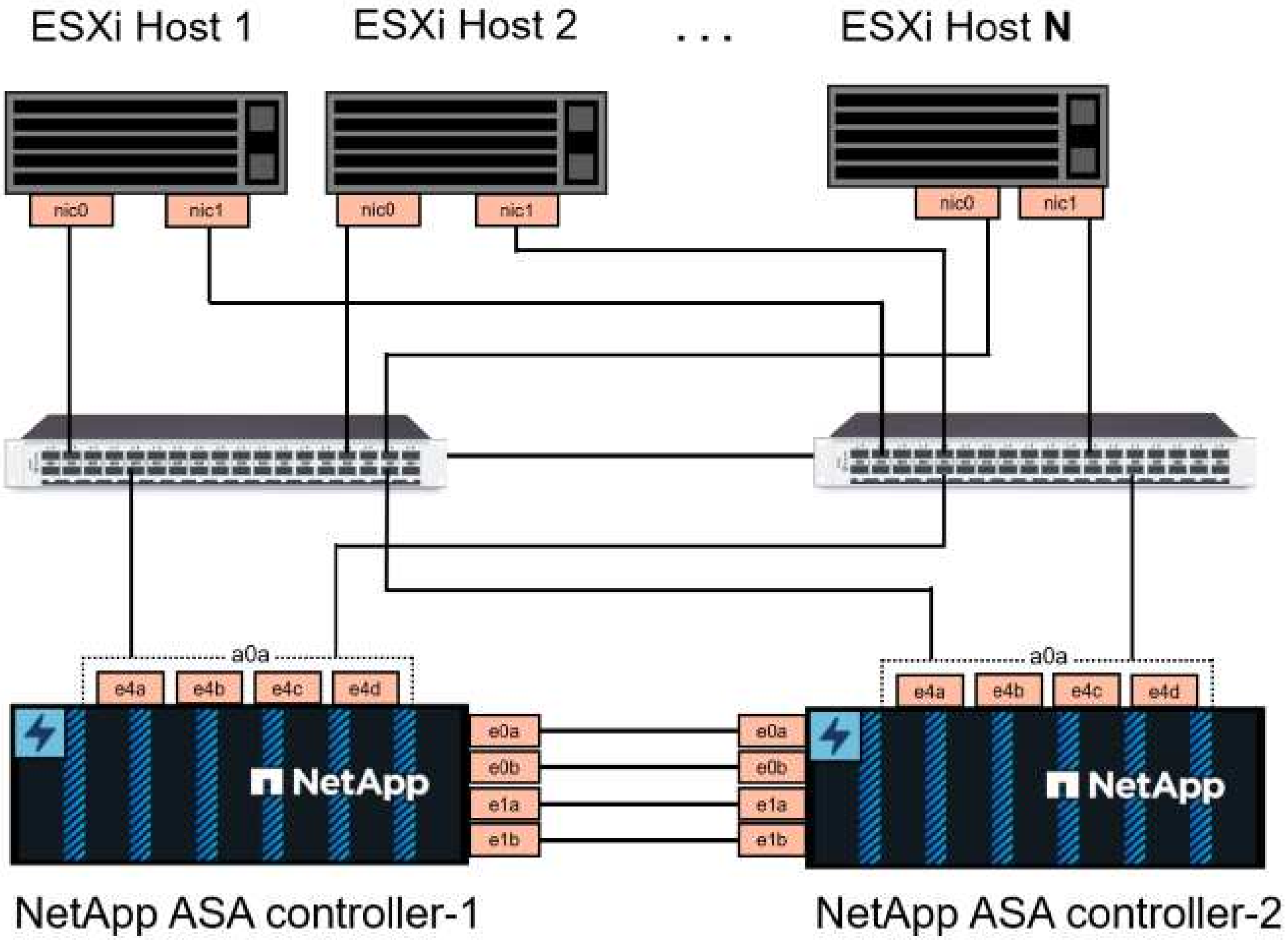
- Create a storage virtual machine (SVM) with logical interfaces (LIFs) for iSCSI traffic.
- Create distributed port groups for iSCSI networks on the VCF management domain.
- Create vmkernel adapters for iSCSI on the ESXi hosts for the VCF management domain.
- Deploy ONTAP Tools on the VCF management domain.
- Create a new VMFS datastore on the VCF management domain.

Prerequisites

This scenario requires the following components and configurations:

- An ONTAP ASA storage system with physical data ports on ethernet switches dedicated to storage traffic.
- VCF management domain deployment is complete and the vSphere client is accessible.

NetApp recommends fully redundant network designs for iSCSI. The following diagram illustrates an example of a redundant configuration, providing fault tolerance for storage systems, switches, networks adapters and host systems. Refer to the NetApp SAN configuration reference for additional information.



For multipathing and failover across multiple paths, NetApp recommends having a minimum of two LIFs per storage node in separate ethernet networks for all SVMs in iSCSI configurations.

This documentation demonstrates the process of creating a new SVM and specifying the IP address information to create multiple LIFs for iSCSI traffic. To add new LIFs to an existing SVM refer to Create a LIF (network interface).

For additional information on using VMFS iSCSI datastores with VMware refer to vSphere VMFS Datastore - iSCSI Storage backend with ONTAP.

In situations where multiple VMkernel adapters are configured on the same IP network, it is recommended to use software iSCSI port binding on the ESXi hosts to ensure that load balancing across the adapters occurs. Refer to KB article Considerations for using software iSCSI port binding in ESX/ESXi (2038869).

Deployment Steps

To deploy ONTAP Tools and use it to create a VMFS datastore on the VCF management domain, complete the following steps:

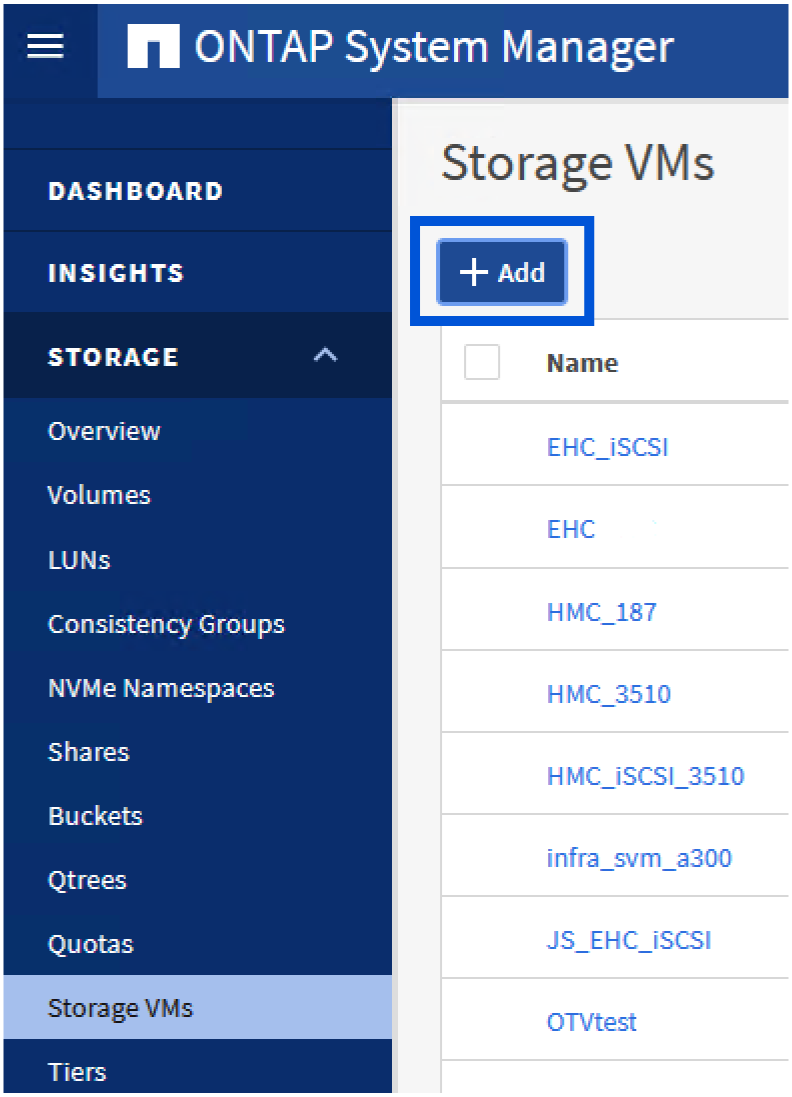
Create SVM and LIFs on ONTAP storage system

The following step is is performed in ONTAP System Manager.

Create the storage VM and LIFs

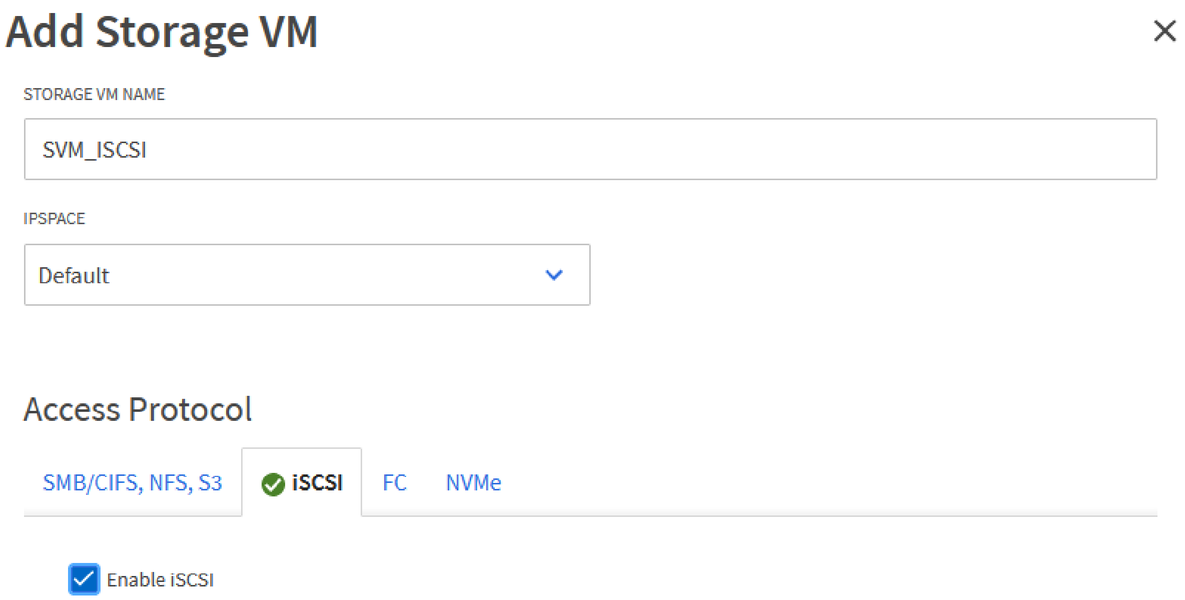
Complete the following steps to create an SVM together with multiple LIFs for iSCSI traffic.

1. From ONTAP System Manager navigate to **Storage VMs** in the left-hand menu and click on **+ Add** to start.



□	Name
	EHC_iSCSI
	EHC
	HMC_187
	HMC_3510
	HMC_iSCSI_3510
	infra_svm_a300
	JS_EHC_iSCSI
	OTVtest

2. In the **Add Storage VM** wizard provide a **Name** for the SVM, select the **IP Space** and then, under **Access Protocol, click on the *iSCSI** tab and check the box to **Enable iSCSI**.



Add Storage VM

STORAGE VM NAME

SVM_ISCSI

IPSPACE

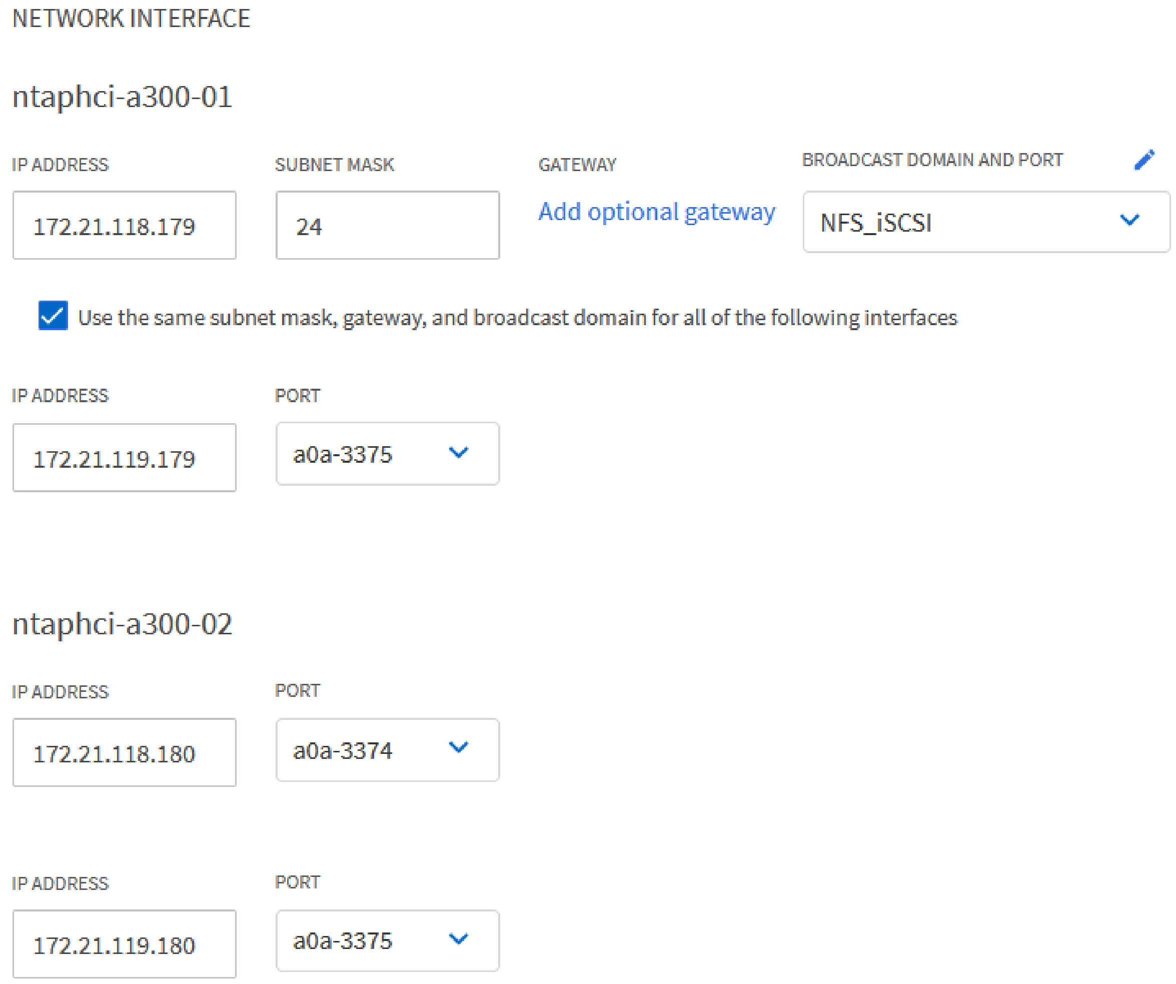
Default

Access Protocol

☑ Enable iSCSI

3. In the **Network Interface** section fill in the **IP address**, **Subnet Mask**, and **Broadcast Domain and Port** for the first LIF. For subsequent LIFs the checkbox may be enabled to use common settings across all remaining LIFs or use separate settings.

   For multipathing and failover across multiple paths, NetApp recommends having a minimum of two LIFs per storage node in separate Ethernet networks for all SVMs in iSCSI configurations.



NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS: 172.21.118.179

SUBNET MASK: 24

GATEWAY: Add optional gateway

BROADCAST DOMAIN AND PORT: NFS_iSCSI

☑ Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS: 172.21.119.179

PORT: a0a-3375

ntaphci-a300-02

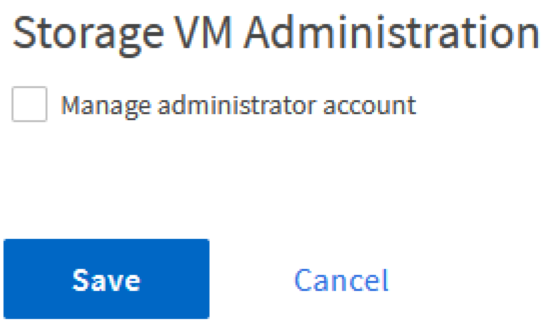
IP ADDRESS: 172.21.118.180

PORT: a0a-3374

IP ADDRESS: 172.21.119.180

PORT: a0a-3375

4. Choose whether to enable the Storage VM Administration account (for multi-tenancy environments) and click on **Save** to create the SVM.



Storage VM Administration

□ Manage administrator account

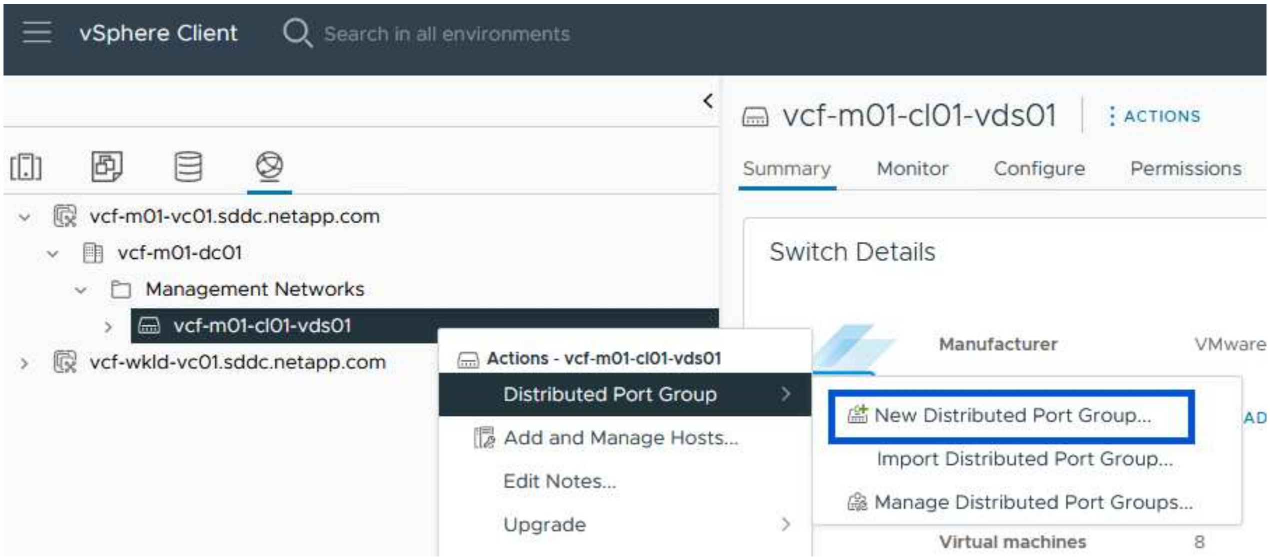
Set up networking for iSCSI on ESXi hosts

The following steps are performed on the VCF management domain cluster using the vSphere client.

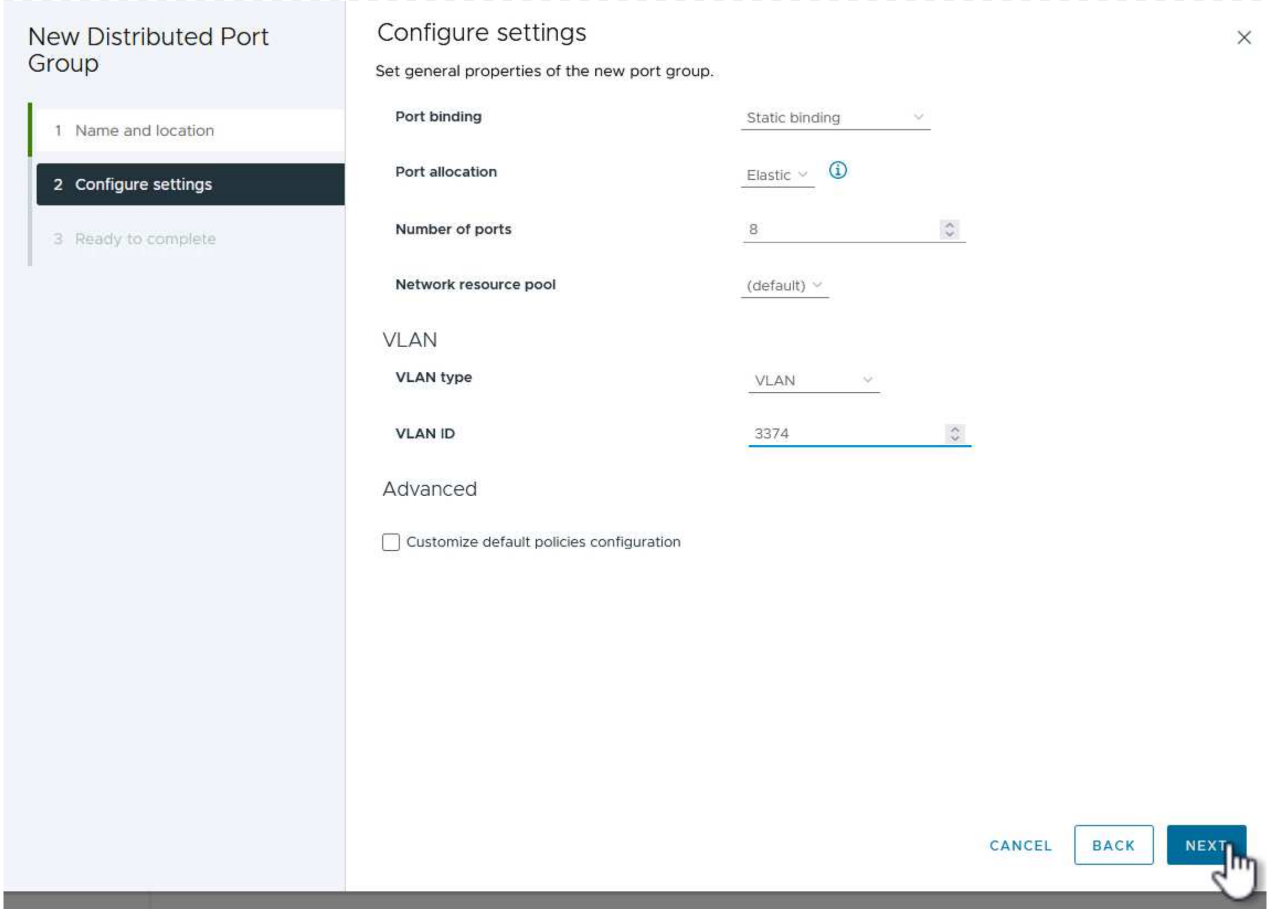
Create Distributed Port Groups for iSCSI traffic

Complete the following to create a new distributed port group for each iSCSI network:

1. From the vSphere client for the management domain cluster, navigate to **Inventory > Networking**. Navigate to the existing Distributed Switch and choose the action to create **New Distributed Port Group…**.



2. In the **New Distributed Port Group** wizard fill in a name for the new port group and click on **Next** to continue.
3. On the **Configure settings** page fill out all settings. If VLANs are being used be sure to provide the correct VLAN ID. Click on **Next** to continue.



New Distributed Port Group

1. Name and location
2. Configure settings
3. Ready to complete

Configure settings

Set general properties of the new port group.

Port binding	Static binding
Port allocation	Elastic
Number of ports	8
Network resource pool	(default)

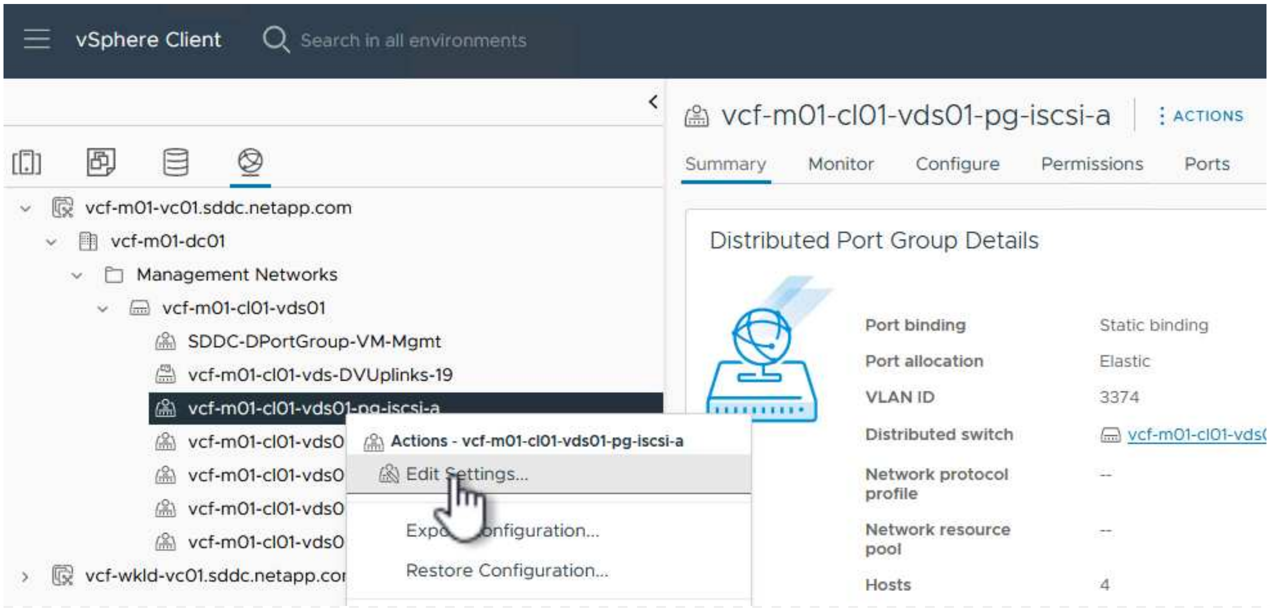
VLAN

VLAN type	VLAN
VLAN ID	3374

Advanced

□ Customize default policies configuration

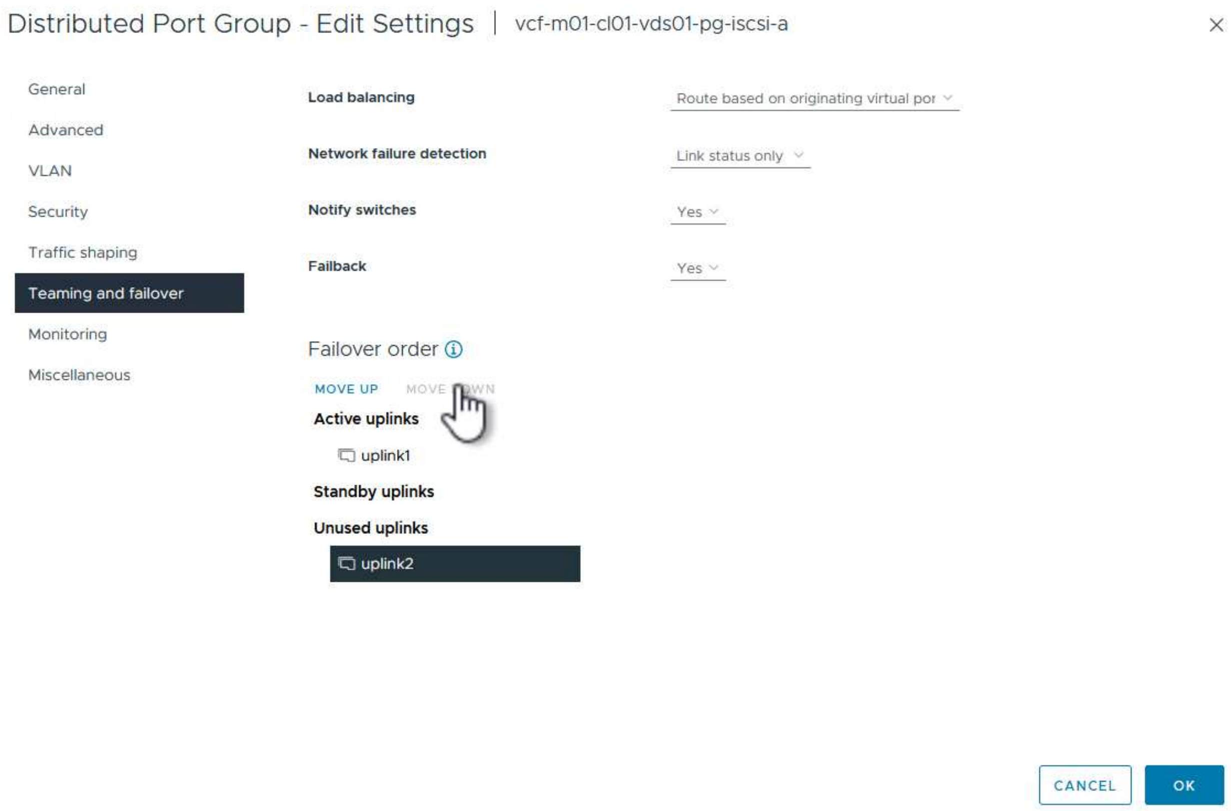
4. On the **Ready to complete** page, review the changes and click on **Finish** to create the new distributed port group.
5. Repeat this process to create a distributed port group for the second iSCSI network being used and ensure you have input the correct **VLAN ID**.
6. Once both port groups have been created, navigate to the first port group and select the action to **Edit settings…**.



Distributed Port Group Details

Port binding	Static binding
Port allocation	Elastic
VLAN ID	3374
Distributed switch	vcf-m01-cl01-vds(
Network protocol profile	--
Network resource pool	--
Hosts	4

7. On **Distributed Port Group - Edit Settings** page, navigate to **Teaming and failover** in the left-hand menu and click on **uplink2** to move it down to **Unused uplinks**.



Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-a

Load balancing: Route based on originating virtual por

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

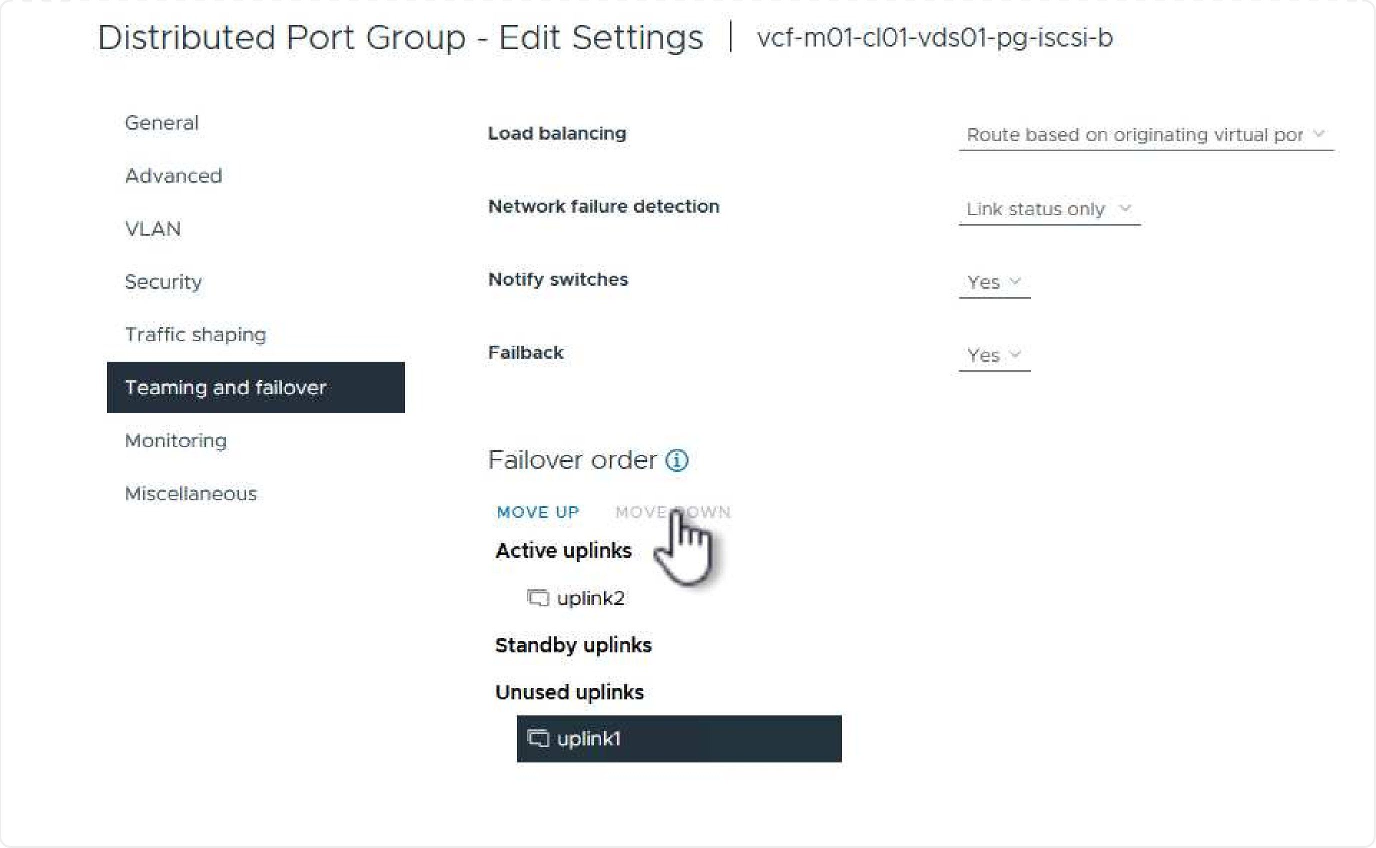
Failover order

Active uplinks
- uplink1

Standby uplinks

Unused uplinks
- uplink2

8. Repeat this step for the second iSCSI port group. However, this time move **uplink1** down to **Unused uplinks**.



Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-b

Load balancing: Route based on originating virtual por

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

Failover order

Active uplinks
- uplink2

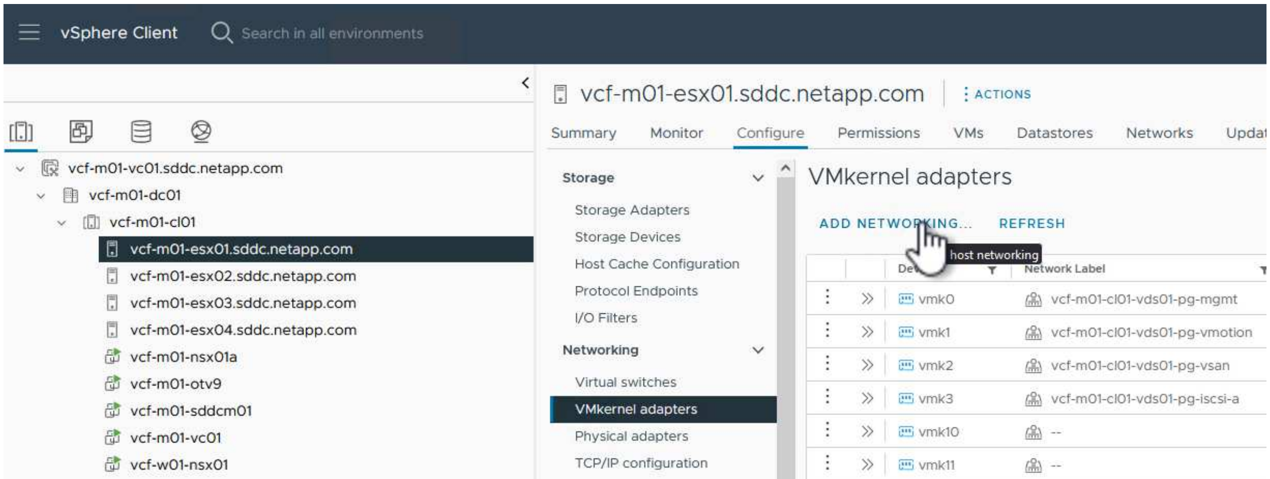
Standby uplinks

Unused uplinks
- uplink1

Create VMkernel adapters on each ESXi host

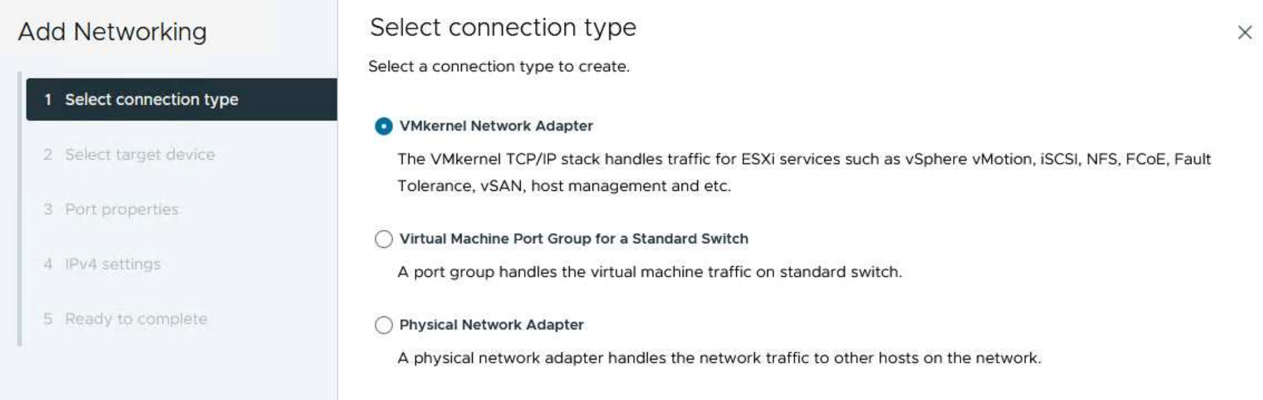
Repeat this process on each ESXi host in the management domain.

1. From the vSphere client navigate to one of the ESXi hosts in the management domain inventory. From the **Configure** tab select **VMkernel adapters** and click on **Add Networking…** to start.



De	Network Label
vmk0	vcf-m01-cl01-vds01-pg-mgmt
vmk1	vcf-m01-cl01-vds01-pg-vmotion
vmk2	vcf-m01-cl01-vds01-pg-vsan
vmk3	vcf-m01-cl01-vds01-pg-iscsi-a
vmk10	--
vmk11	--

2. On the **Select connection type** window choose **VMkernel Network Adapter** and click on **Next** to continue.



Select connection type

Select a connection type to create.

● VMkernel Network Adapter

The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.

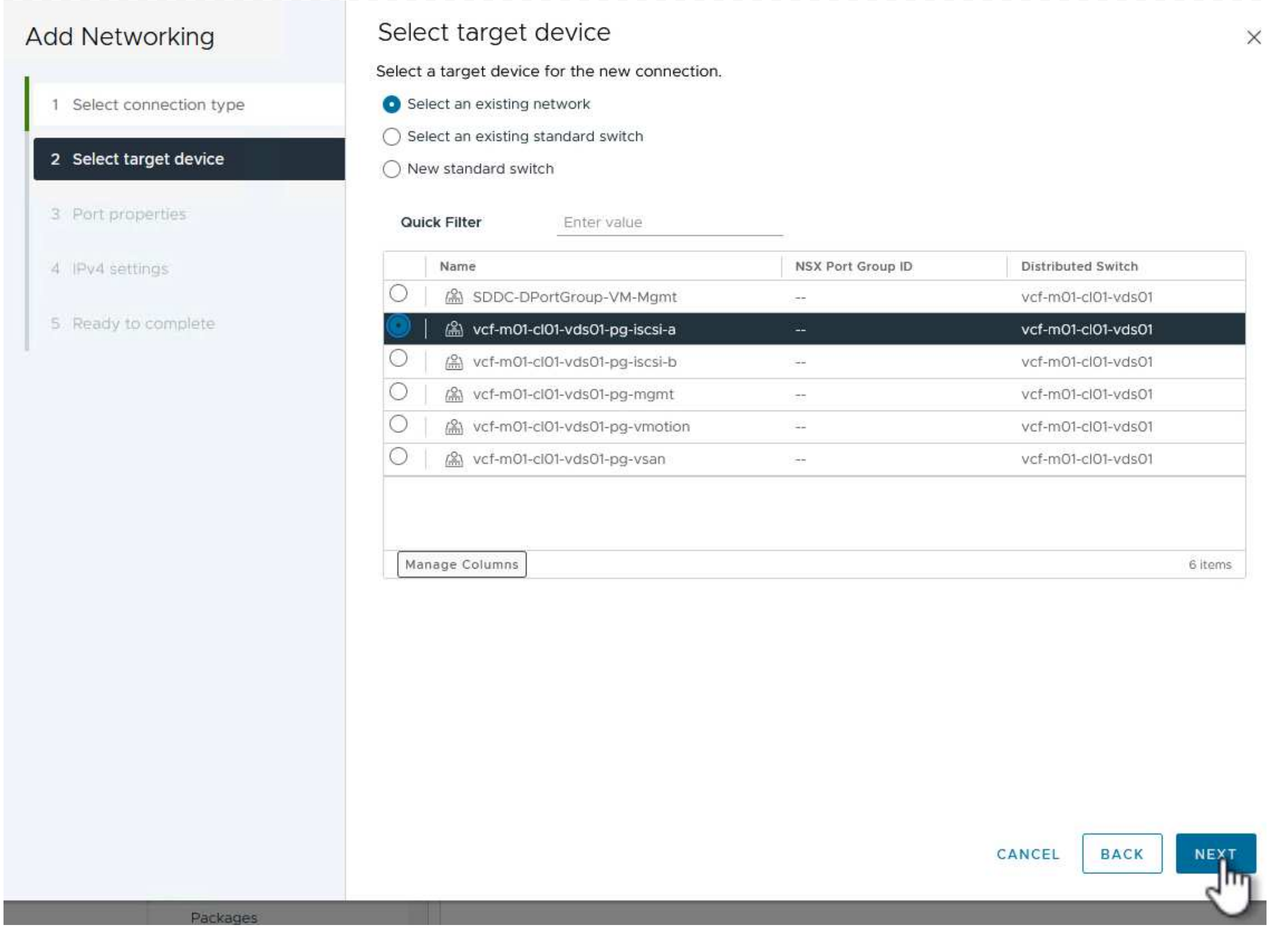
○ Virtual Machine Port Group for a Standard Switch

A port group handles the virtual machine traffic on standard switch.

○ Physical Network Adapter

A physical network adapter handles the network traffic to other hosts on the network.

3. On the **Select target device** page, choose one of the distributed port groups for iSCSI that was created previously.



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

● Select an existing network

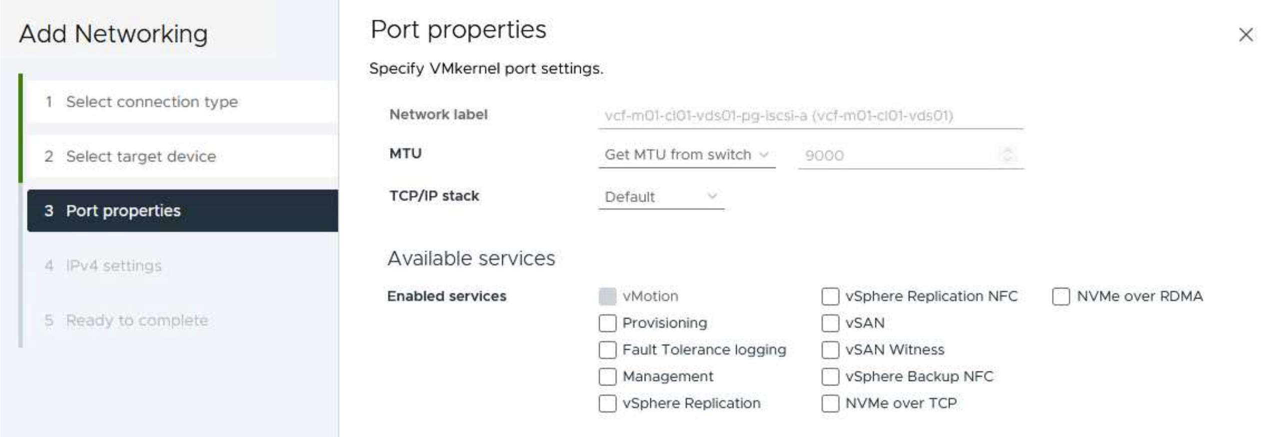
○ Select an existing standard switch

○ New standard switch

Quick Filter: Enter value

	Name	NSX Port Group ID	Distributed Switch
○	SDDC-DPortGroup-VM-Mgmt	--	vcf-m01-cl01-vds01
●	vcf-m01-cl01-vds01-pg-iscsi-a	--	vcf-m01-cl01-vds01
○	vcf-m01-cl01-vds01-pg-iscsi-b	--	vcf-m01-cl01-vds01
○	vcf-m01-cl01-vds01-pg-mgmt	--	vcf-m01-cl01-vds01
○	vcf-m01-cl01-vds01-pg-vmotion	--	vcf-m01-cl01-vds01
○	vcf-m01-cl01-vds01-pg-vsan	--	vcf-m01-cl01-vds01

4. On the **Port properties** page keep the defaults and click on **Next** to continue.



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label: vcf-m01-cl01-vds01-pg-iscsi-a (vcf-m01-cl01-vds01)

MTU: Get MTU from switch 9000

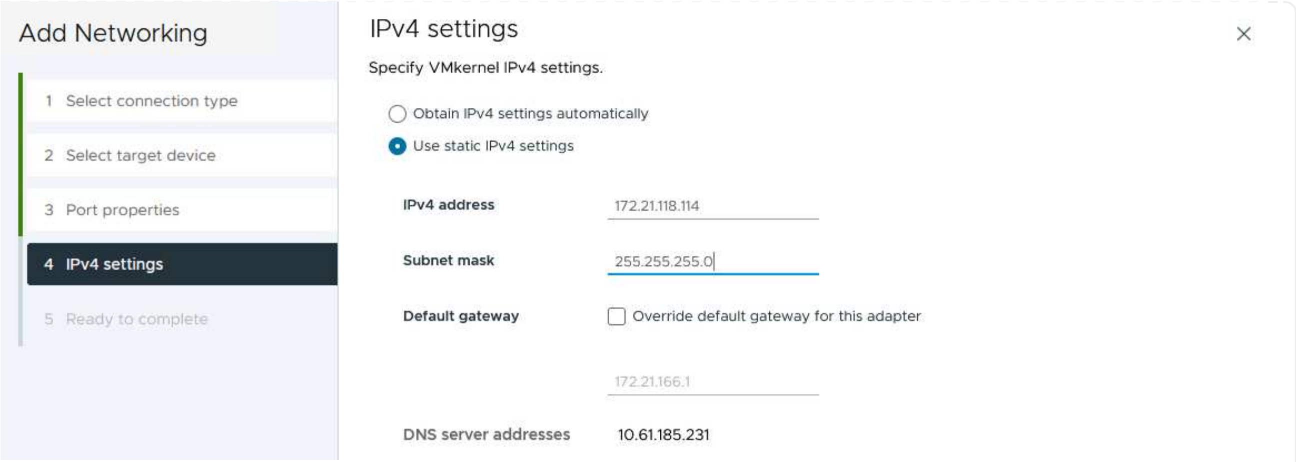
TCP/IP stack: Default

Available services

Enabled services:

□ vMotion
□ Provisioning
□ Fault Tolerance logging
□ Management
□ vSphere Replication
□ vSphere Replication NFC
□ vSAN
□ vSAN Witness
□ vSphere Backup NFC
□ NVMe over TCP
□ NVMe over RDMA

5. On the **IPv4 settings** page fill in the **IP address**, **Subnet mask**, and provide a new Gateway IP address (only if required). Click on **Next** to continue.



IPv4 settings

Specify VMkernel IPv4 settings.

○ Obtain IPv4 settings automatically

● Use static IPv4 settings

IPv4 address: 172.21.118.114

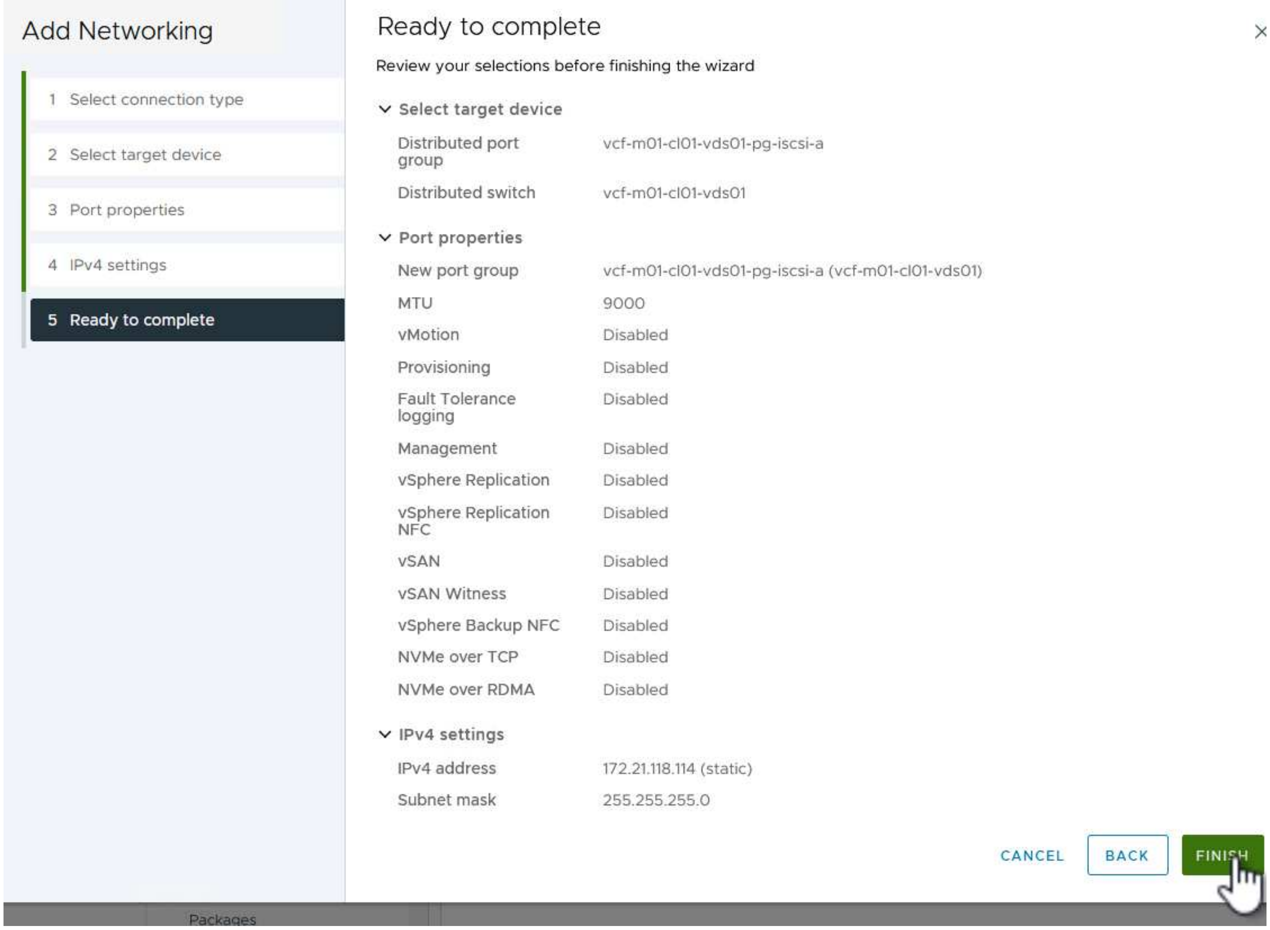
Subnet mask: 255.255.255.0

Default gateway: □ Override default gateway for this adapter

172.21.166.1

DNS server addresses: 10.61.185.231

6. Review the your selections on the **Ready to complete** page and click on **Finish** to create the VMkernel adapter.



Ready to complete

Review your selections before finishing the wizard

Select target device

Distributed port group	vcf-m01-cl01-vds01-pg-iscsi-a
Distributed switch	vcf-m01-cl01-vds01

Port properties

New port group	vcf-m01-cl01-vds01-pg-iscsi-a (vcf-m01-cl01-vds01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Disabled
NVMe over RDMA	Disabled

IPv4 settings

IPv4 address	172.21.118.114 (static)
Subnet mask	255.255.255.0

7. Repeat this process to create a VMkernel adapter for the second iSCSI network.

Deploy and use ONTAP Tools to configure storage

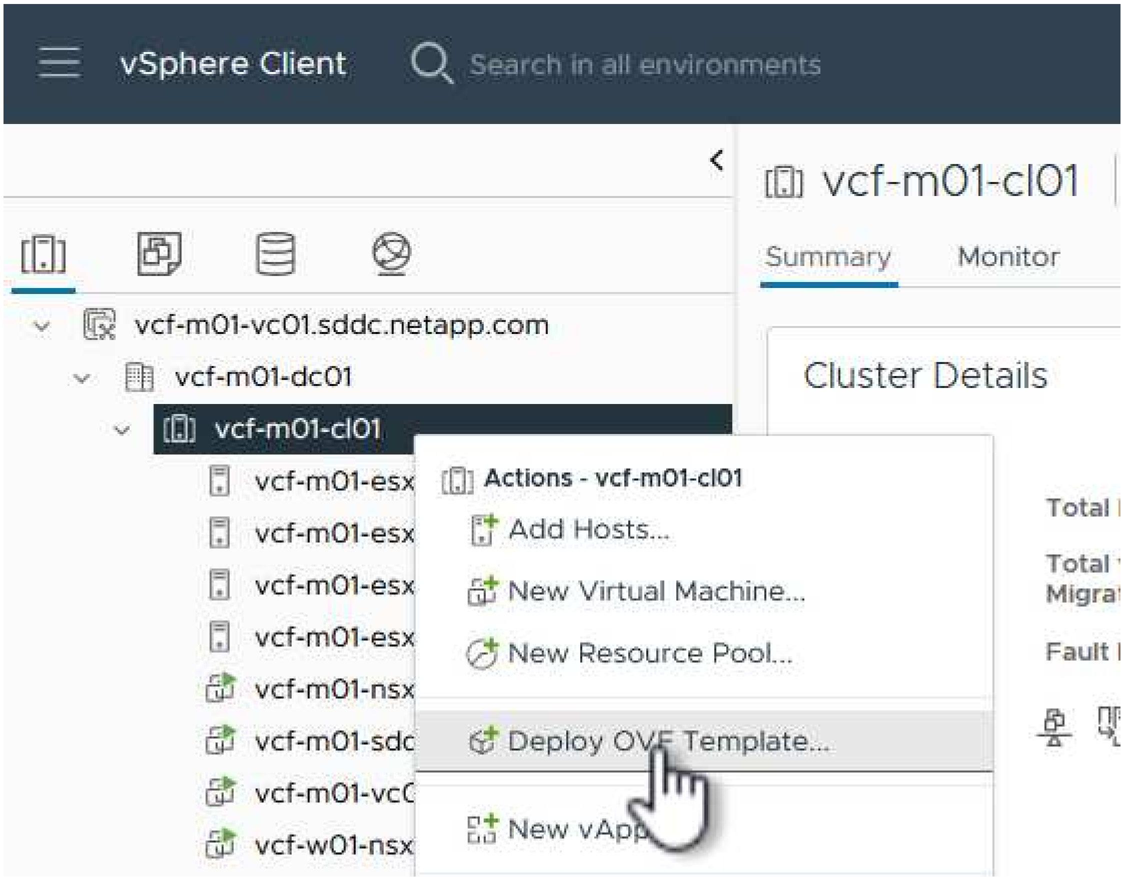
The following steps are performed on the VCF management domain cluster using the vSphere client and involve deploying OTV, creating a VMFS iSCSI datastore, and migrating management VM’s to the new datastore.

Deploy ONTAP tools for VMware vSphere

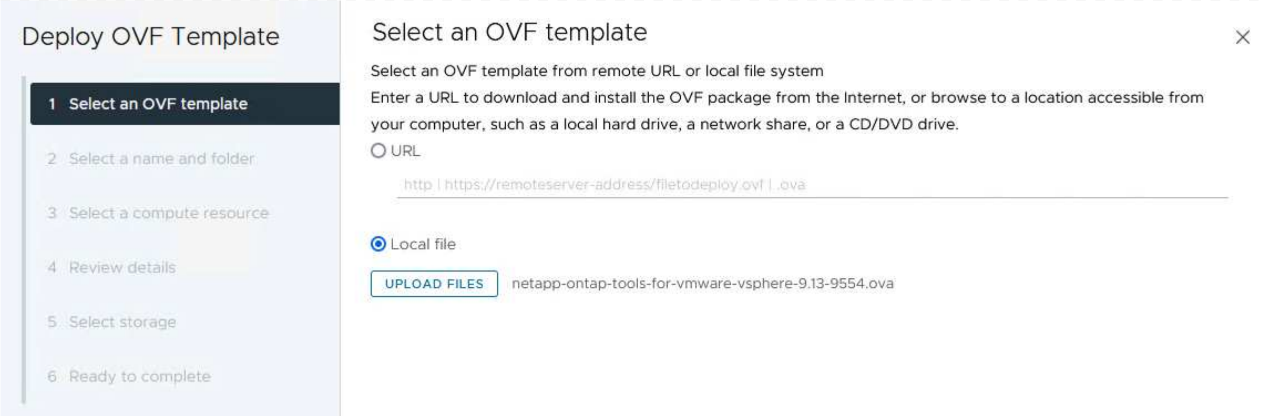
ONTAP tools for VMware vSphere (OTV) is deployed as a VM appliance and provides an integrated vCenter UI for managing ONTAP storage.

Complete the following to Deploy ONTAP tools for VMware vSphere:

1. Obtain the ONTAP tools OVA image from the NetApp Support site and download to a local folder.
2. Log into the vCenter appliance for the VCF management domain.
3. From the vCenter appliance interface right-click on the management cluster and select **Deploy OVF Template…**



4. In the **Deploy OVF Template** wizard click the **Local file** radio button and select the ONTAP tools OVA file downloaded in the previous step.



Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

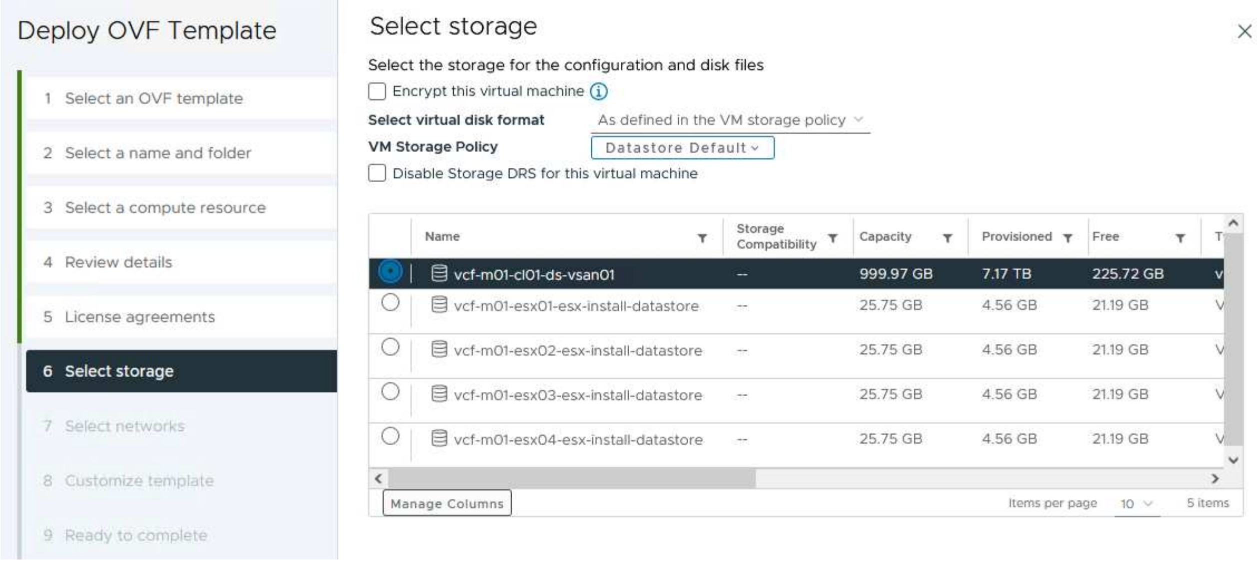
○ URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

● Local file

UPLOAD FILES netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. For steps 2 through 5 of the wizard select a name and folder for the VM, select the compute resource, review the details, and accept the license agreement.
6. For the storage location of the configuration and disk files, select the vSAN datastore of the VCF management domain cluster.



Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine

Select virtual disk format: As defined in the VM storage policy

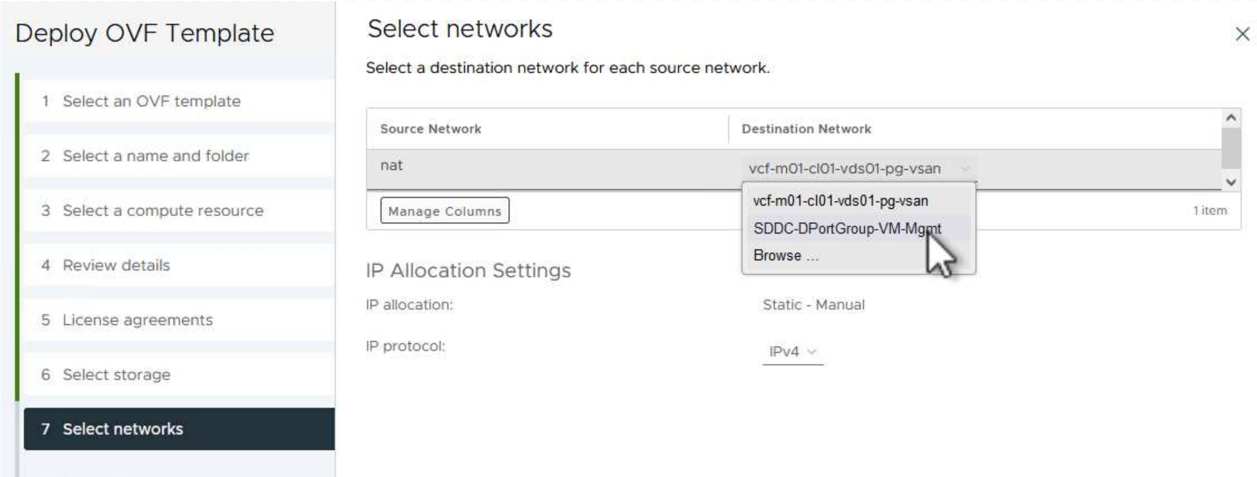
VM Storage Policy: Datastore Default

□ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	v
○	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V

Manage Columns Items per page 10 5 items

7. On the Select network page select the network used for management traffic.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks

Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	vcf-m01-cl01-vds01-pg-vsan

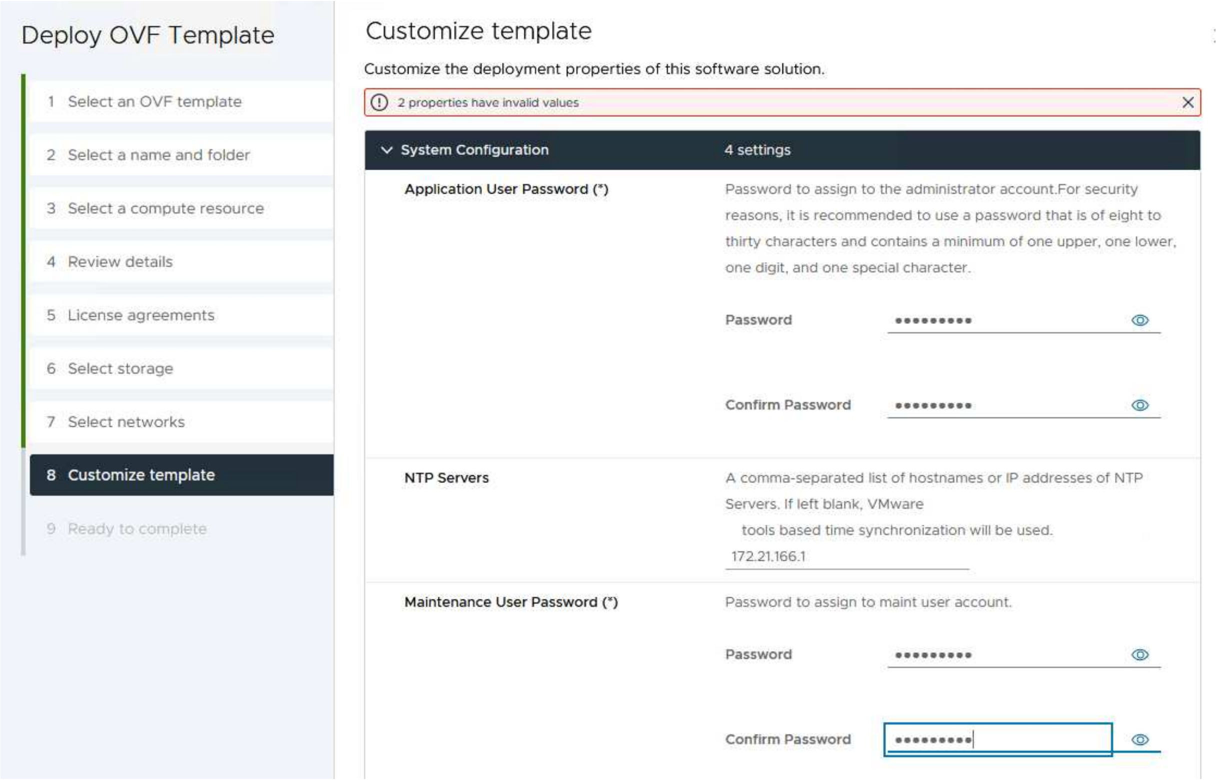
IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

8. On the Customize template page fill out all required information:
   - Password to be used for administrative access to OTV.
   - NTP server IP address.
   - OTV maintenance account password.
   - OTV Derby DB password.
   - Do not check the box to **Enable VMware Cloud Foundation (VCF)**. VCF mode is not required for deploying supplemental storage.
   - FQDN or IP address of the vCenter appliance and provide credentials for vCenter.
   - Provide the required network properties fields.

   Click on **Next** to continue.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Customize template

Customize the deployment properties of this software solution.

2 properties have invalid values

System Configuration 4 settings

Application User Password (*)

Password to assign to the administrator account.For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.

Password ●●●●●●●●●

Confirm Password ●●●●●●●●●

NTP Servers

A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used.

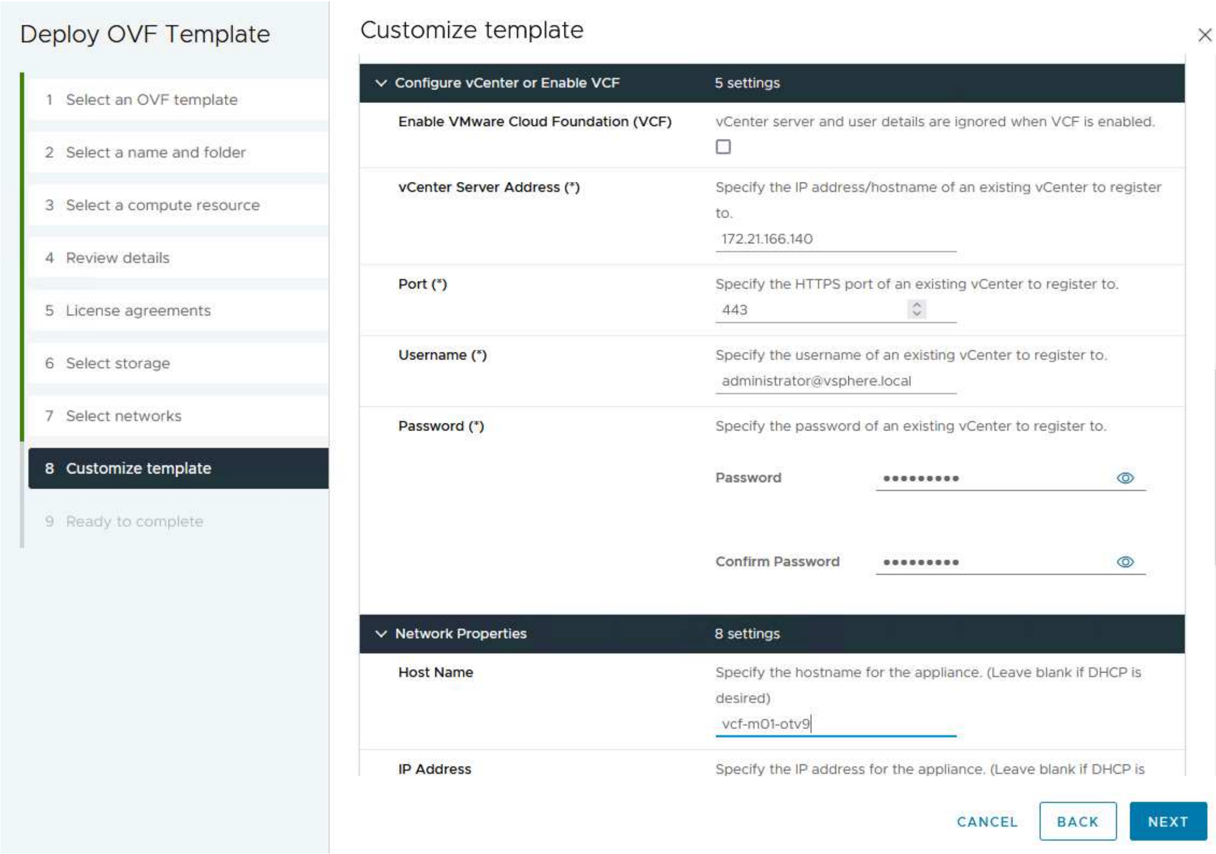
172.21.166.1

Maintenance User Password (*)

Password to assign to maint user account.

Password ●●●●●●●●●

Confirm Password ●●●●●●●●●



Customize template

Configure vCenter or Enable VCF — 5 settings

Enable VMware Cloud Foundation (VCF): vCenter server and user details are ignored when VCF is enabled. □

vCenter Server Address (*): Specify the IP address/hostname of an existing vCenter to register to. 172.21.166.140

Port (*): Specify the HTTPS port of an existing vCenter to register to. 443

Username (*): Specify the username of an existing vCenter to register to. administrator@vsphere.local

Password (*): Specify the password of an existing vCenter to register to.
Password: •••••••••
Confirm Password: •••••••••

Network Properties — 8 settings

Host Name: Specify the hostname for the appliance. (Leave blank if DHCP is desired) vcf-m01-otv9

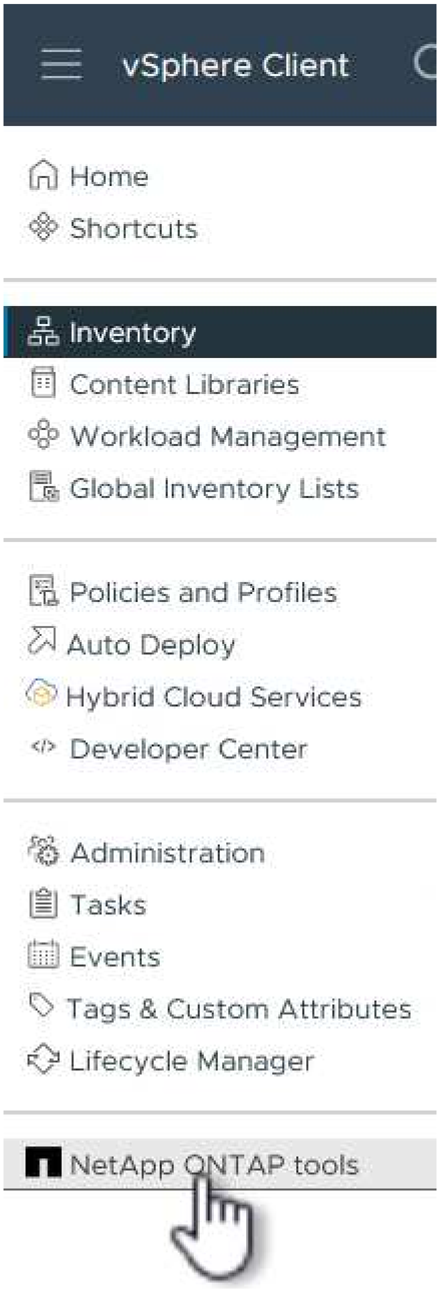
IP Address: Specify the IP address for the appliance. (Leave blank if DHCP is

9. Review all information on the Ready to complete page and the click Finish to begin deploying the OTV appliance.

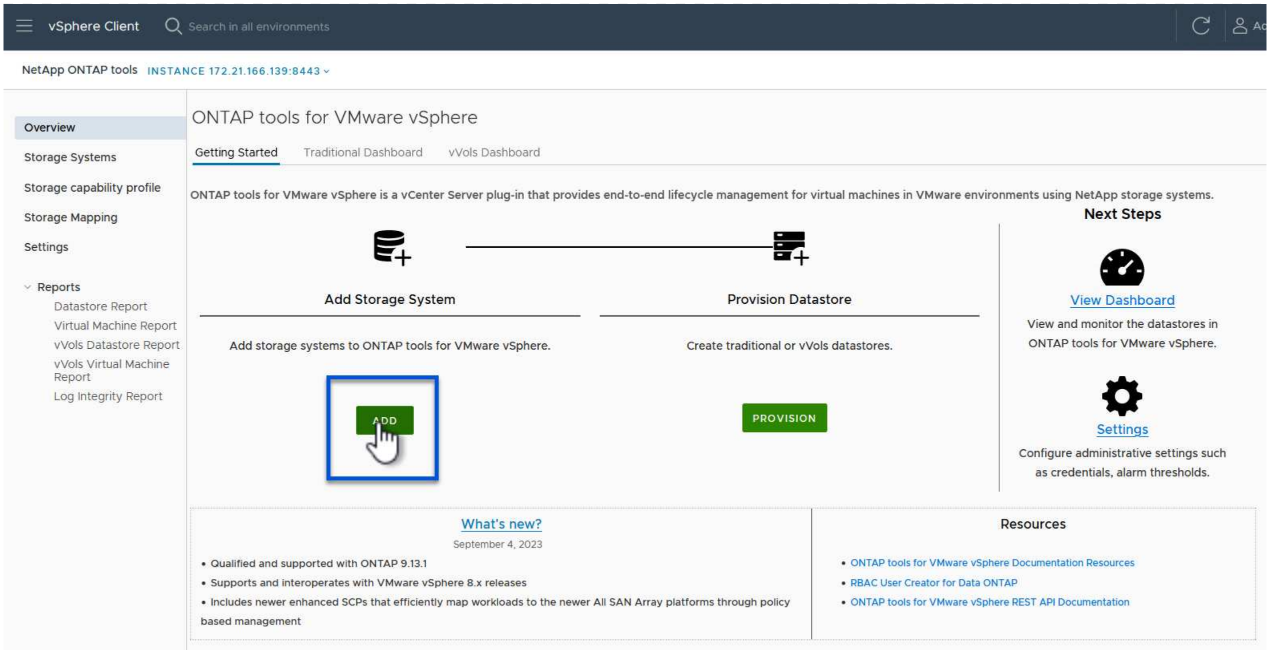
Configure a VMFS iSCSI datastore on Management Domain using OTV

Complete the following to use OTV to configure a VMFS iSCSI datastore as supplemental storage on the management domain:

1. In the vSphere client navigate to the main menu and select **NetApp ONTAP Tools**.



2. Once in **ONTAP Tools**, from the Getting Started page (or from **Storage Systems**), click on **Add** to add a new storage system.



ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.

Add storage systems to ONTAP tools for VMware vSphere.

Create traditional or vVols datastores.

View and monitor the datastores in ONTAP tools for VMware vSphere.

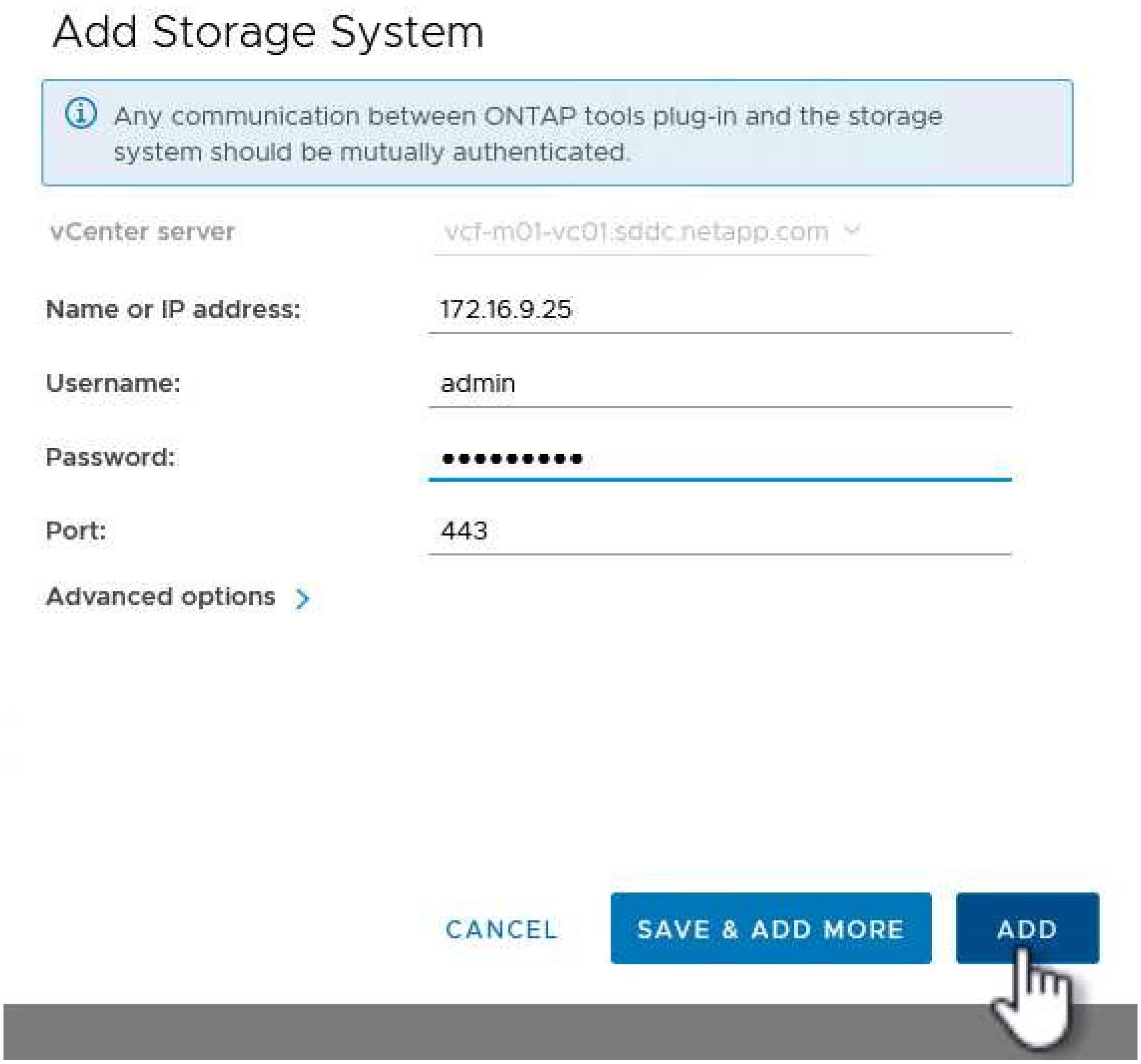
Configure administrative settings such as credentials, alarm thresholds.

September 4, 2023

- Qualified and supported with ONTAP 9.13.1
- Supports and interoperates with VMware vSphere 8.x releases
- Includes newer enhanced SCPs that efficiently map workloads to the newer All SAN Array platforms through policy based management

- ONTAP tools for VMware vSphere Documentation Resources
- RBAC User Creator for Data ONTAP
- ONTAP tools for VMware vSphere REST API Documentation

3. Provide the IP address and credentials of the ONTAP storage system and click on **Add**.



Add Storage System

Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server: vcf-m01-vc01.sddc.netapp.com

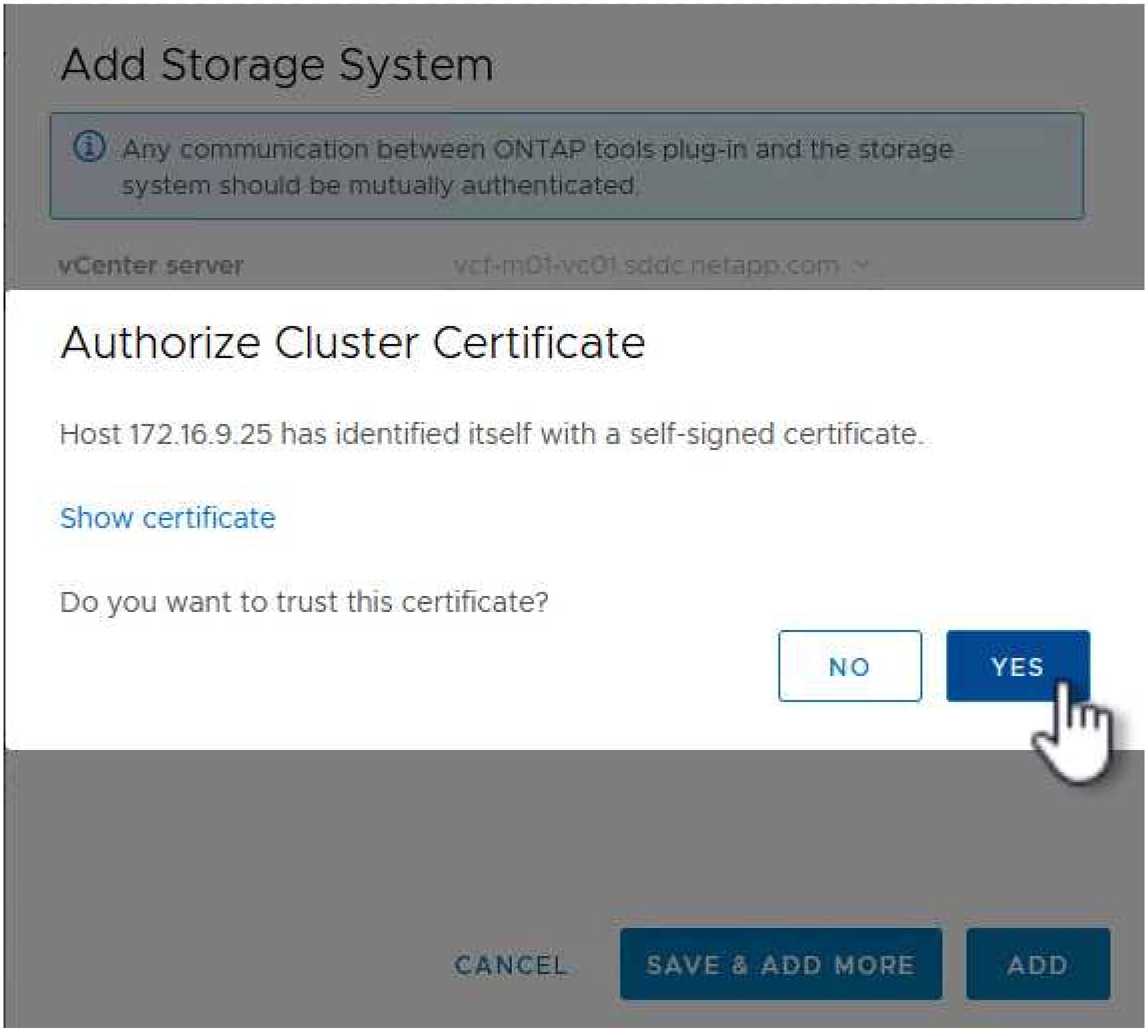
Name or IP address: 172.16.9.25

Username: admin

Password: ●●●●●●●●●●

Port: 443

4. Click on **Yes** to authorize the cluster certificate and add the storage system.



Add Storage System

Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server vcf-m01-vc01.sddc.netapp.com

Authorize Cluster Certificate

Host 172.16.9.25 has identified itself with a self-signed certificate.

Show certificate

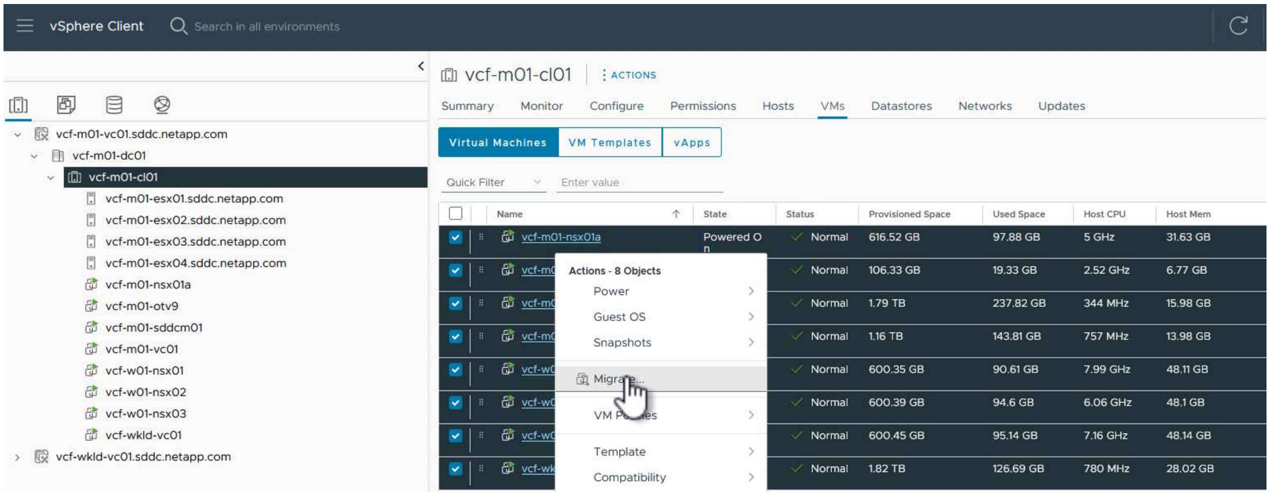
Do you want to trust this certificate?

Migrate management VM’s to iSCSI Datastore

In cases where it is preferred to use ONTAP storage to protect the VCF management VM’s vMotion can be use to migrate the VM’s to the newly created iSCSI datastore.

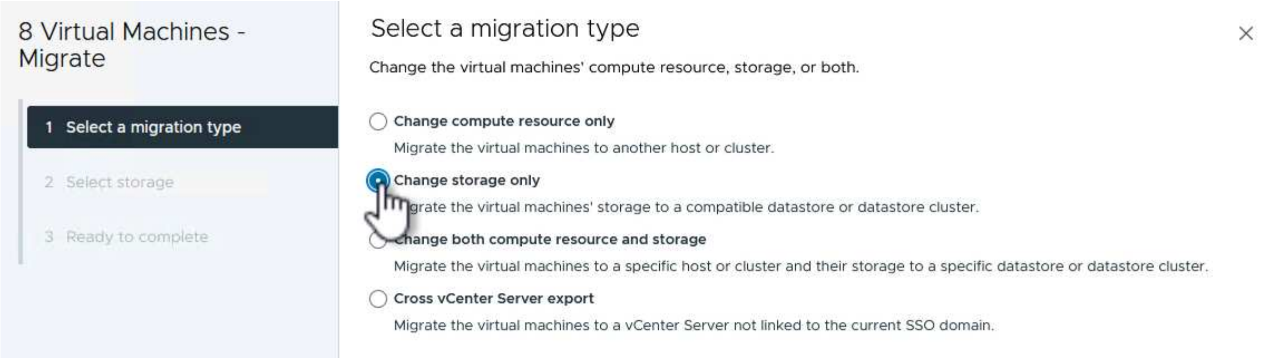
Complete the following steps to migrate the VCF management VM’s to the iSCSI datastore.

1. From the vSphere Client navigate to the management domain cluster and click on the **VMs** tab.
2. Select the VMs to be migrated to the iSCSI datastore, right click and select **Migrate...**.



☐	Name	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
☑	vcf-m01-nsx01a	Powered On	✓ Normal	616.52 GB	97.88 GB	5 GHz	31.63 GB
☑	vcf-m0		✓ Normal	106.33 GB	19.33 GB	2.52 GHz	6.77 GB
☑	vcf-m0		✓ Normal	1.79 TB	237.82 GB	344 MHz	15.98 GB
☑	vcf-m0		✓ Normal	1.16 TB	143.81 GB	757 MHz	13.98 GB
☑	vcf-w0		✓ Normal	600.35 GB	90.61 GB	7.99 GHz	48.11 GB
☑	vcf-w0		✓ Normal	600.39 GB	94.6 GB	6.06 GHz	48.1 GB
☑	vcf-w0		✓ Normal	600.45 GB	95.14 GB	7.16 GHz	48.14 GB
☑	vcf-wk		✓ Normal	1.82 TB	126.69 GB	780 MHz	28.02 GB

3. In the **Virtual Machines - Migrate** wizard, select **Change storage only** as the migration type and click on **Next** to continue.



Select a migration type

Change the virtual machines' compute resource, storage, or both.

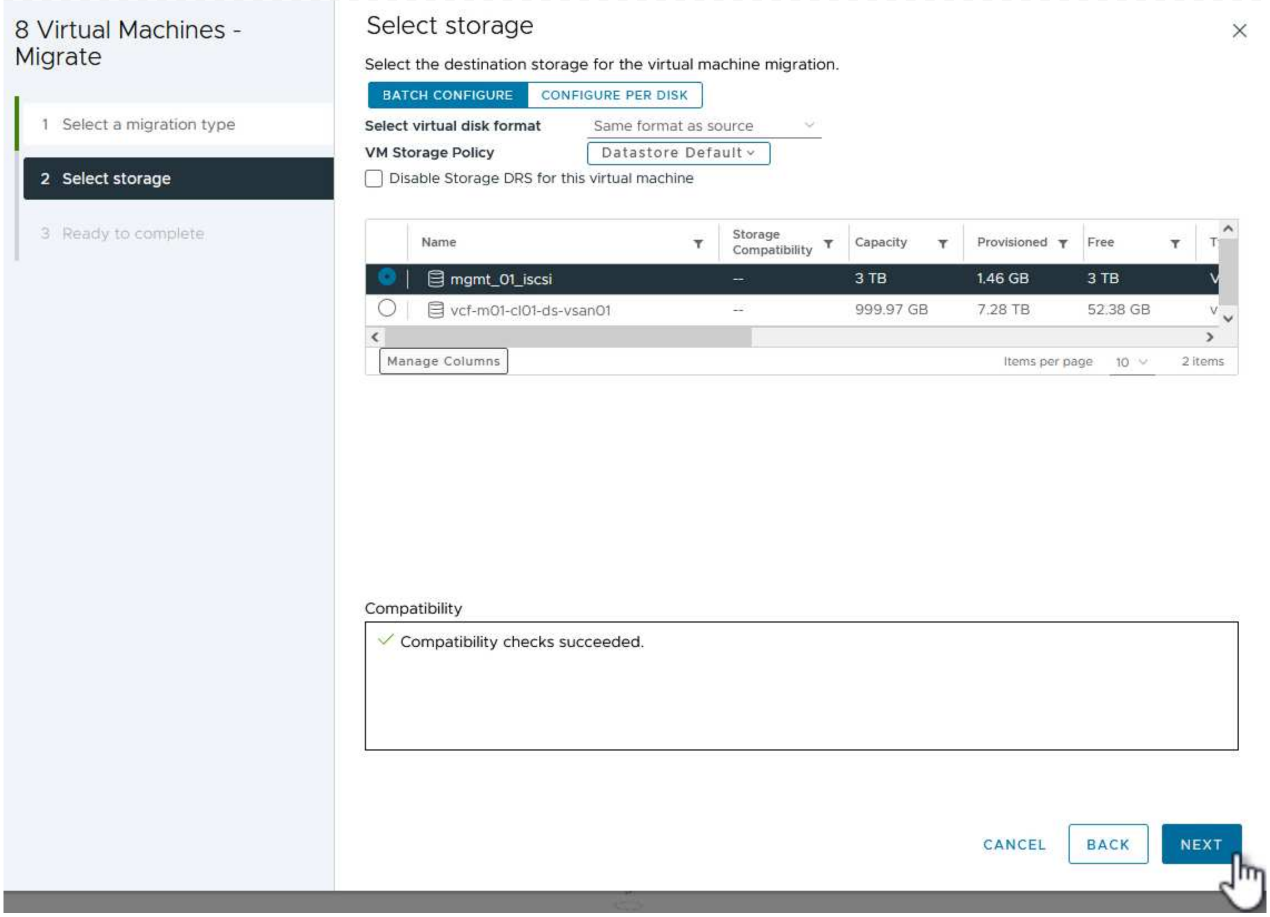
○ **Change compute resource only**
Migrate the virtual machines to another host or cluster.

● **Change storage only**
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

○ **Change both compute resource and storage**
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

○ **Cross vCenter Server export**
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

4. On the **Select storage** page, select the iSCSi datastore and select **Next** to continue.



8 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE | CONFIGURE PER DISK

Select virtual disk format: Same format as source

VM Storage Policy: Datastore Default

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	mgmt_01_iscsi	--	3 TB	1.46 GB	3 TB	V
○	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.28 TB	52.38 GB	v

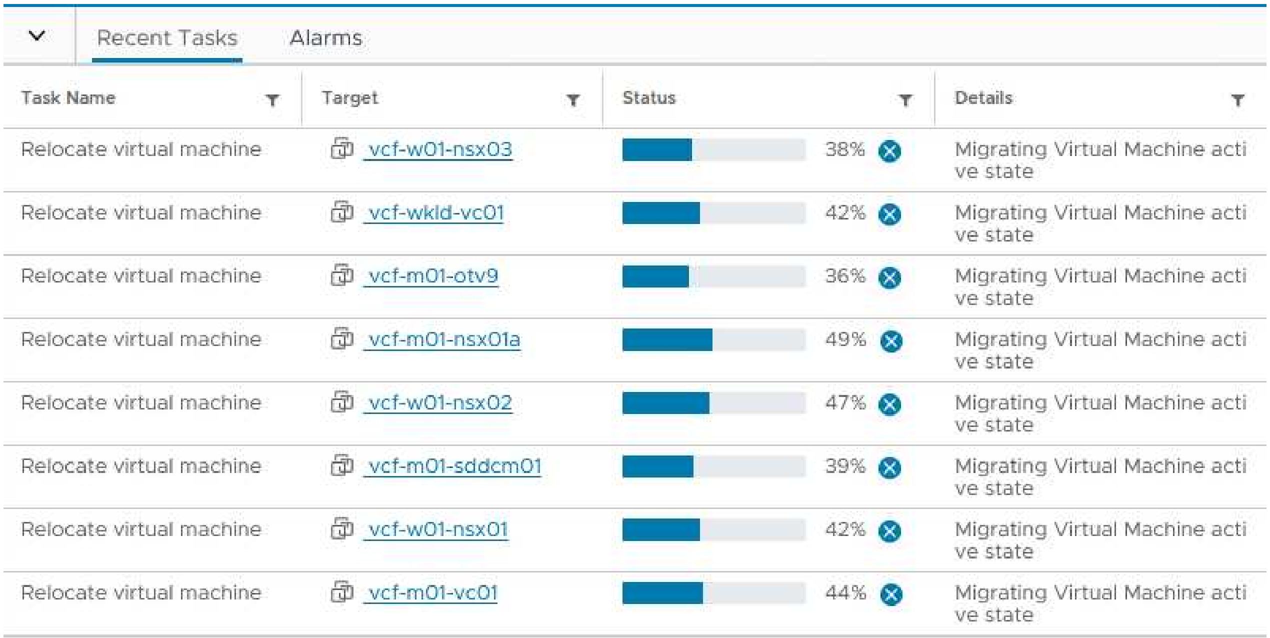
Manage Columns   Items per page 10   2 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL   BACK   NEXT

5. Review the selections and click on **Finish** to start the migration.
6. The relocation status can be viewed from the **Recent Tasks** pane.



Recent Tasks   Alarms

Task Name	Target	Status	Details
Relocate virtual machine	vcf-w01-nsx03	38%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-wkld-vc01	42%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-otv9	36%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-nsx01a	49%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-w01-nsx02	47%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-sddcm01	39%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-w01-nsx01	42%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-vc01	44%	Migrating Virtual Machine active state

Additional information

For information on configuring ONTAP storage systems refer to the ONTAP 9 Documentation center.

For information on configuring VCF refer to VMware Cloud Foundation Documentation.

Video demo for this solution

iSCSI Datastores as Supplemental Storage for VCF Management Domains

Use ONTAP Tools to configure supplemental storage (vVols) for VCF Workload Domains

In this scenario we will demonstrate how to deploy and use ONTAP Tools for VMware vSphere to configure a **vVols datastore** for a VCF workload domain.

iSCSI is used as the storage protocol for the vVols datastore.

Author: Josh Powell

Scenario Overview

This scenario covers the following high level steps:

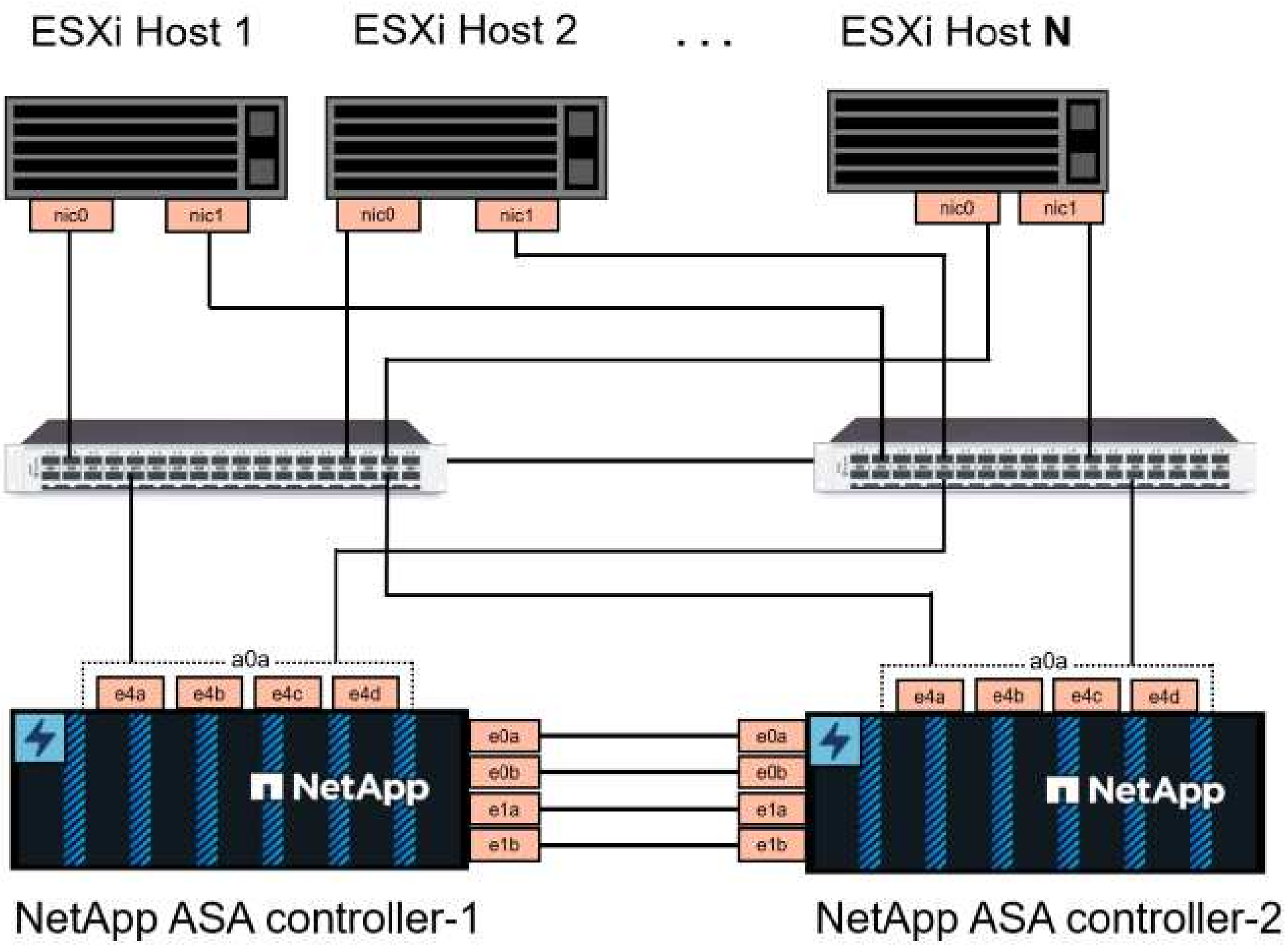
- Create a storage virtual machine (SVM) with logical interfaces (LIFs) for iSCSI traffic.
- Create distributed port groups for iSCSI networks on the VI workload domain.
- Create vmkernel adapters for iSCSI on the ESXi hosts for the VI workload domain.
- Deploy ONTAP Tools on the VI workload domain.
- Create a new vVols datastore on the VI workload domain.

Prerequisites

This scenario requires the following components and configurations:

- An ONTAP ASA storage system with physical data ports on ethernet switches dedicated to storage traffic.
- VCF management domain deployment is complete and the vSphere client is accessible.
- A VI workload domain has been previously deployed.

NetApp recommends fully redundant network designs for iSCSI. The following diagram illustrates an example of a redundant configuration, providing fault tolerance for storage systems, switches, networks adapters and host systems. Refer to the NetApp SAN configuration reference for additional information.



For multipathing and failover across multiple paths, NetApp recommends having a minimum of two LIFs per storage node in separate ethernet networks for all SVMs in iSCSI configurations.

This documentation demonstrates the process of creating a new SVM and specifying the IP address information to create multiple LIFs for iSCSI traffic. To add new LIFs to an existing SVM refer to Create a LIF (network interface).

In situations where multiple VMkernel adapters are configured on the same IP network, it is recommended to use software iSCSI port binding on the ESXi hosts to ensure that load balancing across the adapters occurs. Refer to KB article Considerations for using software iSCSI port binding in ESX/ESXi (2038869).

For additional information on using VMFS iSCSI datastores with VMware refer to vSphere VMFS Datastore - iSCSI Storage backend with ONTAP.

Deployment Steps

To deploy ONTAP Tools and use it to create a vVols datastore on the VCF management domain, complete the following steps:

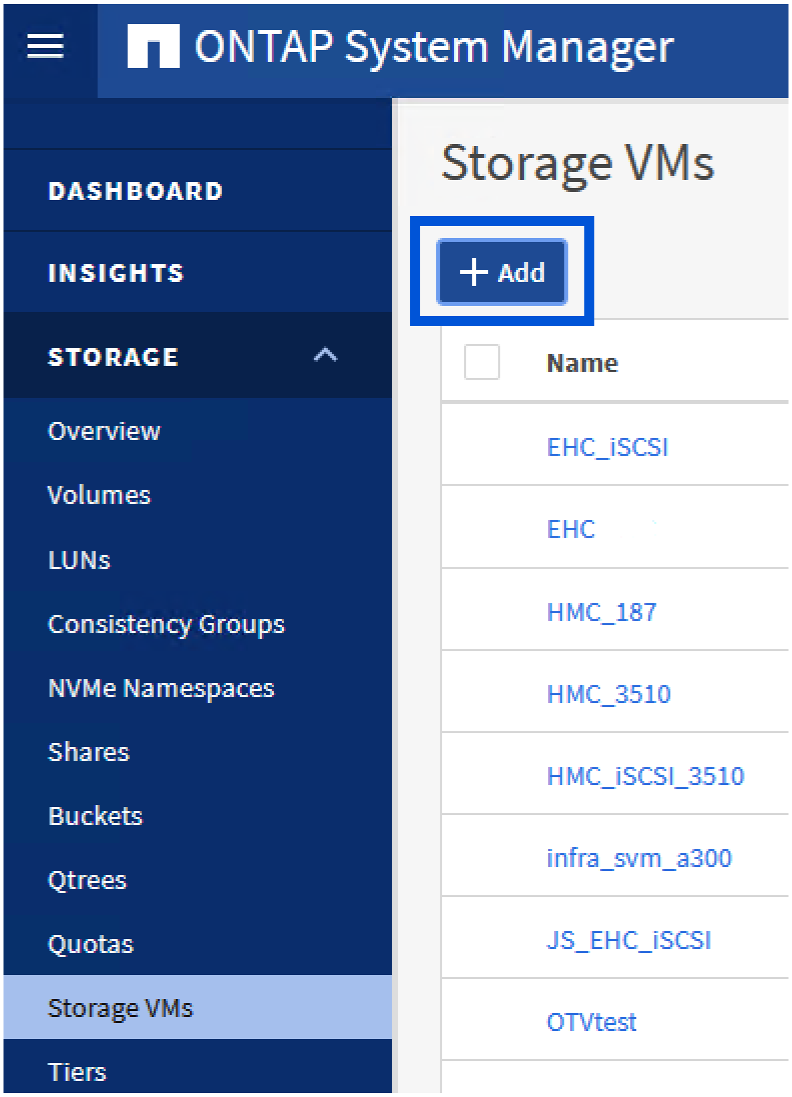
Create SVM and LIFs on ONTAP storage system

The following step is performed in ONTAP System Manager.

Create the storage VM and LIFs

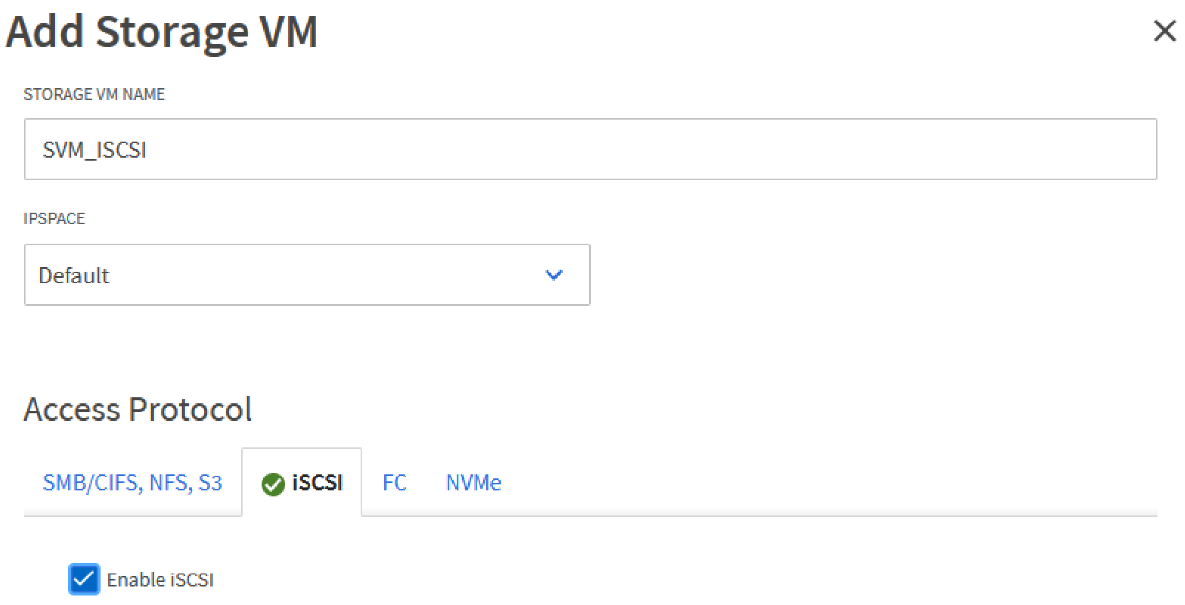
Complete the following steps to create an SVM together with multiple LIFs for iSCSI traffic.

1. From ONTAP System Manager navigate to **Storage VMs** in the left-hand menu and click on **+ Add** to start.



Name
EHC_iSCSI
EHC
HMC_187
HMC_3510
HMC_iSCSI_3510
infra_svm_a300
JS_EHC_iSCSI
OTVtest

2. In the **Add Storage VM** wizard provide a **Name** for the SVM, select the **IP Space** and then, under **Access Protocol**, click on the **iSCSI** tab and check the box to **Enable iSCSI**.



Add Storage VM

STORAGE VM NAME

SVM_ISCSI

IPSPACE

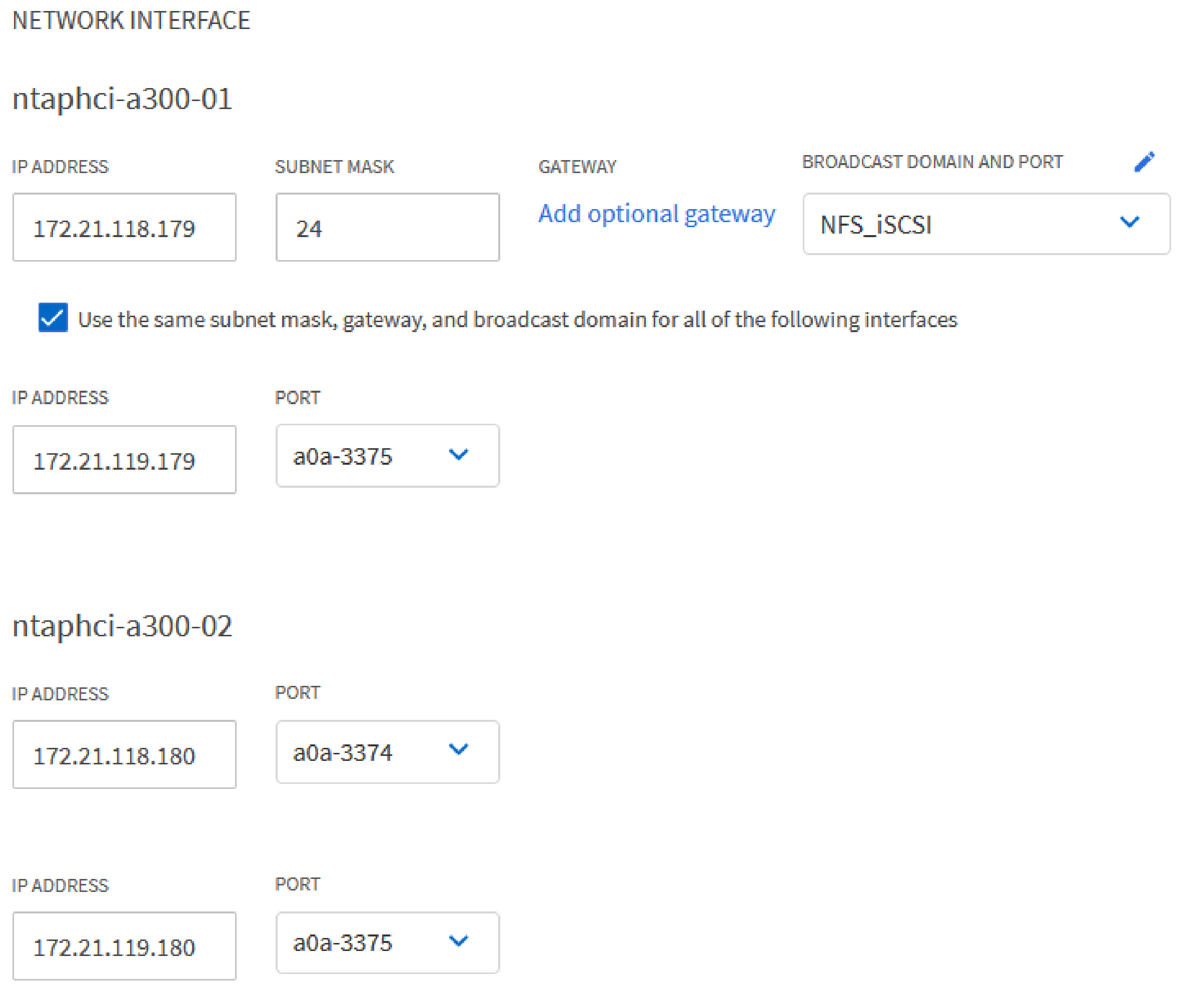
Default

Access Protocol

☑ Enable iSCSI

3. In the **Network Interface** section fill in the **IP address**, **Subnet Mask**, and **Broadcast Domain and Port** for the first LIF. For subsequent LIFs the checkbox may be enabled to use common settings across all remaining LIFs or use separate settings.

> ⓘ For multipathing and failover across multiple paths, NetApp recommends having a minimum of two LIFs per storage node in separate Ethernet networks for all SVMs in iSCSI configurations.



NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS	SUBNET MASK	GATEWAY	BROADCAST DOMAIN AND PORT
172.21.118.179	24	Add optional gateway	NFS_iSCSI

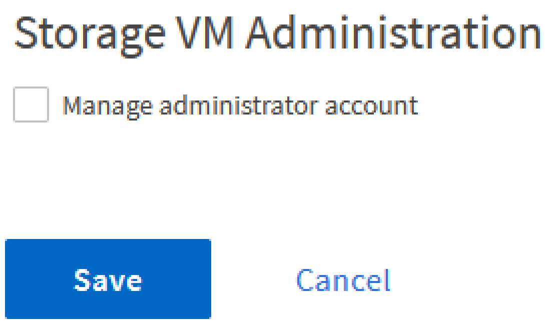
☑ Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS	PORT
172.21.119.179	a0a-3375

ntaphci-a300-02

IP ADDRESS	PORT
172.21.118.180	a0a-3374
172.21.119.180	a0a-3375

4. Choose whether to enable the Storage VM Administration account (for multi-tenancy environments) and click on **Save** to create the SVM.



Storage VM Administration

☐ Manage administrator account

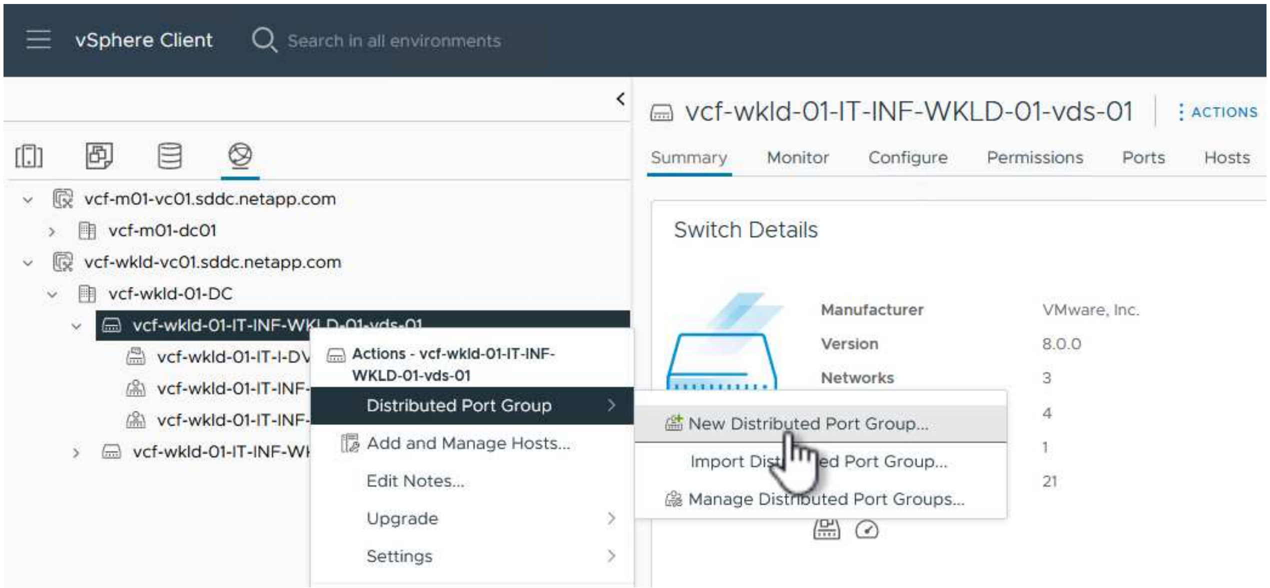
Set up networking for iSCSI on ESXi hosts

The following steps are performed on the VI Workload Domain cluster using the vSphere client. In this case vCenter Single Sign-On is being used so the vSphere client is common across the management and workload domains.

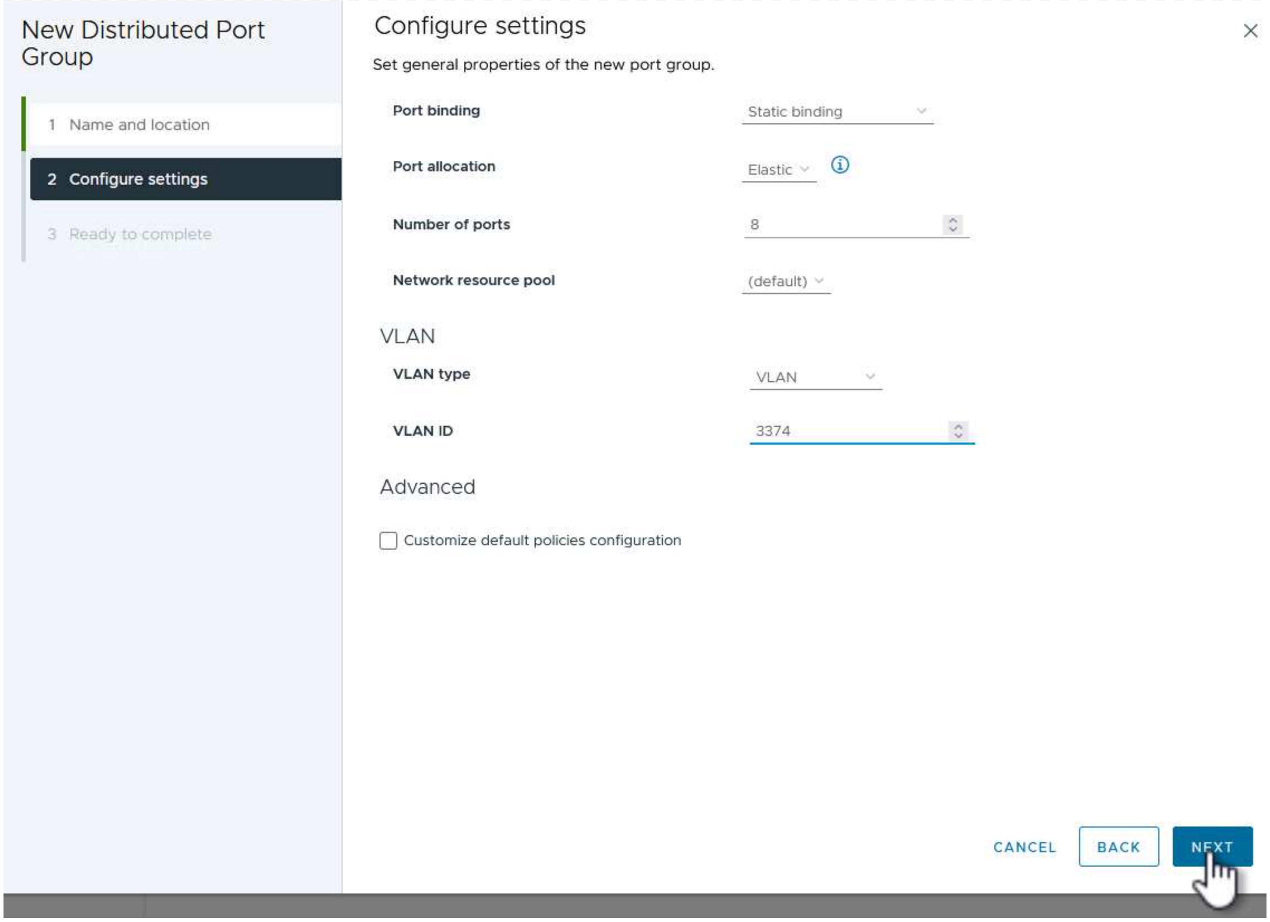
Create Distributed Port Groups for iSCSI traffic

Complete the following to create a new distributed port group for each iSCSI network:

1. From the vSphere client , navigate to **Inventory > Networking** for the workload domain. Navigate to the existing Distributed Switch and choose the action to create **New Distributed Port Group…**.



2. In the **New Distributed Port Group** wizard fill in a name for the new port group and click on **Next** to continue.
3. On the **Configure settings** page fill out all settings. If VLANs are being used be sure to provide the correct VLAN ID. Click on **Next** to continue.



New Distributed Port Group

1 Name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding: Static binding

Port allocation: Elastic

Number of ports: 8

Network resource pool: (default)

VLAN

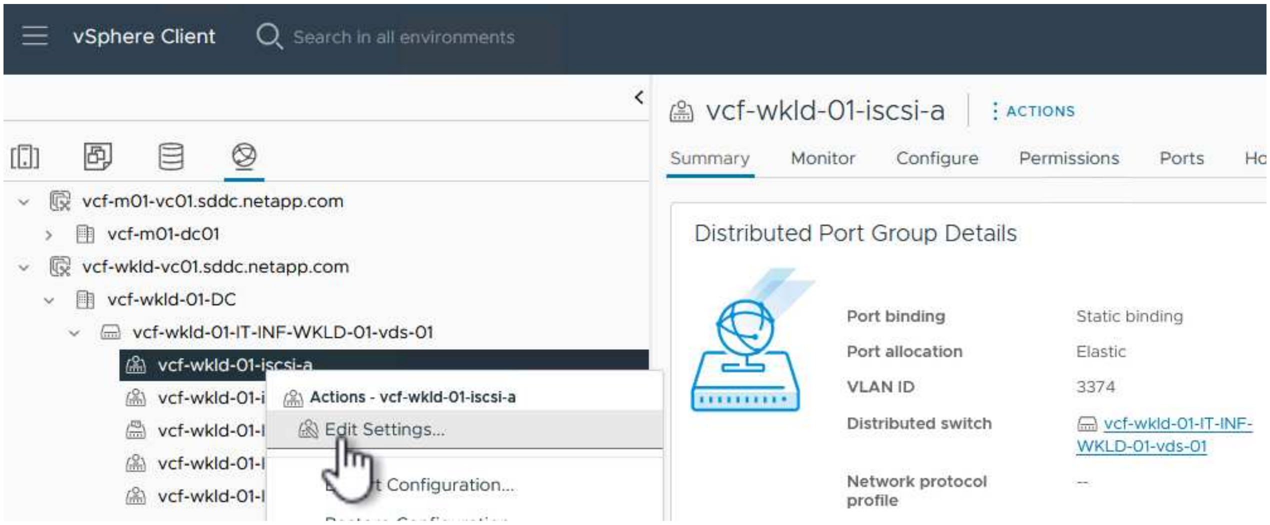
VLAN type: VLAN

VLAN ID: 3374

Advanced

□ Customize default policies configuration

4. On the **Ready to complete** page, review the changes and click on **Finish** to create the new distributed port group.
5. Repeat this process to create a distributed port group for the second iSCSI network being used and ensure you have input the correct **VLAN ID**.
6. Once both port groups have been created, navigate to the first port group and select the action to **Edit settings…**.



vcf-wkld-01-iscsi-a

Distributed Port Group Details

Port binding: Static binding

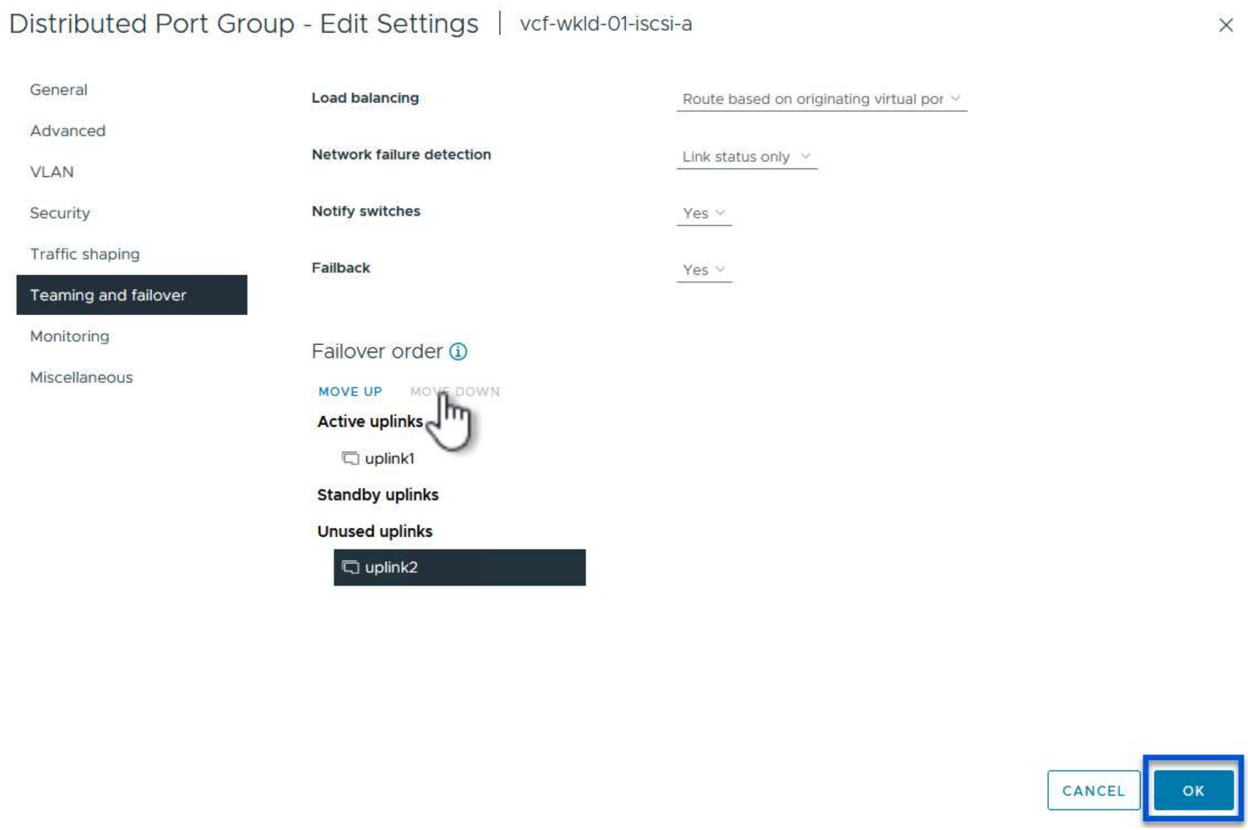
Port allocation: Elastic

VLAN ID: 3374

Distributed switch: vcf-wkld-01-IT-INF-WKLD-01-vds-01

Network protocol profile: --

7. On **Distributed Port Group - Edit Settings** page, navigate to **Teaming and failover** in the left-hand menu and click on **uplink2** to move it down to **Unused uplinks**.



Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-a

Load balancing: Route based on originating virtual por

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

Failover order

Active uplinks

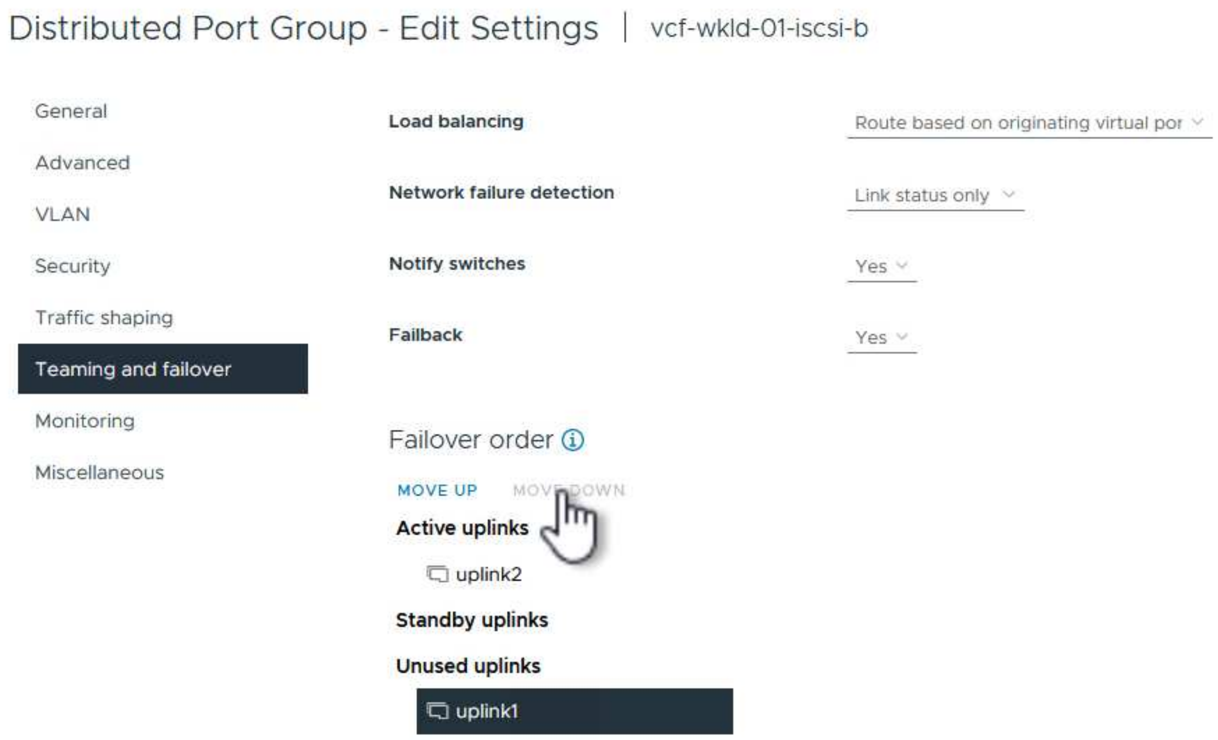
- uplink1

Standby uplinks

Unused uplinks

- uplink2

8. Repeat this step for the second iSCSI port group. However, this time move **uplink1** down to **Unused uplinks**.



Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-b

Load balancing: Route based on originating virtual por

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

Failover order

Active uplinks

- uplink2

Standby uplinks

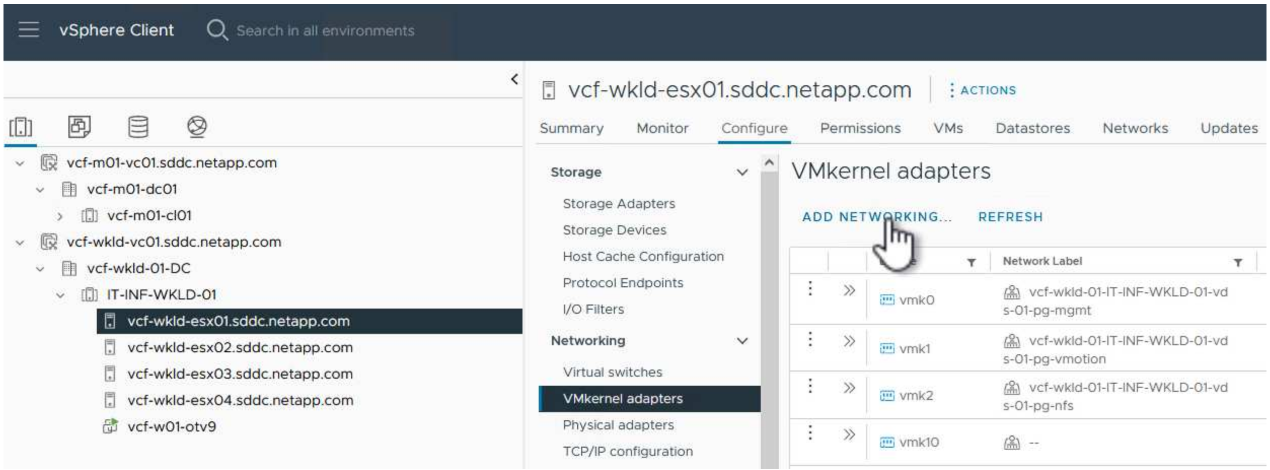
Unused uplinks

- uplink1

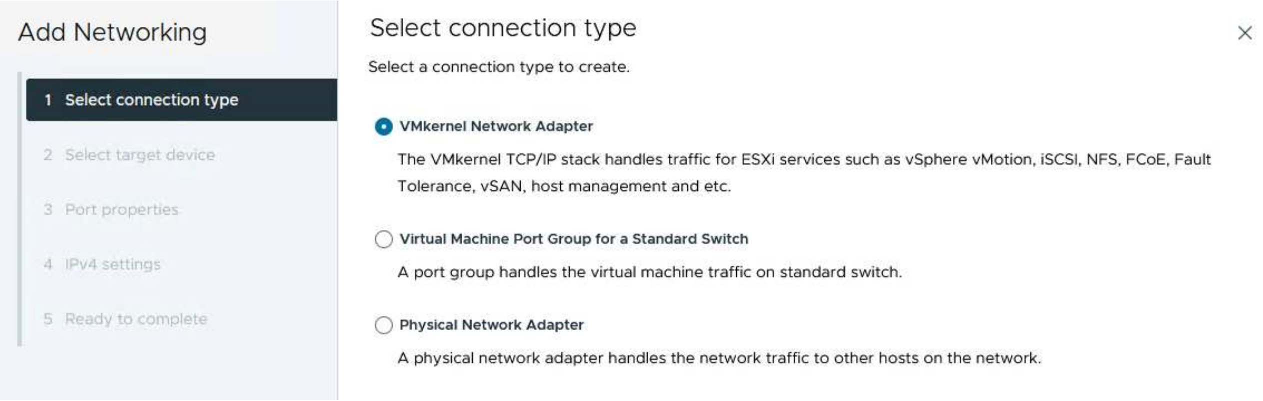
Create VMkernel adapters on each ESXi host

Repeat this process on each ESXi host in the workload domain.

1. From the vSphere client navigate to one of the ESXi hosts in the workload domain inventory. From the **Configure** tab select **VMkernel adapters** and click on **Add Networking…** to start.



2. On the **Select connection type** window choose **VMkernel Network Adapter** and click on **Next** to continue.



Select connection type

Select a connection type to create.

● VMkernel Network Adapter

The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.

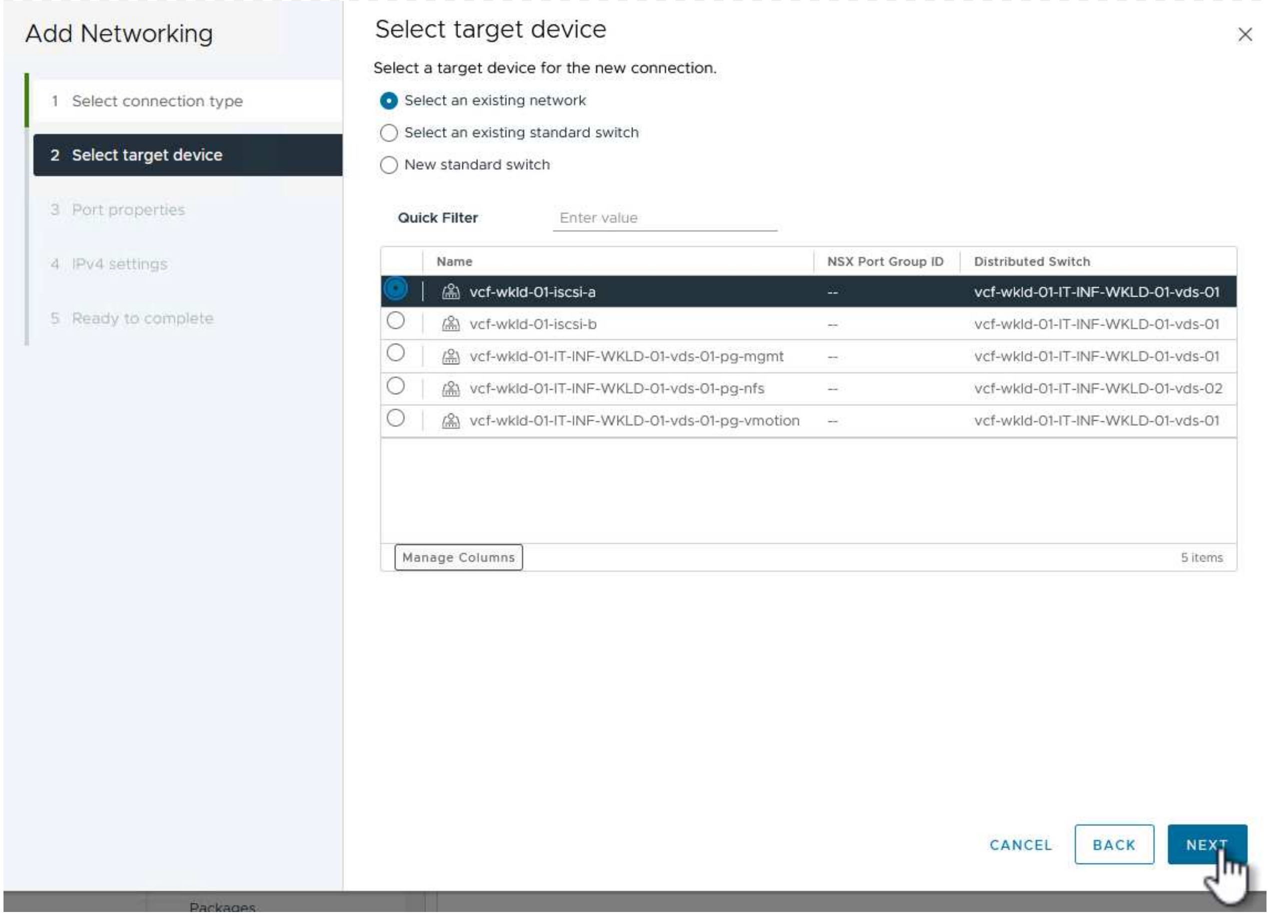
○ Virtual Machine Port Group for a Standard Switch

A port group handles the virtual machine traffic on standard switch.

○ Physical Network Adapter

A physical network adapter handles the network traffic to other hosts on the network.

3. On the **Select target device** page, choose one of the distributed port groups for iSCSI that was created previously.



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

● Select an existing network

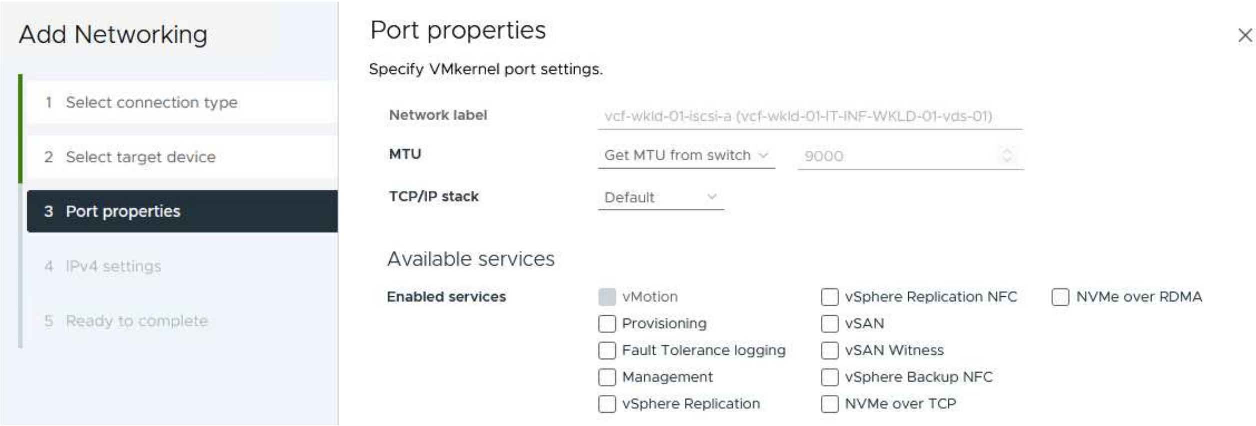
○ Select an existing standard switch

○ New standard switch

Quick Filter: Enter value

	Name	NSX Port Group ID	Distributed Switch
●	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

4. On the **Port properties** page keep the defaults and click on **Next** to continue.



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label: vcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)

MTU: Get MTU from switch 9000

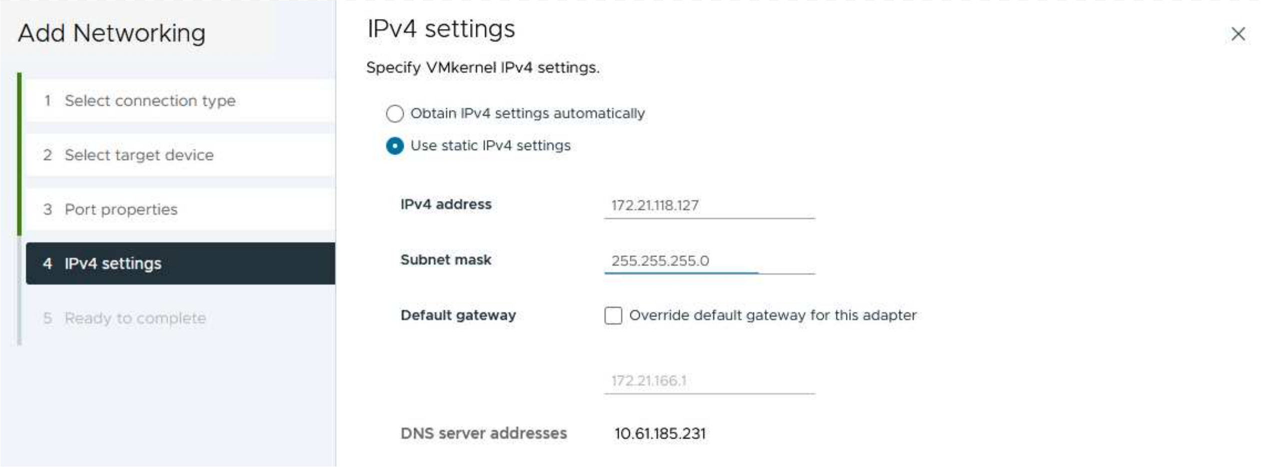
TCP/IP stack: Default

Available services

Enabled services:

□ vMotion
□ Provisioning
□ Fault Tolerance logging
□ Management
□ vSphere Replication
□ vSphere Replication NFC
□ vSAN
□ vSAN Witness
□ vSphere Backup NFC
□ NVMe over TCP
□ NVMe over RDMA

5. On the **IPv4 settings** page fill in the **IP address**, **Subnet mask**, and provide a new Gateway IP address (only if required). Click on **Next** to continue.



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

○ Obtain IPv4 settings automatically

● Use static IPv4 settings

IPv4 address 172.21.118.127

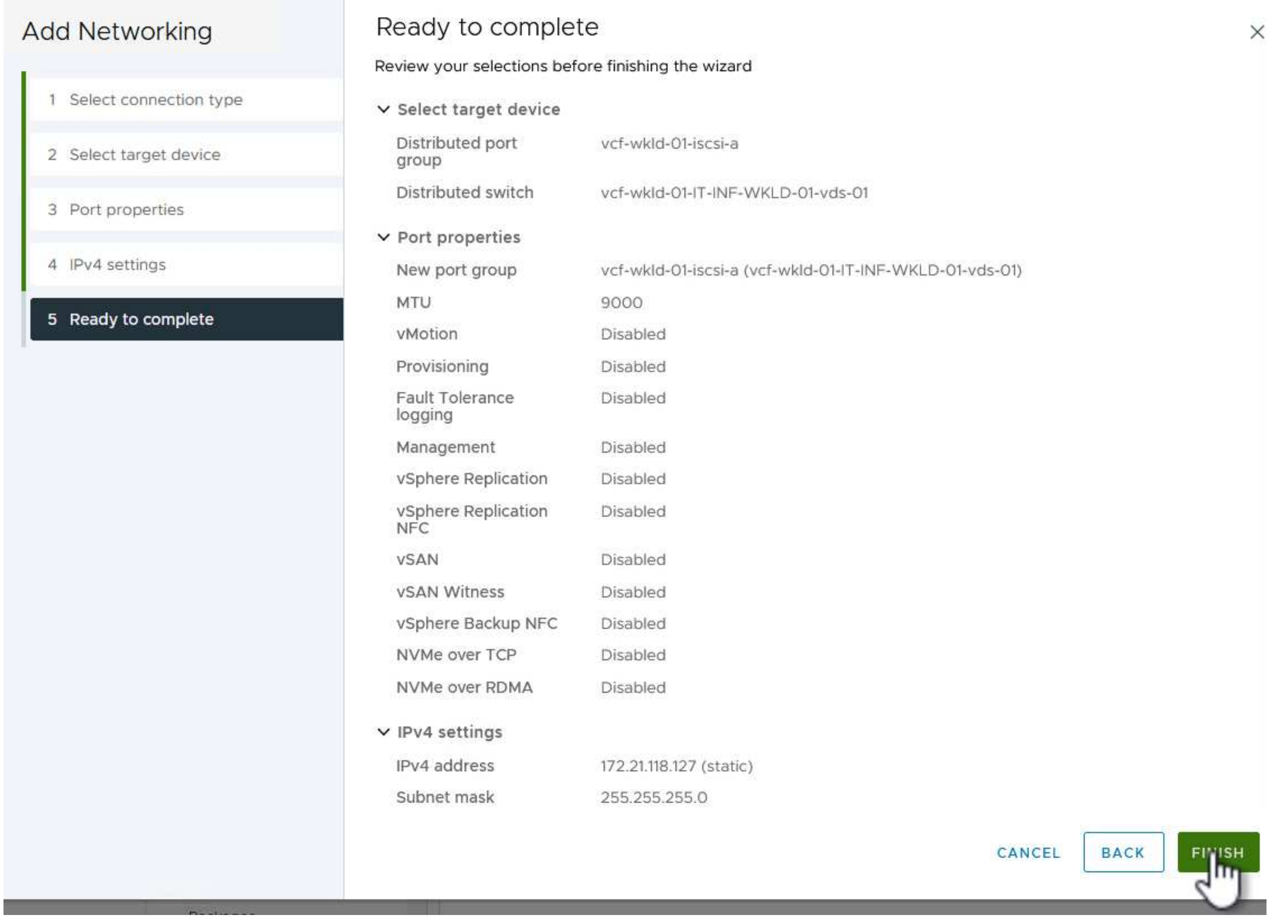
Subnet mask 255.255.255.0

Default gateway □ Override default gateway for this adapter

172.21.166.1

DNS server addresses 10.61.185.231

6. Review the your selections on the **Ready to complete** page and click on **Finish** to create the VMkernel adapter.



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

Select target device

Distributed port group	vcf-wkld-01-iscsi-a
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Port properties

New port group	vcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Disabled
NVMe over RDMA	Disabled

IPv4 settings

IPv4 address	172.21.118.127 (static)
Subnet mask	255.255.255.0

7. Repeat this process to create a VMkernel adapter for the second iSCSI network.

Deploy and use ONTAP Tools to configure storage

The following steps are performed on the VCF management domain cluster using the vSphere client and involve deploying ONTAP Tools, creating a vVols iSCSI datastore, and migrating management VM’s to the new datastore.

For VI workload domains, ONTAP Tools is installed to the VCF Management Cluster but registered with the vCenter associated with the VI workload domain.

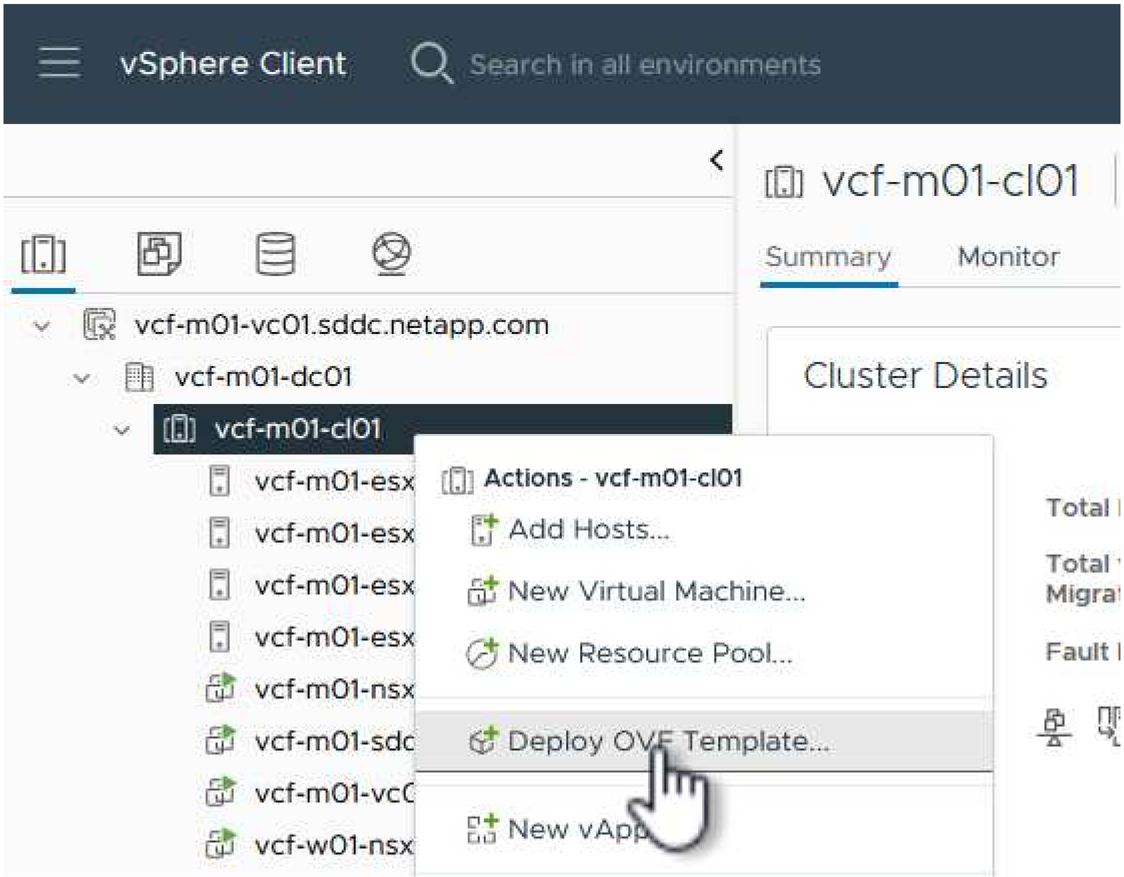
For additional information on deploying and using ONTAP Tools in a multiple vCenter environment refer to Requirements for registering ONTAP tools in multiple vCenter Servers environment.

Deploy ONTAP tools for VMware vSphere

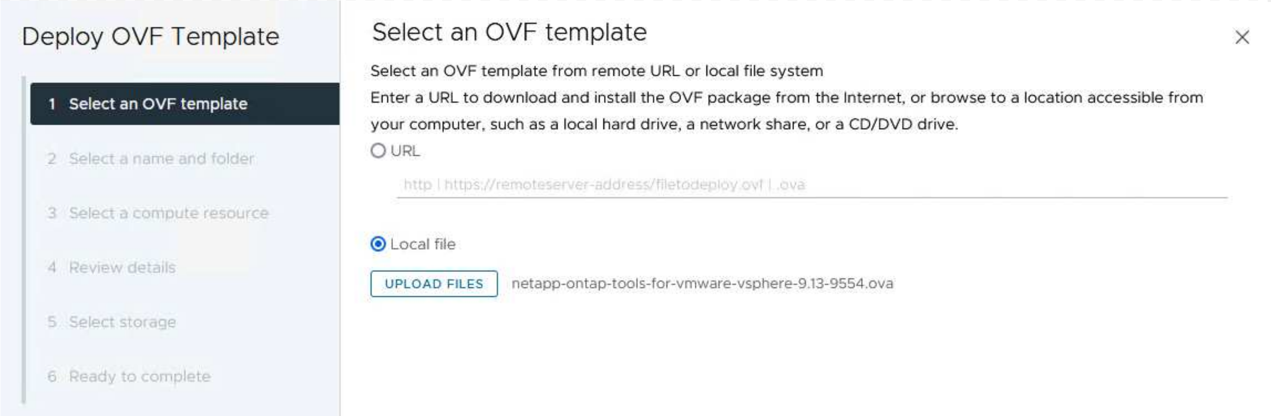
ONTAP tools for VMware vSphere is deployed as a VM appliance and provides an integrated vCenter UI for managing ONTAP storage.

Complete the following to Deploy ONTAP tools for VMware vSphere:

1. Obtain the ONTAP tools OVA image from the NetApp Support site and download to a local folder.
2. Log into the vCenter appliance for the VCF management domain.
3. From the vCenter appliance interface right-click on the management cluster and select **Deploy OVF Template…**



4. In the **Deploy OVF Template** wizard click the **Local file** radio button and select the ONTAP tools OVA file downloaded in the previous step.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

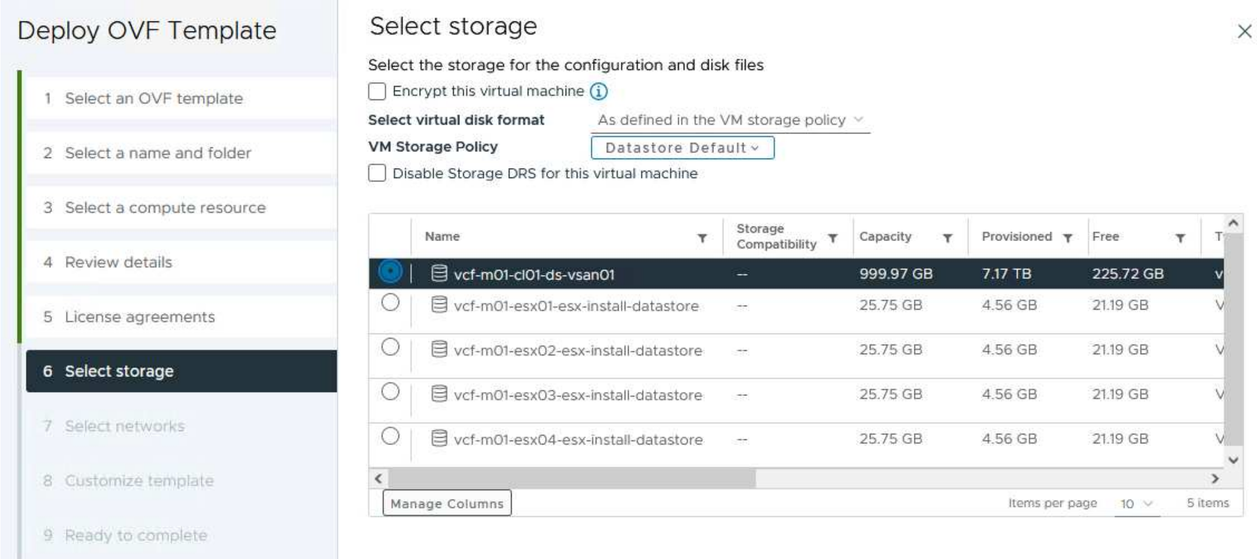
○ URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

● Local file

UPLOAD FILES netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. For steps 2 through 5 of the wizard select a name and folder for the VM, select the compute resource, review the details, and accept the license agreement.
6. For the storage location of the configuration and disk files, select the vSAN datastore of the VCF management domain cluster.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine

Select virtual disk format: As defined in the VM storage policy

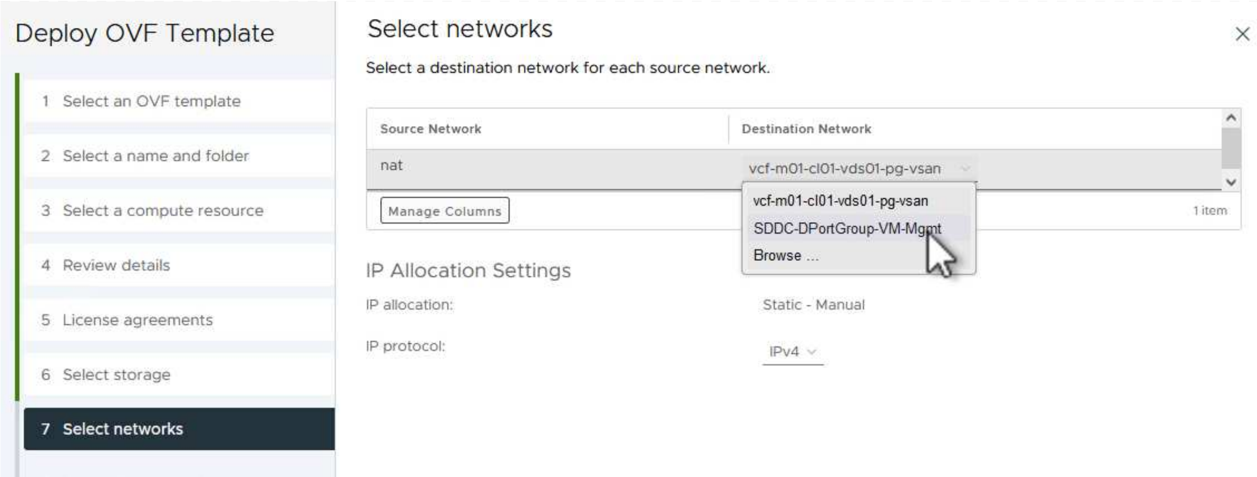
VM Storage Policy: Datastore Default

□ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	v
○	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V

Manage Columns Items per page 10 5 items

7. On the Select network page select the network used for management traffic.



Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	vcf-m01-cl01-vds01-pg-vsan

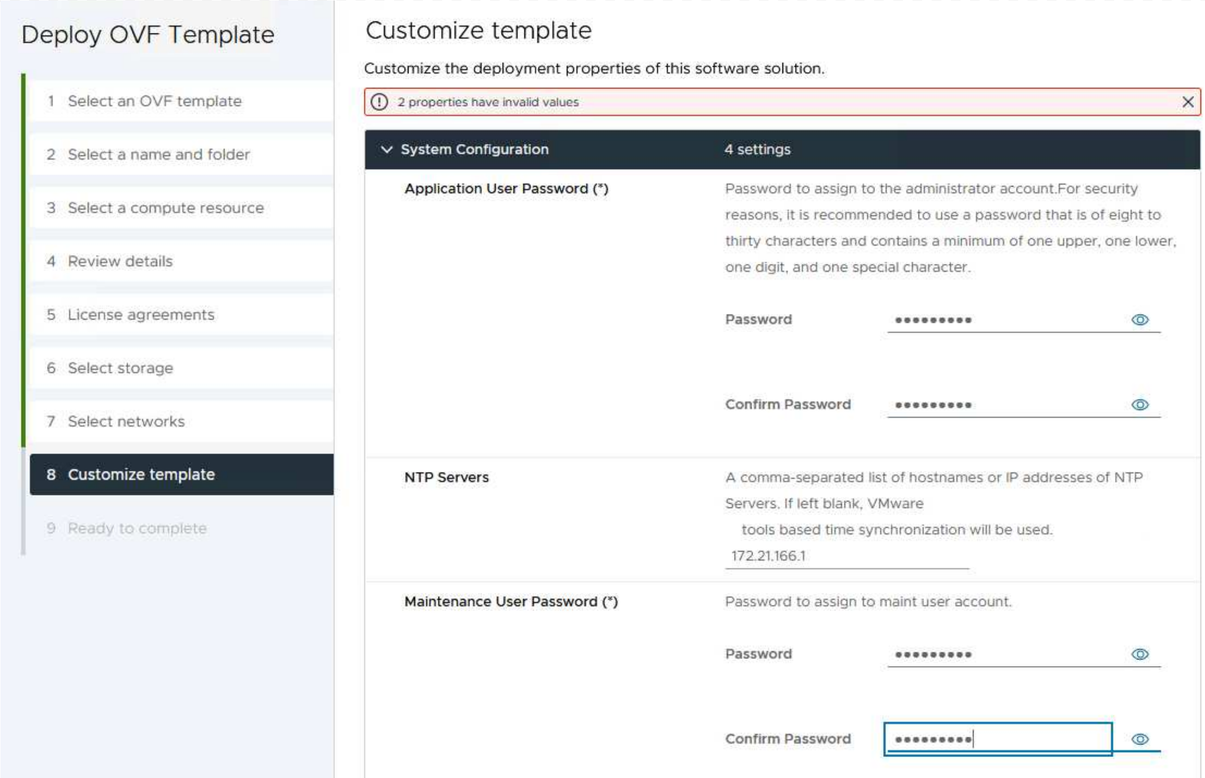
IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

8. On the Customize template page fill out all required information:
   - Password to be used for administrative access to ONTAP Tools.
   - NTP server IP address.
   - ONTAP Tools maintenance account password.
   - ONTAP Tools Derby DB password.
   - Do not check the box to **Enable VMware Cloud Foundation (VCF)**. VCF mode is not required for deploying supplemental storage.
   - FQDN or IP address of the vCenter appliance for the **VI Workload Domain**
   - Credentials for the vCenter appliance of the **VI Workload Domain**
   - Provide the required network properties fields.

     Click on **Next** to continue.



Customize template

Customize the deployment properties of this software solution.

ⓘ 2 properties have invalid values

System Configuration — 4 settings

Application User Password (*) — Password to assign to the administrator account.For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.

Password: •••••••••

Confirm Password: •••••••••

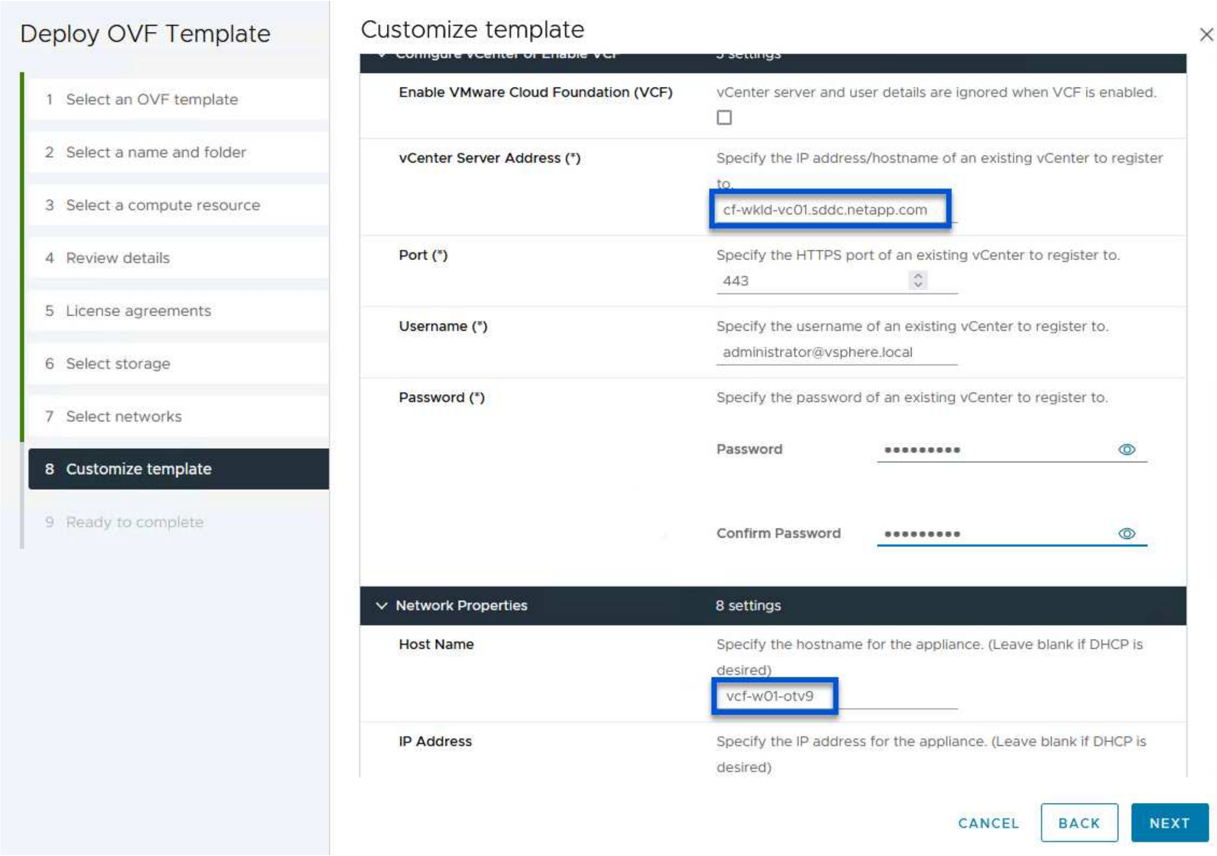
NTP Servers — A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used.

172.21.166.1

Maintenance User Password (*) — Password to assign to maint user account.

Password: •••••••••

Confirm Password: •••••••••



Customize template

Configure vCenter or Enable VCF — 3 settings

Enable VMware Cloud Foundation (VCF) — vCenter server and user details are ignored when VCF is enabled.

□

vCenter Server Address (*) — Specify the IP address/hostname of an existing vCenter to register to.

cf-wkld-vc01.sddc.netapp.com

Port (*) — Specify the HTTPS port of an existing vCenter to register to.

443

Username (*) — Specify the username of an existing vCenter to register to.

administrator@vsphere.local

Password (*) — Specify the password of an existing vCenter to register to.

Password: •••••••••

Confirm Password: •••••••••

Network Properties — 8 settings

Host Name — Specify the hostname for the appliance. (Leave blank if DHCP is desired)

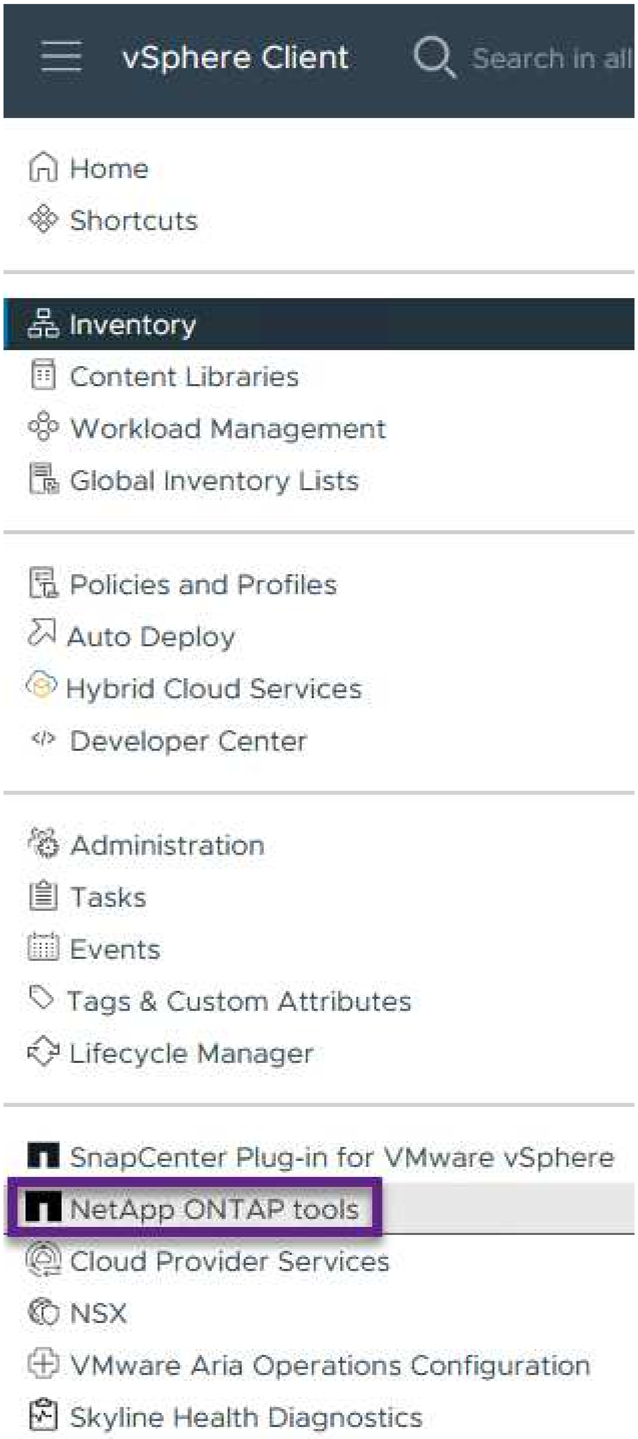
vcf-w01-otv9

IP Address — Specify the IP address for the appliance. (Leave blank if DHCP is desired)

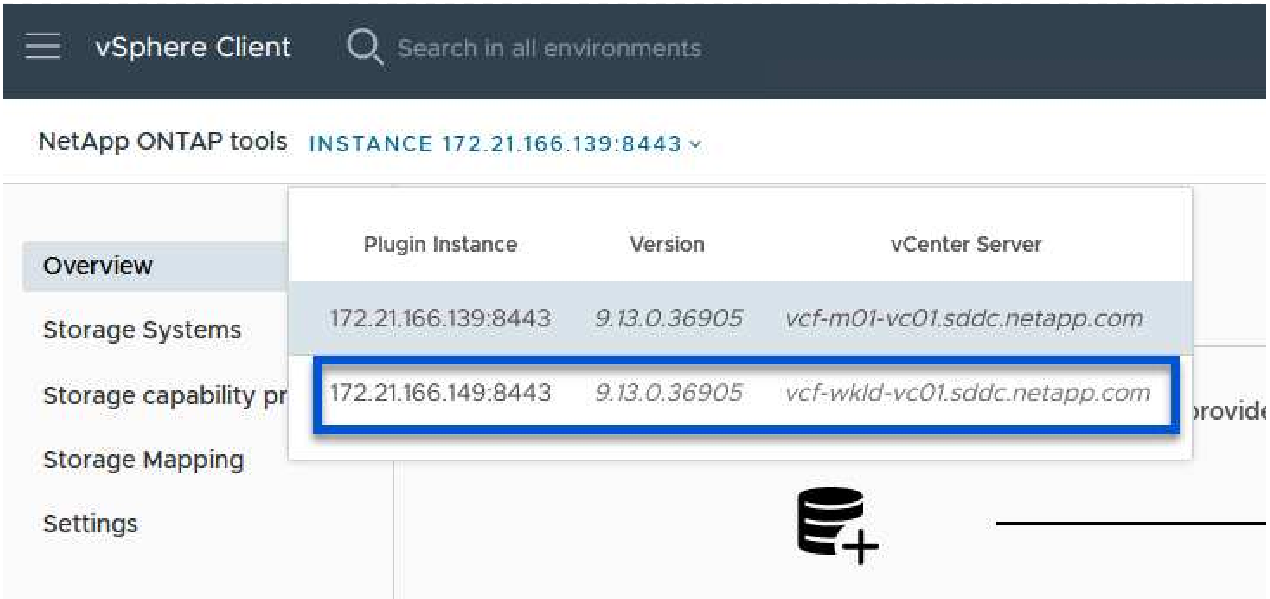
9. Review all information on the Ready to complete page and the click Finish to begin deploying the ONTAP Tools appliance.

Add a storage system to ONTAP Tools.

1. Access NetApp ONTAP Tools by selecting it from the main menu in the vSphere client.

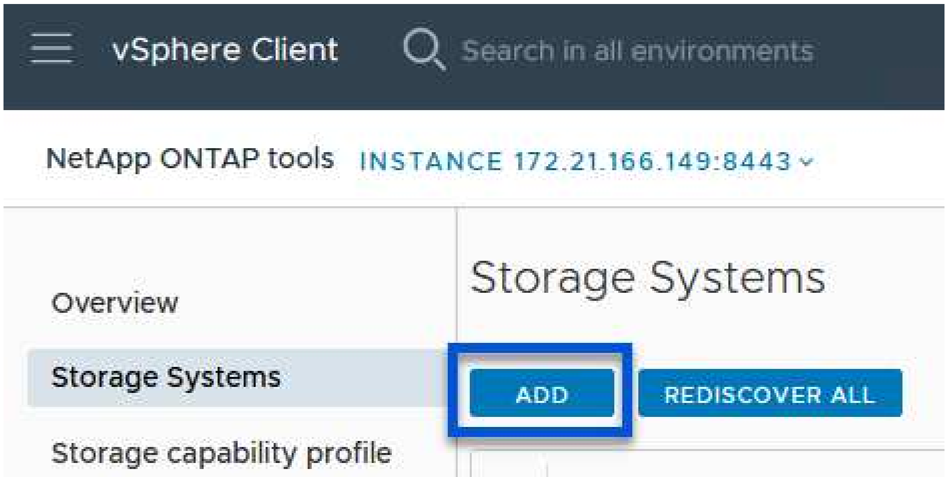


2. From the **INSTANCE** drop down menu in the ONTAP Tool interface, select the ONTAP Tools instance associated with the workload domain to be managed.



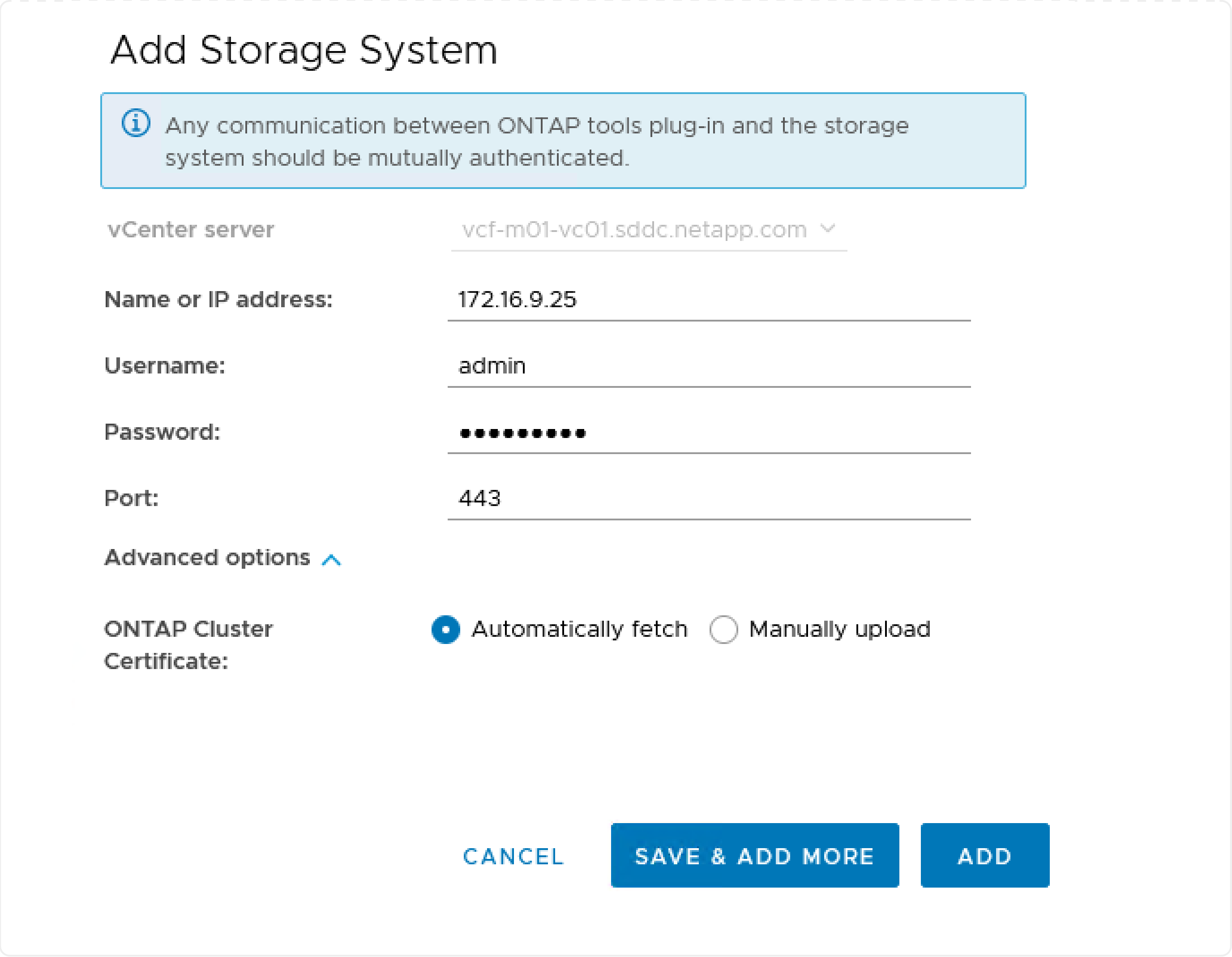
Plugin Instance	Version	vCenter Server
172.21.166.139:8443	9.13.0.36905	vcf-m01-vc01.sddc.netapp.com
172.21.166.149:8443	9.13.0.36905	vcf-wkld-vc01.sddc.netapp.com

3. In ONTAP Tools select **Storage Systems** from the left hand menu and then press **Add**.



4. Fill out the IP Address, credentials of the storage system and the port number. Click on **Add** to start the discovery process.

ⓘ vVol requires ONTAP cluster credentials rather than SVM credentials. For more information refer to Add storage systems In the ONTAP Tools documentation.



Add Storage System

Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server: vcf-m01-vc01.sddc.netapp.com

Name or IP address: 172.16.9.25

Username: admin

Password: ●●●●●●●●●●

Port: 443

Advanced options

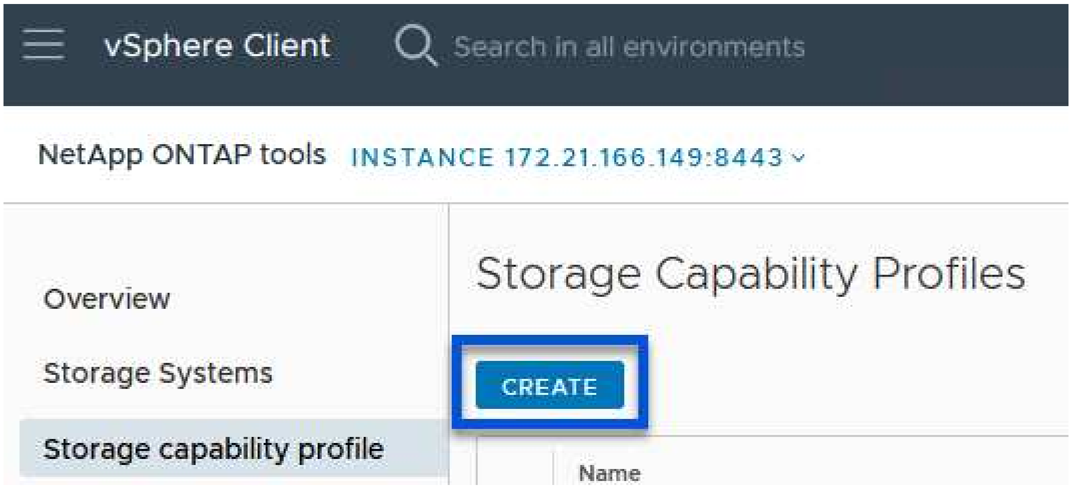
ONTAP Cluster Certificate: ● Automatically fetch ○ Manually upload

Create a storage capability profile in ONTAP Tools

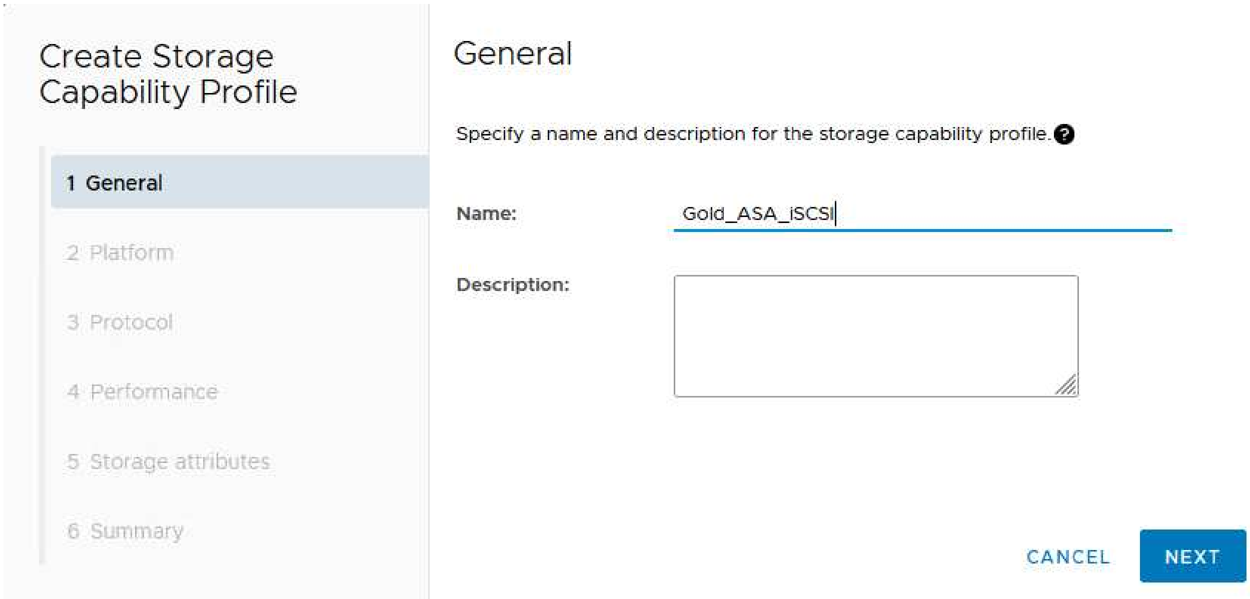
Storage capability profiles describe the features provided by a storage array or storage system. They include quality of service definitions and are used to select storage systems that meet the parameters defined in the profile. One of the provided profiles can be used or new ones can be created.

To create a storage capability profile in ONTAP Tools complete the following steps:

1. In ONTAP Tools select **Storage capability profile** from the left-hand menu and then press **Create**.


vSphere Client
Search in all environments
NetApp ONTAP tools
INSTANCE 172.21.166.149:8443
Overview
Storage Systems
Storage capability profile
Storage Capability Profiles
CREATE
Name

2. In the **Create Storage Capability profile** wizard provide a name and description of the profile and click on **Next**.

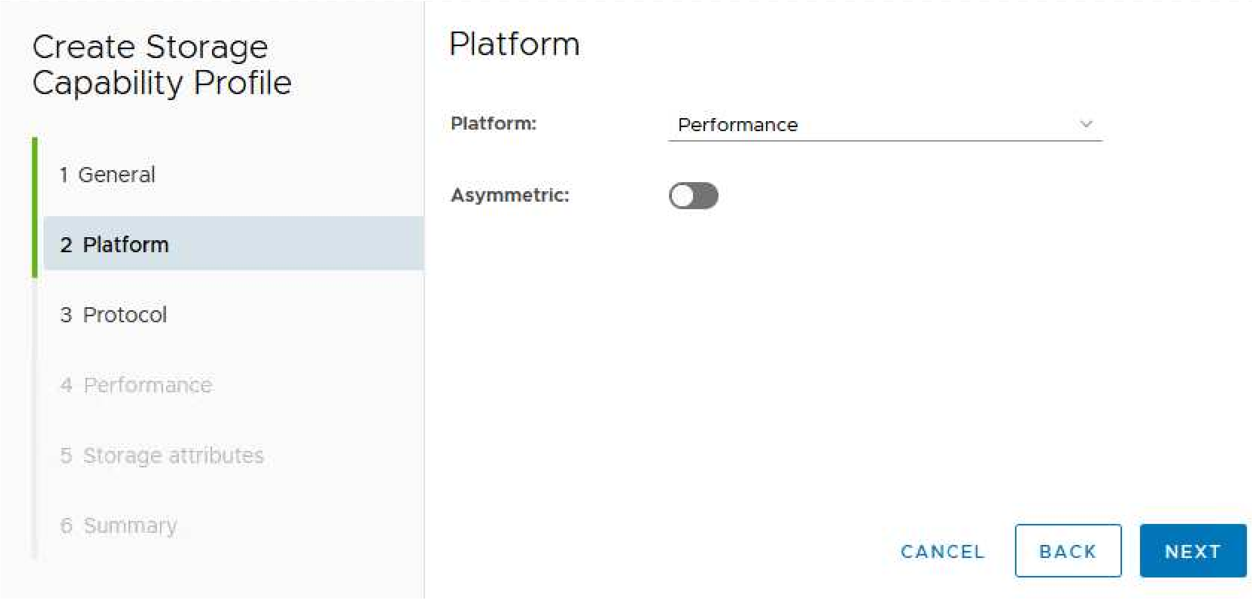


Specify a name and description for the storage capability profile.

Name: Gold_ASA_iSCSI

Description:

3. Select the platform type and to specify the storage system is to be an All-Flash SAN Array set **Asymmetric** to false.

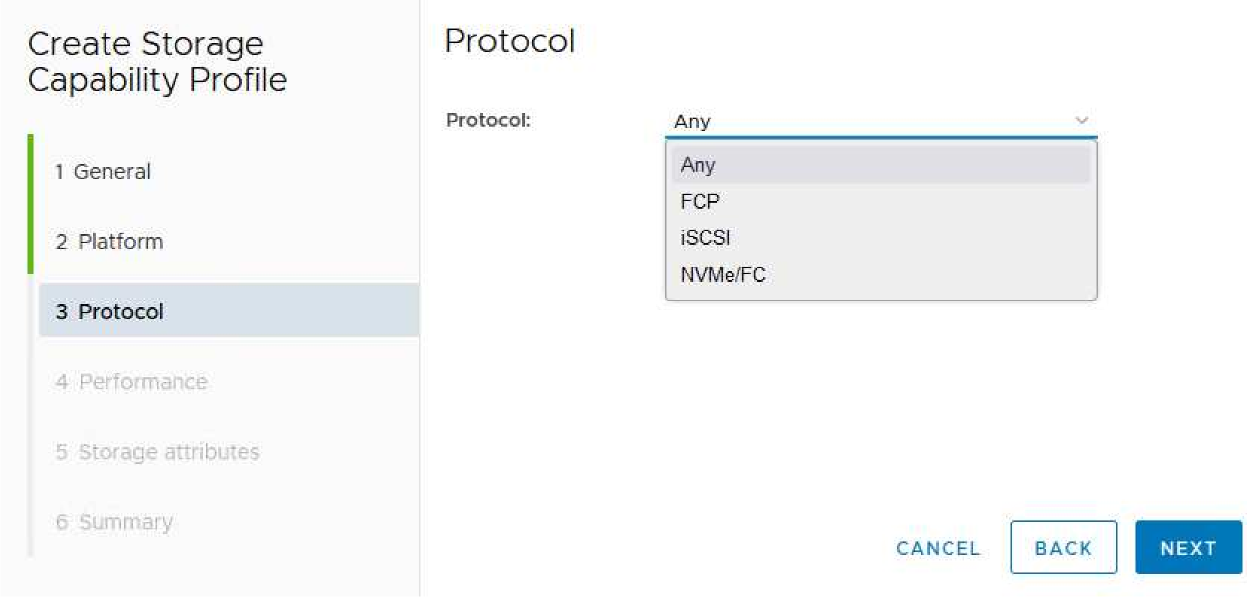


Platform

Platform: Performance

Asymmetric:

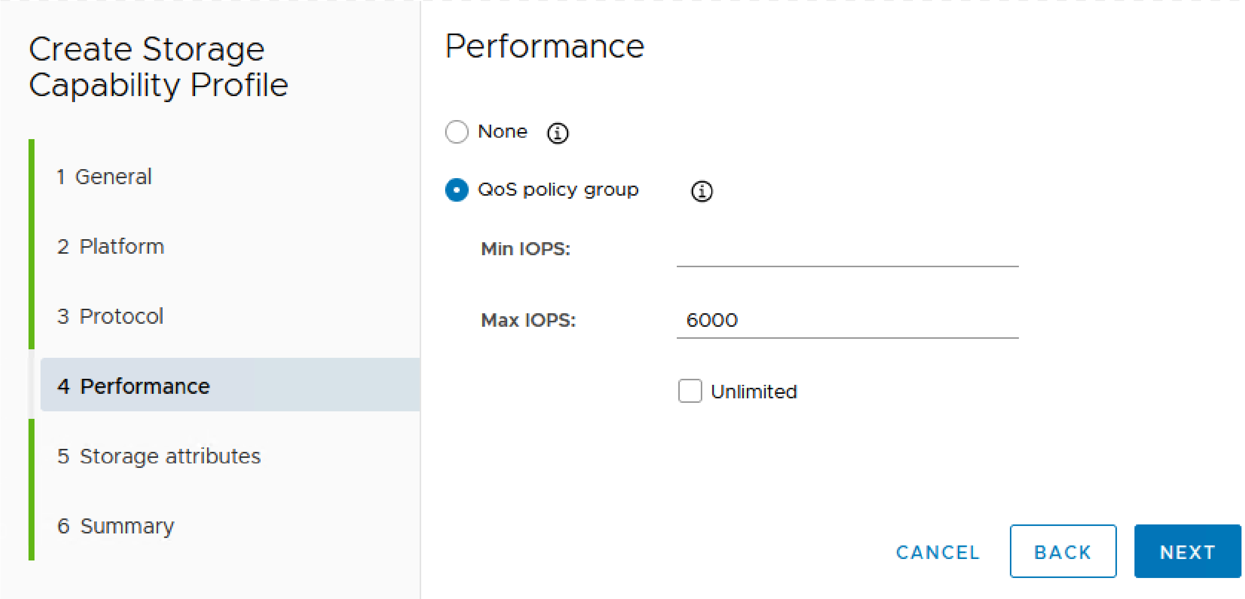
4. Next, select choice of protocol or **Any** to allow all possible protocols. Click **Next** to continue.



Protocol

Protocol: Any

5. The **performance** page allows setting of quality of service in form of minimum and maximum IOPs allowed.



Performance

○ None

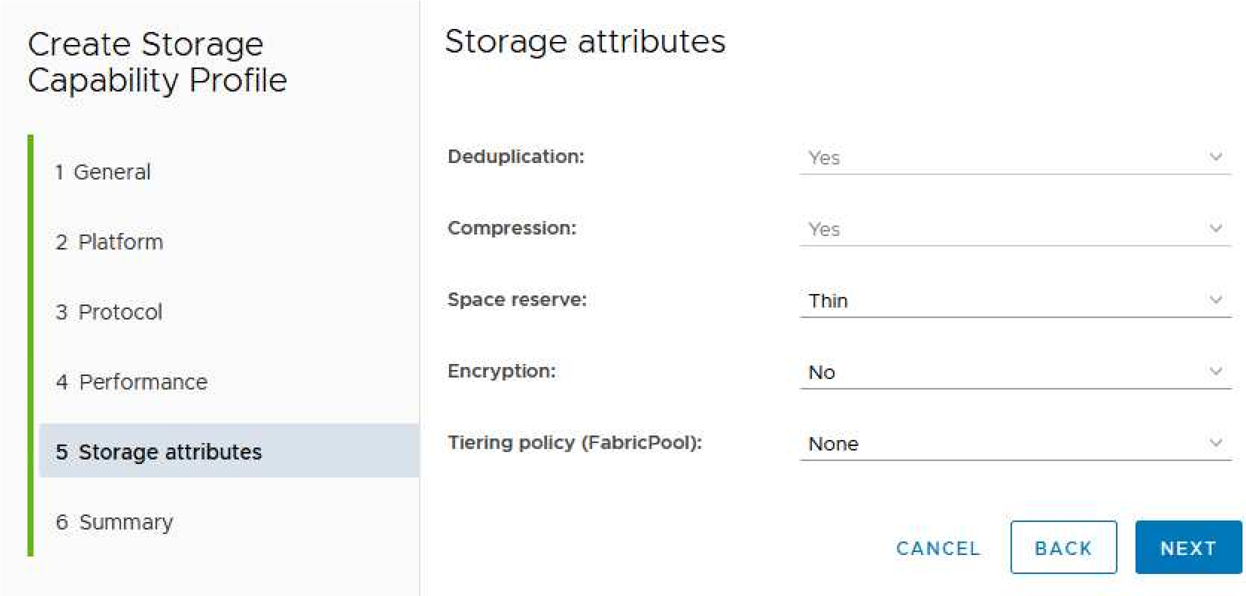
● QoS policy group

Min IOPS:

Max IOPS: 6000

□ Unlimited

6. Complete the **storage attributes** page selecting storage efficiency, space reservation, encryption and any tiering policy as needed.



Storage attributes

Deduplication: Yes

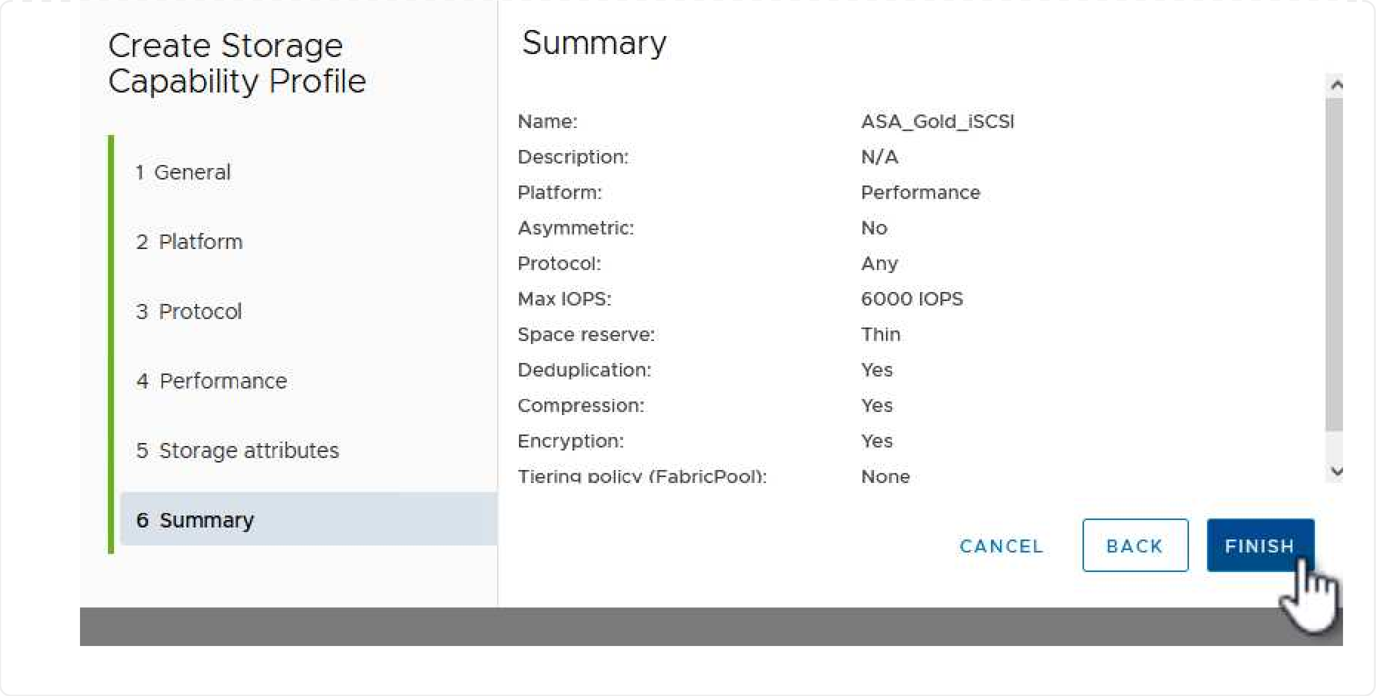
Compression: Yes

Space reserve: Thin

Encryption: No

Tiering policy (FabricPool): None

7. Finally, review the summary and click on Finish to create the profile.



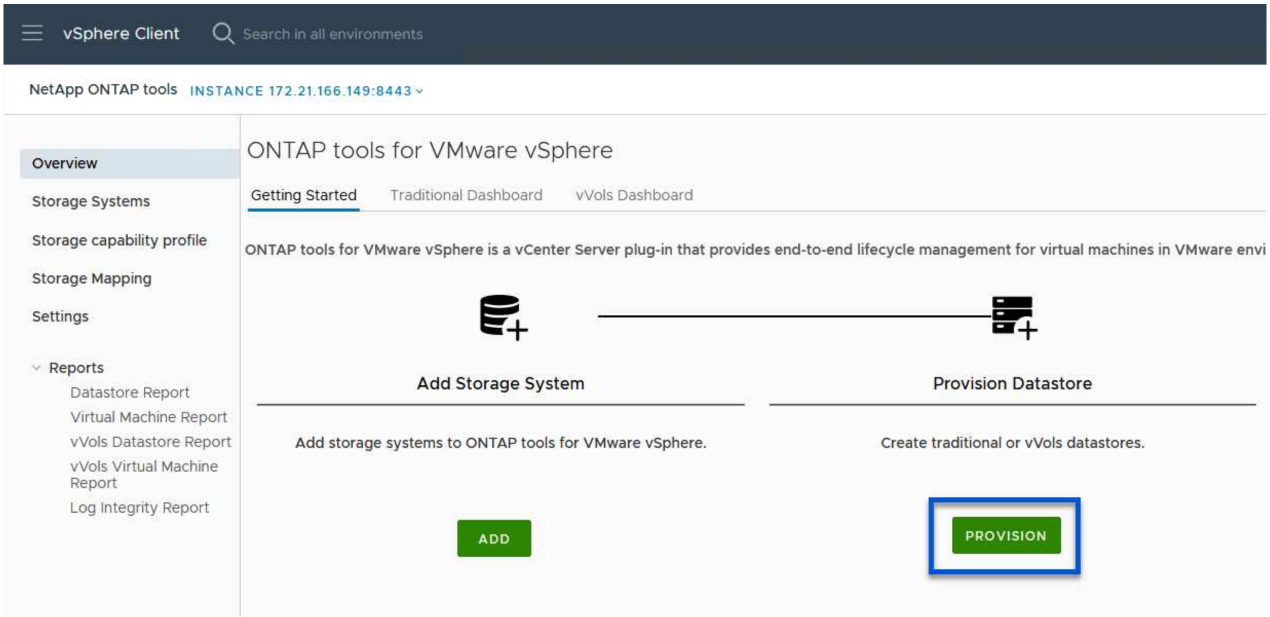
Summary

Name:	ASA_Gold_iSCSI
Description:	N/A
Platform:	Performance
Asymmetric:	No
Protocol:	Any
Max IOPS:	6000 IOPS
Space reserve:	Thin
Deduplication:	Yes
Compression:	Yes
Encryption:	Yes
Tiering policy (FabricPool):	None

Create a vVols datastore in ONTAP Tools

To create a vVols datastore in ONTAP Tools complete the following steps:

1. In ONTAP Tools select **Overview** and from the **Getting Started** tab click on **Provision** to start the wizard.

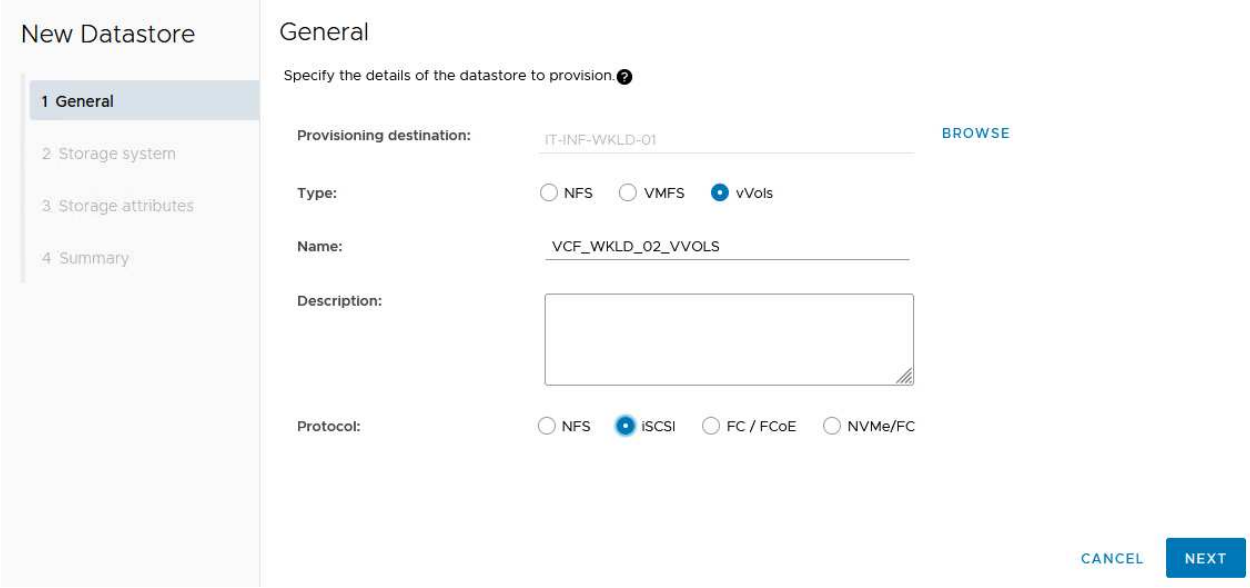


ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware envi

Add storage systems to ONTAP tools for VMware vSphere.

Create traditional or vVols datastores.

2. On the **General** page of the New Datastore wizard select the vSphere datacenter or cluster destination. Select **vVols** as the datastore type, fill out a name for the datastore, and select **iSCSI** as the protocol. Click on **Next** to continue.



Specify the details of the datastore to provision.

Provisioning destination: IT-INF-WKLD-01

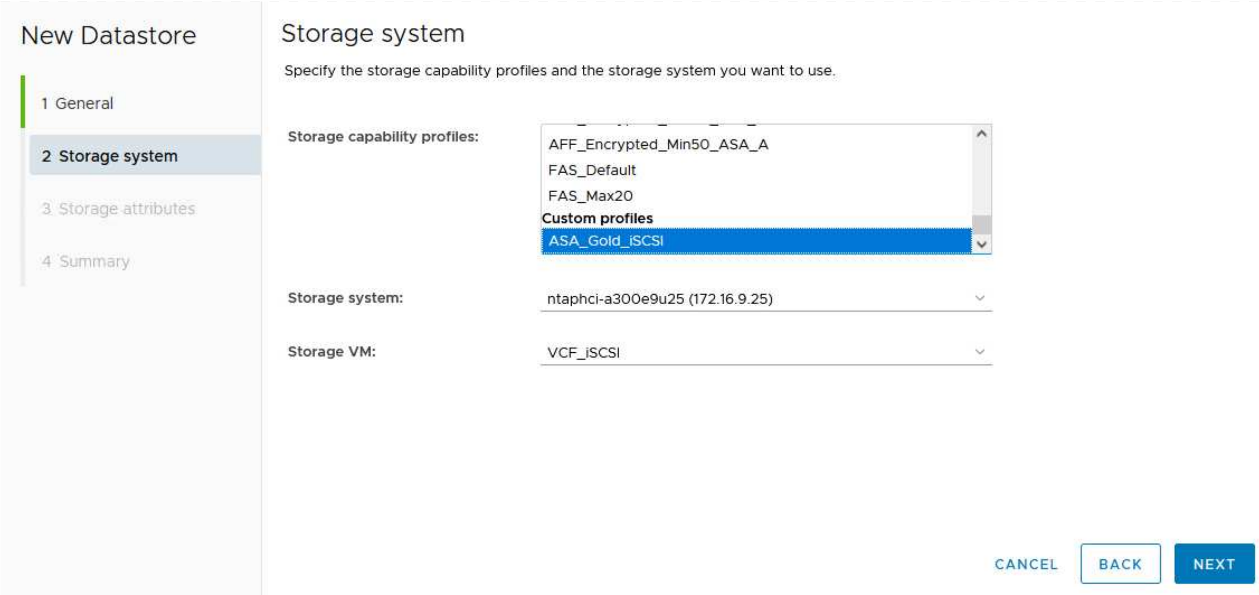
Type: ○ NFS ○ VMFS ● vVols

Name: VCF_WKLD_02_VVOLS

Description:

Protocol: ○ NFS ● iSCSI ○ FC / FCoE ○ NVMe/FC

3. On the **Storage system** page select the select a storage capability profile, the storage system and SVM. Click on **Next** to continue.



New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

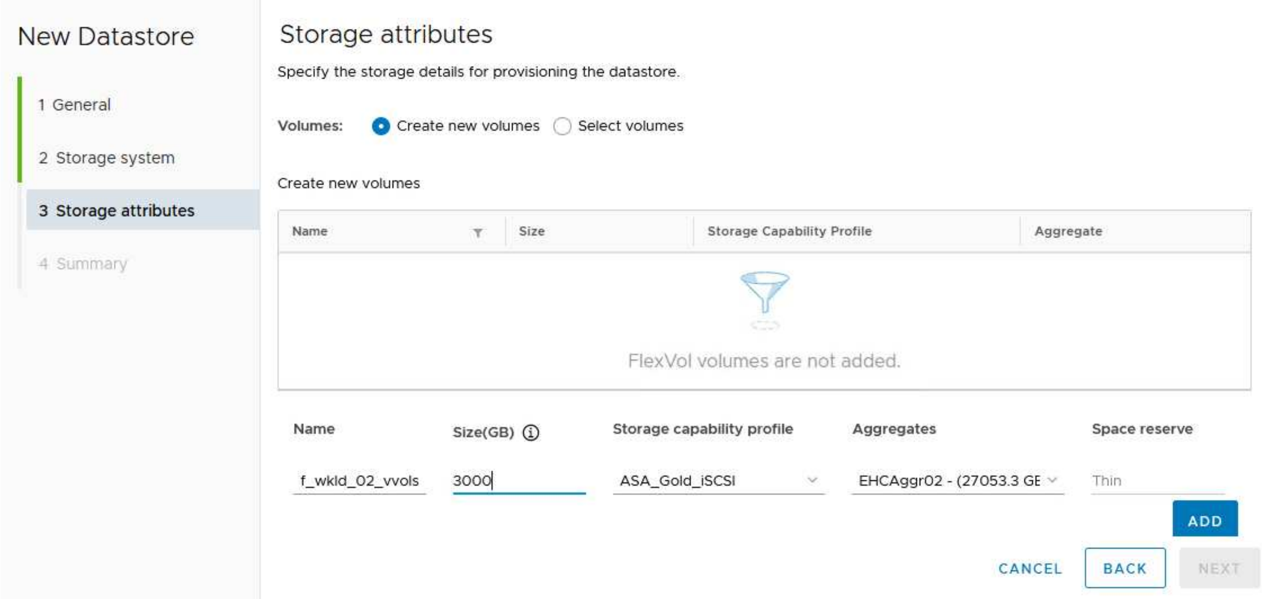
Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles: AFF_Encrypted_Min50_ASA_A, FAS_Default, FAS_Max20, Custom profiles, ASA_Gold_iSCSI (selected)

Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: VCF_iSCSI

4. On the **Storage attributes** page select to create a new volume for the datastore and fill out the storage attributes of the volume to be created. Click on **Add** to create the volume and then **Next** to continue.



New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: ● Create new volumes ○ Select volumes

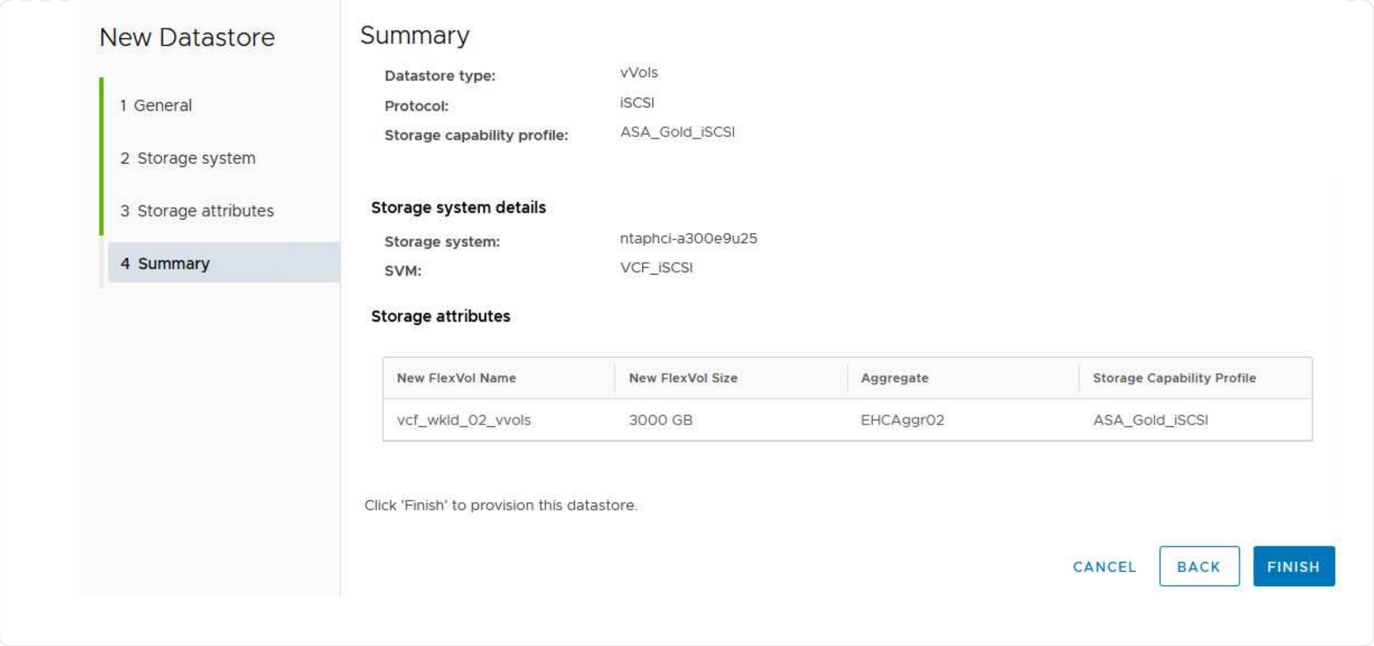
Create new volumes

Name	Size	Storage Capability Profile	Aggregate

FlexVol volumes are not added.

Name	Size(GB)	Storage capability profile	Aggregates	Space reserve
f_wkld_02_vvols	3000	ASA_Gold_iSCSI	EHCAggr02 - (27053.3 GE	Thin

5. Finally, review the summary and click on **Finish** to start the vVol datastore creation process.



Summary

Datastore type: vVols
Protocol: iSCSI
Storage capability profile: ASA_Gold_iSCSI

Storage system details

Storage system: ntaphci-a300e9u25
SVM: VCF_iSCSI

Storage attributes

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile
vcf_wkld_02_vvols	3000 GB	EHCAggr02	ASA_Gold_iSCSI

Click 'Finish' to provision this datastore.

Additional information

For information on configuring ONTAP storage systems refer to the ONTAP 9 Documentation center.

For information on configuring VCF refer to VMware Cloud Foundation Documentation.

Configure NVMe/TCP supplemental storage for VCF Workload Domains

In this scenario we will demonstrate how to configure NVMe/TCP supplemental storage for a VCF workload domain.

Author: Josh Powell

Scenario Overview

This scenario covers the following high level steps:

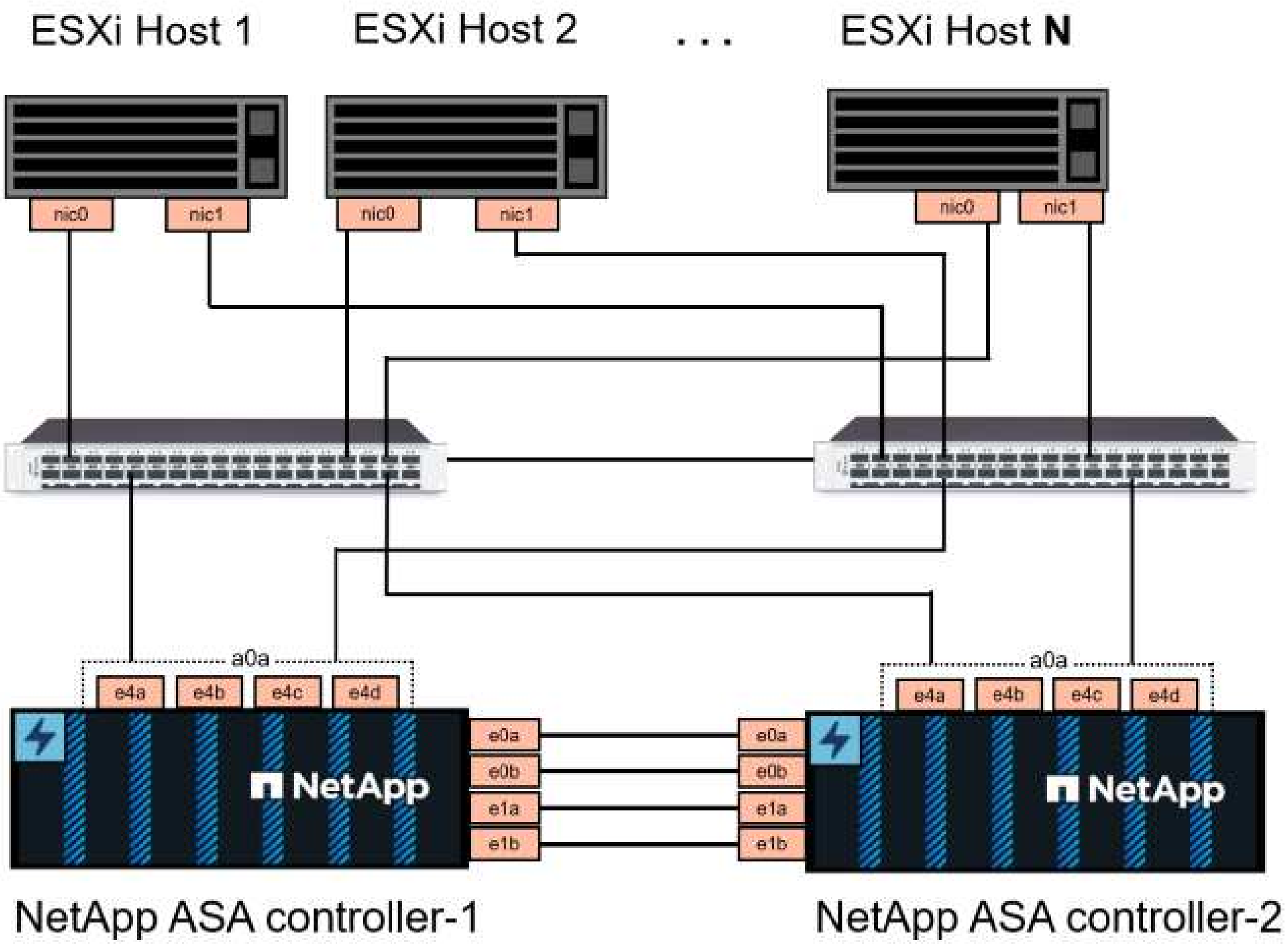
- Create a storage virtual machine (SVM) with logical interfaces (LIFs) for NVMe/TCP traffic.
- Create distributed port groups for iSCSI networks on the VI workload domain.
- Create vmkernel adapters for iSCSI on the ESXi hosts for the VI workload domain.
- Add NVMe/TCP adapters on ESXi hosts.
- Deploy NVMe/TCP datastore.

Prerequisites

This scenario requires the following components and configurations:

- An ONTAP ASA storage system with physical data ports on ethernet switches dedicated to storage traffic.
- VCF management domain deployment is complete and the vSphere client is accessible.
- A VI workload domain has been previously deployed.

NetApp recommends fully redundant network designs for NVMe/TCP. The following diagram illustrates an example of a redundant configuration, providing fault tolerance for storage systems, switches, networks adapters and host systems. Refer to the NetApp SAN configuration reference for additional information.



For multipathing and failover across multiple paths, NetApp recommends having a minimum of two LIFs per storage node in separate ethernet networks for all SVMs in NVMe/TCP configurations.

This documentation demonstrates the process of creating a new SVM and specifying the IP address information to create multiple LIFs for NVMe/TCP traffic. To add new LIFs to an existing SVM refer to Create a LIF (network interface).

For additional information on NVMe design considerations for ONTAP storage systems, refer to NVMe configuration, support and limitations.

Deployment Steps

To create a VMFS datastore on a VCF workload domain using NVMe/TCP, complete the following steps.

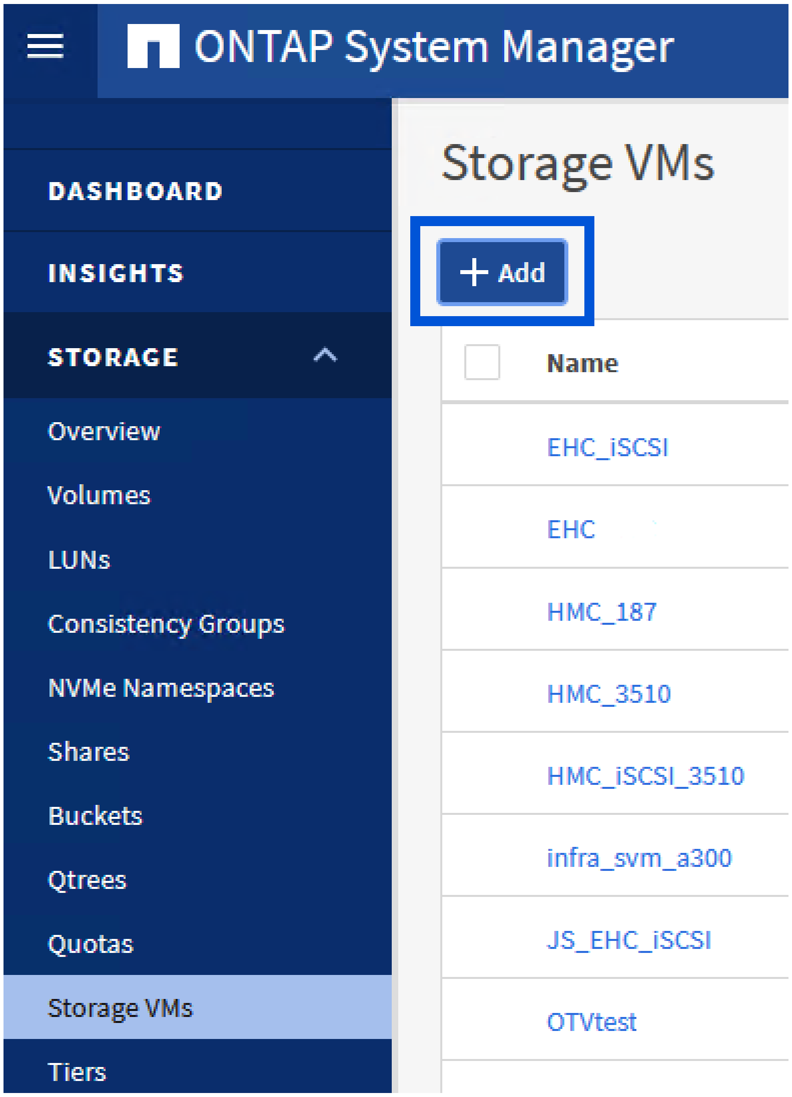
Create SVM, LIFs and NVMe Namespace on ONTAP storage system

The following step is performed in ONTAP System Manager.

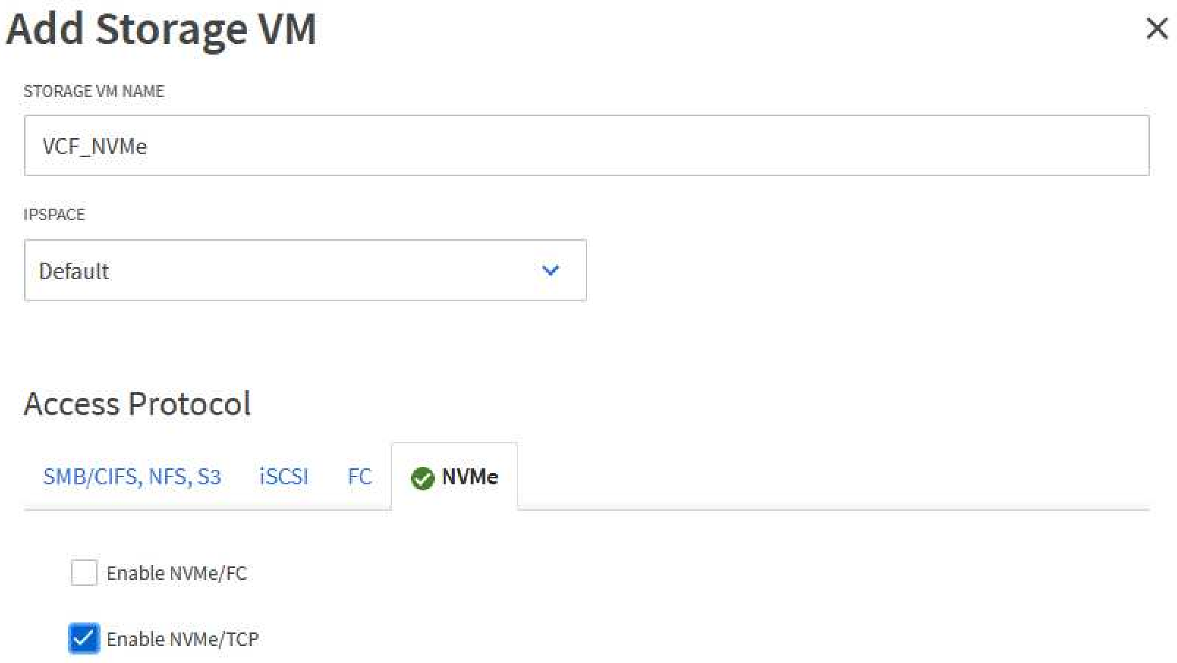
Create the storage VM and LIFs

Complete the following steps to create an SVM together with multiple LIFs for NVMe/TCP traffic.

1. From ONTAP System Manager navigate to **Storage VMs** in the left-hand menu and click on **+ Add** to start.



2. In the **Add Storage VM** wizard provide a **Name** for the SVM, select the **IP Space** and then, under **Access Protocol**, click on the **NVMe** tab and check the box to **Enable NVMe/TCP**.



Add Storage VM

STORAGE VM NAME

VCF_NVMe

IPSPACE

Default

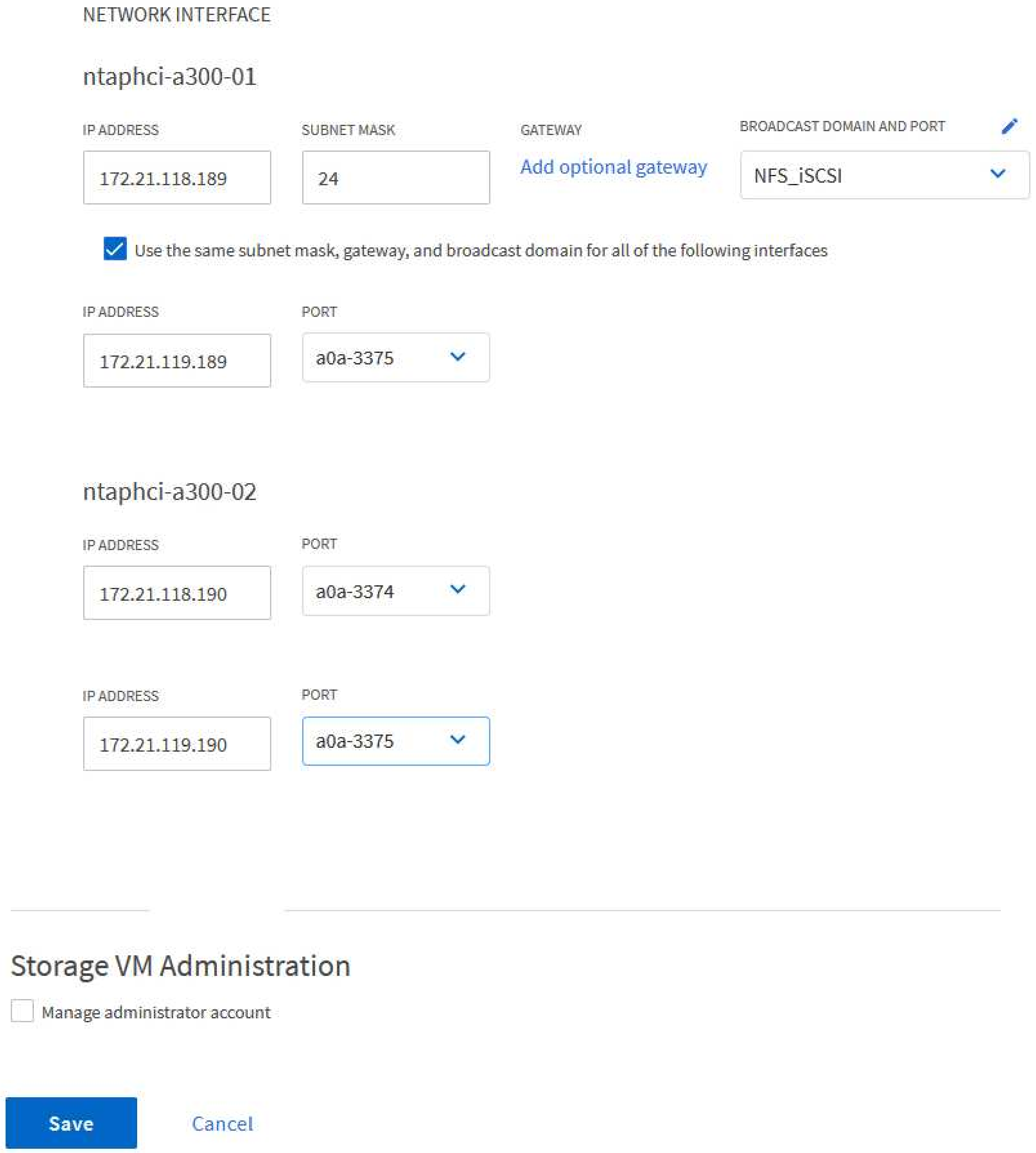
Access Protocol

☐ Enable NVMe/FC

☑ Enable NVMe/TCP

3. In the **Network Interface** section fill in the **IP address**, **Subnet Mask**, and **Broadcast Domain and Port** for the first LIF. For subsequent LIFs the checkbox may be enabled to use common settings across all remaining LIFs, or use separate settings.

> For multipathing and failover across multiple paths, NetApp recommends having a minimum of two LIFs per storage node in separate Ethernet networks for all SVMs in NVMe/TCP configurations.


NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS	SUBNET MASK	GATEWAY	BROADCAST DOMAIN AND PORT
172.21.118.189	24	Add optional gateway	NFS_iSCSI

☑ Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS	PORT
172.21.119.189	a0a-3375

ntaphci-a300-02

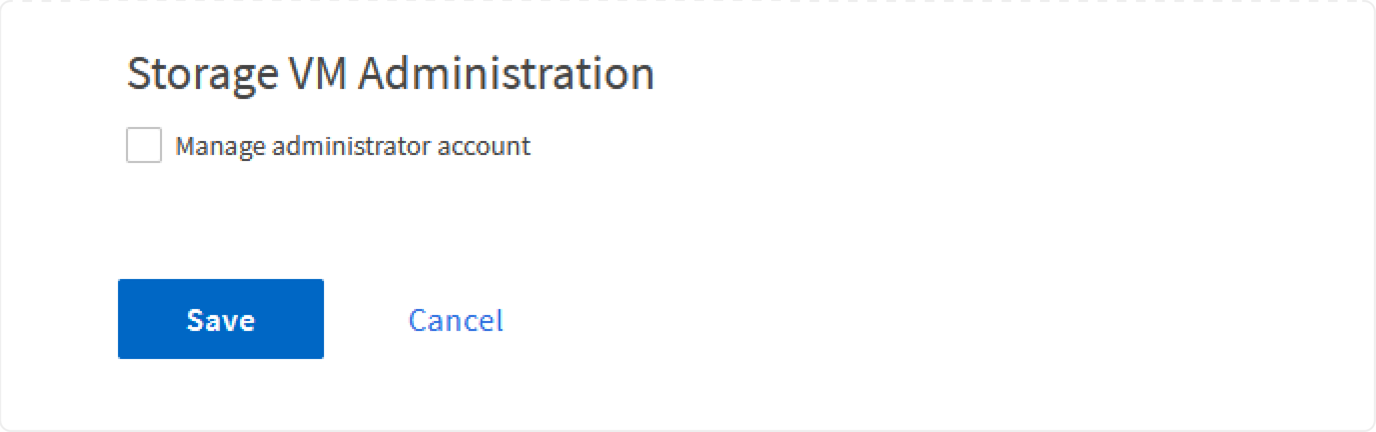
IP ADDRESS	PORT
172.21.118.190	a0a-3374

IP ADDRESS	PORT
172.21.119.190	a0a-3375

Storage VM Administration

☐ Manage administrator account

4. Choose whether to enable the Storage VM Administration account (for multi-tenancy environments) and click on **Save** to create the SVM.



Storage VM Administration

☐ Manage administrator account

Create the NVMe Namespace

NVMe namespaces are analogous to LUNs for iSCSi or FC. The NVMe Namespace must be created before a VMFS datastore can be deployed from the vSphere Client. To create the NVMe namespace, the NVMe Qualified Name (NQN) must first be obtained from each ESXi host in the cluster. The NQN is used by ONTAP to provide access control for the namespace.

Complete the following steps to create an NVMe Namespace:

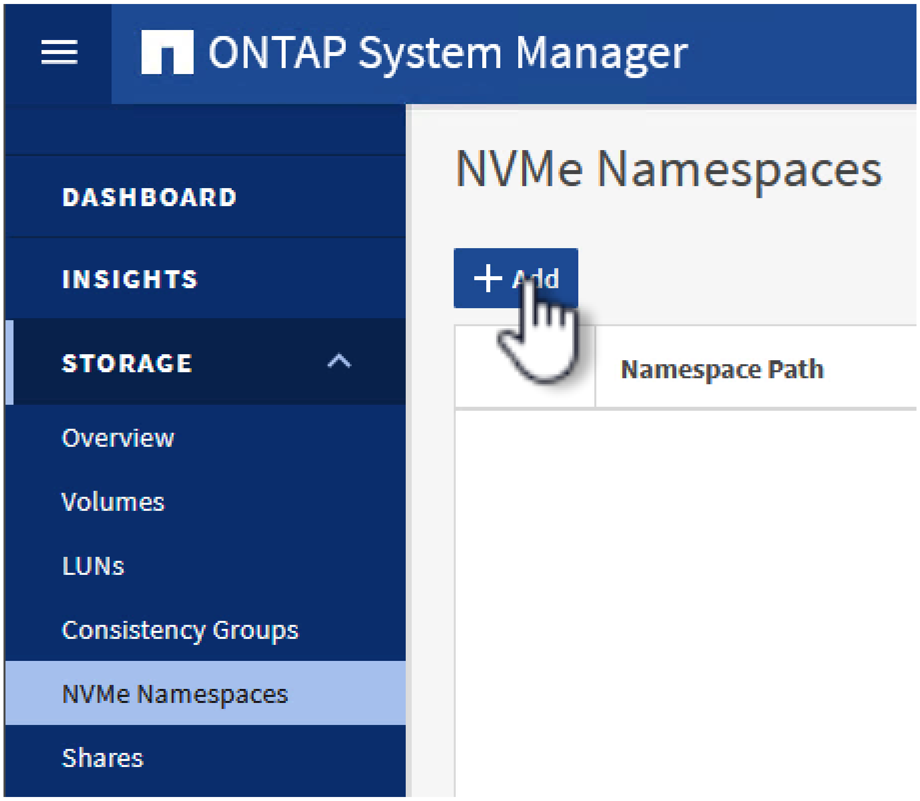
1. Open an SSH session with an ESXi host in the cluster to obtain its NQN. Use the following command from the CLI:

   ```
   esxcli nvme info get
   ```

   An output similar to the following should be displayed:

   ```
   Host NQN: nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-esx01
   ```

2. Record the NQN for each ESXi host in the cluster
3. From ONTAP System Manager navigate to **NVMe Namespaces** in the left-hand menu and click on **+ Add** to start.

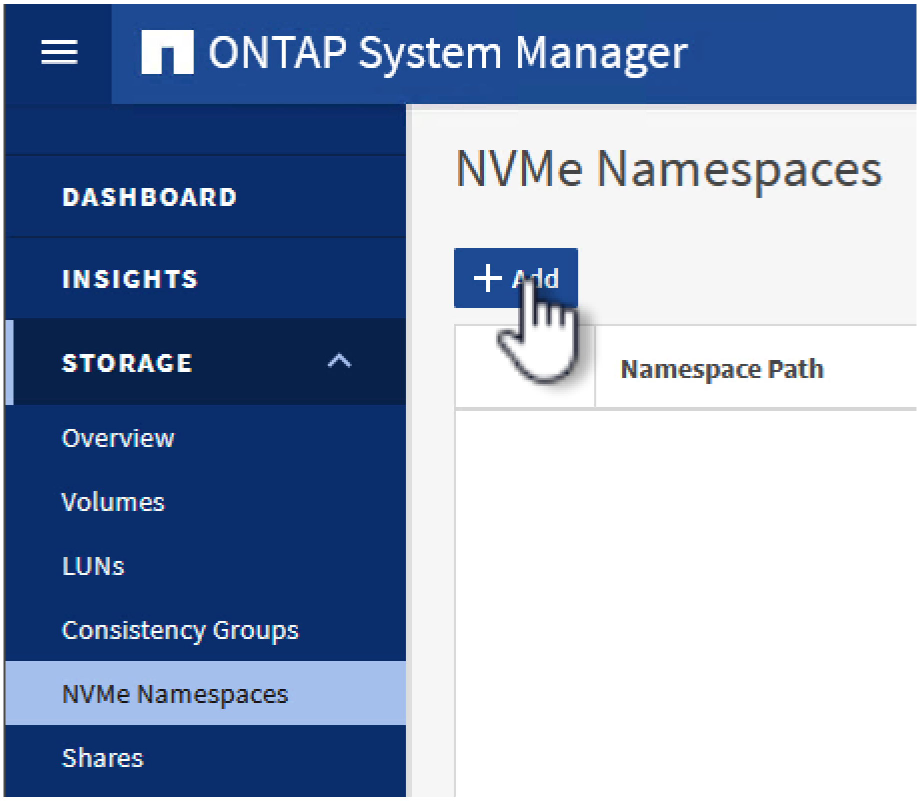


4. On the **Add NVMe Namespace** page, fill in a name prefix, the number of namespaces to create, the size of the namespace, and the host operating system that will be accessing the namespace. In the

Host NQN section create a comma separated list of the NQN's previously collected from the ESXi hosts that will be accessing the namespaces.

Click on **More Options** to configure additional items such as the snapshot protection policy. Finally, click on **Save** to create the NVMe Namespace.

+



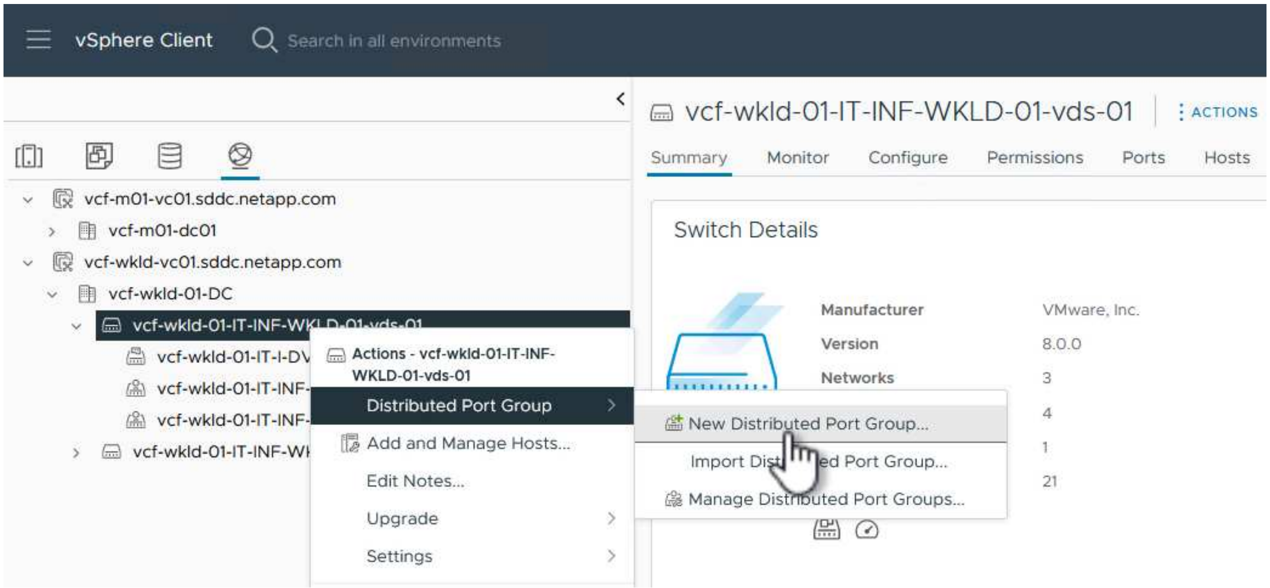
Set up networking and NVMe software adapters on ESXi hosts

The following steps are performed on the VI workload domain cluster using the vSphere client. In this case vCenter Single Sign-On is being used so the vSphere client is common to both the management and workload domains.

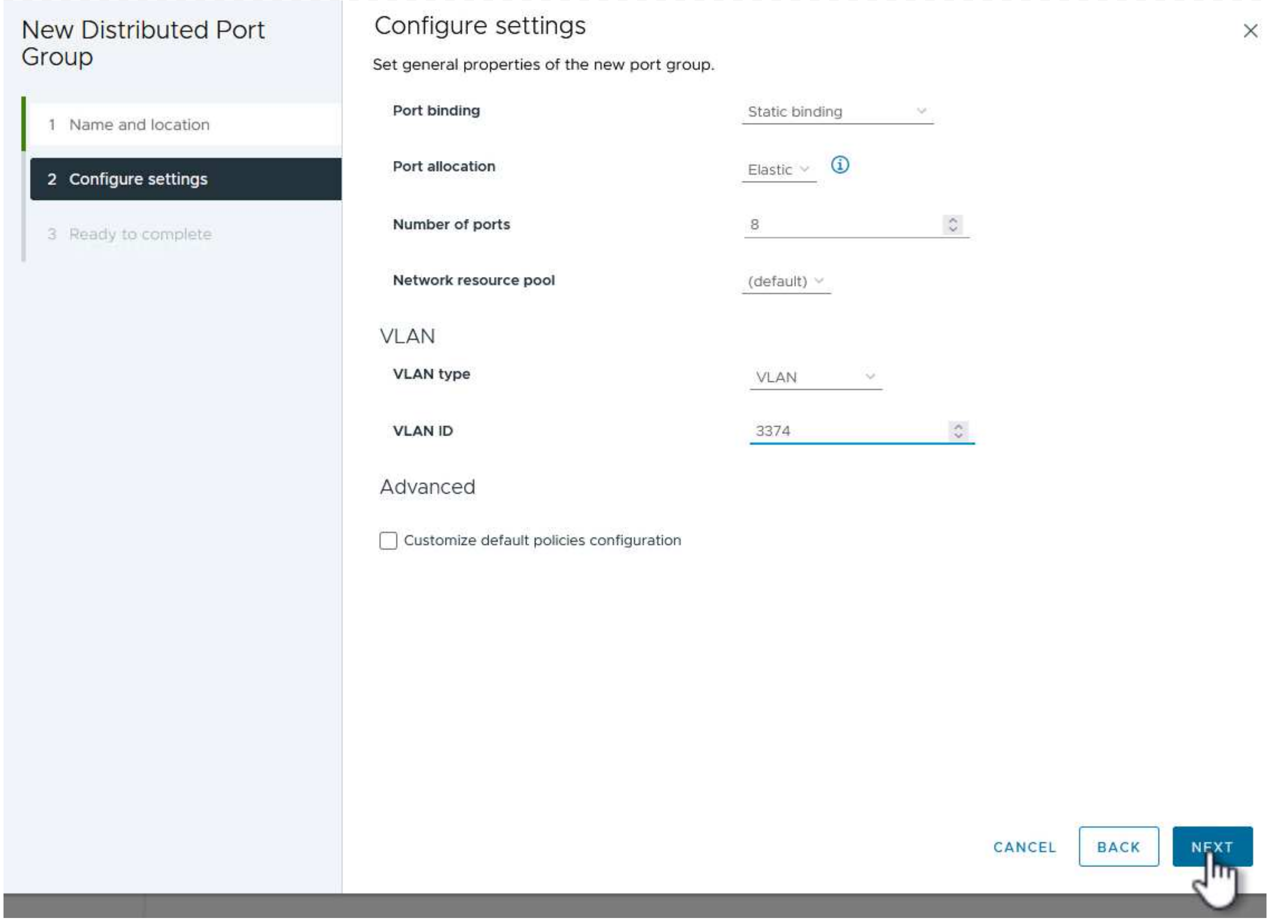
Create Distributed Port Groups for NVME/TCP traffic

Complete the following to create a new distributed port group for each NVMe/TCP network:

1. From the vSphere client , navigate to **Inventory > Networking** for the workload domain. Navigate to the existing Distributed Switch and choose the action to create **New Distributed Port Group…**.



2. In the **New Distributed Port Group** wizard fill in a name for the new port group and click on **Next** to continue.
3. On the **Configure settings** page fill out all settings. If VLANs are being used be sure to provide the correct VLAN ID. Click on **Next** to continue.



New Distributed Port Group

1 Name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding	Static binding
Port allocation	Elastic
Number of ports	8
Network resource pool	(default)

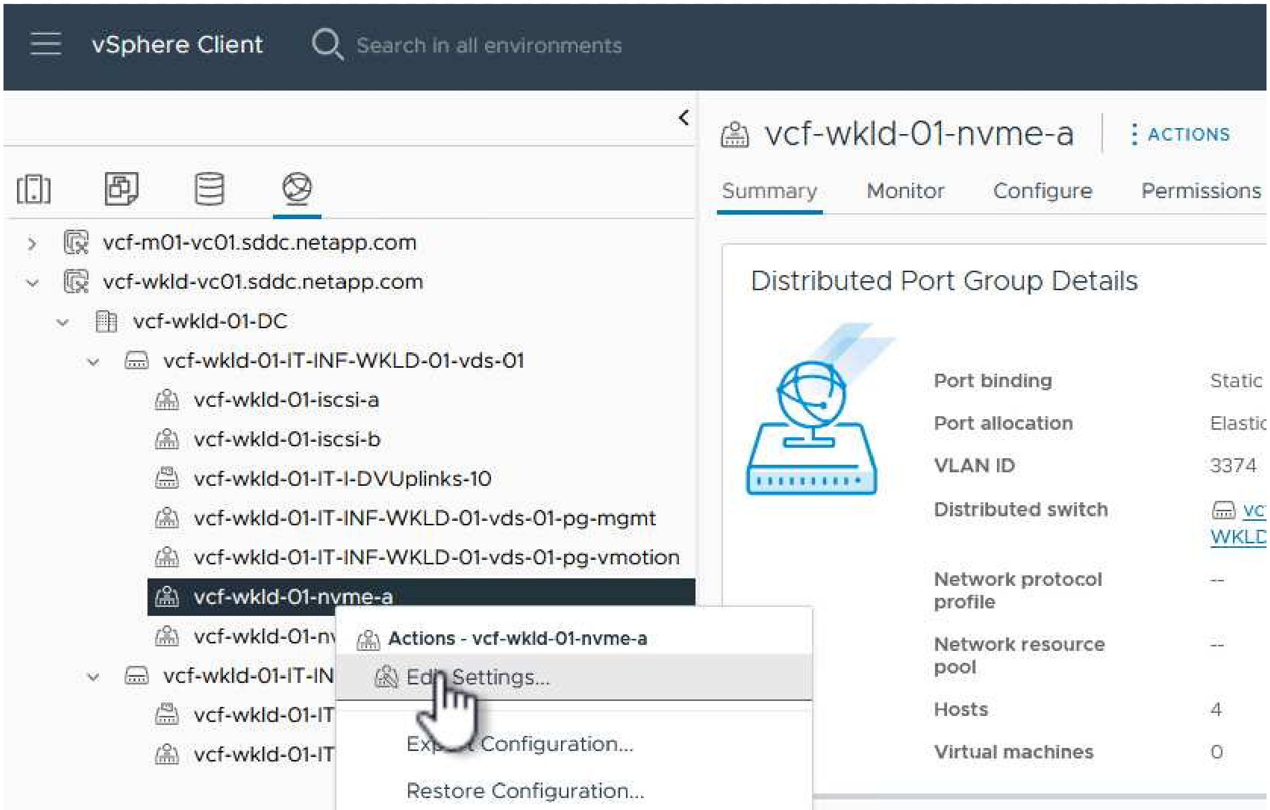
VLAN

VLAN type	VLAN
VLAN ID	3374

Advanced

□ Customize default policies configuration

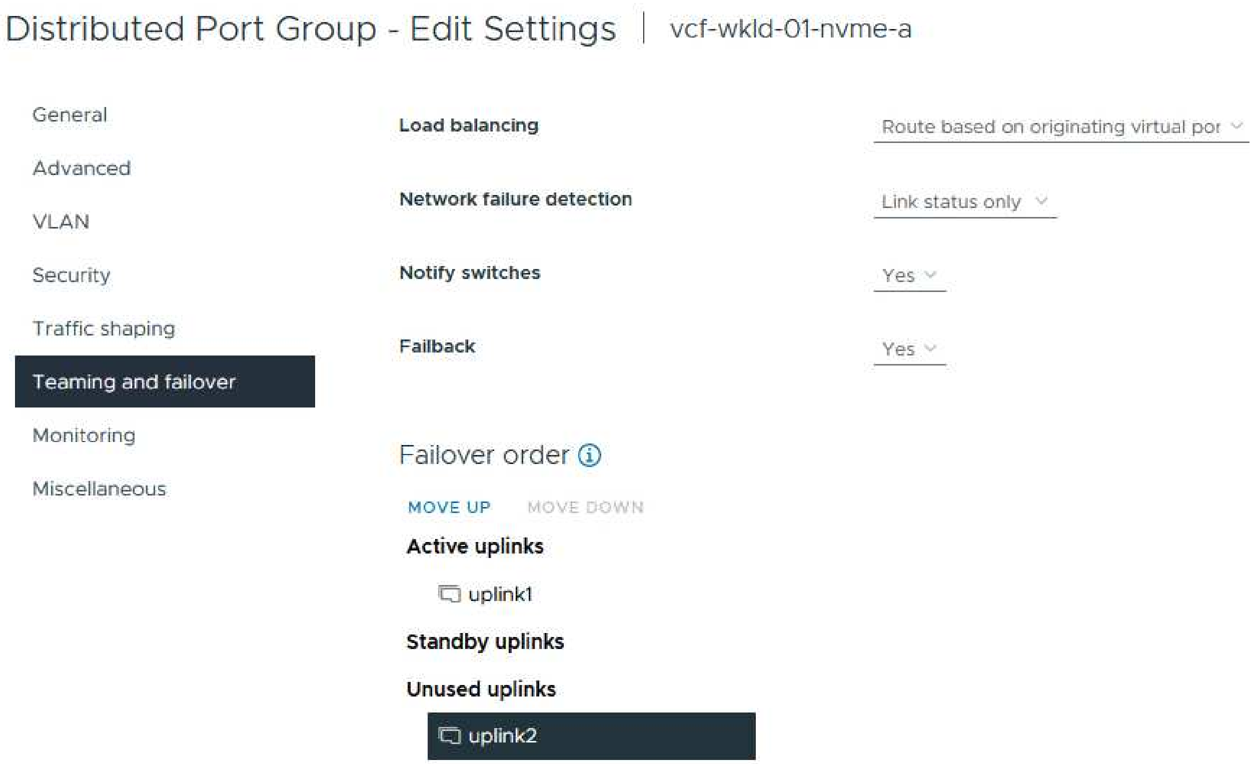
4. On the **Ready to complete** page, review the changes and click on **Finish** to create the new distributed port group.
5. Repeat this process to create a distributed port group for the second NVMe/TCP network being used and ensure you have input the correct **VLAN ID**.
6. Once both port groups have been created, navigate to the first port group and select the action to **Edit settings…**.



Distributed Port Group Details

Port binding: Static
Port allocation: Elastic
VLAN ID: 3374
Distributed switch: vc WKLD
Network protocol profile: --
Network resource pool: --
Hosts: 4
Virtual machines: 0

7. On **Distributed Port Group - Edit Settings** page, navigate to **Teaming and failover** in the left-hand menu and click on **uplink2** to move it down to **Unused uplinks**.


Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-a

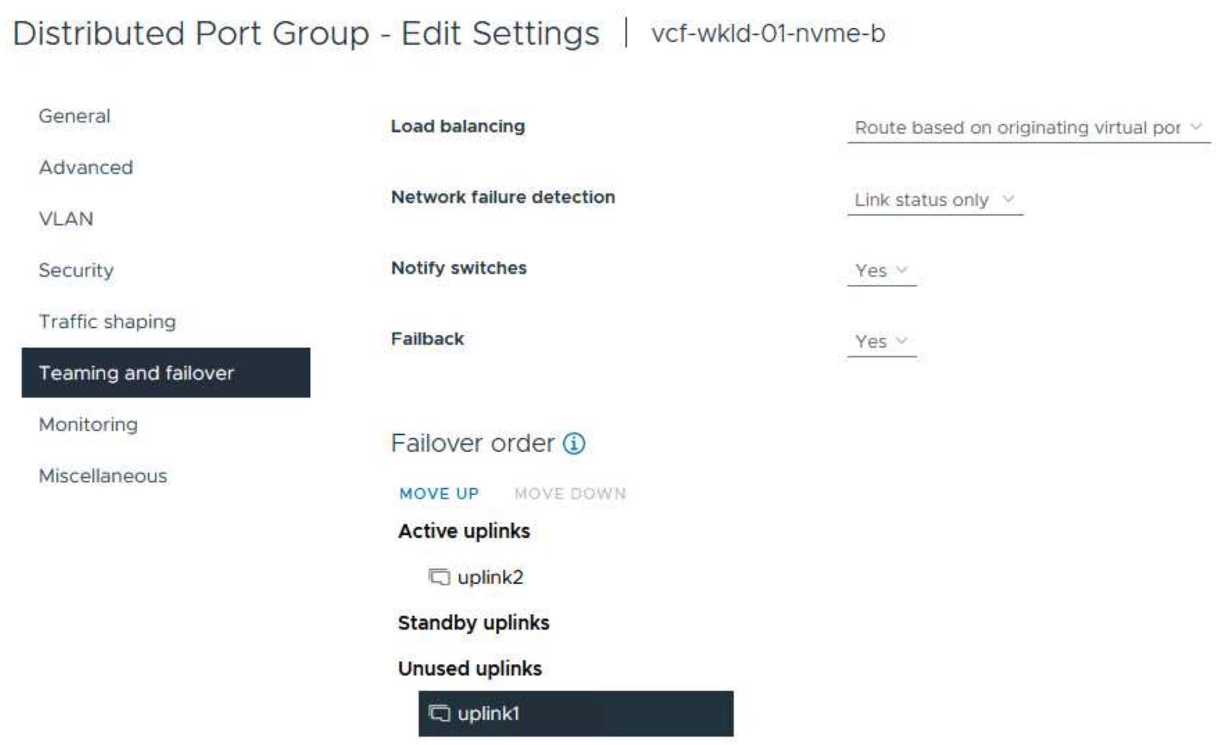
Load balancing: Route based on originating virtual por
Network failure detection: Link status only
Notify switches: Yes
Failback: Yes

Failover order

Active uplinks
uplink1
Standby uplinks
Unused uplinks
uplink2

8. Repeat this step for the second NVMe/TCP port group. However, this time move **uplink1** down to

Unused uplinks.



Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-b

Load balancing: Route based on originating virtual por

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

Failover order

Active uplinks

uplink2

Standby uplinks

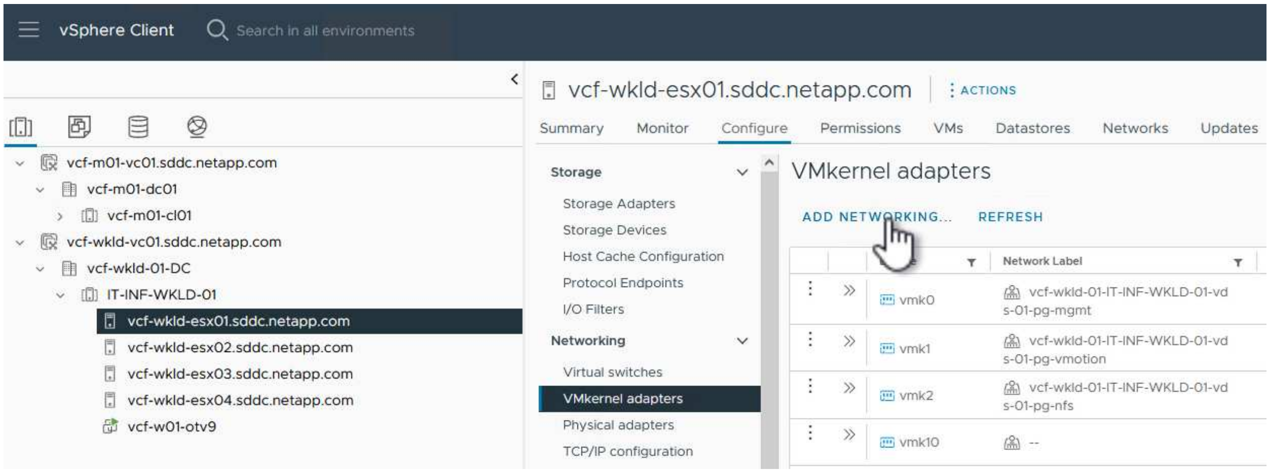
Unused uplinks

uplink1

Create VMkernel adapters on each ESXi host

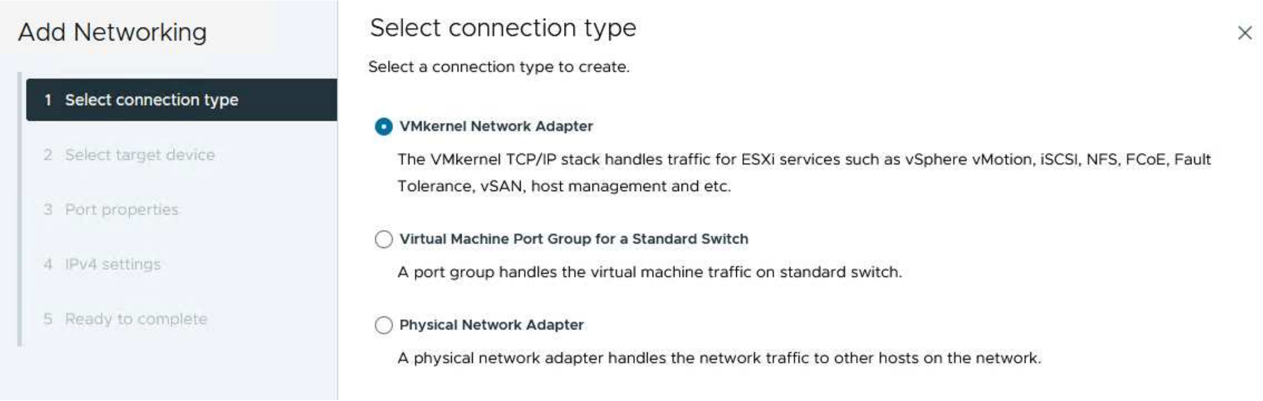
Repeat this process on each ESXi host in the workload domain.

1. From the vSphere client navigate to one of the ESXi hosts in the workload domain inventory. From the **Configure** tab select **VMkernel adapters** and click on **Add Networking…** to start.



	Network Label
vmk0	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt
vmk1	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion
vmk2	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs
vmk10	--

2. On the **Select connection type** window choose **VMkernel Network Adapter** and click on **Next** to continue.



Select a connection type to create.

● VMkernel Network Adapter

The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.

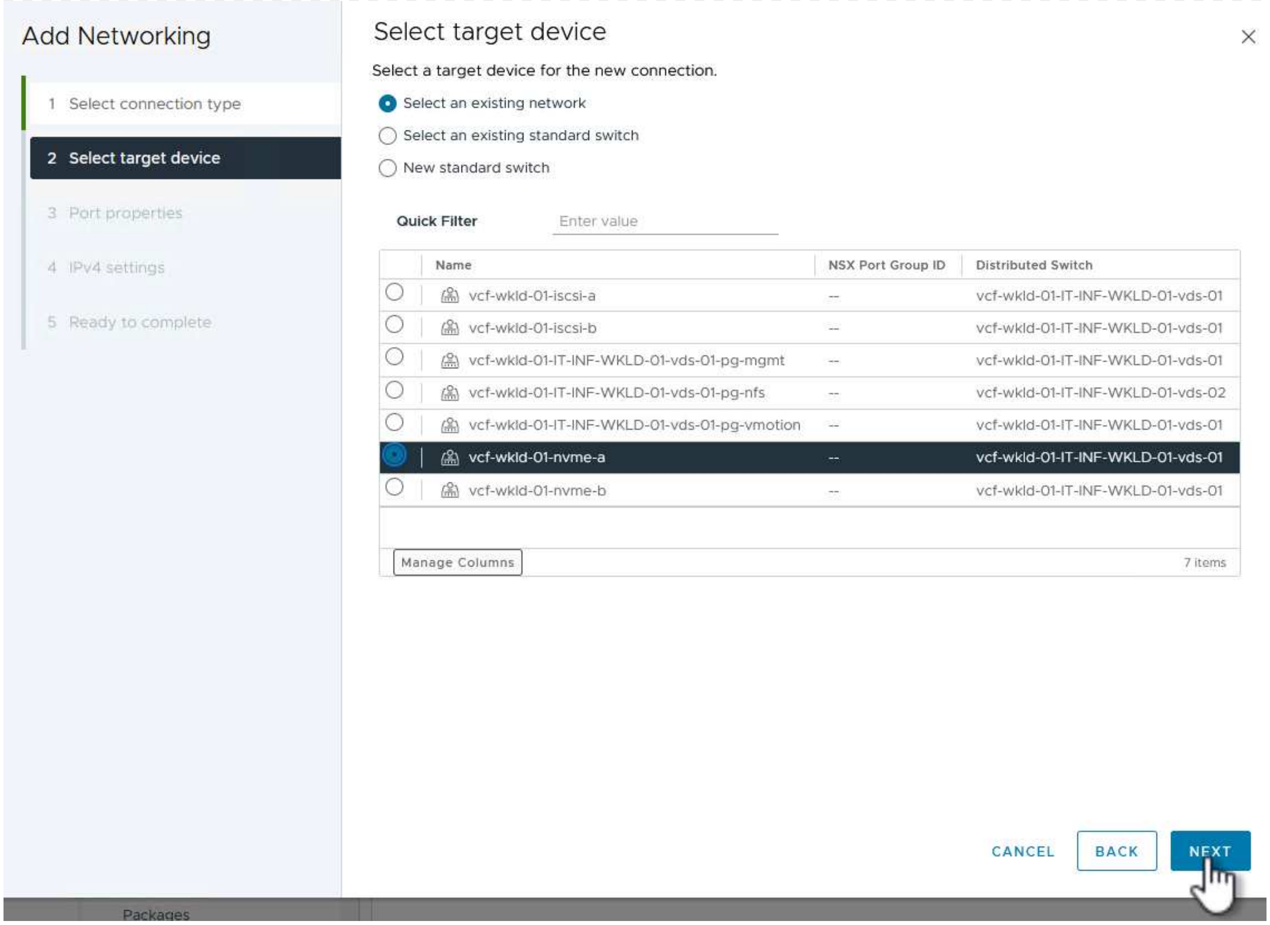
○ Virtual Machine Port Group for a Standard Switch

A port group handles the virtual machine traffic on standard switch.

○ Physical Network Adapter

A physical network adapter handles the network traffic to other hosts on the network.

3. On the **Select target device** page, choose one of the distributed port groups for iSCSI that was created previously.



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

● Select an existing network

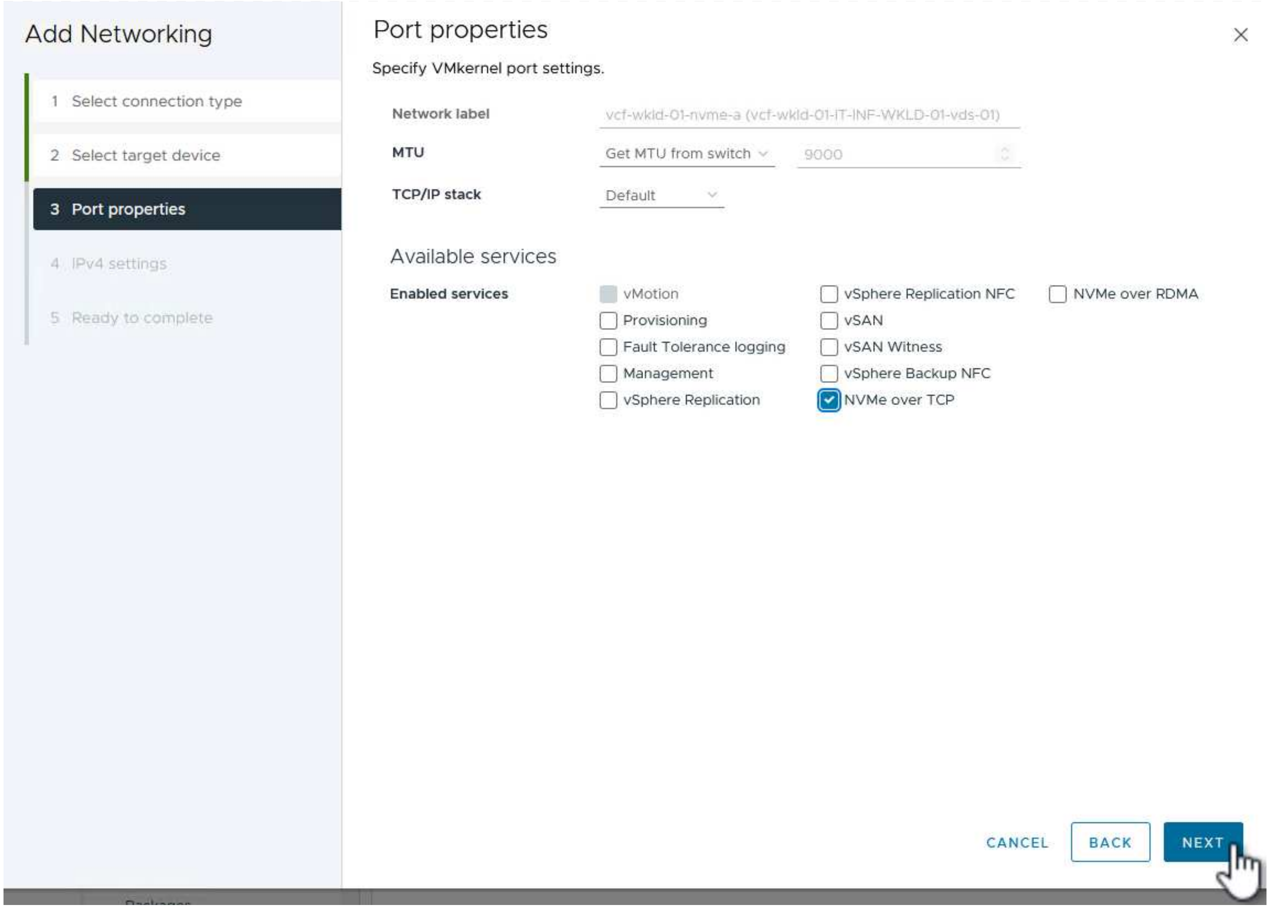
○ Select an existing standard switch

○ New standard switch

Quick Filter: Enter value

	Name	NSX Port Group ID	Distributed Switch
○	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
●	vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

4. On the **Port properties** page click the box for **NVMe over TCP** and click on **Next** to continue.



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Port properties

Specify VMkernel port settings.

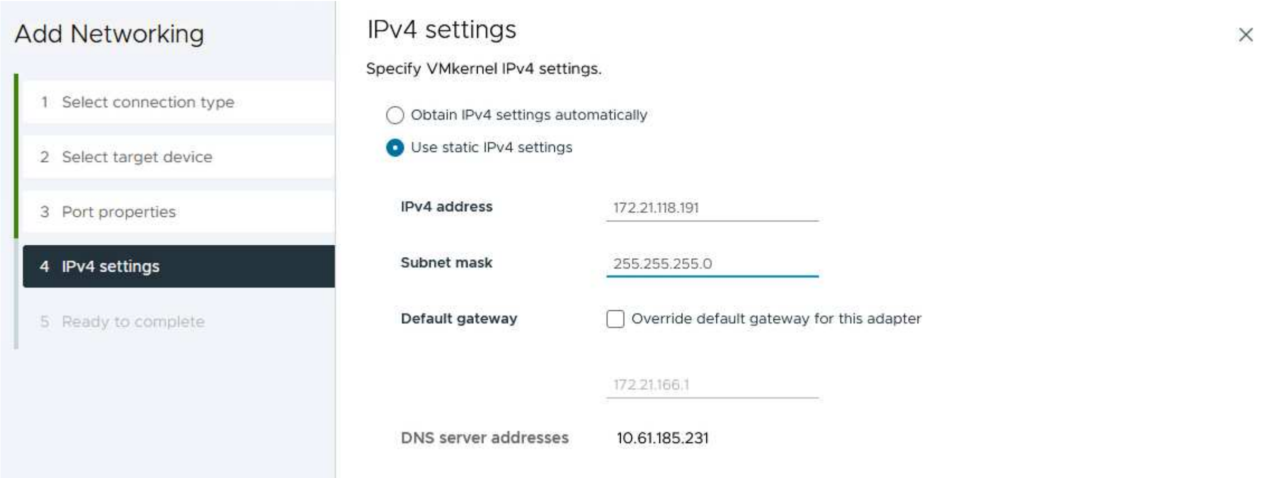
Network label	vcf-wkld-01-nvme-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)	
MTU	Get MTU from switch	9000
TCP/IP stack	Default	

Available services

Enabled services

□ vMotion	□ vSphere Replication NFC	□ NVMe over RDMA
□ Provisioning	□ vSAN	
□ Fault Tolerance logging	□ vSAN Witness	
□ Management	□ vSphere Backup NFC	
□ vSphere Replication	☑ NVMe over TCP	

5. On the **IPv4 settings** page fill in the **IP address**, **Subnet mask**, and provide a new Gateway IP address (only if required). Click on **Next** to continue.



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

IPv4 settings

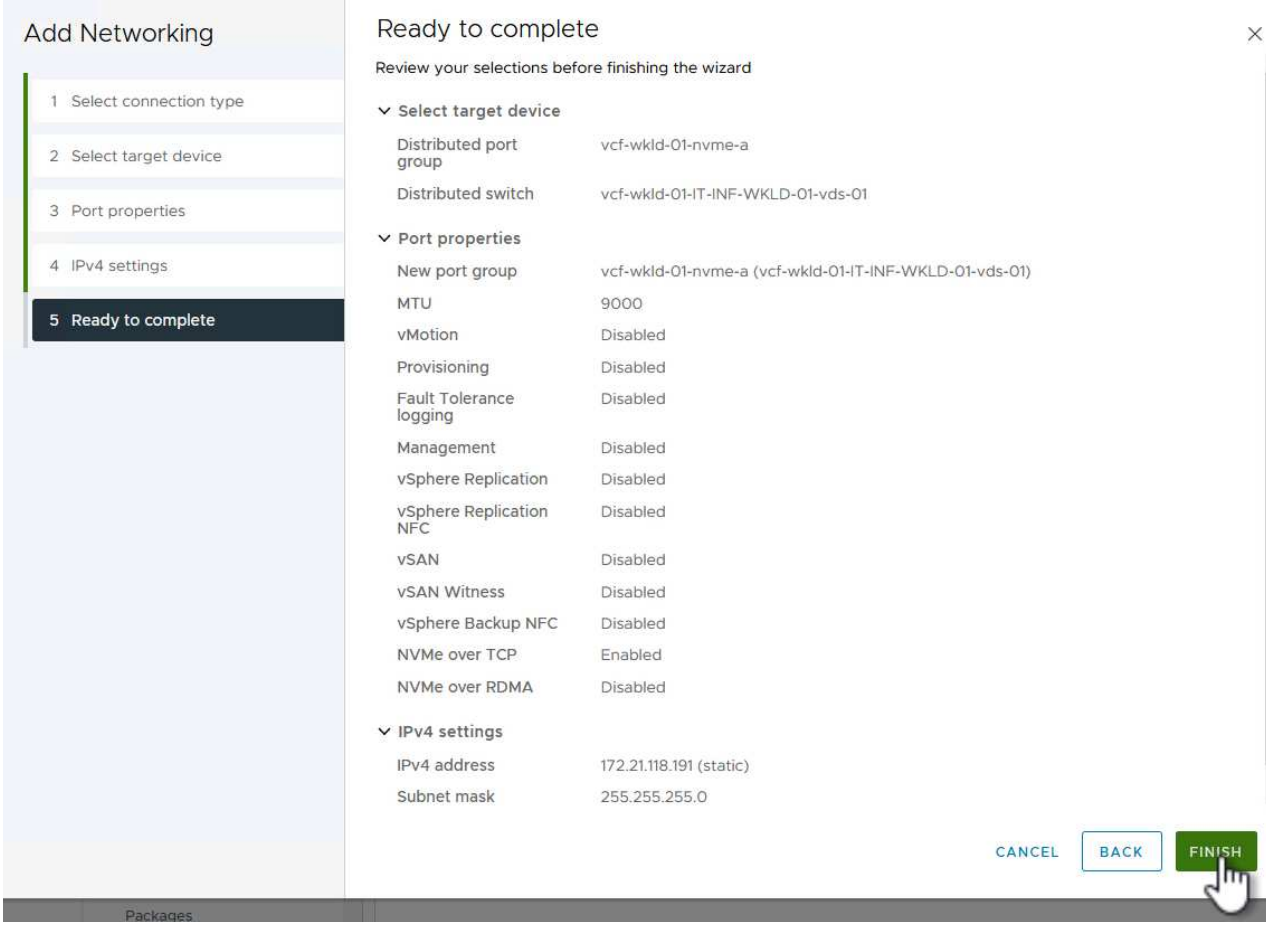
Specify VMkernel IPv4 settings.

○ Obtain IPv4 settings automatically

● Use static IPv4 settings

IPv4 address	172.21.118.191
Subnet mask	255.255.255.0
Default gateway	□ Override default gateway for this adapter
	172.21.166.1
DNS server addresses	10.61.185.231

6. Review the your selections on the **Ready to complete** page and click on **Finish** to create the VMkernel adapter.



Add Networking

Ready to complete

Review your selections before finishing the wizard

Select target device

Distributed port group	vcf-wkld-01-nvme-a
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Port properties

New port group	vcf-wkld-01-nvme-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Enabled
NVMe over RDMA	Disabled

IPv4 settings

IPv4 address	172.21.118.191 (static)
Subnet mask	255.255.255.0

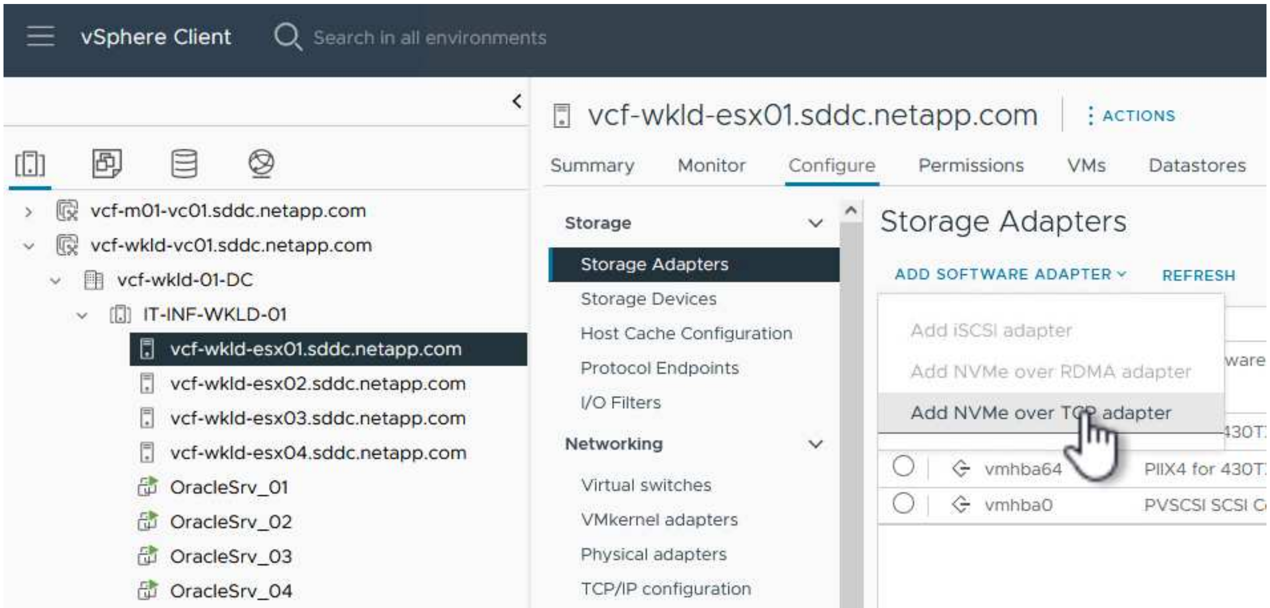
7. Repeat this process to create a VMkernel adapter for the second iSCSI network.

Add NVMe over TCP adapter

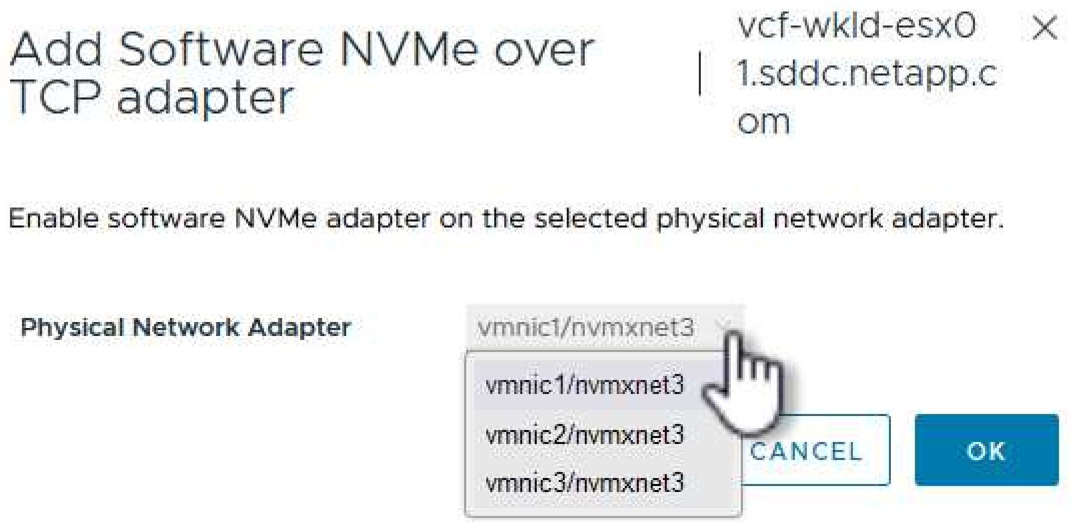
Each ESXi host in the workload domain cluster must have an NVMe over TCP software adapter installed for every established NVMe/TCP network dedicated to storage traffic.

To install NVMe over TCP adapters and discover the NVMe controllers, complete the following steps:

1. In the vSphere client navigate to one of the ESXi hosts in the workload domain cluster. From the **Configure** tab click on **Storage Adapters** in the menu and then, from the **Add Software Adapter** drop-down menu, select **Add NVMe over TCP adapter**.



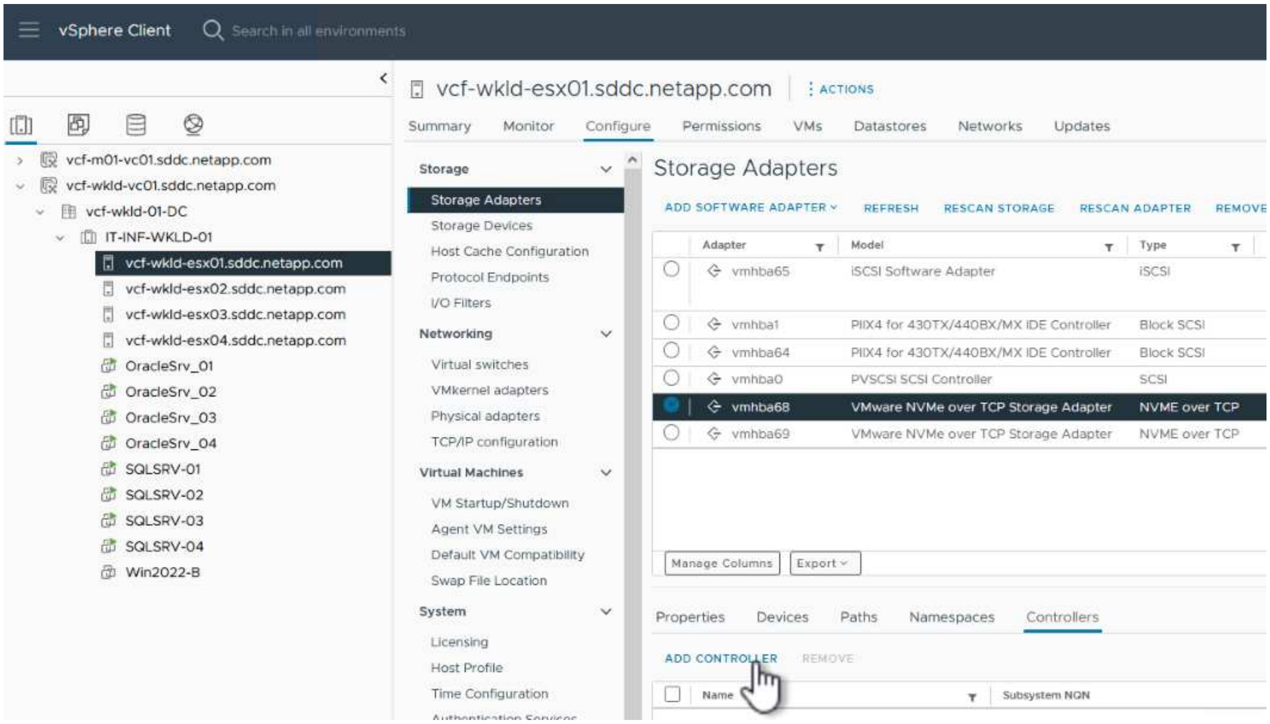
2. In the **Add Software NVMe over TCP adapter** window, access the **Physical Network Adapter** drop-down menu and select the correct physical network adapter on which to enable the NVMe adapter.


Add Software NVMe over TCP adapter | vcf-wkld-esx01.sddc.netapp.com

Enable software NVMe adapter on the selected physical network adapter.

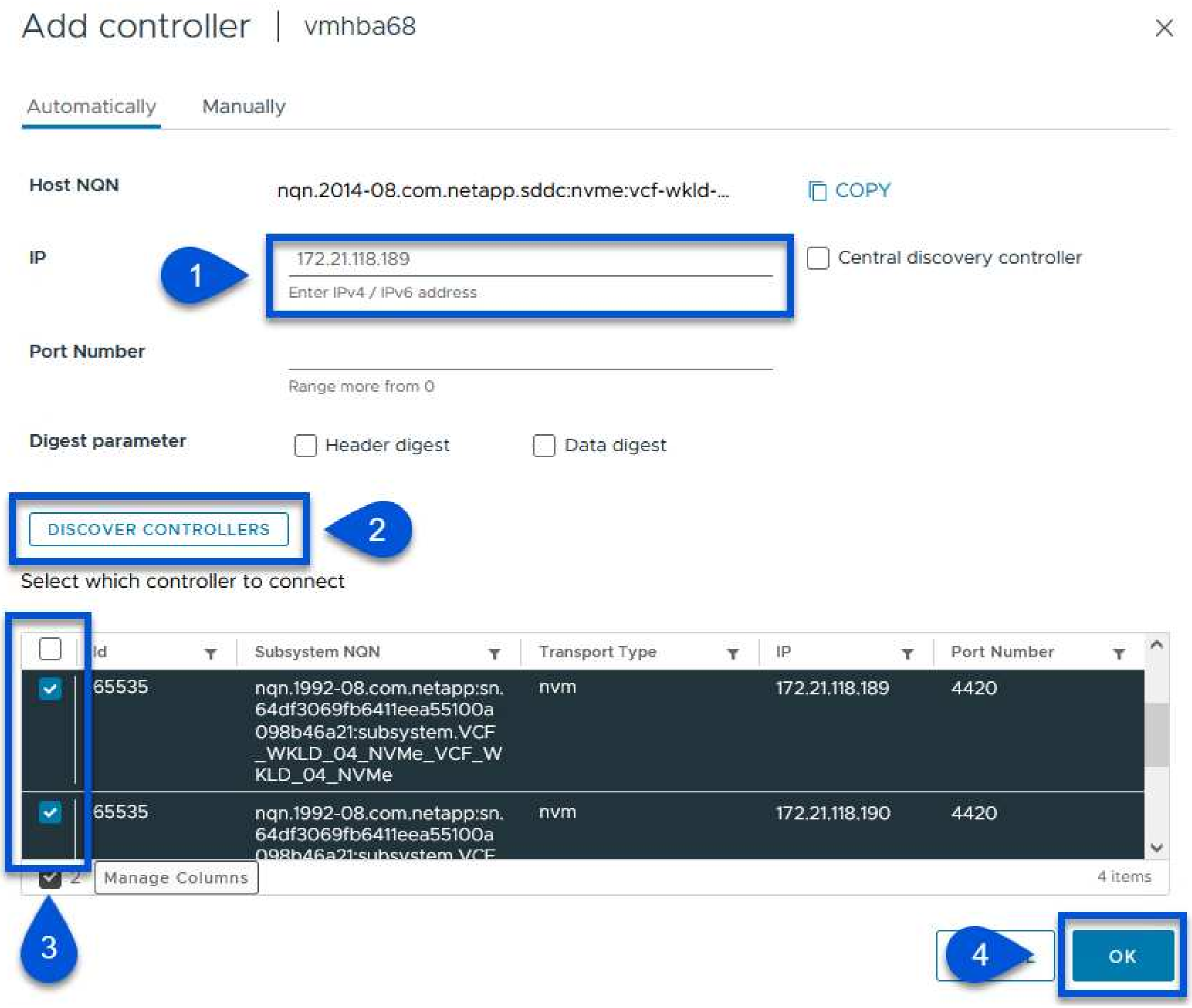
Physical Network Adapter: vmnic1/nvmxnet3

3. Repeat this process for the second network assigned to NVMe over TCP traffic, assigning the correct physical adapter.
4. Select one of the newly installed NVMe over TCP adapters and, on the **Controllers** tab, select **Add Controller**.



	Adapter	Model	Type
○	vmhba65	iSCSI Software Adapter	iSCSI
○	vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI
○	vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI
○	vmhba0	PVSCSI SCSI Controller	SCSI
●	vmhba68	VMware NVMe over TCP Storage Adapter	NVME over TCP
○	vmhba69	VMware NVMe over TCP Storage Adapter	NVME over TCP

5. In the **Add controller** window, select the **Automatically** tab and complete the following steps.
   - Fill in an IP addresses for one of the SVM logical interfaces on the same network as the physical adapter assigned to this NVMe over TCP adapter.
   - Click on the **Discover Controllers** button.
   - From the list of discovered controllers, click the check box for the two controllers with network addresses aligned with this NVMe over TCP adapter.
   - Click on the **OK** button to add the selected controllers.



Add controller | vmhba68

Automatically   Manually

Host NQN: nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-... COPY

IP: 172.21.118.189 (Enter IPv4 / IPv6 address) □ Central discovery controller

Port Number: (Range more from 0)

Digest parameter: □ Header digest □ Data digest

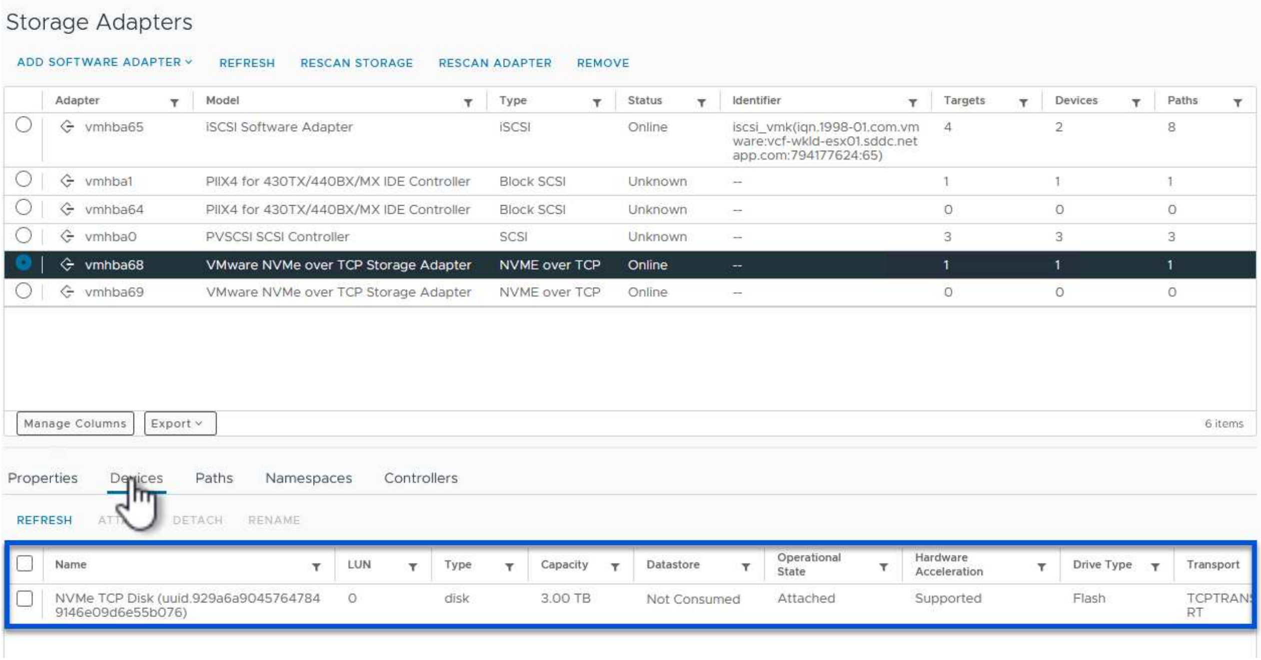
DISCOVER CONTROLLERS

Select which controller to connect

□	Id	Subsystem NQN	Transport Type	IP	Port Number
☑	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF_WKLD_04_NVMe_VCF_WKLD_04_NVMe	nvm	172.21.118.189	4420
☑	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF	nvm	172.21.118.190	4420

☑ 2 Manage Columns 4 items

6. After a few seconds you should see the NVMe namespace appear on the Devices tab.



Storage Adapters

	Adapter	Model	Type	Status	Identifier	Targets	Devices	Paths
○	vmhba65	iSCSI Software Adapter	iSCSI	Online	iscsi_vmk(iqn.1998-01.com.vmware:vcf-wkld-esx01.sddc.netapp.com:794177624:65)	4	2	8
○	vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	1	1	1
○	vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	0	0	0
○	vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	3	3	3
●	vmhba68	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	1	1	1
○	vmhba69	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	0	0	0

Manage Columns Export ⌄ 6 items

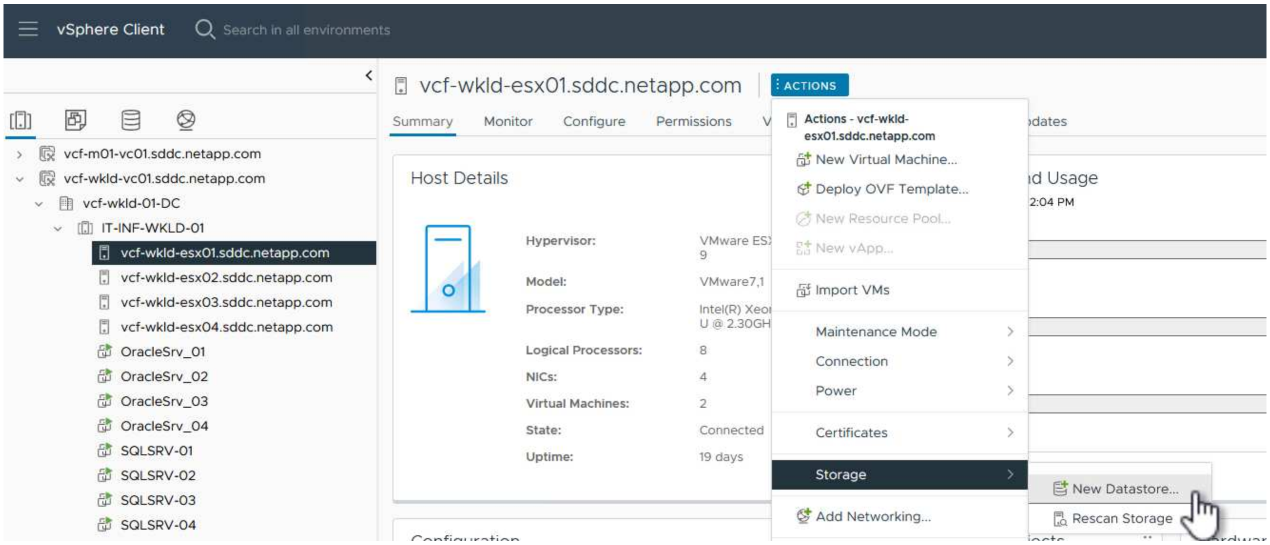
□	Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type	Transport
□	NVMe TCP Disk (uuid.929a6a90457647849146e09d6e55b076)	0	disk	3.00 TB	Not Consumed	Attached	Supported	Flash	TCPTRANSRT

7. Repeat this procedure to create an NVMe over TCP adapter for the second network established for NVMe/TCP traffic.

Deploy NVMe over TCP datastore

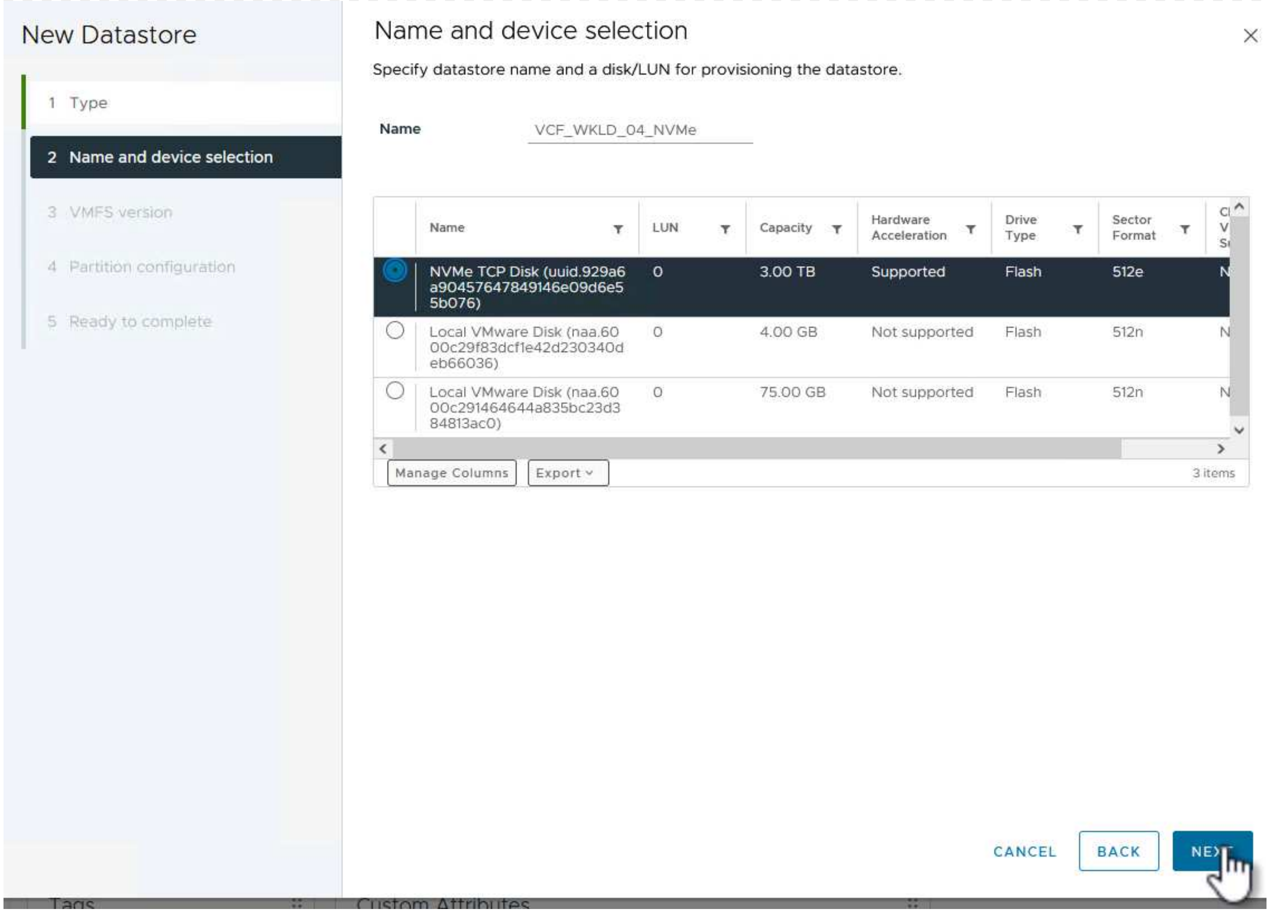
To create a VMFS datastore on the NVMe namespace, complete the following steps:

1. In the vSphere client navigate to one of the ESXi hosts in the workload domain cluster. From the **Actions** menu select **Storage > New Datastore…**.



Hypervisor: VMware ESX 9
Model: VMware7,1
Processor Type: Intel(R) Xeon U @ 2.30GH
Logical Processors: 8
NICs: 4
Virtual Machines: 2
State: Connected
Uptime: 19 days

2. In the **New Datastore** wizard, select **VMFS** as the type. Click on **Next** to continue.
3. On the **Name and device selection** page, provide a name for the datastore and select the NVMe namespace from the list of available devices.



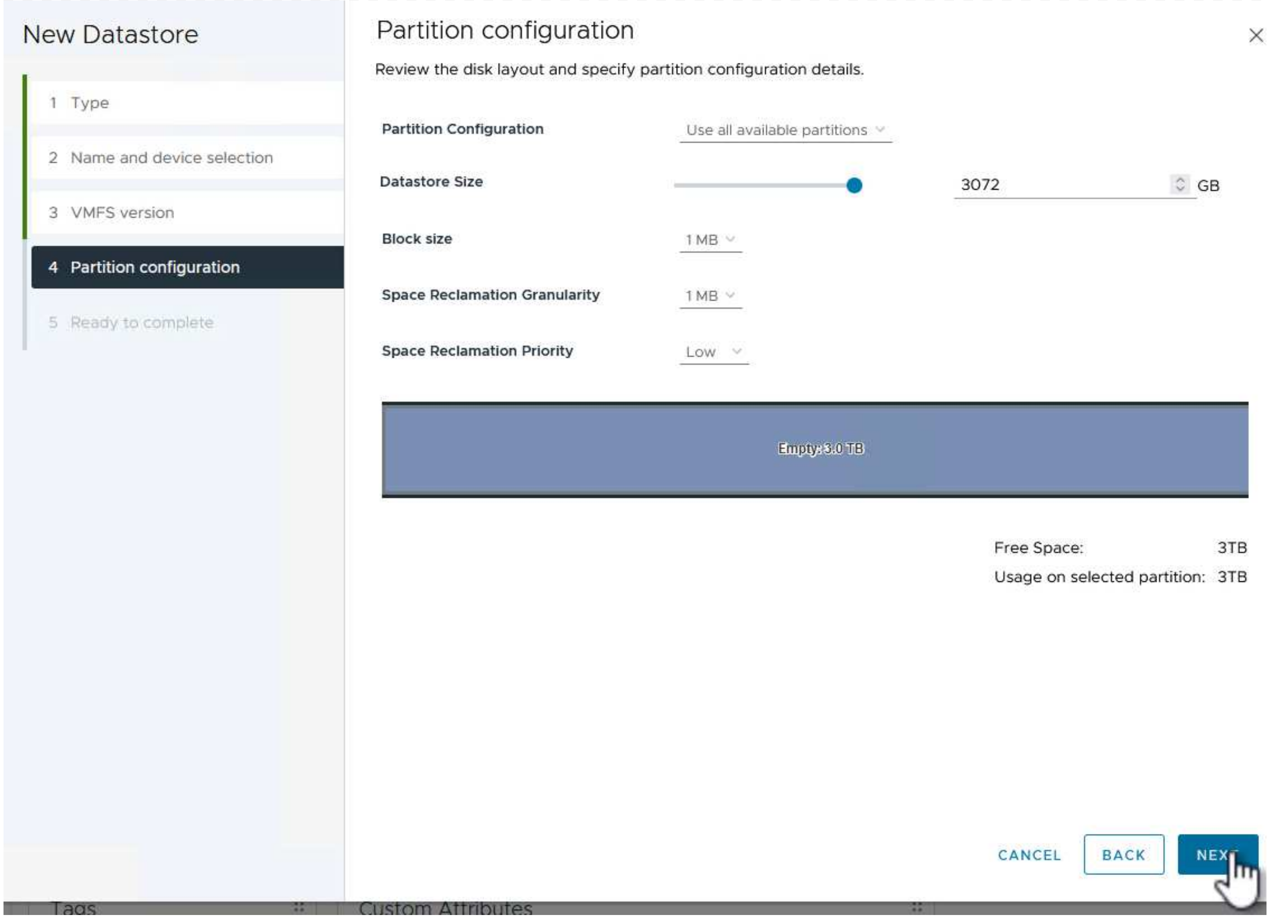
Name and device selection

Specify datastore name and a disk/LUN for provisioning the datastore.

Name VCF_WKLD_04_NVMe

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format	Cl V S
●	NVMe TCP Disk (uuid.929a6a90457647849146e09d6e55b076)	0	3.00 TB	Supported	Flash	512e	N
○	Local VMware Disk (naa.6000c29f83dcf1e42d230340deb66036)	0	4.00 GB	Not supported	Flash	512n	N
○	Local VMware Disk (naa.6000c291464644a835bc23d384813ac0)	0	75.00 GB	Not supported	Flash	512n	N

4. On the **VMFS version** page select the version of VMFS for the datastore.
5. On the **Partition configuration** page, make any desired changes to the default partition scheme. Click on **Next** to continue.



Partition configuration

Review the disk layout and specify partition configuration details.

Partition Configuration: Use all available partitions

Datastore Size: 3072 GB

Block size: 1 MB

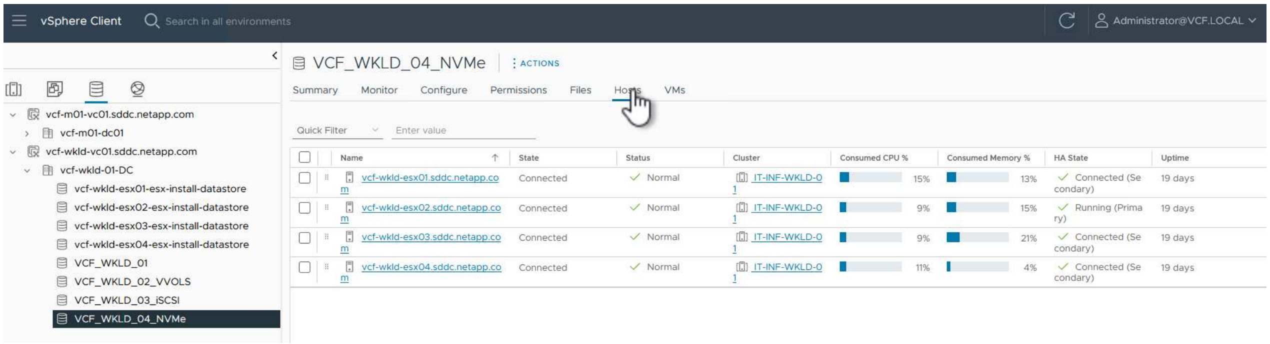
Space Reclamation Granularity: 1 MB

Space Reclamation Priority: Low

Free Space: 3TB

Usage on selected partition: 3TB

6. On the **Ready to complete** page, review the summary and click on **Finish** to create the datastore.
7. Navigate to the new datastore in inventory and click on the **Hosts** tab. If configured correctly, all ESXi hosts in the cluster should be listed and have access to the new datastore.


vSphere Client
Search in all environments
Administrator@VCF.LOCAL
vcf-m01-vc01.sddc.netapp.com
vcf-m01-dc01
vcf-wkld-vc01.sddc.netapp.com
vcf-wkld-01-DC
vcf-wkld-esx01-esx-install-datastore
vcf-wkld-esx02-esx-install-datastore
vcf-wkld-esx03-esx-install-datastore
vcf-wkld-esx04-esx-install-datastore
VCF_WKLD_01
VCF_WKLD_02_VVOLS
VCF_WKLD_03_iSCSI
VCF_WKLD_04_NVMe
ACTIONS
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
Quick Filter
Enter value

VCF_WKLD_04_NVMe

Name	State	Status	Cluster	Consumed CPU %	Consumed Memory %	HA State	Uptime
vcf-wkld-esx01.sddc.netapp.com	Connected	✓ Normal	IT-INF-WKLD-01	15%	13%	✓ Connected (Secondary)	19 days
vcf-wkld-esx02.sddc.netapp.com	Connected	✓ Normal	IT-INF-WKLD-01	9%	15%	✓ Running (Primary)	19 days
vcf-wkld-esx03.sddc.netapp.com	Connected	✓ Normal	IT-INF-WKLD-01	9%	21%	✓ Connected (Secondary)	19 days
vcf-wkld-esx04.sddc.netapp.com	Connected	✓ Normal	IT-INF-WKLD-01	11%	4%	✓ Connected (Secondary)	19 days

Additional information

For information on configuring ONTAP storage systems refer to the ONTAP 9 Documentation center.

For information on configuring VCF refer to VMware Cloud Foundation Documentation.

Use SnapCenter Plug-in for VMware vSphere to protect VMs on VCF Workload Domains

In this scenario we will demonstrate how to deploy and use the SnapCenter Plug-in for VMware vSphere (SCV) to backup and restore VM's and datastores on a VCF workload domain. SCV uses ONTAP snapshot technology to take fast and efficient backup copies of the ONTAP storage volumes hosting vSphere datastores. SnapMirror and SnapVault technology are used to create secondary backups on a separate storage system and with retention policies that mimic the original volume or can be independent of the original volume for longer term retention.

iSCSI is used as the storage protocol for the VMFS datastore in this solution.

Author: Josh Powell

Scenario Overview

This scenario covers the following high level steps:

- Deploy the SnapCenter Plug-in for VMware vSphere (SCV) on the VI workload domain.
- Add storage systems to SCV.
- Create backup policies in SCV.
- Create Resource Groups in SCV.
- Use SCV to backup datastores or specific VMs.
- Use SCV to restores VMs to an alternate location in the cluster.
- Use SCV to restores files to a windows file system.

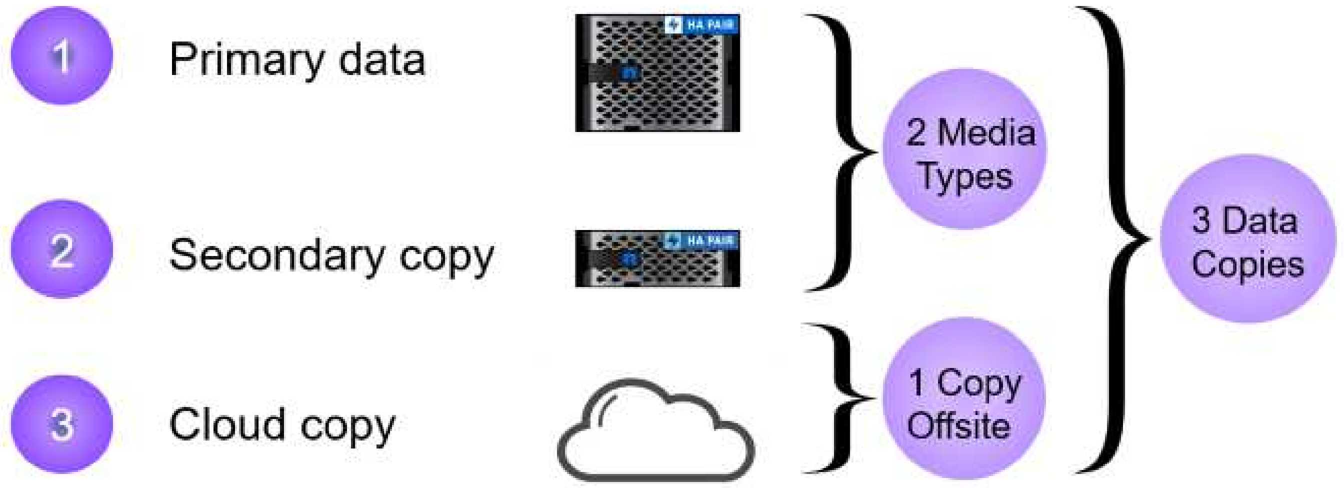
Prerequisites

This scenario requires the following components and configurations:

- An ONTAP ASA storage system with iSCSI VMFS datastores allocated to the workload domain cluster.
- A secondary ONTAP storage system configured to received secondary backups using SnapMirror.
- VCF management domain deployment is complete and the vSphere client is accessible.
- A VI workload domain has been previously deployed.
- Virtual machines are present on the cluster SCV is designated to protect.

For information on configuring iSCSI VMFS datastores as supplemental storage refer to **iSCSI as supplemental storage for Management Domains** in this documentation. The process for using OTV to deploy datastores is identical for management and workload domains.

> In addition to replicating backups taken with SCV to secondary storage, offsite copies of data can be made to object storage on one of the three (3) leading cloud providers using NetApp BlueXP backup and recovery for VMs. For more information refer to the solution 3-2-1 Data Protection for VMware with SnapCenter Plug-in and BlueXP backup and recovery for VMs.



Deployment Steps

To deploy the SnapCenter Plug-in and use it to create backups, and restore VMs and datastores, complete the following steps:

Deploy and use SCV to protect data in a VI workload domain

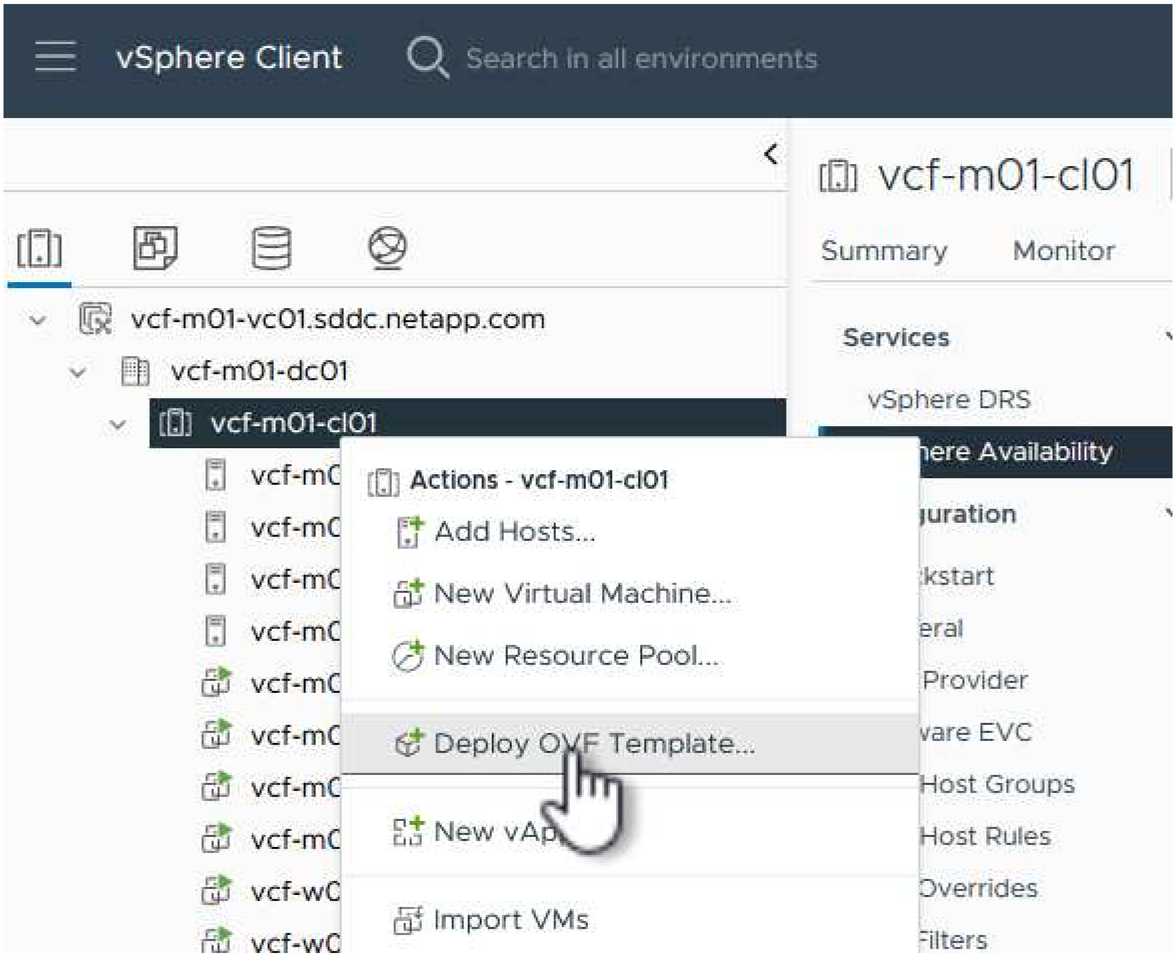
Complete the following steps to deploy, configure, and use SCV to protect data in a VI workload domain:

Deploy the SnapCenter Plug-in for VMware vSphere

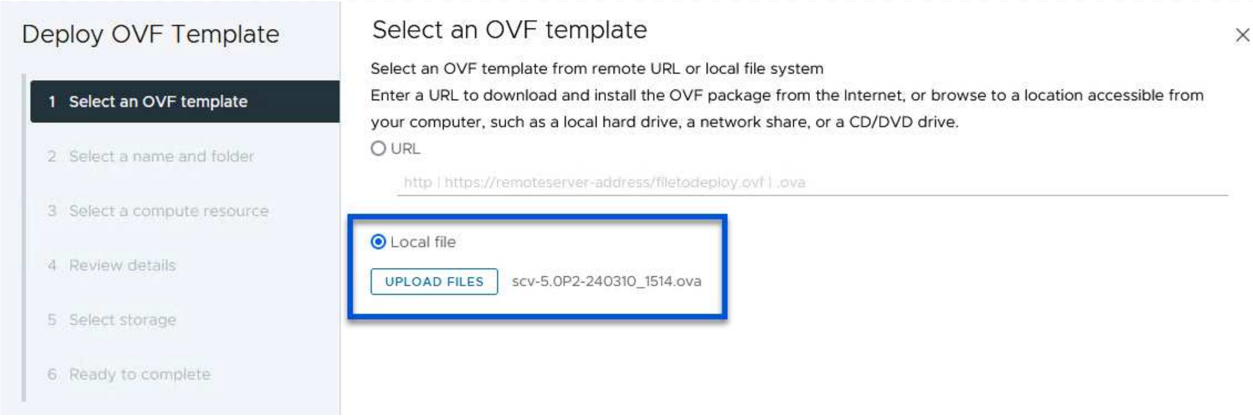
The SnapCenter Plug-in is hosted on the VCF management domain but registered to the vCenter for the VI workload domain. One SCV instance is required for each vCenter instance and, keep in mind that, a Workload domain can include multiple clusters managed by a single vCenter instance.

Complete the following steps from the vCenter client to deploy SCV to the VI workload domain:

1. Download the OVA file for the SCV deployment from the download area of the NetApp support site **HERE**.
2. From the management domain vCenter Client, select to **Deploy OVF Template…**.



3. In the **Deploy OVF Template** wizard, click on the **Local file** radio button and then select to upload the previously downloaded OVF template. Click on **Next** to continue.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

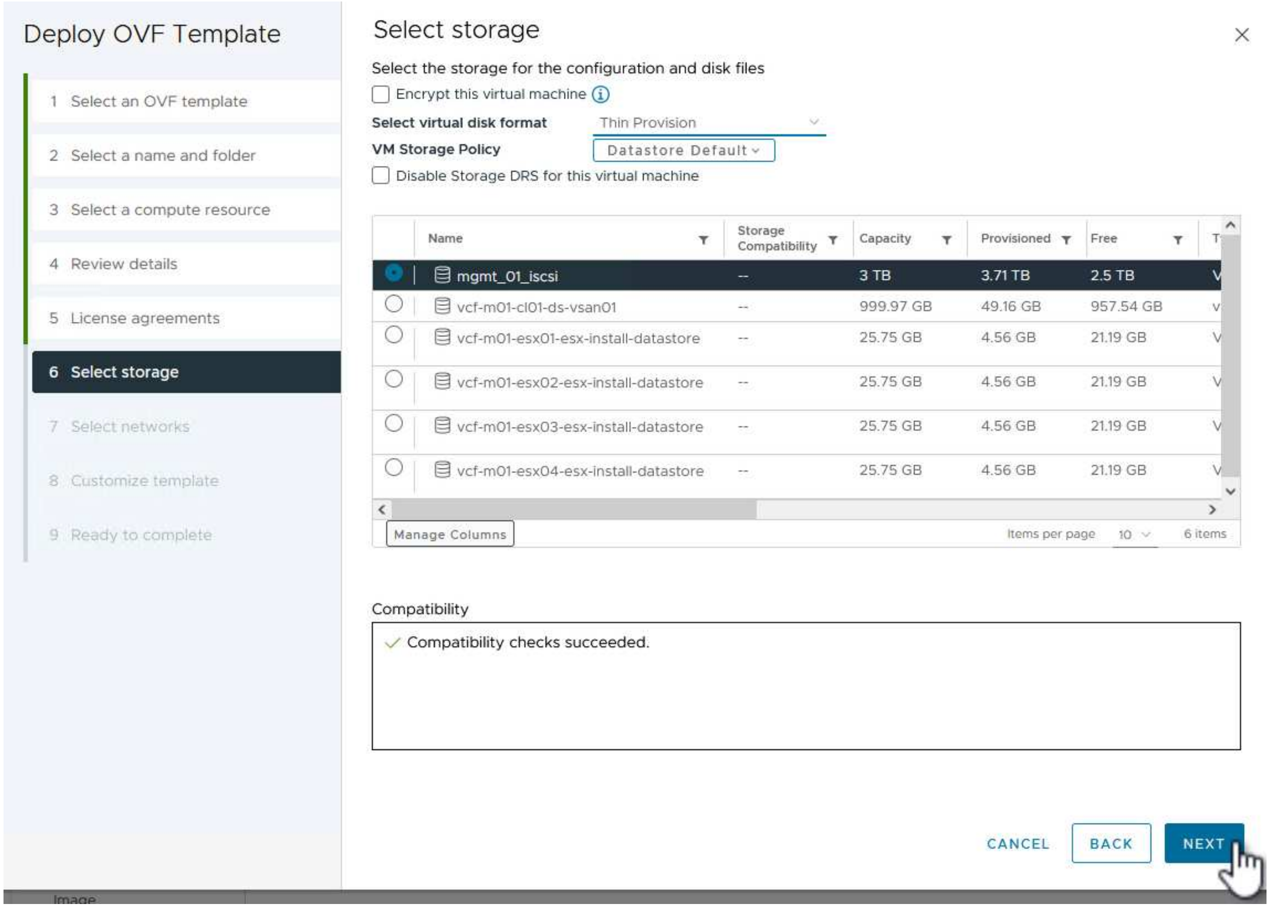
○ URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

● Local file

UPLOAD FILES scv-5.0P2-240310_1514.ova

4. On the **Select name and folder** page, provide a name for the SCV data broker VM and a folder on the management domain. Click on **Next** to continue.
5. On the **Select a compute resource** page, select the management domain cluster or specific ESXi host within the cluster to install the VM to.
6. Review information pertaining to the OVF template on the **Review details** page and agree to the licensing terms on the **Licensing agreements** page.
7. On the **Select storage** page choose the datastore which the VM will be installed to and select the **virtual disk format** and **VM Storage Policy**. In this solution, the VM will be installed on an iSCSI VMFS datastore located on an ONTAP storage system, as previously deployed in a separate section of this documentation. Click on **Next** to continue.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine

Select virtual disk format: Thin Provision

VM Storage Policy: Datastore Default

□ Disable Storage DRS for this virtual machine

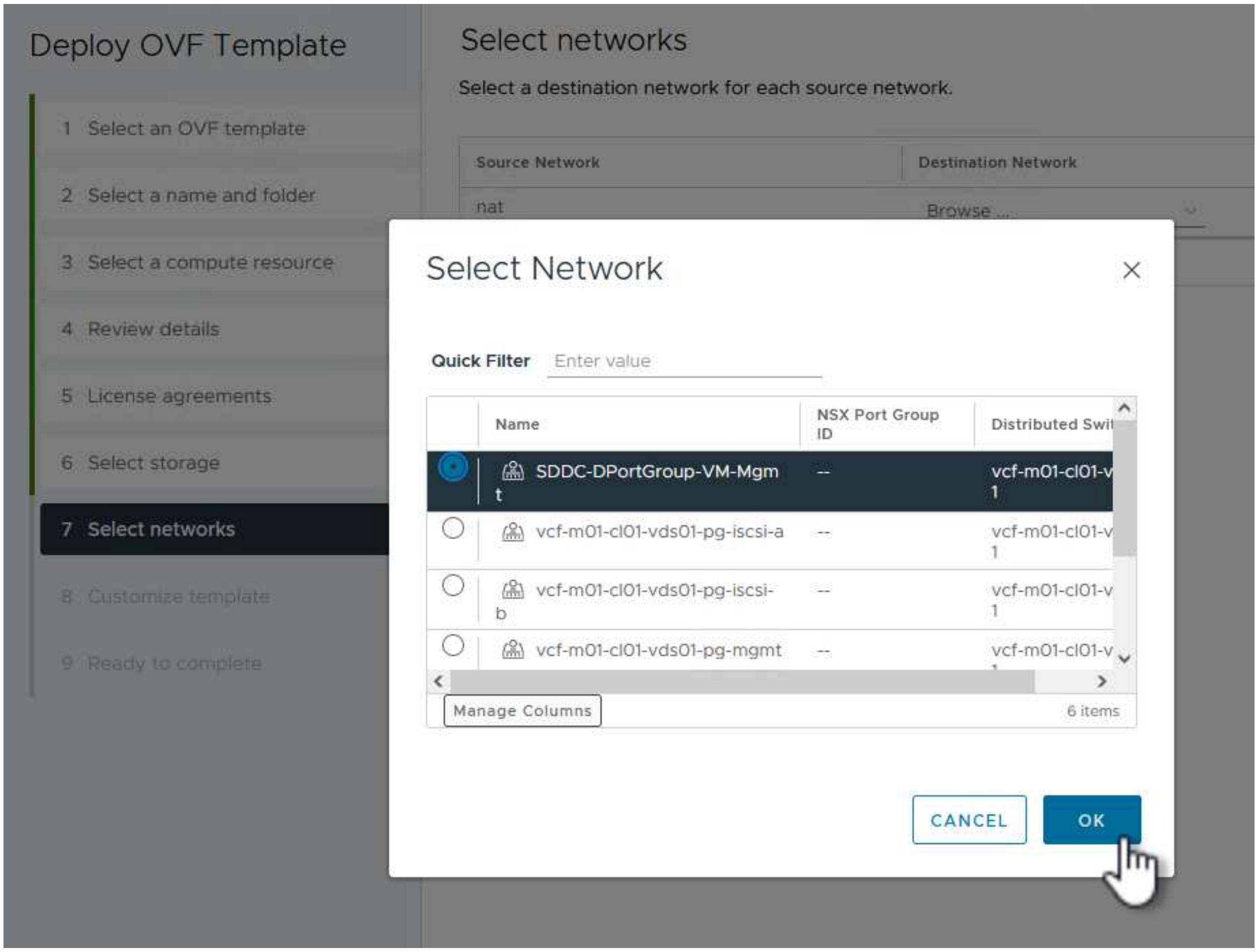
	Name	Storage Compatibility	Capacity	Provisioned	Free
●	mgmt_01_iscsi	--	3 TB	3.71 TB	2.5 TB
○	vcf-m01-cl01-ds-vsan01	--	999.97 GB	49.16 GB	957.54 GB
○	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB
○	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB
○	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB
○	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB

Manage Columns Items per page 10 6 items

Compatibility

✓ Compatibility checks succeeded.

8. On the **Select network** page, select the management network that is able to communicate with the workload domain vCenter appliance and both the primary and secondary ONTAP storage systems.



Select networks

Select a destination network for each source network.

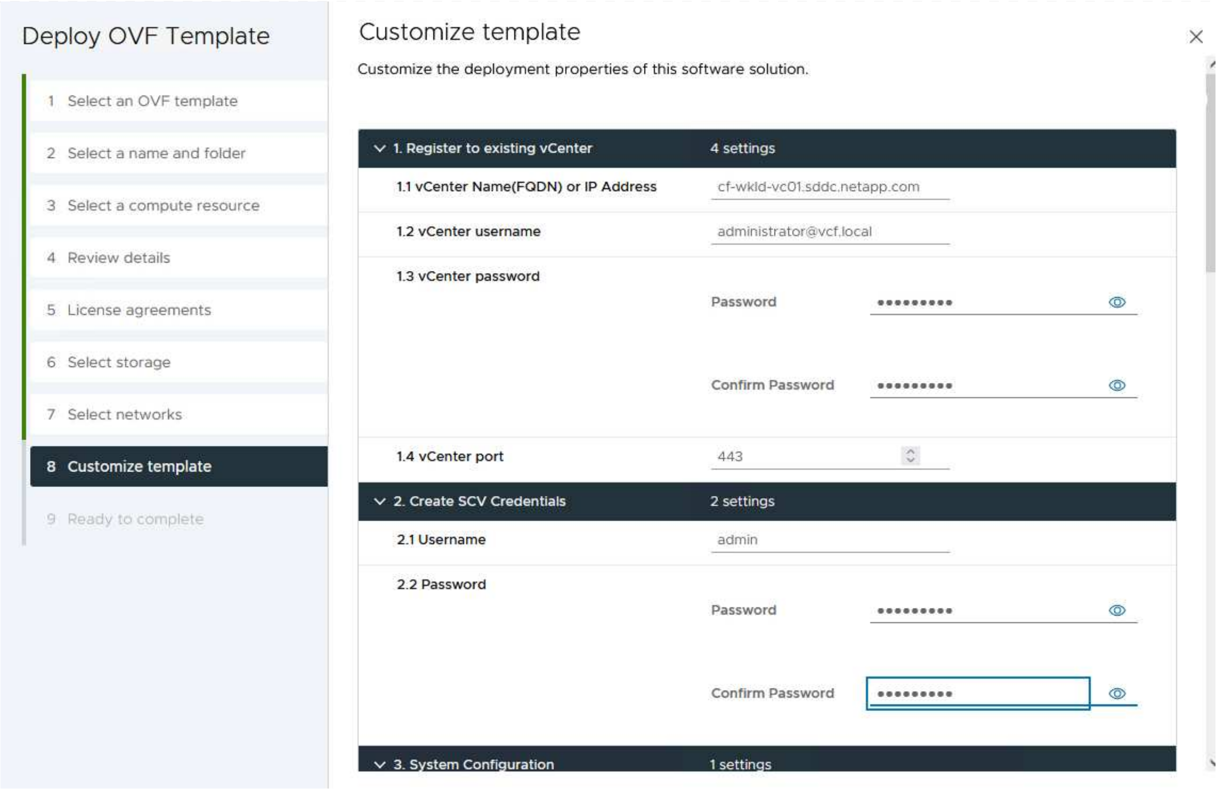
Source Network	Destination Network
nat	Browse ...

Select Network

	Name	NSX Port Group ID	Distributed Swi
●	SDDC-DPortGroup-VM-Mgmt	--	vcf-m01-cl01-v 1
○	vcf-m01-cl01-vds01-pg-iscsi-a	--	vcf-m01-cl01-v 1
○	vcf-m01-cl01-vds01-pg-iscsi-b	--	vcf-m01-cl01-v 1
○	vcf-m01-cl01-vds01-pg-mgmt	--	vcf-m01-cl01-v

9. On the **Customize template** page fill out all information required for the deployment:
   - FQDN or IP, and credentials for the workload domain vCenter appliance.
   - Credentials for the SCV administrative account.
   - Credentials for the SCV maintenance account.
   - IPv4 Network Properties details (IPv6 can also be used).
   - Date and Time settings.

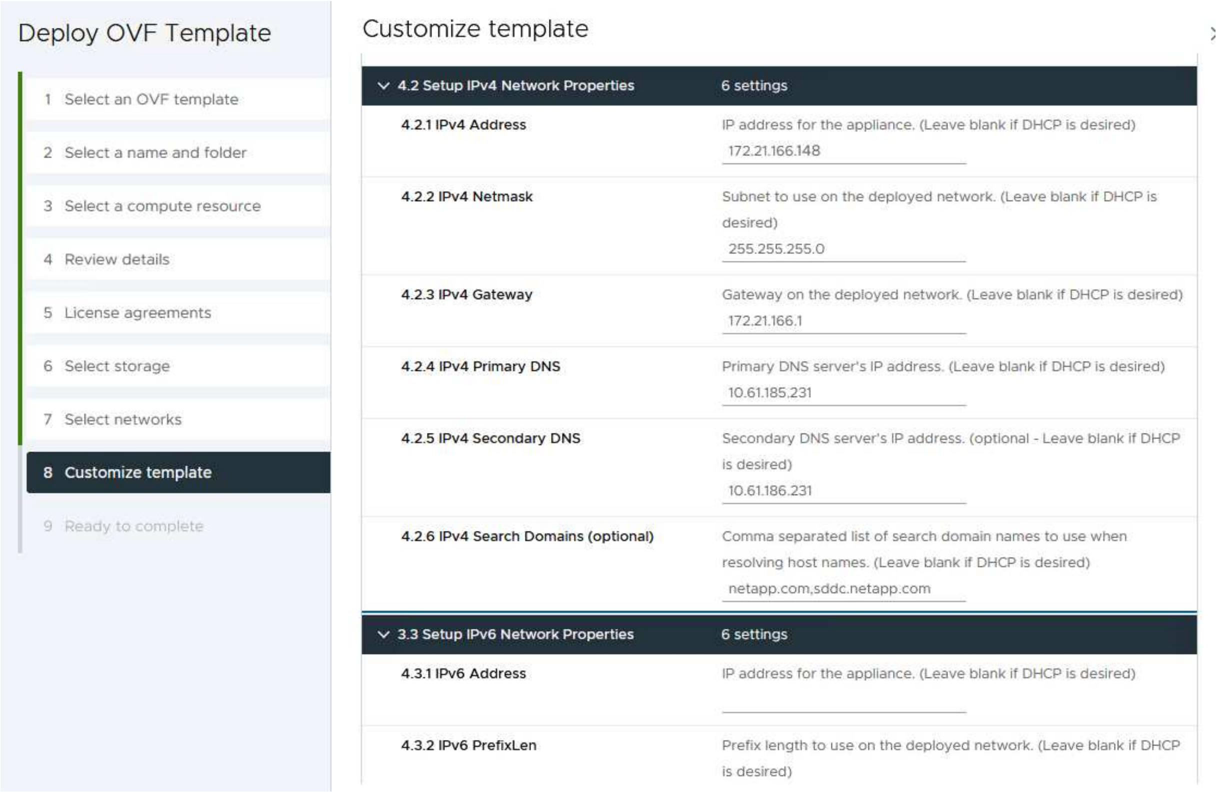
   Click on **Next** to continue.



Customize template

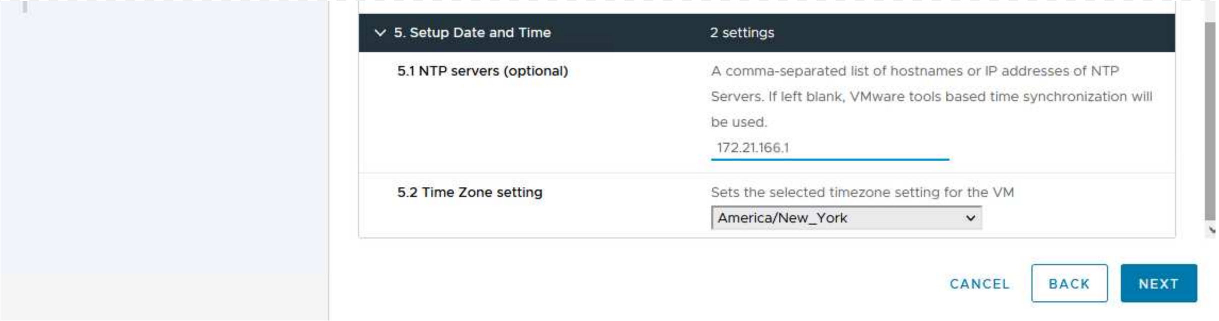
Customize the deployment properties of this software solution.

1. Register to existing vCenter	4 settings
1.1 vCenter Name(FQDN) or IP Address	cf-wkld-vc01.sddc.netapp.com
1.2 vCenter username	administrator@vcf.local
1.3 vCenter password	Password ••••••••• Confirm Password •••••••••
1.4 vCenter port	443
2. Create SCV Credentials	2 settings
2.1 Username	admin
2.2 Password	Password ••••••••• Confirm Password •••••••••
3. System Configuration	1 settings



Customize template

4.2 Setup IPv4 Network Properties	6 settings
4.2.1 IPv4 Address	IP address for the appliance. (Leave blank if DHCP is desired) 172.21.166.148
4.2.2 IPv4 Netmask	Subnet to use on the deployed network. (Leave blank if DHCP is desired) 255.255.255.0
4.2.3 IPv4 Gateway	Gateway on the deployed network. (Leave blank if DHCP is desired) 172.21.166.1
4.2.4 IPv4 Primary DNS	Primary DNS server's IP address. (Leave blank if DHCP is desired) 10.61.185.231
4.2.5 IPv4 Secondary DNS	Secondary DNS server's IP address. (optional - Leave blank if DHCP is desired) 10.61.186.231
4.2.6 IPv4 Search Domains (optional)	Comma separated list of search domain names to use when resolving host names. (Leave blank if DHCP is desired) netapp.com,sddc.netapp.com
3.3 Setup IPv6 Network Properties	6 settings
4.3.1 IPv6 Address	IP address for the appliance. (Leave blank if DHCP is desired)
4.3.2 IPv6 PrefixLen	Prefix length to use on the deployed network. (Leave blank if DHCP is desired)


5. Setup Date and Time 2 settings

5.1 NTP servers (optional) A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used.
172.21.166.1

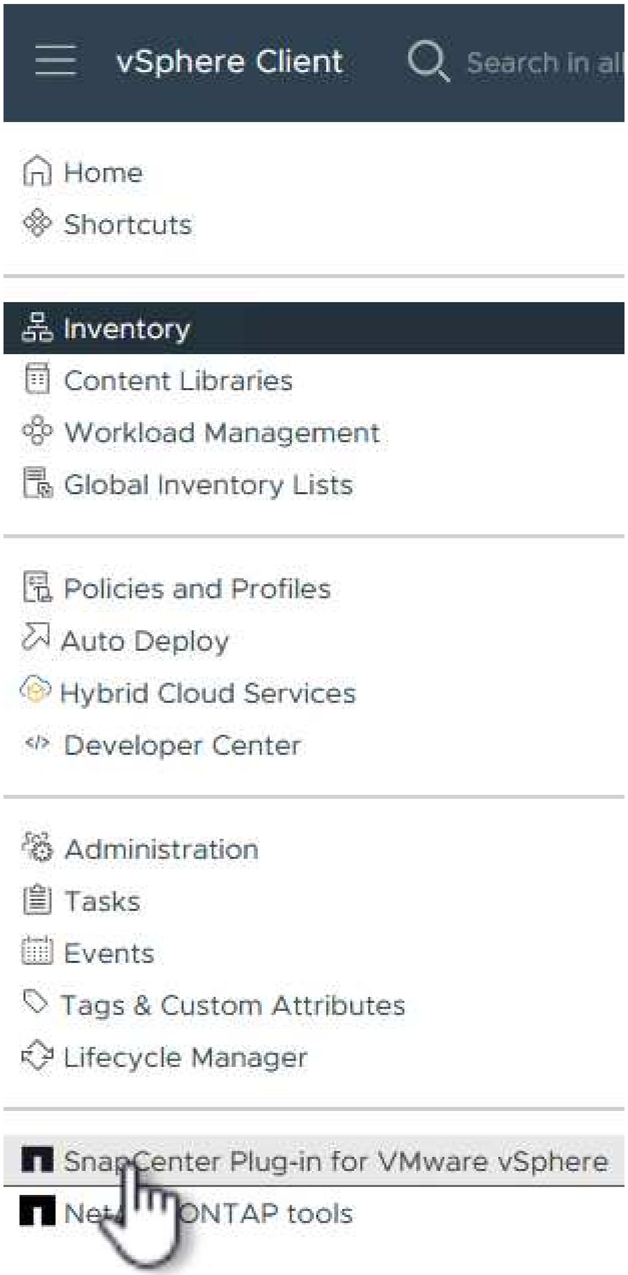
5.2 Time Zone setting Sets the selected timezone setting for the VM
America/New_York

10. Finally, on the **Ready to complete page**, review all settings and click on Finish to start the deployment.

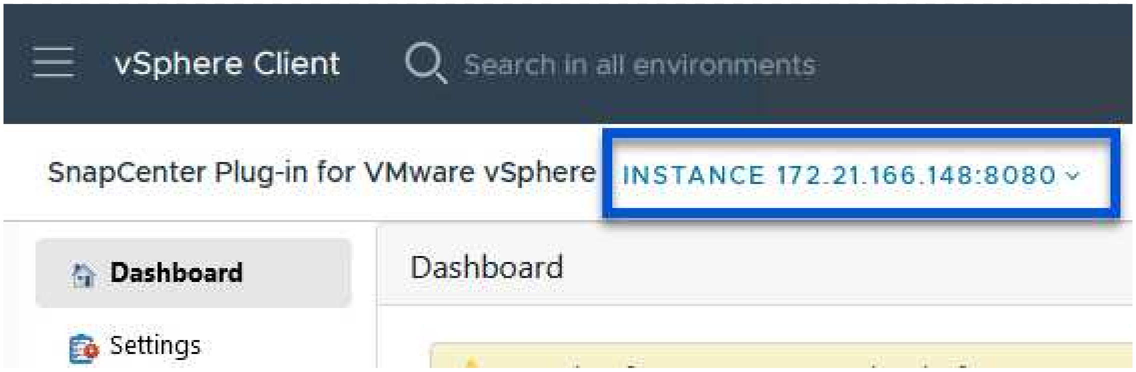
Add Storage Systems to SCV

Once the SnapCenter Plug-in is installed complete the following steps to add storage systems to SCV:

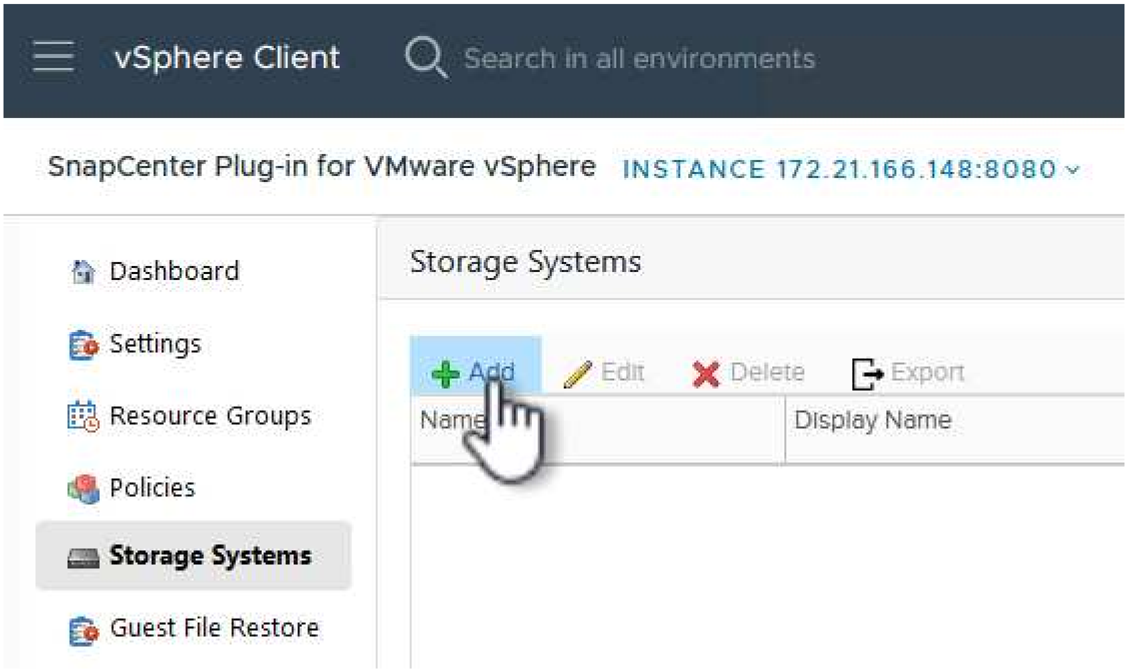
1. SCV can be accessed from the main menu in the vSphere Client.



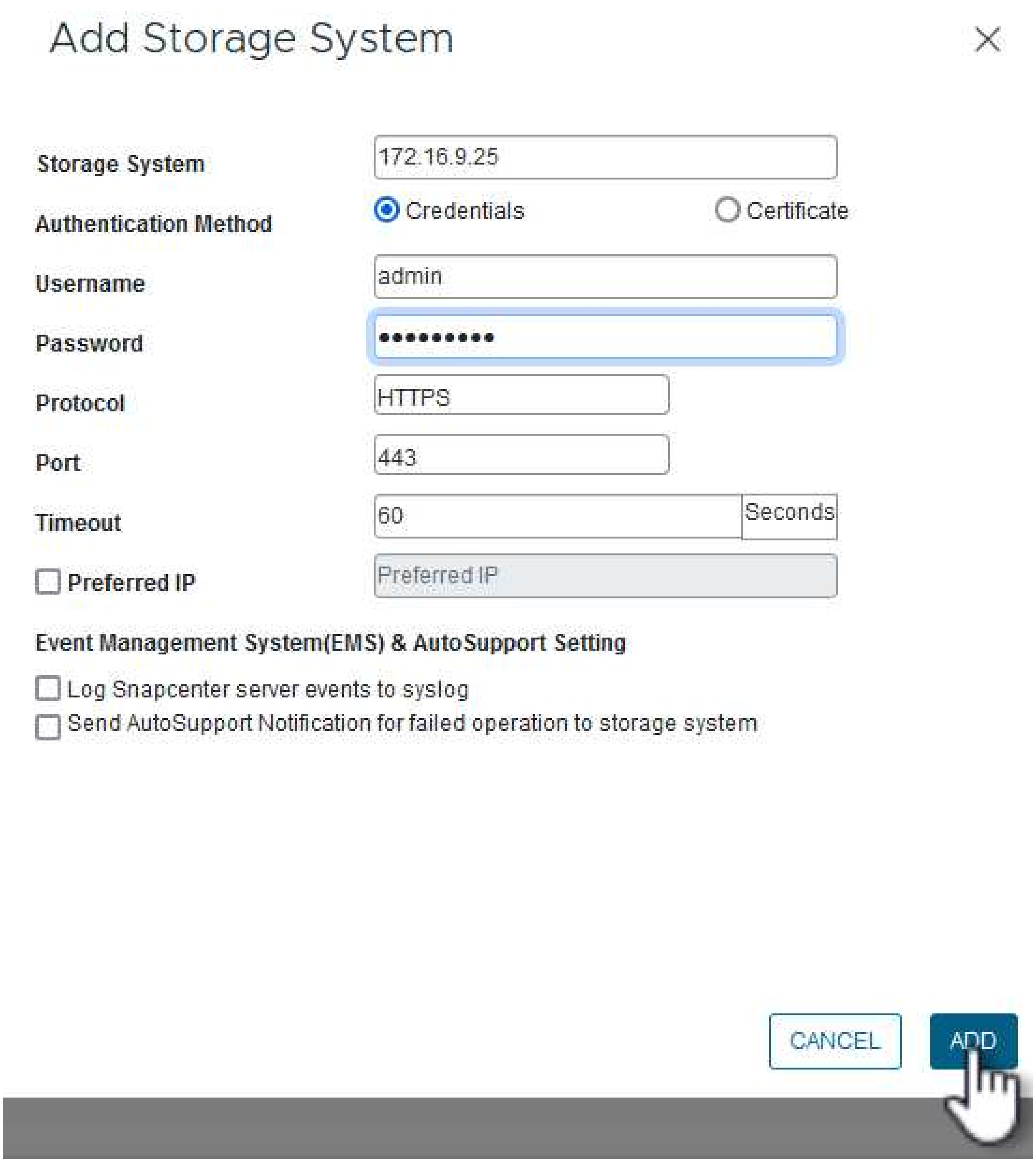
2. At the top of the SCV UI interface, select the correct SCV instance that matches the vSphere cluster to be protected.


vSphere Client
Search in all environments
SnapCenter Plug-in for VMware vSphere
INSTANCE 172.21.166.148:8080
Dashboard
Settings
Dashboard

3. Navigate to **Storage Systems** in the left-hand menu and click on **Add** to get started.



4. On the **Add Storage System** form, fill in the IP address and credentials of the ONTAP storage system to be added, and click on **Add** to complete the action.



Add Storage System

Storage System: 172.16.9.25

Authentication Method: ● Credentials ○ Certificate

Username: admin

Password: ••••••••••

Protocol: HTTPS

Port: 443

Timeout: 60 Seconds

□ Preferred IP: Preferred IP

Event Management System(EMS) & AutoSupport Setting

□ Log Snapcenter server events to syslog

□ Send AutoSupport Notification for failed operation to storage system

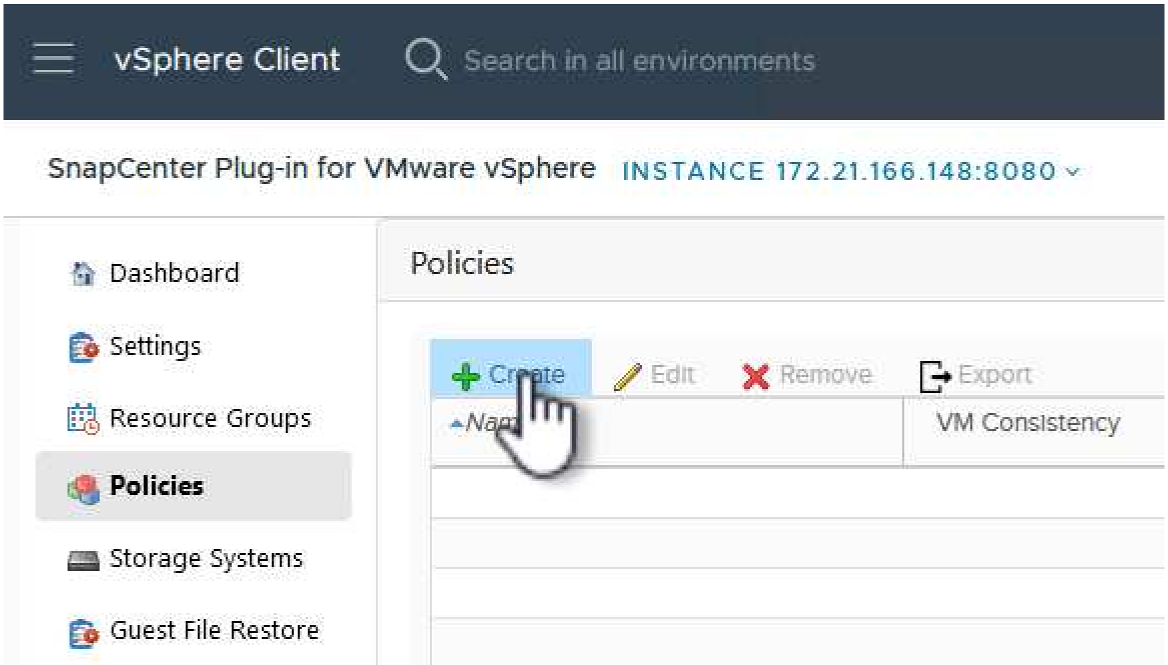
5. Repeat this procedure for any additional storage systems to be managed, including any systems to be used as secondary backup targets.

Configure backup policies in SCV

For more information on creating SCV backup policies refer to Create backup policies for VMs and datastores.

Complete the following steps to create a new backup policy:

1. From the left-hand menu select **Policies** and click on **Create** to begin.



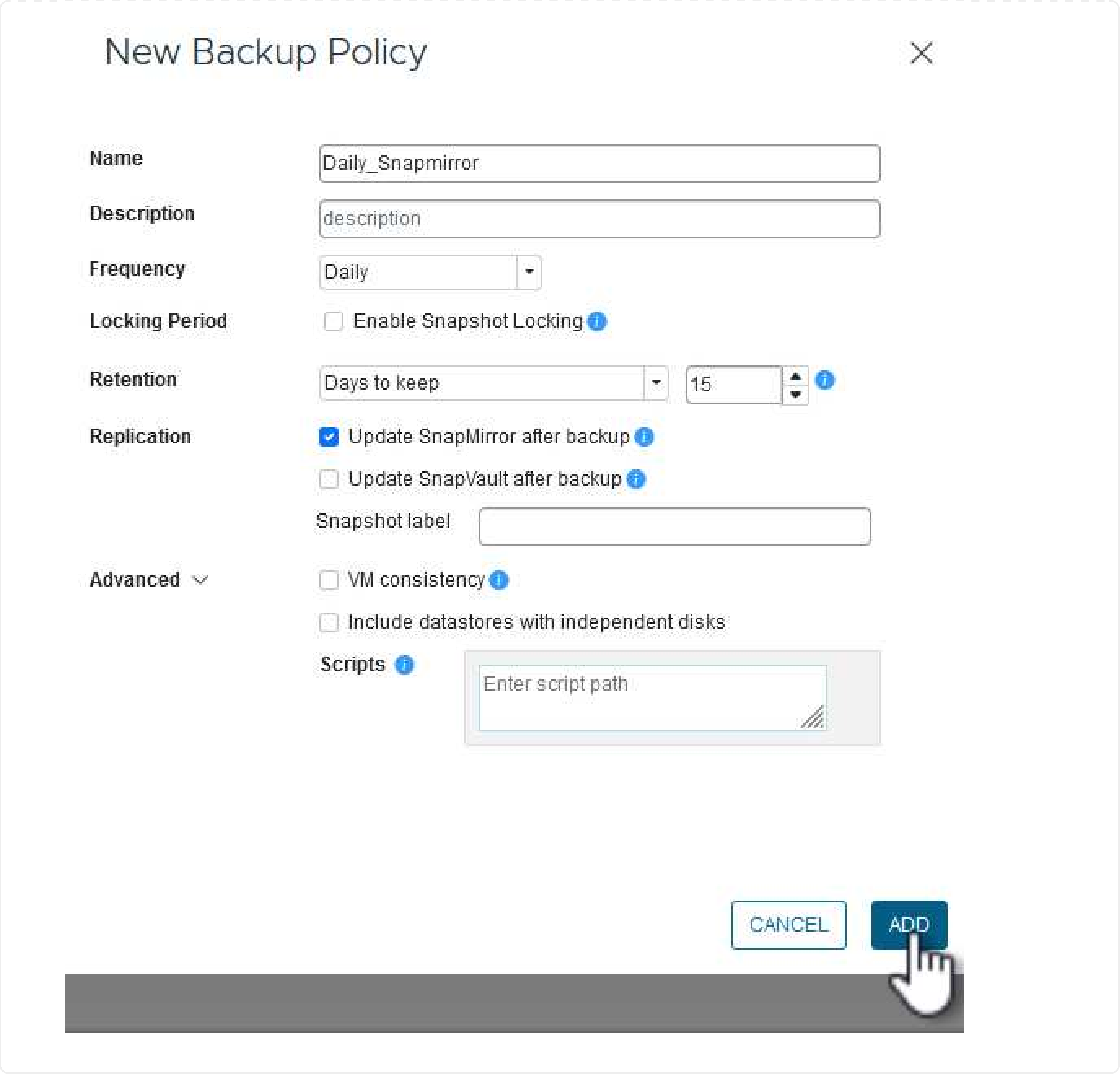
2. On the **New Backup Policy** form, provide a **Name** and **Description** for the policy, the **Frequency** at which the backups will take place, and the **Retention** period which specifies how long the backup is retained.

   Locking Period enables the ONTAP SnapLock feature to create tamper proof snapshots and allows configuration of the locking period.

   For **Replication** Select to update the underlying SnapMirror or SnapVault relationships for the ONTAP storage volume.

   > SnapMirror and SnapVault replication are similar in that they both utilize ONTAP SnapMirror technology to asynchronously replicate storage volumes to a secondary storage system for increased protection and security. For SnapMirror relationships, the retention schedule specified in the SCV backup policy will govern retention for both the primary and secondary volume. With SnapVault relationships, a separate retention schedule can be established on the secondary storage system for longer term or differing retention schedules. In this case the snapshot label is specified in the SCV backup policy and in the policy associated with the secondary volume, to identify which volumes to apply the independent retention schedule to.

   Choose any additional advanced options and click on **Add** to create the policy.



New Backup Policy

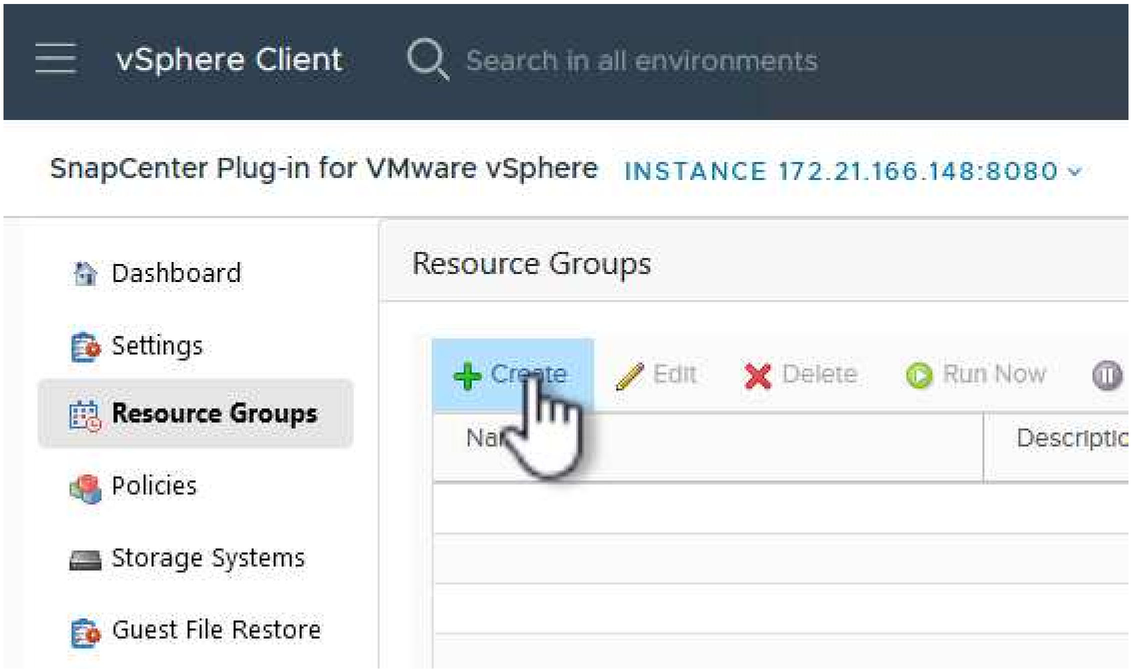
Name	Daily_Snapmirror
Description	description
Frequency	Daily
Locking Period	□ Enable Snapshot Locking
Retention	Days to keep 15
Replication	☑ Update SnapMirror after backup □ Update SnapVault after backup Snapshot label
Advanced	□ VM consistency □ Include datastores with independent disks Scripts: Enter script path

Create resource groups in SCV

For more information on creating SCV Resource Groups refer to Create resource groups.

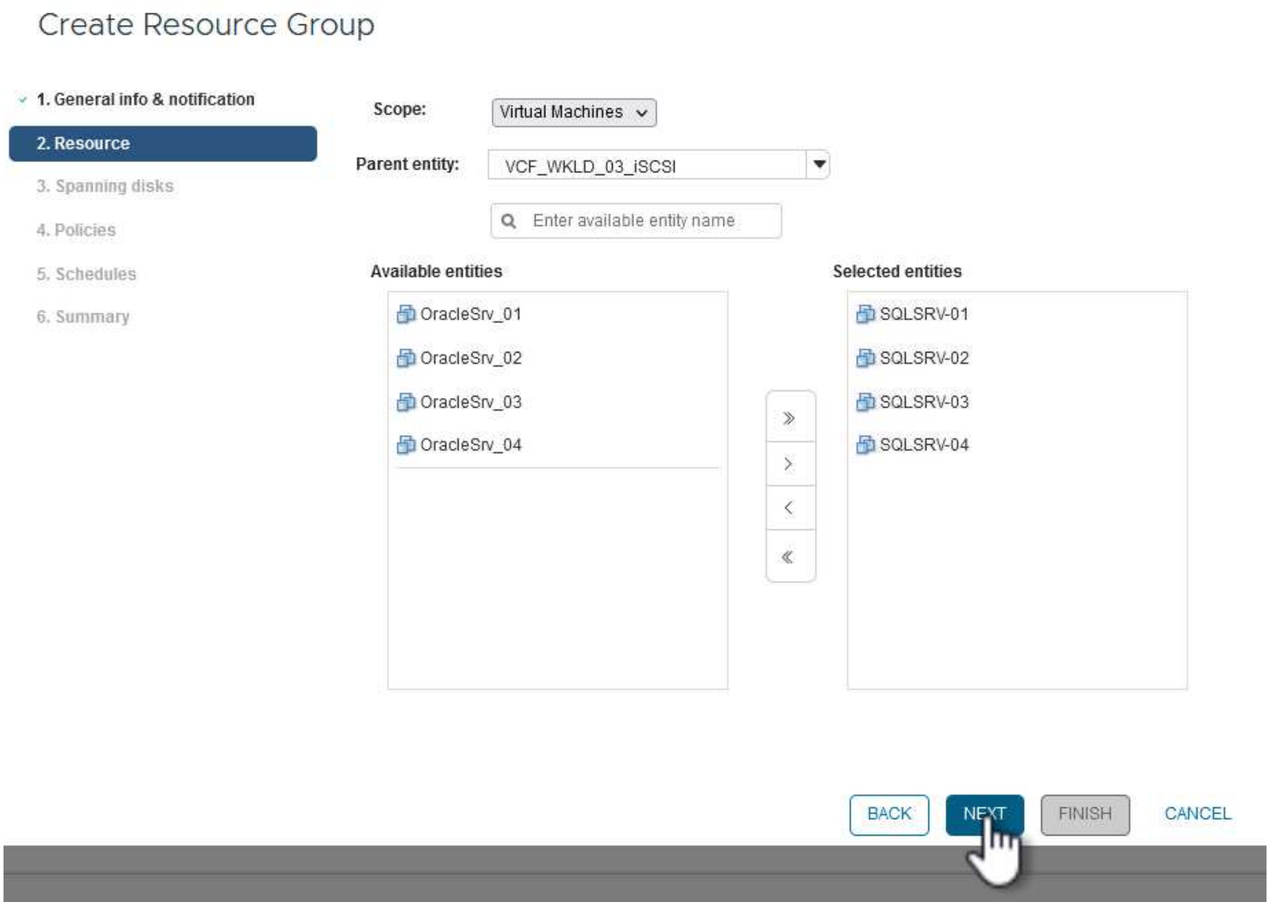
Complete the following steps to create a new resource group:

1. From the left-hand menu select **Resource Groups** and click on **Create** to begin.



2. On the **General info & notification** page, provide a name for for the resource group, notification settings, and any additional options for the naming of the snapshots.
3. On the **Resource** page select the datastores and VM's to be protected in the resource group. Click on **Next** to continue.

> Even when only specific VMs are selected, the entire datastore is always backed up. This is because ONTAP takes snapshots of the volume hosting the datastore. However, note that selecting only specific VMs for backup limits the ability to restore to only those VMs.

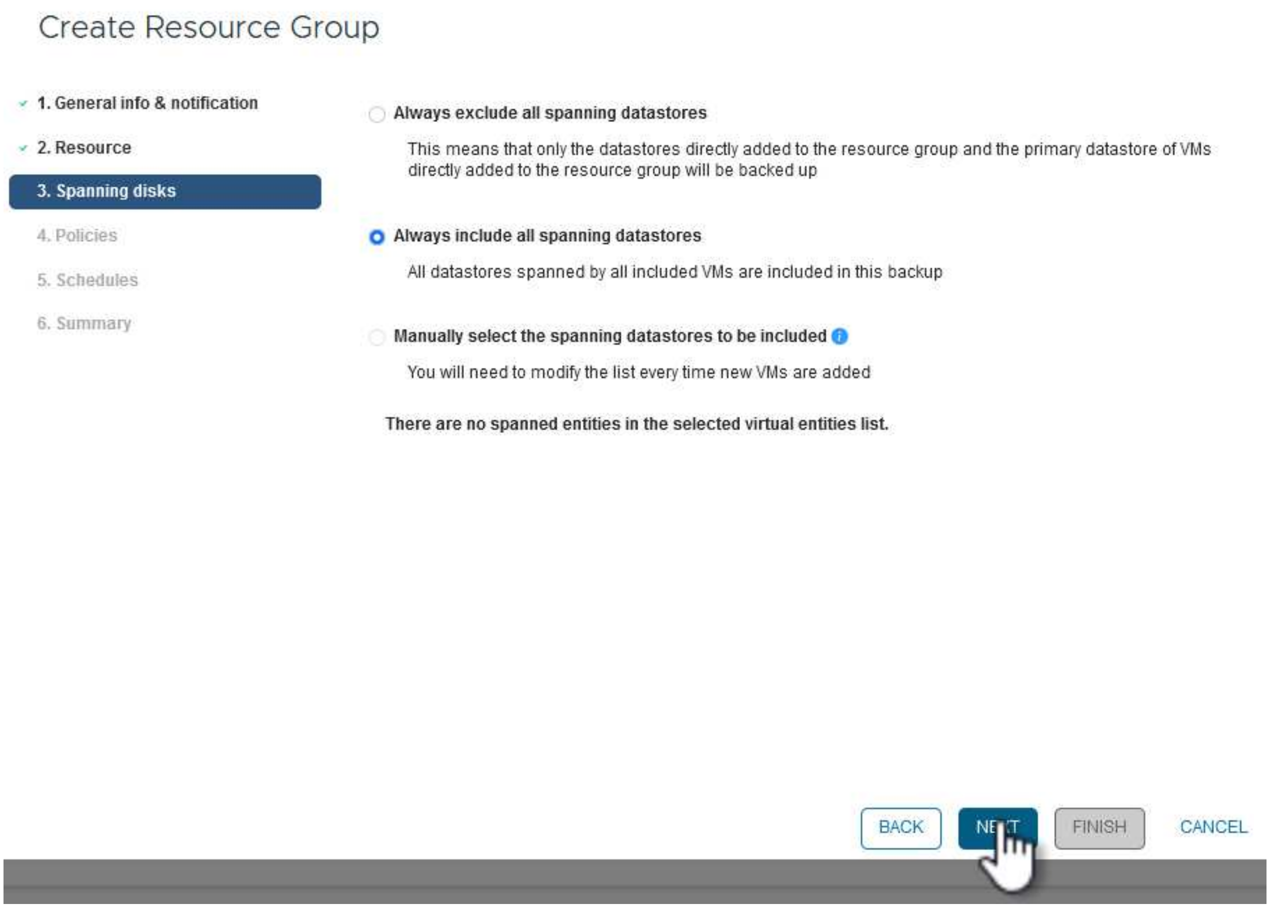

Create Resource Group

Scope: Virtual Machines

Parent entity: VCF_WKLD_03_iSCSI

Available entities	Selected entities
OracleSrv_01	SQLSRV-01
OracleSrv_02	SQLSRV-02
OracleSrv_03	SQLSRV-03
OracleSrv_04	SQLSRV-04

4. On the **Spanning disks** page select the option for how to handle VMs with VMDK’s that span multiple datastores. Click on **Next** to continue.


Create Resource Group

○ **Always exclude all spanning datastores**

This means that only the datastores directly added to the resource group and the primary datastore of VMs directly added to the resource group will be backed up

● **Always include all spanning datastores**

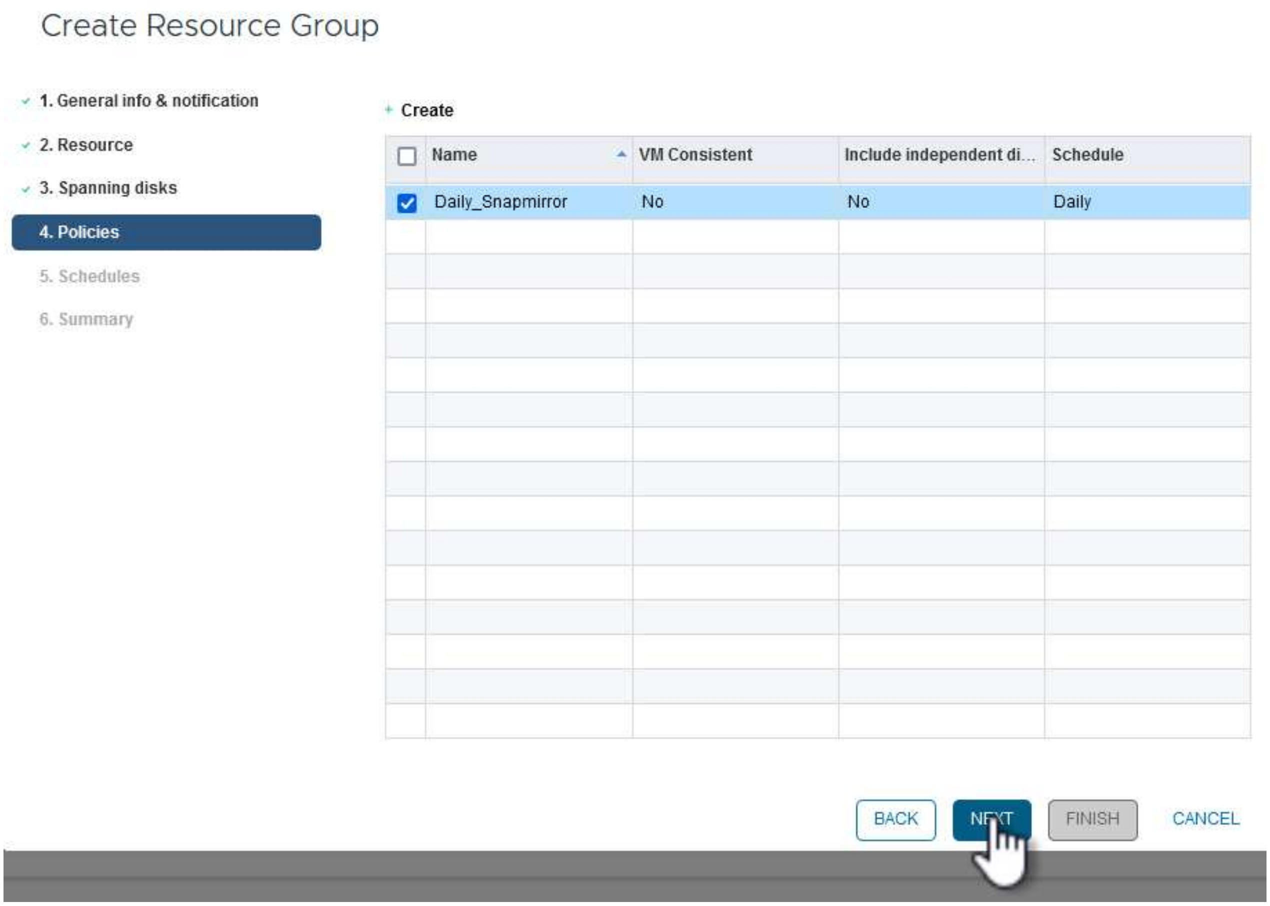
All datastores spanned by all included VMs are included in this backup

○ **Manually select the spanning datastores to be included**

You will need to modify the list every time new VMs are added

There are no spanned entities in the selected virtual entities list.

5. On the **Policies** page select a previously created policy or multiple policies that will be used with this resource group. Click on **Next** to continue.



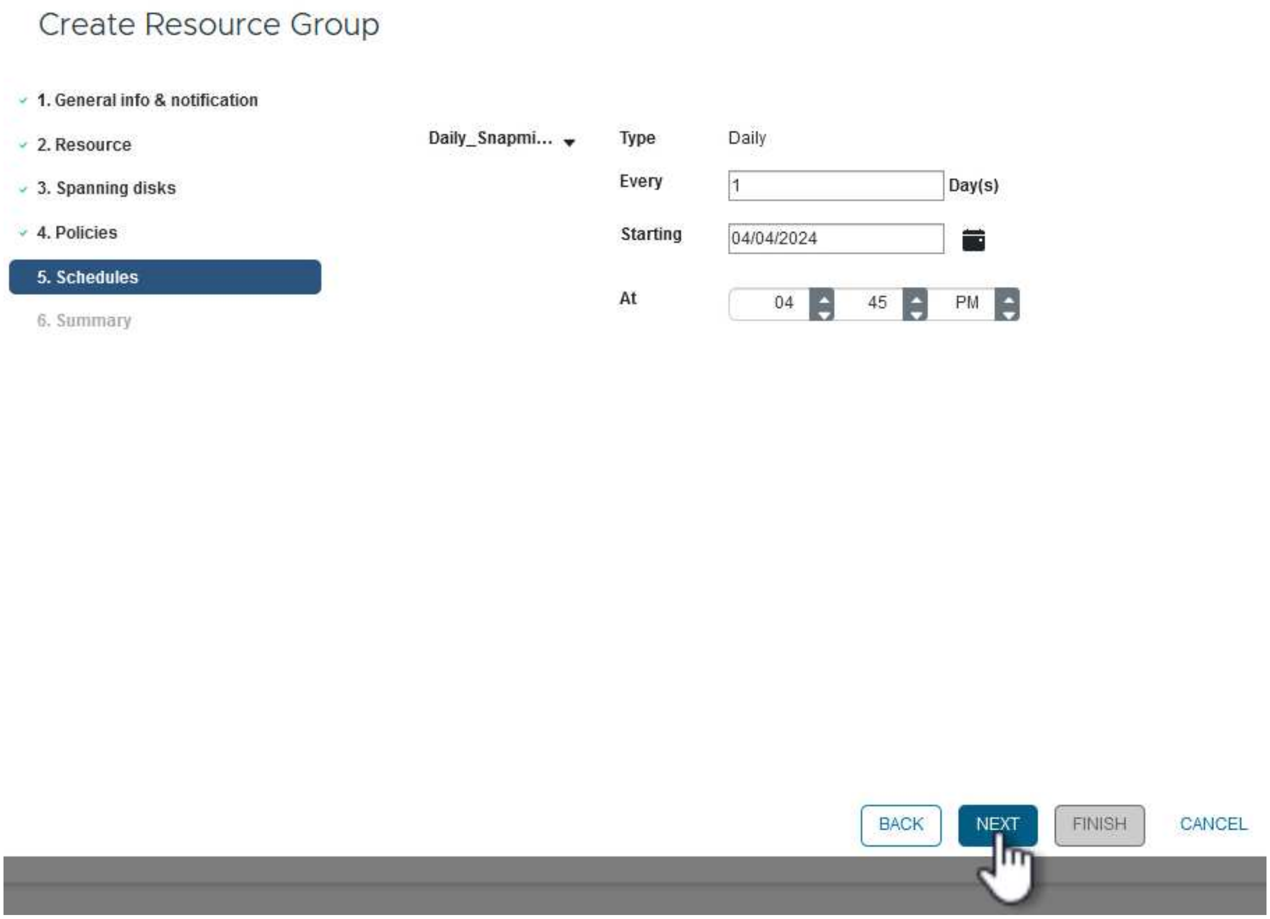
Create Resource Group

- ✓ 1. General info & notification
- ✓ 2. Resource
- ✓ 3. Spanning disks
- 4. Policies
- 5. Schedules
- 6. Summary

+ Create

□	Name	VM Consistent	Include independent di...	Schedule
☑	Daily_Snapmirror	No	No	Daily

6. On the **Schedules** page establish for when the backup will run by configuring the recurrence and time of day. Click on **Next** to continue.


Create Resource Group

Daily_Snapmi...

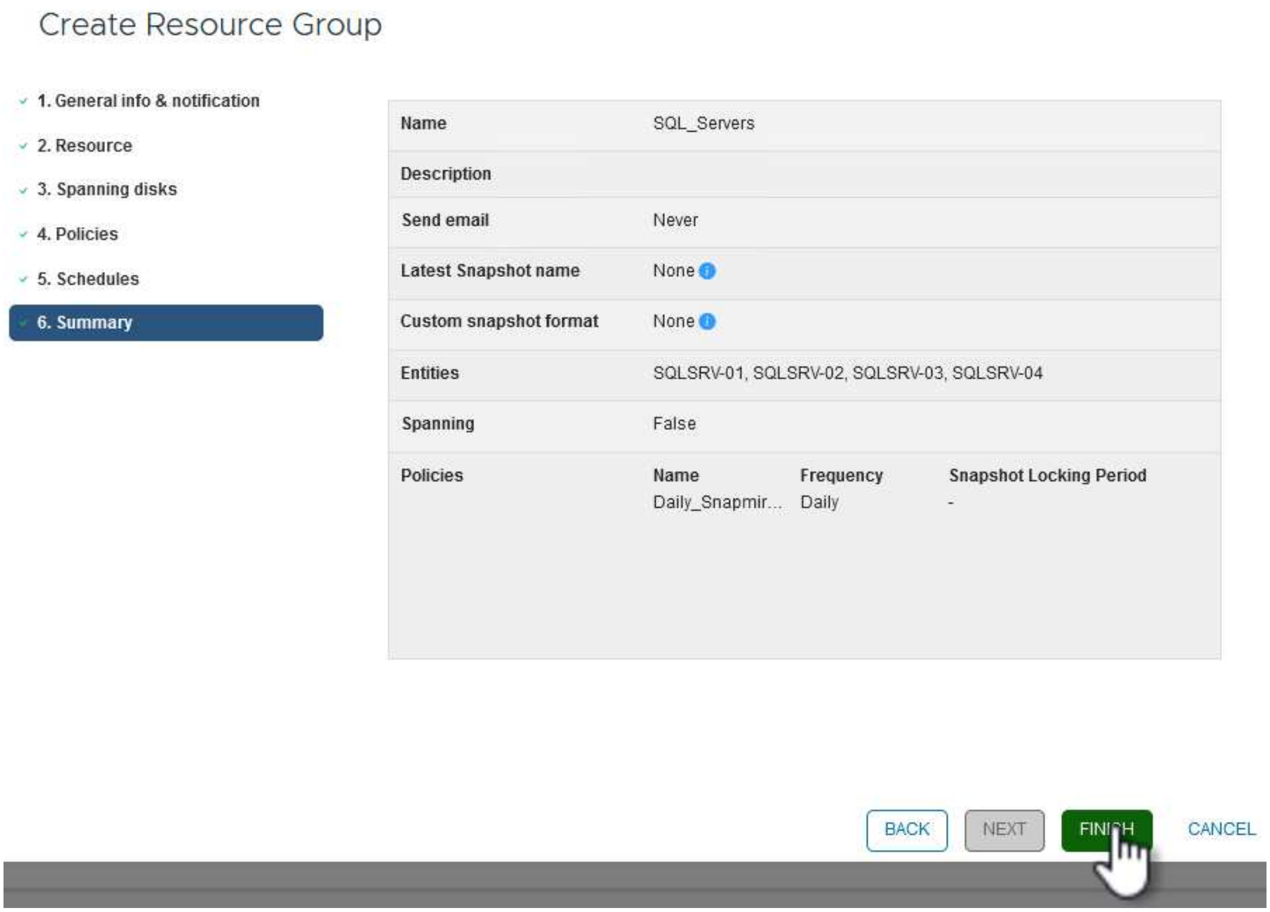
Type: Daily

Every: 1 Day(s)

Starting: 04/04/2024

At: 04 45 PM

7. Finally review the **Summary** and click on **Finish** to create the resource group.

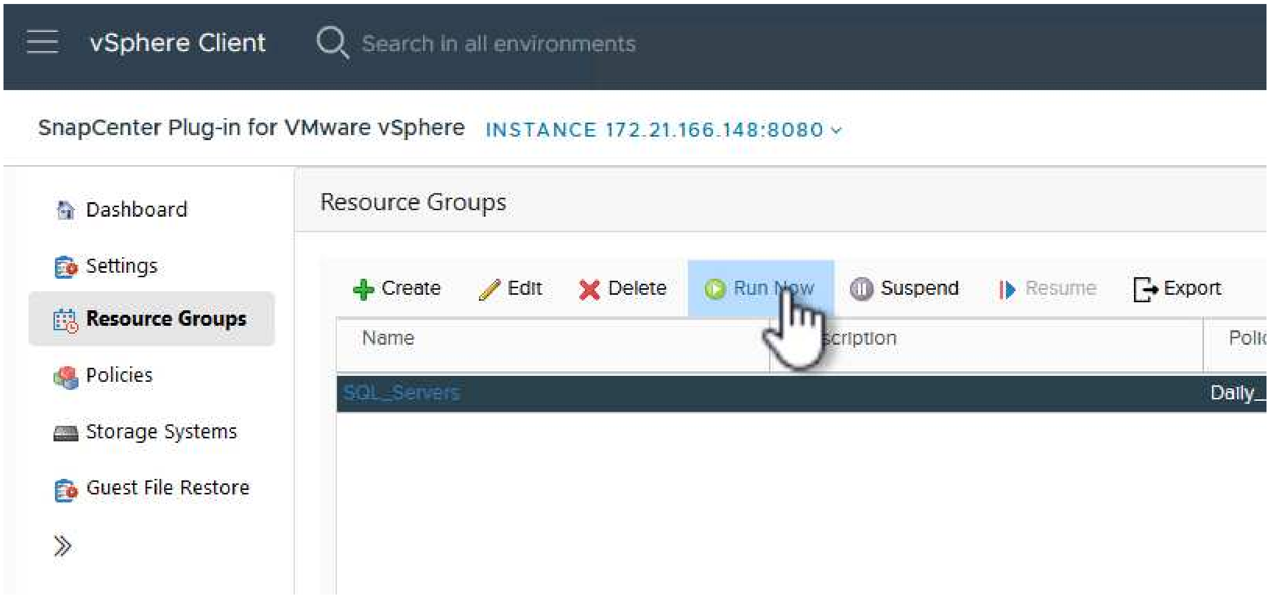


Create Resource Group

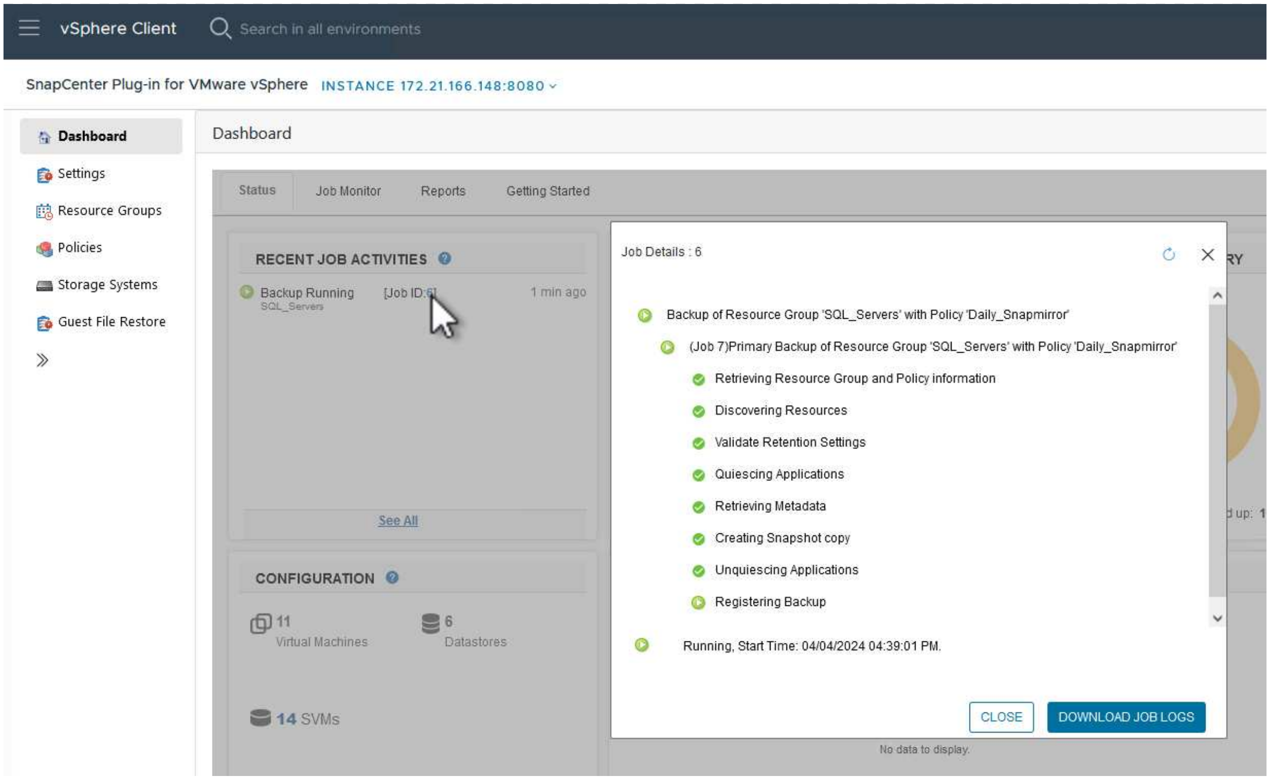
- ✓ 1. General info & notification
- ✓ 2. Resource
- ✓ 3. Spanning disks
- ✓ 4. Policies
- ✓ 5. Schedules
- ✓ 6. Summary

Name	SQL_Servers		
Description			
Send email	Never		
Latest Snapshot name	None		
Custom snapshot format	None		
Entities	SQLSRV-01, SQLSRV-02, SQLSRV-03, SQLSRV-04		
Spanning	False		
Policies	Name Daily_Snapmir...	Frequency Daily	Snapshot Locking Period -

8. With the resource group created click on the **Run Now** button to run the first backup.



9. Navigate to the **Dashboard** and, under **Recent Job Activities** click on the number next to **Job ID** to open the job monitor and view the progress of the running job.



Job Details : 6

Backup of Resource Group 'SQL_Servers' with Policy 'Daily_Snapmirror'

(Job 7)Primary Backup of Resource Group 'SQL_Servers' with Policy 'Daily_Snapmirror'

- Retrieving Resource Group and Policy information
- Discovering Resources
- Validate Retention Settings
- Quiescing Applications
- Retrieving Metadata
- Creating Snapshot copy
- Unquiescing Applications
- Registering Backup

Running, Start Time: 04/04/2024 04:39:01 PM.

Use SCV to restore VMs, VMDKs and files

The SnapCenter Plug-in allows restores of VMs, VMDKs, files, and folders from primary or secondary backups.

VMs can be restored to the original host, or to an alternate host in the same vCenter Server, or to an alternate ESXi host managed by the same vCenter or any vCenter in linked mode.

vVol VMs can be restored to the original host.

VMDKs in traditional VMs can be restored to either the original or to an alternate datastore.

VMDKs in vVol VMs can be restored to the original datastore.

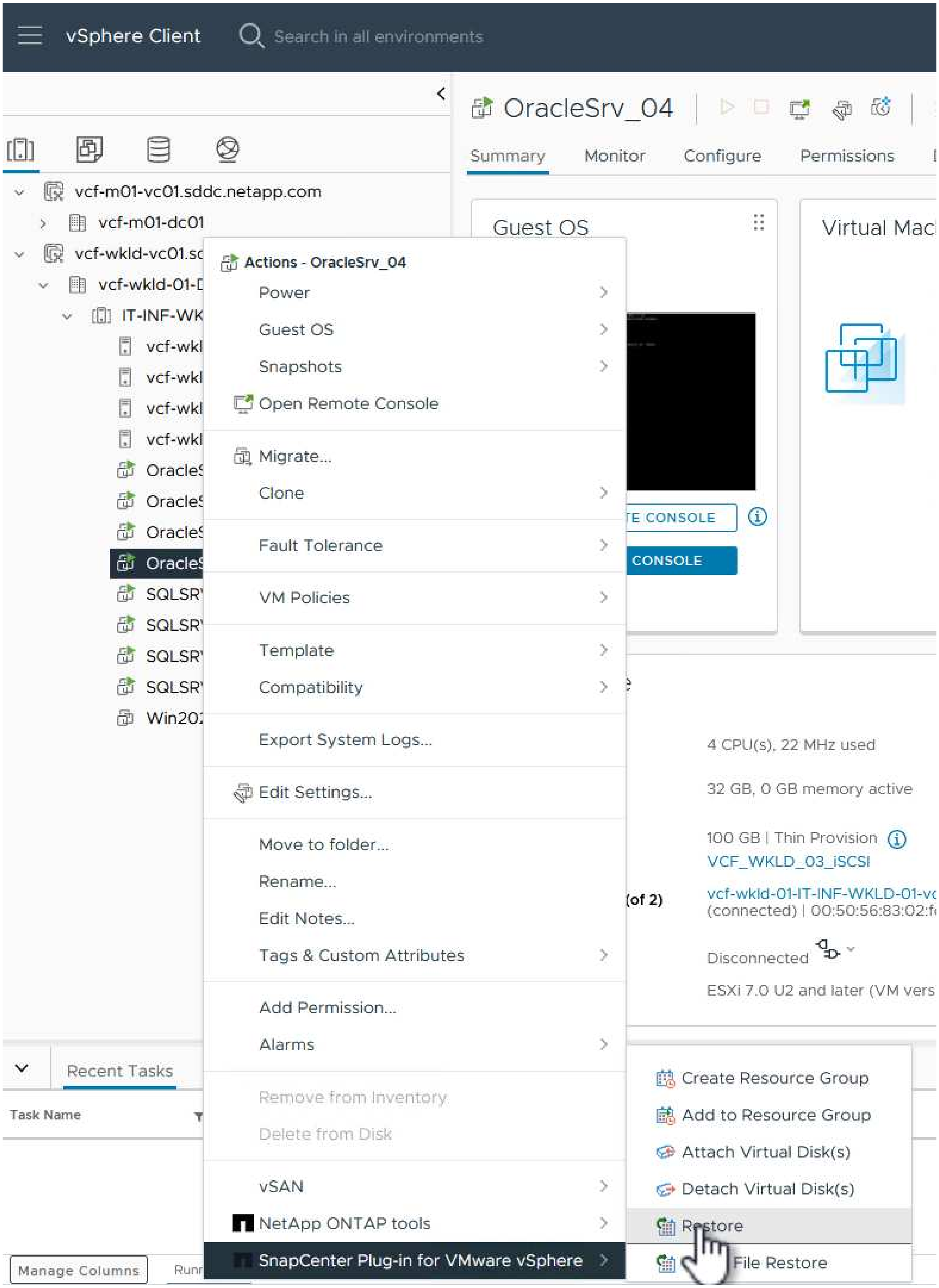
Individual files and folders in a guest file restore session can be restored, which attaches a backup copy of a virtual disk and then restores the selected files or folders.

Complete the following steps to restore VMs, VMDKs or individual folders.

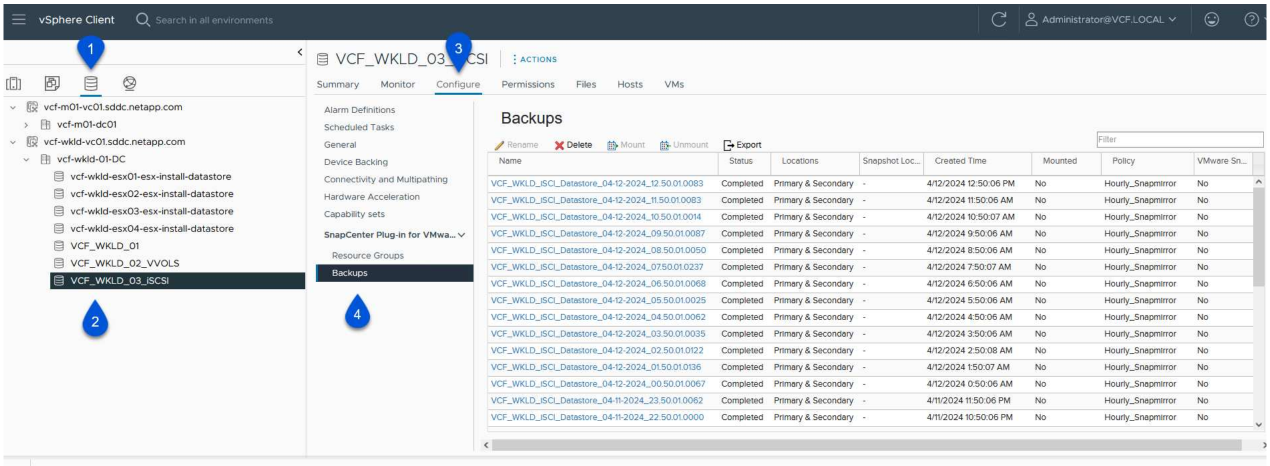
Restore VMs using SnapCenter Plug-in

Complete the following steps to restore a VM with SCV:

1. Navigate to the VM to be restored in the vSphere client, right click and navigate to **SnapCenter Plug-in for VMware vSphere**. Select **Restore** from the sub-menu.


vSphere Client
Search in all environments
vcf-m01-vc01.sddc.netapp.com
vcf-m01-dc01
vcf-wkld-vc01.sc
vcf-wkld-01-D
IT-INF-WK
vcf-wkl
vcf-wkl
vcf-wkl
vcf-wkl
OracleS
OracleS
OracleS
OracleS
SQLSR
SQLSR
SQLSR
SQLSR
Win20
OracleSrv_04
Summary
Monitor
Configure
Permissions
Guest OS
Virtual Mac
TE CONSOLE
CONSOLE
Actions - OracleSrv_04
Power
Guest OS
Snapshots
Open Remote Console
Migrate...
Clone
Fault Tolerance
VM Policies
Template
Compatibility
Export System Logs...
Edit Settings...
Move to folder...
Rename...
Edit Notes...
Tags & Custom Attributes
Add Permission...
Alarms
Remove from Inventory
Delete from Disk
vSAN
NetApp ONTAP tools
SnapCenter Plug-in for VMware vSphere
Create Resource Group
Add to Resource Group
Attach Virtual Disk(s)
Detach Virtual Disk(s)
Restore
File Restore
4 CPU(s), 22 MHz used
32 GB, 0 GB memory active
100 GB | Thin Provision
VCF_WKLD_03_iSCSI
(of 2)
vcf-wkld-01-IT-INF-WKLD-01-vc
(connected) | 00:50:56:83:02:f
Disconnected
ESXi 7.0 U2 and later (VM vers
Recent Tasks
Task Name
Manage Columns
Runr

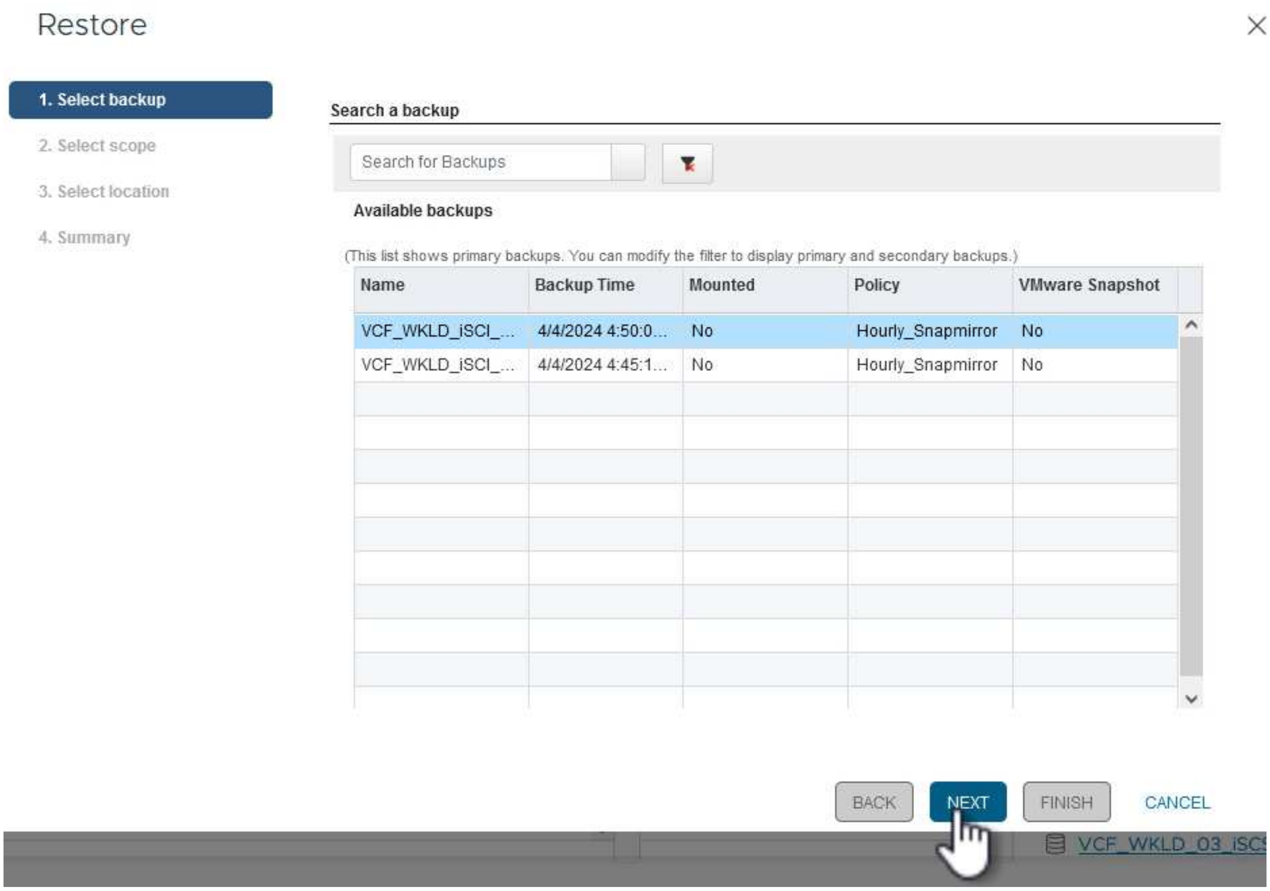
An alternative is to navigate to the datastore in inventory and then under the **Configure** tab go to **SnapCenter Plug-in for VMware vSphere > Backups**. From the chosen backup, select the VMs to be restored.



Backups

Name	Status	Locations	Snapshot Loc...	Created Time	Mounted	Policy	VMware Sn...
VCF_WKLD_iSCI_Datastore_04-12-2024_12.50.01.0083	Completed	Primary & Secondary	-	4/12/2024 12:50:06 PM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_11.50.01.0083	Completed	Primary & Secondary	-	4/12/2024 11:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_10.50.01.0014	Completed	Primary & Secondary	-	4/12/2024 10:50:07 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_09.50.01.0087	Completed	Primary & Secondary	-	4/12/2024 9:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_08.50.01.0050	Completed	Primary & Secondary	-	4/12/2024 8:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_07.50.01.0237	Completed	Primary & Secondary	-	4/12/2024 7:50:07 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_06.50.01.0068	Completed	Primary & Secondary	-	4/12/2024 6:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_05.50.01.0025	Completed	Primary & Secondary	-	4/12/2024 5:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_04.50.01.0062	Completed	Primary & Secondary	-	4/12/2024 4:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_03.50.01.0035	Completed	Primary & Secondary	-	4/12/2024 3:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_02.50.01.0122	Completed	Primary & Secondary	-	4/12/2024 2:50:08 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_01.50.01.0136	Completed	Primary & Secondary	-	4/12/2024 1:50:07 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_00.50.01.0067	Completed	Primary & Secondary	-	4/12/2024 0:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-11-2024_23.50.01.0062	Completed	Primary & Secondary	-	4/11/2024 11:50:06 PM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-11-2024_22.50.01.0000	Completed	Primary & Secondary	-	4/11/2024 10:50:06 PM	No	Hourly_Snapmirror	No

2. In the **Restore** wizard select the backup to be used. Click on **Next** to continue.



Search a backup

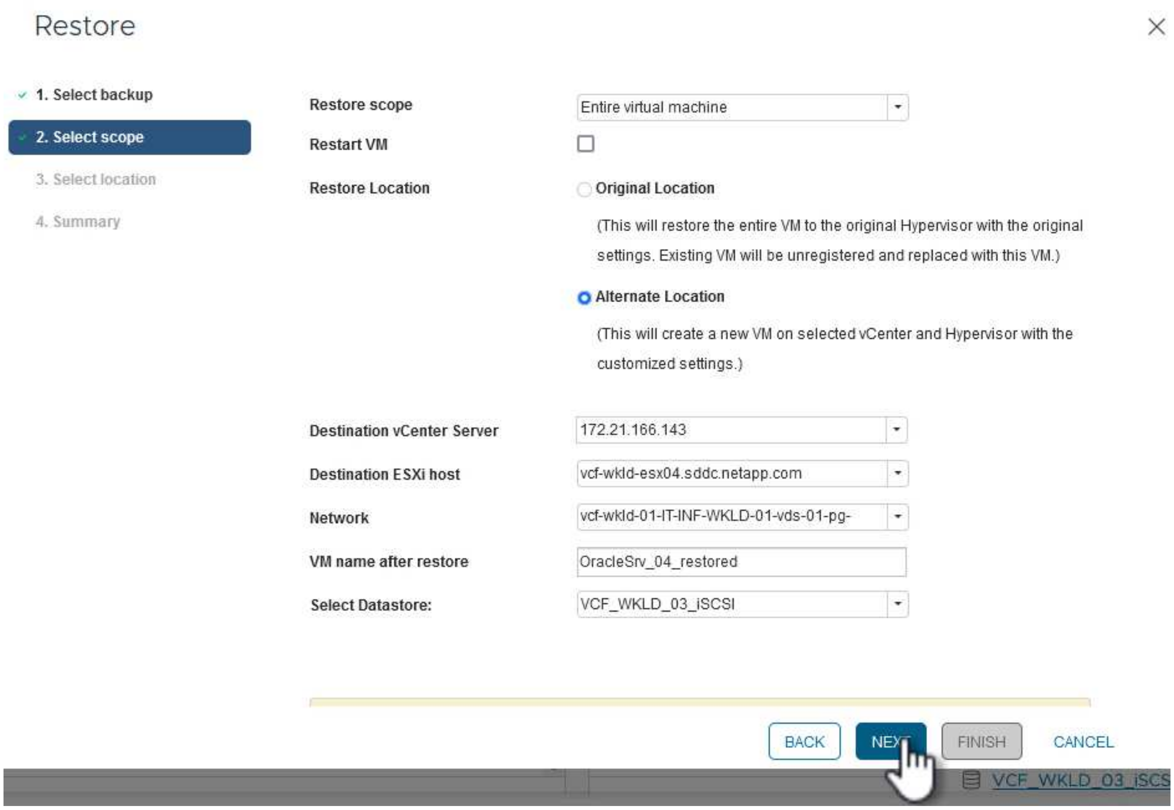
Available backups

(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF_WKLD_iSCI_...	4/4/2024 4:50:0...	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_...	4/4/2024 4:45:1...	No	Hourly_Snapmirror	No

3. On the **Select scope** page fill out all required fields:

- **Restore scope** - Select to restore the entire virtual machine.
- **Restart VM** - Choose whether to start the VM after the restore.
- **Restore Location** - Choose to restore to the orginal location or to an alternate location. When choosing alternate location select the options from each of the fields:
  - **Destination vCenter Server** - local vCenter or alternate vCenter in linked mode
  - **Destination ESXi host**
  - **Network**
  - **VM name after restore**
  - **Select datastore:**



Restore

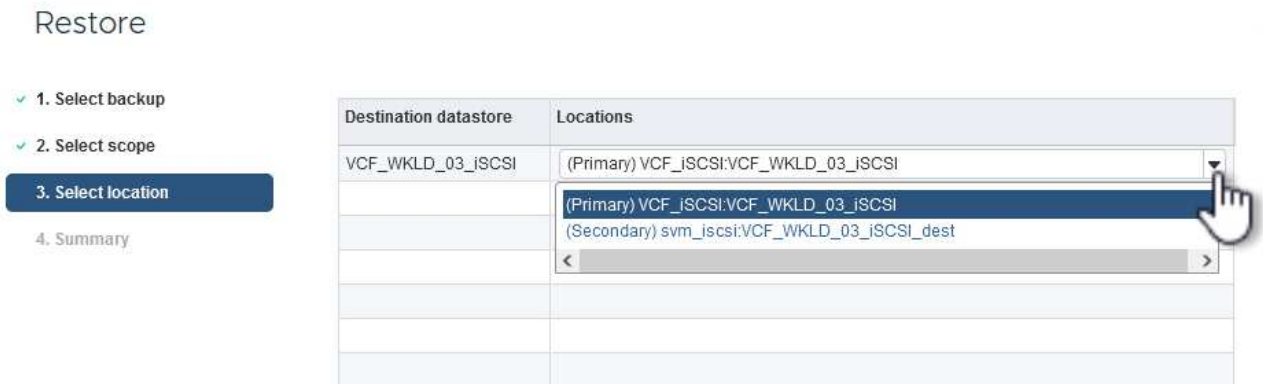
✓ 1. Select backup
✓ 2. Select scope
3. Select location
4. Summary

Restore scope: Entire virtual machine
Restart VM: □
Restore Location:
○ Original Location
(This will restore the entire VM to the original Hypervisor with the original settings. Existing VM will be unregistered and replaced with this VM.)
● Alternate Location
(This will create a new VM on selected vCenter and Hypervisor with the customized settings.)

Destination vCenter Server: 172.21.166.143
Destination ESXi host: vcf-wkld-esx04.sddc.netapp.com
Network: vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-
VM name after restore: OracleSrv_04_restored
Select Datastore: VCF_WKLD_03_iSCSI

Click on **Next** to continue.

4. On the **Select location** page, choose to restore the VM from the primary or secondary ONTAP storage system. Click on **Next** to continue.



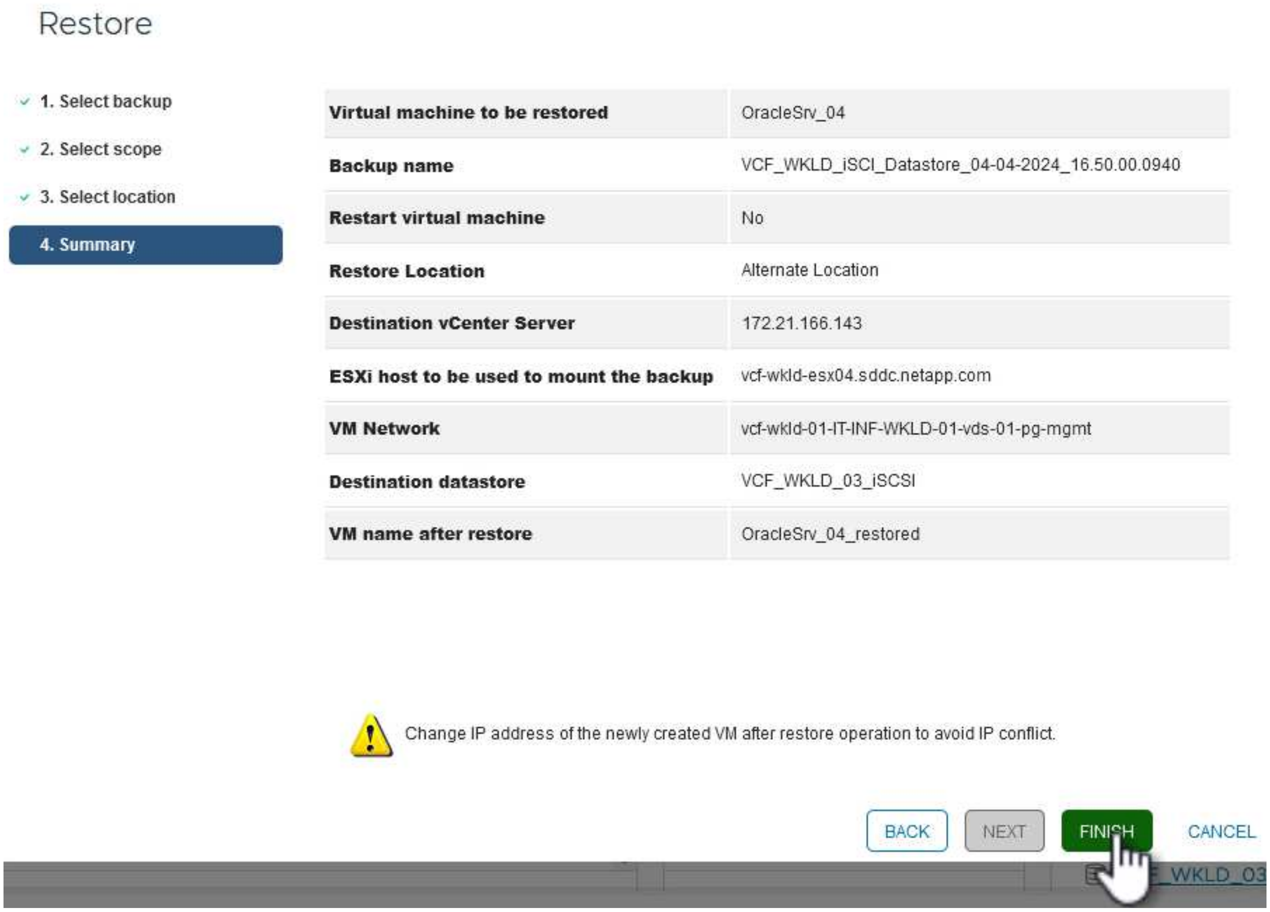
Restore

- ✓ 1. Select backup
- ✓ 2. Select scope
- 3. Select location
- 4. Summary

Destination datastore	Locations
VCF_WKLD_03_iSCSI	(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI

(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI
(Secondary) svm_iscsi:VCF_WKLD_03_iSCSI_dest

5. Finally, review the **Summary** and click on **Finish** to start the restore job.



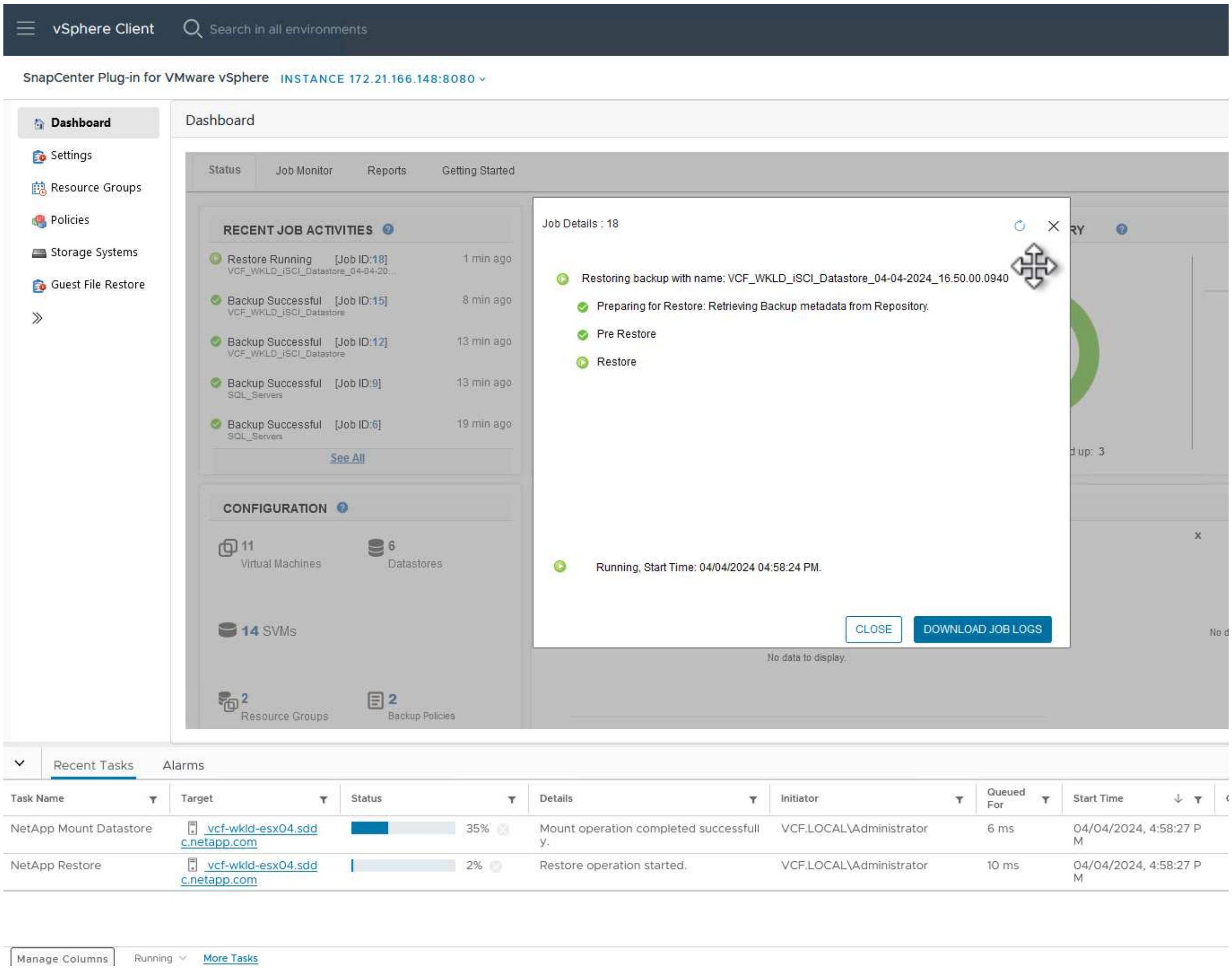
Restore

- ✓ 1. Select backup
- ✓ 2. Select scope
- ✓ 3. Select location
- 4. Summary

Virtual machine to be restored	OracleSrv_04
Backup name	VCF_WKLD_iSCI_Datastore_04-04-2024_16.50.00.0940
Restart virtual machine	No
Restore Location	Alternate Location
Destination vCenter Server	172.21.166.143
ESXi host to be used to mount the backup	vcf-wkld-esx04.sddc.netapp.com
VM Network	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt
Destination datastore	VCF_WKLD_03_iSCSI
VM name after restore	OracleSrv_04_restored

Change IP address of the newly created VM after restore operation to avoid IP conflict.

6. The restore job progress can be monitored from the **Recent Tasks** pane in the vSphere Client and from the job monitor in SCV.



Job Details : 18

- Restoring backup with name: VCF_WKLD_iSCI_Datastore_04-04-2024_16.50.00.0940
  - Preparing for Restore: Retrieving Backup metadata from Repository.
  - Pre Restore
  - Restore

Running, Start Time: 04/04/2024 04:58:24 PM.

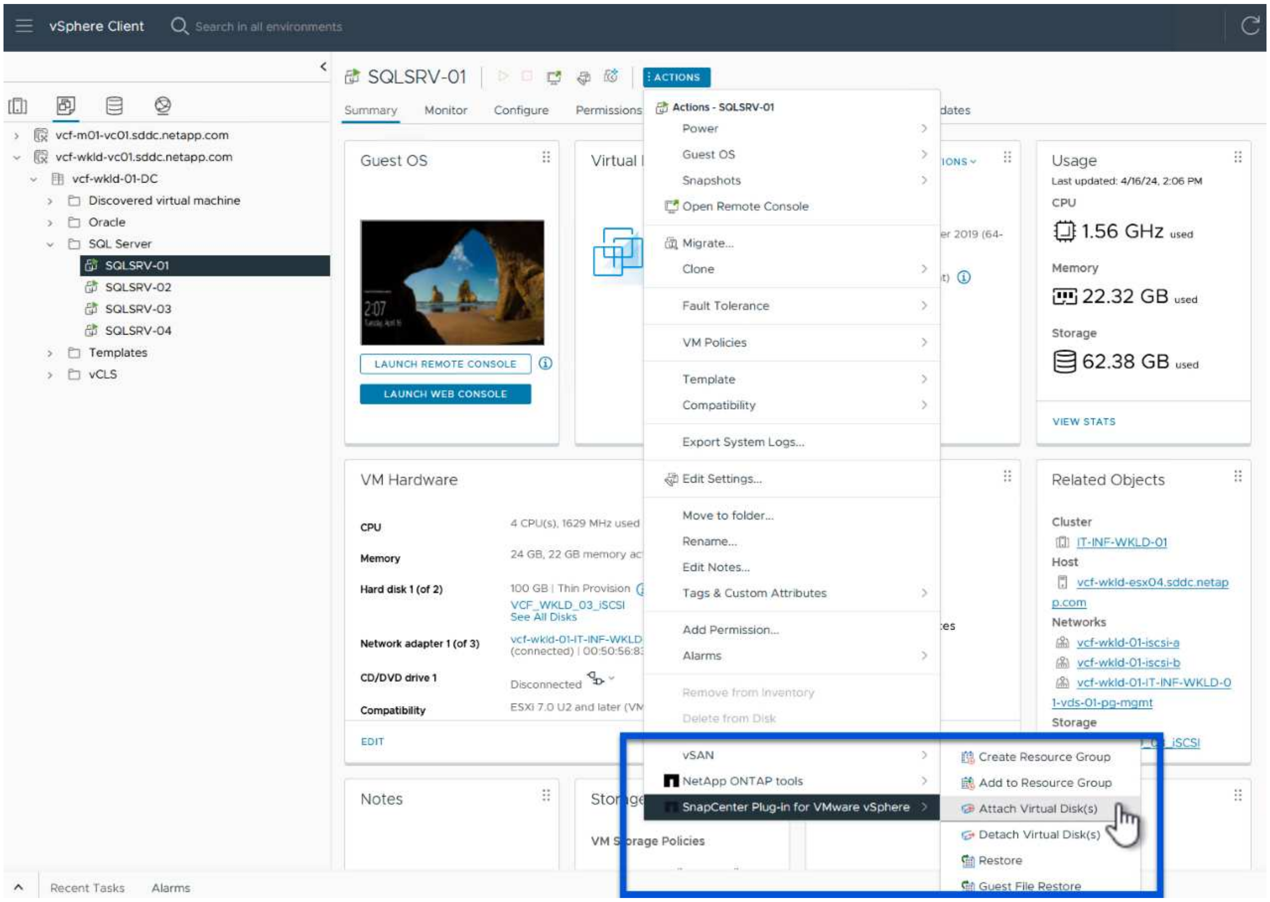
Task Name	Target	Status	Details	Initiator	Queued For	Start Time
NetApp Mount Datastore	vcf-wkld-esx04.sddc.netapp.com	35%	Mount operation completed successfully.	VCF.LOCAL\Administrator	6 ms	04/04/2024, 4:58:27 PM
NetApp Restore	vcf-wkld-esx04.sddc.netapp.com	2%	Restore operation started.	VCF.LOCAL\Administrator	10 ms	04/04/2024, 4:58:27 PM

Restore VMDKs using SnapCenter Plug-in

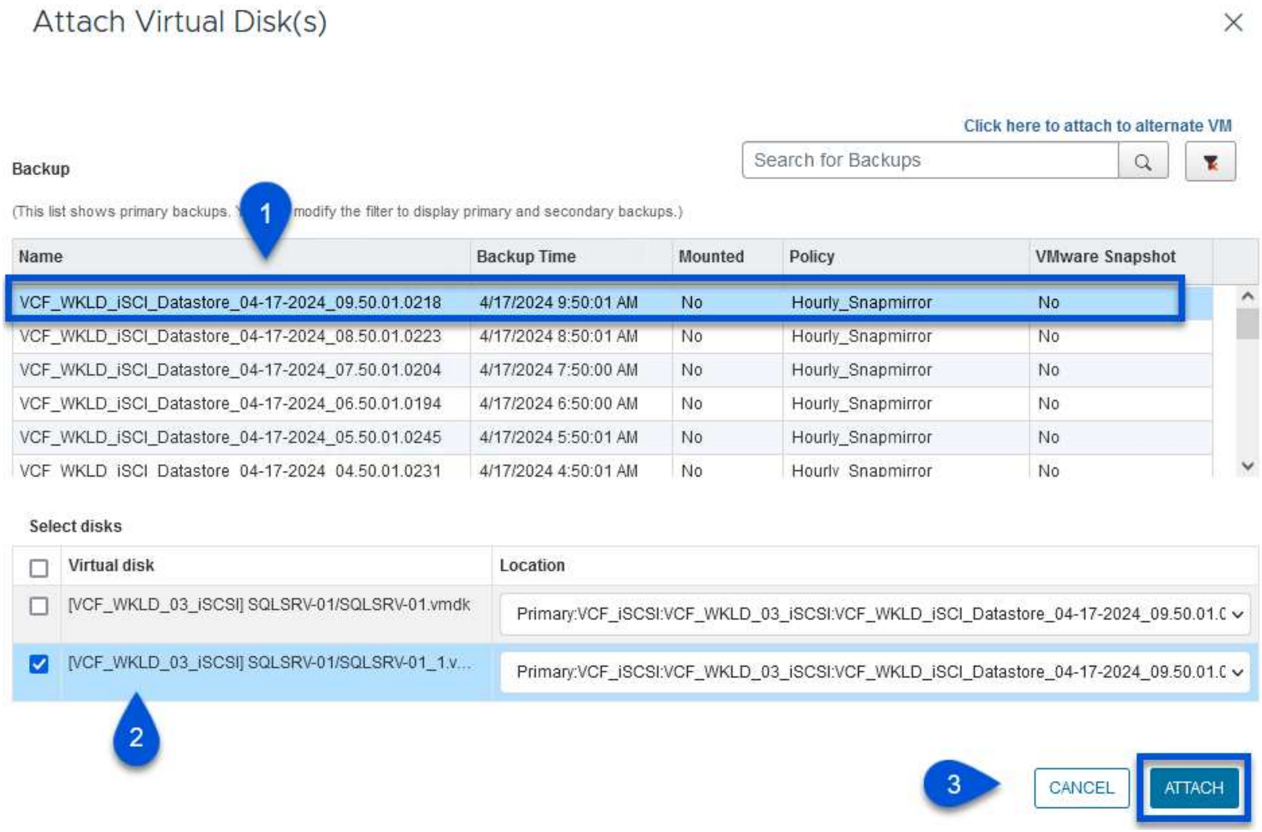
ONTAP Tools allows full restore of VMDK’s to their original location or the ability to attach a VMDK as a new disk to a host system. In this scenario a VMDK will be attached to a Windows host in order to access the file system.

To attach a VMDK from a backup, complete the following steps:

1. In the vSphere Client navigate to a VM and, from the **Actions** menu, select **SnapCenter Plug-in for VMware vSphere > Attach Virtual Disk(s)**.



2. In the **Attach Virtual Disk(s)** wizard, select the backup instance to be used and the particular VMDK to be attached.



Attach Virtual Disk(s)

Click here to attach to alternate VM

Backup

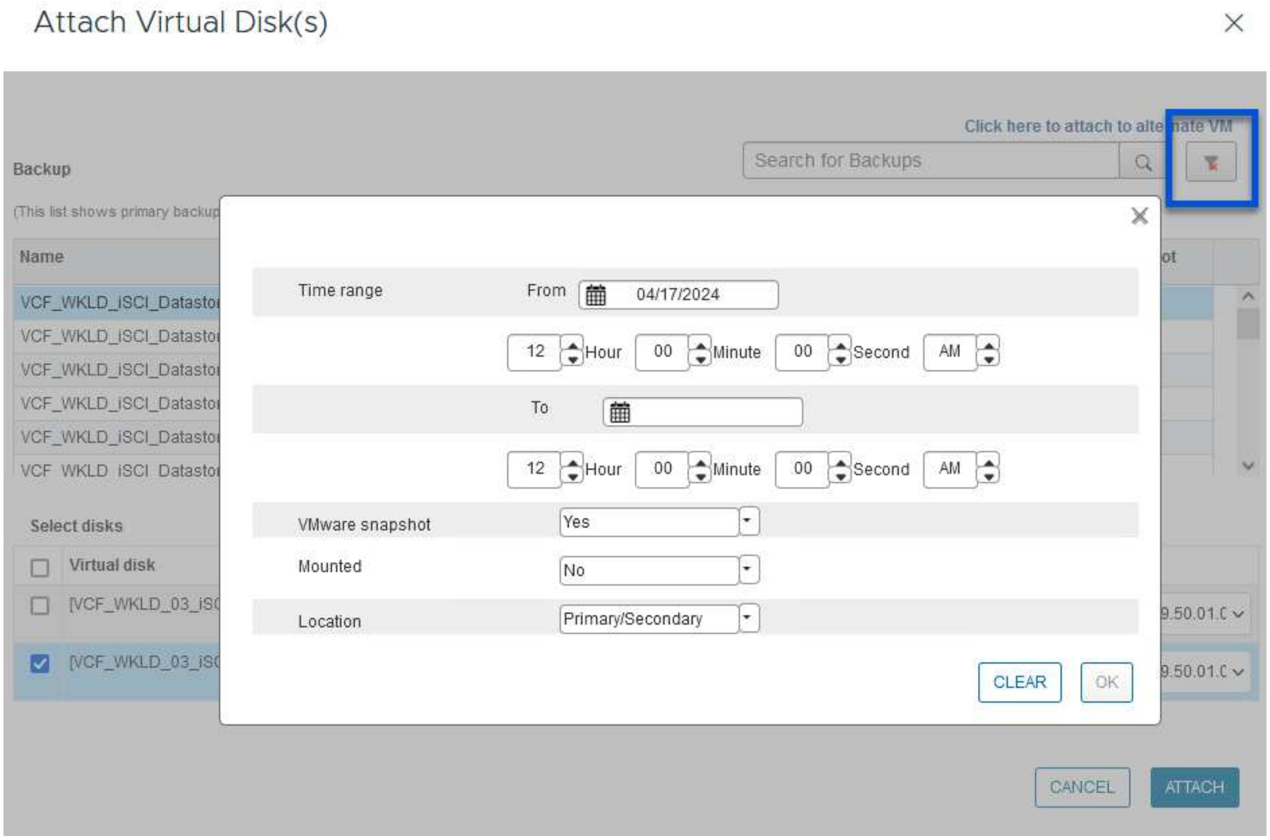
(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF_WKLD_iSCI_Datastore_04-17-2024_09.50.01.0218	4/17/2024 9:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-17-2024_08.50.01.0223	4/17/2024 8:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-17-2024_07.50.01.0204	4/17/2024 7:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-17-2024_06.50.01.0194	4/17/2024 6:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-17-2024_05.50.01.0245	4/17/2024 5:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-17-2024_04.50.01.0231	4/17/2024 4:50:01 AM	No	Hourly_Snapmirror	No

Select disks

☐	Virtual disk	Location
☐	[VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCI_Datastore_04-17-2024_09.50.01.0
☑	[VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.v...	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCI_Datastore_04-17-2024_09.50.01.0

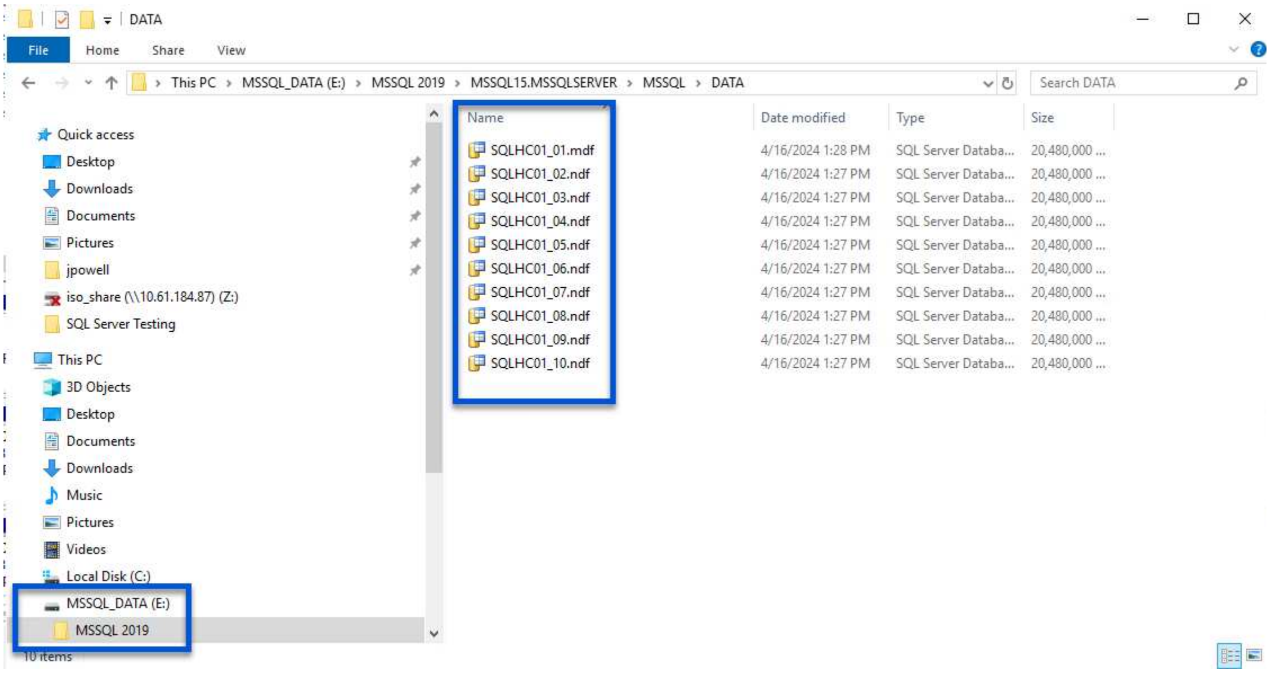
Filter options can be used to locate backups and to display backups from both primary and secondary storage systems.



Attach Virtual Disk(s)

Time range	From	04/17/2024
		12 Hour 00 Minute 00 Second AM
	To	
		12 Hour 00 Minute 00 Second AM
VMware snapshot		Yes
Mounted		No
Location		Primary/Secondary

3. After selecting all options, click on the **Attach** button to begin the restore process and attached the VMDK to the host.
4. Once the attach procedure is complete the disk can be accessed from the OS of the host system. In this case SCV attached the disk with its NTFS file system to the E: drive of our Windows SQL Server and the SQL database files on the file system are accessible through File Explorer.



This PC > MSSQL_DATA (E:) > MSSQL 2019 > MSSQL15.MSSQLSERVER > MSSQL > DATA

Name	Date modified	Type	Size
SQLHC01_01.mdf	4/16/2024 1:28 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_02.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_03.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_04.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_05.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_06.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_07.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_08.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_09.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_10.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...

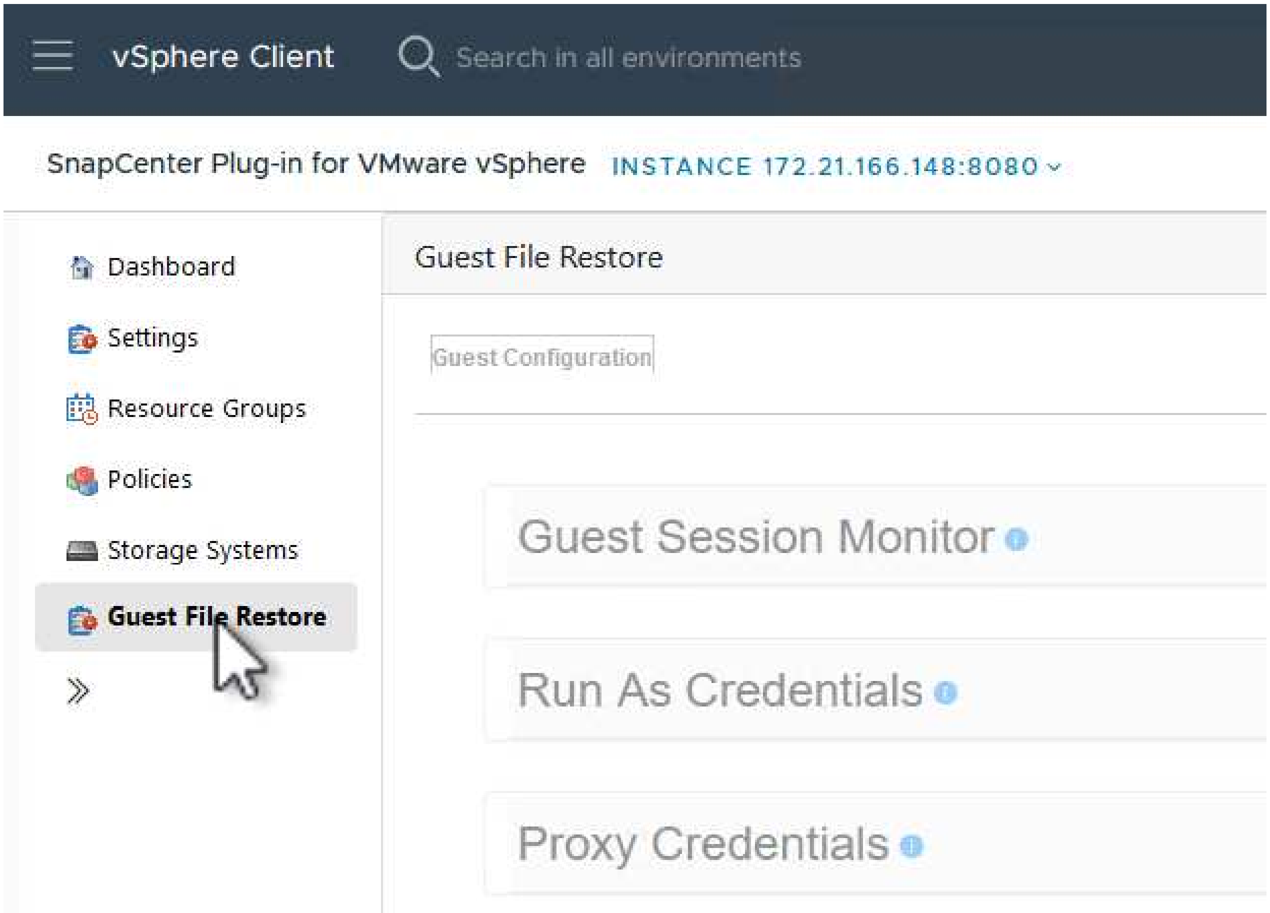
Guest File System Restore using SnapCenter Plug-in

ONTAP Tools features guest file system restores from a VMDK on Windows Server OSes. This is preformed centrally from the SnapCenter Plug-in interface.

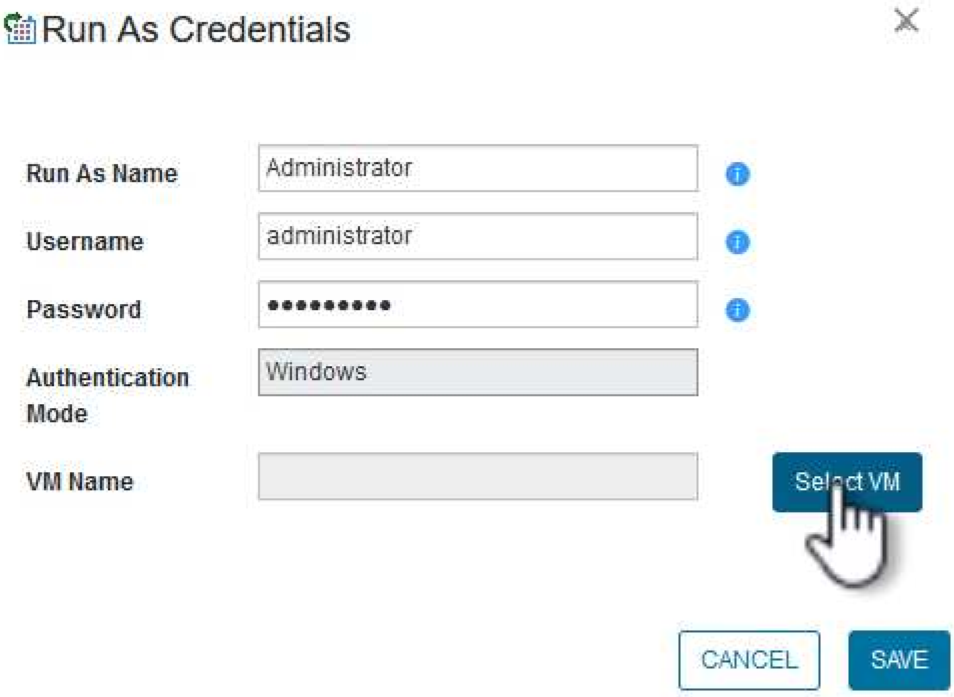
For detailed information refer to Restore guest files and folders at the SCV documentation site.

To perform a guest file system restore for a Windows system, complete the following steps:

1. The first step is to create Run As credentials to provide access to the Windows host system. In the vSphere Client navigate to the CSV plug-in interface and click on **Guest File Restore** in the main menu.



2. Under **Run As Credentials** click on the **+** icon to open the **Run As Credentials** window.
3. Fill in a name for the credentials record, an administrator username and password for the Windows system, and then click on the **Select VM** button to select an optional Proxy VM to be used for the restore.



Run As Credentials

Run As Name: Administrator

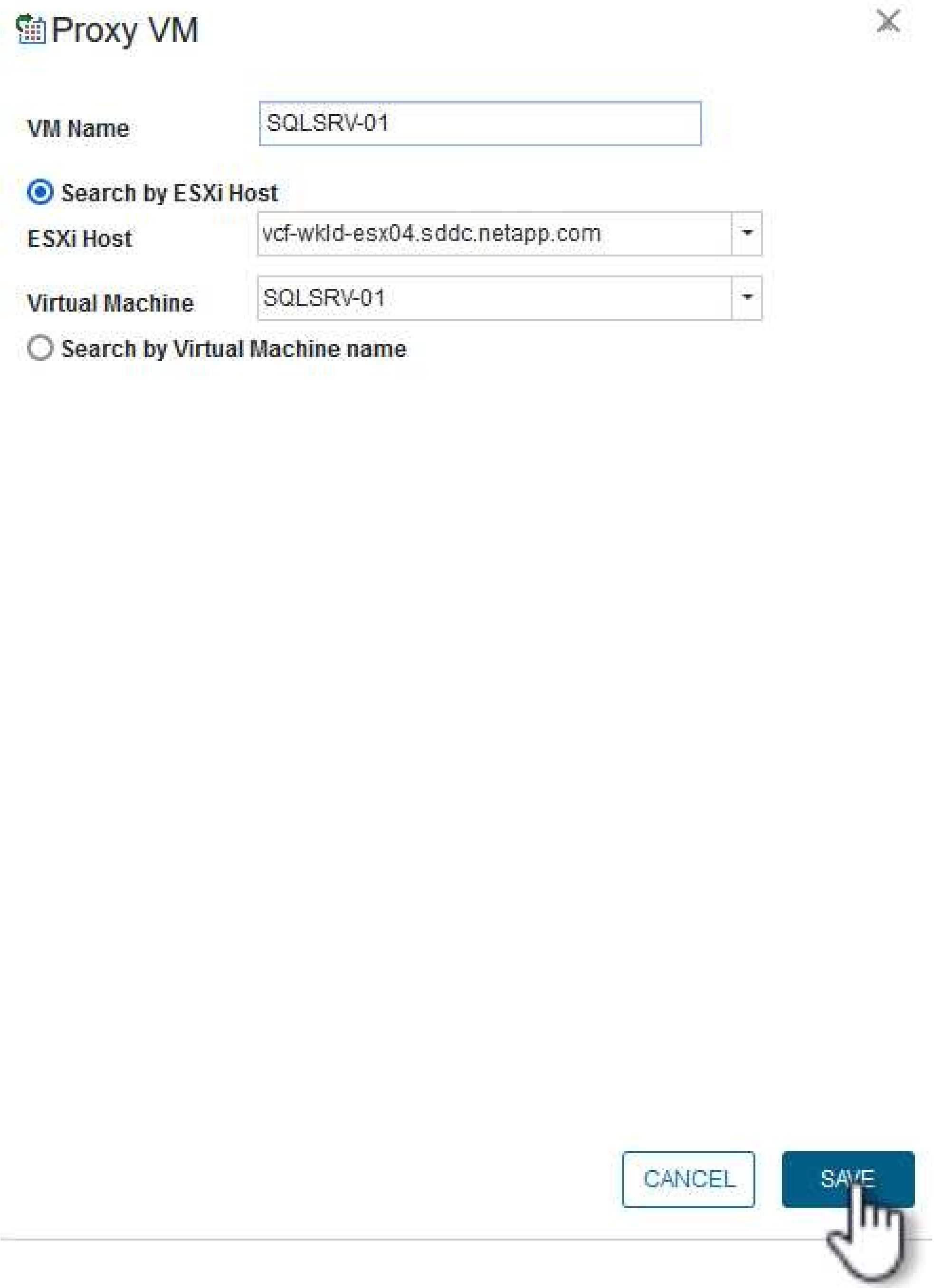
Username: administrator

Password: ●●●●●●●●●●

Authentication Mode: Windows

VM Name:

4. On the Proxy VM page provide a name for the VM and locate it by searching by ESXi host or by name. Once selected, click on **Save**.



VM Name: SQLSRV-01

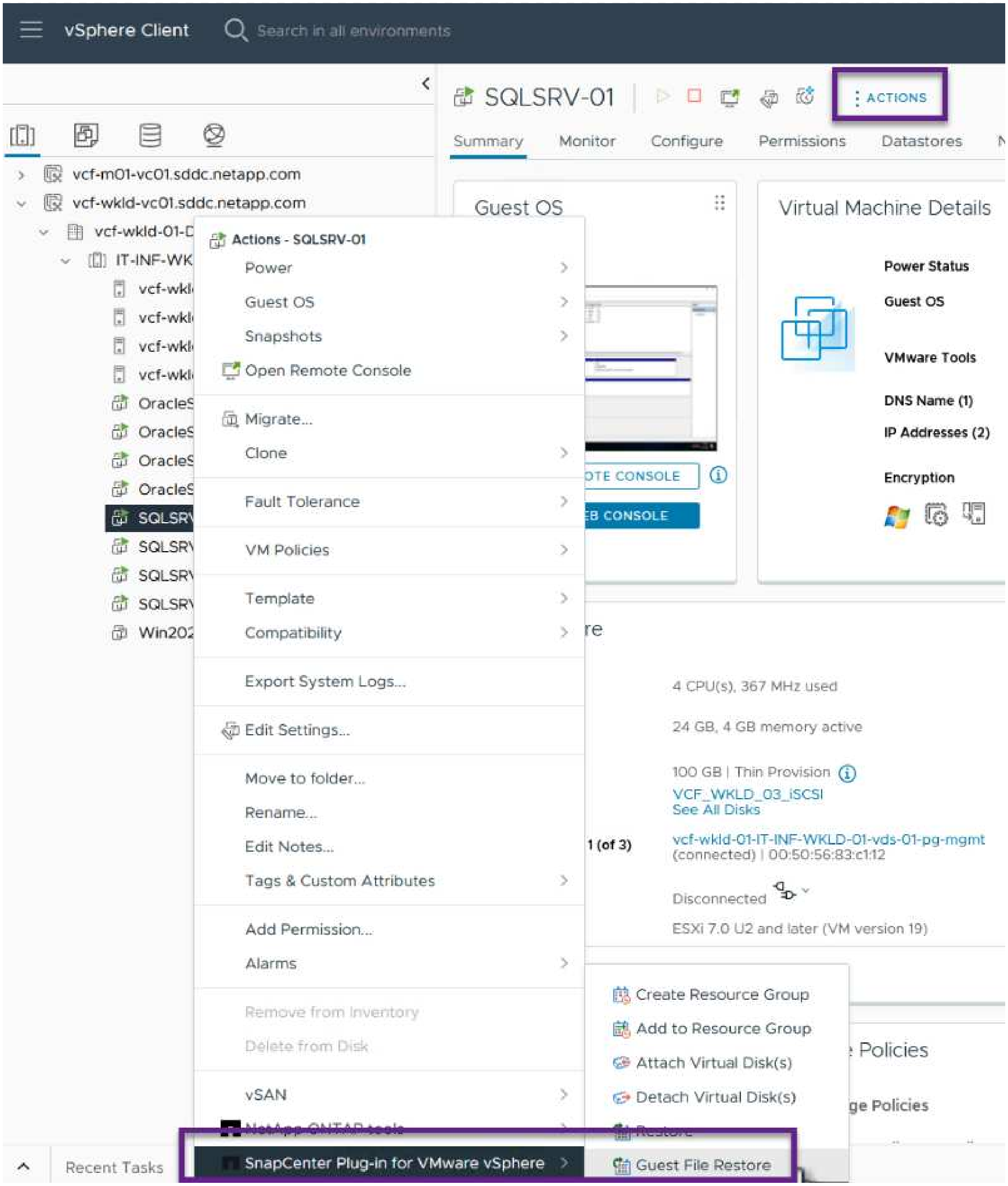
● Search by ESXi Host

ESXi Host: vcf-wkld-esx04.sddc.netapp.com

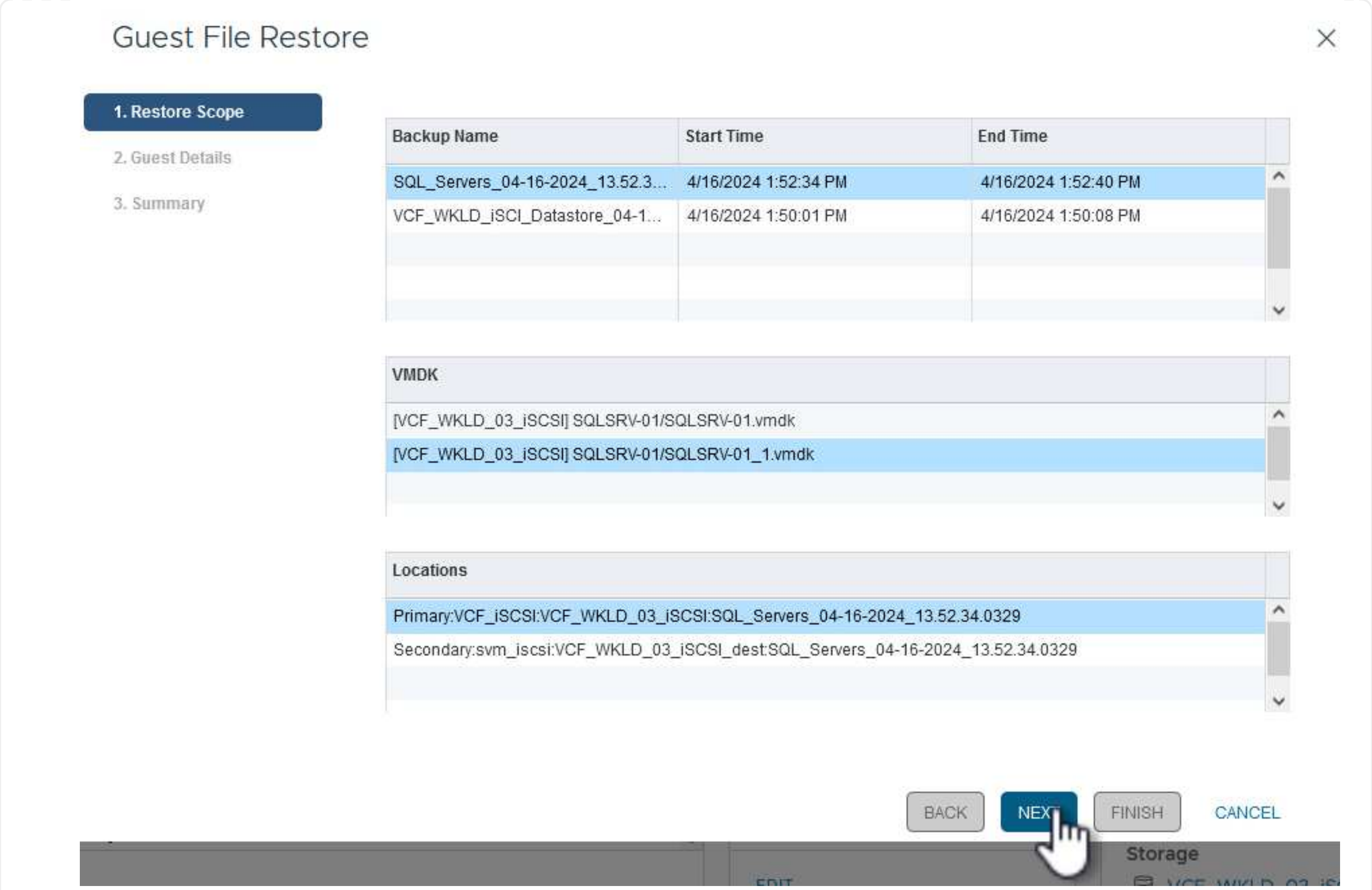
Virtual Machine: SQLSRV-01

○ Search by Virtual Machine name

5. Click on **Save** again in the **Run As Credentials** window to complete saving the record.
6. Next, navigate to a VM in the inventory. From the **Actions** menu, or by right-clicking on the VM, select **SnapCenter Plug-in for VMware vSphere > Guest File Restore**.



7. On the **Restore Scope** page of the **Guest File Restore** wizard, select the backup to restore from, the particular VMDK, and the location (primary or secondary) to restore the VMDK from. Click on **Next** to continue.

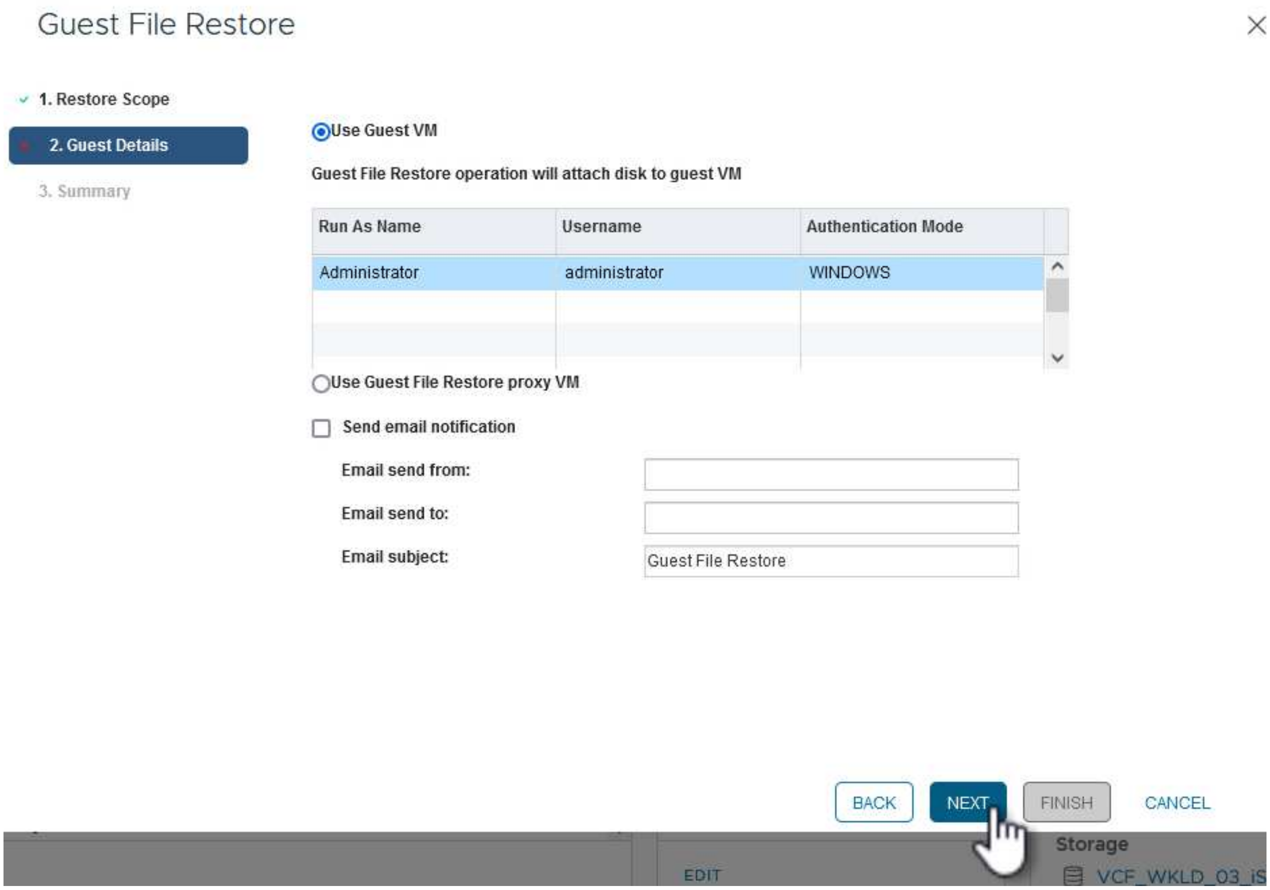


Backup Name	Start Time	End Time
SQL_Servers_04-16-2024_13.52.3...	4/16/2024 1:52:34 PM	4/16/2024 1:52:40 PM
VCF_WKLD_iSCI_Datastore_04-1...	4/16/2024 1:50:01 PM	4/16/2024 1:50:08 PM

VMDK
[VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk
[VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.vmdk

Locations
Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:SQL_Servers_04-16-2024_13.52.34.0329
Secondary:svm_iscsi:VCF_WKLD_03_iSCSI_dest:SQL_Servers_04-16-2024_13.52.34.0329

8. On the **Guest Details** page, select to use **Guest VM** or **Use Gues File Restore proxy VM** for the restore. Also, fill out email notification settings here if desired. Click on **Next** to continue.



Guest File Restore

● Use Guest VM

Guest File Restore operation will attach disk to guest VM

Run As Name	Username	Authentication Mode
Administrator	administrator	WINDOWS

○ Use Guest File Restore proxy VM

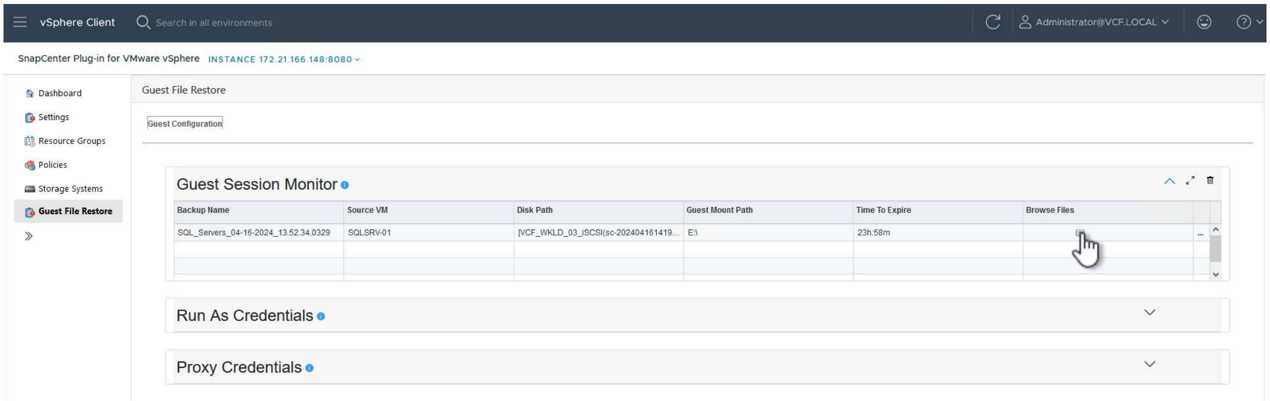
□ Send email notification

Email send from:

Email send to:

Email subject: Guest File Restore

9. Finally, review the **Summary** page and click on **Finish** to begin the Guest File System Restore session.
10. Back in the SnapCenter Plug-in interface, navigate to **Guest File Restore** again and view the running session under **Guest Session Monitor**. Click on the icon under **Browse Files** to continue.

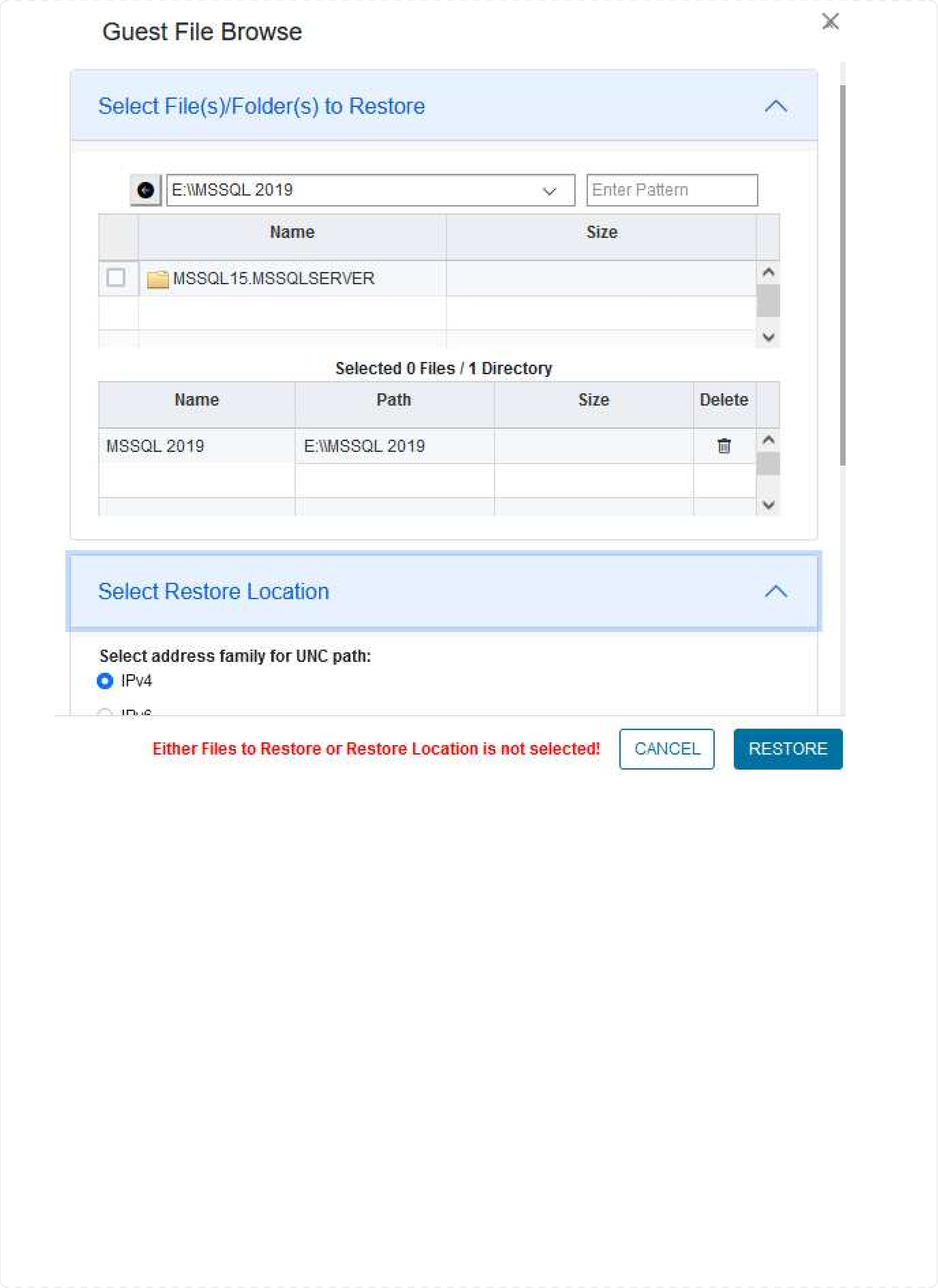


Guest File Restore

Guest Session Monitor

Backup Name	Source VM	Disk Path	Guest Mount Path	Time To Expire	Browse Files
SQL_Servers_04-16-2024_13.52.34.0329	SQLSRV-01	[VCF_WKLD_03_iSCSI(sc-202404161419...	E:\	23h:58m	

11. In the **Guest File Browse** wizard select the folder or files to restore and the file system location to restore them to. Finally, click on **Restore** to start the **Restore** process.



Guest File Browse

Select File(s)/Folder(s) to Restore

E:\\MSSQL 2019

Enter Pattern

	Name	Size
□	MSSQL15.MSSQLSERVER	

Selected 0 Files / 1 Directory

Name	Path	Size	Delete
MSSQL 2019	E:\\MSSQL 2019		🗑

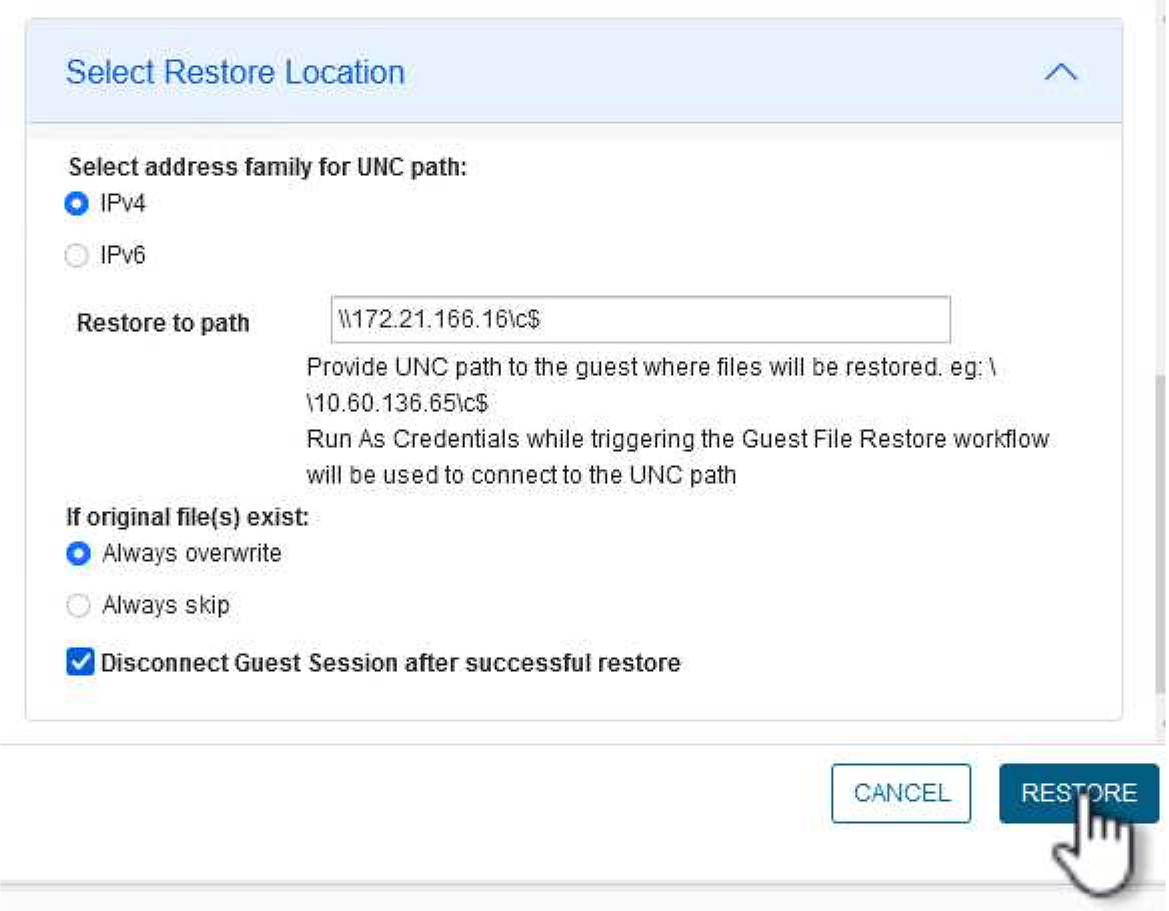
Select Restore Location

Select address family for UNC path:

● IPv4

○ IPv6

Either Files to Restore or Restore Location is not selected!



Select Restore Location

Select address family for UNC path:

● IPv4

○ IPv6

Restore to path: \\172.21.166.16\c$

Provide UNC path to the guest where files will be restored. eg: \\10.60.136.65\c$
Run As Credentials while triggering the Guest File Restore workflow will be used to connect to the UNC path

If original file(s) exist:

● Always overwrite

○ Always skip

☑ Disconnect Guest Session after successful restore

12. The restore job can be monitored from the vSphere Client task pane.

Additional information

For information on configuring VCF refer to VMware Cloud Foundation Documentation.

For information on configuring ONTAP storage systems refer to the ONTAP 9 Documentation center.

For information on using the SnapCenter Plug-in for VMware vSphere refer to the SnapCenter Plug-in for VMware vSphere documentation.

VMware Cloud Foundation with NetApp AFF Arrays

VMware Cloud Foundation (VCF) is an integrated software defined data center (SDDC) platform that provides a complete stack of software-defined infrastructure for running enterprise applications in a hybrid cloud environment. It combines compute, storage, networking, and management capabilities into a unified platform, offering a consistent operational experience across private and public clouds.

Author: Josh Powell, Ravi BCB

This document provides information on storage options available for VMware Cloud Foundation using the NetApp All-Flash AFF storage system. Supported storage options are covered with specific instruction for creating workload domains with NFS and vVol datastores as principal storage as well as a range of supplemental storage options.

Use Cases

Use cases covered in this documentation:

- Storage options for customers seeking uniform environments across both private and public clouds.
- Automated solution for deploying virtual infrastructure for workload domains.
- Scalable storage solution tailored to meet evolving needs, even when not aligned directly with compute resource requirements.
- Deploy VCF VI Workload Domains using ONTAP as principal storage.
- Deploy supplemental storage to VI Workload Domains using ONTAP Tools for VMware vSphere.

Audience

This solution is intended for the following people:

- Solution architects looking for more flexible storage options for VMware environments that are designed to maximize TCO.
- Solution architects looking for VCF storage options that provide data protection and disaster recovery options with the major cloud providers.
- Storage administrators wanting to understand how to configure VCF with principal and supplemental storage.

Technology Overview

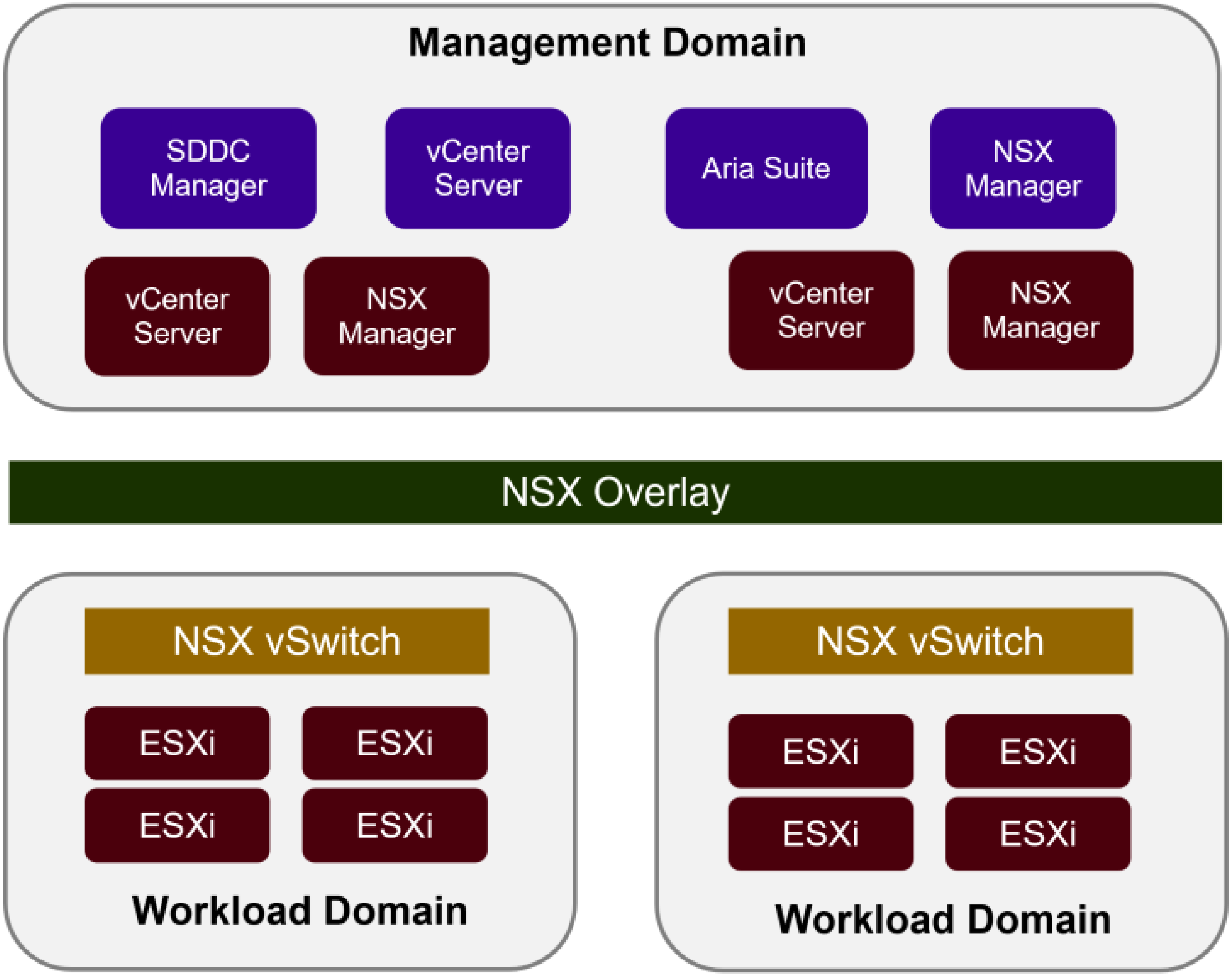
The VCF with NetApp AFF solution is comprised of the following major components:

VMware Cloud Foundation

VMware Cloud Foundation extends VMware’s vSphere hypervisor offerings by combining key components such as SDDC Manager, vSphere, vSAN, NSX, and VMware Aria Suite to create a virtualized datacenter.

The VCF solution supports both native Kubernetes and virtual machine-based workloads. Key services such as VMware vSphere, VMware vSAN, VMware NSX-T Data Center, and VMware vRealize Cloud Management are integral components of the VCF package. When combined, these services establish a software-defined infrastructure capable of efficiently managing compute, storage, networking, security, and cloud management.

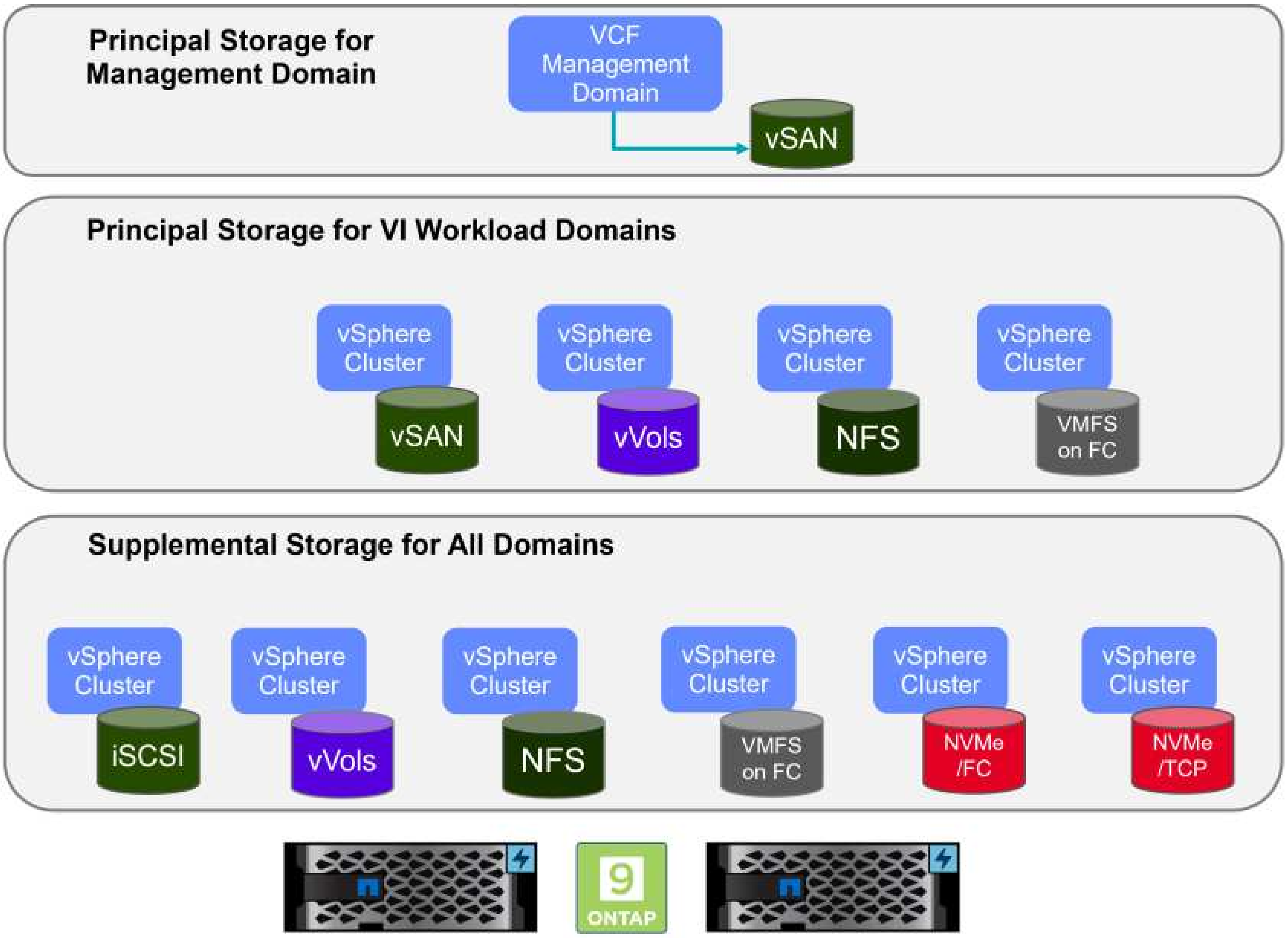
VCF is comprised of a single management domain and up to 24 VI Workload Domains that each represent a unit of application-ready infrastructure. A workload domain is comprised of one or more vSphere clusters managed by a single vCenter instance.



For more information on VCF architecture and planning, refer to Architecture Models and Workload Domain Types in VMware Cloud Foundation.

VCF Storage Options

VMware divides storage options for VCF into **principal** and **supplemental** storage. The VCF Management Domain must use vSAN as its principal storage. However, there are many supplemental storage options for the Management Domain and both principal and supplemental storage options available for VI Workload Domains.



Principal Storage for Workload Domains
Principal Storage refers to any type of storage that can be directly connected to a VI Workload Domain during the setup process within SDDC Manager. Principal storage is the first datastore configured for a Workload Domain and includes vSAN, vVols (VMFS), NFS and VMFS on Fibre Channel.

Supplemental Storage for Management and Workload Domains
Supplemental storage is the storage type that can be added to the management or workload domains at any time after the cluster has been created. Supplemental storage represents the widest range of supported storage options, all of which are supported on NetApp AFF arrays.

Additional documentation resources for VMware Cloud Foundation:
* VMware Cloud Foundation Documentation
* Supported Storage Types for VMware Cloud Foundation
* Managing Storage in VMware Cloud Foundation

NetApp All-Flash Storage Arrays

NetApp AFF (All Flash FAS) arrays are high-performance storage solutions designed to leverage the speed and efficiency of flash technology. AFF arrays incorporate integrated data management features such as snapshot-based backups, replication, thin provisioning, and data protection capabilities.

NetApp AFF arrays utilize the ONTAP storage operating system, offering comprehensive storage protocol support for all storage options compatible with VCF, all within a unified architecture.

NetApp AFF storage arrays are available in the highest performing A-Series and a QLC flash-based C-Series. Both series use NVMe flash drives.

For more information on NetApp AFF A-Series storage arrays see the NetApp AFF A-Series landing page.

For more information on NetApp C-Series storage arrays see the NetApp AFF C-Series landing page.

NetApp ONTAP Tools for VMware vSphere

ONTAP Tools for VMware vSphere (OTV) allows administrators to manage NetApp storage directly from within the vSphere Client. ONTAP Tools allows you to deploy and manage datastores, as well as provision vVol datastores.

ONTAP Tools allows mapping of datastores to storage capability profiles which determine a set of storage system attributes. This allows the creation of datastores with specific attributes such as storage performance and QoS.

ONTAP Tools also includes a **VMware vSphere APIs for Storage Awareness (VASA) Provider** for ONTAP storage systems which enables the provisioning of VMware Virtual Volumes (vVols) datastores, creation and use of storage capability profiles, compliance verification, and performance monitoring.

For more information on NetApp ONTAP tools see the ONTAP tools for VMware vSphere Documentation page.

Solution Overview

In the scenarios presented in this documentation we will demonstrate how to use ONTAP storage systems as principal storage for VCF VI Workload Domain deployments. In addition, we will install and use ONTAP Tools for VMware vSphere to configure supplemental datastores for VI Workload Domains.

Scenarios covered in this documentation:

- **Configure and use an NFS datastore as principal storage during VI Workload Domain deployment.** Click **here** for deployment steps.
- **Install and demonstrate the use of ONTAP Tools to configure and mount NFS datastores as supplemental storage in VI Workload Domains.** Click **here** for deployment steps.

NFS as principal storage for VI Workload Domains

In this scenario we will demonstrate how to configure an NFS datastore as principal storage for the deployment of a VI Workload Domain in VCF. Where appropriate we will refer to external documentation for the steps that must be performed in VCF’s SDDC Manager, and cover those steps that are specific to the storage configuration portion.

Author: Josh Powell, Ravi BCB

Scenario Overview

This scenario covers the following high level steps:

- Verify networking for the ONTAP storage virtual machine (SVM) and that a logical interface (LIF) is present to carry NFS traffic.

- Create an export policy to allow the ESXi hosts access to the NFS volume.
- Create an NFS volume on the ONTAP storage system.
- Create a Network Pool for NFS and vMotion traffic in SDDC Manager.
- Commission hosts in VCF for use in a VI Workload Domain.
- Deploy a VI Workload Domain in VCF using an NFS datastore as principal storage.
- Install NetApp NFS Plug-in for VMware VAAI

Prerequisites

This scenario requires the following components and configurations:

- NetApp AFF storage system with a storage virtual machine (SVM) configured to allow NFS traffic.
- Logical interface (LIF) has been created on the IP network that is to carry NFS traffic and is associated with the SVM.
- VCF management domain deployment is complete and the SDDC Manager interface is accessible.
- 4 x ESXi hosts configured for communication on the VCF management network.
- IP addresses reserved for vMotion and NFS storage traffic on the VLAN or network segment established for this purpose.

> ⓘ When deploying a VI Workload Domain, VCF validates connectivity to the NFS Server. This is done using the management adapter on the ESXi hosts before any additional vmkernel adapter is added with the NFS IP address. Therefore, it is necessary to ensure that either 1) the management network is routable to the NFS Server, or 2) a LIF for the management network has been added to the SVM hosting the NFS datastore volume, to ensure that the validation can proceed.

For information on configuring ONTAP storage systems refer to the ONTAP 9 Documentation center.

For information on configuring VCF refer to VMware Cloud Foundation Documentation.

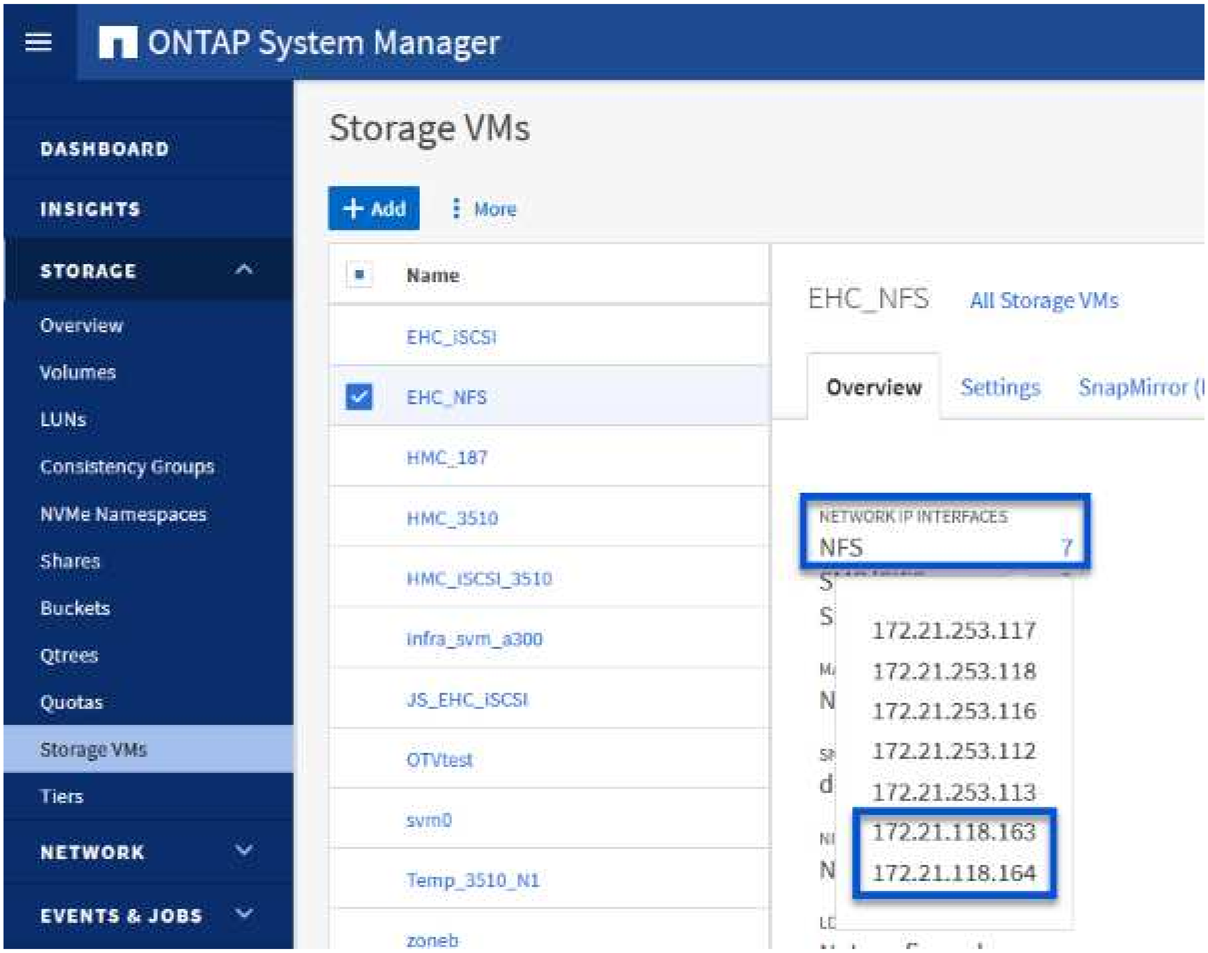
Deployment Steps

To deploy a VI Workload Domain with an NFS datastore as principal storage, complete the following steps:

Verify networking for ONTAP SVM

Verify that the required logical interfaces have been established for the network that will carry NFS traffic between the ONTAP storage cluster and VI Workload Domain.

1. From ONTAP System Manager navigate to **Storage VMs** in the left-hand menu and click on the SVM to be used for NFS traffic. On the **Overview** tab, under **NETWORK IP INTERFACES**, click on the numeric to the right of **NFS**. In the list verify that the required LIF IP addresses are listed.



☐	Name
	EHC_iSCSI
☑	EHC_NFS
	HMC_187
	HMC_3510
	HMC_iSCSI_3510
	infra_svm_a300
	JS_EHC_iSCSI
	OTVtest
	svm0
	Temp_3510_N1
	zoneb

172.21.253.117
172.21.253.118
172.21.253.116
172.21.253.112
172.21.253.113
172.21.118.163
172.21.118.164

Alternately, verify the LIFs associated with an SVM from the ONTAP CLI with the following command:

```
network interface show -vserver <SVM_NAME>
```

1. Verify that the ESXi hosts can communicate to the ONTAP NFS Server. Log into the ESXi host via SSH and ping the SVM LIF:

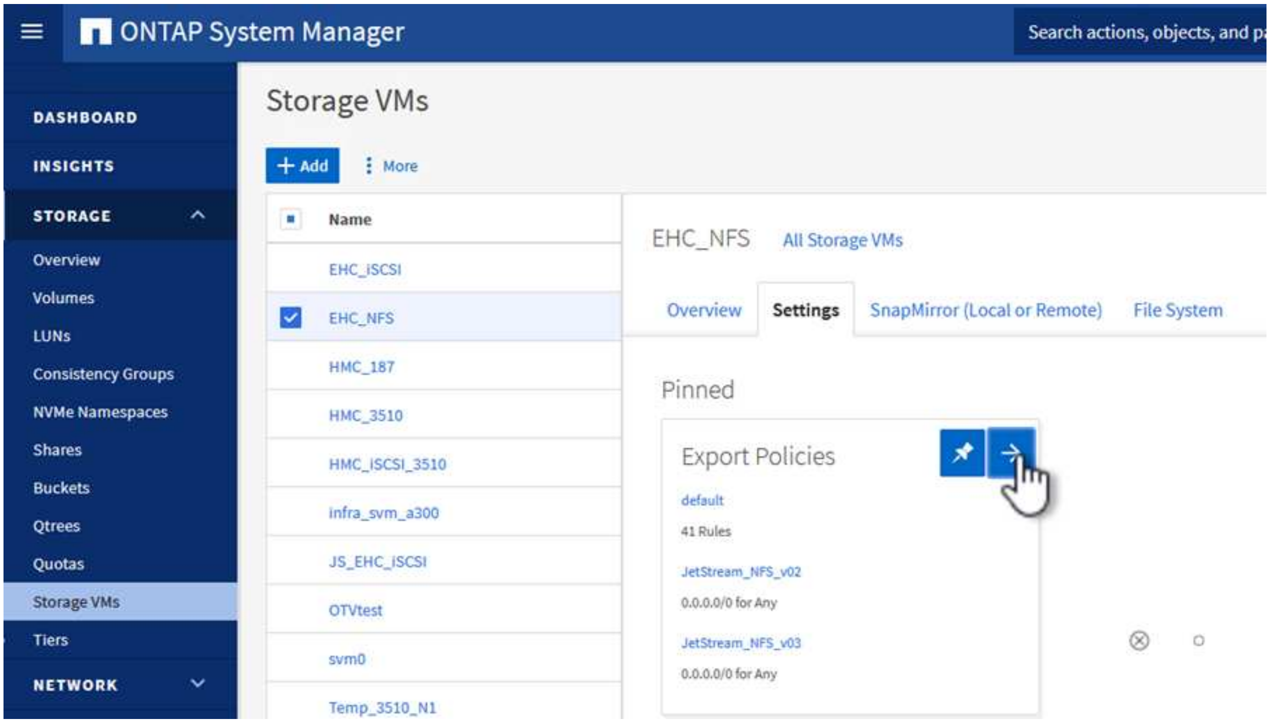
```
vmkping <IP Address>
```

ⓘ When deploying a VI Workload Domain, VCF validates connectivity to the NFS Server. This is done using the management adapter on the ESXi hosts before any additional vmkernel adapter is added with the NFS IP address. Therefore, it is necessary to ensure that either 1) the management network is routable to the NFS Server, or 2) a LIF for the management network has been added to the SVM hosting the NFS datastore volume, to ensure that the validation can proceed.

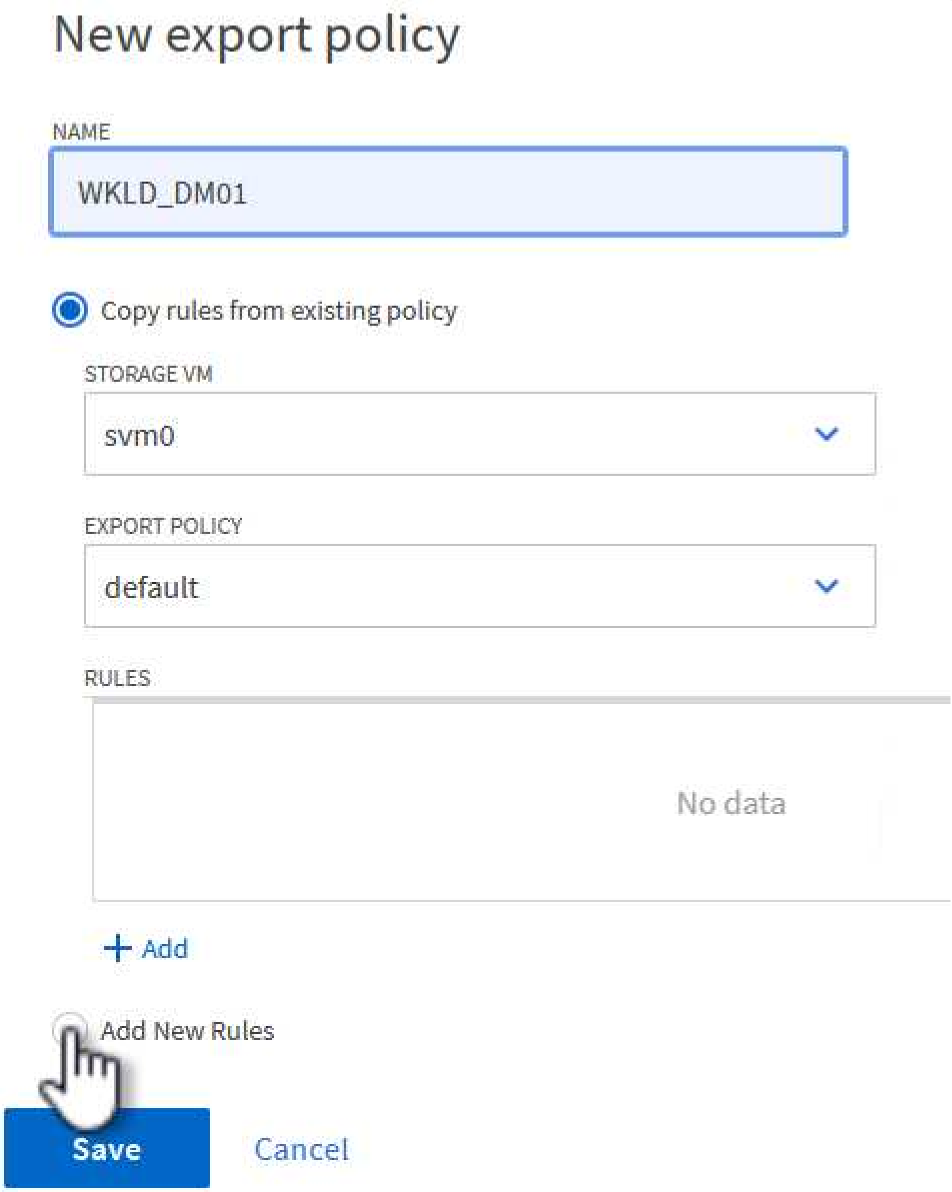
Create Export Policy for sharing NFS volume

Create an export policy in ONTAP System Manager to define access control for NFS volumes.

1. In ONTAP System Manager click on **Storage VMs** in the left-hand menu and select an SVM from the list.
2. On the **Settings** tab locate **Export Policies** and click on the arrow to access.



3. In the **New export policy** window add a name for the policy, click on the **Add new rules** button and then on the **+Add** button to begin adding a new rule.



New export policy

NAME

WKLD_DM01

● Copy rules from existing policy

STORAGE VM

svm0

EXPORT POLICY

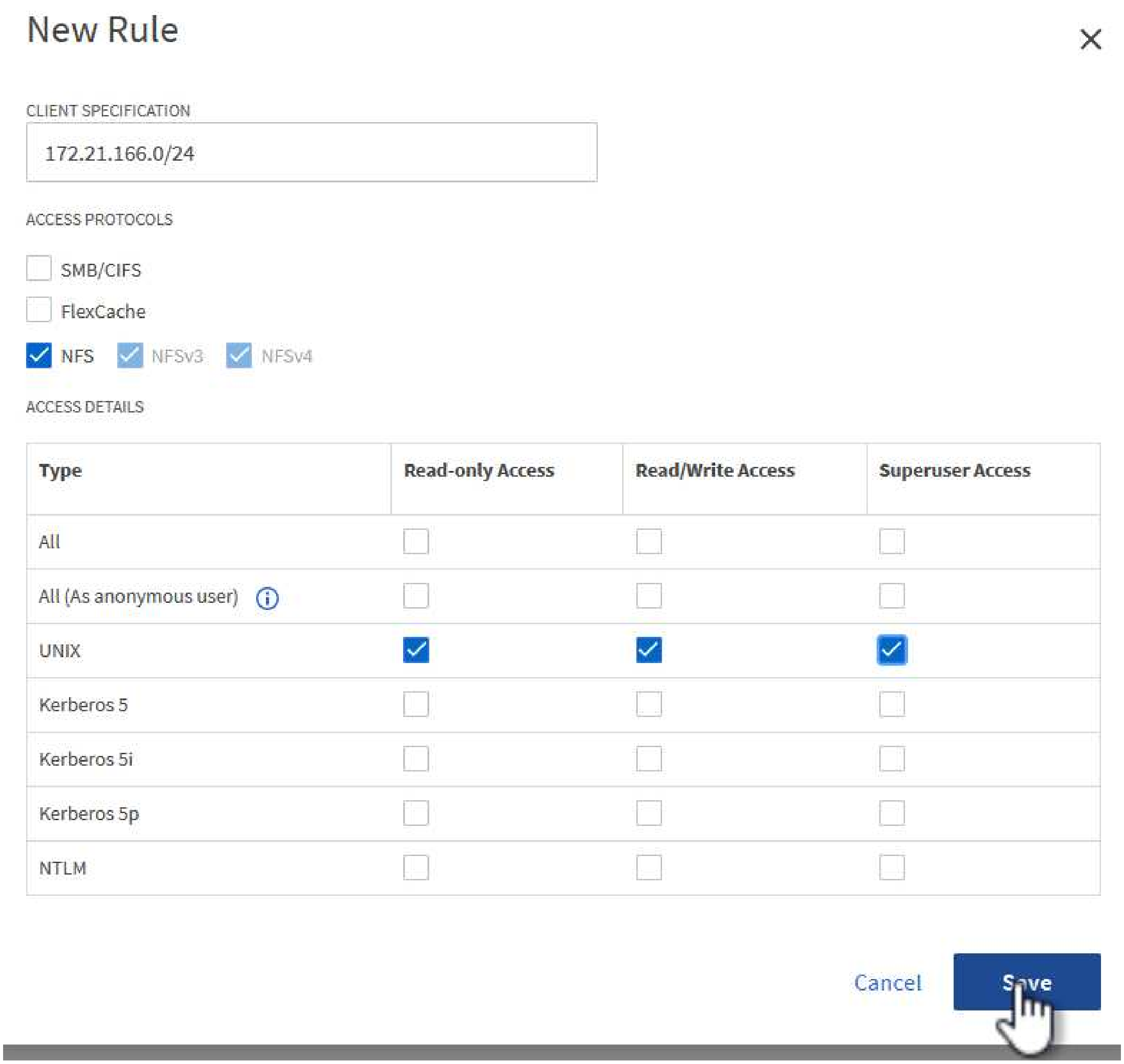
default

RULES

No data

○ Add New Rules

4. Fill in the IP Addresses, IP address range, or network that you wish to include in the rule. Uncheck the **SMB/Cifs** and **FlexCache** boxes and make selections for the access details below. Selecting the UNIX boxes is sufficient for ESXi host access.



New Rule

CLIENT SPECIFICATION

172.21.166.0/24

ACCESS PROTOCOLS

□ SMB/CIFS

□ FlexCache

☑ NFS ☑ NFSv3 ☑ NFSv4

ACCESS DETAILS

Type	Read-only Access	Read/Write Access	Superuser Access
All	□	□	□
All (As anonymous user)	□	□	□
UNIX	☑	☑	☑
Kerberos 5	□	□	□
Kerberos 5i	□	□	□
Kerberos 5p	□	□	□
NTLM	□	□	□

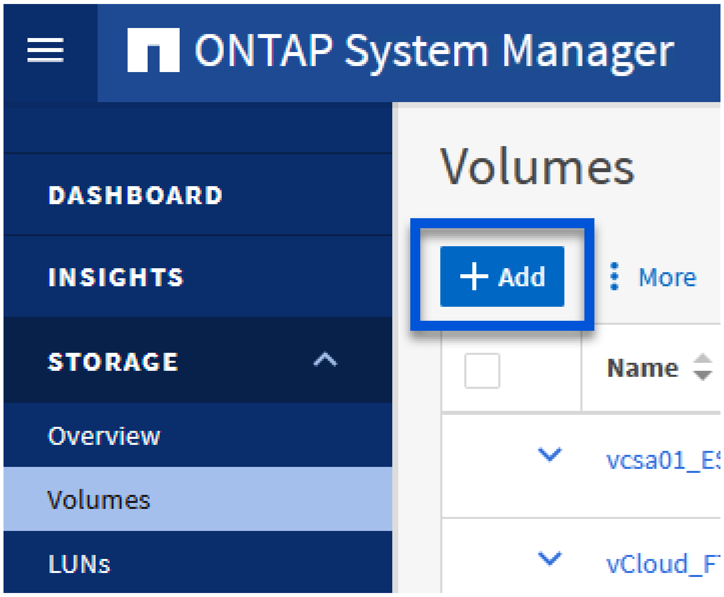
When deploying a VI Workload Domain, VCF validates connectivity to the NFS Server. This is done using the management adapter on the ESXi hosts before any additional vmkernel adapter is added with the NFS IP address. Therefore, it is necessary to ensure that the export policy includes the VCF management network in order to allow the validation to proceed.

5. Once all rules have been entered click on the **Save** button to save the new Export Policy.
6. Alternately, you can create export policies and rules in the ONTAP CLI. Refer to the steps for creating an export policy and adding rules in the ONTAP documentation.
   - Use the ONTAP CLI to Create an export policy.
   - Use the ONTAP CLI to Add a rule to an export policy.

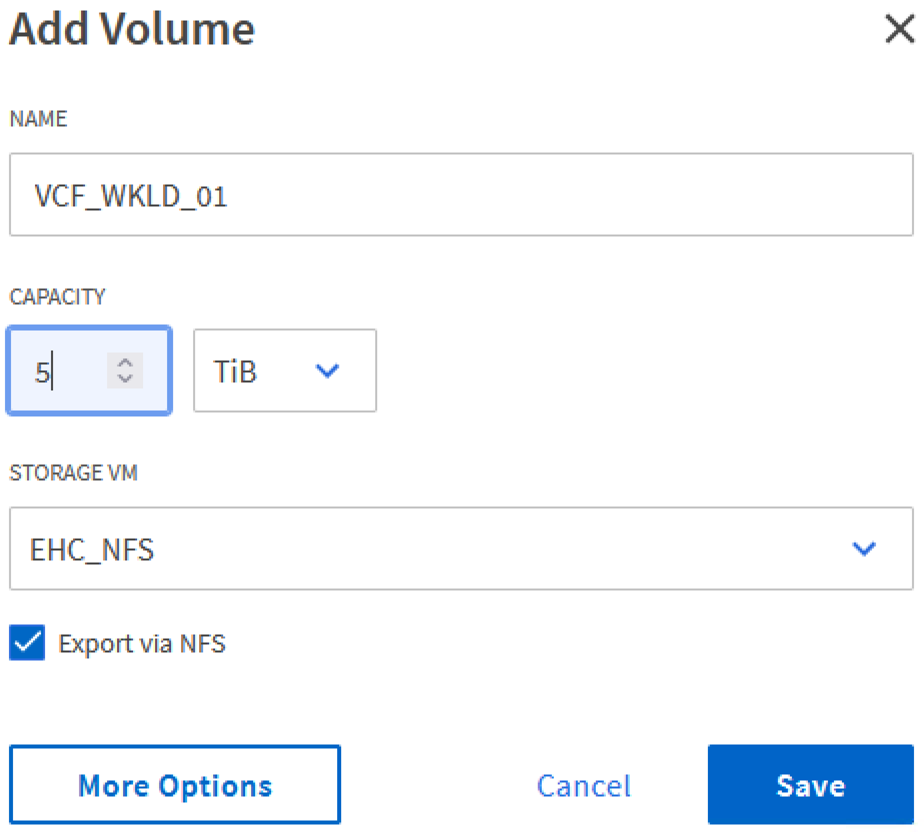
Create NFS volume

Create an NFS volume on the ONTAP storage system to be used as a datastore in the Workload Domain deployment.

1. From ONTAP System Manager navigate to **Storage > Volumes** in the left-hand menu and click on **+Add** to create a new volume.



2. Add a name for the volume, fill out the desired capacity and selection the storage VM that will host the volume. Click on **More Options** to continue.



Add Volume

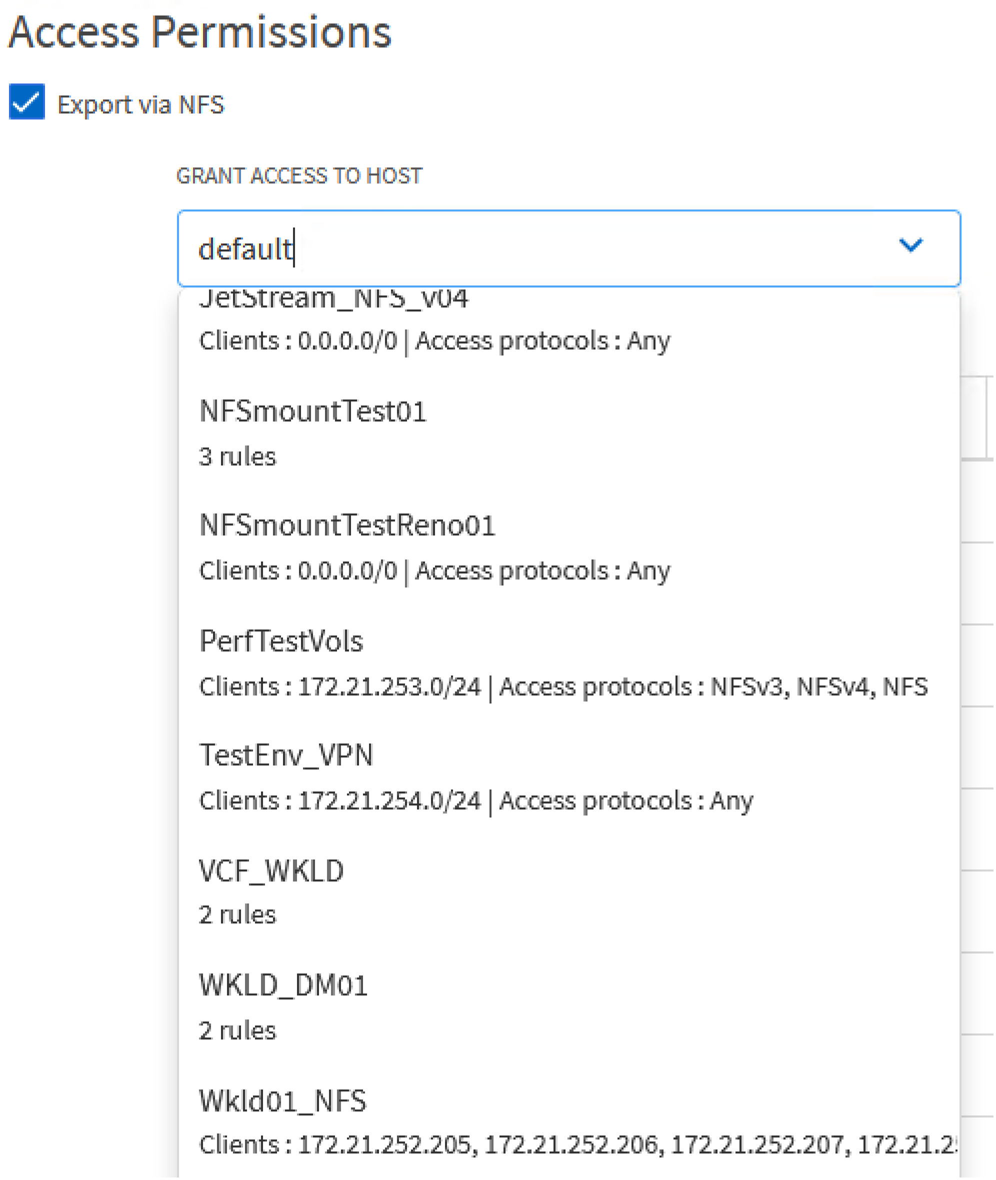
NAME
VCF_WKLD_01

CAPACITY
5 TiB

STORAGE VM
EHC_NFS

☑ Export via NFS

3. Under Access Permissions, select the Export Policy which includes the VCF management network or IP address and NFS network IP addresses that will be used for both validation of the NFS Server and NFS traffic.



Access Permissions

☑ Export via NFS

GRANT ACCESS TO HOST

default

JetStream_NFS_v04
Clients : 0.0.0.0/0 | Access protocols : Any

NFSmountTest01
3 rules

NFSmountTestReno01
Clients : 0.0.0.0/0 | Access protocols : Any

PerfTestVols
Clients : 172.21.253.0/24 | Access protocols : NFSv3, NFSv4, NFS

TestEnv_VPN
Clients : 172.21.254.0/24 | Access protocols : Any

VCF_WKLD
2 rules

WKLD_DM01
2 rules

Wkld01_NFS
Clients : 172.21.252.205, 172.21.252.206, 172.21.252.207, 172.21.2

+

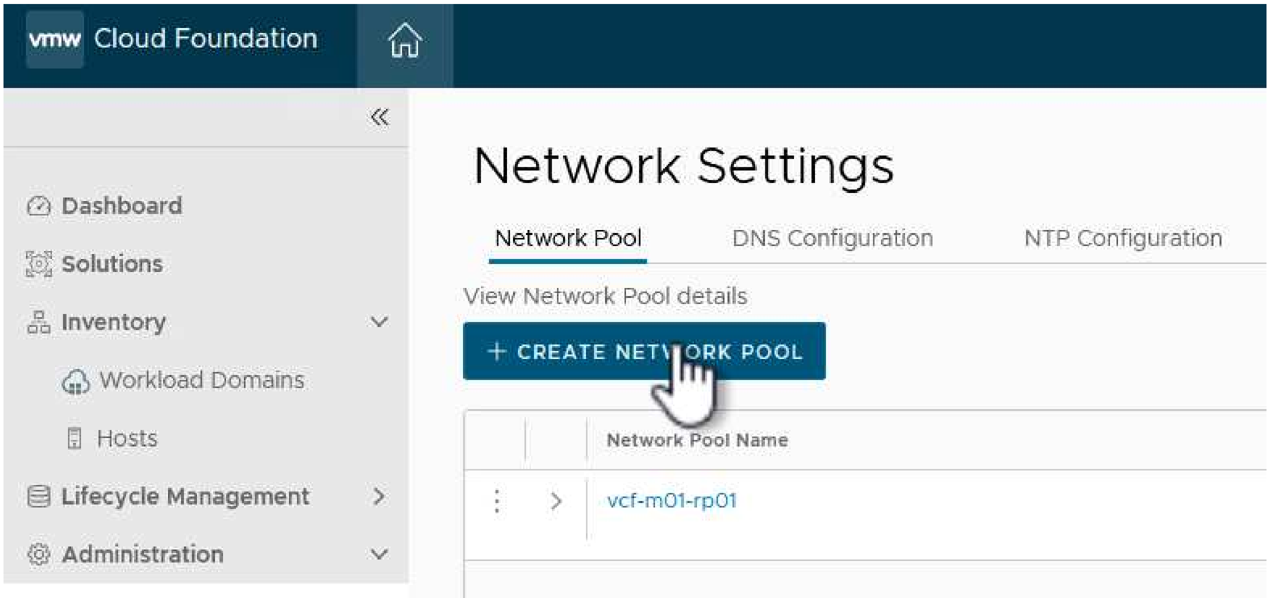
> When deploying a VI Workload Domain, VCF validates connectivity to the NFS Server. This is done using the management adapter on the ESXi hosts before any additional vmkernel adapter is added with the NFS IP address. Therefore, it is necessary to ensure that either 1) the management network is routable to the NFS Server, or 2) a LIF for the management network has been added to the SVM hosting the NFS datastore volume, to ensure that the validation can proceed.

4. Alternately, ONTAP Volumes can be created in the ONTAP CLI. For more information refer to the lun create command in the ONTAP commands documentation.

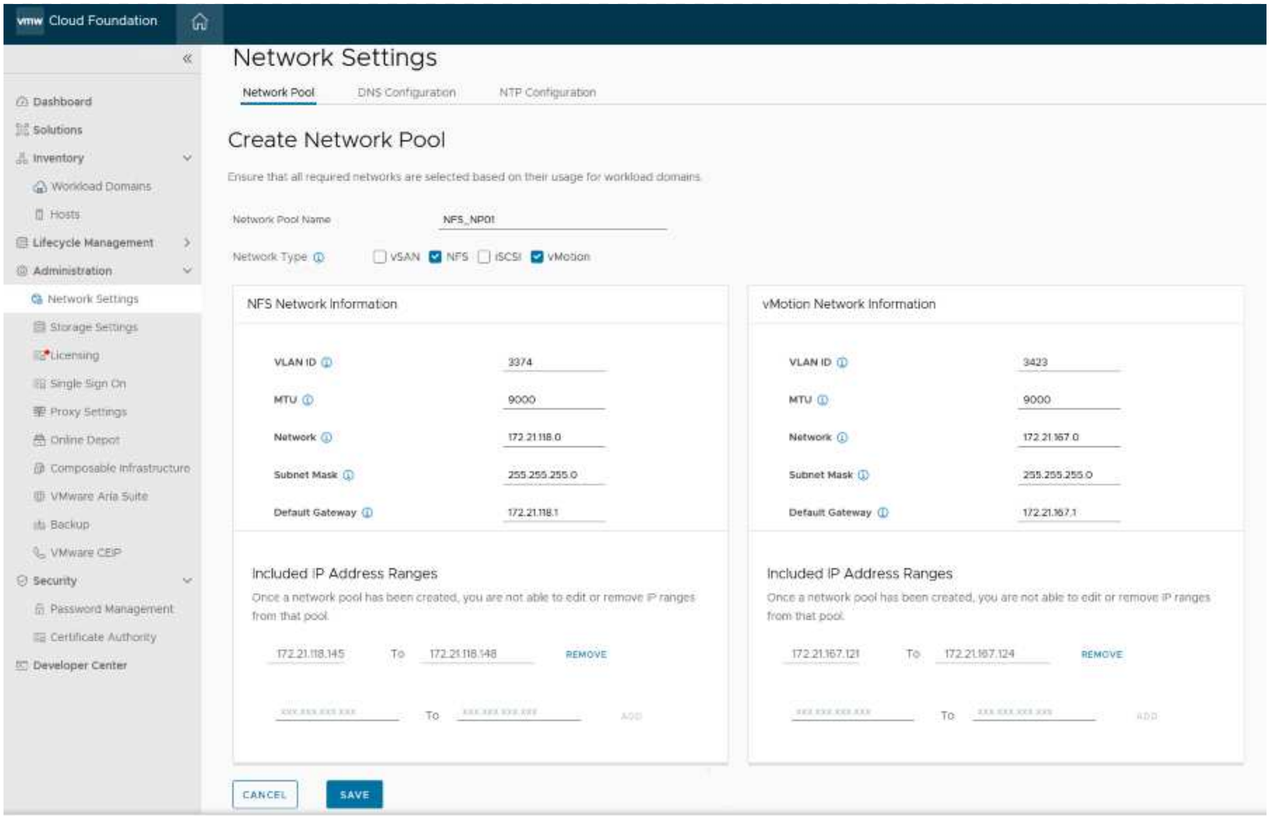
Create Network Pool in SDDC Manager

ANetwork Pool must be created in SDDC Manager before commissioning the ESXi hosts, as preparation for deploying them in a VI Workload Domain. The Network Pool must include the network information and IP address range(s) for VMkernel adapters to be used for communication with the NFS server.

1. From the SDDC Manager web interface navigate to **Network Settings** in the left-hand menu and click on the **+ Create Network Pool** button.



2. Fill out a name for the Network Pool, select the check box for NFS and fill out all networking details. Repeat this for the vMotion network information.



Network Settings

Create Network Pool

Ensure that all required networks are selected based on their usage for workload domains.

Network Pool Name: NFS_NP01

Network Type: □ vSAN ☑ NFS □ iSCSI ☑ vMotion

NFS Network Information		vMotion Network Information	
VLAN ID	3374	VLAN ID	3423
MTU	9000	MTU	9000
Network	172.21.118.0	Network	172.21.167.0
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
Default Gateway	172.21.118.1	Default Gateway	172.21.167.1

Included IP Address Ranges

Once a network pool has been created, you are not able to edit or remove IP ranges from that pool.

NFS: 172.21.118.145 To 172.21.118.148

vMotion: 172.21.167.121 To 172.21.167.124

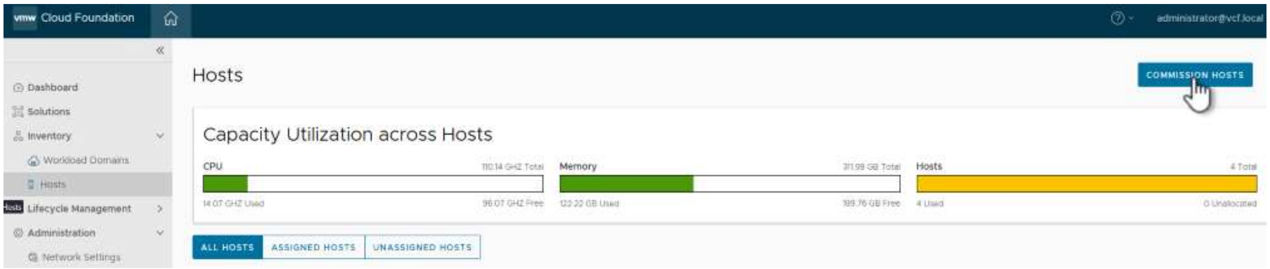
3. Click the **Save** button to complete creating the Network Pool.

Commission Hosts

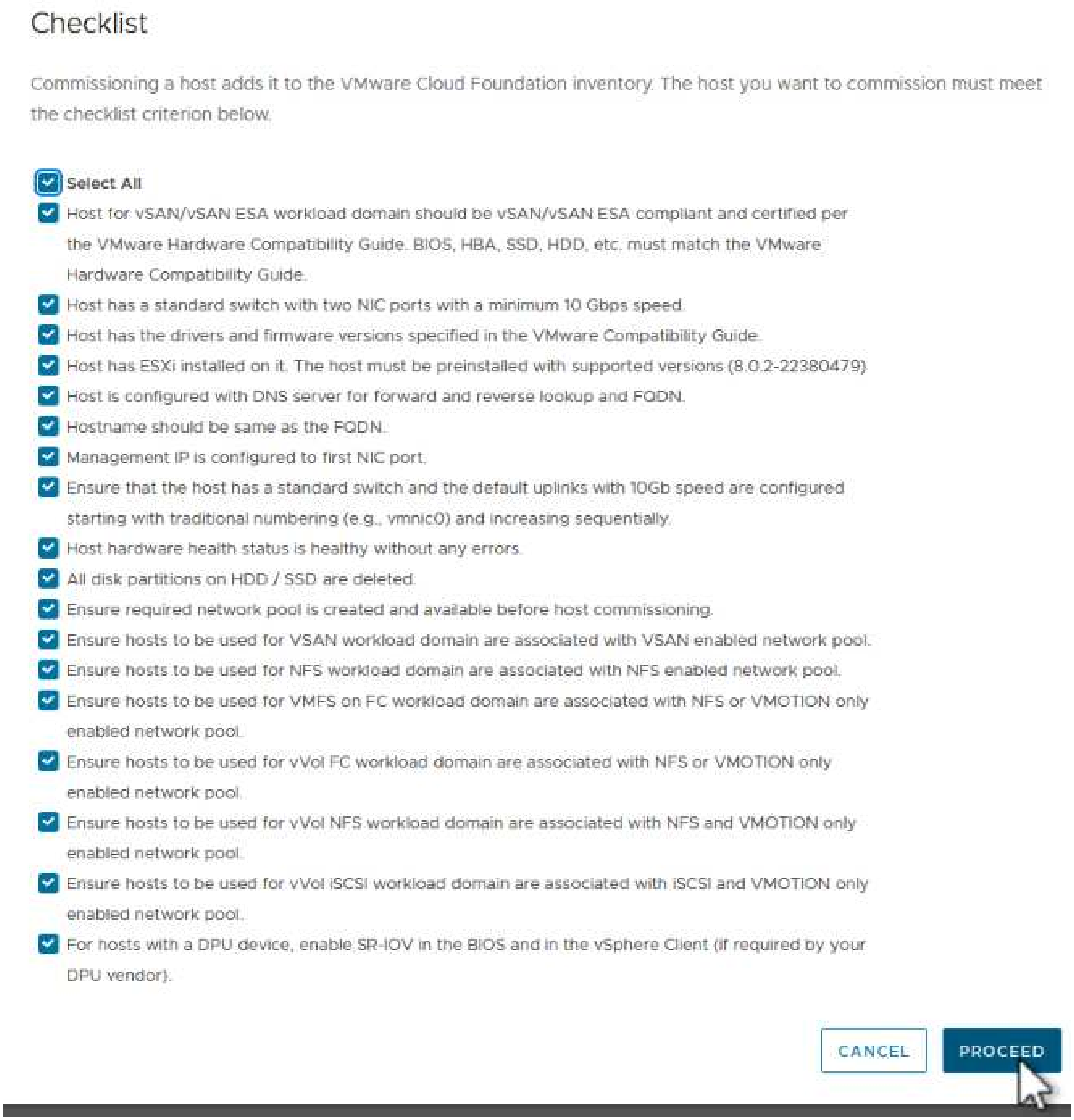
Before ESXi hosts can be deployed as a workload domain they must be added to the SDDC Manager inventory. This involves providing the required information, passing validation and starting the commissioning process.

For more information see Commission Hosts in the VCF Administration Guide.

1. From the SDDC Manager interface navigate to **Hosts** in the left-hand menu and click on the **Commission Hosts** button.



2. The first page is a prerequisite checklist. Double-check all prerequisites and select all checkboxes to proceed.



Checklist

Commissioning a host adds it to the VMware Cloud Foundation inventory. The host you want to commission must meet the checklist criterion below.

☑ Select All

☑ Host for vSAN/vSAN ESA workload domain should be vSAN/vSAN ESA compliant and certified per the VMware Hardware Compatibility Guide. BIOS, HBA, SSD, HDD, etc. must match the VMware Hardware Compatibility Guide.

☑ Host has a standard switch with two NIC ports with a minimum 10 Gbps speed.

☑ Host has the drivers and firmware versions specified in the VMware Compatibility Guide.

☑ Host has ESXi installed on it. The host must be preinstalled with supported versions (8.0.2-22380479)

☑ Host is configured with DNS server for forward and reverse lookup and FQDN.

☑ Hostname should be same as the FQDN.

☑ Management IP is configured to first NIC port.

☑ Ensure that the host has a standard switch and the default uplinks with 10Gb speed are configured starting with traditional numbering (e.g., vmnic0) and increasing sequentially.

☑ Host hardware health status is healthy without any errors.

☑ All disk partitions on HDD / SSD are deleted.

☑ Ensure required network pool is created and available before host commissioning.

☑ Ensure hosts to be used for VSAN workload domain are associated with VSAN enabled network pool.

☑ Ensure hosts to be used for NFS workload domain are associated with NFS enabled network pool.

☑ Ensure hosts to be used for VMFS on FC workload domain are associated with NFS or VMOTION only enabled network pool.

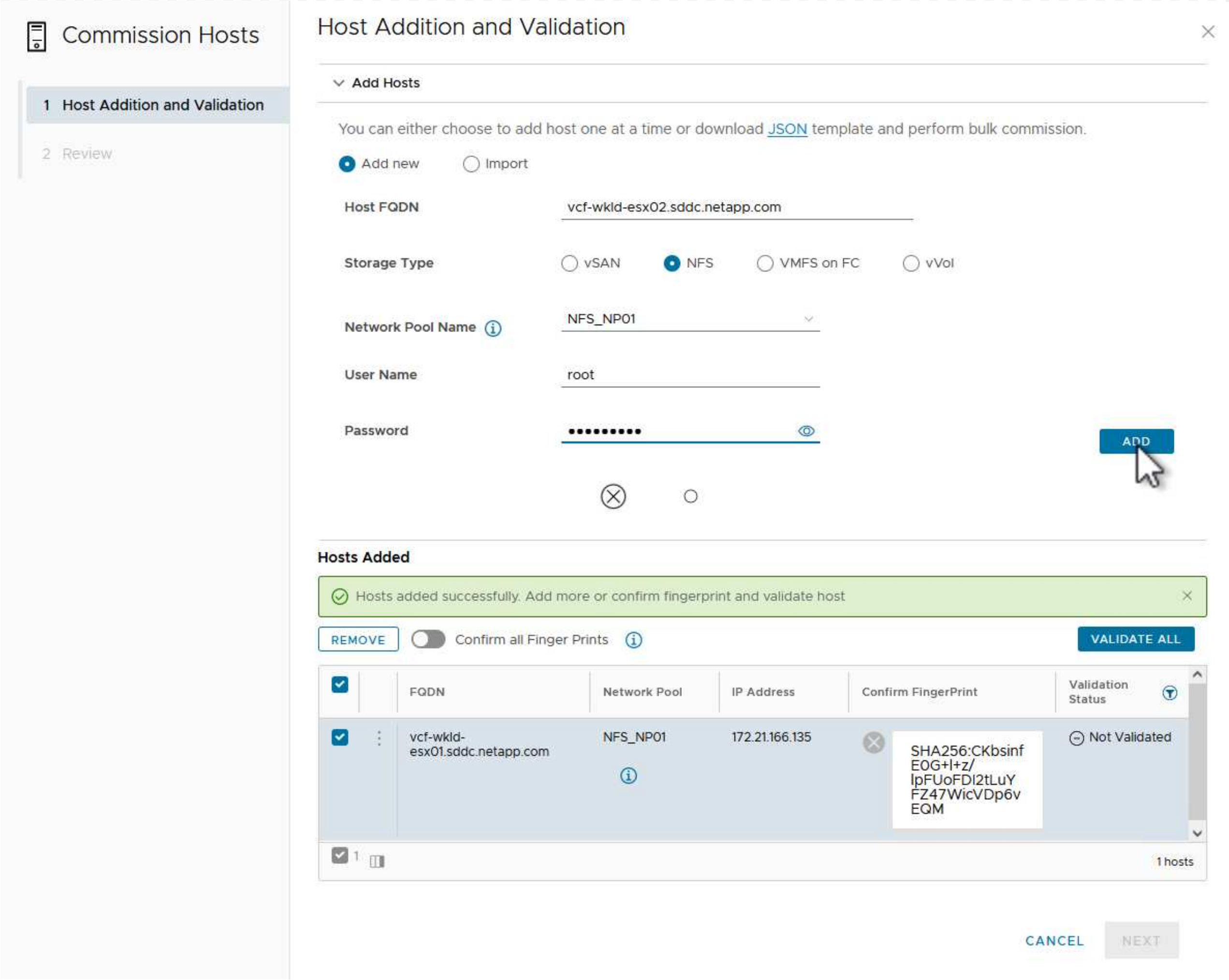
☑ Ensure hosts to be used for vVol FC workload domain are associated with NFS or VMOTION only enabled network pool.

☑ Ensure hosts to be used for vVol NFS workload domain are associated with NFS and VMOTION only enabled network pool.

☑ Ensure hosts to be used for vVol iSCSI workload domain are associated with iSCSI and VMOTION only enabled network pool.

☑ For hosts with a DPU device, enable SR-IOV in the BIOS and in the vSphere Client (if required by your DPU vendor).

3. In the **Host Addition and Validation** window fill out the **Host FQDN**, **Storage Type**, The **Network Pool** name that includes the vMotion and NFS storage IP addresses to be used for the workload domain, and the credentials to access the ESXi host. Click on **Add** to add the host to the group of hosts to be validated.



Host Addition and Validation

Add Hosts

You can either choose to add host one at a time or download JSON template and perform bulk commission.

● Add new ○ Import

Host FQDN: vcf-wkld-esx02.sddc.netapp.com

Storage Type: ○ vSAN ● NFS ○ VMFS on FC ○ vVol

Network Pool Name: NFS_NP01

User Name: root

Password: ••••••••••

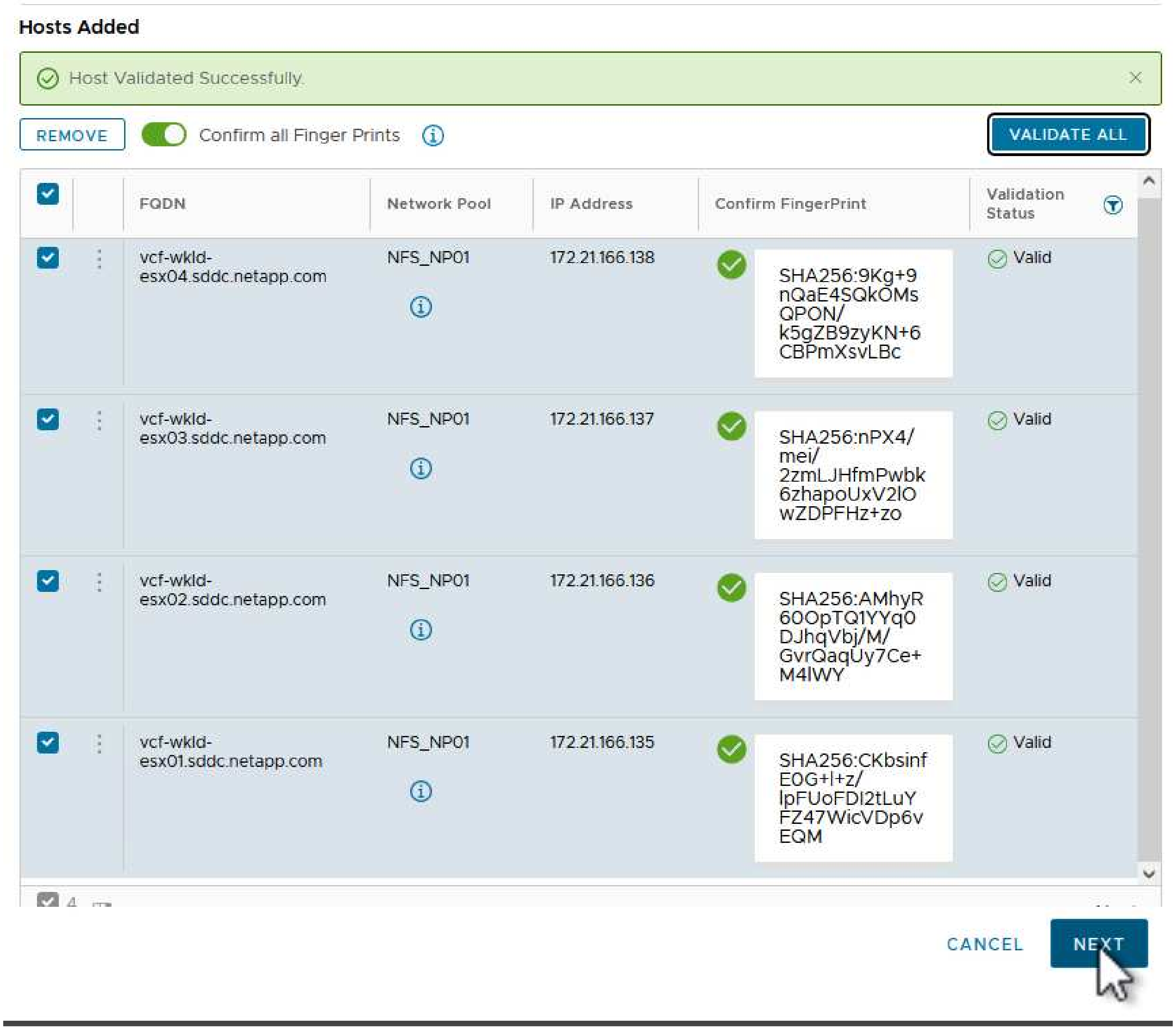
Hosts Added

Hosts added successfully. Add more or confirm fingerprint and validate host

☑	FQDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
☑	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01	172.21.166.135	SHA256:CKbsinfE0G+l+z/lpFUoFDI2tLuYFZ47WicVDp6vEQM	Not Validated

1 hosts

4. Once all hosts to be validated have been added, click on the **Validate All** button to continue.
5. Assuming all hosts are validated, click on **Next** to continue.

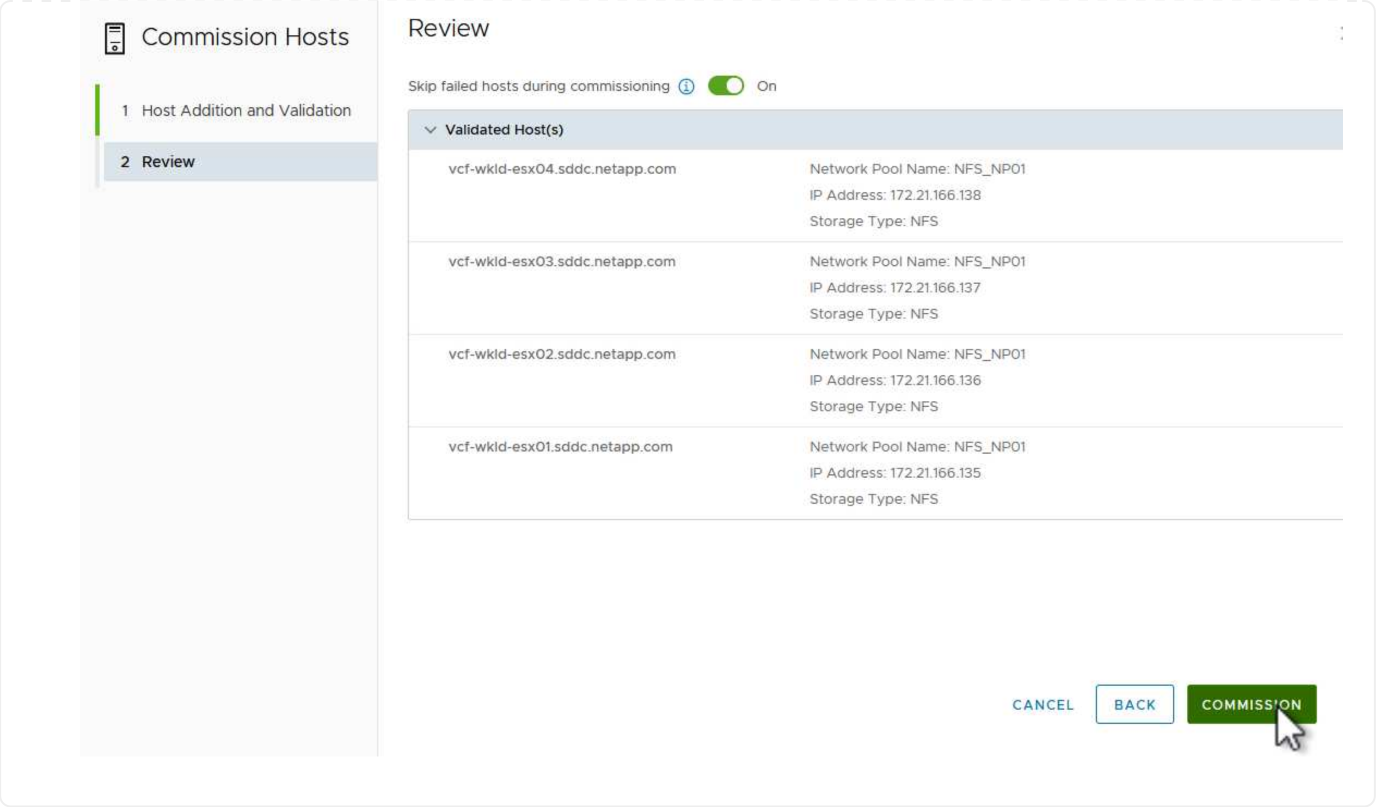


Hosts Added

Host Validated Successfully.

☑	FQDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
☑	vcf-wkld-esx04.sddc.netapp.com	NFS_NP01	172.21.166.138	✓ SHA256:9Kg+9nQaE4SQkOMsQPON/k5gZB9zyKN+6CBPmXsvLBc	✓ Valid
☑	vcf-wkld-esx03.sddc.netapp.com	NFS_NP01	172.21.166.137	✓ SHA256:nPX4/mei/2zmLJHfmPwbk6zhapoUxV2lOwZDPFHz+zo	✓ Valid
☑	vcf-wkld-esx02.sddc.netapp.com	NFS_NP01	172.21.166.136	✓ SHA256:AMhyR60OpTQ1YYq0DJhqVbj/M/GvrQaqUy7Ce+M4lWY	✓ Valid
☑	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01	172.21.166.135	✓ SHA256:CKbsinfE0G+l+z/lpFUoFDI2tLuYFZ47WicVDp6vEQM	✓ Valid

6. Review the list of hosts to be commissioned and click on the **Commission** button to start the process. Monitor the commissioning process from the Task pane in SDDC manager.


Commission Hosts

1 Host Addition and Validation

2 Review

Review

Skip failed hosts during commissioning On

Validated Host(s)

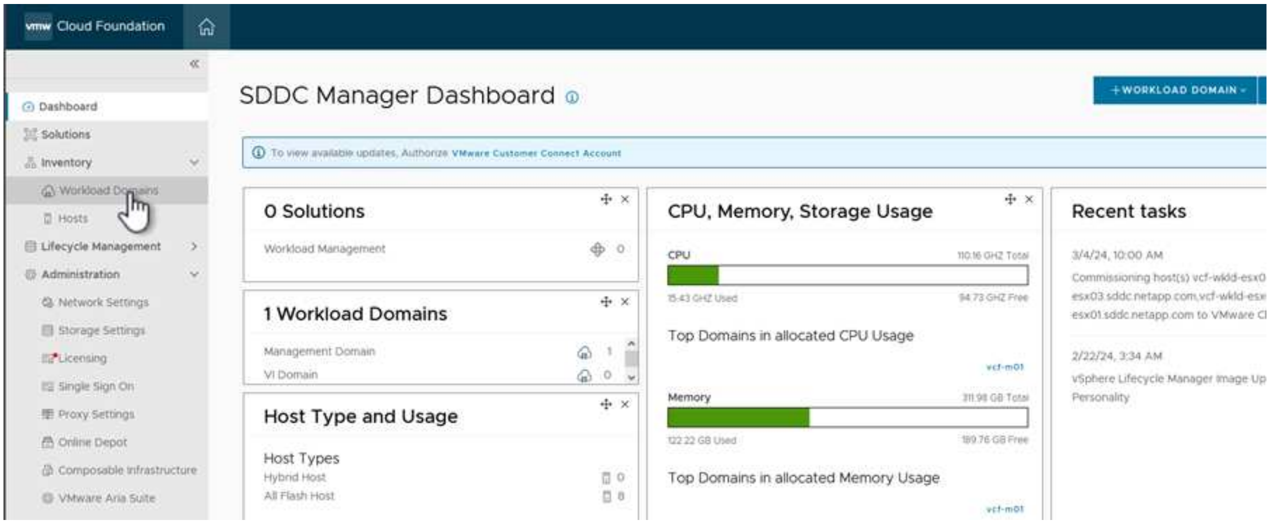
vcf-wkld-esx04.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.138 Storage Type: NFS
vcf-wkld-esx03.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.137 Storage Type: NFS
vcf-wkld-esx02.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.136 Storage Type: NFS
vcf-wkld-esx01.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.135 Storage Type: NFS

Deploy VI Workload Domain

Deploying VI workload domains is accomplished using the VCF Cloud Manager interface. Only the steps related to the storage configuration will be presented here.

For step-by-step instructions on deploying a VI workload domain refer to Deploy a VI Workload Domain Using the SDDC Manager UI.

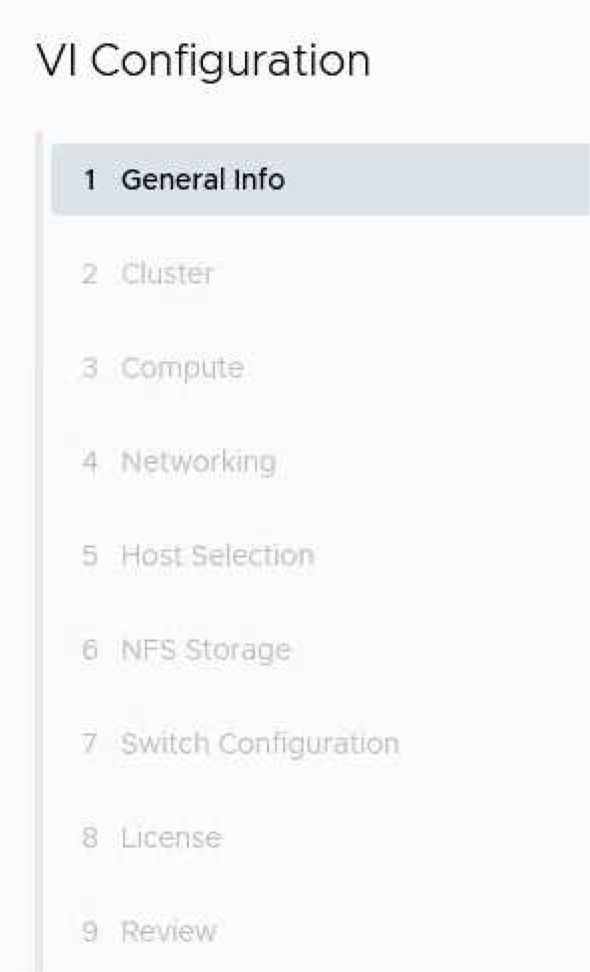
1. From the SDDC Manager Dashboard click on **+ Workload Domain** in the upper right hand corner to create a new Workload Domain.



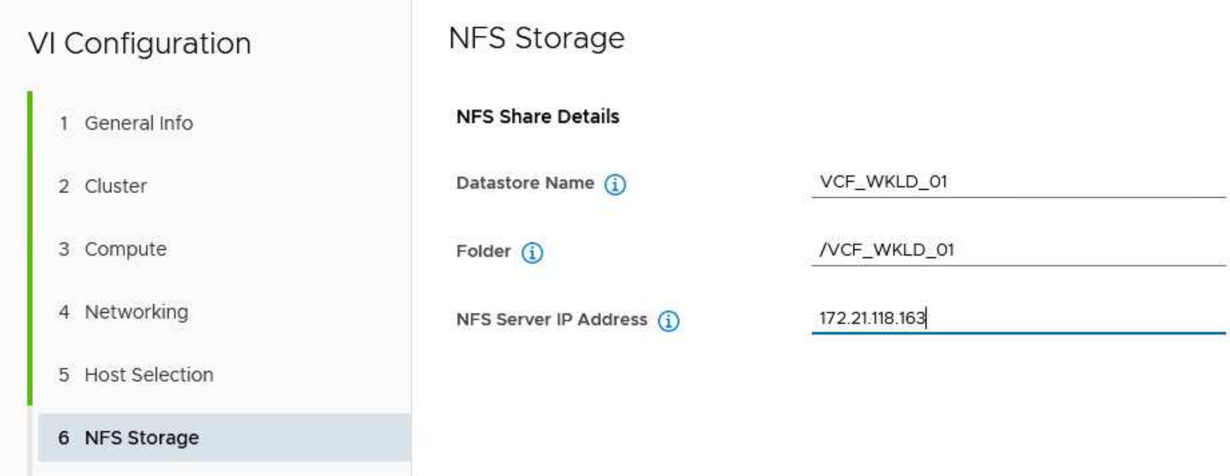
2. In the VI Configuration wizard fill out the sections for **General Info, Cluster, Compute, Networking**, and **Host Selection** as required.

For information on filling out the information required in the VI Configuration wizard refer to Deploy a VI Workload Domain Using the SDDC Manager UI.

+



1. In the NFS Storage section fill out the Datastore Name, the folder mount point of the NFS volume and the IP address of the ONTAP NFS storage VM LIF.



NFS Storage

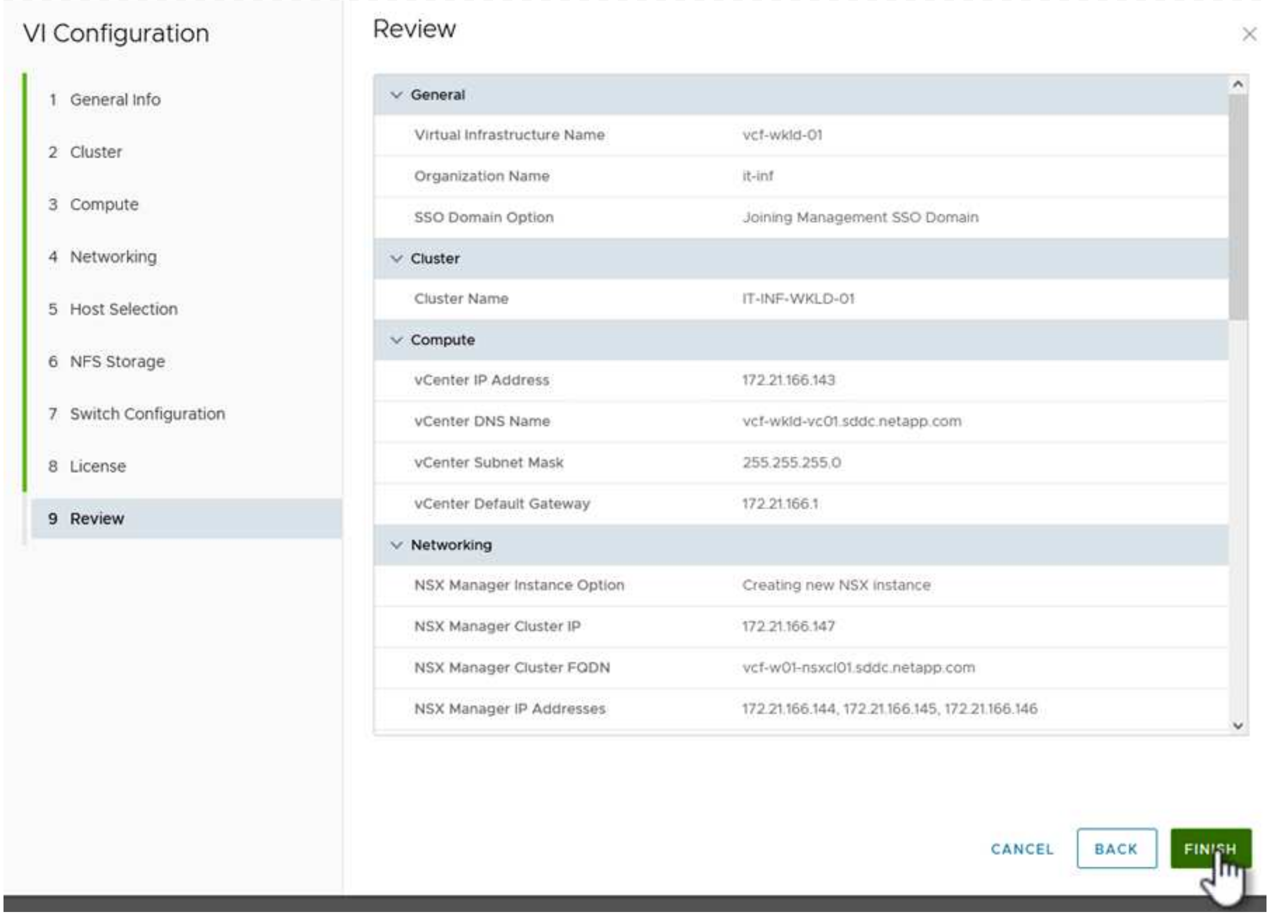
NFS Share Details

Datastore Name: VCF_WKLD_01

Folder: /VCF_WKLD_01

NFS Server IP Address: 172.21.118.163

2. In the VI Configuration wizard complete the Switch Configuration and License steps, and then click on **Finish** to start the Workload Domain creation process.



VI Configuration

1 General Info
2 Cluster
3 Compute
4 Networking
5 Host Selection
6 NFS Storage
7 Switch Configuration
8 License
9 Review

Review

General	
Virtual Infrastructure Name	vcf-wkld-01
Organization Name	it-inf
SSO Domain Option	Joining Management SSO Domain
Cluster	
Cluster Name	IT-INF-WKLD-01
Compute	
vCenter IP Address	172.21.166.143
vCenter DNS Name	vcf-wkld-vc01.sddc.netapp.com
vCenter Subnet Mask	255.255.255.0
vCenter Default Gateway	172.21.166.1
Networking	
NSX Manager Instance Option	Creating new NSX instance
NSX Manager Cluster IP	172.21.166.147
NSX Manager Cluster FQDN	vcf-w01-nsxcl01.sddc.netapp.com
NSX Manager IP Addresses	172.21.166.144, 172.21.166.145, 172.21.166.146

3. Monitor the process and resolve any validation issues that arise during the process.

Install NetApp NFS Plug-in for VMware VAAI

The NetApp NFS Plug-in for VMware VAAI integrates the VMware Virtual Disk Libraries installed on the ESXi host and provides higher performance cloning operations that finish faster. This is a recommended procedure when using ONTAP storage systems with VMware vSphere.

For step-by-step instructions on deploying the NetApp NFS Plug-in for VMware VAAI following the instructions at Install NetApp NFS Plug-in for VMware VAAI.

Video demo for this solution

NFS Datastores as Principal Storage for VCF Workload Domains

Use ONTAP Tools to configure supplemental storage (NFS and vVols) for VCF Workload Domains

In this scenario we will demonstrate how to deploy and use ONTAP Tools for VMware vSphere to configure both an **NFS datastore**, and a **vVols datastore** for a VCF workload domain.

NFS is used as the storage protocol for the vVols datastore.

Author: Josh Powell, Ravi BCB

Scenario Overview

This scenario covers the following high level steps:

- Create a storage virtual machine (SVM) with logical interfaces (LIFs) for NFS traffic.
- Create a distributed port group for the NFS network on the VI workload domain.
- Create a vmkernel adapter for NFS on the ESXi hosts for the VI workload domain.
- Deploy ONTAP Tools on the VI workload domain.
- Create a new NFS datastore on the VI workload domain.
- Create a new vVols datastore on the VI workload domain.

Prerequisites

This scenario requires the following components and configurations:

- An ONTAP AFF storage system with physical data ports on ethernet switches dedicated to storage traffic.
- VCF management domain deployment is complete and the vSphere client is accessible.
- A VI workload domain has been previously deployed.

NetApp recommends a redundant network designs for NFS, providing fault tolerance for storage systems, switches, networks adapters and host systems. It is common to deploy NFS with a single subnet or multiple subnets depending on the architectural requirements.

Refer to Best Practices For Running NFS with VMware vSphere for detailed information specific to VMware vSphere.

For network guidance on using ONTAP with VMware vSphere refer to the Network configuration - NFS section of the NetApp enterprise applications documentation.

This documentation demonstrates the process of creating a new SVM and specifying the IP address information to create multiple LIFs for NFS traffic. To add new LIFs to an existing SVM refer to Create a LIF (network interface).

Deployment Steps

To deploy ONTAP Tools and use it to create a vVols and NFS datastore on the VCF management domain, complete the following steps:

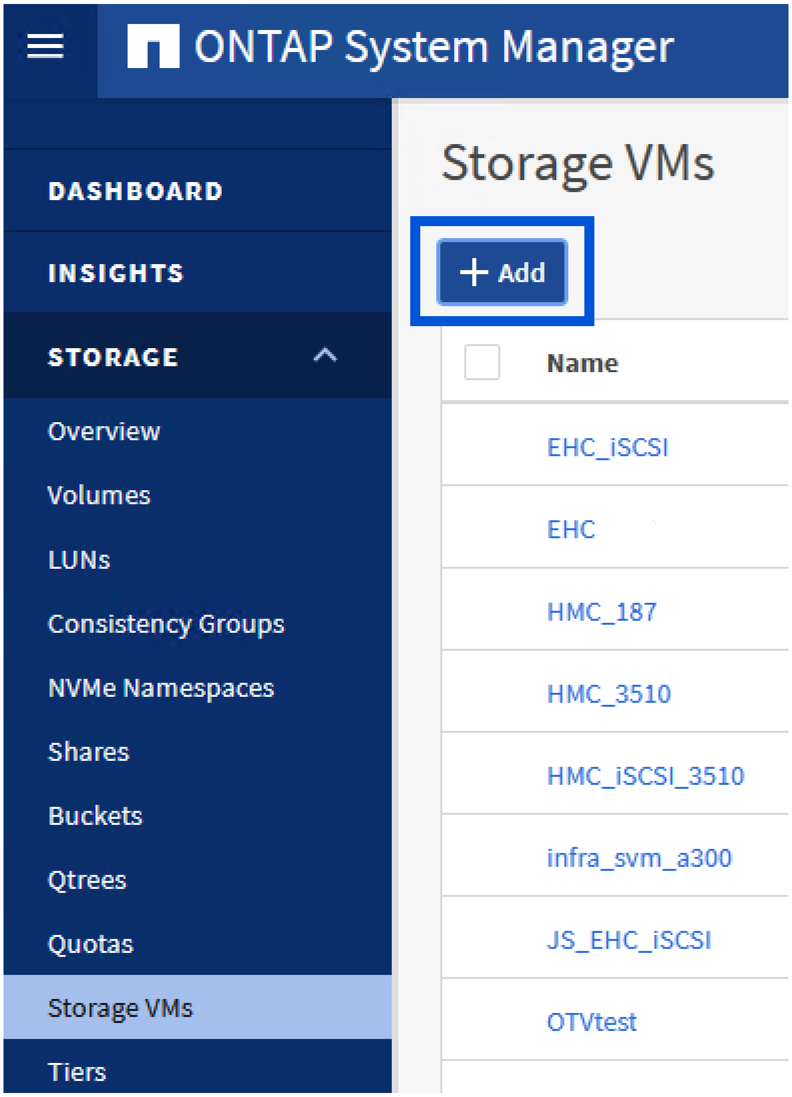
Create SVM and LIFs on ONTAP storage system

The following step is performed in ONTAP System Manager.

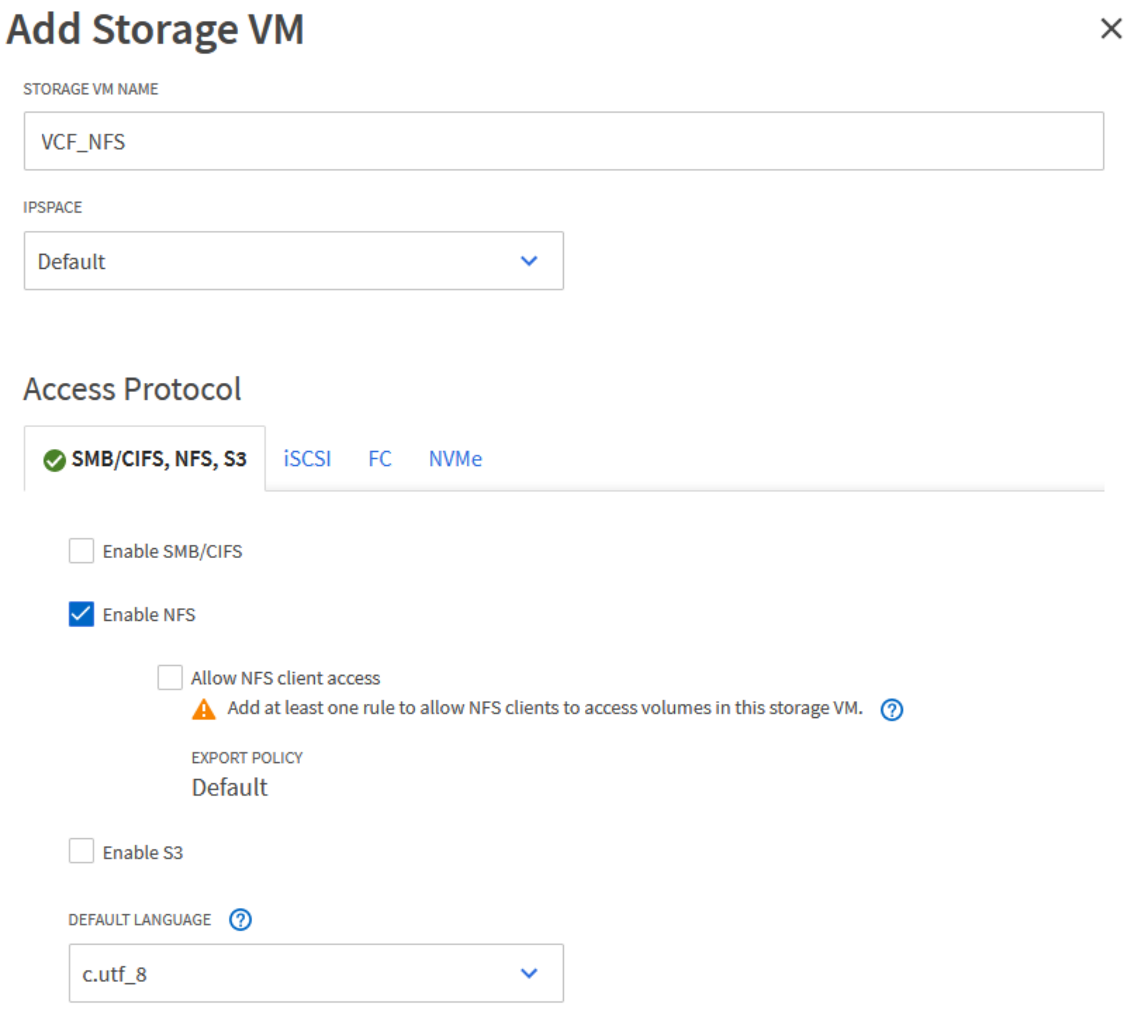
Create the storage VM and LIFs

Complete the following steps to create an SVM together with multiple LIFs for NFS traffic.

1. From ONTAP System Manager navigate to **Storage VMs** in the left-hand menu and click on **+ Add** to start.



2. In the **Add Storage VM** wizard provide a **Name** for the SVM, select the **IP Space** and then, under **Access Protocol**, click on the **SMB/CIFS, NFS, S3** tab and check the box to **Enable NFS**.



Add Storage VM

STORAGE VM NAME: VCF_NFS

IPSPACE: Default

Access Protocol

□ Enable SMB/CIFS

☑ Enable NFS

□ Allow NFS client access

⚠ Add at least one rule to allow NFS clients to access volumes in this storage VM.

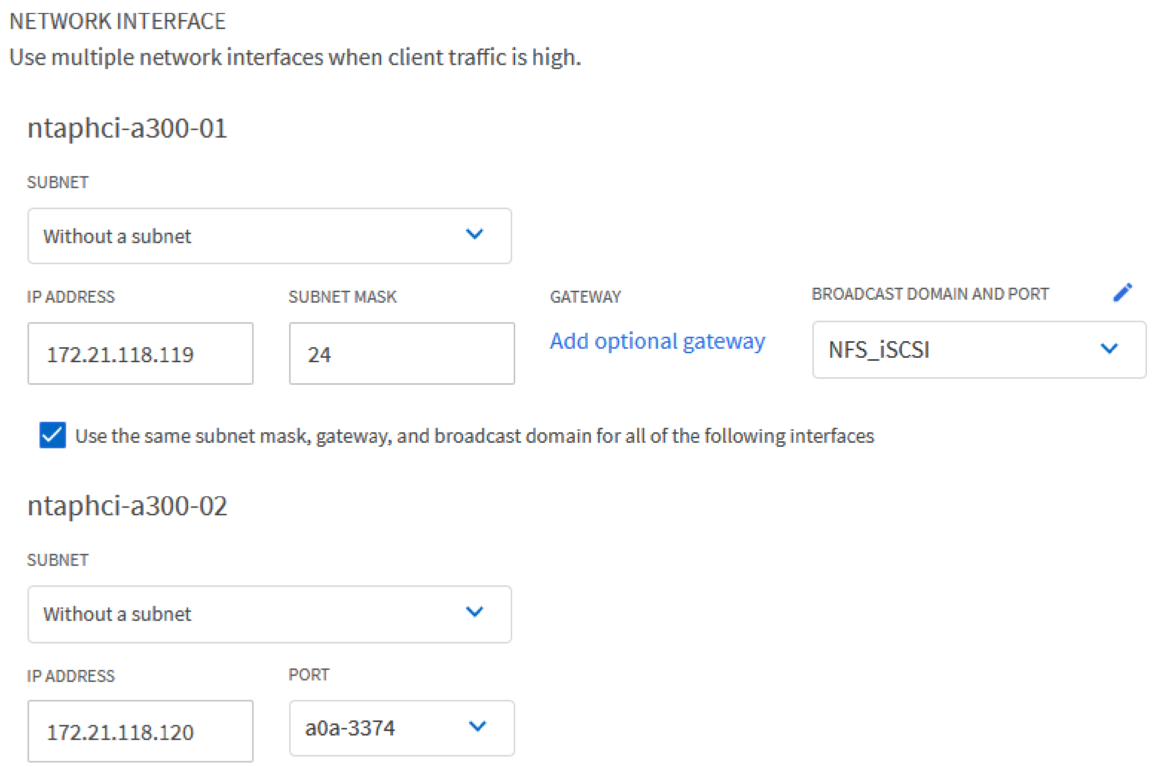
EXPORT POLICY: Default

□ Enable S3

DEFAULT LANGUAGE: c.utf_8

It is not necessary to check the **Allow NFS client access** button here as Ontap Tools for VMware vSphere will be used to automate the datastore deployment process. This includes providing client access for the ESXi hosts.

3. In the **Network Interface** section fill in the **IP address**, **Subnet Mask**, and **Broadcast Domain and Port** for the first LIF. For subsequent LIFs the checkbox may be enabled to use common settings across all remaining LIFs or use separate settings.



NETWORK INTERFACE
Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET: Without a subnet

IP ADDRESS: 172.21.118.119

SUBNET MASK: 24

GATEWAY: Add optional gateway

BROADCAST DOMAIN AND PORT: NFS_iSCSI

☑ Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

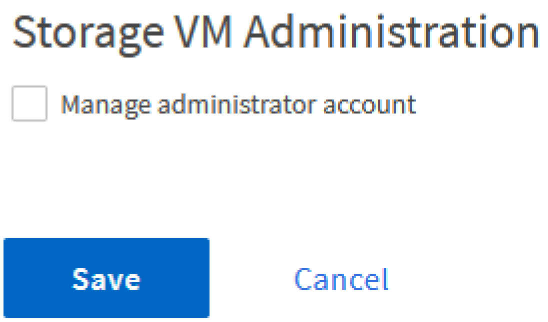
ntaphci-a300-02

SUBNET: Without a subnet

IP ADDRESS: 172.21.118.120

PORT: a0a-3374

4. Choose whether to enable the Storage VM Administration account (for multi-tenancy environments) and click on **Save** to create the SVM.



Storage VM Administration

□ Manage administrator account

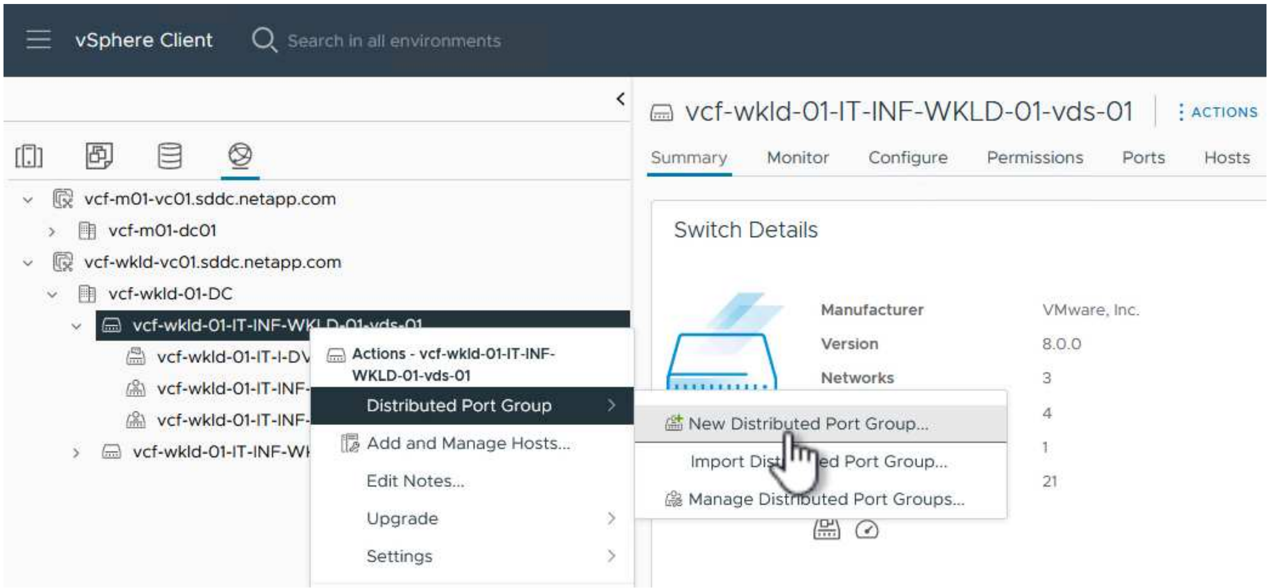
Set up networking for NFS on ESXi hosts

The following steps are performed on the VI Workload Domain cluster using the vSphere client. In this case vCenter Single Sign-On is being used so the vSphere client is common across the management and workload domains.

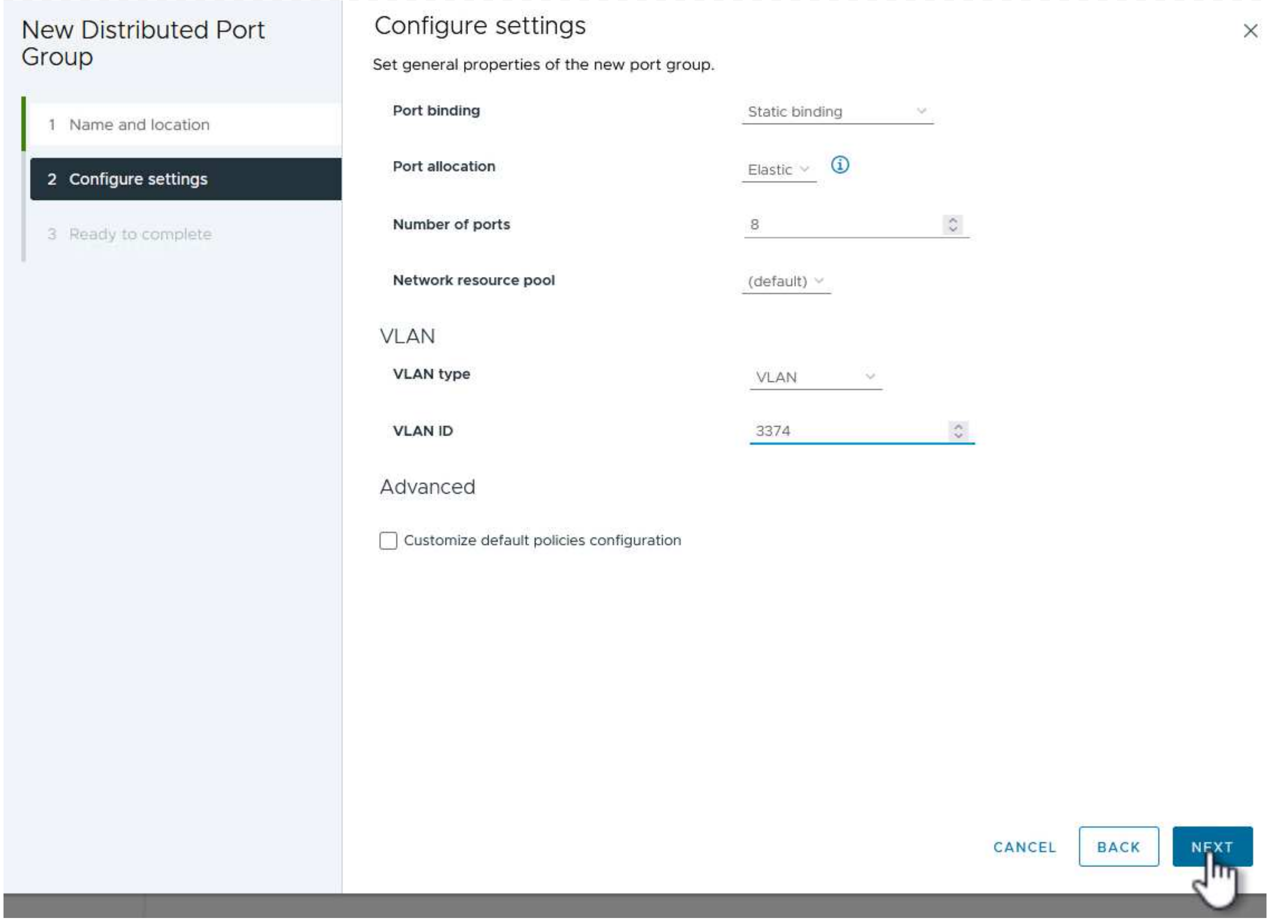
Create a Distributed Port Group for NFS traffic

Complete the following to create a new distributed port group for the network to carry NFS traffic:

1. From the vSphere client , navigate to **Inventory > Networking** for the workload domain. Navigate to the existing Distributed Switch and choose the action to create **New Distributed Port Group…**.



2. In the **New Distributed Port Group** wizard fill in a name for the new port group and click on **Next** to continue.
3. On the **Configure settings** page fill out all settings. If VLANs are being used be sure to provide the correct VLAN ID. Click on **Next** to continue.


New Distributed Port Group

1 Name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding	Static binding
Port allocation	Elastic
Number of ports	8
Network resource pool	(default)

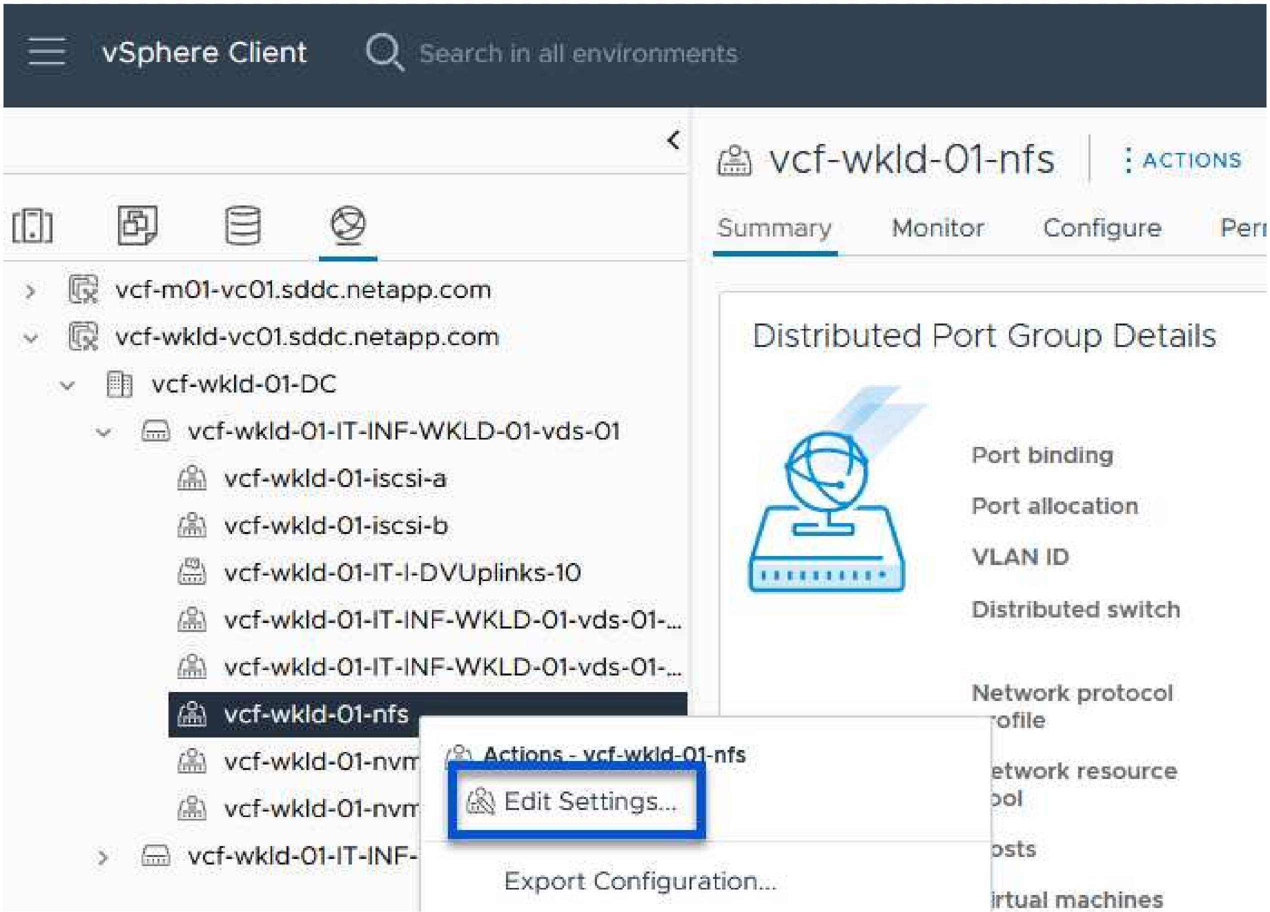
VLAN

VLAN type	VLAN
VLAN ID	3374

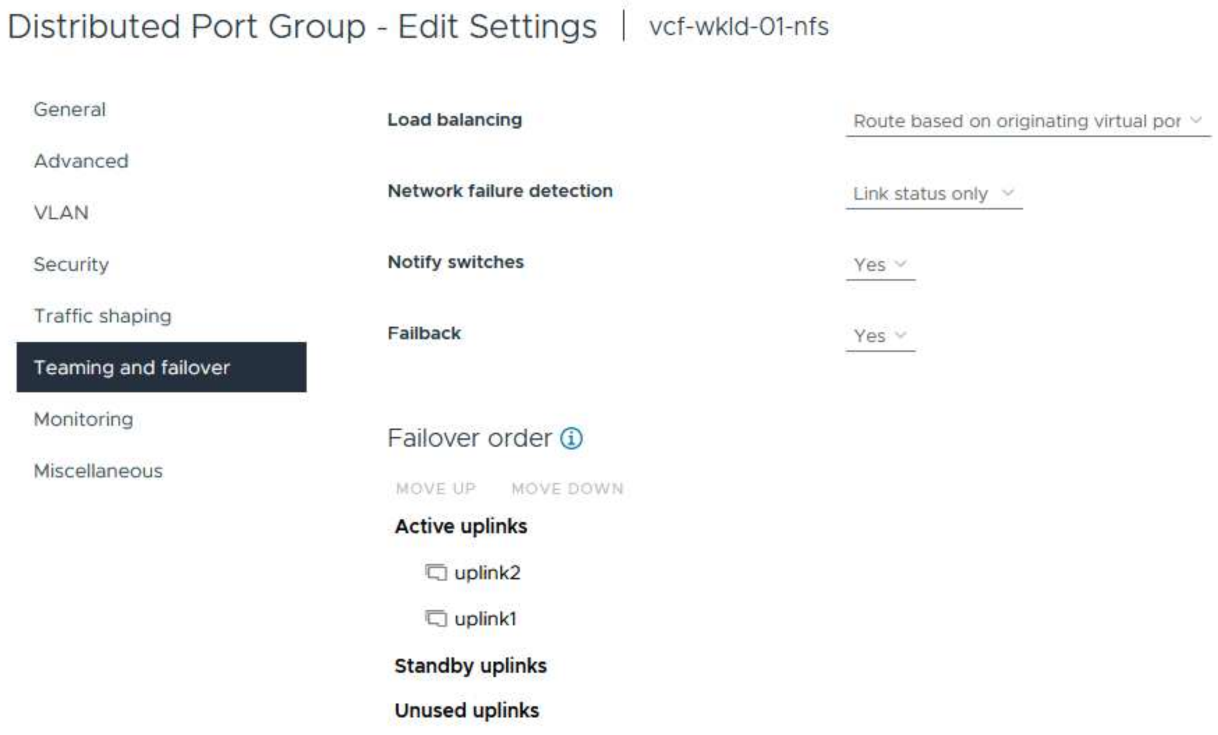
Advanced

□ Customize default policies configuration

4. On the **Ready to complete** page, review the changes and click on **Finish** to create the new distributed port group.
5. Once the port group has been created, navigate to the port group and select the action to **Edit settings…**.



6. On **Distributed Port Group - Edit Settings** page, navigate to **Teaming and failover** in the left-hand menu. Enable teaming for the Uplinks to be used for NFS traffic by ensuring they are together in the **Active uplinks** area. Move any unused uplinks down to **Unused uplinks**.



Distributed Port Group - Edit Settings | vcf-wkld-01-nfs

Load balancing: Route based on originating virtual por

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

Failover order

Active uplinks
- uplink2
- uplink1

Standby uplinks

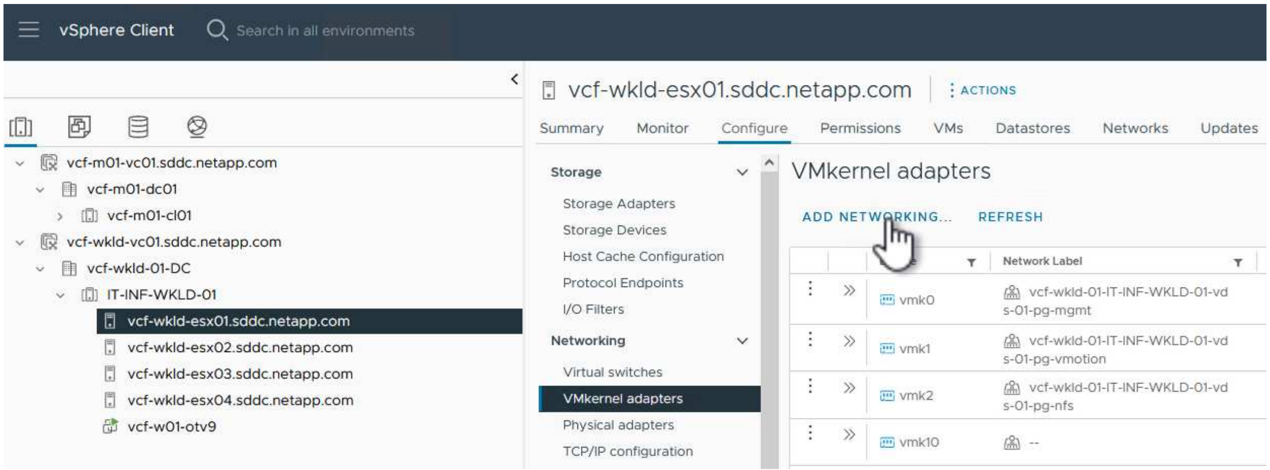
Unused uplinks

7. Repeat this process for each ESXi host in the cluster.

Create a VMkernel adapter on each ESXi host

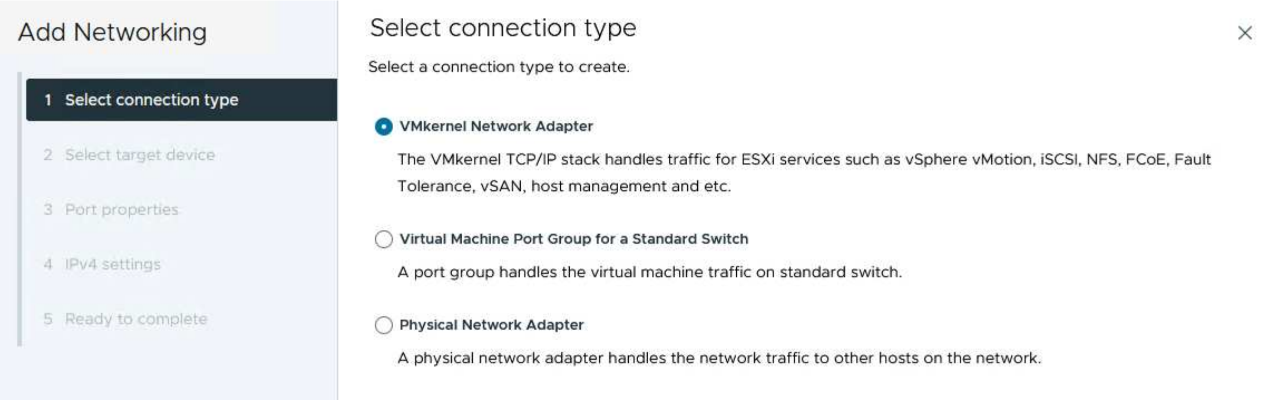
Repeat this process on each ESXi host in the workload domain.

1. From the vSphere client navigate to one of the ESXi hosts in the workload domain inventory. From the **Configure** tab select **VMkernel adapters** and click on **Add Networking…** to start.



	Network Label
vmk0	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt
vmk1	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion
vmk2	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs
vmk10	--

2. On the **Select connection type** window choose **VMkernel Network Adapter** and click on **Next** to continue.



Select connection type

Select a connection type to create.

● **VMkernel Network Adapter**

The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.

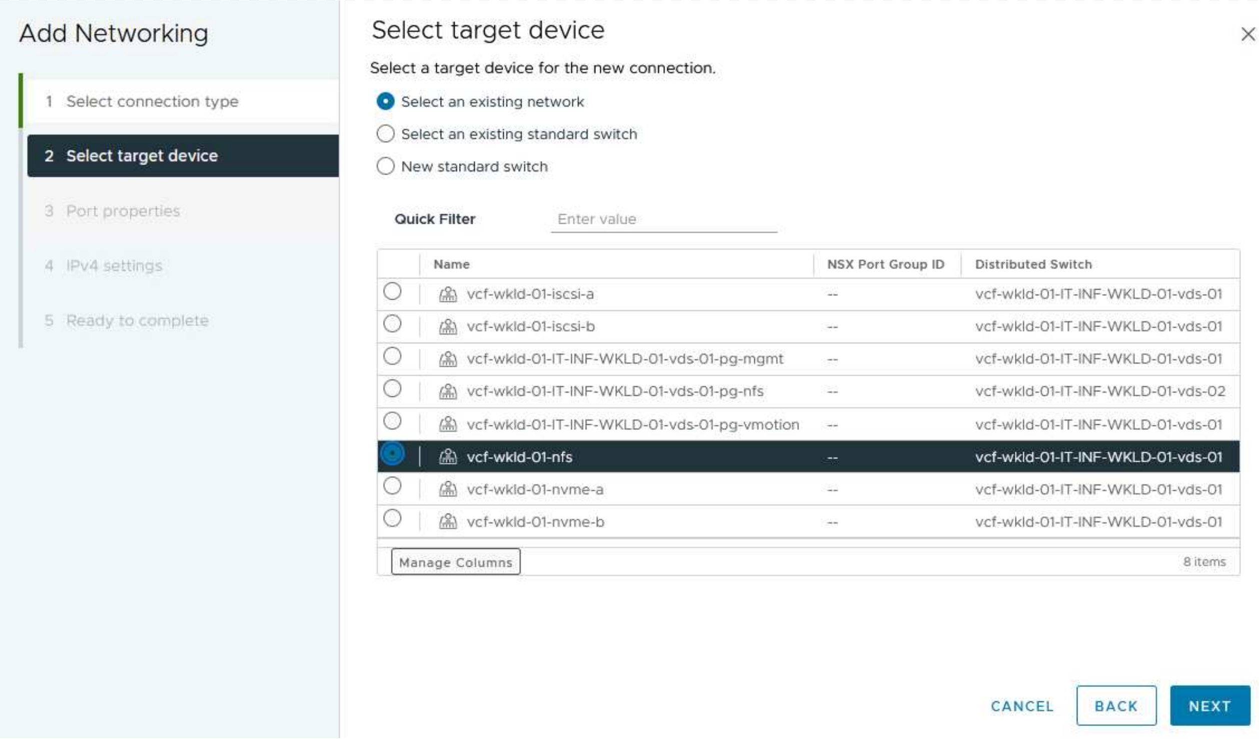
○ **Virtual Machine Port Group for a Standard Switch**

A port group handles the virtual machine traffic on standard switch.

○ **Physical Network Adapter**

A physical network adapter handles the network traffic to other hosts on the network.

3. On the **Select target device** page, choose one of the distributed port groups for NFS that was created previously.



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

● Select an existing network

○ Select an existing standard switch

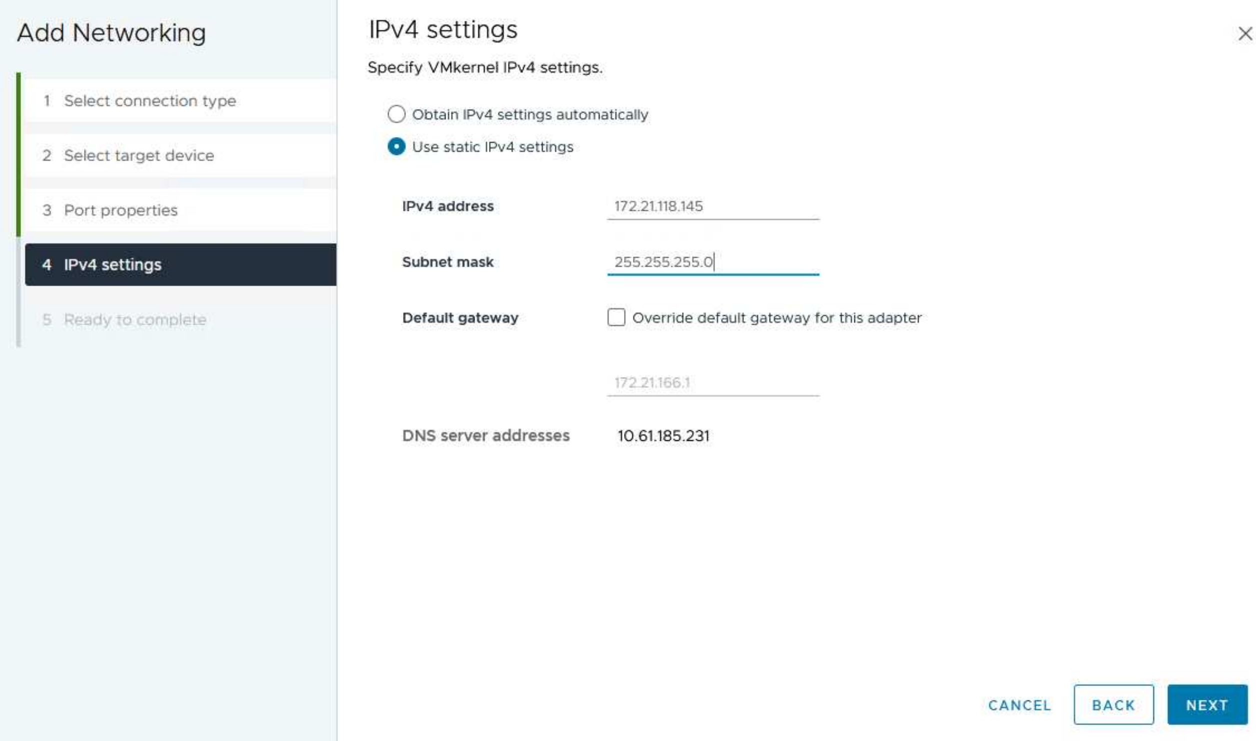
○ New standard switch

Quick Filter: Enter value

	Name	NSX Port Group ID	Distributed Switch
○	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
●	vcf-wkld-01-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

8 items

4. On the **Port properties** page keep the defaults (no enabled services) and click on **Next** to continue.
5. On the **IPv4 settings** page fill in the **IP address**, **Subnet mask**, and provide a new Gateway IP address (only if required). Click on **Next** to continue.



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

○ Obtain IPv4 settings automatically

● Use static IPv4 settings

IPv4 address: 172.21.118.145

Subnet mask: 255.255.255.0

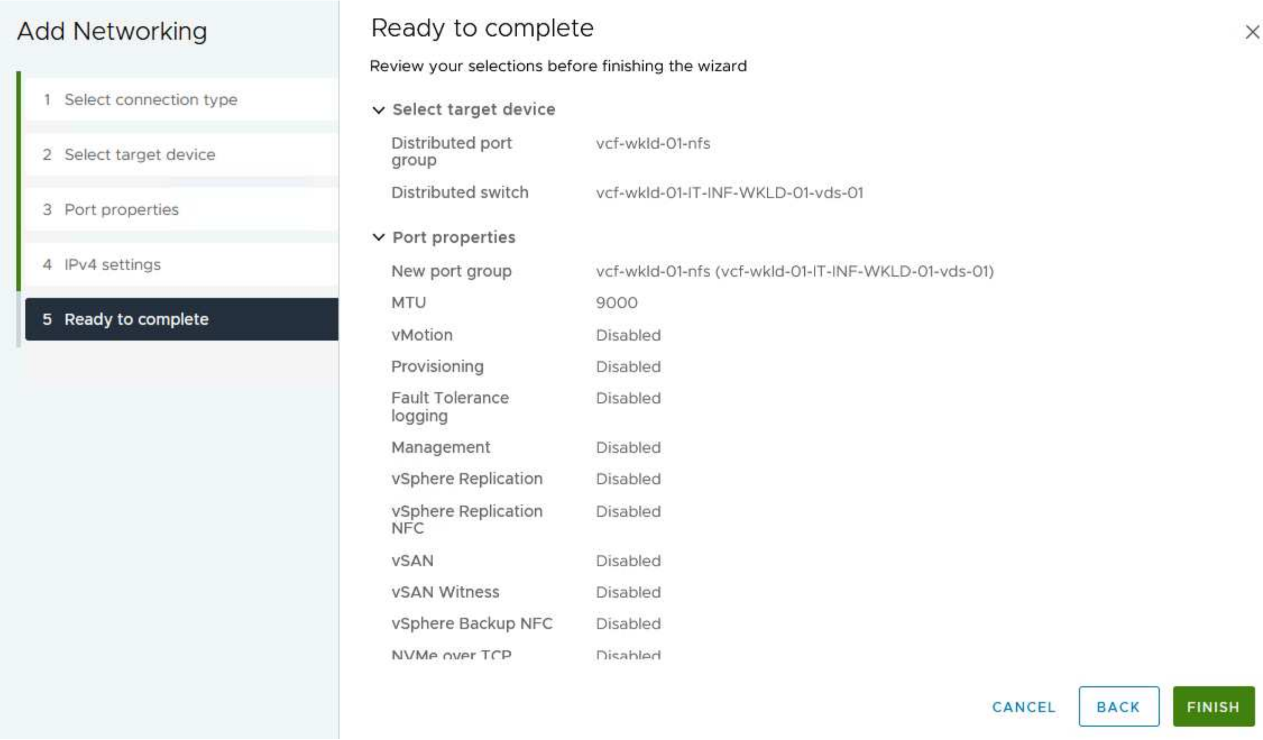
Default gateway: □ Override default gateway for this adapter

172.21.166.1

DNS server addresses: 10.61.185.231

6. Review the your selections on the **Ready to complete** page and click on **Finish** to create the

VMkernel adapter.



Add Networking

1 Select connection type
2 Select target device
3 Port properties
4 IPv4 settings
5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

Select target device

Distributed port group	vcf-wkld-01-nfs
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Port properties

New port group	vcf-wkld-01-nfs (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Disabled

Deploy and use ONTAP Tools to configure storage

The following steps are performed on the VCF management domain cluster using the vSphere client and involve deploying OTV, creating a vVols NFS datastore, and migrating management VM’s to the new datastore.

For VI workload domains, OTV is installed to the VCF Management Cluster but registered with the vCenter associated with the VI workload domain.

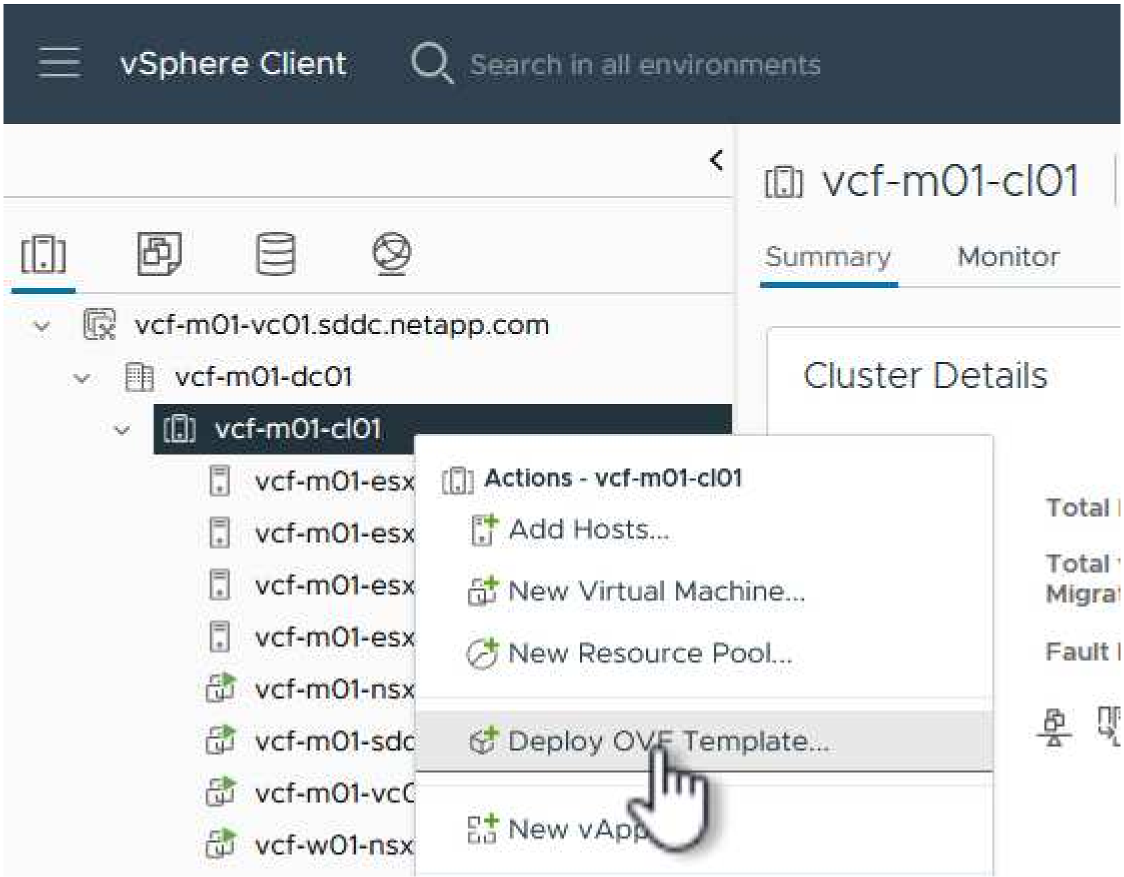
For additional information on deploying and using ONTAP Tools in a multiple vCenter environment refer to Requirements for registering ONTAP tools in multiple vCenter Servers environment.

Deploy ONTAP tools for VMware vSphere

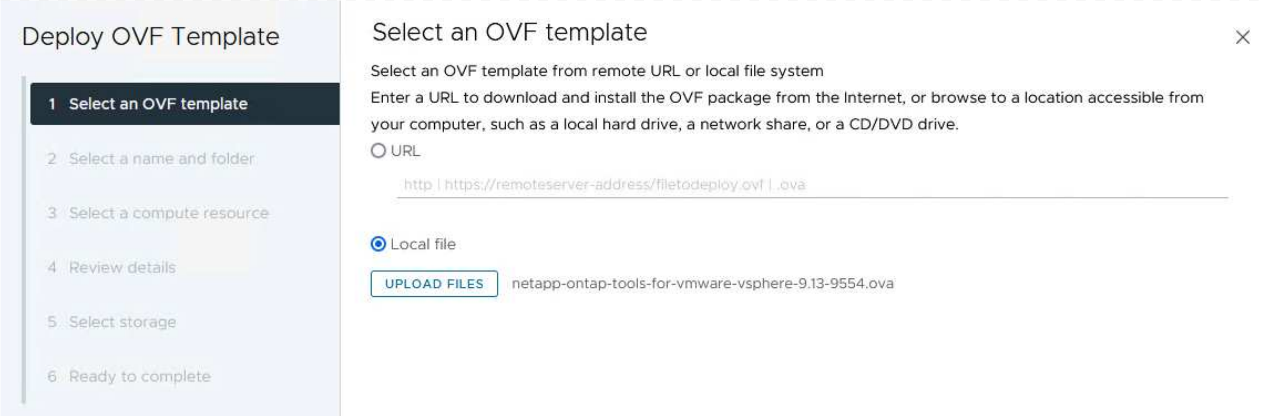
ONTAP tools for VMware vSphere (OTV) is deployed as a VM appliance and provides an integrated vCenter UI for managing ONTAP storage.

Complete the following to Deploy ONTAP tools for VMware vSphere:

1. Obtain the ONTAP tools OVA image from the NetApp Support site and download to a local folder.
2. Log into the vCenter appliance for the VCF management domain.
3. From the vCenter appliance interface right-click on the management cluster and select **Deploy OVF Template…**



4. In the **Deploy OVF Template** wizard click the **Local file** radio button and select the ONTAP tools OVA file downloaded in the previous step.



Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

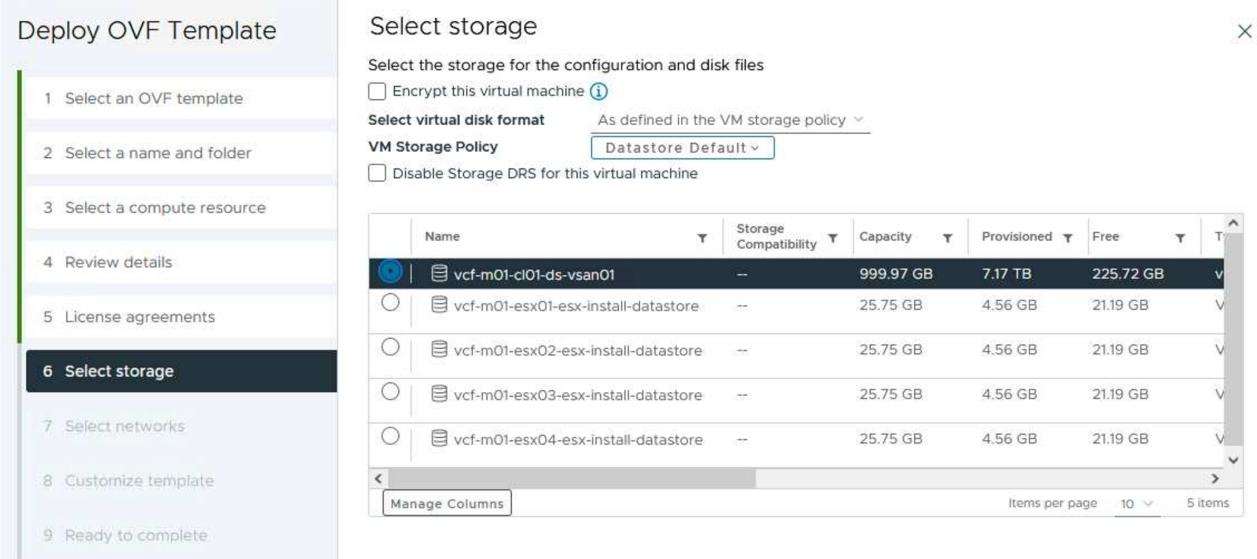
○ URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

● Local file

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. For steps 2 through 5 of the wizard select a name and folder for the VM, select the compute resource, review the details, and accept the license agreement.
6. For the storage location of the configuration and disk files, select the vSAN datastore of the VCF management domain cluster.



Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine

Select virtual disk format: As defined in the VM storage policy

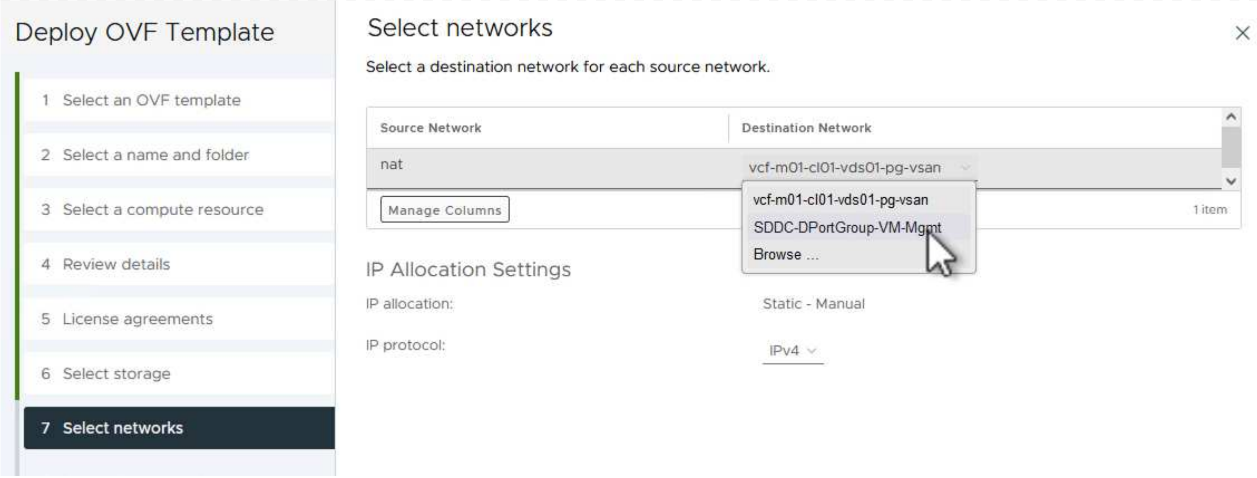
VM Storage Policy: Datastore Default

□ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	v
○	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V

Items per page 10 5 items

7. On the Select network page select the network used for management traffic.



Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	vcf-m01-cl01-vds01-pg-vsan

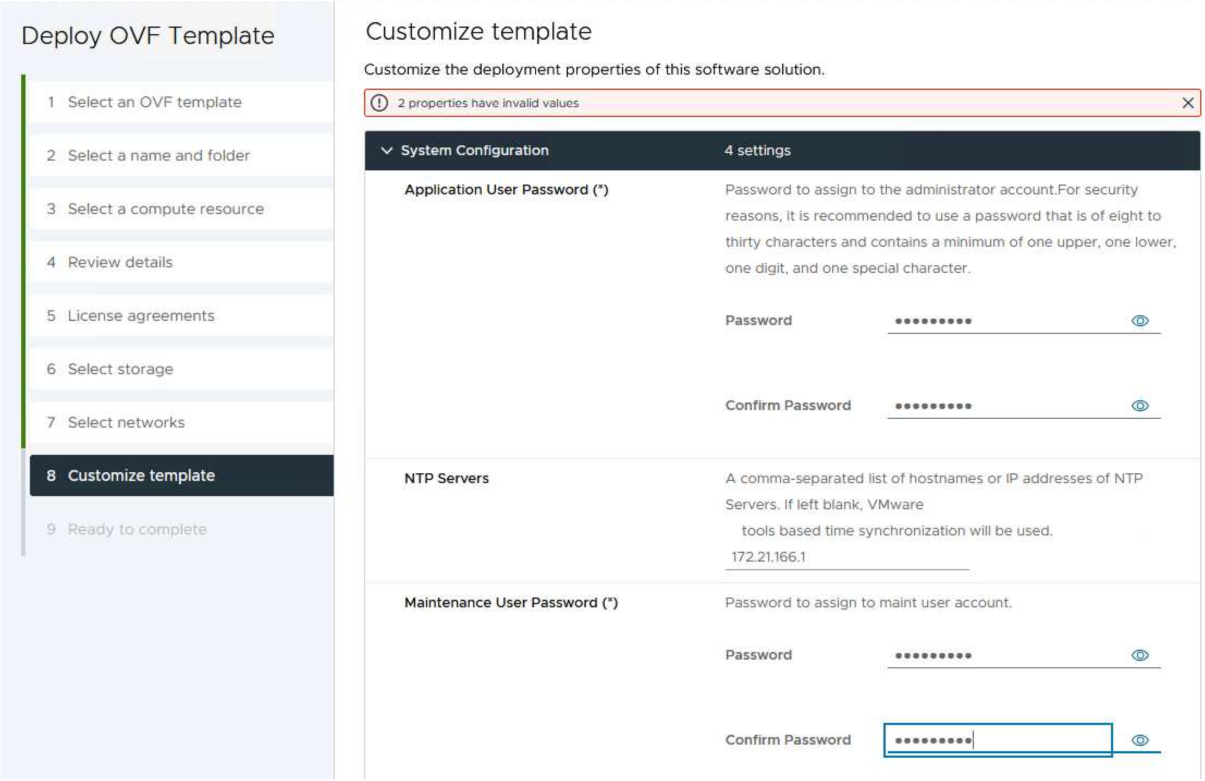
IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

8. On the Customize template page fill out all required information:
   - Password to be used for administrative access to OTV.
   - NTP server IP address.
   - OTV maintenance account password.
   - OTV Derby DB password.
   - Do not check the box to **Enable VMware Cloud Foundation (VCF)**. VCF mode is not required for deploying supplemental storage.
   - FQDN or IP address of the vCenter appliance for the **VI Workload Domain**
   - Credentials for the vCenter appliance of the **VI Workload Domain**
   - Provide the required network properties fields.

     Click on **Next** to continue.



Customize template

Customize the deployment properties of this software solution.

ⓘ 2 properties have invalid values

System Configuration — 4 settings

Application User Password (*): Password to assign to the administrator account.For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.

Password: •••••••••

Confirm Password: •••••••••

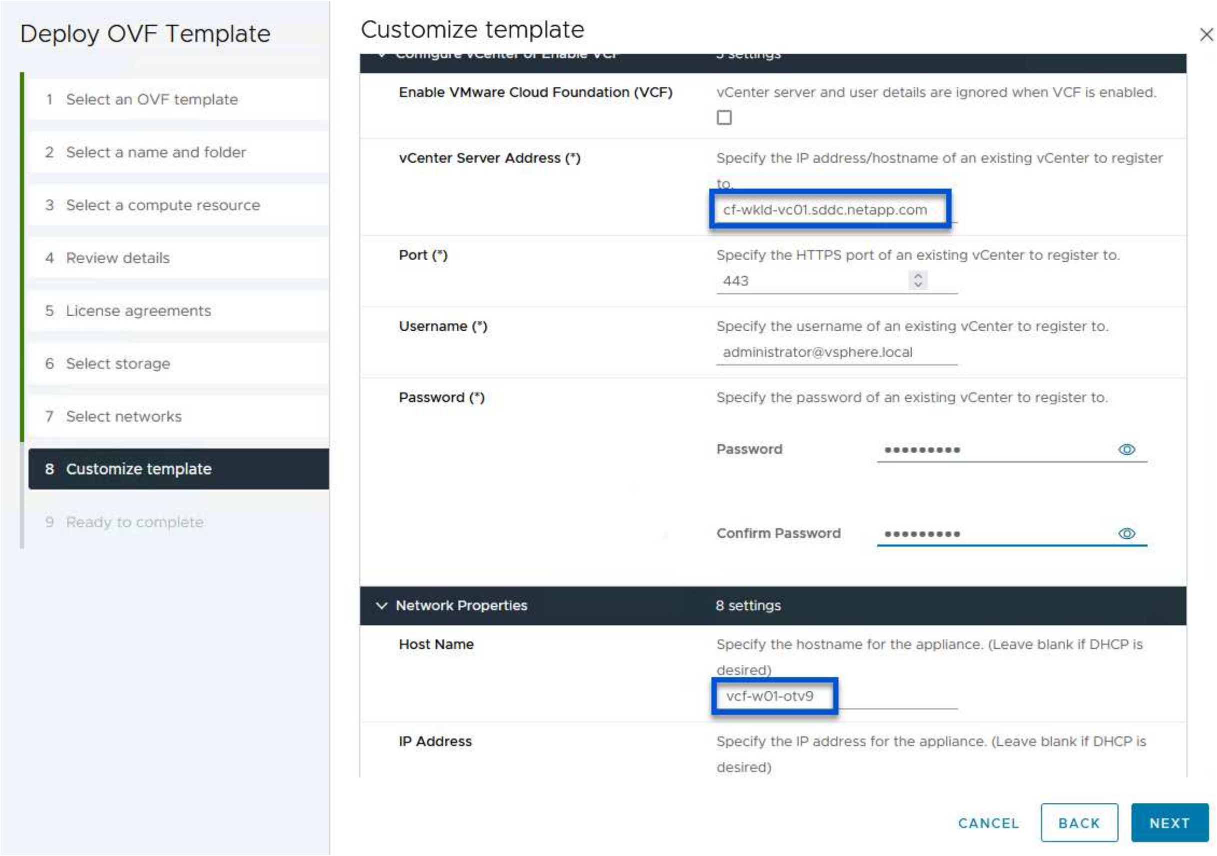
NTP Servers: A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used.

172.21.166.1

Maintenance User Password (*): Password to assign to maint user account.

Password: •••••••••

Confirm Password: •••••••••



Customize template

Configure vCenter or Enable VCF — 5 settings

Enable VMware Cloud Foundation (VCF): vCenter server and user details are ignored when VCF is enabled.

☐

vCenter Server Address (*): Specify the IP address/hostname of an existing vCenter to register to.

cf-wkld-vc01.sddc.netapp.com

Port (*): Specify the HTTPS port of an existing vCenter to register to.

443

Username (*): Specify the username of an existing vCenter to register to.

administrator@vsphere.local

Password (*): Specify the password of an existing vCenter to register to.

Password: •••••••••

Confirm Password: •••••••••

Network Properties — 8 settings

Host Name: Specify the hostname for the appliance. (Leave blank if DHCP is desired)

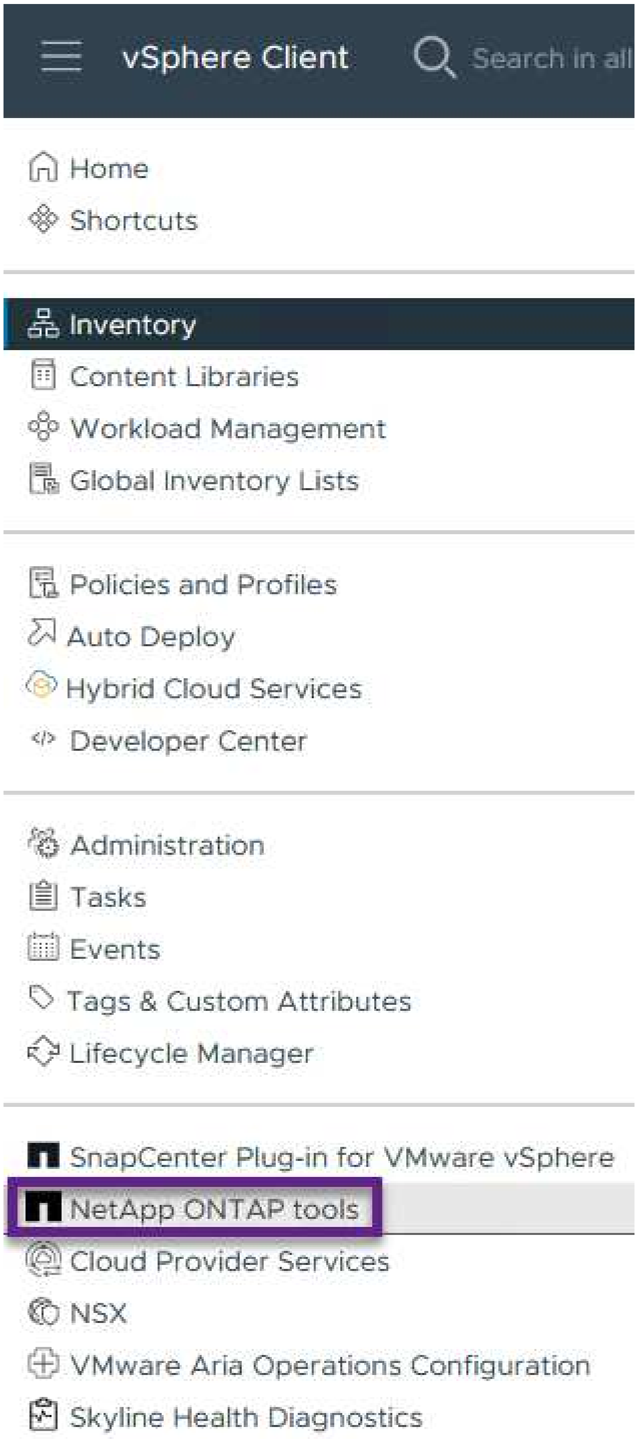
vcf-w01-otv9

IP Address: Specify the IP address for the appliance. (Leave blank if DHCP is desired)

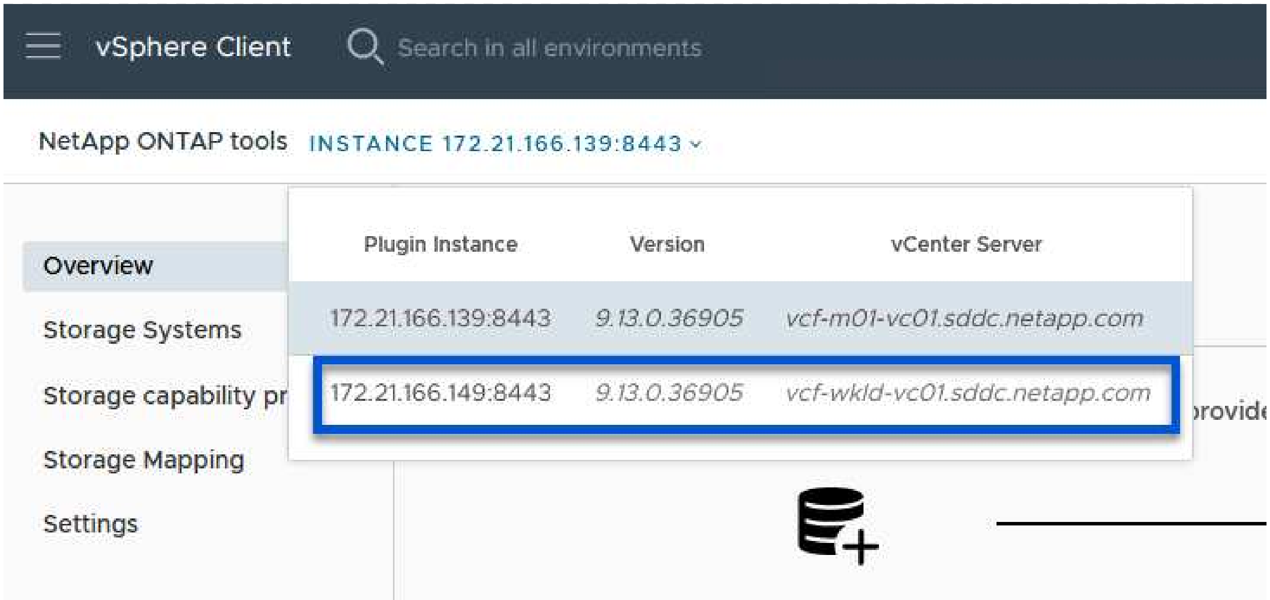
9. Review all information on the Ready to complete page and the click Finish to begin deploying the OTV appliance.

Add a storage system to ONTAP Tools.

1. Access NetApp ONTAP Tools by selecting it from the main menu in the vSphere client.

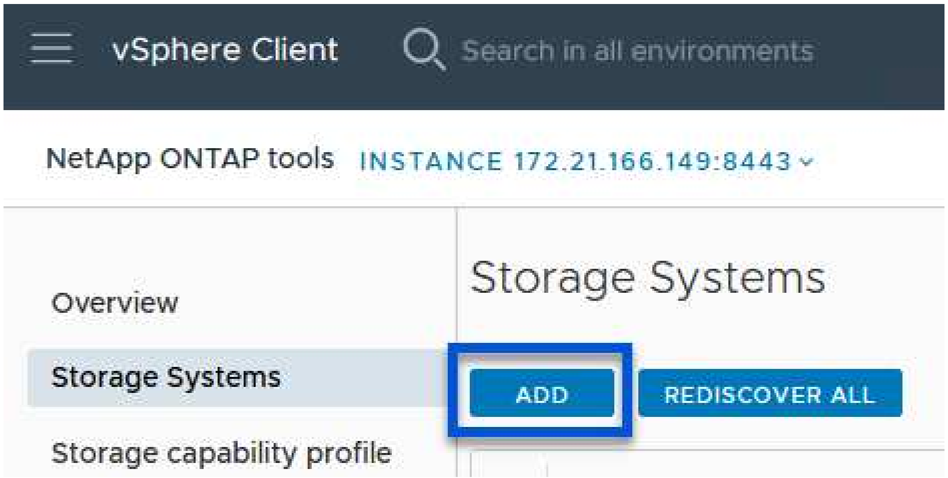


2. From the **INSTANCE** drop down menu in the ONTAP Tool interface, select the OTV instance associated with the workload domain to be managed.

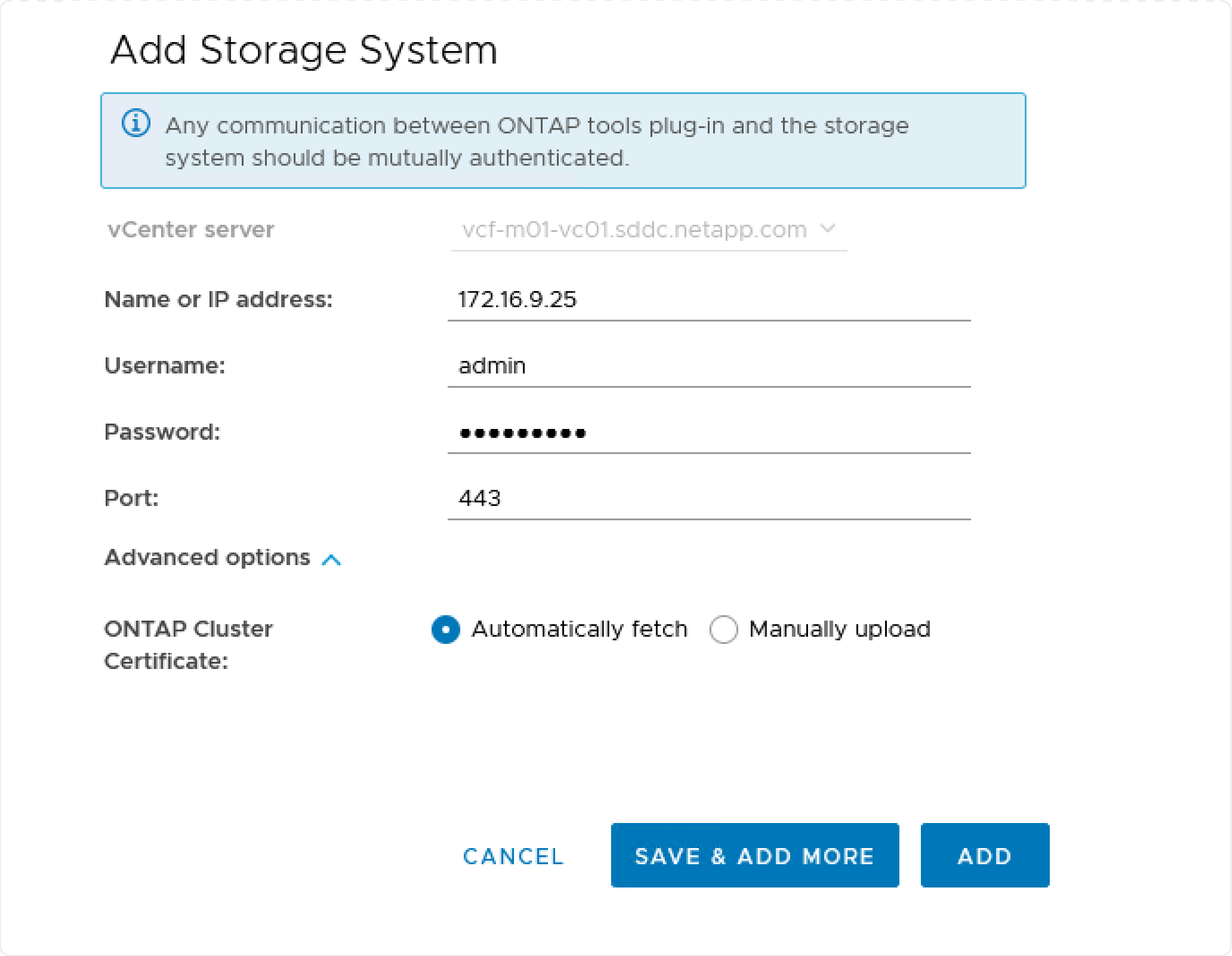


Plugin Instance	Version	vCenter Server
172.21.166.139:8443	9.13.0.36905	vcf-m01-vc01.sddc.netapp.com
172.21.166.149:8443	9.13.0.36905	vcf-wkld-vc01.sddc.netapp.com

3. In ONTAP Tools select **Storage Systems** from the left hand menu and then press **Add**.



4. Fill out the IP Address, credentials of the storage system and the port number. Click on **Add** to start the discovery process.



Add Storage System

Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server: vcf-m01-vc01.sddc.netapp.com

Name or IP address: 172.16.9.25

Username: admin

Password: ••••••••••

Port: 443

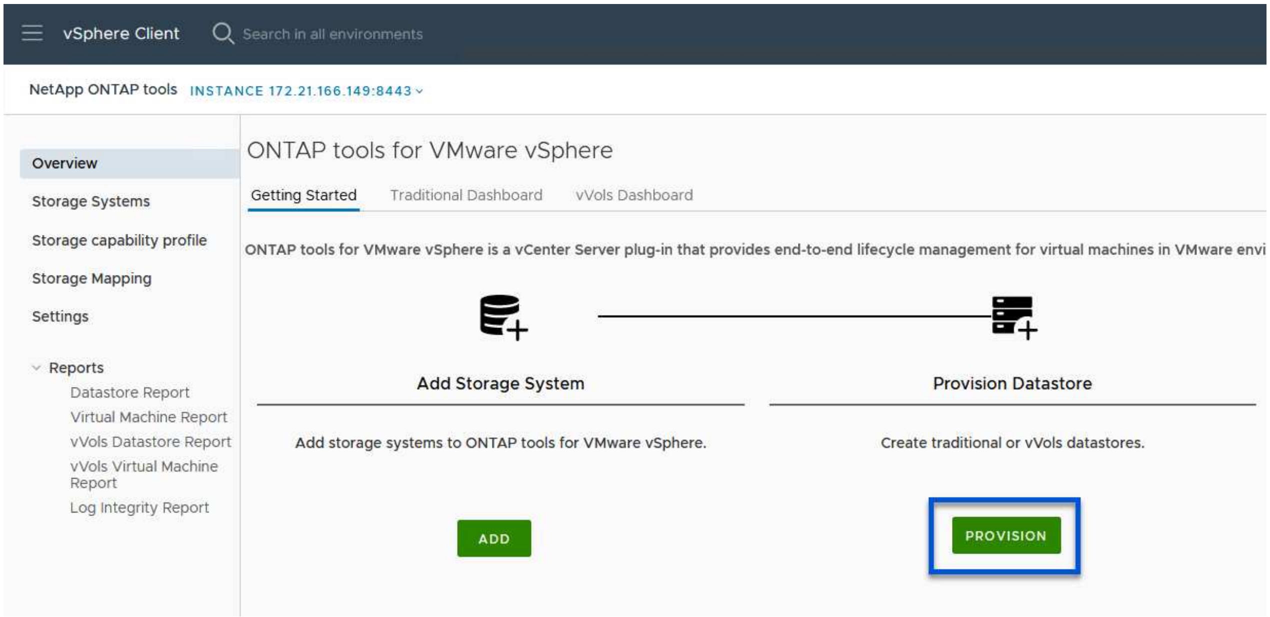
Advanced options

ONTAP Cluster Certificate: ● Automatically fetch ○ Manually upload

Create an NFS datastore in ONTAP Tools

Complete the following steps to deploy an ONTAP datastore, running on NFS, using ONTAP Tools.

1. In ONTAP Tools select **Overview** and from the **Getting Started** tab click on **Provision** to start the wizard.



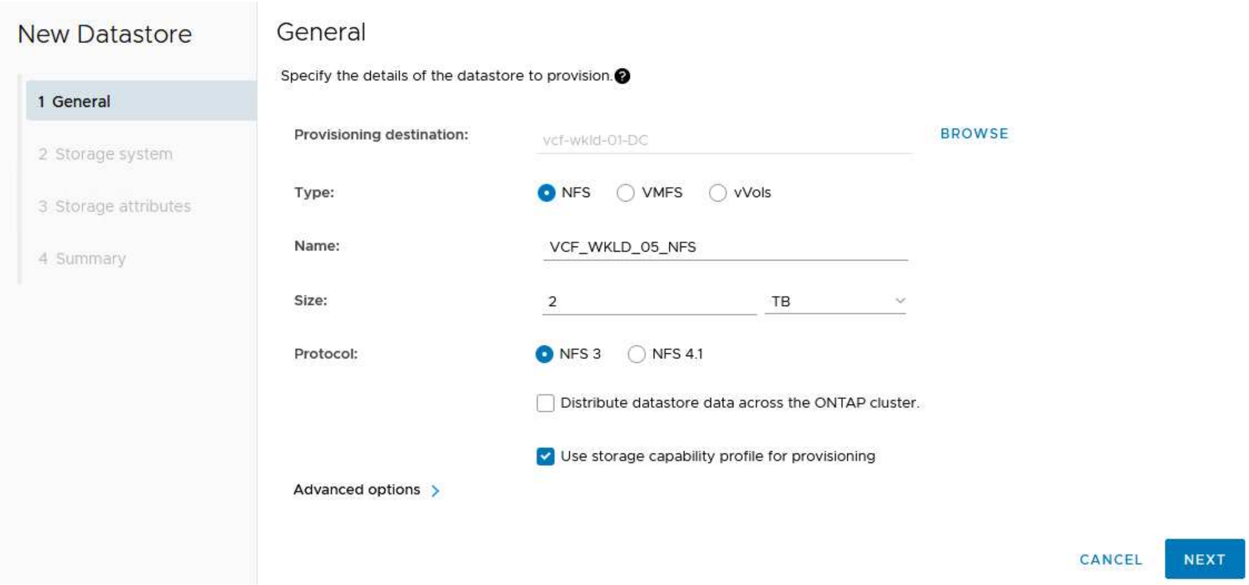
ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware envi

Add storage systems to ONTAP tools for VMware vSphere.

Create traditional or vVols datastores.

2. On the **General** page of the New Datastore wizard select the vSphere datacenter or cluster destination. Select **NFS** as the datastore type, fill out a name for the datastore, and select the protocol. Choose whether to use FlexGroup volumes and whether to use a storage capability file for provisioning. Click on **Next** to continue.

   Note: Selecting to **Distribute datastore data across the cluster** will create the underlying volume as a FlexGroup volume which precludes the use of Storage Capability Profiles. Refer to Supported and unsupported configurations for FlexGroup volumes for more information on using FlexGroup Volumes.



Specify the details of the datastore to provision.

Provisioning destination: vcf-wkld-01-DC

Type: ● NFS ○ VMFS ○ vVols

Name: VCF_WKLD_05_NFS

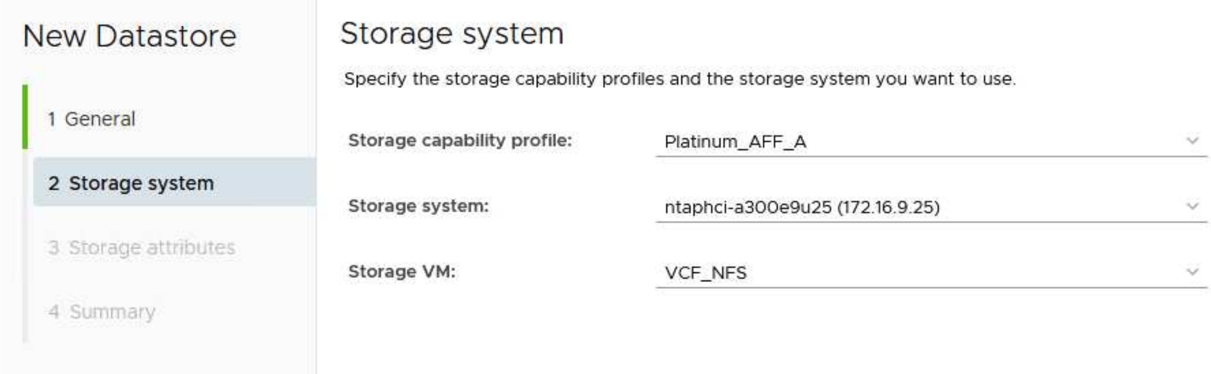
Size: 2 TB

Protocol: ● NFS 3 ○ NFS 4.1

☐ Distribute datastore data across the ONTAP cluster.

☑ Use storage capability profile for provisioning

3. On the **Storage system** page select the select a storage capability profile, the storage system and SVM. Click on **Next** to continue.



Storage system

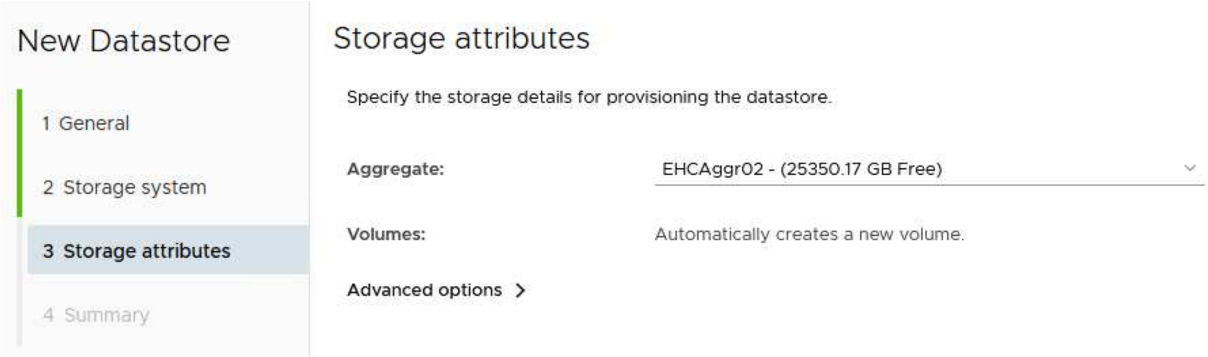
Specify the storage capability profiles and the storage system you want to use.

Storage capability profile: Platinum_AFF_A

Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: VCF_NFS

4. On the **Storage attributes** page select the aggregate to use and then click on **Next** to continue.



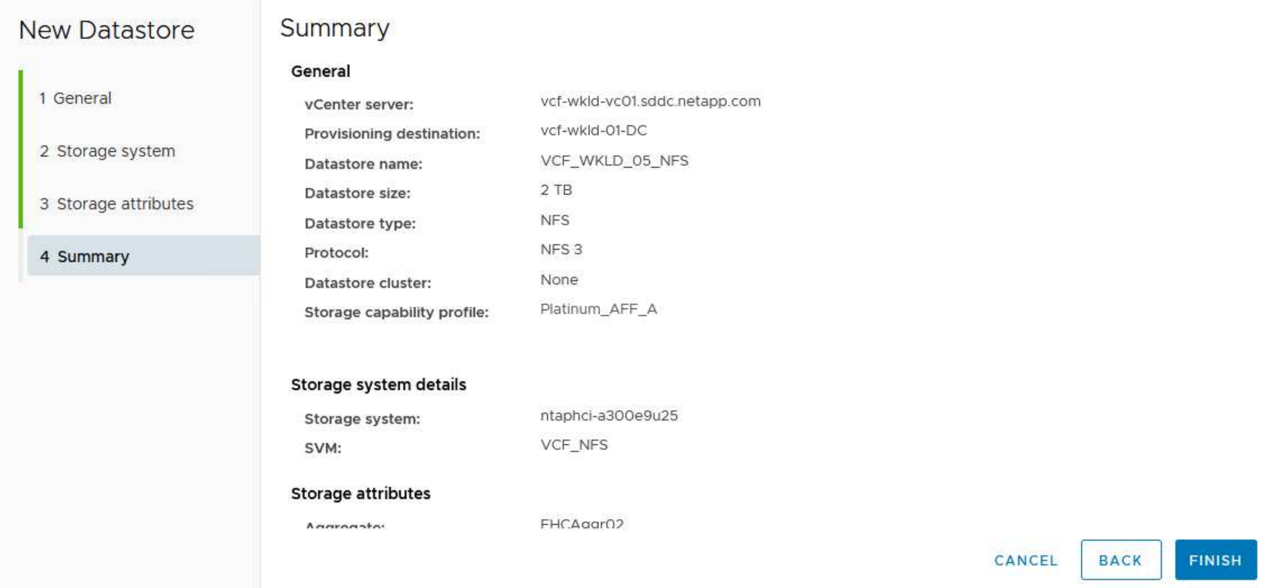
Storage attributes

Specify the storage details for provisioning the datastore.

Aggregate: EHCAggr02 - (25350.17 GB Free)

Volumes: Automatically creates a new volume.

5. Finally, review the **Summary** and click on Finish to begin creating the NFS datastore.



Summary

General

vCenter server: vcf-wkld-vc01.sddc.netapp.com

Provisioning destination: vcf-wkld-01-DC

Datastore name: VCF_WKLD_05_NFS

Datastore size: 2 TB

Datastore type: NFS

Protocol: NFS 3

Datastore cluster: None

Storage capability profile: Platinum_AFF_A

Storage system details

Storage system: ntaphci-a300e9u25

SVM: VCF_NFS

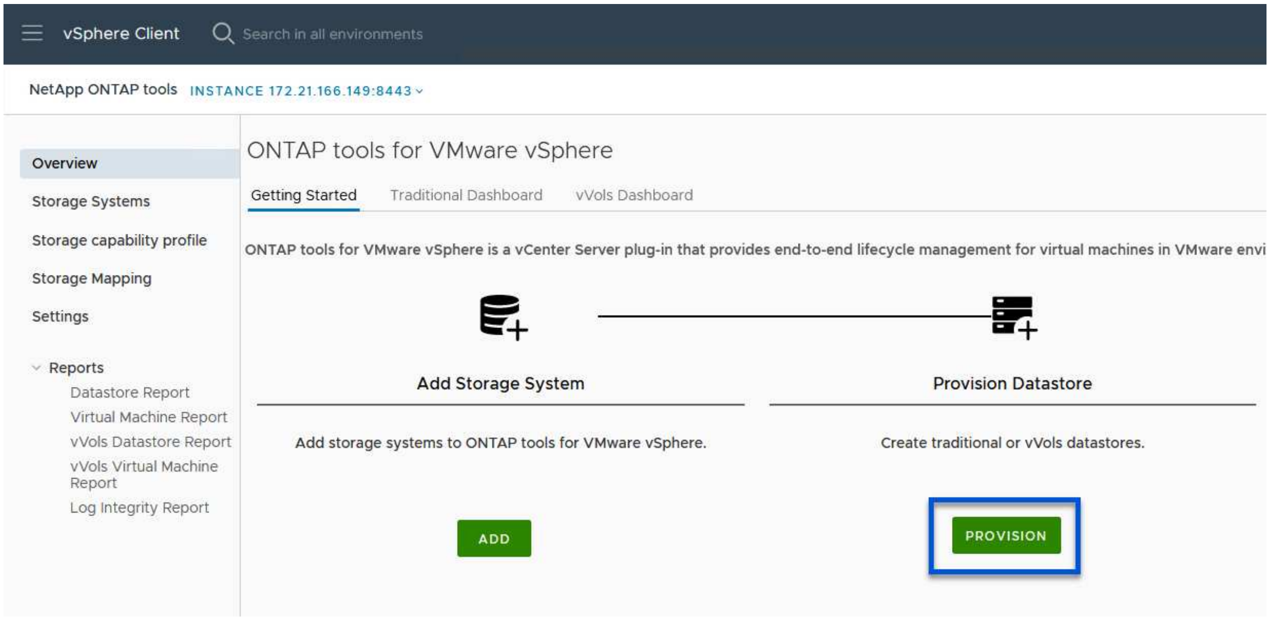
Storage attributes

Aggregate: EHCAggr02

Create a vVols datastore in ONTAP Tools

To create a vVols datastore in ONTAP Tools complete the following steps:

1. In ONTAP Tools select **Overview** and from the **Getting Started** tab click on **Provision** to start the wizard.

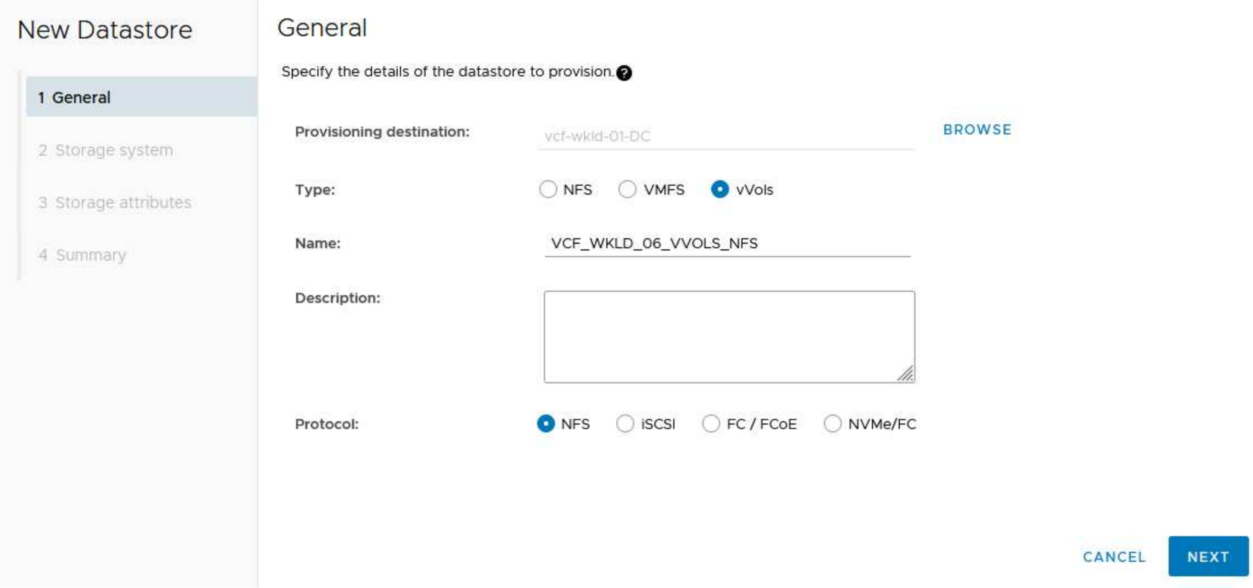


ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware envi

Add storage systems to ONTAP tools for VMware vSphere.

Create traditional or vVols datastores.

2. On the **General** page of the New Datastore wizard select the vSphere datacenter or cluster destination. Select **vVols** as the datastore type, fill out a name for the datastore, and select **NFS** as the protocol. Click on **Next** to continue.



General

Specify the details of the datastore to provision.

Provisioning destination: vcf-wkld-01-DC

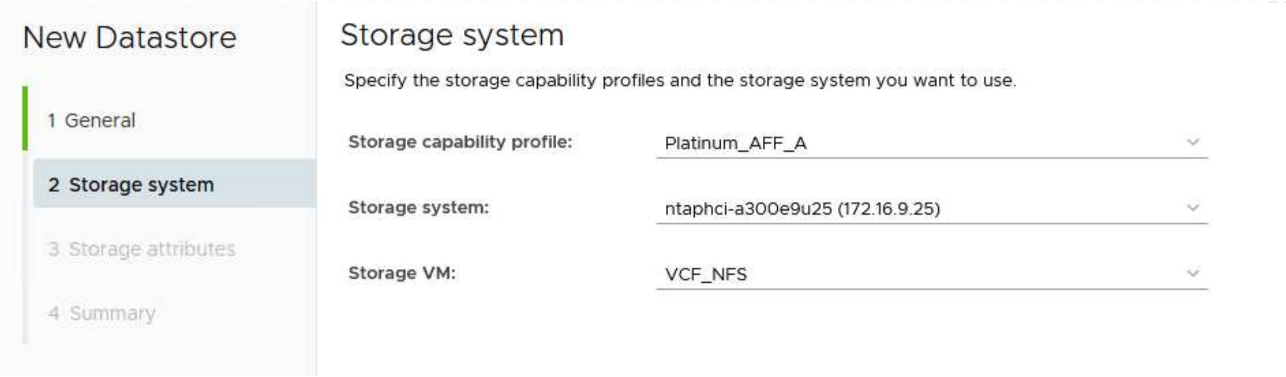
Type: ○ NFS ○ VMFS ● vVols

Name: VCF_WKLD_06_VVOLS_NFS

Description:

Protocol: ● NFS ○ iSCSI ○ FC / FCoE ○ NVMe/FC

3. On the **Storage system** page select the select a storage capability profile, the storage system and SVM. Click on **Next** to continue.



New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

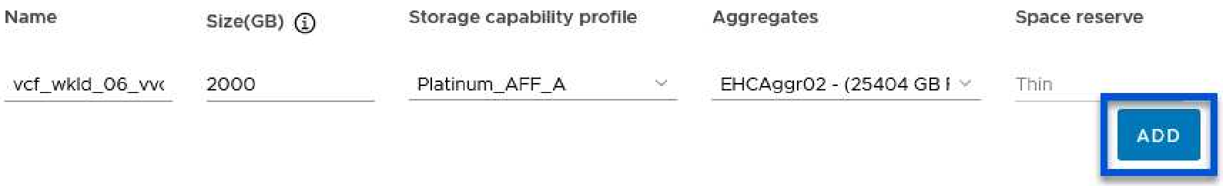
Specify the storage capability profiles and the storage system you want to use.

Storage capability profile: Platinum_AFF_A

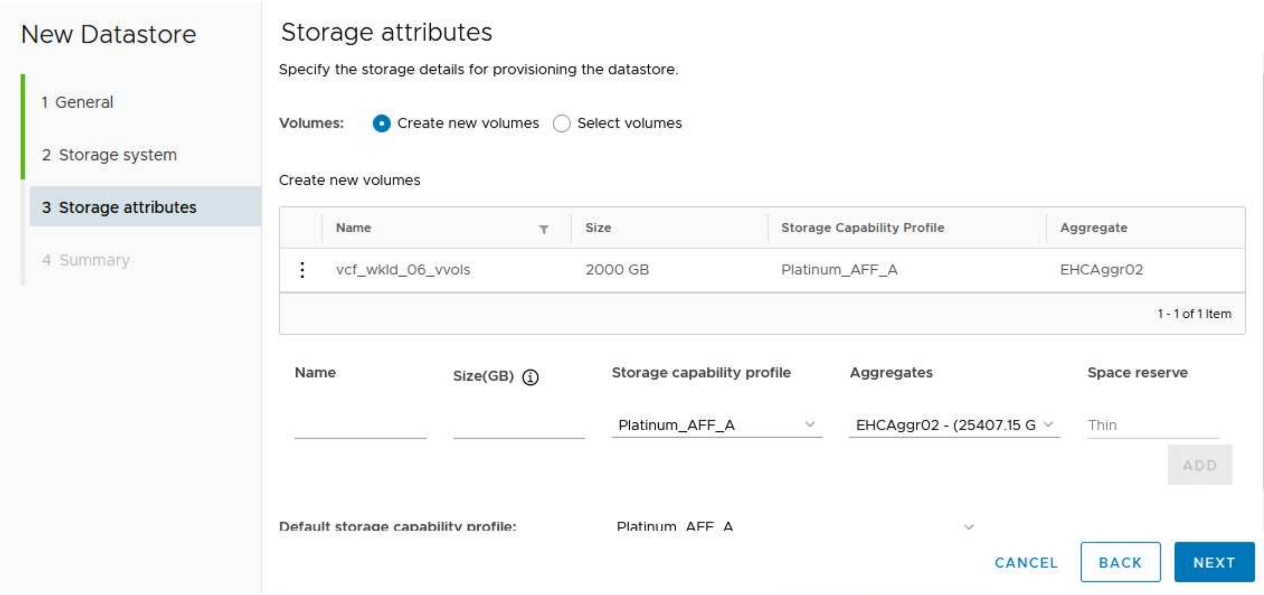
Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: VCF_NFS

4. On the **Storage attributes** page select to create a new volume for the datastore and fill out the storage attributes of the volume to be created. Click on **Add** to create the volume and then **Next** to continue.



Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
vcf_wkld_06_vv(	2000	Platinum_AFF_A	EHCAggr02 - (25404 GB F	Thin



New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: ● Create new volumes ○ Select volumes

Create new volumes

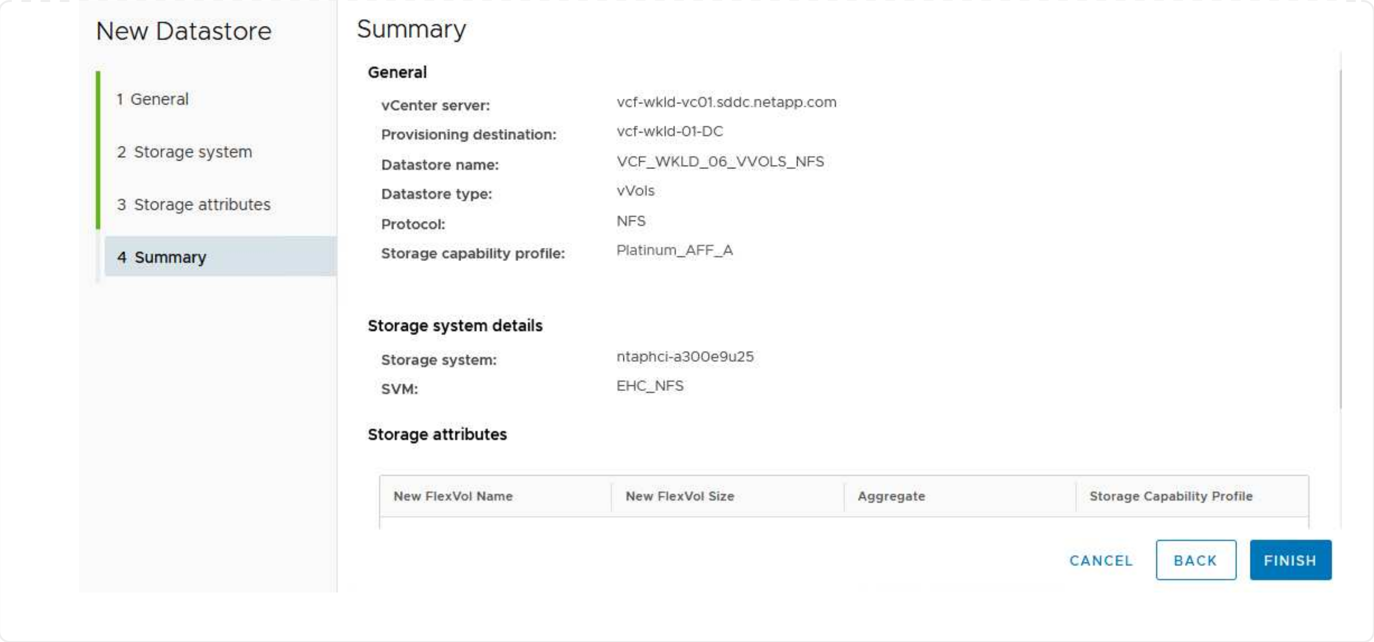
	Name	Size	Storage Capability Profile	Aggregate
⋮	vcf_wkld_06_vvols	2000 GB	Platinum_AFF_A	EHCAggr02

1 - 1 of 1 Item

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
		Platinum_AFF_A	EHCAggr02 - (25407.15 G	Thin

Default storage capability profile: Platinum_AFF_A

5. Finally, review the **Summary** and click on **Finish** to start the vVol datastore creation process.



Summary

General

vCenter server: vcf-wkld-vc01.sddc.netapp.com
Provisioning destination: vcf-wkld-01-DC
Datastore name: VCF_WKLD_06_VVOLS_NFS
Datastore type: vVols
Protocol: NFS
Storage capability profile: Platinum_AFF_A

Storage system details

Storage system: ntaphci-a300e9u25
SVM: EHC_NFS

Storage attributes

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile

Additional information

For information on configuring ONTAP storage systems refer to the ONTAP 9 Documentation center.

For information on configuring VCF refer to VMware Cloud Foundation Documentation.

Migration of VMs

Migrate VMs to ONTAP Datastores

Author: Suresh Thoppay

VMware vSphere by Broadcom supports VMFS, NFS, and vVol datastores for hosting virtual machines. Customers have the option to create those datastores with hyper converged infrastructures or with centralized shared storage systems. Customers often see the value with hosting on ONTAP based storage systems to provide space efficient snapshots and clones of Virtual machines, flexiblity to choose various deployment models across the datacenters and clouds, operational efficiency with monitoring and alerting tools, security, governance and optional compliance tools to inspect VM data, etc,.

VMs hosted on ONTAP datastores can be protected using SnapCenter Plugin for VMware vSphere (SCV). SCV creates storage based snapshots and also replicates to remote ONTAP storage system. Restores can be performed either from Primary or Secondary storage systems.

Customers has flexibility to choose Cloud Insights or Aria Operations or combination of both or other third party tools that use ONTAP api to troubleshoot, performance monitoring, reporting and alert notification features.

Customers can easily provision datastore using ONTAP Tools vCenter Plug-in or its API and VMs can be migrated to ONTAP datastores even while it is powered on.

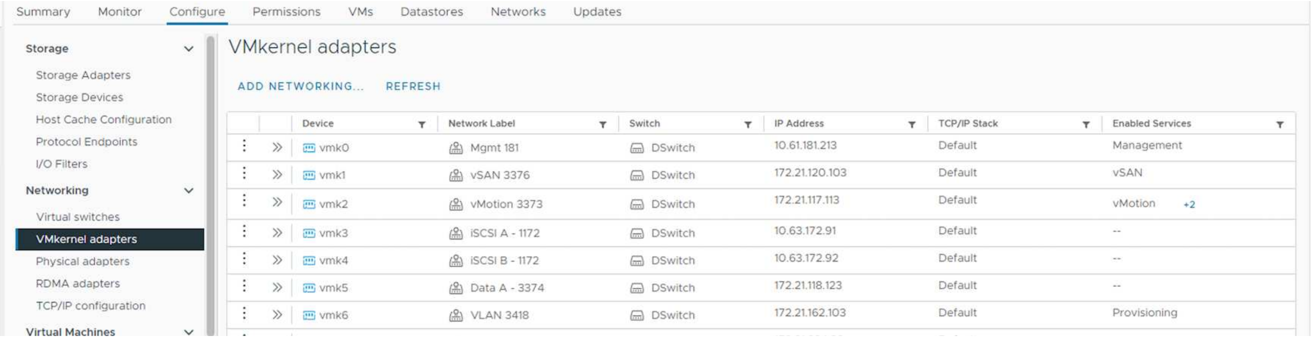
ⓘ Some VMs which are deployed with external management tool like Aria Automation, Tanzu (or other Kubernetes flavors) are usually depends on VM storage policy. If migrating between the datastores within same VM storage policy, it should be of less impact for the applications. Check with Application owners to properly migrate those VMs to new datastore. vSphere 8 introduced vMotion notification to prepare application for the vMotion.

Network Requirements

VM migration with vMotion

It is assumed that dual storage network is already in place for the ONTAP datastore to provide connectivity, fault tolerance and performance boost.

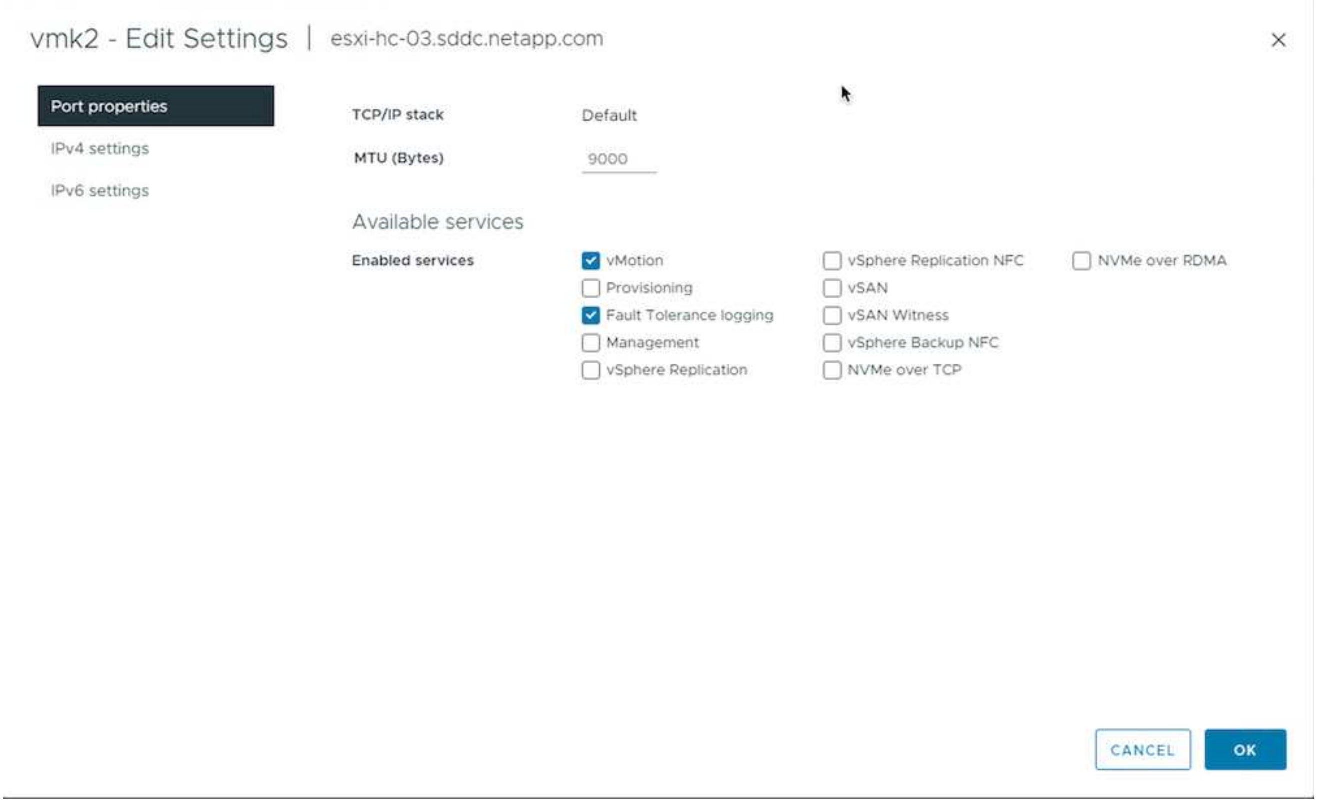
Migration of VMs across the vSphere hosts are also handled by the VMKernel interface of the vSphere host. For hot migration (powered on VMs), VMKernel interface with vMotion enabled service is used and for cold migration (powered off VMs), VMKernel interface with Provisioning service enabled is consumed to move the data. If no valid interface was found, it will use the management interface to move the data which may not be desirable for certain use cases.



VMkernel adapters

Device	Network Label	Switch	IP Address	TCP/IP Stack	Enabled Services
vmk0	Mgmt 181	DSwitch	10.61.181.213	Default	Management
vmk1	vSAN 3376	DSwitch	172.21.120.103	Default	vSAN
vmk2	vMotion 3373	DSwitch	172.21.117.113	Default	vMotion +2
vmk3	iSCSI A - 1172	DSwitch	10.63.172.91	Default	--
vmk4	iSCSI B - 1172	DSwitch	10.63.172.92	Default	--
vmk5	Data A - 3374	DSwitch	172.21.118.123	Default	--
vmk6	VLAN 3418	DSwitch	172.21.162.103	Default	Provisioning

When you edit the VMKernel interface, here is the option to enable the required services.



vmk2 - Edit Settings | esxi-hc-03.sddc.netapp.com

TCP/IP stack: Default

MTU (Bytes): 9000

Available services

Enabled services

☑ vMotion
□ Provisioning
☑ Fault Tolerance logging
□ Management
□ vSphere Replication
□ vSphere Replication NFC
□ vSAN
□ vSAN Witness
□ vSphere Backup NFC
□ NVMe over TCP
□ NVMe over RDMA

Ensure at least two high-speed active uplink nics are available for the portgroup used by vMotion and Provisioning VMkernel interfaces.

VM Migration Scenarios

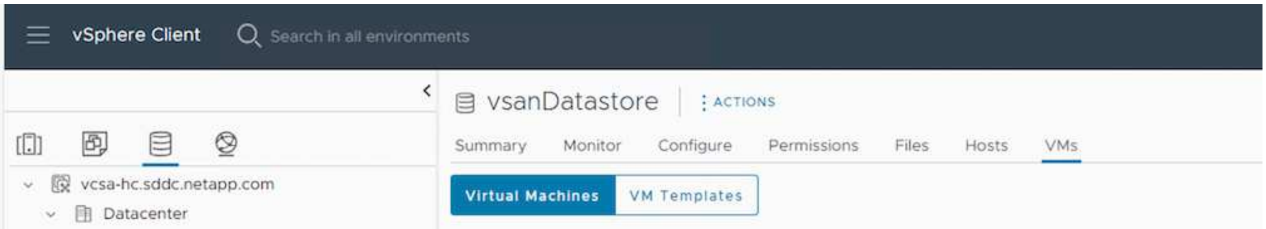
vMotion is often used to migrate the VMs irrespective of its power state. Additional considerations and migration procedure for specific scenarios is available below.

ⓘ Understand VM Conditions and Limitation of vSphere vMotion before proceeding with any VM migration options.

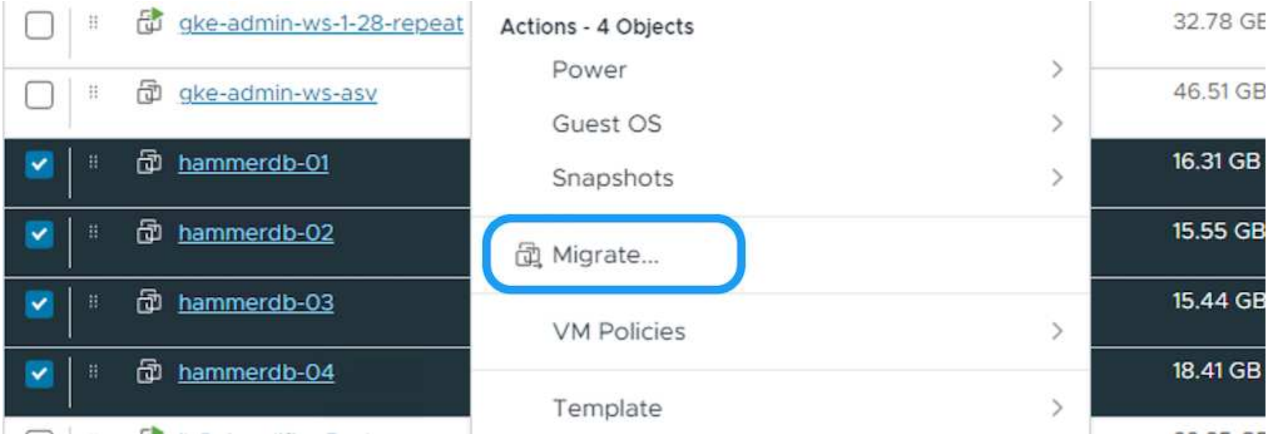
Migration of VMs from specific vSphere Datastore

Follow the procedure below to migrate VMs to new Datastore using UI.

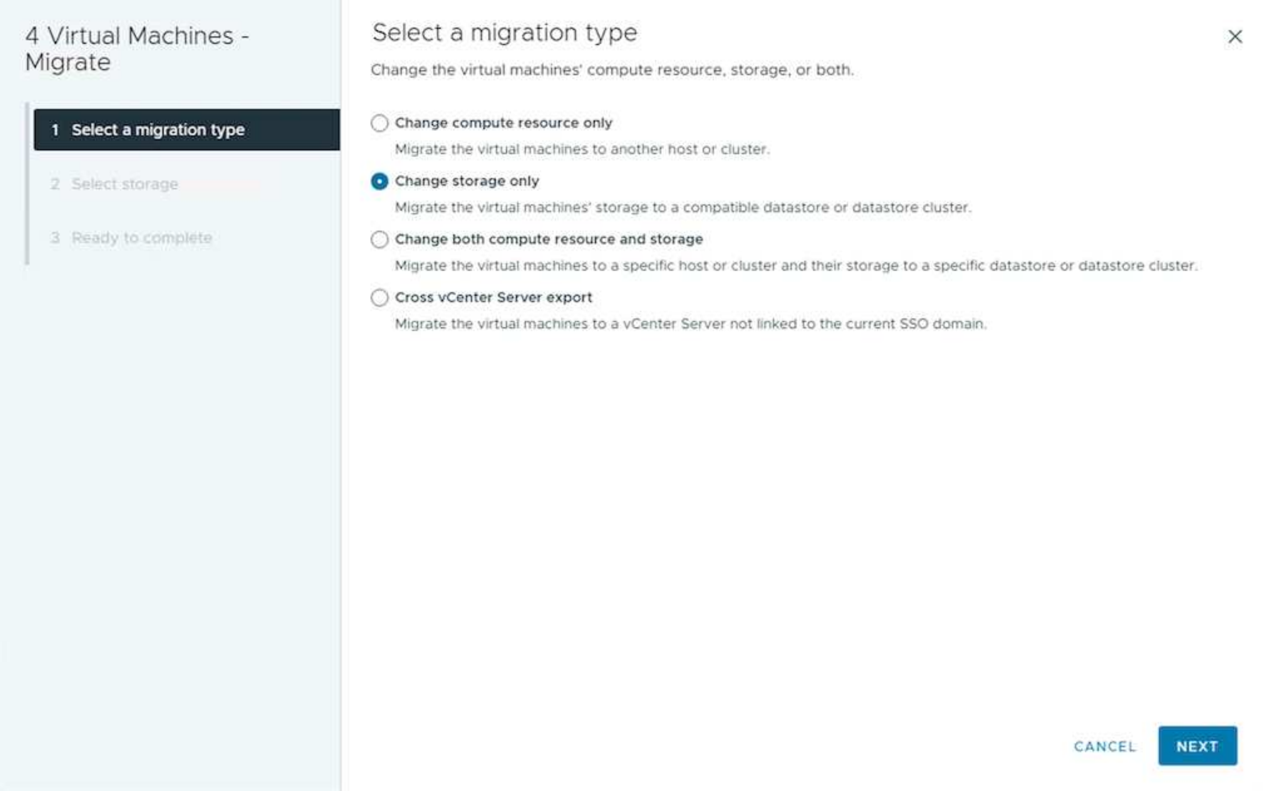
1. With vSphere Web Client, select the Datastore from the storage inventory and click on VMs tab.



2. Select the VMs that needs to be migrated and right click to select Migrate option.



3. Choose option to change storage only, Click Next



Select a migration type

Change the virtual machines' compute resource, storage, or both.

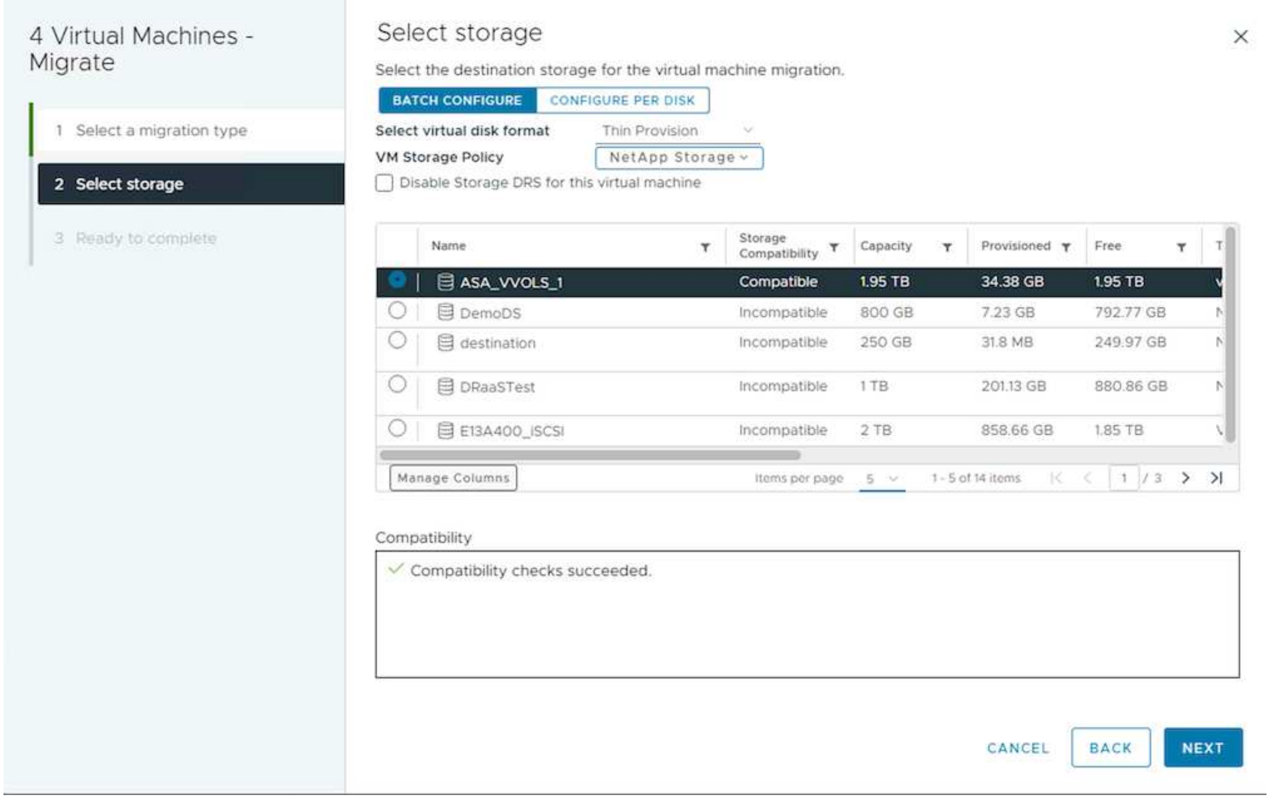
○ Change compute resource only
Migrate the virtual machines to another host or cluster.

● Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

○ Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

○ Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

4. Select the desired VM Storage Policy and pick the datastore that is compatible. Click Next.



Select storage

Select the destination storage for the virtual machine migration.

Select virtual disk format: Thin Provision

VM Storage Policy: NetApp Storage

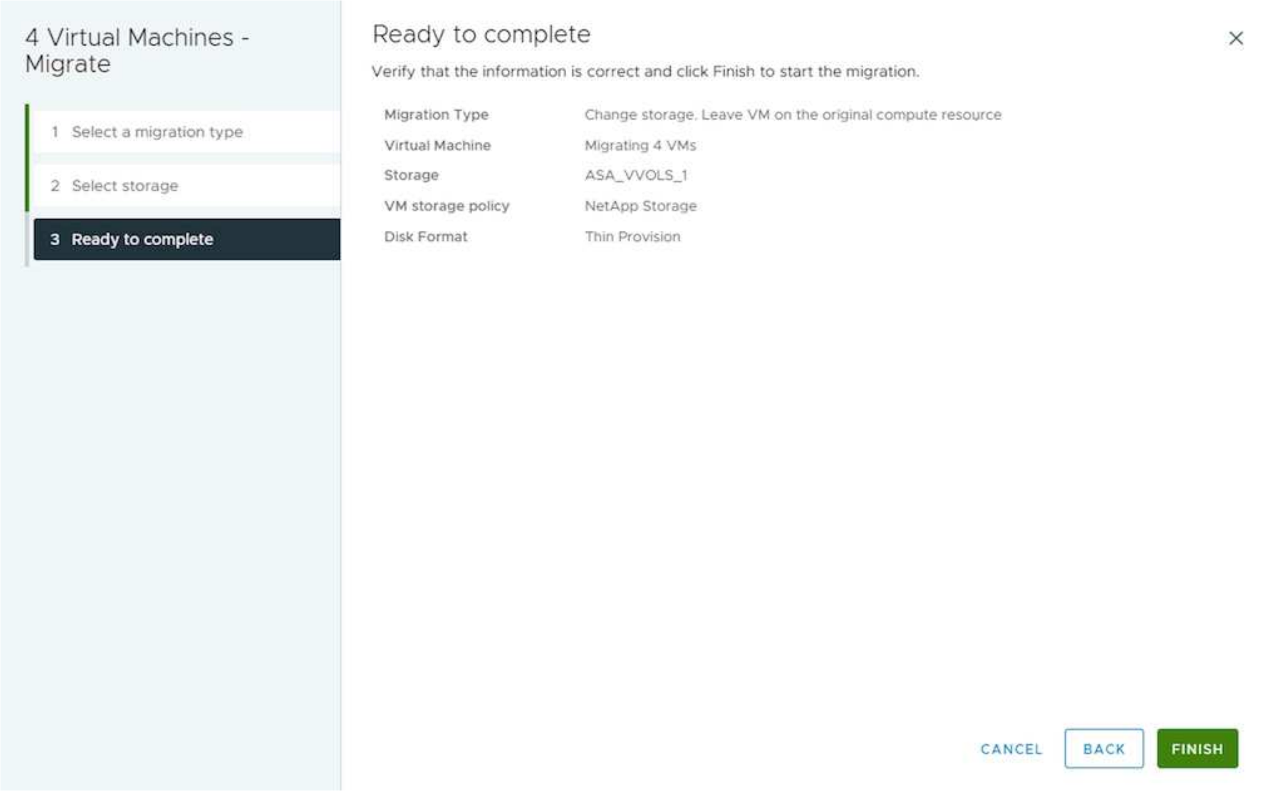
□ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB	V
○	DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB	N
○	destination	Incompatible	250 GB	31.8 MB	249.97 GB	N
○	DRaaSTest	Incompatible	1 TB	201.13 GB	880.86 GB	N
○	E13A400_ISCSI	Incompatible	2 TB	858.66 GB	1.85 TB	V

Compatibility

✓ Compatibility checks succeeded.

5. Review and click on Finish.



Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

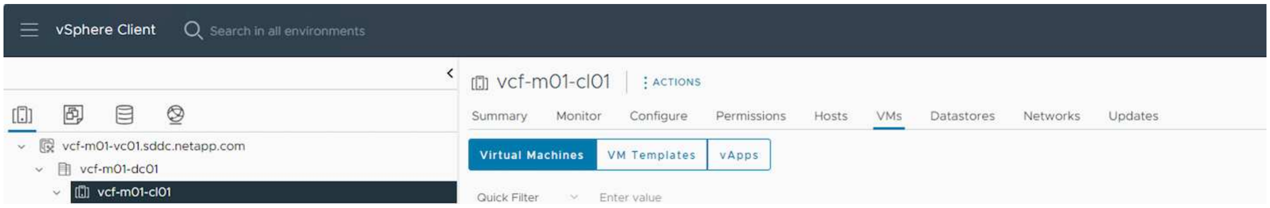
To migrate VMs using PowerCLI, here is the sample script.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific datastore
$vm = Get-DataStore 'vSanDatastore' | Get-VM Har*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

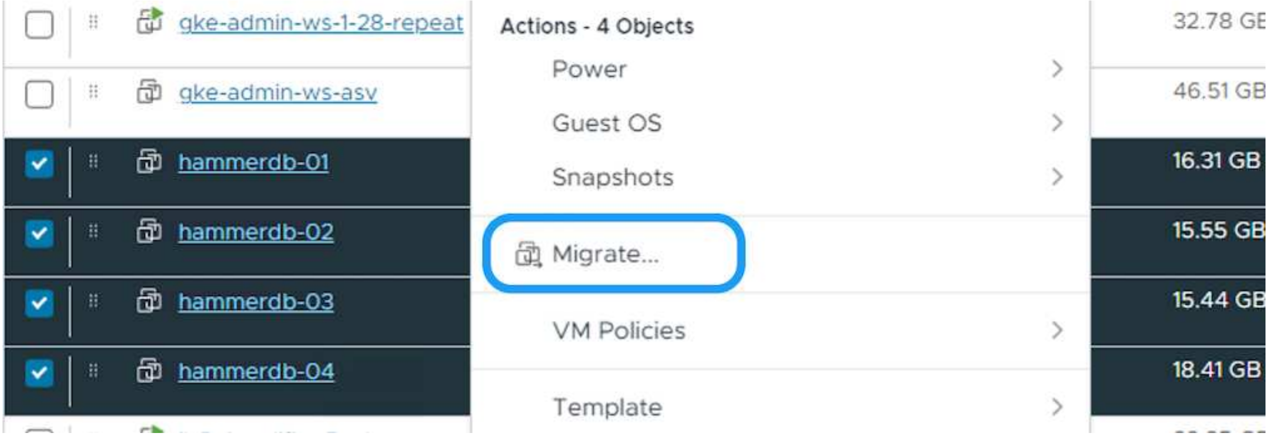
Migration of VMs in same vSphere cluster

Follow the procedure below to migrate VMs to new Datastore using UI.

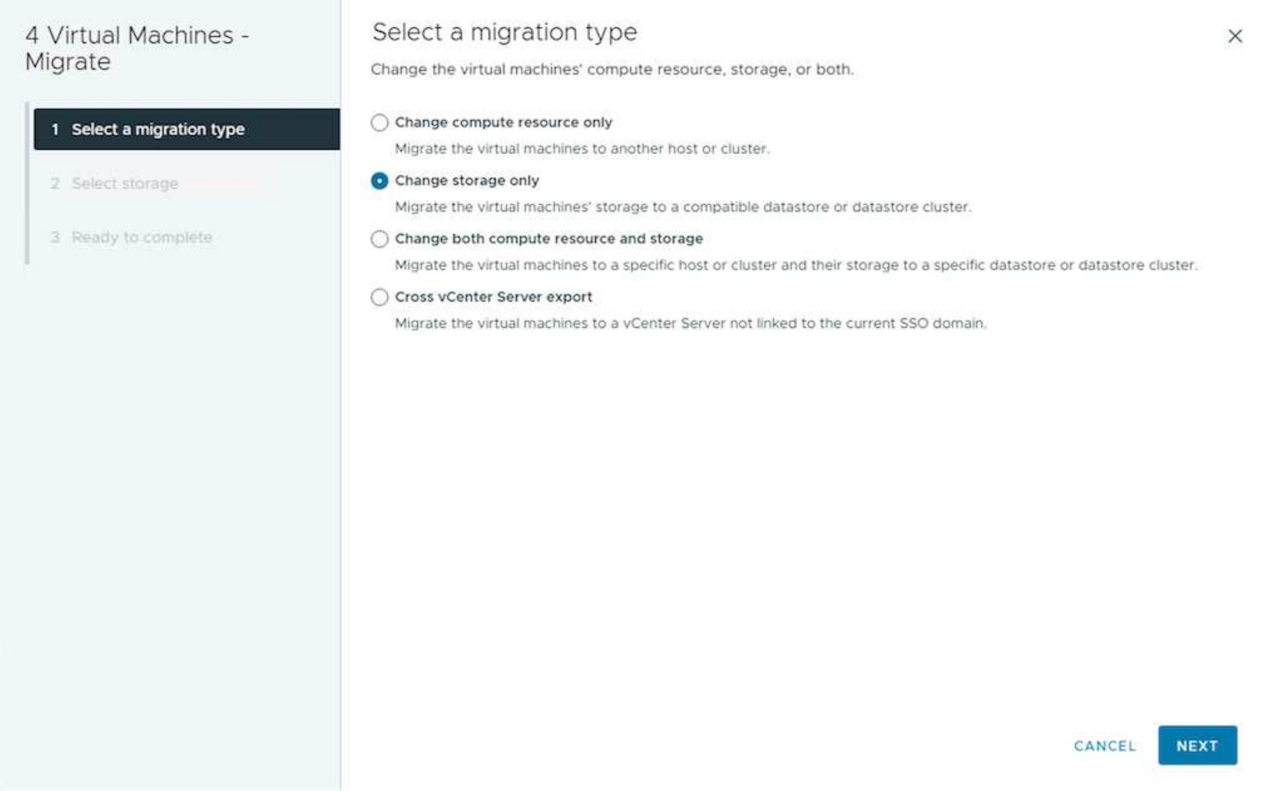
1. With vSphere Web Client, select the Cluster from the Host and Cluster inventory and click on VMs tab.



2. Select the VMs that needs to be migrated and right click to select Migrate option.



3. Choose option to change storage only, Click Next


4 Virtual Machines - Migrate

1 Select a migration type
2 Select storage
3 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

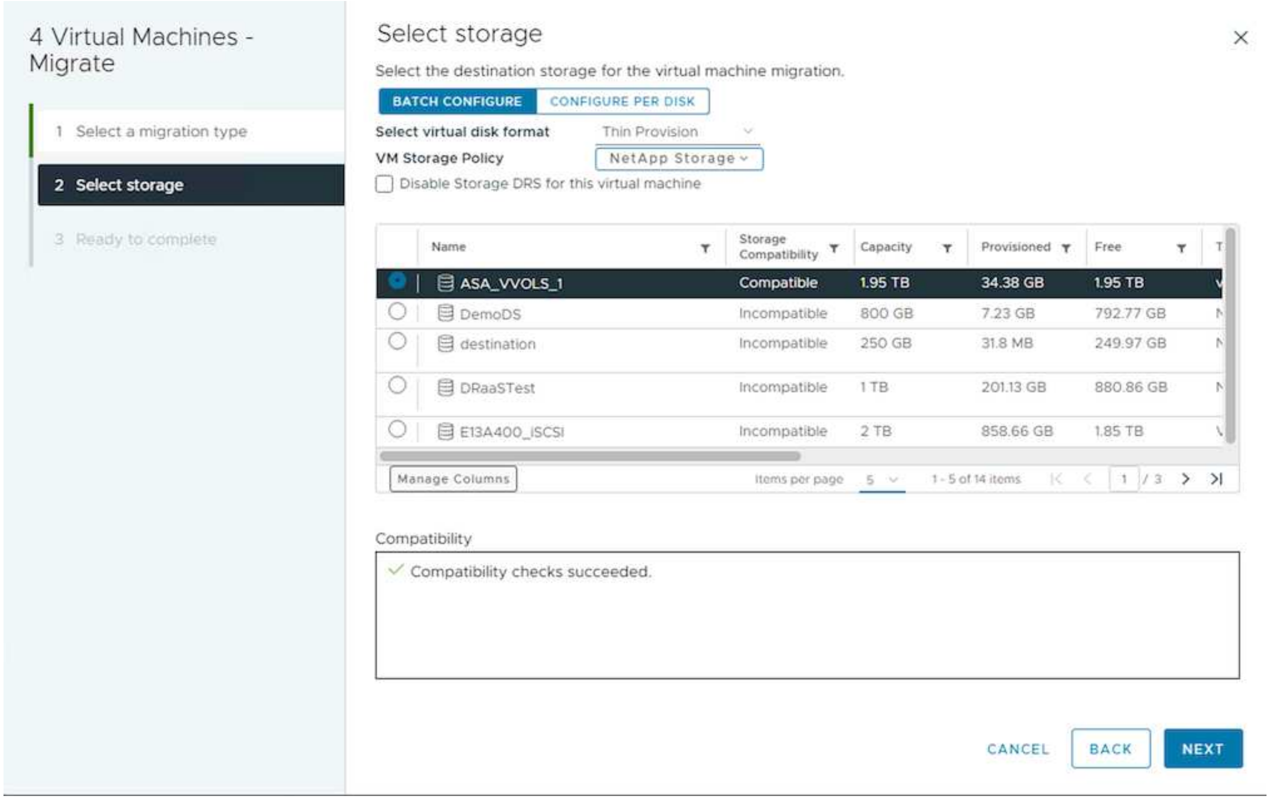
○ Change compute resource only
Migrate the virtual machines to another host or cluster.

● Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

○ Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

○ Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

4. Select the desired VM Storage Policy and pick the datastore that is compatible. Click Next.



4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE | CONFIGURE PER DISK

Select virtual disk format: Thin Provision

VM Storage Policy: NetApp Storage

□ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB	V
○	DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB	N
○	destination	Incompatible	250 GB	31.8 MB	249.97 GB	N
○	DRaaSTest	Incompatible	1 TB	201.13 GB	880.86 GB	N
○	E13A400_ISCSI	Incompatible	2 TB	858.66 GB	1.85 TB	V

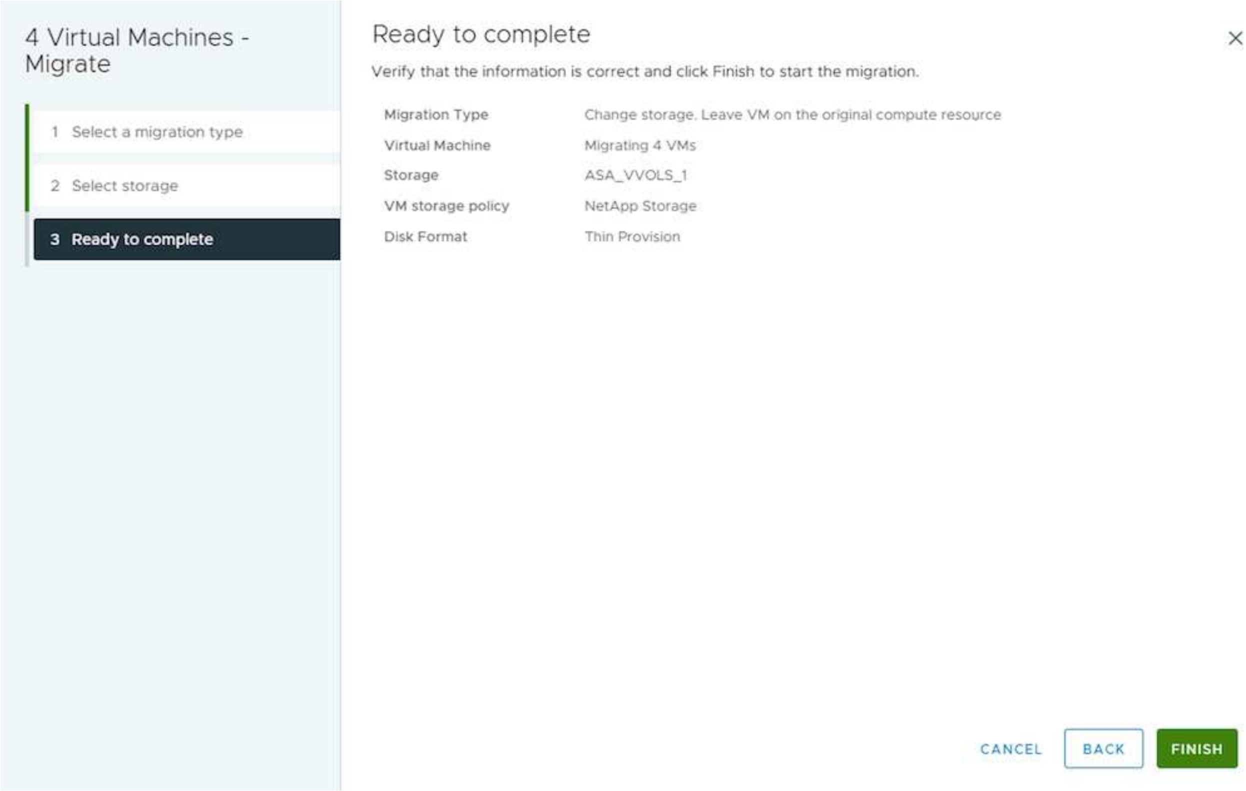
Manage Columns   Items per page 5   1 - 5 of 14 items   1 / 3

Compatibility

✓ Compatibility checks succeeded.

CANCEL   BACK   NEXT

5. Review and click on Finish.



4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL   BACK   FINISH

To migrate VMs using PowerCLI, here is the sample script.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

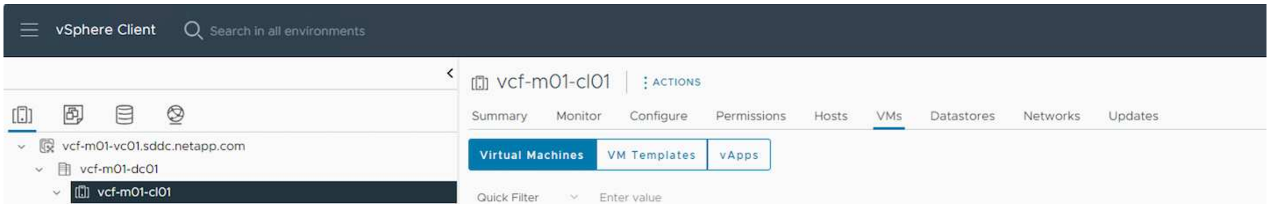
When Datastore Cluster is in use with fully automated storage DRS (Dynamic Resource Scheduling) and both (source & target) datastores are of same type (VMFS/NFS/vVol), Keep both datastores in same storage cluster and migrate VMs from source datastore by enabling maintenance mode on the source. Experience will be similar to how compute hosts are handled for maintenance.

Migration of VMs across multiple vSphere clusters

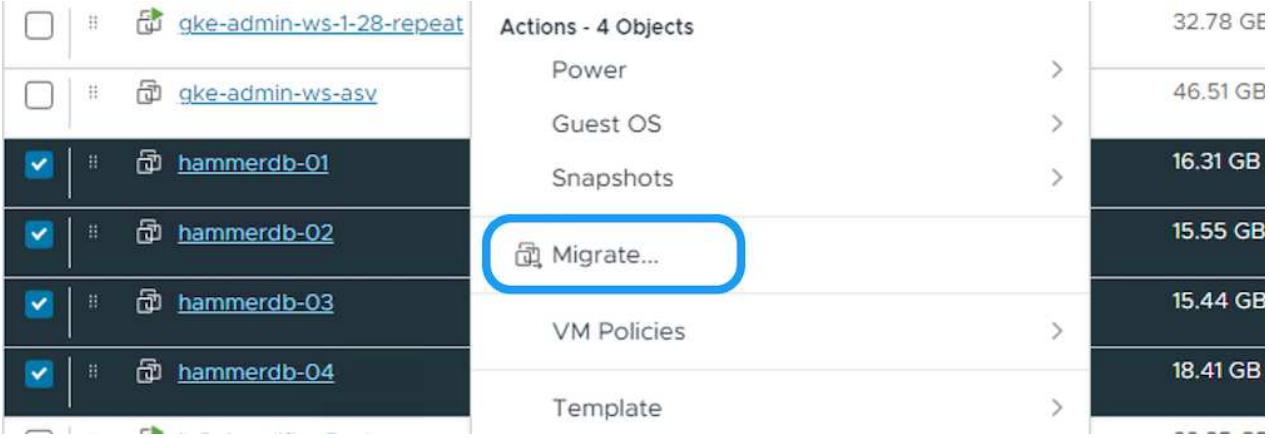
> Refer CPU Compatibility and vSphere Enhanced vMotion Compatibility when source and target hosts are of different CPU family or model.

Follow the procedure below to migrate VMs to new Datastore using UI.

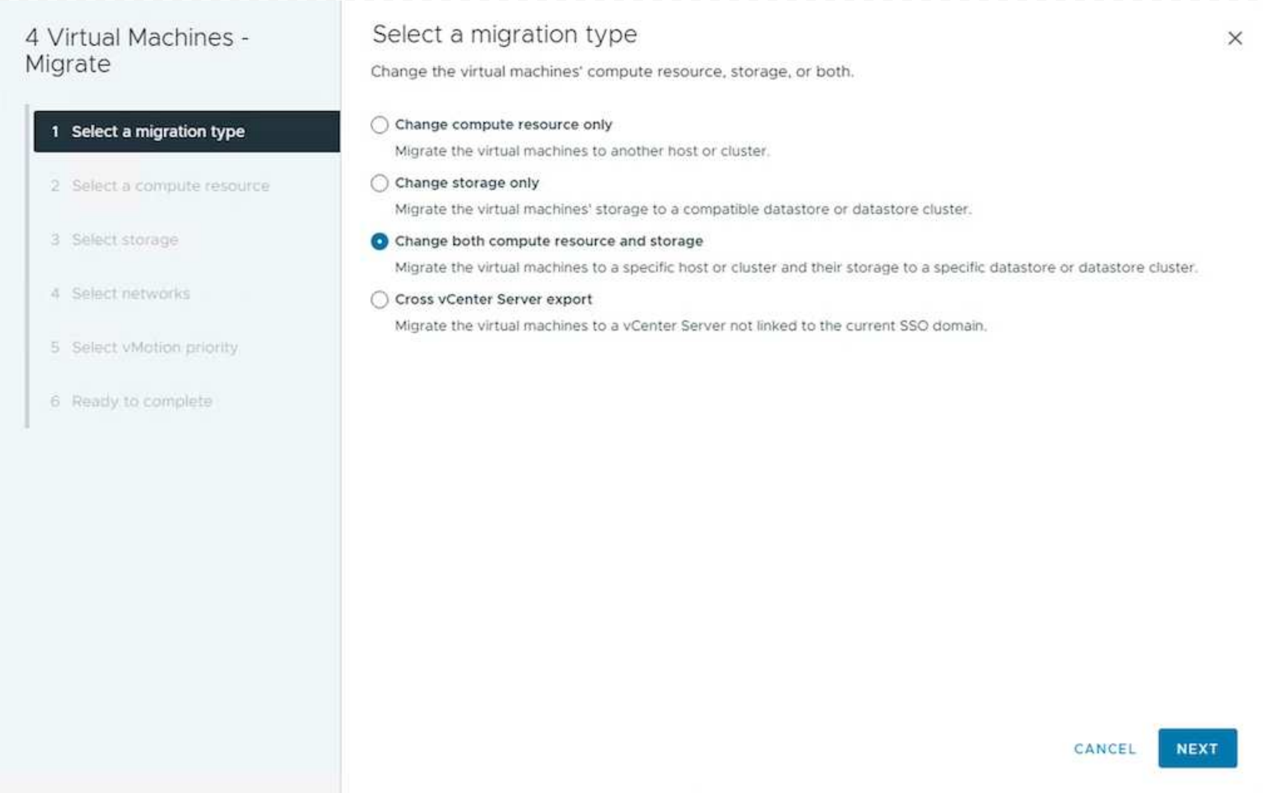
1. With vSphere Web Client, select the Cluster from the Host and Cluster inventory and click on VMs tab.



2. Select the VMs that needs to be migrated and right click to select Migrate option.



3. Choose option to change compute resource and storage, Click Next


4 Virtual Machines - Migrate

1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select networks
5 Select vMotion priority
6 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

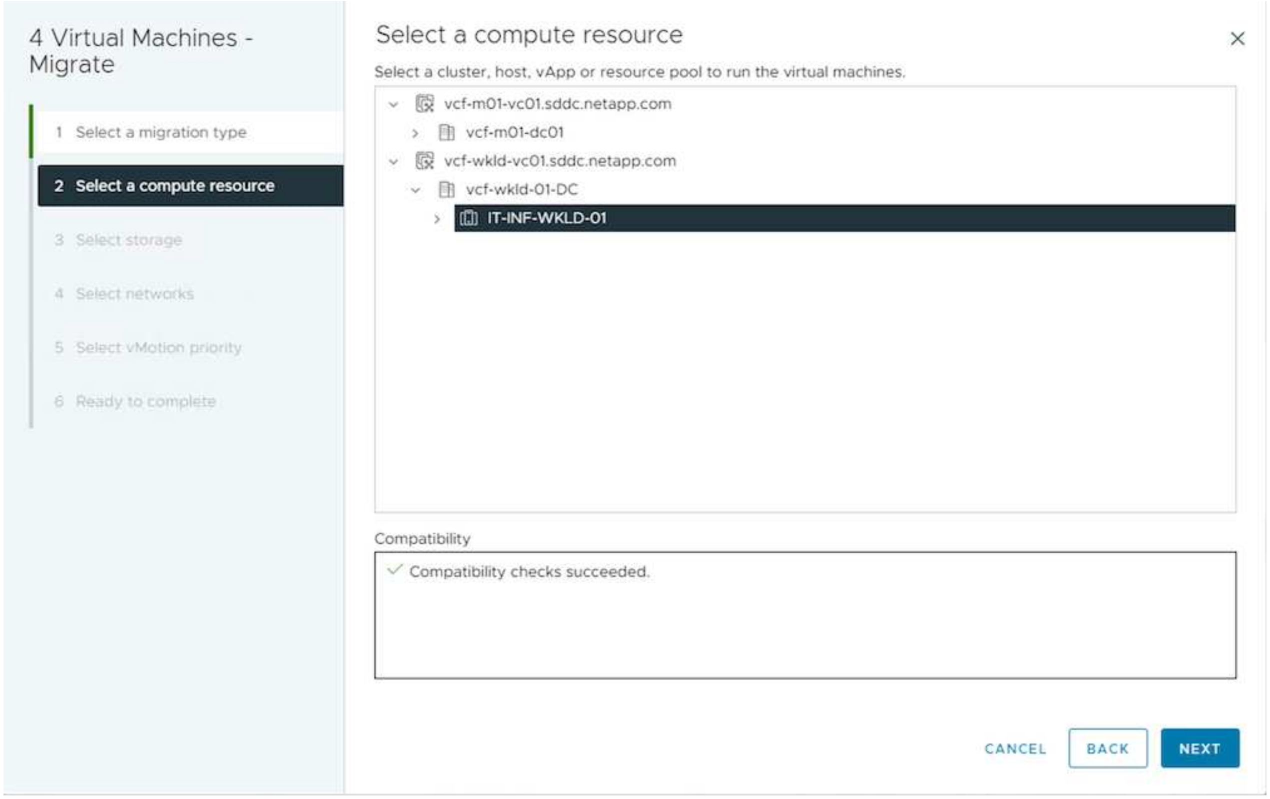
○ Change compute resource only
Migrate the virtual machines to another host or cluster.

○ Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

● Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

○ Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

4. Navigate and pick the right cluster to migrate.


4 Virtual Machines - Migrate

1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select networks
5 Select vMotion priority
6 Ready to complete

Select a compute resource

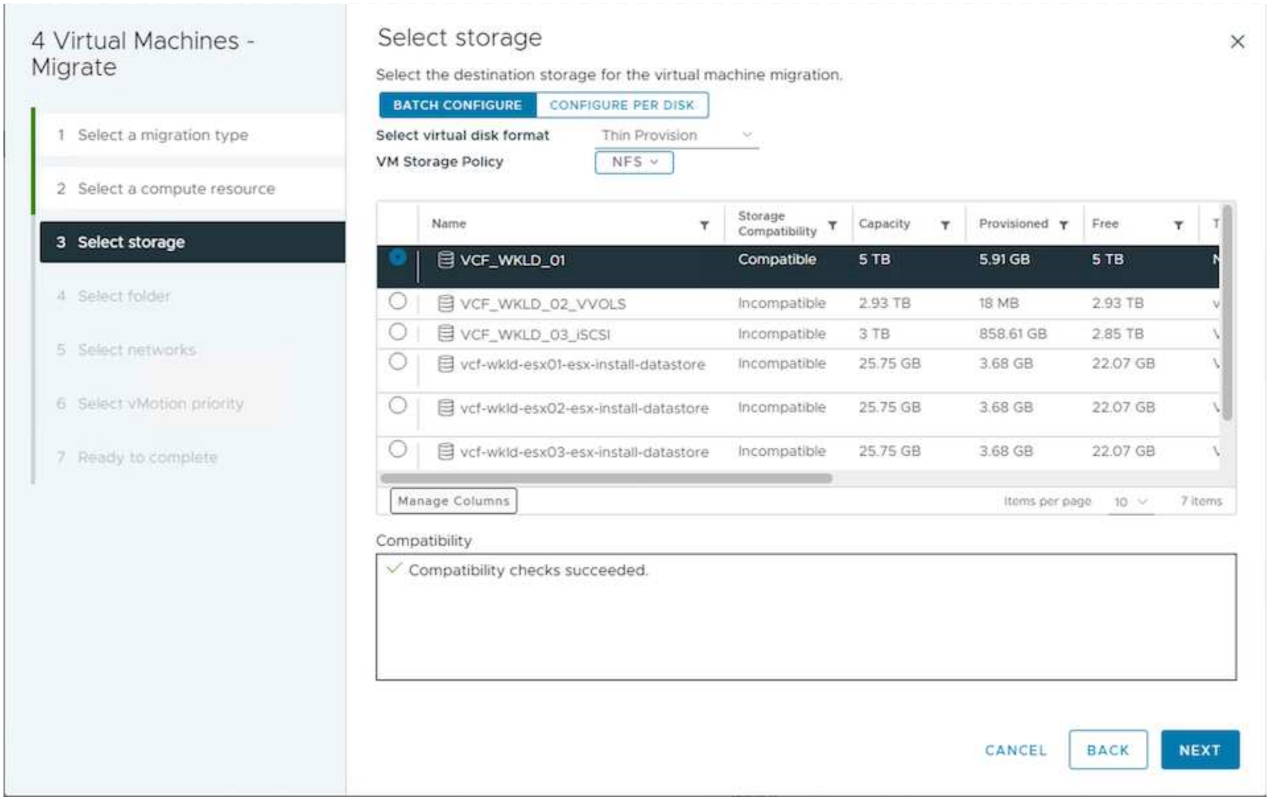
Select a cluster, host, vApp or resource pool to run the virtual machines.

- vcf-m01-vc01.sddc.netapp.com
  - vcf-m01-dc01
- vcf-wkld-vc01.sddc.netapp.com
  - vcf-wkld-01-DC
    - IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

5. Select the desired VM Storage Policy and pick the datastore that is compatible. Click Next.



4 Virtual Machines - Migrate

1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select folder
5 Select networks
6 Select vMotion priority
7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

Select virtual disk format: Thin Provision

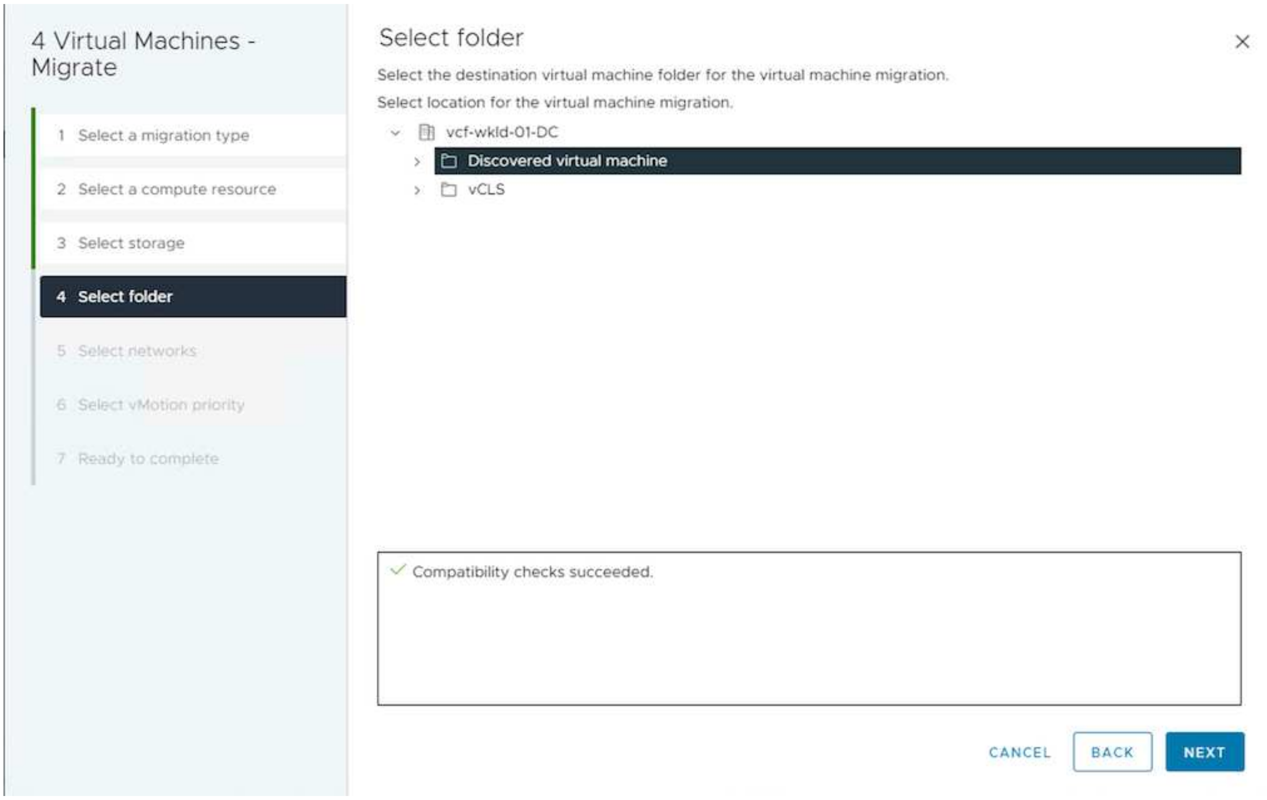
VM Storage Policy: NFS

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB	N
○	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB	V
○	VCF_WKLD_03_iSCSI	Incompatible	3 TB	858.61 GB	2.85 TB	V
○	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	V
○	vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	V
○	vcf-wkld-esx03-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	V

Compatibility

✓ Compatibility checks succeeded.

6. Pick the VM folder to place the target VMs.



4 Virtual Machines - Migrate

1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select folder
5 Select networks
6 Select vMotion priority
7 Ready to complete

Select folder

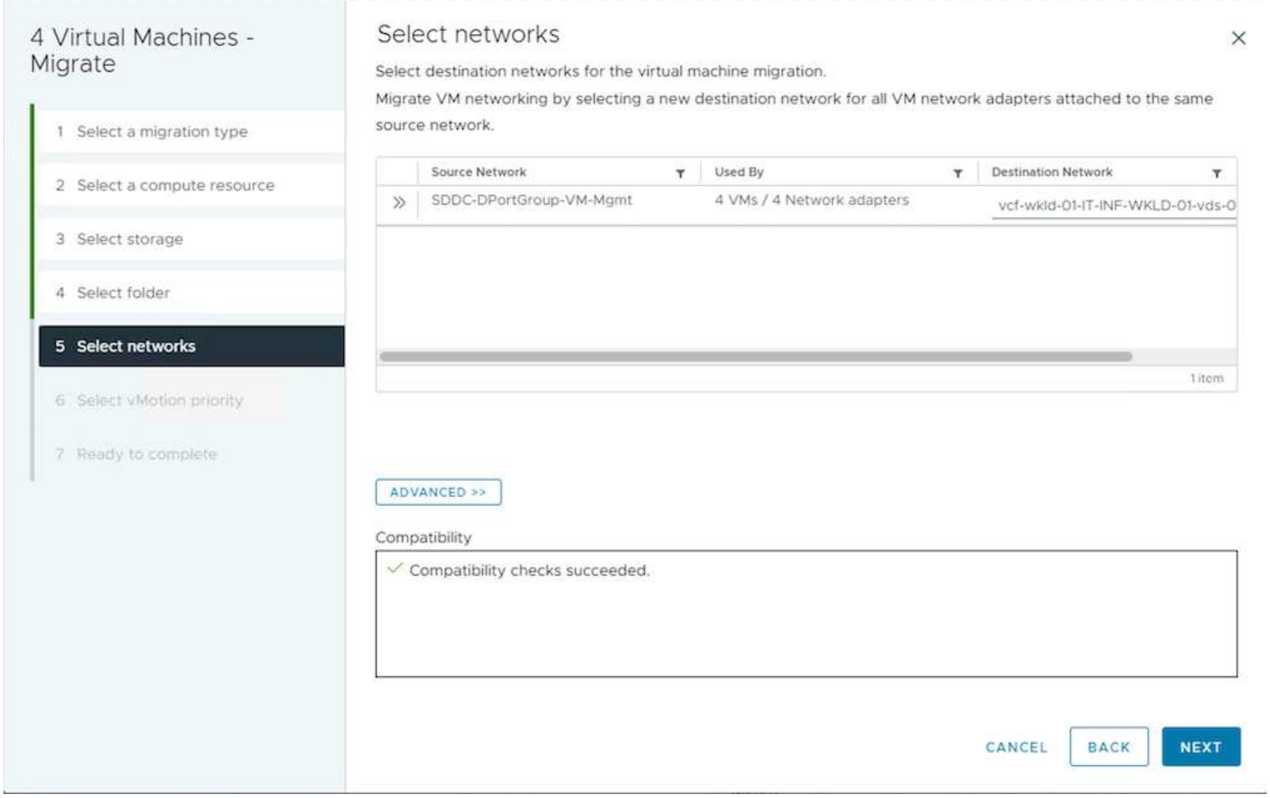
Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

vcf-wkld-01-DC
Discovered virtual machine
vCLS

✓ Compatibility checks succeeded.

7. Select the target port group.


4 Virtual Machines - Migrate
1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select folder
5 Select networks
6 Select vMotion priority
7 Ready to complete
ADVANCED >>
CANCEL
BACK
NEXT

Select networks

Select destination networks for the virtual machine migration.

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

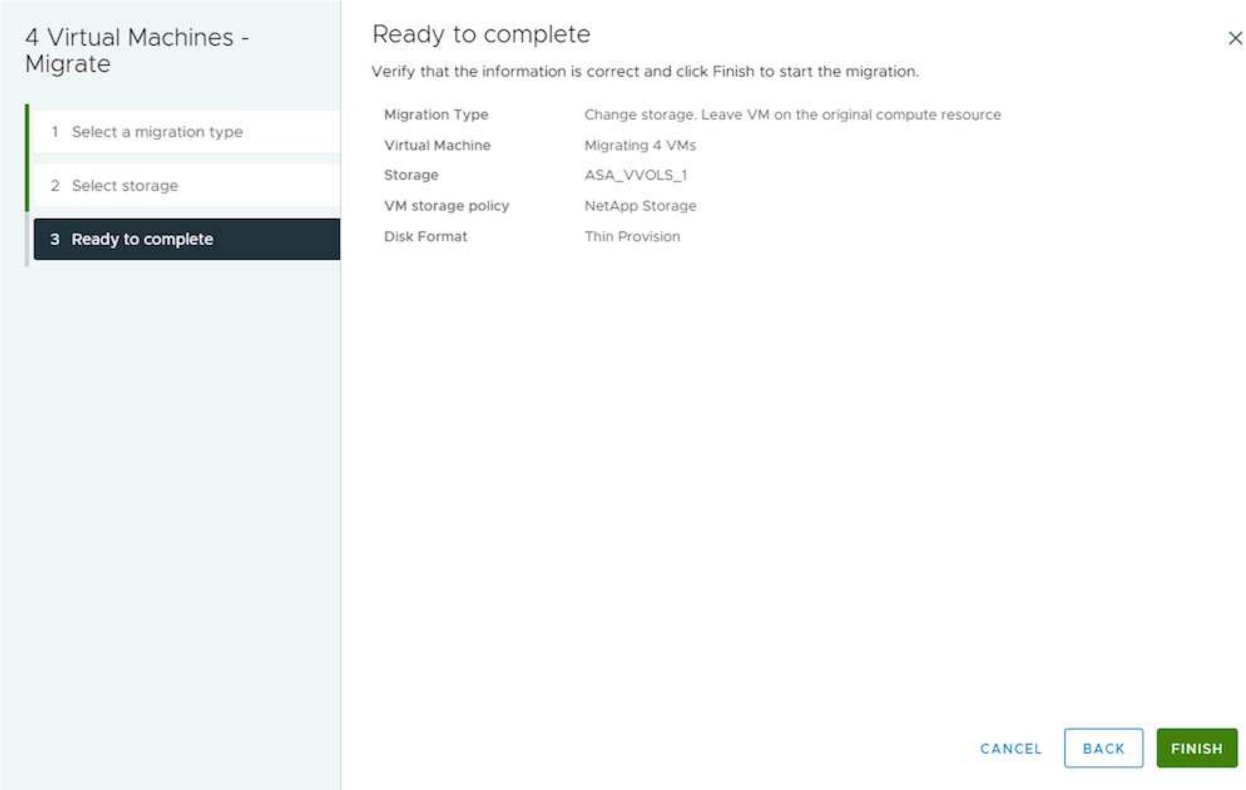
Source Network	Used By	Destination Network
SDDC-DPortGroup-VM-Mgmt	4 VMs / 4 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-0

1 item

Compatibility

✓ Compatibility checks succeeded.

8. Review and click on Finish.



Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

To migrate VMs using PowerCLI, here is the sample script.

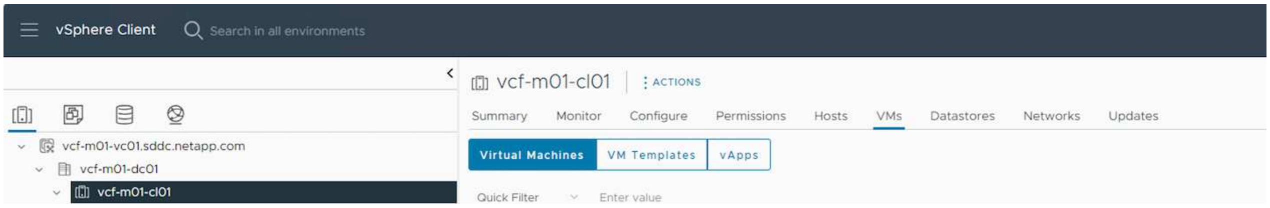
```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to another cluster and Datastore specified by Policy
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy)

#When Portgroup is specific to each cluster, replace the above command
with
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy) -PortGroup
(Get-VirtualPortGroup 'VLAN 101')

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

Migration of VMs across vCenter servers in same SSO domain

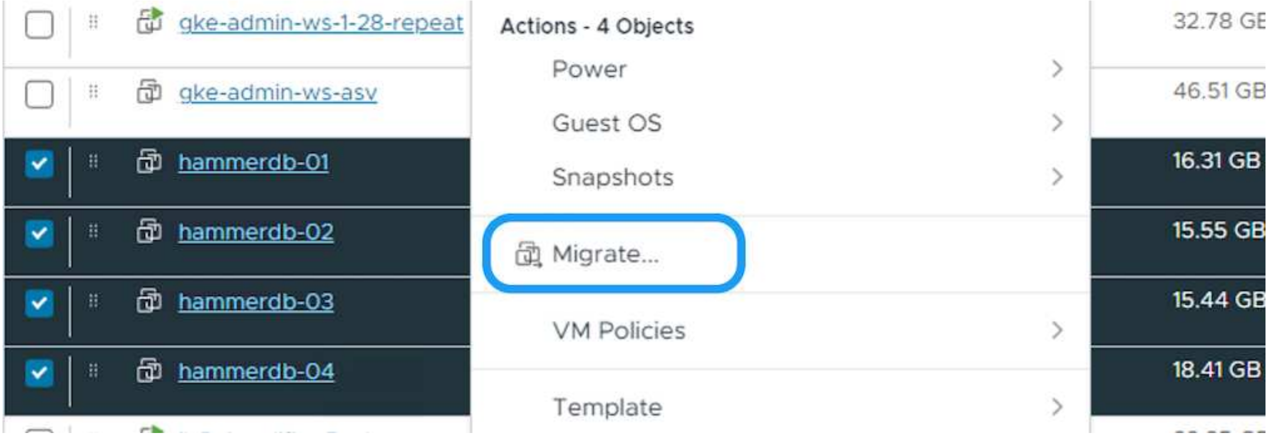
Follow the procedure below to migrate VMs to new vCenter server which is listed on same vSphere Client UI.

> For additional requirements like source and target vCenter versions,etc., check vSphere documentation on requirements for vMotion between vCenter server instances

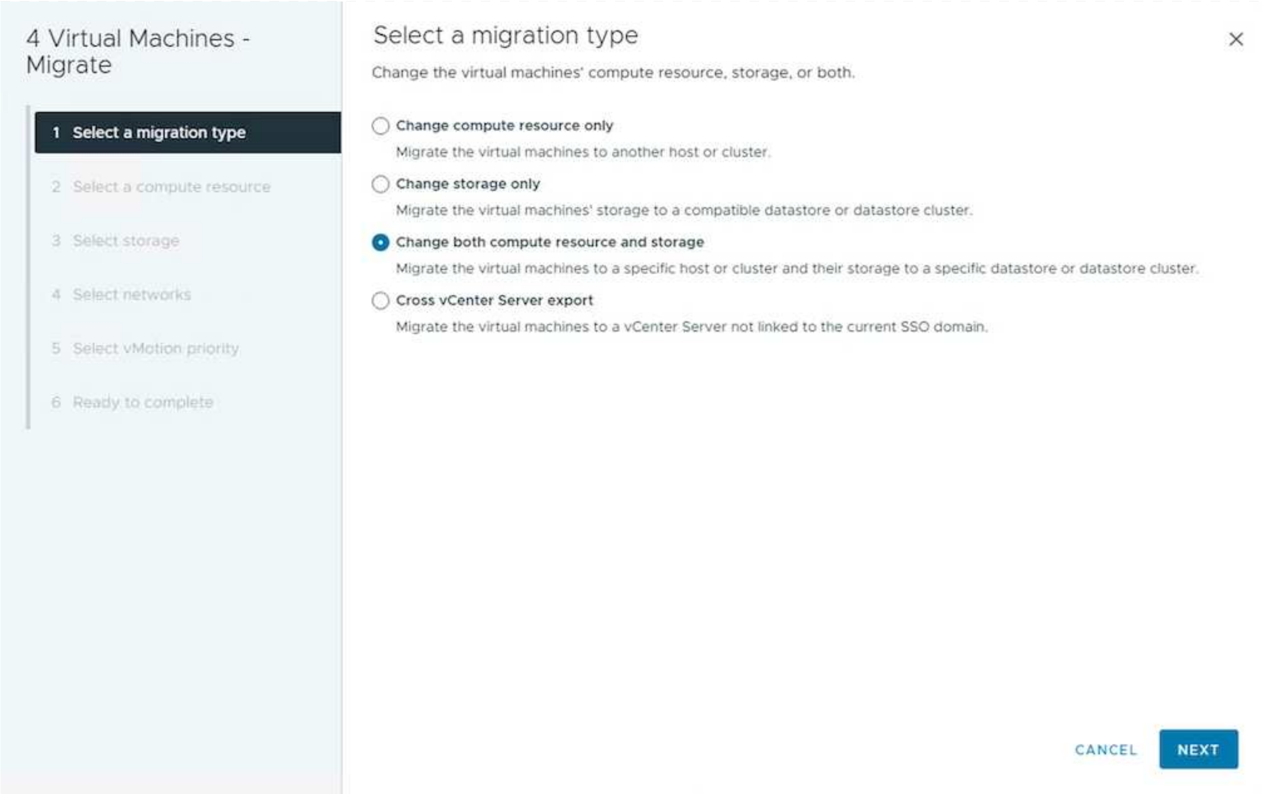
1. With vSphere Web Client, select the Cluster from the Host and Cluster inventory and click on VMs tab.



2. Select the VMs that needs to be migrated and right click to select Migrate option.



3. Choose option to change compute resource and storage, Click Next



4 Virtual Machines - Migrate

1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select networks
5 Select vMotion priority
6 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

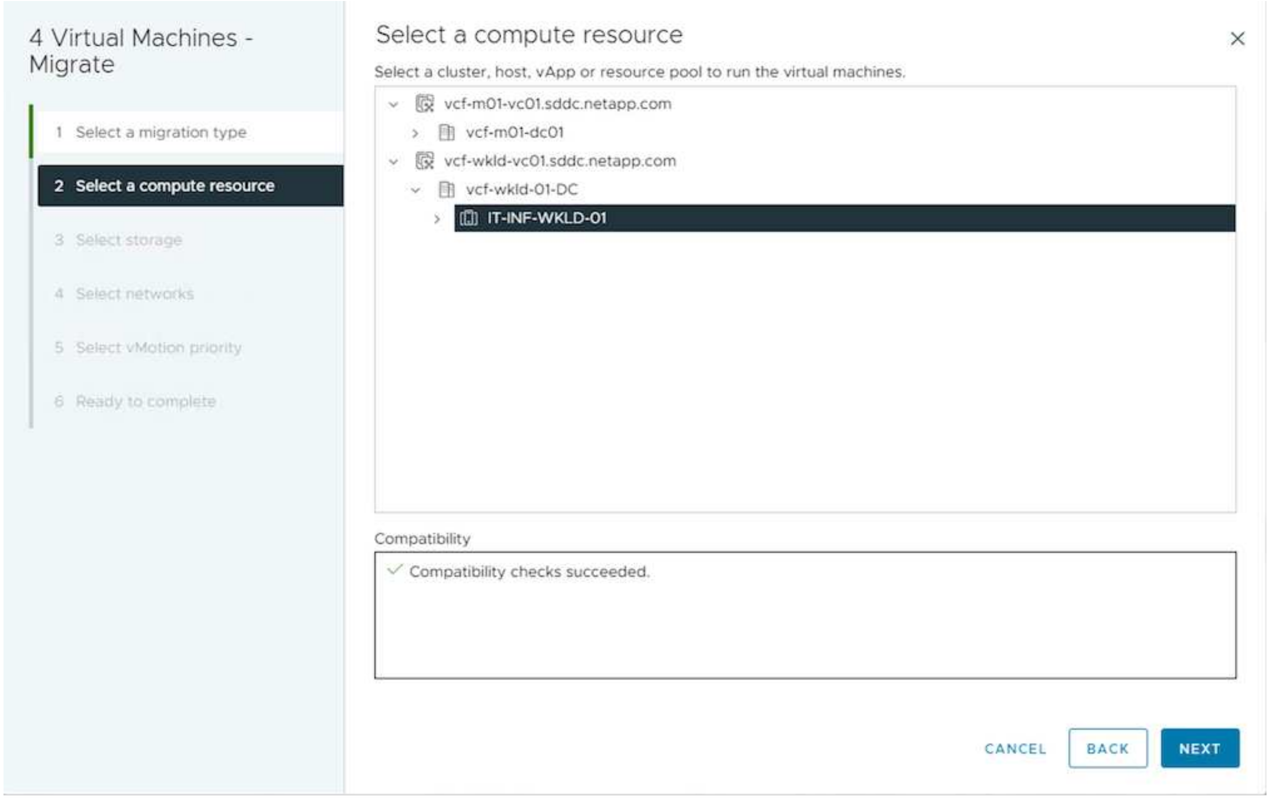
○ Change compute resource only
Migrate the virtual machines to another host or cluster.

○ Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

● Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

○ Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

4. Select the target cluster in target vCenter server.



4 Virtual Machines - Migrate

1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select networks
5 Select vMotion priority
6 Ready to complete

Select a compute resource

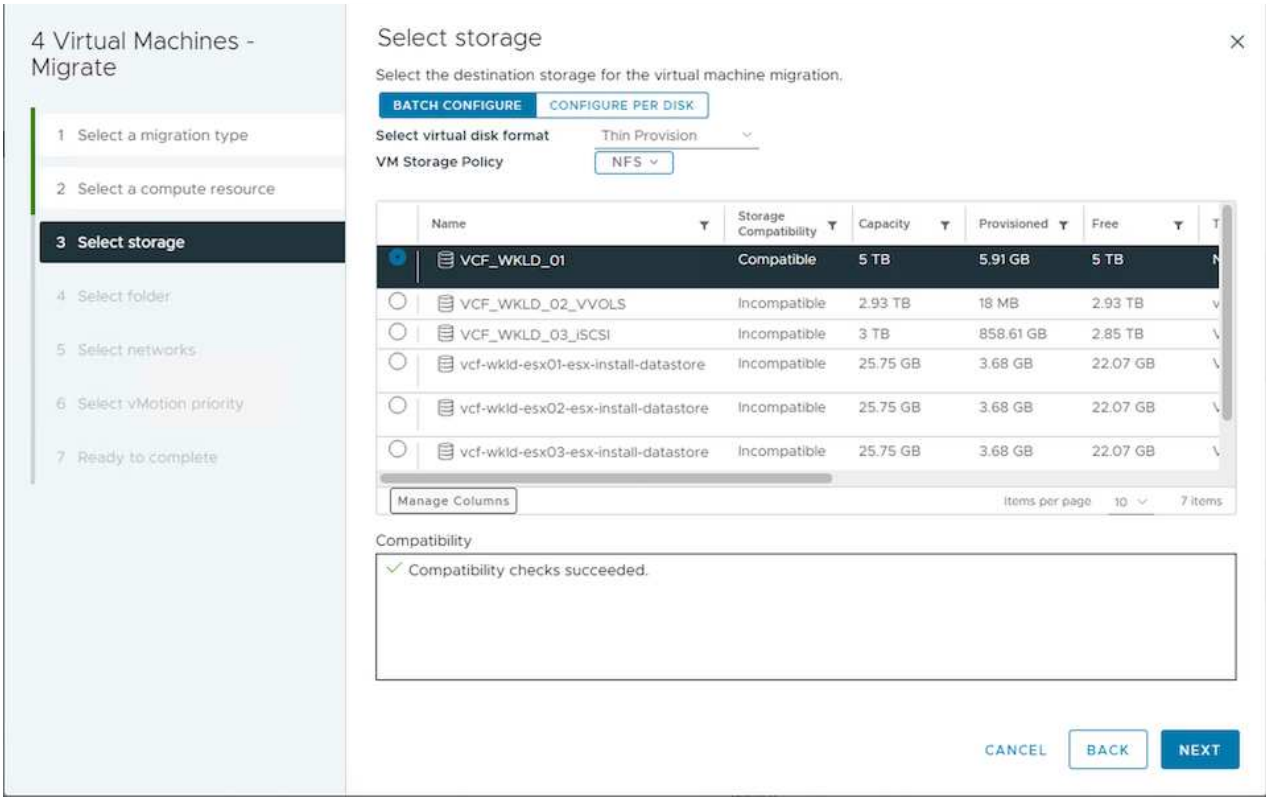
Select a cluster, host, vApp or resource pool to run the virtual machines.

```
⌄ vcf-m01-vc01.sddc.netapp.com
  › vcf-m01-dc01
⌄ vcf-wkld-vc01.sddc.netapp.com
  ⌄ vcf-wkld-01-DC
    › IT-INF-WKLD-01
```

Compatibility

✓ Compatibility checks succeeded.

5. Select the desired VM Storage Policy and pick the datastore that is compatible. Click Next.



4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select folder

5 Select networks

6 Select vMotion priority

7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE | CONFIGURE PER DISK

Select virtual disk format: Thin Provision

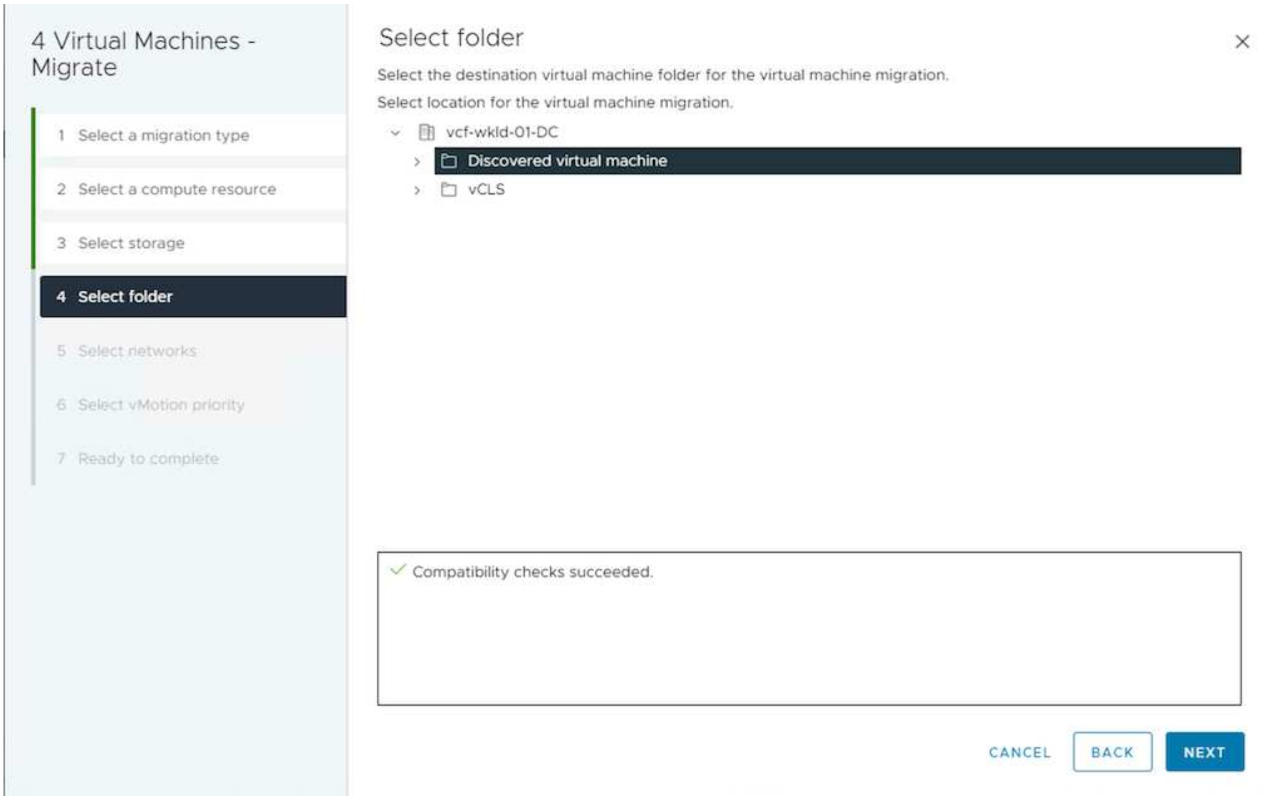
VM Storage Policy: NFS

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB	N
○	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB	V
○	VCF_WKLD_03_iSCSI	Incompatible	3 TB	858.61 GB	2.85 TB	V
○	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	V
○	vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	V
○	vcf-wkld-esx03-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	V

Compatibility

✓ Compatibility checks succeeded.

6. Pick the VM folder to place the target VMs.



4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select folder

5 Select networks

6 Select vMotion priority

7 Ready to complete

Select folder

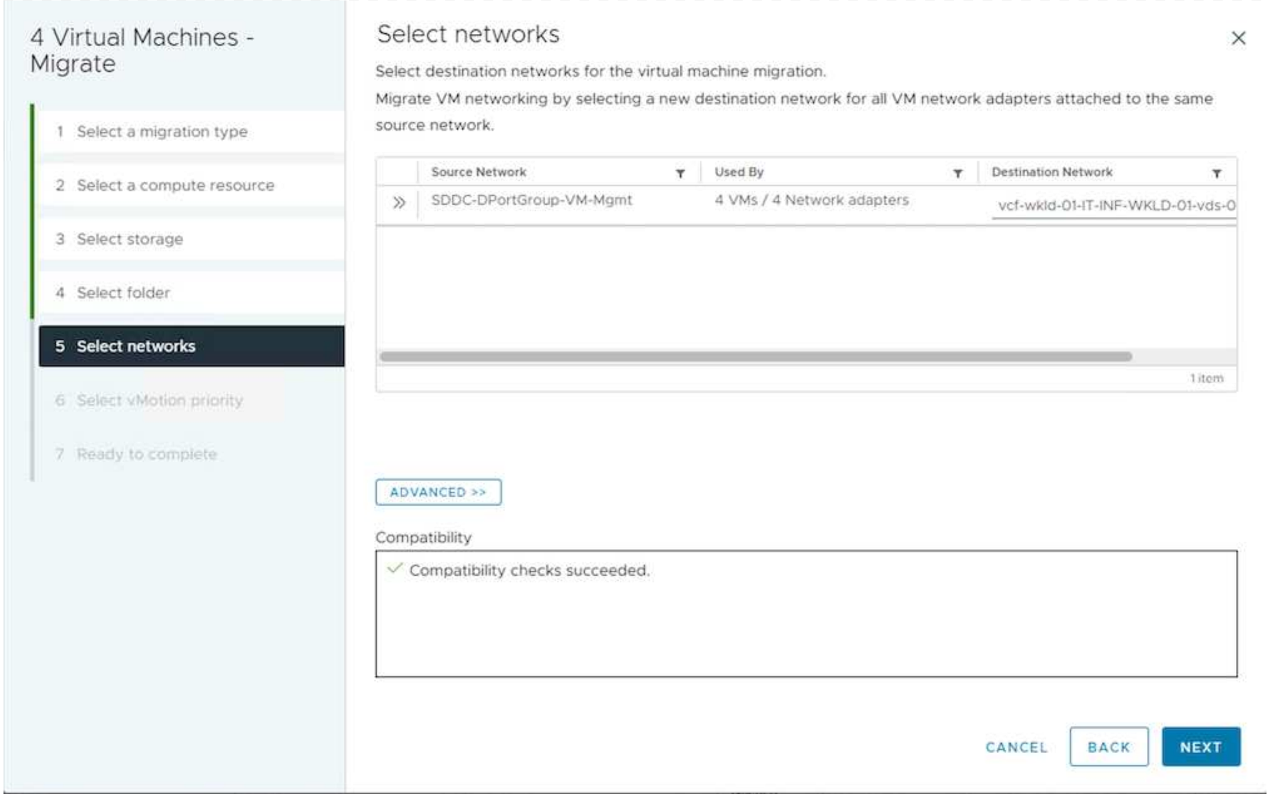
Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

- vcf-wkld-01-DC
  - Discovered virtual machine
  - vCLS

✓ Compatibility checks succeeded.

7. Select the target port group.


4 Virtual Machines - Migrate
1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select folder
5 Select networks
6 Select vMotion priority
7 Ready to complete
ADVANCED >>
CANCEL
BACK
NEXT

Select networks

Select destination networks for the virtual machine migration.

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

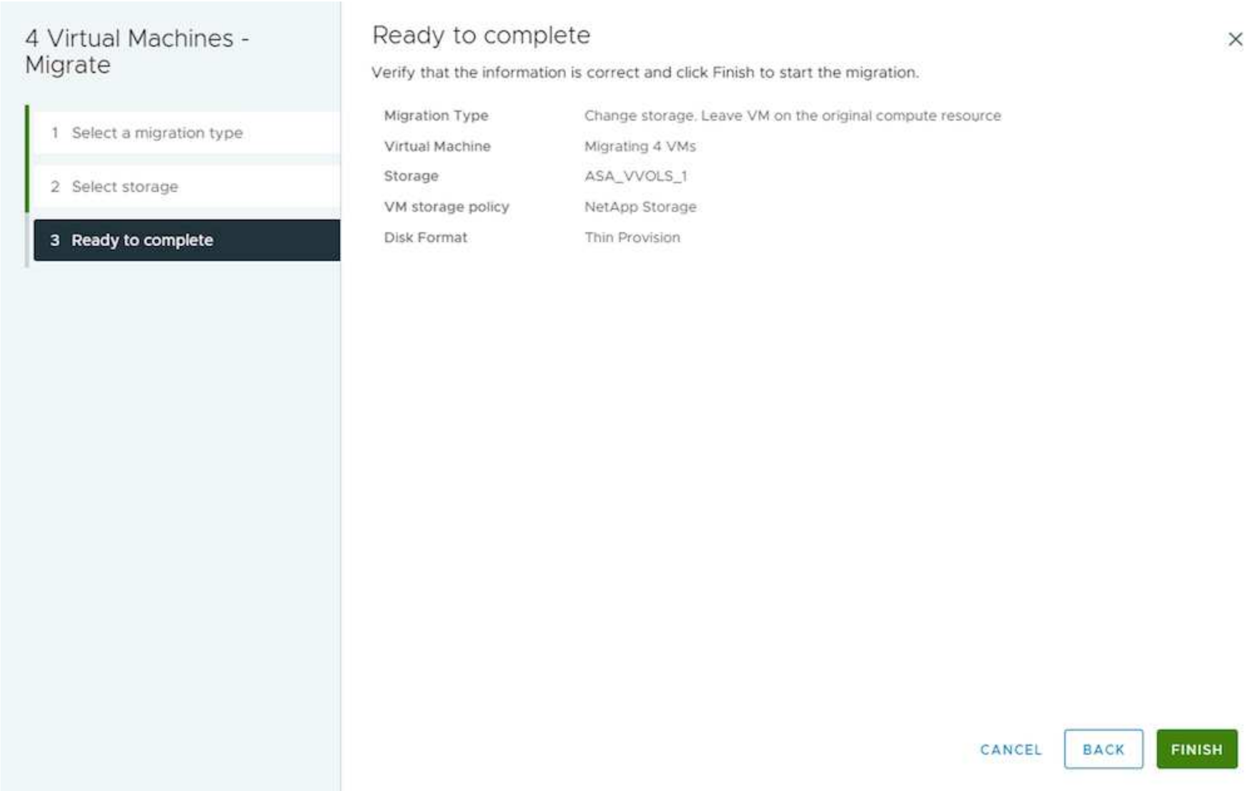
	Source Network	Used By	Destination Network
»	SDDC-DPortGroup-VM-Mgmt	4 VMs / 4 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-0

1 item

Compatibility

✓ Compatibility checks succeeded.

8. Review the migration options and click Finish.



Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

To migrate VMs using PowerCLI, here is the sample script.

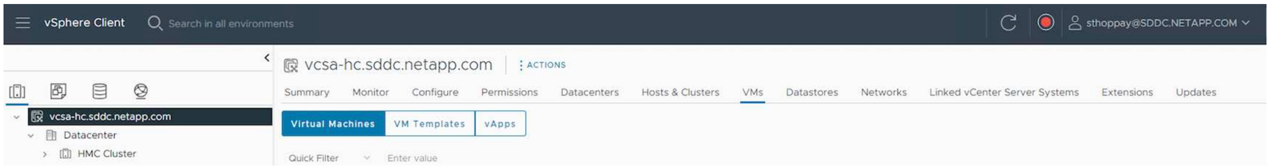
```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

Migration of VMs across vCenter servers in different SSO domain

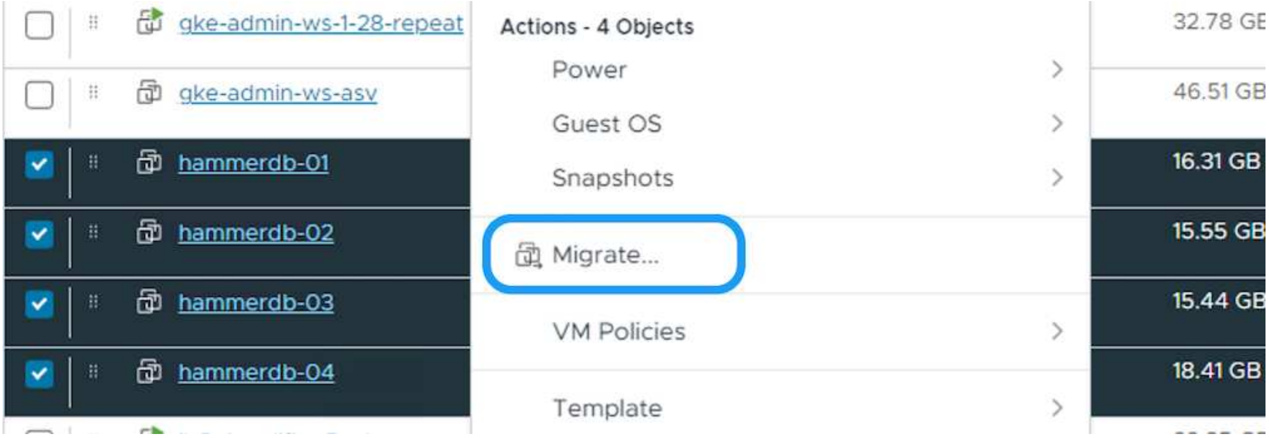
This scenario assumes the communication exists between the vCenter servers. Otherwise check the across datacenter location scenario listed below. For prerequisites, check vSphere documentation on Advanced Cross vCenter vMotion

Follow the procedure below to migrate VMs to differnt vCenter server using UI.

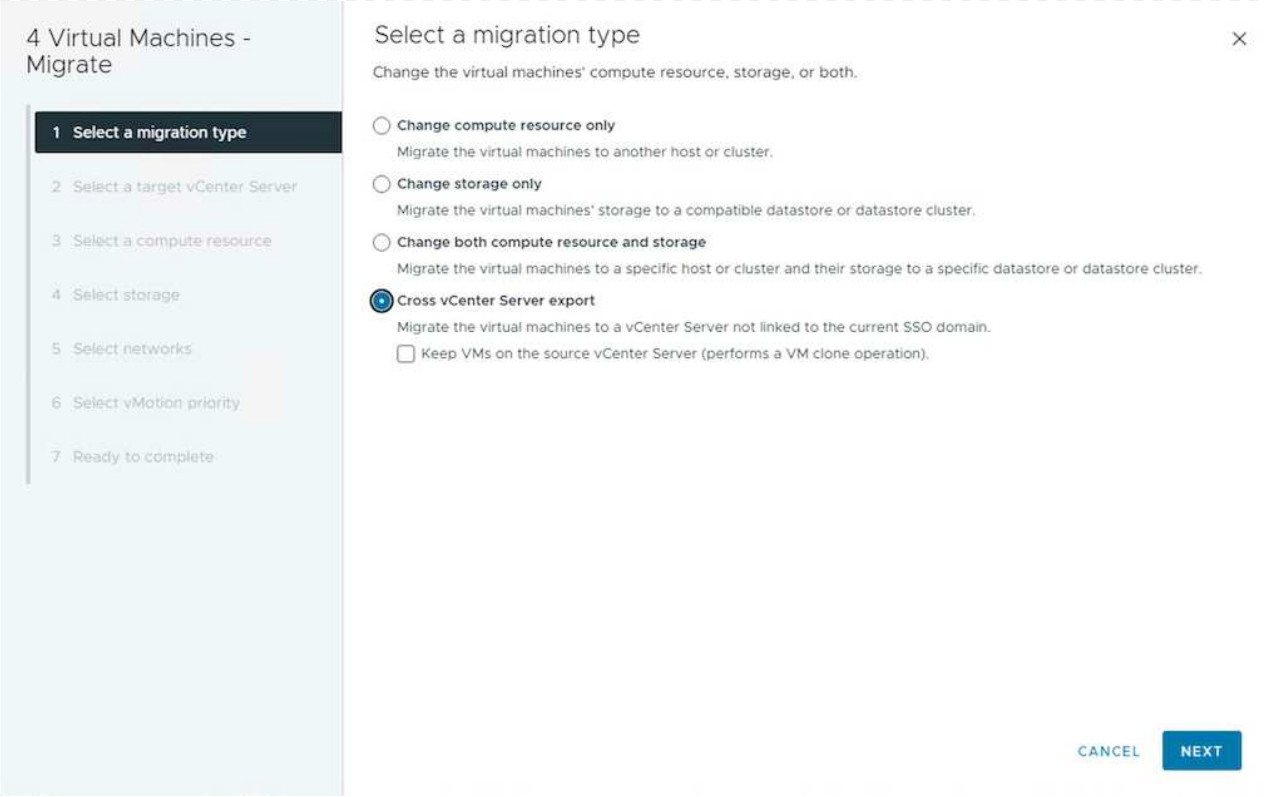
1. With vSphere Web Client, select the source vCenter server and click on VMs tab.



2. Select the VMs that needs to be migrated and right click to select Migrate option.



3. Choose option Cross vCenter Server export, Click Next



4 Virtual Machines - Migrate

1 Select a migration type
2 Select a target vCenter Server
3 Select a compute resource
4 Select storage
5 Select networks
6 Select vMotion priority
7 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

○ Change compute resource only
Migrate the virtual machines to another host or cluster.

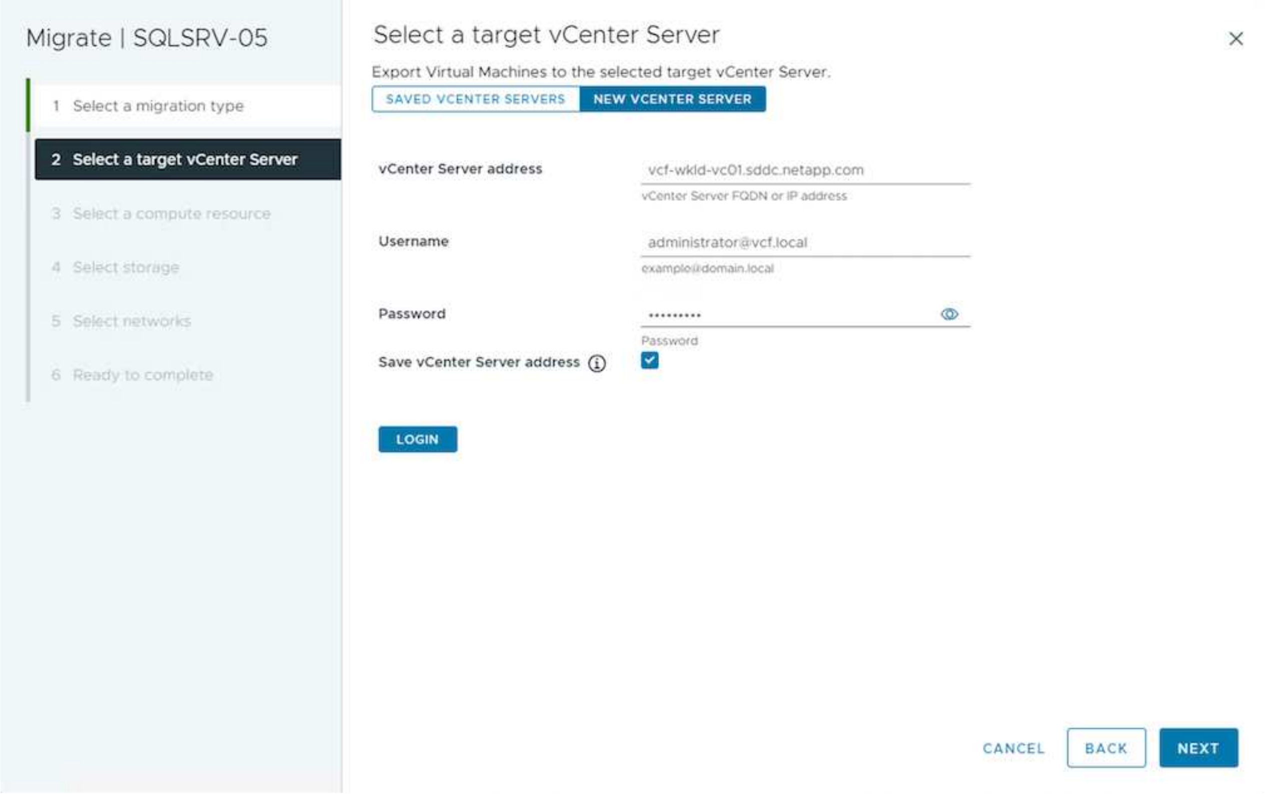
○ Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

○ Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

● Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.
□ Keep VMs on the source vCenter Server (performs a VM clone operation).

VM can also be imported from the target vCenter server. For that procedure, check Import or Clone a Virtual Machine with Advanced Cross vCenter vMotion

4. Provide vCenter credential details and click Login.



Migrate | SQLSRV-05

1 Select a migration type
2 Select a target vCenter Server
3 Select a compute resource
4 Select storage
5 Select networks
6 Ready to complete

Select a target vCenter Server

Export Virtual Machines to the selected target vCenter Server.

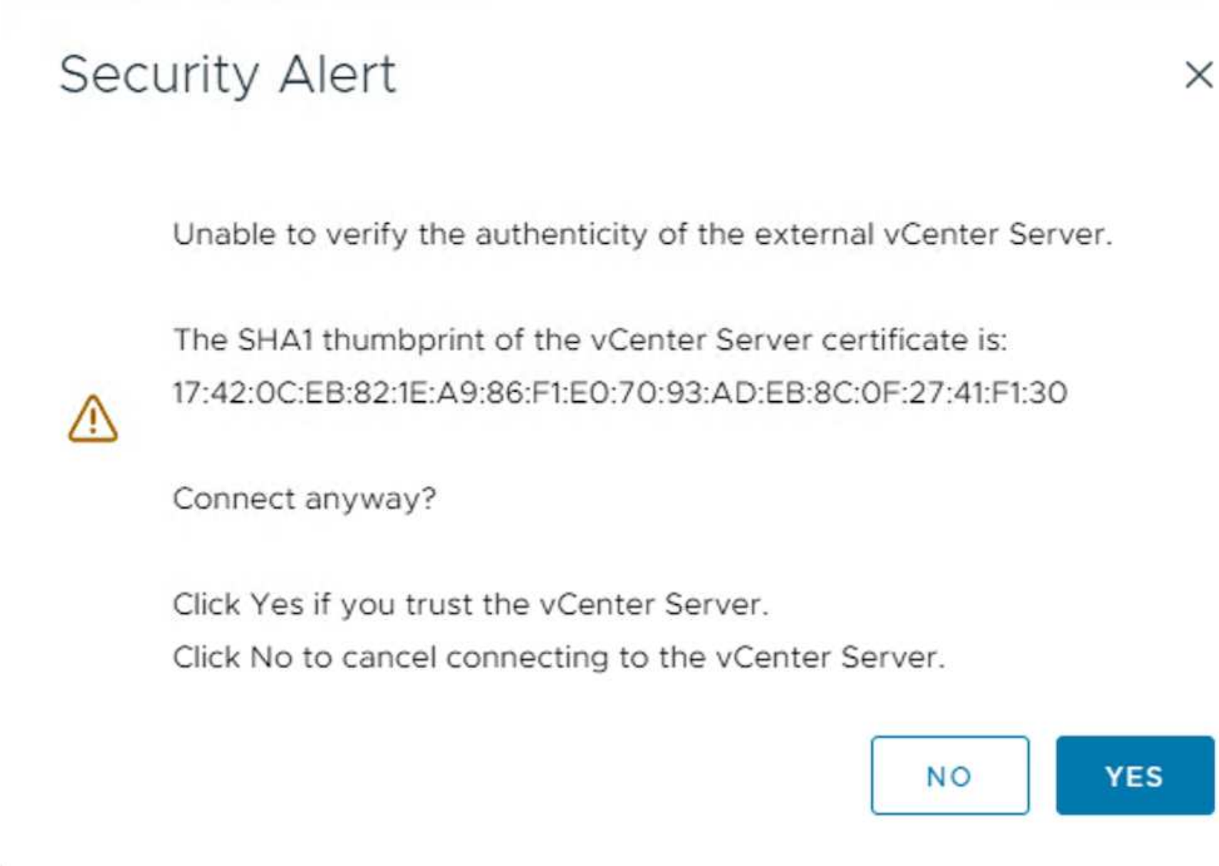
vCenter Server address: vcf-wkld-vc01.sddc.netapp.com
vCenter Server FQDN or IP address

Username: administrator@vcf.local
example@domain.local

Password: •••••••••
Password

Save vCenter Server address ☑

5. Confirm and Accept the SSL certificate thumbprint of vCenter server



Security Alert

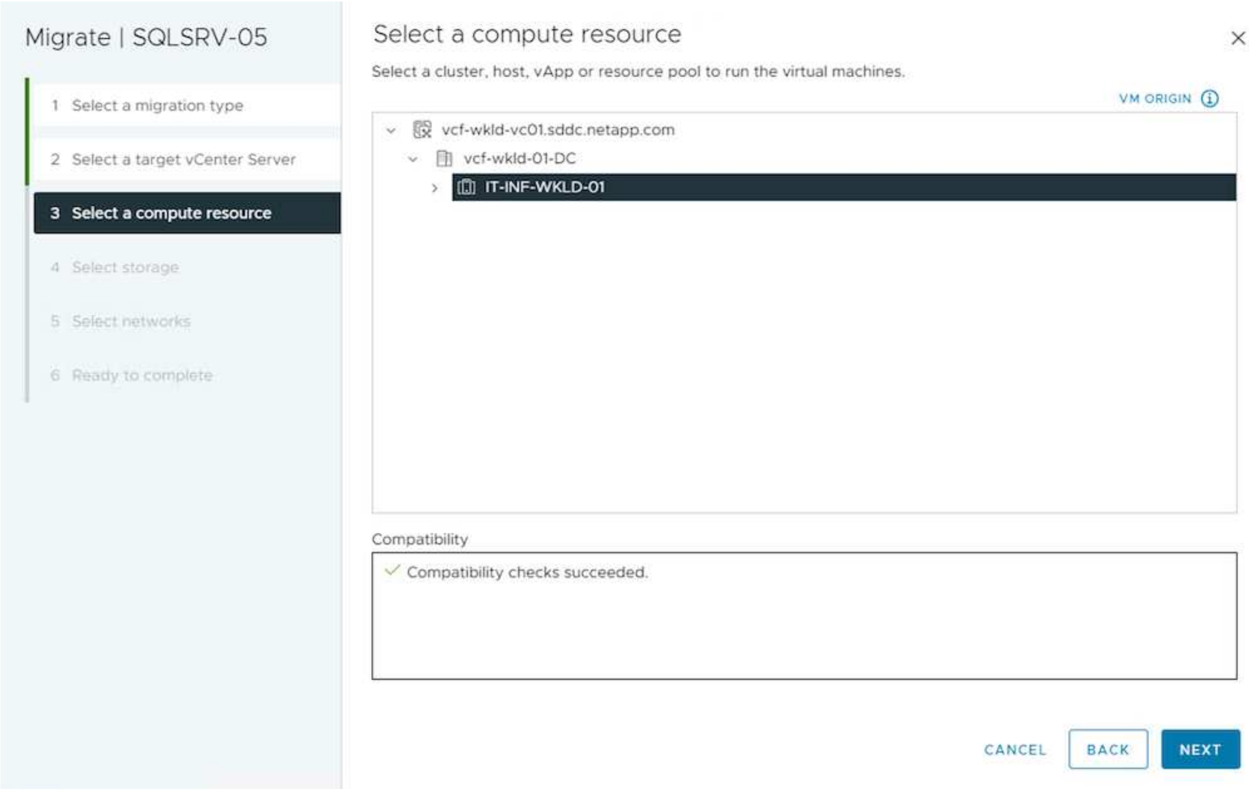
Unable to verify the authenticity of the external vCenter Server.

The SHA1 thumbprint of the vCenter Server certificate is:
17:42:0C:EB:82:1E:A9:86:F1:E0:70:93:AD:EB:8C:0F:27:41:F1:30

Connect anyway?

Click Yes if you trust the vCenter Server.
Click No to cancel connecting to the vCenter Server.

6. Expand target vCenter and select the target compute cluster.



Migrate | SQLSRV-05

1 Select a migration type
2 Select a target vCenter Server
3 Select a compute resource
4 Select storage
5 Select networks
6 Ready to complete

Select a compute resource

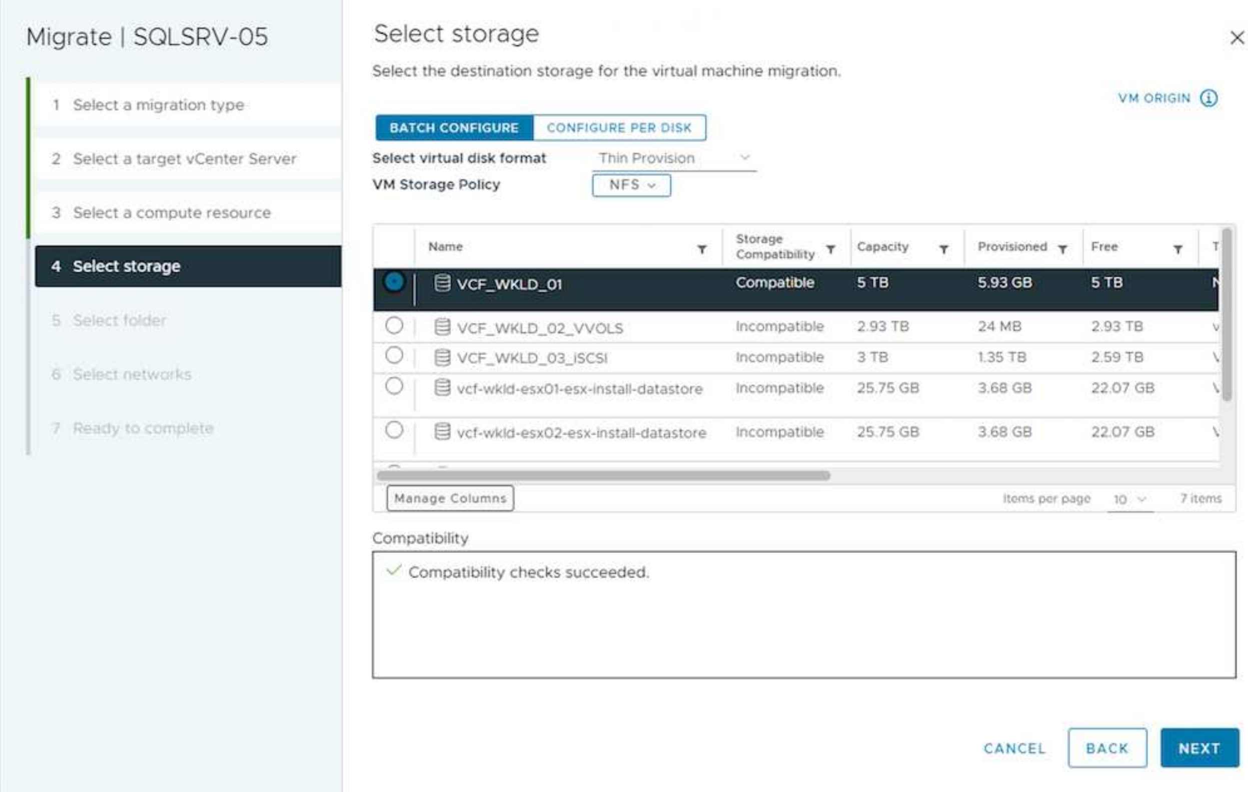
Select a cluster, host, vApp or resource pool to run the virtual machines.

vcf-wkld-vc01.sddc.netapp.com
vcf-wkld-01-DC
IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

7. Select the target datastore based on the VM Storage Policy.



Migrate | SQLSRV-05

Select storage

Select the destination storage for the virtual machine migration.

Select virtual disk format: Thin Provision

VM Storage Policy: NFS

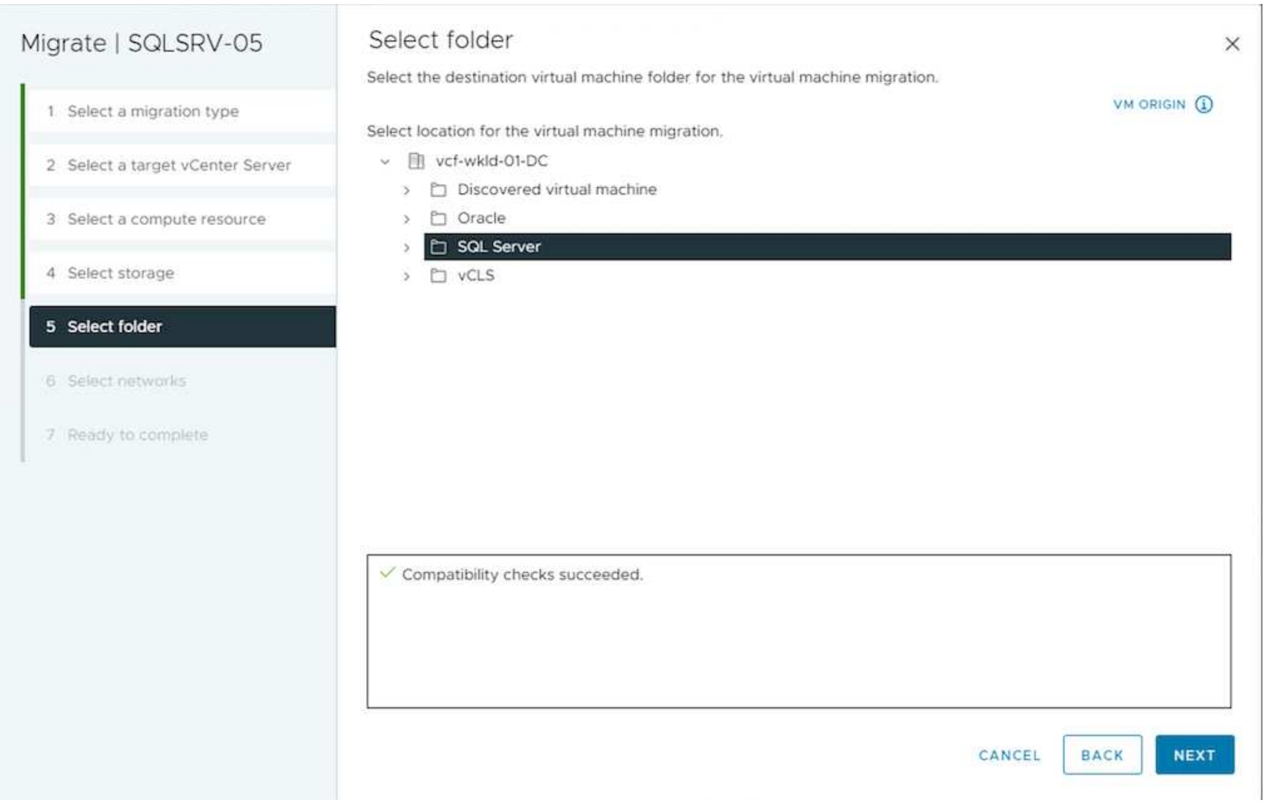
	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	VCF_WKLD_01	Compatible	5 TB	5.93 GB	5 TB	N
○	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	24 MB	2.93 TB	v
○	VCF_WKLD_03_iSCSI	Incompatible	3 TB	1.35 TB	2.59 TB	\
○	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	\
○	vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	\

Items per page 10 7 items

Compatibility

✓ Compatibility checks succeeded.

8. Select the target VM folder.



Migrate | SQLSRV-05

Select folder

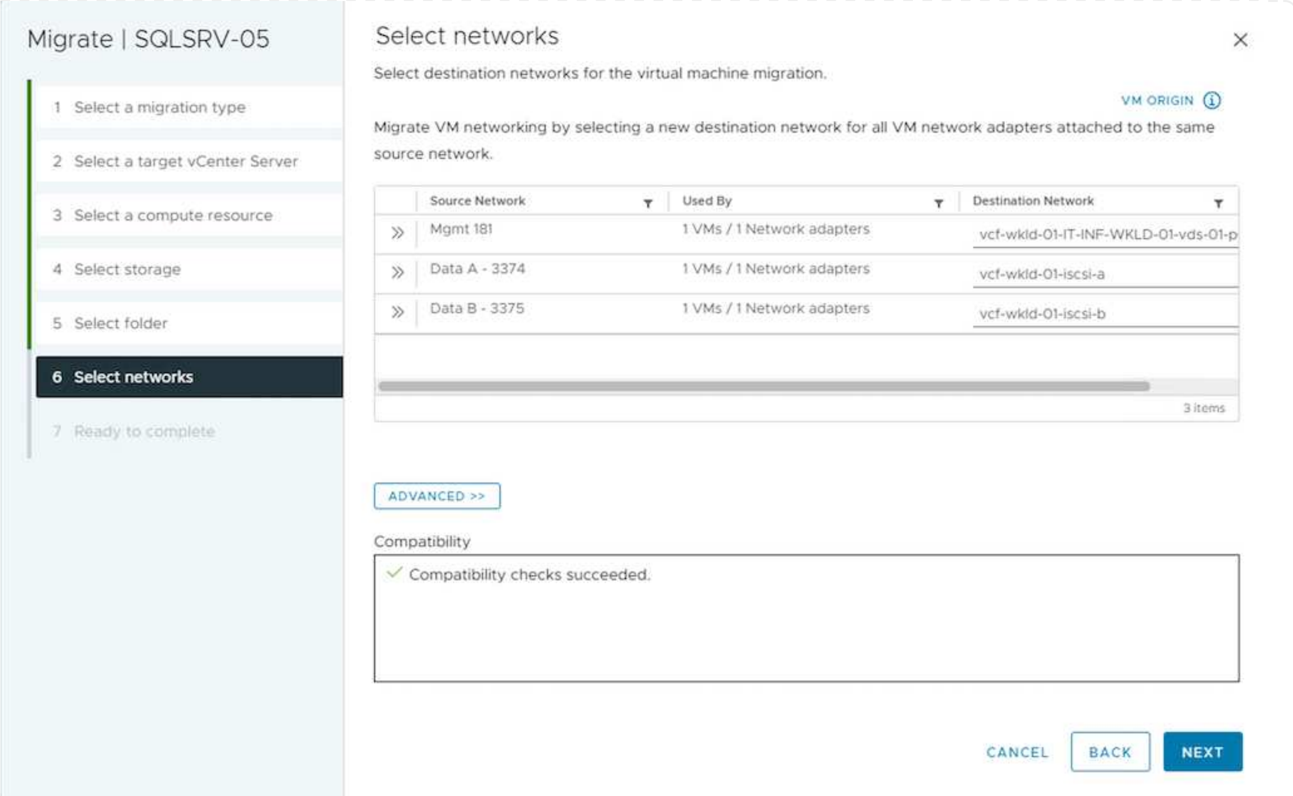
Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

- vcf-wkld-01-DC
  - Discovered virtual machine
  - Oracle
  - SQL Server
  - vCLS

✓ Compatibility checks succeeded.

9. Pick the VM portgroup for each network interface card mapping.



Migrate | SQLSRV-05

1 Select a migration type
2 Select a target vCenter Server
3 Select a compute resource
4 Select storage
5 Select folder
6 Select networks
7 Ready to complete

Select networks

Select destination networks for the virtual machine migration.

VM ORIGIN

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
Mgmt 181	1 VMs / 1 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-01-p
Data A - 3374	1 VMs / 1 Network adapters	vcf-wkld-01-iscsi-a
Data B - 3375	1 VMs / 1 Network adapters	vcf-wkld-01-iscsi-b

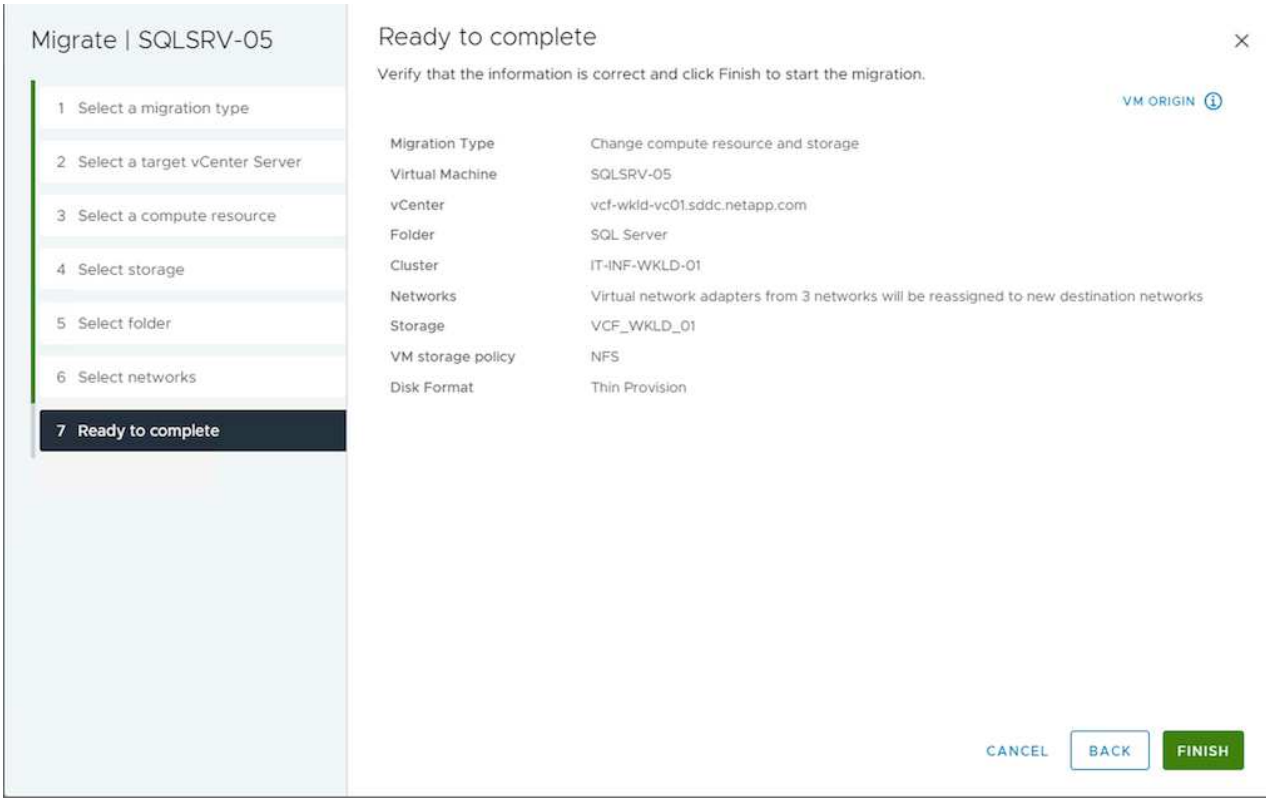
3 items

ADVANCED >>

Compatibility

✓ Compatibility checks succeeded.

10. Review and click Finish to start the vMotion across the vCenter servers.



Migrate | SQLSRV-05

1 Select a migration type
2 Select a target vCenter Server
3 Select a compute resource
4 Select storage
5 Select folder
6 Select networks
7 Ready to complete

Ready to complete

Verify that the information is correct and click Finish to start the migration.

VM ORIGIN

Migration Type	Change compute resource and storage
Virtual Machine	SQLSRV-05
vCenter	vcf-wkld-vc01.sddc.netapp.com
Folder	SQL Server
Cluster	IT-INF-WKLD-01
Networks	Virtual network adapters from 3 networks will be reassigned to new destination networks
Storage	VCF_WKLD_01
VM storage policy	NFS
Disk Format	Thin Provision

To migrate VMs using PowerCLI, here is the sample script.

```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'Source Cluster'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

Migration of VMs across datacenter locations

- When Layer 2 traffic is stretched across datacenters either by using NSX Federation or other options, follow the procedure for migrating VMs across vCenter servers.
- HCX provides various migration types including Replication Assisted vMotion across the datacenters to move VM without any downtime.
- Site Recovery Manager (SRM) is typically meant for Disaster Recovery purposes and also often used for planned migration utilizing storage array based replication.
- Continous Data Protection (CDP) products use vSphere API for IO (VAIO) to intercept the data and send a copy to remote location for near zero RPO solution.
- Backup and Recovery products can also be utilized. But often results in longer RTO.
- BlueXP Disaster Recovery as a Service (DRaaS) utilizes storage array based replication and automates certain tasks to recover the VMs at target site.

Migration of VMs in hybrid cloud environment

- Configure Hybrid Linked Mode and follow the procedure of Migration of VMs across vCenter servers in same SSO domain
- HCX provides various migration types including Replication Assisted vMotion across the datacenters to move VM while it is powered on.
  - TR 4942: Migrate Workloads to FSx ONTAP datastore using VMware HCX
  - TR-4940: Migrate workloads to Azure NetApp Files datastore using VMware HCX - Quickstart guide
  - Migrate workloads to NetApp Cloud Volume Service datastore on Google Cloud VMware Engine using VMware HCX - Quickstart guide
- BlueXP Disaster Recovery as a Service (DRaaS) utilizes storage array based replication and automates certain tasks to recover the VMs at target site.
- With supported Continous Data Protection (CDP) products that use vSphere API for IO (VAIO) to intercept the data and send a copy to remote location for near zero RPO solution.

> When the source VM resides on block vVol datastore, it can be replicated with SnapMirror to Amazon FSx for NetApp ONTAP or Cloud Volumes ONTAP (CVO) at other supported cloud providers and consume as iSCSI volume with cloud native VMs.

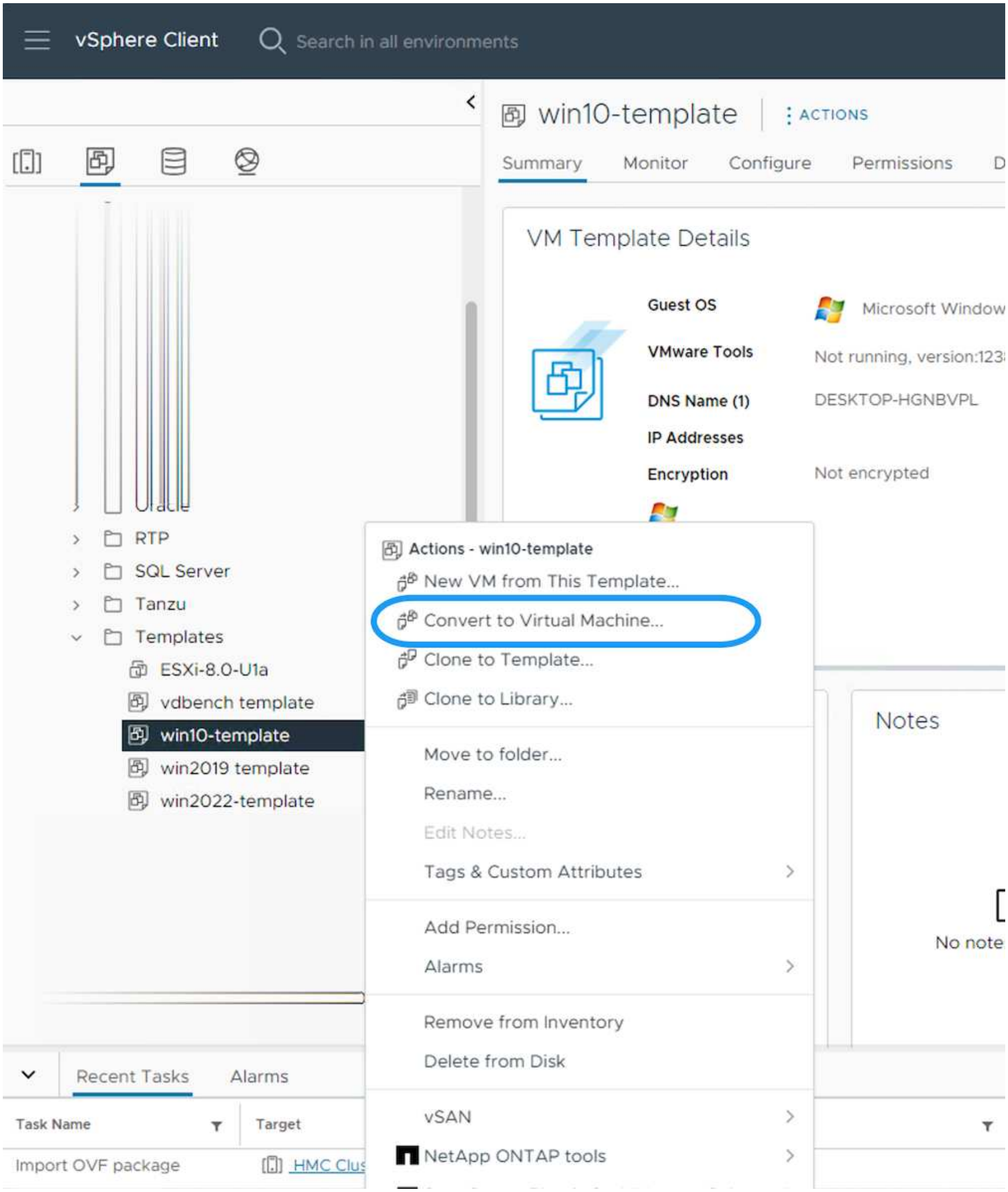
VM Template Migration Scenarios

VM Templates can be managed by vCenter Server or by a content library. Distribution of VM templates, OVF and OVA templates, other types of files are handled by publishing it in local content library and remote content libraries can subscribe to it.

- VM templates stored on vCenter inventory can be converted to VM and use the VM migration options.
- OVF and OVA templates, other types of files stored on content library can be cloned to other content libraries.
- Content library VM Templates can be hosted on any datastore and needs to be added into new content library.

Migration of VM templates hosted on datastore

1. In vSphere Web Client, right click on the VM template under VM and Templates folder view and select option to convert to VM.



VM Template Details

Guest OS: Microsoft Window

VMware Tools: Not running, version:123

DNS Name (1): DESKTOP-HGNBVPL

IP Addresses

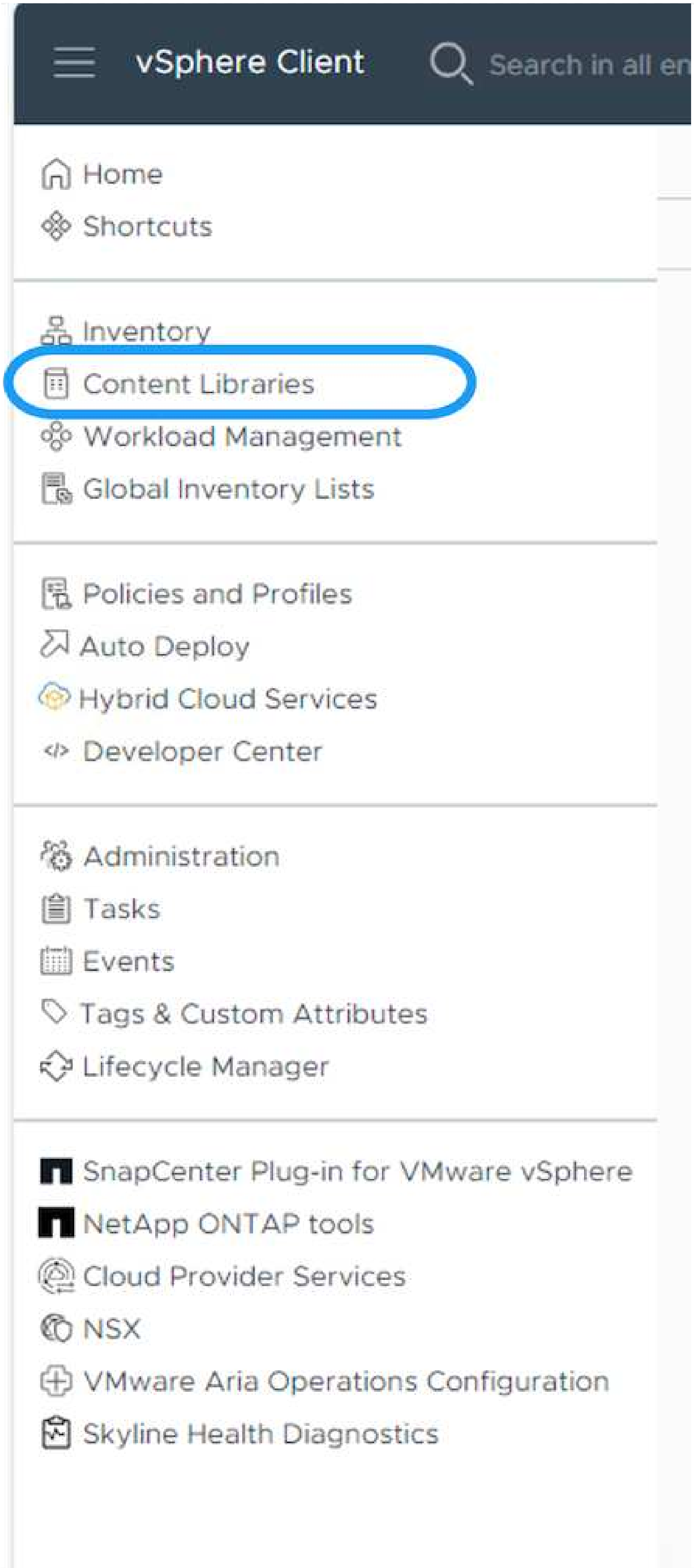
Encryption: Not encrypted

Task Name	Target
Import OVF package	HMC Clus

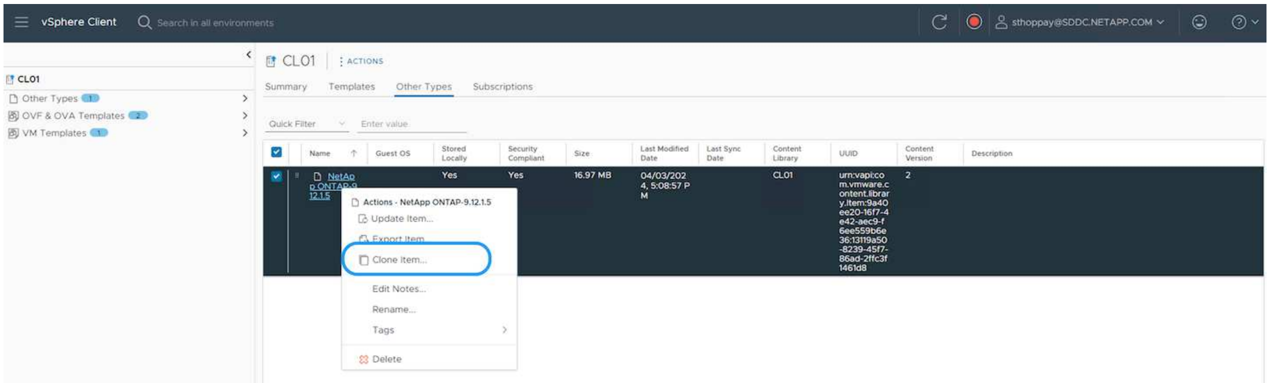
2. Once it is converted as VM, follow the VM migration options.

Clone of Content Library items

1. In vSphere Web Client, select Content Libraries


vSphere Client
Search in all en
Home
Shortcuts
Inventory
Content Libraries
Workload Management
Global Inventory Lists
Policies and Profiles
Auto Deploy
Hybrid Cloud Services
Developer Center
Administration
Tasks
Events
Tags & Custom Attributes
Lifecycle Manager
SnapCenter Plug-in for VMware vSphere
NetApp ONTAP tools
Cloud Provider Services
NSX
VMware Aria Operations Configuration
Skyline Health Diagnostics

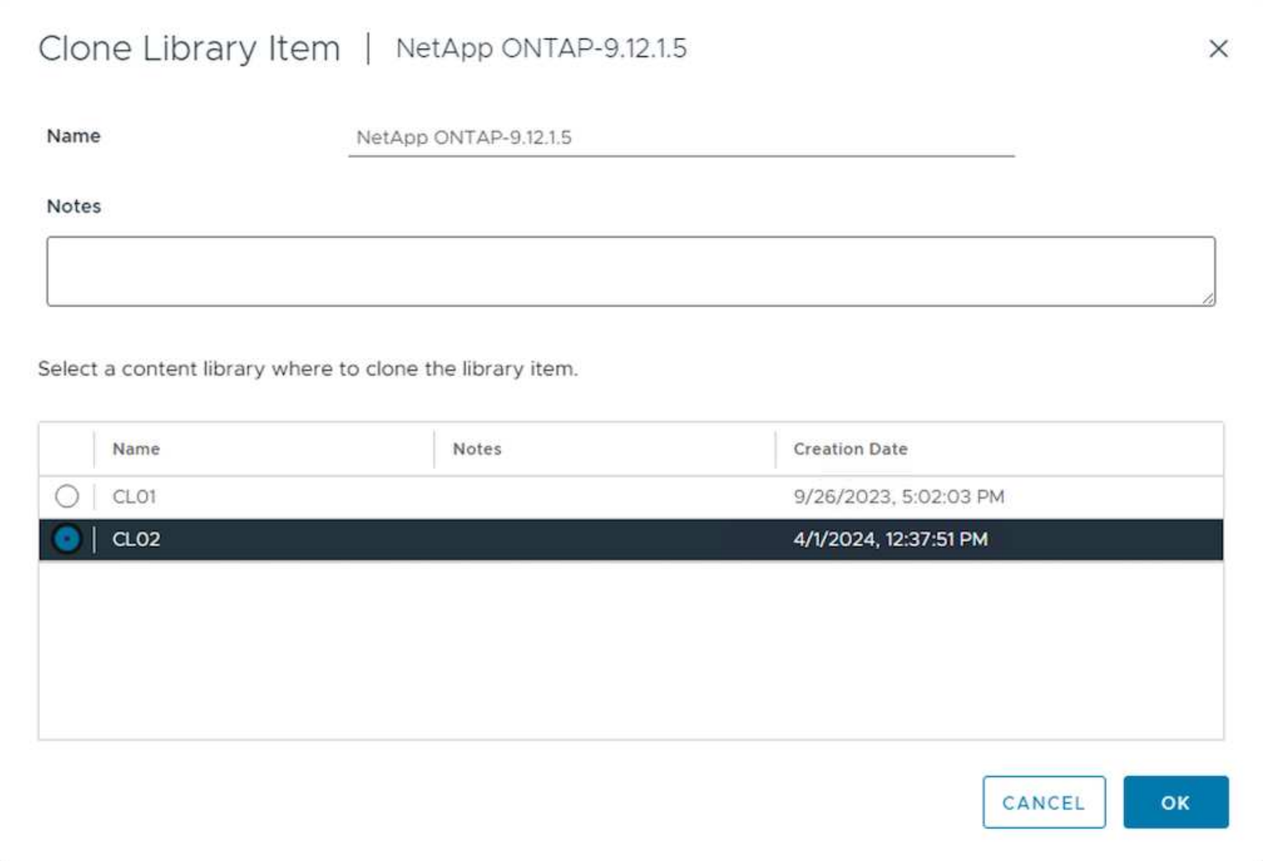
2. Select the content library in which the item you like to clone
3. Right click on the item and click on Clone Item ..



☑	Name	Guest OS	Stored Locally	Security Compliant	Size	Last Modified Date	Last Sync Date	Content Library	UUID	Content Version	Description
☑	NetApp ONTAP-9.12.1.5		Yes	Yes	16.97 MB	04/03/2024, 5:08:57 PM		CL01	urn:vapi:com.vmware.content.library.Item:9a40ee20-16f7-4e42-aec9-f6ee559b6e36:13119a50-8239-45f7-86ad-2ffc3f1461d8	2	

If using action menu, make sure correct target object is listed to perform action.

4. Select the target content library and click on OK.


Clone Library Item | NetApp ONTAP-9.12.1.5

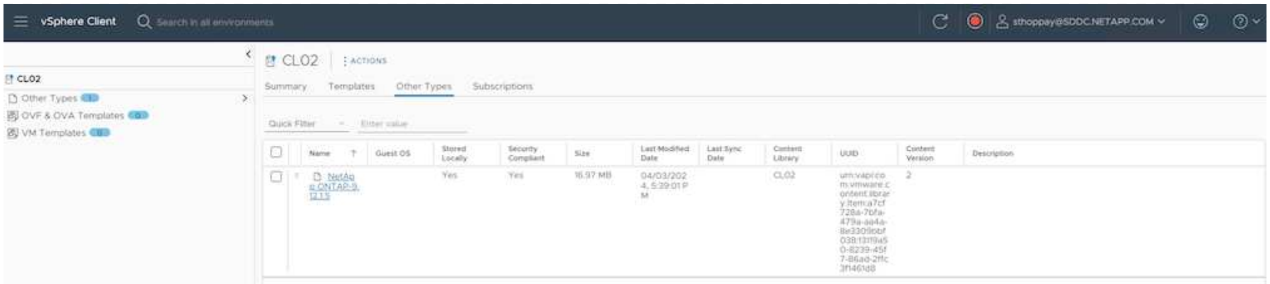
Name: NetApp ONTAP-9.12.1.5

Notes

Select a content library where to clone the library item.

	Name	Notes	Creation Date
○	CL01		9/26/2023, 5:02:03 PM
●	CL02		4/1/2024, 12:37:51 PM

5. Validate the item is available on target content library.



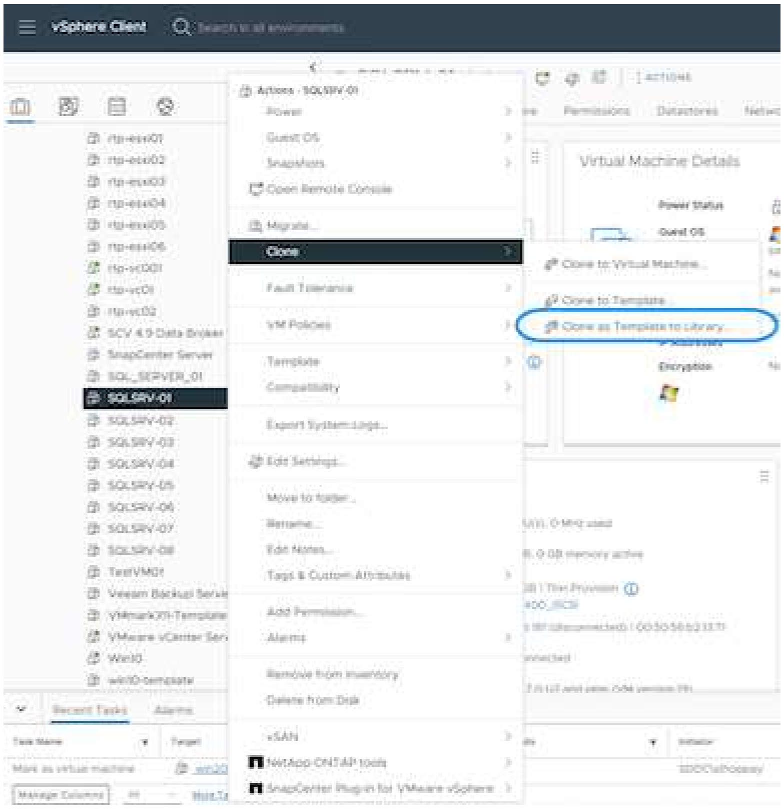
Name	Guest OS	Stored Locally	Security Compliant	Size	Last Modified Date	Last Sync Date	Content Library	UUID	Content Version	Description
NetApp ONTAP-9.12.1.5		Yes	Yes	16.97 MB	04/03/2024, 5:39:01 PM		CL02	urn:vapi:com:vmware:content:library:item:a7cf728a-7bfa-479a-aa4a-8e3309bbf038:13119a50-8239-45f7-86ad-2ffc3f1461d8	2	

Here is the sample PowerCLI script to copy the content libary items from content library CL01 to CL02.

```
#Authenticate to vCenter Server(s)
$sourcevc = Connect-VIServer -server 'vcenter01.domain' -force
$targetvc = Connect-VIServer -server 'vcenter02.domain' -force

#Copy content library items from source vCenter content library CL01 to
target vCenter content library CL02.
Get-ContentLibaryItem -ContentLibary (Get-ContentLibary 'CL01' -Server
$sourcevc) | Where-Object { $_.ItemType -ne 'vm-template' } | Copy-
ContentLibaryItem -ContentLibary (Get-ContentLibary 'CL02' -Server
$targetvc)
```

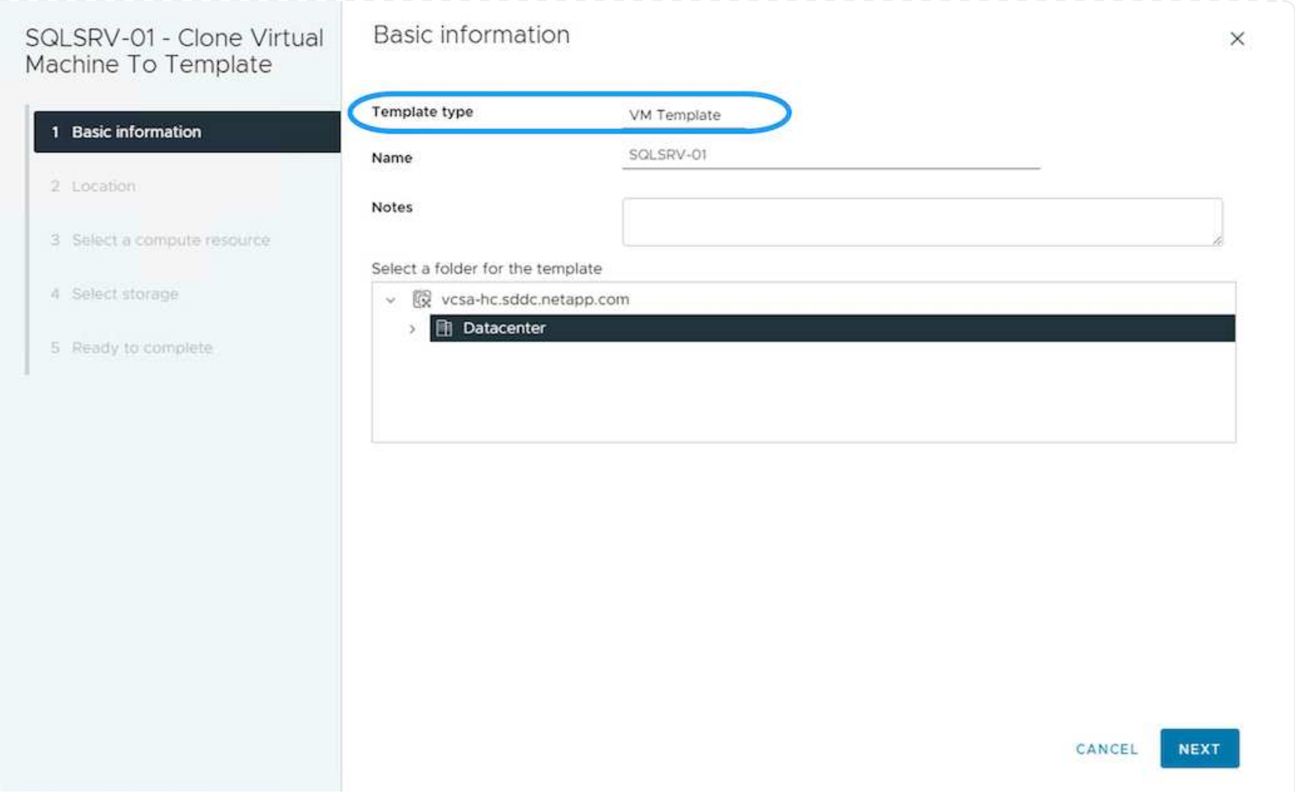
Adding VM as Templates in Content Library

1. In vSphere Web Client, select the VM and right click to choose Clone as Template in Library



When VM template is selected to clone in libary, it can only store it as OVF & OVA template and not as VM template.

2. Confirm Template type is selected as VM Template and follow answering the wizard to complete the operation.


SQLSRV-01 - Clone Virtual Machine To Template

1 Basic information
2 Location
3 Select a compute resource
4 Select storage
5 Ready to complete

Basic information

Template type: VM Template

Name: SQLSRV-01

Notes

Select a folder for the template

- vcsa-hc.sddc.netapp.com
  - Datacenter

For additional details on VM templates on content library, check vSphere VM administration guide

Use Cases

Migration from third party storage systems (including vSAN) to ONTAP datastores.

- Based on where the ONTAP datastore is provisioned, pick the VM migration options from above.

Migration from previous version to latest version of vSphere.

- If in-place upgrade is not possible, can bring up new environment and use the migration options above.

In Cross vCenter migration option, import from target if export option is not available on source. For that procedure, check Import or Clone a Virtual Machine with Advanced Cross vCenter vMotion

Migration to VCF Workload Domain.

- Migrate VMs from each vSphere Cluster to target workload domain.

> To allow network communication with existing VMs on other clusters on source vCenter, either extend NSX segment by adding the source vcenter vSphere hosts to transport zone or use L2 bridge on edge to allow L2 communication in VLAN. Check NSX documentation of Configure an Edge VM for Bridging

Additional Resources

- vSphere Virtual Machine Migration
- What's New in vSphere 8 for vMotion
- vSphere vMotion Resources
- Tier-0 Gateway Configurations in NSX Federation
- HCX 4.8 User Guide
- VMware Site Recovery Manager Documentation
- BlueXP disaster recovery for VMware

Migrate VMs to Amazon EC2 using FSxN

Migrate VMs to Amazon EC2 using FSxN: Overview

Organizations are accelerating their migrations to cloud computing solutions on AWS, taking advantage of services such as Amazon Elastic Compute Cloud (Amazon EC2) instances and Amazon FSx for NetApp ONTAP (FSx for ONTAP) to modernize their IT infrastructures, achieve cost savings, and improve operational efficiency. These AWS offerings enable migrations that optimize total cost of ownership (TCO) through consumption-based pricing models, enterprise storage features, providing the flexibility and scalability to meet evolving global business demands.

Overview

For enterprises deeply invested in VMware vSphere, migrating to AWS is a cost-effective option given the current market conditions, one that presents a unique opportunity.

As these organizations transition to AWS, they seek to capitalize on the cloud's agility and cost benefits while preserving familiar feature sets, particularly when it comes to storage. Maintaining seamless operations with familiar storage protocols—especially iSCSI—processes, tools, and skillsets is crucial when migrating workloads or setting up disaster recovery solutions.

Using the AWS managed storage service FSx for ONTAP for retaining the enterprise storage capabilities, that too coming from any third-party vendor storage from on-premises, enterprises can unlock the power of AWS while minimizing disruption and maximizing their future investments.

This technical report covers how to migrate on-premises VMware vSphere VMs to an Amazon EC2 instance with data disks placed on FSx for ONTAP iSCSI LUNs using the MigrateOps "data-mobility-as-code" functionality of Cirrus Migrate Cloud (CMC).

Solution requirements

There are a number of challenges that VMware customers are currently looking to solve. These organizations want to:

1. Leverage enterprise storage capabilities, such as thin provisioning, storage efficiency technologies, zero footprint clones, integrated backups, block-level replication, and tiering. This helps optimize migration efforts and future proof deployment on AWS from Day 1.
2. Optimize storage deployments currently on AWS that use Amazon EC2 instances by incorporating FSx for ONTAP and the cost-optimizing features it provides.
3. Reduce the total cost of ownership (TCO) of using Amazon EC2 instances with block storage solutions by rightsizing Amazon EC2 instances to meet the required IOPS and throughput parameters. With block storage, Amazon EC2 disk operations have a cap on bandwidth and I/O rates. File storage with FSx for ONTAP uses network bandwidth. In other words, FSx for ONTAP has no VM-level I/O limits.

Technical components overview

FSx for ONTAP concepts

Amazon FSx for NetApp ONTAP is a fully managed AWS storage service that provides NetApp® ONTAP® file systems with all the familiar ONTAP data management features, performance, and APIs on AWS. Its high-performance storage supports multiple protocols (NFS, SMB, iSCSI), providing a single service for workloads using Windows, Linux, and macOS EC2 instances.

Since FSx for ONTAP is an ONTAP file system, it brings a host of familiar NetApp features and services with it, including SnapMirror® data replication technology, thin clones, and NetApp Snapshot™ copies. By leveraging a low-cost capacity tier via data tiering, FSx for ONTAP is elastic and can reach a virtually unlimited scale. Plus, with signature NetApp storage efficiency technology, it reduces storage costs on AWS even further. For more, see Getting started with Amazon FSx for ONTAP.

File System

The central resource of FSx for ONTAP is its file system based on solid-state drive (SSD) storage. When provisioning an FSx for ONTAP file system, the user inputs a desired throughput and storage capacity, and selects an Amazon VPC where the file system will reside.

Users also have a choice between two built-in high-availability deployment models for the file system: Multi-Availability Zone (AZ) or single-AZ deployment. Each of these options offers its own level of durability and availability, which customers can select depending on their use case's business continuity requirements. Multi-AZ deployments consist of dual nodes that replicate seamlessly across two AZs. The more cost-optimized single-AZ deployment option structures the file system in two nodes split between two separate fault domains that both reside within a single AZ.
Storage Virtual Machines
Data in the FSx for ONTAP file system is accessed through a logical storage partition which is called a storage virtual machine (SVM). An SVM is actually its own file server equipped with its own data and admin access points. When accessing iSCSI LUNs on an FSx for ONTAP file system, the Amazon EC2 instance interfaces directly with the SVM using the SVM's iSCSI endpoint IP address.

While maintaining a single SVM in a cluster is possible, the option of running multiple SVMs in a cluster has a wide range of uses and benefits. Customers can determine the optimal number of SVMs to configure by considering their business needs, including their requirements for workload isolation.

Volumes

Data within an FSx for ONTAP SVM is stored and organized in structures known as volumes, which act as virtual containers. An individual volume can be configured with a single or multiple LUNs. The data stored in each volume consumes storage capacity in the file system. However, since FSx for ONTAP thinly provisions the volume, the volume only takes up storage capacity for the amount of data being stored.

The Cirrus Migrate Cloud MigrateOps concept

CMC is a transactable software-as-a-service (SaaS) offering from Cirrus Data Solutions, Inc. which is available via the AWS Marketplace. MigrateOps is a Data-Mobility-as-Code automation feature of CMC that allows you to declaratively manage your data mobility operations at scale using simple operation configurations in YAML. A MigrateOps configuration determines how you want your data mobility tasks to be executed. To learn more about MigrateOps, see About MigrateOps.

MigrateOps takes an automation-first approach, which is purpose-built to streamline the entire process, ensuring cloud-scale enterprise data mobility without operational disruptions. In addition to the already feature-rich functionalities that CMC offers for automation, MigrateOps further adds other automations that are often managed externally, such as:

- OS remediation
- Application cutover and approval scheduling
- Zero-downtime cluster migration
- Public/Private cloud platform integration
- Virtualization platform integration
- Enterprise storage management integration
- SAN (iSCSI) configuration

With the above tasks fully automated, all the tedious steps in preparing the on-prem source VM (such as adding AWS agents and tools), creation of destination FSx LUNs, setting up iSCSI and Multipath/MPIO at the AWS destination instance, and all the tasks of stopping/starting application services are eliminated by simply specifying parameters in a YAML file.

FSx for ONTAP is used to provide the data LUNs and rightsize the Amazon EC2 instance type, while providing all the features that organizations previously had in their on-premises environments. The MigrateOps feature of CMC will be used to automate all the steps involved, including provisioning mapped iSCSI LUNs, turning this into a predictable, declarative operation.

Note: CMC requires a very thin agent to be installed on the source and destination virtual machine instances to ensure secure data transfer from the storage source storage to FSx for ONTAP.

Benefits of using Amazon FSx for NetApp ONTAP with EC2 instances

FSx for ONTAP storage for Amazon EC2 instances provides several benefits:

- High throughput and low latency storage that provide consistent high performance for the most demanding workloads
- Intelligent NVMe caching improves performance
- Adjustable capacity, throughput, and IOPs can be changed on the fly and quickly adapt to changing storage demands
- Block-based data replication from on-premises ONTAP storage to AWS

- Multi-protocol accessibility, including for iSCSI, which is widely used in on-premises VMware deployments
- NetApp Snapshot™ technology and DR orchestrated by SnapMirror prevent data loss and speed up recovery
- Storage efficiency features that reduce storage footprint and costs, including thin provisioning, data deduplication, compression, and compaction
- Efficient replication reduces the time it takes to create backups from hours to just minutes, optimizing RTO
- Granular options for file back up and restores using NetApp SnapCenter®

Deploying Amazon EC2 instances with FSx ONTAP as the iSCSI-based storage layer delivers high performance, mission-critical data management features, and cost-reducing storage efficiency features that can transform your deployment on AWS.

Running a Flash Cache, multiple iSCSI sessions, and leveraging a working set size of 5%, it’s possible for FSx for ONTAP to deliver IOPS of ~350K, providing performance levels to meet even the most intensive workloads.

Since only network bandwidth limits are applied against FSx for ONTAP, not block storage bandwidth limits, users can leverage small Amazon EC2 instance types while achieving the same performance rates as much larger instance types. Using such small instance types also keeps compute costs low, optimizing TCO.

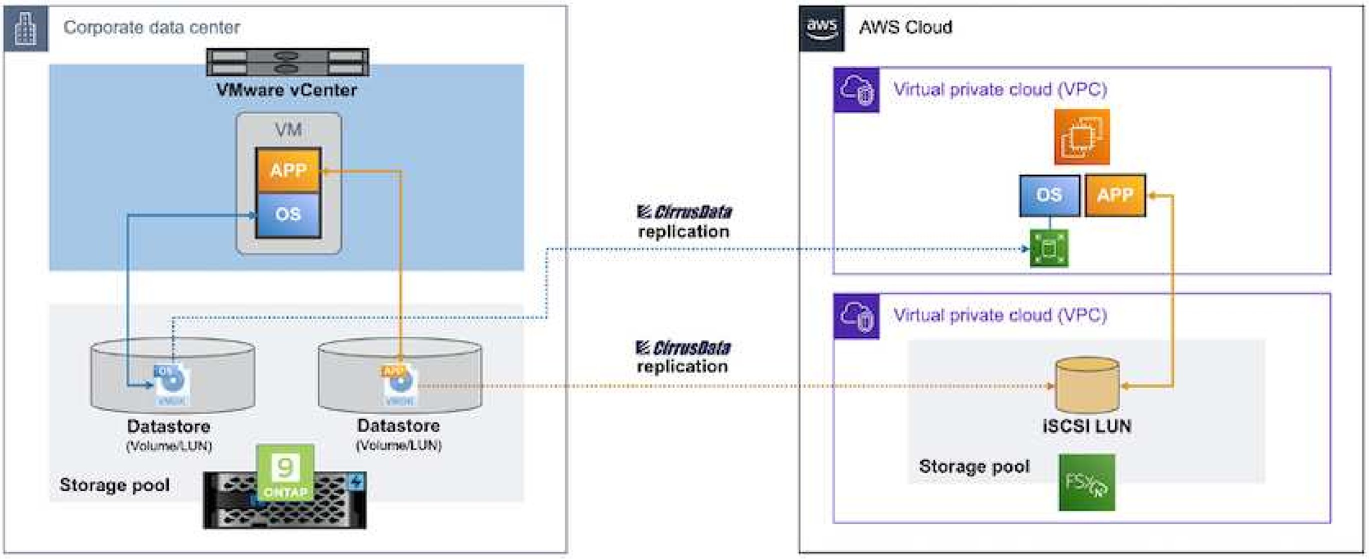
The ability of FSx for ONTAP to serve multiple protocols is another advantage, one that helps standardize a single AWS storage service for a wide range of existing data and file services requirements.
For enterprises deeply invested in VMware vSphere, migrating to AWS is a cost-effective option given the current market conditions, one that presents a unique opportunity.

Migrate VMs to Amazon EC2 using FSxN: Architecture and Pre-Requisites

This article shows the high-level architecture and deployment pre-requisites for completing the migration.

High level architecture

The diagram below illustrates the high-level architecture of migrating Virtual Machine Disk (VMDK) data on VMware to AWS using CMC MigrateOps:



Prerequisites

Before starting the walkthrough steps, make sure the following prerequisites are met:

On AWS

- An AWS account. This includes permissions for subnets, VPC setup, routing tables, security rule migration, security groups, and other requirements for networking such as load balancing. As with any migration, the most effort and consideration should go into networking.
- Appropriate IAM roles that allow you to provision both FSx for ONTAP and Amazon EC2 instances.
- Route tables and security groups are allowed to communicate with FSx for ONTAP.
- Add an inbound rule to the appropriate security group (see below for more details) to allow for secure data transfer from your on-premises data center to AWS.
- A valid DNS that can resolve public internet domain names.
- Check that your DNS resolution is functional and allows you to resolve host names.
- For optimal performance and rightsizing, use performance data from your source environment to rightsize your FSx for ONTAP storage.
- Each MigrateOps session uses one EIP, hence the quota for EIP should be increased for more parallelism. Keep in mind, the default EIP quota is 5.
- (If Active Directory-based workloads are being migrated) A Windows Active Directory domain on Amazon EC2.

For Cirrus Migrate Cloud

- A Cirrus Data Cloud account at cloud.cirrusdata.com must be created before using CMC. Outbound communication with the CDN, Cirrus Data endpoints, and software repository via HTTPS must be allowed.
- Allow communication (outbound) with Cirrus Data Cloud services via HTTPS protocol (Port 443).
- For a host to be managed by the CMC project, the deployed CMC software must initiate a one-way outbound TCP connection to Cirrus Data Cloud.
- Allow TCP protocol, Port 443 access to portal-gateway.cloud.cirrusdata.com which is currently at 208.67.222.222.
- Allow HTTP POST requests (via HTTPS connection) with binary data payload (application/octet-stream). This is similar to a file upload.
- Ensure that portal-gateway.cloud.cirrusdata.com is resolvable by your DNS (or via OS host file).
- If you have strict rules for prohibiting product instances to make outbound connections, the “Management Relay” feature of CMC can be used where the outbound 443 connection is from a single, secured non-production host.

Note: No storage data is ever sent to the Cirrus Data Cloud endpoint. Only management metadata is sent, and this can be optionally masked so that no real host name, volume name, network IP are included.

For migrating data from on-premises storage repositories to AWS, MigrateOps automates the management of a Host-to-Host (H2H) connection. These are optimized, one-way, TCP-based network connections that CMC uses to facilitate remote migration. This process features always-on compression and encryption that can reduce the amount of traffic by up to eight times, depending on the nature of the data.

Note: CMC is designed so that no production data / I/O leaves the production network during the entire migration phase. As a result, direct connectivity between the source and destination host is required.

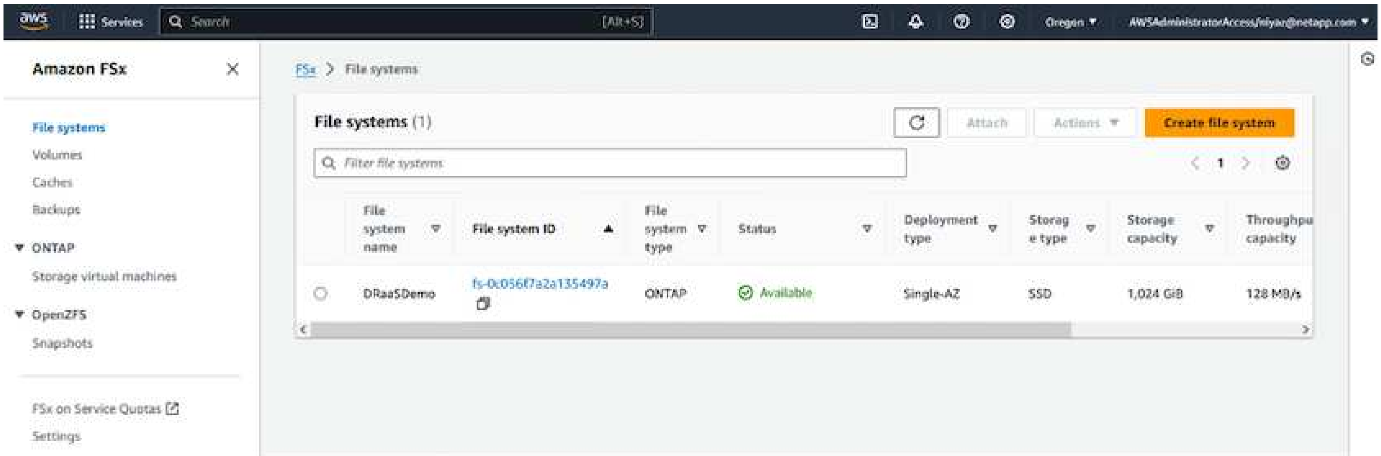
Migrate VMs to Amazon EC2 using FSxN: Deployment Guide

This article describes the deployment procedure for this migration solutions.

Configure FSx for ONTAP and Cirrus Data for migration operations

This step-by-step deployment guide shows how to add FSx for ONTAP volume to a VPC. Since these steps are sequential in nature, make sure they are covered in order.

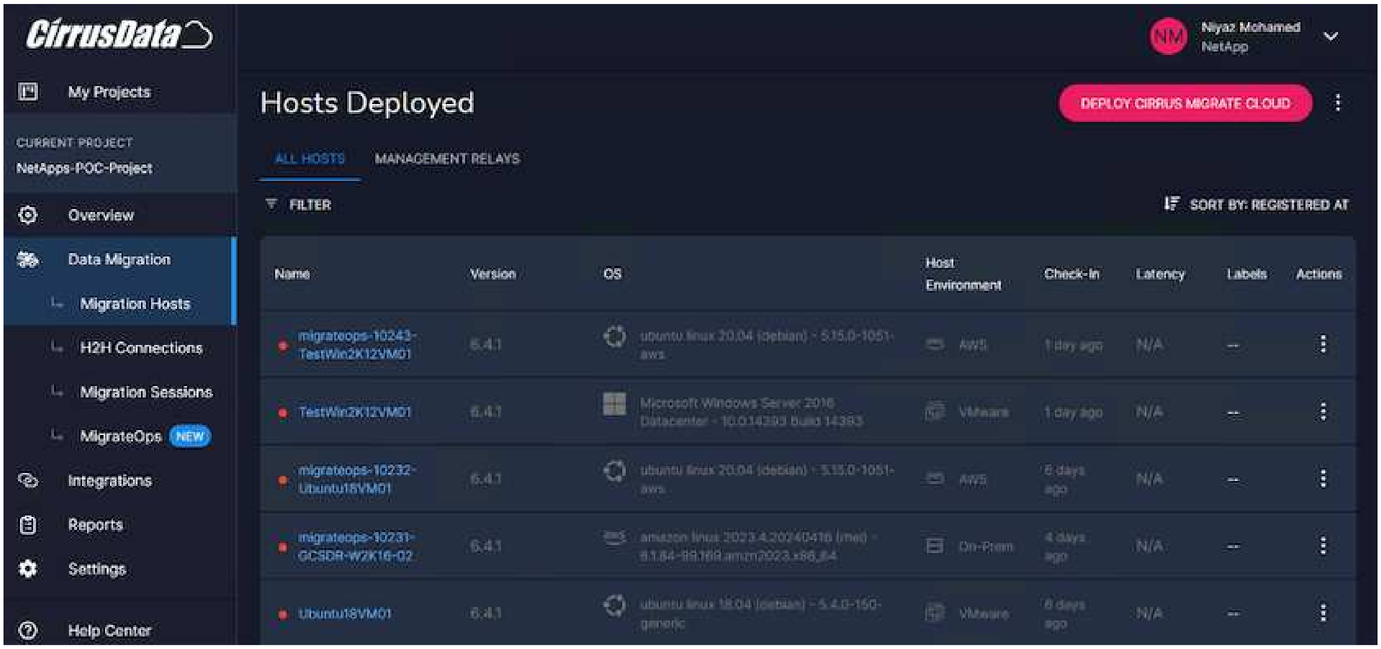
For the purposes of this demonstration, “DRaaSDemo” is the name of the file system created.



File systems (1)

	File system name	File system ID	File system type	Status	Deployment type	Storage type	Storage capacity	Throughput capacity
○	DRaaSDemo	fs-0c056f7a2a135497a	ONTAP	Available	Single-AZ	SSD	1,024 GiB	128 MB/s

Once your AWS VPC is configured and FSx for ONTAP is provisioned based on your performance requirements, log in to cloud.cirrusdata.com and create a new project or access an existing project.



Hosts Deployed

Name	Version	OS	Host Environment	Check-In	Latency	Labels	Actions
migrateops-10243-TestWin2K12VM01	6.4.1	ubuntu linux 20.04 (debian) - 5.15.0-1051-aws	AWS	1 day ago	N/A	--	⋮
TestWin2K12VM01	6.4.1	Microsoft Windows Server 2016 Datacenter - 10.0.14393 build 14393	VMware	1 day ago	N/A	--	⋮
migrateops-10232-Ubuntu18VM01	6.4.1	ubuntu linux 20.04 (debian) - 5.15.0-1051-aws	AWS	6 days ago	N/A	--	⋮
migrateops-10231-GCSDR-W2K16-02	6.4.1	amazon linux 2023.4.20240416 (rhel) - 6.1.84-99.169.amzn2023.x86_64	On-Prem	4 days ago	N/A	--	⋮
Ubuntu18VM01	6.4.1	ubuntu linux 18.04 (debian) - 5.4.0-150-generic	VMware	6 days ago	N/A	--	⋮

Before creating the recipe for MigrationOps, AWS Cloud should be added as an integration. CMC provides built-in integration with FSx for ONTAP and AWS. The integration for FSx for ONTAP provides the following automated functionalities:

Prepare your FSx for ONTAP file system:

- Create new volumes and LUNs that match the source volumes

Note: A destination disk in the FSx for ONTAP FS model is a “LUN” that is created on a “Volume” that has enough capacity to contain the LUN plus a reasonable amount of overhead for facilitating snapshots and meta-data. The CMC automation takes care of all these details to create the appropriate Volume and the LUN with optional user-defined parameters.

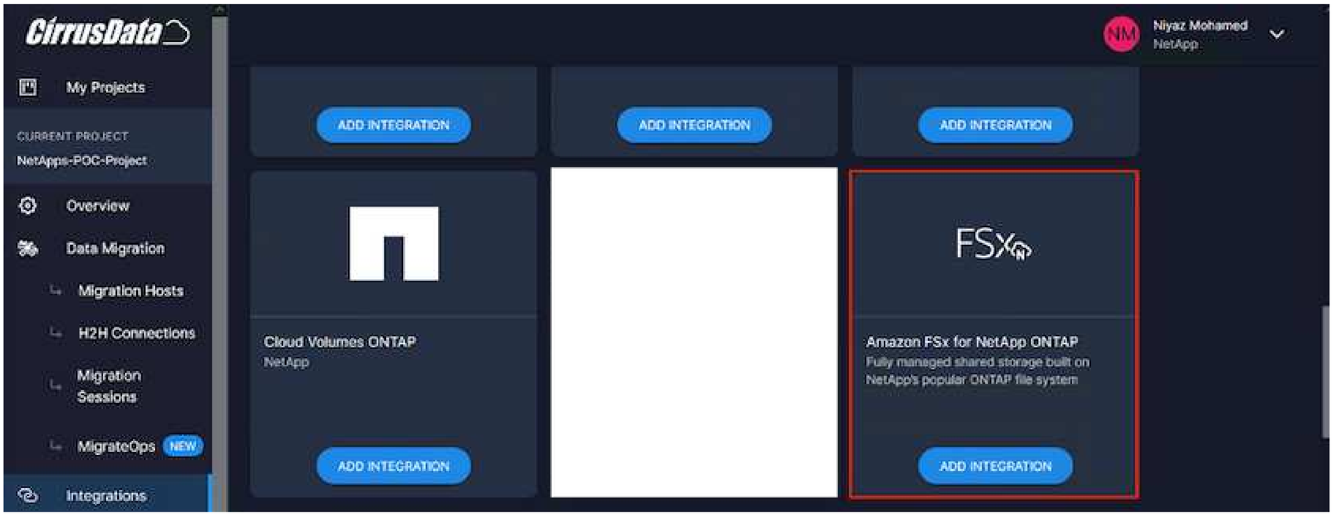
- Create Host entity (called iGroups in FSx) with the Host Initiator IQN
- Map newly created volumes to appropriate host entities using mappings
- Create all other necessary configurations

Prepare Production Host for iSCSI connection:

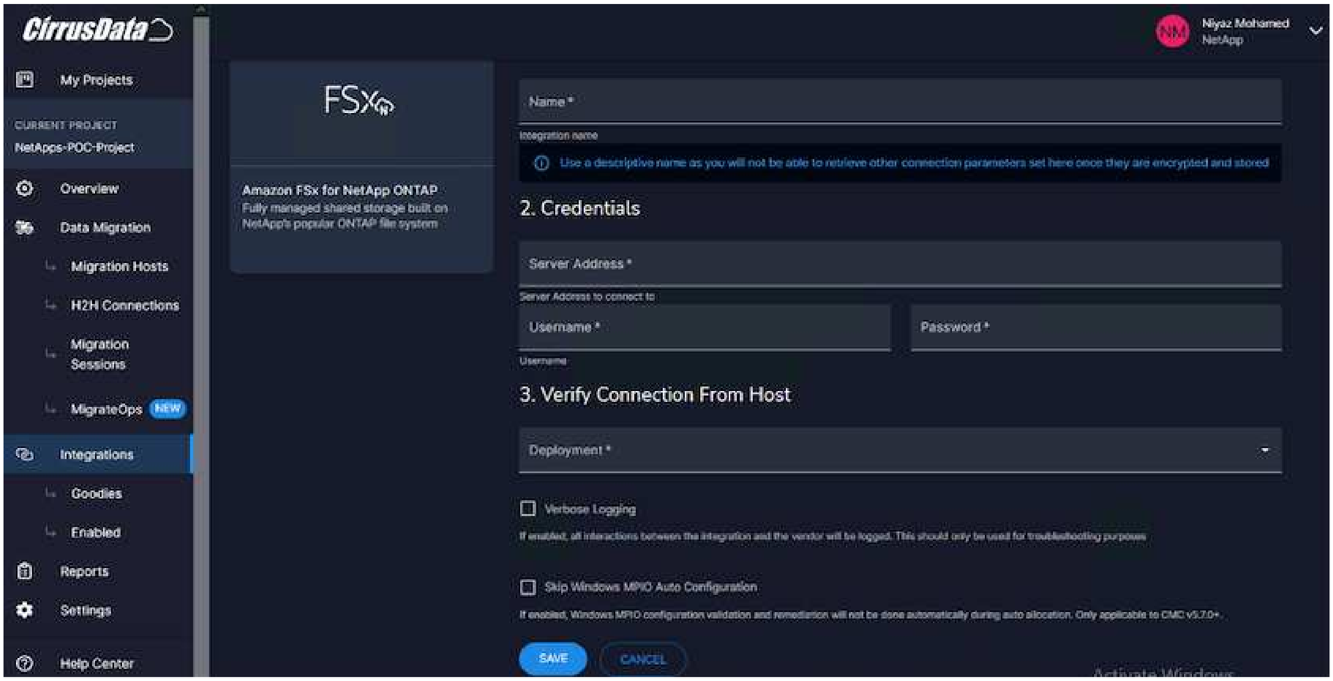
- If necessary, install and configure iSCSI feature and set up Initiator.
- If necessary, install and configure multipath (MPIO for Windows) with proper vendor identifiers.
- Adjust system settings, if necessary, according to vendor best practices, e.g. with udev settings on Linux.
- Create and manage iSCSI connections such as persistent/favorite iSCSI targets on Windows.

To configure CMC Integration for FSx for ONTAP and AWS, perform the following steps:

1. Log in to the Cirrus Data Cloud portal.
2. Go to the Project for which you want to enable the integration.
3. Navigate to Integrations → Goodies.
4. Scroll to find FSx for NetApp ONTAP and click ADD INTEGRATION.



5. Provide a descriptive name (strictly for display purposes) and add the appropriate credentials.



Amazon FSx for NetApp ONTAP
Fully managed shared storage built on NetApp's popular ONTAP file system

Integration name

Use a descriptive name as you will not be able to retrieve other connection parameters set here once they are encrypted and stored

Server Address to connect to

Username

□ Verbose Logging

If enabled, all interactions between the integration and the vendor will be logged. This should only be used for troubleshooting purposes

□ Skip Windows MPIO Auto Configuration

If enabled, Windows MPIO configuration validation and remediation will not be done automatically during auto allocation. Only applicable to CMC v5.7.0+.

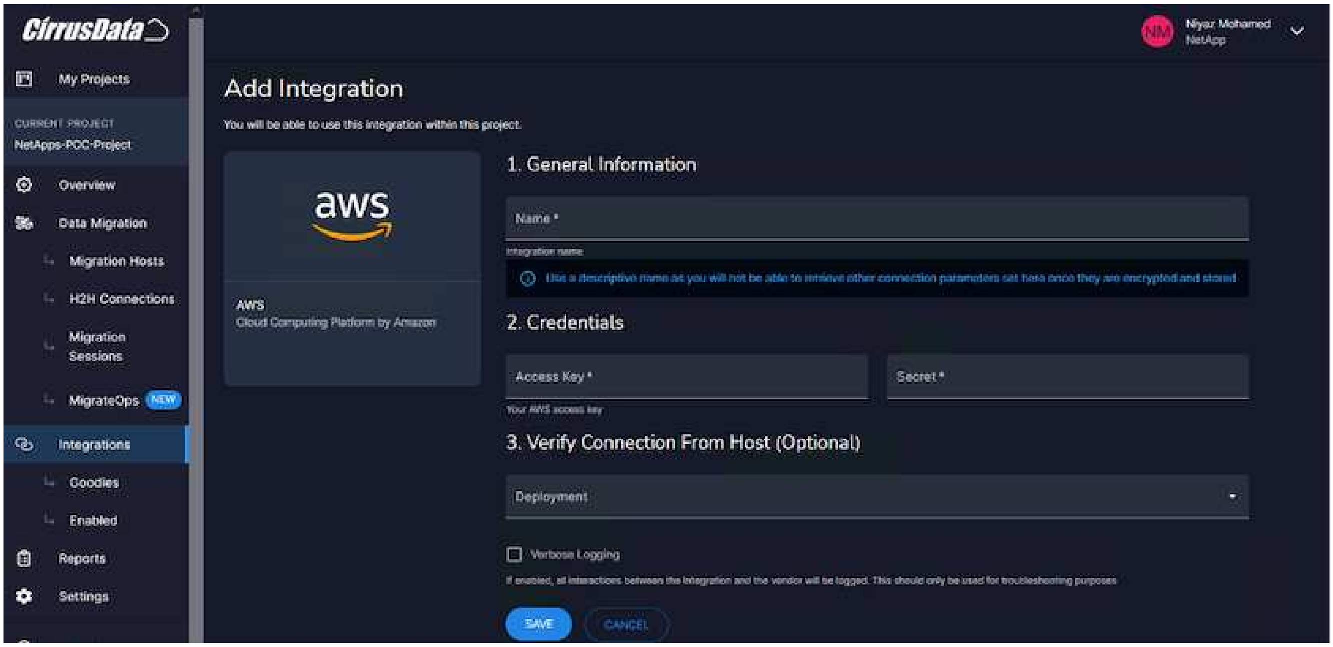
6. Once the integration is created, during the creation of a new migration session, select Auto Allocate Destination Volumes to automatically allocate new volumes on FSx for ONTAP.

   Note: New LUNs will be created with the same size as the source volume’s size, unless “Migrate to Smaller Volumes” is enabled for the migration.

   Note: If a host entity (iGroup) doesn’t already exist, a new one will be created. All host iSCSI Initiator IQNs will be added to that new host entity.

   Note: If an existing host entity with any of the iSCSI initiators already exists, it will be reused.

7. Once done, add the integration for AWS, following the steps on the screen.



Add Integration

You will be able to use this integration within this project.

AWS
Cloud Computing Platform by Amazon

Integration name

Use a descriptive name as you will not be able to retrieve other connection parameters set here once they are encrypted and stored

Your AWS access key

□ Verbose Logging

If enabled, all interactions between the integration and the vendor will be logged. This should only be used for troubleshooting purposes

Note: This integration is used while migrating virtual machines from on-premises storage to AWS along with FSx for ONTAP integration.

Note: Use management relays to communicate with Cirrus Data Cloud if there is no direct outbound connection for production instances to be migrated.

With Integrations added, it’s time to register hosts with the Project. Let’s cover this with an example scenario.

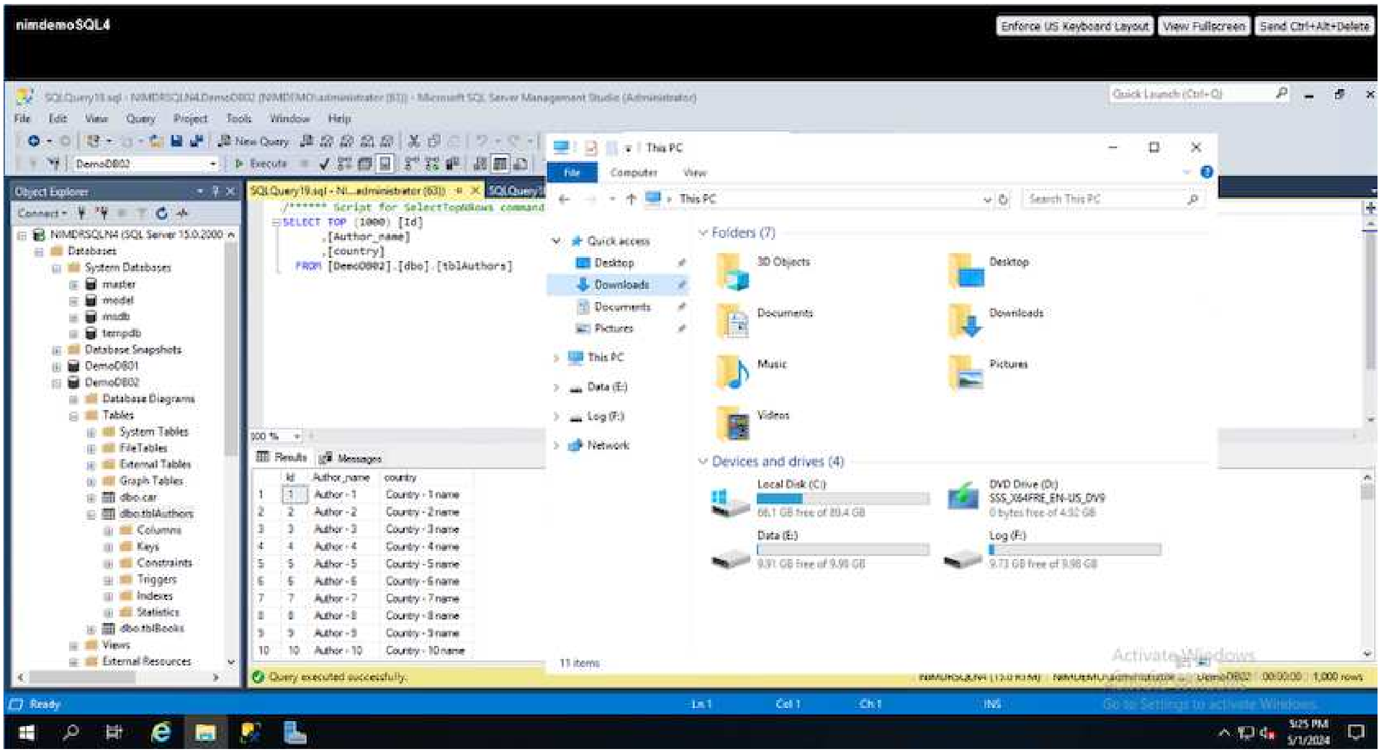
Host registration scenario

Guest VMware VMs residing on vCenter in on-premises data center:

- Windows 2016 running with SQL Server with three VMDKs including OS and data disks. It is running an active database. The database is located on a data volume backed by two VMDKs.

Note: Since the source is a VMware environment and VMDKs are used, the Windows iSCSI Initiator software is not currently configured on this guest VM. To connect to our destination storage via iSCSI, both iSCSI and MPIO will have to be installed and configured. Cirrus Data Cloud integration will perform this installation automatically during the process.

Note: The Integration configured in the previous section automates the configuration of the new destination storage in creating the new disks, setting up the host entities and their IQNs, and even remediation of the application VM (host) for iSCSI and multipath configurations.



```
/****** Script for SelectTopNRows command
SELECT TOP (1000) [Id]
      ,[Author_name]
      ,[country]
  FROM [DemoDB02].[dbo].[tblAuthors]
```

	Id	Author_name	country
1	1	Author - 1	Country - 1 name
2	2	Author - 2	Country - 2 name
3	3	Author - 3	Country - 3 name
4	4	Author - 4	Country - 4 name
5	5	Author - 5	Country - 5 name
6	6	Author - 6	Country - 6 name
7	7	Author - 7	Country - 7 name
8	8	Author - 8	Country - 8 name
9	9	Author - 9	Country - 9 name
10	10	Author - 10	Country - 10 name

Query executed successfully.

This demonstration will migrate the application VMDKs from each VM to an automatically provisioned and mapped iSCSI volume from FSx for ONTAP. The OS VMDK in this case will be migrated to an Amazon EBS volume as Amazon EC2 instances support this Amazon EBS only as the boot disk.

Note: The scale factor with this migration approach is the network bandwidth and the pipe connecting on-premises to AWS VPC. Since each VM has 1:1 host session configured, the overall migration performance depends on two factors:

- Network bandwidth

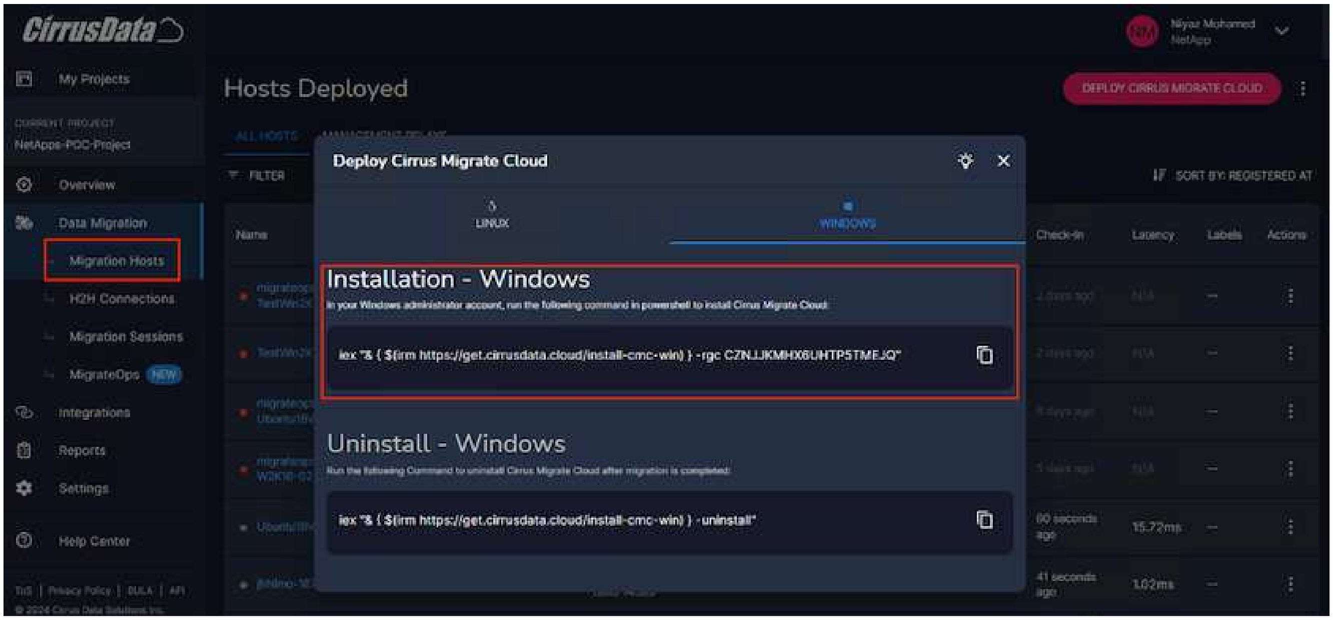
- Target instance type and ENI bandwidth

The migration steps are as follows:

1. Install CMC agent on each host (Windows and Linux) designated for the migration wave. This can be performed by executing a one-line installation command.

   To do this, access Data Migration > Migration Hosts > Click on “Deploy Cirrus Migrate Cloud” and click to select “Windows”.

   Then, copy the `iex` command to the host and run it using PowerShell. Once the deployment of the agent is successful, the host will be added to the Project under “Migration hosts”.



Deploy Cirrus Migrate Cloud

Installation - Windows

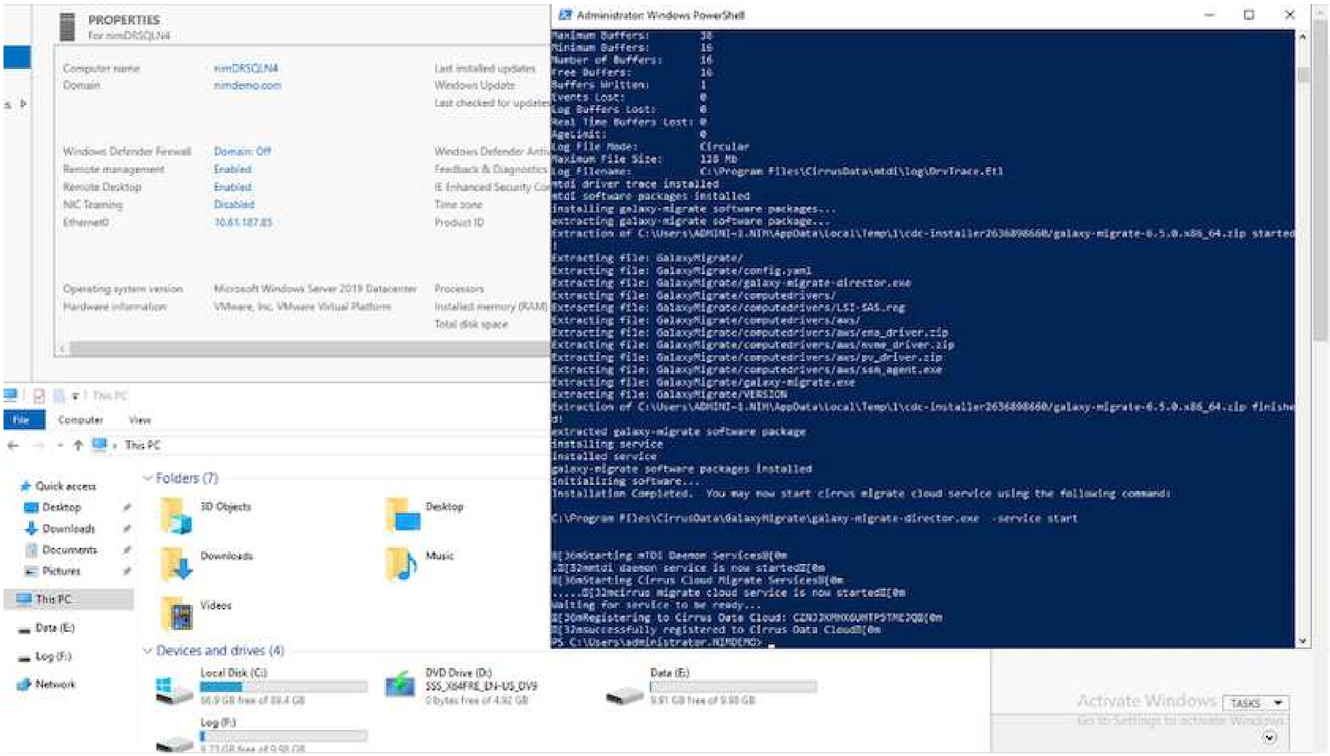
In your Windows administrator account, run the following command in powershell to install Cirrus Migrate Cloud:

```
iex "& { $(irm https://get.cirrusdata.cloud/install-cmc-win) } -rgc CZNJJKMHX6UHTP5TMEJQ"
```

Uninstall - Windows

Run the following Command to uninstall Cirrus Migrate Cloud after migration is completed:

```
iex "& { $(irm https://get.cirrusdata.cloud/install-cmc-win) } -uninstall"
```



Computer name nimDRSQLN4
Domain nimdemo.com

Windows Defender Firewall Domain: Off
Remote management Enabled
Remote Desktop Enabled
NIC Teaming Disabled
Ethernet0 10.61.187.85

Operating system version Microsoft Windows Server 2019 Datacenter
Hardware information VMware, Inc. VMware Virtual Platform

Administrator: Windows PowerShell

```
Maximum Buffers:          38
Minimum Buffers:          16
Number of Buffers:        16
Free Buffers:             16
Buffers Written:          1
Events Lost:              0
Log Buffers Lost:         0
Real Time Buffers Lost:   0
AgeLimit:                 0
Log File Mode:            Circular
Maximum File Size:        128 Mb
Log Filename:             C:\Program Files\CirrusData\mtdi\log\DrvTrace.Etl
mtdi driver trace installed
mtdi software packages installed
installing galaxy-migrate software packages...
extracting galaxy-migrate software package...
Extraction of C:\Users\ADMINI~1.NIM\AppData\Local\Temp\1\cdc-installer2636898660/galaxy-migrate-6.5.0.x86_64.zip started
!
Extracting file: GalaxyMigrate/
Extracting file: GalaxyMigrate/config.yaml
Extracting file: GalaxyMigrate/galaxy-migrate-director.exe
Extracting file: GalaxyMigrate/computedrivers/
Extracting file: GalaxyMigrate/computedrivers/LSI-SAS.reg
Extracting file: GalaxyMigrate/computedrivers/aws/
Extracting file: GalaxyMigrate/computedrivers/aws/ena_driver.zip
Extracting file: GalaxyMigrate/computedrivers/aws/nvme_driver.zip
Extracting file: GalaxyMigrate/computedrivers/aws/pv_driver.zip
Extracting file: GalaxyMigrate/computedrivers/aws/ssm_agent.exe
Extracting file: GalaxyMigrate/galaxy-migrate.exe
Extracting file: GalaxyMigrate/VERSION
Extraction of C:\Users\ADMINI~1.NIM\AppData\Local\Temp\1\cdc-installer2636898660/galaxy-migrate-6.5.0.x86_64.zip finishe
d!
extracted galaxy-migrate software package
installing service
installed service
galaxy-migrate software packages installed
initializing software...
Installation Completed.  You may now start cirrus migrate cloud service using the following command:

C:\Program Files\CirrusData\GalaxyMigrate\galaxy-migrate-director.exe  -service start


[36mStarting mTDI Daemon Services[0m
.[32mmtdi daemon service is now started[0m
[36mStarting Cirrus Cloud Migrate Services[0m
.....[32mcirrus migrate cloud service is now started[0m
Waiting for service to be ready...
[36mRegistering to Cirrus Data Cloud: CZNJJKMHX6UHTP5TMEJQ[0m
[32msuccessfully registered to Cirrus Data Cloud[0m
PS C:\Users\administrator.NIMDEMO> _
```

2. Prepare the YAML for each virtual machine.

   Note: It is a vital step to have a YAML for each VM that specifies the necessary recipe or blueprint for the migration task.

   The YAML provides the operation name, notes (description) along with the recipe name as `MIGRATEOPS_AWS_COMPUTE`, the host name (`system_name`) and integration name (`integration_name`) and the source and destination configuration. Custom scripts can be specified as a before and after cutover action.

```
operations:
    -   name: Win2016 SQL server to AWS
        notes: Migrate OS to AWS with EBS and Data to FSx for ONTAP
        recipe: MIGRATEOPS_AWS_COMPUTE
        config:
            system_name: Win2016-123
            integration_name: NimAWShybrid
            migrateops_aws_compute:
                region: us-west-2
                compute:
                    instance_type: t3.medium
                    availability_zone: us-west-2b
                network:
                    vpc_id: vpc-05596abe79cb653b7
                    subnet_id: subnet-070aeb9d6b1b804dd
                    security_group_names:
                        - default
                destination:
                    default_volume_params:
                        volume_type: GP2
                    iscsi_data_storage:
                        integration_name: DemoDRaaS
                        default_volume_params:
                            netapp:
                                qos_policy_name: ""
                migration:
                    session_description: Migrate OS to AWS with EBS and
Data to FSx for ONTAP
                    qos_level: MODERATE
                cutover:
                    stop_applications:
                        - os_shell:
                              script:
                                  - stop-service -name 'MSSQLSERVER'
-Force
                                  - Start-Sleep -Seconds 5
                                  - Set-Service -Name 'MSSQLSERVER'
```

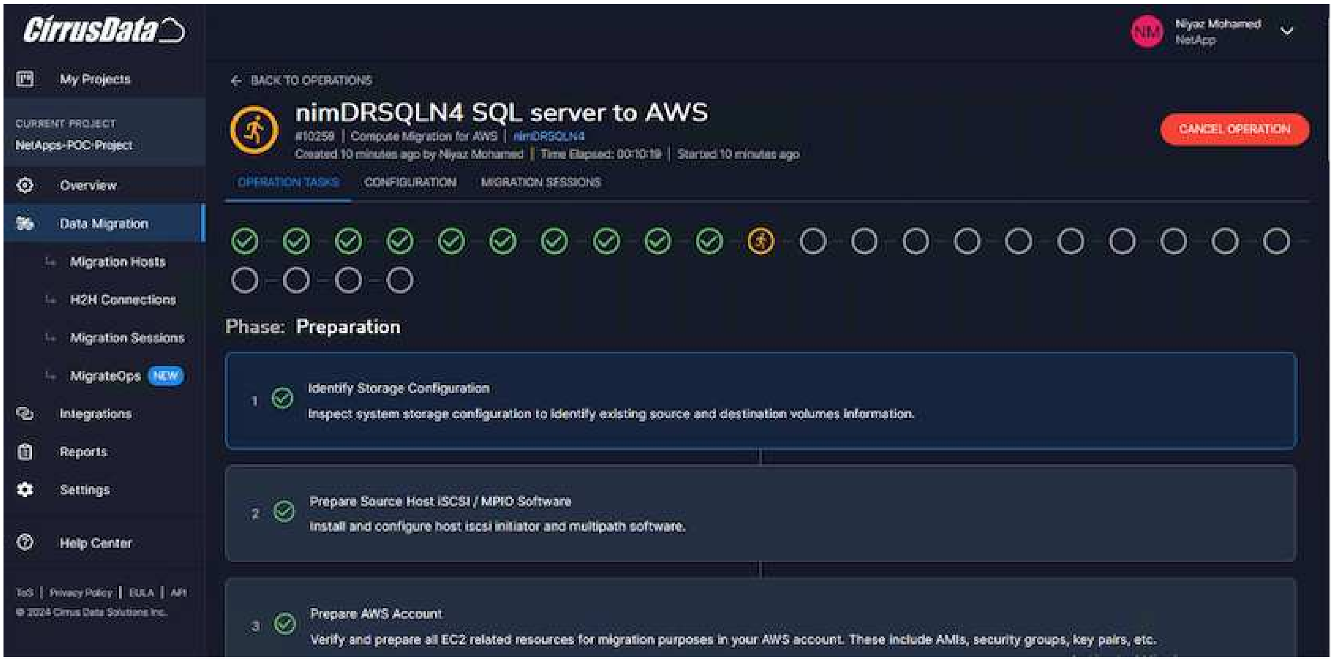
```
-StartupType Disabled
                                  - write-output "SQL service stopped
and disabled"

                        - storage_unmount:
                              mountpoint: e
                        - storage_unmount:
                              mountpoint: f
                    after_cutover:
                        - os_shell:
                              script:
                                  - stop-service -name 'MSSQLSERVER'
-Force
                                  - write-output "Waiting 90 seconds to
mount disks..." > log.txt
                                  - Start-Sleep -Seconds 90
                                  - write-output "Now re-mounting disks
E and F for SQL..." >>log.txt
                        - storage_unmount:
                              mountpoint: e
                        - storage_unmount:
                              mountpoint: f
                        - storage_mount_all: {}
                        - os_shell:
                              script:
                                  - write-output "Waiting 60 seconds to
restart SQL Services..." >>log.txt
                                  - Start-Sleep -Seconds 60
                                  - stop-service -name 'MSSQLSERVER'
-Force
                                  - Start-Sleep -Seconds 3
                                  - write-output "Start SQL Services..."
>>log.txt
                                  - Set-Service -Name 'MSSQLSERVER'
-StartupType Automatic
                                  - start-service -name 'MSSQLSERVER'
                                  - write-output "SQL started" >>log.txt
```

3. Once the YAMLs are in place, create MigrateOps configuration. To do this, go to Data Migration > MigrateOps, click on “Start New Operation” and enter the configuration in valid YAML format.
4. Click “Create operation”.

   Note: To achieve parallelism, each host needs to have a YAML file specified and configured.

5. Unless the `scheduled_start_time` field is specified in the configuration, the operation will start immediately.

6. The operation will now execute and proceed. From the Cirrus Data Cloud UI, you can monitor the progress with detailed messages. These steps automatically include tasks that are normally done manually, such as performing auto allocation and creating migration sessions.



nimDRSQLN4 SQL server to AWS

#10259 | Compute Migration for AWS | nimDRSQLN4

Created 10 minutes ago by Niyaz Mohamed | Time Elapsed: 00:10:19 | Started 10 minutes ago

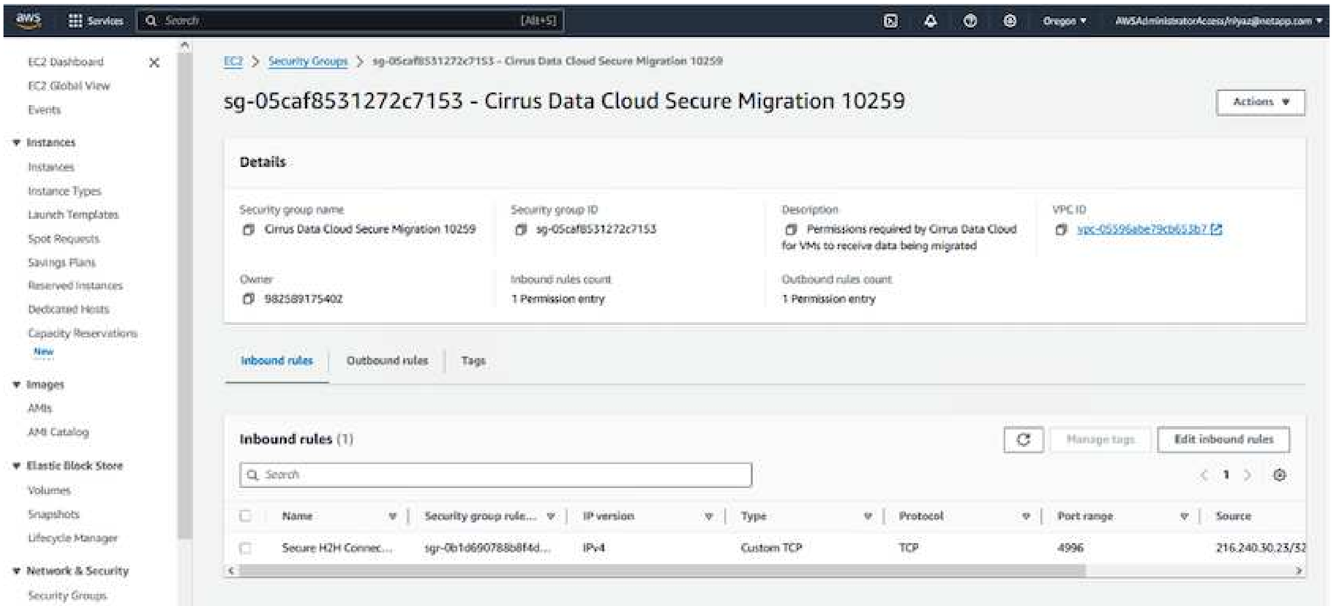
Phase: Preparation

1 ✓ Identify Storage Configuration
Inspect system storage configuration to identify existing source and destination volumes information.

2 ✓ Prepare Source Host iSCSI / MPIO Software
Install and configure host iscsi initiator and multipath software.

3 ✓ Prepare AWS Account
Verify and prepare all EC2 related resources for migration purposes in your AWS account. These include AMIs, security groups, key pairs, etc.

Note: During the host-to-host migration, an additional security group with a rule allowing Inbound 4996 port will be created, which will allow the required port for communication and it will be automatically deleted once the synchronization is complete.



EC2 > Security Groups > sg-05caf8531272c7153 - Cirrus Data Cloud Secure Migration 10259

sg-05caf8531272c7153 - Cirrus Data Cloud Secure Migration 10259

Details

Security group name: Cirrus Data Cloud Secure Migration 10259

Security group ID: sg-05caf8531272c7153

Description: Permissions required by Cirrus Data Cloud for VMs to receive data being migrated

VPC ID: vpc-05596abe79cb653b7

Owner: 982589175402

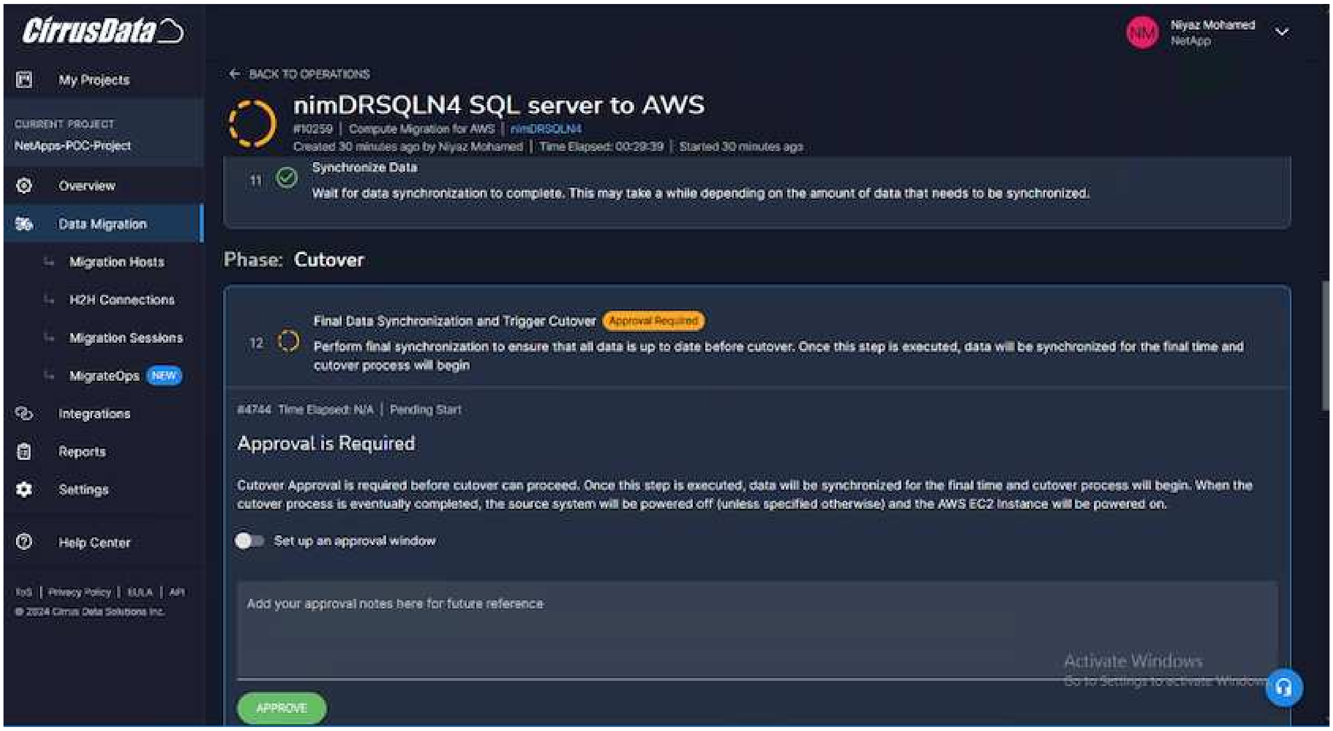
Inbound rules count: 1 Permission entry

Outbound rules count: 1 Permission entry

Inbound rules (1)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
Secure H2H Connec...	sgr-0b1d690788b8f4d...	IPv4	Custom TCP	TCP	4996	216.240.30.23/32

7. While this migration session is synchronizing, there is a future step in phase 3 (cutover) with the label “Approval Required.” In a MigrateOps recipe, critical tasks (such as migration cutovers) require user approval before they can be executed. Project Operators or Administrators can approve these tasks from the UI. A future approval window can also be created.



nimDRSQLN4 SQL server to AWS

#10259 | Compute Migration for AWS | nimDRSQLN4

Created 30 minutes ago by Niyaz Mohamed | Time Elapsed: 00:29:39 | Started 30 minutes ago

11 Synchronize Data

Wait for data synchronization to complete. This may take a while depending on the amount of data that needs to be synchronized.

Phase: Cutover

12 Final Data Synchronization and Trigger Cutover Approval Required

Perform final synchronization to ensure that all data is up to date before cutover. Once this step is executed, data will be synchronized for the final time and cutover process will begin

#4744 Time Elapsed: N/A | Pending Start

Approval is Required

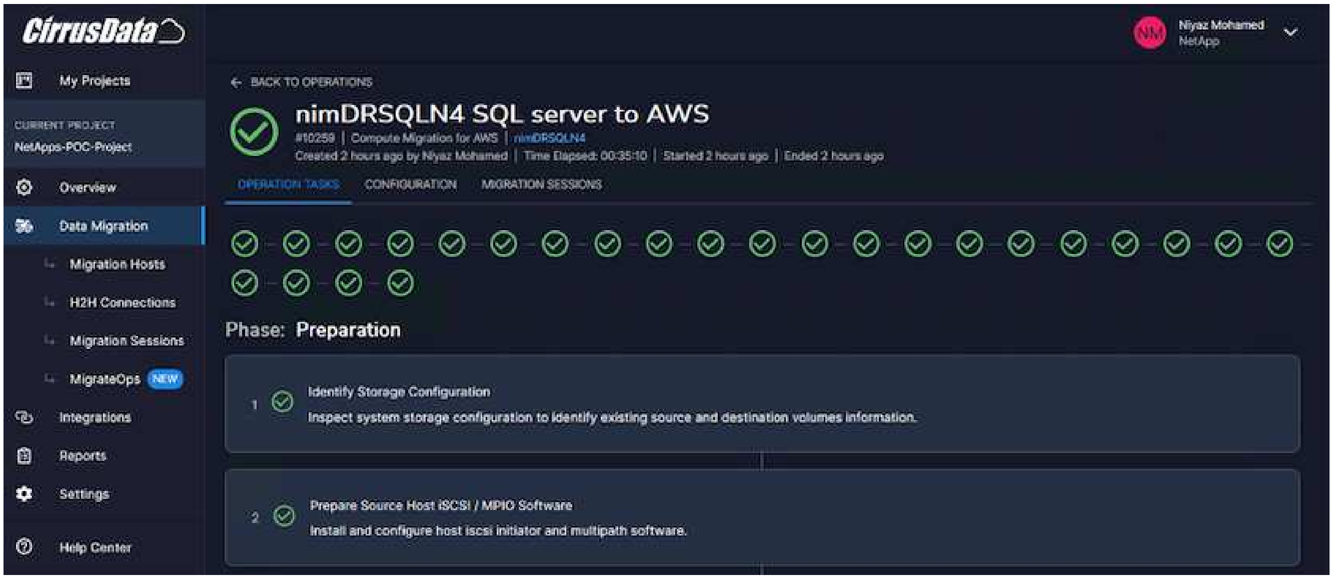
Cutover Approval is required before cutover can proceed. Once this step is executed, data will be synchronized for the final time and cutover process will begin. When the cutover process is eventually completed, the source system will be powered off (unless specified otherwise) and the AWS EC2 Instance will be powered on.

○ Set up an approval window

Add your approval notes here for future reference

APPROVE

8. Once approved, the MigrateOps operation continues with the cutover.
9. After a brief moment, the operation will be completed.



nimDRSQLN4 SQL server to AWS

#10259 | Compute Migration for AWS | nimDRSQLN4

Created 2 hours ago by Niyaz Mohamed | Time Elapsed: 00:35:10 | Started 2 hours ago | Ended 2 hours ago

Phase: Preparation

1 Identify Storage Configuration

Inspect system storage configuration to identify existing source and destination volumes information.

2 Prepare Source Host iSCSI / MPIO Software

Install and configure host iscsi initiator and multipath software.

Note: With the help of Cirrus Data cMotion™ technology, the destination storage has been kept up-to-date with all the latest changes. Therefore, after approval is given, this entire final cutover process will take a very short time—less than a minute—to complete.

Post-migration verification

Let’s look at the migrated Amazon EC2 instance running the Windows Server OS and the following steps that have completed:

1. Windows SQL Services are now started.

2. The database is back online and is using storage from the iSCSI Multipath device.
3. All new database records added during migration can be found in the newly migrated database.
4. The old storage is now offline.

Note: With just one click to submit the data mobility operation as code, and a click to approve the cutover, the VM has successfully migrated from on-premises VMware to an Amazon EC2 instance using FSx for ONTAP and its iSCSI capabilities.

Note: Due to AWS API limitation, the converted VMs would be shown as "Ubuntu." This is strictly a display issue and does not affect functionality of the migrated instance. An upcoming release will address this issue.

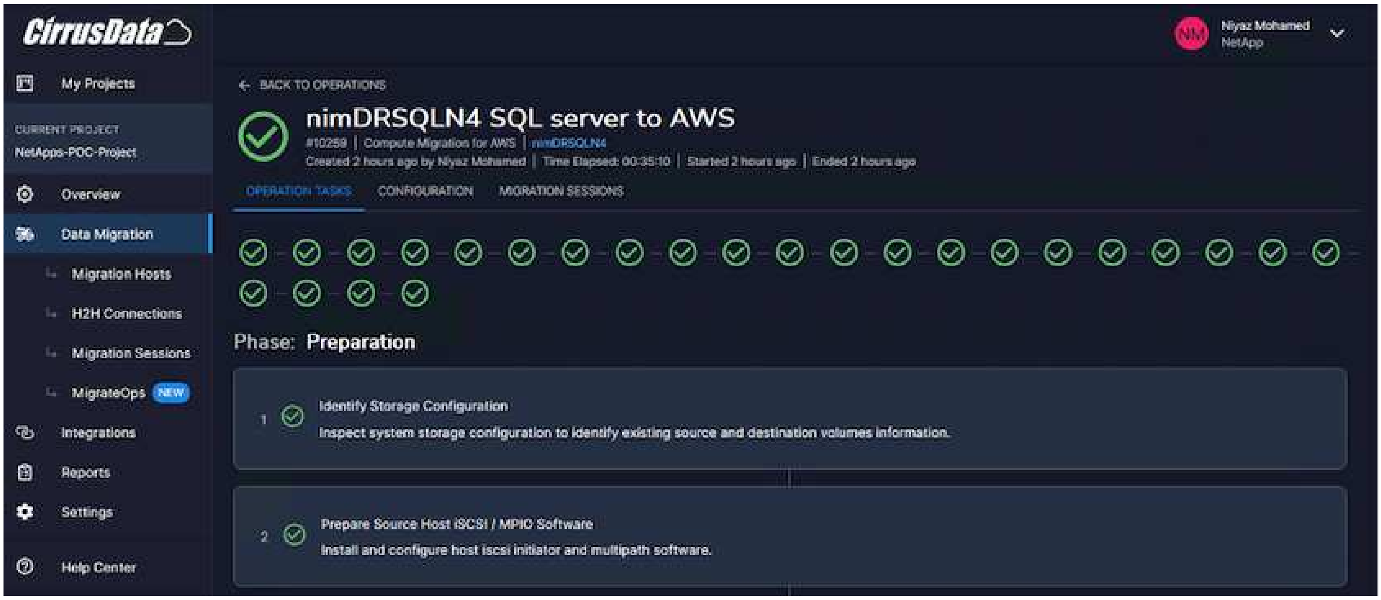
Note: The migrated Amazon EC2 instances can be accessed using the credentials that were used on the on-premises side.

Migrate VMs to Amazon EC2 using FSxN: Other Possibilities and Conclusion

This article highlight other possibilities for this migration solution as well as concluding the topic.

Other possibilities

The same approach can be extended to migrate VMs using in-guest storage on on-premises VMs. The OS VMDK can be migrated using CMC and the in-guest iSCSI LUNs can be replicated using SnapMirror. The process requires breaking the mirror and attaching the LUN to the newly migrated Amazon EC2 instance, as depicted in the diagram below.



nimDRSQLN4 SQL server to AWS

#10259 | Compute Migration for AWS | nimDRSQLN4

Created 2 hours ago by Niyaz Mohamed | Time Elapsed: 00:35:10 | Started 2 hours ago | Ended 2 hours ago

Phase: Preparation

1 ✓ Identify Storage Configuration
Inspect system storage configuration to identify existing source and destination volumes information.

2 ✓ Prepare Source Host iSCSI / MPIO Software
Install and configure host iscsi initiator and multipath software.

Conclusion

This document has provided a complete walkthrough of using the MigrateOps feature of CMC to migrate data stored in on-premises VMware repositories to AWS using Amazon EC2 instances and FSx for ONTAP.

The following video demonstrates the migration process from start to finish:

Migrate VMware VMs to Amazon EC2

To check out the GUI and basic Amazon EBS to FSx for ONTAP local migration, please watch this five-minute demo video:

Migrating to any storage in scale with Cirrus Migrate Cloud

NetApp Hybrid Multicloud with VMware Solutions

VMware Hybrid Multicloud Use Cases

Use Cases for NetApp Hybrid Multicloud with VMware

An overview of the use cases of importance to IT organization when planning hybrid-cloud or cloud-first deployments.

Popular Use Cases

Use cases include:

- Disaster recovery,
- Hosting workloads during data center maintenance, * quick burst in which additional resources are required beyond what’s provisioned in the local data center,
- VMware site expansion,
- Fast migration to the cloud,
- Dev/test, and
- Modernization of apps leveraging cloud supplemental technologies.

Throughout this documentation, cloud workload references will be detailed using the VMware use-cases. These use-cases are:

- Protect (includes both Disaster Recovery and Backup / Restore)
- Migrate
- Extend

Inside the IT Journey

Most organizations are on a journey to transformation and modernization. As part of this process, companies are trying use their existing VMware investments while leveraging cloud benefits and exploring ways to make the migration process as seamless as possible. This approach would make their modernization efforts very easy because the data is already in the cloud.

The easiest answer to this scenario is VMware offerings in each hyperscaler. Like NetApp® Cloud Volumes, VMware provides a way to move or extend on-premises VMware environments to any cloud, allowing you to retain existing on-premises assets, skills, and tools while running workloads natively in the cloud. This reduces risk because there will be no service breaks or a need for IP changes and provides the IT team the ability to operate the way they do on-premises using existing skills and tools. This can lead to accelerated cloud migrations and a much smoother transition to a hybrid Multicloud architecture.

Understanding the Importance of Supplemental NFS Storage Options

While VMware in any cloud delivers unique hybrid capabilities to every customer, limited supplemental NFS storage options have restricted its usefulness for organizations with storage-heavy workloads. Because storage is directly tied to hosts, the only way to scale storage is to add more hosts—and that can increase costs by 35–40 percent or more for storage intensive workloads. These workloads just need additional storage, not additional horsepower. But that means paying for additional hosts.

Let’s consider this scenario:

A customer requires just five hosts for CPU and memory, but has a lot of storage needs, and needs 12 hosts to meet the storage requirement. This requirement ends up really tipping the financial scale by having to buy the additional horsepower, when they only need to increment the storage.

When you’re planning cloud adoption and migrations, it’s always important to evaluate the best approach and take the easiest path that reduces total investments. The most common and easiest approach for any application migration is rehosting (also known as lift and shift) where there is no virtual machine (VM) or data conversion. Using NetApp Cloud Volumes with VMware software-defined data center (SDDC), while complementing vSAN, provides an easy lift-and-shift option.

Introduction to automation for ONTAP and vSphere

This page describes the benefits of automating base ONTAP functionality in a VMware vSphere environment.

VMware automation

Automation has been an integral part of managing VMware environments since the first days of VMware ESX. The ability to deploy infrastructure as code and extend practices to private cloud operations helps to alleviate concerns surrounding scale, flexibility, self-provisioning, and efficiency.

Automation can be organized into the following categories:

- **Virtual infrastructure deployment**

- **Guest machine operations**
- **Cloud operations**

There are many options available to administrators with respect to automating their infrastructure. Whether through using native vSphere features such as Host Profiles or Customization Specifications for virtual machines to available APIs on the VMware software components, operating systems, and NetApp storage systems; there is significant documentation and guidance available.

Data ONTAP 8.0.1 and later supports certain VMware vSphere APIs for Array Integration (VAAI) features when the ESX host is running ESX 4.1 or later. VAAI is a set of APIs that enable communication between VMware vSphere ESXi hosts and storage devices. These features help offload operations from the ESX host to the storage system and increase network throughput. The ESX host enables the features automatically in the correct environment. You can determine the extent to which your system is using VAAI features by checking the statistics contained in the VAAI counters.

The most common starting point for automating the deployment of a VMware environment is provisioning block or file-based datastores. It is important to map out the requirements of the actual tasks prior to developing the corresponding automation.

For more information concerning the automation of VMware environments, see the following resources:

- The NetApp Pub. NetApp configuration management and automation.
- The Ansible Galaxy Community for VMware. A collection of Ansible resources for VMware.
- VMware {code} Resources. Resources needed to design solutions for the software-defined data center, including forums, design standards, sample code, and developer tools.

vSphere traditional block storage provisioning with ONTAP

VMware vSphere supports the following VMFS datastore options with ONTAP SAN protocol support indicated.

VMFS datastore options	ONTAP SAN protocol support
Fibre Channel (FC)	yes
Fibre Channel over Ethernet (FCoE)	yes
iSCSI	yes
iSCSI Extensions for RDMA (iSER)	no
NVMe over Fabric with FC (NVMe/FC)	yes
NVMe over Fabric with RDMA over Converged Ethernet (NVMe/RoCE)	no

If iSER or NVMe/RoCE VMFS is required, check SANtricity-based storage systems.

vSphere VMFS datastore - Fibre Channel storage backend with ONTAP

This section covers the creation of a VMFS datastore with ONTAP Fibre Channel (FC) storage.

What you need

- The basic skills necessary to manage a vSphere environment and ONTAP
- An ONTAP storage system (FAS/AFF/CVO/ONTAP Select/ASA) running {ontap_version}
- ONTAP credentials (SVM name, userID, and password)
- ONTAP WWPN of host, target, and SVM and LUN information
- The completed FC configuration worksheet
- vCenter Server credentials
- vSphere host(s) information
    - {vsphere_version}
- Fabric switch(es)
    - With connected ONTAP FC data ports and vSphere hosts
    - With the N_port ID virtualization (NPIV) feature enabled
    - Create a single initiator single target zone.
        - Create one zone for each initiator (single initiator zone).
        - For each zone, include a target that is the ONTAP FC logical interface (WWPN) for the SVMs. There should be at least two logical interfaces per node per SVM. Do not use the WWPN of the physical ports.
- An ONTAP Tool for VMware vSphere deployed, configured, and ready to consume.

Provisioning a VMFS datastore

To provision a VMFS datastore, complete the following steps:

1. Check compatability with the Interoperability Matrix Tool (IMT)
2. Verify that the FCP Configuration is supported.

ONTAP tasks

1. Verify that you have an ONTAP license for FCP.
    a. Use the `system license show` command to check that FCP is listed.
    b. Use `licen se add -license-code <license code>` to add the license.
2. Make sure that the FCP protocol is enabled on the SVM.
    a. Verify the FCP on an existing SVM.
    b. Configure the FCP on an existing SVM.
    c. Create s new SVM with the FCP.
3. Make sure that FCP logical interfaces are available on an SVM.
    a. Use `Network Interface show` to verify the FCP adapter.
    b. When an SVM is created with the GUI, logical interfaces are a part of that process.
    c. To rename network interfaces, use `Network Interface modify`.

4. Create and Map a LUN. Skip this step if you are using ONTAP tools for VMware vSphere.

VMware vSphere tasks

1. Verfiy that HBA drivers are installed. VMware supported HBAs have drivers deployed out of the box and should be visible in the Storage Adapter Information.
2. Provision a VMFS datastore with ONTAP Tools.

vSphere VMFS Datastore - Fibre Channel over Ethernet storage protocol with ONTAP

This section covers the creation of a VMFS datastore with the Fibre Channel over Ethernet (FCoE) transport protocol to ONTAP storage.

What you need

- The basic skills necessary to manage a vSphere environment and ONTAP
- An ONTAP storage system (FAS/AFF/CVO/ONTAP Select) running {ontap_version}
- ONTAP credentials (SVM name, userID, and password)
- A supported FCoE combination
- A completed configuration worksheet
- vCenter Server credentials
- vSphere host(s) information
  - {vsphere_version}
- Fabric switch(es)
  - With either ONTAP FC data ports or vSphere hosts connected
  - With the N_port ID virtualization (NPIV) feature enabled
  - Create a single initiator single target zone.
  - FC/FCoE zoning configured
- Network switch(es)
  - FCoE support
  - DCB support
  - Jumbo frames for FCoE
- ONTAP Tool for VMware vSphere deployed, configured, and ready to consume

Provision a VMFS datastore

- Check compatibility with the Interoperability Matrix Tool (IMT).
- Verify that the FCoE configuration is supported.

ONTAP tasks

1. Verify the ONTAP license for FCP.
   a. Use the `system license show` command to verify that the FCP is listed.
   b. Use `license add -license-code <license code>` to add a license.

2. Verify that the FCP protocol is enabled on the SVM.
    a. Verify the FCP on an existing SVM.
    b. Configure the FCP on an existing SVM.
    c. Create a new SVM with the FCP.
3. Verify that FCP logical interfaces are available on the SVM.
    a. Use `Network Interface show` to verify the FCP adapter.
    b. When the SVM is created with the GUI, logical interfaces are a part of that process.
    c. To rename the network interface, use `Network Interface modify`.
4. Create and map a LUN; skip this step if you are using ONTAP tools for VMware vSphere.

VMware vSphere tasks

1. Verify that HBA drivers are installed. VMware-supported HBAs have drivers deployed out of the box and should be visible in the storage adapter information.
2. Provision a VMFS datastore with ONTAP Tools.

vSphere VMFS Datastore - iSCSI Storage backend with ONTAP

This section covers the creation of a VMFS datastore with ONTAP iSCSI storage.

For automated provisioning, use the following script: Ansible Playbook.

What you need

- The basic skills necessary to manage a vSphere environment and ONTAP.
- An ONTAP storage system (FAS/AFF/CVO/ONTAP Select/ASA) running {ontap_version}
- ONTAP credentials (SVM name, userID, and password)
- ONTAP network port, SVM, and LUN information for iSCSI
- A completed iSCSI configuration worksheet
- vCenter Server credentials
- vSphere host(s) information
    - {vsphere_version}
- iSCSI VMKernel adapter IP information
- Network switch(es)
    - With ONTAP system network data ports and connected vSphere hosts
    - VLAN(s) configured for iSCSI
    - (Optional) link aggregation configured for ONTAP network data ports
- ONTAP Tool for VMware vSphere deployed, configured, and ready to consume

Steps

1. Check compatibility with the Interoperability Matrix Tool (IMT).
2. Verify that the iSCSI configuration is supported.

3. Complete the following ONTAP and vSphere tasks.

ONTAP tasks

1. Verify the ONTAP license for iSCSI.
    a. Use the `system license show` command to check if iSCSI is listed.
    b. Use `license add -license-code <license code>` to add the license.
2. Verify that the iSCSI protocol is enabled on the SVM.
3. Verify that iSCSI network logical interfaces are available on the SVM.

    ⓘ When an SVM is created using the GUI, iSCSI network interfaces are also created.

4. Use the `Network interface` command to view or make changes to the network interface.

    💡 Two iSCSI network interfaces per node are recommended.

5. Create an iSCSI network interface. You can use the default-data-blocks service policy.
6. Verify that the data-iscsi service is included in the service policy. You can use `network interface service-policy show` to verify.
7. Verify that jumbo frames are enabled.
8. Create and map the LUN. Skip this step if you are using ONTAP tools for VMware vSphere. Repeat this step for each LUN.

VMware vSphere tasks

1. Verify that at least one NIC is available for the iSCSI VLAN. Two NICs are preferred for better performance and fault tolerance.
2. Identify the number of physical NICs available on the vSphere host.
3. Configure the iSCSI initiator. A typical use case is a software iSCSI initiator.
4. Verify that the TCPIP stack for iSCSI is available.
5. Verify that iSCSI portgroups are available.
    - We typically use a single virtual switch with multiple uplink ports.
    - Use 1:1 adapter mapping.
6. Verify that iSCSI VMKernel adapters are enabled to match the number of NICs and that IPs are assigned.
7. Bind the iSCSI software adapter to the iSCSI VMKernel adapter(s).
8. Provision the VMFS datastore with ONTAP Tools. Repeat this step for all datastores.
9. Verify hardware acceleration support.

What's next?

After these the tasks are completed, the VMFS datastore is ready to consume for provisioning virtual machines.

Ansible Playbook

```

```

```
## Disclaimer: Sample script for reference purpose only.

- hosts: '{{ vsphere_host }}'
  name: Play for vSphere iSCSI Configuration
  connection: local
  gather_facts: false
  tasks:
    # Generate Session ID for vCenter
    - name: Generate a Session ID for vCenter
      uri:
        url: "https://{{ vcenter_hostname }}/rest/com/vmware/cis/session"
        validate_certs: false
        method: POST
        user: "{{ vcenter_username }}"
       password: "{{ vcenter_password }}"
        force_basic_auth: yes
        return_content: yes
      register: vclogin

    # Generate Session ID for ONTAP tools with vCenter
    - name: Generate a Session ID for ONTAP tools with vCenter
      uri:
        url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/security/user/login"
        validate_certs: false
        method: POST
        return_content: yes
        body_format: json
        body:
          vcenterUserName: "{{ vcenter_username }}"
          vcenterPassword: "{{ vcenter_password }}"
      register: login

    # Get existing registered ONTAP Cluster info with ONTAP tools
    - name: Get ONTAP Cluster info from ONTAP tools
      uri:
        url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters"
        validate_certs: false
        method: Get
        return_content: yes
        headers:
          vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
      register: clusterinfo

    - name: Get ONTAP Cluster ID
```

```
      set_fact:
        ontap_cluster_id: "{{ clusterinfo.json |
json_query(clusteridquery) }}"
      vars:
        clusteridquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='Cluster'].id | [0]"

    - name: Get ONTAP SVM ID
      set_fact:
        ontap_svm_id: "{{ clusterinfo.json | json_query(svmidquery) }}"
      vars:
        svmidquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='SVM' && name == '{{ svm_name }}'].id | [0]"

    - name: Get Aggregate detail
      uri:
        url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters/{{ ontap_svm_id }}/aggregates"
        validate_certs: false
        method: GET
        return_content: yes
        headers:
          vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
          cluster-id: "{{ ontap_svm_id }}"
      when: ontap_svm_id != ''
      register: aggrinfo

    - name: Select Aggregate with max free capacity
      set_fact:
        aggr_name: "{{ aggrinfo.json | json_query(aggrquery) }}"
      vars:
        aggrquery: "max_by(records, &freeCapacity).name"

    - name: Convert datastore size in MB
      set_fact:
        datastoreSizeInMB: "{{ iscsi_datastore_size |
human_to_bytes/1024/1024 | int }}"

    - name: Get vSphere Cluster Info
      uri:
        url: "https://{{ vcenter_hostname }}/api/vcenter/cluster?names={{
vsphere_cluster }}"
        validate_certs: false
        method: GET
        return_content: yes
        body_format: json
        headers:
          vmware-api-session-id: "{{ vclogin.json.value }}"
      when: vsphere_cluster != ''
      register: vcenterclusterid

    - name: Create iSCSI VMFS-6 Datastore with ONTAP tools
      uri:
        url: "https://{{ ontap_tools_ip
}}:8143/api/rest/3.0/admin/datastore"
        validate_certs: false
        method: POST
        return_content: yes
        status_code: [200]
        body_format: json
        body:
          traditionalDatastoreRequest:
            name: "{{ iscsi_datastore_name }}"
            datastoreType: VMFS
            protocol: ISCSI
            spaceReserve: Thin
            clusterID:  "{{ ontap_cluster_id }}"
            svmID: "{{ ontap_svm_id }}"
            targetMoref: ClusterComputeResource:{{
vcenterclusterid.json[0].cluster }}
            datastoreSizeInMB: "{{ datastoreSizeInMB | int }}"
            vmfsFileSystem: VMFS6
            aggrName: "{{ aggr_name }}"
            existingFlexVolName: ""
            volumeStyle: FLEXVOL
            datastoreClusterMoref: ""
        headers:
          vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
      when: ontap_cluster_id != '' and ontap_svm_id != '' and aggr_name !=
''
      register: result
      changed_when: result.status == 200
```

vSphere VMFS Datastore - NVMe/FC with ONTAP

This section covers the creation of a VMFS datastore with ONTAP storage using NVMe/FC.

What you need

- Basic skills needed to manage a vSphere environment and ONTAP.
- Basic understanding of NVMe/FC.

- An ONTAP Storage System (FAS/AFF/CVO/ONTAP Select/ASA) running {ontap_version}
- ONTAP credentials (SVM name, userID, and password)
- ONTAP WWPN for host, target, and SVMs and LUN information
- A completed FC configuration worksheet
- vCenter Server
- vSphere host(s) information ({vsphere_version})
- Fabric switch(es)
  - With ONTAP FC data ports and vSphere hosts connected.
  - With the N_port ID virtualization (NPIV) feature enabled.
  - Create a single initiator target zone.
  - Create one zone for each initiator (single initiator zone).
  - For each zone, include a target that is the ONTAP FC logical interface (WWPN) for the SVMs. There should be at least two logical interfaces per node per SVM. DO not use the WWPN of physical ports.

Provision VMFS datastore

1. Check compatibility with the Interoperability Matrix Tool (IMT).
2. Verify that the NVMe/FC configuration is supported.

ONTAP tasks

1. Verify the ONTAP license for FCP.
   Use the `system license show` command and check if NVMe_oF is listed.
   Use `license add -license-code <license code>` to add a license.
2. Verify that NVMe protocol is enabled on the SVM.
   a. Configure SVMs for NVMe.
3. Verify that NVMe/FC Logical Interfaces are available on the SVMs.
   a. Use `Network Interface show` to verify the FCP adapter.
   b. When an SVM is created with the GUI, logical interfaces are as part of that process.
   c. To rename the network interface, use the command `Network Interface modify`.
4. Create NVMe namespace and subsystem

VMware vSphere Tasks

1. Verify that HBA drivers are installed. VMware supported HBAs have the drivers deployed out of the box and should be visible at Storage Adapter Information
2. Perform vSphere Host NVMe driver installatioln and validation tasks
3. Create VMFS Datastore

vSphere traditional file storage provisioning with ONTAP

VMware vSphere supports following NFS protocols, both of which support ONTAP.

- NFS Version 3

- NFS Version 4.1

If you need help selecting the correct NFS version for vSphere, check this comparison of NFS client versions.

Reference

vSphere datastore and protocol features: NFS

vSphere NFS datastore - Version 3 with ONTAP

Creation of NFS version 3 datastore with ONTAP NAS storage.

What you need

- The basic skill necessary to manage a vSphere environment and ONTAP.
- An ONTAP storage system (FAS/AFF/CVO/ONTAP Select/Cloud Volume Service/Azure NetApp Files) running {ontap_version}
- ONTAP credentials (SVM name, userID, password)
- ONTAP network port, SVM, and LUN information for NFS
  - A completed NFS configuration worksheet
- vCenter Server credentials
- vSphere host(s) information for {vsphere_version}
- NFS VMKernel adapter IP information
- Network switch(es)
  - with ONTAP system network data ports and connected vSphere hosts
  - VLAN(s) configured for NFS
  - (Optional) link aggregation configured for ONTAP network data ports
- ONTAP Tool for VMware vSphere deployed, configured, and ready to consume

Steps

- Check compatibility with the Interoperability Matrix Tool (IMT)
  - Verify that the NFS configuration is supported.
- Complete the following ONTAP and vSphere tasks.

ONTAP tasks

1. Verify the ONTAP license for NFS.
   a. Use the `system license show` command and check that NFS is listed.
   b. Use `license add -license-code <license code>` to add a license.
2. Follow the NFS configuration workflow.

VMware vSphere Tasks

Follow the workflow for NFS client configuration for vSphere.

Reference

vSphere datastore and protocol features: NFS

What’s next?

After these tasks are completed, the NFS datastore is ready to consume for provisioning virtual machines.

vSphere NFS Datastore - Version 4.1 with ONTAP

This section describes the creation of an NFS version 4.1 datastore with ONTAP NAS storage.

What you need

- The basic skills necessary to manage a vSphere environment and ONTAP
- ONTAP Storage System (FAS/AFF/CVO/ONTAP Select/Cloud Volume Service/Azure NetApp Files) running {ontap_version}
- ONTAP credentials (SVM name, userID, password)
- ONTAP network port, SVM, and LUN information for NFS
- A completed NFS configuration worksheet
- vCenter Server credentials
- vSphere host(s) information {vsphere_version}
- NFS VMKernel adapter IP information
- Network switch(es)
  - with ONTAP system network data ports, vSphere hosts, and connected
  - VLAN(s) configured for NFS
  - (Optional) link aggregation configured for ONTAP network data ports
- ONTAP Tools for VMware vSphere deployed, configured, and ready to consume

Steps

- Check compatability with the Interoperability Matrix Tool (IMT).
  - Verify that the NFS configuration is supported.
- Complete the ONTAP and vSphere Tasks provided below.

ONTAP tasks

1. Verify ONTAP license for NFS
   a. Usethe `system license show` command to check whether NFS is listed.
   b. Use `license add -license-code <license code>` to add a license.
2. Follow the NFS configuration workflow

VMware vSphere tasks

Follow the NFS Client Configuration for vSphere workflow.

What’s next?

After these tasks are completed, the NFS datastore is ready to consume for provisioning virtual machines.

Virtual Desktops

Virtual Desktop Services (VDS)

TR-4861: Hybrid Cloud VDI with Virtual Desktop Service

Suresh Thoppay, NetApp

The NetApp Virtual Desktop Service (VDS) orchestrates Remote Desktop Services (RDS) in major public clouds as well as on private clouds. VDS supports Windows Virtual Desktop (WVD) on Microsoft Azure. VDS automates many tasks that must be performed after deployment of WVD or RDS, including setting up SMB file shares (for user profiles, shared data, and the user home drive), enabling Windows features, application and agent installation, firewall, and policies, and so on.

Users consume VDS for dedicated desktops, shared desktops, and remote applications. VDS provides scripted events for automating application management for desktops and reduces the number of images to manage.

VDS provides a single management portal for handling deployments across public and private cloud environments.

Customer Value

The remote workforce explosion of 2020 has changed requirements for business continuity. IT departments are faced with new challenges to rapidly provision virtual desktops and thus require provisioning agility, remote management, and the TCO advantages of a hybrid cloud that makes it easy to provision on-premises and cloud resources. They need a hybrid-cloud solution that:

- Addresses the post-COVID workspace reality to enable flexible work models with global dynamics
- Enables shift work by simplifying and accelerating the deployment of work environments for all employees, from task workers to power users
- Mobilizes your workforce by providing rich, secure VDI resources regardless of the physical location
- Simplifies hybrid-cloud deployment
- Automates and simplifies risk reduction management

Use Cases

Hybrid VDI with NetApp VDS allows service providers and enterprise virtual desktop administrators to easily expand resources to other cloud environment without affecting their users. Having on-premises resources provides better control of resources and offers wide selection of choices (compute, GPU, storage, and network) to meet demand.

This solution applies to the following use cases:

- Bursting into the cloud for surges in demand for remote desktops and applications
- Reducing TCO for long running remote desktops and applications by hosting them on-premises with flash storage and GPU resources
- Ease of management of remote desktops and applications across cloud environments
- Experience remote desktops and applications by using a software-as-a- service model with on-premises resources

Target Audience

The target audience for the solution includes the following groups:

- EUC/VDI architects who wants to understand the requirements for a hybrid VDS
- NetApp partners who would like to assist customers with their remote desktop and application needs
- Existing NetApp HCI customers who want to address remote desktop and application demands

NetApp Virtual Desktop Service Overview

NetApp offers many cloud services, including the rapid provisioning of virtual desktop with WVD or remote applications and rapid integration with Azure NetApp Files.

Traditionally, it takes weeks to provision and deliver remote desktop services to customers. Apart from provisioning, it can be difficult to manage applications, user profiles, shared data, and group policy objects to enforce policies. Firewall rules can increase complexity and require a separate skillset and tools.

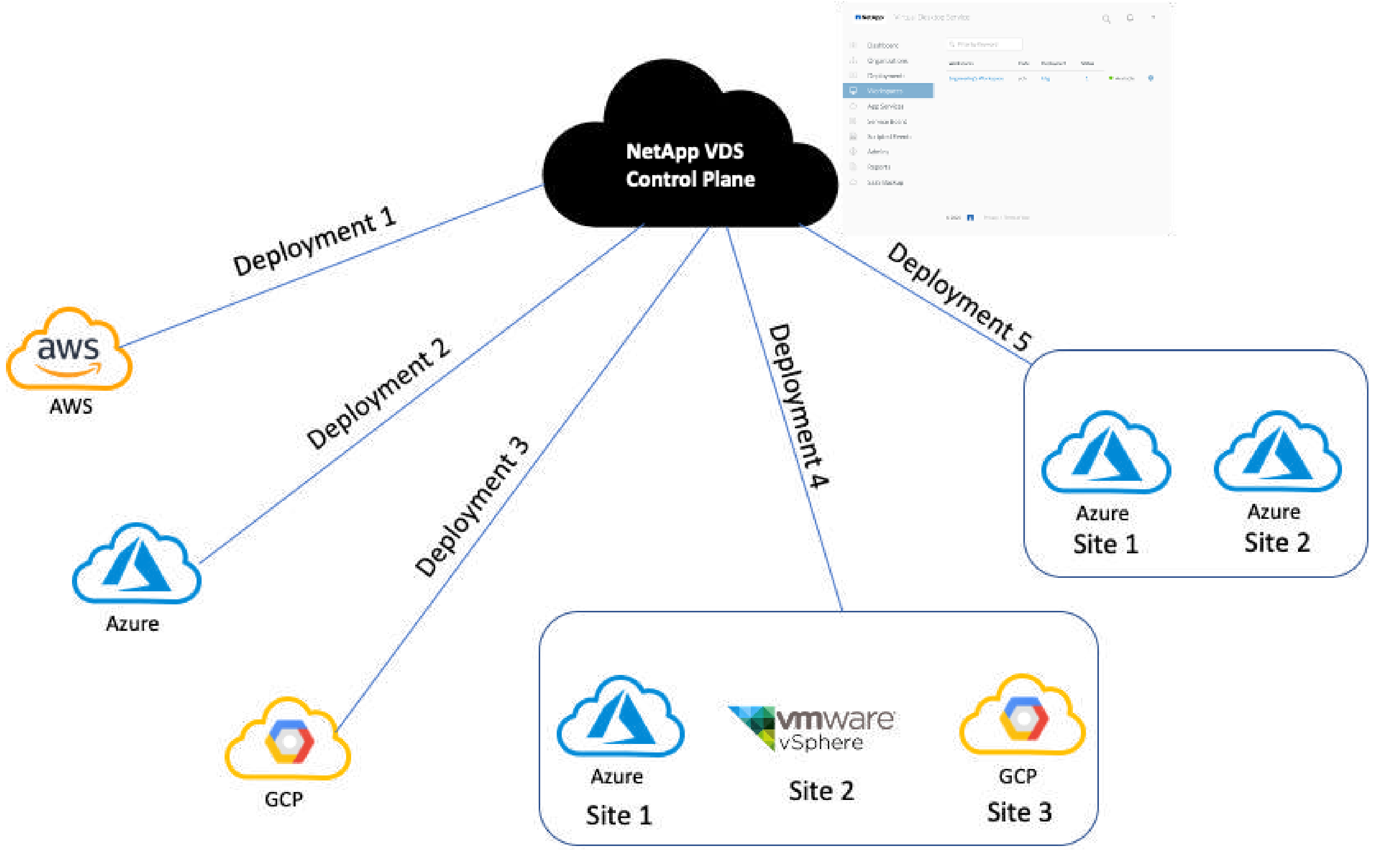
With Microsoft Azure Windows Virtual Desktop service, Microsoft takes care of maintenance for Remote Desktop Services components, allowing customers to focus on provisioning workspaces in the cloud. Customers must provision and manage the complete stack which requires special skills to manage VDI environments.

With NetApp VDS, customers can rapidly deploy virtual desktops without worrying about where to install the architecture components like brokers, gateways, agents, and so on. Customers who require complete control of their environment can work with a professional services team to achieve their goals. Customers consume VDS as a service and thus can focus on their key business challenges.

NetApp VDS is a software-as-a-service offering for centrally managing multiple deployments across AWS, Azure, GCP, or private cloud environments. Microsoft Windows Virtual Desktop is available only on Microsoft Azure. NetApp VDS orchestrates Microsoft Remote Desktop Services in other environments.

Microsoft offers multisession on Windows 10 exclusively for Windows Virtual Desktop environments on Azure. Authentication and identity are handled by the virtual desktop technology; WVD requires Azure Active Directory synced (with AD Connect) to Active Directory and session VMs joined to Active Directory. RDS requires Active Directory for user identity and authentication and VM domain join and management.

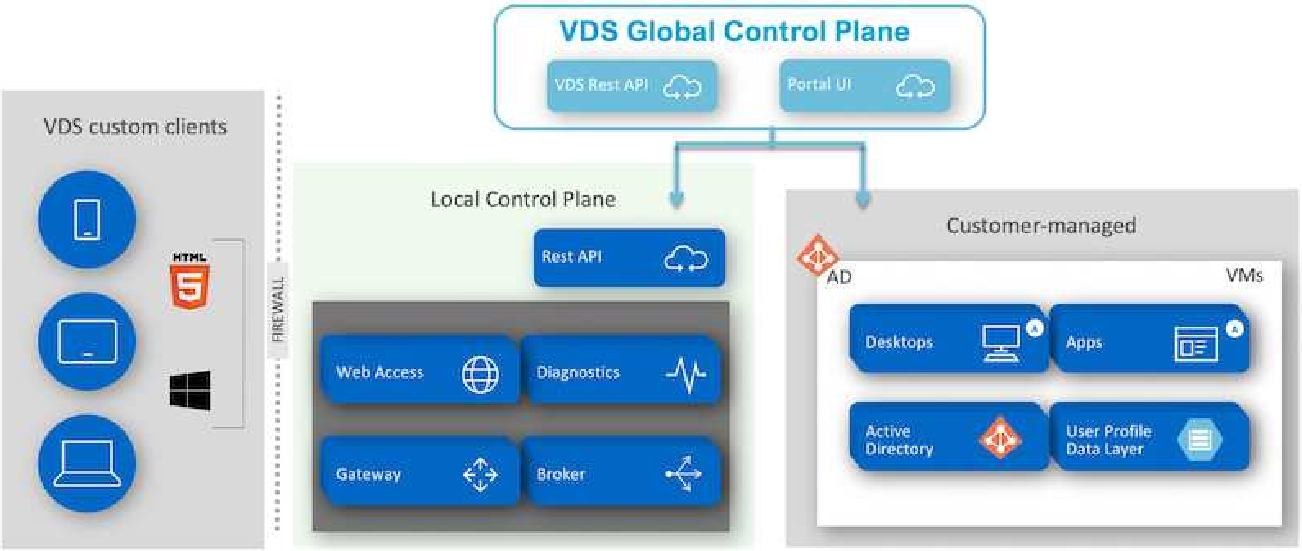
A sample deployment topology is shown in the following figure.



Each deployment is associated with an active directory domain and provides clients with an access entry point for workspaces and applications. A service provider or enterprise that has multiple active directory domains typically has more deployments. A single Active Directory domain that spans multiple regions typically has a single deployment with multiple sites.

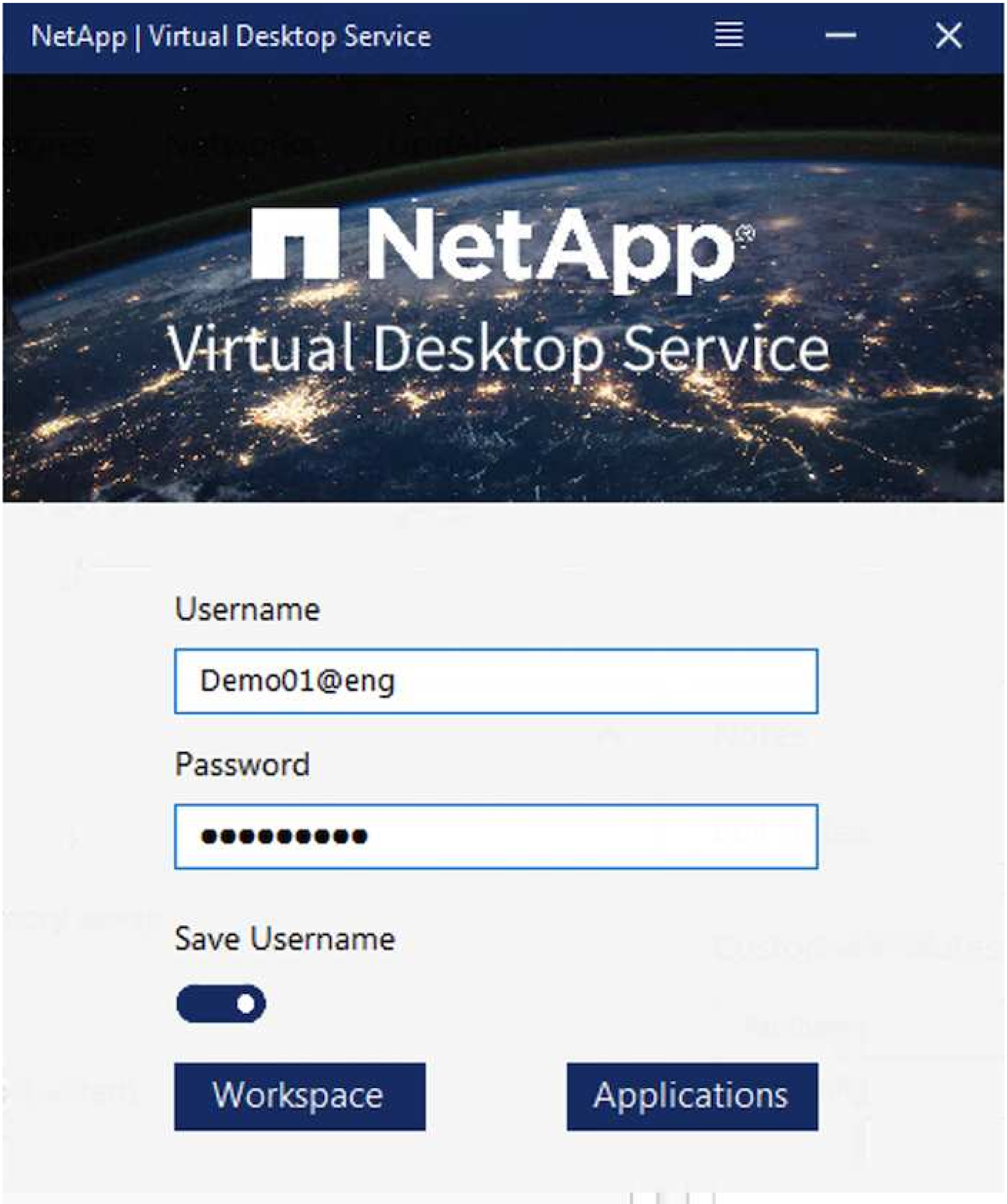
For WVD in Azure, Microsoft provides a platform-as-a-service that is consumed by NetApp VDS. For other environments, NetApp VDS orchestrates the deployment and configuration of Microsoft Remote Desktop Services. NetApp VDS supports both WVD Classic and WVD ARM and can also be used to upgrade existing versions.

Each deployment has its own platform services, which consists of Cloud Workspace Manager (REST API endpoint), an HTML 5 Gateway (connect to VMs from a VDS management portal), RDS Gateways (Access point for clients), and a Domain Controller. The following figure depicts the VDS Control Plane architecture for RDS implementation.



For RDS implementations, NetApp VDS can be readily accessed from Windows and browsers using client software that can be customized to include customer logo and images. Based on user credentials, it provides user access to approved workspaces and applications. There is no need to configure the gateway details.

The following figure shows the NetApp VDS client.



NetApp | Virtual Desktop Service

Username

Demo01@eng

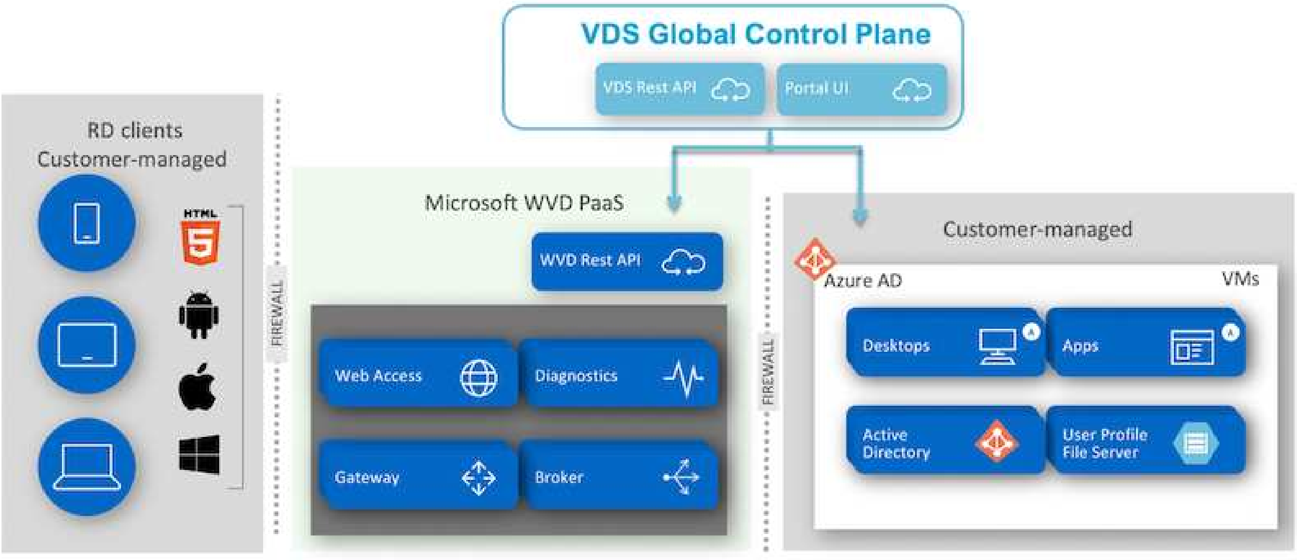
Password

●●●●●●●●●

Save Username

In the Azure WVD implementation, Microsoft handles the access entry point for the clients and can be consumed by a Microsoft WVD client available natively for various OSs. It can also be accessed from a web-based portal. The configuration of client software must be handled by the Group Policy Object (GPO) or in other ways preferred by customers.

The following figure depicts the VDS Control Plane architecture for Azure WVD implementations.



In addition to the deployment and configuration of required components, NetApp VDS also handles user management, application management, resource scaling, and optimization.

NetApp VDS can create users or grant existing user accounts access to cloud workspace or application services. The portal can also be used for password resets and the delegation of administrating a subset of components. Helpdesk administrators or Level-3 technicians can shadow user sessions for troubleshooting or connect to servers from within the portal.

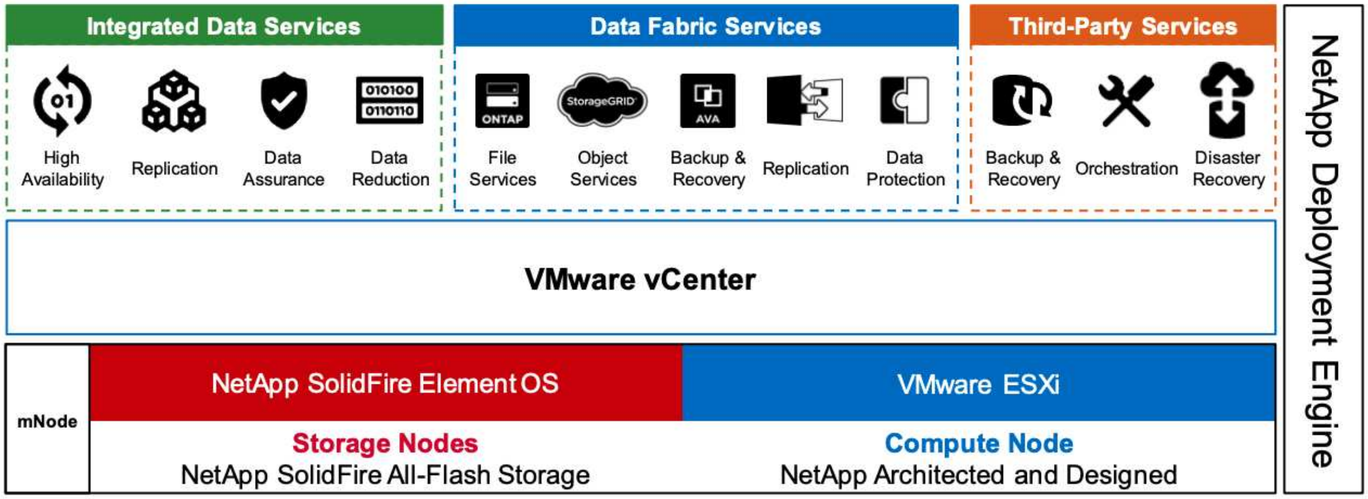
NetApp VDS can use image templates that you create, or it can use existing ones from the marketplace for cloud-based provisioning. To reduce the number of images to manage, you can use a base image, and any additional applications that you require can be provisioned using the provided framework to include any command-line tools like Chocolatey, MSIX app attach, PowerShell, and so on. Even custom scripts can be used as part of machine lifecycle events.

NetApp HCI Overview

NetApp HCI is a hybrid cloud infrastructure that consists of a mix of storage nodes and compute nodes. It is available as either a two-rack unit or single-rack unit, depending on the model. The installation and configuration required to deploy VMs are automated with the NetApp Deployment Engine (NDE). Compute clusters are managed with VMware vCenter, and storage clusters are managed with the vCenter Plug-in deployed with NDE. A management VM called the mNode is deployed as part of the NDE.

NetApp HCI handles the following functions:

- Version upgrades
- Pushing events to vCenter
- vCenter Plug-In management
- A VPN tunnel for support
- The NetApp Active IQ Digital Advisor (also known as Digital Advisor) collector
- The extension of NetApp Cloud Services to on the premises, enabling a hybrid cloud infrastructure. The following figure depicts HCI components.



Storage Nodes

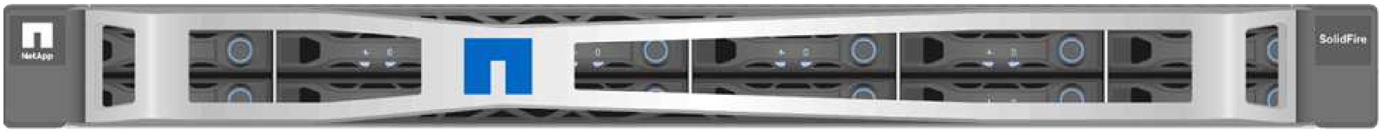
Storage nodes are available as either a half-width or full-width rack unit. A minimum of four storage nodes is required at first, and a cluster can expand to up to 40 nodes. A storage cluster can be shared across multiple compute clusters. All the storage nodes contain a cache controller to improve write performance. A single node provides either 50K or 100K IOPS at a 4K block size.

NetApp HCI storage nodes run NetApp Element software, which provides minimum, maximum, and burst QoS limits. The storage cluster supports a mix of storage nodes, although one storage node cannot exceed one-third of total capacity.

Compute Nodes

> ⓘ NetApp supports its storage connected to any compute servers listed in the VMware Compatability Guide.

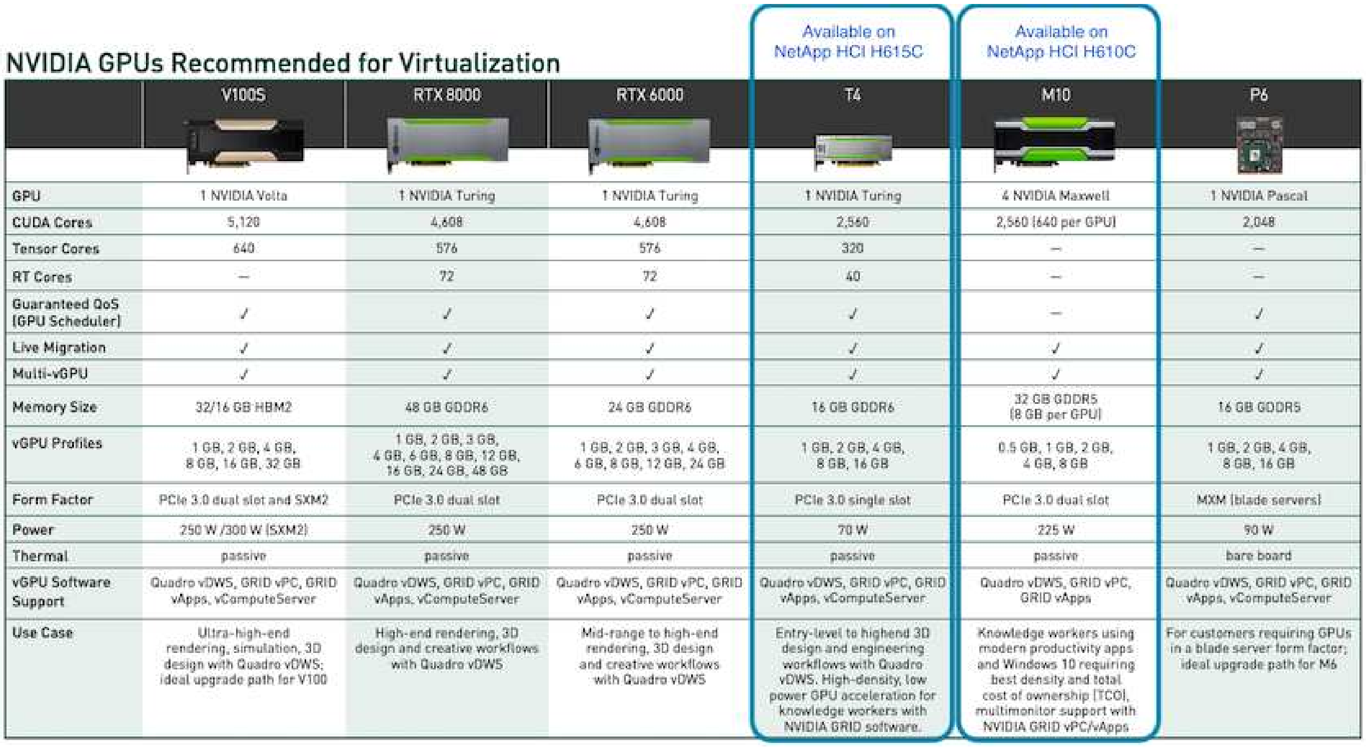
Compute nodes are available in half-width, full-width, and two rack-unit sizes. The NetApp HCI H410C and H610C are based on scalable Intel Skylake processors. The H615C is based on second-generation scalable Intel Cascade Lake processors. There are two compute models that contain GPUs: the H610C contains two NVIDIA M10 cards and the H615C contains three NVIDIA T4 cards.



The NVIDIA T4 has 40 RT cores that provide the computation power needed to deliver real-time ray tracing. The same server model used by designers and engineers can now also be used by artists to create photorealistic imagery that features light bouncing off surfaces just as it would in real life. This RTX-capable GPU produces real-time ray tracing performance of up to five Giga Rays per second. The NVIDIA T4, when combined with Quadro Virtual Data Center Workstation (Quadro vDWS) software, enables artists to create photorealistic designs with accurate shadows, reflections, and refractions on any device from any location.

Tensor cores enable you to run deep learning inferencing workloads. When running these workloads, an NVIDIA T4 powered with Quadro vDWS can perform up to 25 times faster than a VM driven by a CPU-only server. A NetApp H615C with three NVIDIA T4 cards in one rack unit is an ideal solution for graphics and compute-intensive workloads.

The following figure lists NVIDIA GPU cards and compares their features.



NVIDIA GPUs Recommended for Virtualization

				Available on NetApp HCI H615C	Available on NetApp HCI H610C	
	V100S	RTX 8000	RTX 6000	T4	M10	P6
GPU	1 NVIDIA Volta	1 NVIDIA Turing	1 NVIDIA Turing	1 NVIDIA Turing	4 NVIDIA Maxwell	1 NVIDIA Pascal
CUDA Cores	5,120	4,608	4,608	2,560	2,560 (640 per GPU)	2,048
Tensor Cores	640	576	576	320	—	—
RT Cores	—	72	72	40	—	—
Guaranteed QoS (GPU Scheduler)	✓	✓	✓	✓	—	✓
Live Migration	✓	✓	✓	✓	✓	✓
Multi-vGPU	✓	✓	✓	✓	✓	✓
Memory Size	32/16 GB HBM2	48 GB GDDR6	24 GB GDDR6	16 GB GDDR6	32 GB GDDR5 (8 GB per GPU)	16 GB GDDR5
vGPU Profiles	1 GB, 2 GB, 4 GB, 8 GB, 16 GB, 32 GB	1 GB, 2 GB, 3 GB, 4 GB, 6 GB, 8 GB, 12 GB, 16 GB, 24 GB, 48 GB	1 GB, 2 GB, 3 GB, 4 GB, 6 GB, 8 GB, 12 GB, 24 GB	1 GB, 2 GB, 4 GB, 8 GB, 16 GB	0.5 GB, 1 GB, 2 GB, 4 GB, 8 GB	1 GB, 2 GB, 4 GB, 8 GB, 16 GB
Form Factor	PCIe 3.0 dual slot and SXM2	PCIe 3.0 dual slot	PCIe 3.0 dual slot	PCIe 3.0 single slot	PCIe 3.0 dual slot	MXM (blade servers)
Power	250 W /300 W (SXM2)	250 W	250 W	70 W	225 W	90 W
Thermal	passive	passive	passive	passive	passive	bare board
vGPU Software Support	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer
Use Case	Ultra-high-end rendering, simulation, 3D design with Quadro vDWS; ideal upgrade path for V100	High-end rendering, 3D design and creative workflows with Quadro vDWS	Mid-range to high-end rendering, 3D design and creative workflows with Quadro vDWS	Entry-level to highend 3D design and engineering workflows with Quadro vDWS. High-density, low power GPU acceleration for knowledge workers with NVIDIA GRID software.	Knowledge workers using modern productivity apps and Windows 10 requiring best density and total cost of ownership (TCO), multimonitor support with NVIDIA GRID vPC/vApps	For customers requiring GPUs in a blade server form factor; ideal upgrade path for M6

The M10 GPU remains the best TCO solution for knowledge-worker use cases. However, the T4 makes a great alternative when IT wants to standardize on a GPU that can be used across multiple use cases, such as virtual workstations, graphics performance, real-time interactive rendering, and inferencing. With the T4, IT can take advantage of the same GPU resources to run mixed workloads—for example, running VDI during the day and repurposing the resources to run compute workloads at night.

The H610C compute node is two rack units in size; the H615C is one rack unit in size and consumes less power. The H615C supports H.264 and H.265 (High Efficiency Video Coding [HEVC]) 4:4:4 encoding and decoding. It also supports the increasingly mainstrean VP9 decoder; even the WebM container package served by YouTube uses the VP9 codec for video.

The number of nodes in a compute cluster is dictated by VMware; currently, it is 96 with VMware vSphere 7.0 Update 1. Mixing different models of compute nodes in a cluster is supported when Enhanced vMotion Compatibility (EVC) is enabled.

NVIDIA Licensing

When using an H610C or H615C, the license for the GPU must be procured from NVIDIA partners that are authorized to resell the licenses. You can find NVIDIA partners with the partner locator. Search for competencies such as virtual GPU (vGPU) or Tesla.

NVIDIA vGPU software is available in four editions:

- NVIDIA GRID Virtual PC (GRID vPC)
- NVIDIA GRID Virtual Applications (GRID vApps)
- NVIDIA Quadro Virtual Data Center Workstation (Quadro vDWS)
- NVIDIA Virtual ComputeServer (vComputeServer)

GRID Virtual PC

This product is ideal for users who want a virtual desktop that provides a great user experience for Microsoft Windows applications, browsers, high-definition video, and multi-monitor support. The NVIDIA GRID Virtual PC delivers a native experience in a virtual environment, allowing you to run all your PC applications at full performance.

GRID Virtual Applications

GRID vApps are for organizations deploying a Remote Desktop Session Host (RDSH) or other app-streaming or session-based solutions. Designed to deliver Microsoft Windows applications at full performance, Windows Server-hosted RDSH desktops are also supported by GRID vApps.

Quadro Virtual Data Center Workstation

This edition is ideal for mainstream and high-end designers who use powerful 3D content creation applications like Dassault CATIA, SOLIDWORKS, 3Dexcite, Siemens NX, PTC Creo, Schlumberger Petrel, or Autodesk Maya. NVIDIA Quadro vDWS allows users to access their professional graphics applications with full features and performance anywhere on any device.

NVIDIA Virtual ComputeServer

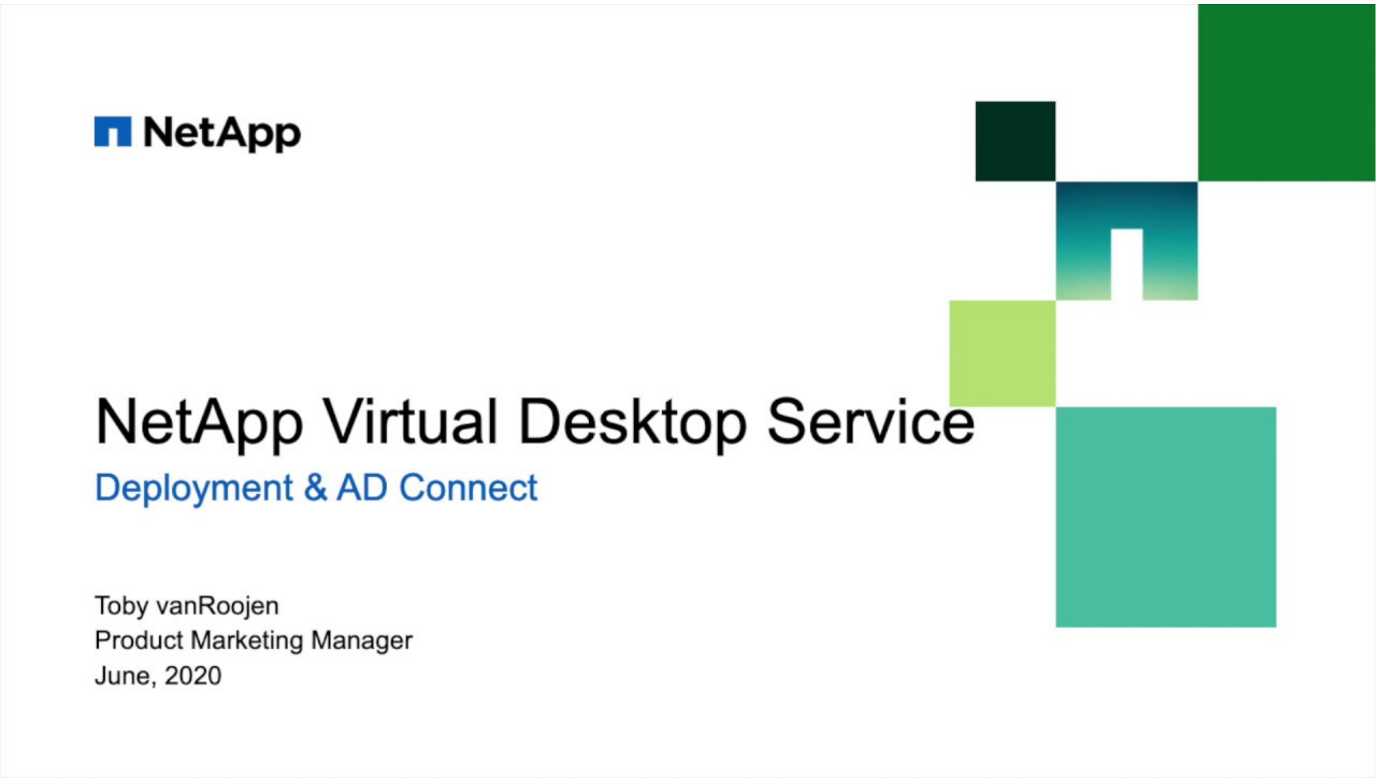
Many organizations run compute-intensive server workloads such as artificial intelligence (AI), deep learning (DL), and data science. For these use cases, NVIDIA vComputeServer software virtualizes the NVIDIA GPU, which accelerates compute-intensive server workloads with features such as error correction code, page retirement, peer-to-peer over NVLink, and multi-vGPU.

> A Quadro vDWS license enables you to use GRID vPC and NVIDIA vComputeServer.

Deployment

NetApp VDS can be deployed to Microsoft Azure using a setup app available based on the required codebase. The current release is available here and the preview release of the upcoming product is available here.

See this video for deployment instructions.



NetApp

NetApp Virtual Desktop Service

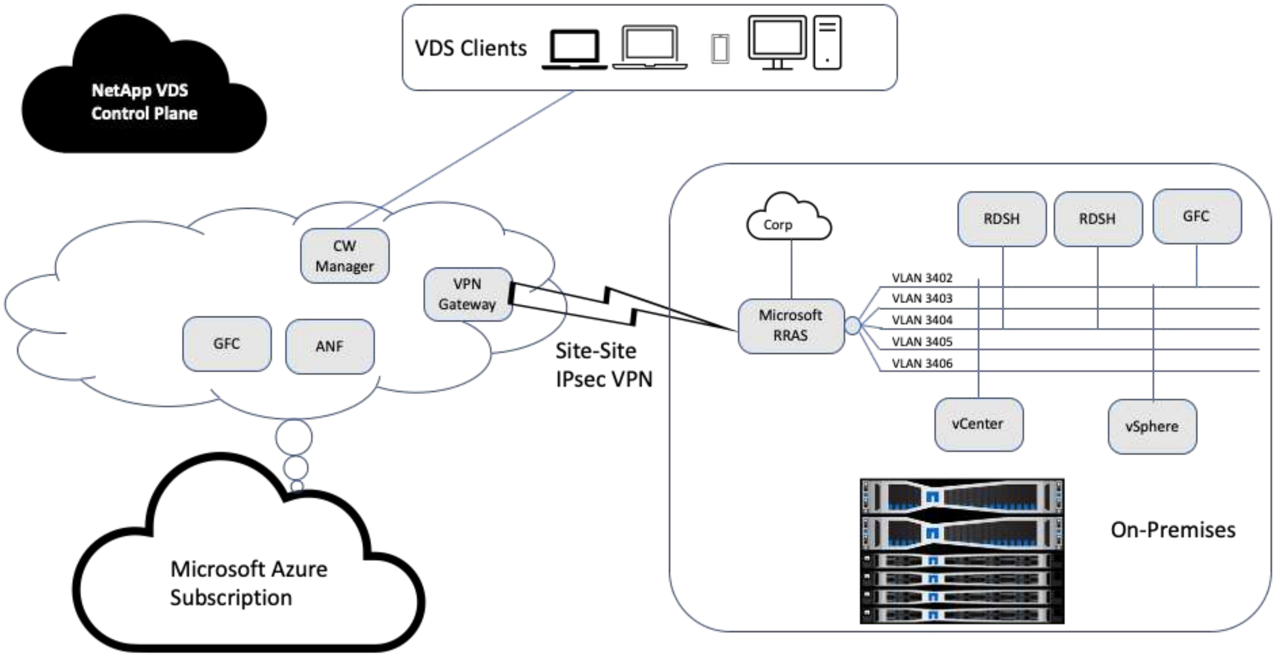
Deployment & AD Connect

Toby vanRoojen
Product Marketing Manager
June, 2020

Hybrid Cloud Environment

NetApp Virtual Desktop Service can be extended to on-premises when connectivity exists between on-premises resources and cloud resources. Enterprises can establish the link to Microsoft Azure using Express Route or a site-to-site IPsec VPN connection. You can also create links to other clouds in a similar way either using a dedicated link or with an IPsec VPN tunnel.

For the solution validation, we used the environment depicted in the following figure.



On-premises, we had multiple VLANs for management, remote-desktop-session hosts, and so on. They were on the 172.21.146-150.0/24 subnet and routed to the corporate network using the Microsoft Remote Routing Access Service. We also performed the following tasks:

1. We noted the public IP of the Microsoft Routing and Remote Access Server (RRAS; identified with IPchicken.com).
2. We created a Virtual Network Gateway resource (route-based VPN) on Azure Subscription.
3. We created the connection providing the local network gateway address for the public IP of the Microsoft RRAS server.
4. We completed VPN configuration on RRAS to create a virtual interface using pre-shared authentication that was provided while creating the VPN gateway. If configured correctly, the VPN should be in the connected state. Instead of Microsoft RRAS, you can also use pfSense or other relevant tools to create the site-to-site IPsec VPN tunnel. Since it is route-based, the tunnel redirects traffic based on the specific subnets configured.

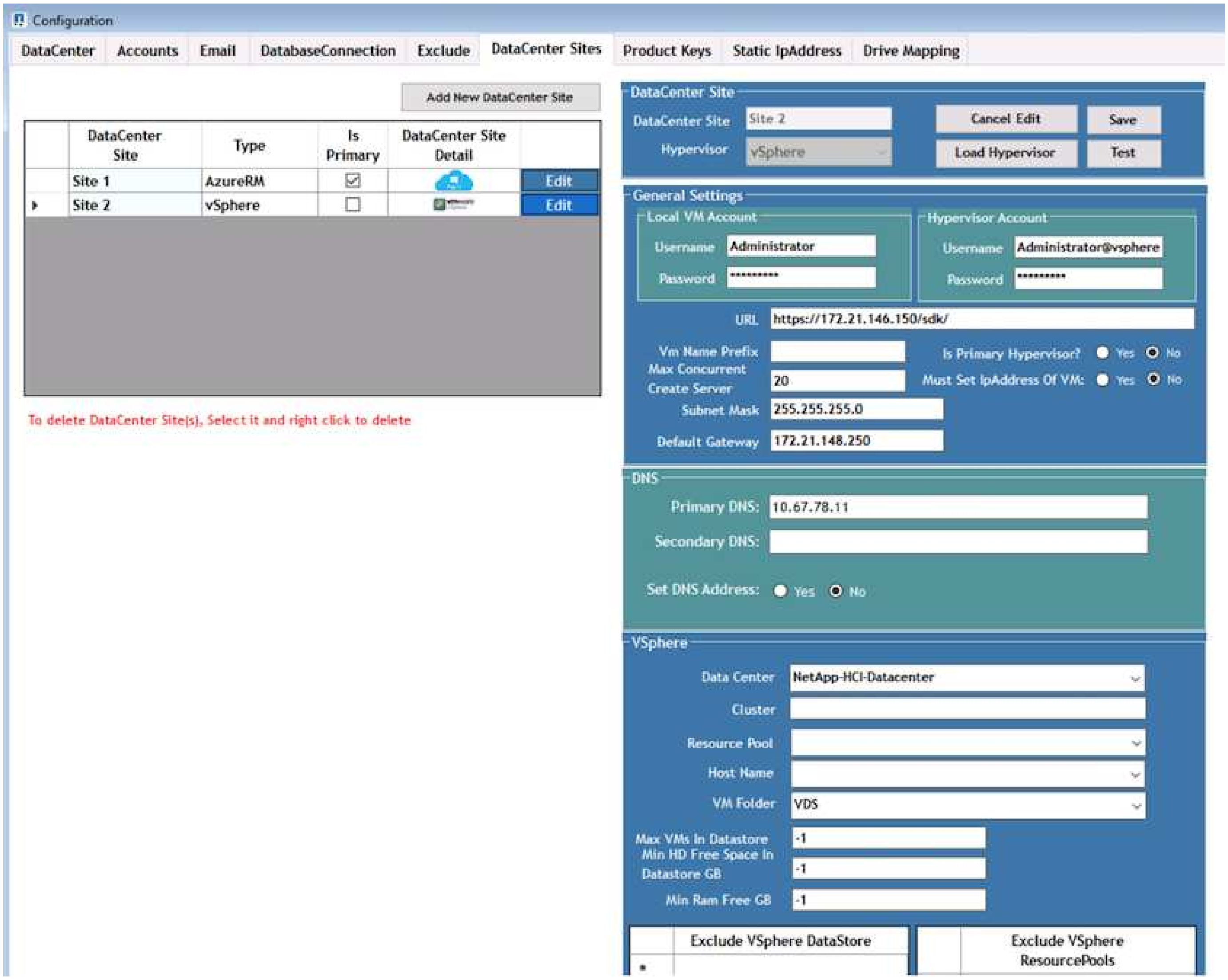
Microsoft Azure Active Directory provides identity authentication based on oAuth. Enterprise client authentications typically require NTLM or Kerberos-based authentication. Microsoft Azure Active Directory Domain Services perform password hash sync between Azure Active Directory and on-prem domain controllers using ADConnect.

For this Hybrid VDS solution validation, we initially deployed to Microsoft Azure and added an additional site with vSphere. The advantage with this approach is that platform services were deployed to Microsoft Azure and were then readily backed up using the portal. Services can then be easily accessed from anywhere, even if the site-site VPN link is down.

To add another site, we used a tool called DCConfig. The shortcut to that application is available on the desktop of the cloud workspace manager (CWMgr) VM. After this application is launched, navigate to the DataCenter Sites tab, add the new datacenter site, and fill in the required info as shown below. The URL points to the vCenter IP. Make sure that the CWMgr VM can communicate with vCenter before adding the configuration.

Make sure that vSphere PowerCLI 5.1 on CloudWorkspace manager is installed to enable communication with VMware vSphere environment.

The following figure depicts on- premises datacenter site configuration.



	DataCenter Site	Type	Is Primary	DataCenter Site Detail	
	Site 1	AzureRM	☑		Edit
▸	Site 2	vSphere	□		Edit

To delete DataCenter Site(s), Select it and right click to delete

DataCenter Site

DataCenter Site: Site 2
Hypervisor: vSphere

General Settings

Local VM Account
Username: Administrator
Password: *********

Hypervisor Account
Username: Administrator@vsphere
Password: *********

URL: https://172.21.146.150/sdk/
Vm Name Prefix:
Is Primary Hypervisor? ○ Yes ● No
Max Concurrent Create Server: 20
Must Set IpAddress Of VM: ○ Yes ● No
Subnet Mask: 255.255.255.0
Default Gateway: 172.21.148.250

DNS

Primary DNS: 10.67.78.11
Secondary DNS:
Set DNS Address: ○ Yes ● No

VSphere

Data Center: NetApp-HCI-Datacenter
Cluster:
Resource Pool:
Host Name:
VM Folder: VDS
Max VMs In Datastore: -1
Min HD Free Space In Datastore GB: -1
Min Ram Free GB: -1

	Exclude VSphere DataStore
*	

	Exclude VSphere ResourcePools

Note that there are filtering options available for compute resource based on the specific cluster, host name, or free RAM space. Filtering options for storage resource includes the minimum free space on datastores or the maximum VMs per datastore. Datastores can be excluded using regular expressions. Click Save button to save the configuration.

To validate the configuration, click the Test button or click Load Hypervisor and check any dropdown under the vSphere section. It should be populated with appropriate values. It is a best practice to keep the primary hypervisor set to yes for the default provisioning site.

The VM templates created on VMware vSphere are consumed as provisioning collections on VDS. Provisioning collections come in two forms: shared and VDI. The shared provisioning collection type is used for remote desktop services for which a single resource policy is applied to all servers. The VDI type is used for WVD instances for which the resource policy is individually assigned. The servers in a provisioning collection can be assigned one of the following three roles:

- **TSDATA.** Combination of Terminal Services and Data server role.
- **TS.** Terminal Services (Session Host).
- **DATA.** File Server or Database Server. When you define the server role, you must pick the VM template and storage (datastore). The datastore chosen can be restricted to a specific datastore or you can use the least-used option in which the datastore is chosen based on data usage.

Each deployment has VM resource defaults for the cloud resource allocation based on Active Users, Fixed, Server Load, or User Count.

Single server load test with Login VSI

The NetApp Virtual Desktop Service uses the Microsoft Remote Desktop Protocol to access virtual desktop sessions and applications, and the Login VSI tool determines the maximum number of users that can be hosted on a specific server model. Login VSI simulates user login at specific intervals and performs user operations like opening documents, reading and composing mails, working with Excel and PowerPoint, printing documents, compressing files, and taking random breaks. It then measures response times. User response time is low when server utilization is low and increases when more user sessions are added. Login VSI determines the baseline based on initial user login sessions and it reports the maximum user session when the user response exceeds 2 seconds from the baseline.

NetApp Virtual Desktop Service utilizes Microsoft Remote Desktop Protocol to access the Virtual Desktop session and Applications. To determine the maximum number of users that can be hosted on a specific server model, we used the Login VSI tool. Login VSI simulates user login at specific intervals and performs user operations like opening documents, reading and composing mails, working with Excel and PowerPoint, printing documents, compressing files, taking random breaks, and so on. It also measures response times. User response time is low when server utilization is low and increases when more user sessions are added. Login VSI determines the baseline based on the initial user login sessions and it reports maximum user sessions when the user response exceeds 2sec from the baseline.

The following table contains the hardware used for this validation.

Model	Count	Description
NetApp HCI H610C	4	Three in a cluster for launchers, AD, DHCP, and so on. One server for load testing.
NetApp HCI H615C	1	2x24C Intel Xeon Gold 6282 @2.1GHz. 1.5TB RAM.

The following table contains the software used for this validation.

Product	Description
NetApp VDS 5.4	Orchestration
VM Template Windows 2019 1809	Server OS for RDSH
Login VSI	4.1.32.1
VMware vSphere 6.7 Update 3	Hypervisor

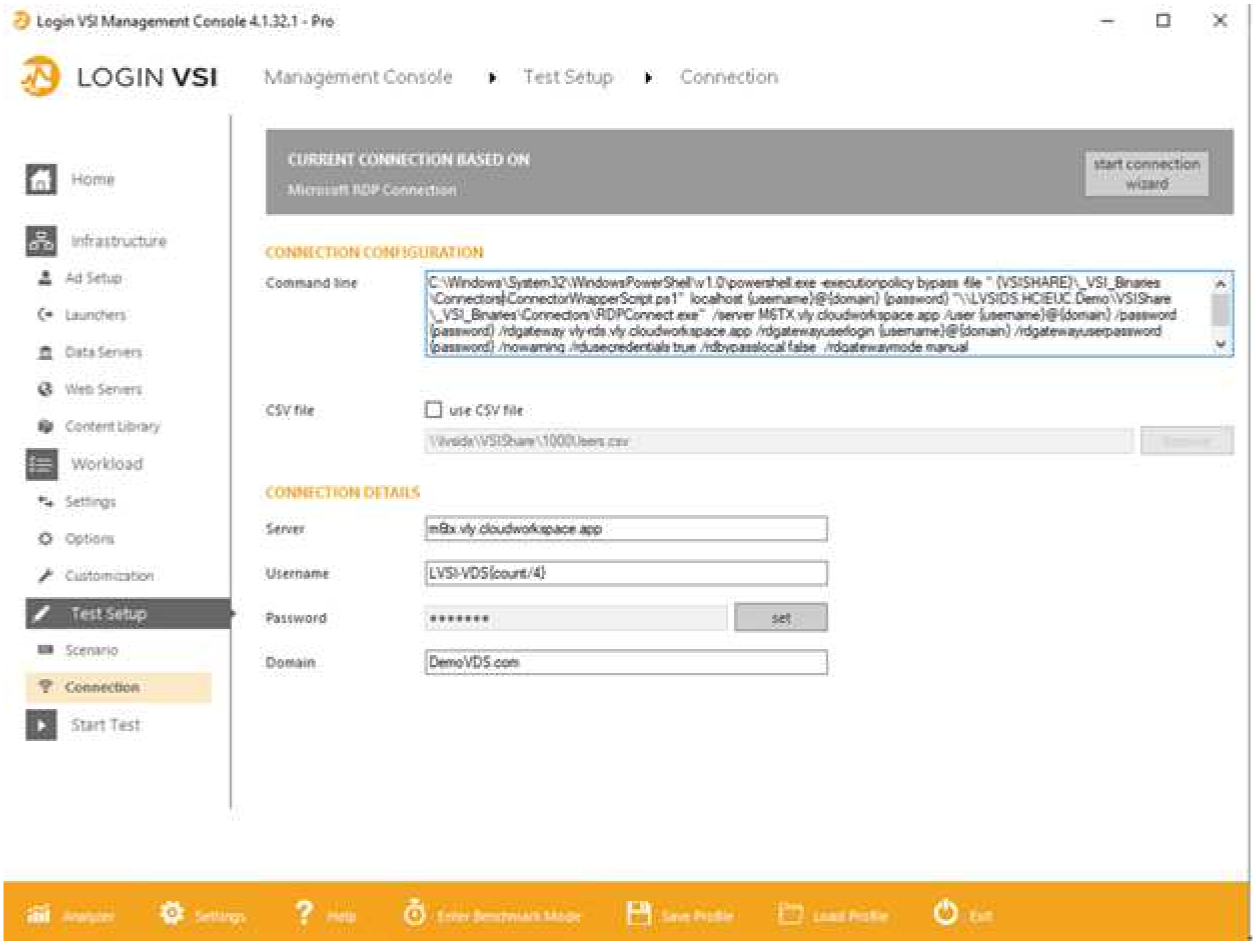
Product	Description
VMware vCenter 6.7 Update 3f	VMware management tool

The Login VSI test results are as follows:

Model	VM configuration	Login VSI baseline	Login VSI Max
H610C	8 vCPU, 48GB RAM, 75GB disk, 8Q vGPU profile	799	178
H615C	12 vCPU, 128GB RAM, 75GB disk	763	272

Considering sub-NUMA boundaries and hyperthreading, the eight VMs chosen for VM testing and configuration depended on the cores available on the host.

We used 10 launcher VMs on the H610C, which used the RDP protocol to connect to the user session. The following figure depicts the Login VSI connection information.



Login VSI Management Console 4.1.32.1 - Pro

CURRENT CONNECTION BASED ON

Microsoft RDP Connection

CONNECTION CONFIGURATION

Command line

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -executionpolicy bypass -file " {VSISHARE}\_VSI_Binaries
\Connectors\ConnectorWrapperScript.ps1" localhost {username}@{domain} {password} "\\LVSIDS.HCIEUC.Demo\VSIShare
\_VSI_Binaries\Connectors\RDPConnect.exe" /server M6TX.vly.cloudworkspace.app /user {username}@{domain} /password
{password} /rdgateway vly-rds.vly.cloudworkspace.app /rdgatewayuserlogin {username}@{domain} /rdgatewayuserpassword
{password} /nowarning /rduseCredentials true /rdbypasslocal false /rdgatewaymode manual
```

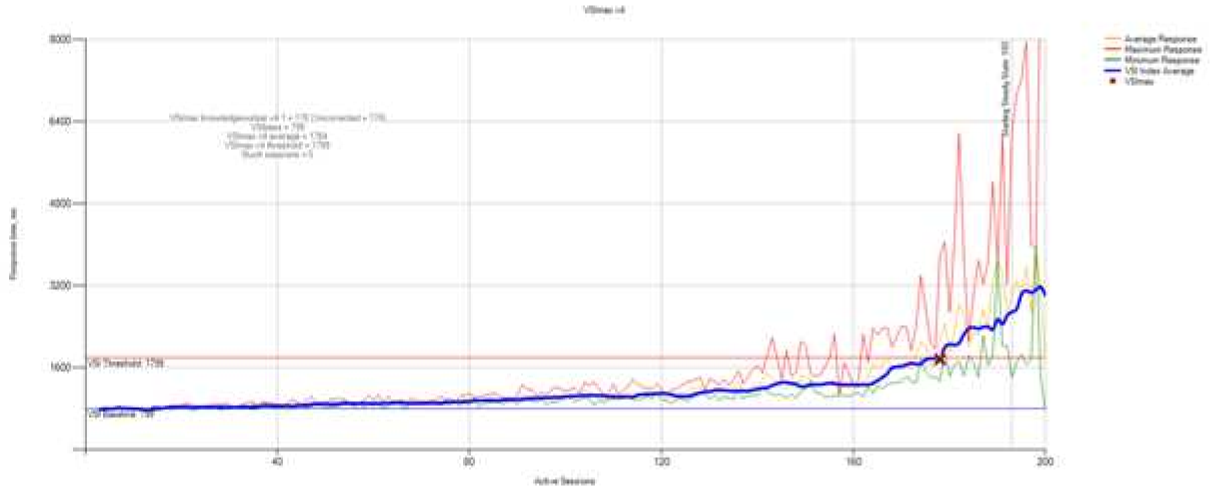
CSV file: ☐ use CSV file

\\vsids\VSIShare\1000Users.csv

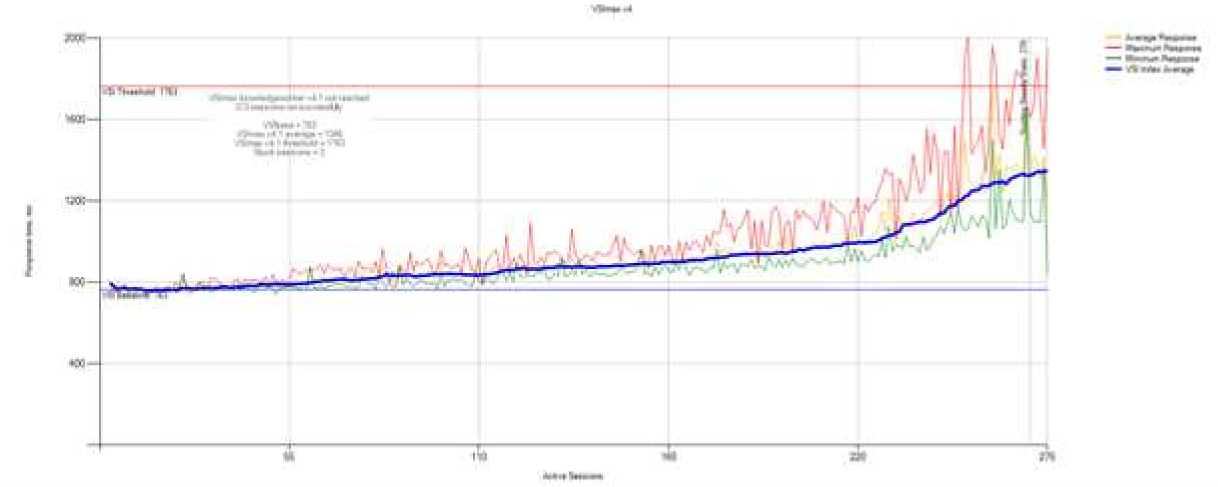
CONNECTION DETAILS

Server	m6tx.vly.cloudworkspace.app
Username	LVSI-VDS{count/4}
Password	•••••••
Domain	DemoVDS.com

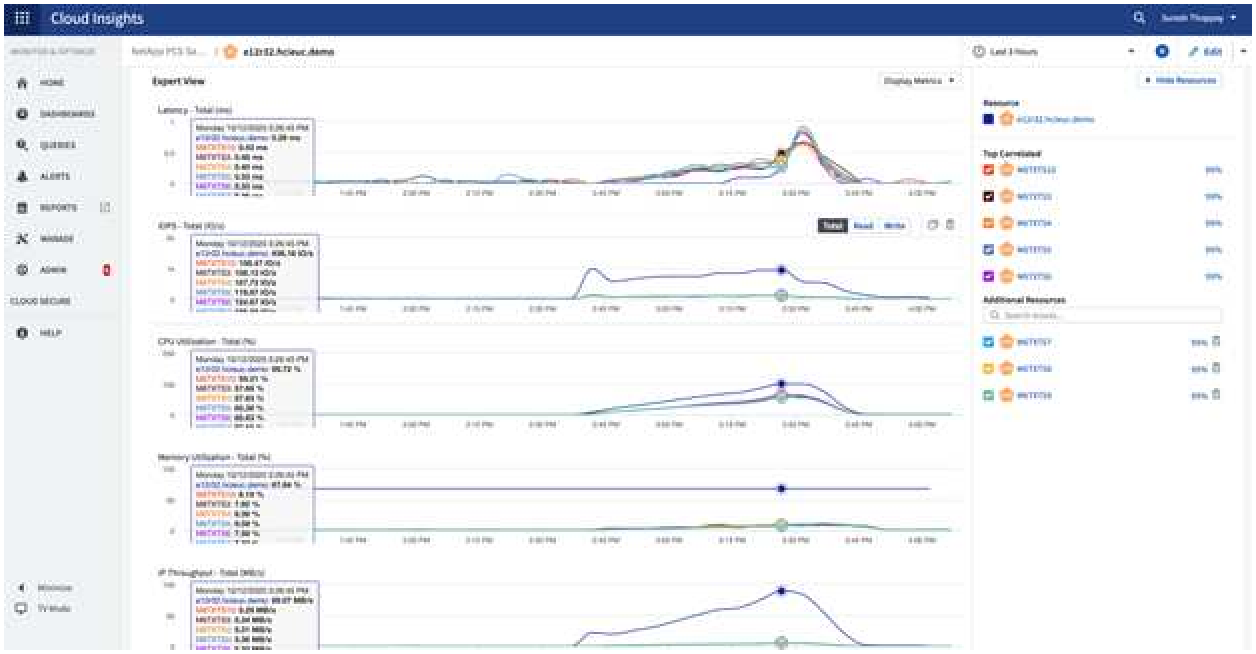
The following figure displays the Login VSI response time versus the active sessions for the H610C.



The following figure displays the Login VSI response time versus active sessions for the H615C.



The performance metrics from Cloud Insights during H615C Login VSI testing for the vSphere host and VMs are shown in the following figure.



Management Portal

NetApp VDS Cloud Workspace Management Suite portal is available here and the upcoming version is available here.

The portal allows centralized management for various VDS deployments including one that has sites defined for on-premises, administrative users, the application catalog, and scripted events. The portal is also used by administrative users for the manual provisioning of applications if required and to connect to any machines for troubleshooting.

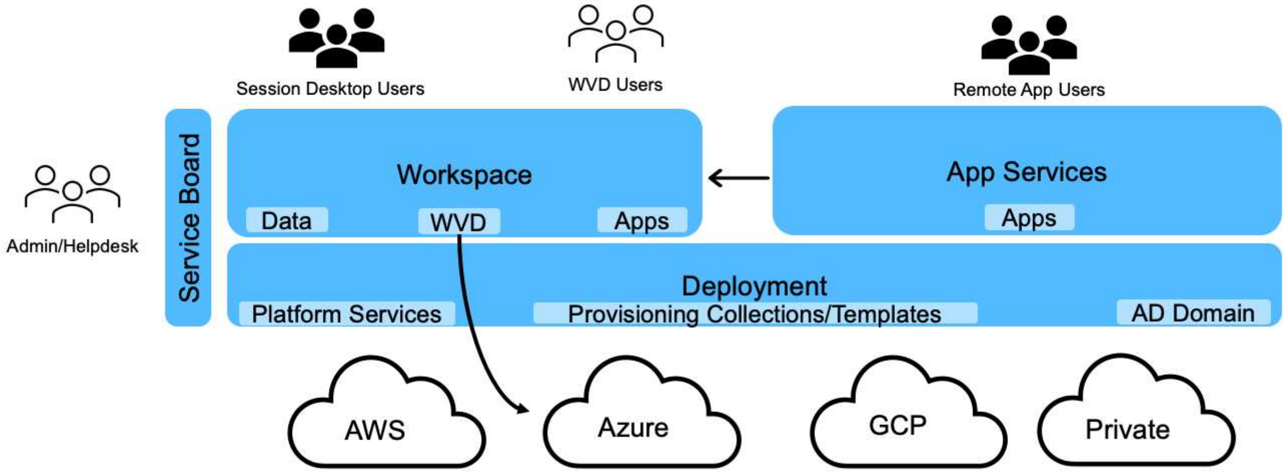
Service providers can use this portal to add their own channel partners and allow them to manage their own clients.

User Management

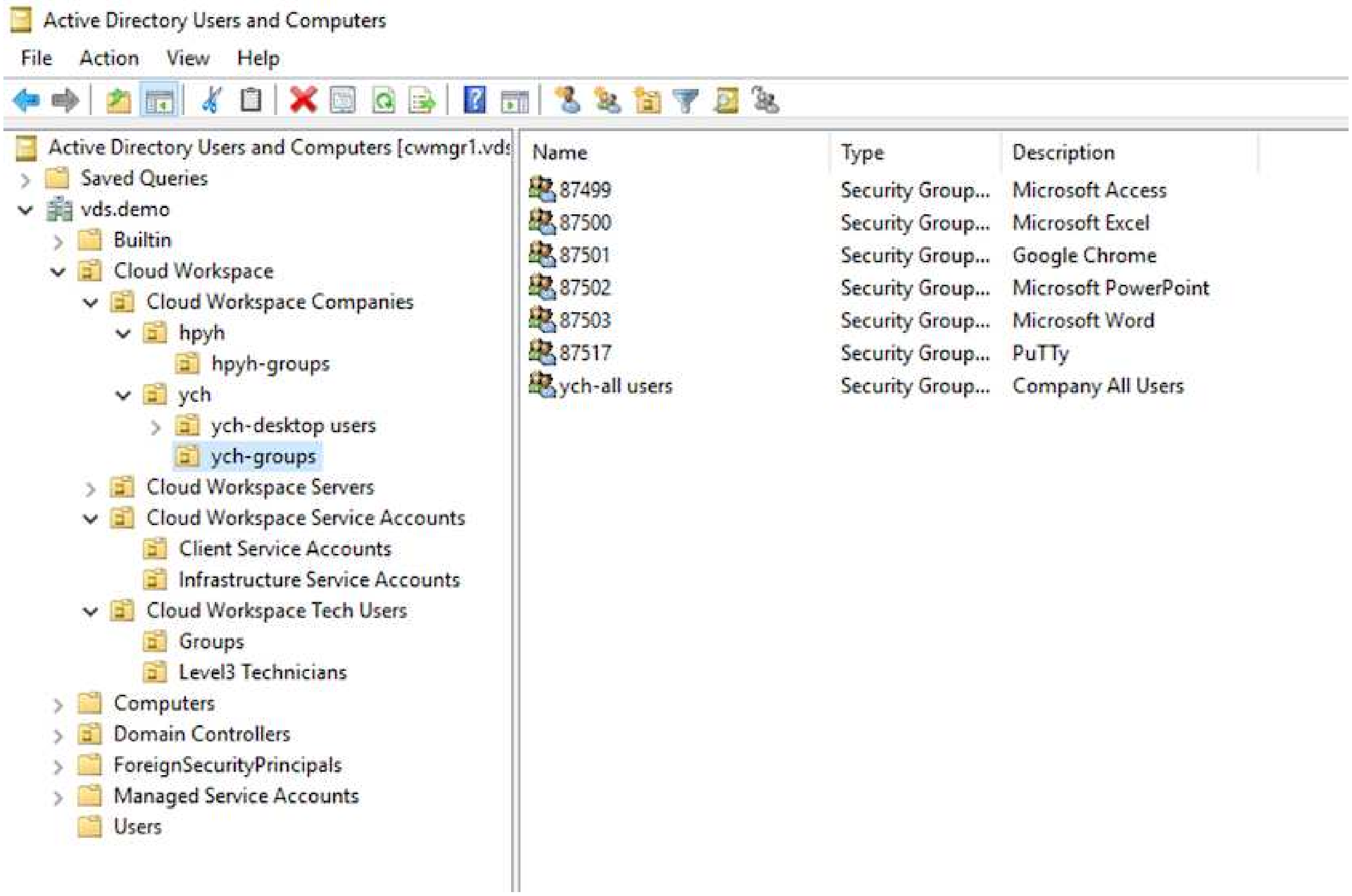
NetApp VDS uses Azure Active Directory for identity authentication and Azure Active Directory Domain Services for NTLM/Kerberos authentication. The ADConnect tool can be used to sync an on-prem Active Directory domain with Azure Active Directory.

New users can be added from the portal, or you can enable cloud workspace for existing users. Permissions for workspaces and application services can be controlled by individual users or by groups. From the management portal, administrative users can be defined to control permissions for the portal, workspaces, and so on.

The following figure depicts user management in NetApp VDS.



Each workspace resides in its own Active Directory organization unit (OU) under the Cloud Workspace OU as shown in the following figure.

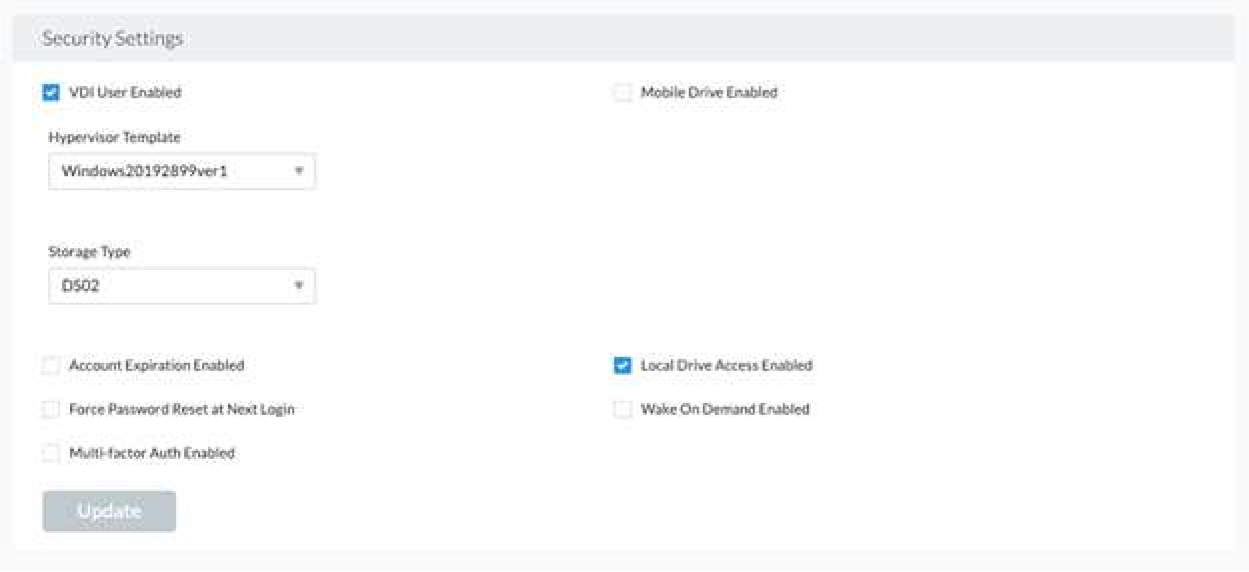


Name	Type	Description
87499	Security Group...	Microsoft Access
87500	Security Group...	Microsoft Excel
87501	Security Group...	Google Chrome
87502	Security Group...	Microsoft PowerPoint
87503	Security Group...	Microsoft Word
87517	Security Group...	PuTTy
ych-all users	Security Group...	Company All Users

For more info, see this video on user permissions and user management in NetApp VDS.

When an Active Directory group is defined as a CRAUserGroup using an API call for the datacenter, all the users in that group are imported into the CloudWorkspace for management using the UI. As the cloud workspace is enabled for the user, VDS creates user home folders, settings permissions, user properties updates, and so on.

If VDI User Enabled is checked, VDS creates a single-session RDS machine dedicated to that user. It prompts for the template and the datastore to provision.



Security Settings

☑ VDI User Enabled

□ Mobile Drive Enabled

Hypervisor Template

Windows20192899ver1

Storage Type

DS02

□ Account Expiration Enabled

□ Force Password Reset at Next Login

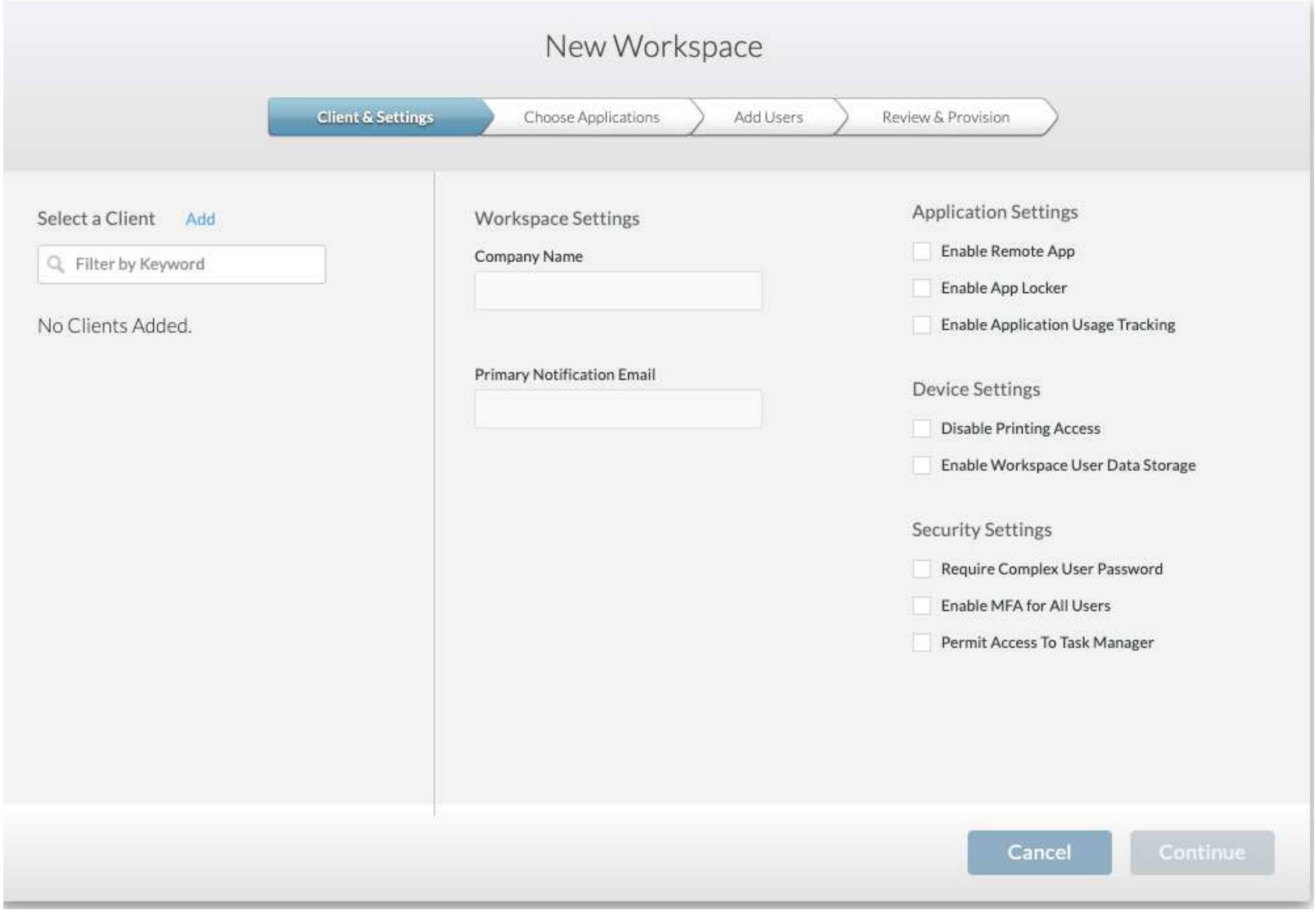
□ Multi-factor Auth Enabled

☑ Local Drive Access Enabled

□ Wake On Demand Enabled

Workspace Management

A workspace consists of a desktop environment; this can be shared remote desktop sessions hosted on-premises or on any supported cloud environment. With Microsoft Azure, the desktop environment can be persistent with Windows Virtual Desktops. Each workspace is associated with a specific organization or client. Options available when creating a new workspace can be seen in the following figure.



New Workspace

Client & Settings › Choose Applications › Add Users › Review & Provision

Select a Client Add

Filter by Keyword

No Clients Added.

Workspace Settings

Company Name

Primary Notification Email

Application Settings

□ Enable Remote App
□ Enable App Locker
□ Enable Application Usage Tracking

Device Settings

□ Disable Printing Access
□ Enable Workspace User Data Storage

Security Settings

□ Require Complex User Password
□ Enable MFA for All Users
□ Permit Access To Task Manager

Cancel Continue

Each workspace is associated with specific deployment.

Workspaces contain associated apps and app services, shared data folders, servers, and a WVD instance. Each workspace can control security options like enforcing password complexity, multifactor authentication, file audits, and so on.

Workspaces can control the workload schedule to power on extra servers, limit the number of users per server, or set the schedule for the resources available for given period (always on/off). Resources can also be configured to wake up on demand.

The workspace can override the deployment VM resource defaults if required. For WVD, WVD host pools (which contains session hosts and app groups) and WVD workspaces can also be managed from the cloud workspace management suite portal. For more info on the WVD host pool, see this video.

Application Management

Task workers can quickly launch an application from the list of applications made available to them. App services publish applications from the Remote Desktop Services session hosts. With WVD, App Groups provide similar functionality from multi-session Windows 10 host pools.

For office workers to power users, the applications that they require can be provisioned manually using a service board, or they can be auto-provisioned using the scripted events feature in NetApp VDS.

For more information, see the NetApp Application Entitlement page.

ONTAP features for Virtual Desktop Service

The following ONTAP features make it attractive choice for use with a virtual desktop service.

- **Scale-out filesystem.** ONTAP FlexGroup volumes can grow to more than 20PB in size and can contain more than 400 billion files within a single namespace. The cluster can contain up to 24 storage nodes, each with a flexible the number of network interface cards depending on the model used.

  User's virtual desktops, home folders, user profile containers, shared data, and so on can grow based on demand with no concern for filesystem limitations.

- **File system analytics.** You can use the XCP tool to gain insights into shared data. With ONTAP 9.8+ and ActiveIQ Unified Manager, you can easily query and retrieve file metadata information and identify cold data.
- **Cloud tiering.** You can migrage cold data to an object store in the cloud or to any S3-compatible storage in your datacenter.
- **File versions.** Users can recover files protected by NetApp ONTAP Snapshot copies. ONTAP Snapshot copies are very space efficient because they only record changed blocks.
- **Global namespace.** ONTAP FlexCache technology allows remote caching of file storage making it easier to manage shared data across locations containing ONTAP storage systems.
- **Secure multi-tenancy support.** A single physical storage cluster can be presented as multiple virtual storage arrays each with its own volumes, storage protocols, logical network interfaces, identity and authentication domain, management users, and so on. Therefore, you can share the storage array across multiple business units or environments, such as test, development, and production.

  To guarantee performance, you can use adaptive QoS to set performance levels based on used or allocated space, and you can control storage capacity by using quotas.

- **VMware integration.** ONTAP tools for VMware vSphere provides a vCenter plug-in to provision datastores, implement vSphere host best practices, and monitor ONTAP resources.

  ONTAP supports vStorage APIs for Array Integration (VAAI) for offloading SCSI/file operations to the storage array. ONTAP also supports vStorage APIs for Storage Awareness (VASA) and Virtual Volumes support for both block and file protocols.

  The Snapcenter Plug-in for VMware vSphere provides an easy way to back up and restore virtual machines using the Snapshot feature on a storage array.

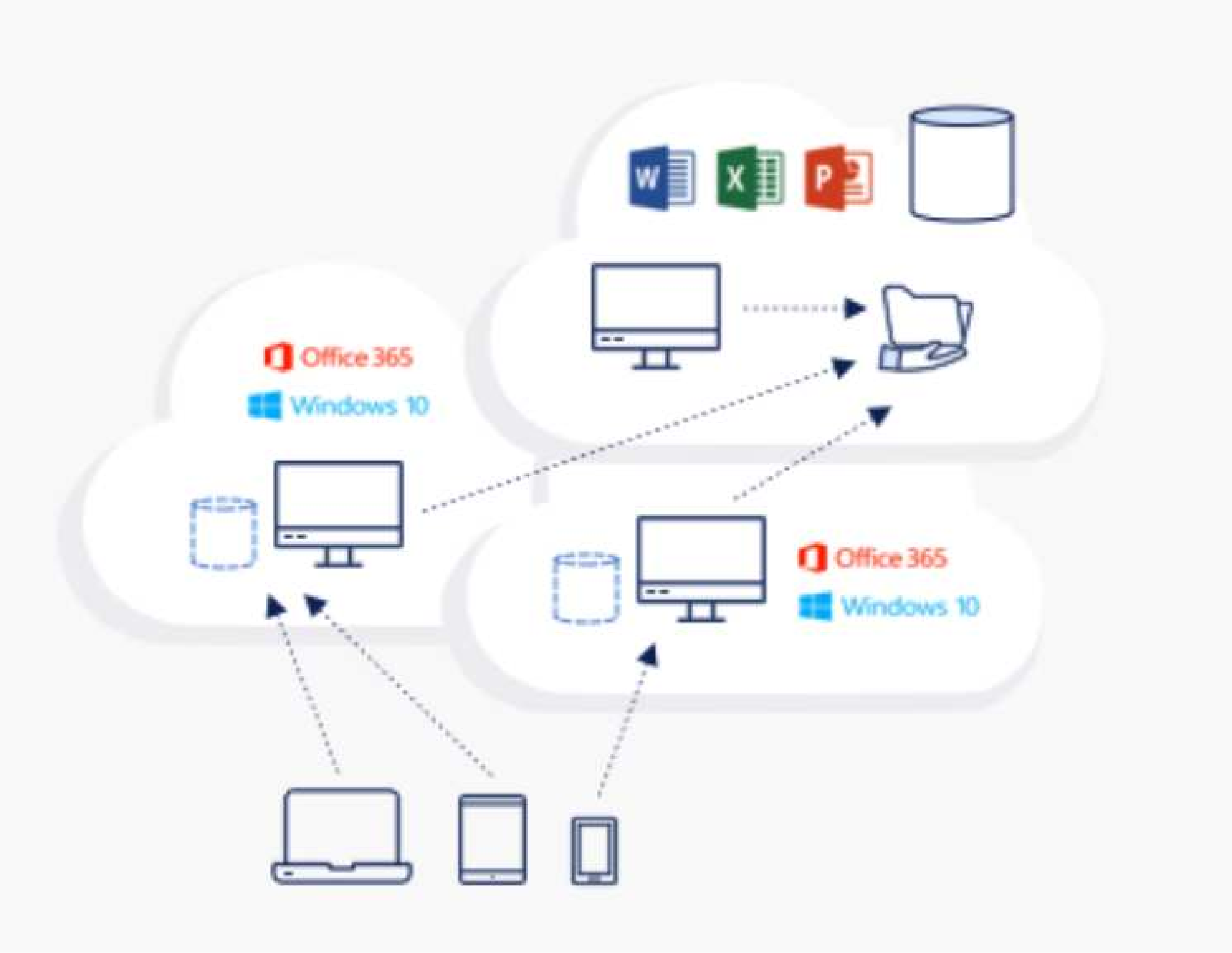
  ActiveIQ Unified Manager provides end-to-end storage network visibility in a vSphere environment. Administrators can easily identify any latency issues that might occur on virtual desktop environments hosted on ONTAP.

- **Security compliance.** With ActiveIQ Unified Manager, you can monitor multiple ONTAP systems with alerts for any policy violations.
- **Multi-protocol support.** ONTAP supports block (iSCSI, FC, FCoE, and NVMe/FC), file (NFSv3, NFSv4.1, SMB2.x, and SMB3.x), and object (S3) storage protocols.
- **Automation support.** ONTAP provides REST API, Ansible, and PowerShell modules to automate tasks with the VDS Management Portal.

As a part of deployment, you can choose the file-services method to host the user profile, shared data, and the home drive folder. The available options are File Server, Azure Files, or Azure NetApp Files. However, after deployment, you can modify this choice with the Command Center tool to point to any SMB share. There are various advantages to hosting with NetApp ONTAP. To learn how to change the SMB share, see Change Data Layer.

Global File Cache

When users are spread across multiple sites within a global namespace, Global File Cache can help reduce latency for frequently accessed data. Global File Cache deployment can be automated using a provisioning collection and scripted events. Global File Cache handles the read and write caches locally and maintains file locks across locations. Global File Cache can work with any SMB file servers, including Azure NetApp Files.



Global File Cache requires the following:

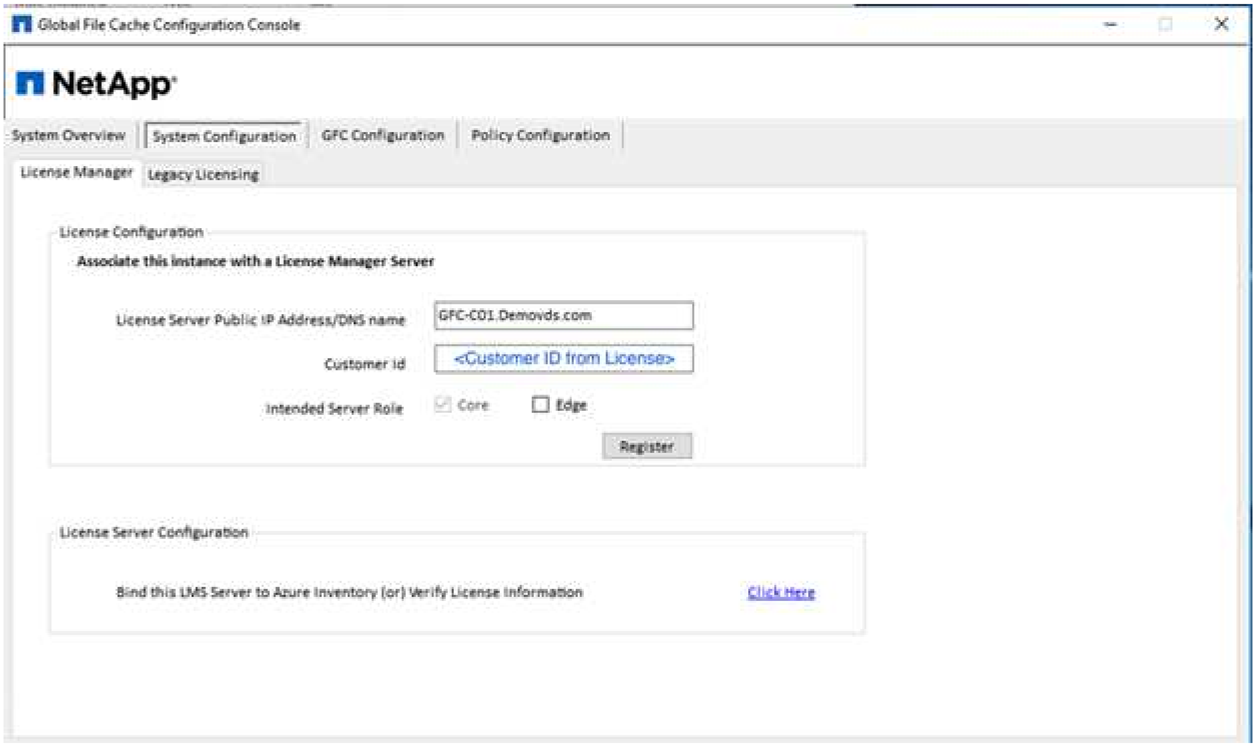
- Management server (License Management Server)
- Core

- Edge with enough disk capacity to cache the data

To download the software and to calculate the disk cache capacity for Edge, see the GFC documentation.

For our validation, we deployed the core and management resources on the same VM at Azure and edge resources on NetApp HCI. Please note that the core is where high-volume data access is required and the edge is a subset of the core. After the software is installed, you must activate the license activated before use. To do so, complete the following steps:

1. Under the License Configuration section, use the link Click Here to complete the license activation. Then register the core.



License Configuration

Associate this instance with a License Manager Server

License Server Public IP Address/DNS name: GFC-C01.Demovds.com

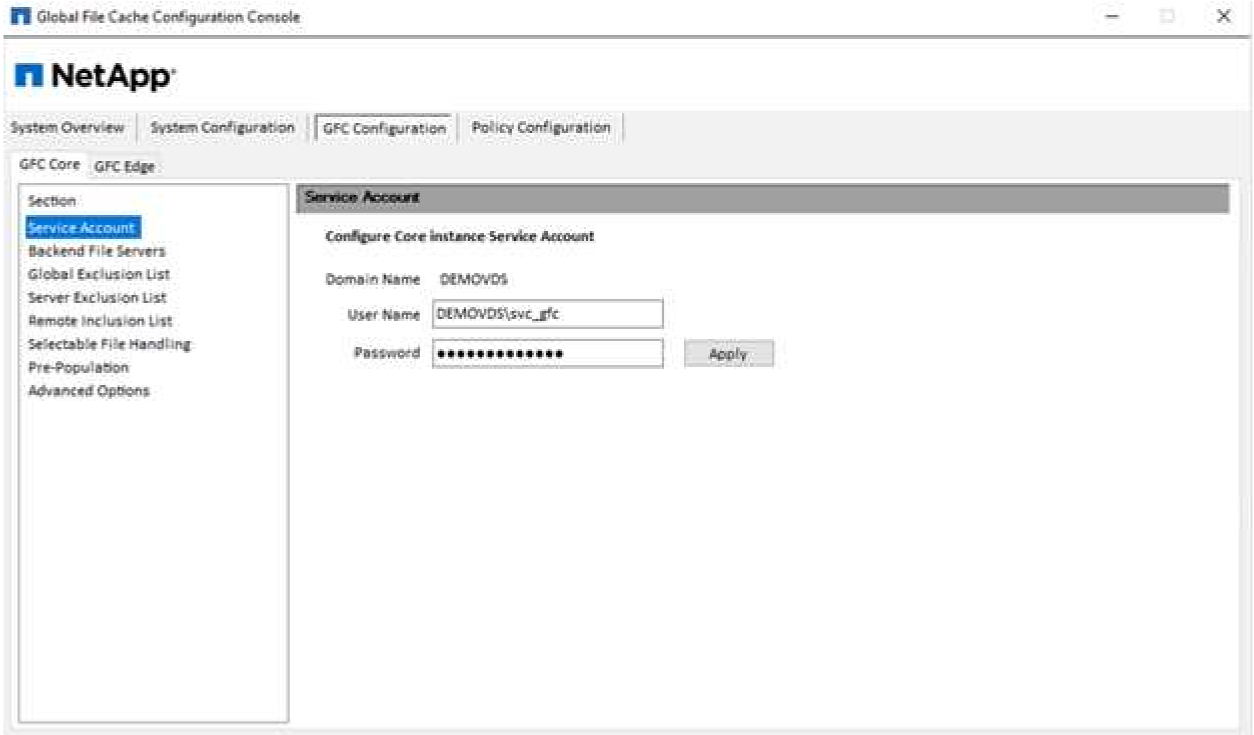
Customer Id: <Customer ID from License>

Intended Server Role: ☑ Core ☐ Edge

License Server Configuration

Bind this LMS Server to Azure Inventory (or) Verify License Information

2. Provide the service account to be used for the Global File Cache. For the required permissions for this account, see the GFC documentation.



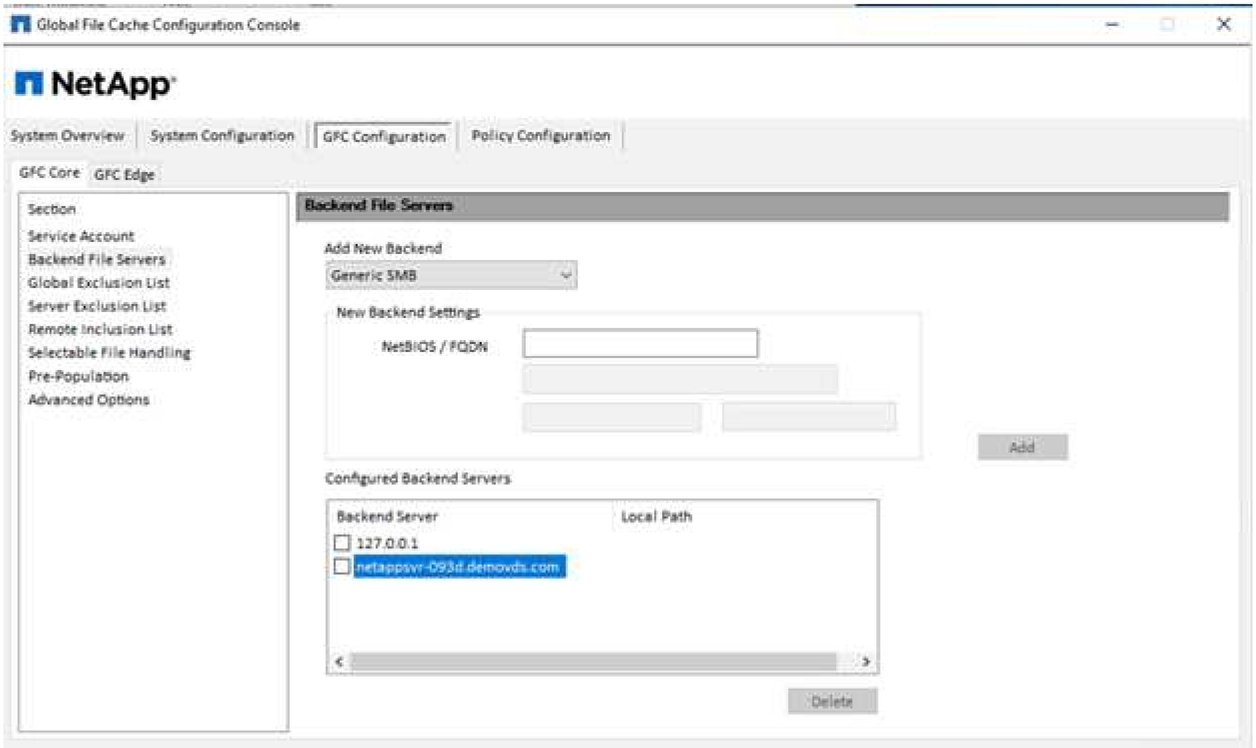
Configure Core instance Service Account

Domain Name DEMOVDS

User Name DEMOVDS\svc_gfc

Password ••••••••••••••

3. Add a new backend file server and provide the file server name or IP.



Add New Backend: Generic SMB

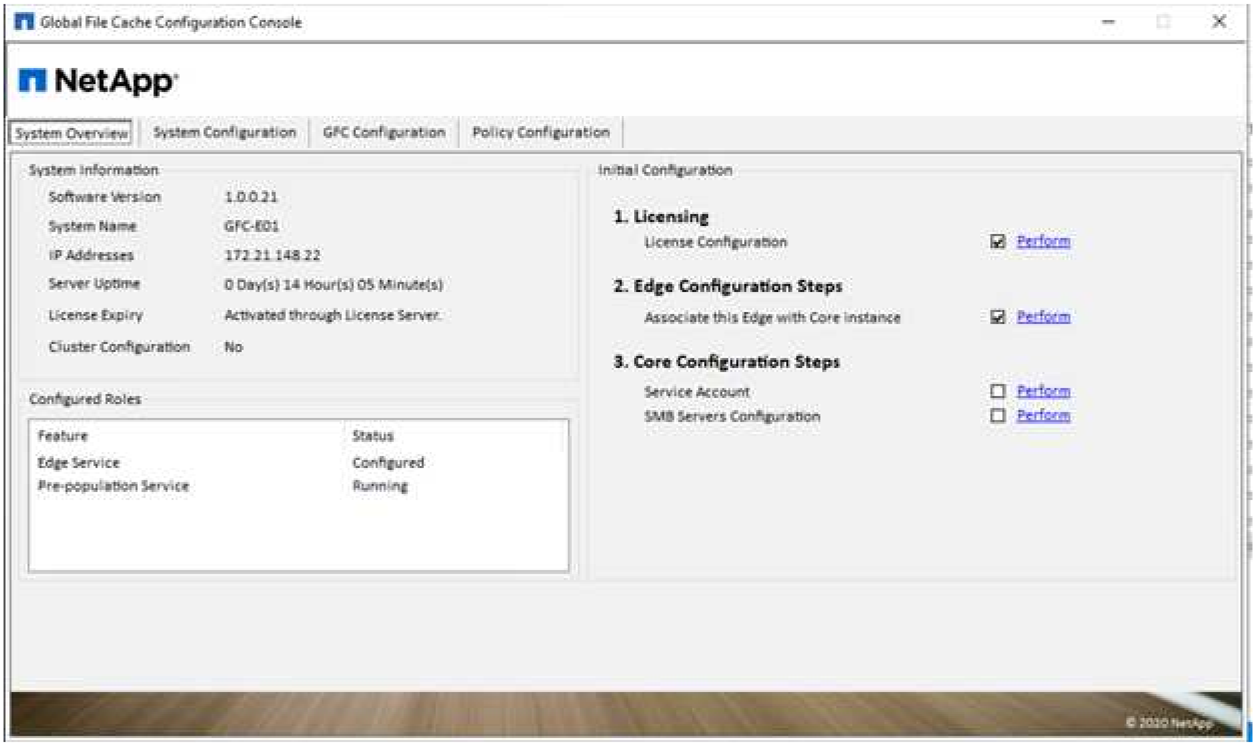
New Backend Settings

NetBIOS / FQDN

Configured Backend Servers

Backend Server	Local Path
□ 127.0.0.1	
□ netappsvr-093d.demovds.com	

4. On the edge, the cache drive must have the drive letter D. If it does not, use diskpart.exe to select the volume and change drive letter. Register with the license server as edge.



System Information

Software Version	1.0.0.21
System Name	GFC-E01
IP Addresses	172.21.148.22
Server Uptime	0 Day(s) 14 Hour(s) 05 Minute(s)
License Expiry	Activated through License Server.
Cluster Configuration	No

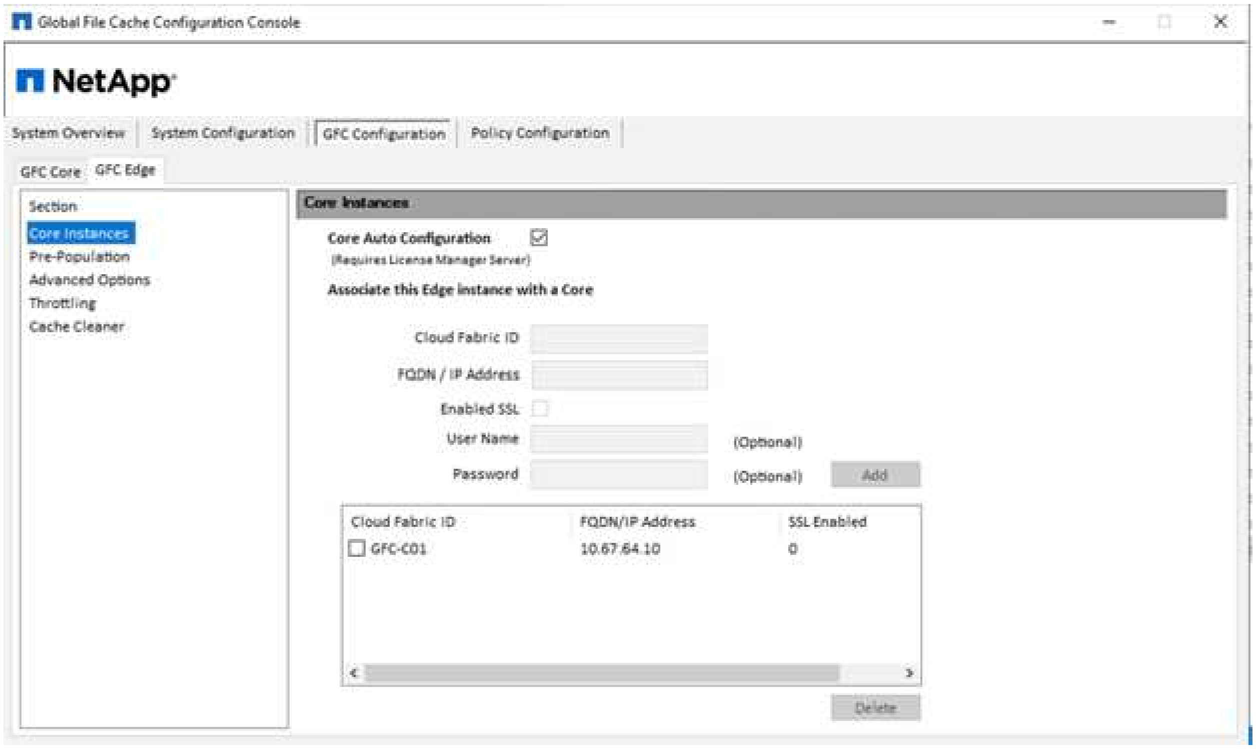
Configured Roles

Feature	Status
Edge Service	Configured
Pre-population Service	Running

Initial Configuration

1. Licensing
   - License Configuration ☑ Perform
2. Edge Configuration Steps
   - Associate this Edge with Core instance ☑ Perform
3. Core Configuration Steps
   - Service Account ☐ Perform
   - SMB Servers Configuration ☐ Perform

If core auto-configuration is enabled, core information is retrieved from the license management server automatically.



Core Instances

Core Auto Configuration ☑
(Requires License Manager Server)

Associate this Edge instance with a Core

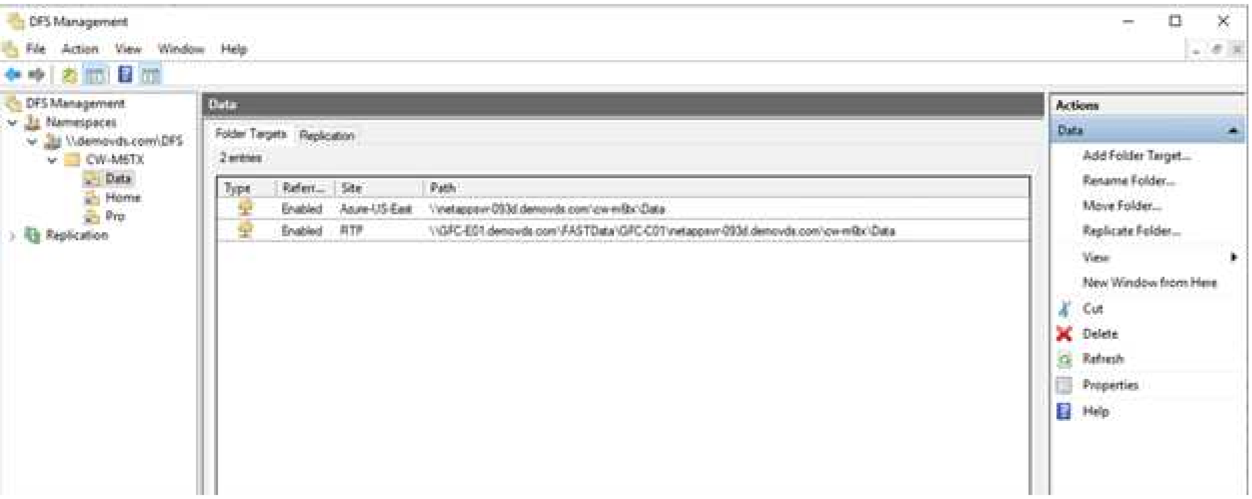
Cloud Fabric ID
FQDN / IP Address
Enabled SSL ☐
User Name (Optional)
Password (Optional)

Cloud Fabric ID	FQDN/IP Address	SSL Enabled
☐ GFC-C01	10.67.64.10	0

From any client machine, the administrators that used to access the share on the file server can access it with GFC edge using UNC Path `\\<edge server name>\FASTDATA\<core server name>\<backend file server name>\<share name>`. Administrators can include this path in user logonscript or GPO for users drive mapping at the edge location.

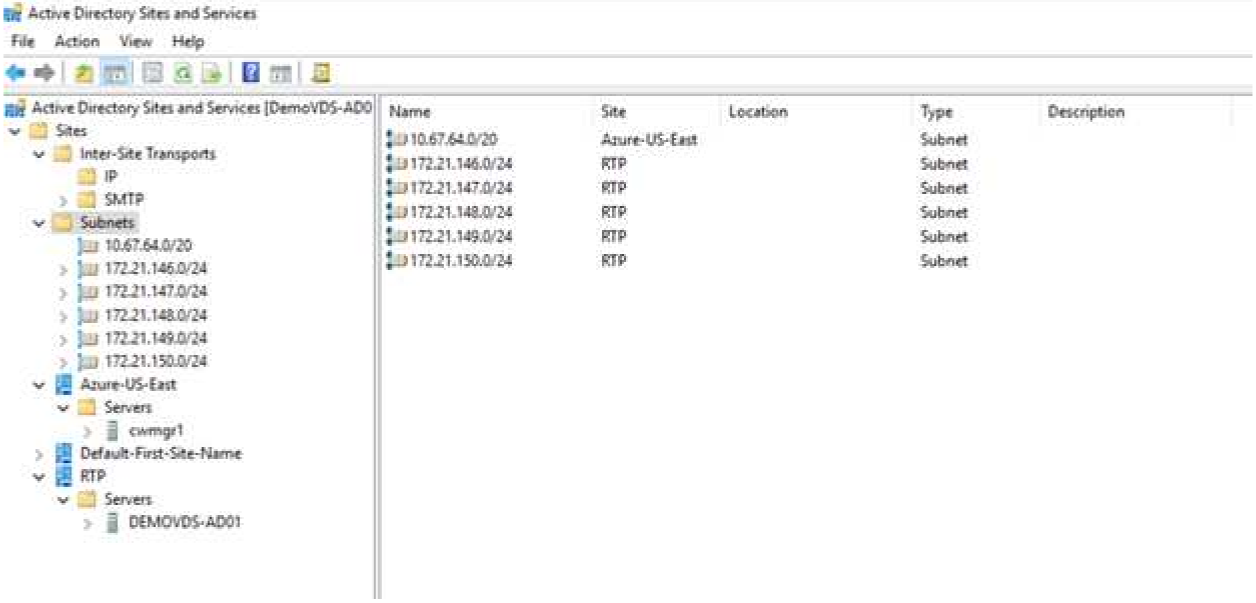
To provide transparent access for users across the globe, an administrator can setup the Microsoft Distributed

Filesystem (DFS) with links pointing to file server shares and to edge locations.



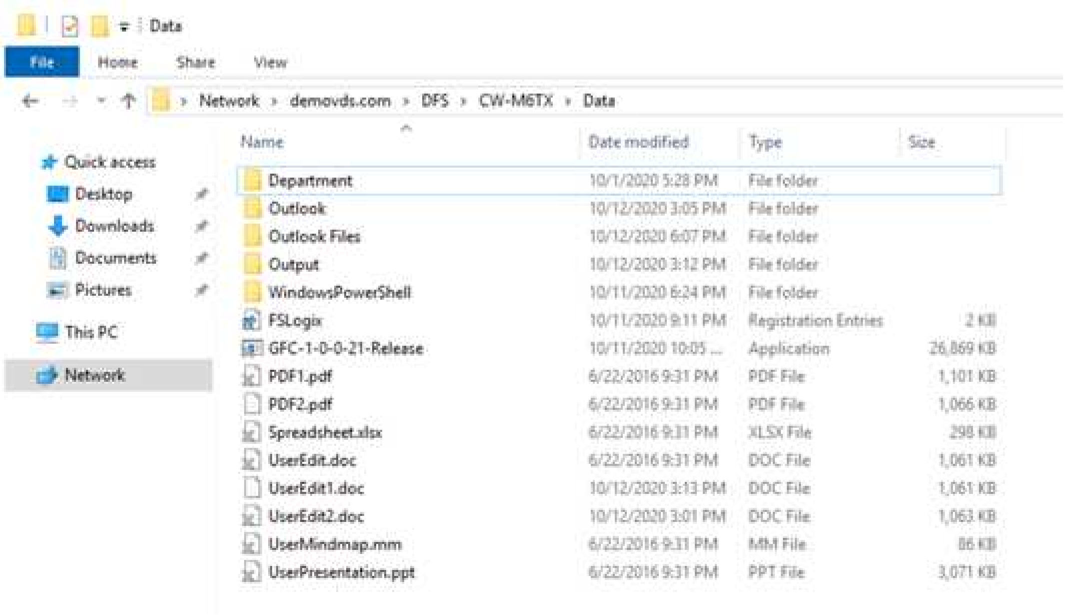
Type	Referr...	Site	Path
	Enabled	Azure-US-East	\\netappsvr-093d.demovds.com\cw-m6tx\Data
	Enabled	RTP	\\GFC-E01.demovds.com\FASTData\GFC-C01\netappsvr-093d.demovds.com\cw-m6tx\Data

When users log in with Active Directory credentials based on the subnets associated with the site, the appropriate link is utilized by the DFS client to access the data.



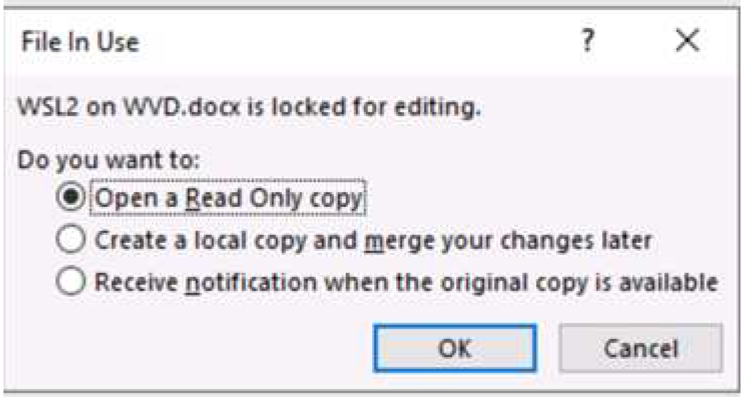
Name	Site	Location	Type	Description
10.67.64.0/20	Azure-US-East		Subnet	
172.21.146.0/24	RTP		Subnet	
172.21.147.0/24	RTP		Subnet	
172.21.148.0/24	RTP		Subnet	
172.21.149.0/24	RTP		Subnet	
172.21.150.0/24	RTP		Subnet	

File icons change depending on whether a file is cached; files that are not cached have a grey X on the lower left corner of the icon. After a user in an edge location accesses a file, that file is cached, and the icon changes.



Name	Date modified	Type	Size
Department	10/1/2020 5:28 PM	File folder	
Outlook	10/12/2020 3:05 PM	File folder	
Outlook Files	10/12/2020 6:07 PM	File folder	
Output	10/12/2020 3:12 PM	File folder	
WindowsPowerShell	10/11/2020 6:24 PM	File folder	
FSLogix	10/11/2020 9:11 PM	Registration Entries	2 KB
GFC-1-0-0-21-Release	10/11/2020 10:05 ...	Application	26,869 KB
PDF1.pdf	6/22/2016 9:31 PM	PDF File	1,101 KB
PDF2.pdf	6/22/2016 9:31 PM	PDF File	1,066 KB
Spreadsheet.xlsx	6/22/2016 9:31 PM	XLSX File	298 KB
UserEdit.doc	6/22/2016 9:31 PM	DOC File	1,061 KB
UserEdit1.doc	10/12/2020 3:13 PM	DOC File	1,061 KB
UserEdit2.doc	10/12/2020 3:01 PM	DOC File	1,063 KB
UserMindmap.mm	6/22/2016 9:31 PM	MM File	86 KB
UserPresentation.ppt	6/22/2016 9:31 PM	PPT File	3,071 KB

When a file is open and another user is trying to open the same file from an edge location, the user is prompted with the following selection:



File In Use

WSL2 on WVD.docx is locked for editing.

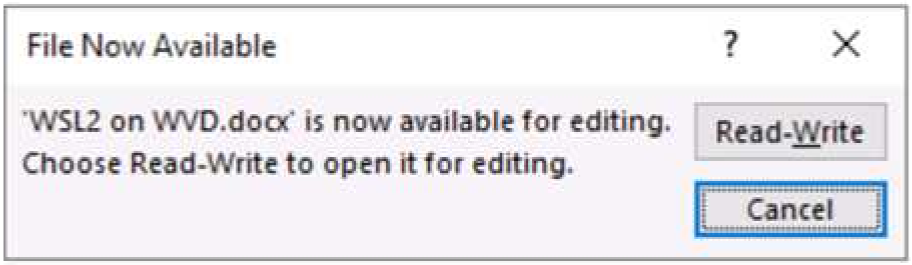
Do you want to:

● Open a Read Only copy

○ Create a local copy and merge your changes later

○ Receive notification when the original copy is available

If the user selects the option to receive a notification when the original copy is available, the user is notified as follows:



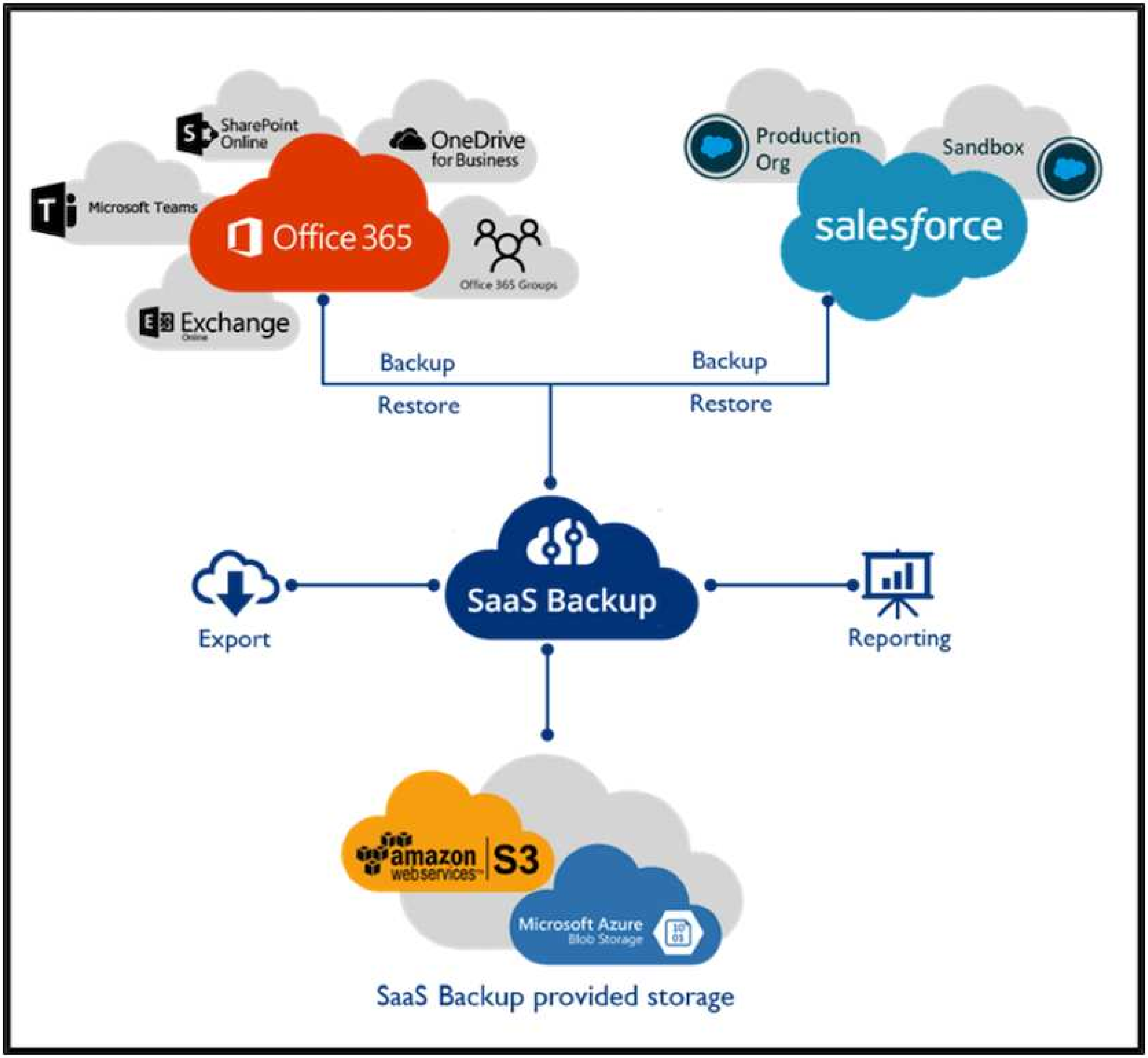
File Now Available

'WSL2 on WVD.docx' is now available for editing. Choose Read-Write to open it for editing.

For more information, see this video on Talon and Azure NetApp Files Deployment.

SaaS Backup

NetApp VDS provides data protection for Salesforce and Microsoft Office 365, including Exchange, SharePoint, and Microsoft OneDrive. The following figure shows how NetApp VDS provides SaaS Backup for these data services.



For a demonstration of Microsoft Office 365 data protection, see this video.

For a demonstration of Salesforce data protection, see this video.

Operation management

With NetApp VDS, administrators can delegate tasks to others. They can connect to deployed servers to troubleshoot, view logs, and run audit reports. While assisting customers, helpdesk or level-3 technicians can shadow user sessions, view process lists, and kill processes if required.

For information on VDS logfiles, see the Troubleshooting Failed VDA Actions page.

For more information on the required minimum permissions, see the VDA Components and Permissions page.

If you would like to manually clone a server, see the Cloning Virtual Machines page.

To automatically increase the VM disk size, see the Auto-Increase Disk Space Feature page.

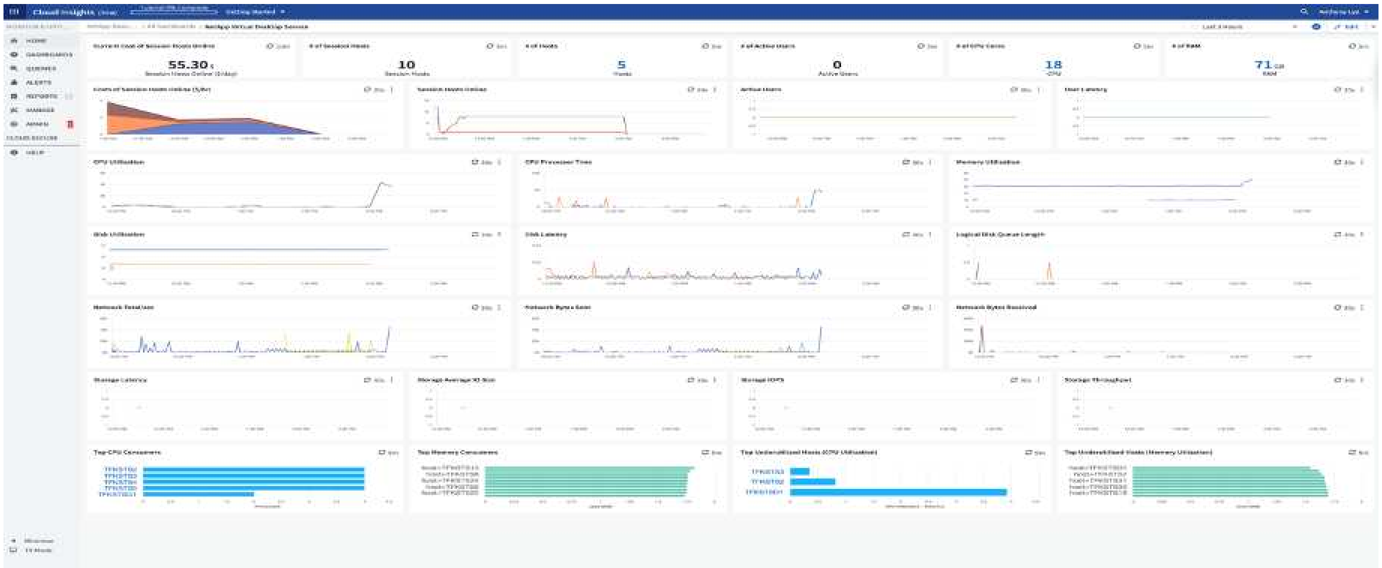
To identify the gateway address to manually configure the client, see the End User Requirements page.

Cloud Insights

NetApp Cloud Insights is a web-based monitoring tool that gives you complete visibility into infrastructure and applications running on NetApp and other third-party infrastructure components. Cloud Insights supports both private cloud and public clouds for monitoring, troubleshooting, and optimizing resources.

Only the acquisition unit VM (can be Windows or Linux) must be installed on a private cloud to collect metrics from data collectors without the need for agents. Agent-based data collectors allow you to pull custom metrics from Windows Performance Monitor or any input agents that Telegraf supports.

The following figure depicts the Cloud Insights VDS dashboard.



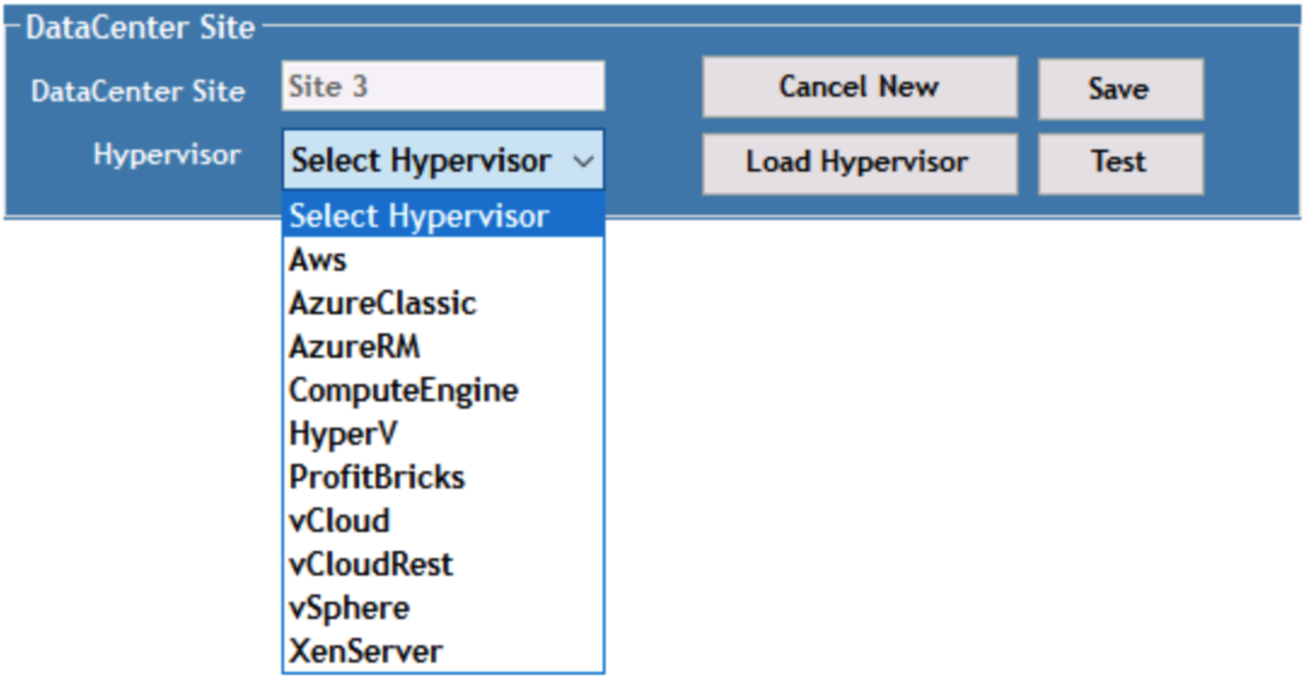
For more info on NetApp Cloud Insights, see this video.

Tools and Logs

This page discusses the DCConfig Tool, TestVdc Tools, and log files.

DCConfig Tool

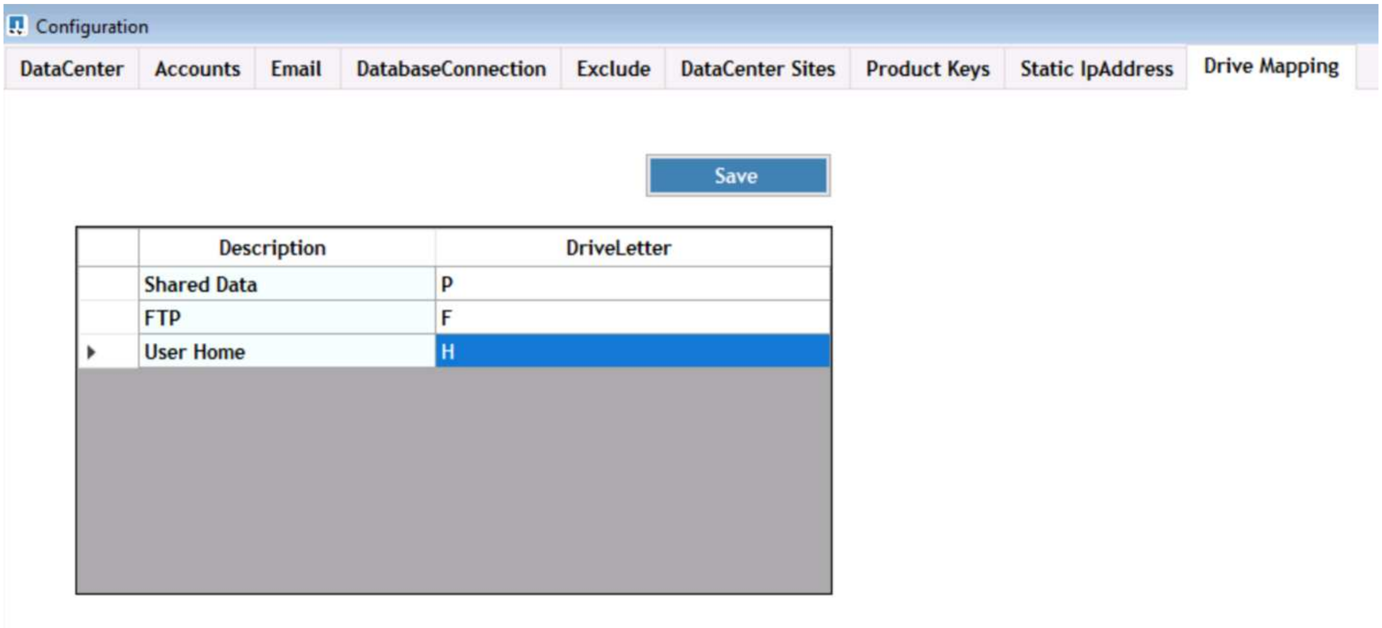
The DCCconfig tool supports the following hypervisor options for adding a site:



DataCenter Site

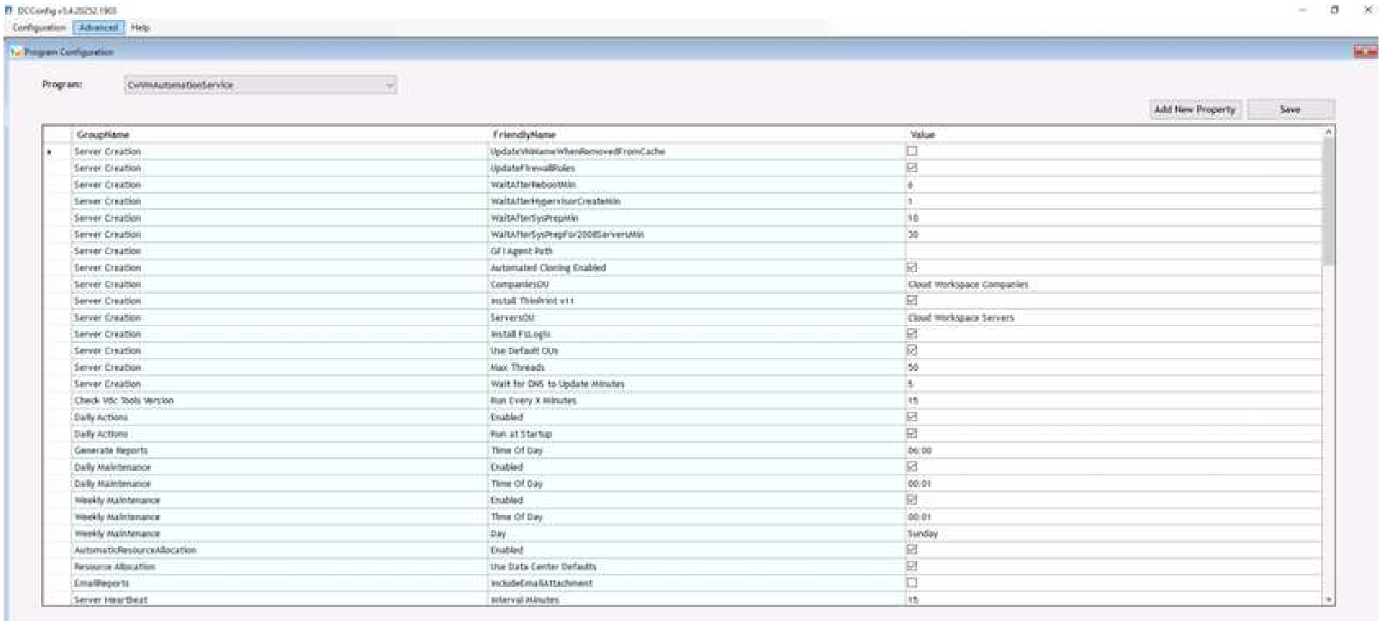
DataCenter Site: Site 3

Hypervisor: Select Hypervisor



Description	DriveLetter
Shared Data	P
FTP	F
User Home	H

Workspace-specific drive-letter mapping for shared data can be handled using GPO. Professional Services or the support team can use the advanced tab to customize settings like Active Directory OU names, the option to enable or disable deployment of FSLogix, various timeout values, and so on.



Program: CwVmAutomationService

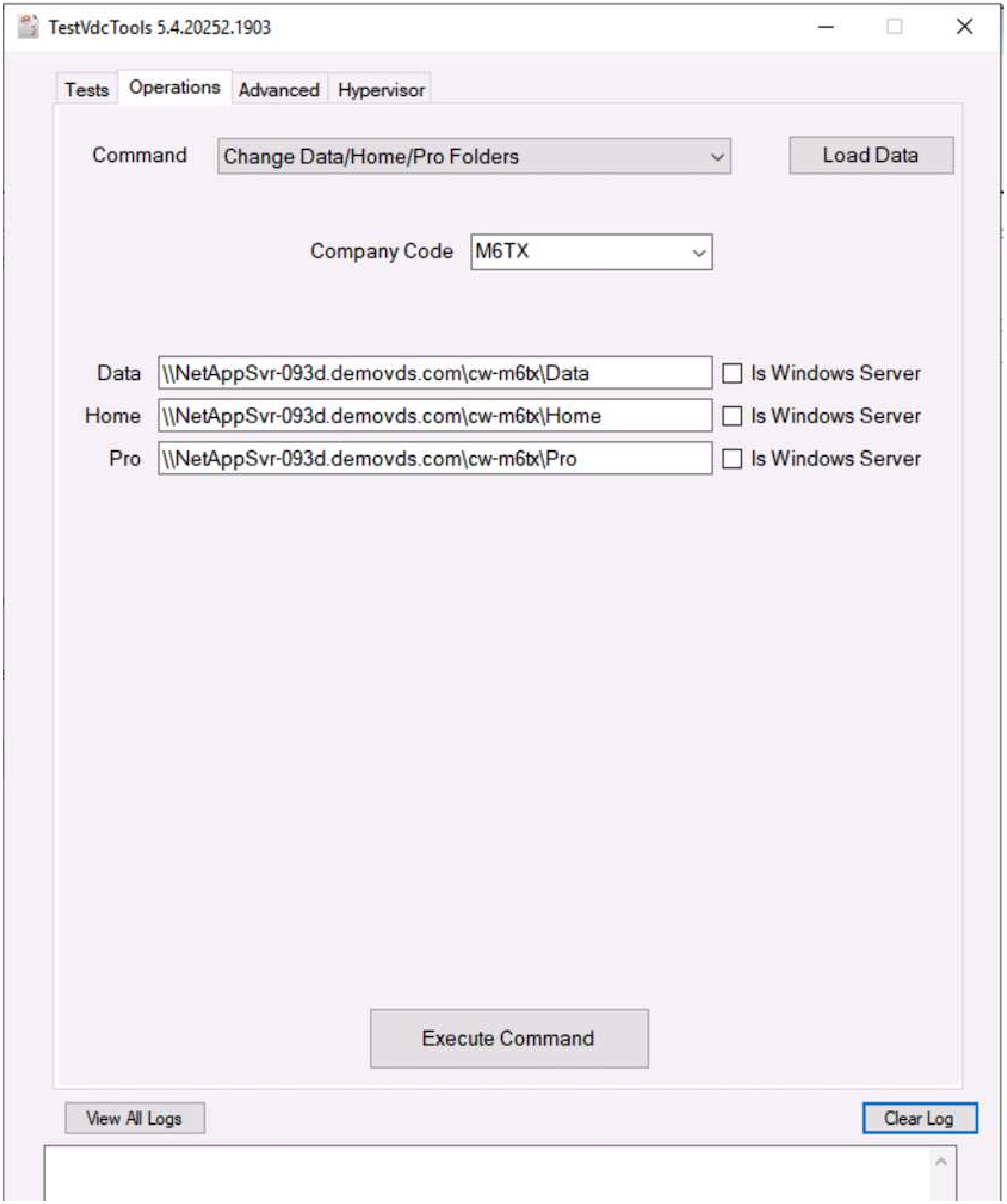
GroupName	FriendlyName	Value
Server Creation	UpdateVMNameWhenRemovedFromCache	☐
Server Creation	UpdateFirewallRoles	☑
Server Creation	WaitAfterRebootMin	0
Server Creation	WaitAfterHypervisorCreateMin	1
Server Creation	WaitAfterSysPrepMin	10
Server Creation	WaitAfterSysPrepFor2008ServersMin	30
Server Creation	GFI Agent Path	
Server Creation	Automated Cloning Enabled	☑
Server Creation	CompaniesOU	Cloud Workspace Companies
Server Creation	Install ThinPrint v11	☑
Server Creation	ServersOU	Cloud Workspace Servers
Server Creation	Install FsLogix	☑
Server Creation	Use Default OUs	☑
Server Creation	Max Threads	50
Server Creation	Wait for DNS to Update Minutes	5
Check Vdc Tools Version	Run Every X Minutes	15
Daily Actions	Enabled	☑
Daily Actions	Run at Startup	☑
Generate Reports	Time Of Day	06:00
Daily Maintenance	Enabled	☑
Daily Maintenance	Time Of Day	00:01
Weekly Maintenance	Enabled	☑
Weekly Maintenance	Time Of Day	00:01
Weekly Maintenance	Day	Sunday
AutomaticResourceAllocation	Enabled	☑
Resource Allocation	Use Data Center Defaults	☑
EmailReports	IncludeEmailAttachment	☐
Server HeartBeat	Interval Minutes	15

Command Center (Previously known as TestVdc Tools)

To launch Command Center and the required role, see the Command Center Overview.

You can perform the following operations:

- Change the SMB Path for a workspace.



Command: Change Data/Home/Pro Folders

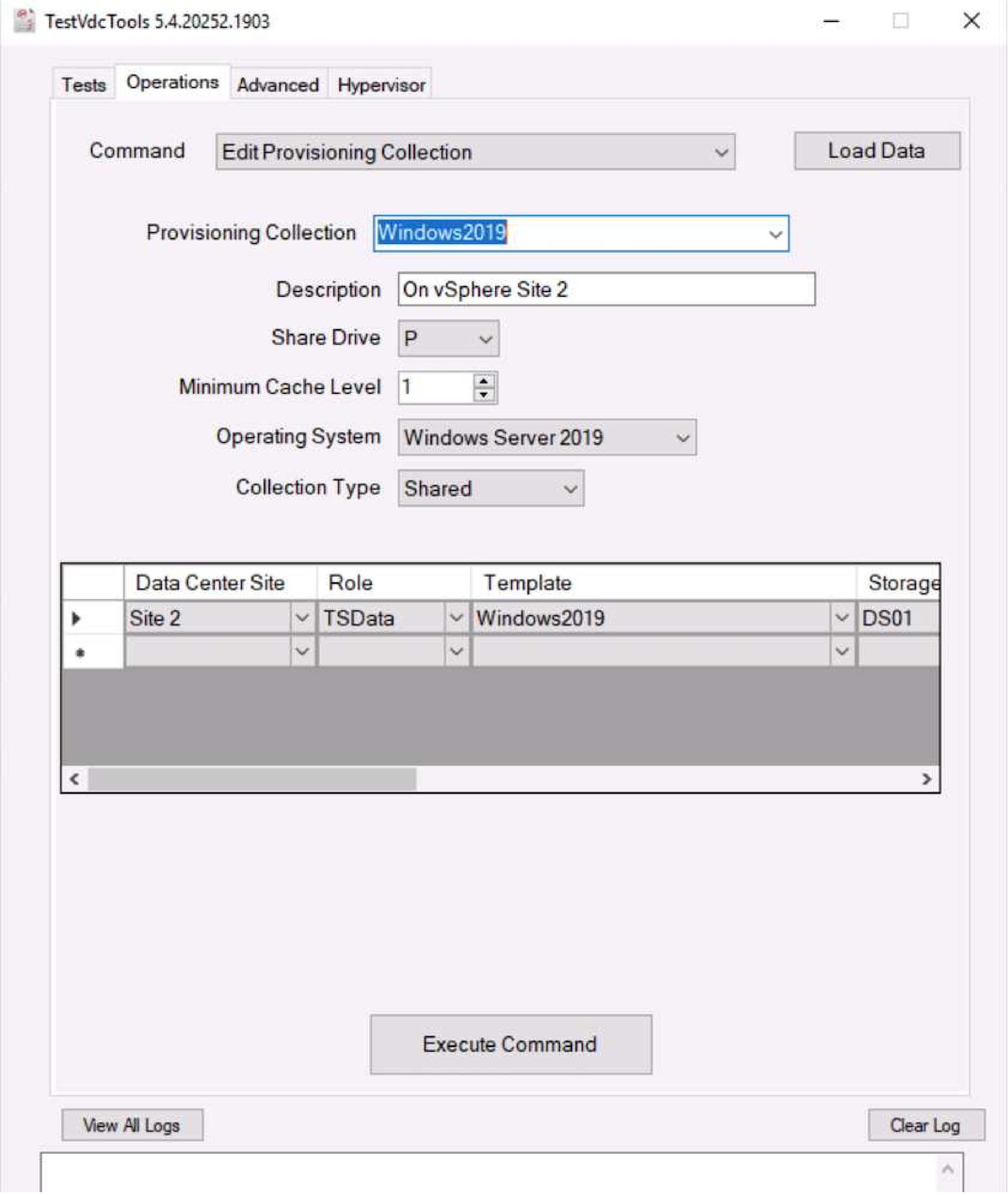
Company Code: M6TX

Data: \\NetAppSvr-093d.demovds.com\cw-m6tx\Data □ Is Windows Server

Home: \\NetAppSvr-093d.demovds.com\cw-m6tx\Home □ Is Windows Server

Pro: \\NetAppSvr-093d.demovds.com\cw-m6tx\Pro □ Is Windows Server

- Change the site for provisioning collection.



TestVdcTools 5.4.20252.1903

Command: Edit Provisioning Collection

Provisioning Collection: Windows2019

Description: On vSphere Site 2

Share Drive: P

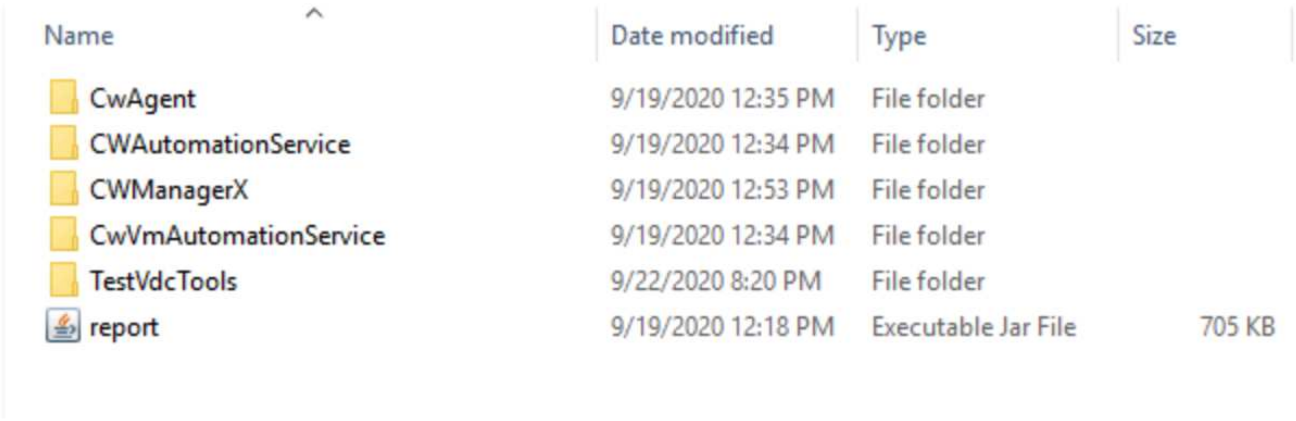
Minimum Cache Level: 1

Operating System: Windows Server 2019

Collection Type: Shared

	Data Center Site	Role	Template	Storage
▶	Site 2	TSData	Windows2019	DS01
*				

Log Files



Name	Date modified	Type	Size
CwAgent	9/19/2020 12:35 PM	File folder	
CWAutomationService	9/19/2020 12:34 PM	File folder	
CWManagerX	9/19/2020 12:53 PM	File folder	
CwVmAutomationService	9/19/2020 12:34 PM	File folder	
TestVdcTools	9/22/2020 8:20 PM	File folder	
report	9/19/2020 12:18 PM	Executable Jar File	705 KB

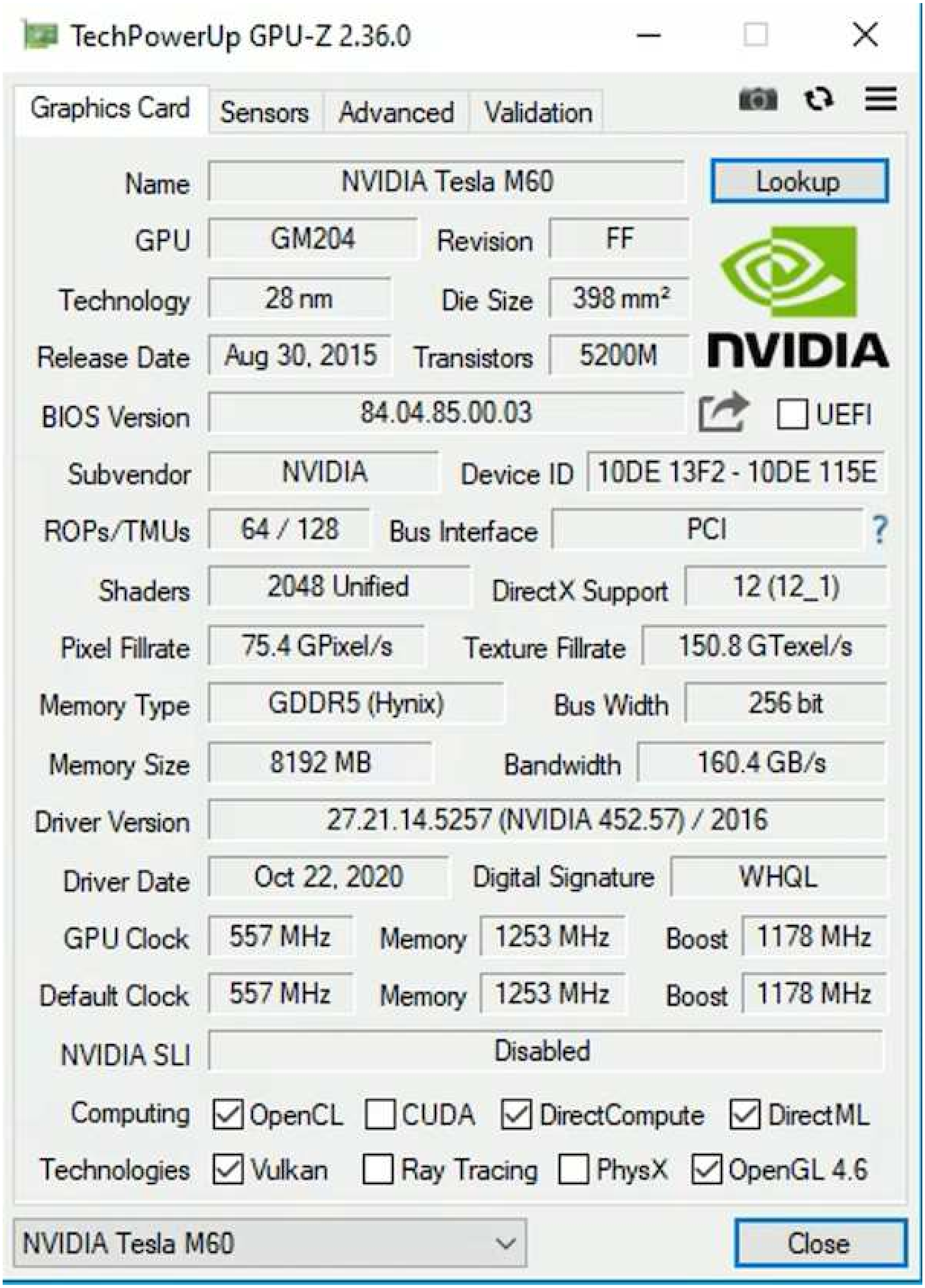
Check automation logs for more info.

GPU considerations

GPUs are typically used for graphic visualization (rendering) by performing repetitive arithmetic calculations. This repetitive compute capability is often used for AI and deep learning use cases.

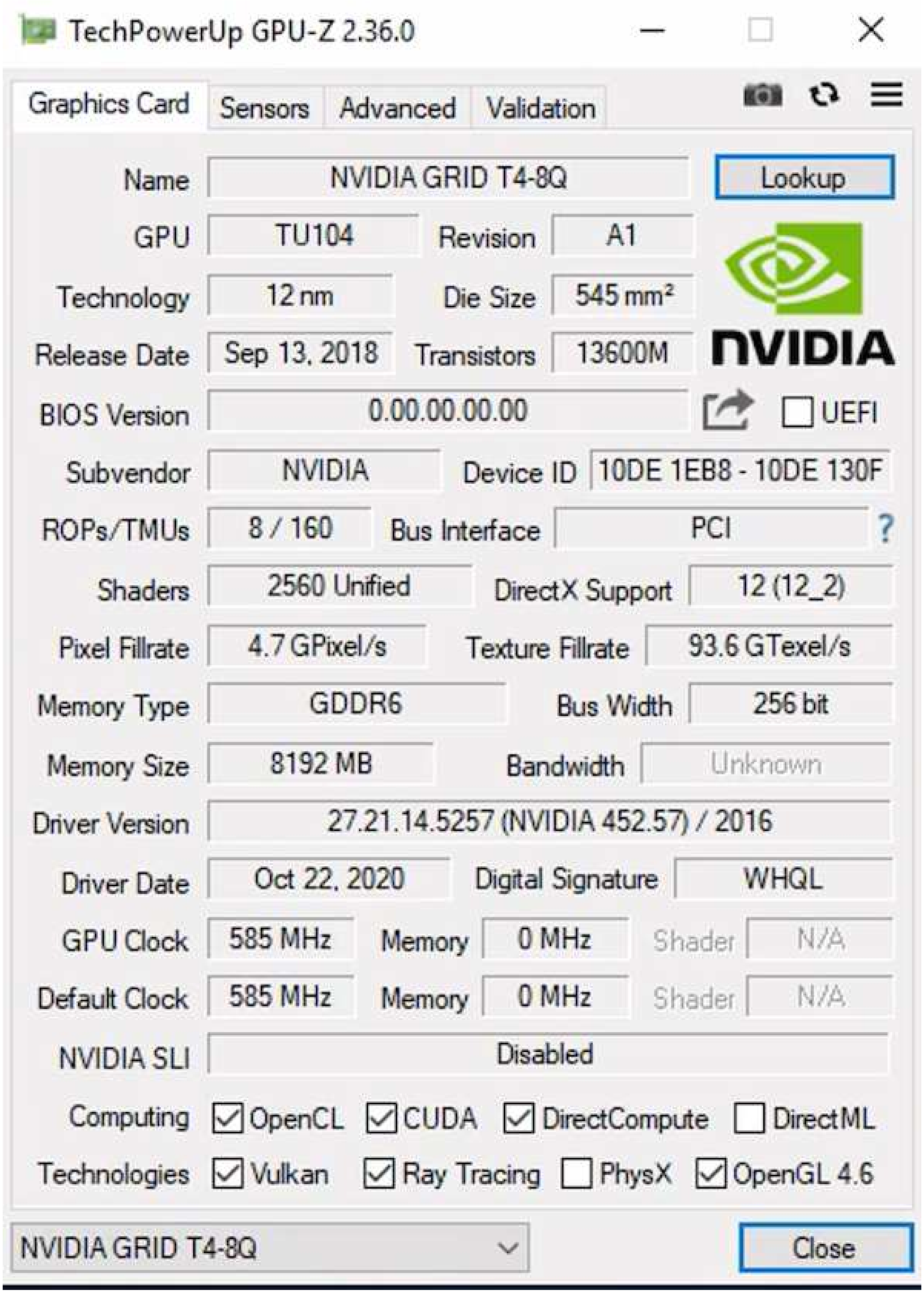
For graphic intensive applications, Microsoft Azure offers the NV series based on the NVIDIA Tesla M60 card with one to four GPUs per VM. Each NVIDIA Tesla M60 card includes two Maxwell-based GPUs, each with 8GB of GDDR5 memory for a total of 16GB.

> ⓘ An NVIDIA license is included with the NV series.



Name: NVIDIA Tesla M60
GPU: GM204 Revision: FF
Technology: 28 nm Die Size: 398 mm²
Release Date: Aug 30, 2015 Transistors: 5200M
BIOS Version: 84.04.85.00.03 □ UEFI
Subvendor: NVIDIA Device ID: 10DE 13F2 - 10DE 115E
ROPs/TMUs: 64 / 128 Bus Interface: PCI ?
Shaders: 2048 Unified DirectX Support: 12 (12_1)
Pixel Fillrate: 75.4 GPixel/s Texture Fillrate: 150.8 GTexel/s
Memory Type: GDDR5 (Hynix) Bus Width: 256 bit
Memory Size: 8192 MB Bandwidth: 160.4 GB/s
Driver Version: 27.21.14.5257 (NVIDIA 452.57) / 2016
Driver Date: Oct 22, 2020 Digital Signature: WHQL
GPU Clock: 557 MHz Memory: 1253 MHz Boost: 1178 MHz
Default Clock: 557 MHz Memory: 1253 MHz Boost: 1178 MHz
NVIDIA SLI: Disabled
Computing: ☑ OpenCL □ CUDA ☑ DirectCompute ☑ DirectML
Technologies: ☑ Vulkan □ Ray Tracing □ PhysX ☑ OpenGL 4.6
NVIDIA Tesla M60

With NetApp HCI, the H615C GPU contains three NVIDIA Tesla T4 cards. Each NVIDIA Tesla T4 card has a Touring-based GPU with 16GB of GDDR6 memory. When used in a VMware vSphere environment, virtual machines are able to share the GPU, with each VM having dedicated frame buffer memory. Ray tracing is available with the GPUs on the NetApp HCI H615C to produce realistic images including light reflections. Please note that you need to have an NVIDIA license server with a license for GPU features.



Name: NVIDIA GRID T4-8Q

GPU: TU104 Revision: A1

Technology: 12 nm Die Size: 545 mm²

Release Date: Sep 13, 2018 Transistors: 13600M

BIOS Version: 0.00.00.00.00 □ UEFI

Subvendor: NVIDIA Device ID: 10DE 1EB8 - 10DE 130F

ROPs/TMUs: 8 / 160 Bus Interface: PCI ?

Shaders: 2560 Unified DirectX Support: 12 (12_2)

Pixel Fillrate: 4.7 GPixel/s Texture Fillrate: 93.6 GTexel/s

Memory Type: GDDR6 Bus Width: 256 bit

Memory Size: 8192 MB Bandwidth: Unknown

Driver Version: 27.21.14.5257 (NVIDIA 452.57) / 2016

Driver Date: Oct 22, 2020 Digital Signature: WHQL

GPU Clock: 585 MHz Memory: 0 MHz Shader: N/A

Default Clock: 585 MHz Memory: 0 MHz Shader: N/A

NVIDIA SLI: Disabled

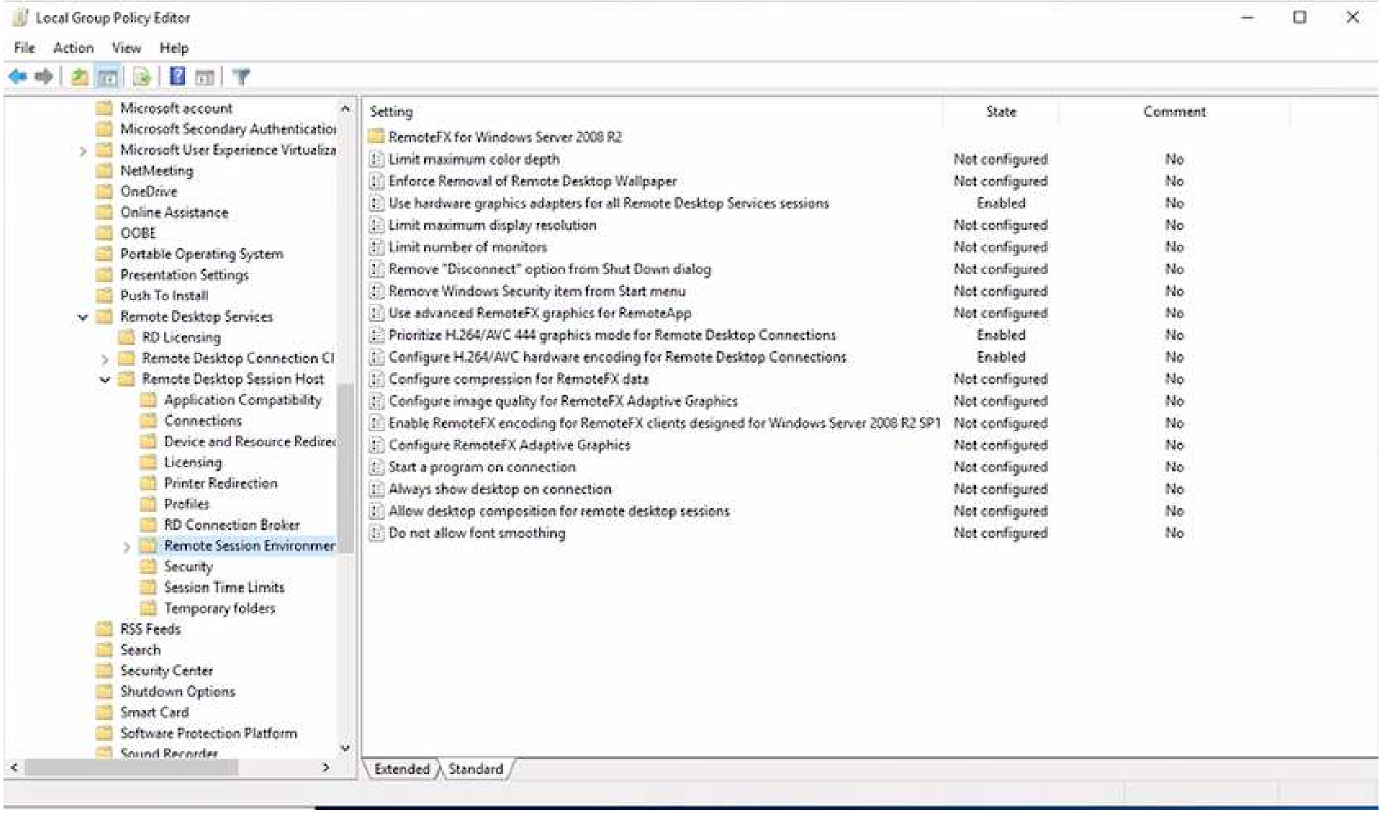
Computing: ☑ OpenCL ☑ CUDA ☑ DirectCompute □ DirectML

Technologies: ☑ Vulkan ☑ Ray Tracing □ PhysX ☑ OpenGL 4.6

NVIDIA GRID T4-8Q

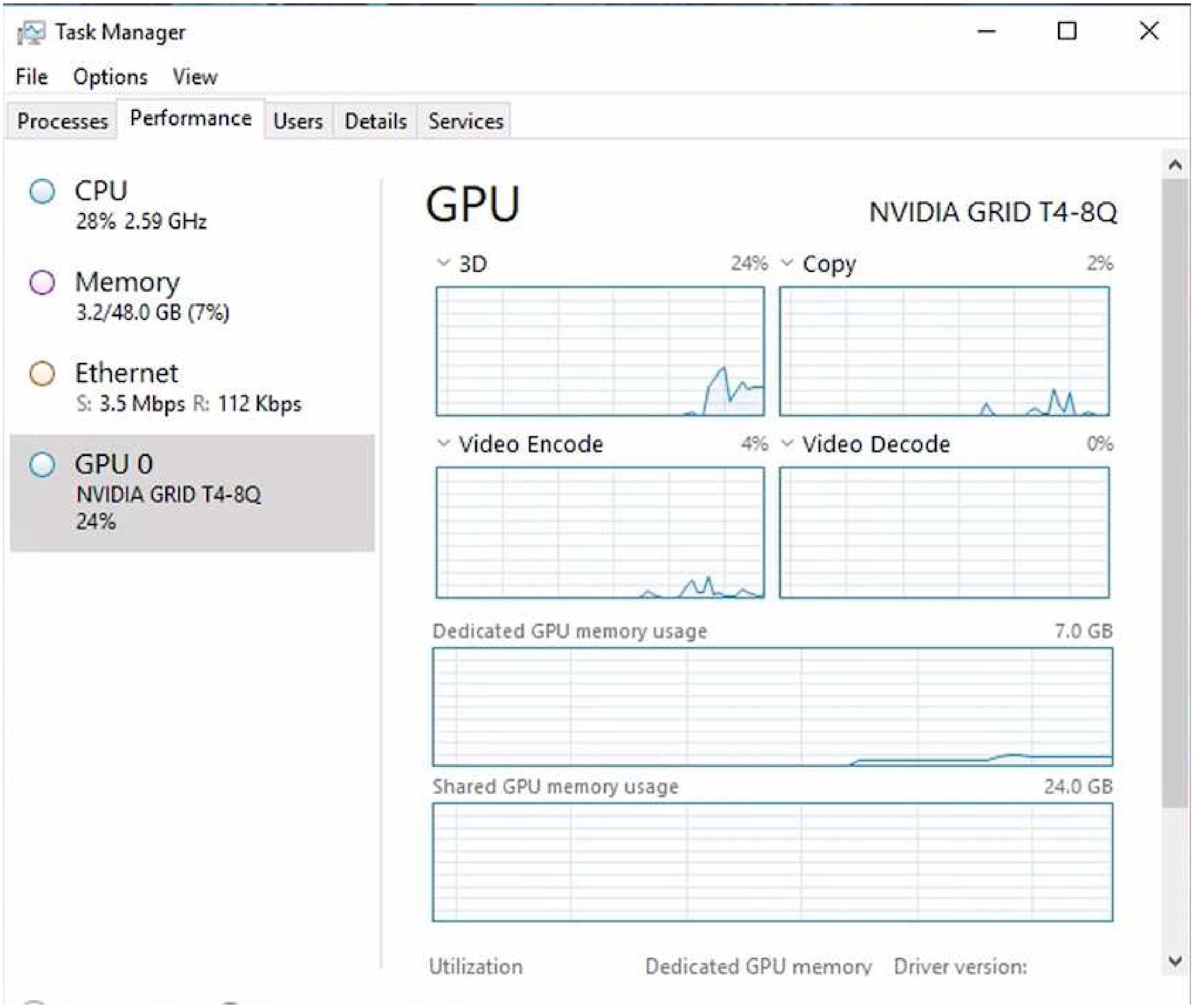
Close

To use the GPU, you must install the appropriate driver, which can be downloaded from the NVIDIA license portal. In an Azure environment, the NVIDIA driver is available as GPU driver extension. Next, the group policies in the following screenshot must be updated to use GPU hardware for remote desktop service sessions. You should prioritize H.264 graphics mode and enable encoder functionality.



Setting	State	Comment
RemoteFX for Windows Server 2008 R2		
Limit maximum color depth	Not configured	No
Enforce Removal of Remote Desktop Wallpaper	Not configured	No
Use hardware graphics adapters for all Remote Desktop Services sessions	Enabled	No
Limit maximum display resolution	Not configured	No
Limit number of monitors	Not configured	No
Remove "Disconnect" option from Shut Down dialog	Not configured	No
Remove Windows Security item from Start menu	Not configured	No
Use advanced RemoteFX graphics for RemoteApp	Not configured	No
Prioritize H.264/AVC 444 graphics mode for Remote Desktop Connections	Enabled	No
Configure H.264/AVC hardware encoding for Remote Desktop Connections	Enabled	No
Configure compression for RemoteFX data	Not configured	No
Configure image quality for RemoteFX Adaptive Graphics	Not configured	No
Enable RemoteFX encoding for RemoteFX clients designed for Windows Server 2008 R2 SP1	Not configured	No
Configure RemoteFX Adaptive Graphics	Not configured	No
Start a program on connection	Not configured	No
Always show desktop on connection	Not configured	No
Allow desktop composition for remote desktop sessions	Not configured	No
Do not allow font smoothing	Not configured	No

Validate GPU performance monitoring with Task Manager or by using the nvidia-smi CLI when running WebGL samples. Make sure that GPU, memory, and encoder resources are being consumed.



To make sure that the virtual machine is deployed to the NetApp HCI H615C with Virtual Desktop Service, define a site with the vCenter cluster resource that has H615C hosts. The VM template must have the required vGPU profile attached.

For shared multi-session environments, consider allocating multiple homogenous vGPU profiles. However, for high end professional graphics application, it is better to have each VM dedicated to a user to keep VMs isolated.

The GPU processor can be controlled by a QoS policy, and each vGPU profile can have dedicated frame buffers. However, the encoder and decoder are shared for each card. The placement of a vGPU profile on a GPU card is controlled by the vSphere host GPU assignment policy, which can emphasize performance (spread VMs) or consolidation (group VMs).

Solutions for Industry

Graphics workstations are typically used in industries such as manufacturing, healthcare, energy, media and entertainment, education, architecture, and so on. Mobility is often limited for graphics-intensive applications.

To address the issue of mobility, Virtual Desktop Services provide a desktop environment for all types of workers, from task workers to expert users, using hardware resources in the cloud or with NetApp HCI, including options for flexible GPU configurations. VDS enables users to access their work environment from anywhere with laptops, tablets, and other mobile devices.

To run manufacturing workloads with software like ANSYS Fluent, ANSYS Mechanical, Autodesk AutoCAD, Autodesk Inventor, Autodesk 3ds Max, Dassault Systèmes SOLIDWORKS, Dassault Systèmes CATIA, PTC Creo, Siemens PLM NX, and so on, the GPUs available on various clouds (as of Jan 2021) are listed in the following table.

GPU Model	Microsoft Azure	Google Compute (GCP)	Amazon Web Services (AWS)	On-Premises (NetApp HCI)
NVIDIA M60	Yes	Yes	Yes	No
NVIDIA T4	No	Yes	Yes	Yes
NVIDIA P100	No	Yes	No	No
NVIDIA P4	No	Yes	No	No

Shared desktop sessions with other users and dedicated personal desktops are also available. Virtual desktops can have one to four GPUs or can utilize partial GPUs with NetApp HCI. The NVIDIA T4 is a versatile GPU card that can address the demands of a wide spectrum of user workloads.
Each GPU card on NetApp HCI H615C has 16GB of frame buffer memory and three cards per server. The number of users that can be hosted on single H615C server depends on the user workload.

Users/Server	Light (4GB)	Medium (8GB)	Heavy (16GB)
H615C	12	6	3

To determine the user type, run the GPU profiler tool while users are working with applications performing typical tasks. The GPU profiler captures memory demands, the number of displays, and the resolution that users require. You can then pick the vGPU profile that satisfies your requirements.

Virtual desktops with GPUs can support a display resolution of up to 8K, and the utility nView can split a single monitor into regions to work with different datasets.

With ONTAP file storage, you can realize the following benefits:

- A single namespace that can grow up to 20PB of storage with 400 billion of files, without much administrative input
- A namespace that can span the globe with a Global File Cache
- Secure multitenancy with managed NetApp storage
- The migration of cold data to object stores using NetApp FabricPool
- Quick file statistics with file system analytics
- Scaling a storage cluster up to 24 nodes increasing capacity and performance
- The ability to control storage space using quotas and guaranteed performance with QoS limits
- Securing data with encryption
- Meeting broad requirements for data protection and compliance
- Delivering flexible business continuity options

Conclusion

The NetApp Virtual Desktop Service provides an easy-to-consume virtual desktop and application environment with a sharp focus on business challenges. By extending VDS with the on-premises ONTAP environment, you can use powerful NetApp features in a VDS environment, including rapid clone, in-line deduplication, compaction, thin provisioning, and compression. These features save storage costs and improve performance with all-flash storage. With VMware vSphere hypervisor, which minimizes server-provisioning time by using Virtual Volumes and vSphere API for Array integration. Using the hybrid cloud, customers can pick the right environment for their demanding workloads and save money. The desktop session running on-premises can access cloud resources based on policy.

Where to Find Additional Information

To learn more about the information that is described in this document, review the following documents and/or websites:

- NetApp Cloud
- NetApp VDS Product Documentation
- Connect your on-premises network to Azure with VPN Gateway
- Azure Portal
- Microsoft Windows Virtual Desktop
- Azure NetApp Files Registration

VMware Horizon

NVA-1132-DESIGN: VMware end-user computing with NetApp HCI

Suresh Thoppay, NetApp

VMware end-user computing with NetApp HCI is a prevalidated, best-practice data center architecture for deploying virtual desktop workloads at an enterprise scale. This document describes the architectural design and best practices for deploying the solution at production scale in a reliable and risk-free manner.

NVA-1132-DESIGN: VMware end-user computing with NetApp HCI

NVA-1129-DESIGN: VMware end-user computing with NetApp HCI and NVIDIA GPUs

Suresh Thoppay, NetApp

VMware end-user computing with NetApp HCI is a prevalidated, best-practice data center architecture for deploying virtual desktop workloads at an enterprise scale. This document describes the architectural design and best practices for deploying the solution at production scale in a reliable and risk-free manner.

NVA-1129-DESIGN: VMware end-user computing with NetApp HCI and NVIDIA GPUs

NVA-1129-DEPLOY: VMware end-user Computing with NetApp HCI and NVIDIA GPUs

Suresh Thoppay, NetApp

VMware end-user Computing with NetApp HCI is a prevalidated, best-practice, data center architecture for deploying virtual desktop workloads at an enterprise scale. This document describes how to deploy the solution at production scale in a reliable and risk-free manner

NVA-1129-DEPLOY: VMware end-user Computing with NetApp HCI and NVIDIA GPUs

NetApp HCI for virtual desktop infrastructure with VMware Horizon 7 - Empower your power users with 3D Graphics

Suresh Thoppay, NetApp

TR-4792 provides guidance on using the NetApp H615C compute node for 3D graphics workloads in a VMware Horizon environment powered by NVIDIA graphics processing units (GPUs) and virtualization software. It also provides the results from the preliminary testing of SPECviewperf 13 for the H615C.

NetApp HCI for virtual desktop infrastructure with VMware Horizon 7 - Empower your power users with 3D Graphics

FlexPod desktop virtualization solutions

Learn more about FlexPod virtualization solutions by reviewing the FlexPod design guides

Demos and Tutorials

Virtualization Videos and Demos

See the following videos and demos highlighting specific features of the hybrid cloud, virtualization, and container solutions.

NetApp ONTAP Tools for VMware vSphere

ONTAP Tools for VMware - Overview

VMware iSCSI Datastore Provisioning with ONTAP

VMware NFS Datastore Provisioning with ONTAP

SnapCenter Plug-in for VMware vSphere

NetApp SnapCenter software is an easy-to-use enterprise platform to securely coordinate and manage data protection across applications, databases, and file systems.

The SnapCenter Plug-in for VMware vSphere allows you to perform backup, restore, and attach operations for VMs and backup and mount operations for datastores that are registered with SnapCenter directly within VMware vCenter.

For more information about NetApp SnapCenter Plug-in for VMware vSphere, see the NetApp SnapCenter Plug-in for VMware vSphere Overview.

SnapCenter Plug-in for VMware vSphere - Solution Pre-Requisites

SnapCenter Plug-in for VMware vSphere - Deployment

SnapCenter Plug-in for VMware vSphere - Backup Workflow

SnapCenter Plug-in for VMware vSphere - Restore Workflow

SnapCenter - SQL Restore Workflow

3-2-1 Data Protection Solutions

3-2-1 data protection solutions combine on-premises primary and secondary backups, using SnapMirror technology, with replicated copies to object storage using BlueXP backup and recovery.

3-2-1 Data Protection for VMFS Datastores with SnapCenter Plug-in for VMware vSphere and BlueXP Backup and Recovery for Virtual Machines

VMware Cloud on AWS with AWS FSx for NetApp ONTAP

Windows Guest Connected Storage with FSx ONTAP using iSCSI

Linux Guest Connected Storage with FSx ONTAP using NFS

VMware Cloud on AWS TCO savings with Amazon FSx for NetApp ONTAP

VMware Cloud on AWS supplemental datastore w/ Amazon FSx for NetApp ONTAP

VMware HCX Deployment and Configuration Setup for VMC

vMotion Migration Demonstration with VMware HCX for VMC and FSxN

Cold Migration Demonstration with VMware HCX for VMC and FSxN

Azure VMware Services on Azure with Azure NetApp Files (ANF)

Azure VMware Solution supplemental datastore overview with Azure NetApp Files

Azure VMware Solution DR with Cloud Volumes ONTAP, SnapCenter and JetStream

Cold Migration Demonstration with VMware HCX for AVS and ANF

vMotion Demonstration with VMware HCX for AVS and ANF

Bulk Migration Demonstration with VMware HCX for AVS and ANF

VMware Cloud Foundation with NetApp ONTAP

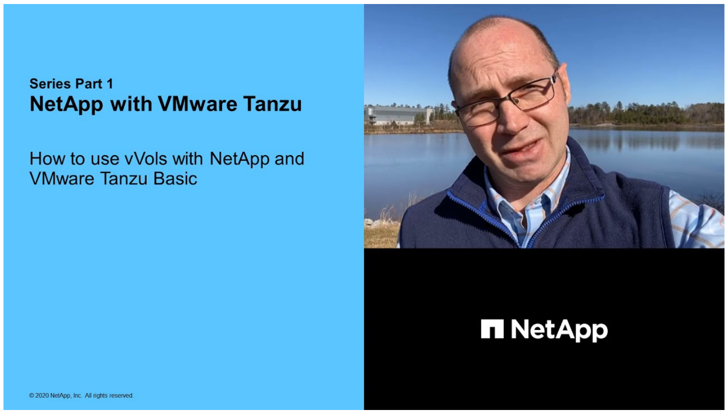
NFS Datastores as Principal Storage for VCF Workload Domains

iSCSI Datastores as Supplemental Storage for VCF Management Domains

NetApp with VMware Tanzu

VMware Tanzu enables customers to deploy, administer, and manage their Kubernetes environment through vSphere or the VMware Cloud Foundation. This portfolio of products from VMware allows customer to manage all their relevant Kubernetes clusters from a single control plane by choosing the VMware Tanzu edition that best suits their needs.

For more information about VMware Tanzu, see the VMware Tanzu Overview. This review covers use cases, available additions, and more about VMware Tanzu.



Series Part 1
NetApp with VMware Tanzu

How to use vVols with NetApp and VMware Tanzu Basic

© 2020 NetApp, Inc. All rights reserved.

How to use vVols with NetApp and VMware Tanzu Basic, part 1

Using vVols with
NetApp & VMware Tanzu Basic
Part 2

© 2020 NetApp, Inc. All rights reserved.

How to use vVols with NetApp and VMware Tanzu Basic, part 2

Using vVols with
NetApp & VMware Tanzu Basic
Part 3

© 2020 NetApp, Inc. All rights reserved.

How to use vVols with NetApp and VMware Tanzu Basic, part 3

NetApp Cloud Insights

NetApp Cloud Insights is comprehensive monitoring and analytics platform designed to provide visibility and control over your on-premises and cloud infrastructure.

NetApp Cloud Insights - Observability for the Modern Datacenter

Copyright information

Trademark information