



# VMware vSphere Foundation

## NetApp Solutions

NetApp  
August 30, 2024

# Table of Contents

- VMware vSphere Foundation ..... 1
- NFS 3.1 Reference Guide for vSphere 8 ..... 1
- VMware Virtual Volumes with ONTAP ..... 78
- Deployment Guide for VMFS ..... 99
- NetApp All-Flash SAN Array with VMware vSphere 8 ..... 121

# VMware vSphere Foundation

## NFS 3.1 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 3.1 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 3.1 VCF 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:

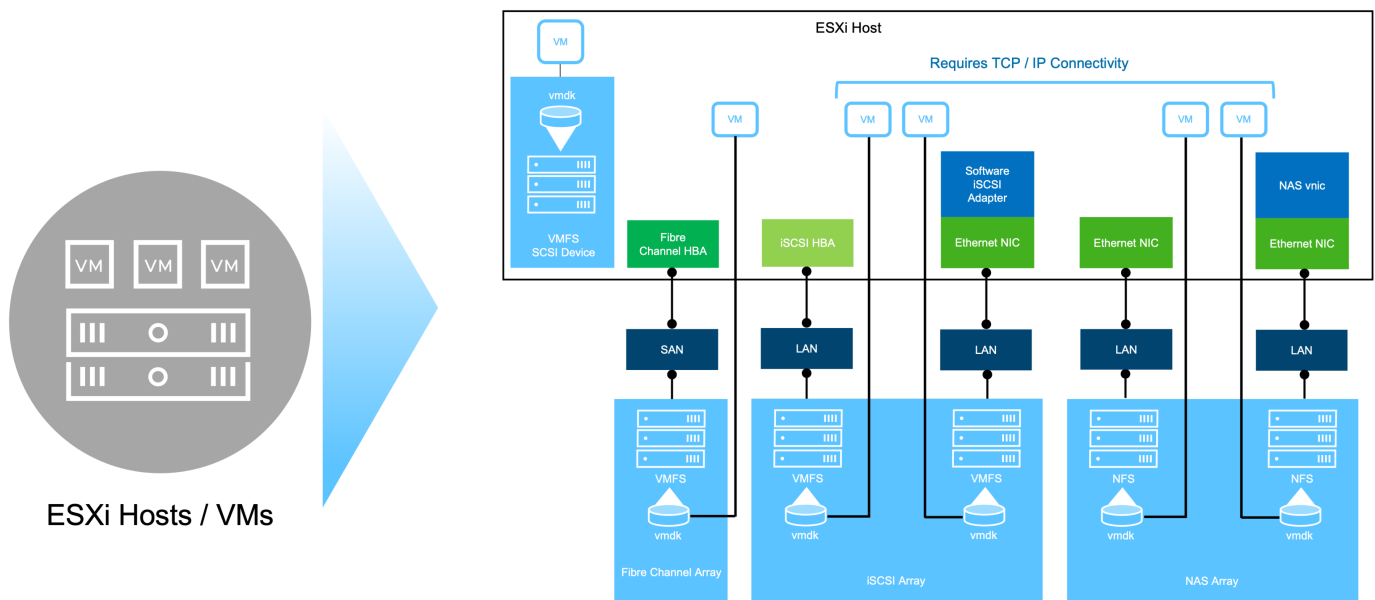
- VMware vSphere
- VMware vSAN
- Aria Standard
- VMware Tanzu Kubernetes Grid Service for vSphere
- vSphere Distributed Switch

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.

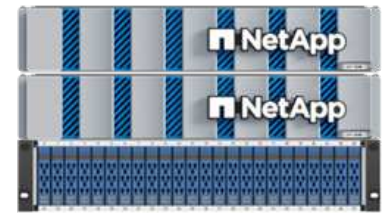
## AFF A70



## 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: [Ransomware 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.



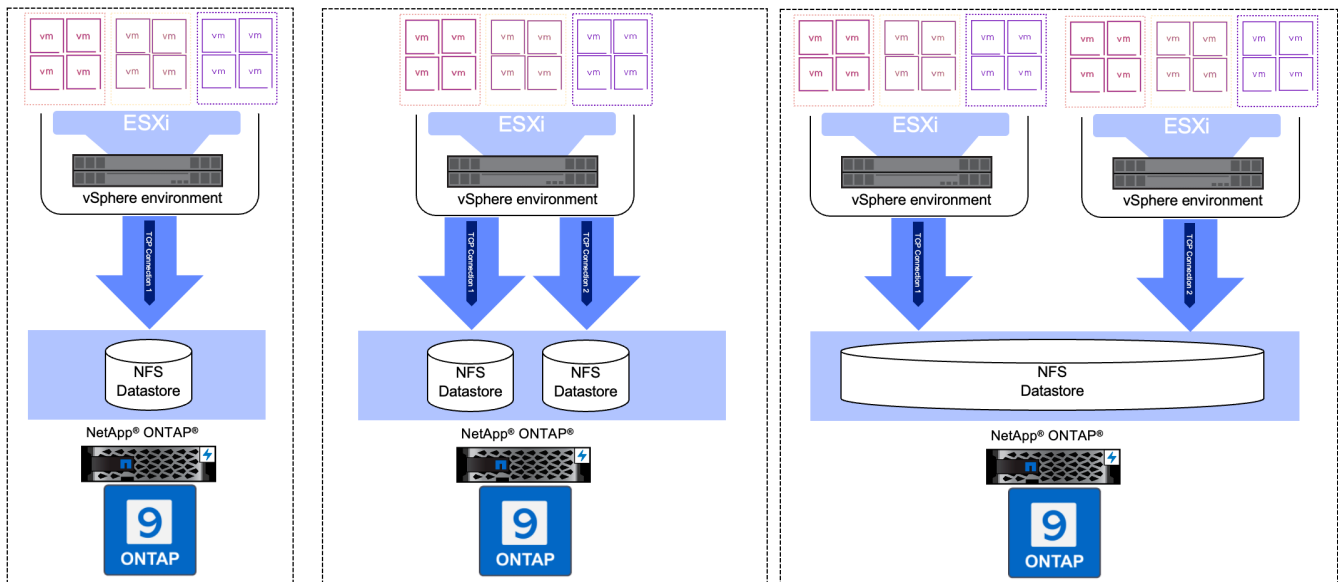
## Technical details

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) is created. 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.

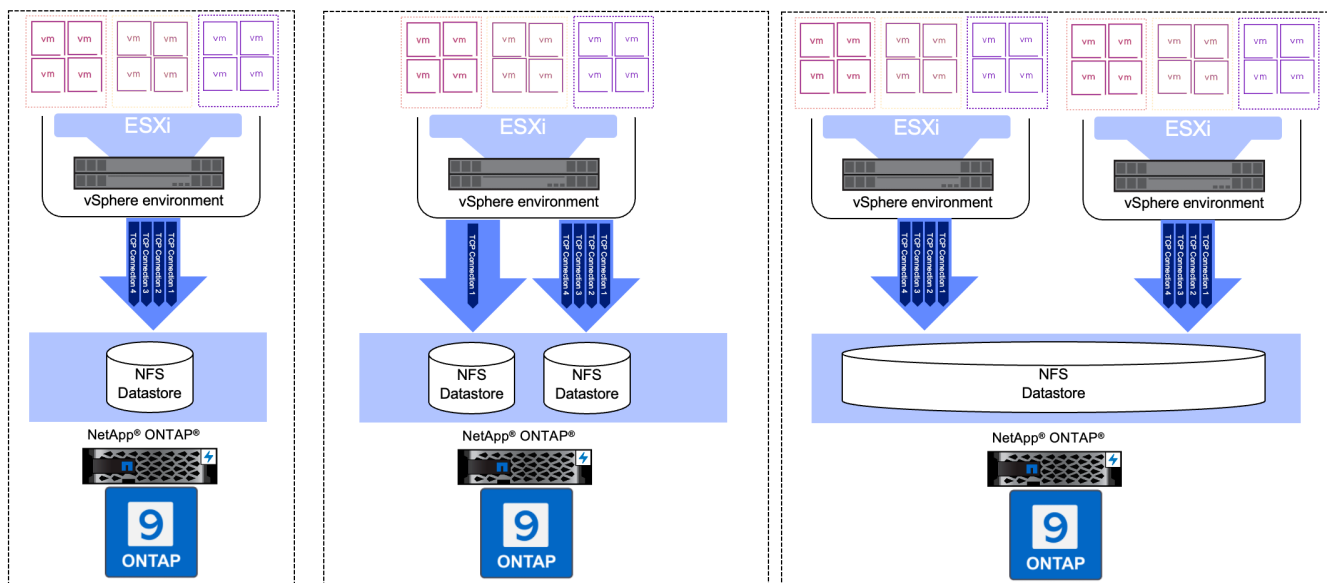
## Without nConnect feature with NetApp and VMware



### 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.

# With nConnect feature with NetApp and VMware



## 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
$nfSpec = New-Object VMware.Vim.HostNasVolumeSpec
$nfSpec.RemoteHost = "nfs_server.ontap.local"
$nfSpec.RemotePath = "/DS01"
$nfSpec.LocalPath = "DS01"
$nfSpec.AccessMode = "readWrite"
$nfSpec.Type = "NFS"
$nfSpec.Connections = 4
$datastoreSys.CreateNasDatastore ($nfSpec)

```

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 = 'XXXXXXXXXX'
$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 limits 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.

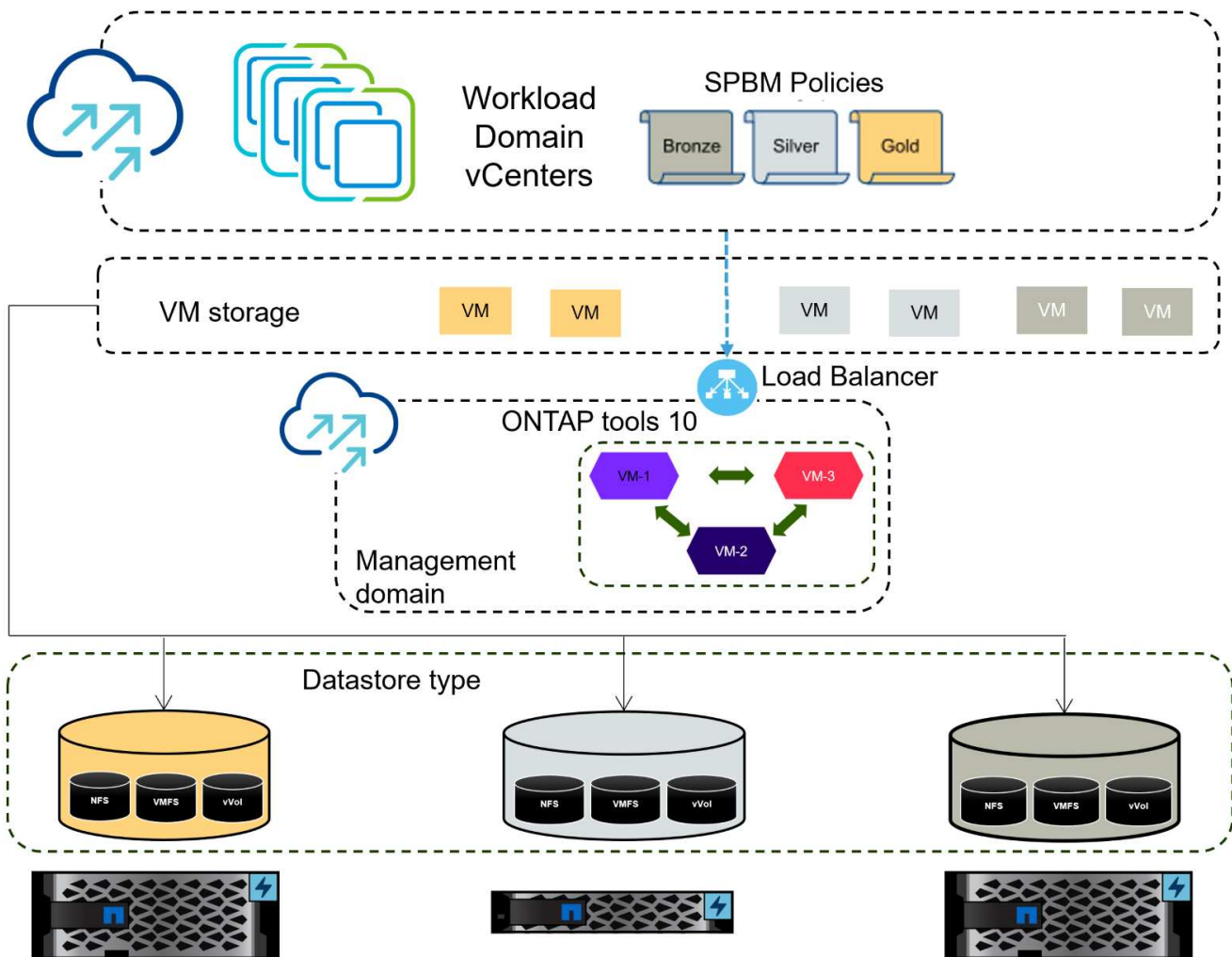
### Solution Overview

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:

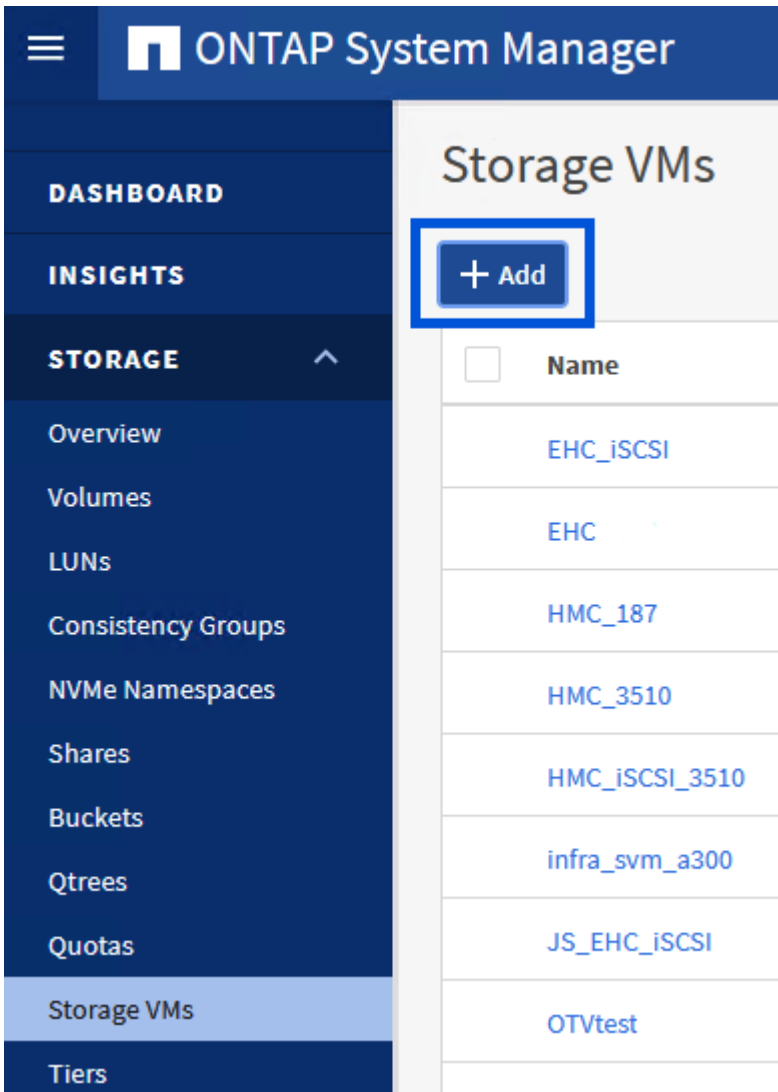
#### **Create SVM and LIFs on ONTAP storage system**

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

SMB/CIFS, NFS, S3 [iSCSI](#) [FC](#) [NVMe](#)

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

Save

Cancel

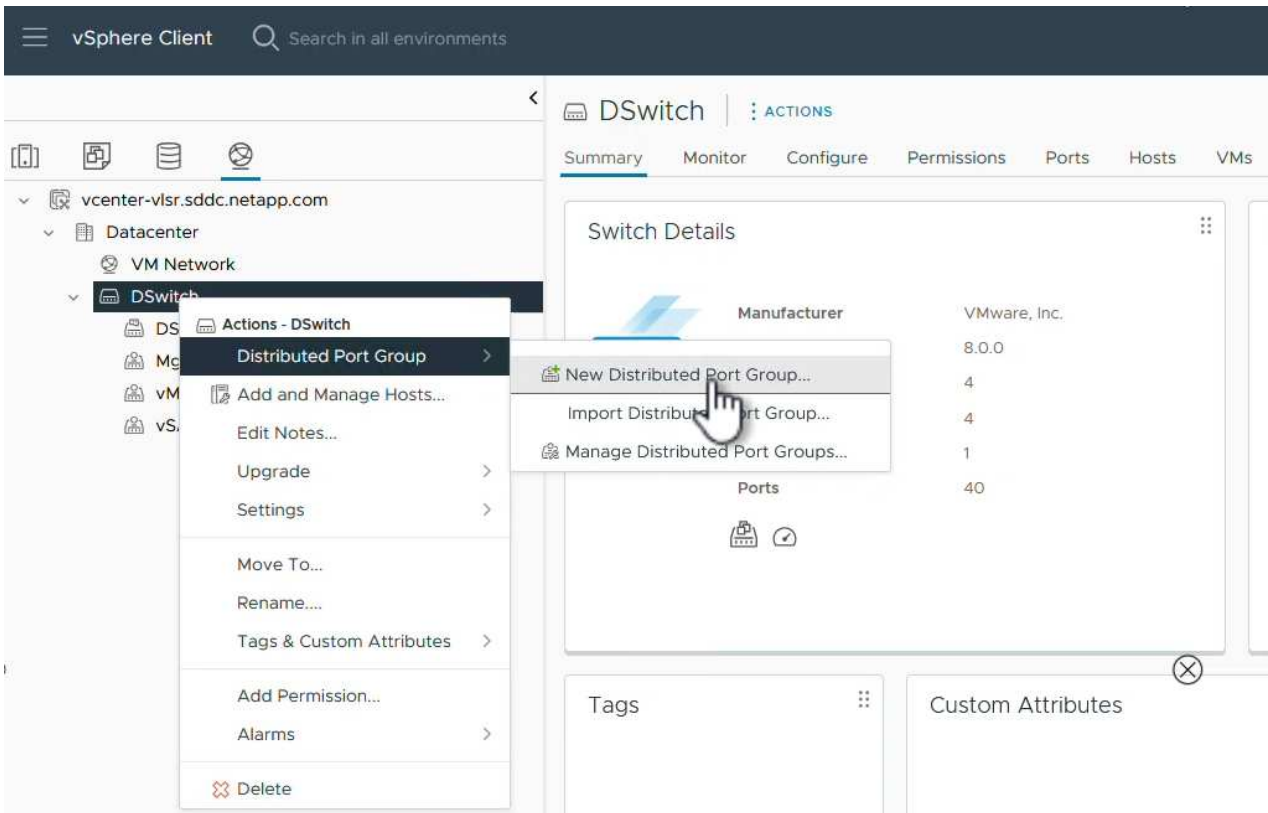
### Set up networking for NFS on ESXi hosts

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.

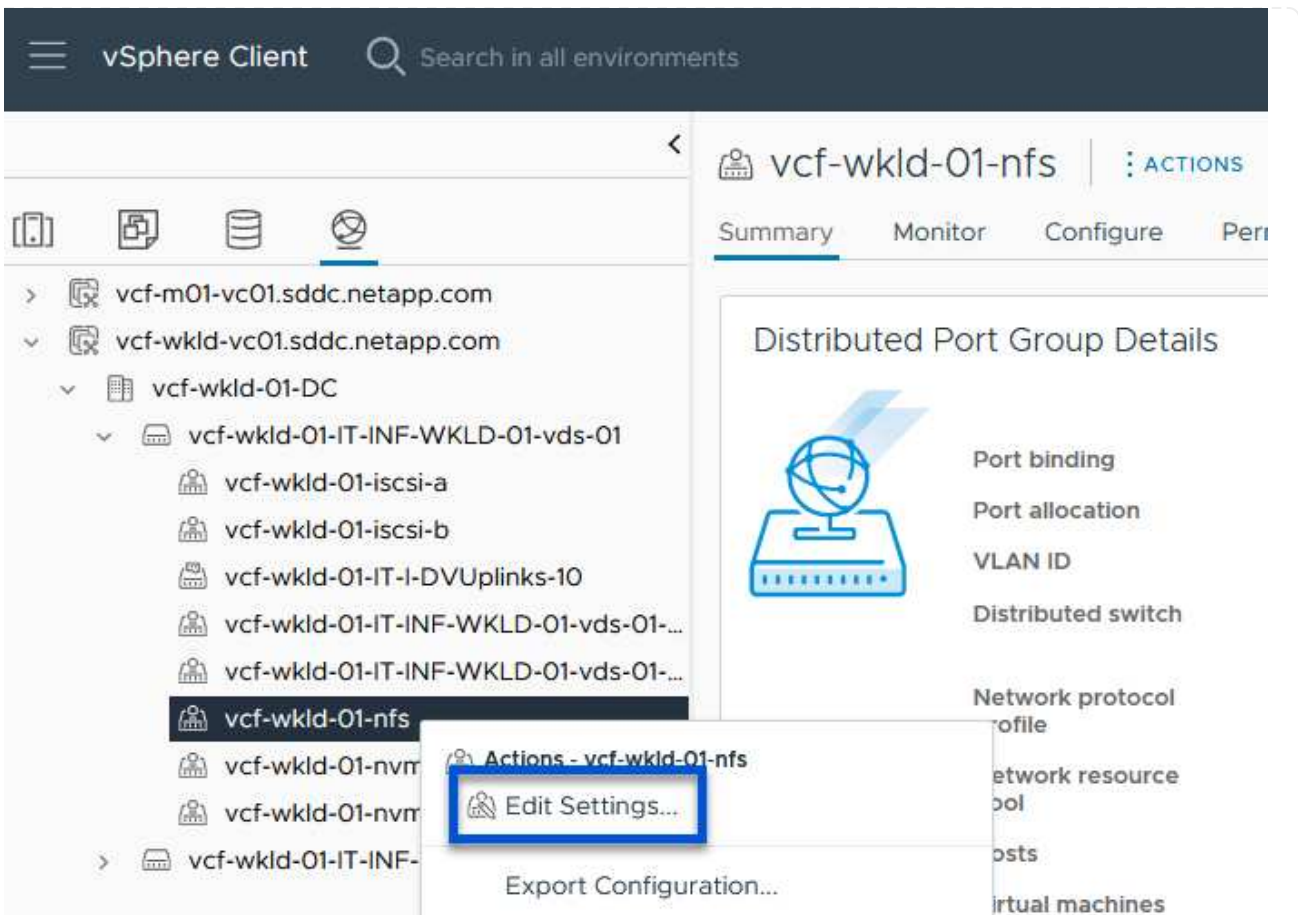
<b>Port binding</b>	Static binding
<b>Port allocation</b>	Elastic <span>?</span>
<b>Number of ports</b>	8
<b>Network resource pool</b>	(default)
<b>VLAN</b>	
<b>VLAN type</b>	VLAN
<b>VLAN ID</b>	3374
<b>Advanced</b>	
<input type="checkbox"/> Customize default policies configuration	

CANCEL

BACK

NEXT

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**.

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual port ▾

Network failure detection

Link status only ▾

Notify switches

Yes ▾

Failback

Yes ▾

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

Uplink 1

Uplink 2

Standby uplinks

Unused uplinks

CANCEL

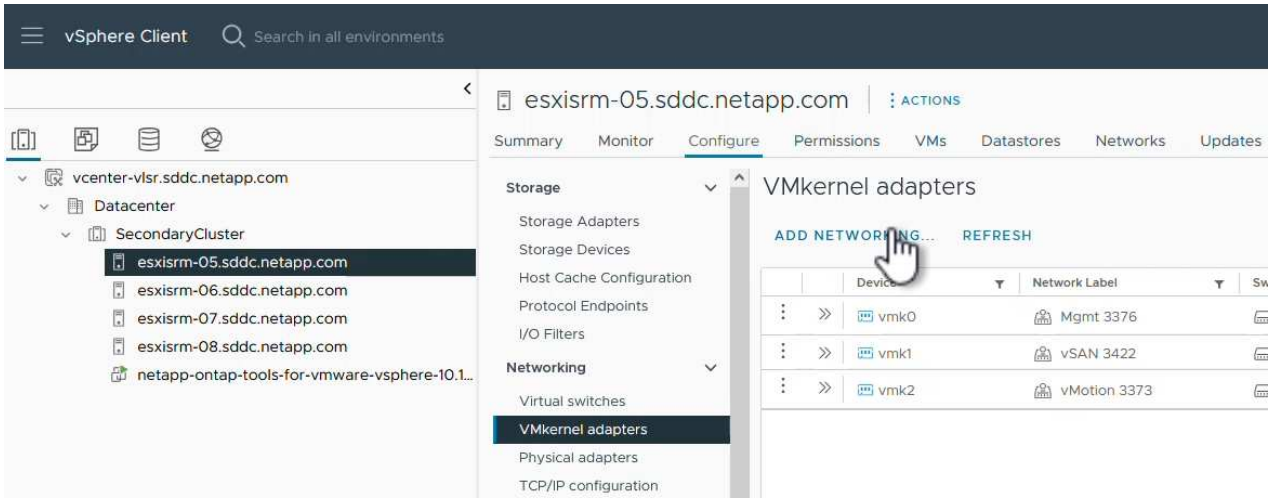
OK

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

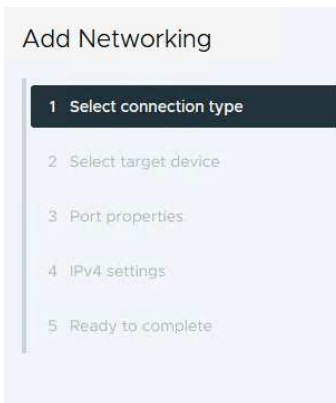
## Create a VMkernel adapter on each ESXi host

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.



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
<input type="radio"/>	Mgmt 3376	--	DSwitch
<input checked="" type="radio"/>	NFS 3374	--	DSwitch
<input type="radio"/>	vMotion 3373	--	DSwitch
<input type="radio"/>	vSAN 3422	--	DSwitch

Manage Columns 4 items

CANCEL

BACK

NEXT

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

Subnet mask

Default gateway  Override default gateway for this adapter

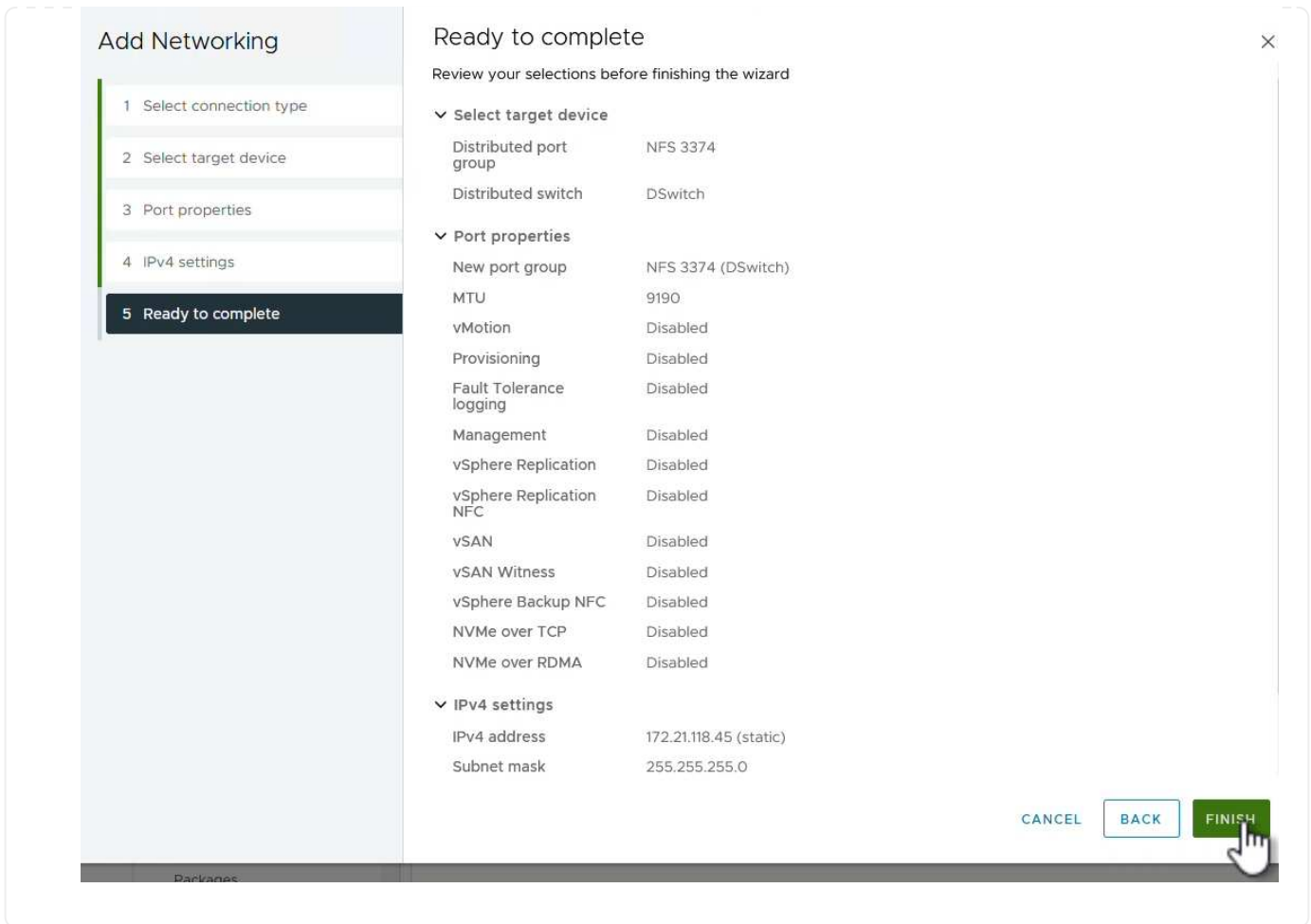
DNS server addresses

CANCEL

BACK

NEXT

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



## 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

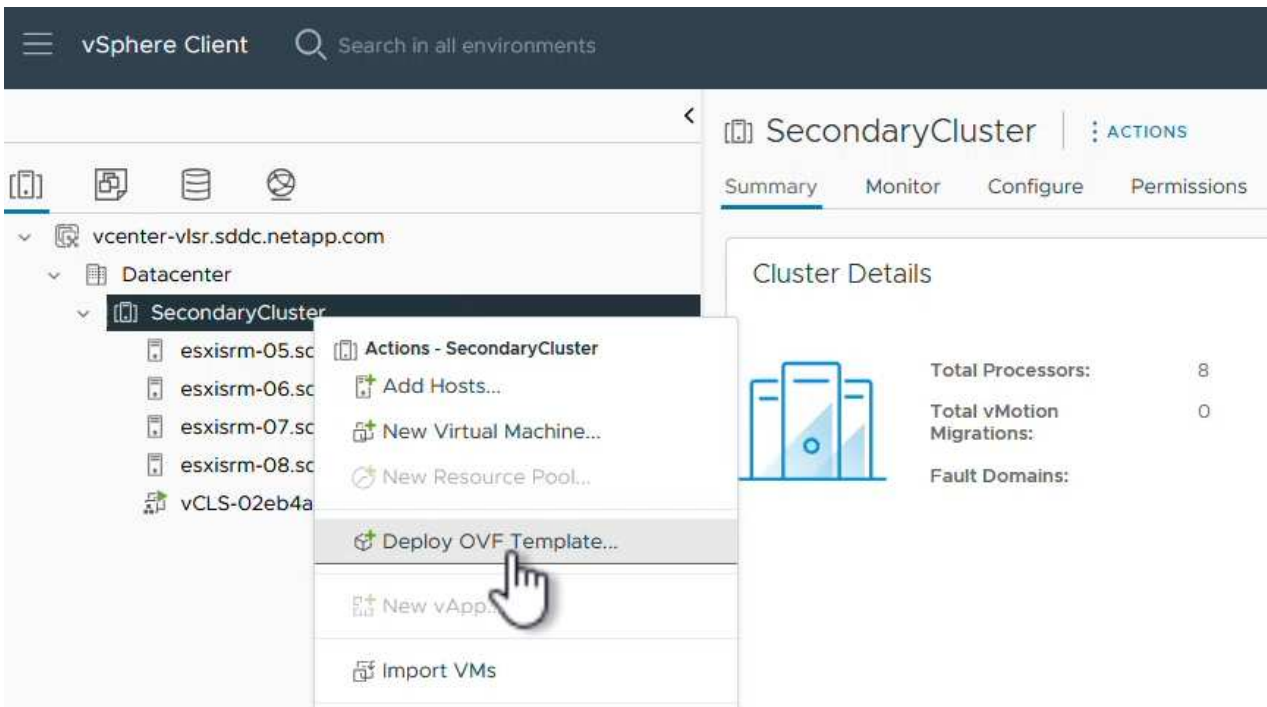
ONTAP tools for VMware vSphere 10 is deployed as a VM appliance and provides an integrated vCenter UI for managing ONTAP storage. ONTAP tools 10 features a new global management portal for managing connections to multiple vCenter servers and ONTAP storage backends.



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

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 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

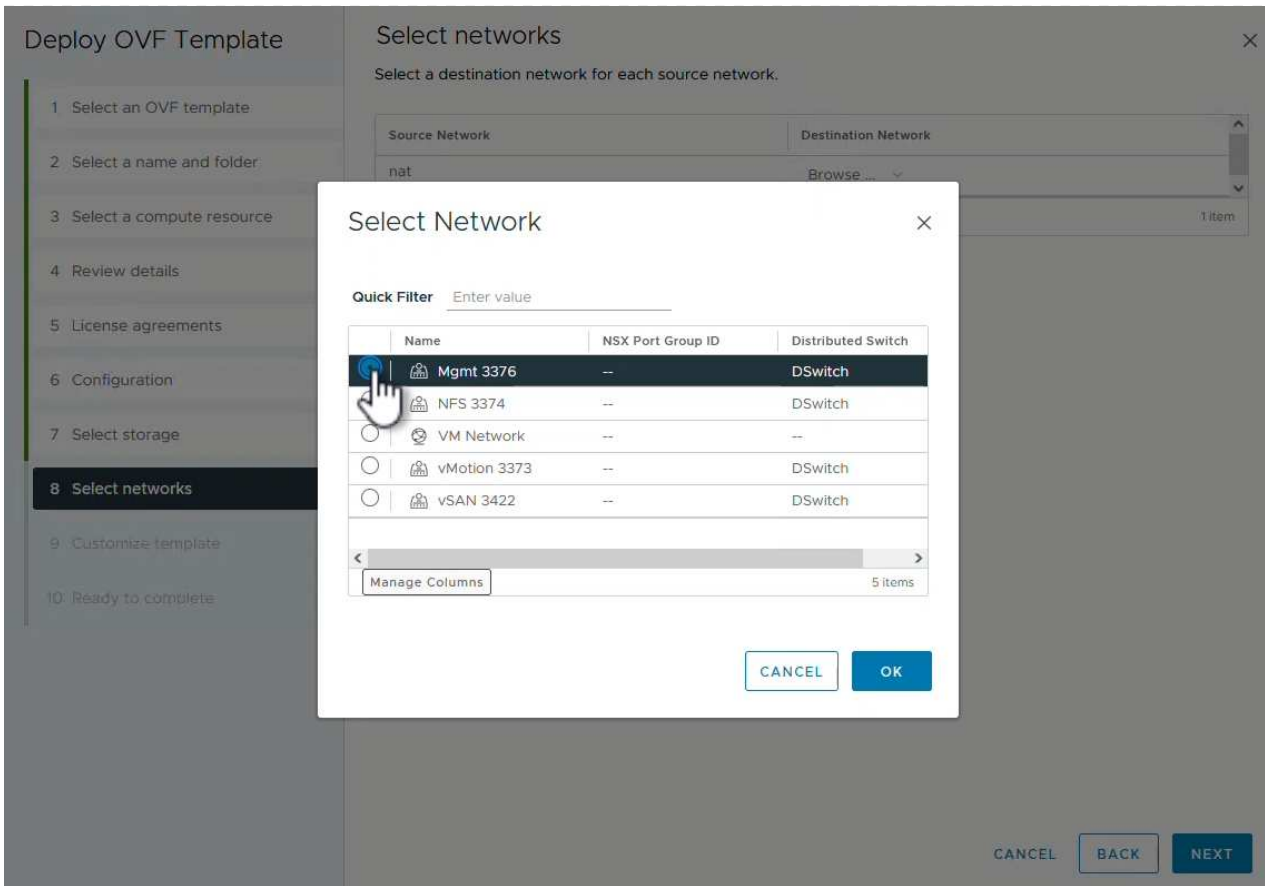
Disable Storage DRS for this virtual machine

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

Items per page 10 1 item

Compatibility

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



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

<input checked="" type="radio"/> Easy deployment (S)	<b>Description</b> Deploy local provisioner Non-HA Small single node instance of ONTAP tools	
<input type="radio"/> Easy deployment (M)		
<input type="radio"/> Advanced deployment (S)		
<input type="radio"/> Advanced deployment (M)		
<input type="radio"/> High-Availability deployment (S)		
<input type="radio"/> High-Availability deployment (M)		
<input type="radio"/> High-Availability deployment (L)		
<input type="radio"/> Recovery		
8 Items		

CANCEL

BACK

NEXT

### 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.

## 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

## Customize template

Customize the deployment properties of this software solution.

! 10 properties have invalid values X

System Configuration		8 settings
<b>Application username(*)</b>	Username to assign to the Application	<input type="text" value="vsphere-services"/>
<b>Application password(*)</b>	Password to assign to the Application	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
<b>Enable ASUP</b>	Select this checkbox to enable ASUP	<input checked="" type="checkbox"/>
<b>ASUP Proxy URL</b>	Proxy url ( in case if egress is blocked in datacenter side), through which we can push the asup bundle.	<input type="text"/>
<b>Administrator username(*)</b>	Username to assign to the Administrator. Please use only a letter as the beginning. And only '@', '_', '.', ':', '-' special characters are supported	<input type="text"/>
<b>Administrator password(*)</b>	Password to assign to the Administrator	<input type="password"/>

CANCEL BACK NEXT

## 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

## Customize template

<b>Maintenance user password(*)</b>	Password to assign to maint user account	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
Deployment Configuration		3 settings
<b>Load balancer IP(*)</b>	Load balancer IP (*)	<input type="text" value="172.21.120.57"/>
<b>Virtual IP for K8s control plane(*)</b>	Provide the virtual IP address for K8s control plane	<input type="text" value="172.21.120.58"/>
<b>Primary VM</b>	Maintain this field as selected to set the current VM as primary and install the ONTAP tools.	<input checked="" type="checkbox"/>
Node Configuration		10 settings
<b>HostName(*)</b>	Specify the hostname for the VM	<input type="text"/>
<b>IP Address(*)</b>	Specify the IP address for the appliance	<input type="text"/>
<b>IPv6 Address</b>	Specify the IPv6 address on the deployed network only when you need dual stack	<input type="text"/>

CANCEL BACK NEXT

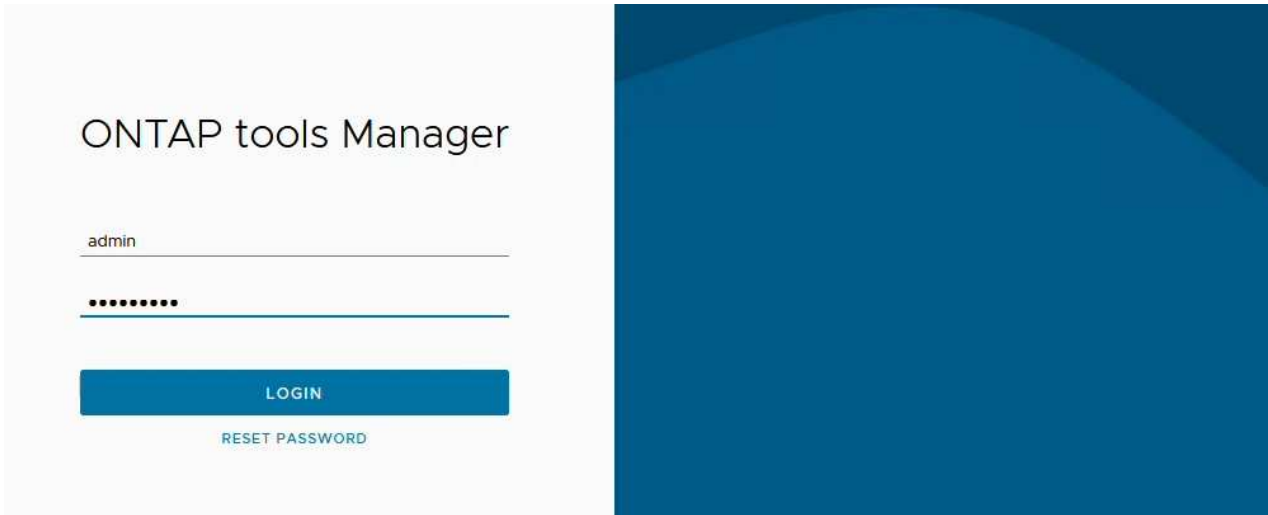
10. Review all information on the Ready to complete page and the click Finish to begin deploying the

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](#)



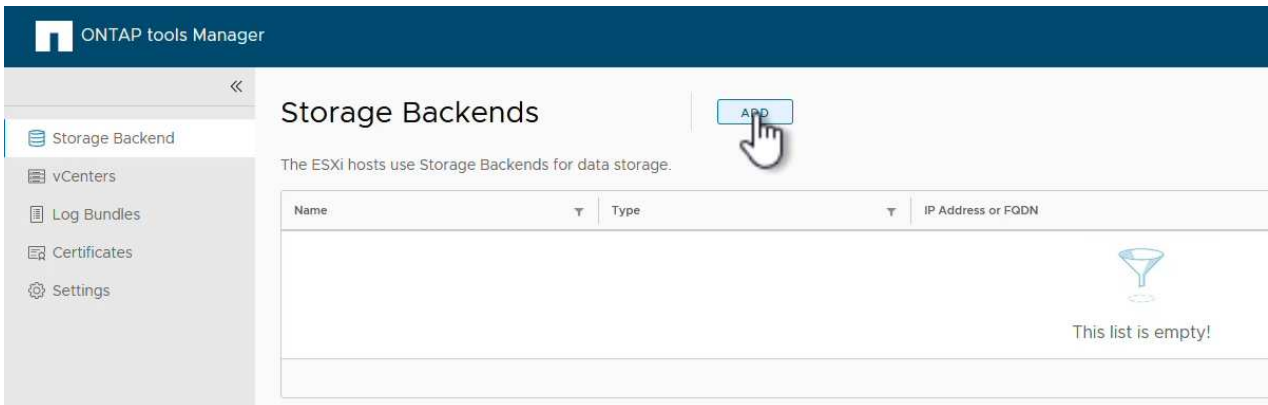
## Log Bundles

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.



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

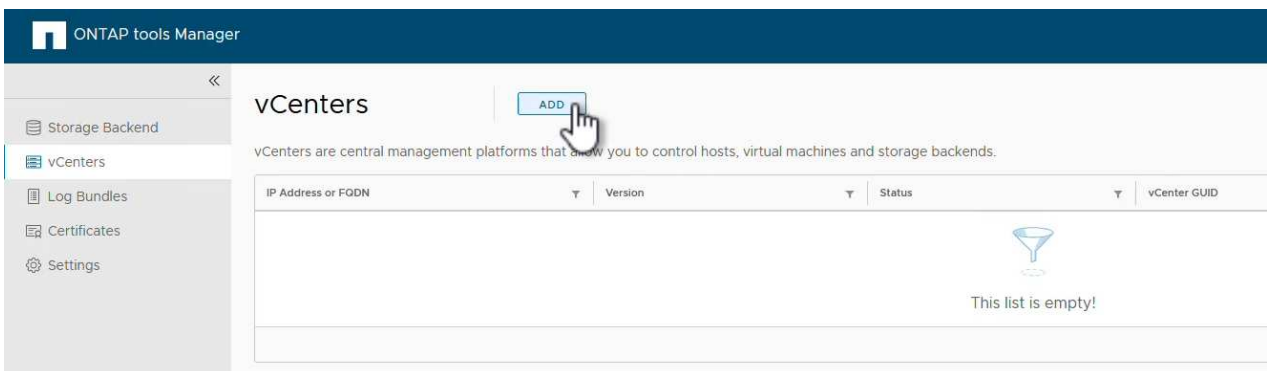
## Add Storage Backend

Hostname: *	172.16.9.25
Username: *	admin
Password: *	•••••••• 
Port: *	443

CANCEL

ADD 

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.



The screenshot shows the ONTAP tools Manager interface. The top navigation bar is dark blue with the ONTAP logo and the text "ONTAP tools Manager". On the left, a sidebar menu contains "Storage Backend", "vCenters" (highlighted), "Log Bundles", "Certificates", and "Settings". The main content area is titled "vCenters" and features a light blue "ADD" button with a hand cursor pointing to it. Below the title, a descriptive sentence reads: "vCenters are central management platforms that allow you to control hosts, virtual machines and storage backends." A table with columns "IP Address or FQDN", "Version", "Status", and "vCenter GUID" is shown, but it is empty. A blue funnel icon and the text "This list is empty!" are centered in the table area.

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



## Add vCenter

Server IP Address or FQDN: \*

Username: \*

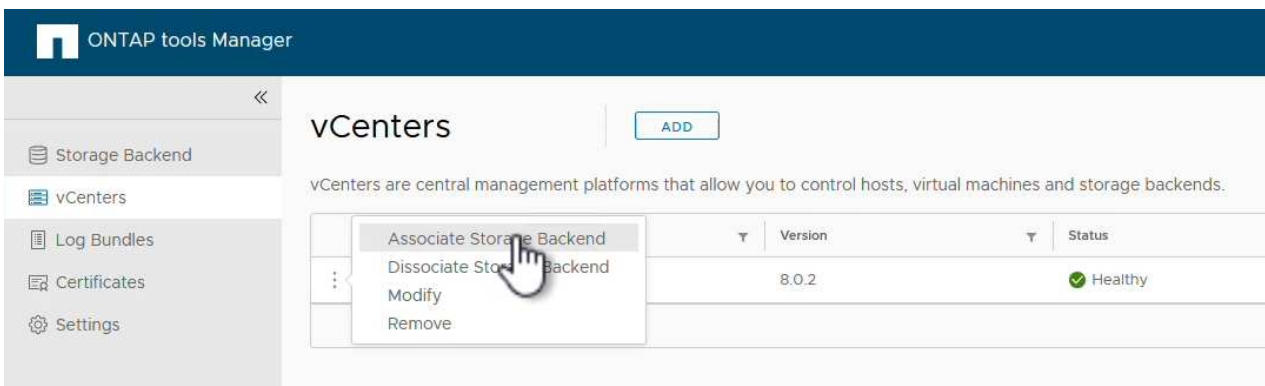
Password: \*  

Port: \*

CANCEL

ADD 


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



ONTAP tools Manager

vCenters

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

	Version	Status
 Associate Storage Backend Dissociate Storage Backend Modify Remove	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

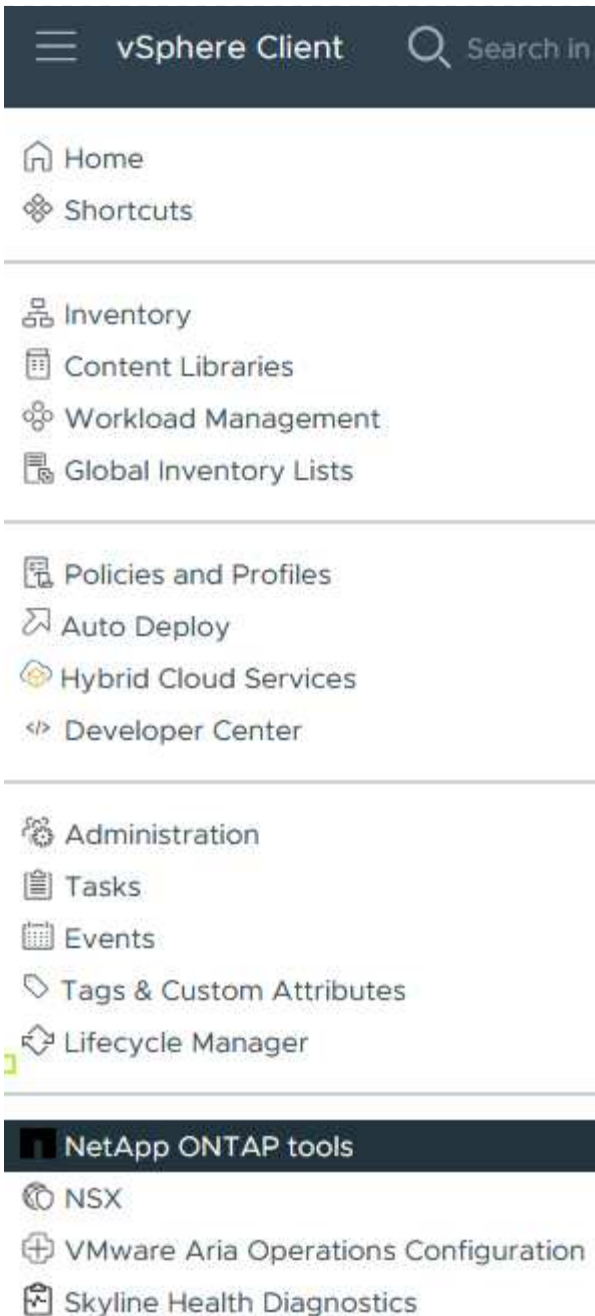


CANCEL

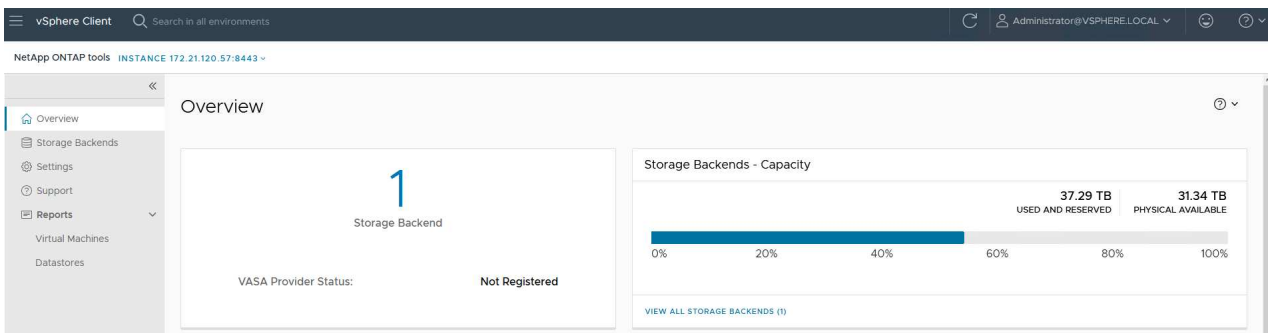
ASSOCIATE



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.

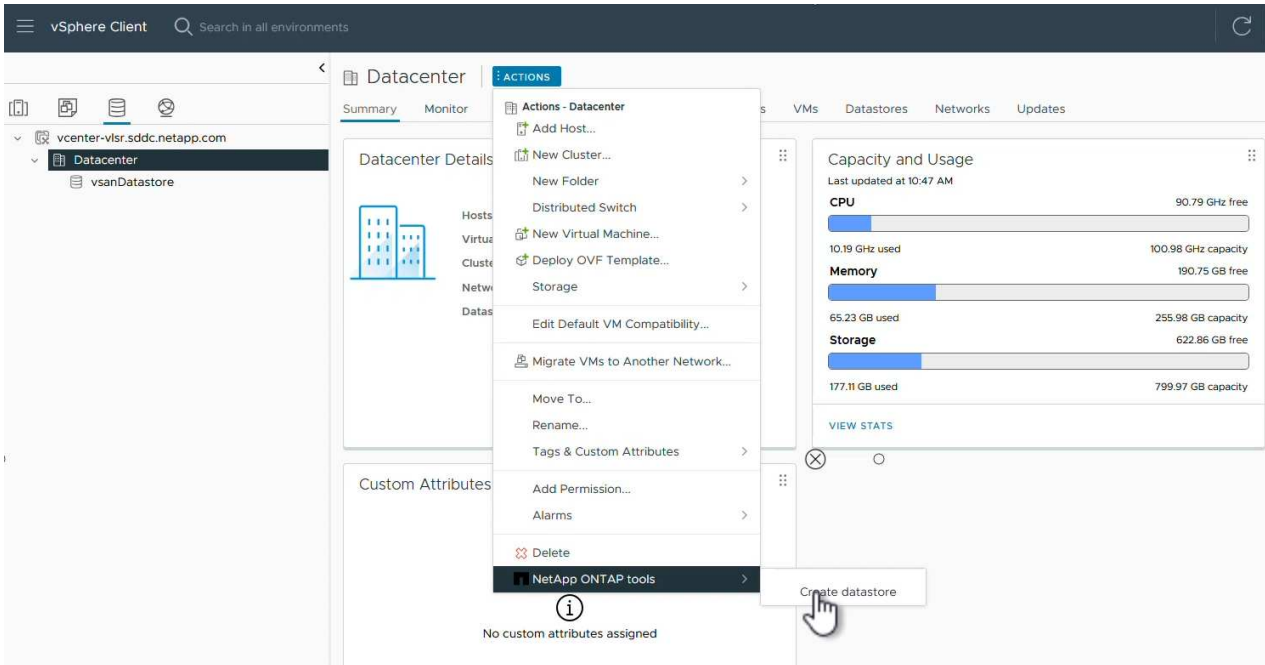




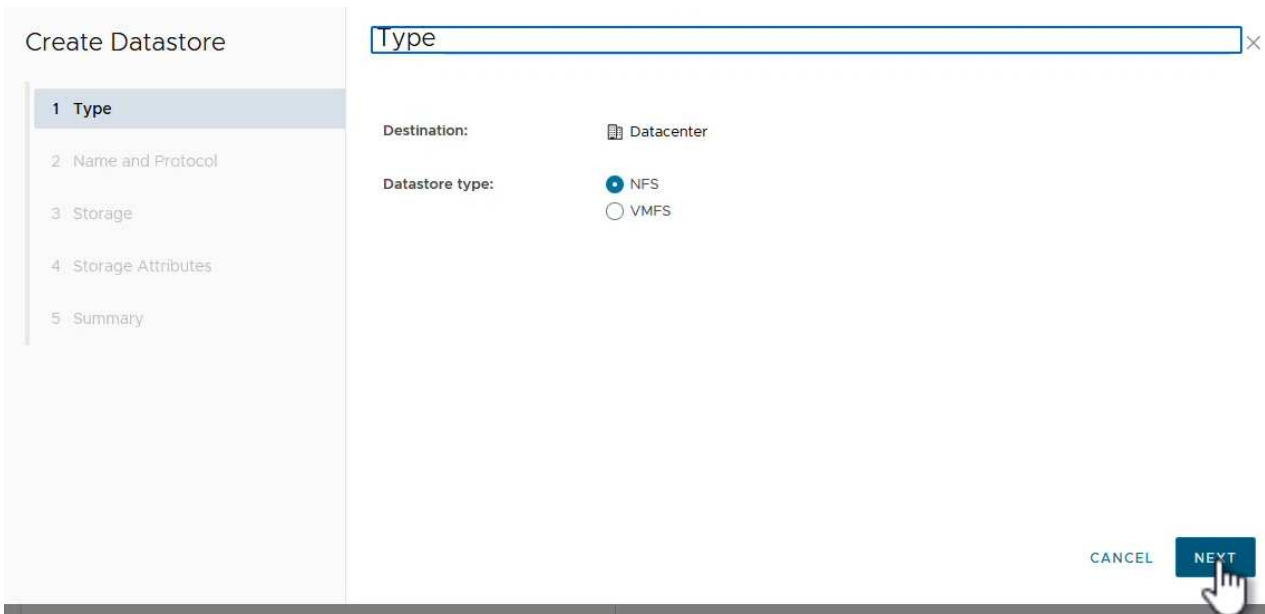
## Create an NFS datastore using ONTAP tools 10

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.



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:**

CANCEL

BACK

NEXT

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.

CANCEL

BACK

NEXT

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

- 1 Type
- 2 Name and Protocol
- 3 Storage
- 4 **Storage Attributes**
- 5 Summary

## 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**

CANCEL

BACK

NEXT

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

## Create Datastore

- 1 Type
- 2 Name and Protocol
- 3 Storage
- 4 Storage Attributes
- 5 **Summary**

## 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

CANCEL

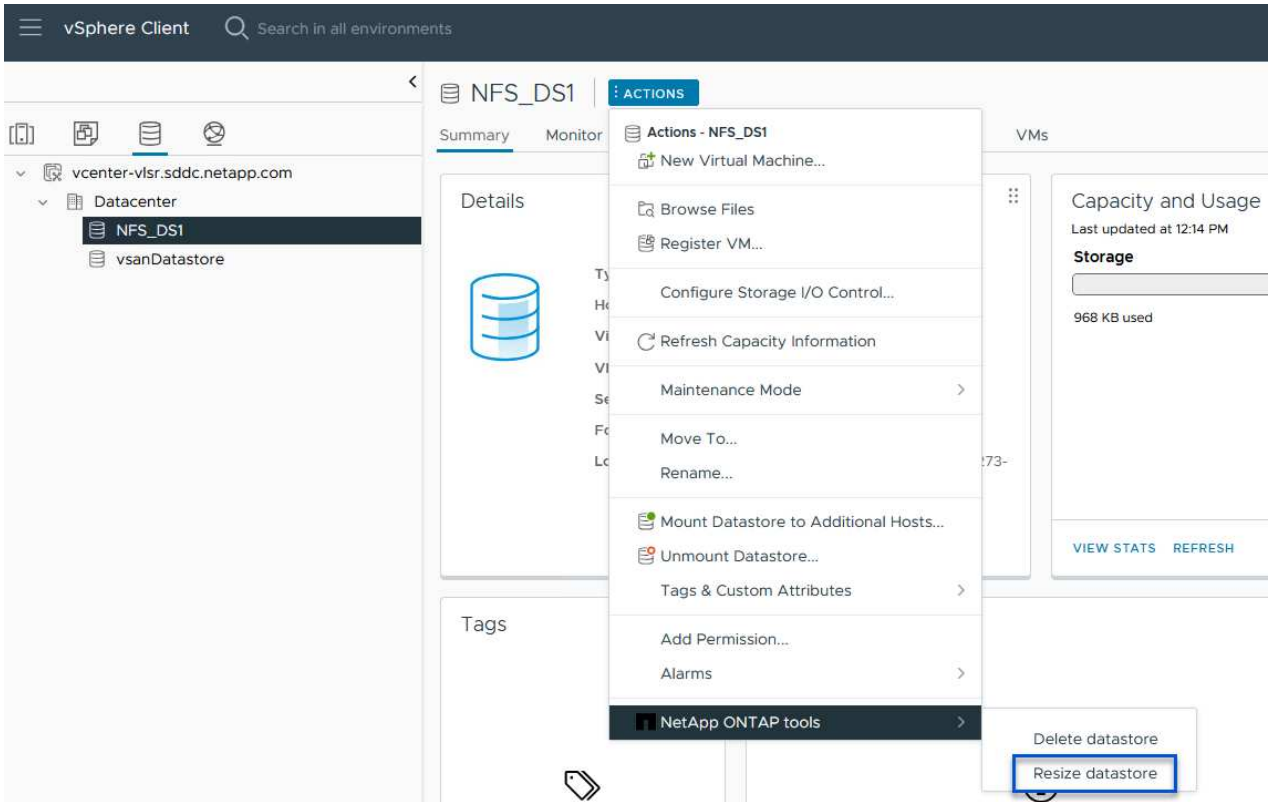
BACK

FINISH

## 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 <input type="text"/>

CANCEL

RESIZE

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

Recent Tasks		Alarms	
Task Name	Target	Status	Details
Expand Datastore	<a href="https://vcenter-vlsr.sddc.net/app.com">vcenter-vlsr.sddc.net app.com</a>	<div style="width: 100%; background-color: #0070c0; height: 10px;"></div> 100% <input checked="" type="checkbox"/>	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.

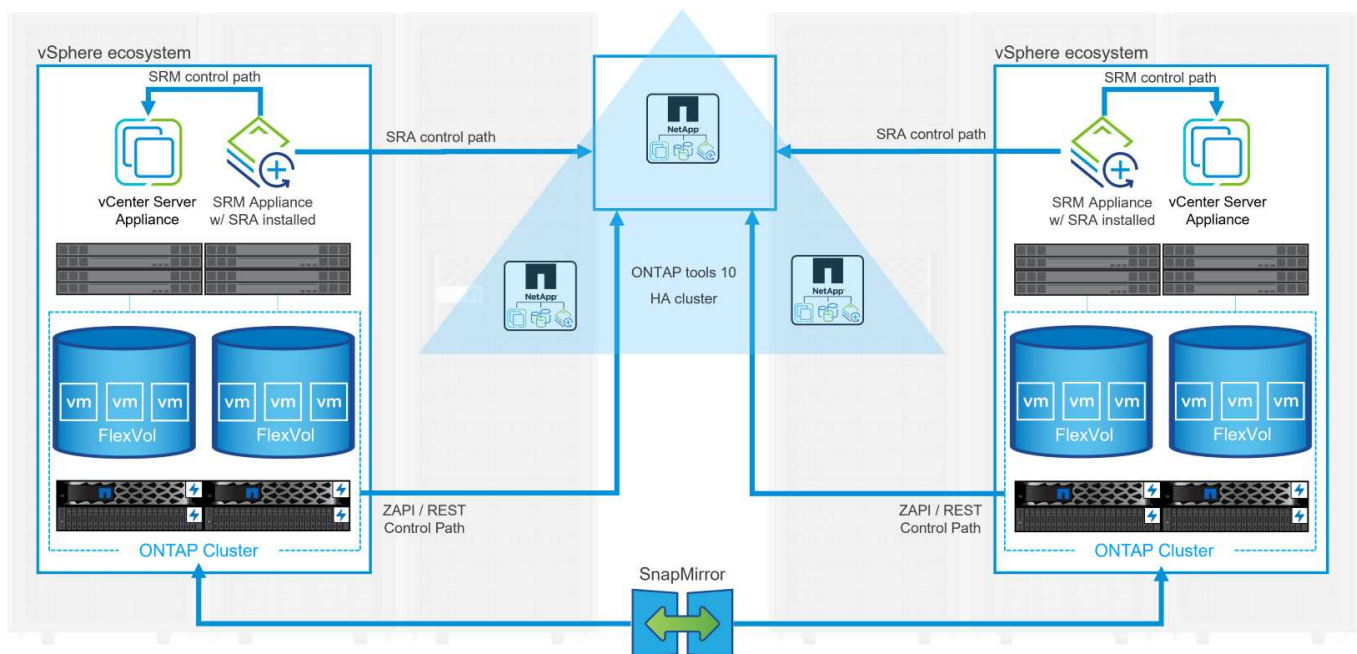
### Scenario Overview

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 Recovery 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.

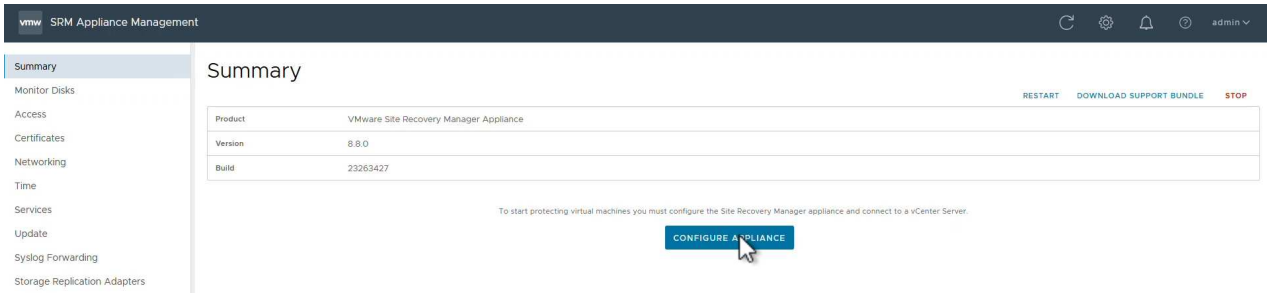
### Configure the SRM appliance

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

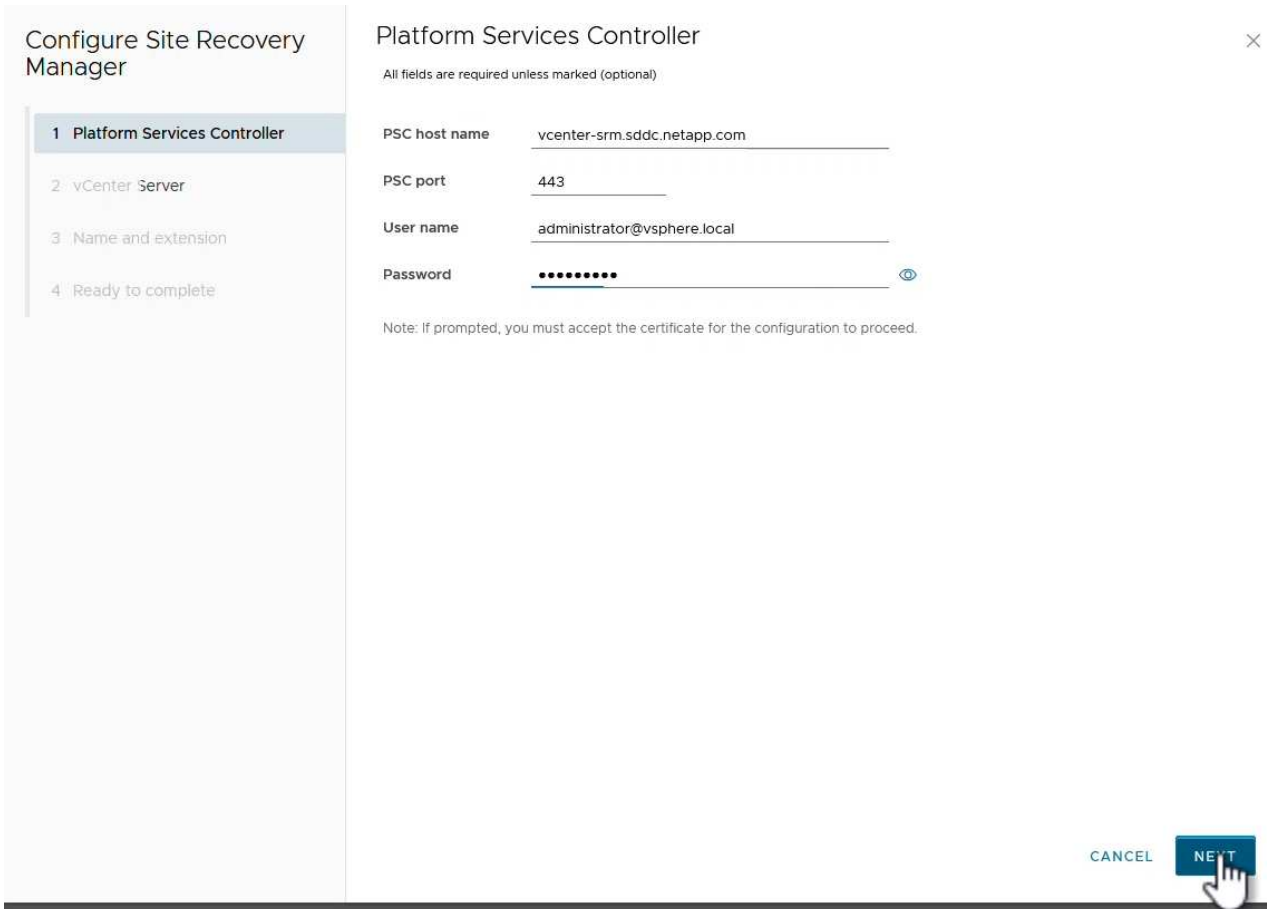
## Connect the SRM appliance for primary and secondary sites

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](https://<SRM_appliance_IP>:5480) and log in. Click on **Configure Appliance** to get started.



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.



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**

A unique display name for this Site Recovery Manager site.

**Administrator email**

An email address to use for system notifications.

**Local host**

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

Organization

Description

CANCEL

BACK

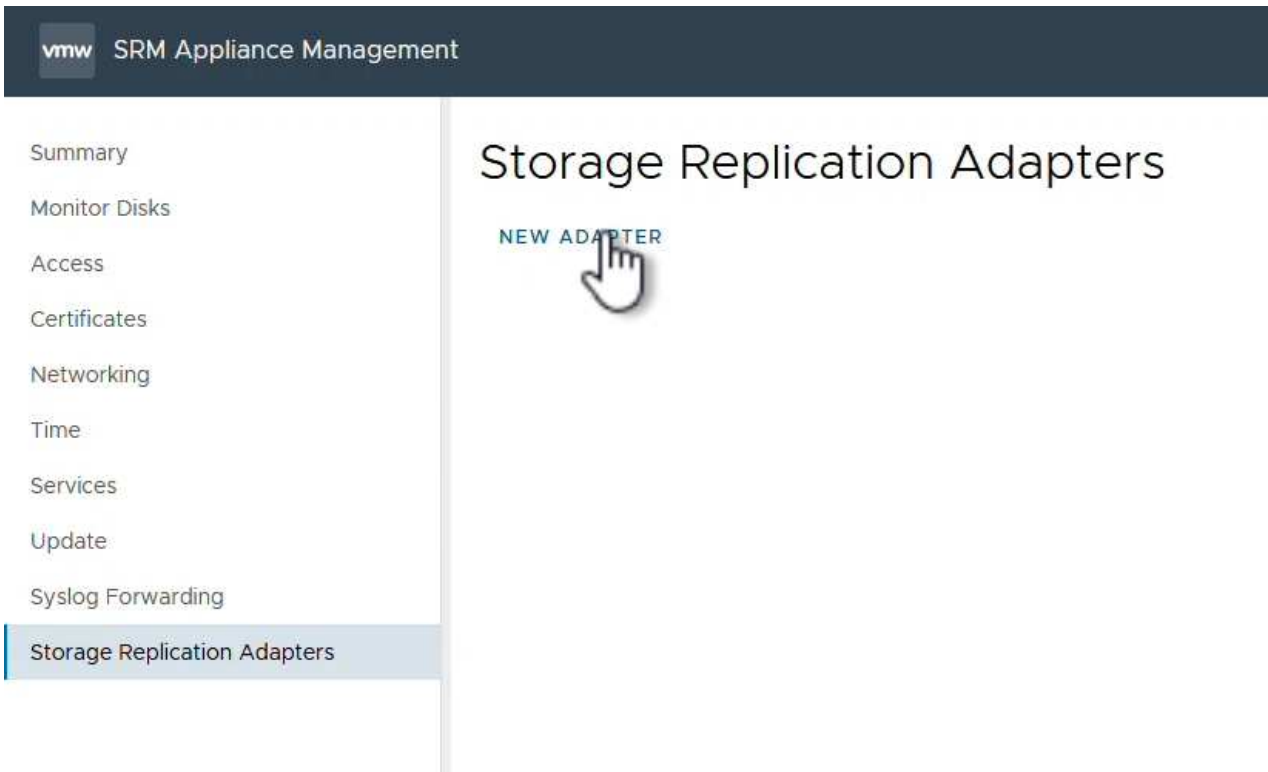
NEXT

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.

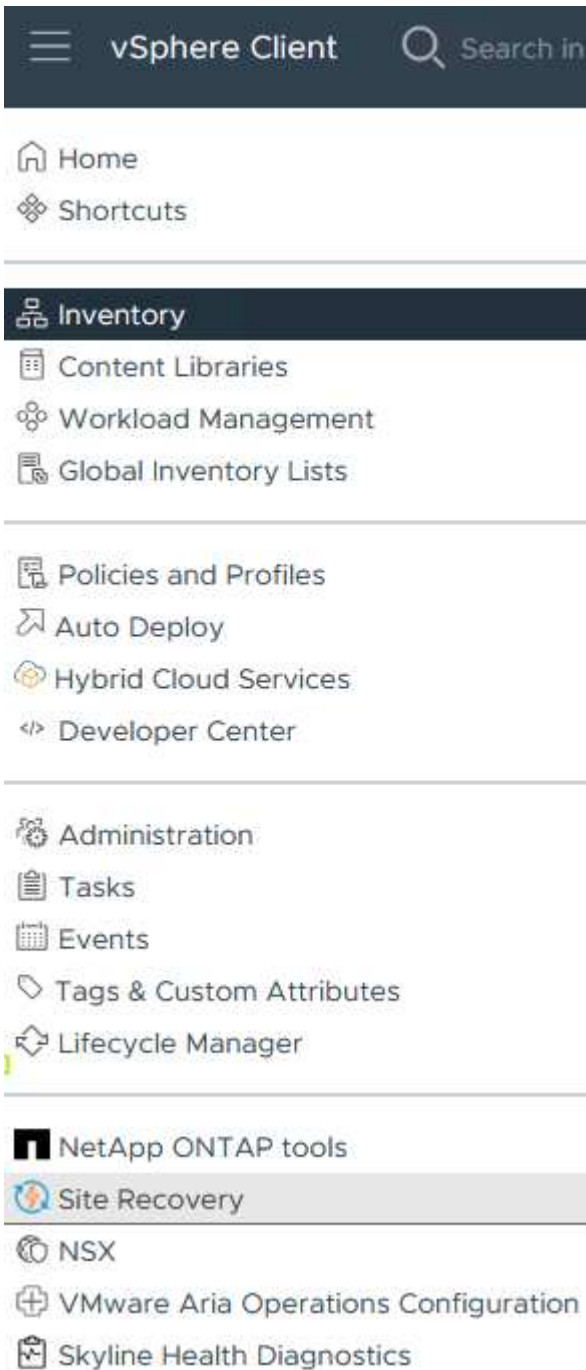
## Configure Site Recovery for SRM

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.

[NEW SITE PAIR](#)[Learn More](#)

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.

New Pair

1 Pair type

2 Peer vCenter Server

3 Services

4 Ready to complete

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

CANCEL NEXT

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.



## New Pair

1 Pair type

2 Peer vCenter Server

3 Services

4 Ready to complete

## Peer vCenter Server



All fields are required unless marked (optional)

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

PSC host name

PSC port

User name

Password

FIND VCENTER SERVER INSTANCES

Select a vCenter Server you want to pair.

vCenter Server

- vcenter-srm.sddc.netapp.com

CANCEL

BACK

NEXT

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

## New Pair

- 1 Pair type
- 2 Peer vCenter Server
- 3 Services
- 4 Ready to complete

## 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
<input checked="" type="checkbox"/> Site Recovery Manager (com.vmware.vc...	Site 1	Site 2

CANCEL

BACK

NEXT

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

RECONNECT

BREAK SITE PAIR



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

EXPORT/IMPORT SRM CONFIGURATION

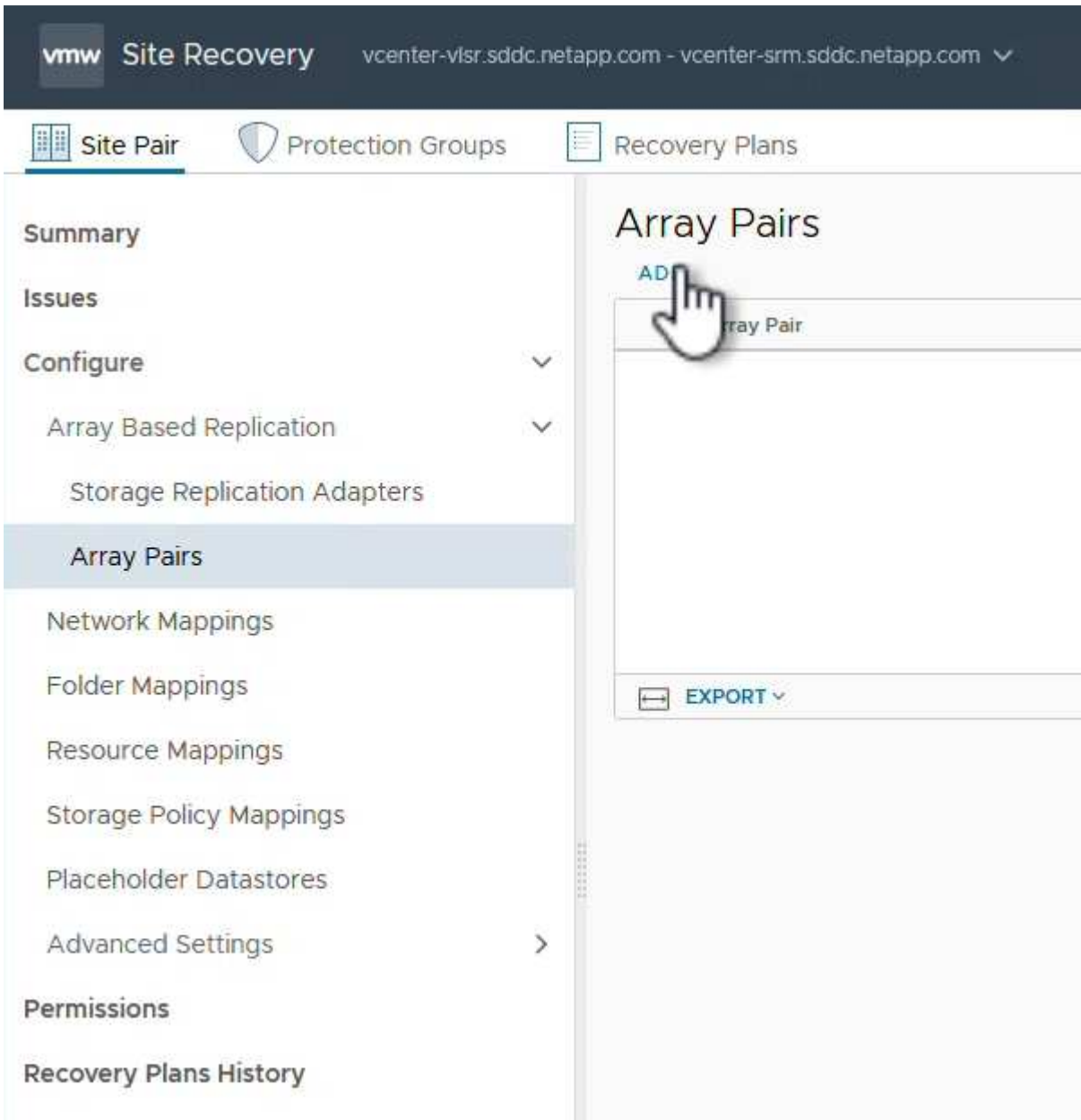
Protection Groups: 0 Recovery Plans: 0

Name	Site 1 <a href="#">RENAME</a>	Site 2 <a href="#">RENAME</a>
Server	srm-site1.sddc.netapp.com:443 <a href="#">ACTIONS</a>	srm-site2.sddc.netapp.com:443 <a href="#">ACTIONS</a>
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

CANCEL

NEXT

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.

## Add Array Pair

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

## 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":

### Storage Array Parameters

Storage System connection parameters

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

**Storage Virtual Machine(SVM) Name**   
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.

CANCEL

BACK

NEXT

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

## Add Array Pair

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

## 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.

CANCEL

BACK

NEXT 

5. On the **Array pairs** page, select the array pairs to enable 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

## Array pairs

Select the array pairs to enable:

<input checked="" type="checkbox"/>	vcenter-vlsr.sddc.netapp.com	vcenter-srm.sddc.netapp.com	Status
<input checked="" type="checkbox"/>	ontap-source:SQL_NFS (Array_1)	ontap-destination:SRM_NFS (Array_2)	Ready to be enabled

1 1 items

CANCEL

BACK

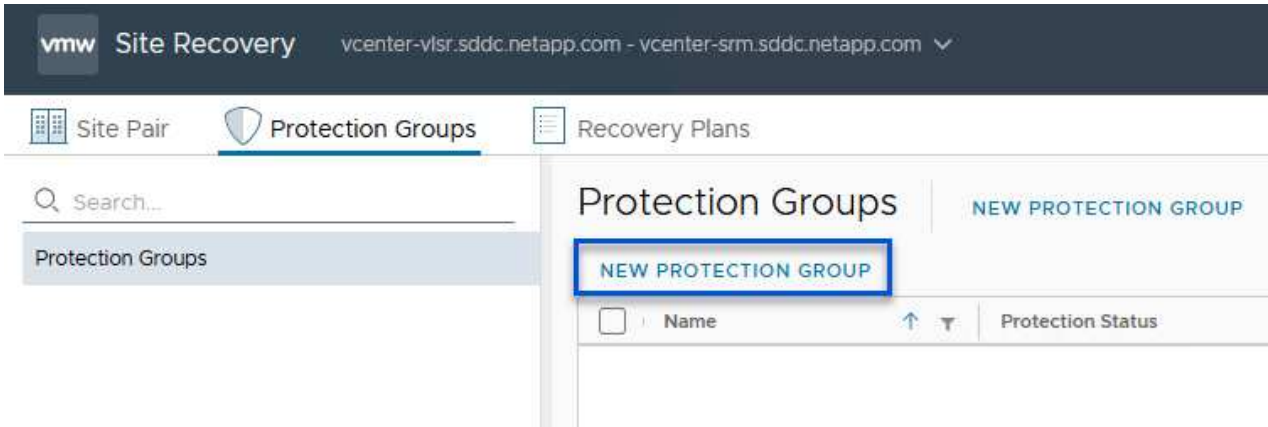
NEXT

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

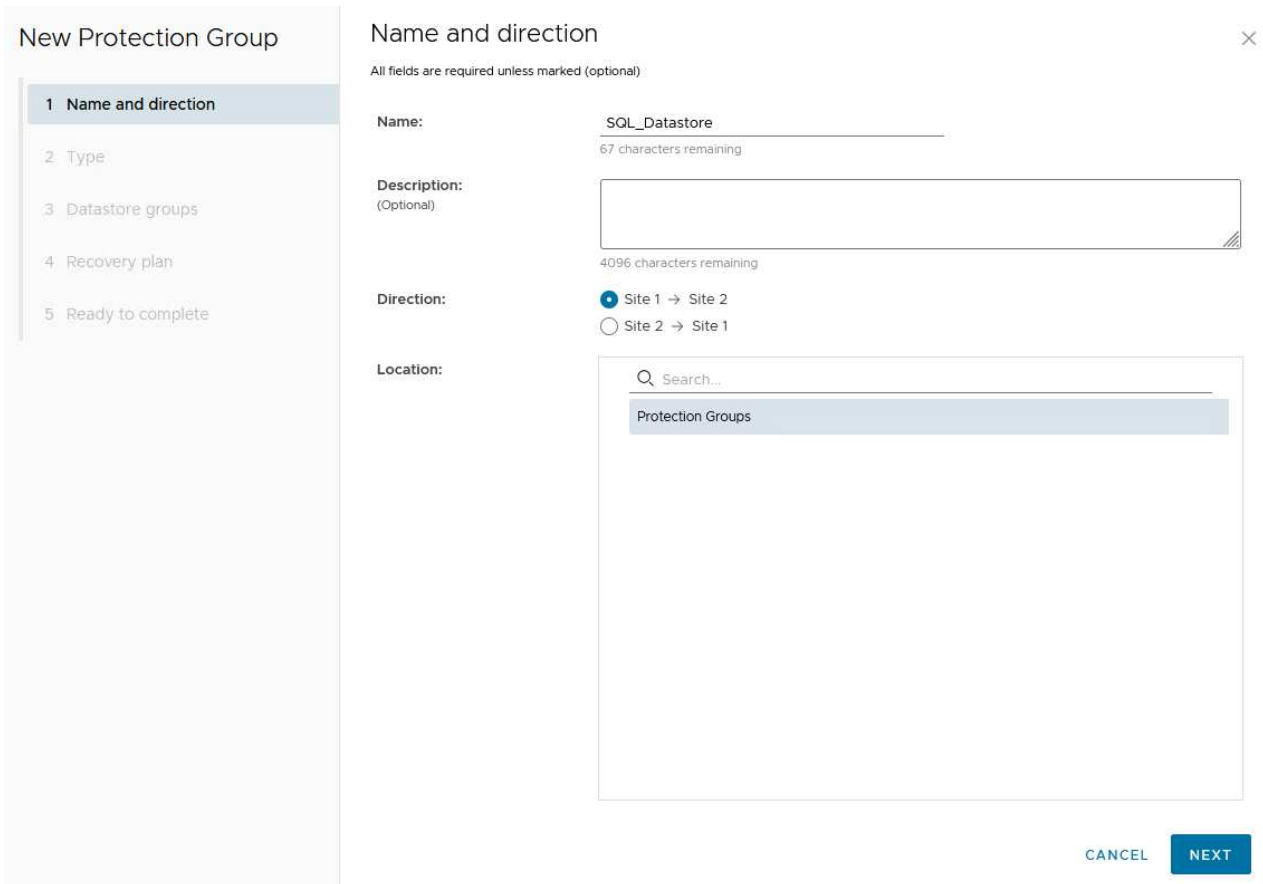
## Configure Protection Groups for SRM

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.





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
<input checked="" type="radio"/> ✓ ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2	nfs_array1 ↔ nfs_Array2
<input type="radio"/> ✓ ontap-source:SQL_NFS ↔ ontap-destination:SRM_NFS	Array_1 ↔ Array_2

Items per page: AUTO 2 array pairs

[CANCEL](#) [BACK](#) [NEXT](#)

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.

[SELECT ALL](#) [CLEAR SELECTION](#)

<input checked="" type="checkbox"/>	Datastore Group	Status
<input checked="" type="checkbox"/>	NFS_DS1	Add to this protection group

1 Items per page: [AUTO](#) 1 datastore groups

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

[CANCEL](#) [BACK](#) [NEXT](#)

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.

## New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete

## 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.

CANCEL

BACK

NEXT

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

## New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete**

## Ready to complete



Review your selected settings.

<b>Name</b>	SQL_Datastore
<b>Description</b>	
<b>Protected site</b>	Site 1
<b>Recovery site</b>	Site 2
<b>Location</b>	Protection Groups
<b>Protection group type</b>	Datastore groups (array-based replication)
<b>Array pair</b>	ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2 (nfs_array1 ↔ nfs_array2)
<b>Datastore groups</b>	NFS_DS1
<b>Total virtual machines</b>	3
<b>Recovery plan</b>	none

CANCEL

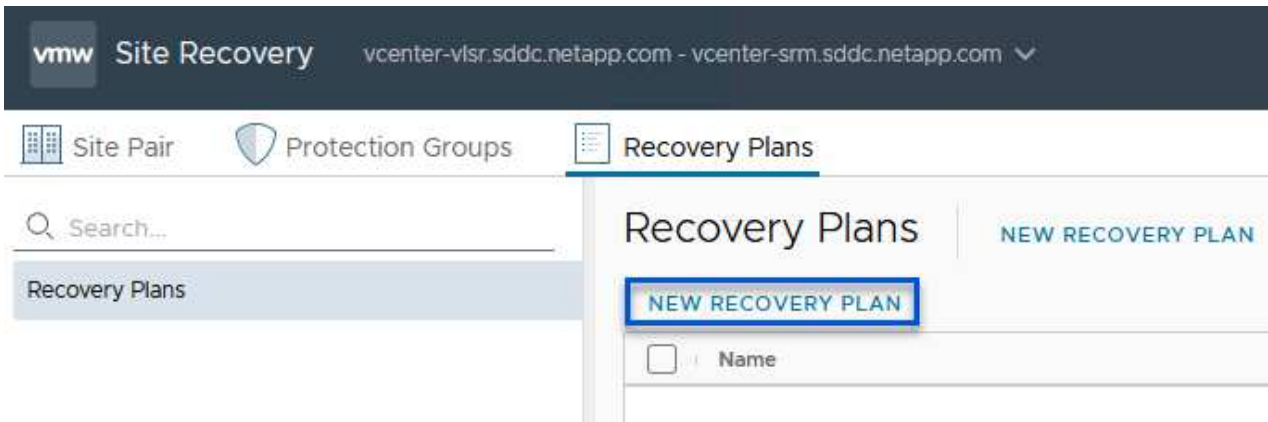
BACK

FINISH

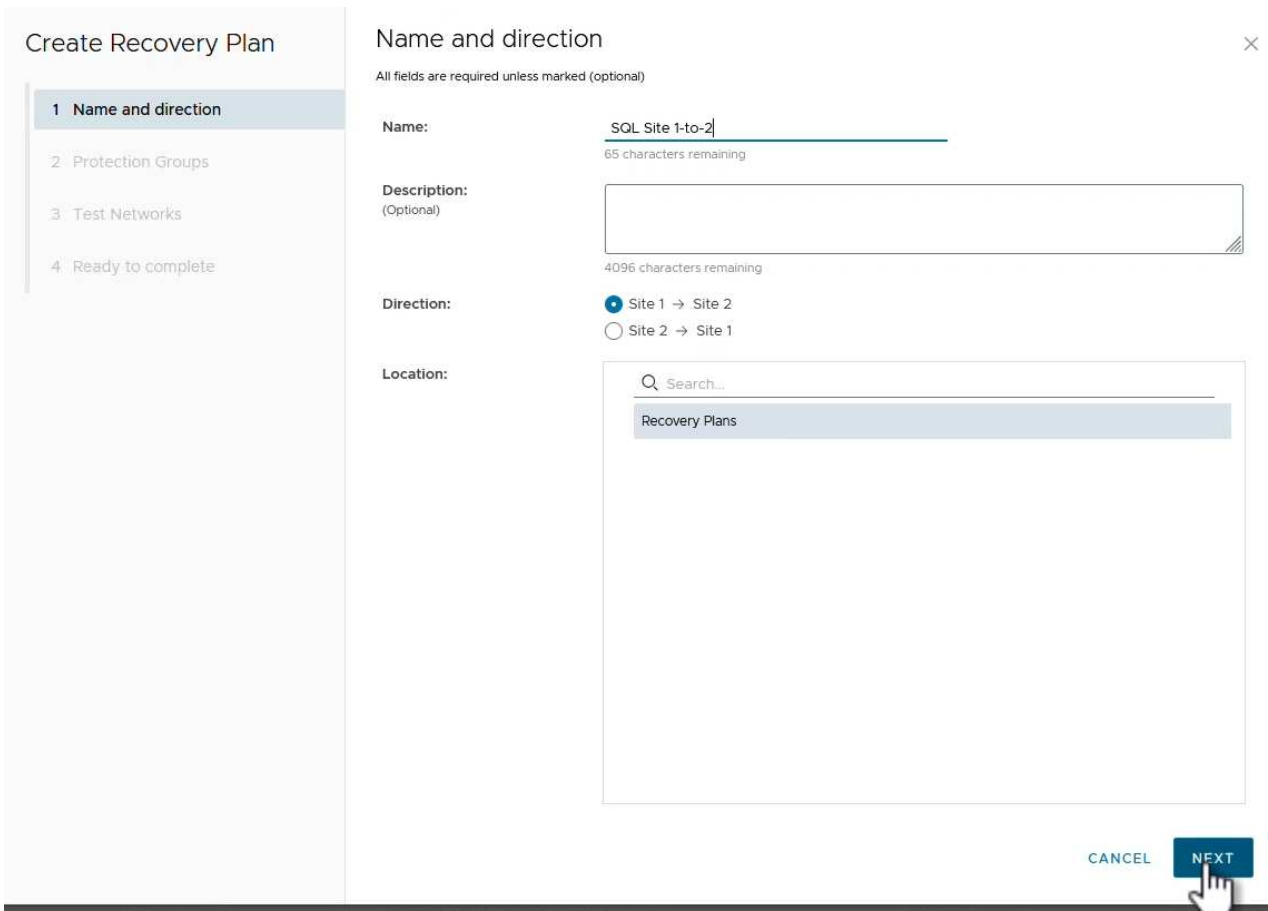
## Configure Recovery Plan for SRM

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.



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

The screenshot shows the 'Create Recovery Plan' wizard in step 2, 'Protection Groups'. On the left, a sidebar lists the steps: 1 Name and direction, 2 Protection Groups (highlighted), 3 Test Networks, and 4 Ready to complete. The main area is titled 'Protection Groups' and shows a table with columns 'Name' and 'Description'. One row is visible: 'SQL\_Datastore' with a checkmark in the selection column. Below the table, there are controls for 'Items per page' set to 'AUTO' and '1 group(s)'. At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'. A mouse cursor is clicking on the 'NEXT' button.

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.

i 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)

CANCEL BACK NEXT

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

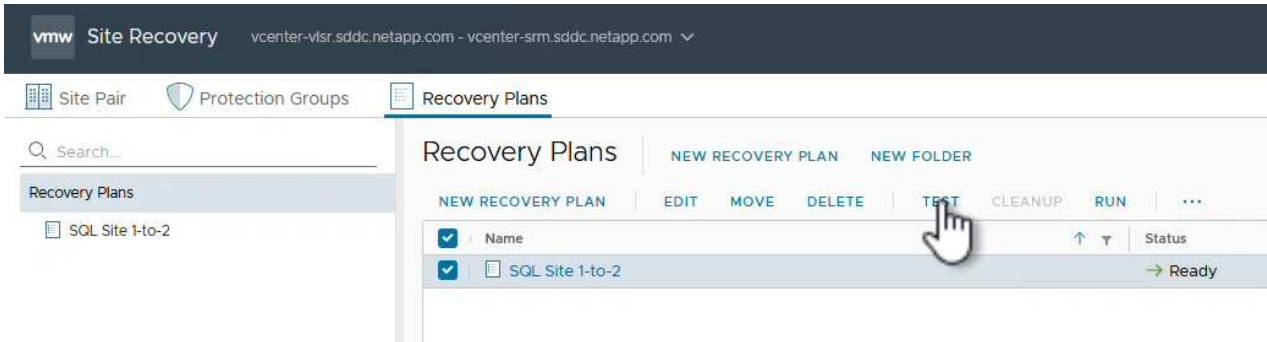
In this section various functions of using disaster recovery with SRM will be covered including, testing failover, performing failover, performing reprotection and failback.

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.

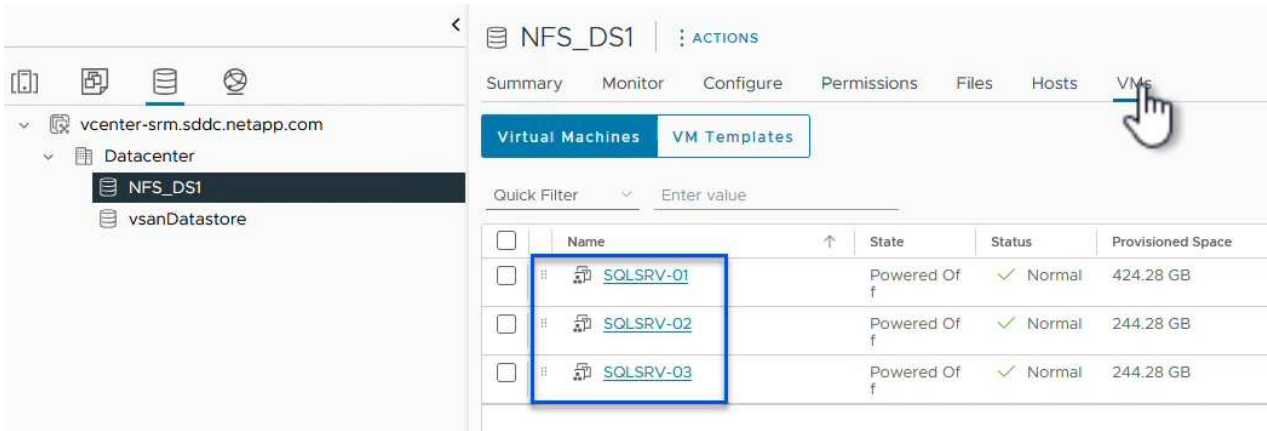


2. You can view the progress of the test from the Site Recovery task pane as well the vCenter task pane.

The screenshot shows the 'Recent Tasks' pane in the Site Recovery interface. It displays a table of tasks with columns for 'Task Name', 'Target', 'Status', 'Initiator', and 'Queued For'. The tasks listed are:

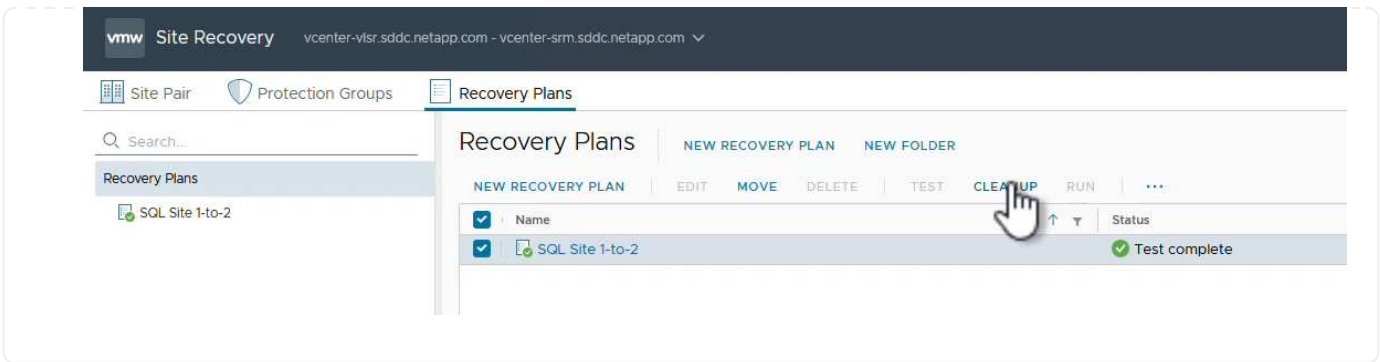
Task Name	Target	Status	Initiator	Queued For
Test Recovery Plan	vcenter-vlsr.sddc.netapp.com	6 %	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	11 ms
Create Recovery Plan	vcenter-vlsr.sddc.netapp.com	Completed	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	10 ms
Set virtual machine custom value	SQLSRV-02	Completed	VSPHERE.LOCAL\SRM-d1369bbb-62c6...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



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

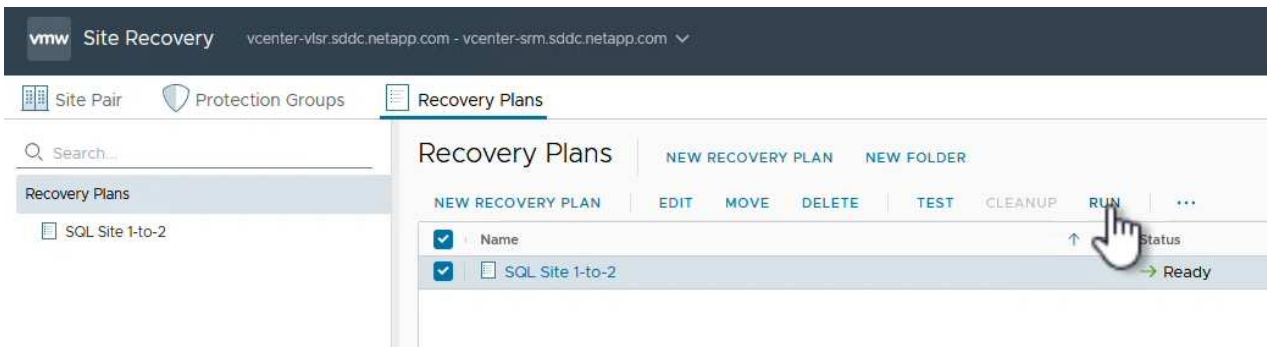




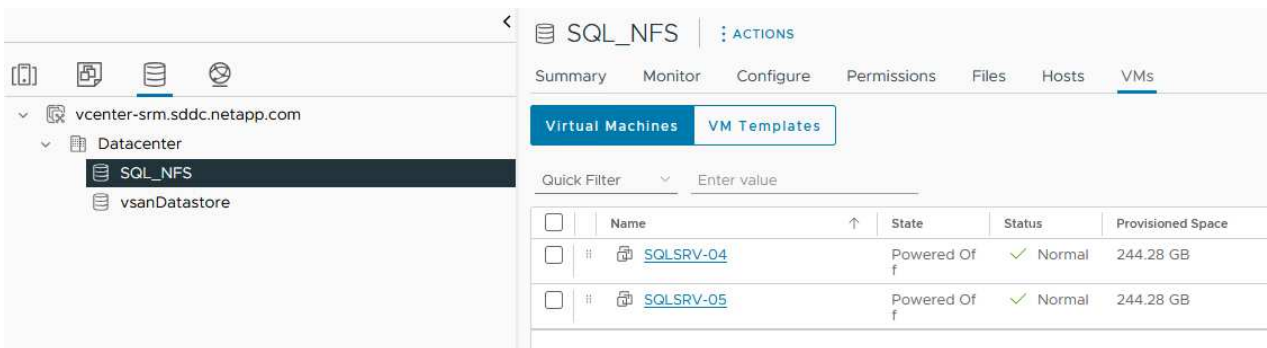
## Run Recovery Plan with SRM

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.



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



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 re-protection 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](#)

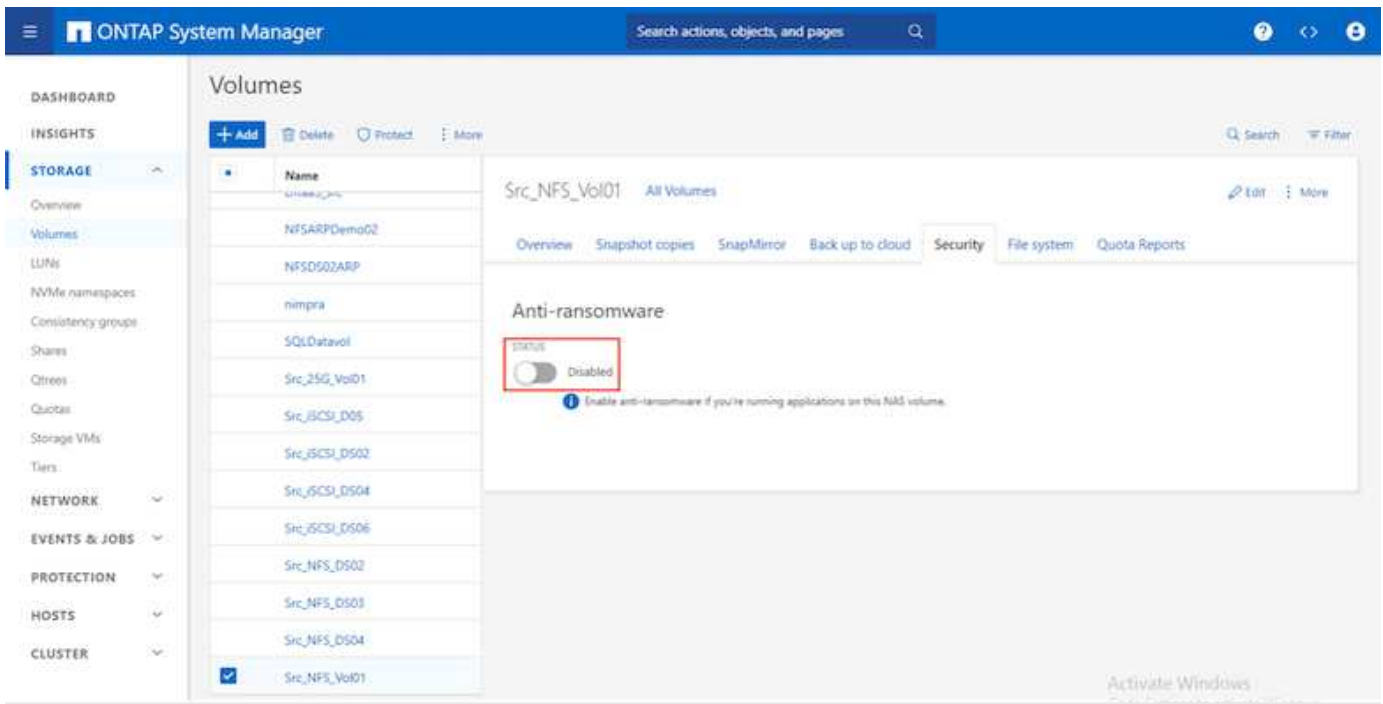
For information on configuring ONTAP storage systems refer to the [ONTAP 9 Documentation](#) center.

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.

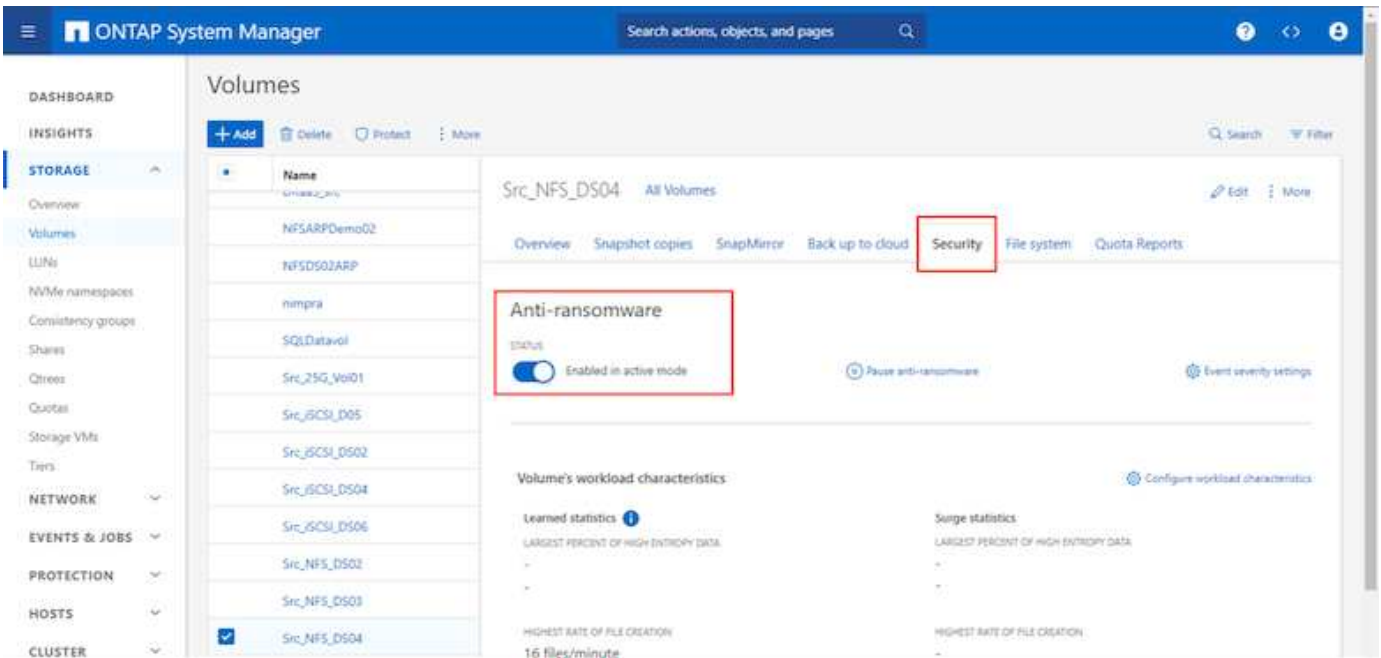


With the new NetApp ARP/AI, which is currently in tech preview, there is no need for a learning mode. Instead, it can go straight to active mode with its AI-powered ransomware detection capability.



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.

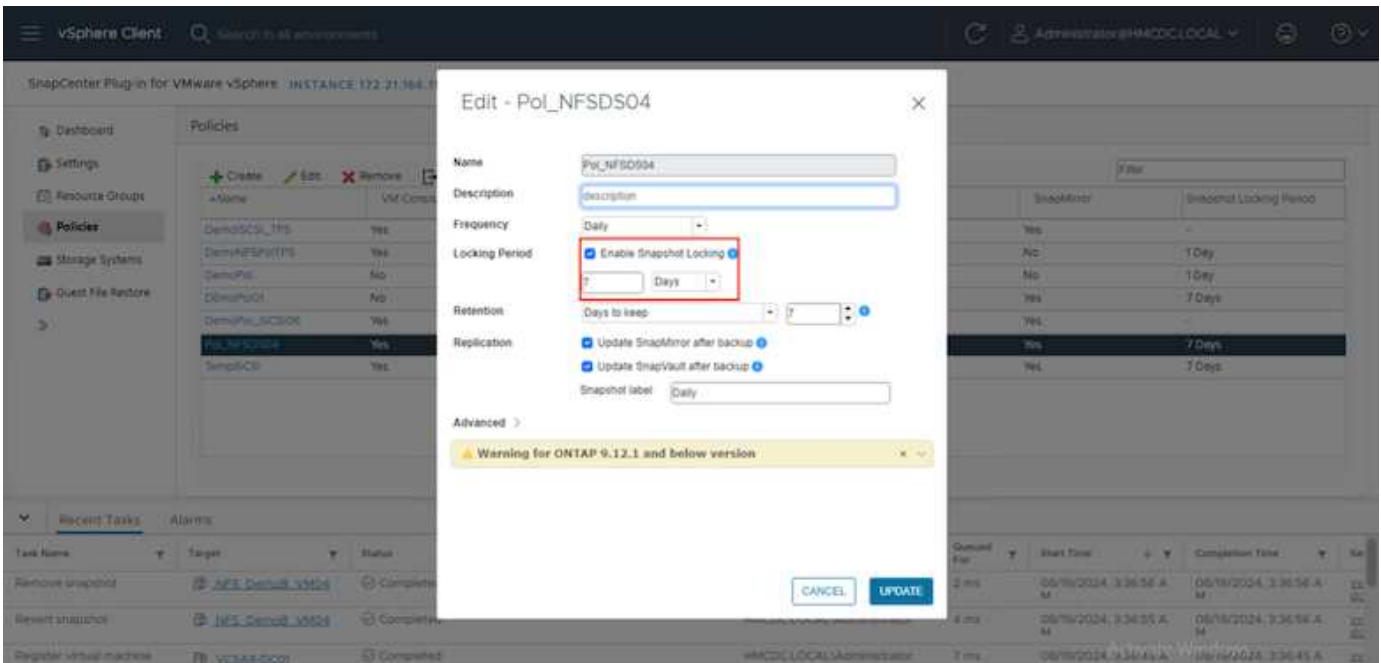
Once in active mode, it starts looking for the abnormal volume activity that might potentially be ransomware. If abnormal activity is detected, an automatic Snapshot copy is immediately taken, which provides a restoration point as close as possible to the file infection. ARP can detect changes in VM 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.



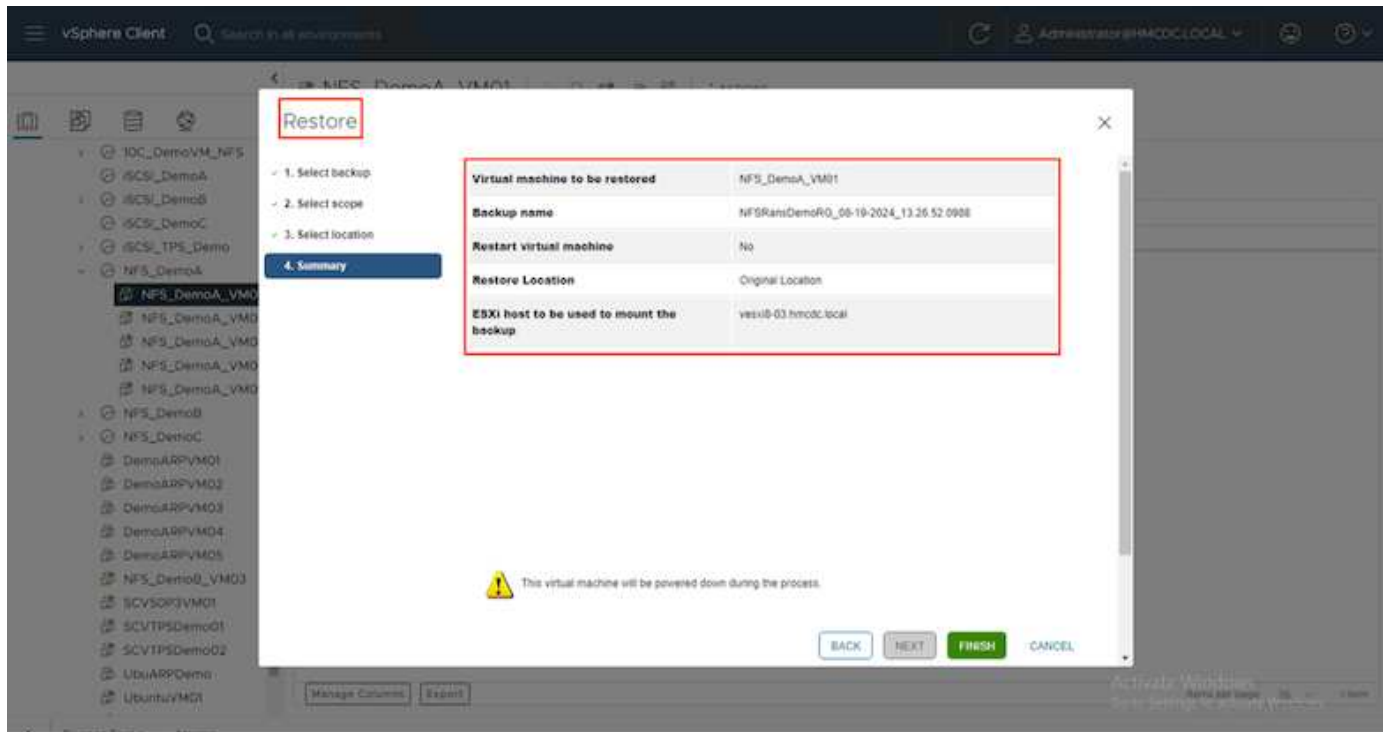
If a ransomware attack targets the virtual machine (VM) and alter files within the VM without making changes outside the VM, the Advanced Ransomware Protection (ARP) will still detect the threat if the default entropy of the VM is low, for example, for file types like .txt, .docx, or .mp4 files. Even 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](#).



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.



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.

NetApp BlueXP

BlueXP Search

Ransomware protection Dashboard Protection Alerts Recovery Reports Free trial (55 days left) - view details

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_vsi01_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
Src_nfs_ds04	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_3419	File share	GISABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	Edit protection

NetApp BlueXP

BlueXP Search

Ransomware protection Dashboard Protection Alerts Recovery

**Datastore protected and No Alerts reported**

Standard Importance

Protected Protection health 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\_NFSD504 Snapshot policy
- 1 Year Daily LTR Backup policy

VM datastore

Location urn:scv:scvm:UJ:Resou...

vCenter server vccsa8-01.hmcdc.local

Connector GISABXPConn

Storage

Cluster id add38626-348c-11ef-6...

Working Env name NTAP915\_Src

Storage VM name svm\_nfs

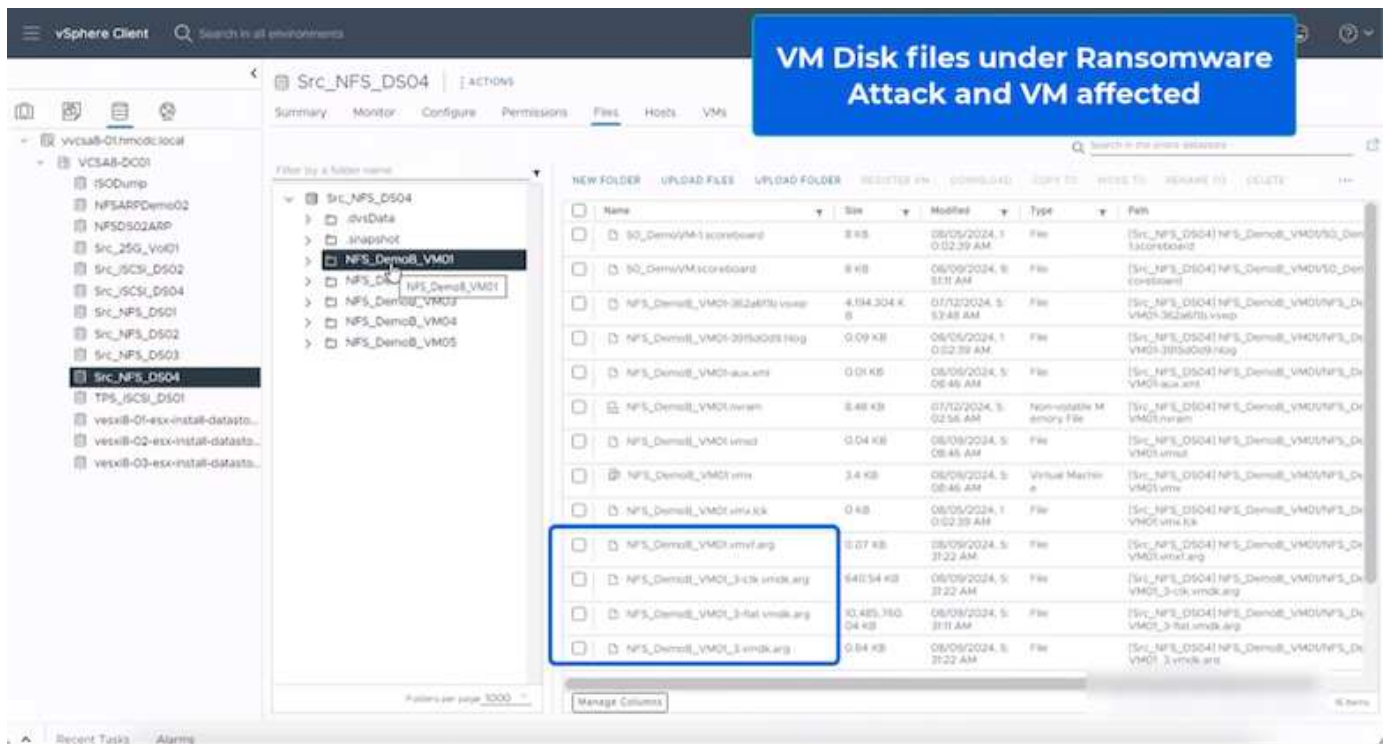
Volume name Src\_NFS\_DS04

Used size 29 GiB

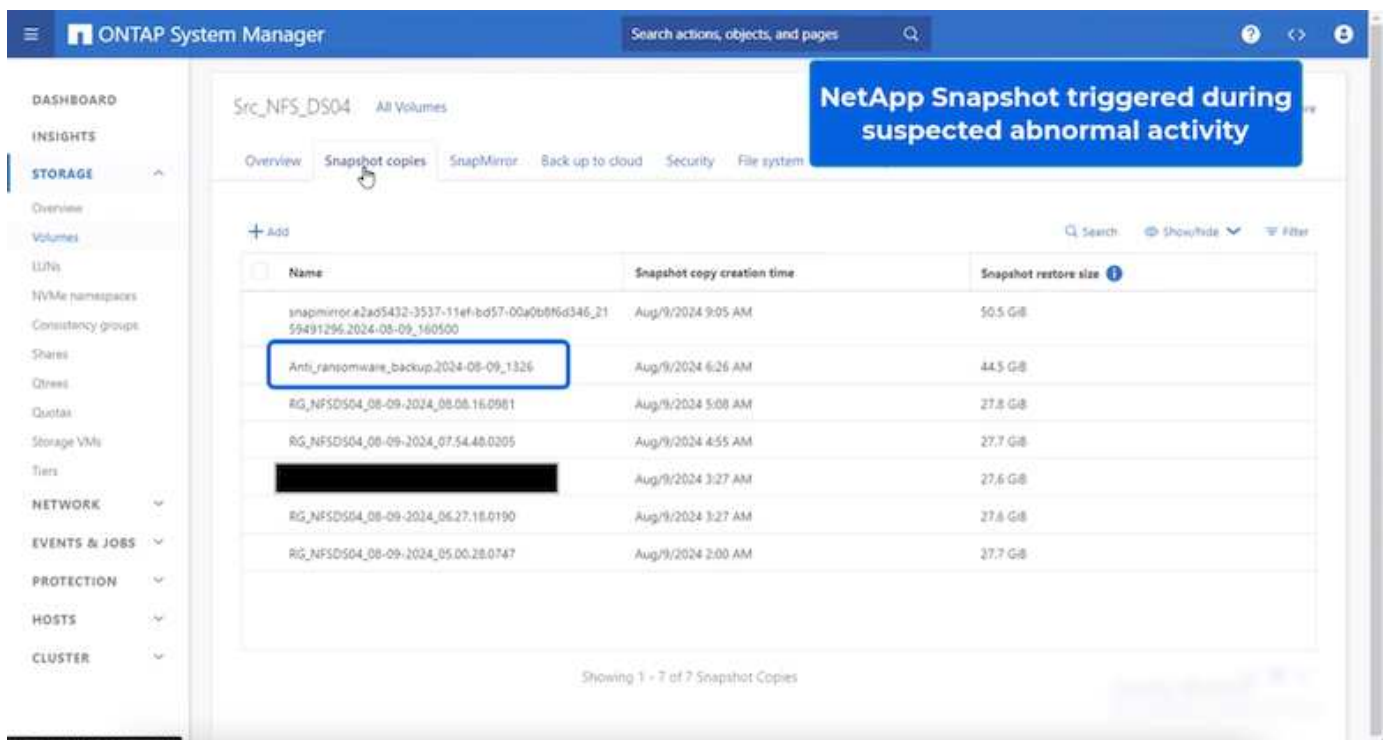
For detailed information on to configure BlueXP ransomware protection, refer to [Setup BlueXP ransomware protection](#) and [Configure BlueXP ransomware protection settings](#).

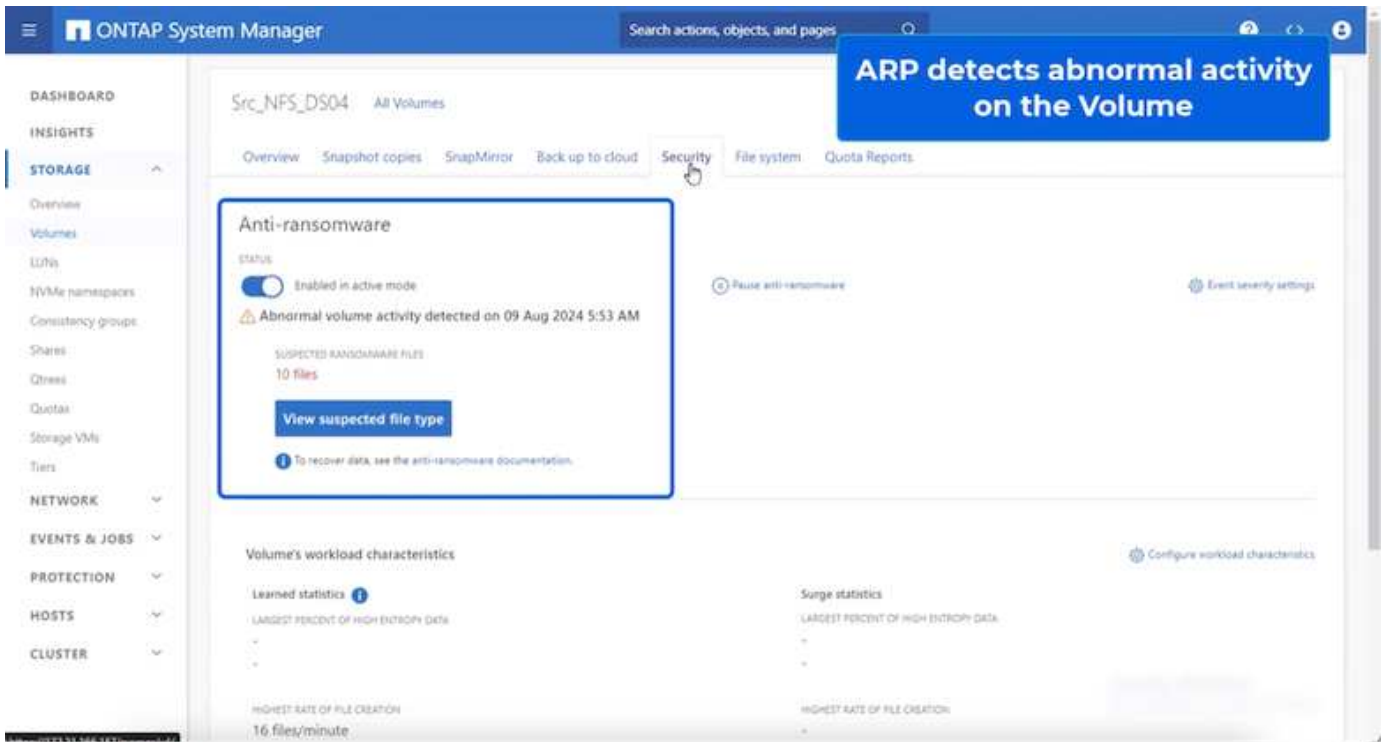
It's time to walk through this with an example. In this walkthrough, the datastore "Src\_NFS\_DS04" is affected.



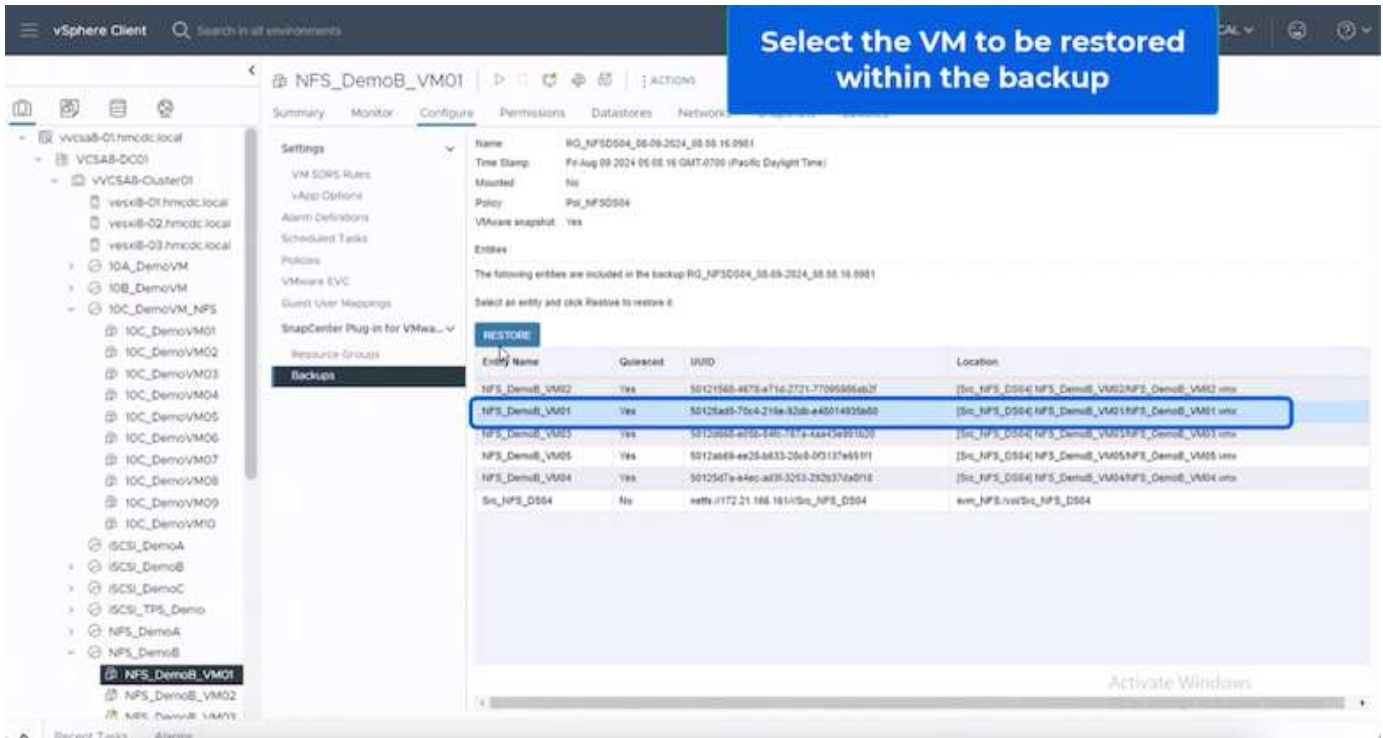


ARP immediately triggered a snapshot on the volume upon detection.





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.



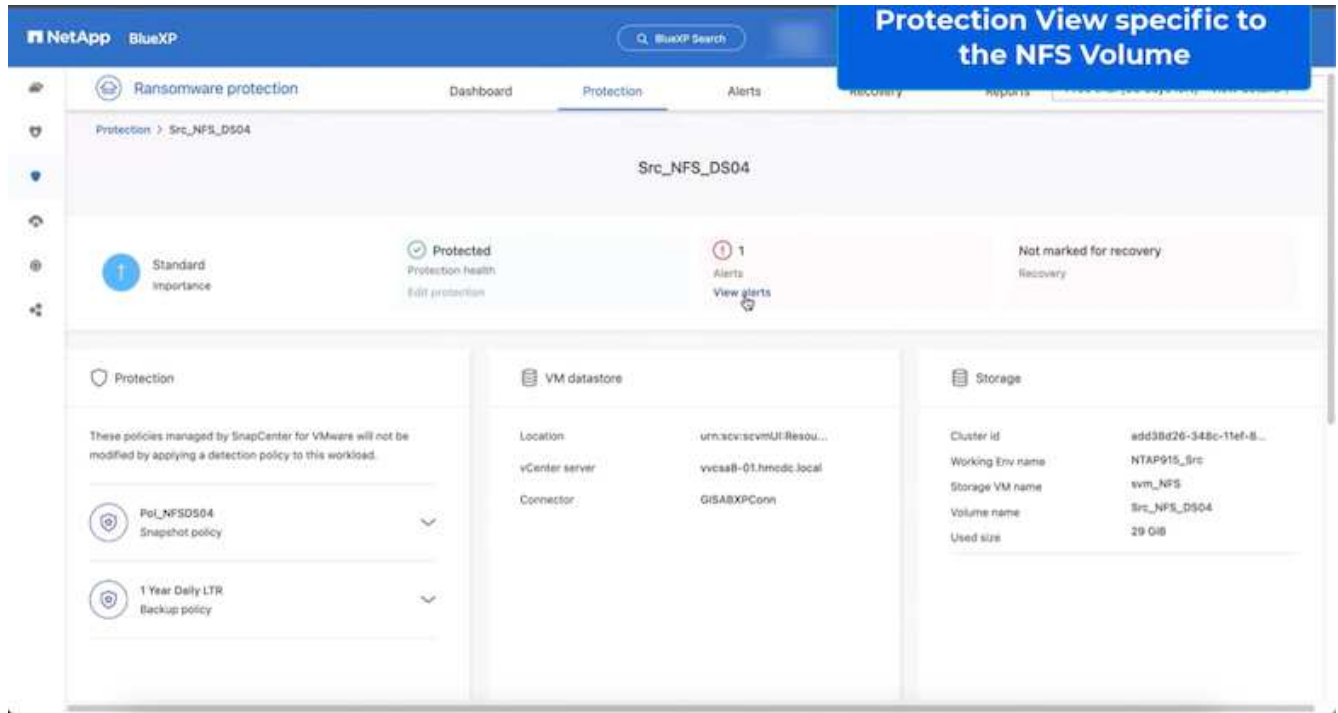
This section looks at how BlueXP ransomware protection orchestrates recovery from a ransomware incident wherein the VM files are encrypted.



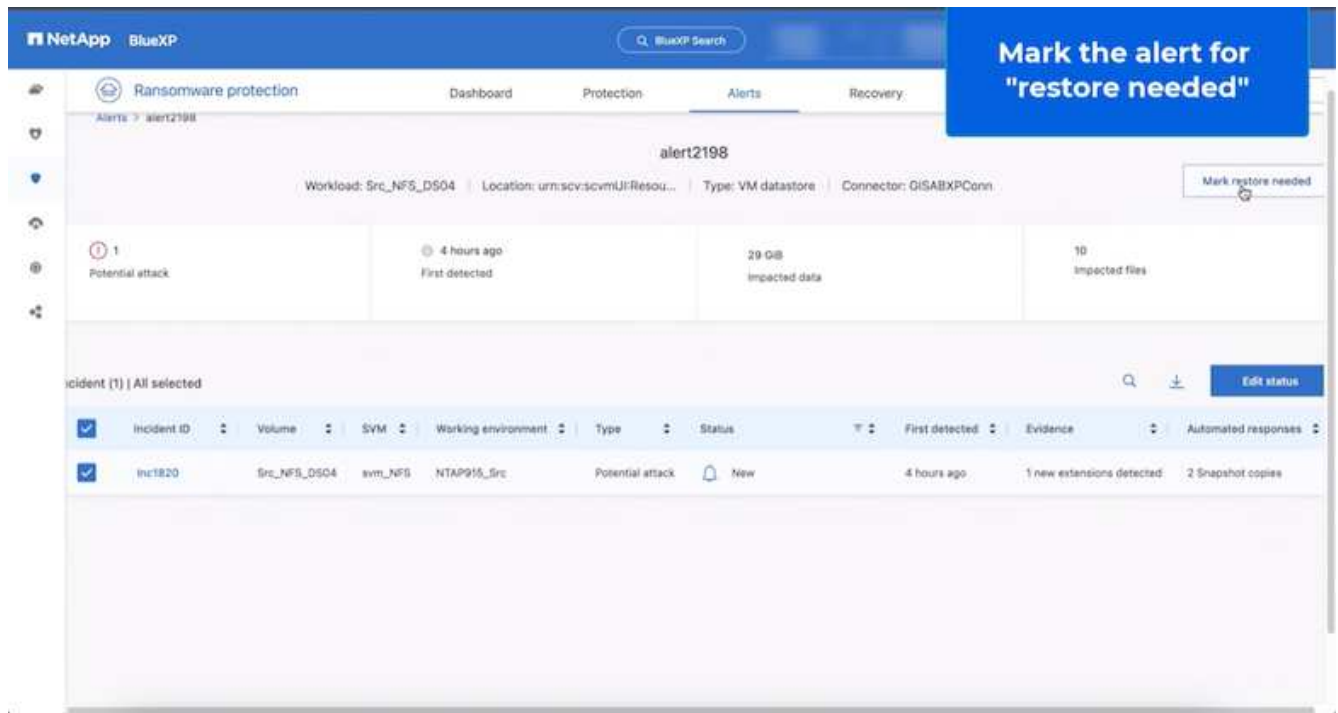
If the VM is managed by SnapCenter, BlueXP ransomware protection restores the VM back to its previous state using the VM-consistent process.




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



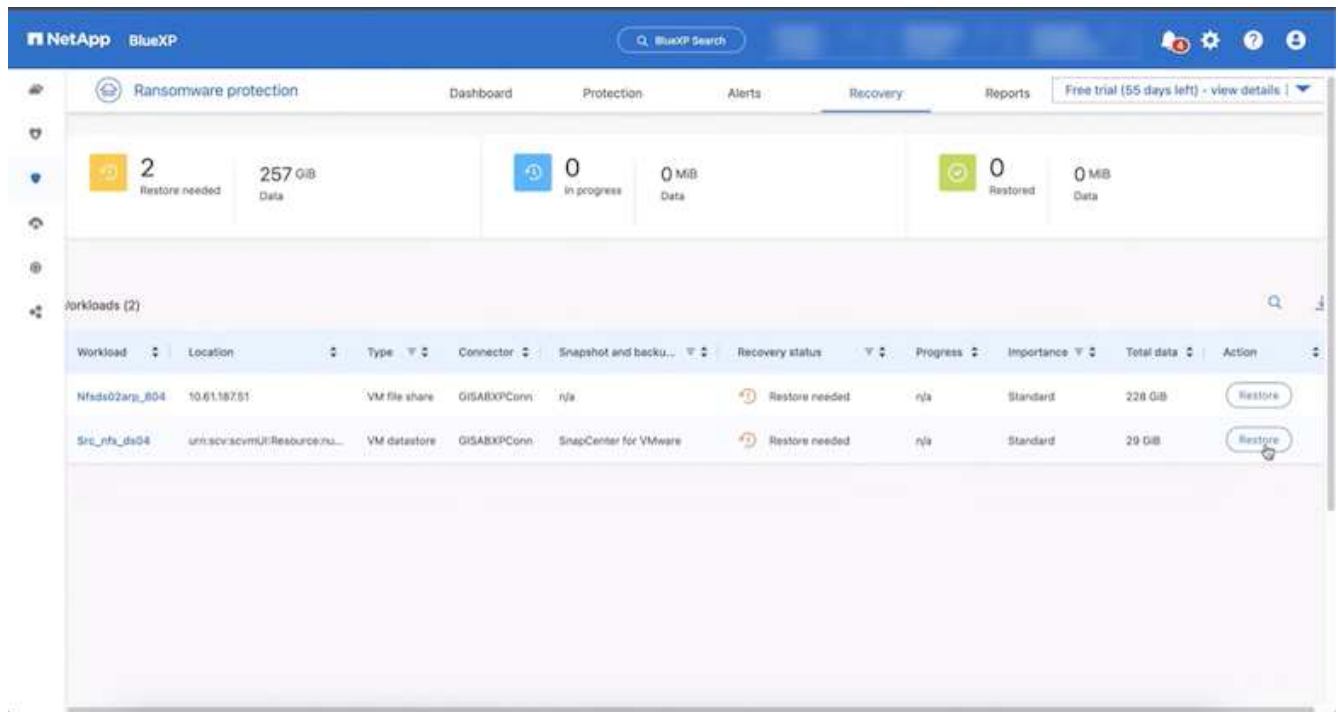
3. Mark the ransomware incident as ready for recovery (after incidents are neutralized) by selecting “Mark restore needed”



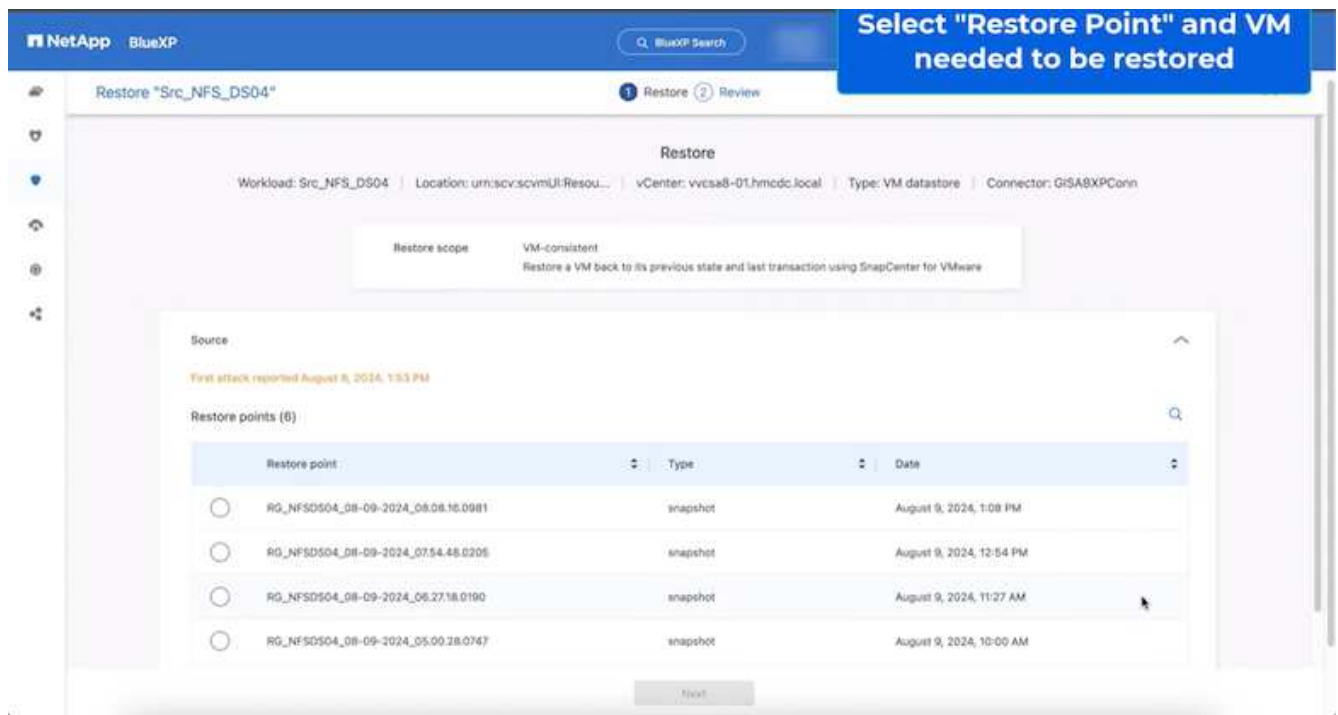
 The alert can be dismissed if the incident turns out to be false positive.

4. Got to Recovery tab and review the workload information in the Recovery page and select the datastore

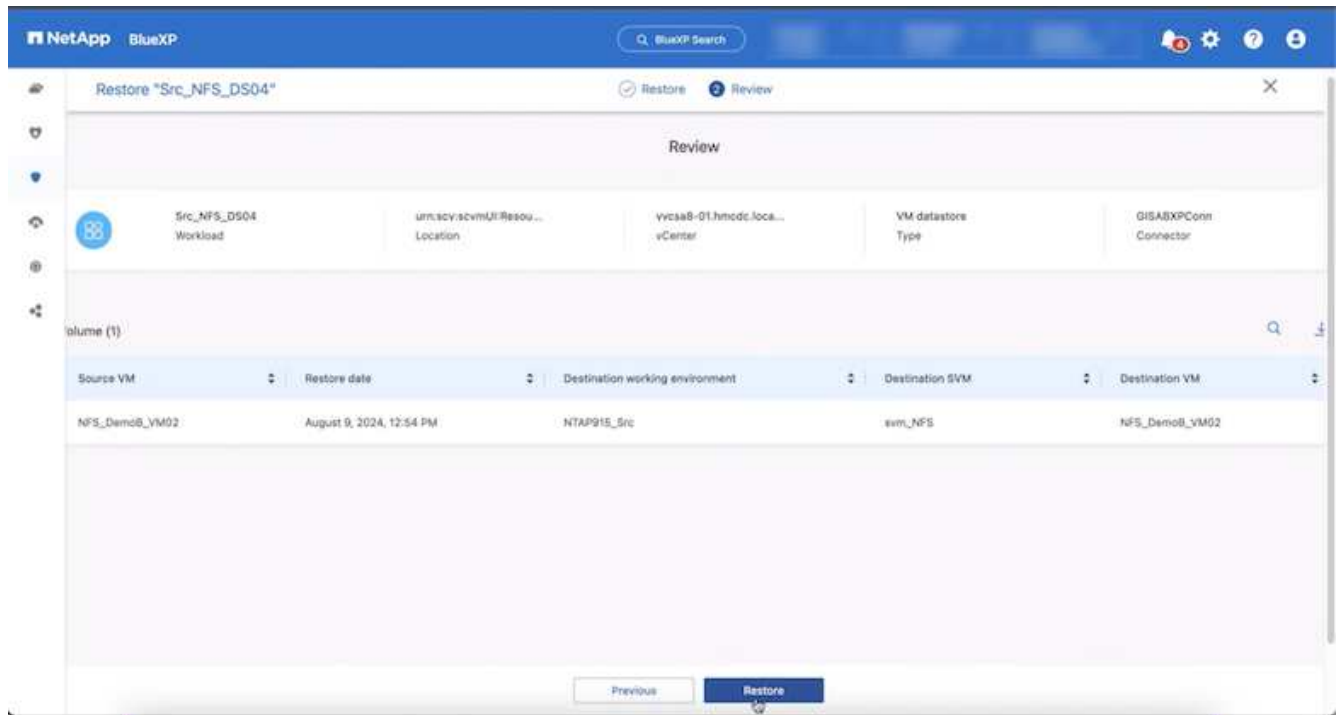
volume that is in the "Restore needed" state and select Restore.



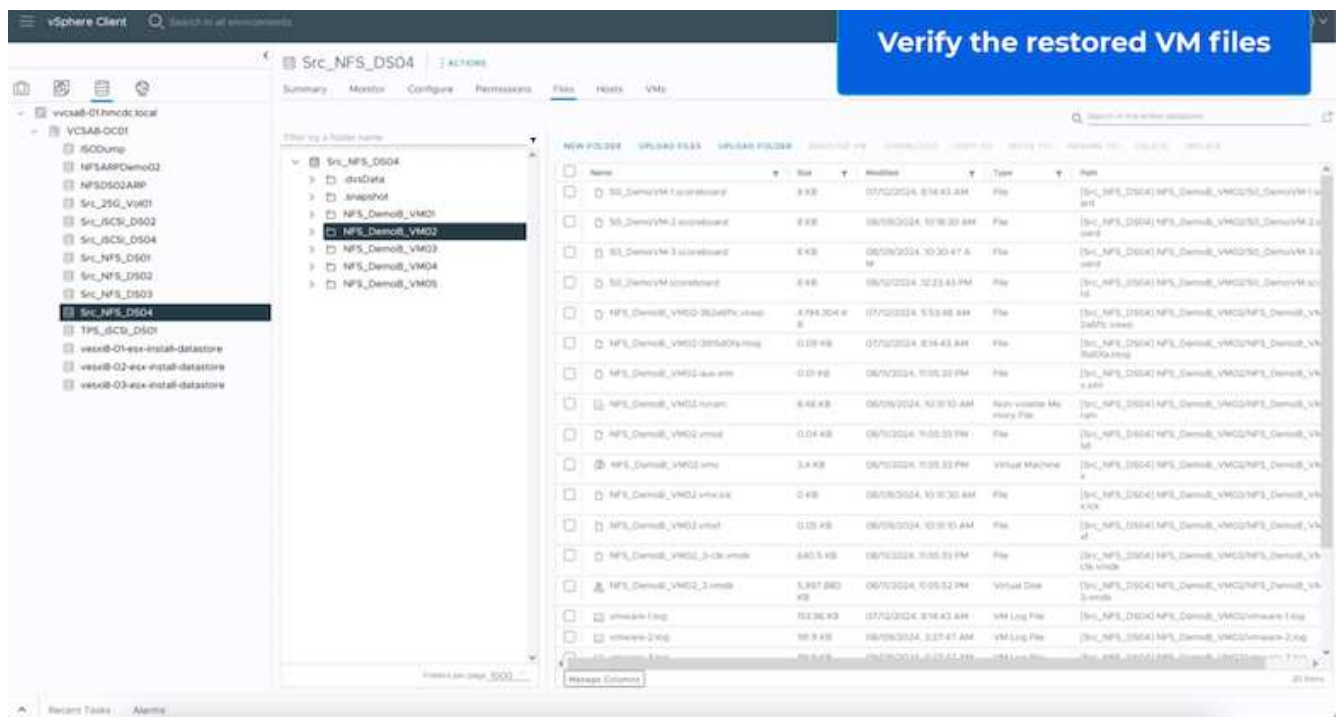
5. In this case, the restore scope is "By VM" (for SnapCenter for VMs, the restore scope is "By VM")



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



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

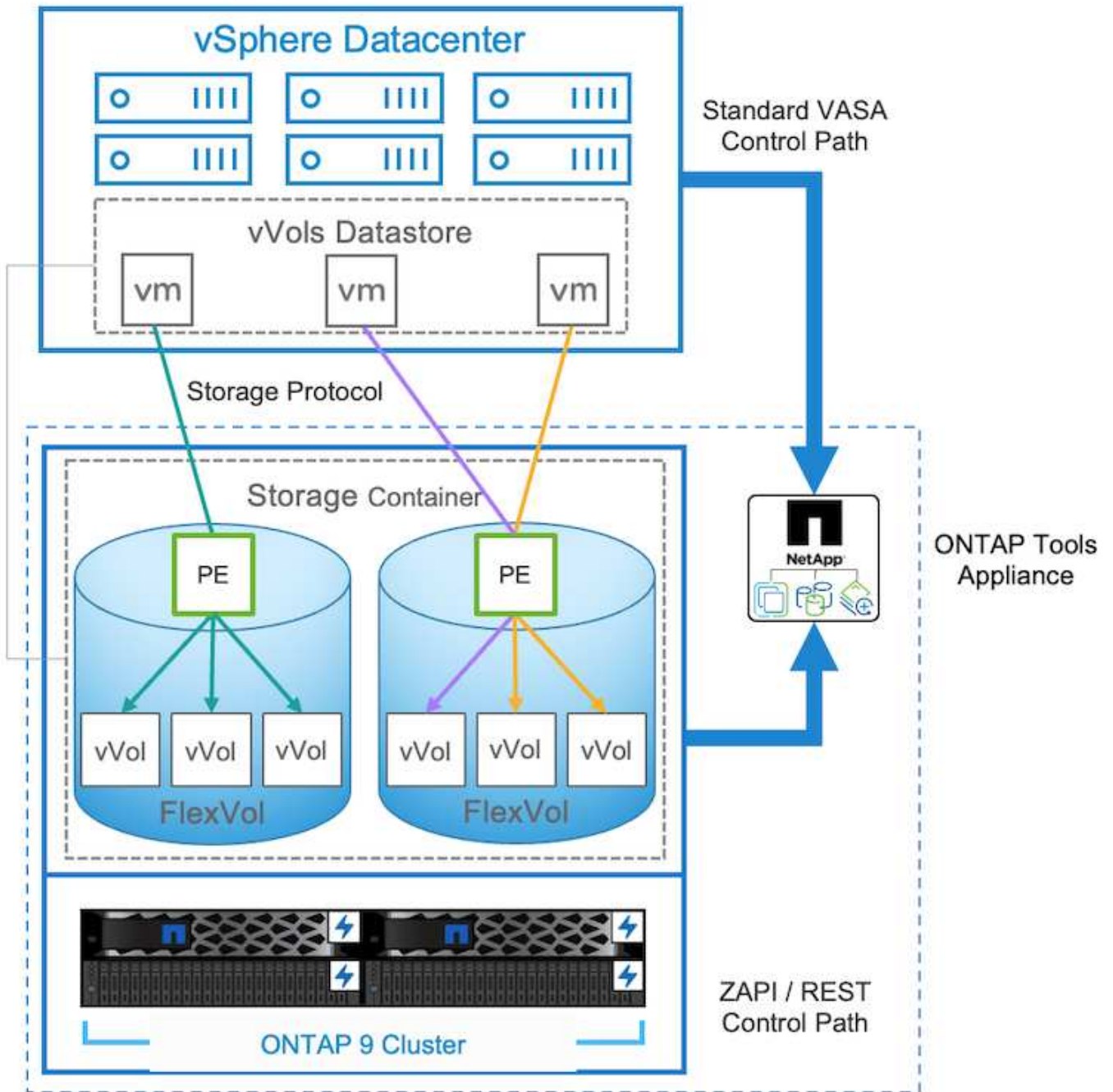
VMware Virtual Volumes (vVols) enables application-specific requirements to drive storage provisioning decisions while leveraging the rich set of capabilities provided by storage arrays. The vSphere API for Storage Awareness (VASA) make it easy for a VM administrator to use whatever storage capabilities 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.



```

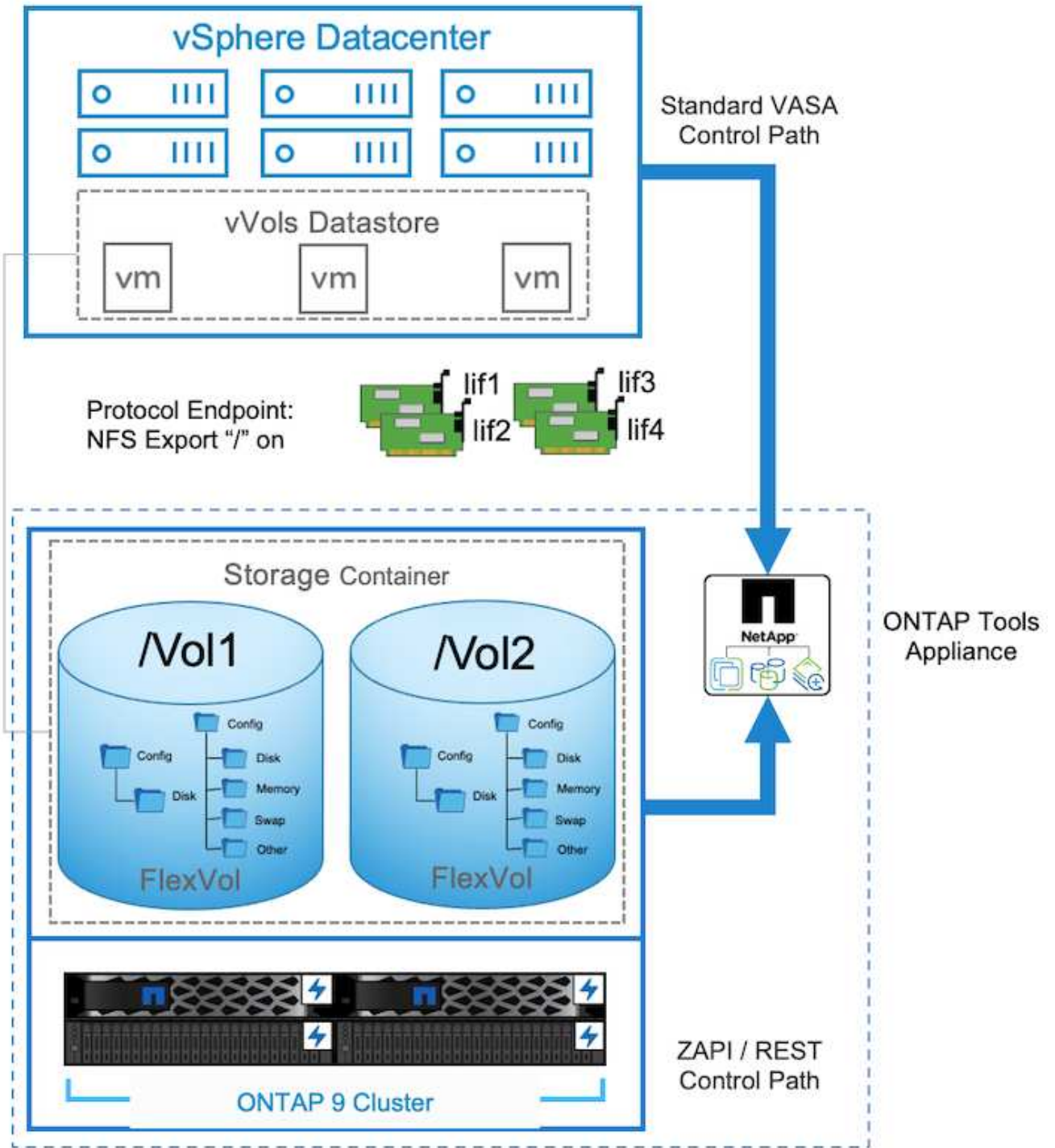
ntaphci-a300e9u25::> lun show -vserver zoneb -class protocol-endpoint -fields size
vserver path size
-----
zoneb /vol/Demo01_fv01/Demo01_fv01-vvolPE-1723681460207 2GB
zoneb /vol/Demo01_fv02/Demo01_fv02-vvolPE-1723681460217 2GB
zoneb /vol/TME01_iSCSI_01/vvolPE-1723727751956 4MB
zoneb /vol/TME01_iSCSI_02/vvolPE-1723727751970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

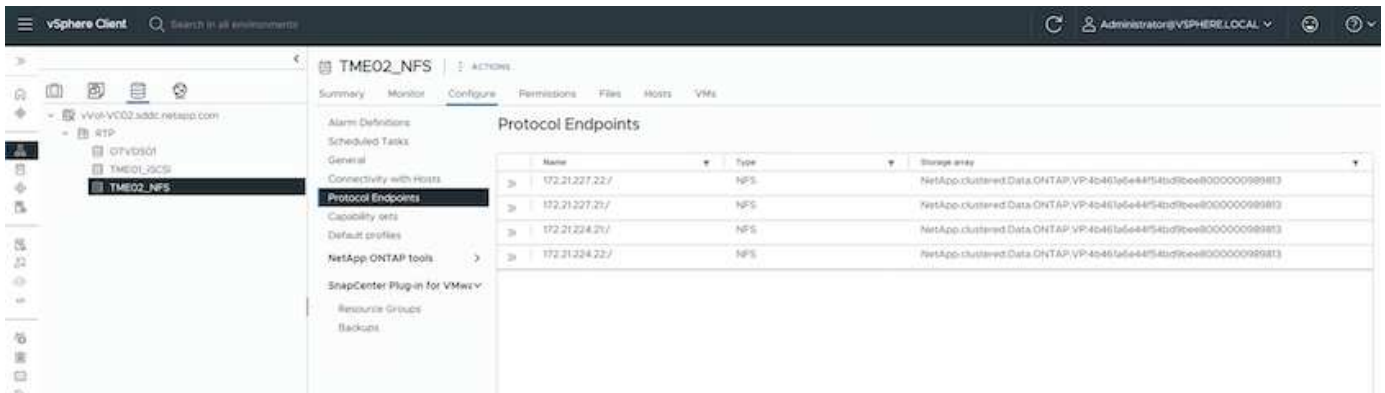
```

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.





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 Availability
- 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 differentiated 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.

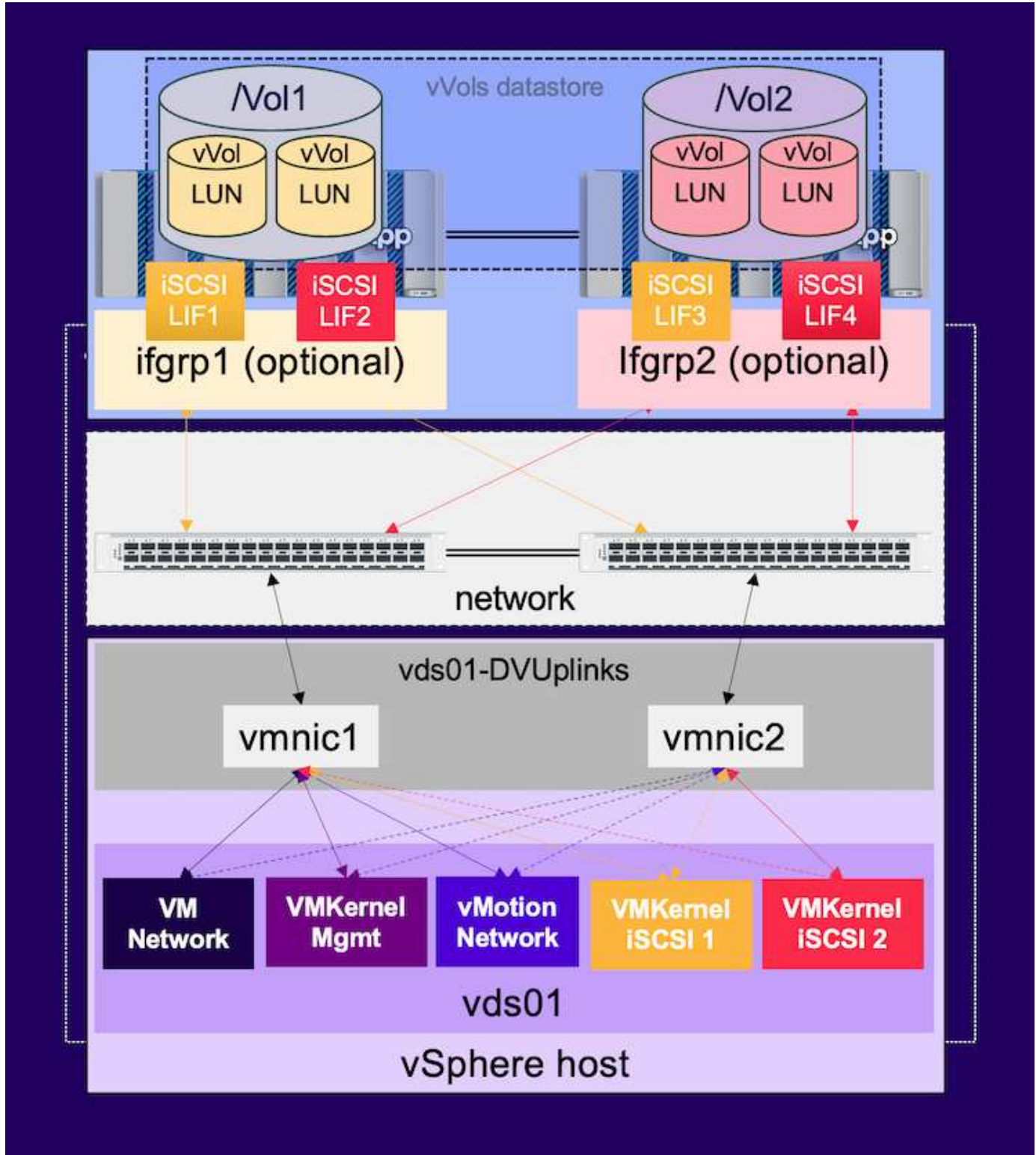
## Connectivity options

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.

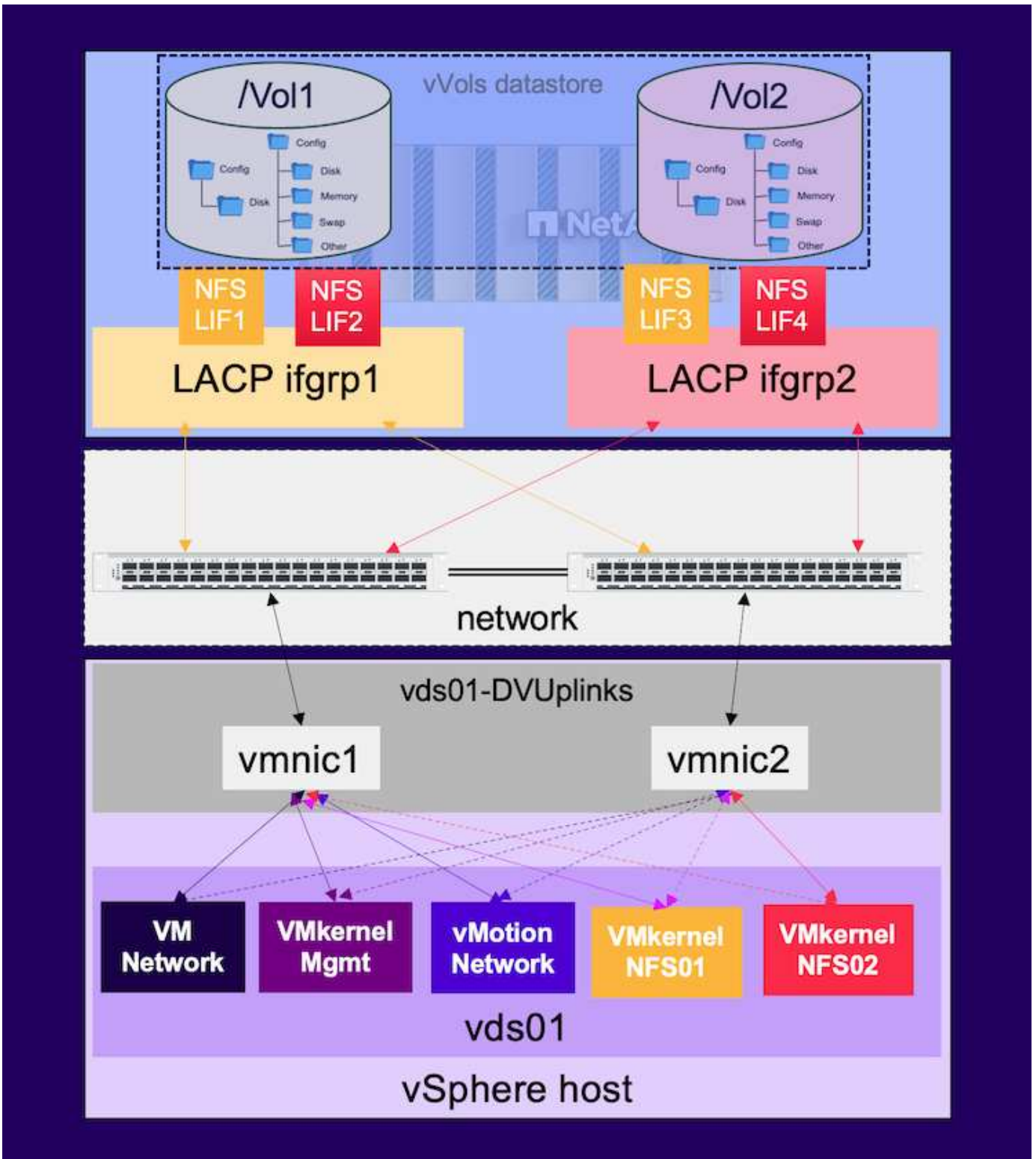
NOTE: Refer [Interoperability Matrix Tool \(IMT\)](#) for supported ONTAP Tool version

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

New Datastore

1 General  
2 Storage system  
3 Storage attributes  
4 Summary

General

Specify the details of the datastore to provision ⓘ

Provisioning destination: Cluster01 BROWSE

Type:  NFS  VMFS  vVols

Name: TME01\_ISCSI

Description:

Protocol:  NFS  iSCSI  FC / FCoE  NVMe/FC

CANCEL NEXT

New Datastore

1 General  
2 Storage system  
3 Storage attributes  
4 Summary

General

Specify the details of the datastore to provision ⓘ

Provisioning destination: Cluster01 BROWSE

Type:  NFS  VMFS  vVols

Name: TME02\_NFS

Description:

Protocol:  NFS  iSCSI  FC / FCoE  NVMe/FC

CANCEL NEXT

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:

Storage VM:

[CANCEL](#) [BACK](#) [NEXT](#)

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

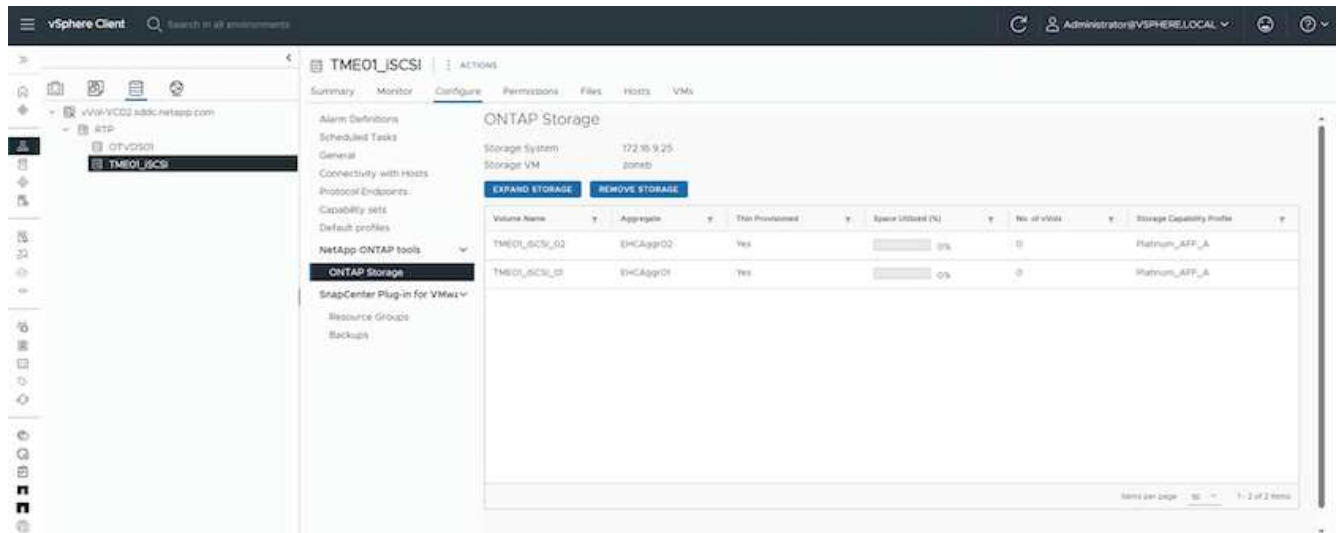
1 - 2 of 2 items

Name	Size(GB)	Storage capability profile	Aggregates	Space reserve
<input type="text"/>	<input type="text"/>	<input type="text" value="Platinum_AFF_A"/>	<input type="text" value="EHCAGgr02 - (17109.63 Gi)"/>	<input type="text" value="Thin"/>

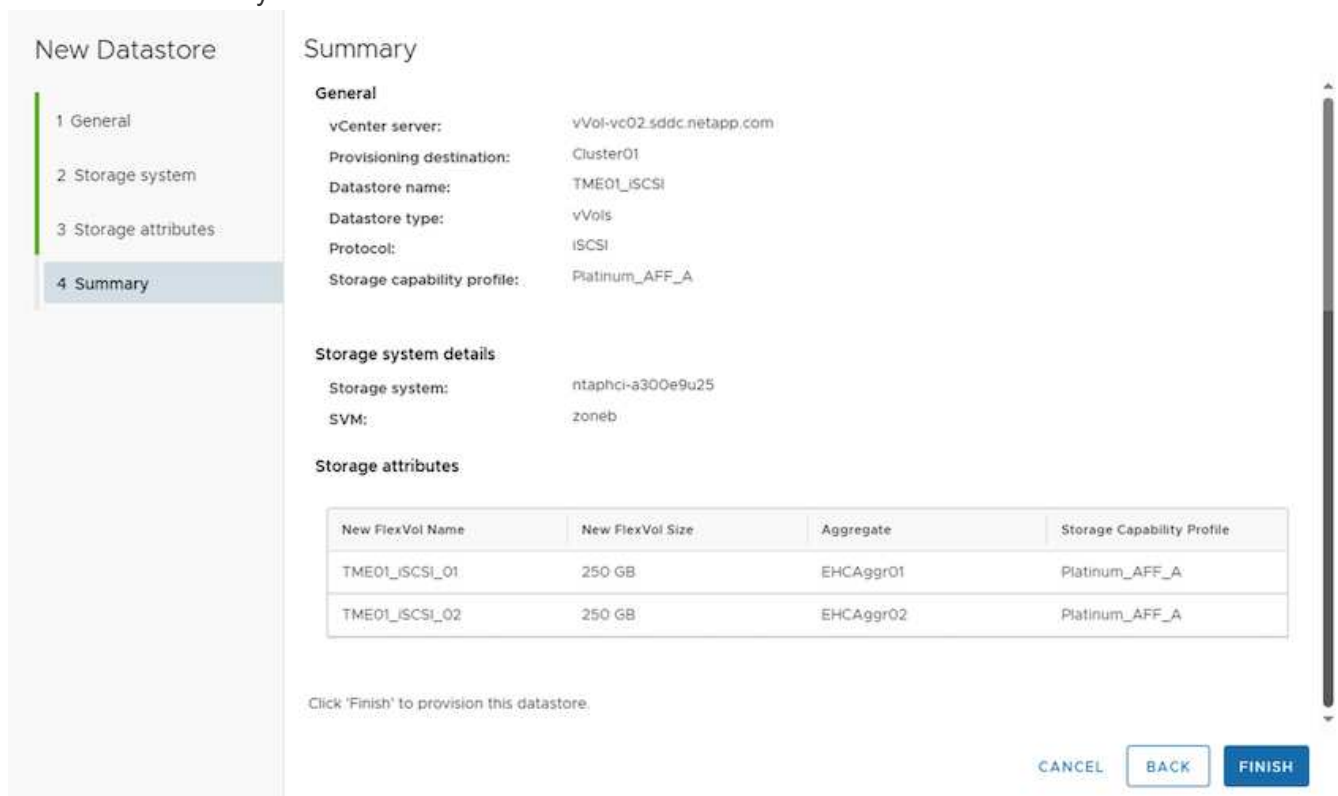
[ADD](#)

[CANCEL](#) [BACK](#) [NEXT](#)

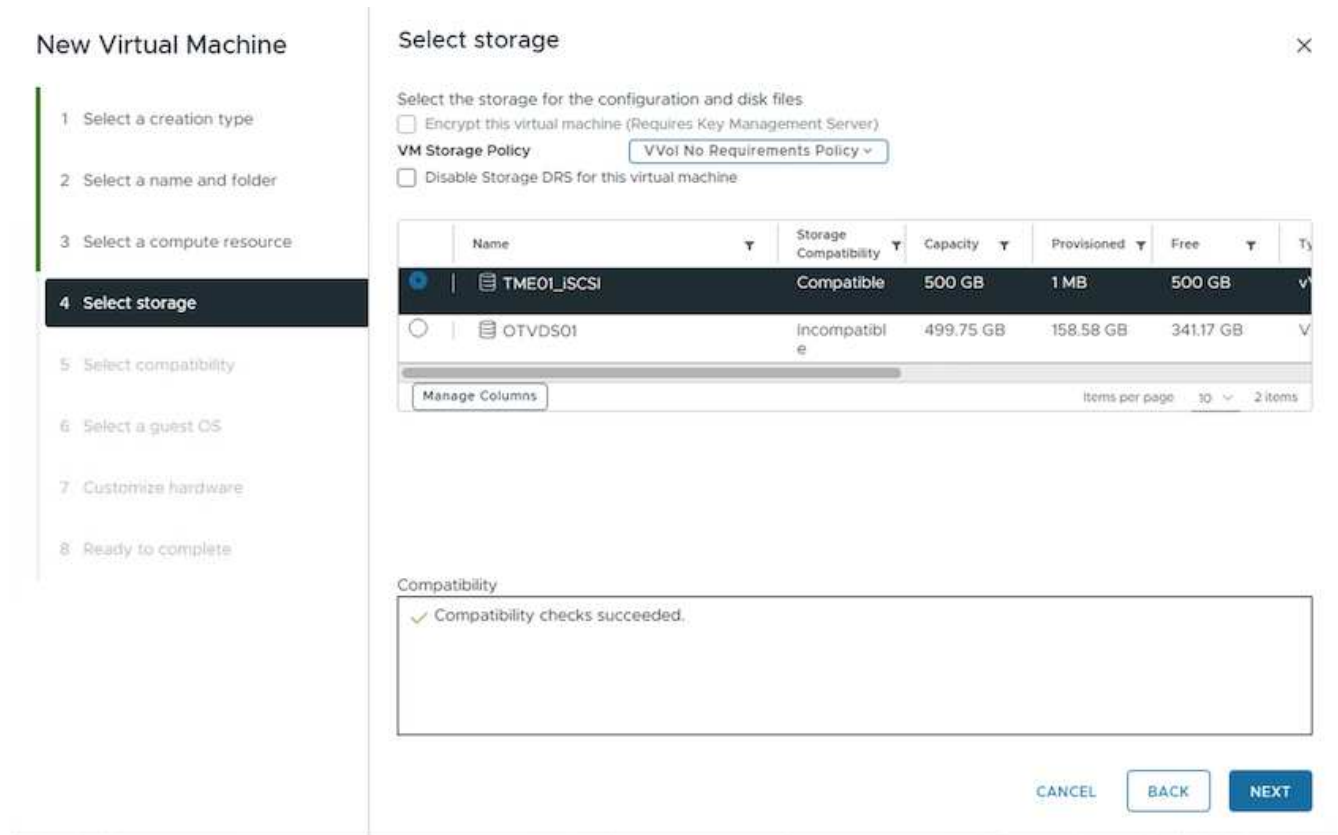
ONTAP volumes can be viewed or change later from the datastore option.



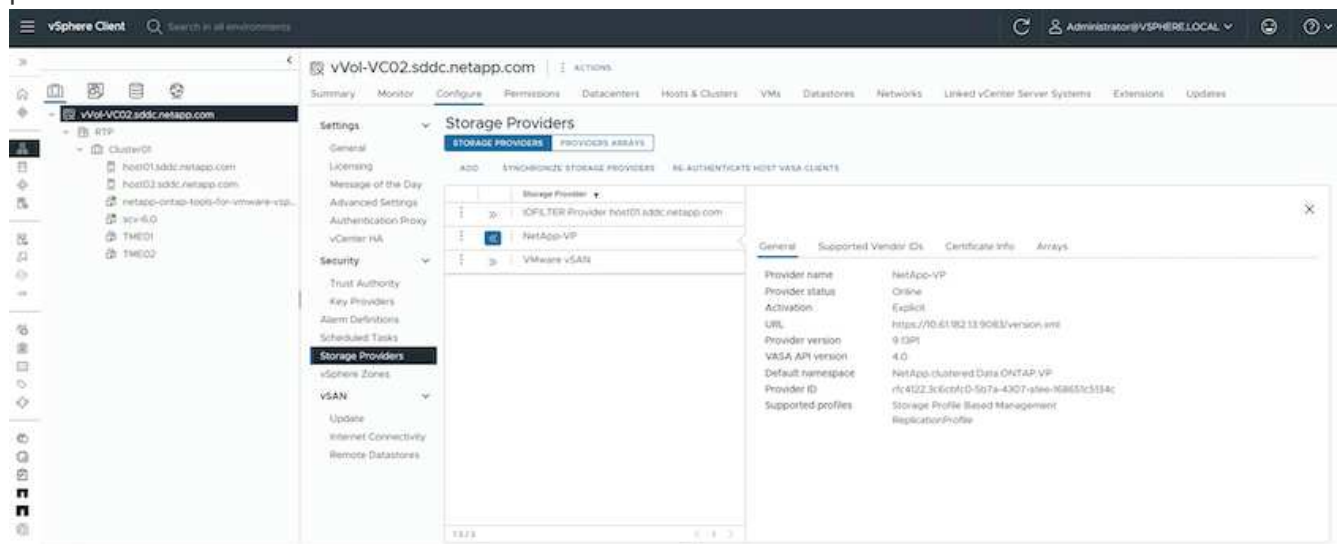
5. Review the summary and click on Finish to create the vVol datastore.



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.



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.



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

← ↻ Not secure | https://10.61.182.13:9083/jsp/login.jsp

- Welcome to VASA Client Login
- Username\* administrator
- Password \* .....
- Token \*
- 

▼ 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
<a href="#">Web based CLI interface</a>	Web based access to the command line interface for administrative tasks
<a href="#">Inventory</a>	Listing of all objects and information currently known in Unified Virtual Appliance database
<a href="#">Statistics</a>	Listing of all counters and information regarding internal state
<a href="#">Right Now</a>	See what operations are in flight right now
<a href="#">Logout</a>	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:
[{"LUNID": "naa.600a0980383043595a2b506b67783041", "METADATA": "StorageLocation=172.18.9.25[zoneb] TME01_iSCSI_01 /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783041.vmdk", "BINDINGFORMATION": "(naa.600a0980383043595a2b506b67783041 bound to EP003842-5F65-8A3A-883A-4A402C4F7F8 -fa)", "LUNID": "naa.600a0980383043595a2b506b67783043", "DATA": "StorageLocation=172.18.9.25[zoneb] TME01_iSCSI_01 /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783043.vmdk", "BINDINGFORMATION": "(keyValuePairs={VM_VolNameSpace=vmfs/volumes/vvol1-40463a644f54b09-bce80000000064907nae)", "LUNID": "naa.600a0980383043595a2b506b67783043", "DATA": "StorageLocation=172.18.9.25[zoneb] TME01_iSCSI_01 /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783043.vmdk", "BINDINGFORMATION": "(keyValuePairs={VM_VolParentLUNID=naa.600a0980383043595a2b506b67783043})", "LUNID": "naa.600a0980383043595a2b506b67783043", "METADATA": "StorageLocation=172.18.9.25[zoneb] TME01_iSCSI_01 /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783043.vmdk", "BINDINGFORMATION": "(keyValuePairs={VM_VolType=Data, VM_VolID=50037592-5D7F-4001-2797-4784F661214-5 Vvol1})",
Available Commands:
Executed Commands:

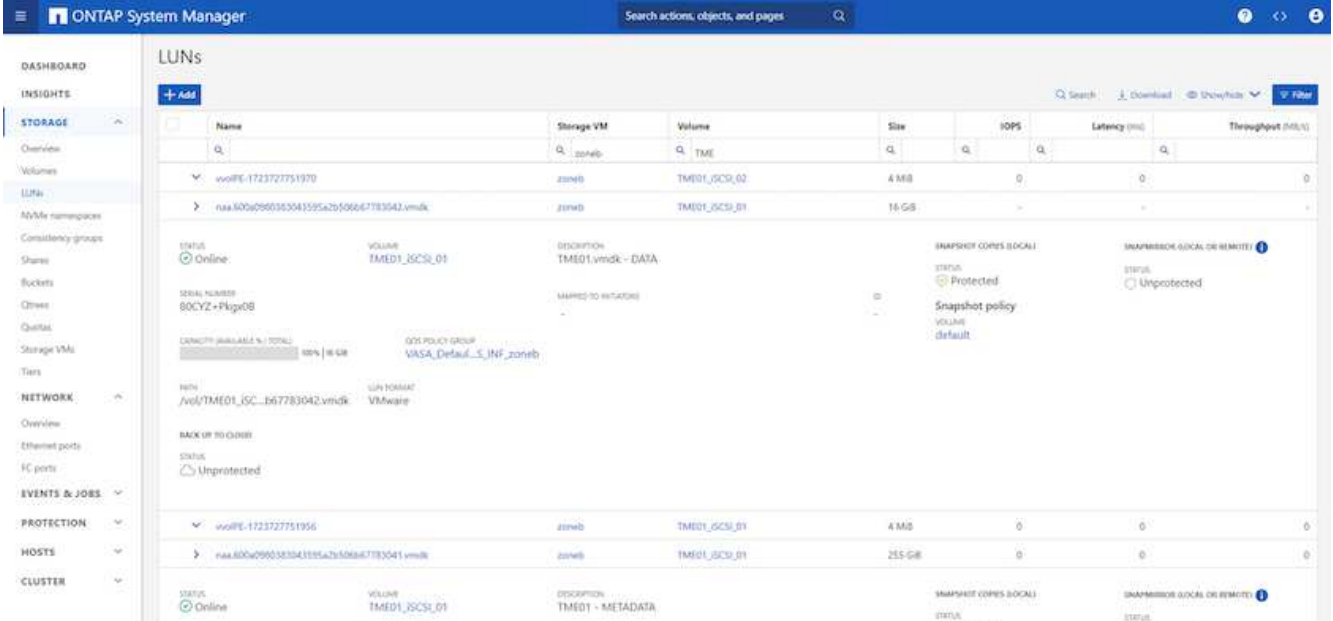
```

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

```

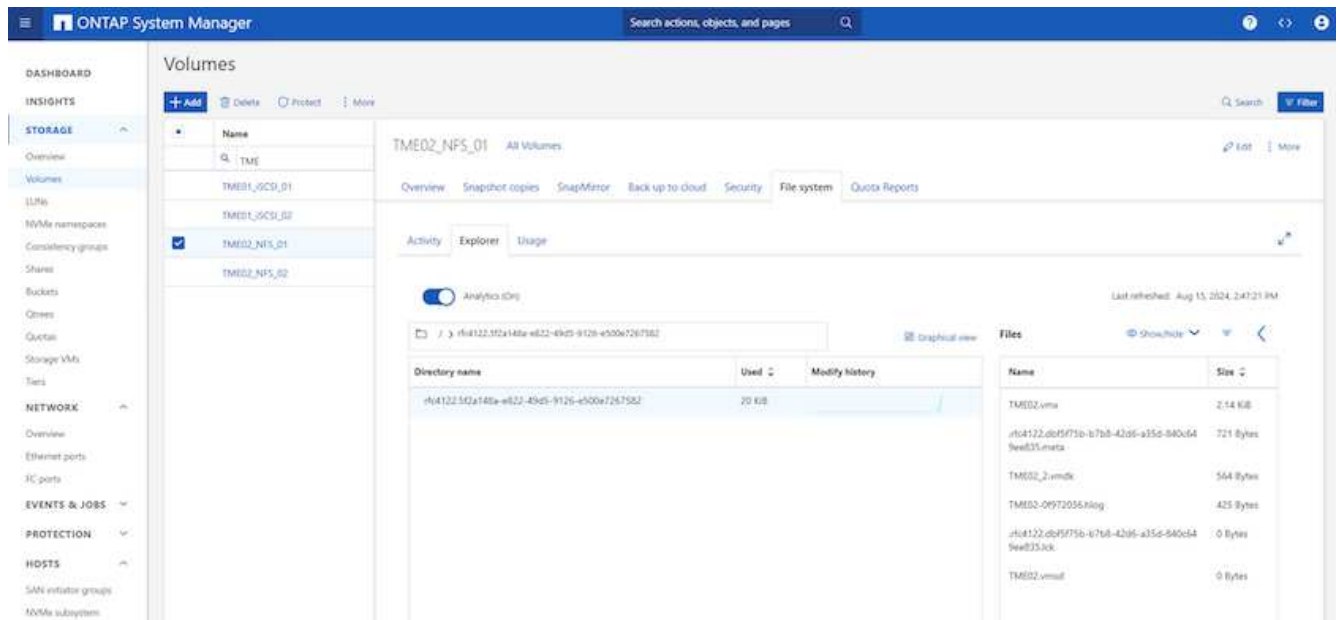
ntaphci-a300e9u25:~> lun show -vserver zoneb -class vvol -fields comment,size
vserver path size comment
-----
zoneb /vol/Demo01_fv01/naa.600a0980383043595a2b506b67783038.vmdk 255GB
zoneb /vol/Demo01_fv02/naa.600a098038304359463f515057683735.vmdk 255GB
zoneb /vol/Demo01_fv02/naa.600a098038304359463f515057683736.vmdk 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

```



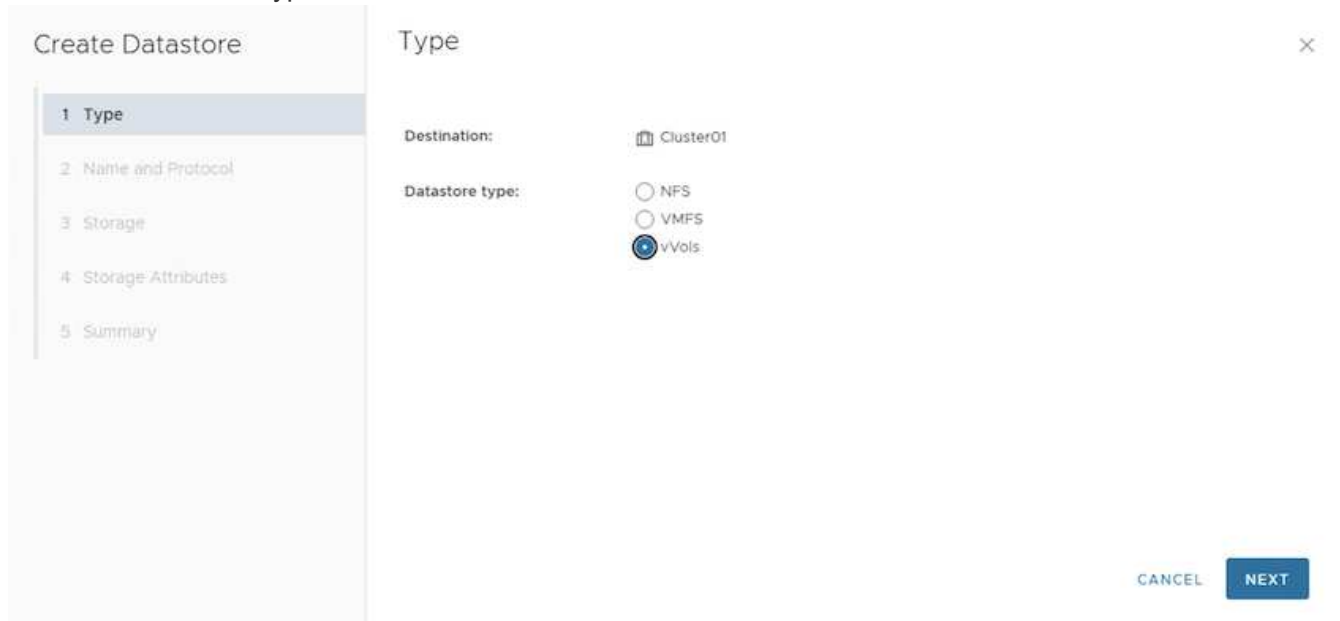
For NFS based, the System Manager can be used to browse the datastore.



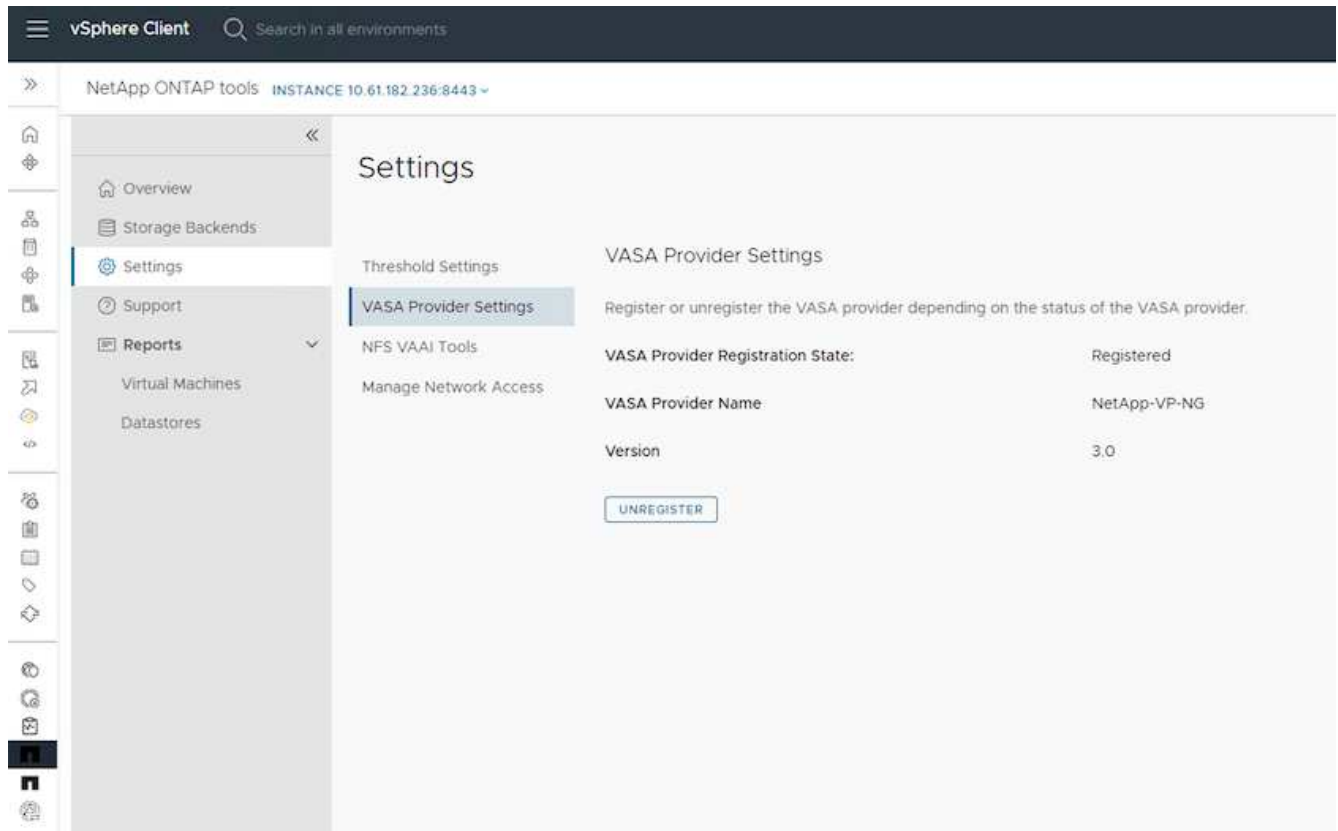


## With ONTAP tools 10.1

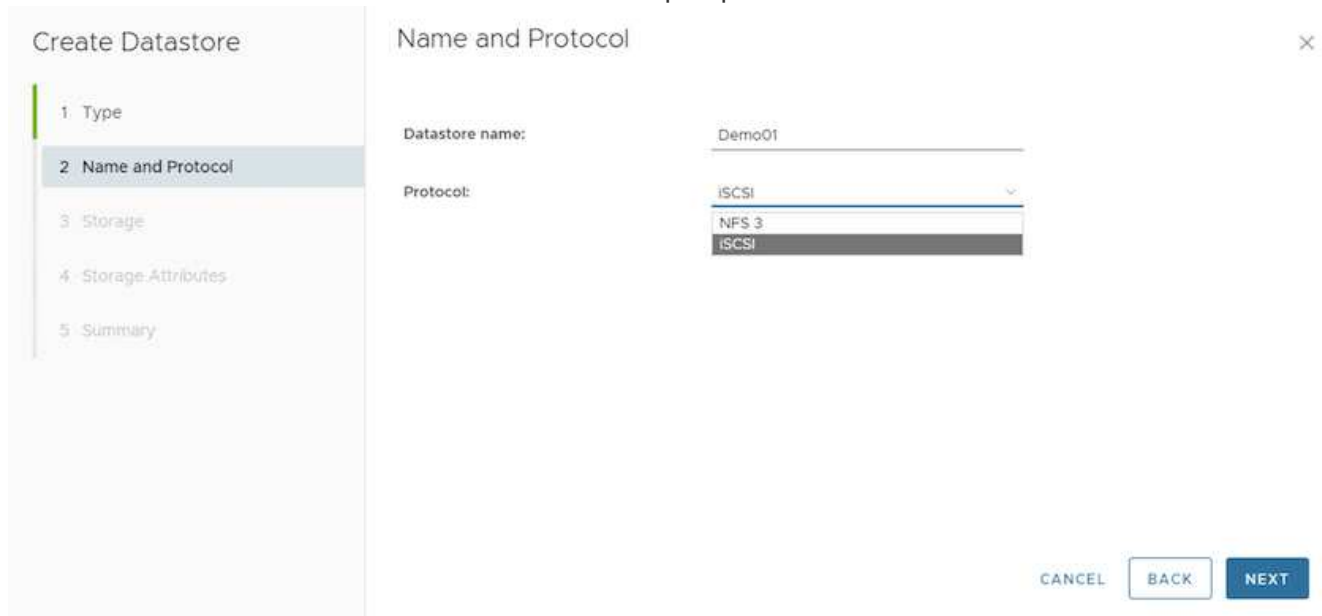
1. Right click on vSphere cluster or host and select Create Datastore (10.1) under NetApp ONTAP tools.
2. Select the datastore type as vVols.



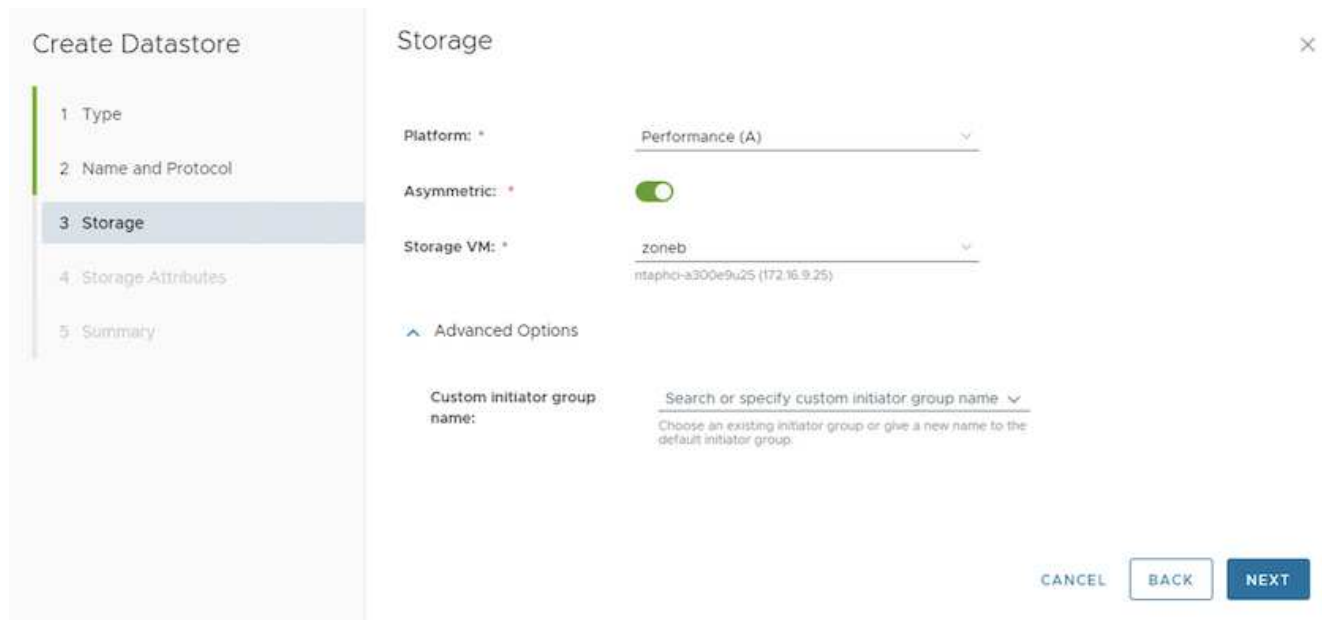
If vVols option is not available, ensure the VASA provider is registered.



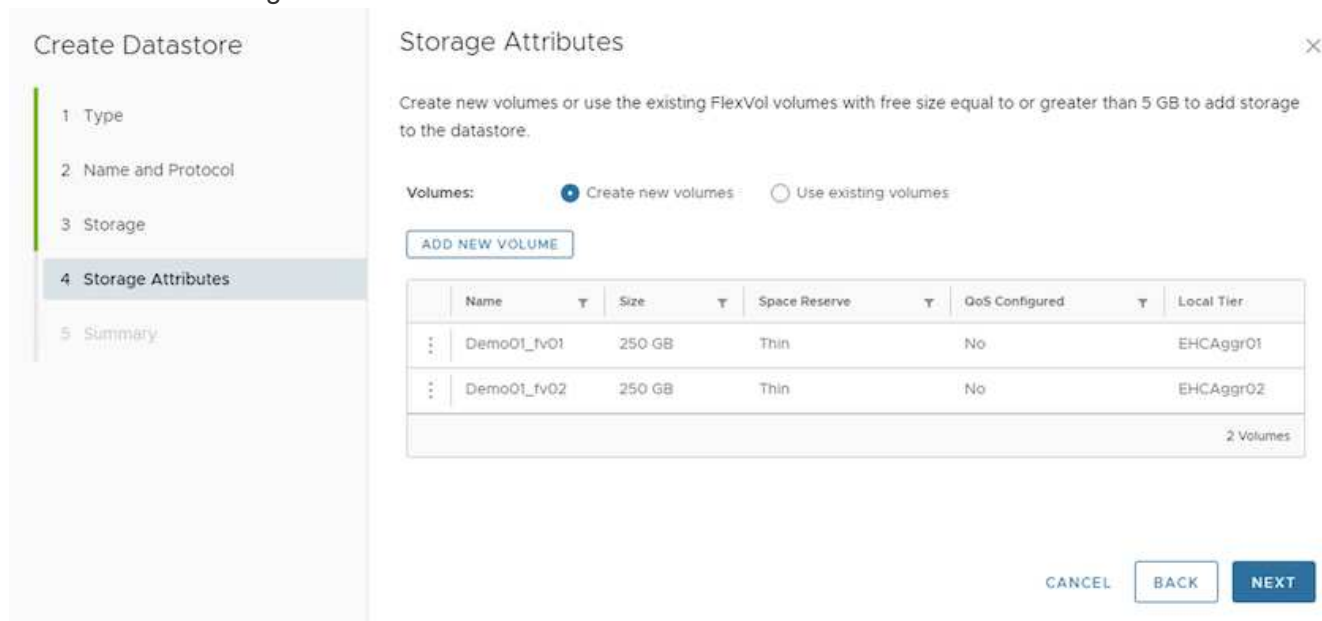
3. Provide the vVol datastore name and select the transport protocol.



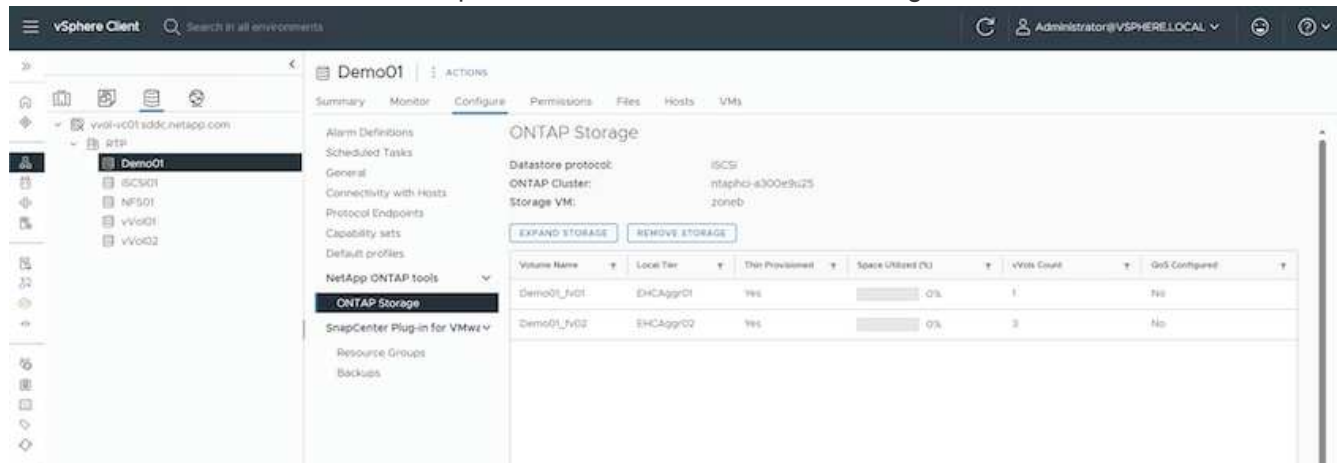
4. Select platform and Storage VM.



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



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



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

## 7. ONTAP tools provide the VM and Datastore report.

The first screenshot shows the 'Virtual Machines' report in the vSphere Client. The table lists three VMs: 'ncv', 'Demo01', and 'Demo02'. Each row includes details on Primary Datastore Type, Primary Datastore Name, vCenter VM Latency, Max Datastore Latency, Total Datastore IOPS, Average Datastore Throughput, Total Datastore Capacity, Uptime, Power State, and vCenter VM Committed Capacity.

VM Name	Primary Datastore Type	Primary Datastore Name	vCenter VM Latency	Max Datastore Latency	Total Datastore IOPS	Average Datastore Throughput	Total Datastore Capacity	Uptime	Power State	vCenter VM Committed Capacity
ncv	VMFS	GCSD01	0 ms	100 µs	0	10.89 KB/s	37.2%	10 hours	On	96.08 GB
Demo01	VVol	Demo01	-	53 µs	1	86 Bytes/s	5.03%	-	Off	287 GB
Demo02	VVol	vVol02	-	0 µs	0	0 Bytes/s	5.03%	-	Off	271 GB

The second screenshot shows the 'Datastores' report. The table lists five datastores: 'GCSD01', 'NFS01', 'vVol01', 'vVol02', and 'Demo01'. Each row includes details on Name, Space Utilized (%), Type, IOPS, Latency, Throughput, Storage VM, and Storage Cluster.

Name	Space Utilized (%)	Type	IOPS	Latency	Throughput	Storage VM	Storage Cluster
GCSD01	37.2%	VMFS	3	100 µs	10.89 KB/s	demo	ntapnci-4300w9u25
NFS01	0.0%	NFS	0	293 µs	21 Bytes/s	demo	ntapnci-4300w9u25
vVol01	5.03%	VVol	2	48 µs	81 Bytes/s	demo	ntapnci-4300w9u25
vVol02	5.0%	VVol	0	0 µs	0 Bytes/s	demo	ntapnci-4300w9u25
Demo01	5.03%	VVol	1	53 µs	86 Bytes/s	demo	ntapnci-4300w9u25

## 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 10.10.102.12-8144

Dashboard Settings Resource Groups Policies **Storage Systems** Guest File Restore

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.

Name	Display Name	Type	Protocol	Port	Username	SVM	TimeOutSec	Certificate
B:RTH-C503-5403-orig.e...	nasadm-4300e9a25	ONTAP Cluster	HTTPS	443	admin	1	60	No
VCF_SCSI	VCF_SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
isur0	isur0	ONTAP SVM	HTTPS	443	-	-	60	No
172.21.228.20	isur0	ONTAP SVM	HTTPS	443	-	-	60	No
HMC_SCSI_3510	HMC_SCSI_3510	ONTAP SVM	HTTPS	443	-	-	60	No
JL_SHC_SCSI	JL_SHC_SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
10.10.102.217	psdriv-symb-SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
HMC_M7	HMC_M7	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	Terna_3510_N1	ONTAP SVM	HTTPS	443	-	-	60	No
172.21.35.10	HYPERV-SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
EHC_NFS	EHC_NFS	ONTAP SVM	HTTPS	443	-	-	60	No
172.21.18.203	EHC_SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
172.21.18.18	VCF_NFS	ONTAP SVM	HTTPS	443	-	-	60	No
HMC_3510	HMC_3510	ONTAP SVM	HTTPS	443	-	-	60	No
10.10.102.4000	HMC_symb_4000	ONTAP SVM	HTTPS	443	-	-	60	No
B:ontap-destination-s40c-ne...	ontap-destination	ONTAP Cluster	HTTPS	443	admin	1	90	No
10.10.102.147	sym2	ONTAP SVM	HTTPS	443	-	-	90	No

2. Create a policy with required attributes.

## New Backup Policy



**Name**

**Description**

**Frequency**

**Locking Period**  Enable Snapshot Locking

**Retention**

**Replication**  Update SnapMirror after backup   
 Update SnapVault after backup

Snapshot label

**Advanced**

VM consistency

Include datastores with independent disks

**Scripts**

CANCEL

ADD

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

## Create Resource Group



### 1. General info & notification

### 2. Resource

### 3. Spanning disks

### 4. Policies

### 5. Schedules

### 6. Summary

Scope:

Virtual Machines

Parent entity:

Datastores

Virtual Machines

Tags

Folders

Enter available entity name

Available entities

TME01

Selected entities

BACK

NEXT

FINISH

CANCEL

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.

The screenshot shows the vSphere Client interface for a VM named TME01. The 'Configure' tab is active, and the 'Backups' section is expanded. A table displays the backup status for various VM snapshots.

Name	Status	Locations	Snapshot Lock Expiration	Created Time	Mounted	Policy	VMware Snapshot
TME_00-05-2024_00.4	Completed	Primary & Secondary	-	8/15/2024 10:44:10 AM	No	hourly	No
TME_00-05-2024_00.2	Completed	Primary & Secondary	-	8/15/2024 10:24:52 AM	No	hourly	No
TME_00-05-2024_00.5	Completed	Primary	-	8/15/2024 9:53:15 AM	No	hourly	No
TME_00-05-2024_00.4	Completed	Primary	-	8/15/2024 9:47:24 AM	No	hourly	No
TME_00-05-2024_00.4	Completed	Primary	-	8/15/2024 9:44:50 AM	No	hourly	No
TME_00-05-2024_00.4	Completed	Primary	-	8/15/2024 9:44:09 AM	No	hourly	No
TME_00-05-2024_00.2	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

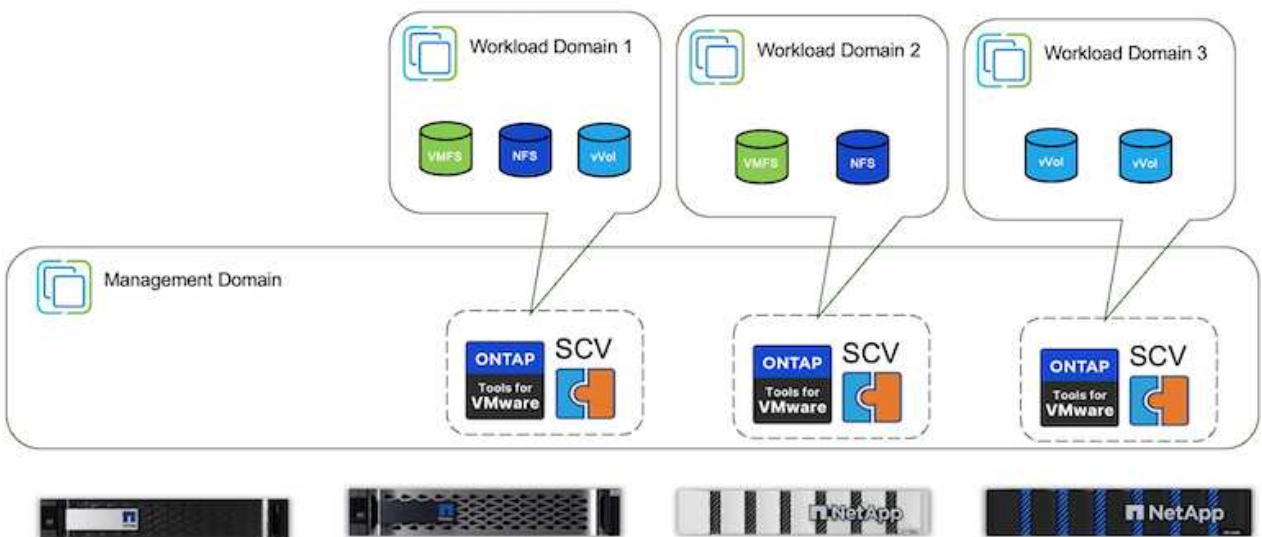
For bulk migration of VMs between vVol datastores, please do check [migrate vms to ONTAP datastore](#).

### 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.

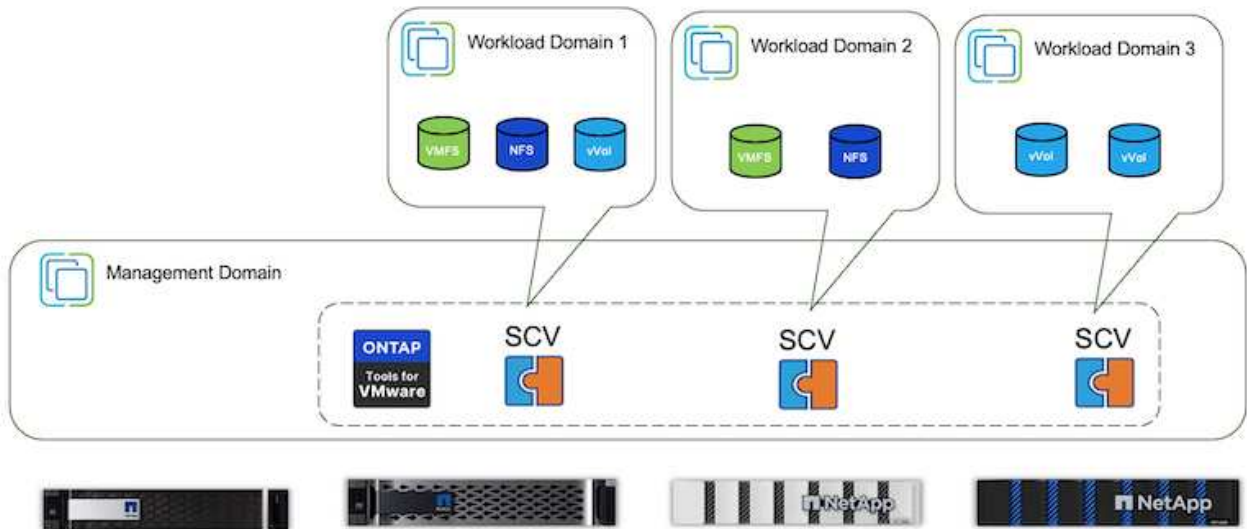


As many customers host their vCenter servers on different one rather than it is managing, similar approach is advised for ONTAP tools & SCV too.

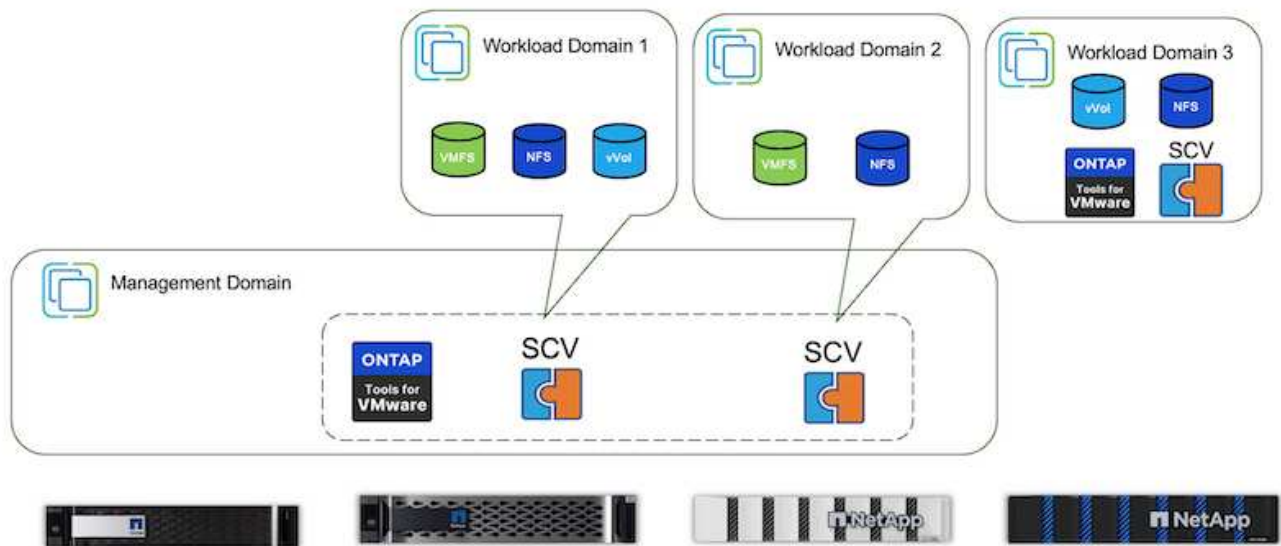


With ONTAP tools 10.x, a single instance can manage multiple vCenter environments. The storage systems are registered globally with cluster credentials and SVMs are assigned to each tenant vCenter servers.





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.

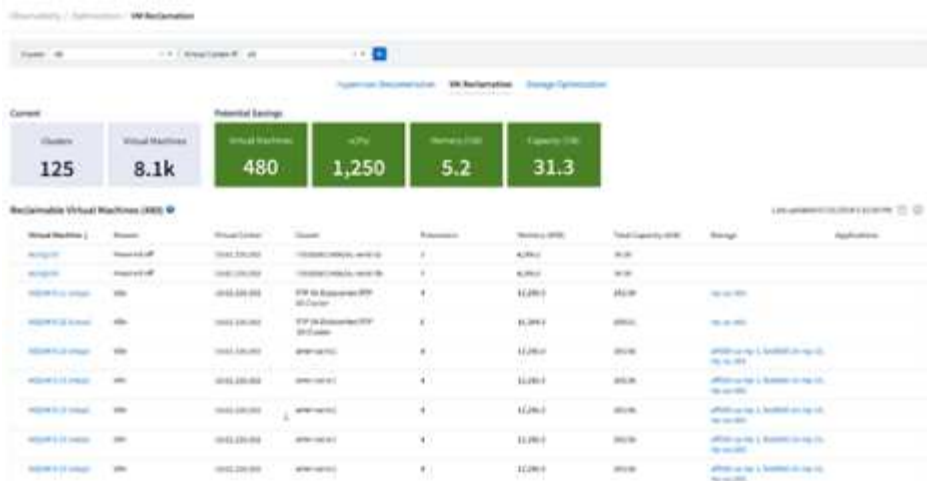
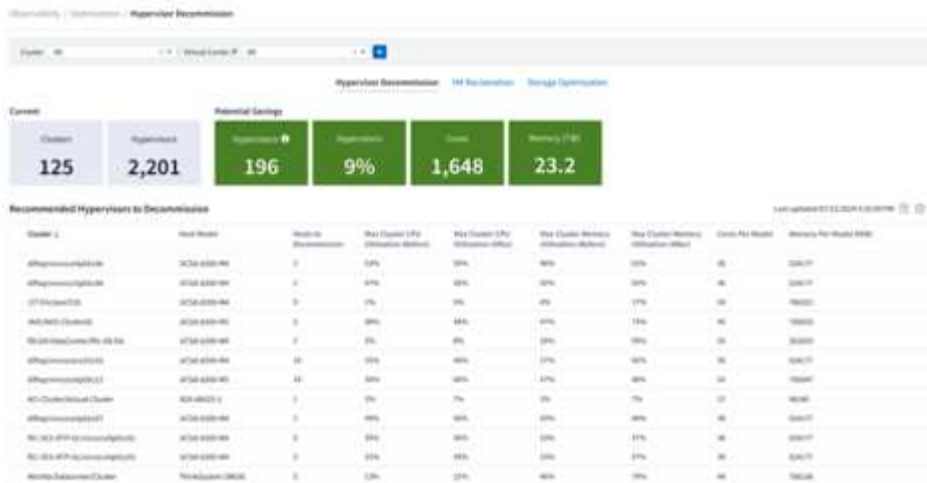
Here is a screenshot from the TCO estimator.



## 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.



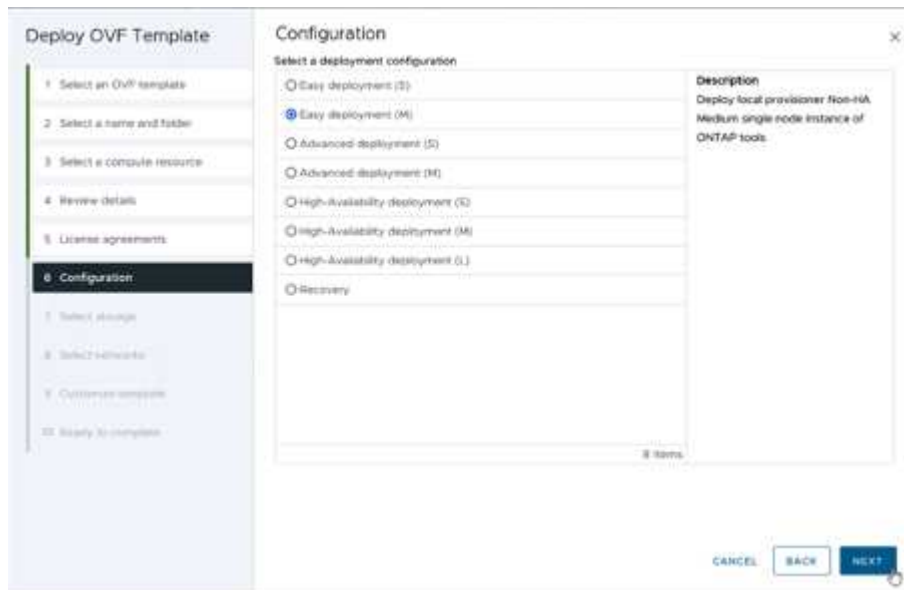
Three IP addresses are required for deployment - one IP address for load balancer, one IP address for the Kubernetes control plane and one for the node.

## 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.



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.

### 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

### Customize template

<b>Administrator username(*)</b>	Username to assign to the Administrator. Please use only a letter as the beginning. And only [a-z, 0-9, -, _] special characters are supported. <input type="text" value="admin"/>						
<b>Administrator password(*)</b>	Password to assign to the Administrator.						
	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 150px;">Password</td> <td><input type="password" value="*****"/></td> <td style="text-align: right;">👁</td> </tr> <tr> <td>Confirm Password</td> <td><input type="password" value="*****"/></td> <td style="text-align: right;">👁</td> </tr> </table>	Password	<input type="password" value="*****"/>	👁	Confirm Password	<input type="password" value="*****"/>	👁
Password	<input type="password" value="*****"/>	👁					
Confirm Password	<input type="password" value="*****"/>	👁					
<b>NTP servers</b>	A comma-separated list of hostnames or IP addresses of NTP servers. If left blank, VMware Tools based time synchronization will be used. <input type="text" value="172.21.166.1"/>						
<b>Maintenance user password(*)</b>	Password to assign to maint user account.						
	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 150px;">Password</td> <td><input type="password" value="*****"/></td> <td style="text-align: right;">👁</td> </tr> <tr> <td>Confirm Password</td> <td><input type="password" value="*****"/></td> <td style="text-align: right;">👁</td> </tr> </table>	Password	<input type="password" value="*****"/>	👁	Confirm Password	<input type="password" value="*****"/>	👁
Password	<input type="password" value="*****"/>	👁					
Confirm Password	<input type="password" value="*****"/>	👁					

CANCEL
BACK
NEXT

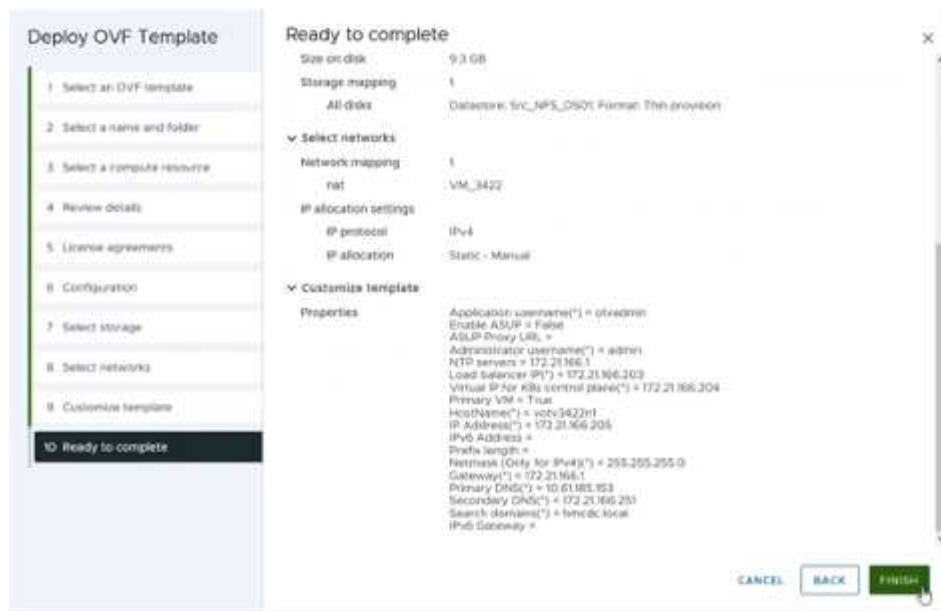
### Deploy OVF Template

- 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

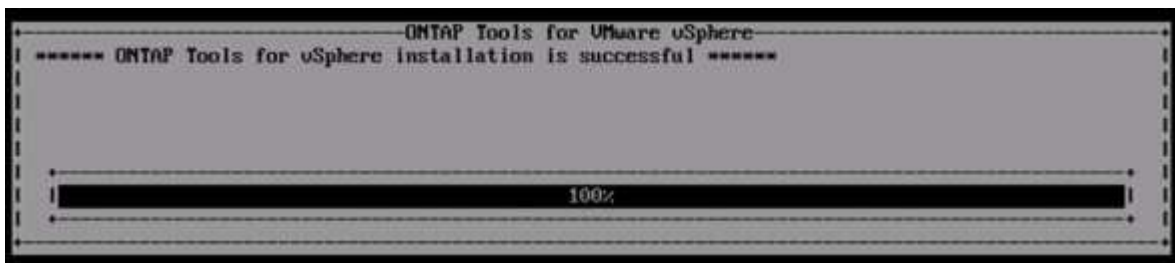
### Customize template

<b>Deployment Configuration</b>	3 settings
<b>Load balancer IP(*)</b>	Load balancer IP (*) <input type="text" value="172.21.166.203"/>
<b>Virtual IP for K8s control plane(*)</b>	Provides the virtual IP address for K8s control plane. <input type="text" value="172.21.166.204"/>
<b>Primary VM</b>	Maintain this field as selected to set the current VM as primary and install the OMTAP tools. <input checked="" type="checkbox"/>
<b>Node Configuration</b>	10 settings
<b>HostName(*)</b>	Specify the hostname for the VM. <input type="text" value="k8n3422n"/>
<b>IP Address(*)</b>	Specify the IP address for the appliance. <input type="text" value="172.21.166.205"/>
<b>IPv6 Address</b>	Specify the IPv6 address on the deployed network only when you need dual stack. <input type="text"/>
<b>Prefix length</b>	Specify the prefix length. <input type="text"/>

CANCEL
BACK
NEXT



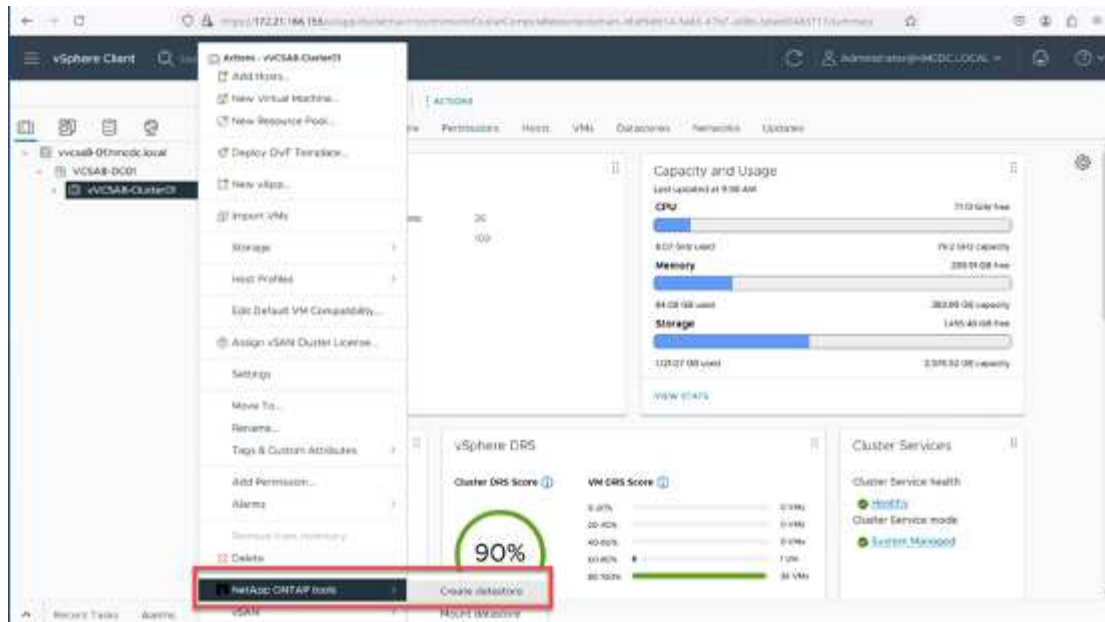
After successful installation, the web console shows the state of ONTAP tools for VMware vSphere.



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.



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.

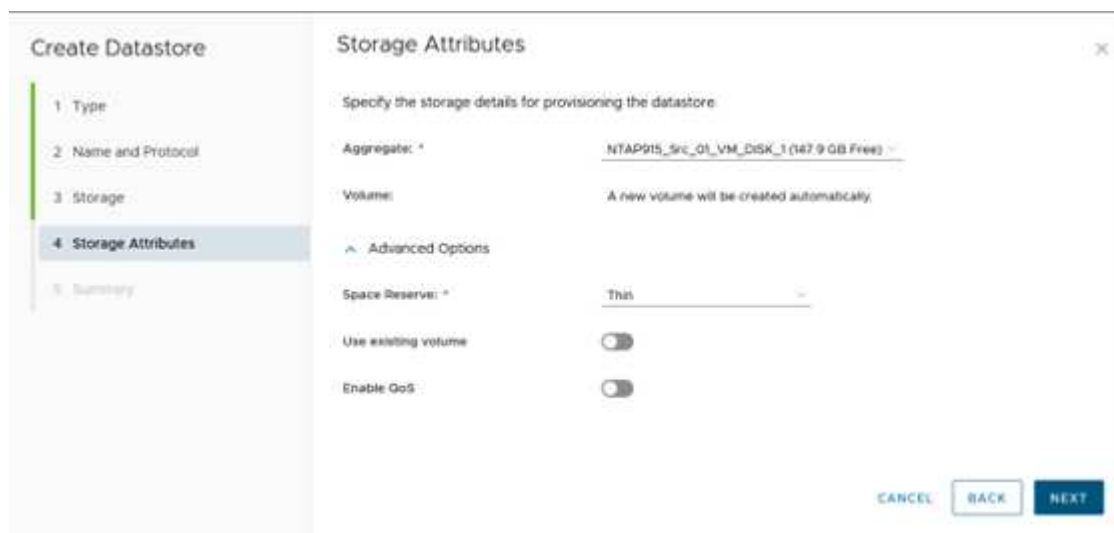


5. Select Platform and storage VM in the Storage pane. Provide the Custom initiator group name in the Advanced options section of the pane (optional). You can either choose an existing igroup for the datastore or create a new igroup with a custom name.





- 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.



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



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 vaa1 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.

The screenshot shows the vSphere Client interface. The left sidebar displays a tree view of storage devices under the path 'vcsa8-01.hmc.local > VCSA8-DC01 > ISODump > Src\_ISCSI\_DS04'. The main pane shows the 'Configure' tab for 'Src\_ISCSI\_DS04'. A table titled 'Hardware acceleration is supported on all hosts' is displayed, with a red box highlighting its content.

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

At the bottom of the interface, a 'Recent Tasks' table is visible, currently showing 'No items found'.



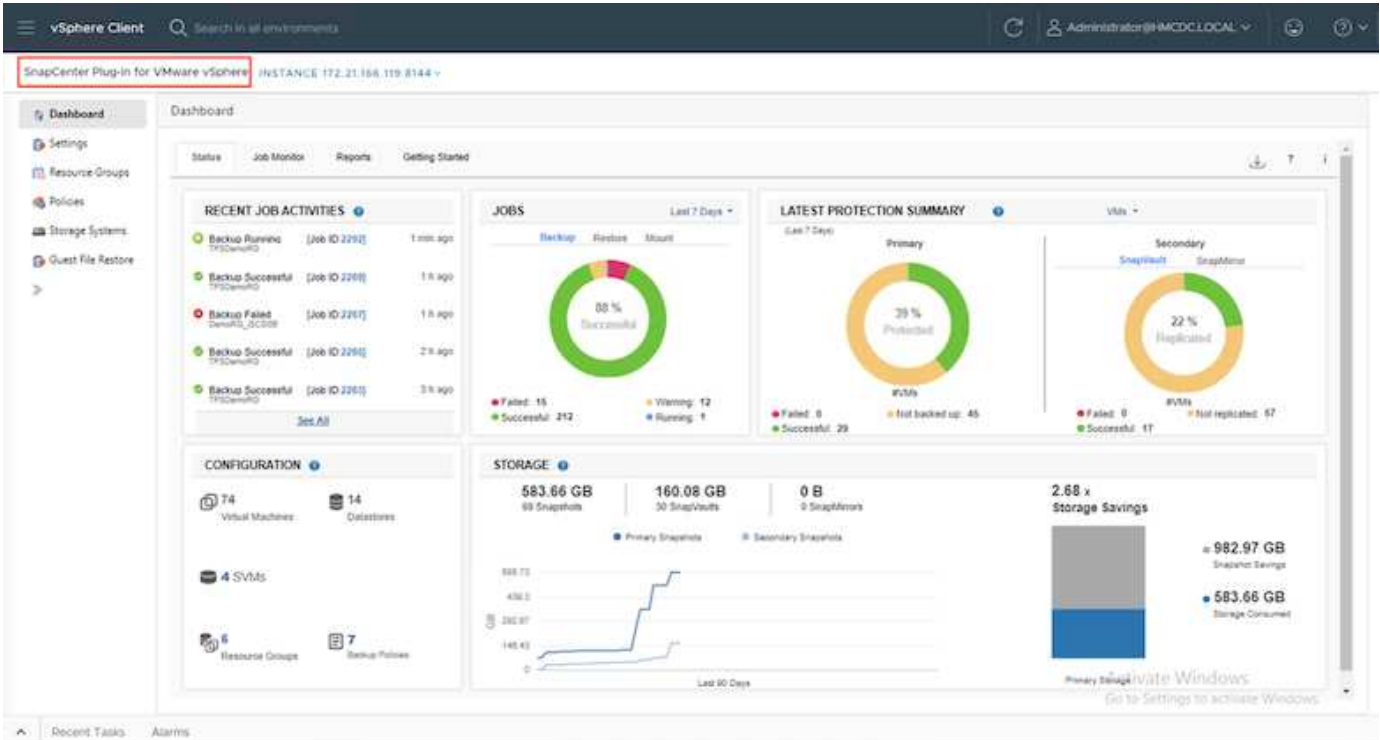
These values are easily set using ONTAP tools for VMware vSphere. From the Overview dashboard, go to ESXi Host compliance card and Select Apply Recommended Settings option. In the Apply recommended host settings window, select the hosts and click Next to apply NetApp recommended host settings.



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

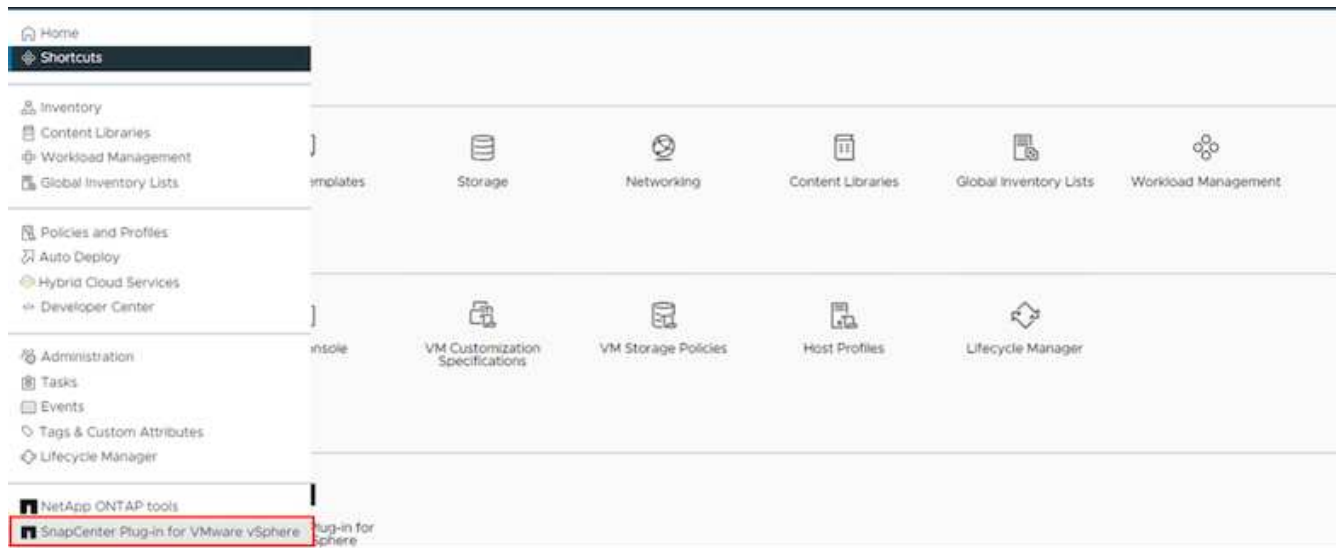
To protect VMs and iSCSI datastores hosting them, SnapCenter Plug-in for VMware must be deployed. It's a simple OVF import.

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



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



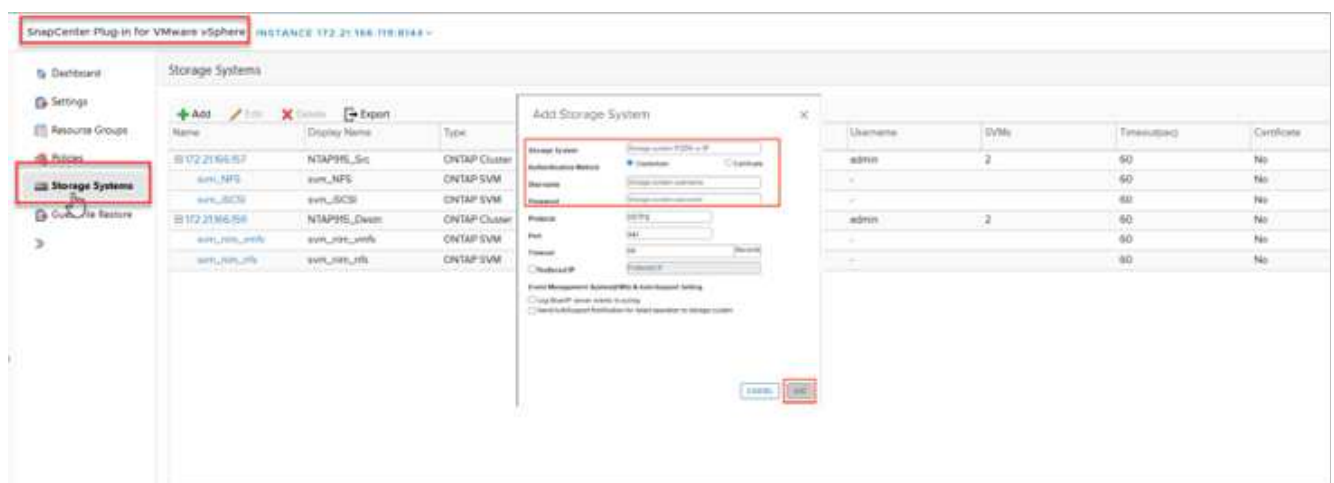
## Add storage, create policy and resource group

### 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.



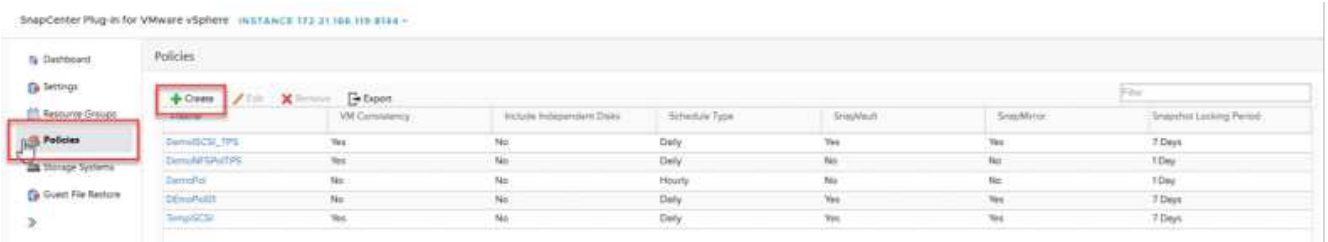


## Create backup policy

A comprehensive backup strategy includes factors like when, what to back up and how long to keep backups. Snapshots can be triggered 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.



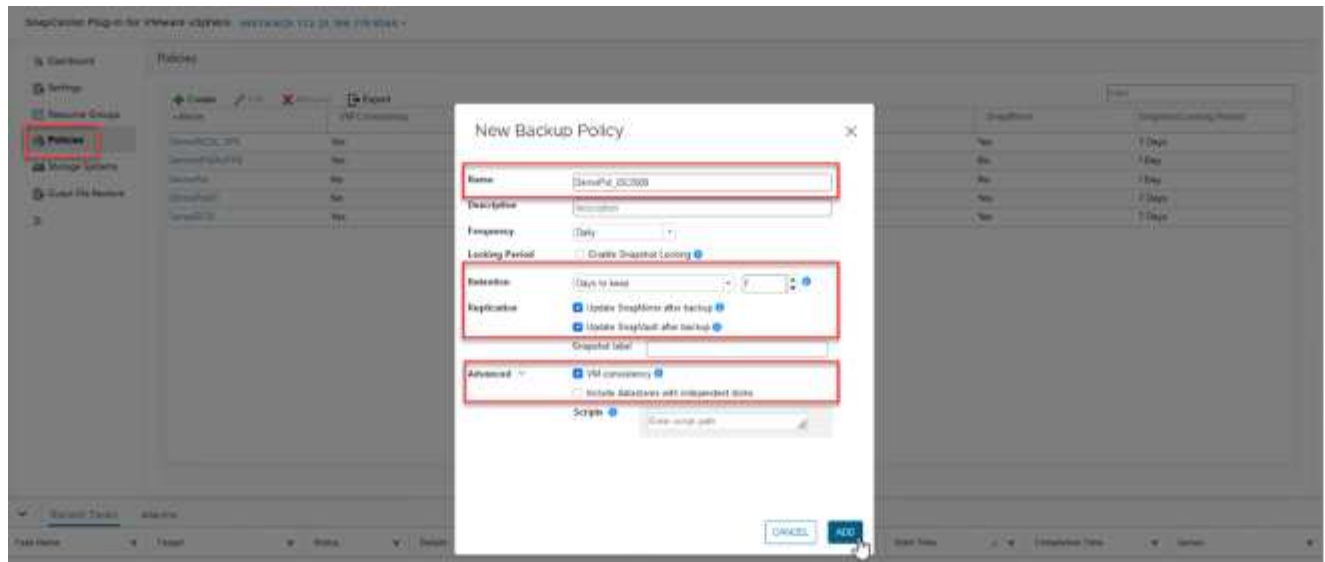
3. On the New Backup Policy page, enter the policy name.
4. Specify the retention, frequency settings and replication.



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.



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.

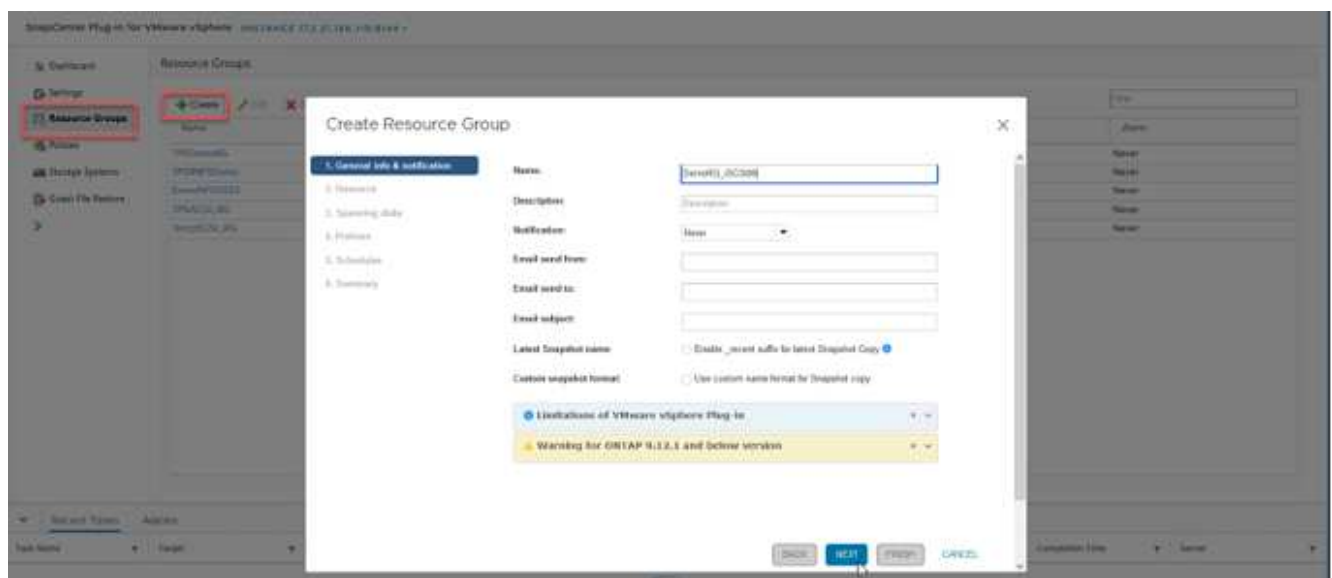
## Create Resource group

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.

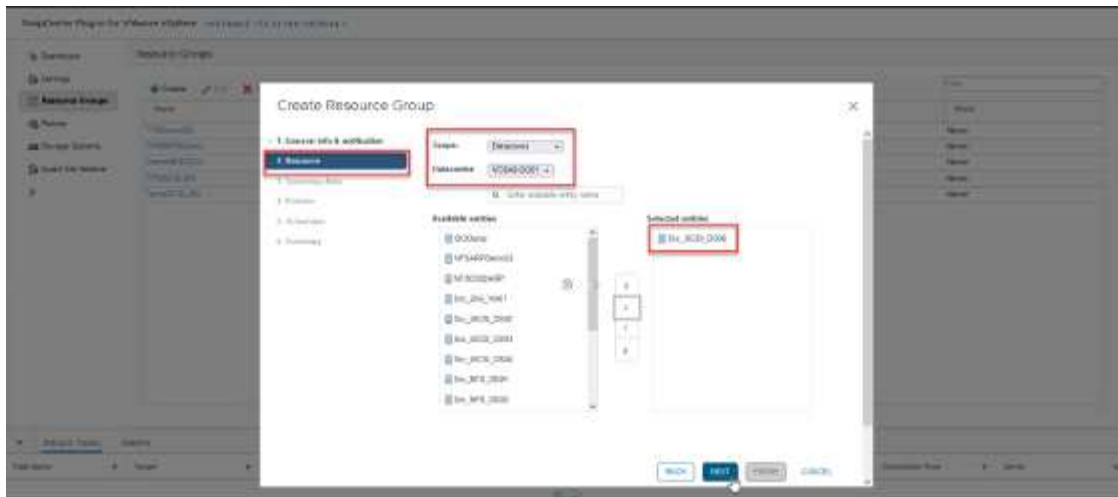
1. In the left Navigator pane of SnapCenter Plug-in for VMware, click Resource Groups.
2. On the Resource Groups page, click Create to start the wizard.

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

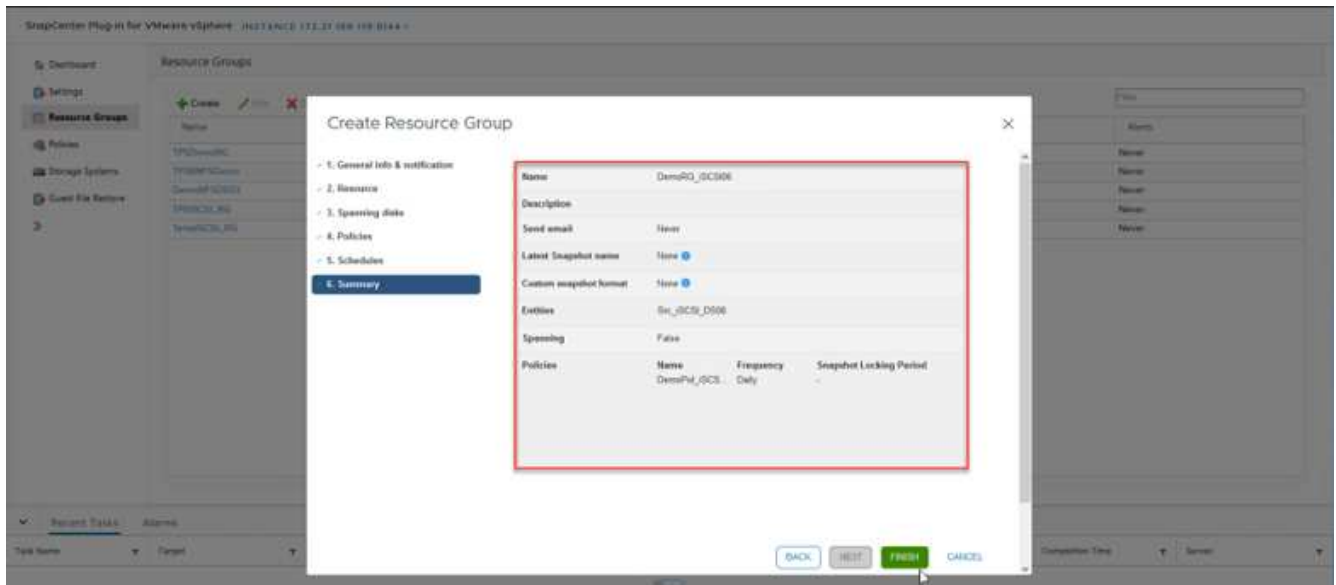


3. On the Resources page, select the scope (virtual machines or datastores) and the datacenter.



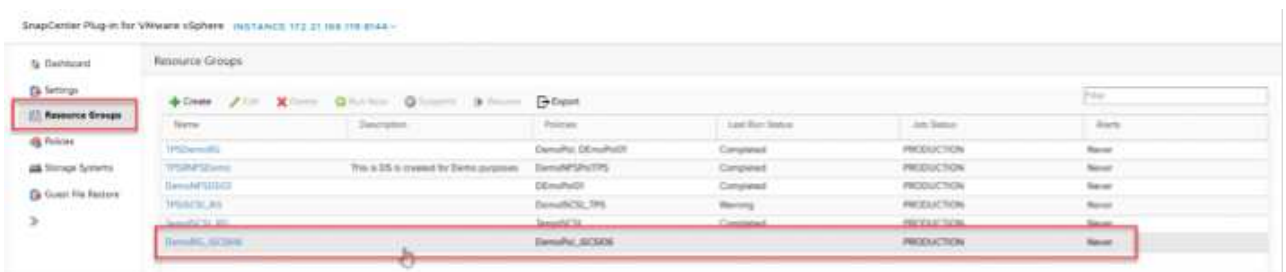


4. On the Spanning disks page, select an option for Virtual Machines with multiple VMDKs across multiple datastores
5. Next step is to associate a backup policy. Select an existing policy or create a new backup policy.
6. On the Schedules page, configure the backup schedule for each selected policy.



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

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





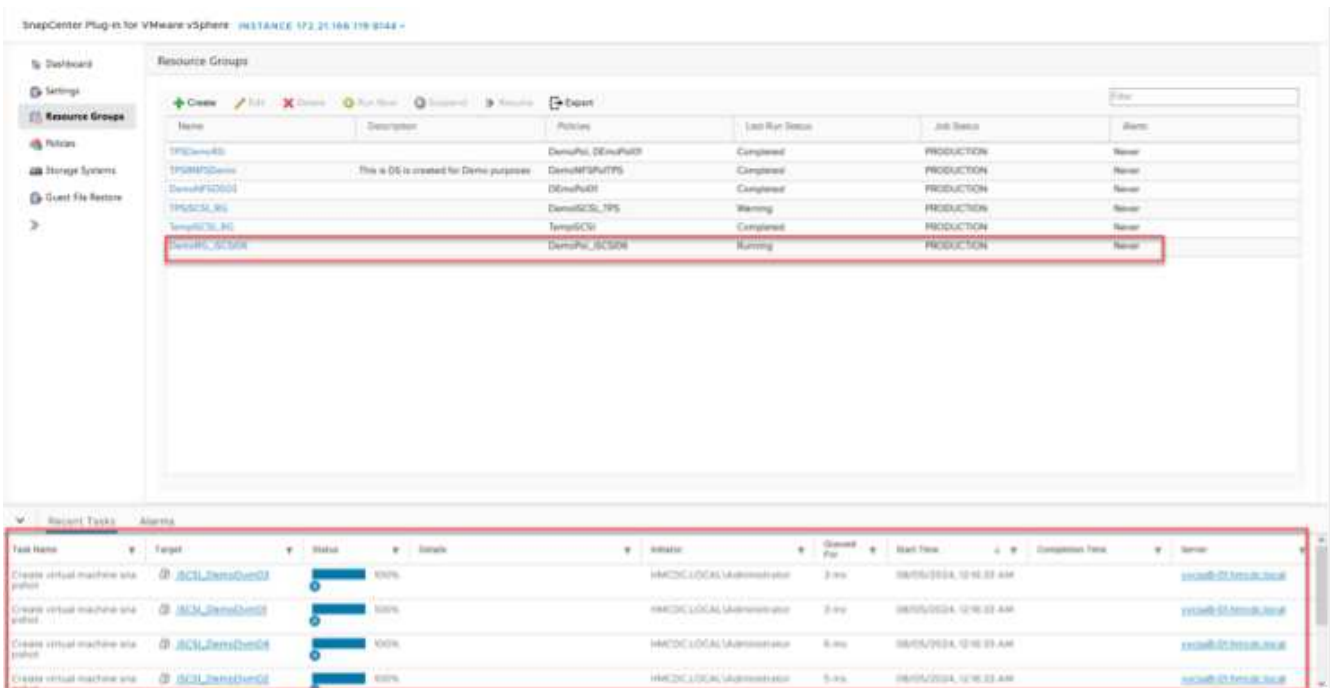
## Back up resource groups

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.



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.



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

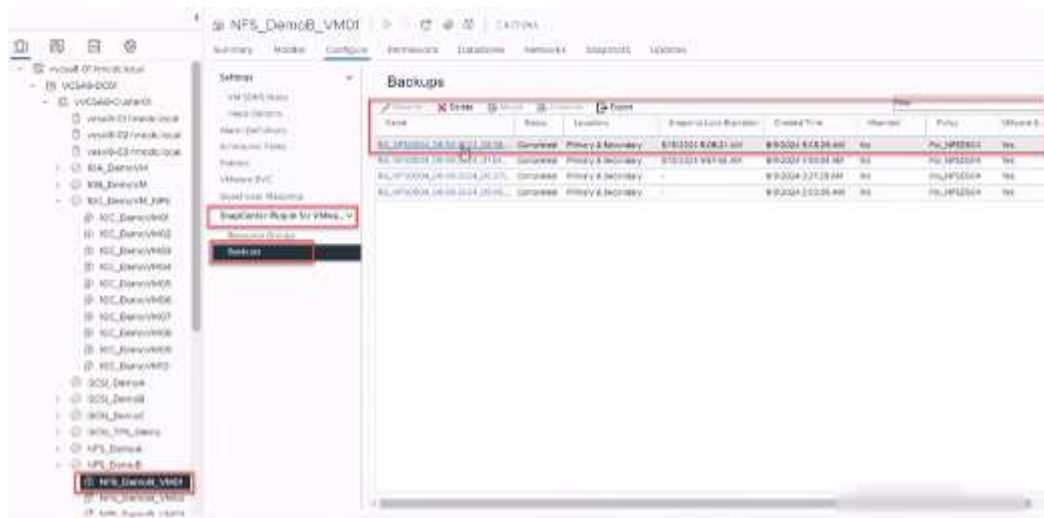
## Restore VMs from backup

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:

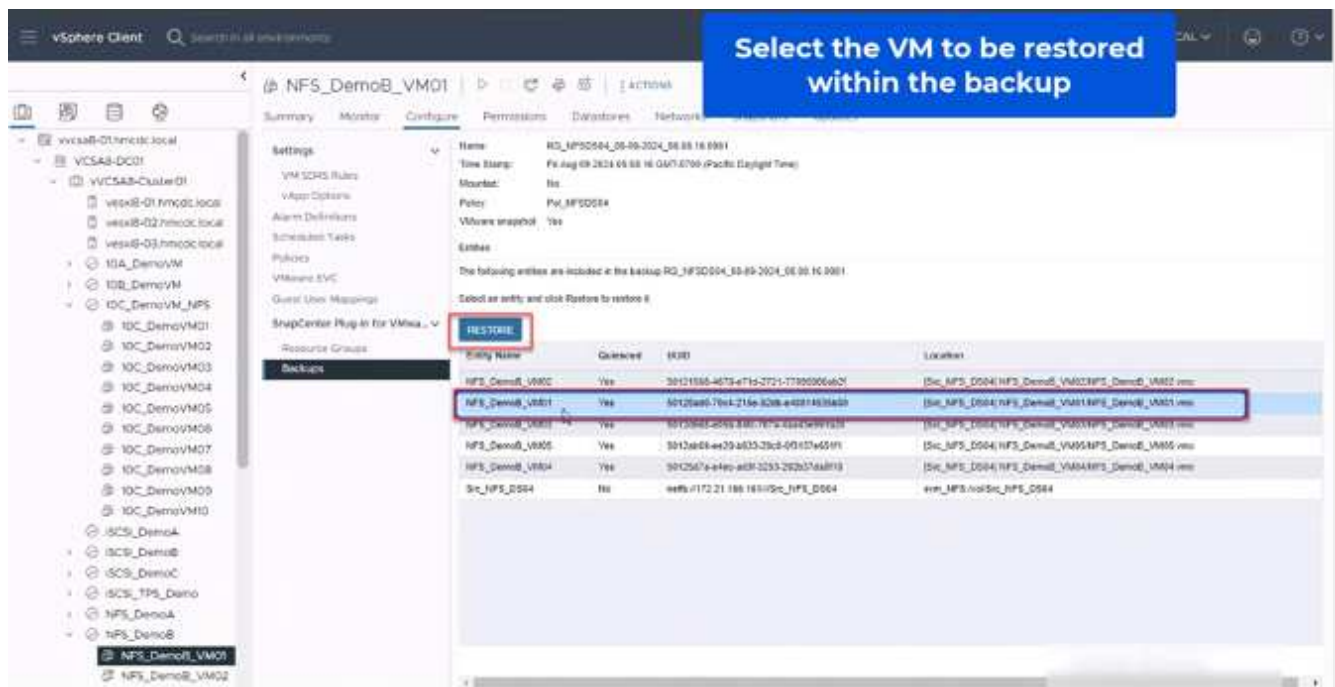
1. In the VMware vSphere web client GUI, select Menu in the toolbar. Select Inventory and then Virtual

Machines and Templates.

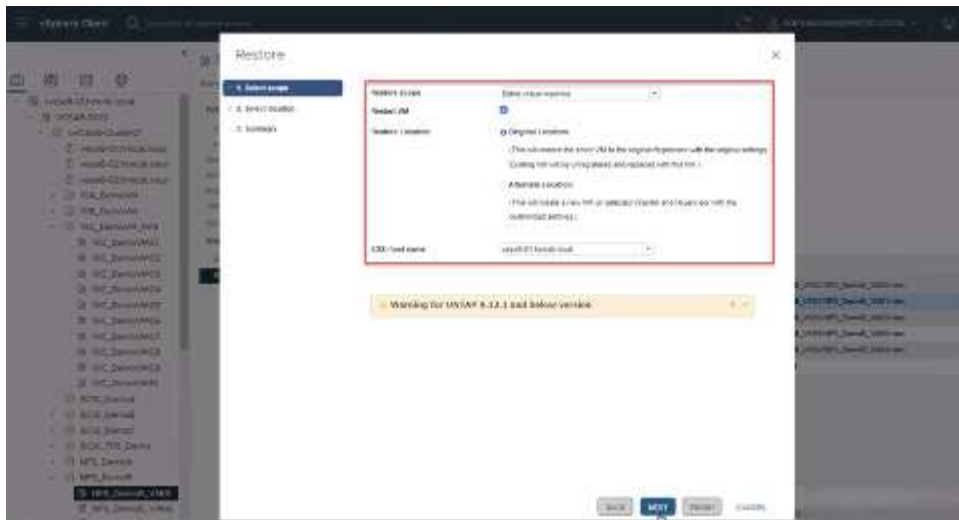
2. In the left navigation, Select the Virtual Machine, then select Configure tab, Select Backups under SnapCenter Plug-in for VMware. Click on the backup job from which the VM needs to be restored.



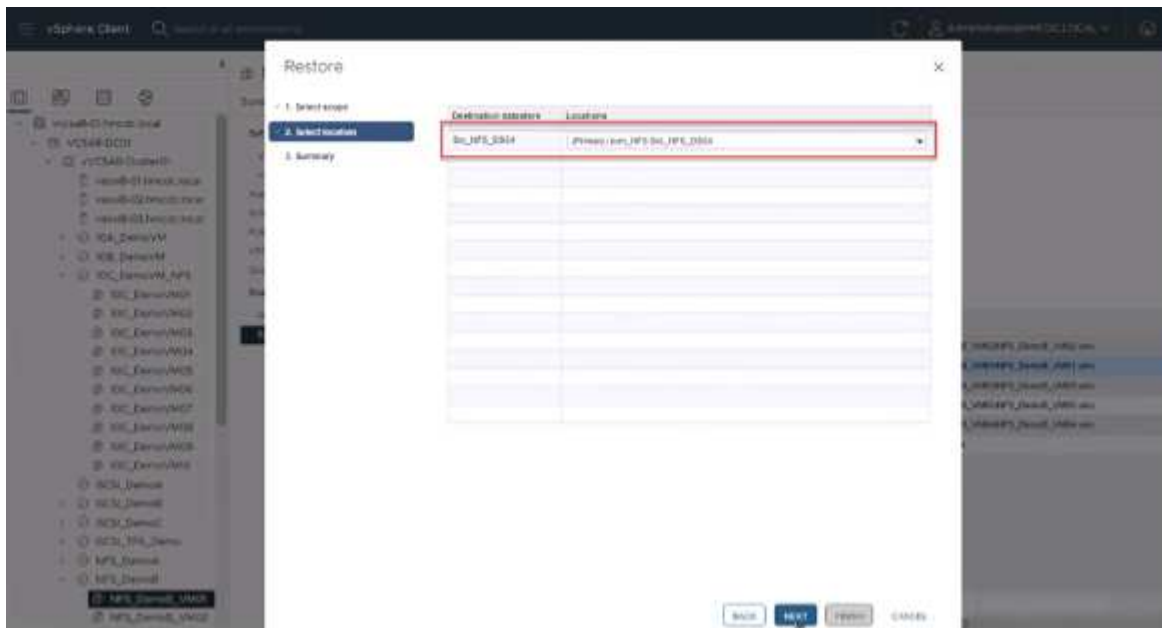
3. Select the VM that needs to be restored from the backup.



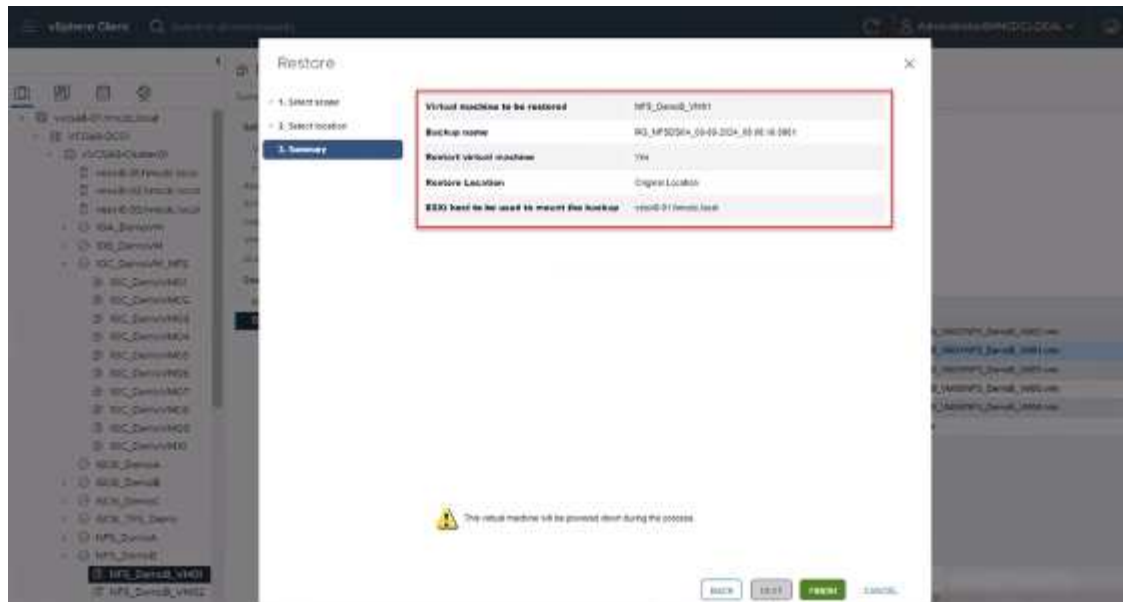
4. On the Select Scope page, select Entire Virtual Machine in the Restore scope field, then select Restore location, and then enter the destination ESXi information where the backup should be mounted. Enable Restart VM checkbox if the VM needs to be powered on after the restore operation.



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



6. Review the Summary page and then select Finish.

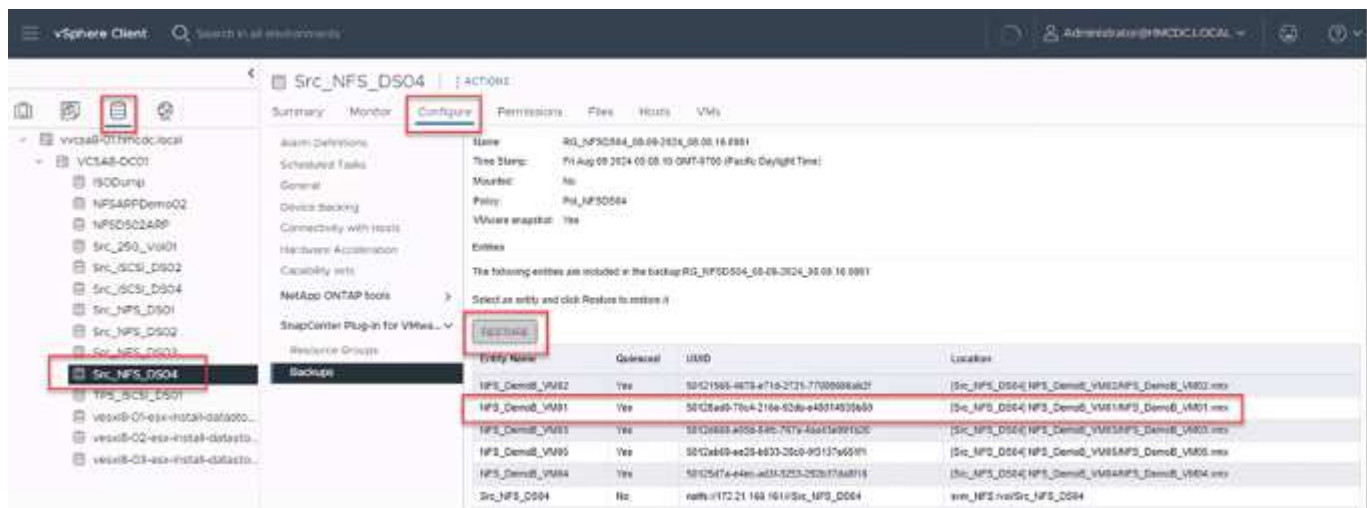


Monitor the operation progress by selecting Recent Tasks at the bottom of the screen.



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.

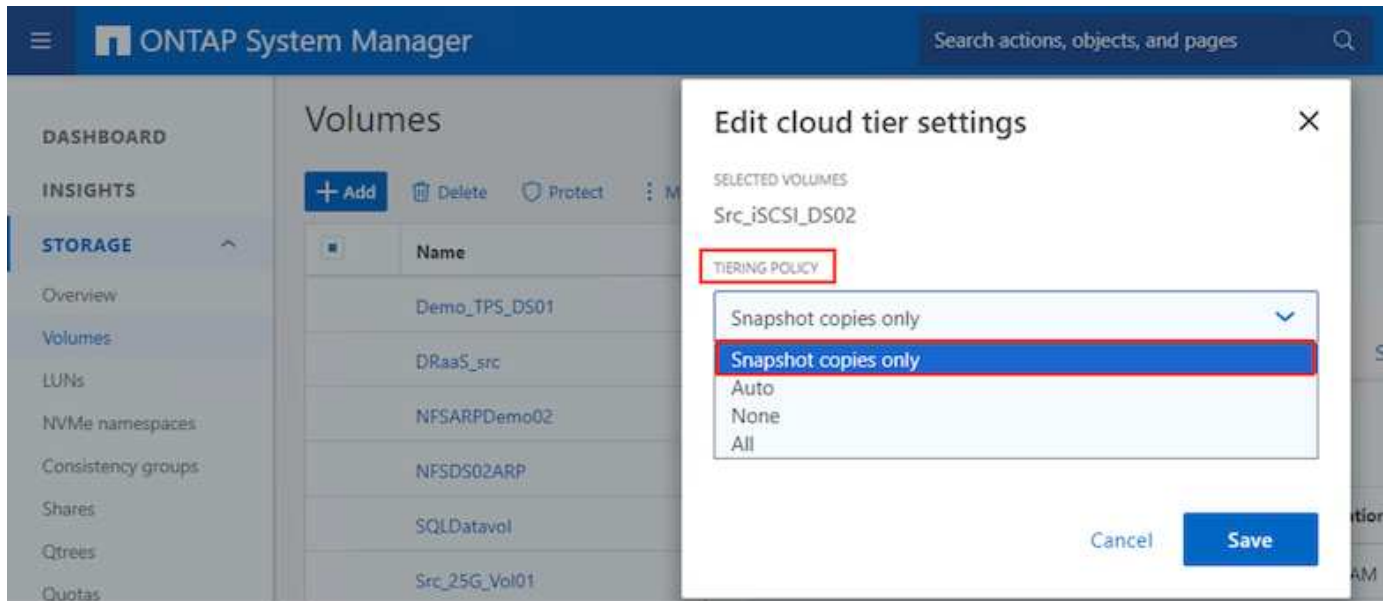


To summarize, when using ONTAP ASA storage to optimise TCO for a VMware deployment, use SnapCenter Plug-in for VMware as a simple and efficient method for backing up VMs. It enables to back up and restore VMs in a seamless and fast manner as snapshot backups take literally seconds to complete.

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).

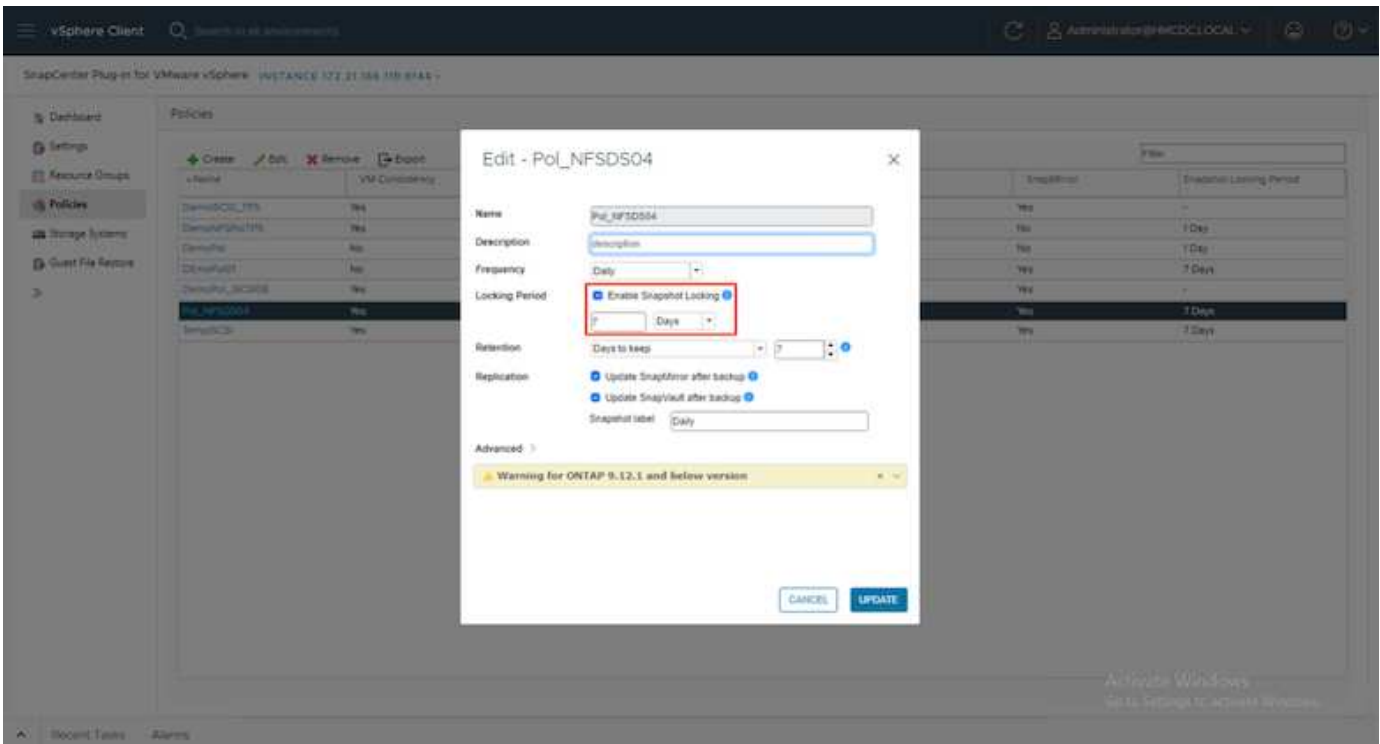


View detailed guidance for [VMware vSphere with ONTAP](#).

## 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.



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 hyperscaler, 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 hyperscaler

For those customers looking to use VMware Cloud on any hyperscaler 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

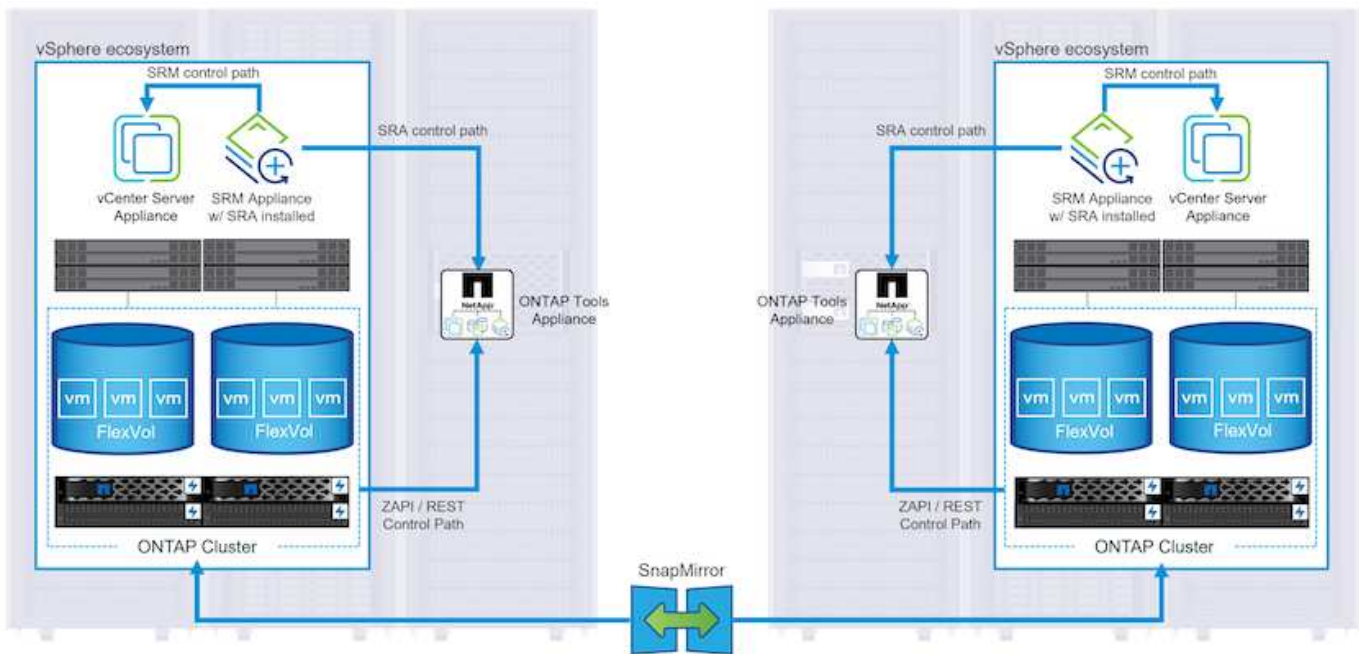
and quick recovery in the case of failure.

### 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.

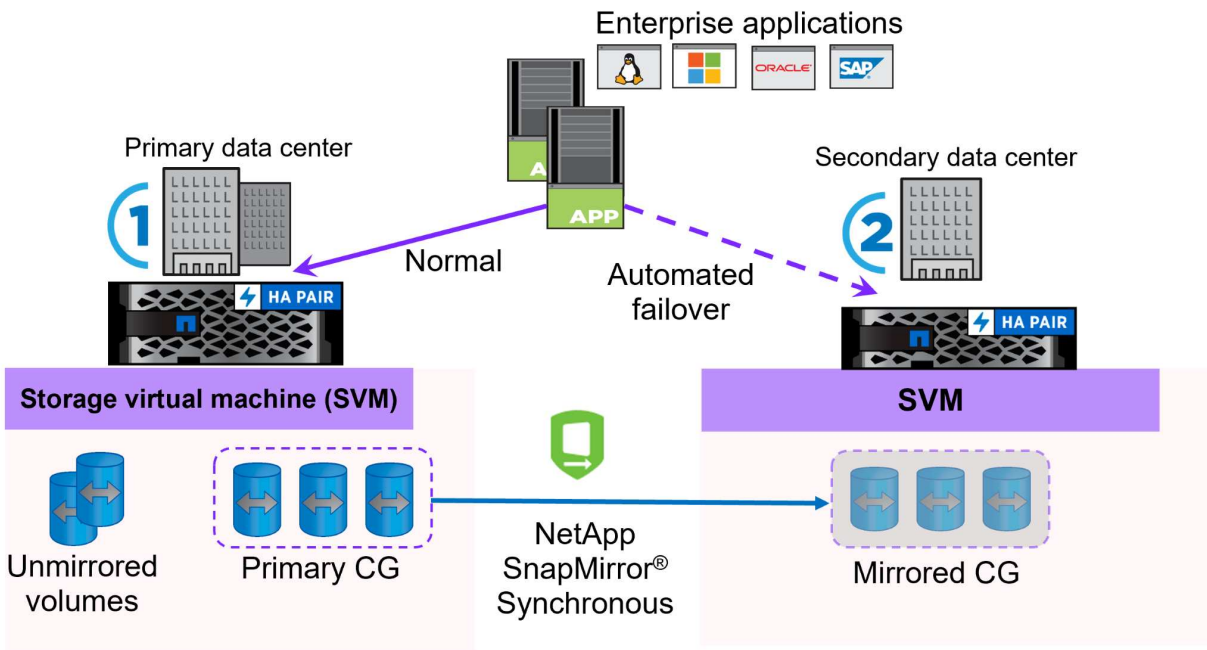
The NetApp SRA is installed as part of ONTAP Tools for VMware vSphere.



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.



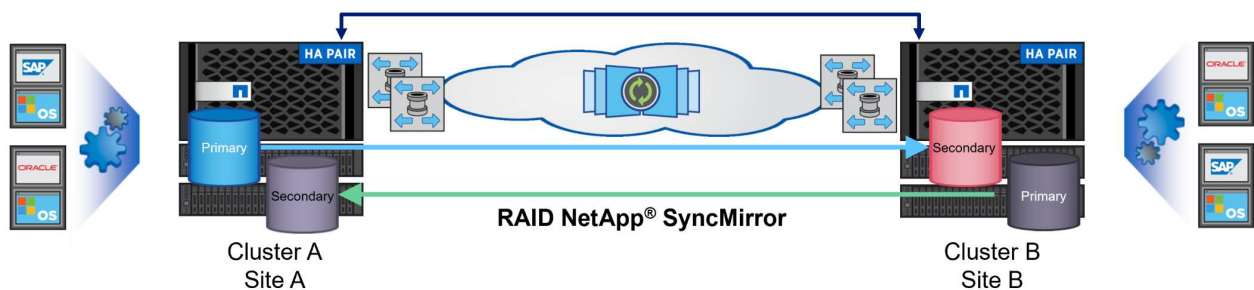
For more information refer to SnapMirror [Business Continuity overview](#).

### 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



## Managing Block Storage with ONTAP Tools for VMware vSphere

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).

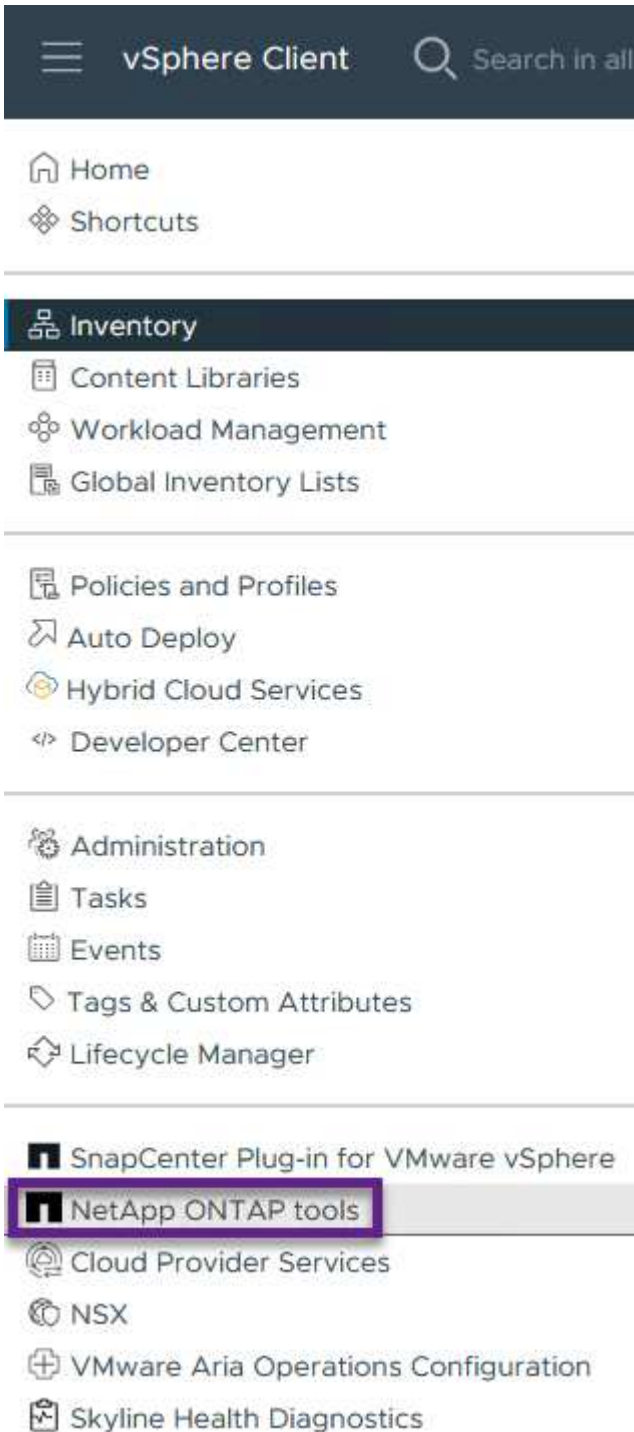
## **Solution Deployment**

### **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**.



Overview

**Storage Systems**

Storage capability profile

**Storage Systems**

**ADD** **REDISCOVER ALL**

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

CANCEL

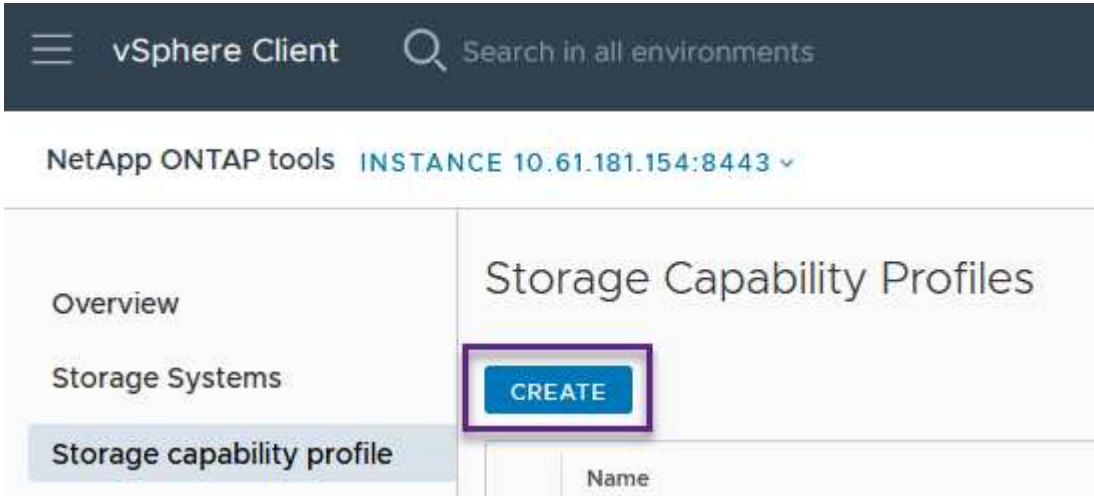
**ADD**

## Create a storage capability profile in ONTAP Tools

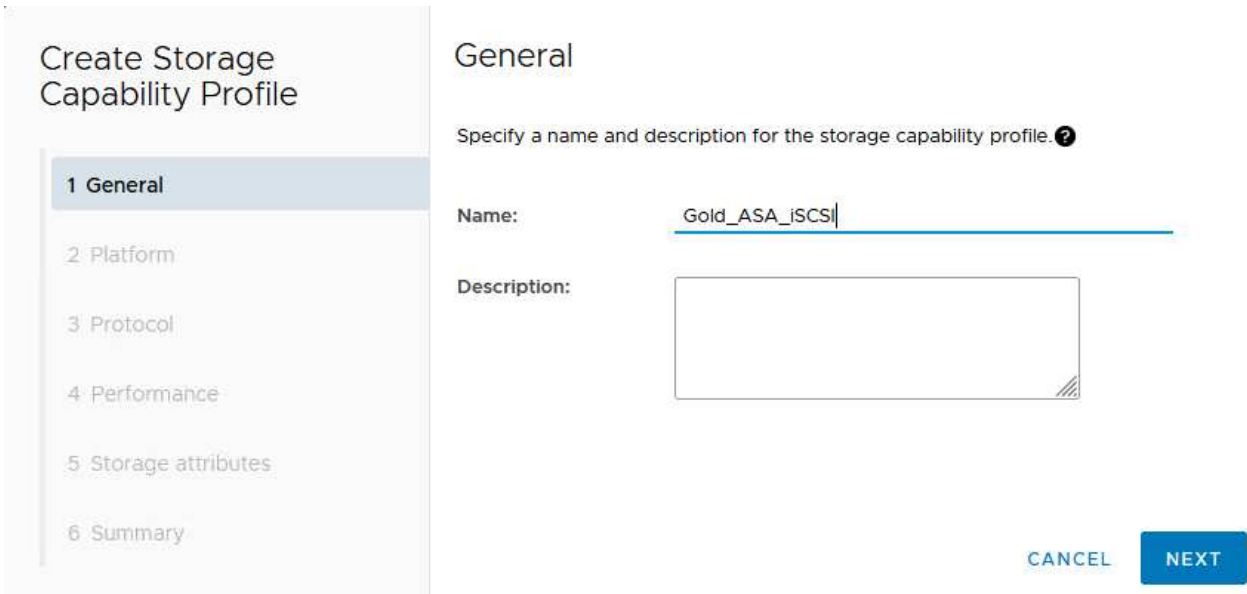
Storage capability profiles describe the features provided by a storage array or storage system. They include quality of service definitions and are used to select storage systems that meet the parameters defined in the profile.

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**.



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



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

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Platform

Platform: Performance

Asymmetric:

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Protocol

Protocol:

Any

Any

FCP

iSCSI

NVMe/FC

CANCEL

BACK

NEXT

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

CANCEL

BACK

NEXT

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

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

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

## 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

CANCEL

BACK

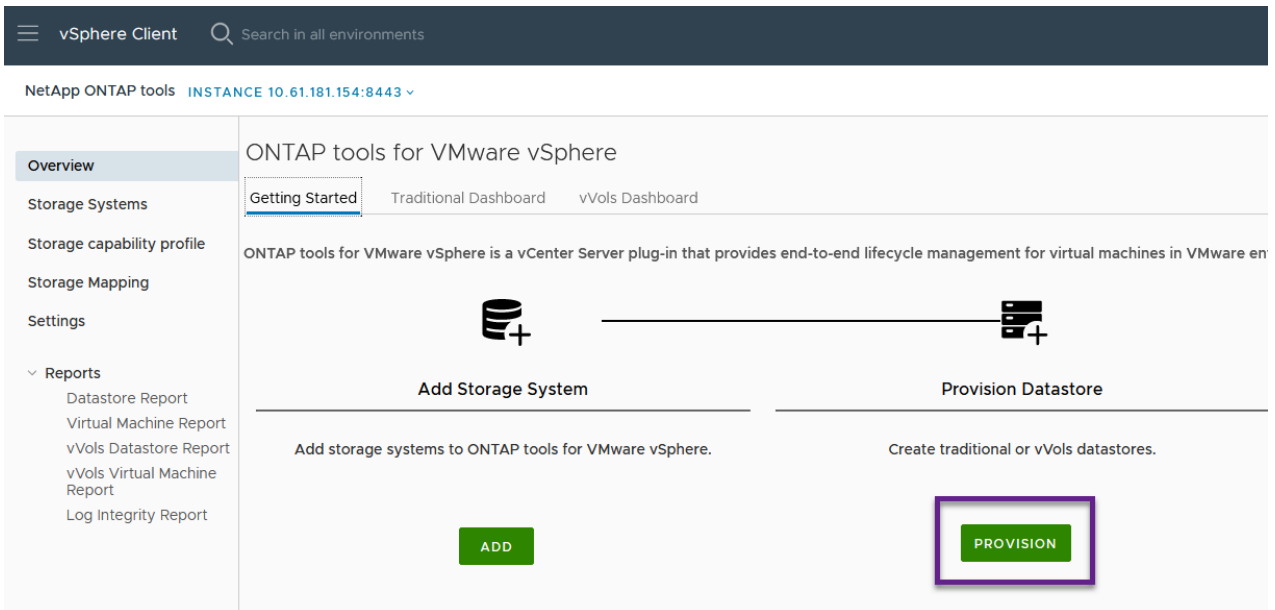
FINISH



## Create a vVols datastore in ONTAP Tools

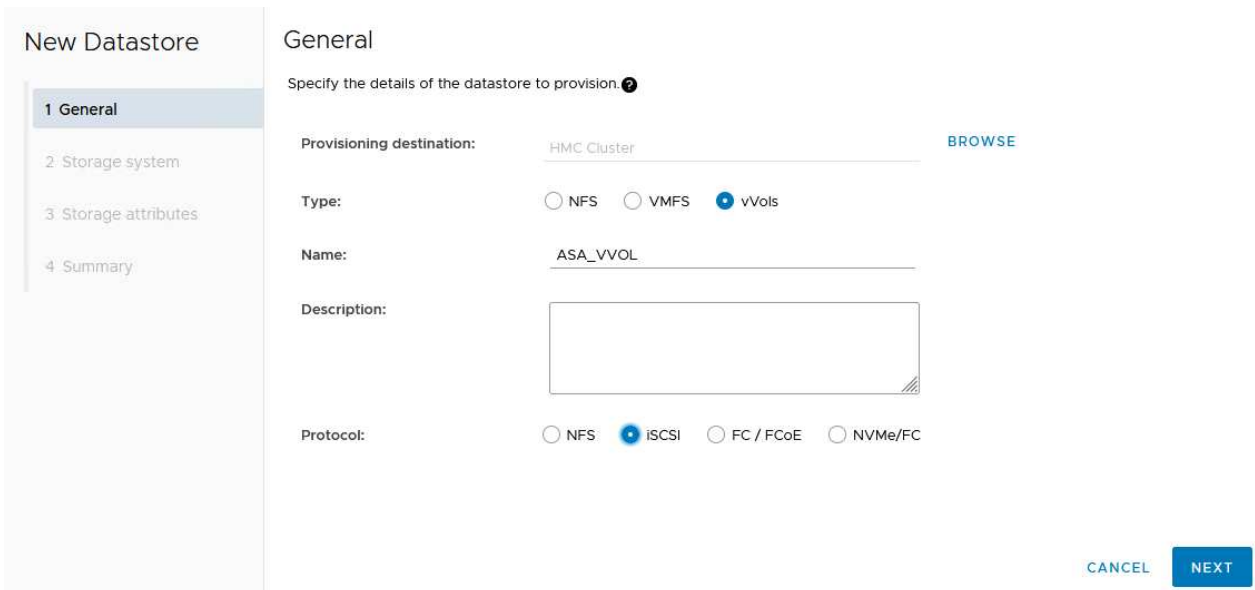
To create a vVols datastore in ONTAP Tools complete the following steps:

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



The screenshot shows the vSphere Client interface for ONTAP tools. The left sidebar has 'Overview' selected. The main content area is titled 'ONTAP tools for VMware vSphere' and has three tabs: 'Getting Started', 'Traditional Dashboard', and 'vVols Dashboard'. Below the tabs, there is a description: 'ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware en'. A diagram shows two server icons connected by a line, with 'Add Storage System' on the left and 'Provision Datastore' on the right. Below the diagram are two buttons: 'ADD' and 'PROVISION'. The 'PROVISION' button is highlighted with a purple box.

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 the protocol.



The screenshot shows the 'New Datastore' wizard in the 'General' step. The left sidebar has '1 General', '2 Storage system', '3 Storage attributes', and '4 Summary'. The main content area is titled 'General' and has a sub-header 'Specify the details of the datastore to provision.' Below this are several fields: 'Provisioning destination:' with 'HMC Cluster' and a 'BROWSE' button; 'Type:' with radio buttons for 'NFS', 'VMFS', and 'vVols' (selected); 'Name:' with 'ASA\_VVOL'; 'Description:' with an empty text area; and 'Protocol:' with radio buttons for 'NFS', 'iSCSI' (selected), 'FC / FCoE', and 'NVMe/FC'. At the bottom right are 'CANCEL' and 'NEXT' buttons.

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:

FAS\_Default  
FAS\_Max20  
**Custom profiles**  
Gold\_ASA\_JSCSI  
Gold\_ASA

Storage system:

HCG-NetApp-A400-E3U03 (10.192.102.103)

Storage VM:

svml

CANCEL

BACK

NEXT

- 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
ASA_VVOL	2000	Gold_ASA	HCG_A400_E3u3b_NVMe	Thin

ADD

CANCEL

BACK

NEXT

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

### New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

### 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

CANCEL
BACK
FINISH

## Create a VM storage policy in the vSphere client

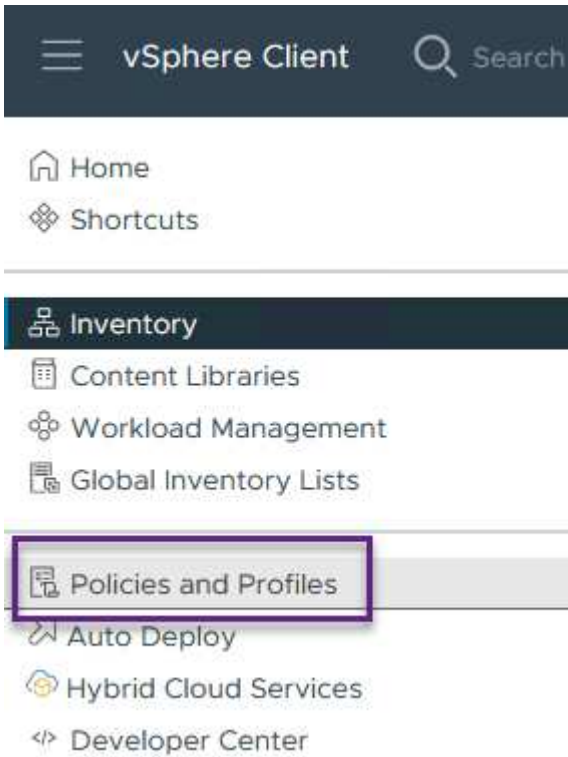
A VM storage policy is a set of rules and requirements that define how virtual machine (VM) data should be stored and managed. It specifies the desired storage characteristics, such as performance, availability, and data services, for a particular VM.

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.

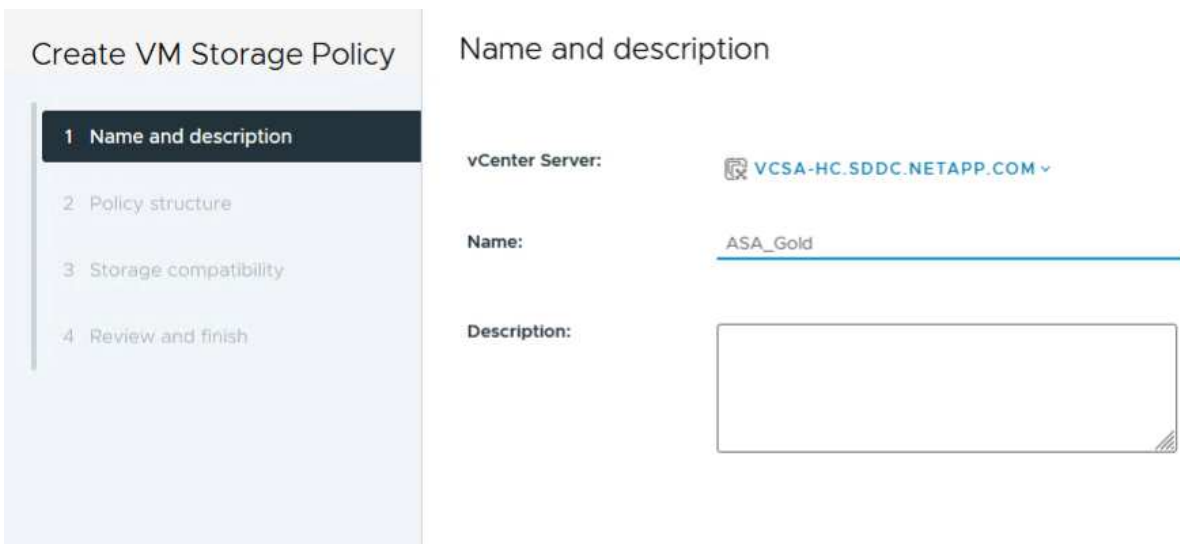
## Create a VM storage policy

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.

A screenshot of the 'Create VM Storage Policy' wizard. The left sidebar shows a progress indicator with four steps: '1 Name and description' (active), '2 Policy structure', '3 Storage compatibility', and '4 Review and finish'. The main area is titled 'Name and description' and contains three fields: 'vCenter Server' with a dropdown menu showing 'VCSA-HC.SDDC.NETAPP.COM', 'Name' with a text input field containing 'ASA\_Gold', and 'Description' with a large empty text area.

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

CANCEL BACK NEXT

- 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**

Placement Replication Tags

ProfileName ⓘ Gold\_ASA

- On the **Storage compatibility** page, review the list of vSAN datastores that match this policy and click **Next**.
- 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.

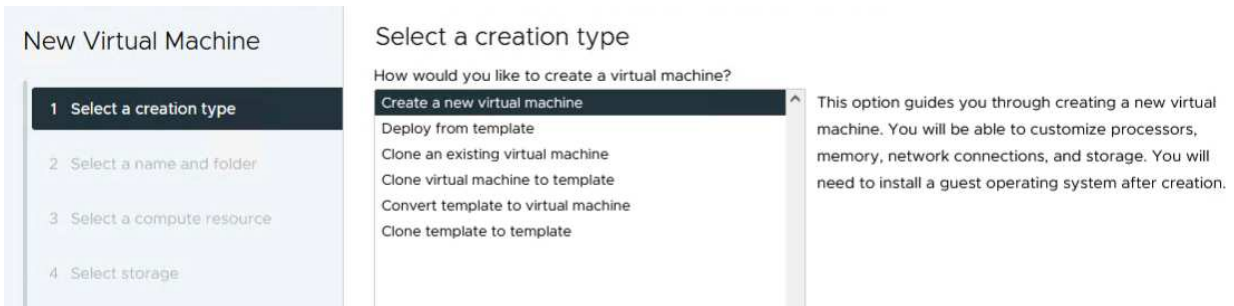
In this case, the task involves creating a VM storage policy to specify that a virtual machine will be generated

on vVol datastores and to establish a one-to-one mapping with the previously generated storage capability profile.

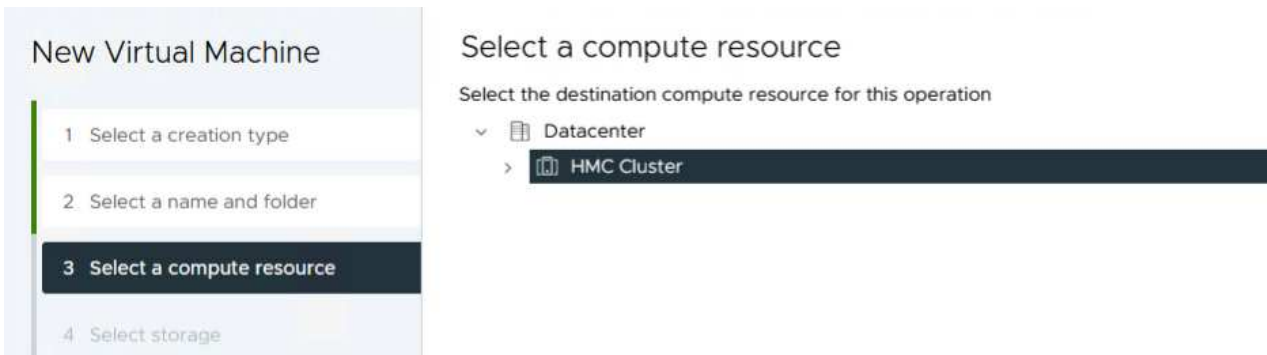
## Create a virtual machine on a vVol datastore

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.



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**.



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	
<input checked="" type="radio"/>	ASA_VVOLS_1	Compatible	1.95 TB	9 MB	1.95 TB	V
<input type="radio"/>	ASA400_ISCSI01	Incompatible	2 TB	185.32 GB	1.9 TB	V
<input type="radio"/>	DemoDS	Incompatible	800 GB	6.99 GB	793.01 GB	N
<input type="radio"/>	destination	Incompatible	250 GB	32.66 MB	249.97 GB	N
<input type="radio"/>	DRaaSTest	Incompatible	1 TB	133.27 GB	956.83 GB	N
<input type="radio"/>	esxi-hc-01 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	V
<input type="radio"/>	esxi-hc-02 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	V
<input type="radio"/>	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...

CANCEL

BACK

NEXT

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).



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

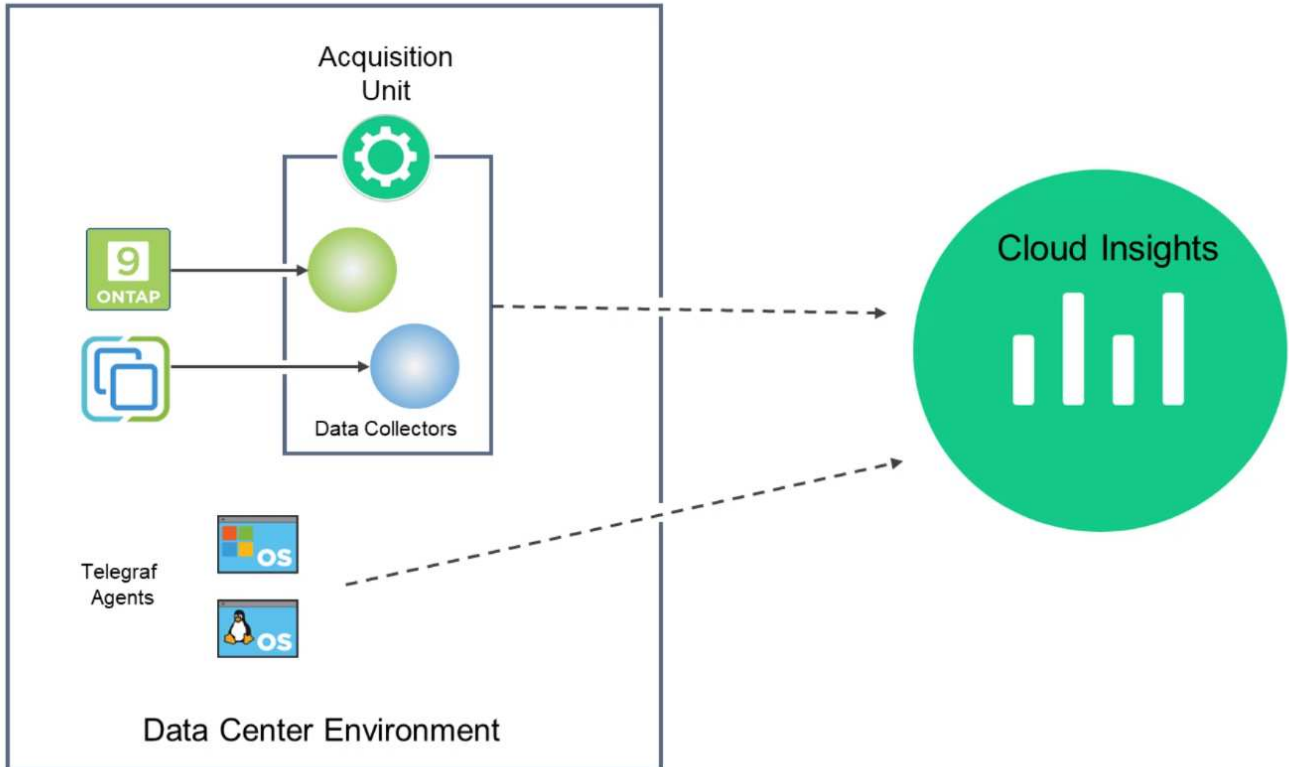
NetApp Cloud Insights is a cloud-based infrastructure monitoring and analytics platform designed to provide comprehensive visibility and insights into the performance, health, and costs of IT infrastructures, both on-premises and in the cloud. Key features of NetApp Cloud Insights include real-time monitoring, 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 Acquisition Unit software installed on a local VM with network connectivity to assets

for data collection.

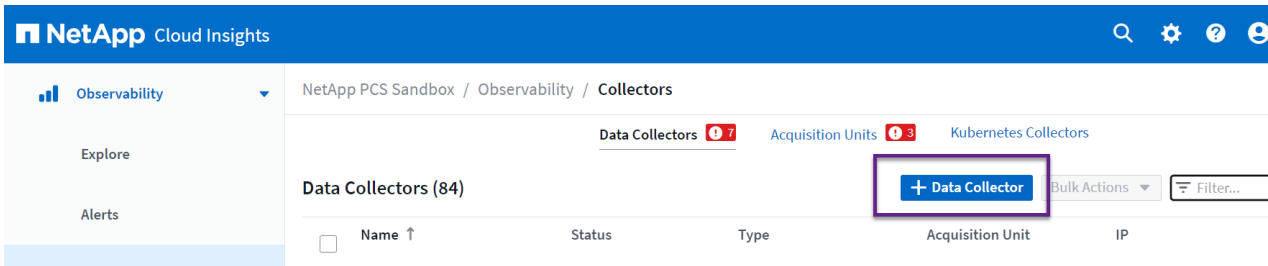
## **Solution Deployment**

### **Configure Data Collectors**

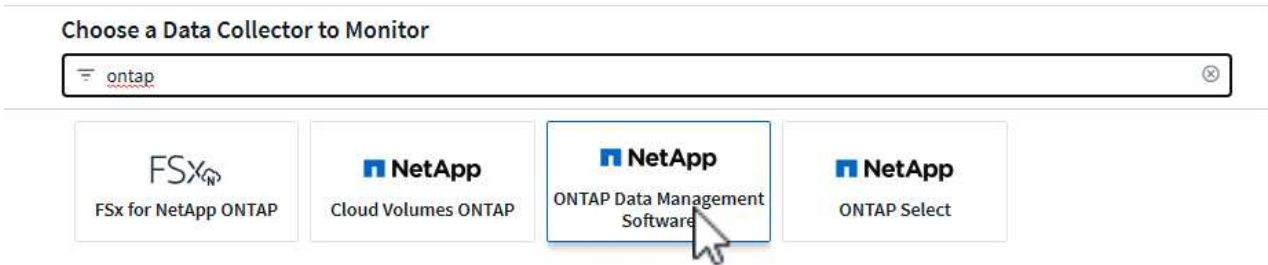
To configure Data Collectors for VMware vSphere and ONTAP storage systems complete the following steps:

## Add a Data Collector for an ONTAP storage systems

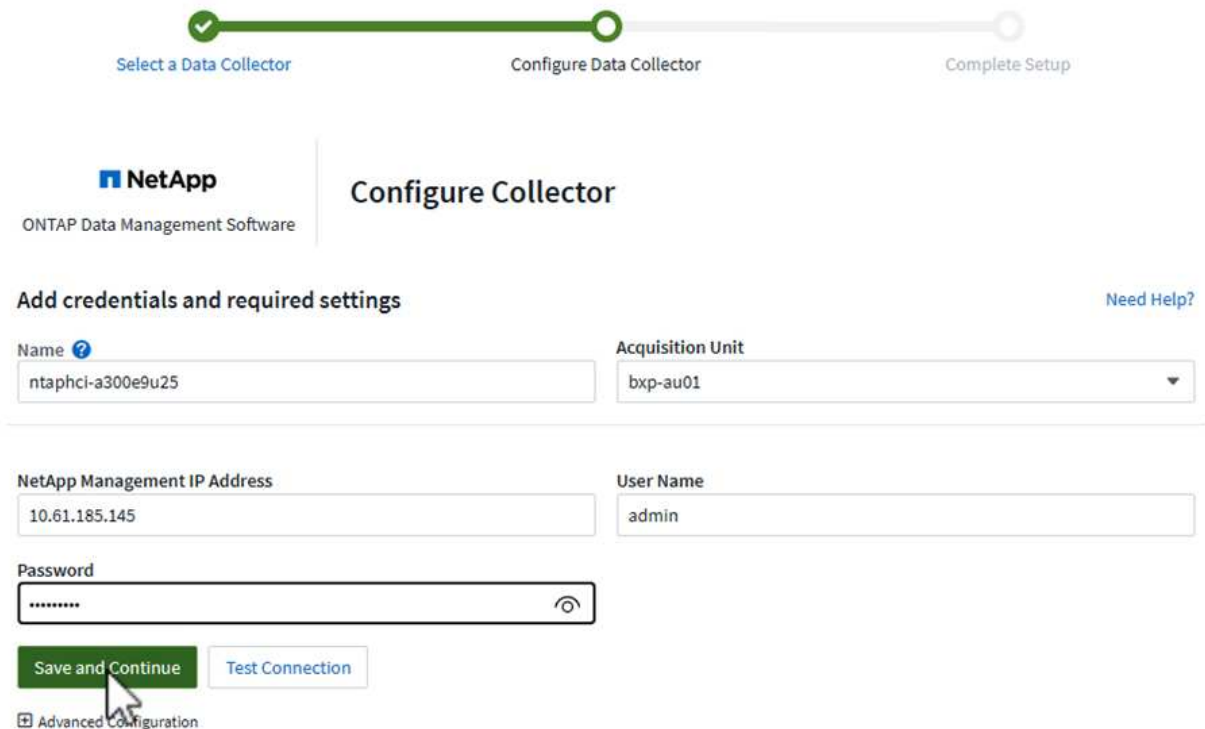
1. Once logged into Cloud Insights, navigate to **Observability > Collectors > Data Collectors** and press the button to install a new Data Collector.



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

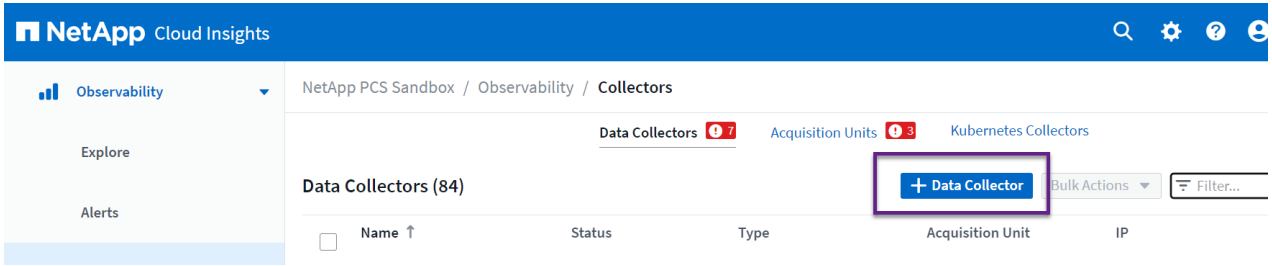


3. On the **Configure Collector** page fill out a name for the collector, specify the correct **Acquisition Unit** and provide the credentials for the ONTAP storage system. Click on **Save and Continue** and then **Complete Setup** at the bottom of the page to complete the configuration.

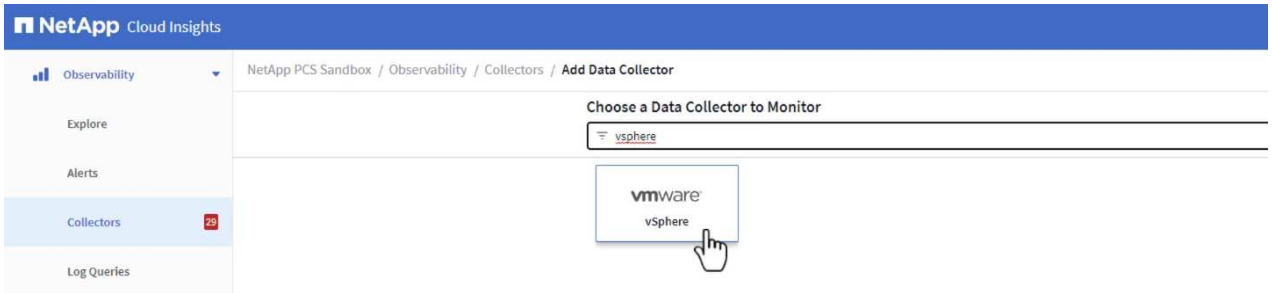


## Add a Data Collector for a VMware vSphere cluster

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**.



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.

✓
—
○

Select a Data Collector
Configure Data Collector

## Configure Collector

### Add credentials and required settings

[Need Help?](#)

Name ?

Acquisition Unit

---

Virtual Center IP Address

User Name

Password

Complete Setup
Test Connection

Advanced Configuration

Collecting:

- Inventory
- VM Performance

Inventory Poll Interval (min)

Communication Port

Filter VMs by

Choose 'Exclude' or 'Include' to Specify a List

Filter Device List (Comma Separated Values For Filtering By ESX\_HOST, CLUSTER, and DATACENTER Only)

Performance Poll Interval (sec)

Collect basic performance metrics only

Complete Setup
Test Connection

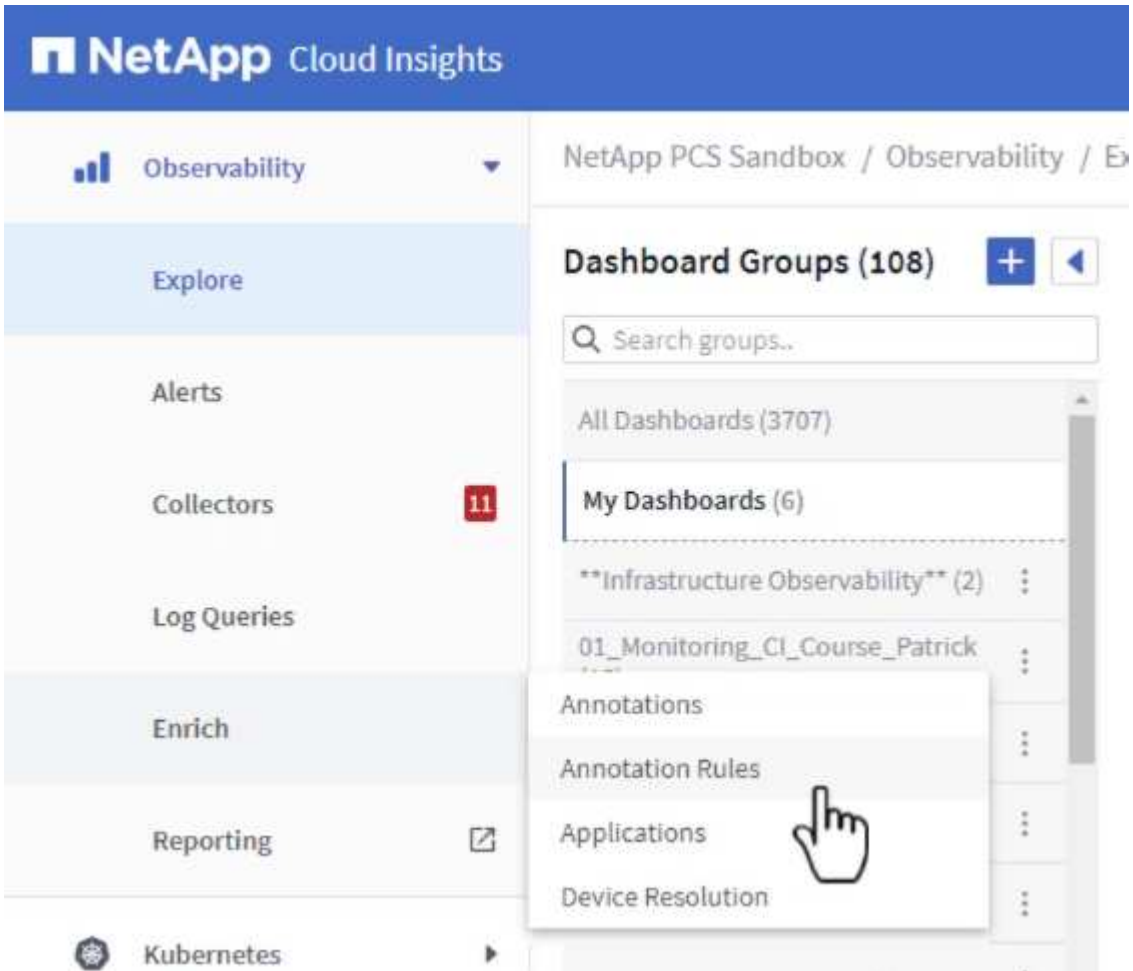
## Add Annotations to assets

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**

**Query**

**Annotation**

**Value**

- 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.

NetApp PCS Sandbox / Observability / Enrich / **Annotation Rules**

Rules running... **Run All Rules**

**Annotation rules (217)** + Rule Filter...

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

### Explore and correlate assets

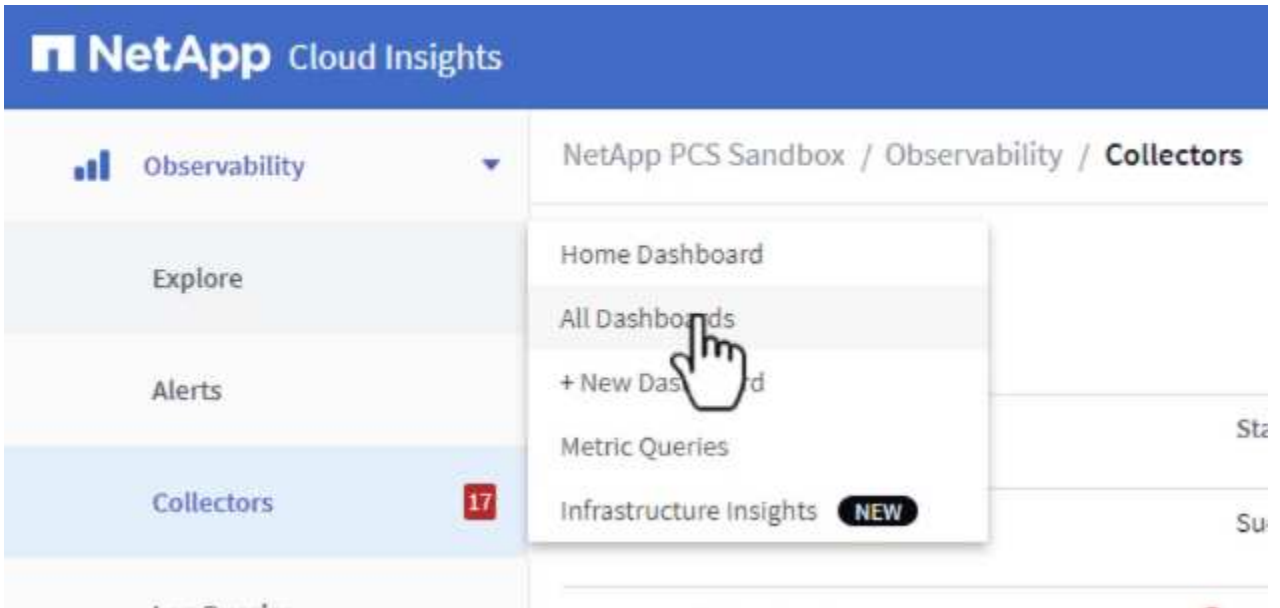
Cloud Insights draws logical conclusions about the assets that are running together on your storage systems and vsphere clusters.

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.



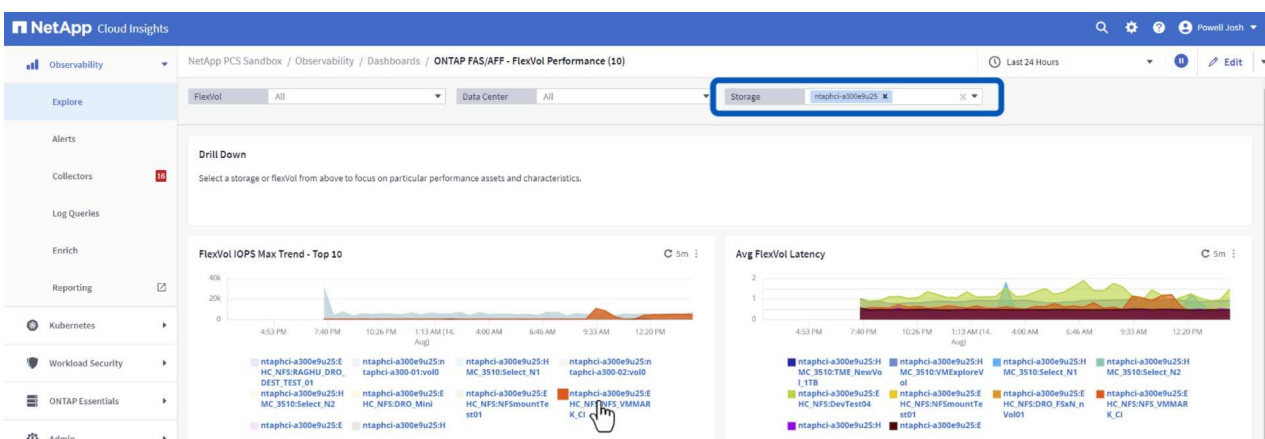
3. Choose a dashboard for FlexVol performance from the list and click on the **Add Dashboards** button at the bottom of the page.

- 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?

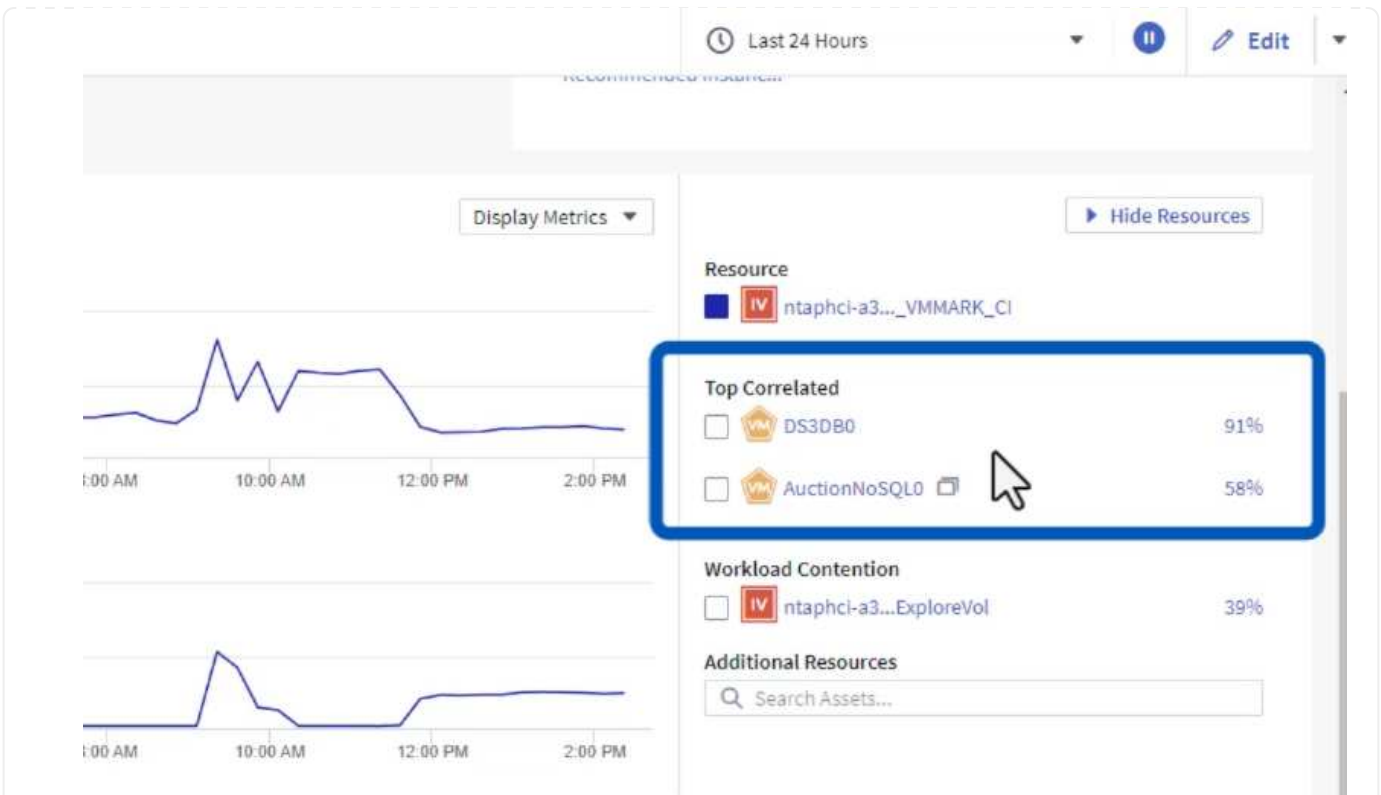
**+ Additional Dashboards (13)**  
 These dashboards require additional data collectors to be installed. [Add More](#)

[Add Dashboards](#) [Go Back](#)

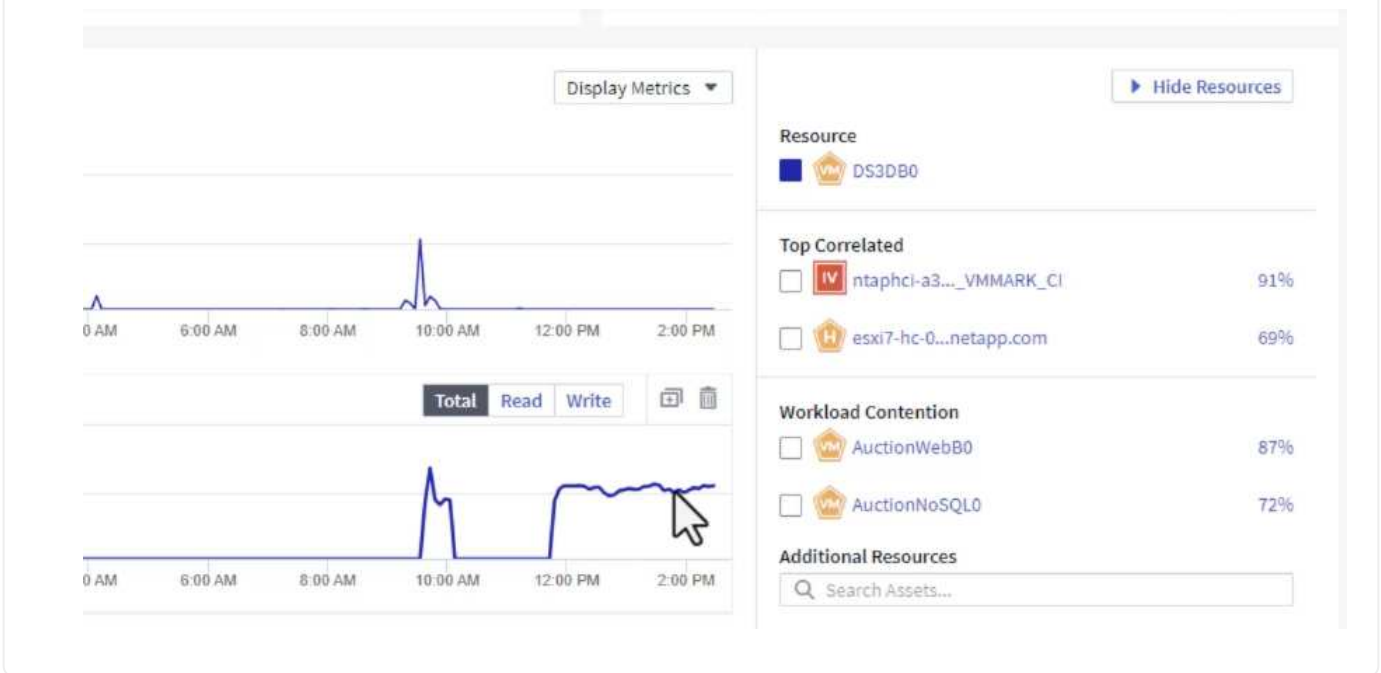
4. Once imported, open the dashboard. From here you can see various widgets with detailed performance data. Add a filter to view a single storage system and select a storage volume to drill into it's details.



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.



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



### 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) + My Dashboards (6) + From Gallery + Dashboard

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
<input checked="" type="checkbox"/> 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

! 5m Avg Latency (all hypervisors) C 5m VM Count With Latency Concern C 5m Avg Latency (all VMs)

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.

VM Count With Latency Concern

5m

50

VM's

Avg Latency (all VMs)

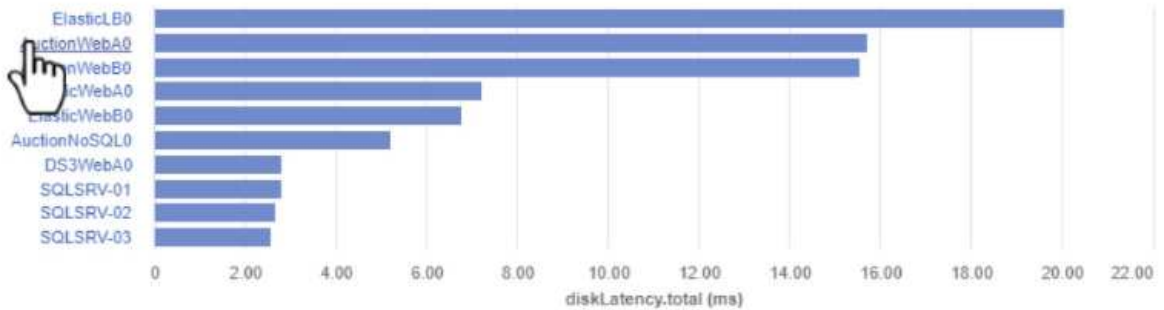
5m

1.55 ms

diskLatency.total

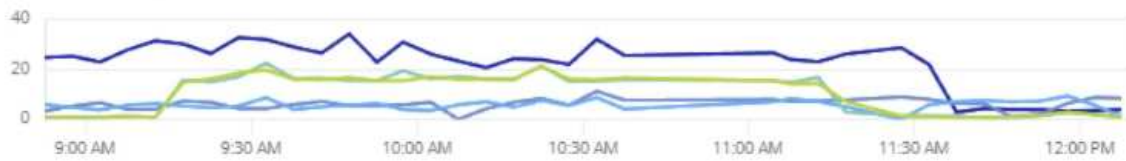
Avg VM Latency - Top 10

5m

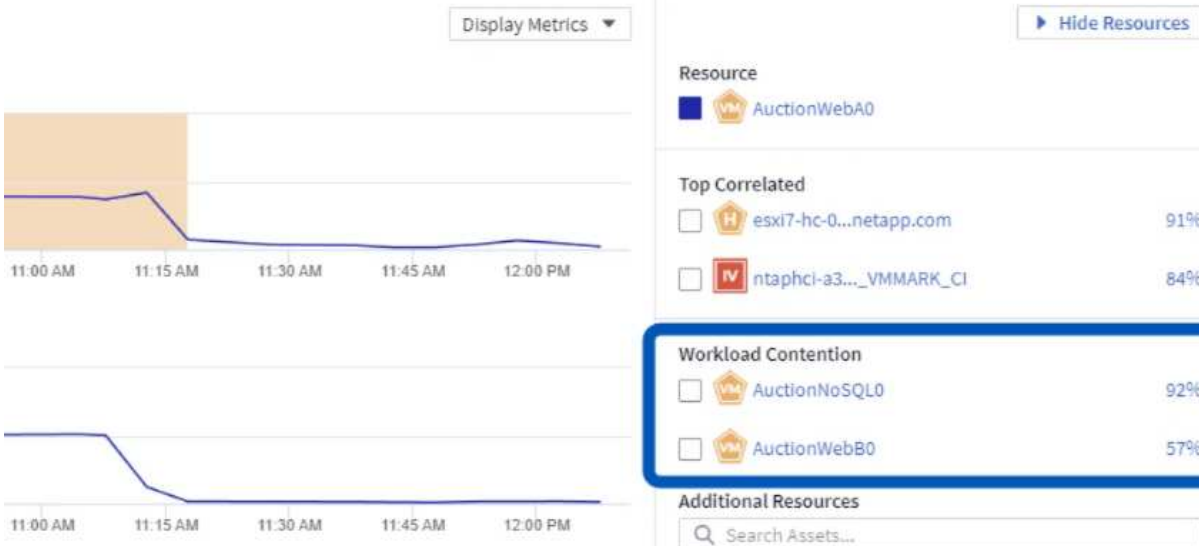


Top 5 Avg VM Latency Trend

30s



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.

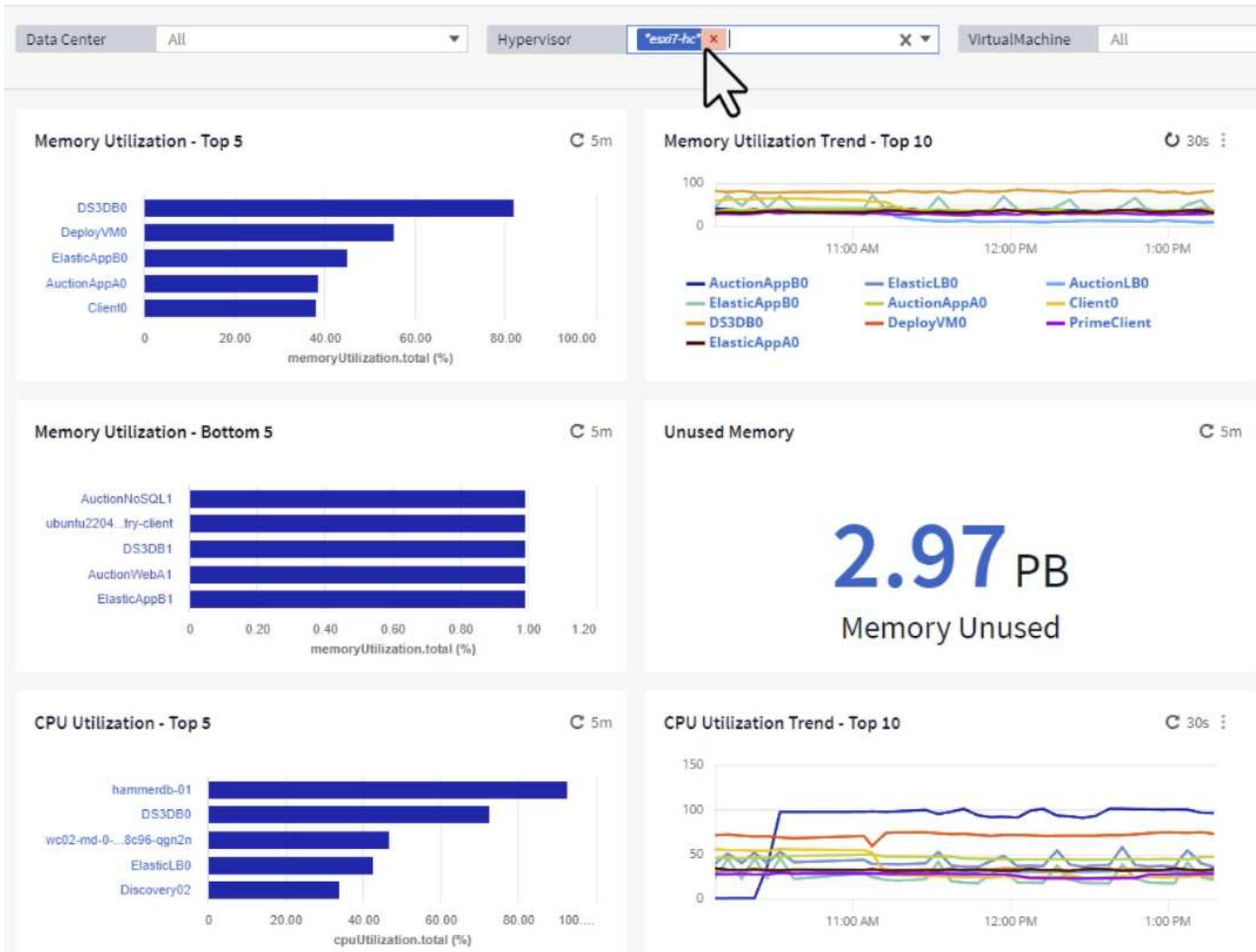
## Identify opportunities to right size VMs

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

### My Dashboards (6)

<input type="checkbox"/>	Name ↑
	<a href="#">All SAN Array Status (2)</a>
	<a href="#">Cloud Volumes ONTAP - FlexVol Performance (6)</a>
	<a href="#">ONTAP - Volume Workload Performance (Frontend) (7)</a>
<input type="checkbox"/>	<a href="#">VMware Admin - Where are opportunities to right size? (37)</a>
	<a href="#">VMware Admin - Where do I have VMs that potentially reclaim waste? (11)</a>
	<a href="#">VMware Admin - Where do I have VM Latency? (9)</a>

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

5m

121 items found

Virtual Machine	memory (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

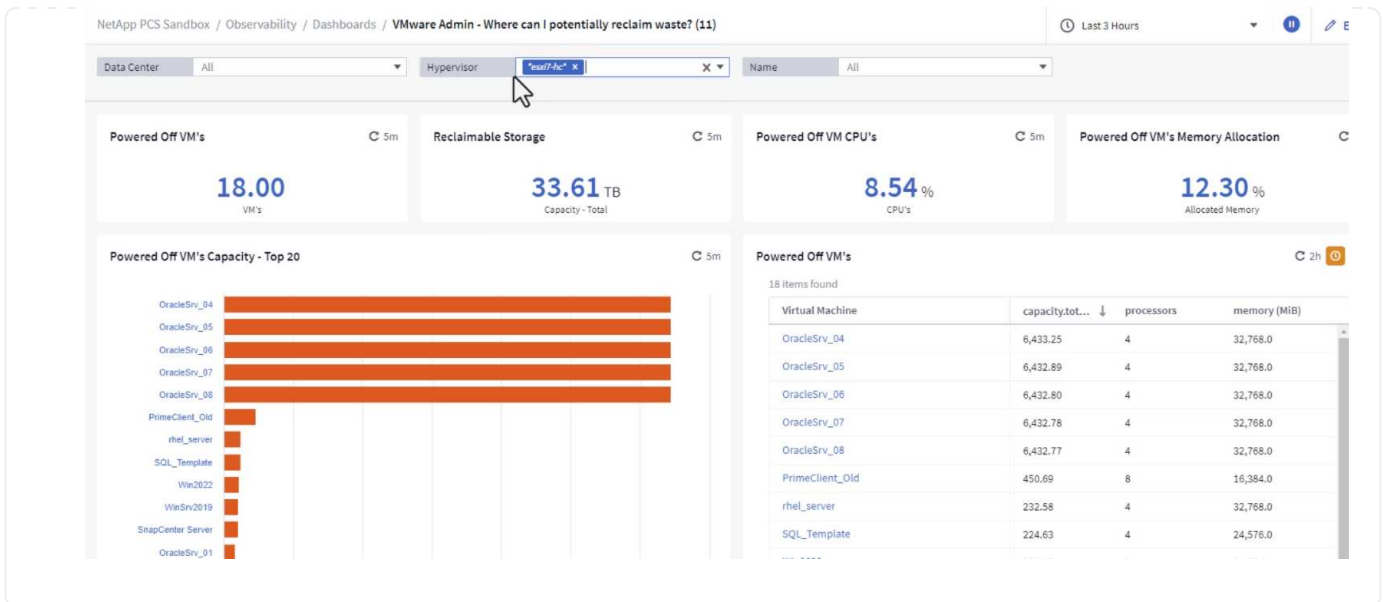
## CPU Utilization

5m

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

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

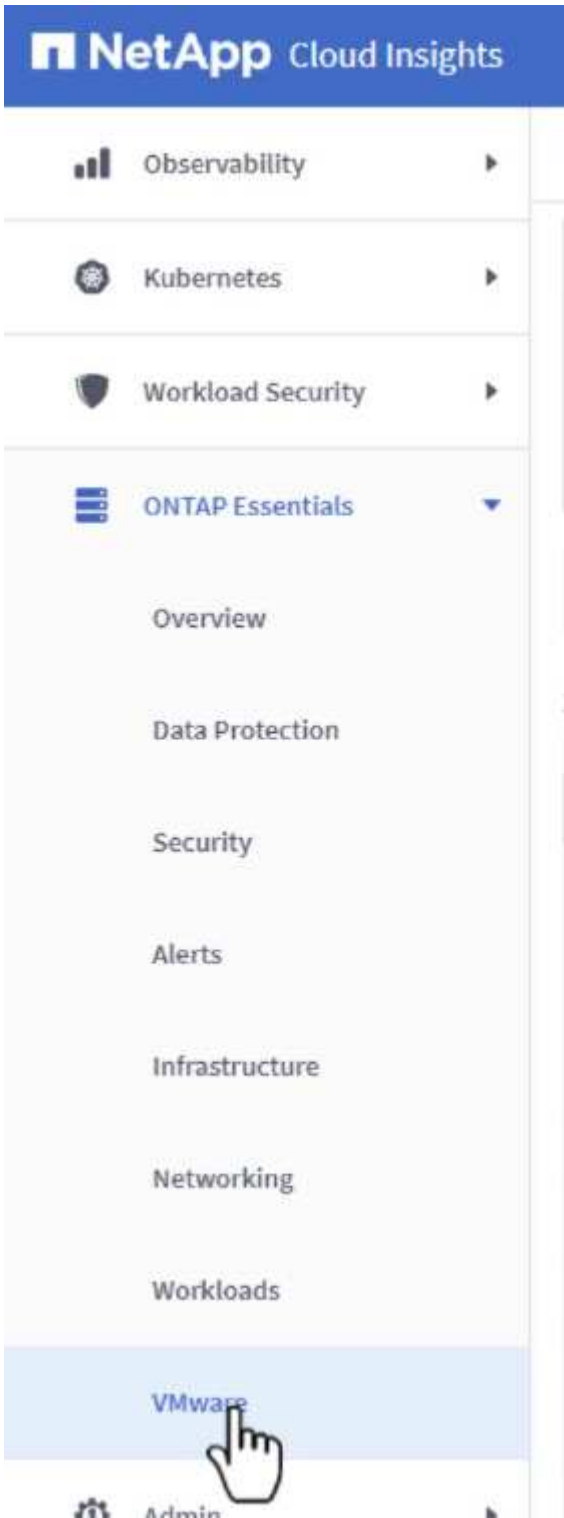


## Use queries to isolate and sort metrics

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.

The screenshot shows a NetApp Cloud Insights dashboard for Virtual Machines. The interface includes filters for 'storageResources.storage.vendor' (NetApp) and 'host.Los' (vmware). A table displays 281 items found, with columns for Virtual Machine name, powerState, capacity.used (GiB), capacity.total (GiB), capacityRatio.us..., diskIops.total (I/O/s), diskLatency.total..., and diskThroughputL... The table lists several VMs including prodclient, prodserver, prodmaster01-03, AIQUM 9.11 (vApp), AIQUM 9.12 (Linux), AN-JumpHost01, and AuctionApp01.

Virtual Machine	name	powerState	capacity.used (GiB)	capacity.total (GiB)	capacityRatio.us...	diskIops.total (I/O/s)	diskLatency.total...	diskThroughputL...
01rfk8prodclient	01rfk8prodclient	On	49.38	69.86	70.68	1.21	8.13	0.01
02rfk8prodserver	02rfk8prodserver	On	63.64	74.06	85.93	22.80	4.13	0.11
03rfk8prodmaster01	03rfk8prodmaster01	On	65.13	77.21	84.36	26.64	5.64	0.20
04rfk8prodmaster02	04rfk8prodmaster02	On	63.89	76.27	83.77	26.82	5.14	0.16
05rfk8prodmaster03	05rfk8prodmaster03	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

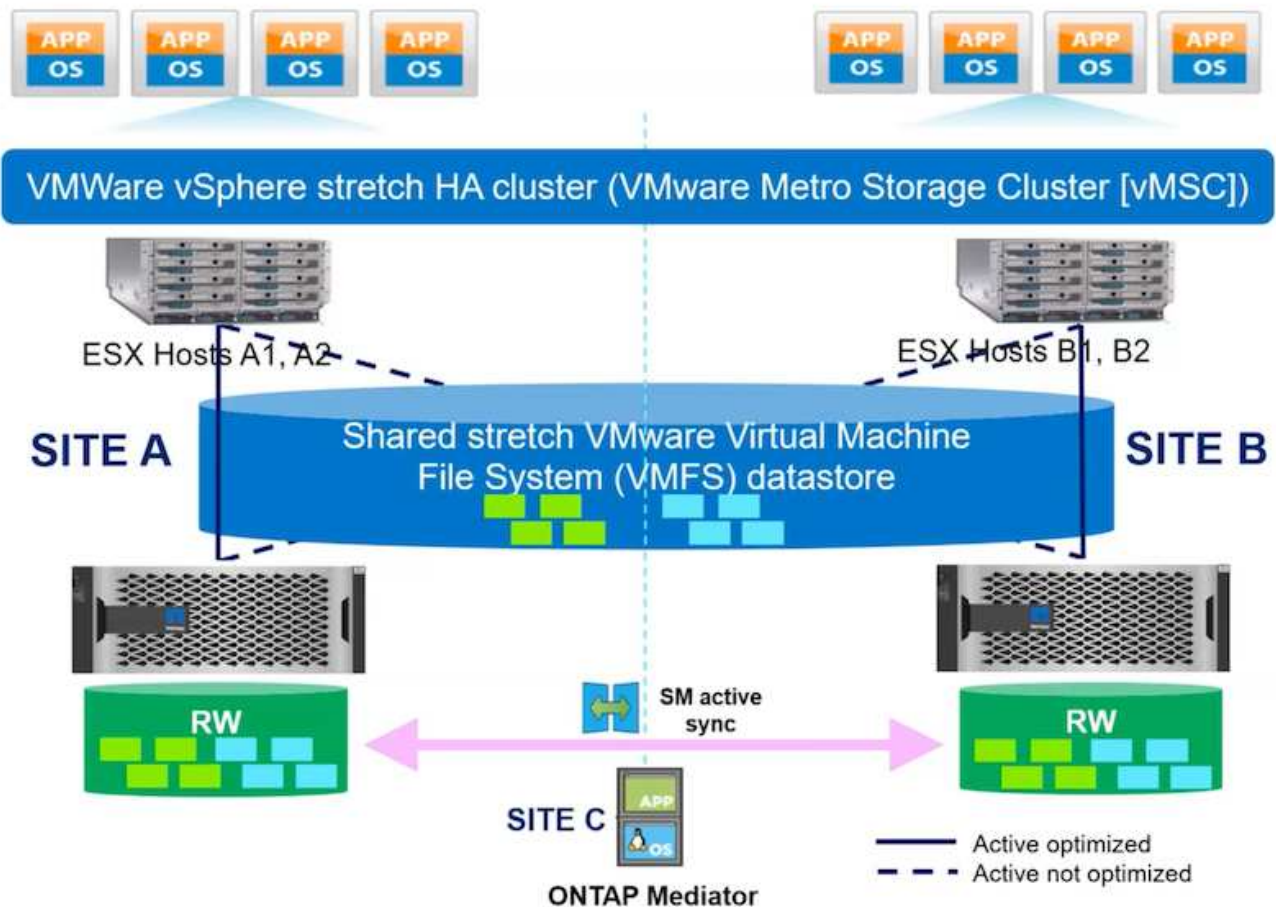
[VMware vSphere Metro Storage Cluster \(vMSC\)](#) is a stretched cluster solution across different fault domains to provide

- \* 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.

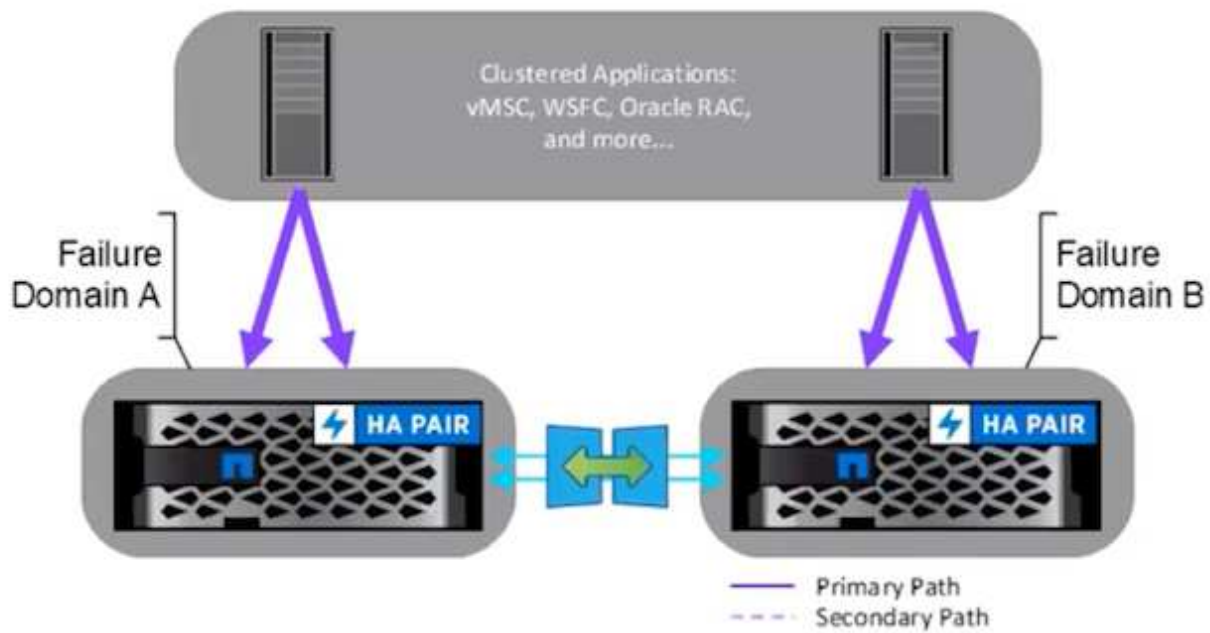
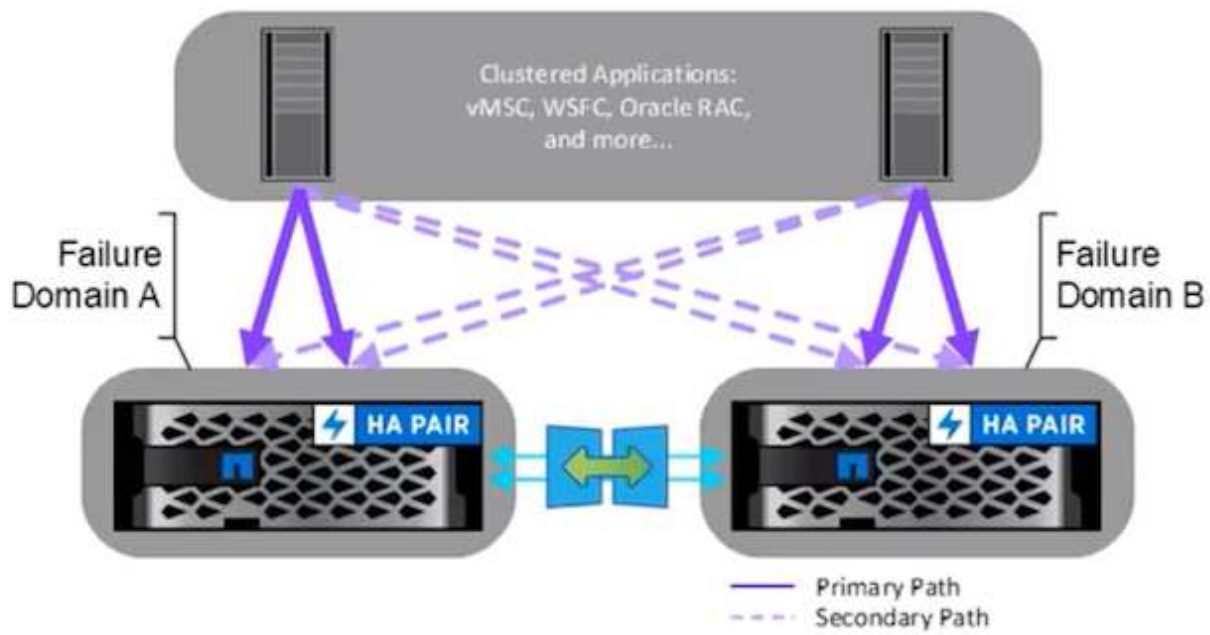
# SnapMirror active sync

General availability release 9.15.1 for symmetric configuration



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.

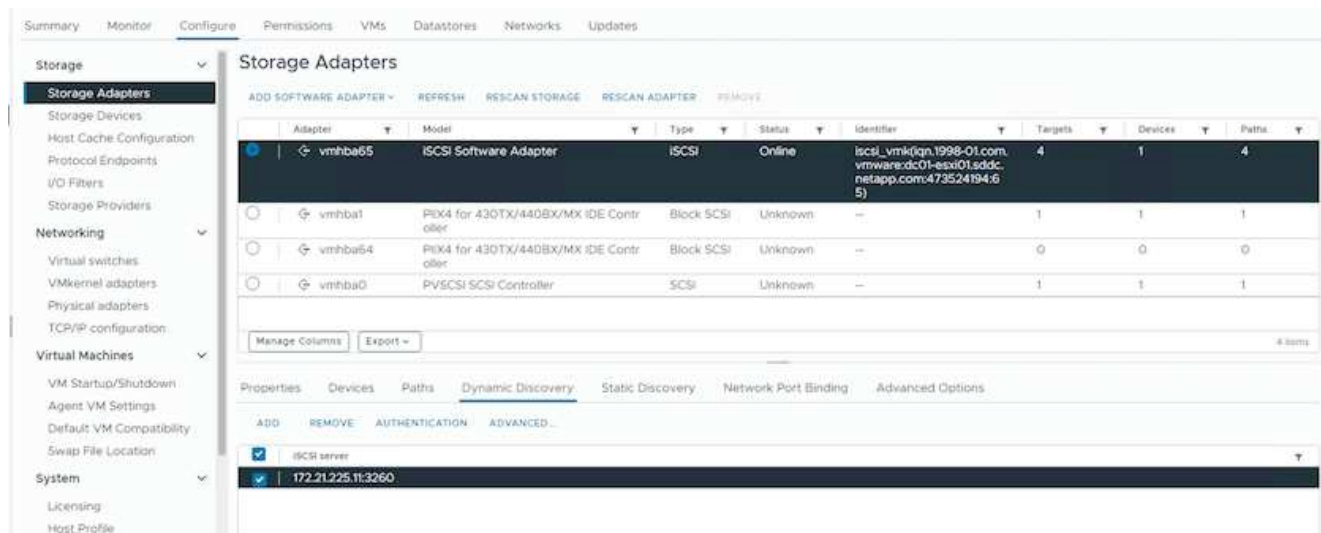
Note: ONTAP Tools 10.2 or above can be used to provision stretched datastore with non-uniform host access mode without switching multiple user interfaces. This section is just for reference if ONTAP Tools is not used.

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
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.





For Uniform access mode, need to provide the source and target fault domain iSCSI data lif address.

- Repeat the above step on vSphere hosts for the other fault domain adding its local iSCSI data lif IP on Dynamic Discovery tab.
- 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 zona -remote-address 172.21.225.71
-----
Vserver      Tpgroup      Conn  Local      Remote      TCP Recv
Name         Name         ID    Address    Address     Size
-----
zona        iscsi01      23    0 172.21.225.11  172.21.225.71  0
zona        iscsi03      17    0 172.21.225.12  172.21.225.71  0
2 entries were displayed.

E13A300::> iscsi connection show -vserver zona -remote-address 172.21.226.71
-----
Vserver      Tpgroup      Conn  Local      Remote      TCP Recv
Name         Name         ID    Address    Address     Size
-----
zona        iscsi02      24    0 172.21.226.11  172.21.226.71  0
zona        iscsi04      16    0 172.21.226.12  172.21.226.71  0
2 entries were displayed.
```

- Create LUN using ONTAP System Manager, setup SnapMirror with replication policy AutomatedFailOverDuplex, pick the host initiators and set host proximity.



## Add LUNs ✕

NAME PREFIX

STORAGE ARRAY

Group with related LUNs ⓘ

---

### Storage and optimization

NUMBER OF LUNS:  CAPACITY PER LUN:  GB

PERFORMANCE SERVICE LEVEL

Not sure? [Get help selecting type](#)

Apply the performance limits enforcement to each LUN. If unchecked, these limits will be applied to the entire set of LUNs.

---

### Protection

Enable Snapshot copies (Dedup)

Enable SnapMirror (local or remote)

RESTRICTION ADJUST

  Show legacy policies ⓘ

Source

CLUSTER: E13A200  
STORAGE VSI: zohba  
COMPARTMENT GROUP: ds

Destination

CLUSTER:  Refresh  
STORAGE VSI:

Destination settings

ⓘ You should manually create anigroup by adding replicated hosts in the destination cluster and map the group to the newly created LUNs.

---

### Host information

HOST OPERATING SYSTEM:  LUN POWER:

HOST VENDOR

Existing initiator group

New initiator group using existing initiator groups

Host initiators

WFFMCCM GROUP NAME:

iSCSI Initiators (2)

Name	Description	In proximity to
<input type="checkbox"/> ipn.1954-01.com.redhat.51e1788998b	-	None
<input type="checkbox"/> ipn.1954-01.com.redhat.a3435046678	-	None
<input checked="" type="checkbox"/> ipn.1958-01.com.vmware.esb01-esx01.s...	-	Source
<input checked="" type="checkbox"/> ipn.1958-01.com.vmware.esb01-esx02.s...	-	Source
<input type="checkbox"/> ipn.1958-01.com.vmware.esb01-esx01.s...	-	Destination

[+ Add initiator](#)

6. On other fault domain storage array, create the SAN initiator group with its vSphere host initiators and set host proximity.

Overview Mapped LUNs

STORAGE VM  
zoneb

TYPE  
VMware

PROTOCOL  
Mixed (iSCSI & FC)

COMMENT  
-

PORTSET  
-

CONNECTION STATUS i  
✔ OK

^ Initiators

Name	De...	Connection status <span style="color: blue;">i</span>	In proximity to
iqn.1998-01.com.vmware:dc02-esxi01.sddc.netap...	-	<span style="color: green;">✔</span> OK	zoneb
iqn.1998-01.com.vmware:dc02-esxi02.sddc.netap...	-	<span style="color: green;">✔</span> 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.

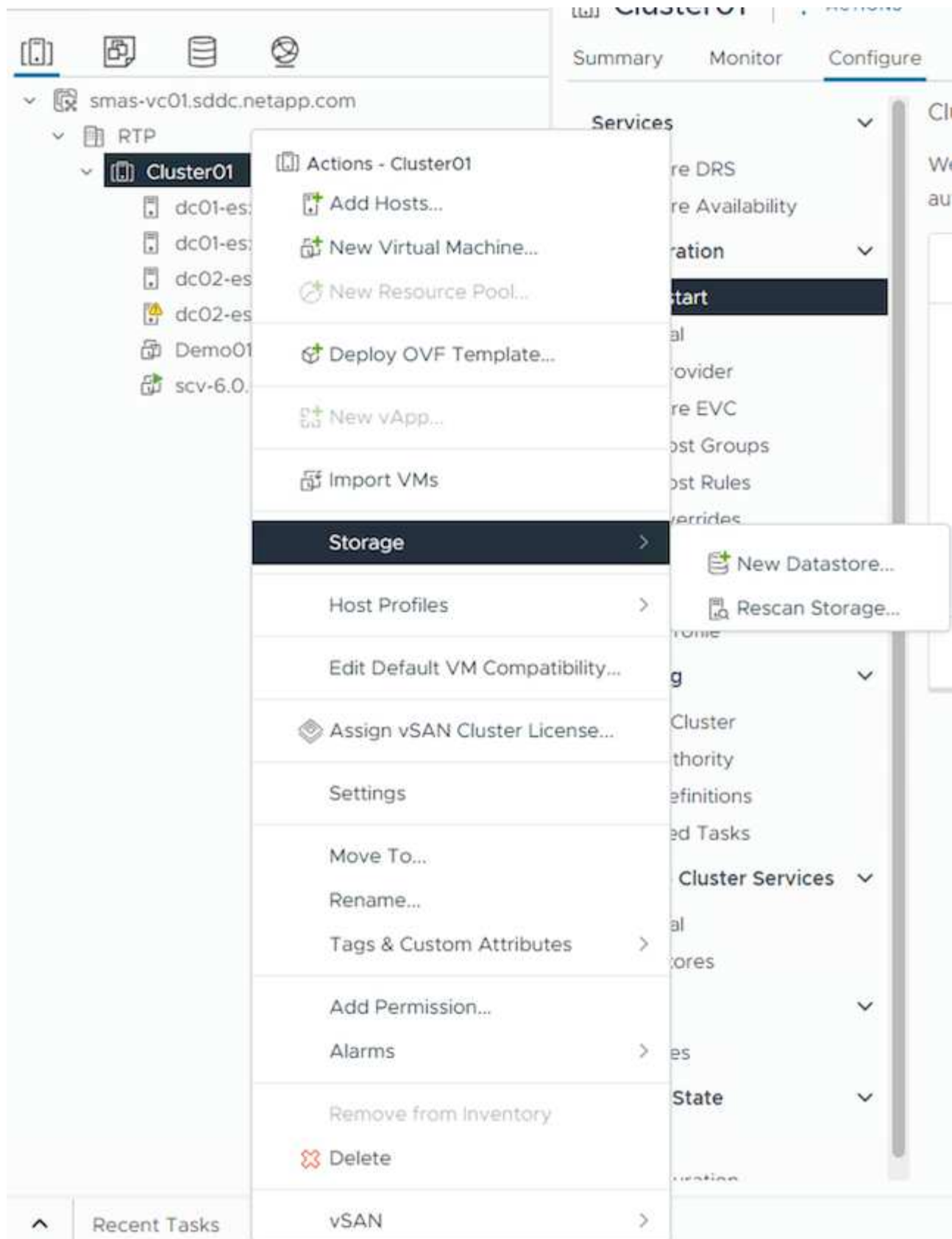
Overview Mapped LUNs

+ Add [Map LUNs](#)

[Filter](#)

<input type="checkbox"/>	Name	ID
<input type="checkbox"/>	ds02	1
<input type="checkbox"/>	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.

dc01-esxi01.sddc.netapp.com | ACTIONS

Summary Monitor **Configure** Permissions VMs Datastores Networks Updates

**Storage**

- Storage Adapters**
  - Storage Devices
  - Host Cache Configuration
  - Protocol Endpoints
  - I/O Filters
  - Storage Providers
- Networking**
  - Virtual switches
  - VMkernel adapters
  - Physical adapters
  - TCP/IP configuration
- Virtual Machines**
  - VM Startup/Shutdown
  - Agent VM Settings
  - Default VM Compatibility
  - Swap File Location
- System**
  - Licensing
  - Host Profile
  - Time Configuration
  - Authentication Services

### Storage Adapters

ADD SOFTWARE ADAPTER REFRESH RESCAN STORAGE RESCAN ADAPTER REMOVE

Adapter	Model	Type	Status	Identifier	Targets	Devices	Paths
vmhba65	ISCSI Software Adapter	ISCSI	Online	iscsi_vmk1(qn.1998-01.com,vmware:dc01-esxi01.sddc.netapp.com:473524194.65)	4	2	8
vmhba1	PIIX4 for 430TX/440BX/MX IDE Contr other	Block SCSI	Unknown	--	1	1	1
vmhba64	PIIX4 for 430TX/440BX/MX IDE Contr other	Block SCSI	Unknown	--	0	0	0
vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	1	1	1

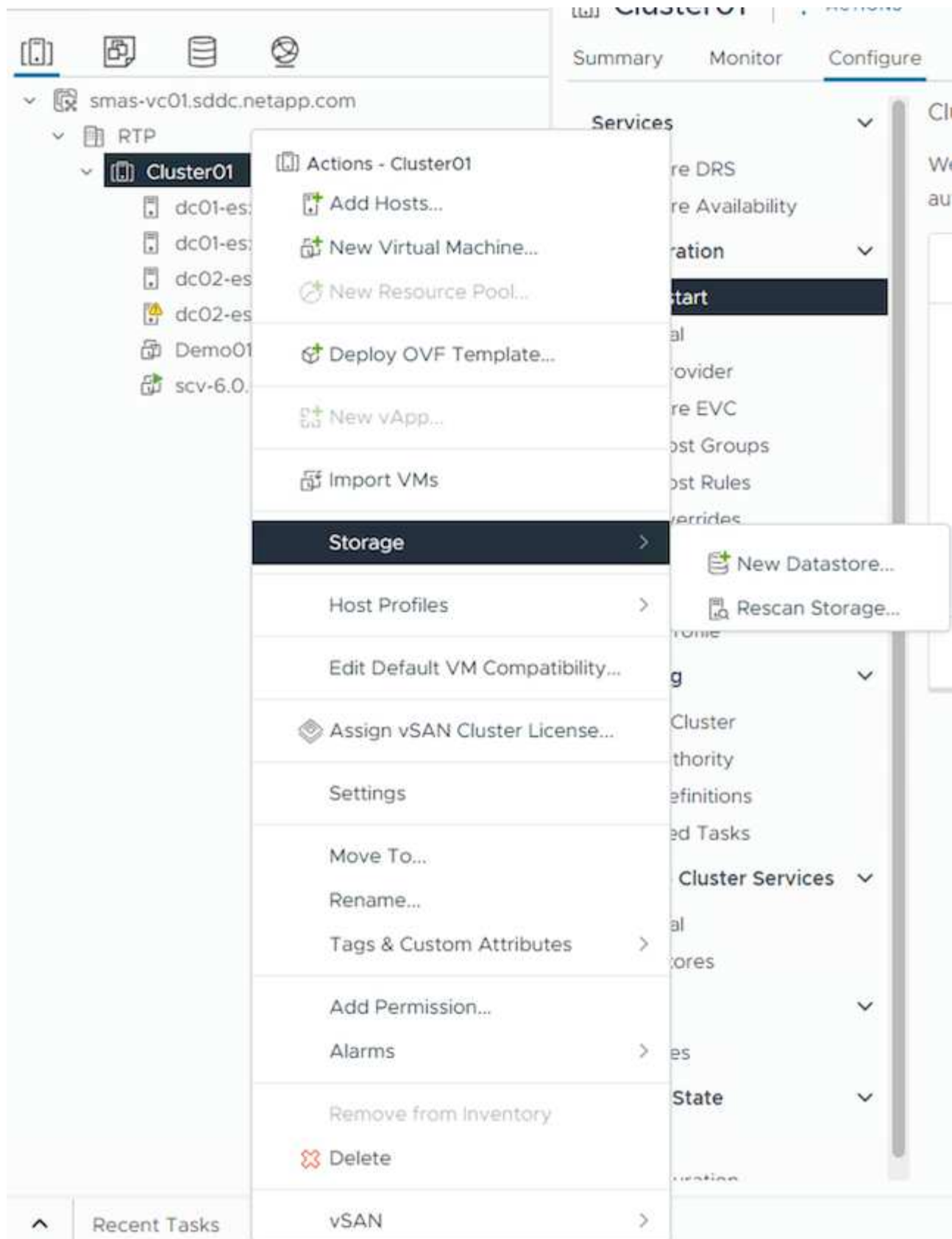
Manage Columns Export 4 items

Properties **Devices** Paths Dynamic Discovery Static Discovery Network Port Binding Advanced Options

REFRESH ATTACH DETACH RENAME

Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type	Transport
NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)	0	disk	250.00 GB	DS01	Attached	Supported	Flash	iSCSI
NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)	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

- Type
- Name and device selection**
- VMFS version
- Partition configuration
- Ready to complete

### Name and device selection

Specify datastore name and a disk/LUN for provisioning the datastore.

Name:

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: 
  
Select a host to view its accessible disks/LUNs:

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format	Ch...
<input checked="" type="radio"/>	NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)	1	300.00 G B	Supported	Flash	512e	Nc
<input type="radio"/>	Local VMware Disk (mpx.vmhba0:CO:T:LO)	0	100.00 G B	Not support ed	HDD	512n	Nc

Manage Columns Export 2 items

CANCEL BACK NEXT

12. Verify the datastore is mounted on all hosts on cluster across both fault domains.

## DS02

Summary Monitor **Configure** Permissions Files Hosts VMs

Alarm Definitions  
Scheduled Tasks  
General  
Device Backing  
**Connectivity and Multipathing**  
Hardware Acceleration  
Capability sets  
SnapCenter Plug-in for VMware  
Resource Groups  
Backups

### Connectivity and Multipathing

Mount Unmount

	Host	Datastore Mounted	Datastore Connectivity	Mount Point
<input checked="" type="radio"/>	dc01-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
<input type="radio"/>	dc01-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
<input type="radio"/>	dc02-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
<input type="radio"/>	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:
 

- Path Selection Policy: Round Robin (VMware)
- Storage Array Type Policy: VMW\_SATP\_ALUA
- Owner Plugin: NMP

Paths

	Runtime Name	Status	Target	LUN	Preferred
<input type="radio"/>	vmhba65:CO:T:LO1	Active	iqn.1992-08.com.netapp:sn.3cb67894c1f1fed819200a098a70d56-vs.28-172.21.225.12-3260	1	No
<input type="radio"/>	vmhba65:C2:T:LO1	Active (I/O)	iqn.1992-08.com.netapp:sn.3cb67894c1f1fed819200a098a70d56-vs.28-172.21.225.12-3260	1	No
<input type="radio"/>	vmhba65:C3:T:LO1	Active	iqn.1992-08.com.netapp:sn.3cb67894c1f1fed819200a098a70d56-vs.28-172.21.226.12-3260	1	No
<input type="radio"/>	vmhba65:C1:T:LO1	Active (I/O)	iqn.1992-08.com.netapp:sn.3cb67894c1f1fed819200a098a70d56-vs.28-172.21.226.12-3260	1	No

DS02 ACTIONS

Summary Monitor **Configure** Permissions Files Hosts VMs

Alarm Definitions  
Scheduled Tasks  
General  
Device Backing  
**Connectivity and Multipathing**  
Hardware Acceleration  
Capability sets  
SnapCenter Plug-in for VMware  
Resource Groups  
Backups

### Connectivity and Multipathing

Mount UNMOUNT

Host	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: VMW\_SATP\_ALUA
- Policy:
- Owner Plugin: NMP

Paths

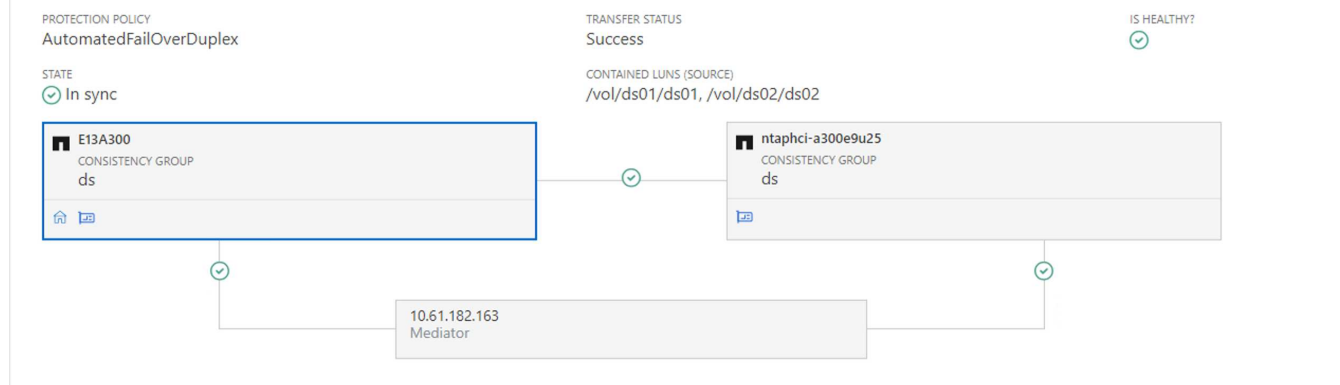
REFRESH ENABLE DISABLE

Runtime Name	Status	Target	LLN	Preferred
vmhba65:C2:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93efce6b1edbb10000a098b46a21vs.12.172.21.225.21.3260	1	No
vmhba65:C0:T0:L1	Active	iqn.1992-08.com.netapp:sn.133a93efce6b1edbb10000a098b46a21vs.12.172.21.225.22.3260	1	No
vmhba65:C3:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93efce6b1edbb10000a098b46a21vs.12.172.21.226.21.3260	1	No
vmhba65:C1:T0:L1	Active	iqn.1992-08.com.netapp:sn.133a93efce6b1edbb10000a098b46a21vs.12.172.21.226.22.3260	1	No



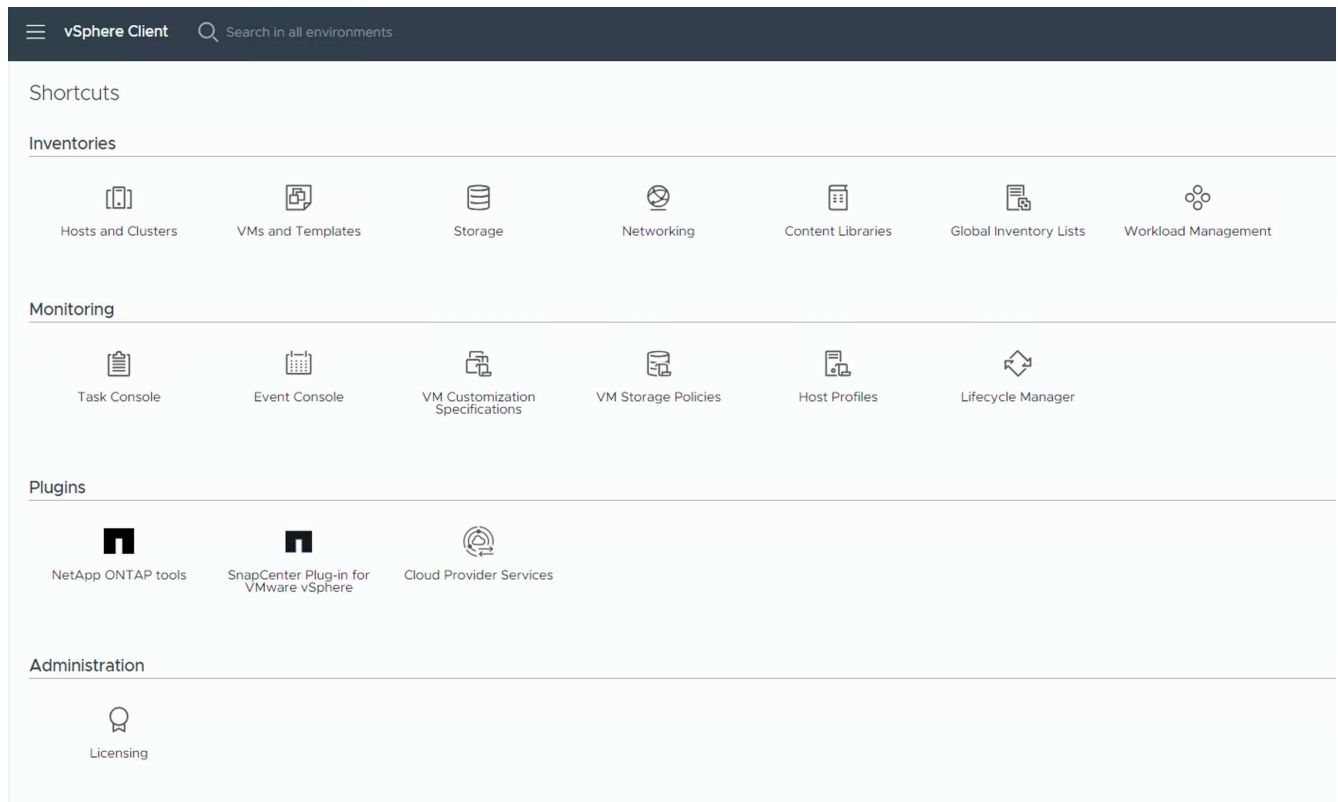
The above screenshots shows Active I/O on single controller since we used AFF. For ASA, it will have Active IO on all paths.

- When additional datastores are added, need to remember to expand the existing Consistency Group to have it consistent across the vSphere cluster.



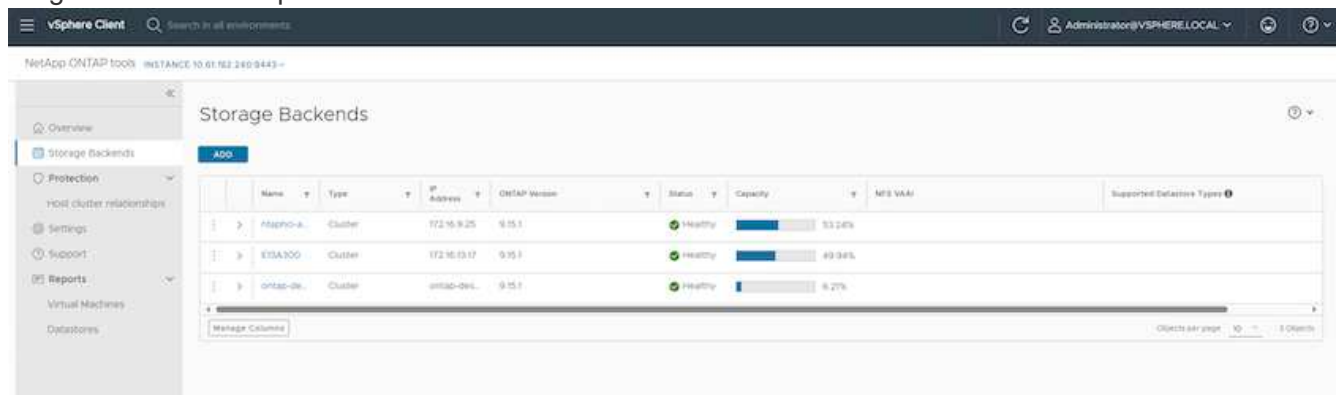
## VMSC uniform host access mode with ONTAP Tools.

- Ensure NetApp ONTAP Tools is deployed and registered to vCenter.



If not, follow [ONTAP Tools deployment](#) and [Add a vCenter server instance](#)

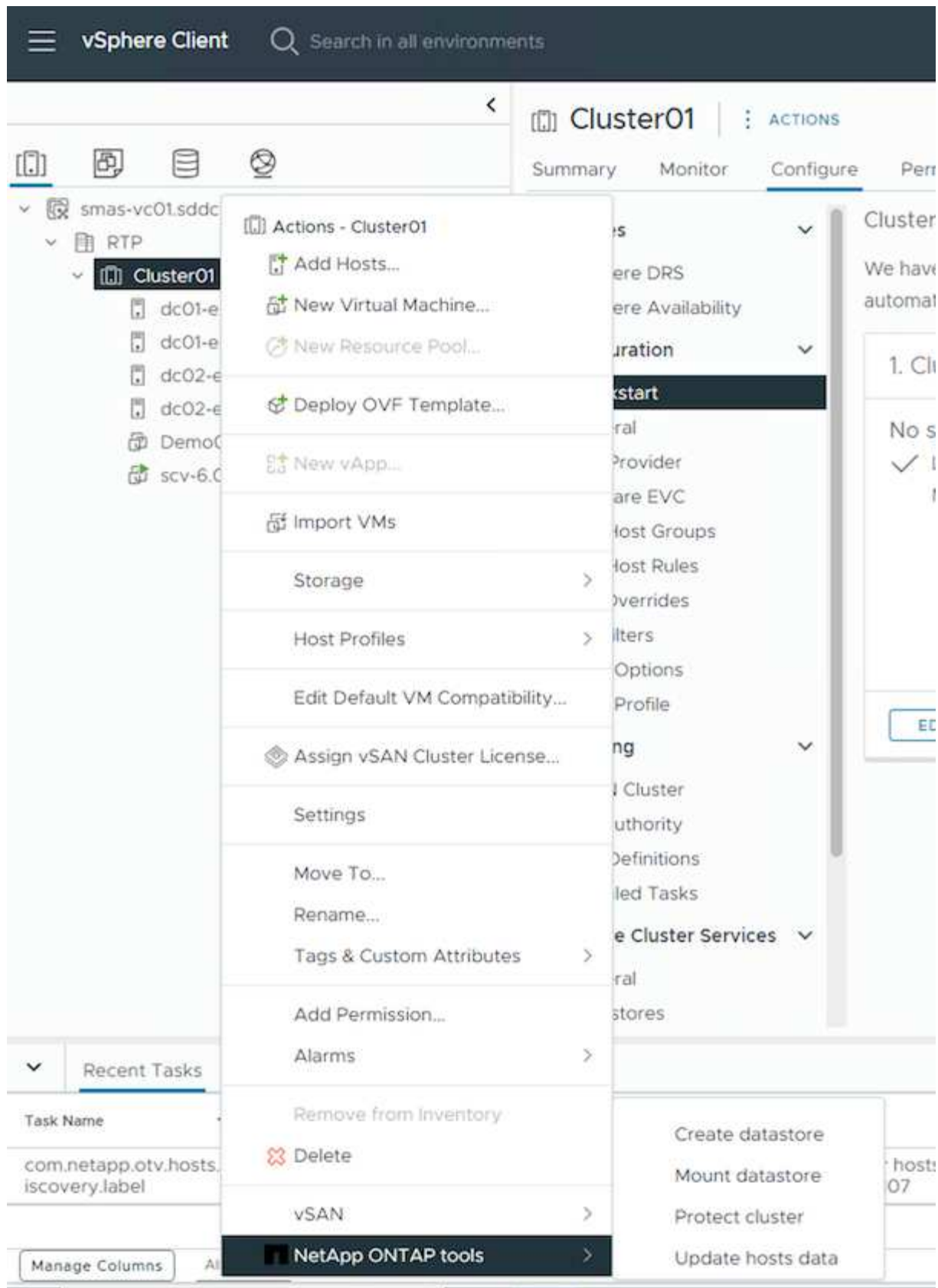
2. Ensure ONTAP Storage systems are registered to ONTAP Tools. This includes both fault domain storage systems and third one for Asynchronous remote replication to use for VM protection with SnapCenter Plugin for VMware vSphere.



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

[ADD RELATIONSHIP](#)

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 <span>5</span> 0 Object

[CANCEL](#)

[PROTECT](#)

- 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.

SET PROXIMAL TO ▾

<input type="checkbox"/>	Hosts	Proximal to
<input type="checkbox"/>		
<input type="checkbox"/>	dc01-esxi02.sddc.netapp.com	Source ▾
<input type="checkbox"/>	dc02-esxi01.sddc.netapp.com	Target ▾

4 Objects

CANCEL

ADD

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 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

[ADD RELATIONSHIP](#)

Target storage VM	Policy	Uniform Host Configuration	Host proximity
⋮ ntaphci-a300e9u25 / zoneb	AutomatedFailOverDuplex	Yes	Source (2), Target (2)

Objects per page 5 1 Object

[CANCEL](#) [PROTECT](#)

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.

- With Uniform host access, the host has iSCSI connection to both fault domain storage arrays.

The screenshot shows the 'Connectivity and Multipathing' configuration page for DS01. It includes a table of connections and a detailed view of the multipathing configuration.

Host	Datastore Mounted	Datastore Connectivity	Mount Point
dc02-esx01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa81f-71dea467-813d-005056b92d7e
dc01-esx02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa81f-71dea467-813d-005056b92d7e
dc02-esx02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa81f-71dea467-813d-005056b92d7e
dc01-esx01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa81f-71dea467-813d-005056b92d7e

**Device:** NETAPP iSCSI Disk (naa.600a0980383038467724524975577931) --

**Multipathing Policies:**

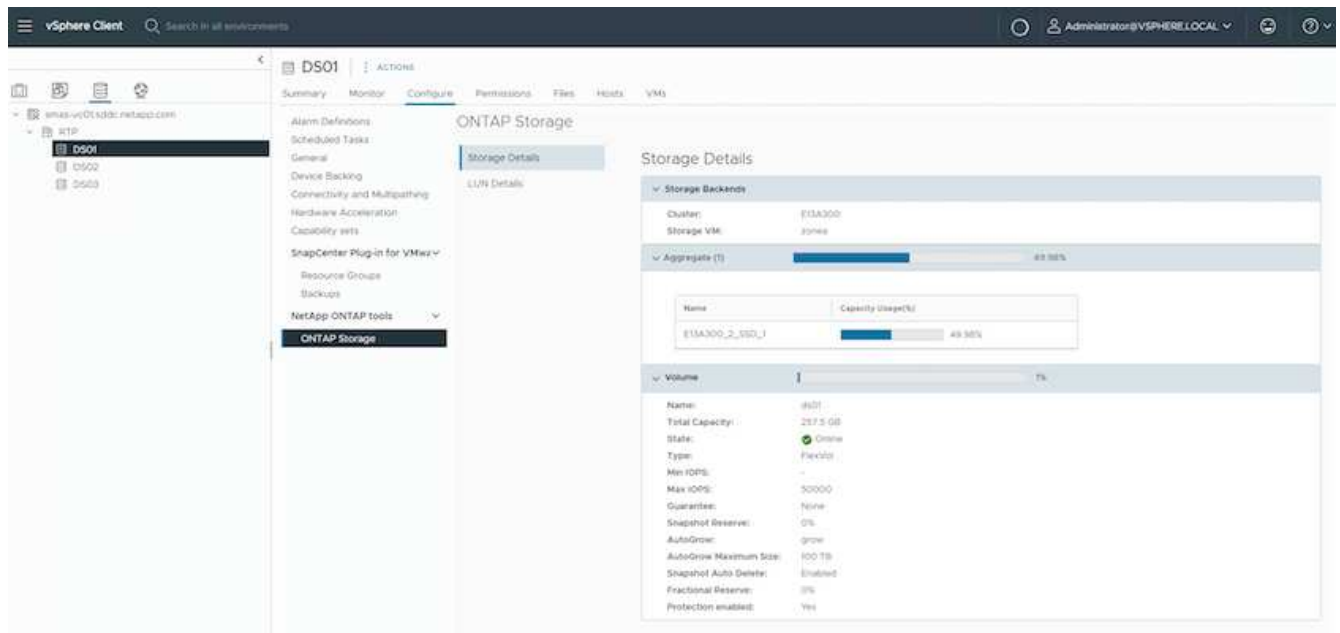
- Path Selection Policy: Round Robin (VMware)
- Storage Array Type Policy: VMW\_SATP\_ALUA
- Owner Plugin: NMP

**Paths:**

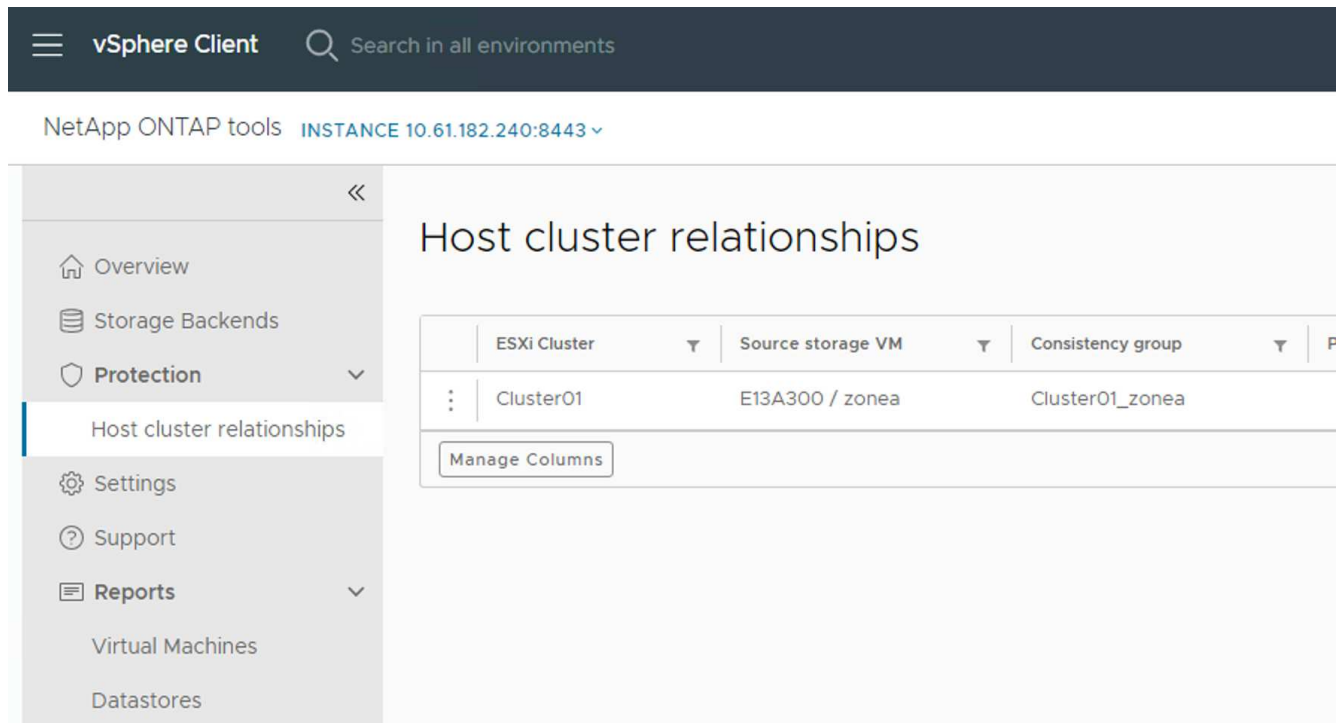
Runtime Name	Status	Target	LUN
vmhba65:C3:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894cf11fed819200a098a70d56-vs.28172.21.225.12:3260	0
vmhba65:C2:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894cf11fed819200a098a70d56-vs.28172.21.226.12:3260	0
vmhba65:C1:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894cf11fed819200a098a70d56-vs.28172.21.225.11:3260	0
vmhba65:C3:T0:L0	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93e1ce6b1fedb10000a098b46a21-vs.12172.21.226.21:3260	0
vmhba65:C0:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894cf11fed819200a098a70d56-vs.28172.21.226.11:3260	0
vmhba65:C2:T0:L0	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93e1ce6b1fedb10000a098b46a21-vs.12172.21.225.21:3260	0
vmhba65:C1:T0:L0	Active	iqn.1992-08.com.netapp:sn.133a93e1ce6b1fedb10000a098b46a21-vs.12172.21.226.22:3260	0
vmhba65:C0:T0:L0	Active	iqn.1992-08.com.netapp:sn.133a93e1ce6b1fedb10000a098b46a21-vs.12172.21.225.22:3260	0

NOTE: The above screenshot is from AFF. If ASA, ACTIVE I/O should be in all paths with proper network connections.

- ONTAP Tools plugin also indicates the volume is protected or not.

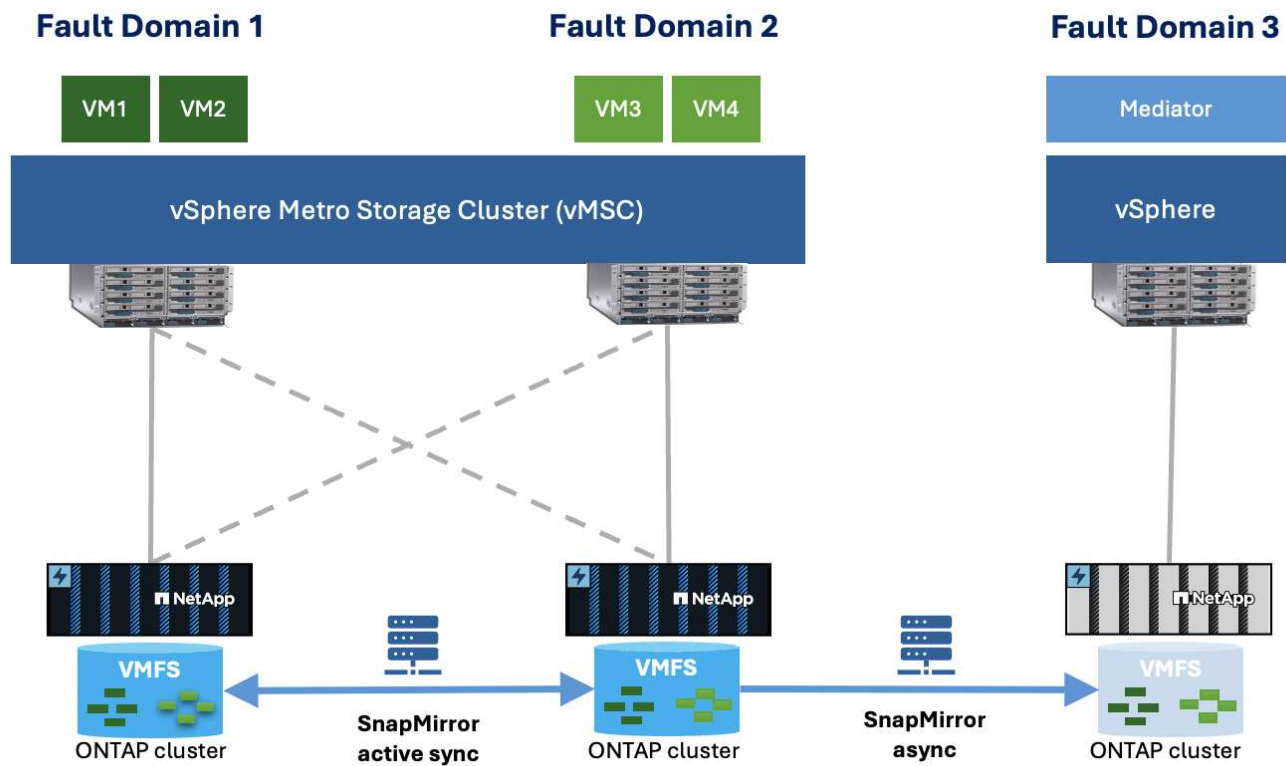


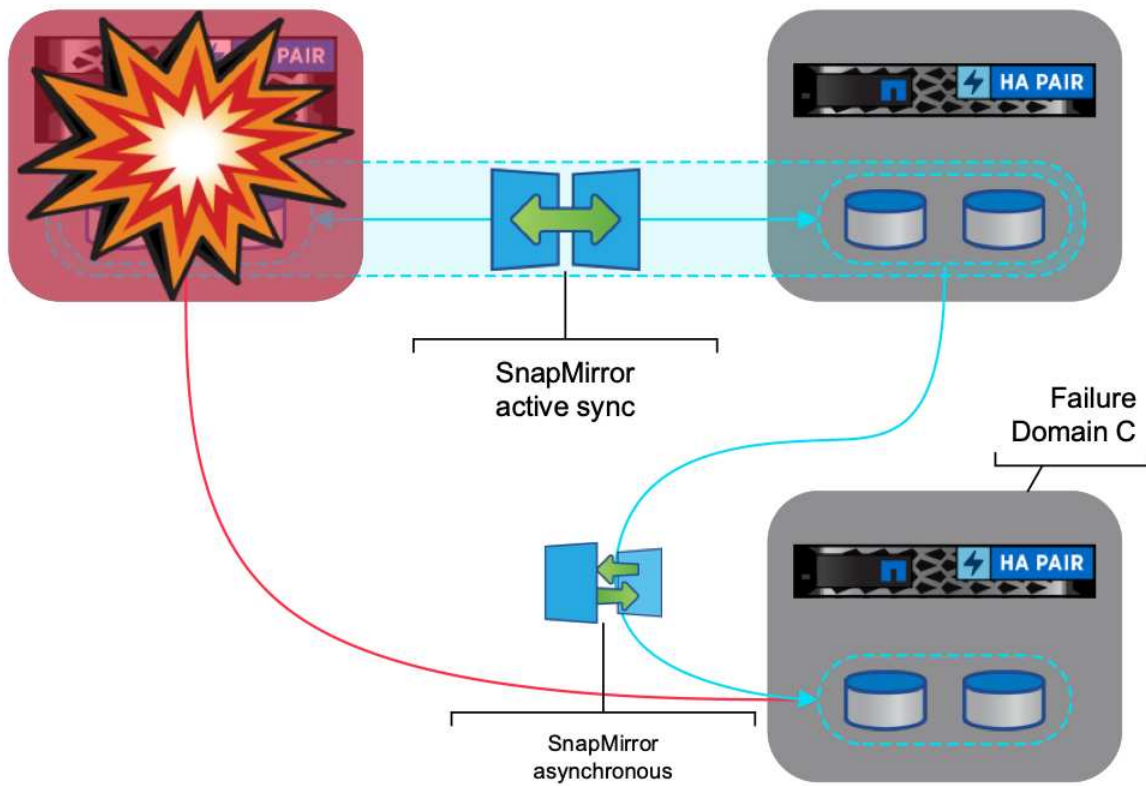
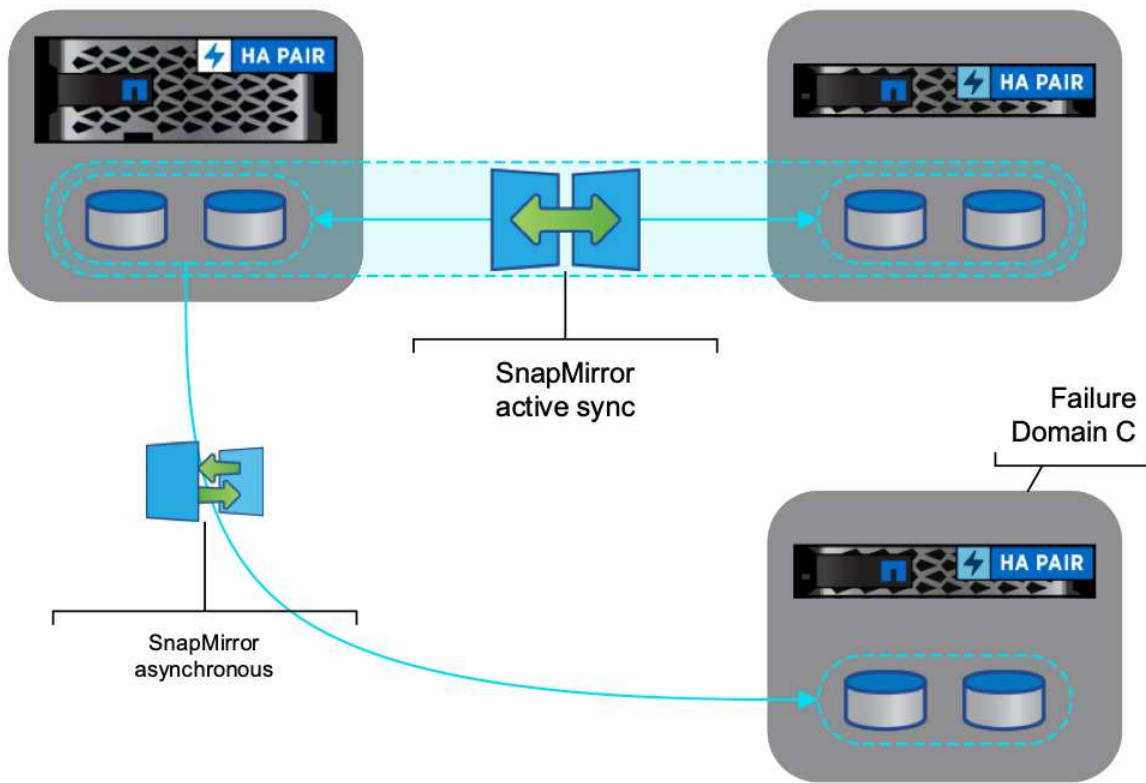
- For more details and to update the host proximity info, Host cluster relationships option under the ONTAP Tools can be utilized.



### 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.



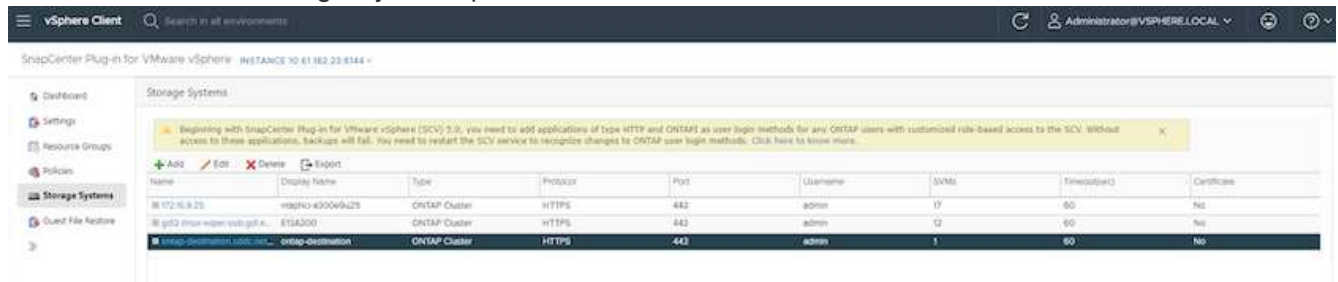




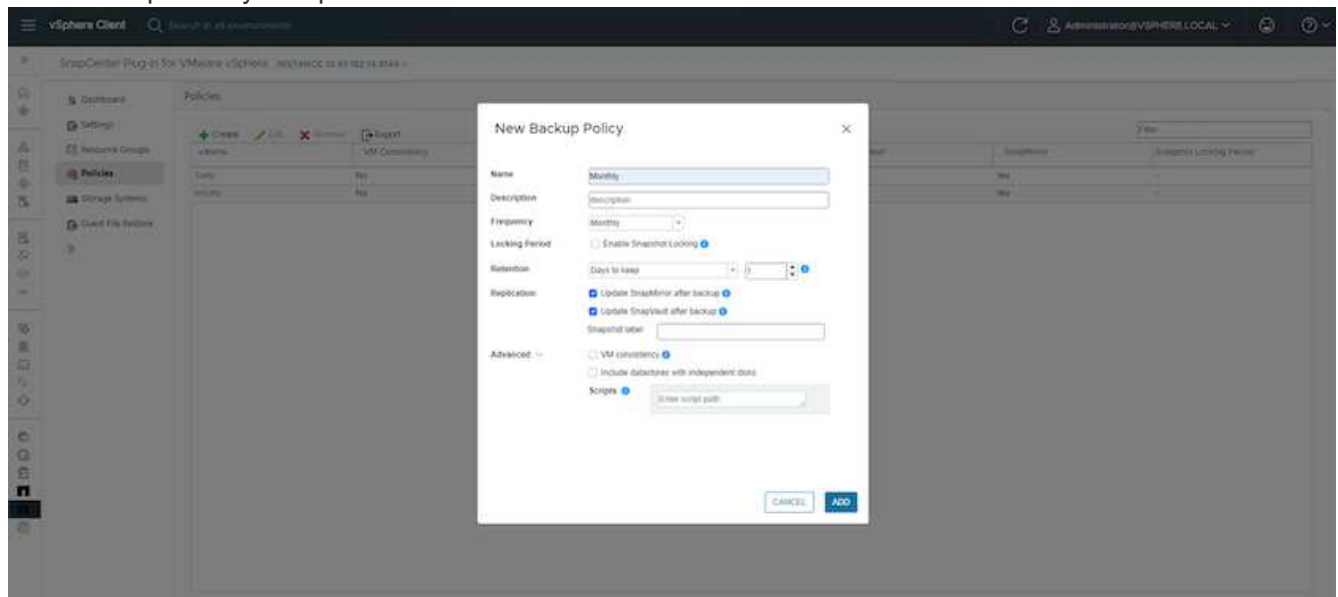
Supported use-cases include:

- \* Backup and Restore the VM or Datastore from either of fault domains with SnapMirror active sync.
- \* Restore resources from third fault domain.

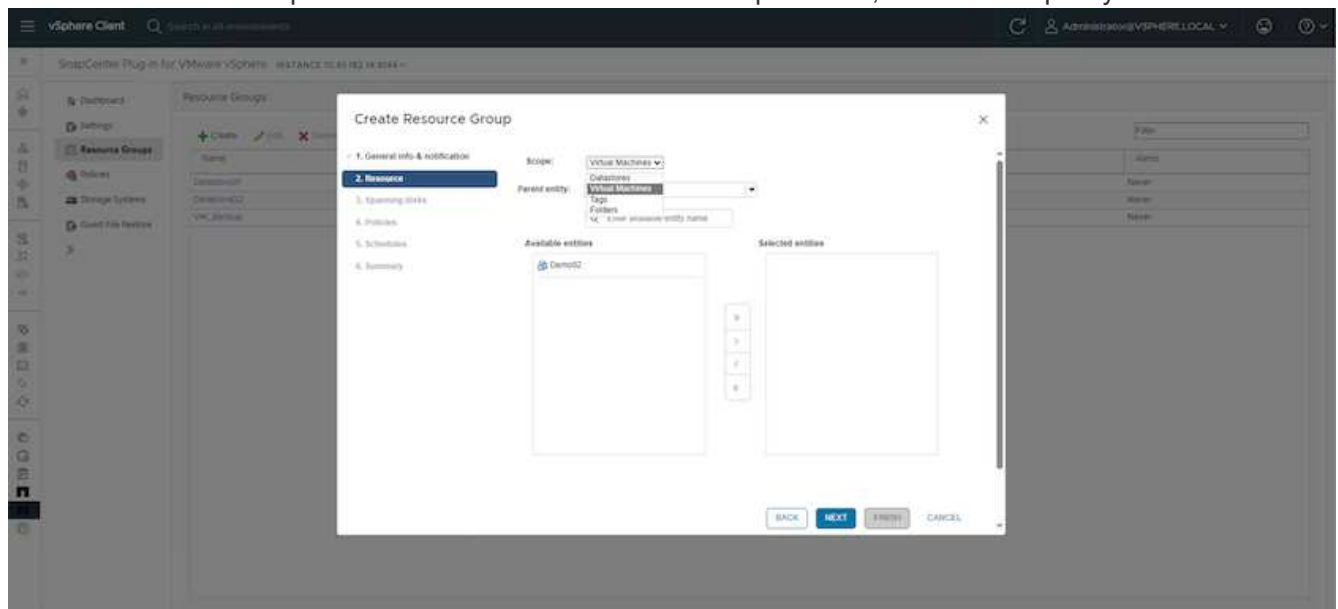
1. Add all the ONTAP Storage Systems planned to use in SCV.



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.



3. Create Resource Group with desired items that need to be protected, associate to policy and schedule.



NOTE: Snapshot name ending with \_recent is not supported with SM-as.



- 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.

**Dashboard**

Beginning with SnapCenter Plug-in for VMware vSphere (SCV) 5.0, you need to add applications of type HTTP and DNTAP as user login methods for any DNTAP 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 DNTAP user login methods. [Click here to know more.](#)

**RECENT JOB ACTIVITIES**

Job Name	Job ID	Status	Time Ago
Backup Warning VM_Backup	[Job ID: 512]	Warning	10 min ago
Backup Successful Datastore1	[Job ID: 512]	Successful	24 min ago
Backup Successful Datastore1	[Job ID: 512]	Successful	31 min ago
Backup Warning VM_Backup	[Job ID: 512]	Warning	1 h ago
Backup Successful Datastore1	[Job ID: 512]	Successful	1 h ago

**JOB STATUS (Last 7 Days)**

52% Successful

- Failed: 11
- Successful: 92
- Warning: 71
- Running: 1

**LATEST PROTECTION SUMMARY (Last 7 Days)**

**Primary: 60% Protected**

- Failed: 0
- Successful: 3
- Warn: 0
- Not backed up: 2

**Secondary: 20% Replicated**

- Failed: 2
- Successful: 1
- Warn: 0
- Not replicated: 2

**CONFIGURATION**

- 5 Virtual Machines
- 2 Datastores
- 30 VMs
- 3 Resource Groups
- 3 Backup Policies

**STORAGE**

- 4.64 GB (82 Snapshots)
- 5.12 GB (98 Snapshots)
- 4.11 GB (42 Snapshots)
- 66.46 Storage Savings
- + 303.43 GB Saved (Snapshots)
- + 4.64 GB Consumed (Storage)

**Datastore01** | ACTIONS

Summary | Monitor | **Configure** | Permissions | Files | Hosts | VMs

Alarm Definitions  
Scheduled Tasks  
General  
Device Backing  
Connectivity and Multipathing  
Hardware Acceleration  
Capability sets  
NetApp ONTAP tools  
SnapCenter Plug-in for VMware v  
Resource Groups  
**Backups**

**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
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 1:28:08 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 9:28:10 AM	No	Hourly	No
VM_Backup_08-11	Completed	Primary & Second	-	8/11/2024 9:00:18 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



6. Similar option is also available for Datastore mount operation.

### Mount Backup ✕

ESXi host name  ▾

Selected backup VM\_Backup\_08-11-2024\_16.00.02.0270

Select datastore

<input type="checkbox"/>	Name	Location
<input type="checkbox"/>	Datastore01	<input type="text" value="Primary:172.21.228.10:Datastore01:VM_Backup_08-11-2024_16.00.02.0270"/> ▾
<input type="checkbox"/>	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
<input type="checkbox"/>		
<input type="checkbox"/>		

⚠ Warning for ONTAP 9.12.1 and below version ✕ ▾

For assistance with additional operations with SCV, refer [SnapCenter Plug-in for VMware vSphere documentation](#)

## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.