NFS Reference Guide for vSphere 8

NetApp Solutions

NetApp
October 03, 2024

Table of Contents

NFS Reference Guide for vSphere 8

NFS v3 Reference Guide for vSphere 8

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

Using NFS v3 with vSphere 8 and ONTAP Storage Systems

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

Use Cases

Use cases covered in this documentation:

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

Audience

This solution is intended for the following people:

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

Technology Overview

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

VMware vSphere Foundation

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

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

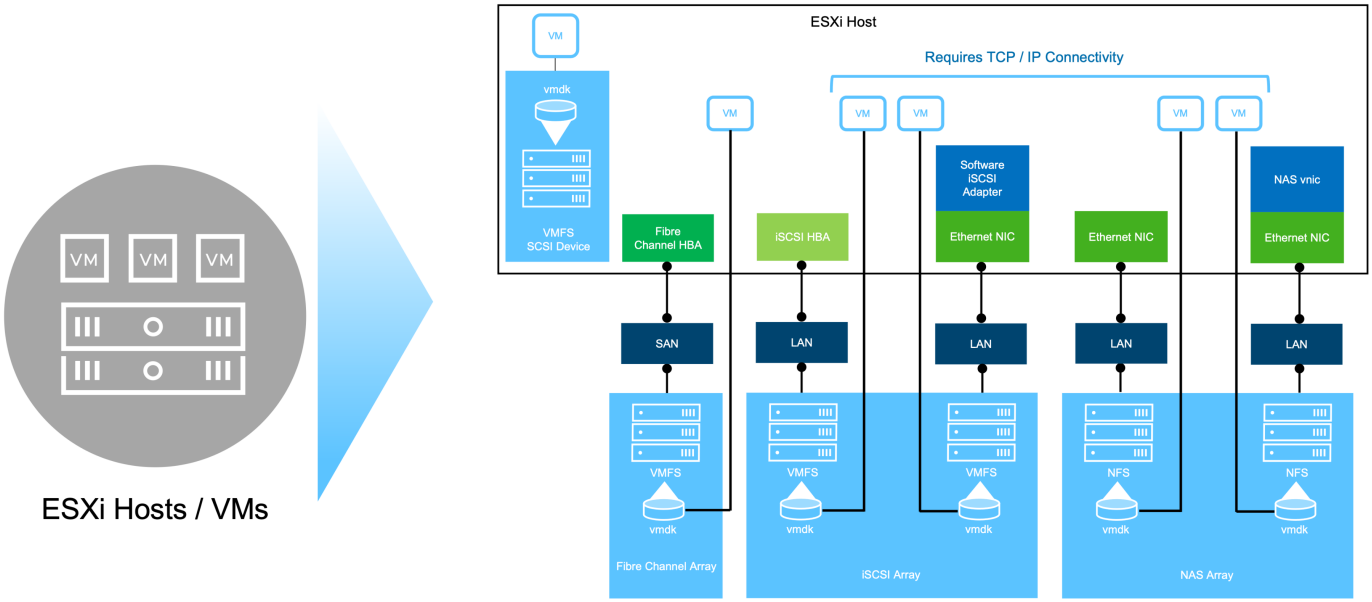
- VMware vSphere
- VMware vSAN
- Aria Standard
- VMware Tanzu Kubernetes Grid Service for vSphere
- vSphere Distributed Switch

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

VVF Storage Options

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

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



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

NetApp ONTAP

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

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

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

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

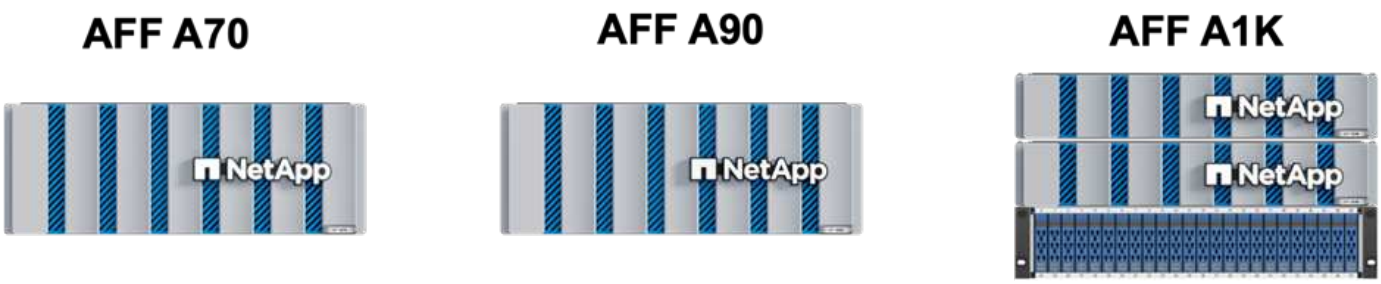
Using ONTAP together with vSphere is a great combination that lets you reduce host hardware and VMware software expenses. You can also protect your data at lower cost with consistent high performance. Because virtualized workloads are mobile, you can explore different approaches using Storage vMotion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

NetApp All-Flash Arrays

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

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

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



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

Storage Protocol Support

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

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

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

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

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

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

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

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

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

Active-active technology

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

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

Storage guarantees

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

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

For detailed information see the NetApp AFF landing page.

NetApp ONTAP Tools for VMware vSphere

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

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

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

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

NetApp NFS Plug-in for VMware VAAI

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

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

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

SnapCenter Plug-in for VMware vSphere

The SnapCenter Plug-in for VMware vSphere (SCV) is a software solution from NetApp that offers comprehensive data protection for VMware vSphere environments. It is designed to simplify and streamline the

process of protecting and managing virtual machines (VMs) and datastores. SCV uses storage based snapshot and replication to secondary arrays to meet lower recovery time objectives.

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

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

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

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

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

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

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

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

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

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

Storage considerations

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

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

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

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

Refer to NFS trunking overview for more information.

FlexVol volumes: NetApp recommends using **FlexVol** volumes for most NFS datastores. While larger

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

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

Ransomware protection

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

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

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

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

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

Disaster recovery considerations

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

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

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

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

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

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

Solutions Overview

Solutions covered in this documentation:

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

NFS nConnect feature with NetApp and VMware

Starting with VMware vSphere 8.0 U1 (as Tech-preview), the nconnect feature enables multiple TCP connections for NFS v3 datastore volumes to achieve more throughput. Customers using NFS datastore can now increase the number of connections to NFS server thus maximizing the utilization of high speed network interface cards.

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

Use cases

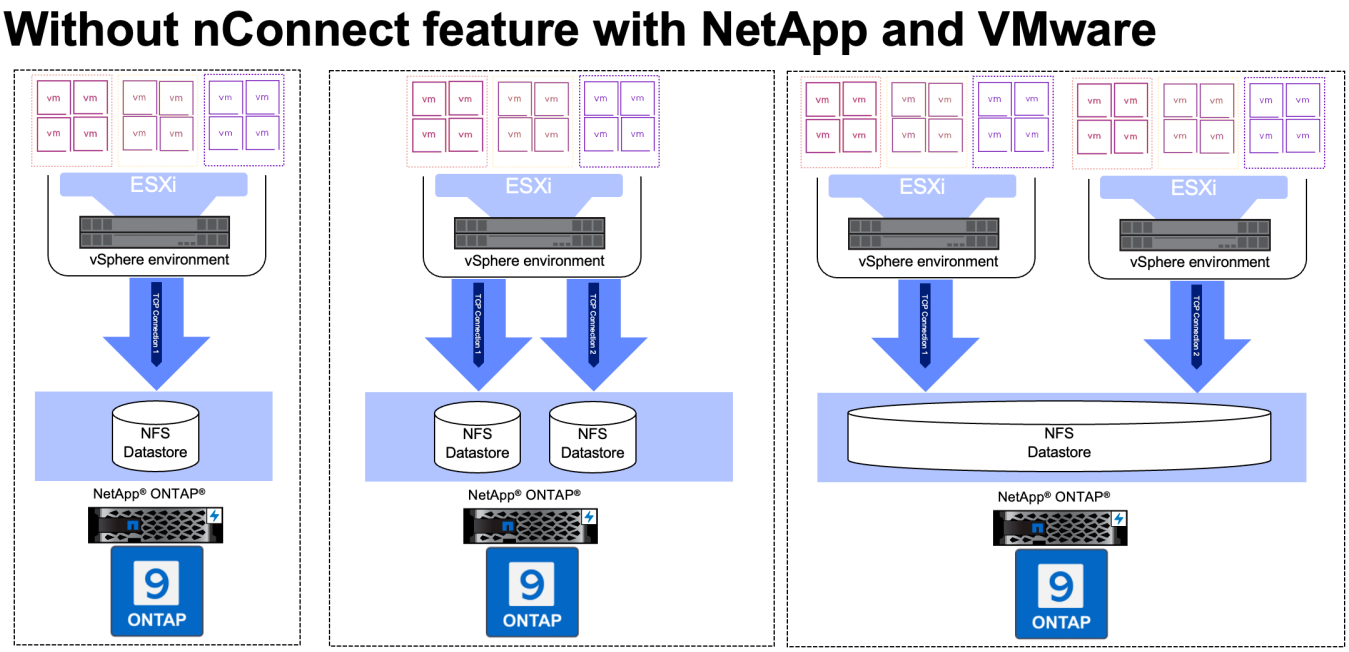
- Host more virtual machines per NFS datastore on the same host.
- Boost NFS datastore performance.
- Provide an option to offer service at a higher tier for VM and Container based applications.

Technical details

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

Default NFS Datastore

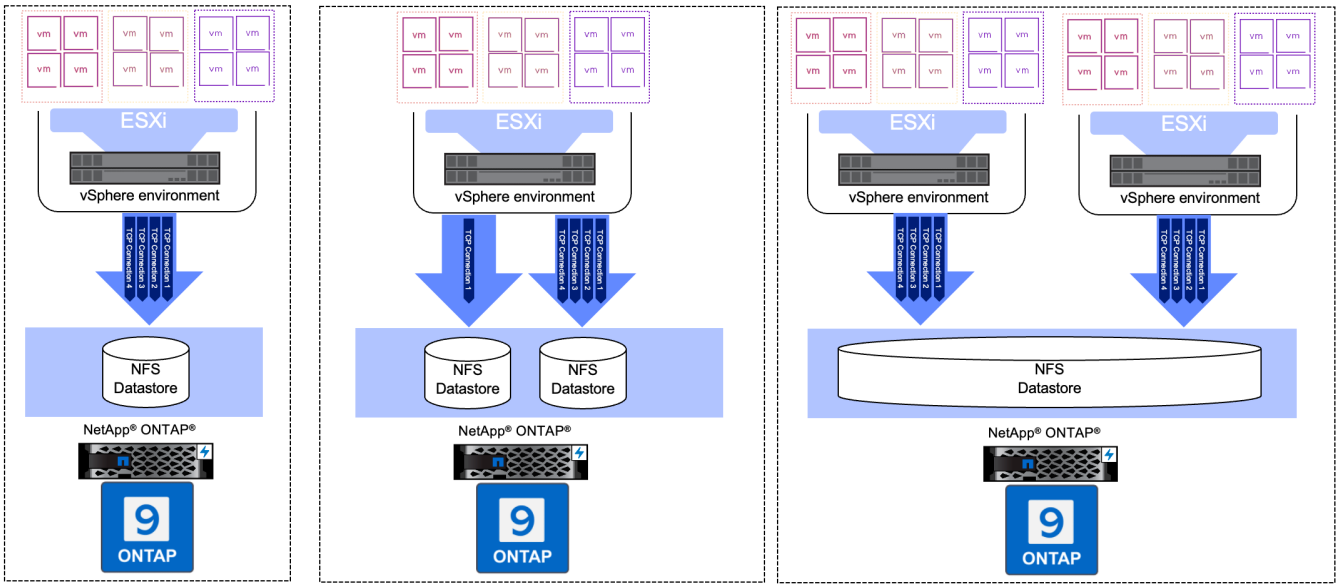
To address the performance limitations of single connection of NFS datastore, additional datastores are mounted or additional hosts are added to increase the connection.



With nConnect NFS Datastore

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

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

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

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

Refer VMware KB article 91497 for more information.

Design considerations

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

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

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

Use ONTAP tools 10 to configure NFS datastores for vSphere 8

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

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

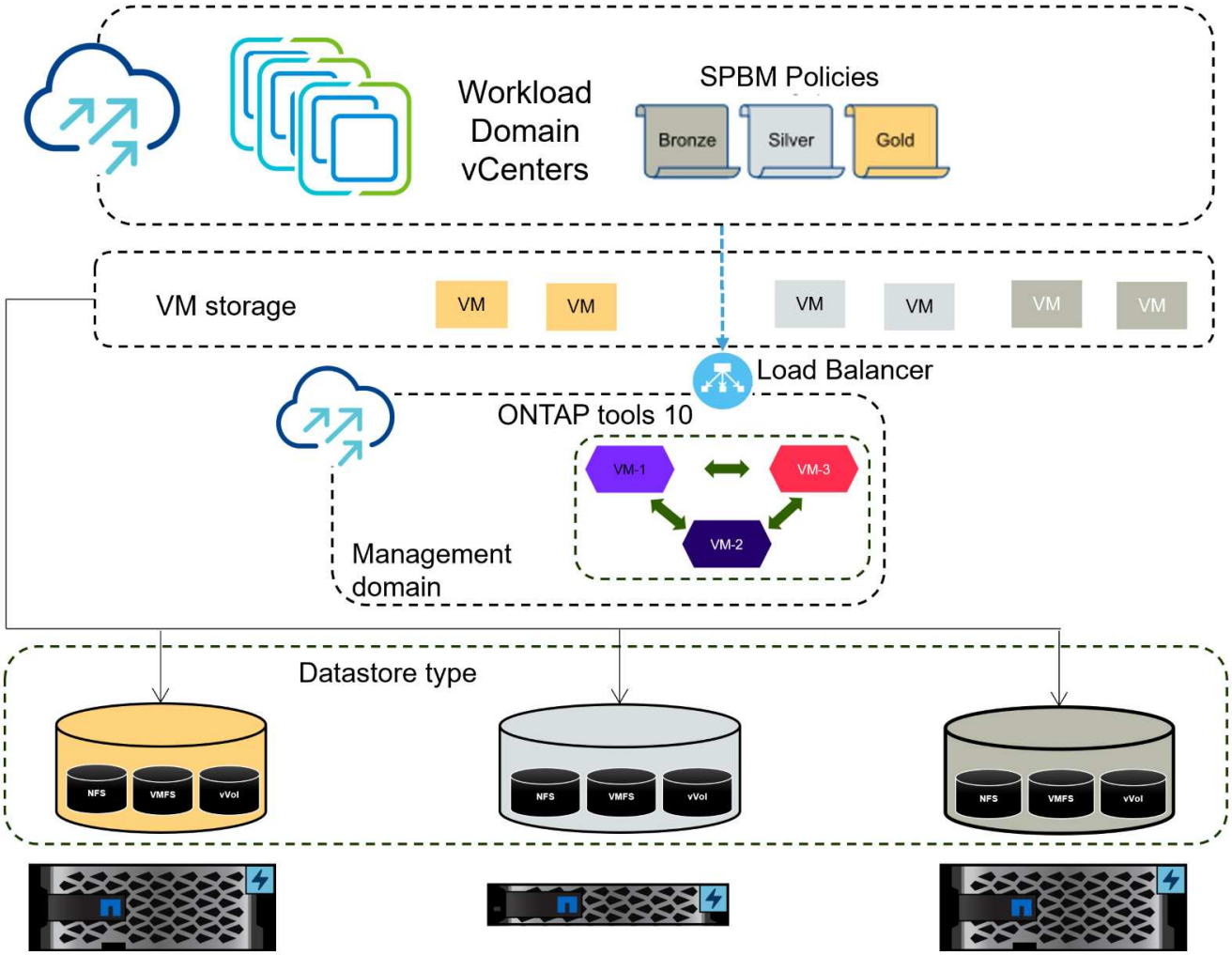
Solution Overview

This scenario covers the following high level steps:

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

Architecture

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



Prerequisites

This solution requires the following components and configurations:

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

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

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

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

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

Deployment Steps

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

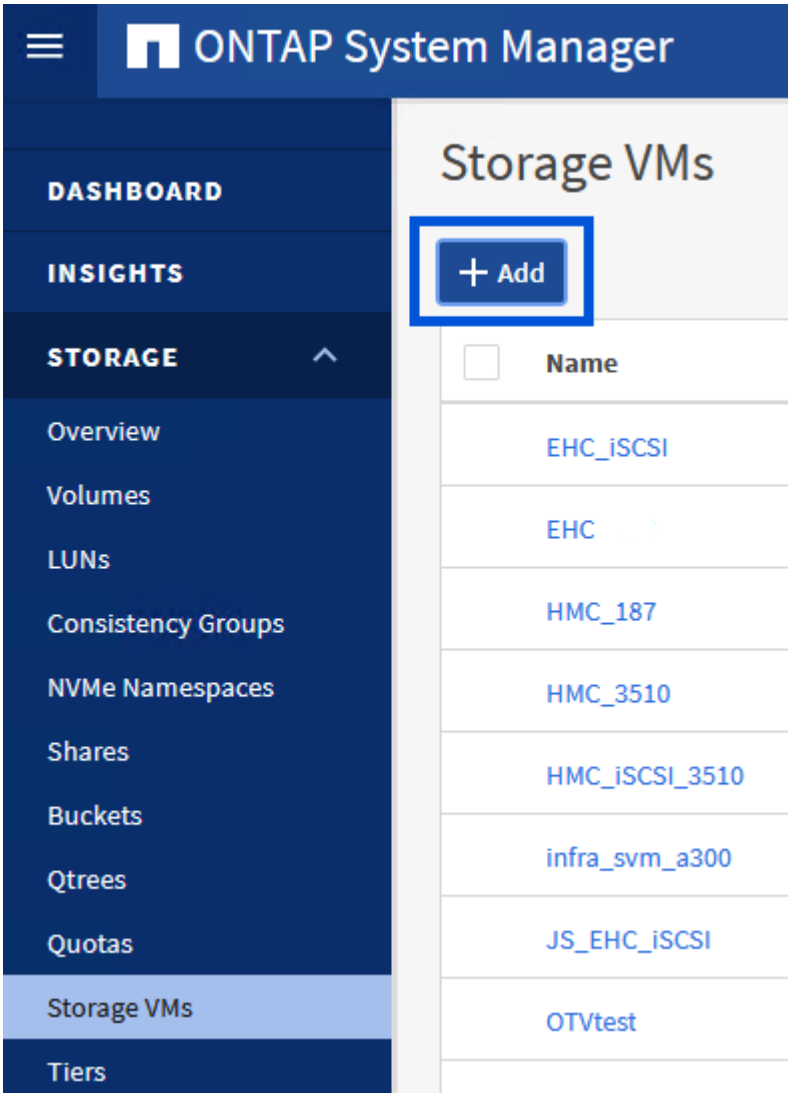
Create SVM and LIFs on ONTAP storage system

The following step is performed in ONTAP System Manager.

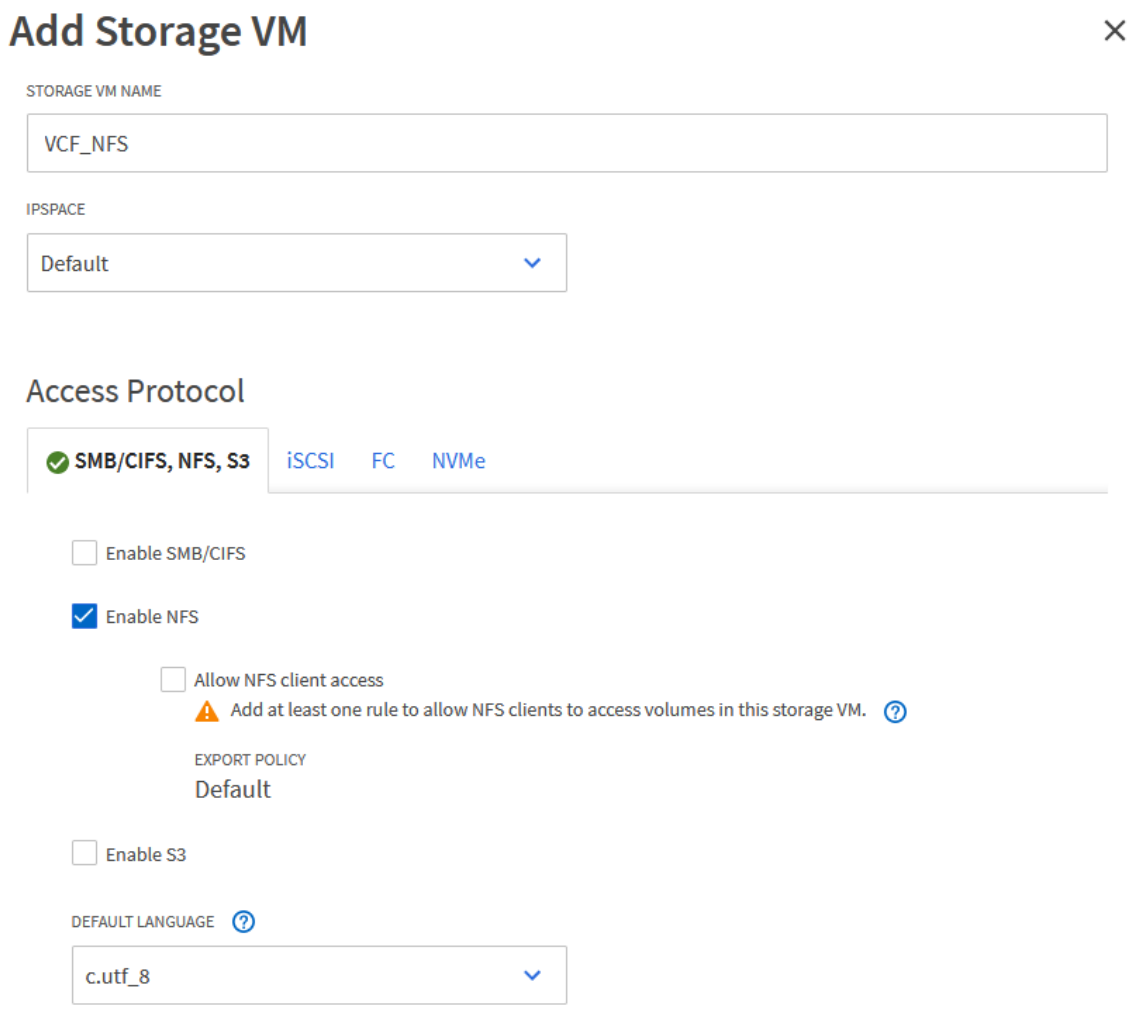
Create the storage VM and LIFs

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

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

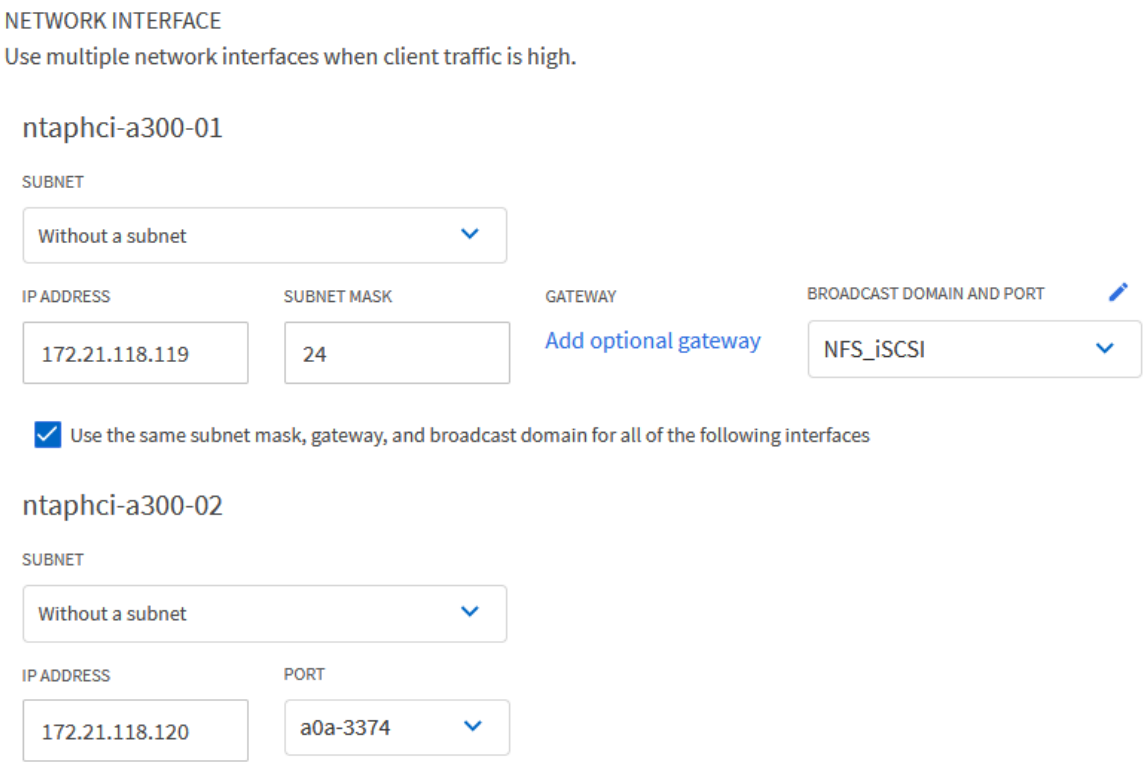


2. In the **Add Storage VM** wizard provide a **Name** for the SVM, select the **IP Space** and then, under **Access Protocol**, click on the **SMB/CIFS, NFS, S3** tab and check the box to **Enable NFS**.

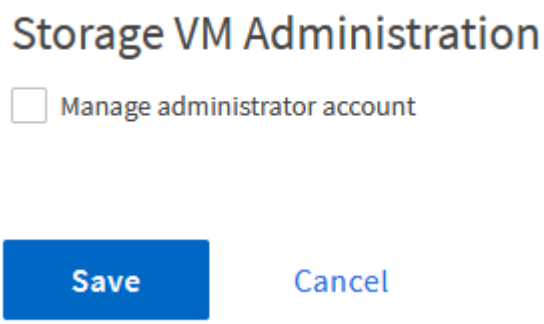


It is not necessary to check the **Allow NFS client access** button here as Ontap tools for VMware vSphere will be used to automate the datastore deployment process. This includes providing client access for the ESXi hosts.

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.



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



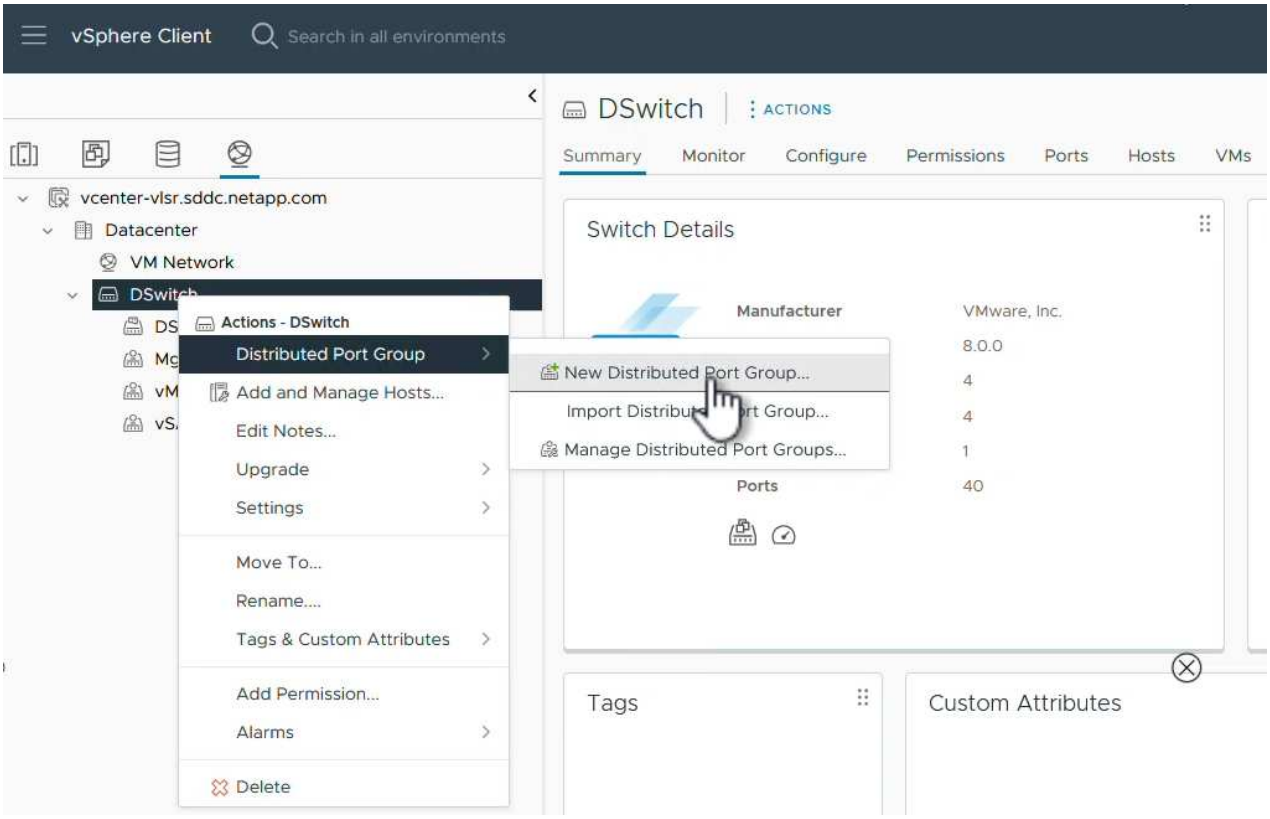
Set up networking for NFS on ESXi hosts

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.

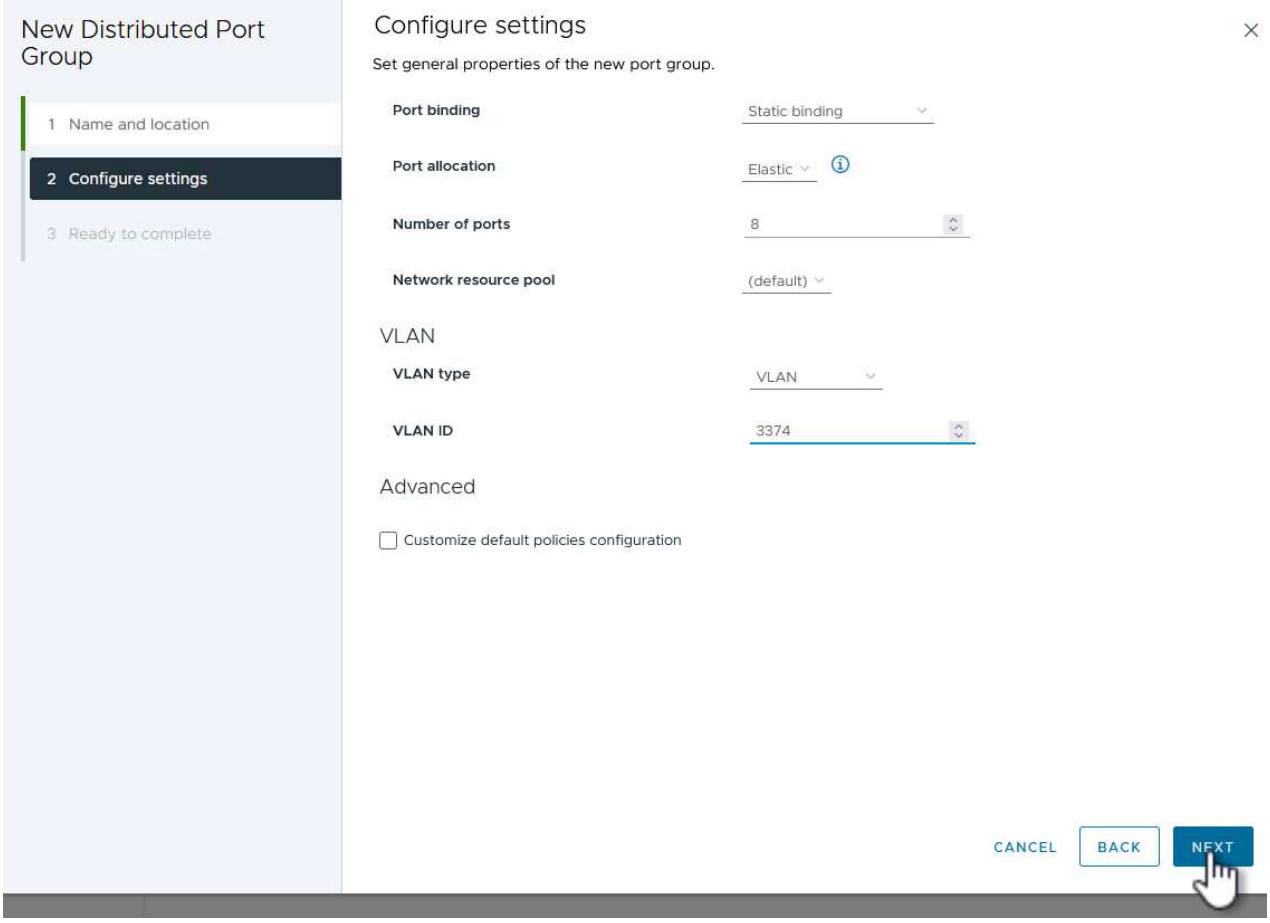
Create a Distributed Port Group for NFS traffic

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

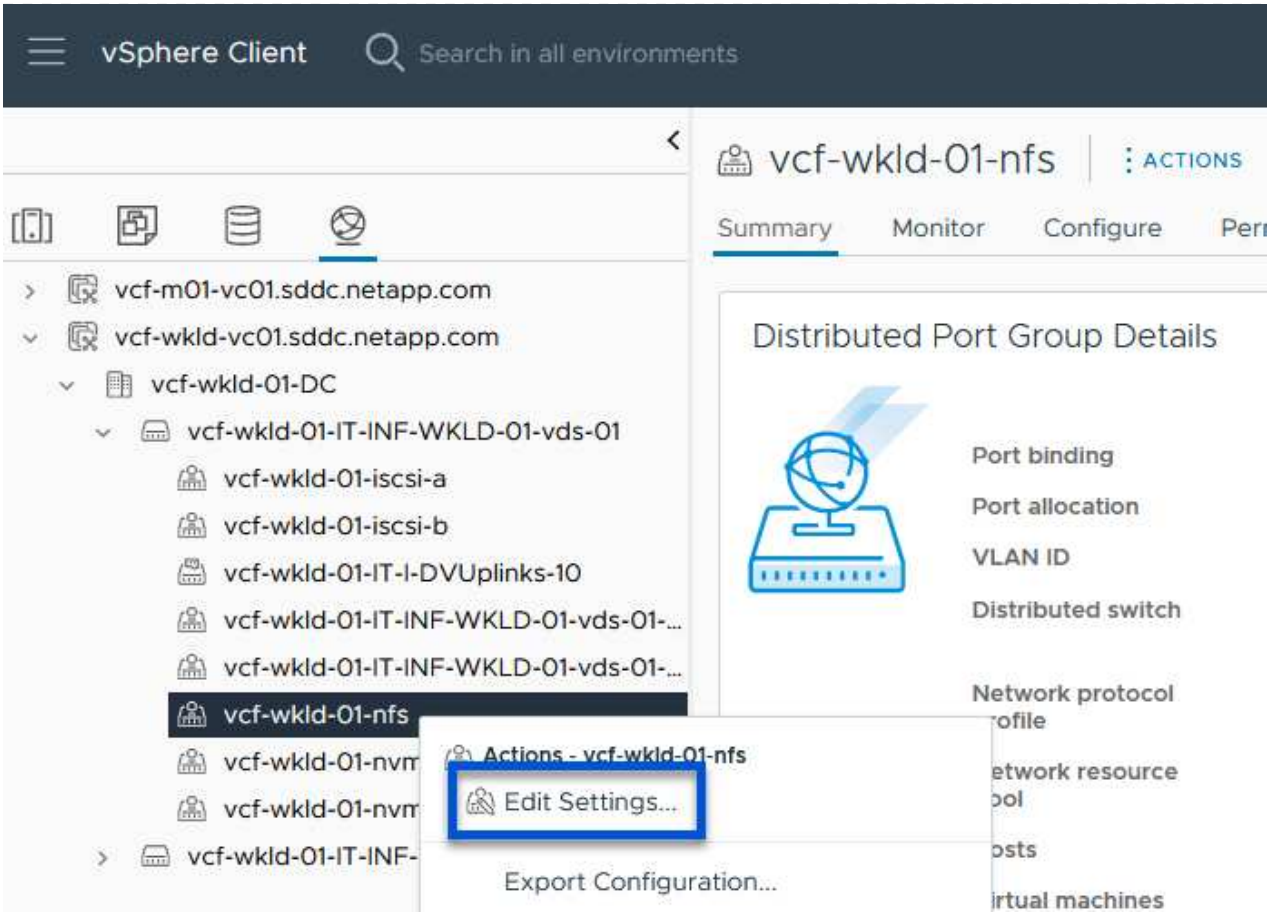
1. From the vSphere client , navigate to **Inventory > Networking** for the workload domain. Navigate to the existing Distributed Switch and choose the action to create **New Distributed Port Group…**.



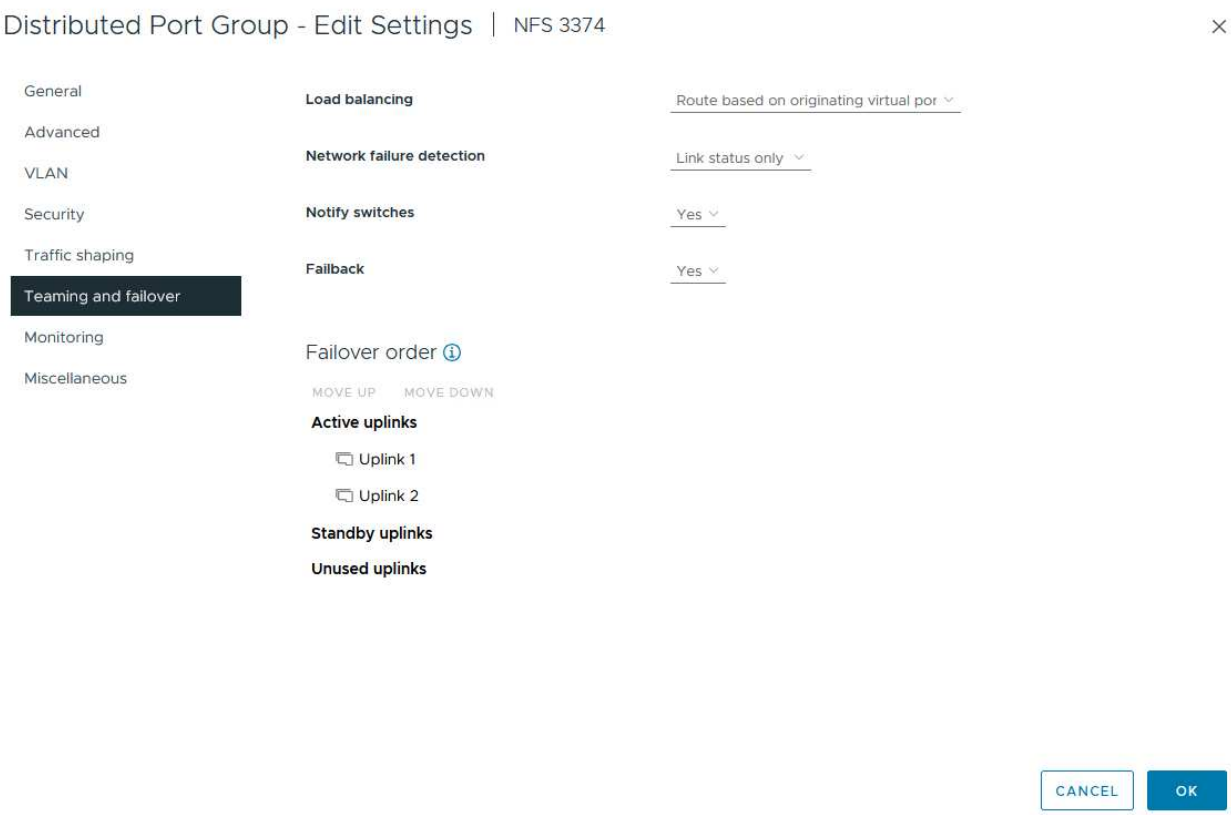
2. In the **New Distributed Port Group** wizard fill in a name for the new port group and click on **Next** to continue.
3. On the **Configure settings** page fill out all settings. If VLANs are being used be sure to provide the correct VLAN ID. Click on **Next** to continue.



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**.

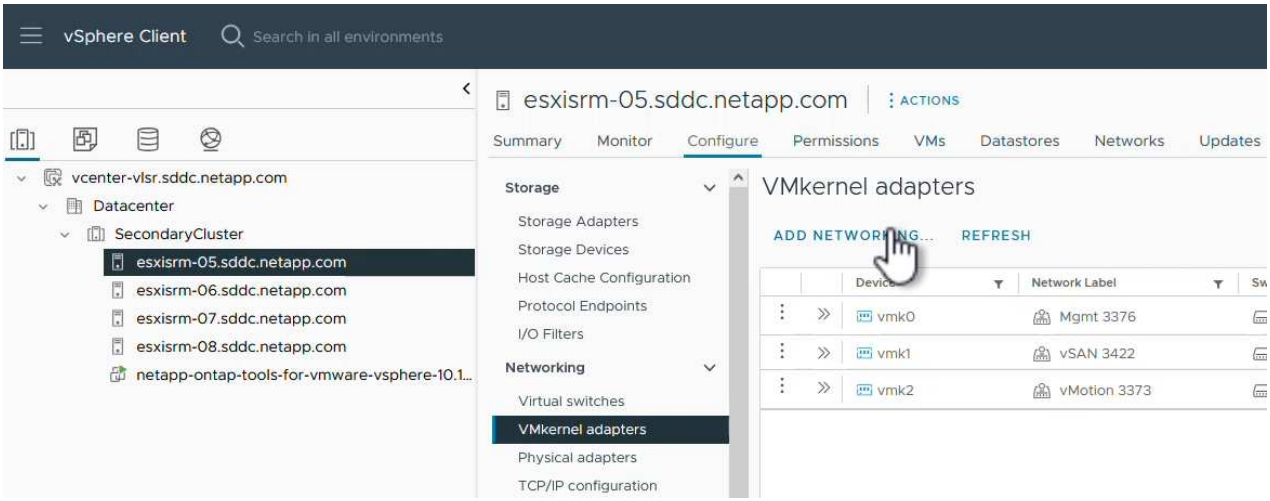


7. Repeat this process for each ESXi host in the cluster.

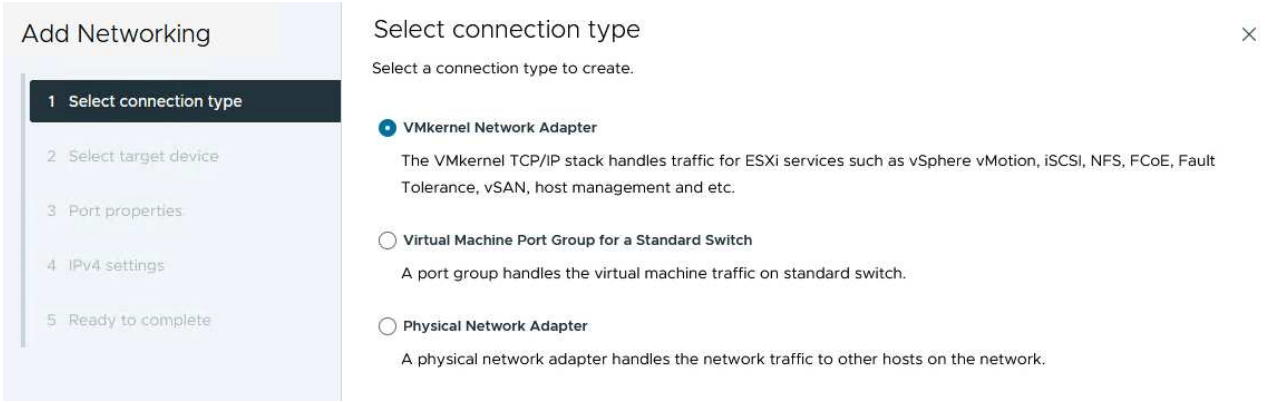
Create a VMkernel adapter on each ESXi host

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

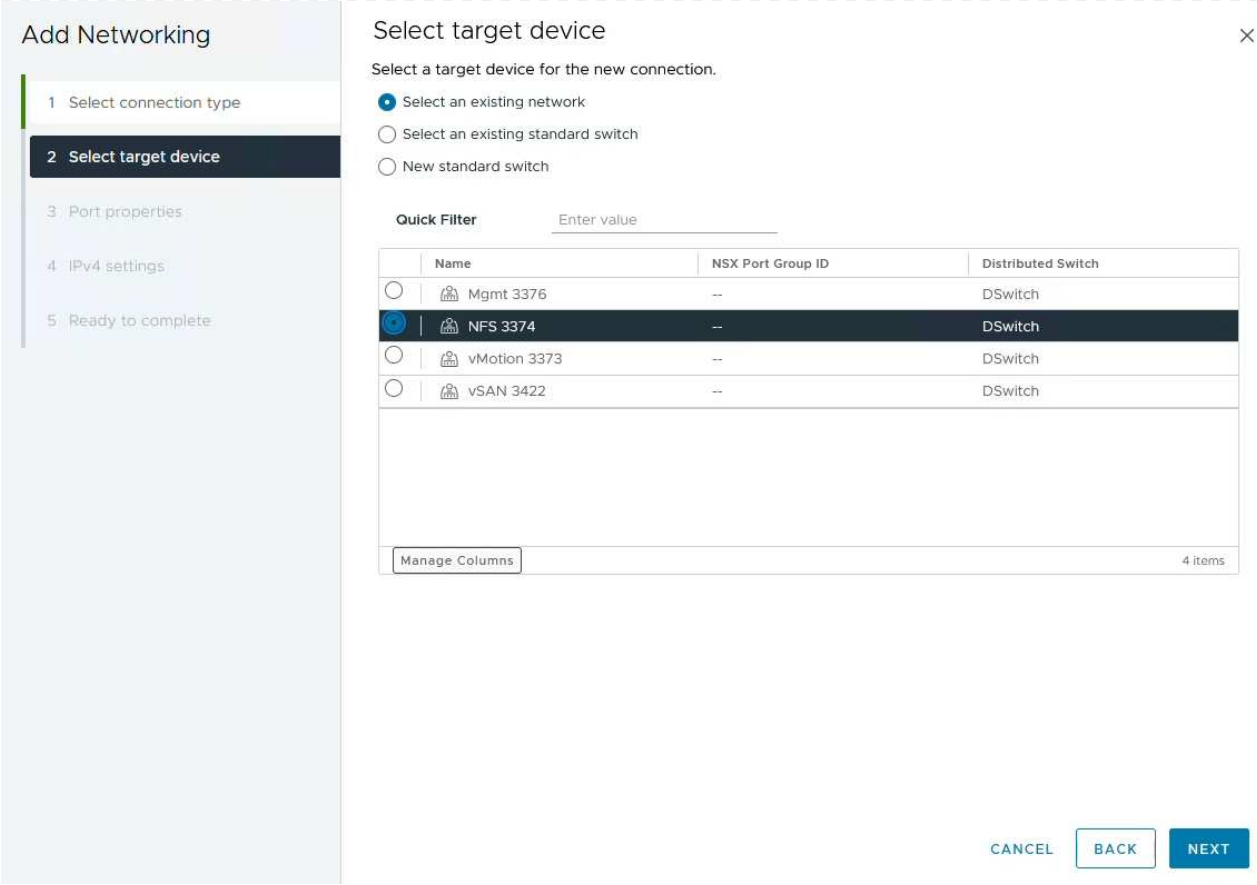
1. From the vSphere client navigate to one of the ESXi hosts in the workload domain inventory. From the **Configure** tab select **VMkernel adapters** and click on **Add Networking…** to start.



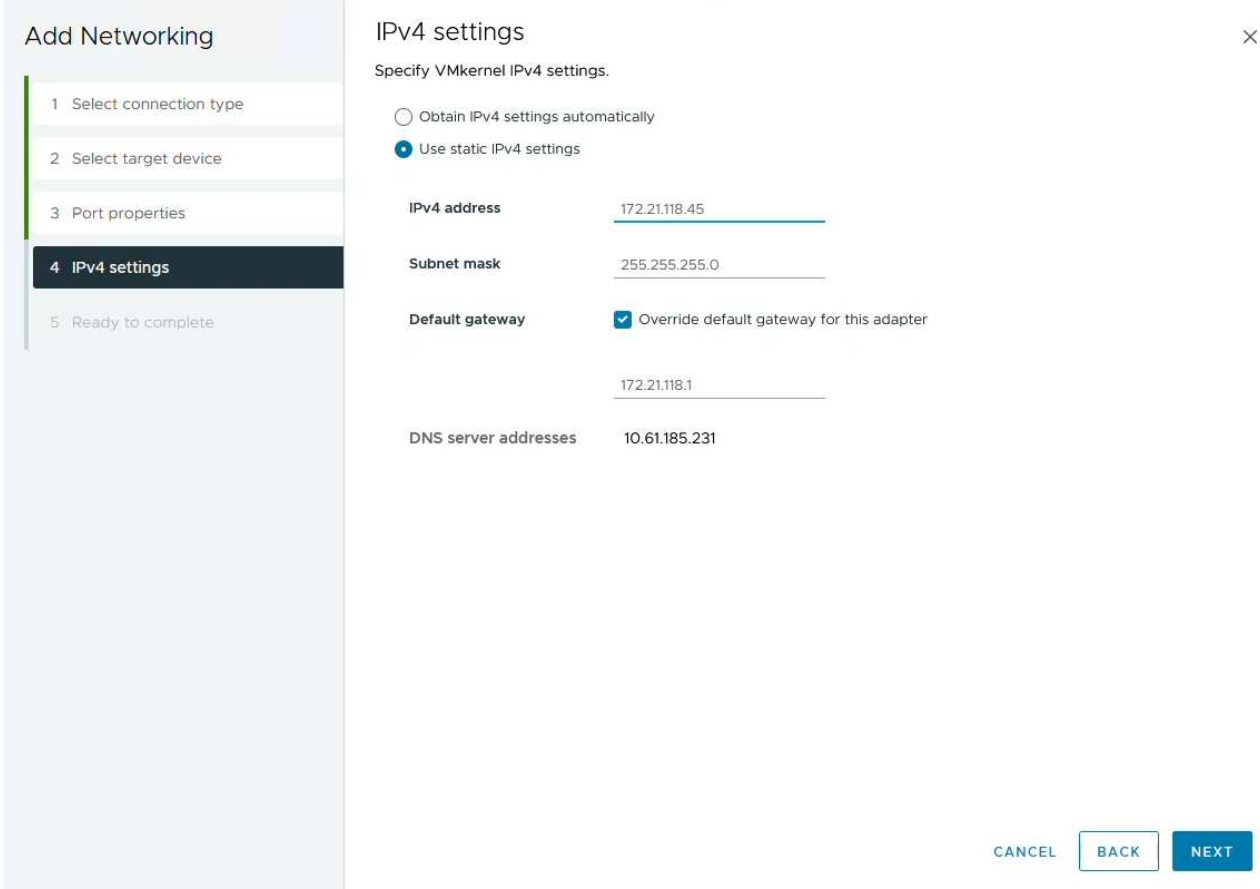
2. On the **Select connection type** window choose **VMkernel Network Adapter** and click on **Next** to continue.



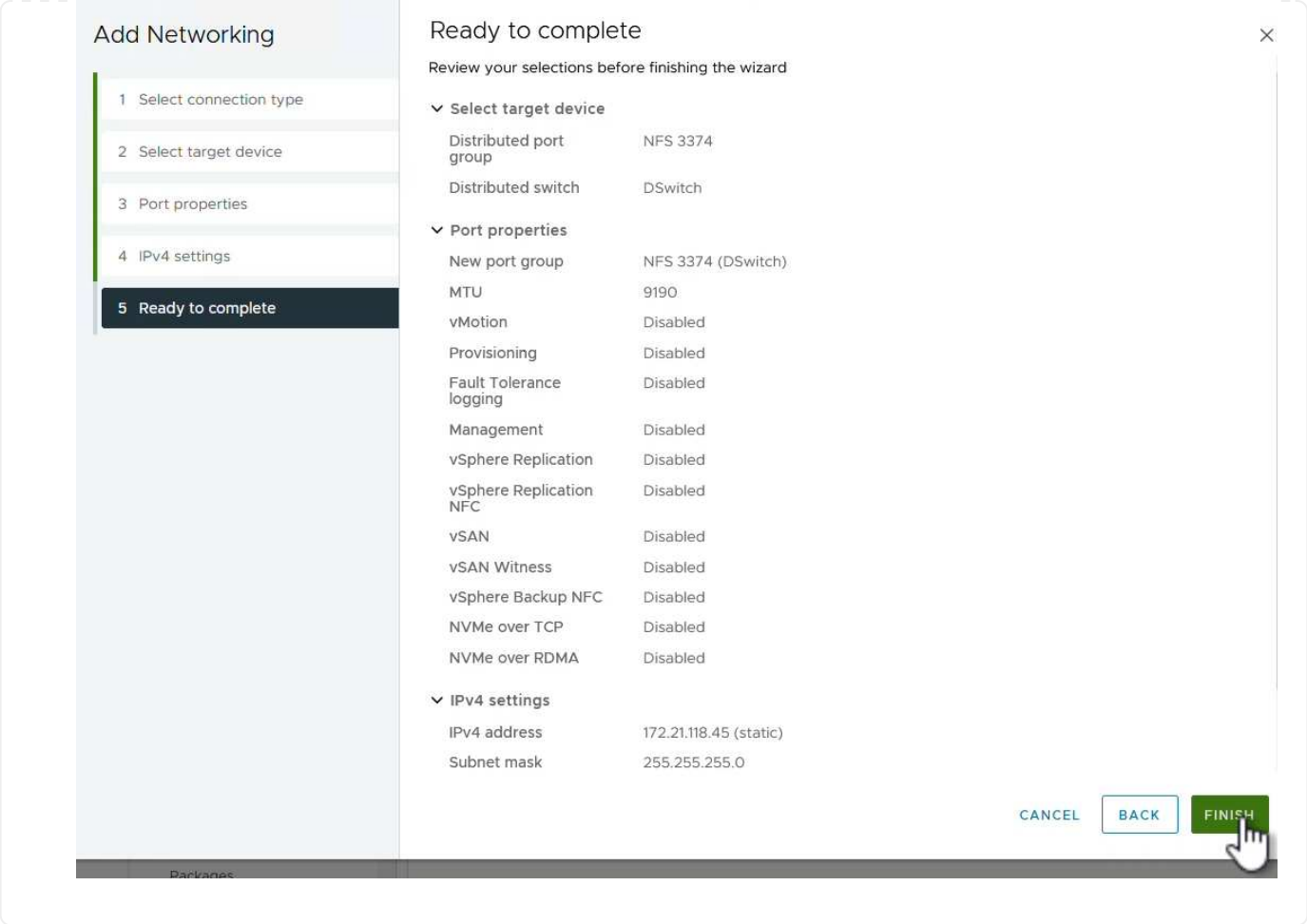
3. On the **Select target device** page, choose one of the distributed port groups for NFS that was created previously.



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.



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.

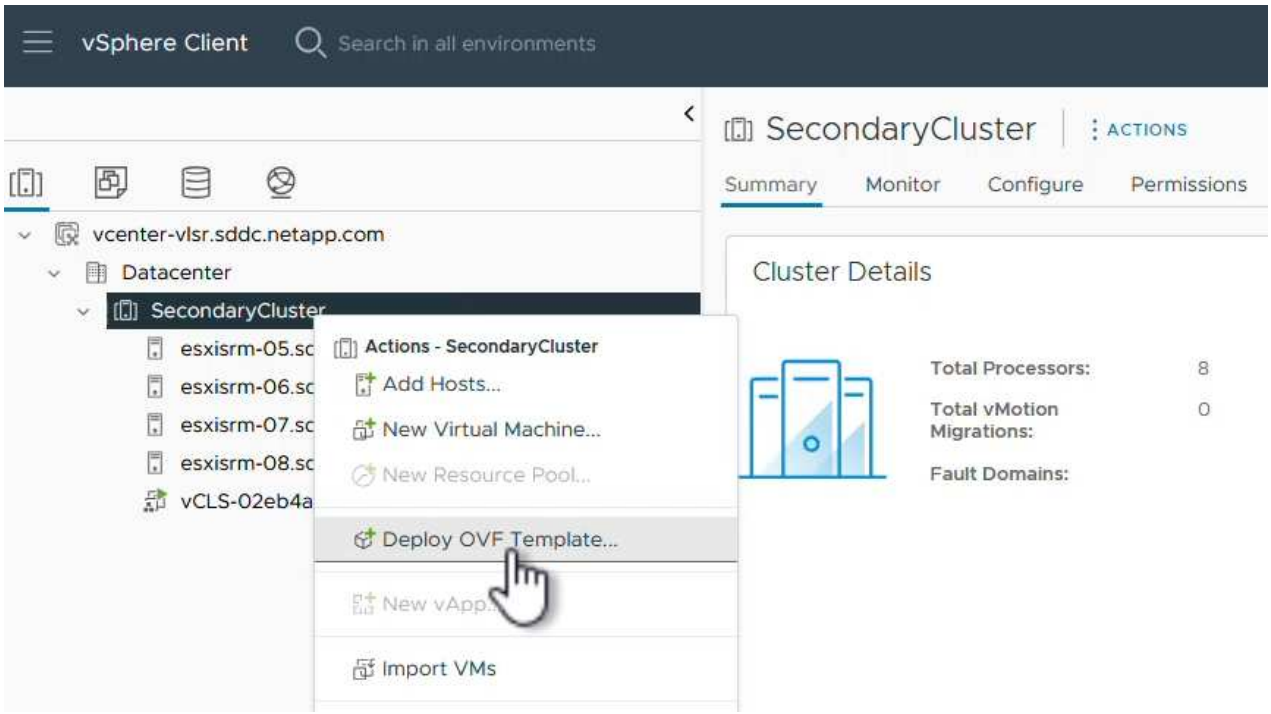
Deploy ONTAP tools for VMware vSphere 10

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.

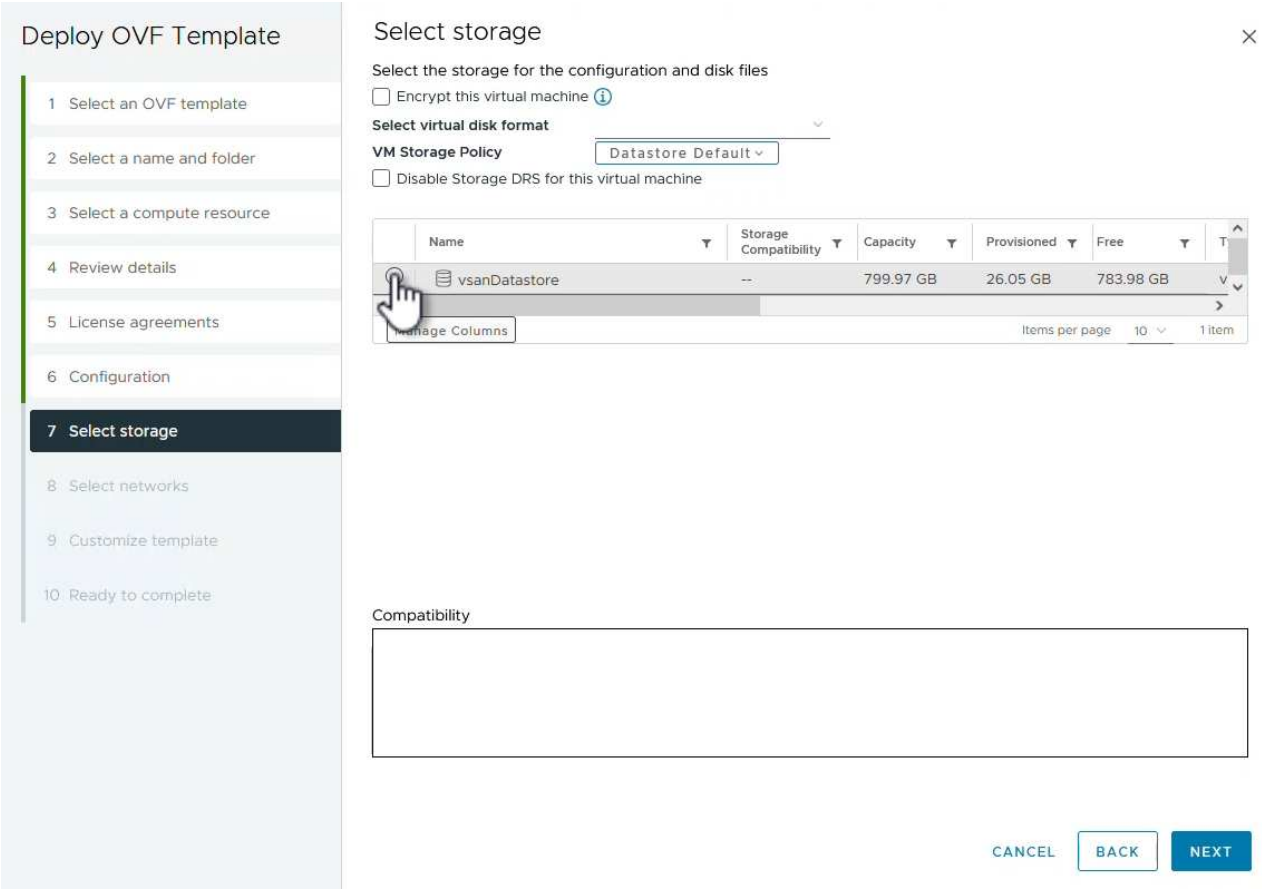
Complete the following to Deploy ONTAP tools for VMware vSphere:

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…**

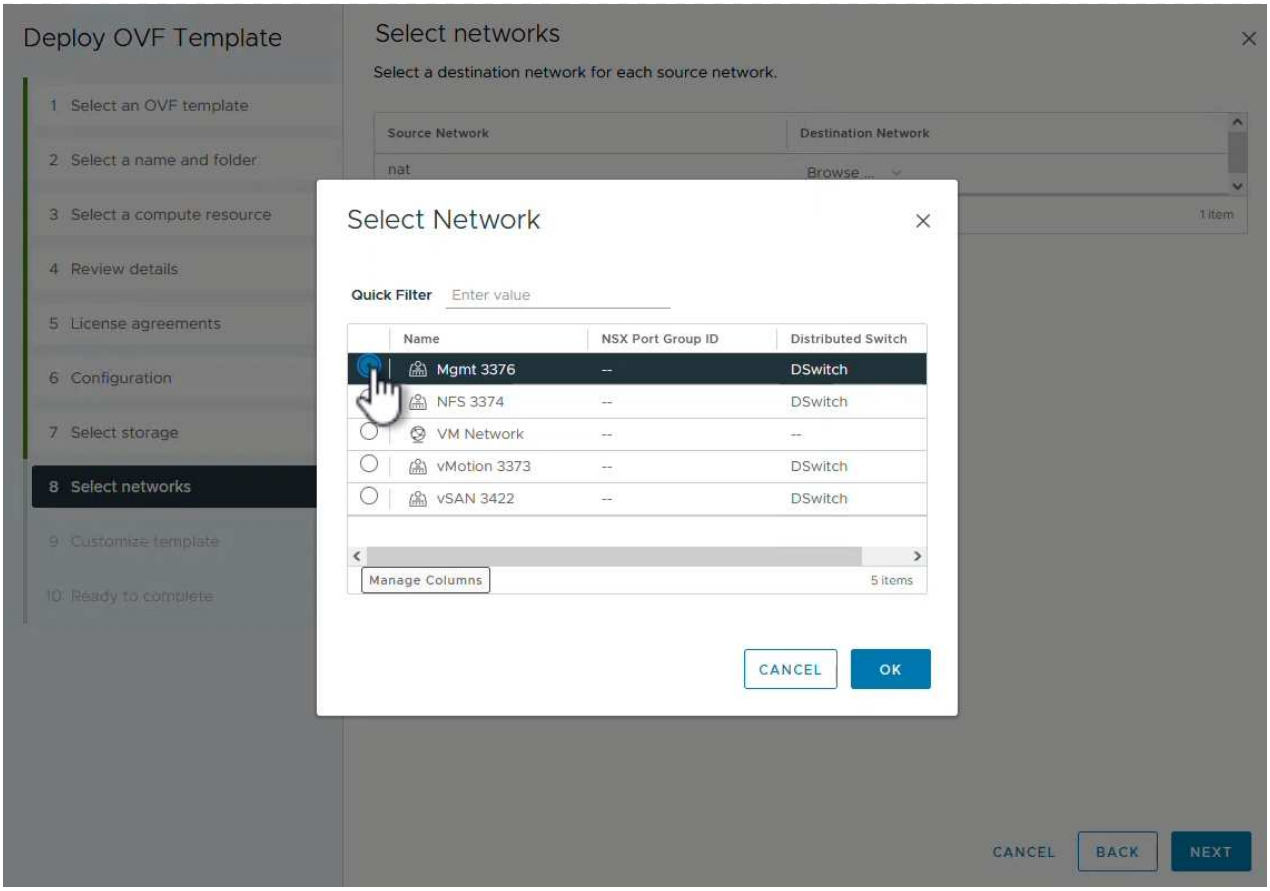


4. In the **Deploy OVF Template** wizard click the **Local file** radio button and select the ONTAP tools OVA file downloaded in the previous step.

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.

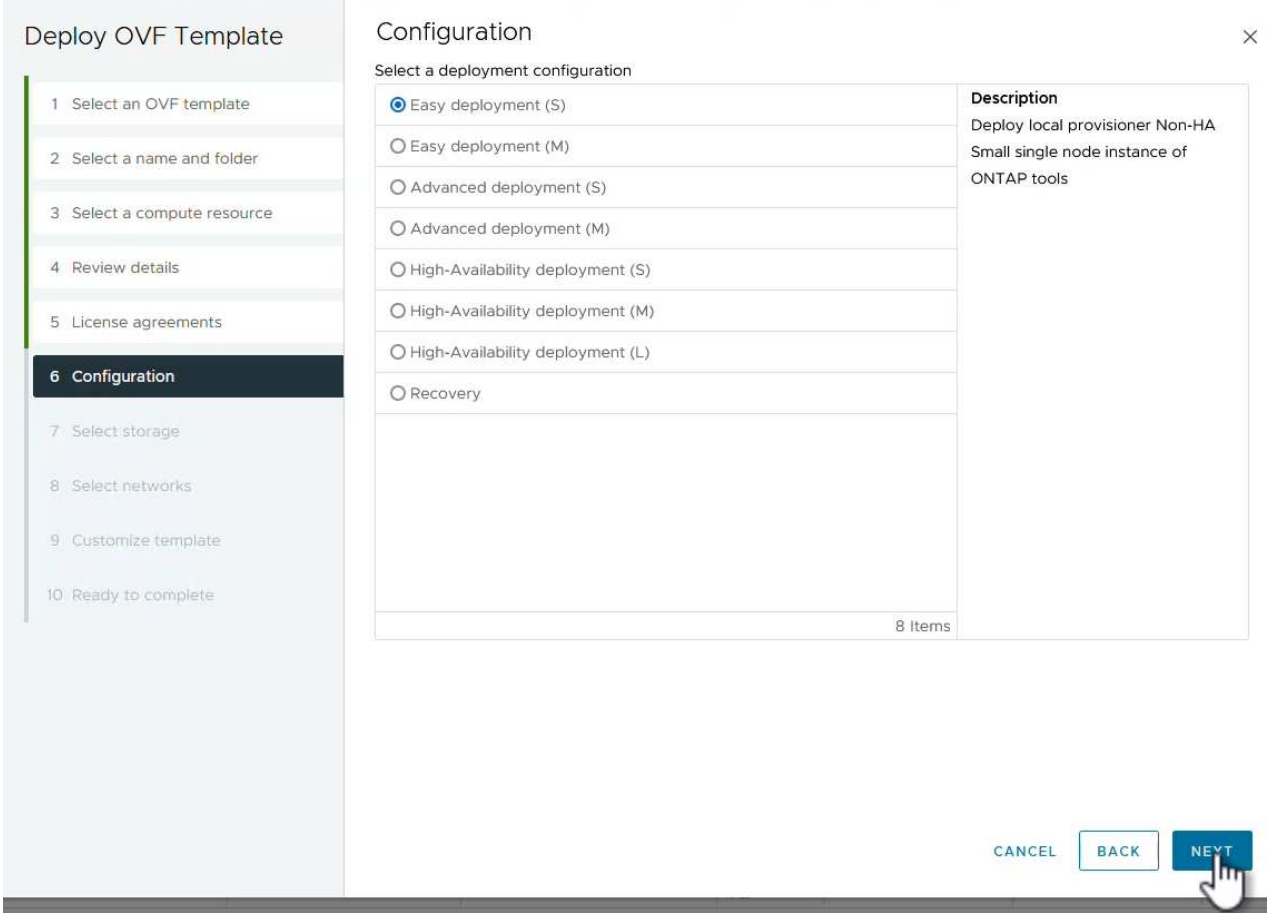


7. On the Select network page select the network used for management traffic.



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.



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

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

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

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

CANCEL BACK NEXT

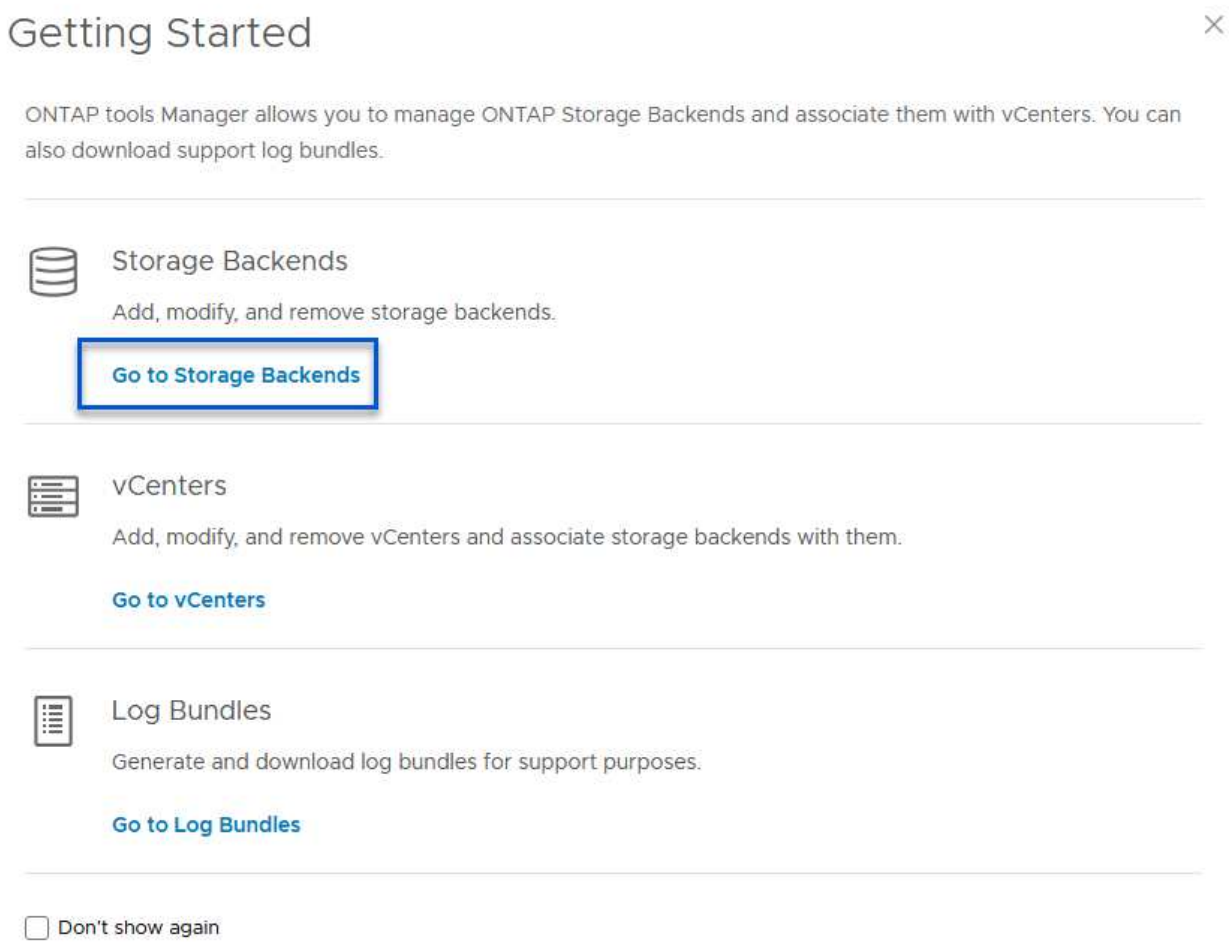
10. Review all information on the Ready to complete page and the click Finish to begin deploying the ONTAP tools appliance.

Connect Storage Backend and vCenter Server to ONTAP tools 10.

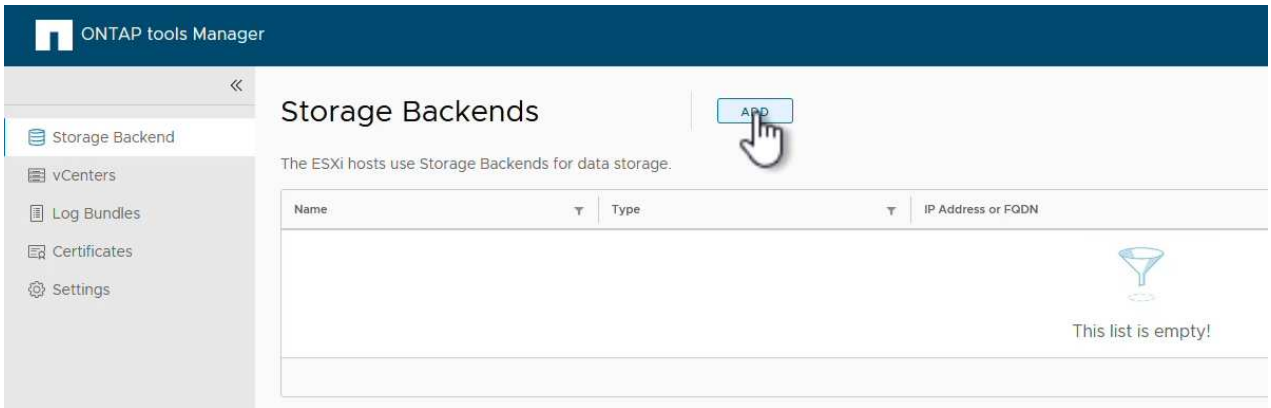
ONTAP tools manager is used to configure global settings for ONTAP Tools 10.

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.

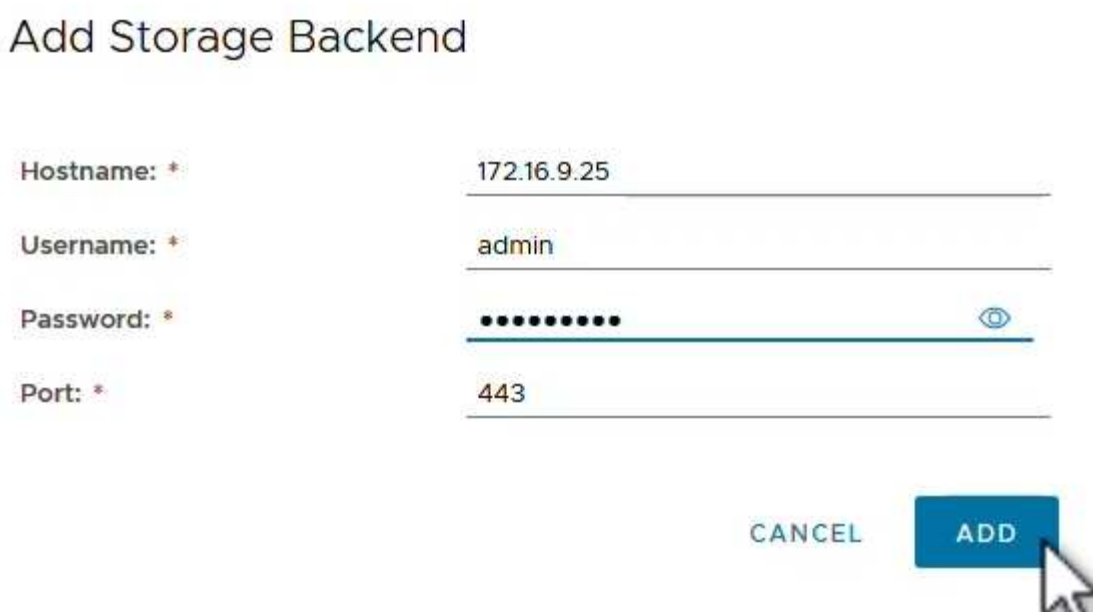
2. On the **Getting Started** page click on **Go to Storage Backends**.



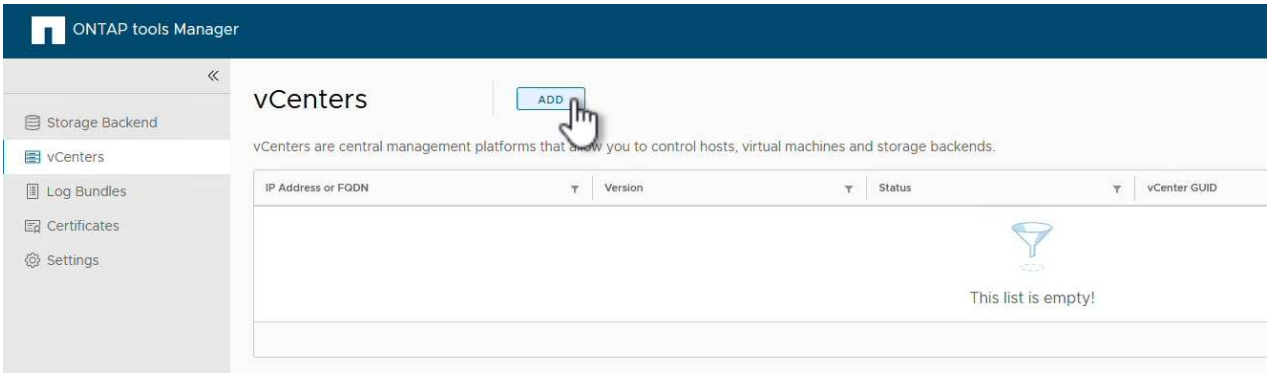
3. On the **Storage Backends** page, click on **ADD** to fill in the credentials of an ONTAP storage system to be registered with ONTAP tools 10.



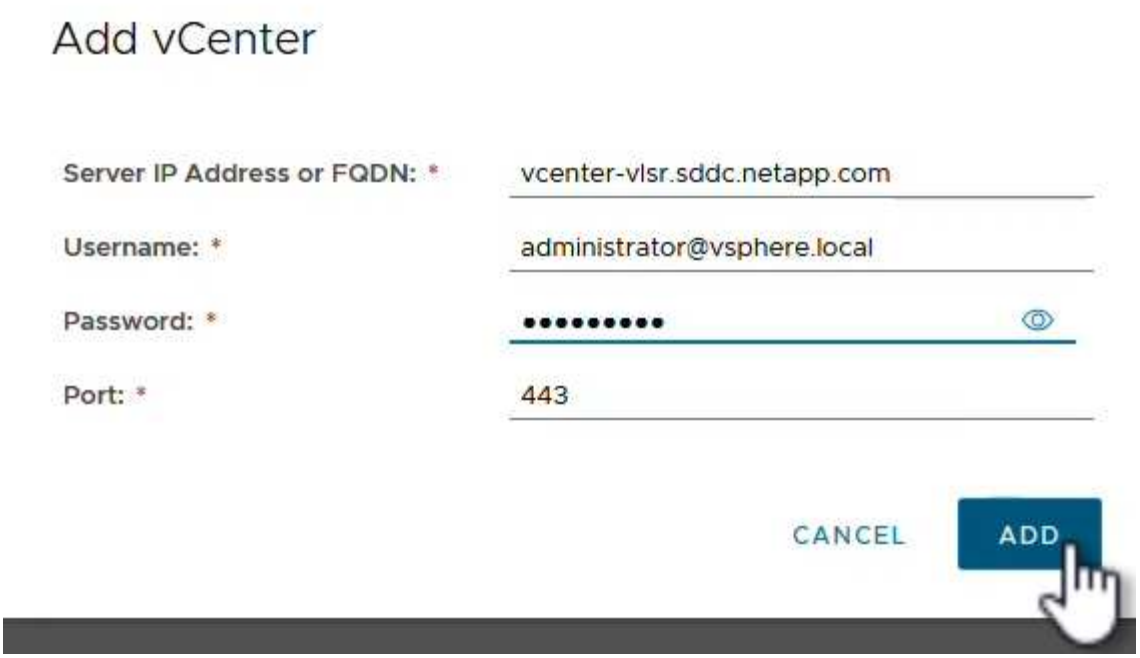
4. On the **Add Storage Backend** box, fill out the credentials for the ONTAP storage system.



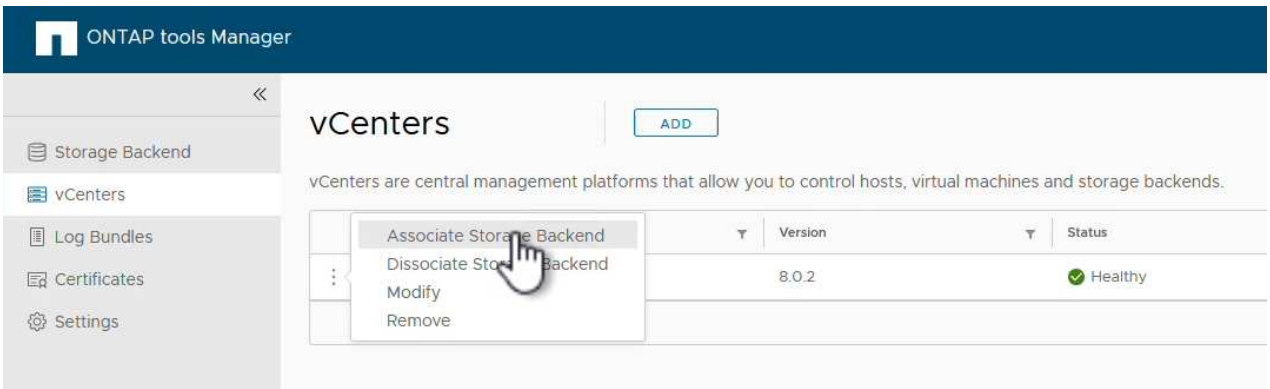
5. In the left hand menu click on **vCenters**, and then on on **ADD** to fill in the credentials of a vCenter server to be registered with ONTAP tools 10.



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

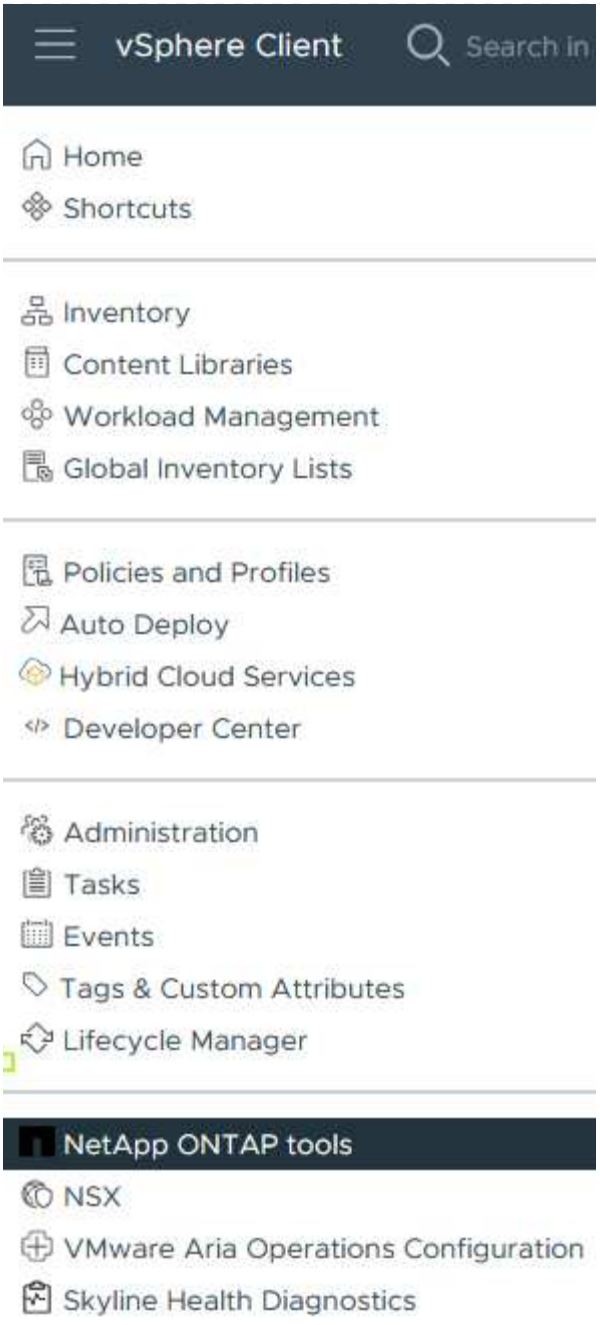


7. From the vertical three-dot menu for the newly discovered vCenter server, select **Associate Storage Backend**.

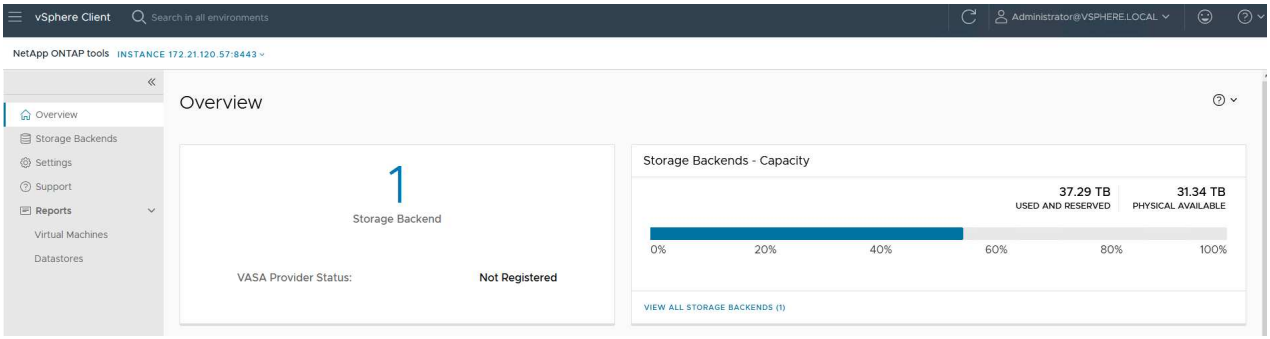


8. On the **Associate Storage Backend** box, select the ONTAP storage system to associated with the vCenter server and click on **Associate** to complete the action.

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



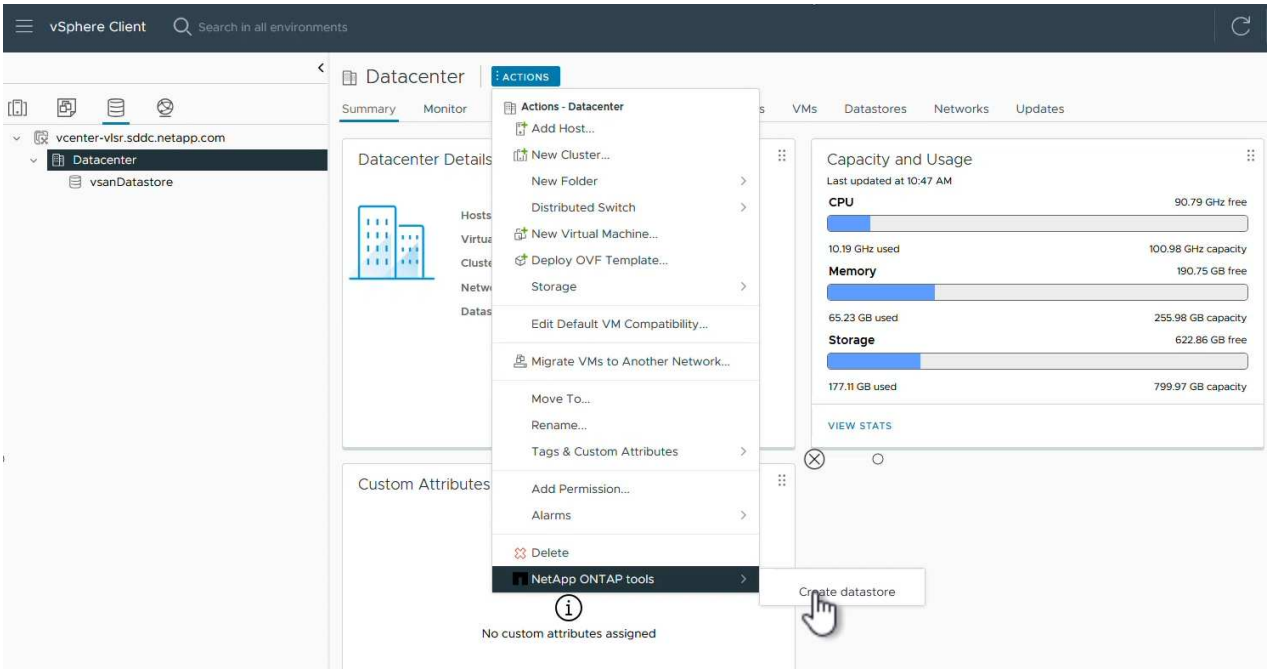
10. From the ONTAP tools dashboard you should see that a Storage Backend was associated with the vCenter Server.



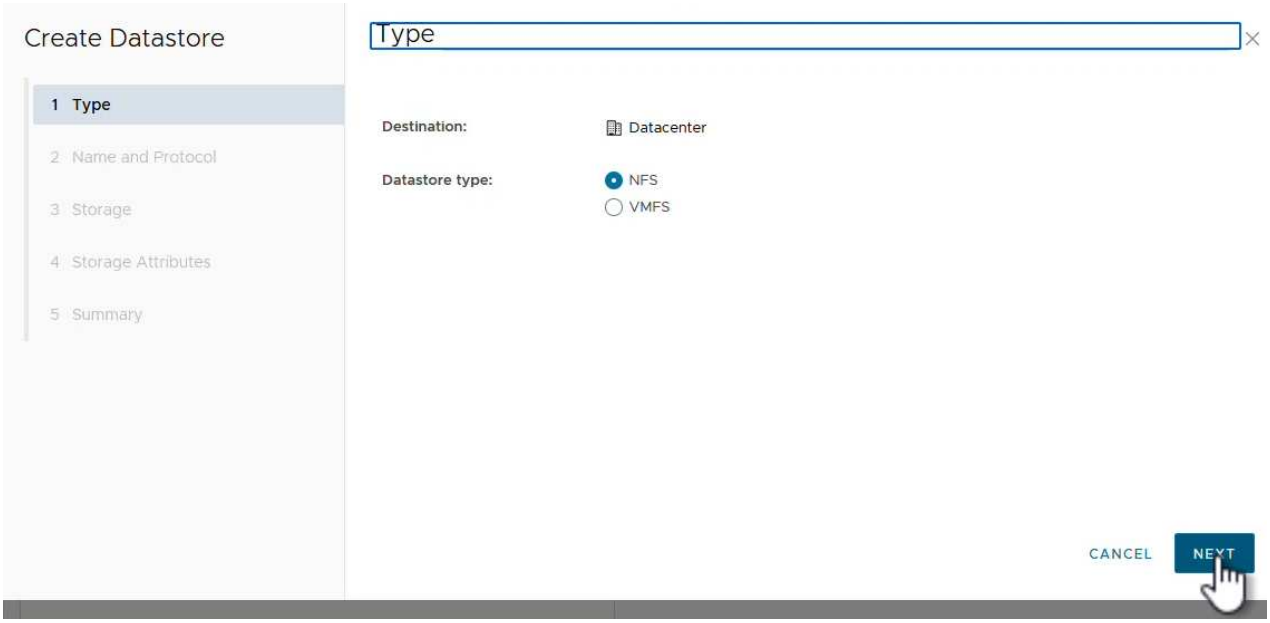
Create an NFS datastore using ONTAP tools 10

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**.

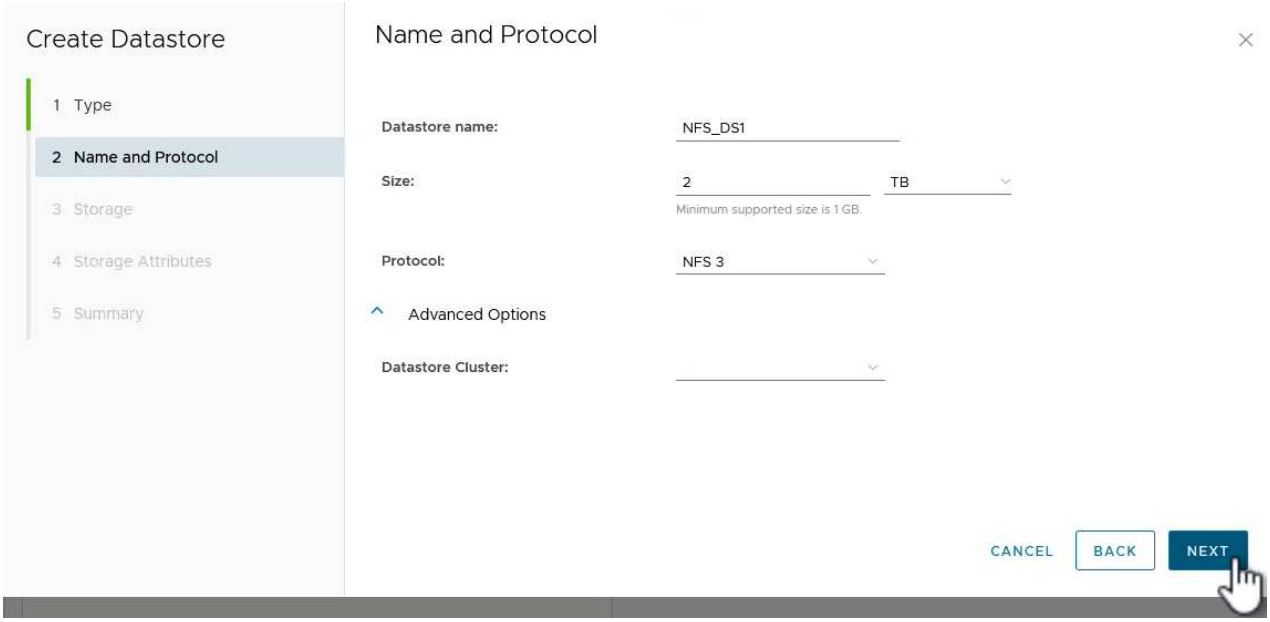


2. On the **Type** page of the Create Datastore wizard, click on the NFS radio button and then on **Next** to continue.



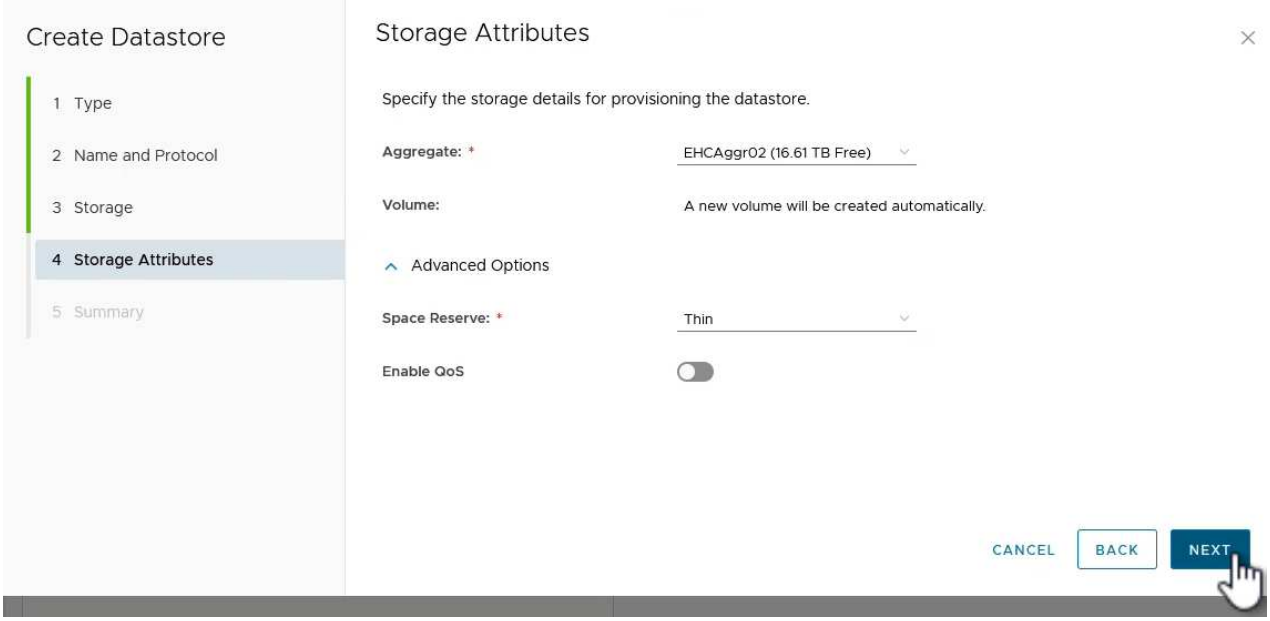
3. On the **Name and Protocol** page, fill out the name, size and protocol for the datastore. Click on **Next**

to continue.

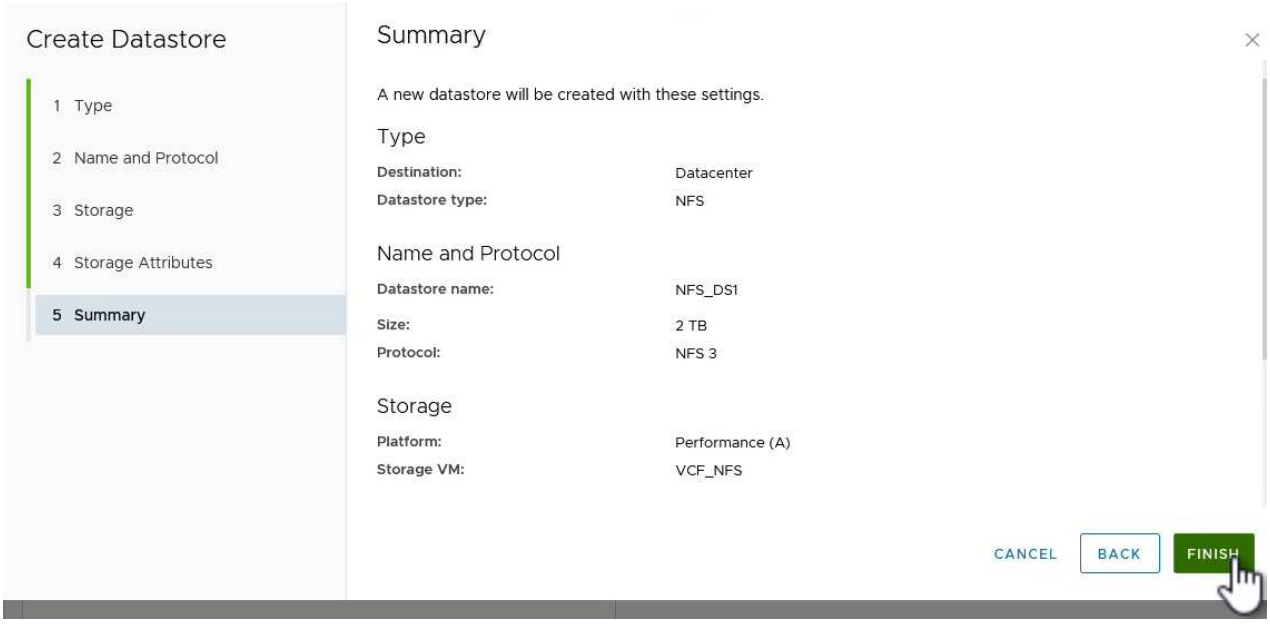


4. On the **Storage** page select a Platform (filters storage system by type) and a storage VM for the volume. Optionally, select a custom export policy. Click on **Next** to continue.

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.



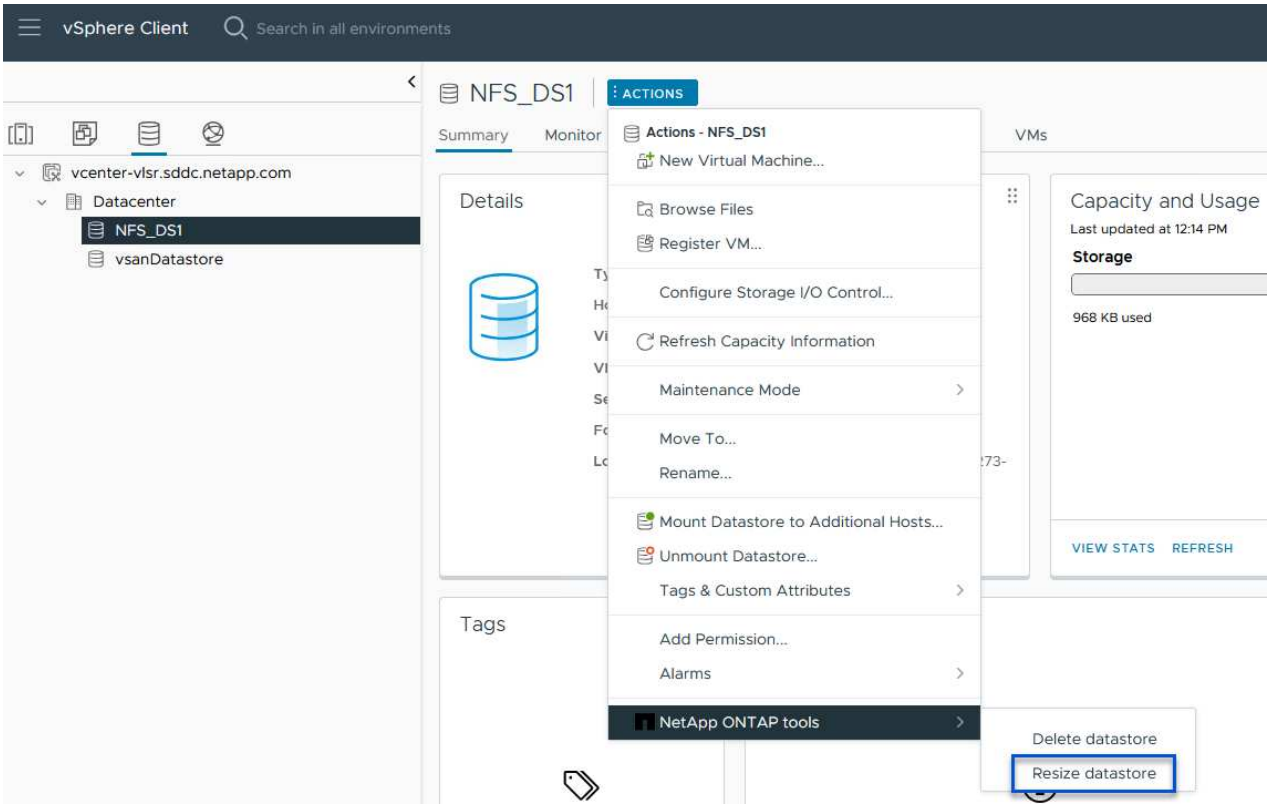
6. Finally, review the **Summary** and click on Finish to begin creating the NFS datastore.



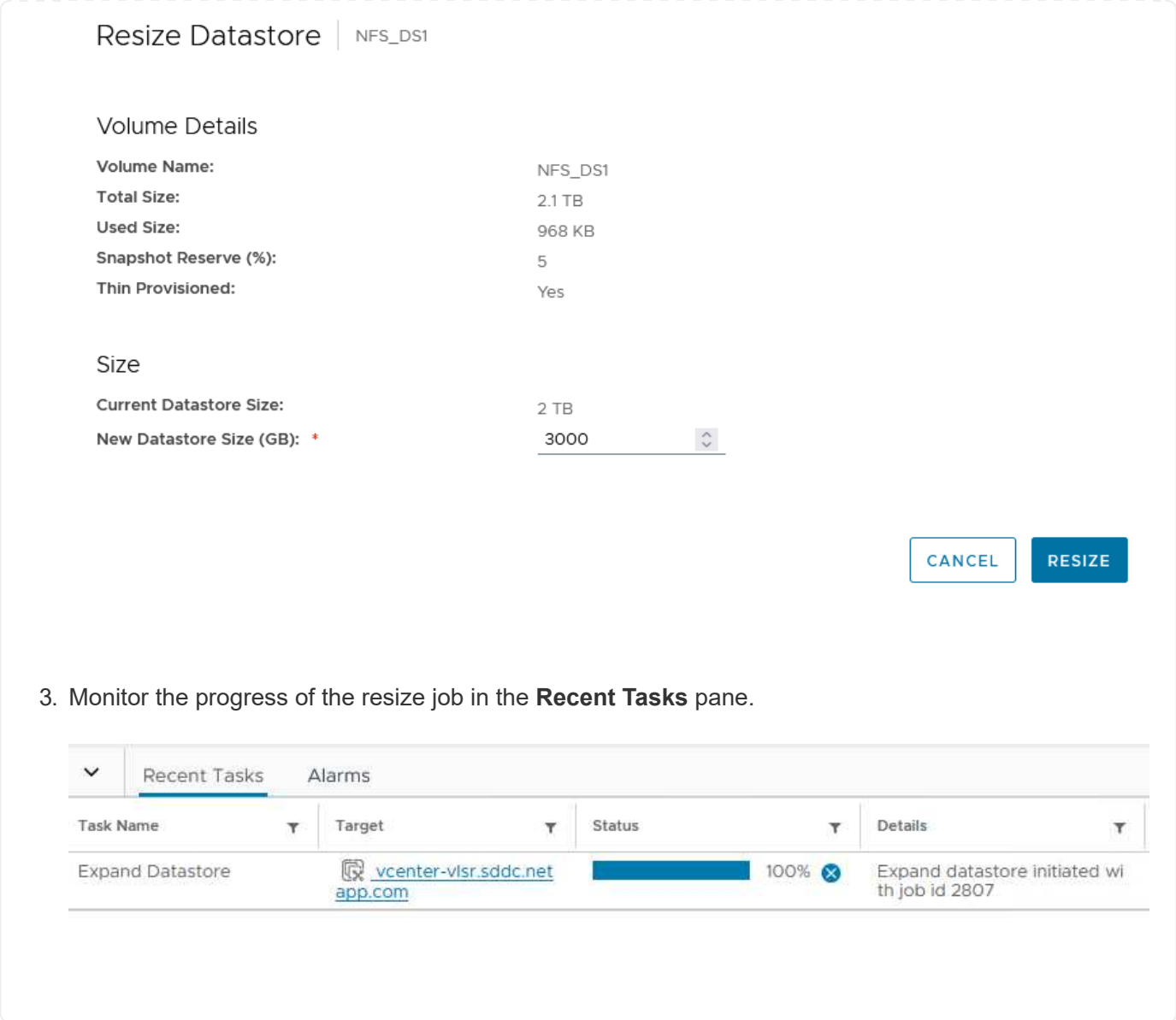
Resize an NFS datastore using ONTAP tools 10

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.



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

Additional information

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

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

Use VMware Site Recovery Manager for Disaster Recovery of NFS datastores

The utilization of ONTAP tools for VMware vSphere 10 and the Site Replication Adapter (SRA) in conjunction with VMware Site Recovery Manager (SRM) brings significant value to disaster recovery efforts. ONTAP tools 10 provide robust storage capabilities, including native high availability and scalability for the VASA Provider, supporting iSCSI and NFS vVols. This ensures data availability and simplifies the management of multiple VMware vCenter servers and ONTAP clusters. By using the SRA with VMware Site Recovery

Manager, organizations can achieve seamless replication and failover of virtual machines and data between sites, enabling efficient disaster recovery processes. The combination of ONTAP tools and the SRA empowers businesses to protect critical workloads, minimize downtime, and maintain business continuity in the face of unforeseen events or disasters.

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

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

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

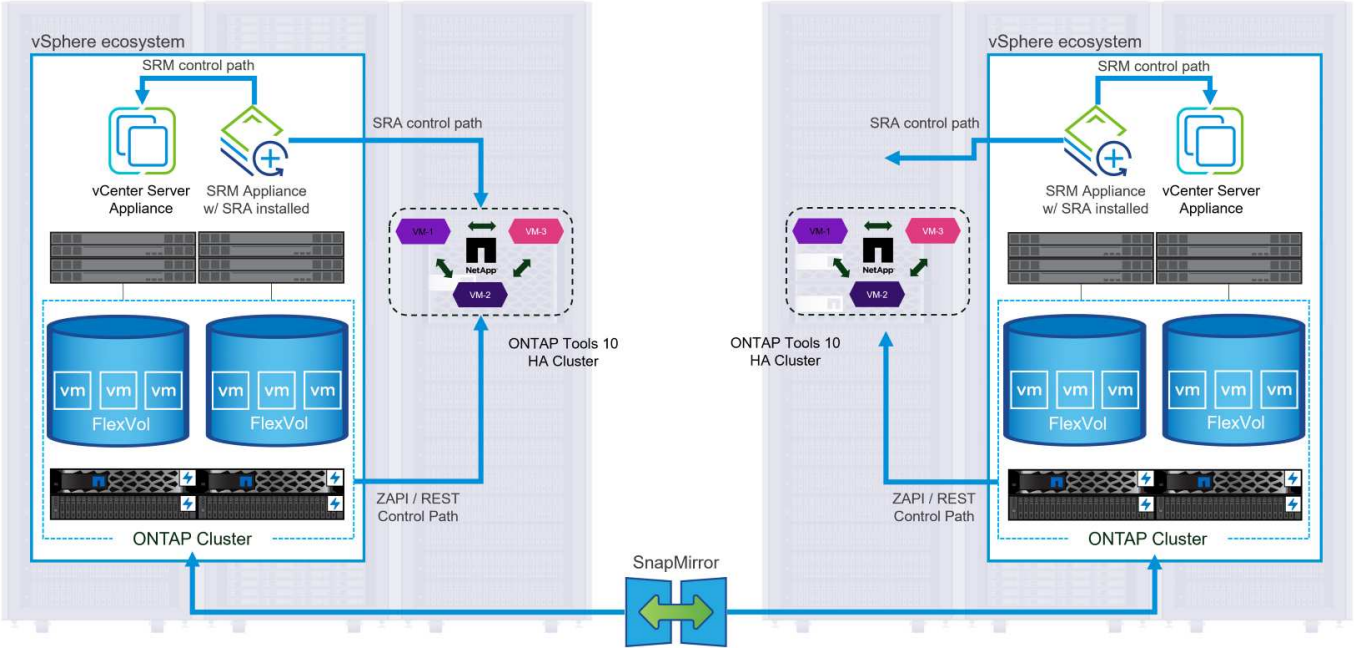
Scenario Overview

This scenario covers the following high level steps:

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

Architecture

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



Prerequisites

This scenario requires the following components and configurations:

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

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

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

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

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

Deployment Steps

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

Create SnapMirror relationship between ONTAP storage systems

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

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

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

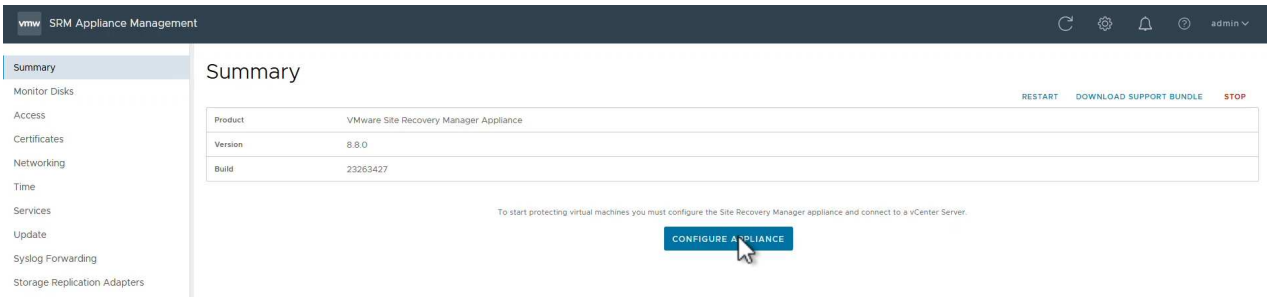
Configure the SRM appliance

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

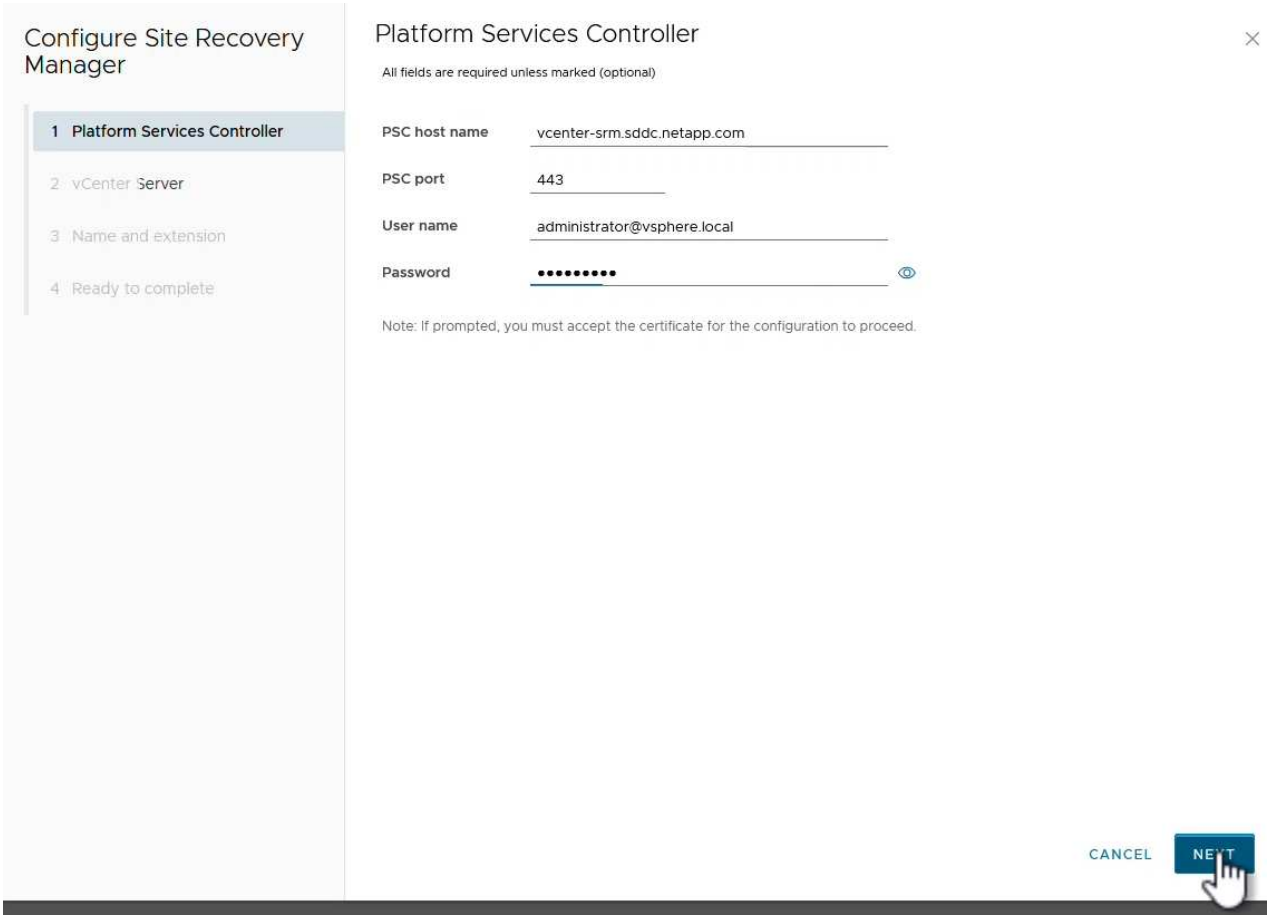
Connect the SRM appliance for primary and secondary sites

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

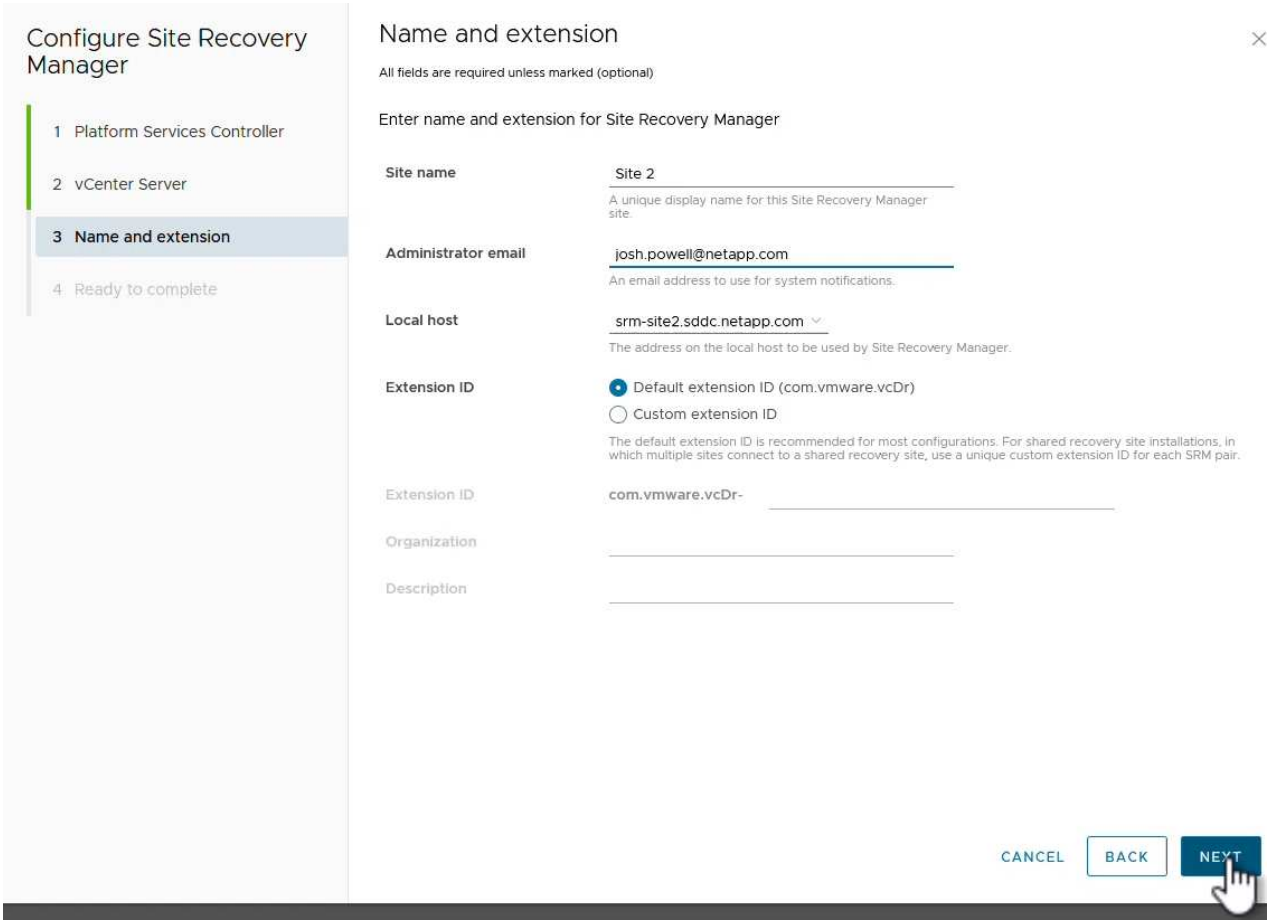
1. In a web browser, navigate to `https://<SRM_appliance_IP>:5480` and log in. Click on **Configure Appliance** to get started.



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.

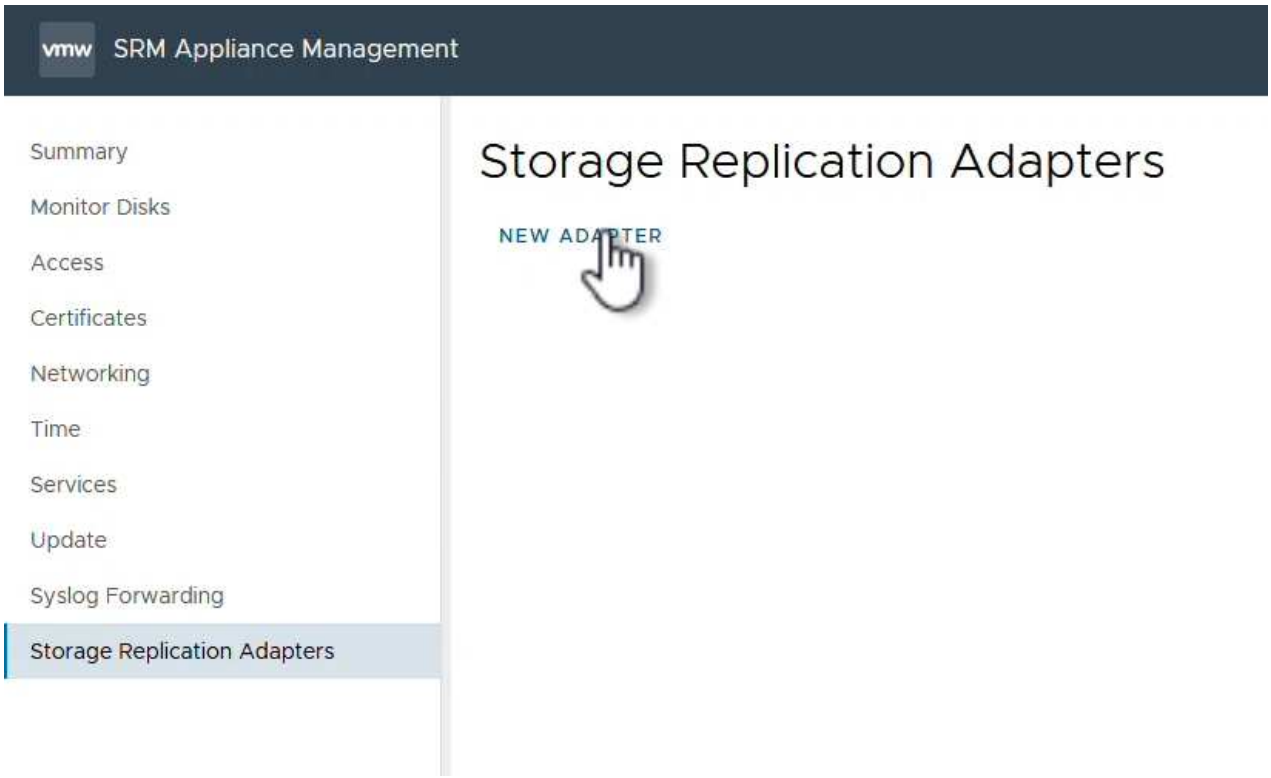


5. On the **Ready to complete** page review the summary of changes

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.

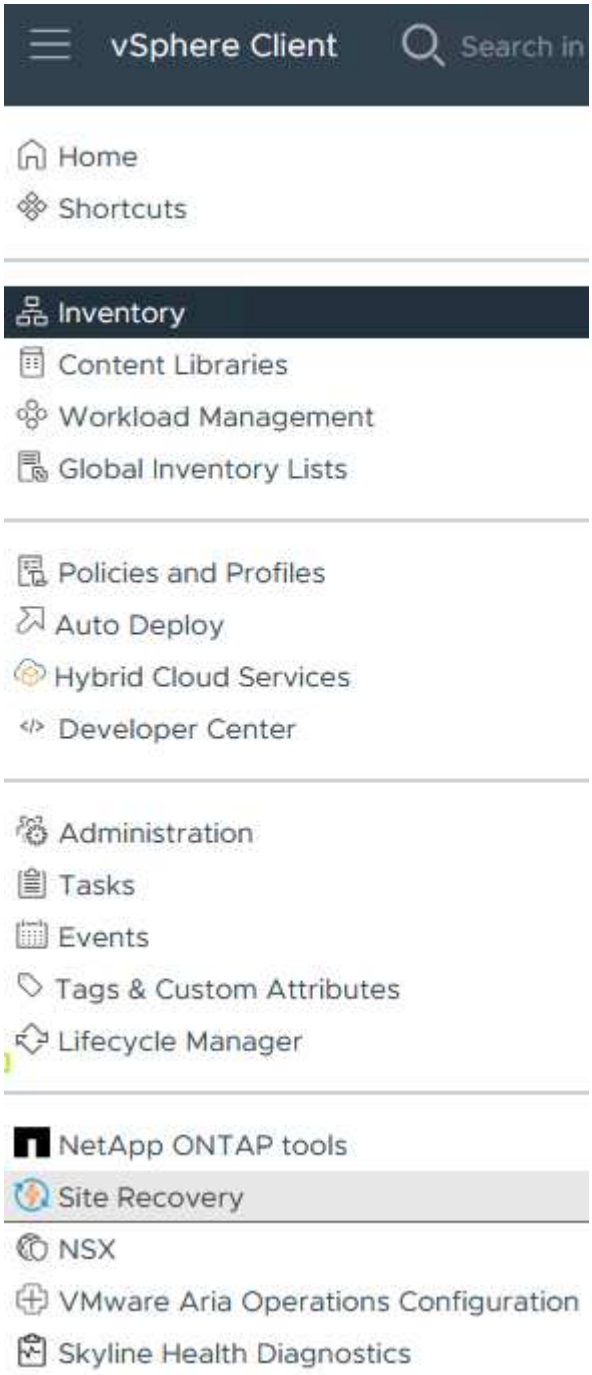
Configure Site Recovery for SRM

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

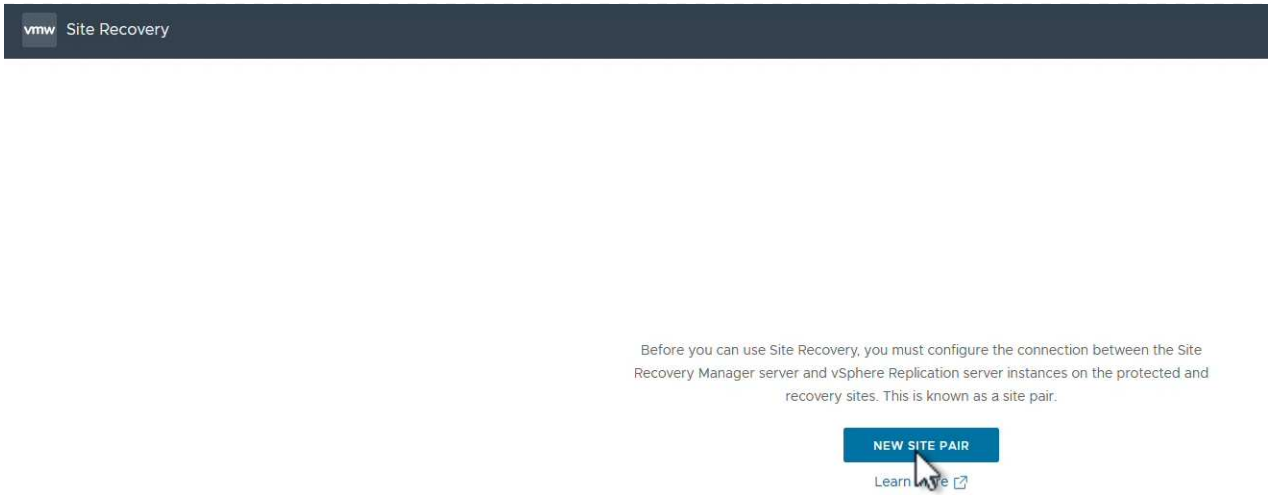
Configure Site Pairing for SRM

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

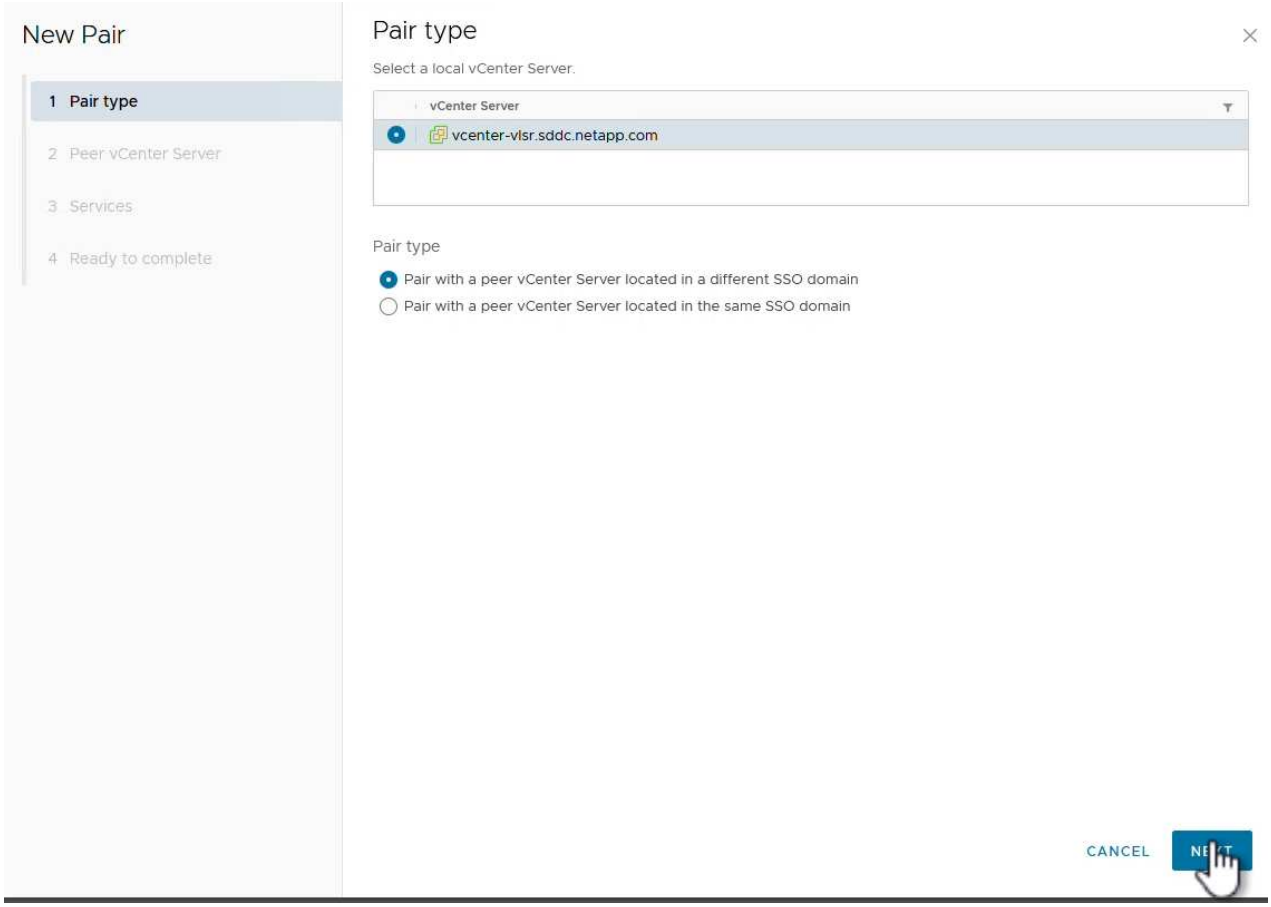
1. In the vSphere client click on **Site Recovery** in the left hand menu. A new browser windows opens to the SRM management UI on the primary site.



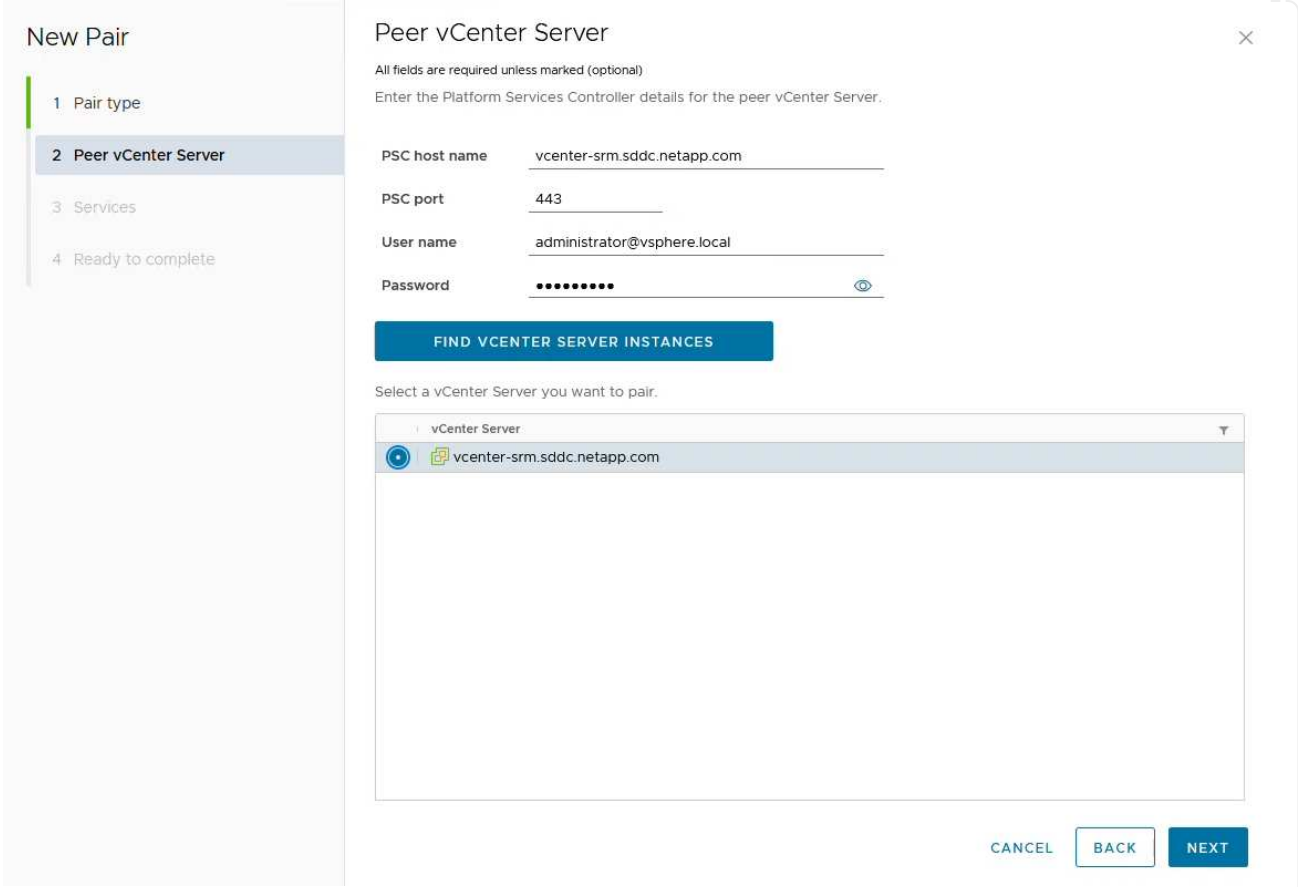
2. On the **Site Recovery** page, click on **NEW SITE PAIR**.



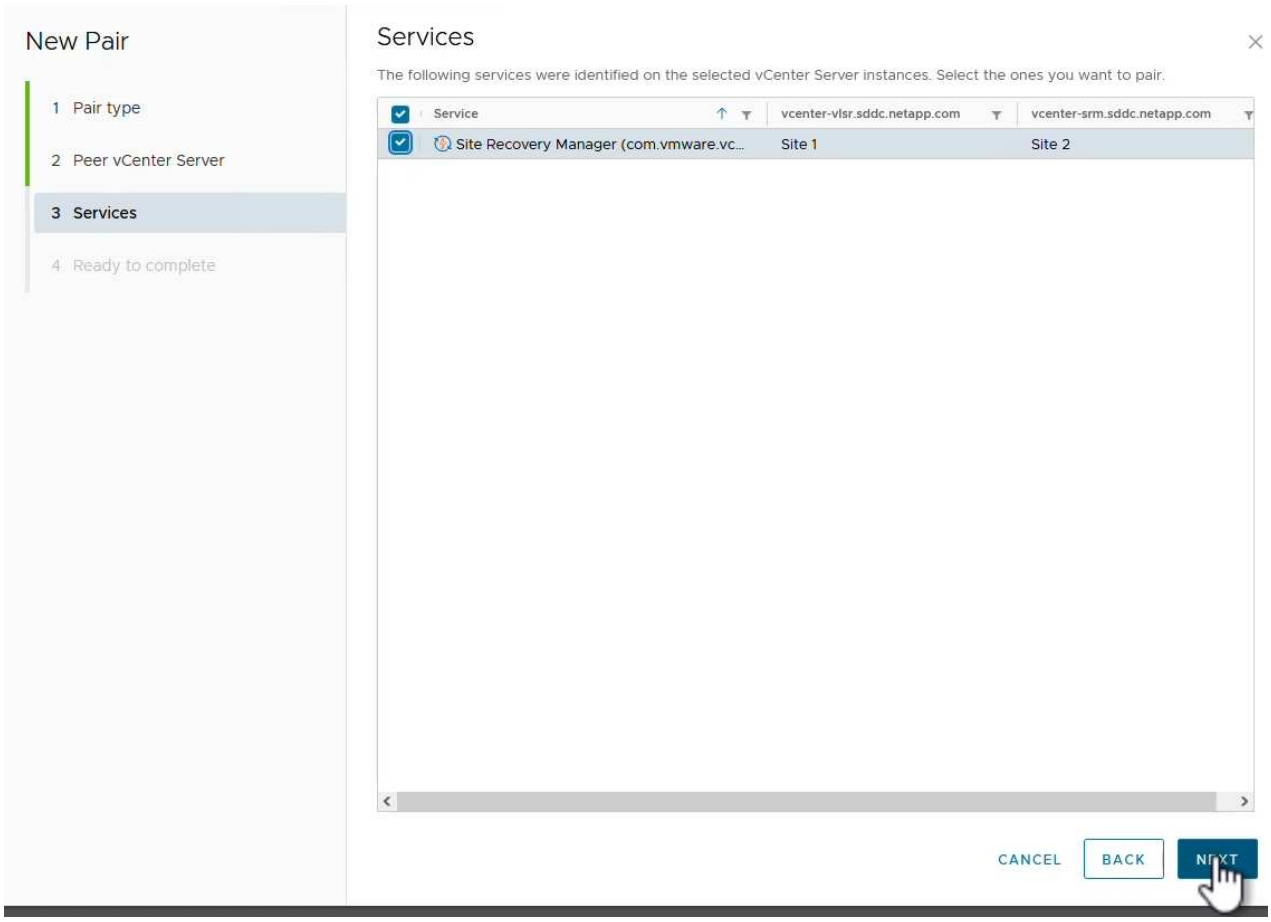
3. On the **Pair type** page of the **New Pair wizard**, verify that the local vCenter server is selected and select the **Pair type**. Click on **Next** to continue.



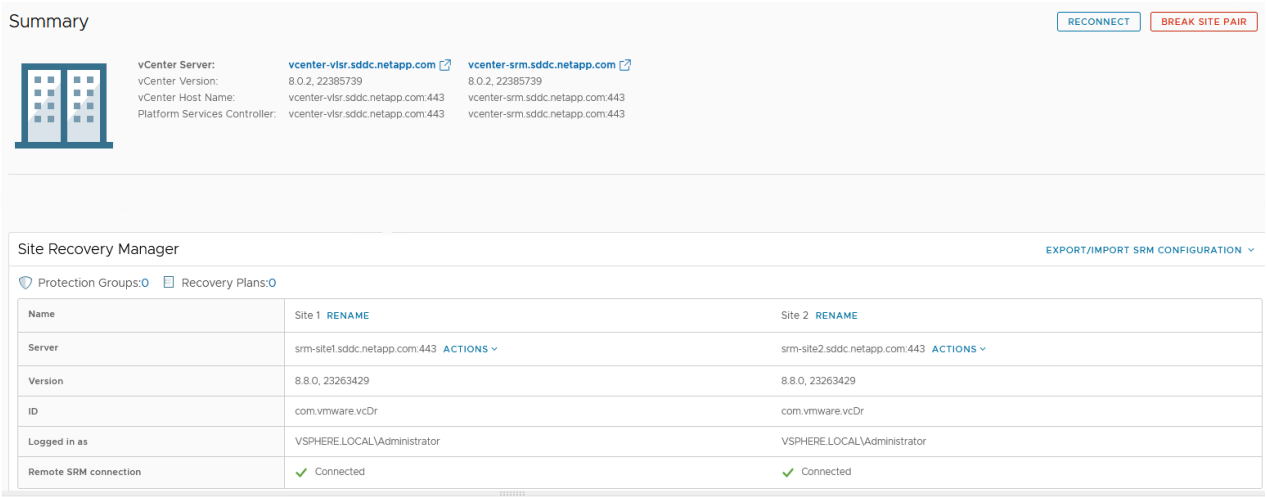
4. On the **Peer vCenter** page fill out the credentials of the vCenter at the secondary site and click on **Find vCenter Instances**. Verify the the vCenter instance has been discovered and click on **Next** to continue.



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



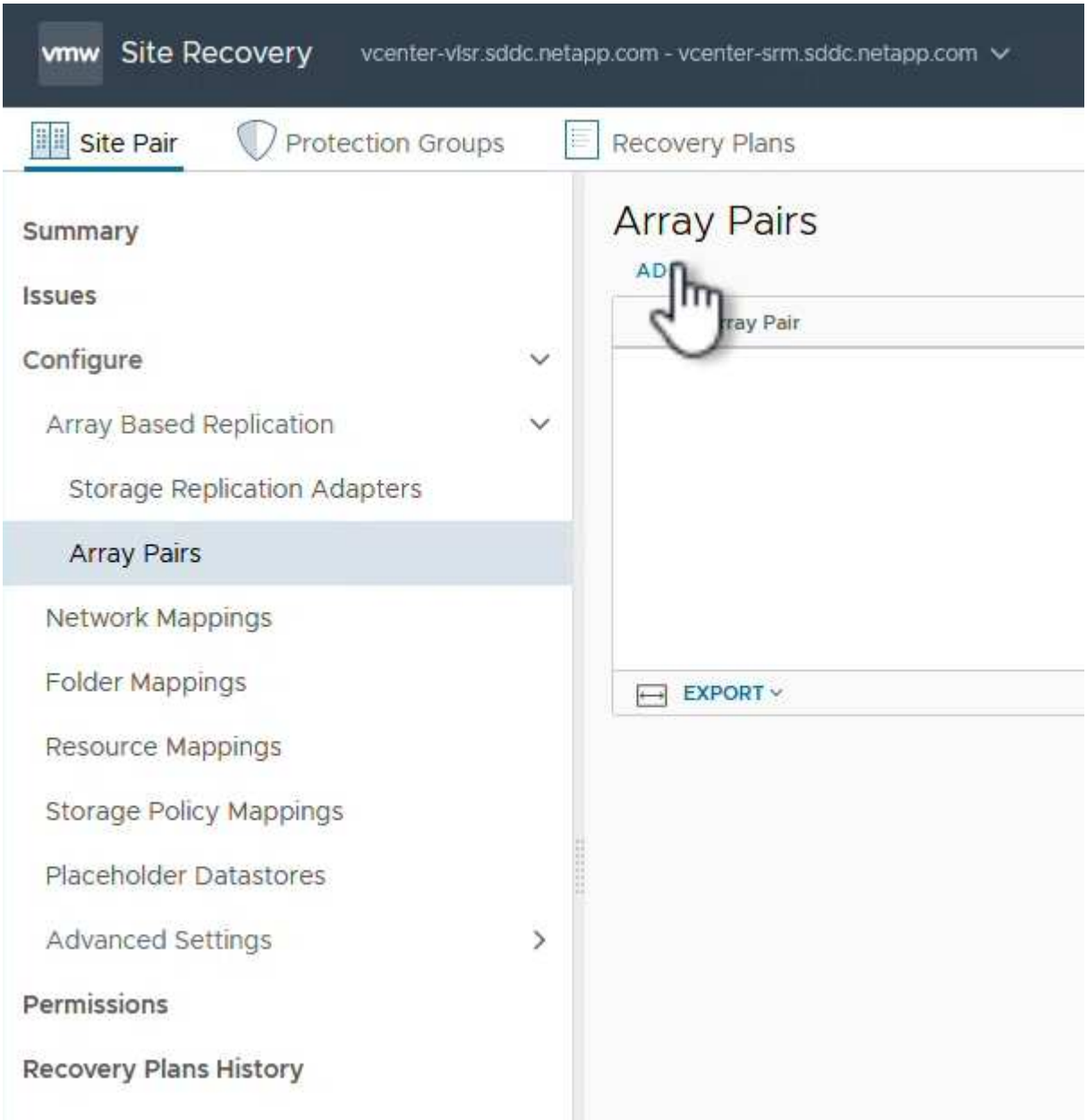
6. On the **Ready to complete** page, review the proposed configuration and then click on the **Finish** button to create the Site Pairing
7. The new Site Pair and its summary can be viewed on the Summary page.



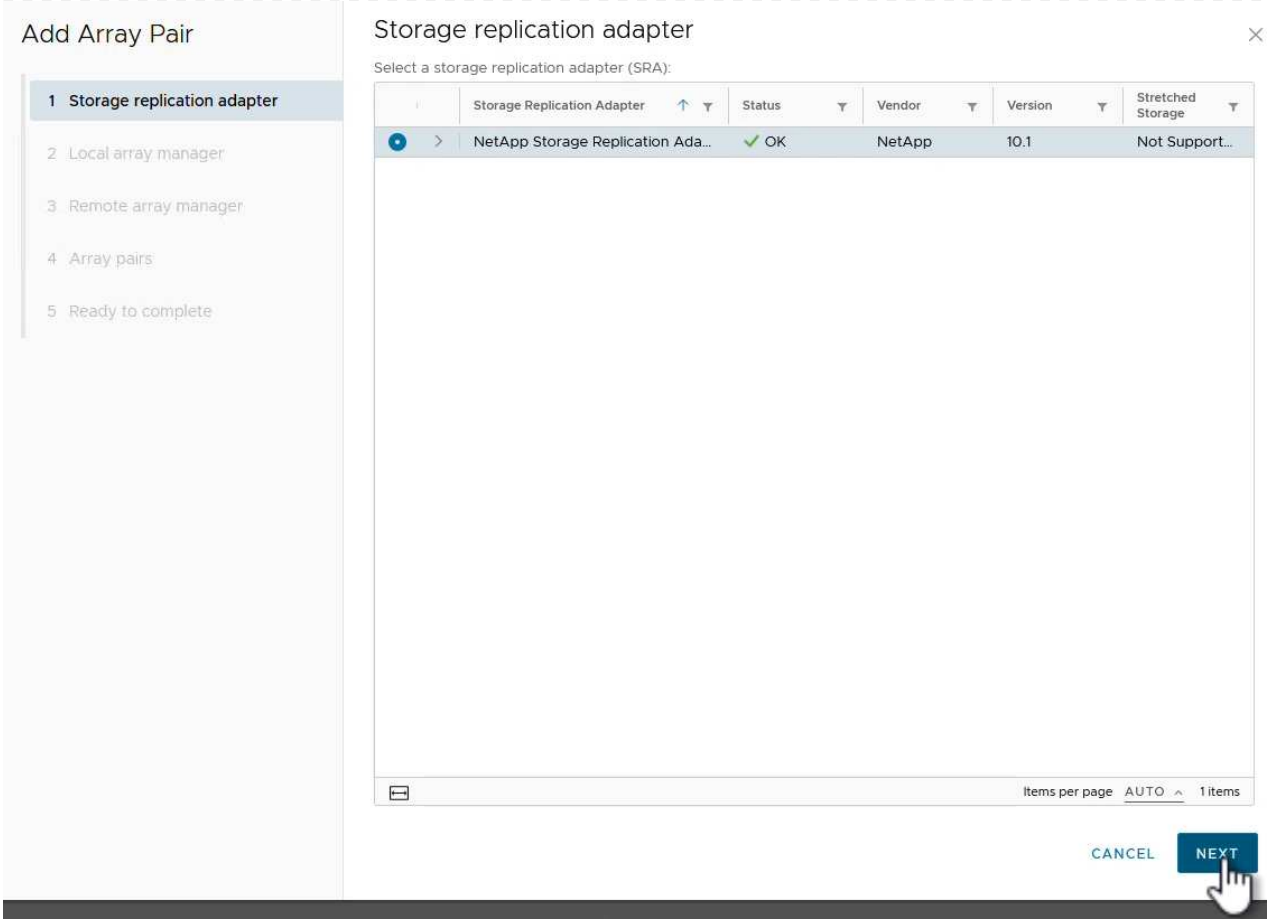
Add an Array Pair for SRM

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

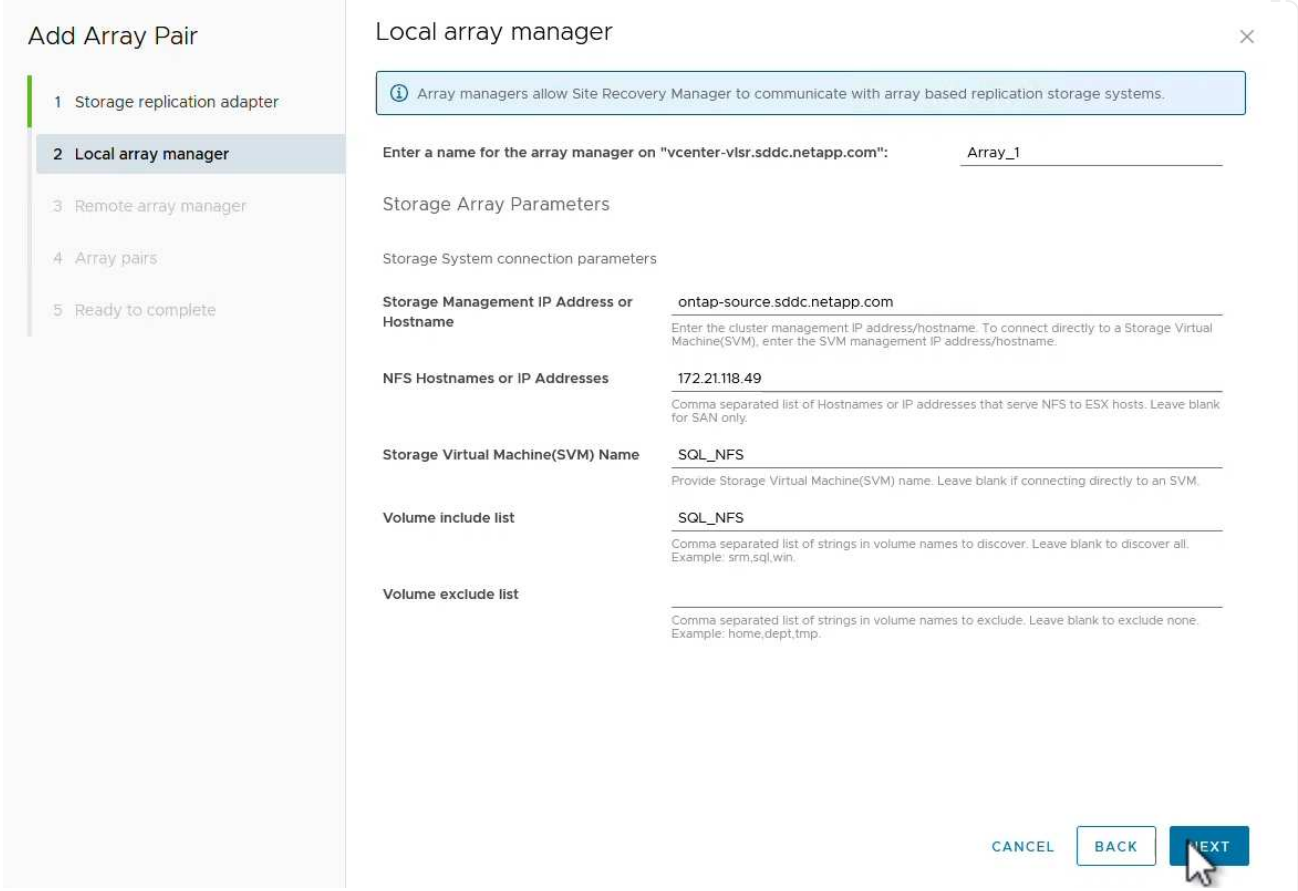
1. In the Site Recovery interface navigate to **Configure > Array Based Replication > Array Pairs** in the left hand menu. Click on **ADD** to get started.



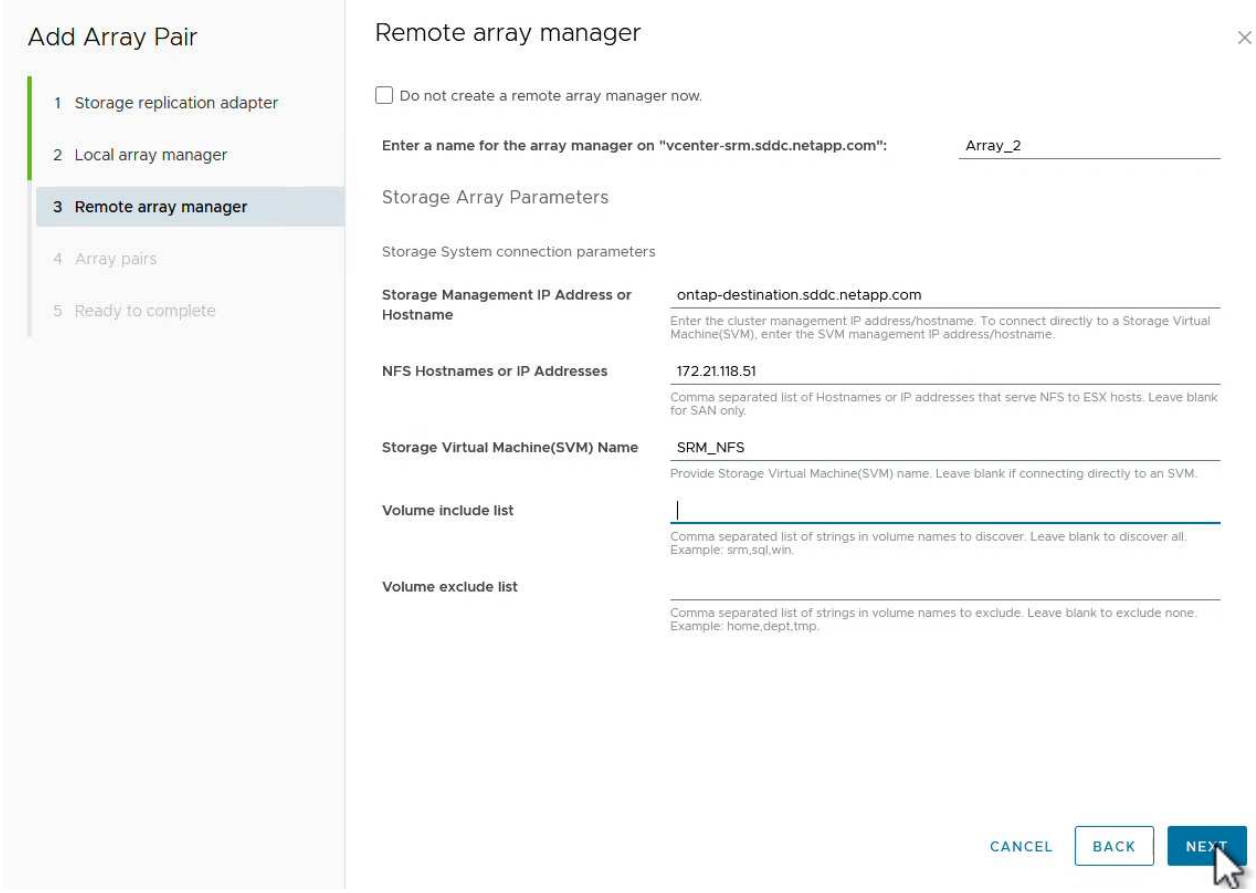
2. On the **Storage replication adapter** page of the **Add Array Pair** wizard, verify the SRA adapter is present for the primary site and click on **Next** to continue.



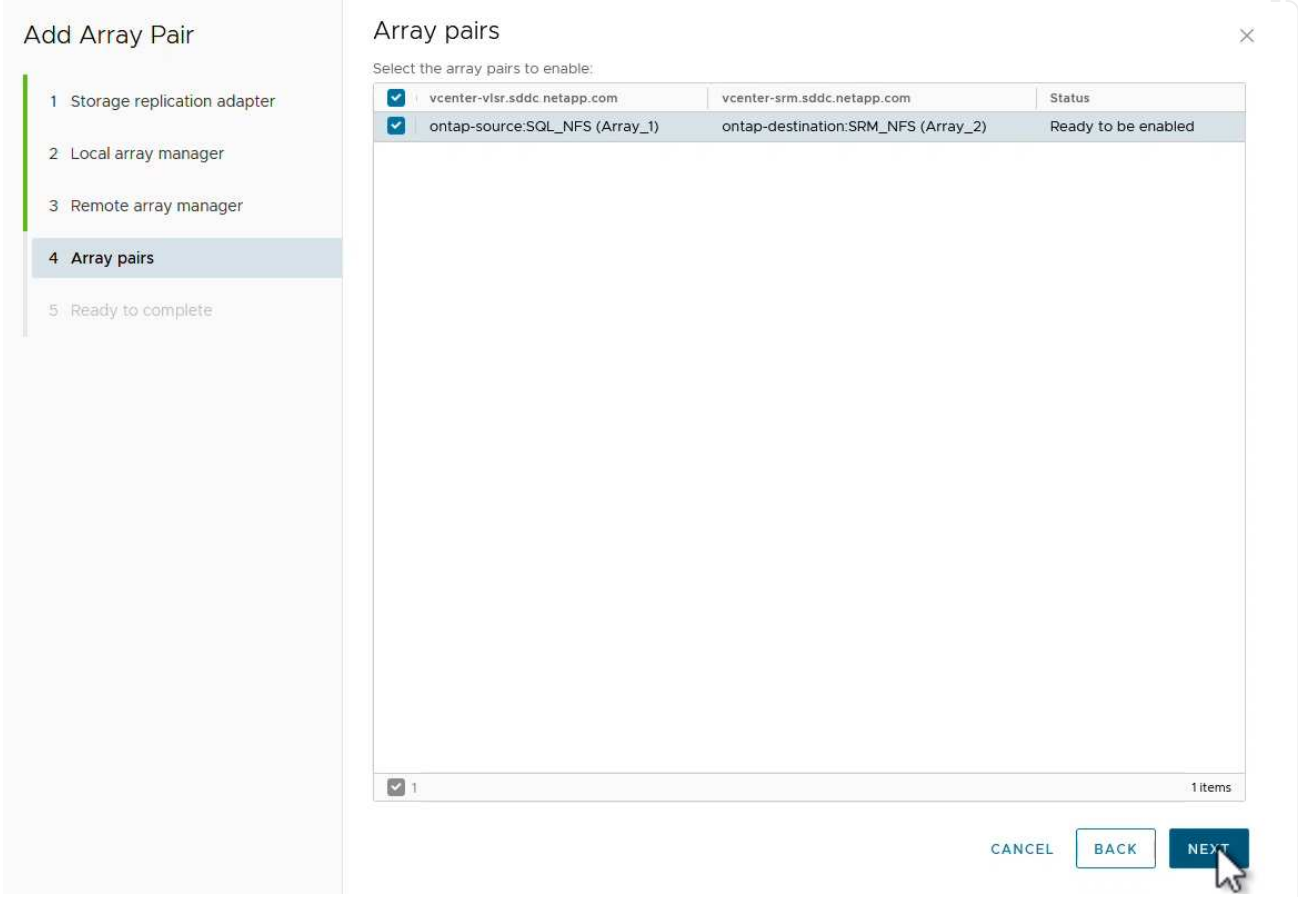
3. On the **Local array manager** page, enter a name for the array at the primary site, the FQDN of the storage system, the SVM IP addresses serving NFS, and optionally, the names of specific volumes to be discovered. Click on **Next** to continue.



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



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

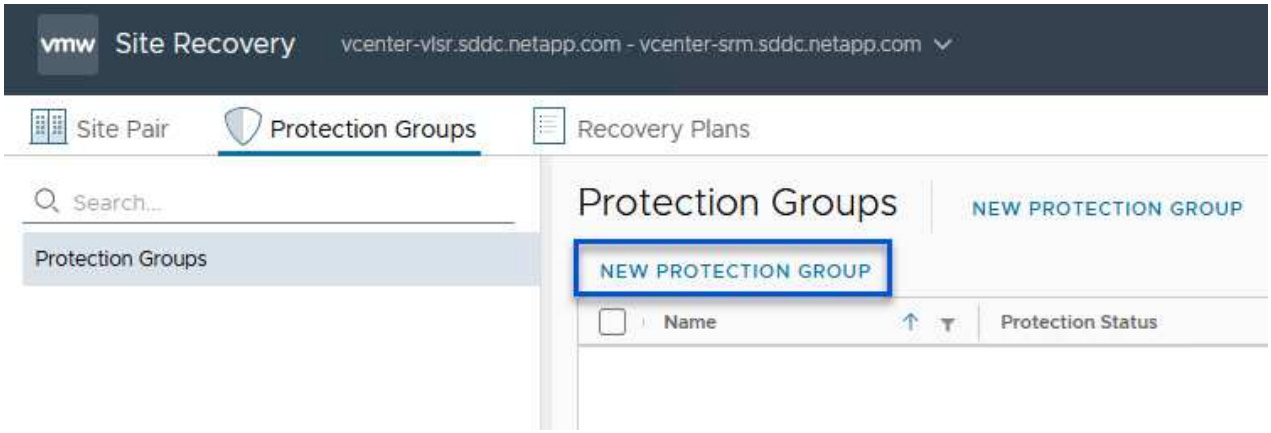


6. Review the information on the **Ready to complete** page and click on **Finish** to create the array pair.

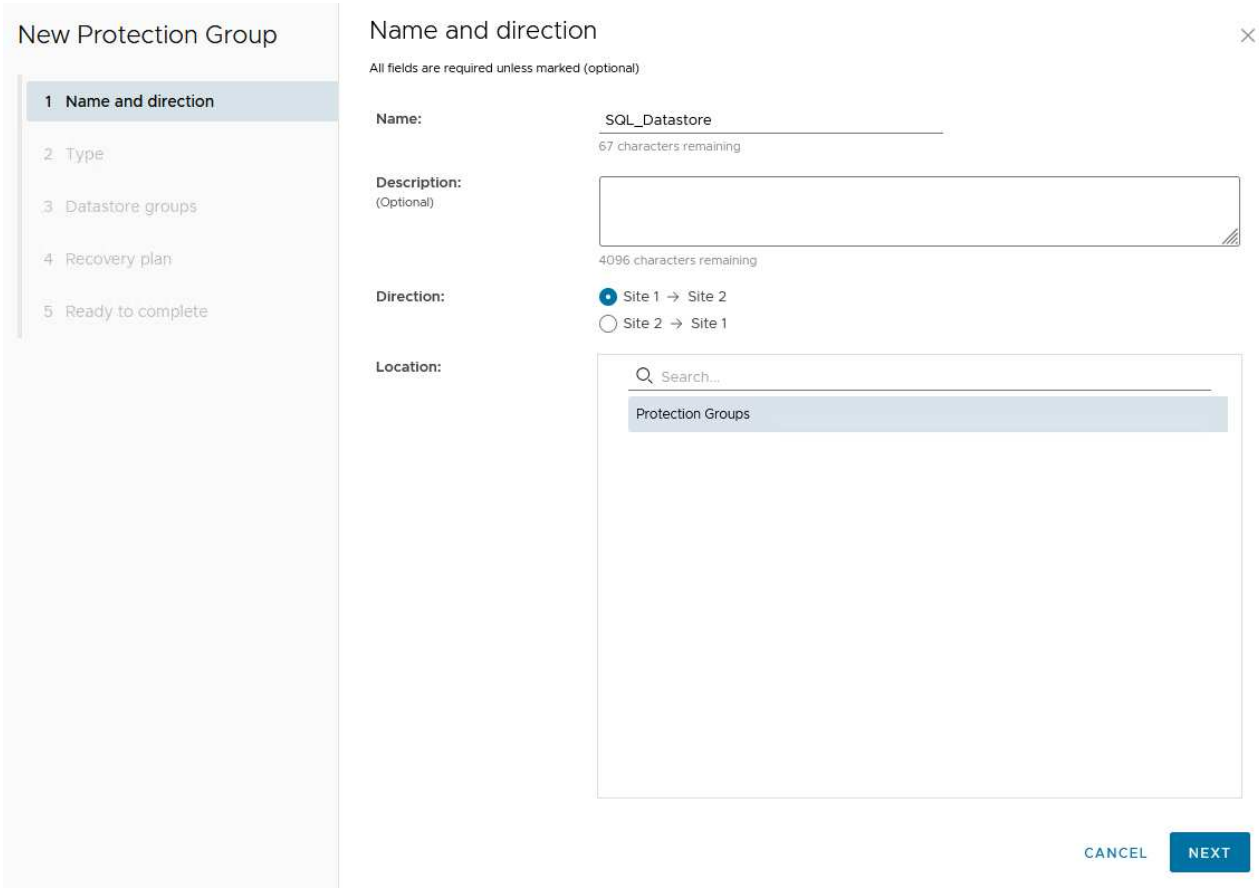
Configure Protection Groups for SRM

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

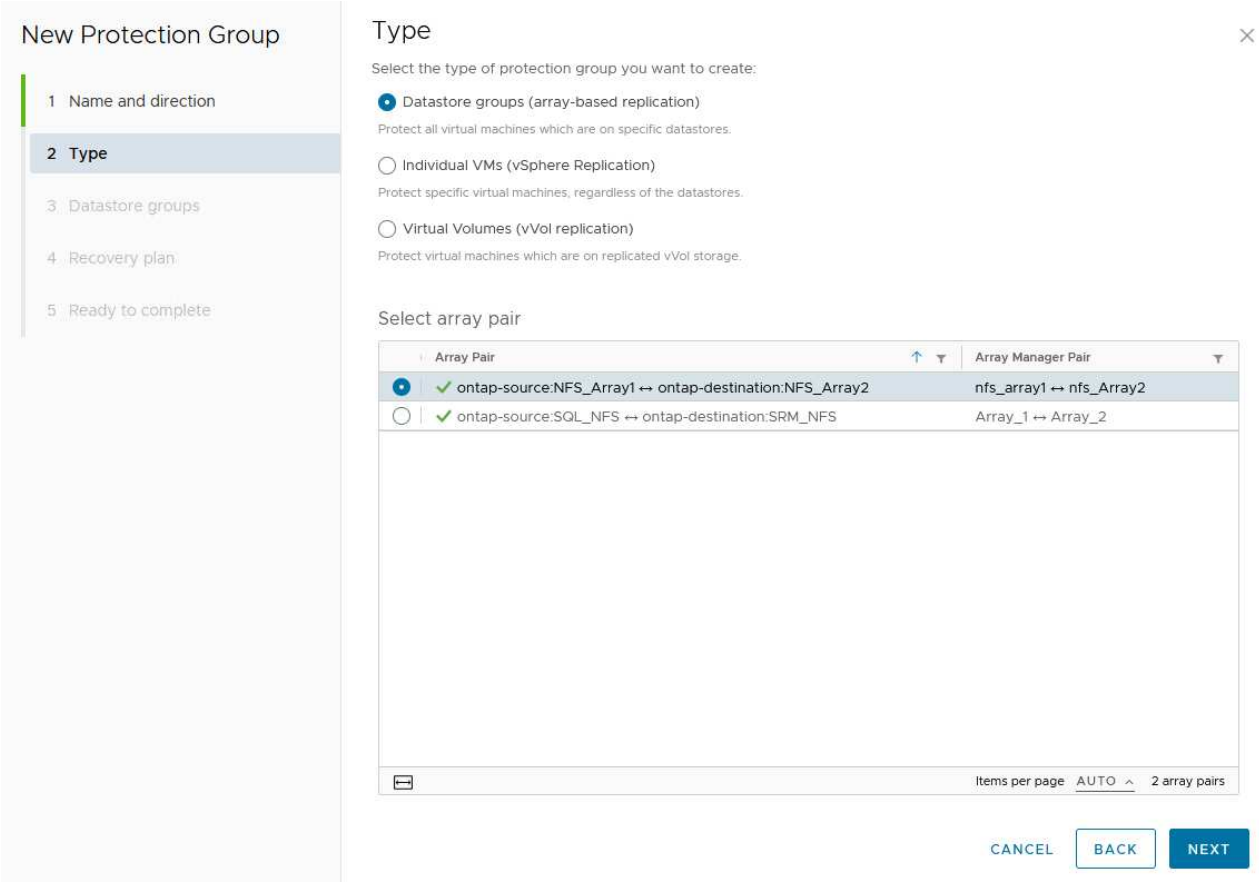
1. In the Site Recovery interface click on the **Protection Groups** tab and then on **New Protection Group** to get started.



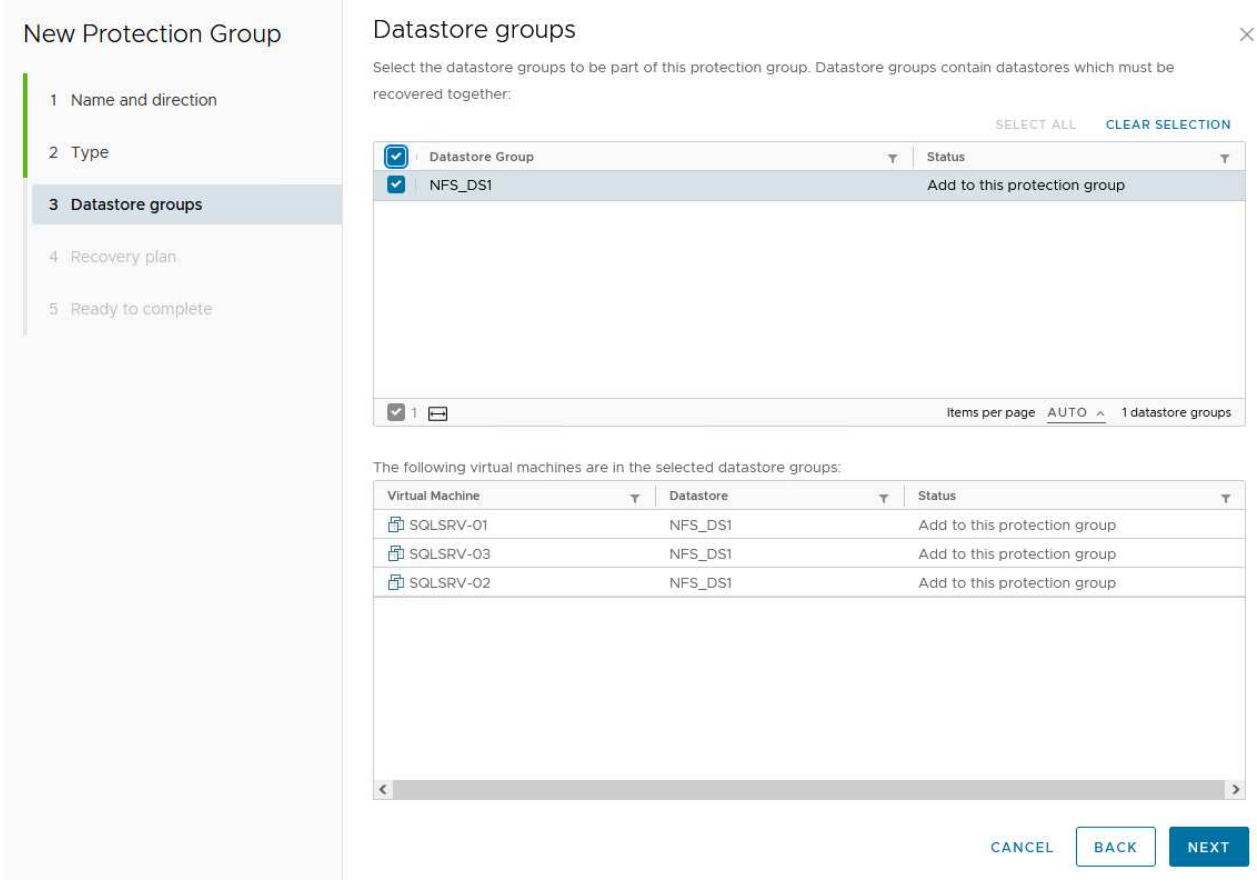
2. On the **Name and direction** page of the **New Protection Group** wizard, provide a name for the group and choose the site direction for protection of the data.



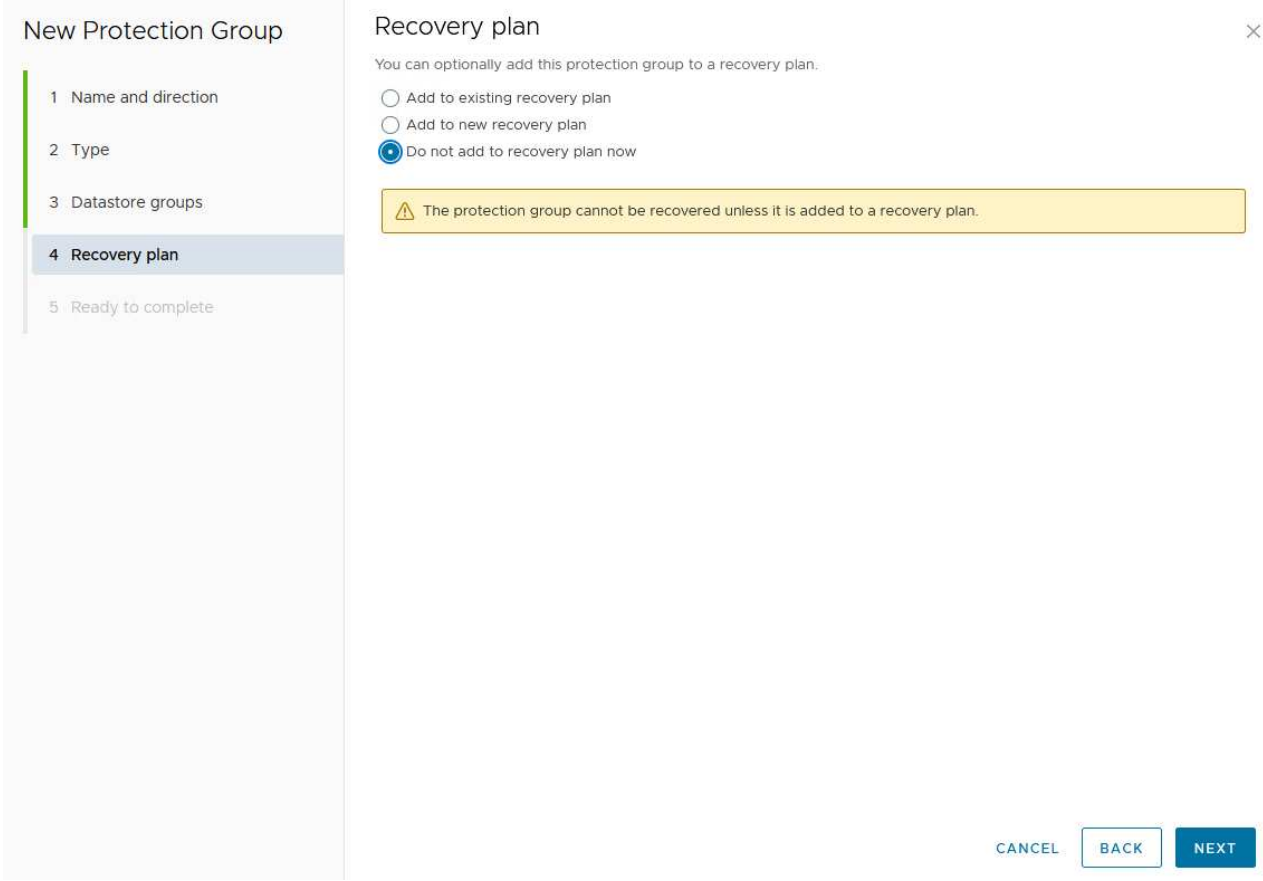
3. On the **Type** page select the protection group type (datastore, VM, or vVol) and select the array pair. Click on **Next** to continue.



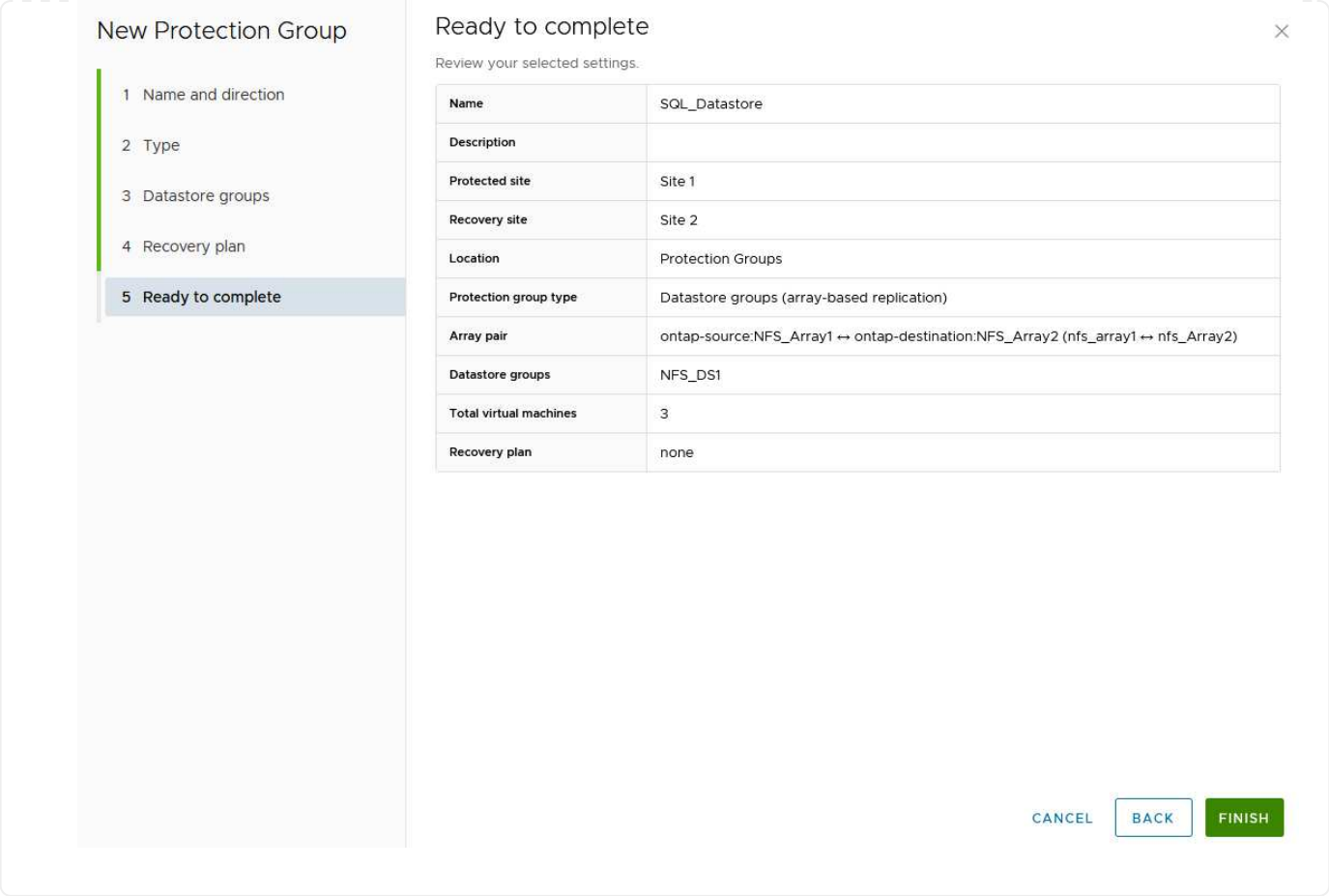
4. On the **Datastore groups** page, select the datastores to include in the protection group. VMs currently residing on the datastore are displayed for each datastore selected. Click on **Next** to continue.



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.



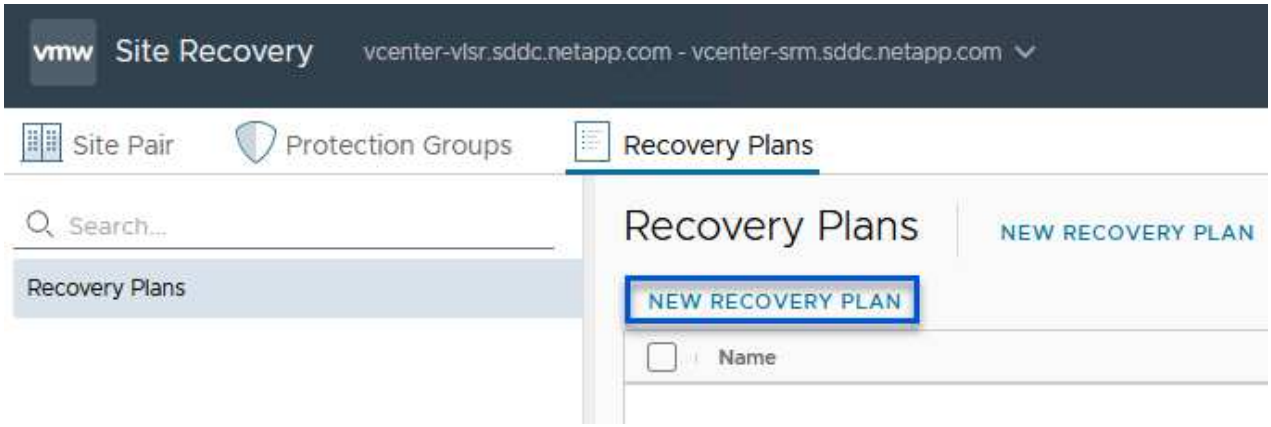
6. On the **Ready to complete** page, review the new protection group parameters and click on **Finish** to create the group.


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

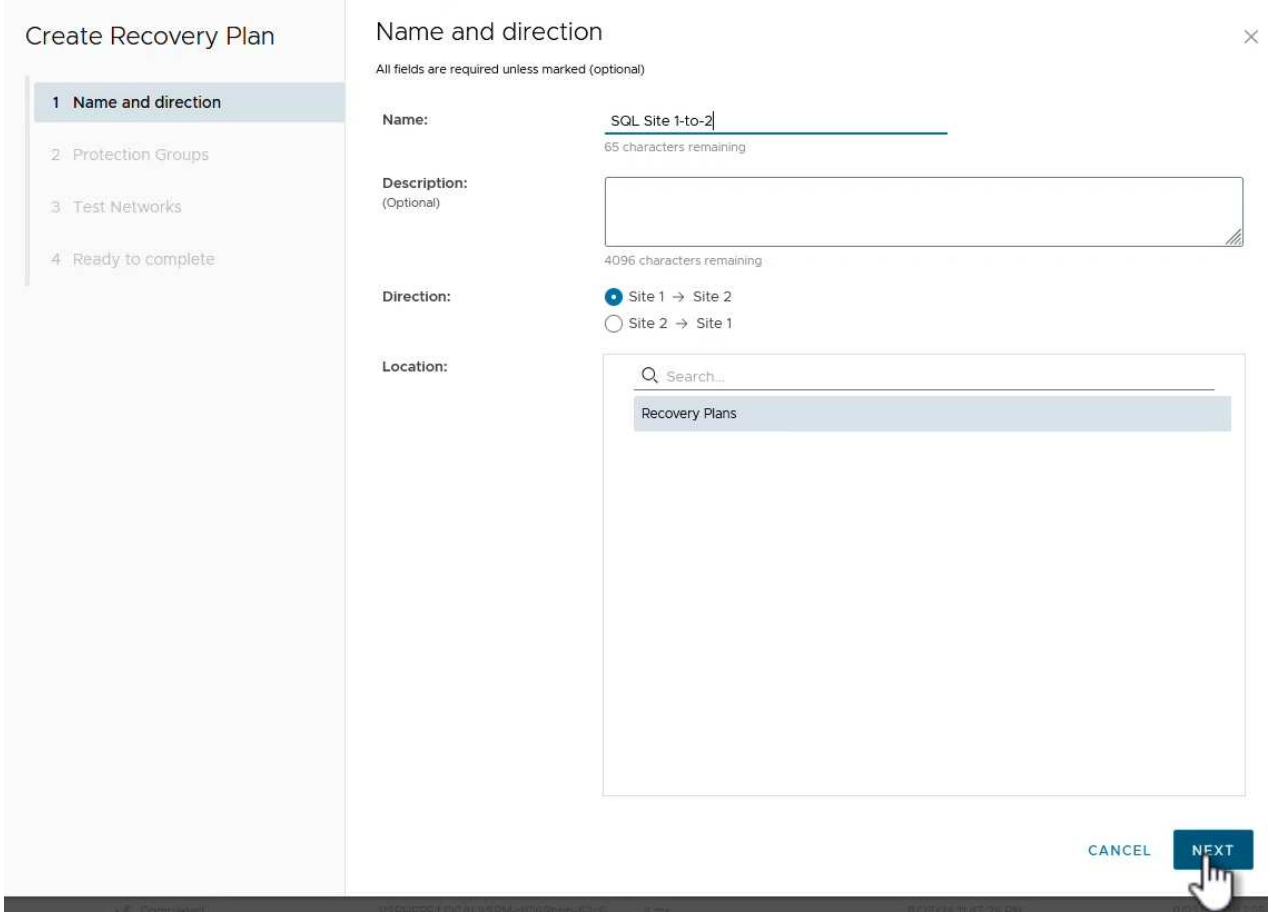
Configure Recovery Plan for SRM

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

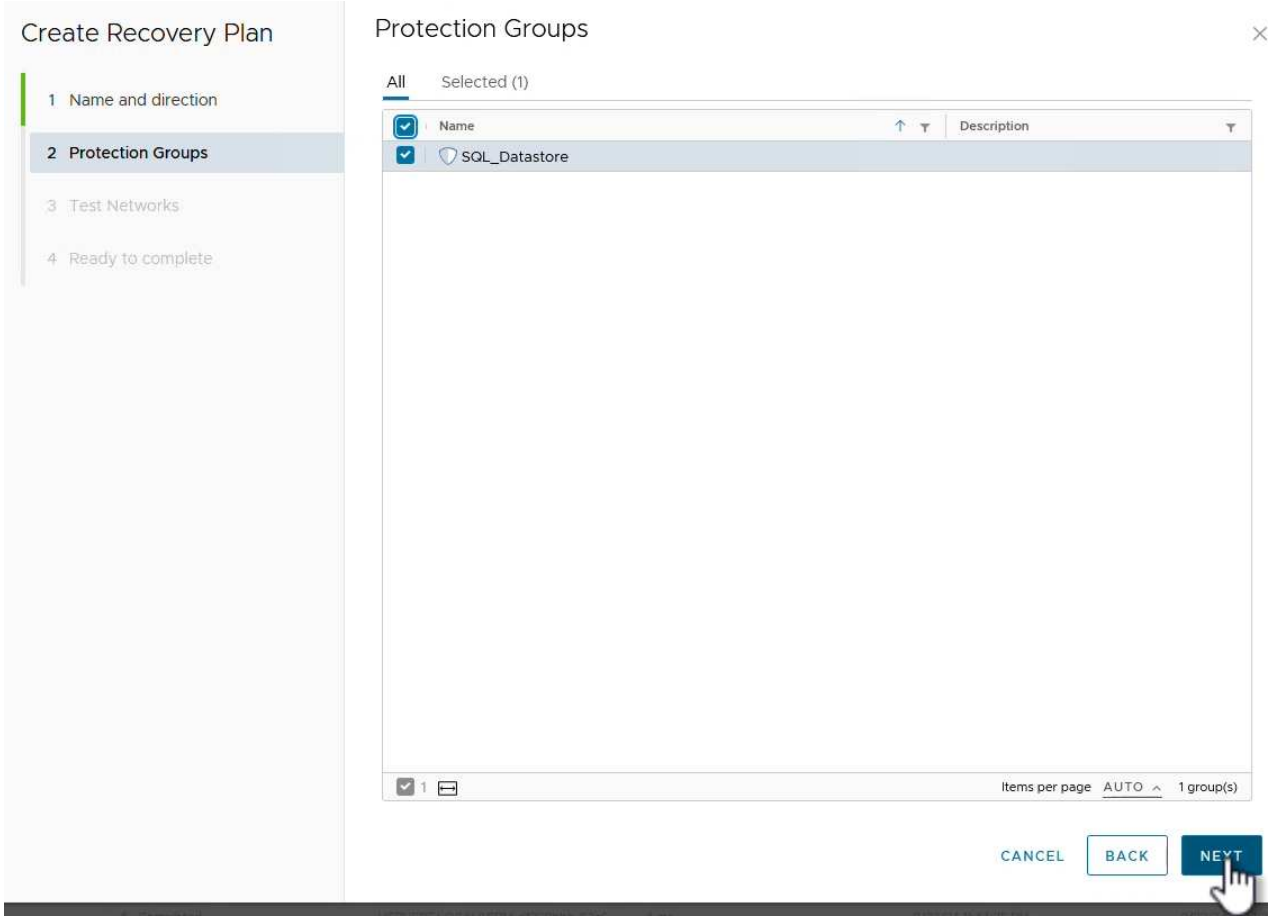
1. In the Site Recovery interface click on the **Recovery plan** tab and then on **New Recovery Plan** to get started.



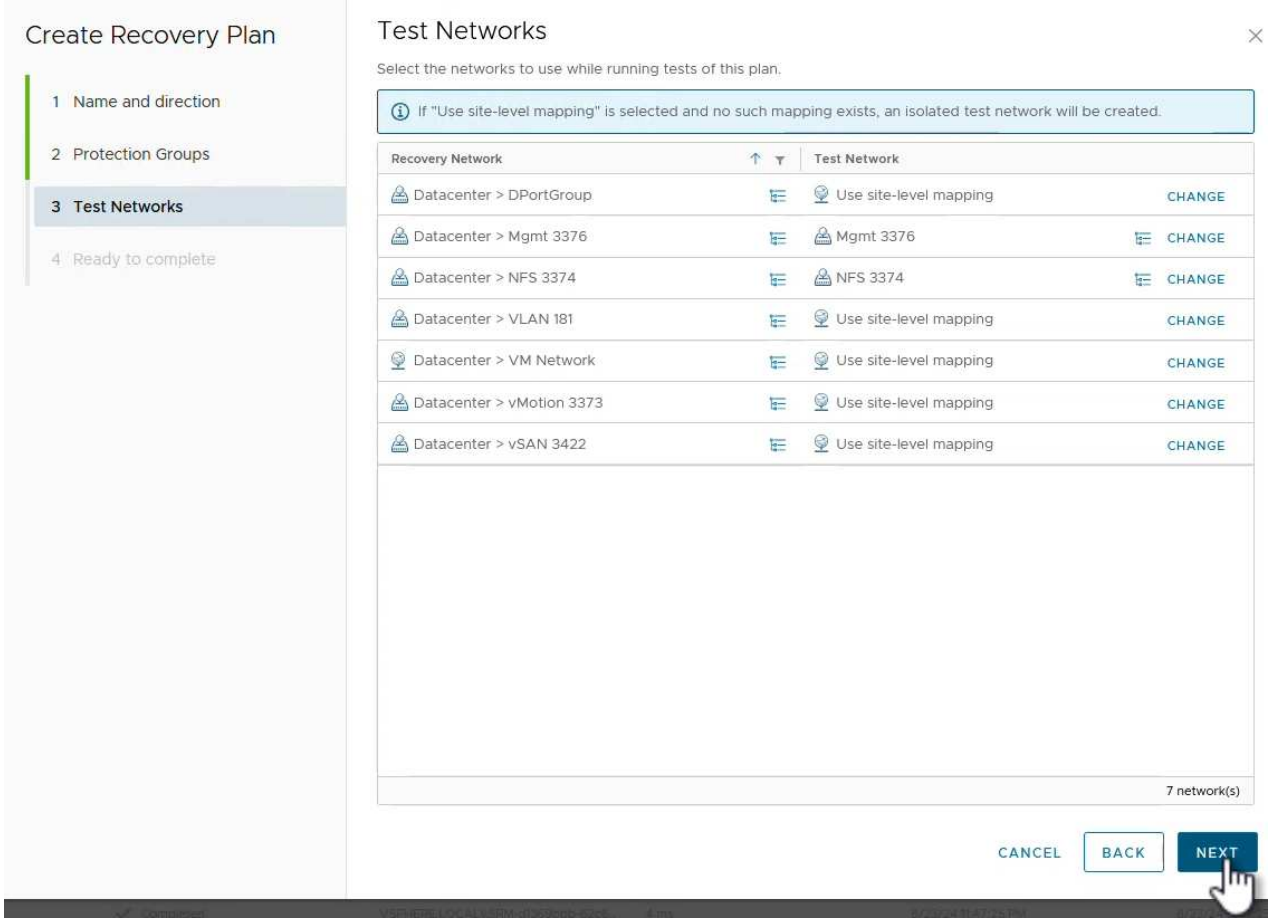
2. On the **Name and direction** page of the **Create Recovery Plan** wizard, provide a name for the recovery plan and choose the direction between source and destination sites. Click on **Next** to continue.



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



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.



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

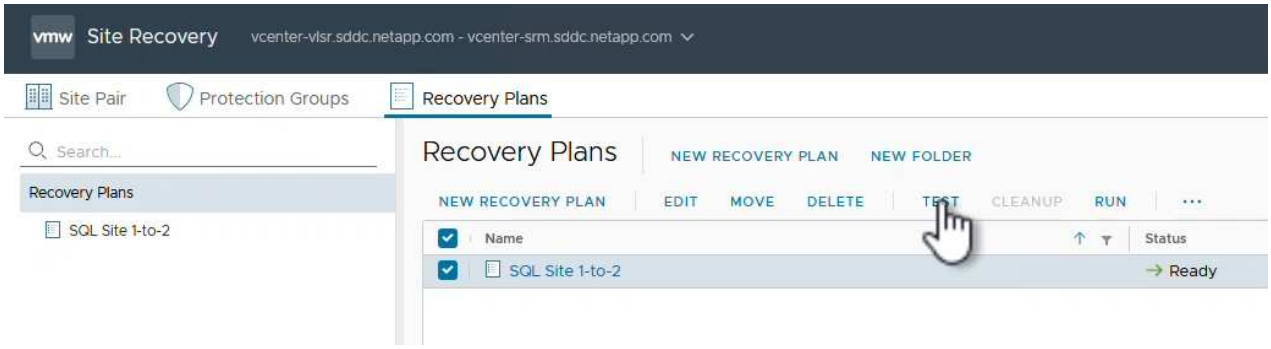
In this section various functions of using disaster recovery with SRM will be covered including, testing failover, performing failover, performing reprotection and failback.

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

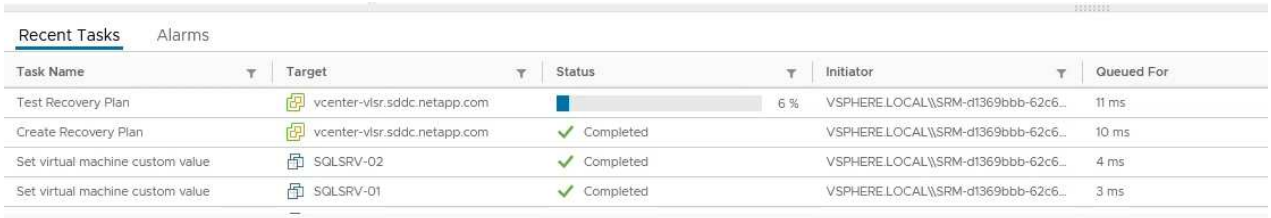
Testing failover with SRM

The following step is completed in the Site Recovery interface.

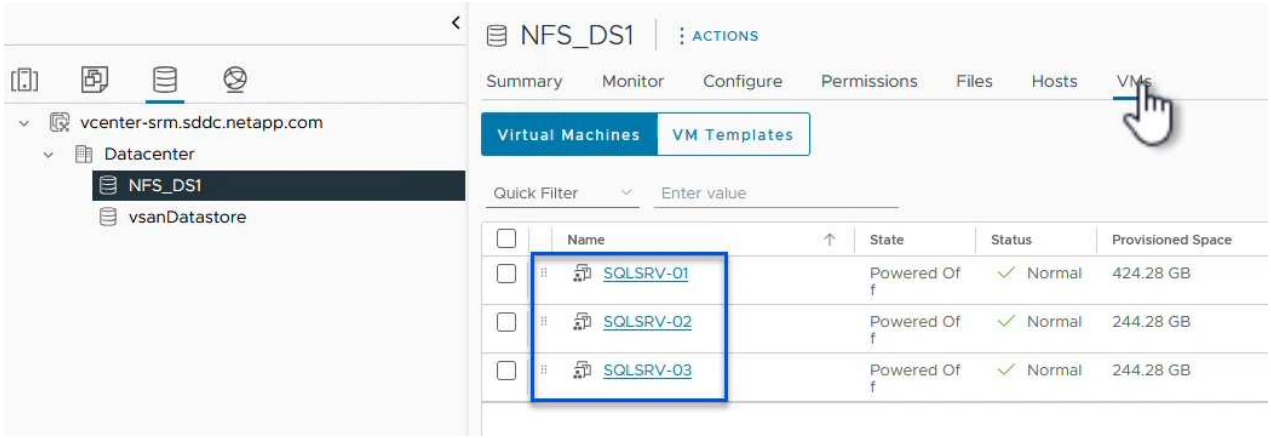
1. In the Site Recovery interface click on the **Recovery plan** tab and then select a recovery plan. Click on the **Test** button to begin testing failover to the secondary site.



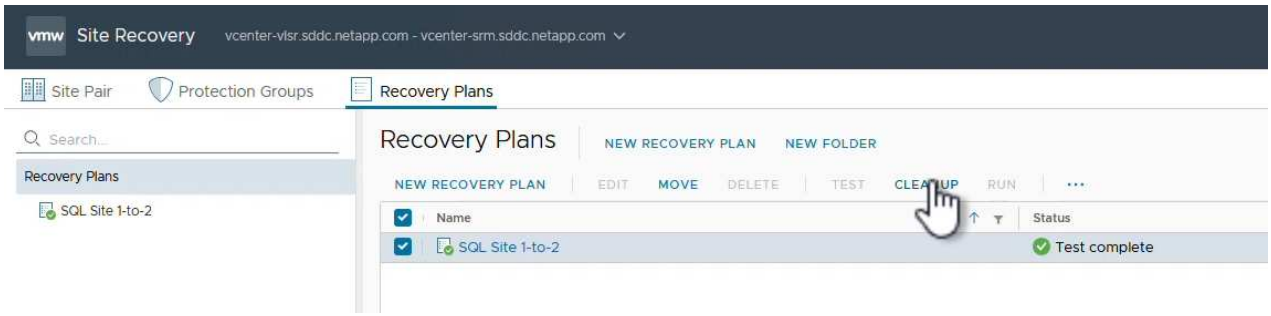
2. You can view the progress of the test from the Site Recovery task pane as well the vCenter task pane.



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.



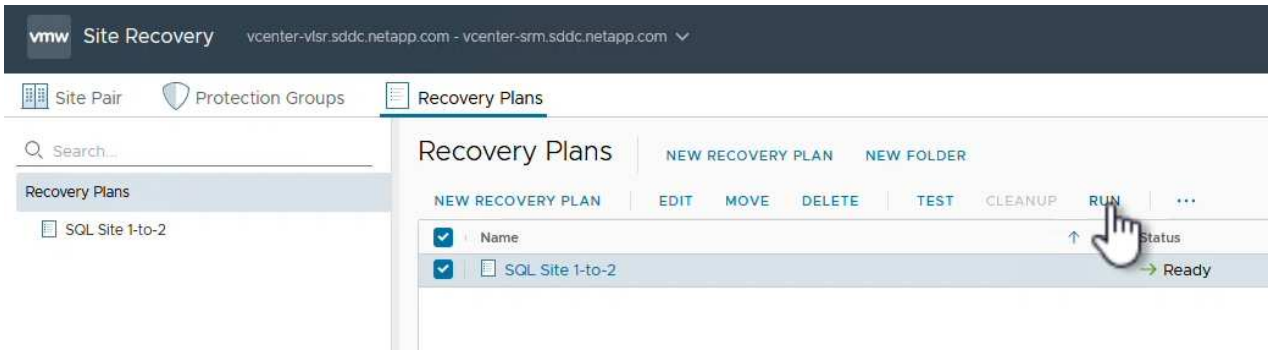
4. Once the test has completed, click on **Cleanup** to unmount the datastore and revert back to the original environment.



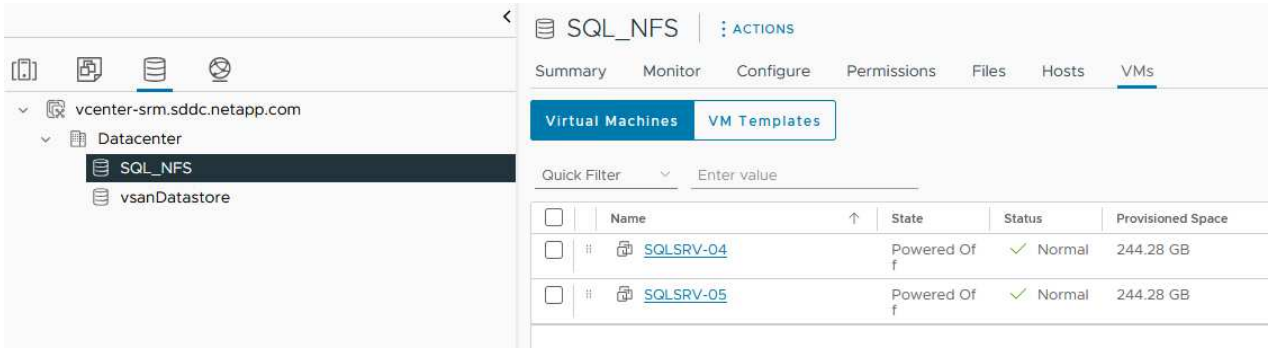
Run Recovery Plan with SRM

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 reprotection process and before executing the final failback. This practice serves as a verification step, confirming that the systems at the original site are fully capable of handling the operation. By following this approach, you can minimize risks and ensure a more reliable transition back to the original production environment.

Additional information

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

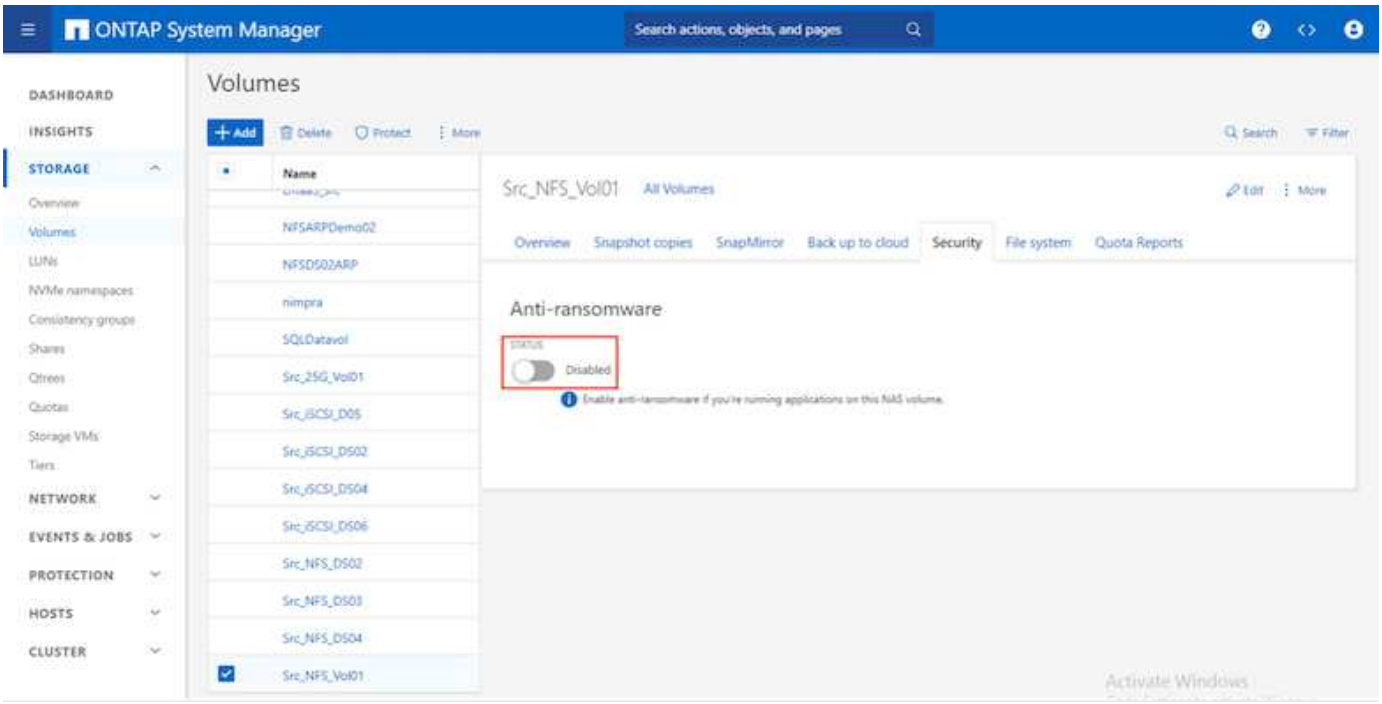
For information on configuring ONTAP storage systems refer to the ONTAP 9 Documentation center.

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

Autonomous Ransomware Protection for NFS Storage

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

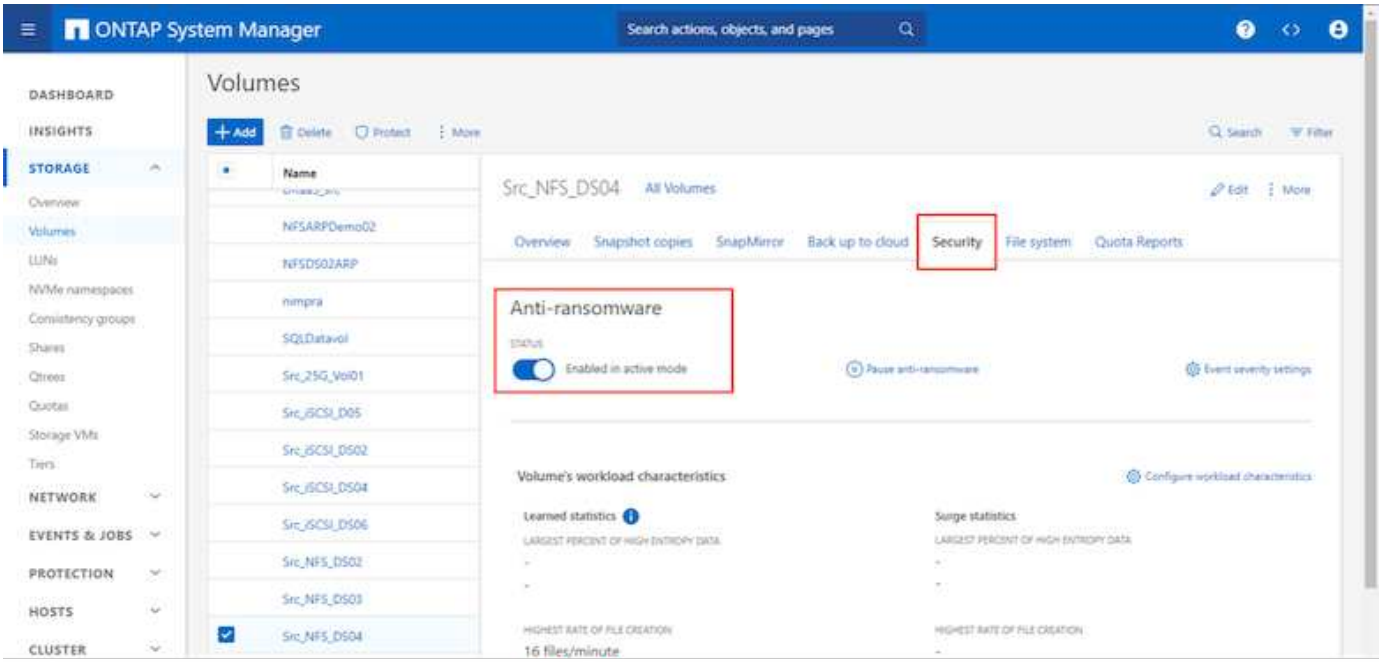
Let's look at how the above-mentioned capabilities work with VMware to protect and recover the data against ransomware. To protect vSphere and guest VMs against attacks, it is essential to take several measures including segmenting, utilizing EDR/XDR/SIEM for endpoints and installing security updates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



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.

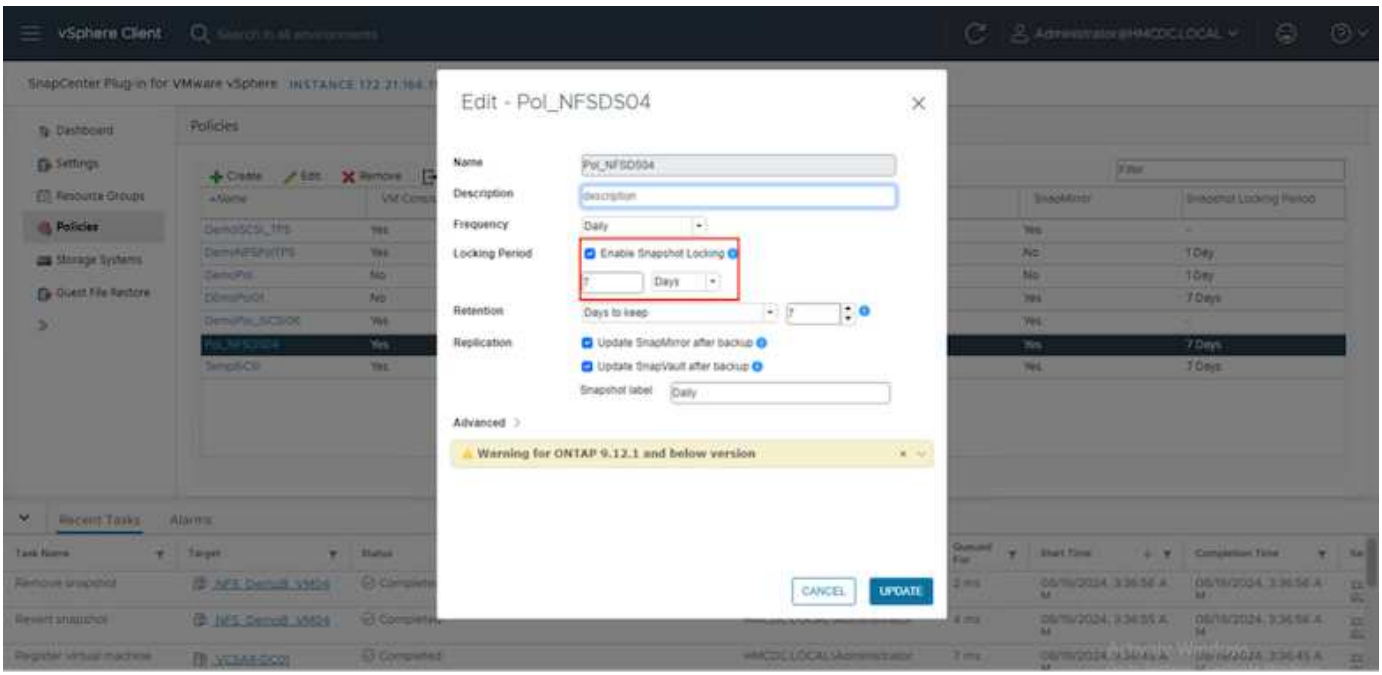
Once in active mode, it starts looking for the abnormal volume activity that might potentially be ransomware. If abnormal activity is detected, an automatic Snapshot copy is immediately taken, which provides a restoration point as close as possible to the file infection. ARP can detect changes in VM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



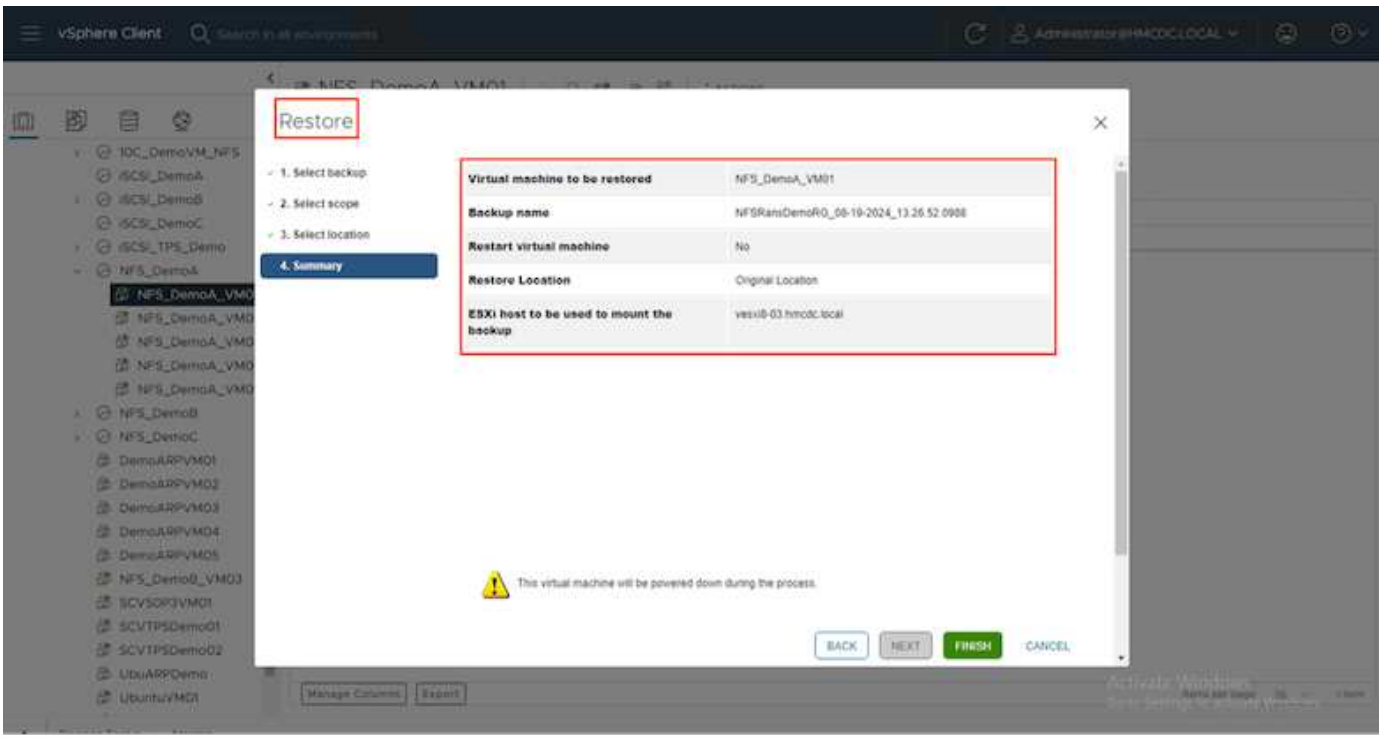
If a ransomware attack targets the virtual machine (VM) and alter files within the VM without making changes outside the VM, the Advanced Ransomware Protection (ARP) will still detect the threat if the default entropy of the VM is low, for example, for file types like .txt, .docx, or .mp4 files. Even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

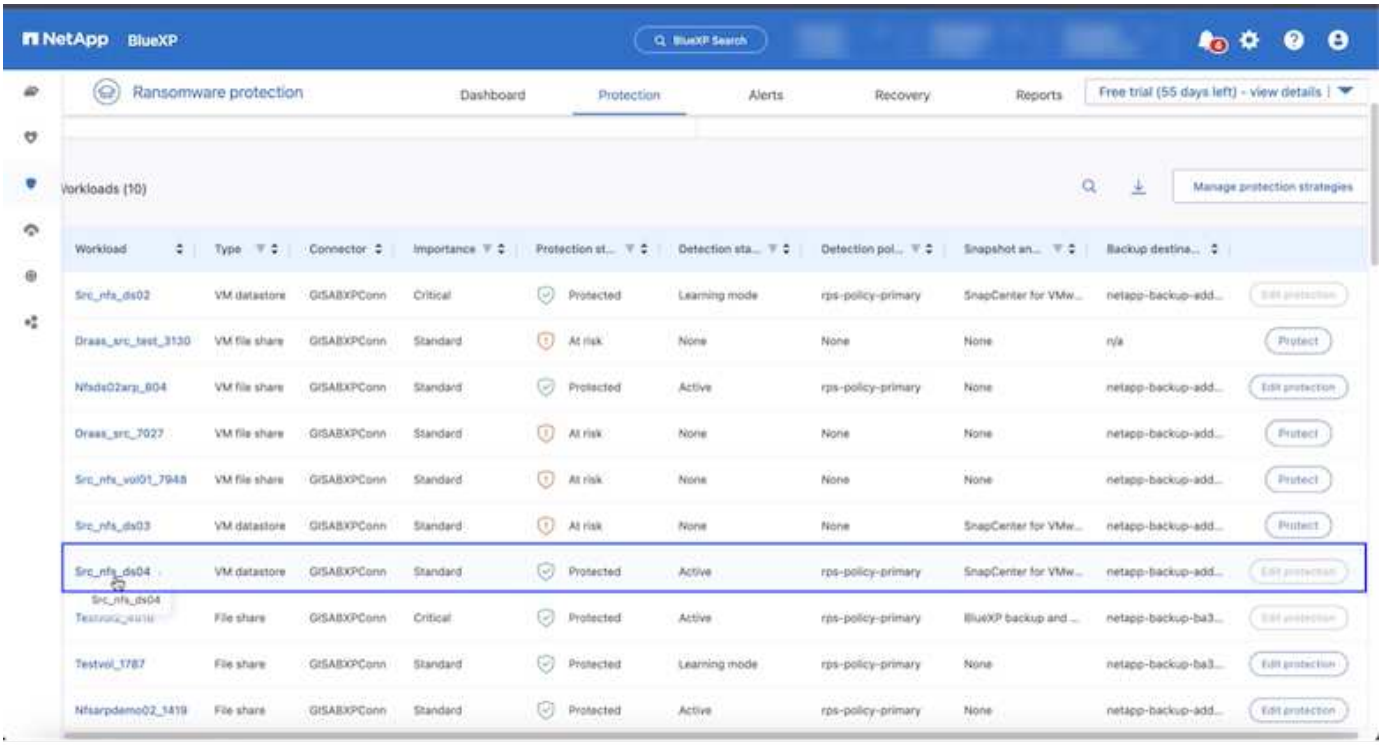


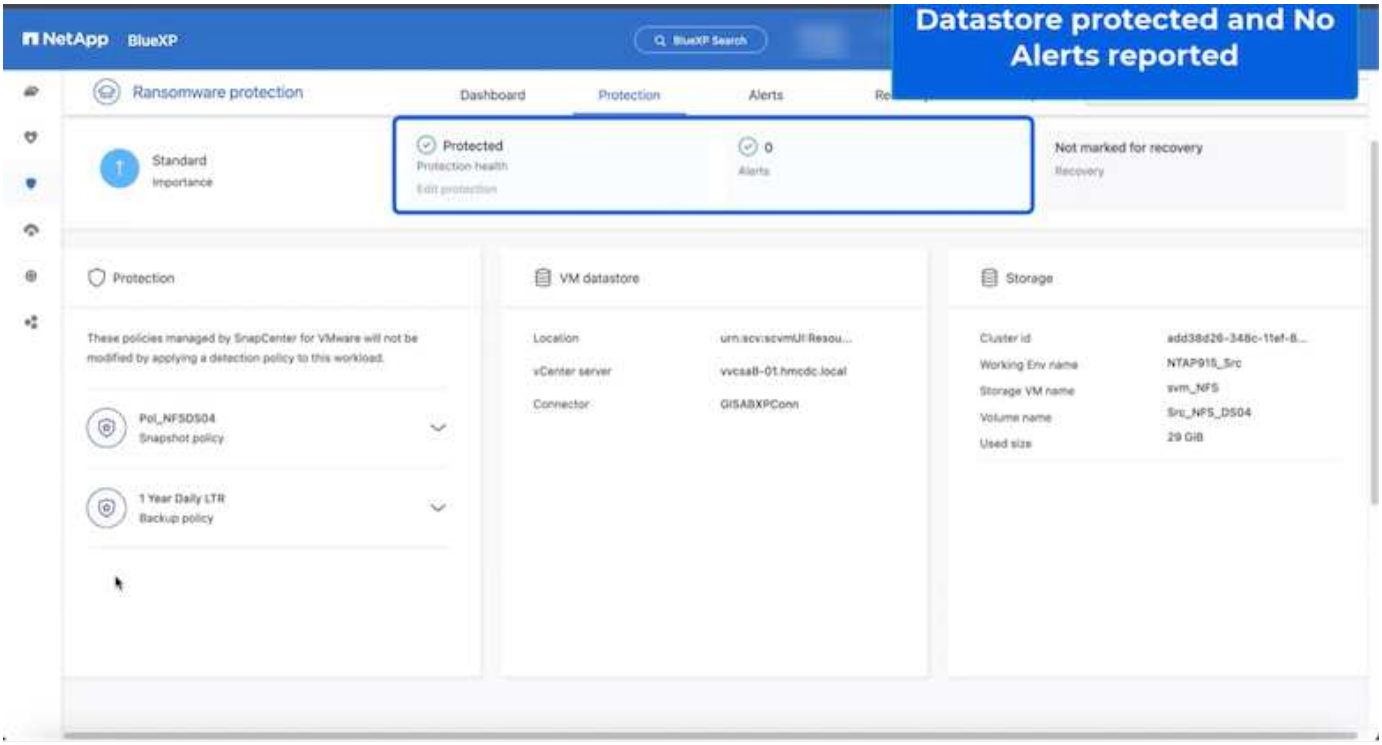
The above demonstrates how ONTAP storage adds an additional layer to the existing techniques, enhancing futureproofing of the environment.

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.

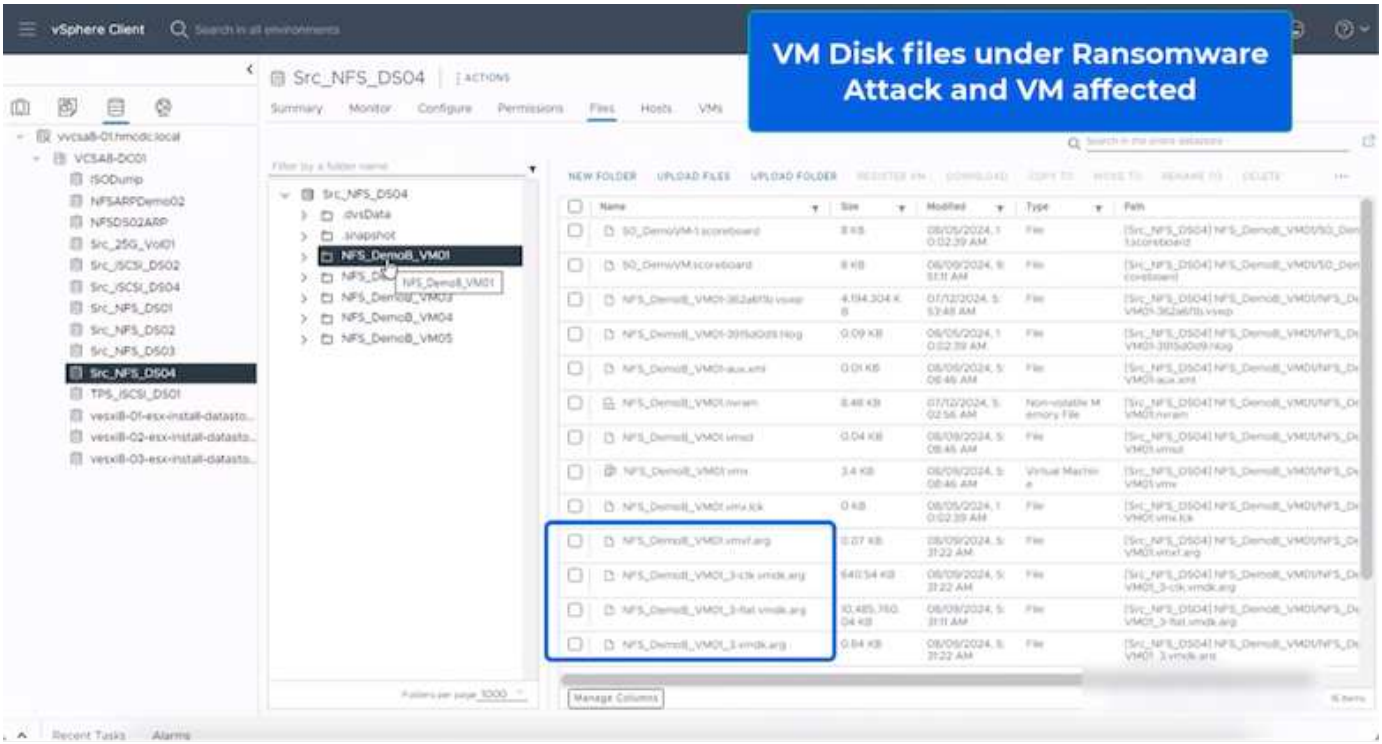
In this example, NFS datastore "Src_NFS_DS04" is protected using BlueXP ransomware protection.



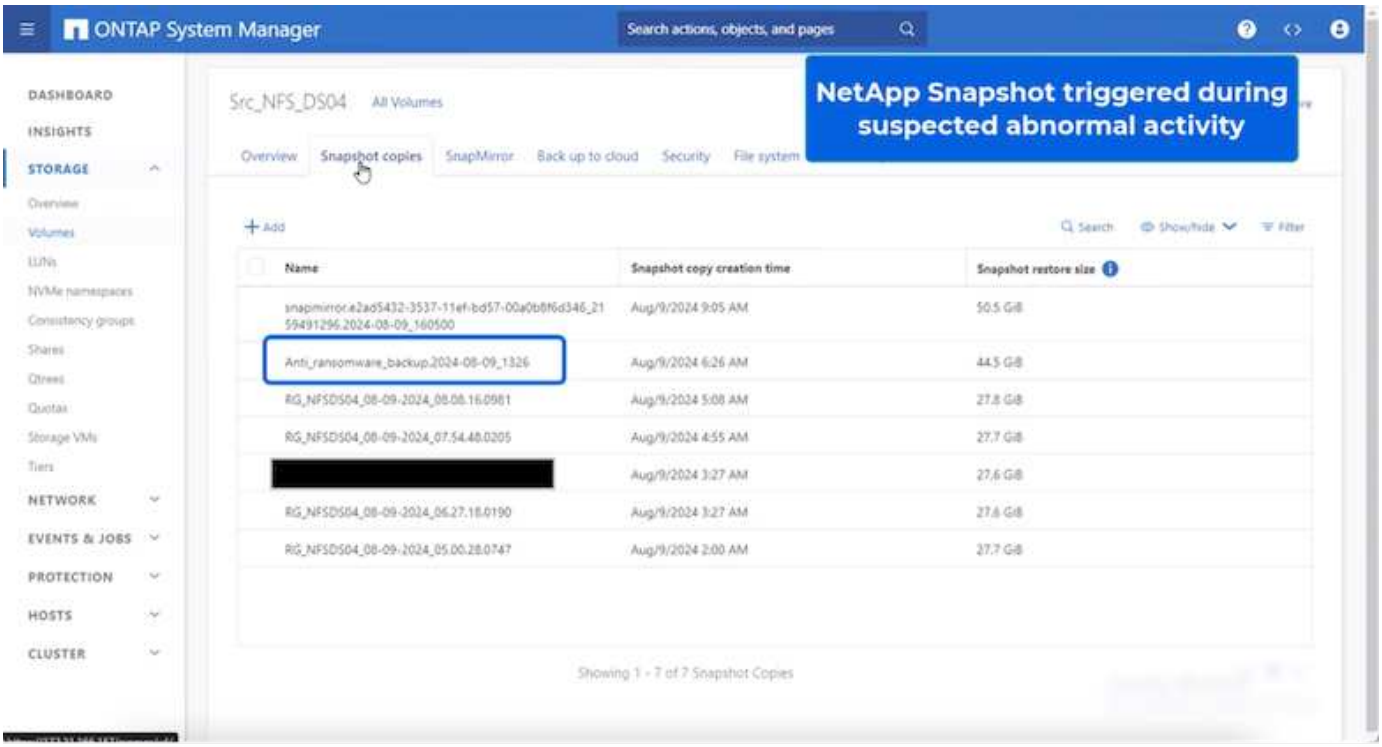


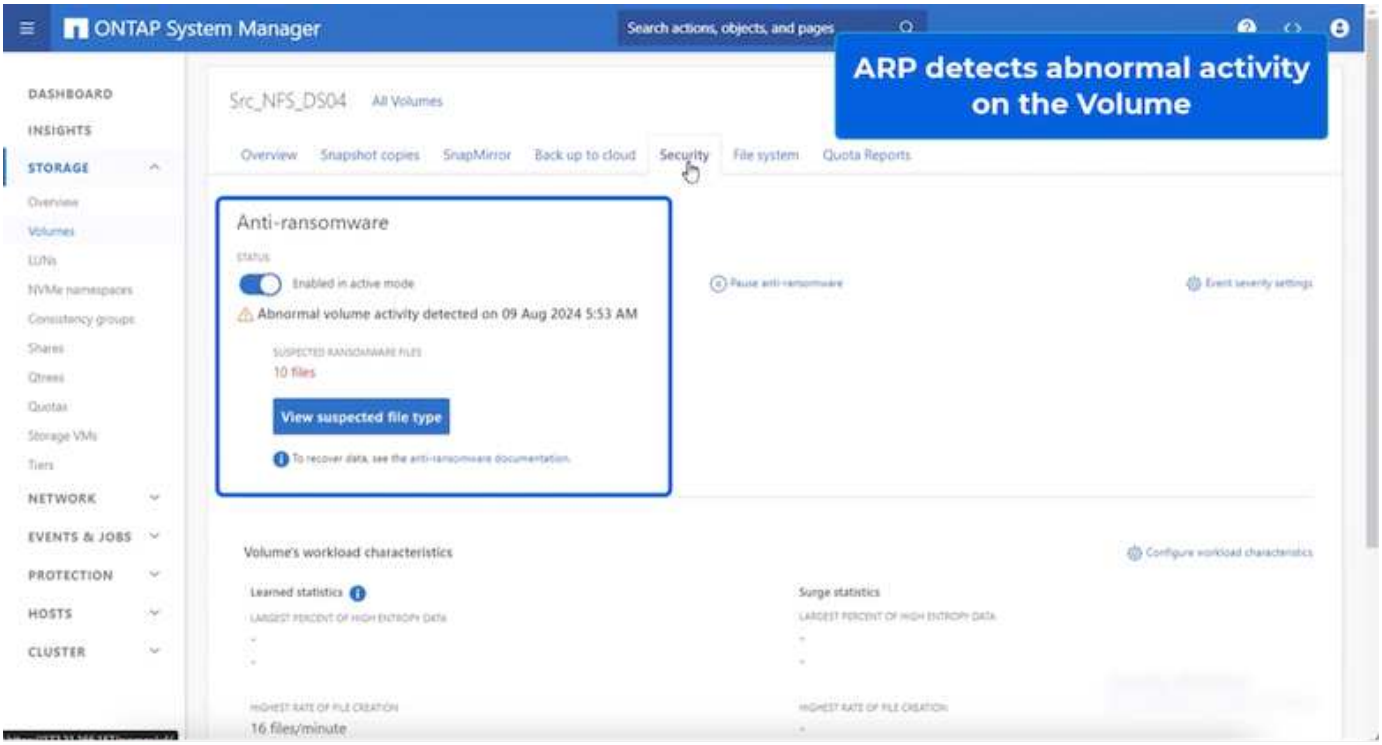
For detailed information on to configure BlueXP ransomware protection, refer to Setup BlueXP ransomware protection and Configure BlueXP ransomware protection settings.

It's time to walk through this with an example. In this walkthrough, the datastore "Src_NFS_DS04" is affected.

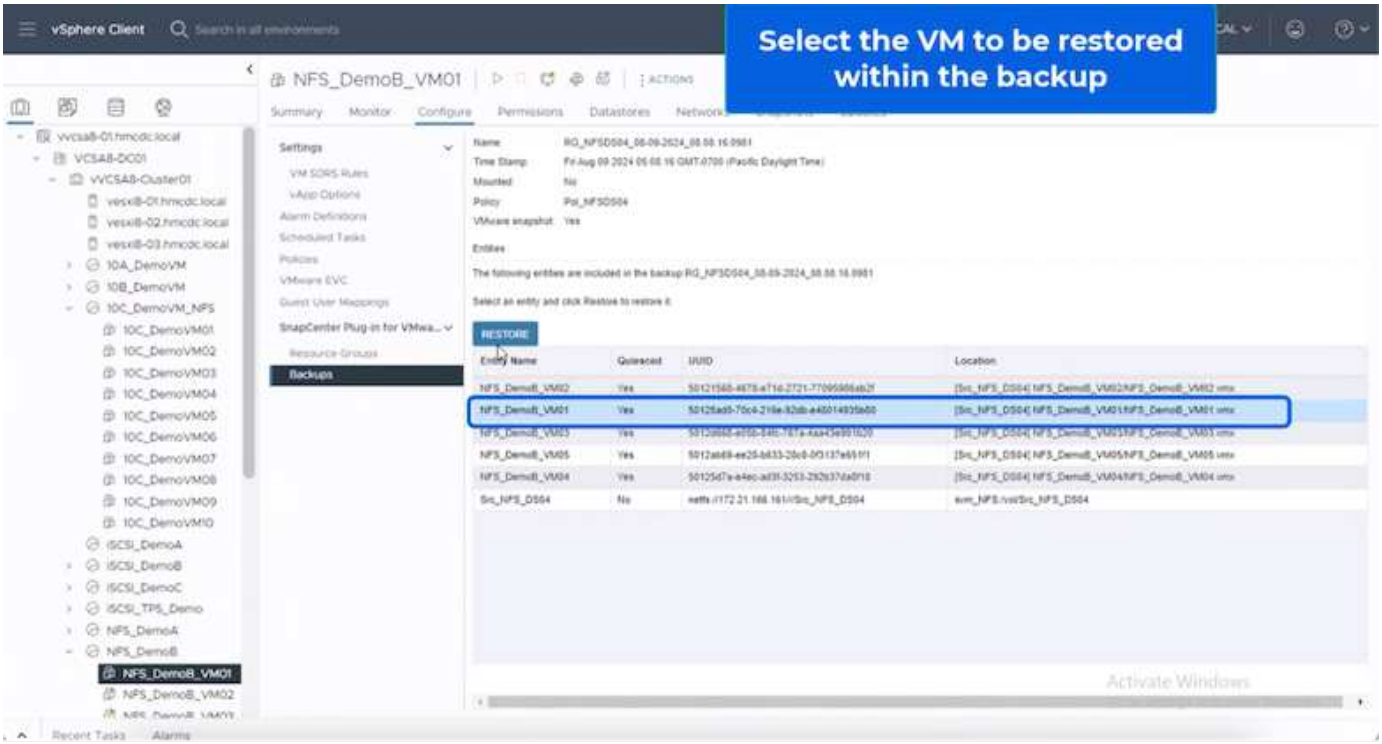


ARP immediately triggered a snapshot on the volume upon detection.





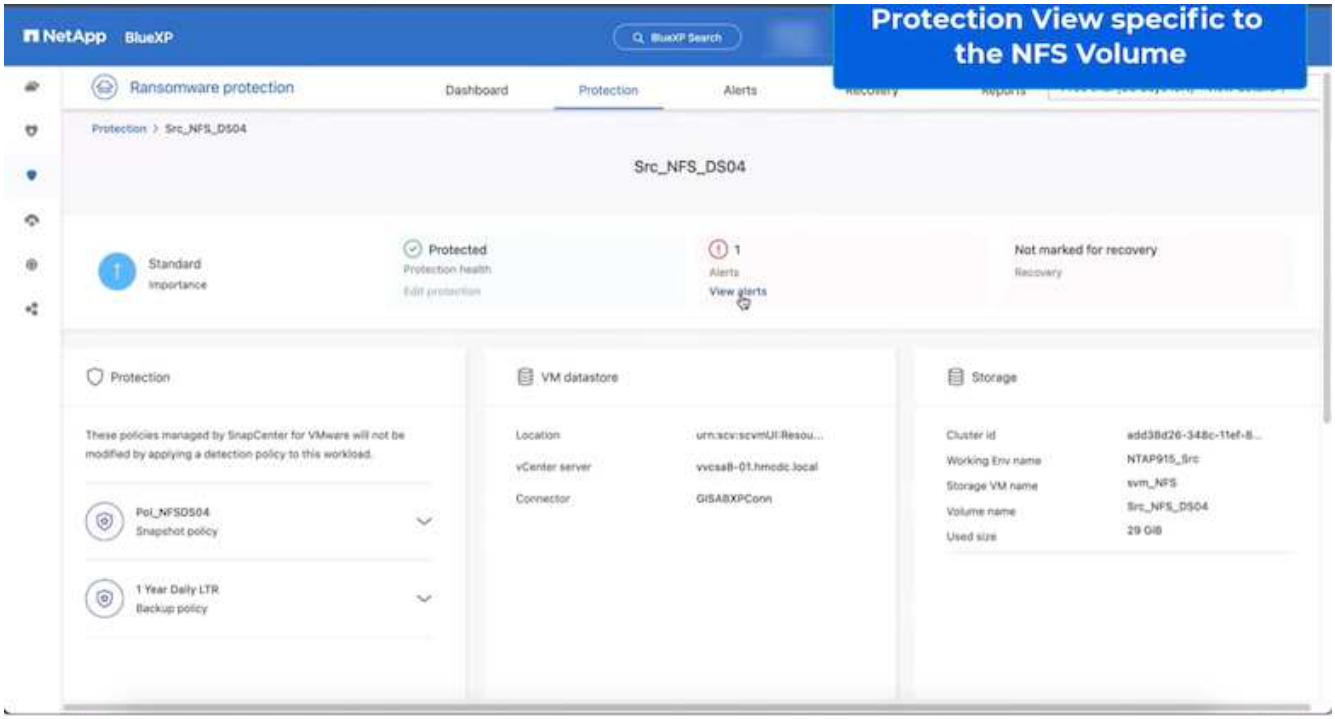
Once the forensic analysis is complete, then the restores can be done quickly and seamlessly using SnapCenter or BlueXP ransomware protection. With SnapCenter, go to the affected virtual machines and select the appropriate snapshot to restore.



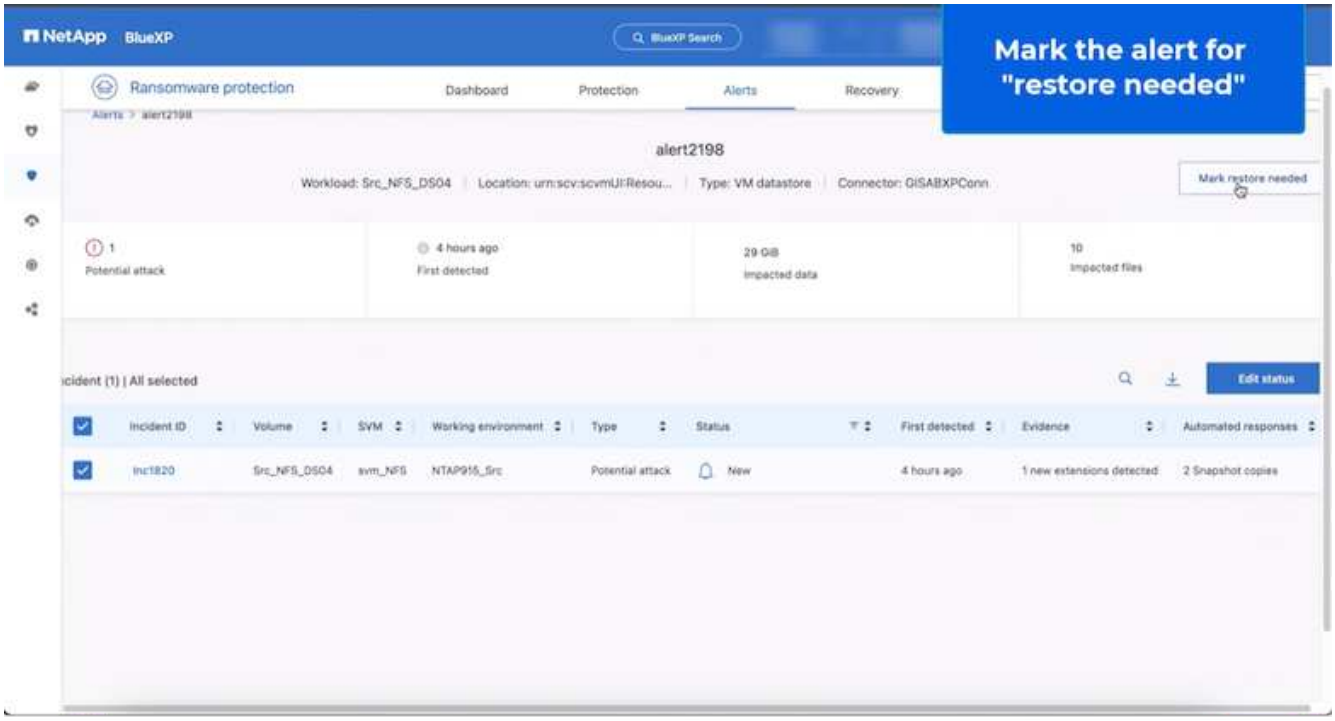
This section looks at how BlueXP ransomware protection orchestrates recovery from a ransomware incident wherein the VM files are encrypted.

> ⓘ 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

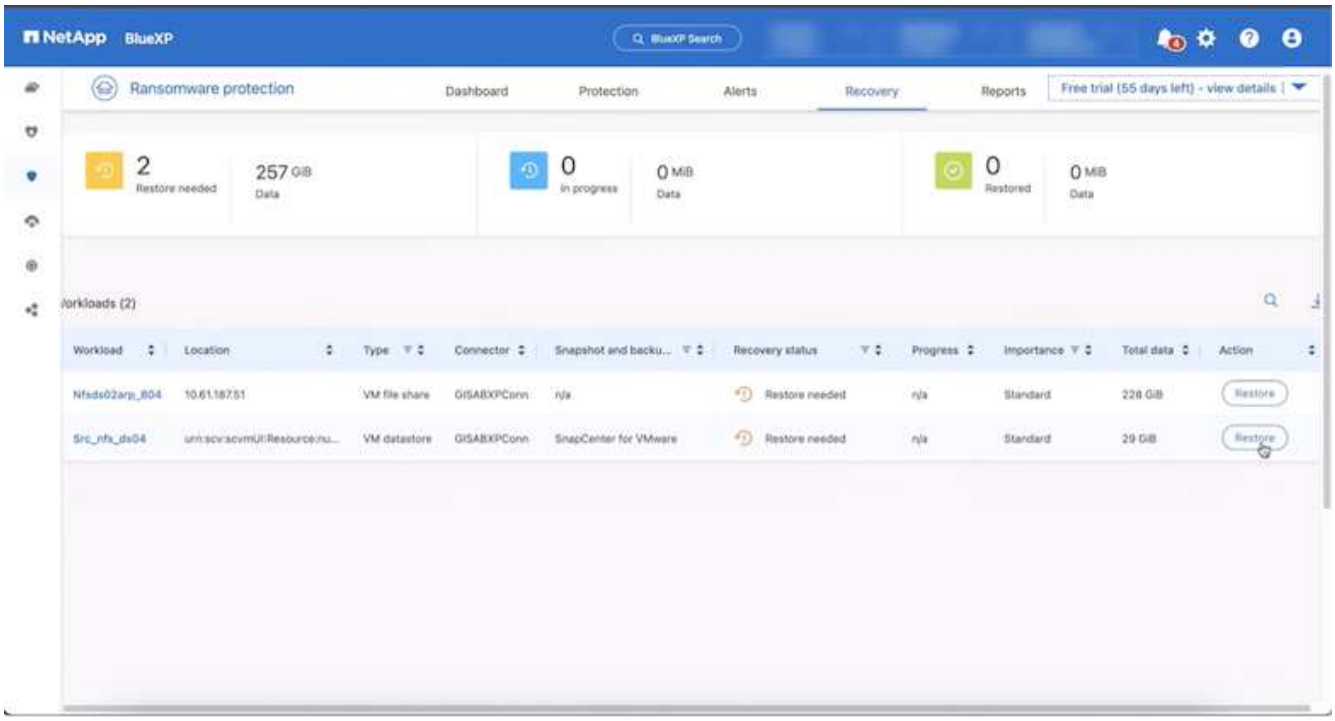


3. Mark the ransomware incident as ready for recovery (after incidents are neutralized) by selecting “Mark restore needed”

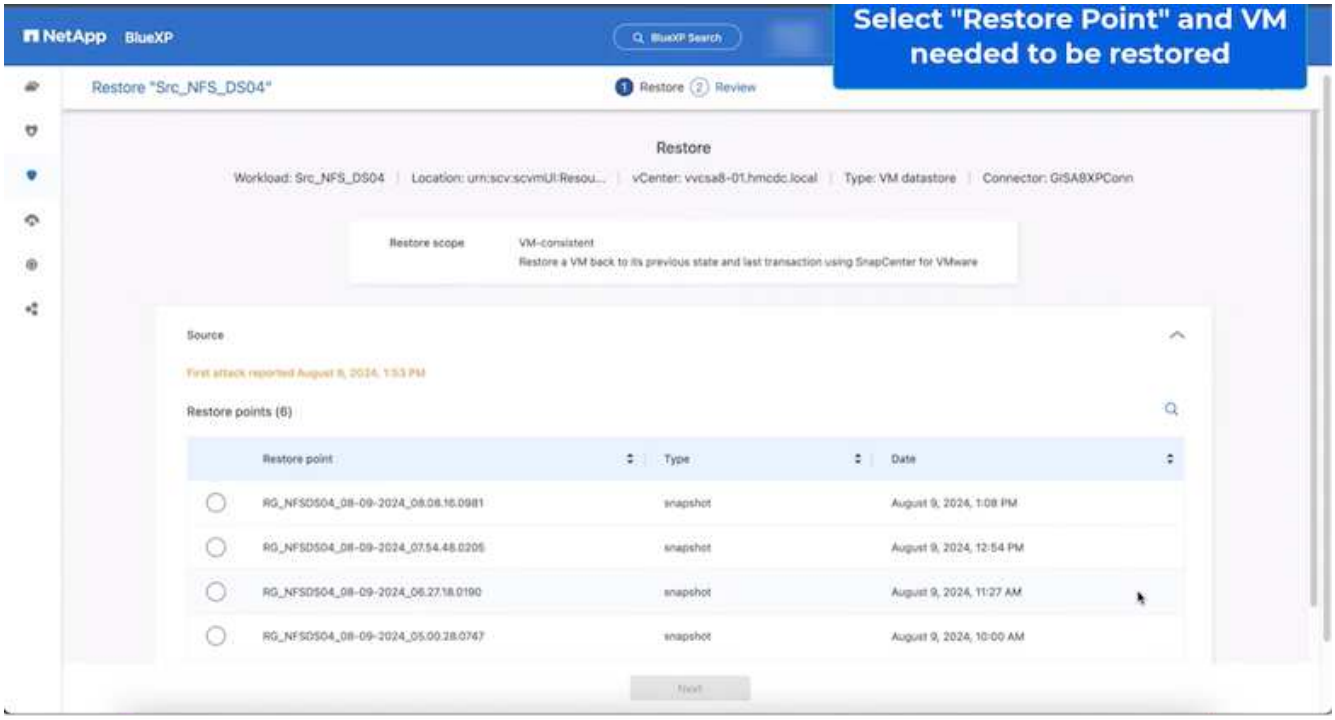


The alert can be dismissed if the incident turns out to be false positive.

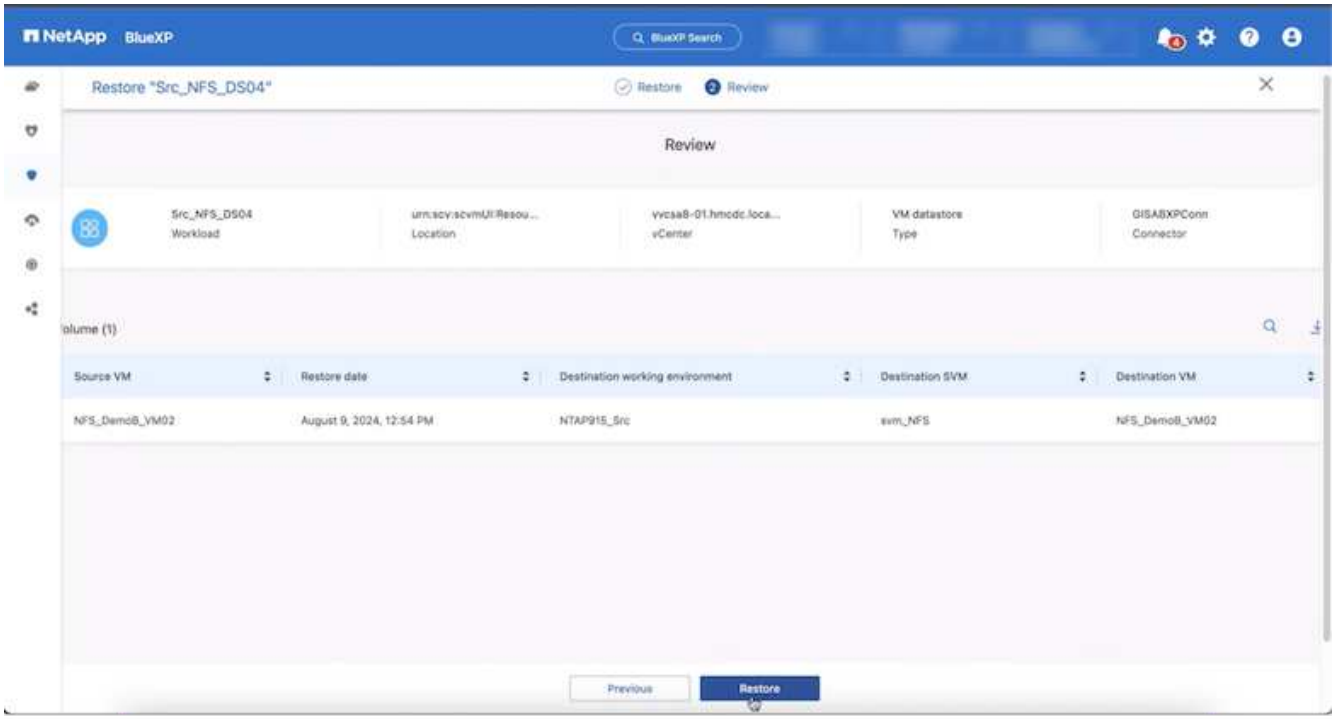
4. Got to Recovery tab and review the workload information in the Recovery page and select the datastore volume that is in the “Restore needed” state and select Restore.



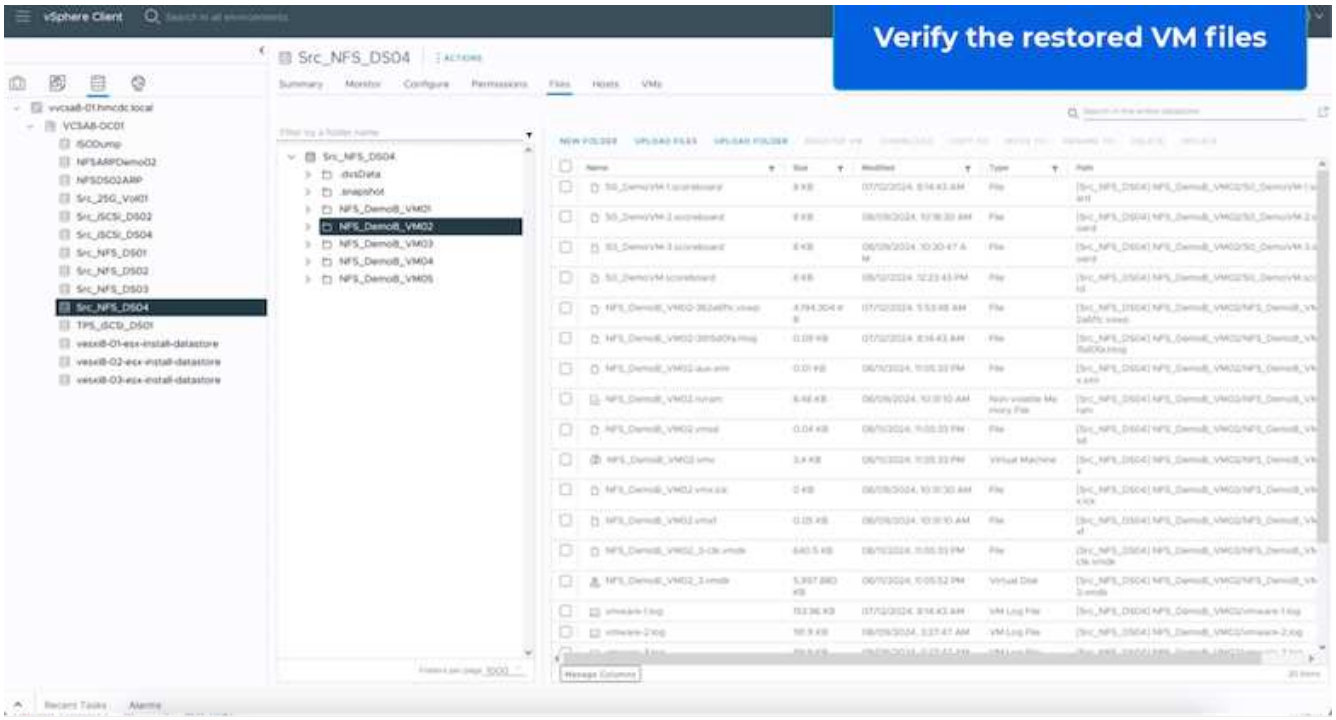
5. In this case, the restore scope is "By VM" (for SnapCenter for VMs, the restore scope is "By VM")



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.