VMware vSphere Foundation on NetApp

NetApp virtualization solutions

NetApp
January 15, 2026

Table of Contents

VMware vSphere Foundation on NetApp . . . 1

Get started . . . 1

Learn about using NFS v3 datastores on ONTAP storage systems with VMware vSphere 8 . . . 1

Learn about NetApp support for VMware vSphere 8 . . . 8

Learn about using VMware vSphere 8 with ONTAP storage . . . 8

What’s new with VMware vSphere 8 . . . 9

Deployment Guide for VMFS . . . 10

Introduction . . . 10

Rightsize and optimize . . . 10

NetApp ONTAP Tools for VMware vSphere . . . 12

VAAI Offloading . . . 18

Data Protection . . . 19

Setting up SnapCenter Plug-in for VMware for VMs . . . 20

Add storage, create policy and resource group . . . 21

Back up resource groups . . . 25

Restore VMs from backup . . . 25

Ransomware Protection . . . 29

Migration . . . 30

Disaster Recovery . . . 30

Conclusion . . . 31

Use nConnect on NFS v3 datastores to improve datastore performance . . . 31

Use cases . . . 31

Technical details . . . 32

Pre-requisite . . . 33

Update number of connection to NFS Datastore . . . 33

Design considerations . . . 35

Configure NFS datastores for vSphere 8 using ONTAP tools for VMware vSphere . . . 35

Solution Overview . . . 36

Architecture . . . 36

Prerequisites . . . 37

Deployment Steps . . . 38

Additional information . . . 67

Configure disaster recovery for NFS datastores using VMware Site Recovery Manager . . . 67

Scenario Overview . . . 68

Architecture . . . 68

Prerequisites . . . 69

Deployment Steps . . . 69

Disaster recovery operations with SRM . . . 90

Additional information . . . 93

VMware vSphere Metro Storage Cluster with SnapMirror active sync . . . 93

Prerequisites . . . 96

vMSC non-uniform host access with ONTAP System Manager UI. . . . 96

vMSC uniform host access mode with ONTAP Tools. . . . 104

- VM protection with SnapCenter plug-in for VMware vSphere. . . . 110

Convert SM active sync from asymmetric to symmetric active/active with VMware vSphere Metro Storage Cluster . . . 116

- Overview . . . 116
- Prerequisites . . . 117
- Steps to convert from asymmetric to symmetric SM active sync . . . 117

Learn about using VMware Virtual Volumes (vVols) with ONTAP storage . . . 119

- Overview . . . 119
- ONTAP tools 9.x . . . 122
- ONTAP tools 10.x . . . 122
- Why vVols? . . . 122
- Connectivity options . . . 123
- Provisioning using ONTAP tools for VMware vSphere . . . 124
- Data Protection of VMs on vVol datastore . . . 135
- VM migration from traditional datastores to vVol datastore . . . 138
- VM migration between vVol datastores . . . 139
- Sample Reference architecture . . . 139
- How to get started . . . 140

Collect data with the Virtual Machine Data Collector . . . 140

- Learn about assessing your VMware infrastructure using the Virtual Machine Data Collector . . . 140
- Virtual Machine Data Collector (VMDC) . . . 141

VMware vSphere Foundation on NetApp

Get started

Learn about using NFS v3 datastores on ONTAP storage systems with VMware vSphere 8

NetApp ONTAP and VMware vSphere 8 work together to deliver scalable and secure NFS v3-based storage solutions for hybrid cloud environments using NetApp All-Flash Arrays. Learn about the supported storage options for VMware vSphere Foundation and the key use cases, including VMware Live Site Recovery for disaster recovery and NetApp's Autonomous Ransomware Protection (ARP) for NFS storage.

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:

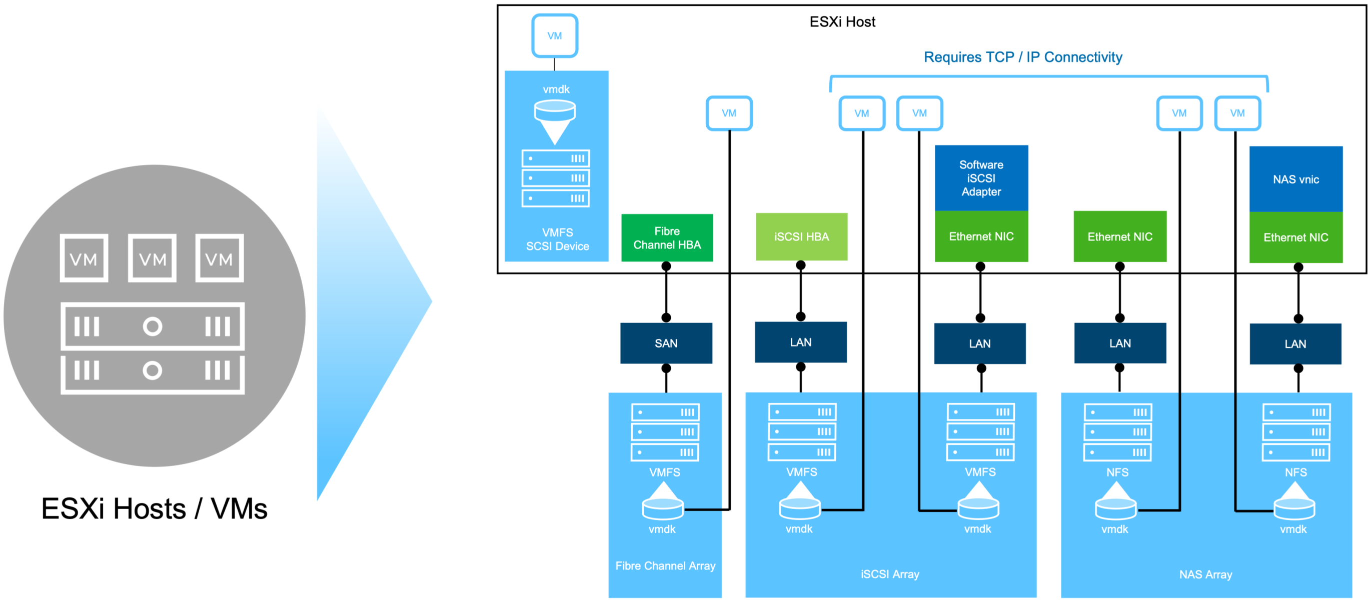
- VMware vSphere
- VMware vSAN
- Aria Standard
- VMware vSphere Kubernetes vSphere
- vSphere Distributed Switch

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.

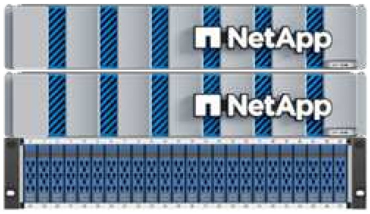
The AFF lineup is comprised of both A-Series and C-Series models.

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.

NetApp Backup and Recovery enables backup strategies that extend copies of data to object storage in the cloud.

For more information on backup strategies with NetApp Backup and Recovery visit NetApp Backup and Recovery Documentation.

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

*NetApp Disaster Recovery 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 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. NetApp Disaster Recovery 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, NetApp Disaster Recovery 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 NetApp Disaster Recovery 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.

Learn about NetApp support for VMware vSphere 8

The NetApp and VMware partnership is the only partnership where a single storage system addresses all of the key VMware defined use cases.

Modern & Cloud-Connected All-Flash For vSphere 8

ONTAP implementations run on a variety of platforms including NetApp-engineered appliances, commodity hardware and in the public cloud. ONTAP offers unified storage whether you access over SAN or NAS protocols and in configurations ranging from high-speed flash to lower-cost media to cloud-based storage. NetApp also offers purpose-built flash platforms to simplify and segment your storage needs without creating silos. Furthermore, NetApp offers software to easily allow data movement across on-premises and cloud. Finally, NetApp Console provides a single dashboard for managing all these relationships and your storage footprint.

- NetApp Platforms

Learn about using VMware vSphere 8 with ONTAP storage

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

For more information, visit VMware vSphere with ONTAP

What’s new with VMware vSphere 8

Learn what’s new in VMware vSphere 8 and ONTAP 9.12. Review the compatibility of ONTAP features and support with VMware infrastructure and software.

The integration of NetApp and VMware technologies has a legacy spanning 20 years and thousands of engineering hours. With the advent of vSphere 8 and ONTAP 9.12, both companies deliver products that satisfy the most demanding customer workloads. When these products are coupled together in solutions, are real customer challenges solved whether on-premises or in the public clouds. When these products are coupled together in solutions, real customer challenges are solved whether on-premises or in the public clouds.

To help you determine support ability of products, protocols, operating systems, etc. please review the resources below:

- The NetApp Interoperability Matrix Tool (IMT). The IMT defines the qualified components and versions you can use to build FC/FCoE, iSCSI, NFS and CIFS configurations as well as integrations with additional plug-ins and software offerings.
- The VMware Compatibility Guide. The VMware Compatibility Guide lists System, I/O, Storage/SAN, Backup compatibility and much more with VMware Infrastructure and software products.
- NetApp ONTAP Tools for VMware. ONTAP tools for VMware vSphere is a single vCenter Server plug-in that includes the Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) extensions. Fully supported with VMware vSphere 8, OTV 9.12 delivers real value to customers on a daily basis.

NetApp ONTAP and VMware supported releases

ⓘ Please let the page(s) build out when selecting a link in the tables below.

Table 1. vSphere 8 currency - NetApp ONTAP and VMware supported releases. NetApp IMT - Login required.

VMware vSphere Release	SAN	NFS	OTV	SnapCenter
vSphere 8	Link	Link	Link	Link
vSphere 8u1	Link	Link	Link	Link

Table 2. vSphere 8 currency - NetApp ONTAP and VMware supported releases. VMware Compatibility Guide

VMware vSphere Release	Storage system / protocols	OTV - SRA	OTV – VASA Provider	SnapCenter Plug-in for VMware vSphere
vSphere 8	Link	Link	Link	Link
vSphere 8u1	Link	Link	Link	Link

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

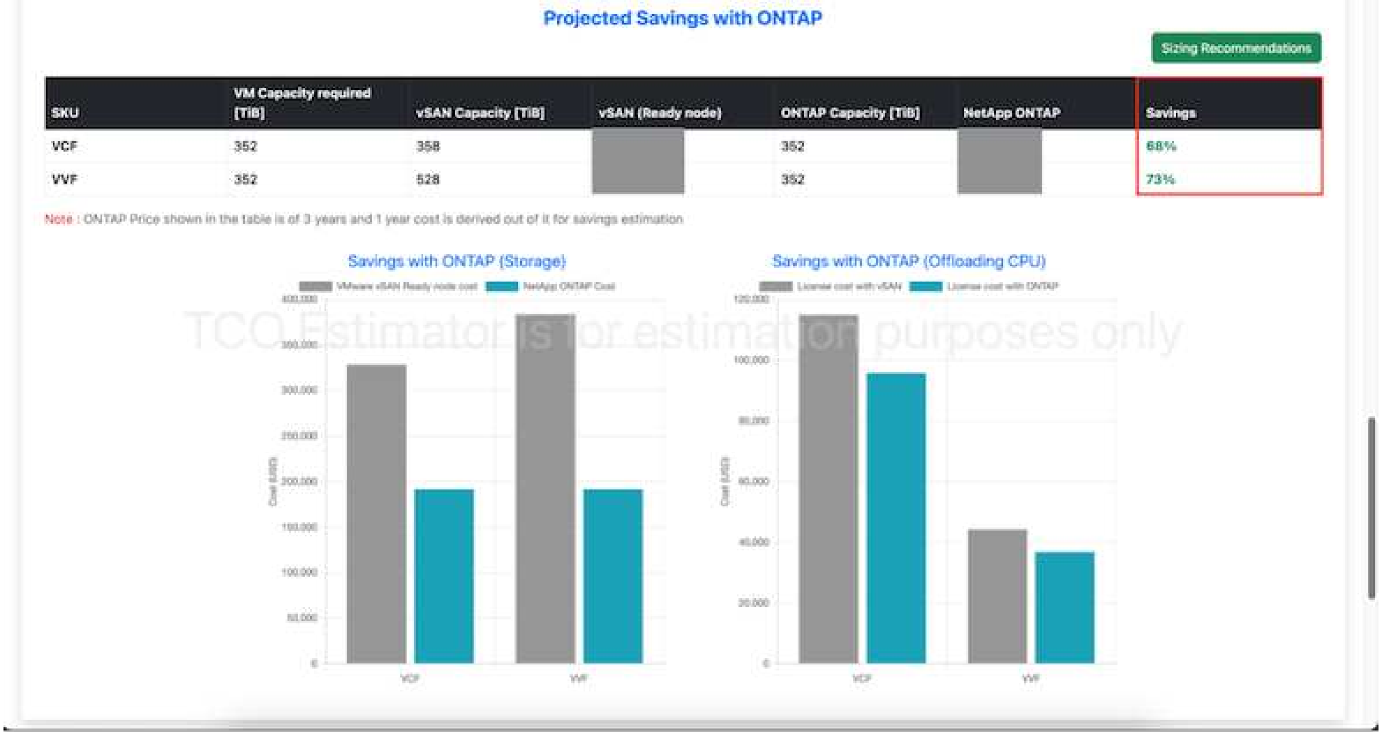
With impending licensing changes, organizations are proactively addressing the potential increase in Total Cost of Ownership (TCO). They are strategically optimizing their VMware infrastructure through aggressive resource management and right-sizing to enhance resource utilization and streamline capacity 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 optimization journey. The TCO estimator uses RVtools or manual input methods to easily project how many hosts are required for the given deployment and calculate the savings to optimize the deployment using NetApp ONTAP storage systems. Keep in mind, this is the stepping stone.

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

Here is a screenshot from the TCO estimator.



Projected Savings with ONTAP

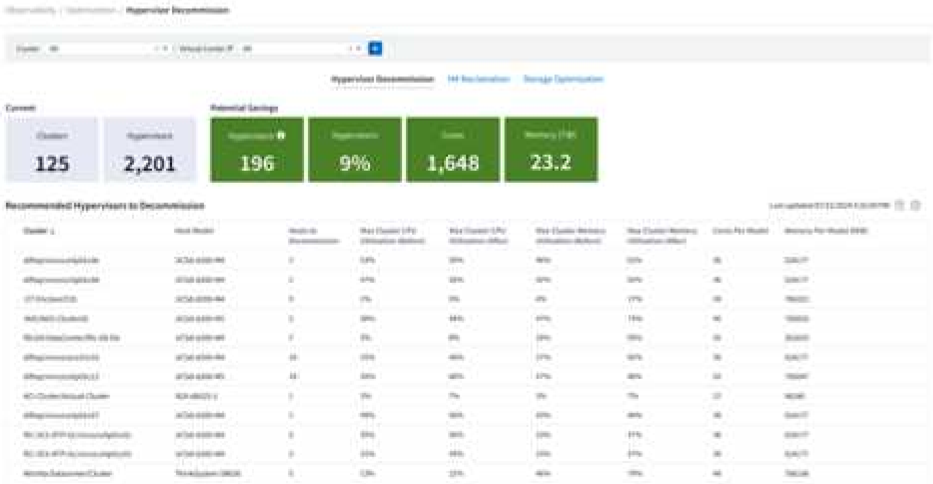
SKU	VM Capacity required [TiB]	vSAN Capacity [TiB]	vSAN (Ready node)	ONTAP Capacity [TiB]	NetApp ONTAP	Savings
VCF	352	358	[redacted]	352	[redacted]	68%
VVF	352	528	[redacted]	352	[redacted]	73%

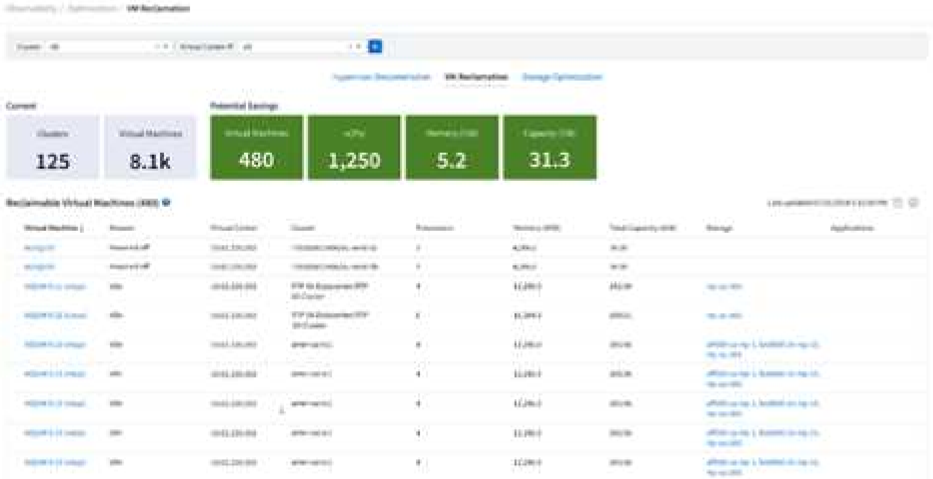
Note : ONTAP Price shown in the table is of 3 years and 1 year cost is derived out of it for savings estimation

Cloud Insights

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

Below are the screenshots from Cloud Insights.





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

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

NetApp ONTAP Tools for VMware vSphere

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

Getting Started

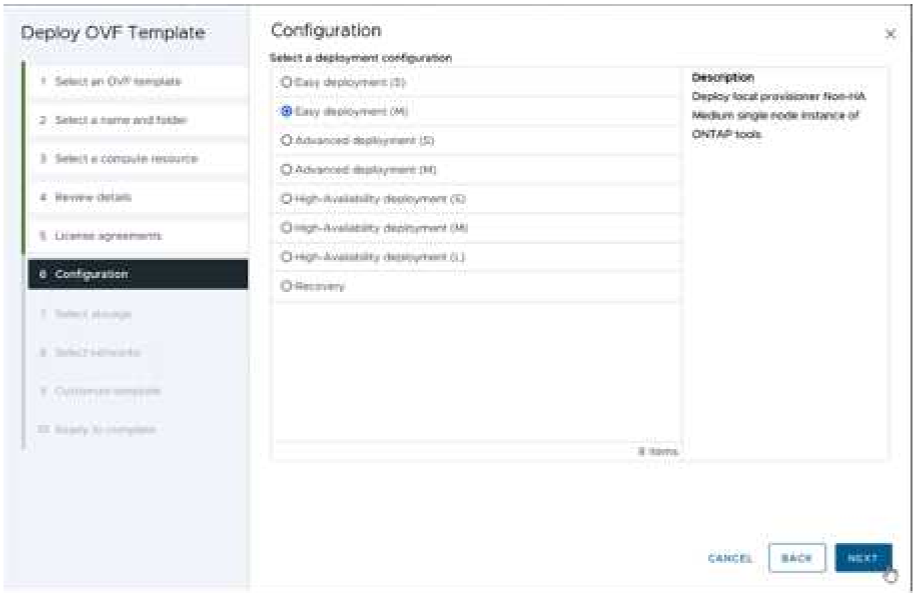
Before deploying and configuring ONTAP tools for VMware, ensure the pre-requisites are met. Once done, deploy a single node configuration.

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

Steps

1. Log in to the vSphere server.
2. Navigate to the cluster or the host where you want to deploy the OVA.
3. Right-click the required location and select Deploy OVF template.
   a. Enter the URL for the .ova file or browse to the folder where the .ova file is saved, and then select Next.
4. Select a name, folder, cluster / host for the virtual machine and select Next.
5. In the Configuration window, select Easy deployment(S), Easy deployment(M), or Advanced deployment(S) or Advanced deployment(M) configuration.

   > The easy deployment option is used in this walkthrough.



Configuration

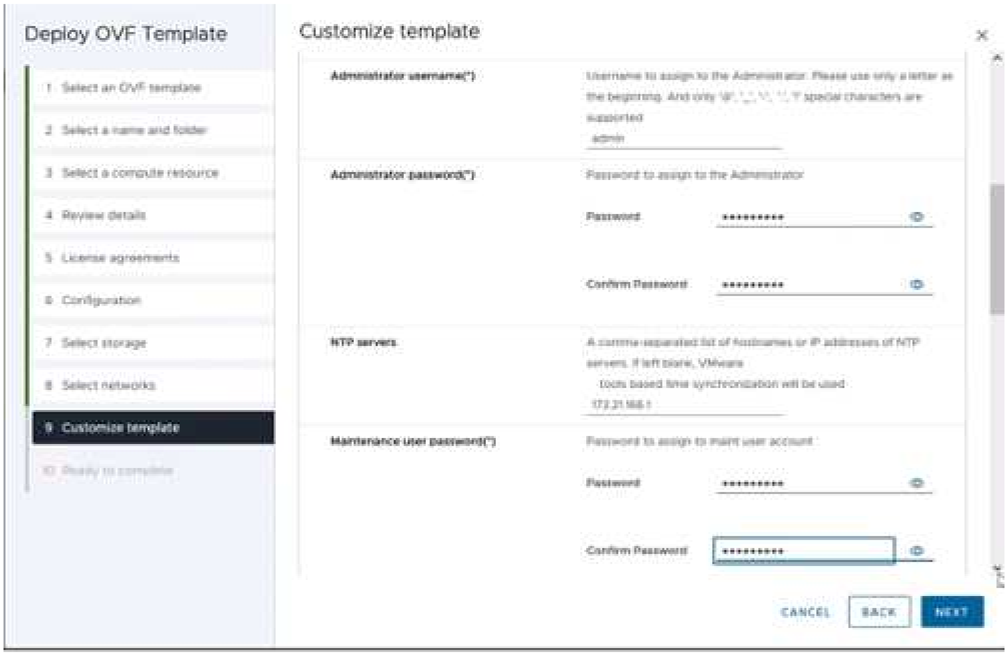
Select a deployment configuration

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

8 items

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

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



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

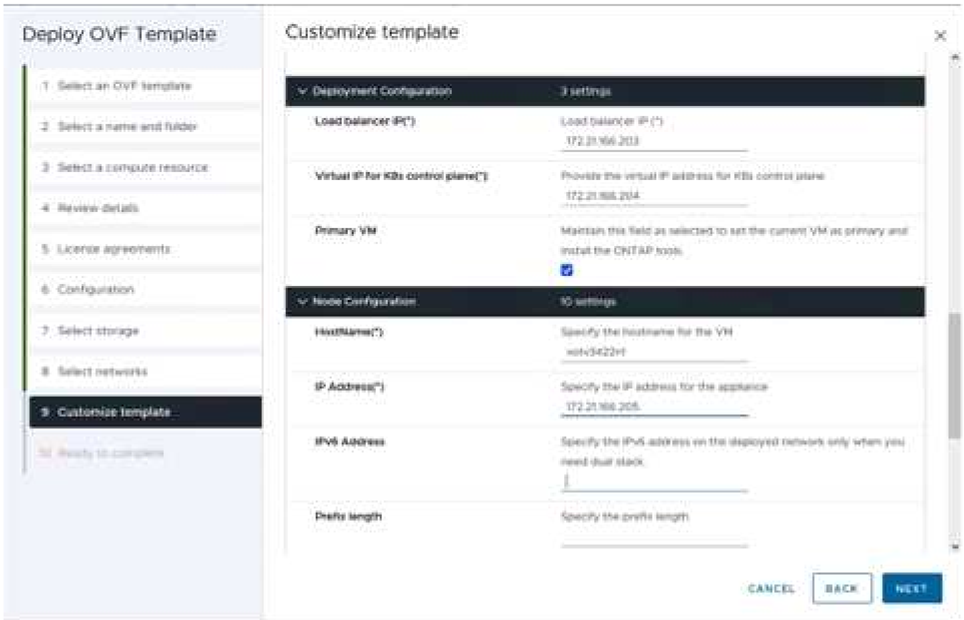
Customize template

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

Administrator password(*)
Password to assign to the Administrator
Password **********
Confirm Password **********

NTP servers
A comma-separated list of hostnames or IP addresses of NTP servers. If left blank, VMware tools based time synchronization will be used
172.21.166.1

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



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

Deployment Configuration 3 settings

Load balancer IP(*)
Load balancer IP (*)
172.21.166.203

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

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

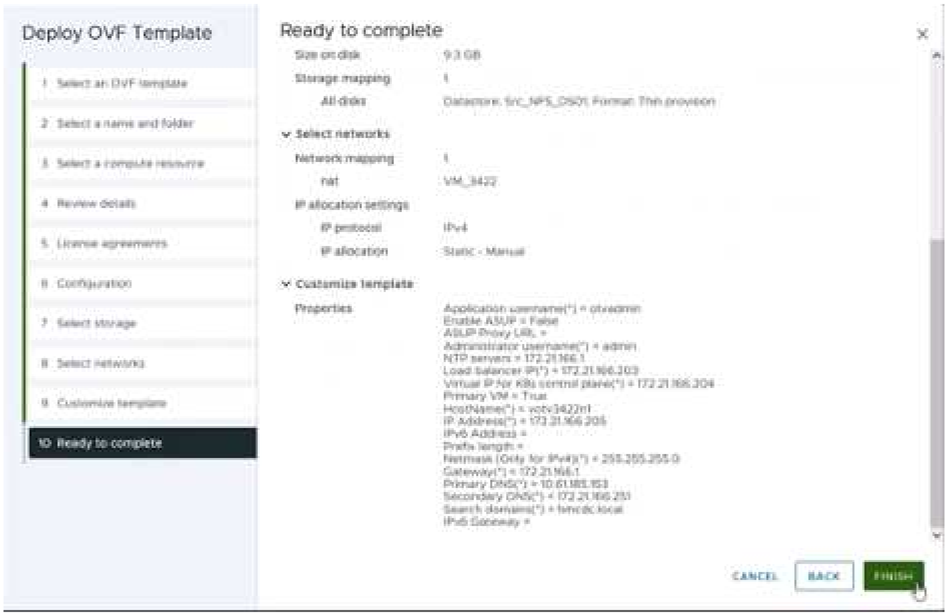
Node Configuration 10 settings

HostName(*)
Specify the hostname for the VM
votv3422ht

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

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

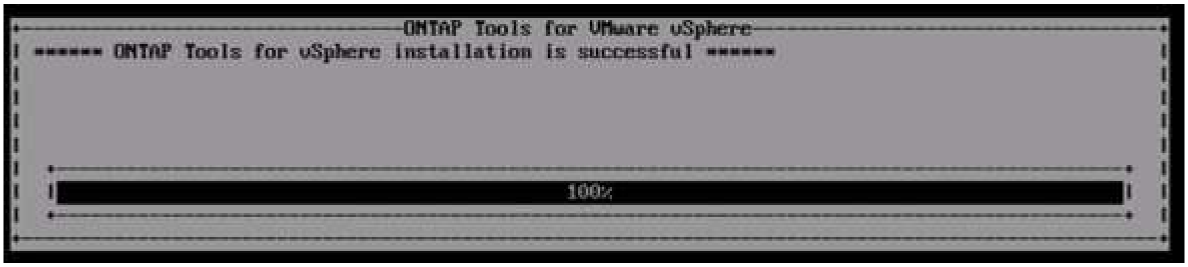
Prefix length
Specify the prefix length



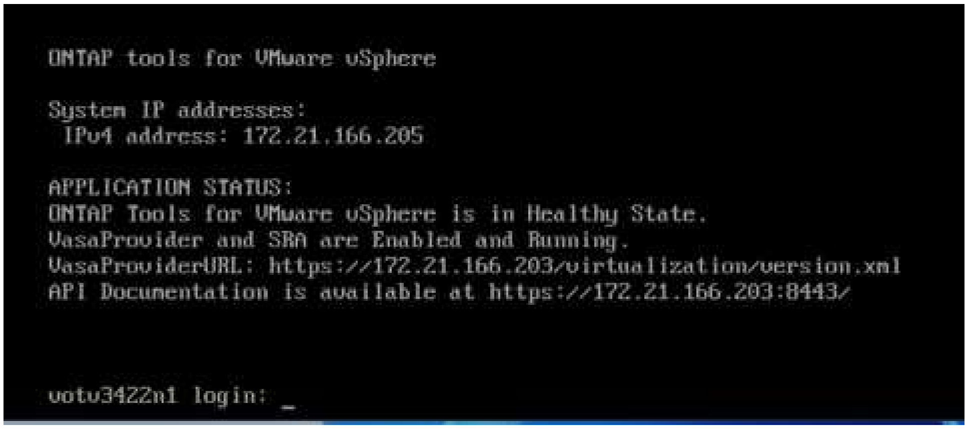
Ready to complete

Size on disk 9.3 GB
Storage mapping 1
All disks Datastore: Src_NFS_DS01; Format: Thin provision
Select networks
Network mapping 1
nat VM_3422
IP allocation settings
IP protocol IPv4
IP allocation Static - Manual
Customize template
Properties
Application username(*) = otvadmin
Enable ASUP = False
ASUP Proxy URL =
Administrator username(*) = admin
NTP servers = 172.21.166.1
Load balancer IP(*) = 172.21.166.203
Virtual IP for K8s control plane(*) = 172.21.166.204
Primary VM = True
HostName(*) = votv3422n1
IP Address(*) = 172.21.166.205
IPv6 Address =
Prefix length =
Netmask (Only for IPv4)(*) = 255.255.255.0
Gateway(*) = 172.21.166.1
Primary DNS(*) = 10.61.185.153
Secondary DNS(*) = 172.21.166.251
Search domains(*) = hmcdc.local
IPv6 Gateway =

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



```
ONTAP Tools for VMware vSphere
****** ONTAP Tools for vSphere installation is successful ******

100%
```

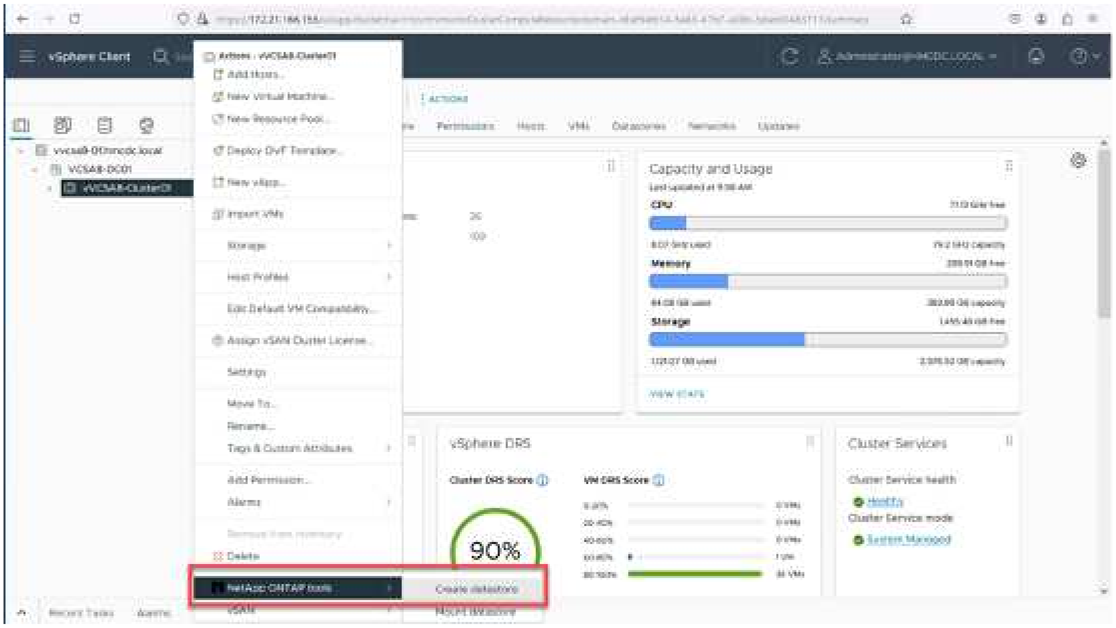


```
ONTAP tools for VMware vSphere

System IP addresses:
 IPv4 address: 172.21.166.205

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


votv3422n1 login: _
```

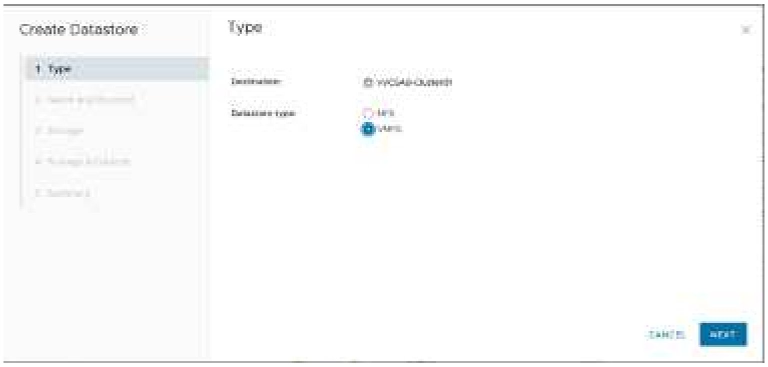
The datastore creation wizard supports provisioning of VMFS, NFS and vVols datastores.

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

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



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


Create Datastore

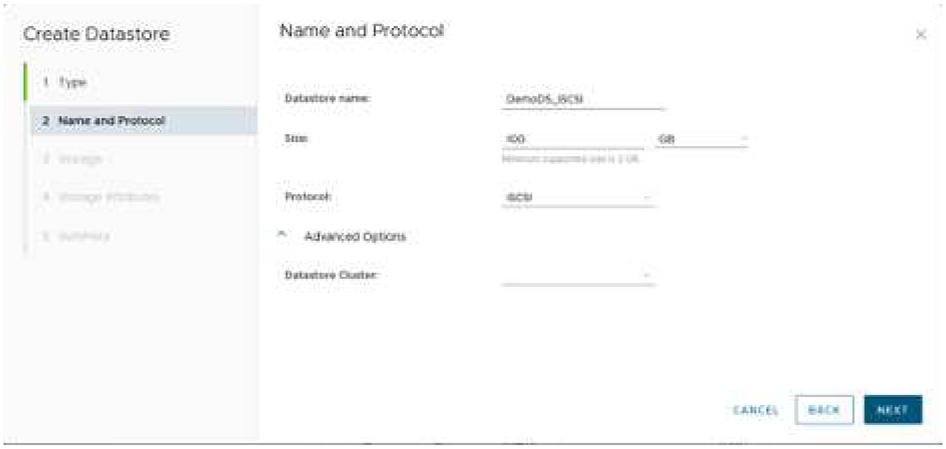
Type

1. Type

Destination: VVCSA8-Cluster01

Datastore type: ○ NFS ● VMFS

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


Create Datastore

Name and Protocol

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

Datastore name: DemoDS_iSCSI

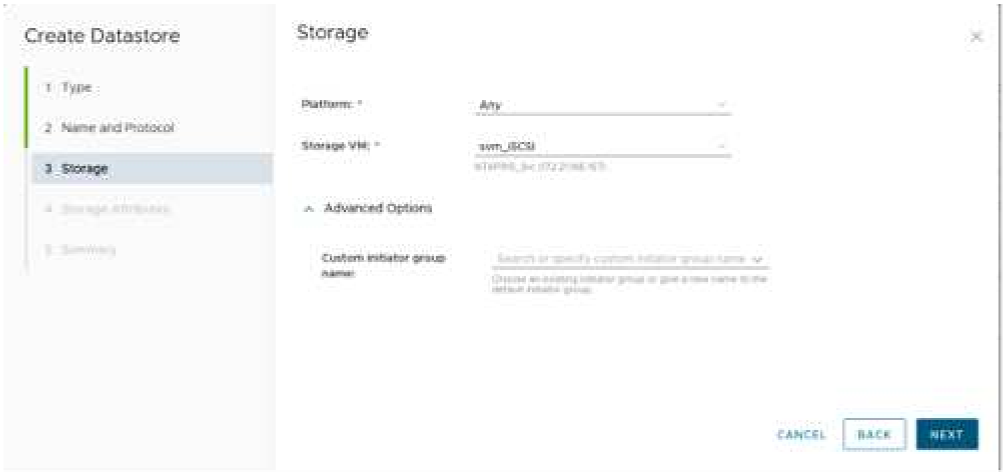
Size: 100 GB

Protocol: iSCSI

Advanced Options

Datastore Cluster:

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



Create Datastore

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

Storage

Platform: * Any

Storage VM: * svm_iSCSI

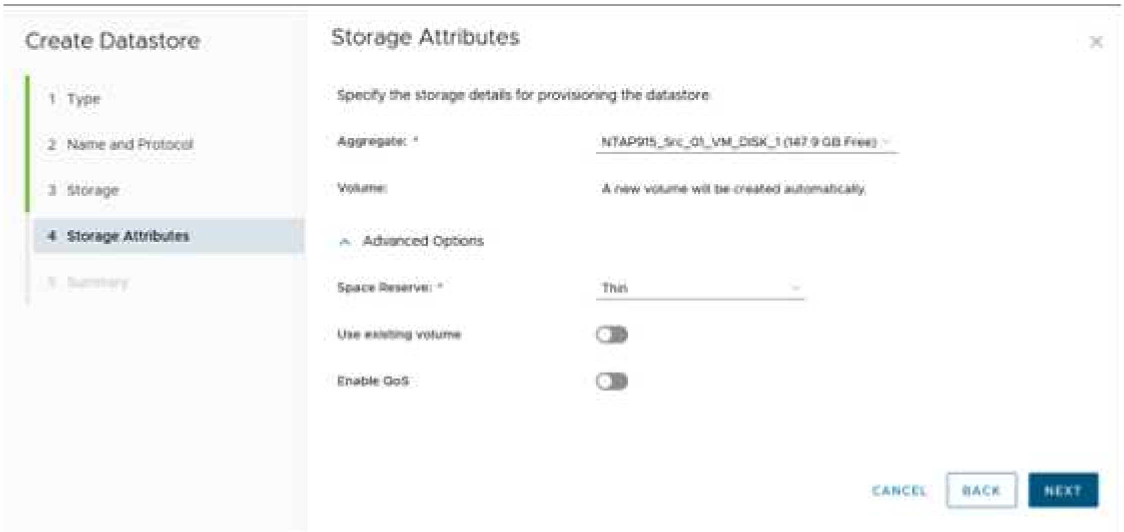
NTAP915_Src (172.21.166.157)

Advanced Options

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

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

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



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: * NTAP915_Src_01_VM_DISK_1 (147.9 GB Free)

Volume: A new volume will be created automatically.

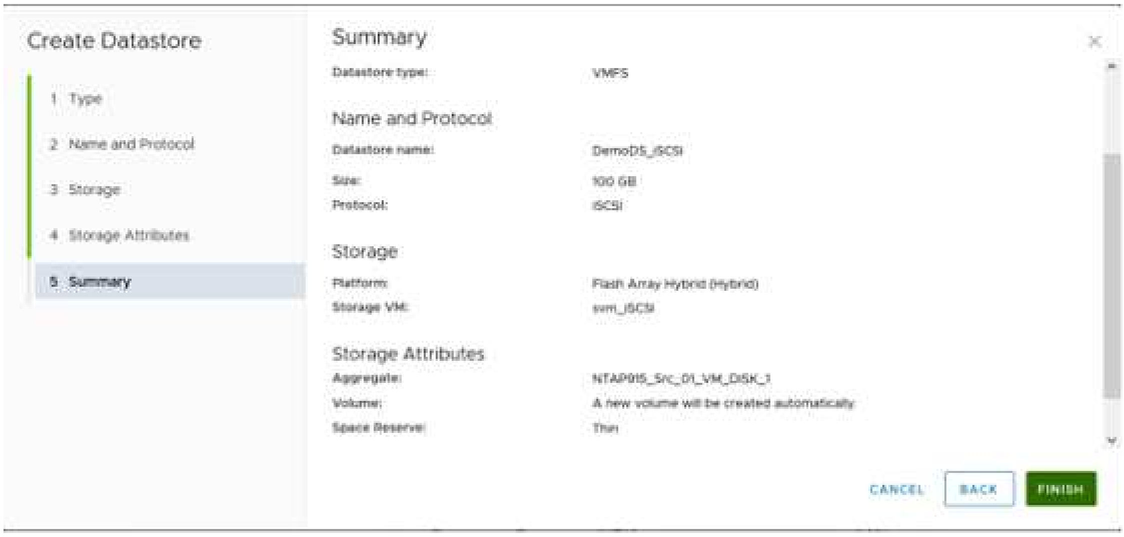
Advanced Options

Space Reserve: * Thin

Use existing volume

Enable QoS

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



Create Datastore

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

Summary

Datastore type: VMFS

Name and Protocol

Datastore name: DemoDS_iSCSI

Size: 100 GB

Protocol: iSCSI

Storage

Platform: Flash Array Hybrid (Hybrid)

Storage VM: svm_iSCSI

Storage Attributes

Aggregate: NTAP915_Src_01_VM_DISK_1

Volume: A new volume will be created automatically

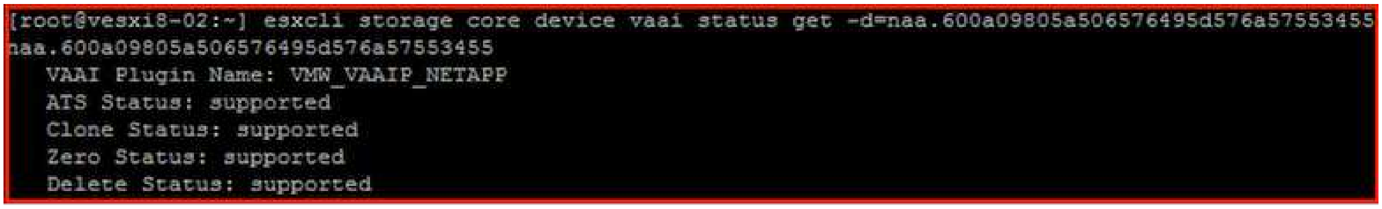
Space Reserve: Thin

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

VAAI Offloading

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

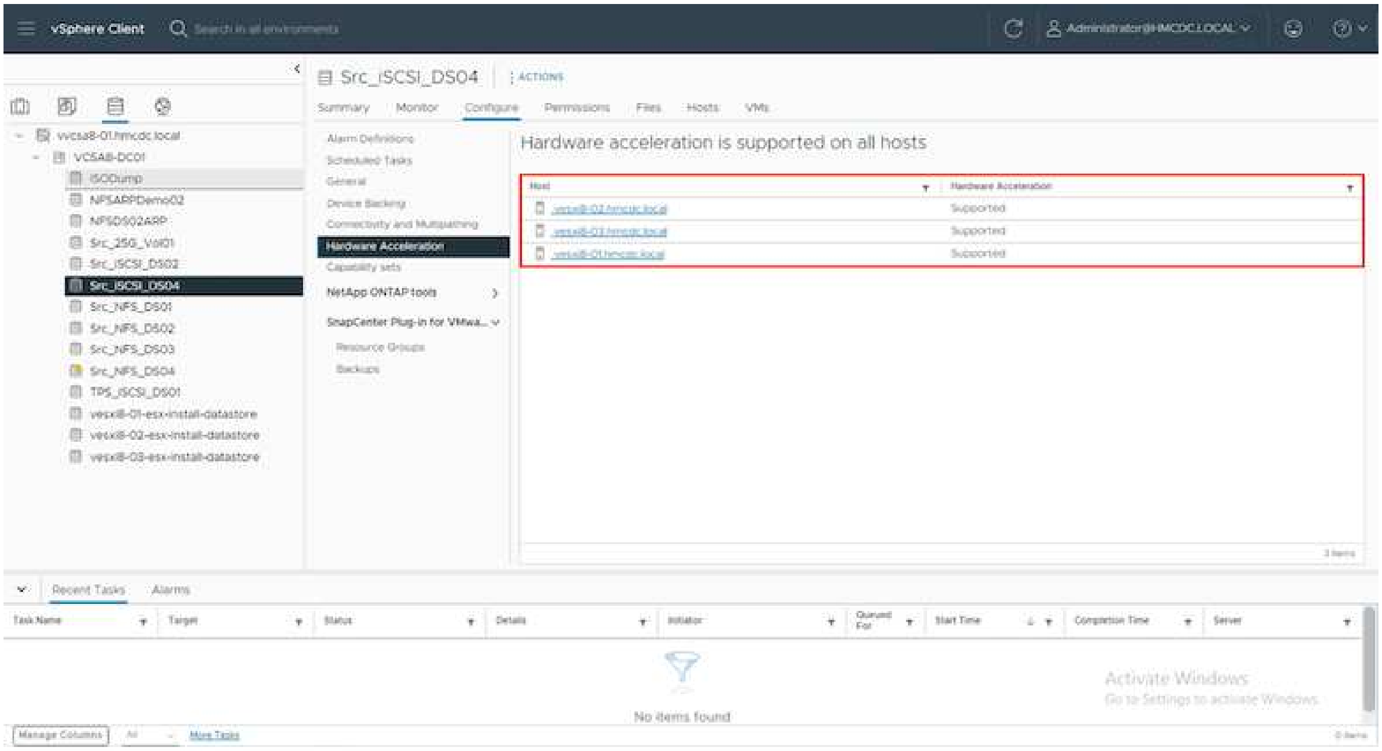
- Copy offload
- Atomic Test & Set (ATS) locking
- Write Same
- Out-of-space condition handling
- Space reclamation



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

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

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



Hardware acceleration is supported on all hosts

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

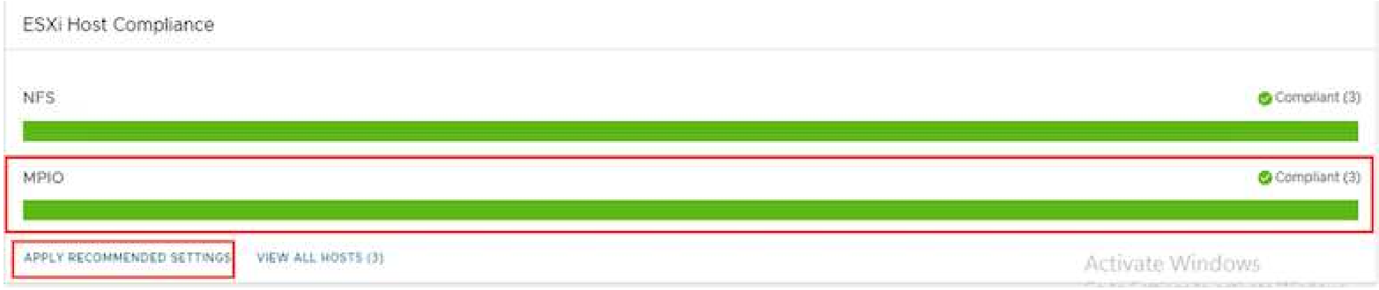
3 items

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server

No items found

0 items

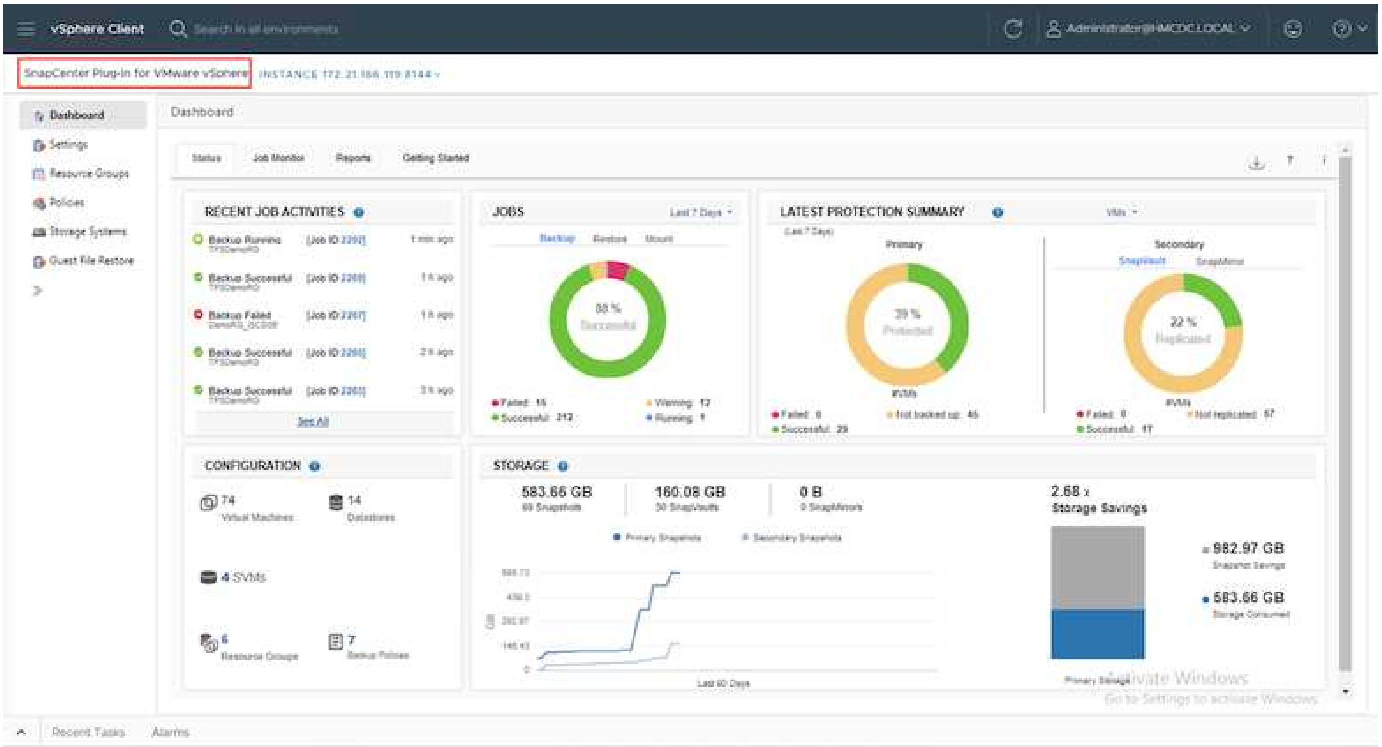
These values are easily set using ONTAP tools for VMware vSphere. From the Overview dashboard, go to ESXi Host compliance card and Select Apply Recommended Settings option. In the Apply recommended host settings window, select the hosts and click Next to apply NetApp recommended host settings.



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:

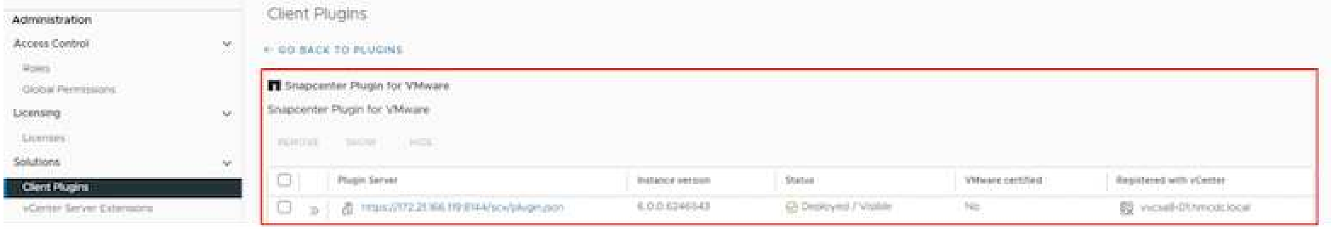
1. Download SnapCenter for VMware Plug-in OVA
2. Log in with the vSphere Client credentials
3. Deploy OVF Template to start the VMware deploy wizard and complete the installation
4. To access the plug-in, select SnapCenter Plug-in for VMware vSphere from the Menu
5. Add Storage
6. Create backup policies
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 customize 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



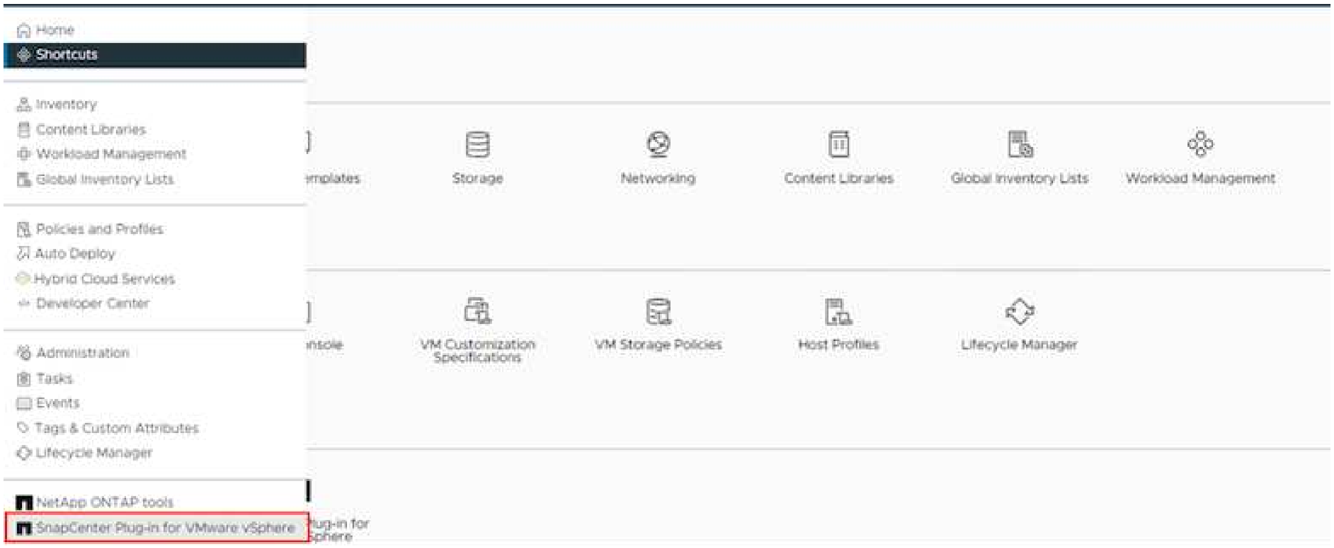
Client Plugins

Snapcenter Plugin for VMware

Snapcenter Plugin for VMware

	Plugin Server	Instance version	Status	VMware certified	Registered with vCenter
□	https://172.21.166.119:8144/scv/plugin.json	6.0.0.6246543	Deployed / Visible	No	vvcsa8-01.hmcdc.local

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



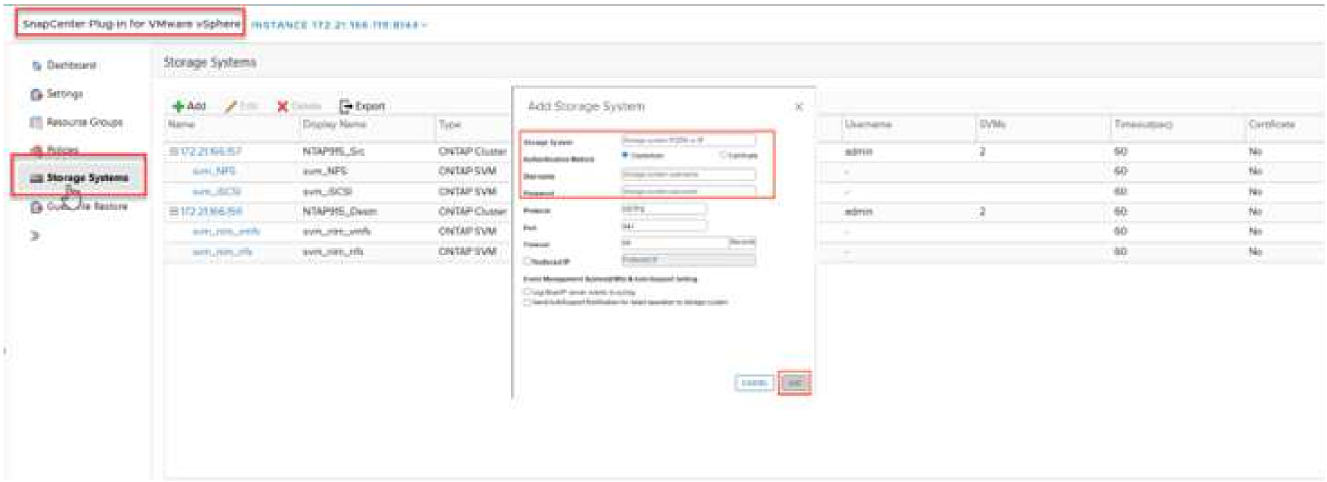
Add storage, create policy and resource group

Adding storage system

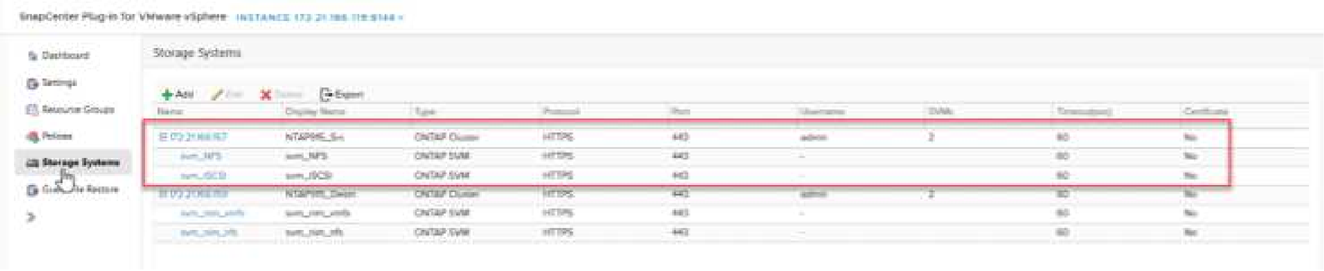
Next step is to add the storage system. Cluster management endpoint or Storage virtual machine (SVM) administration endpoint IP should be added as a storage system to backup or restore VMs. Adding storage enables SnapCenter Plug-in for VMware to recognize and manage backup and restore operations in vCenter.

The process is straight forward.

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



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



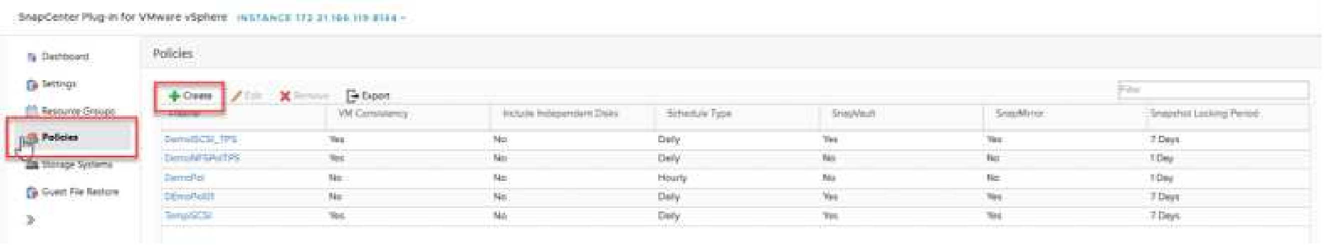
Name	Display Name	Type	Protocol	Port	Username	SVMs	Timeout(sec)	Certificate
⊟ 172.21.166.157	NTAP915_Src	ONTAP Cluster	HTTPS	443	admin	2	60	No
svm_NFS	svm_NFS	ONTAP SVM	HTTPS	443	-		60	No
svm_iSCSI	svm_iSCSI	ONTAP SVM	HTTPS	443	-		60	No
⊟ 172.21.166.158	NTAP915_Destn	ONTAP Cluster	HTTPS	443	admin	2	60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

Create backup policy

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

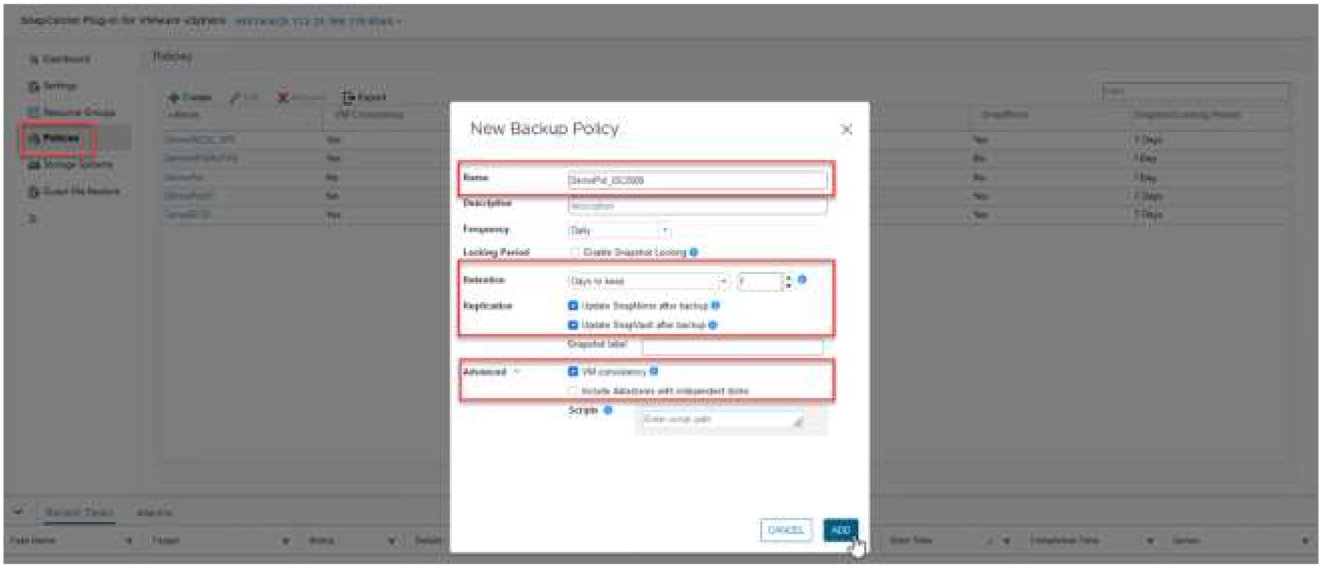


Name	VM Consistency	Include Independent Disks	Schedule Type	SnapVault	SnapMirror	Snapshot Locking Period
DemoISCSI_TPS	Yes	No	Daily	Yes	Yes	7 Days
DemoNFSPolTPS	Yes	No	Daily	No	No	1 Day
DemoPol	No	No	Hourly	No	No	1 Day
DEmoPol01	No	No	Daily	Yes	Yes	7 Days
TempiSCSI	Yes	No	Daily	Yes	Yes	7 Days

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

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

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



New Backup Policy

Name: DemoPol_iSCSI09

Description:

Frequency: Daily

Locking Period: □ Enable Snapshot Locking

Retention: Days to keep 7

Replication: ☑ Update SnapMirror after backup

☑ Update SnapVault after backup

Snapshot label:

Advanced: ☑ VM consistency

□ Include datastores with independent disks

Scripts: Enter script path

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

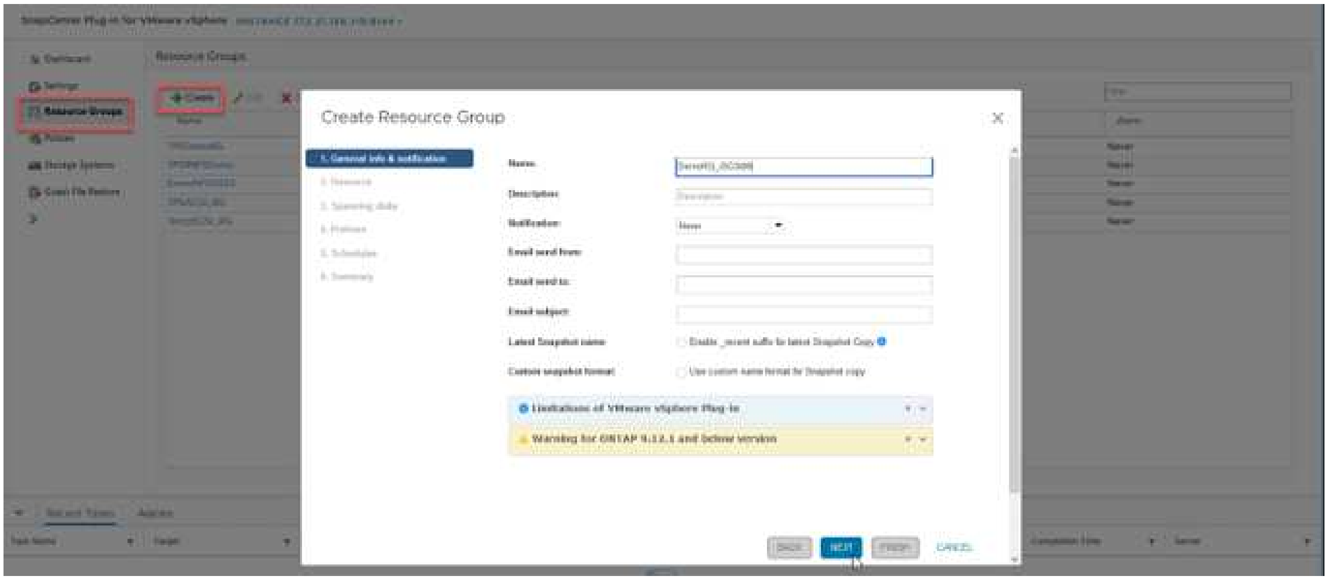
Create Resource group

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

Follow the below steps to create a resource group.

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

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



Create Resource Group

1. General info & notification

Name: DemoRG_iSCSI09

Description:

Notification: Never

Email send from:

Email send to:

Email subject:

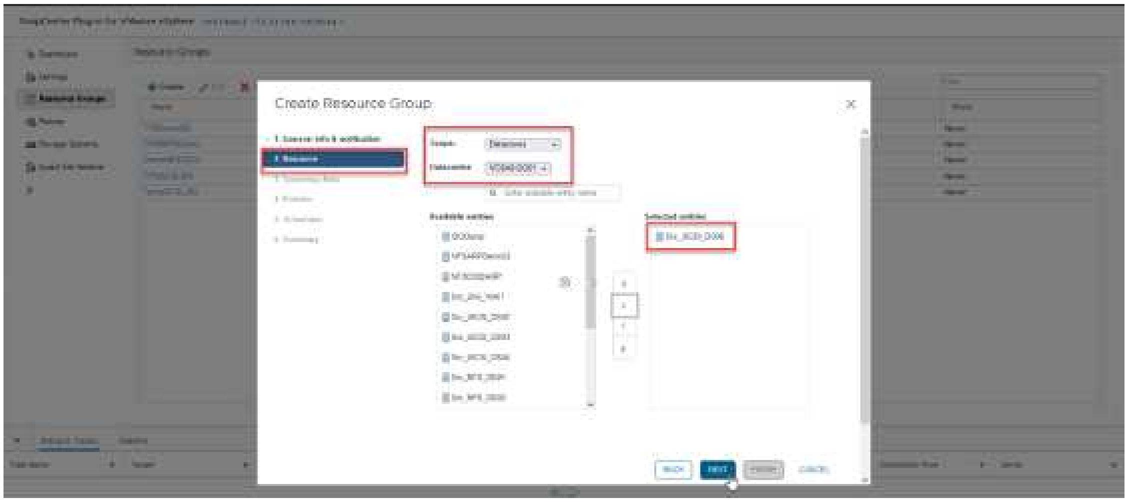
Latest Snapshot name: □ Enable _recent suffix to latest Snapshot Copy

Custom snapshot format: □ Use custom name format for Snapshot copy

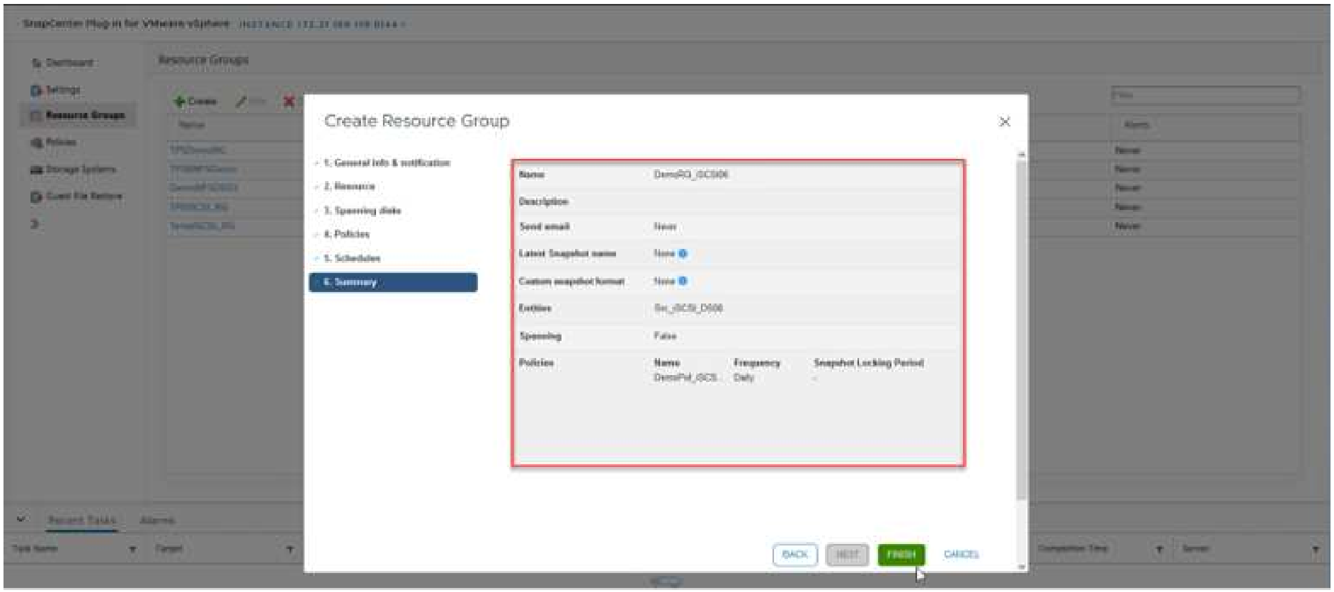
Limitations of VMware vSphere Plug-in

Warning for ONTAP 9.12.1 and below version

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



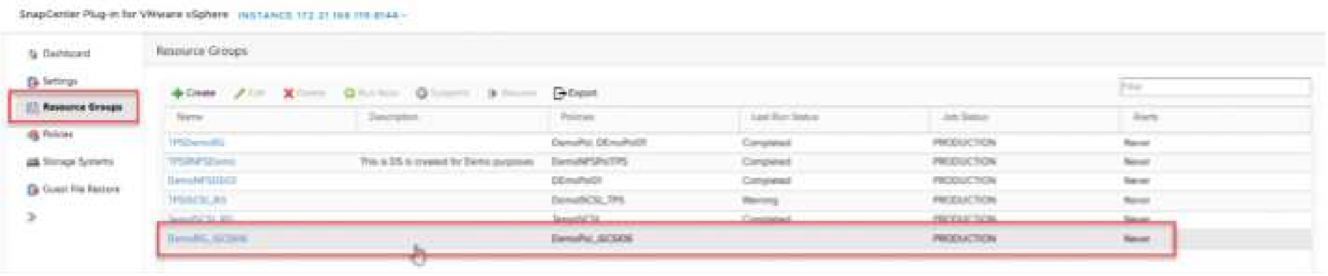
4. On the Spanning disks page, select an option for Virtual Machines with multiple VMDKs across multiple datastores
5. Next step is to associate a backup policy. Select an existing policy or create a new backup policy.
6. On the Schedules page, configure the backup schedule for each selected policy.



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

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

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

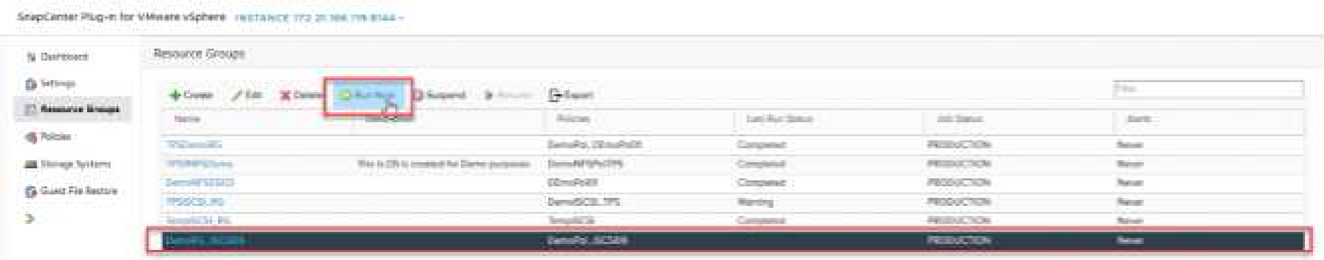


Name	Description	Policies	Last Run Status	Job Status	Alerts
TPSDemoRG		DemoPol, DEmoPol01	Completed	PRODUCTION	Never
TPSNFSDemo	This is DS is created for Demo purposes	DemoNFSPolTPS	Completed	PRODUCTION	Never
DemoNFSDS03		DEmoPol01	Completed	PRODUCTION	Never
TPSiSCSI_RG		DemoiSCSI_TPS	Warning	PRODUCTION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

Back up resource groups

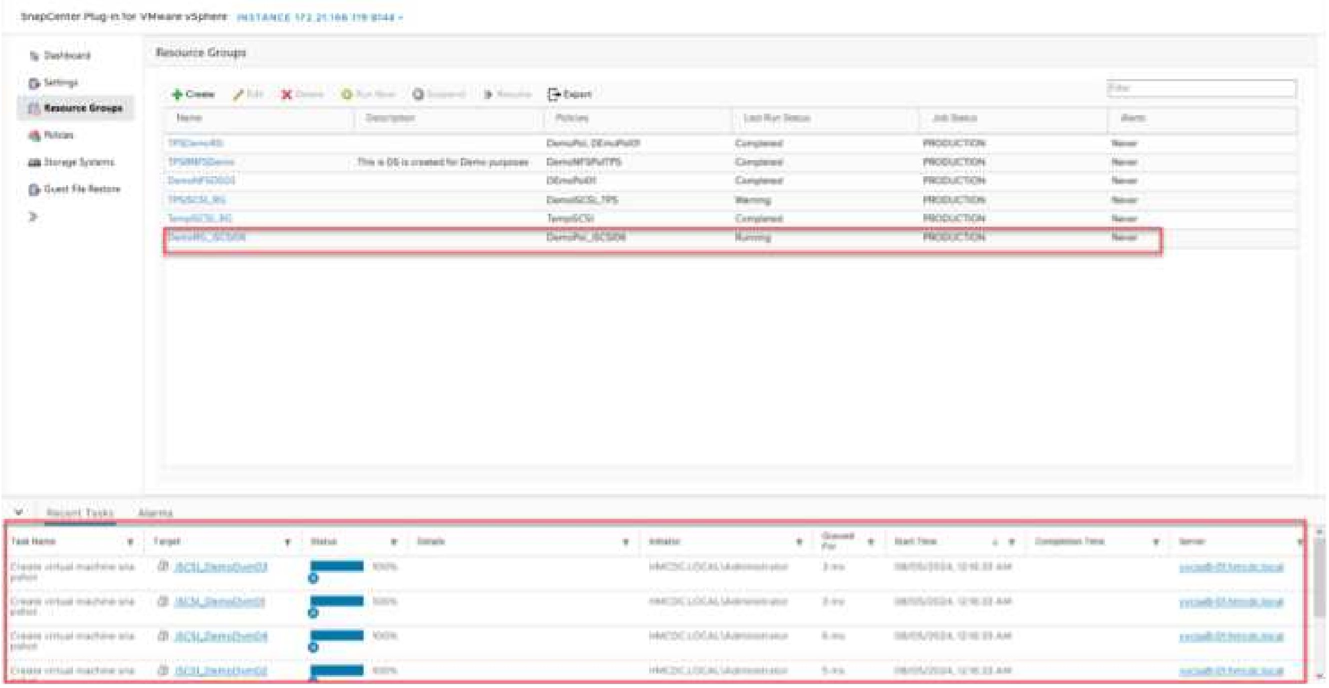
Now it’s time to trigger a backup. The backup operations are performed on all the resources defined in a resource group. If a resource group has a policy attached and a schedule configured, backups occur automatically according to the schedule.

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



Name	Description	Policies	Last Run Status	Job Status	Alerts
TPSDemoRG		DemoPol, DEmoPol01	Completed	PRODUCTION	Never
TPSNFSDemo	This is DS is created for Demo purposes	DemoNFSPolTPS	Completed	PRODUCTION	Never
DemoNFSDS03		DEmoPol01	Completed	PRODUCTION	Never
TPSiSCSI_RG		DemoiSCSI_TPS	Warning	PRODUCTION	Never
TempISCSI_RG		TempISCSI	Completed	PRODUCTION	Never
DemoRG_iSCSI04		DemoPol_iSCSI04		PRODUCTION	Never

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



Name	Description	Policies	Last Run Status	Job Status	Alerts
TPSDemoRG		DemoPol, DEmoPol01	Completed	PRODUCTION	Never
TPSNFSDemo	This is DS is created for Demo purposes	DemoNFSPolTPS	Completed	PRODUCTION	Never
DemoNFSDS03		DEmoPol01	Completed	PRODUCTION	Never
TPSiSCSI_RG		DemoiSCSI_TPS	Warning	PRODUCTION	Never
TempISCSI_RG		TempISCSI	Completed	PRODUCTION	Never
DemoRG_iSCSI04		DemoPol_iSCSI04	Running	PRODUCTION	Never

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Create virtual machine snapshot	iSCSI_DemoOvm03	100%		HMCDC.LOCAL\Administrator	3 ms	08/05/2024, 12:16:33 AM		vcsa8-01.hmcdc.local
Create virtual machine snapshot	iSCSI_DemoOvm01	100%		HMCDC.LOCAL\Administrator	3 ms	08/05/2024, 12:16:33 AM		vcsa8-01.hmcdc.local
Create virtual machine snapshot	iSCSI_DemoOvm04	100%		HMCDC.LOCAL\Administrator	6 ms	08/05/2024, 12:16:33 AM		vcsa8-01.hmcdc.local
Create virtual machine snapshot	iSCSI_DemoOvm02	100%		HMCDC.LOCAL\Administrator	5 ms	08/05/2024, 12:16:33 AM		vcsa8-01.hmcdc.local

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

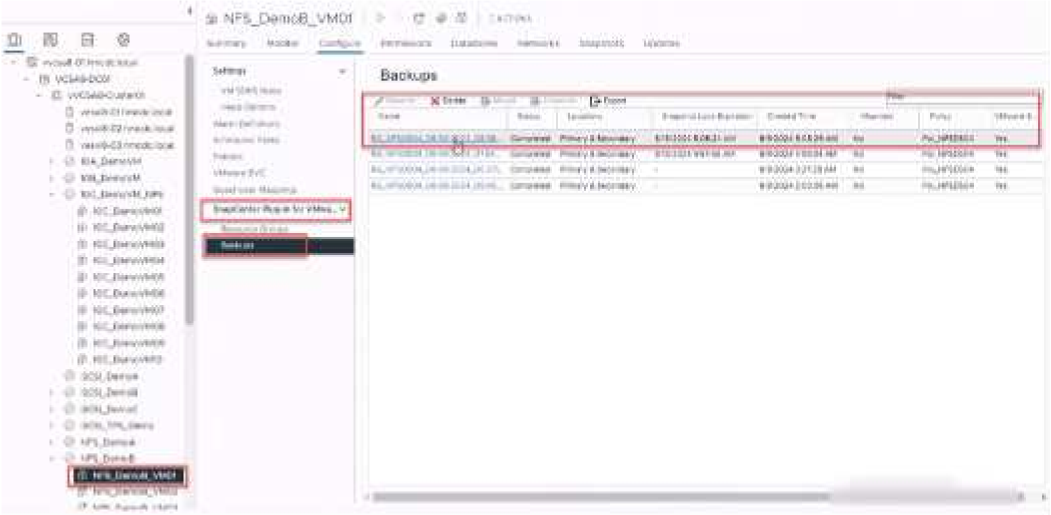
Restore VMs from backup

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.

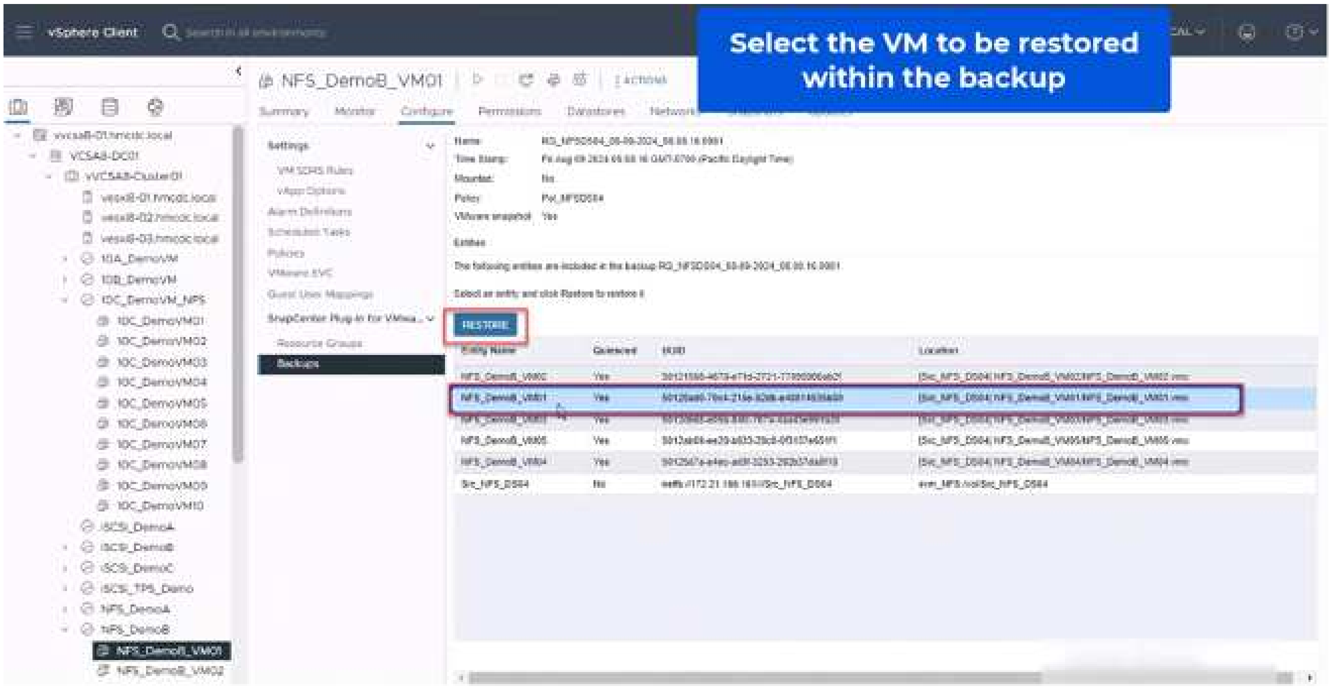
2. In the left navigation, Select the Virtual Machine, then select Configure tab, Select Backups under SnapCenter Plug-in for VMware. Click on the backup job from which the VM needs to be restored.



Backups

Name	Status	Locations	Snapshot Lock Expiration	Created Time	Mounted	Policy	VMware S
[illegible]	Completed	Primary & Secondary	[illegible]	[illegible]	No	Pol_NFSDS04	Yes
[illegible]	Completed	Primary & Secondary	[illegible]	[illegible]	No	Pol_NFSDS04	Yes
[illegible]	Completed	Primary & Secondary	-	[illegible]	No	Pol_NFSDS04	Yes
[illegible]	Completed	Primary & Secondary	-	[illegible]	No	Pol_NFSDS04	Yes

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



Select the VM to be restored within the backup

Name: RG_NFSDS04_08-09-2024_08.08.16.0981
Time Stamp: Fri Aug 09 2024 08:08:16 GMT-0700 (Pacific Daylight Time)
Mounted: No
Policy: Pol_NFSDS04
VMware snapshot: Yes

Entities

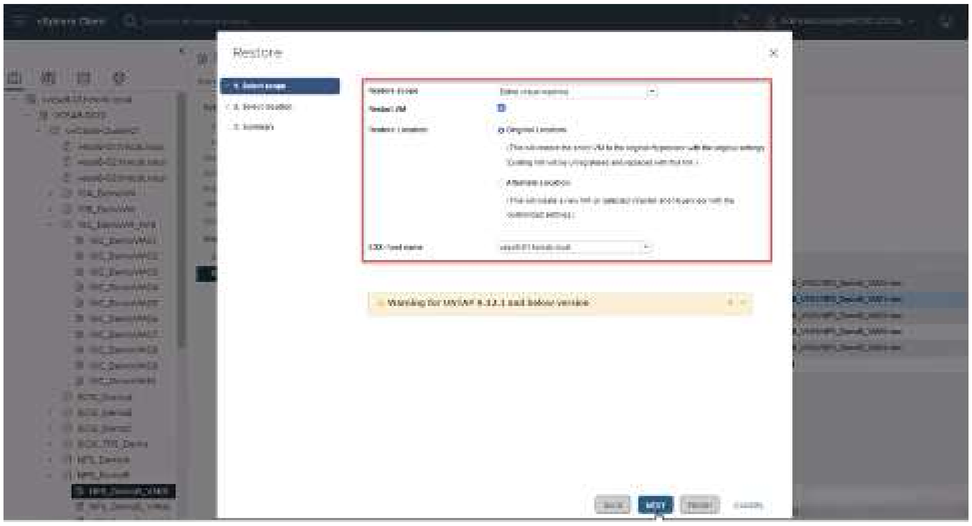
The following entities are included in the backup RG_NFSDS04_08-09-2024_08.08.16.0981

Select an entity and click Restore to restore it

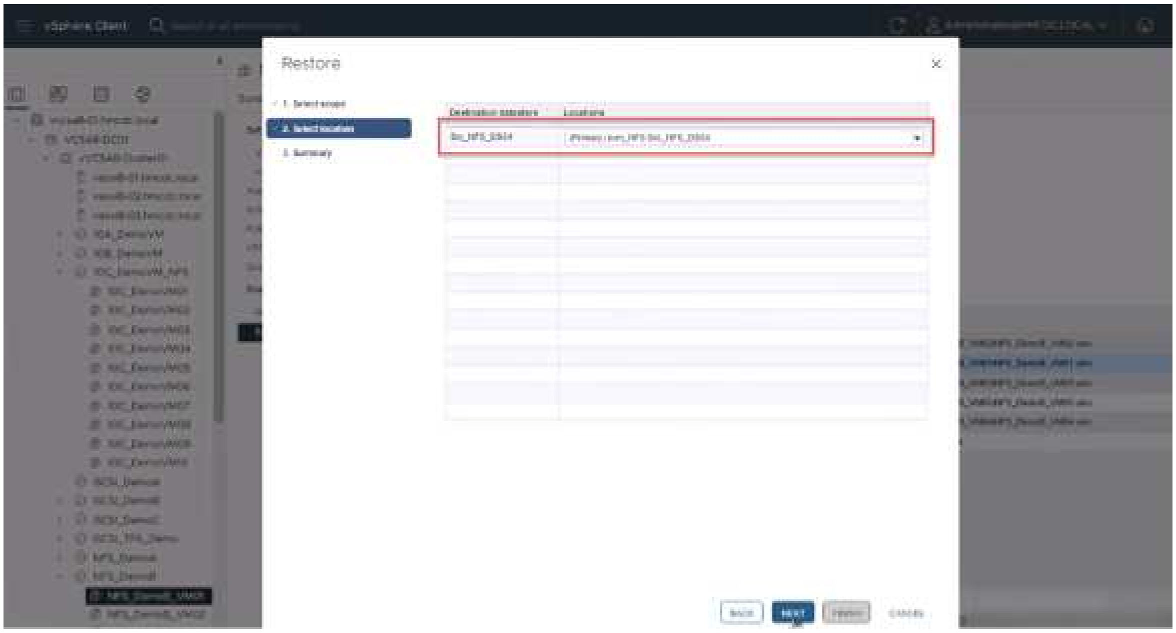
RESTORE

Entity Name	Quiesced	UUID	Location
NFS_DemoB_VM02	Yes	[illegible]	[Src_NFS_DS04] NFS_DemoB_VM02/NFS_DemoB_VM02.vmx
NFS_DemoB_VM01	Yes	[illegible]	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_DemoB_VM01.vmx
NFS_DemoB_VM03	Yes	[illegible]	[Src_NFS_DS04] NFS_DemoB_VM03/NFS_DemoB_VM03.vmx
NFS_DemoB_VM05	Yes	[illegible]	[Src_NFS_DS04] NFS_DemoB_VM05/NFS_DemoB_VM05.vmx
NFS_DemoB_VM04	Yes	[illegible]	[Src_NFS_DS04] NFS_DemoB_VM04/NFS_DemoB_VM04.vmx
Src_NFS_DS04	No	netfs://172.21.166.161//Src_NFS_DS04	svm_NFS:/vol/Src_NFS_DS04

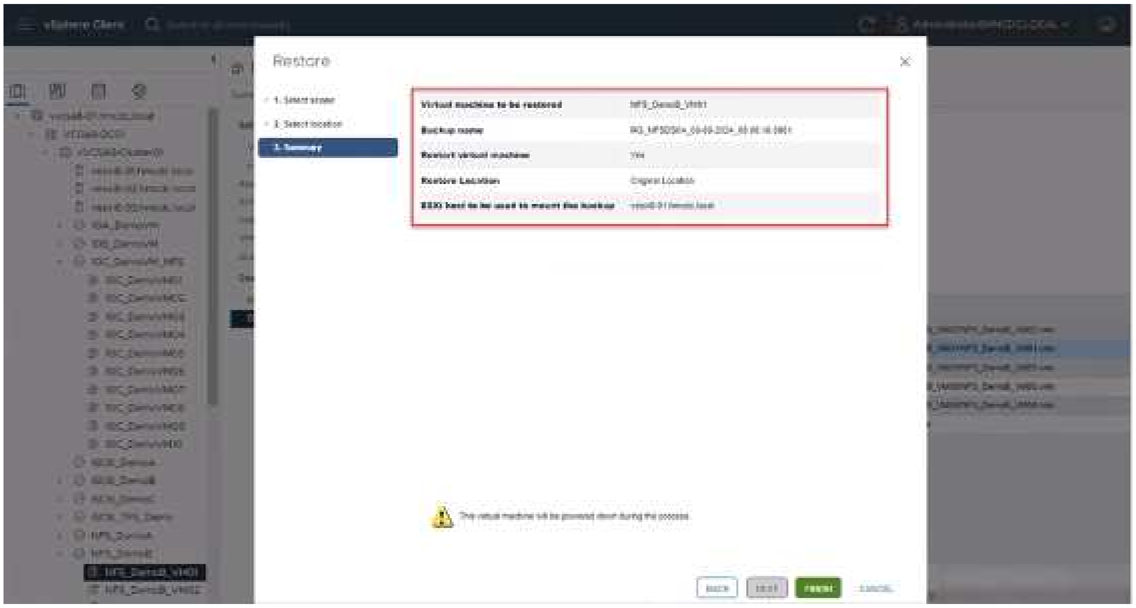
4. On the Select Scope page, select Entire Virtual Machine in the Restore scope field, then select Restore location, and then enter the destination ESXi information where the backup should be mounted. Enable Restart VM checkbox if the VM needs to be powered on after the restore operation.



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



6. Review the Summary page and then select Finish.



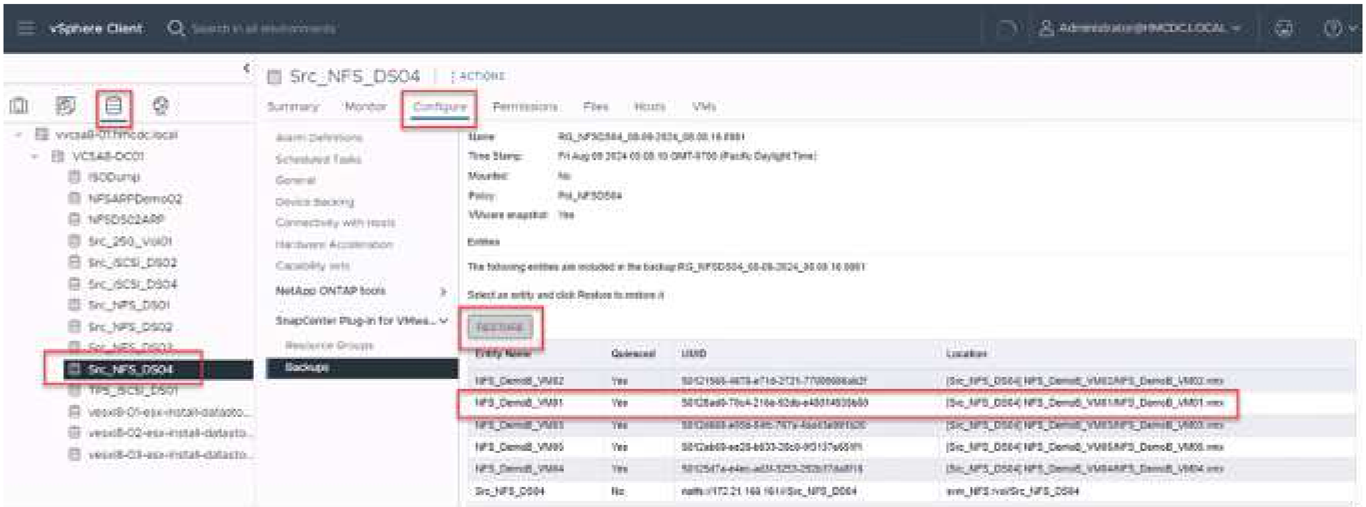
Virtual machine to be restored	NFS_DemoB_VM01
Backup name	RG_NFSDS04_08-09-2024_08.08.16.0861
Restart virtual machine	Yes
Restore Location	Original Location
ESXi host to be used to mount the backup	vesxi8-01.hmcdc.local

⚠ The virtual machine will be powered down during the process.

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

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

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



Name: RG_NFSDS04_08-09-2024_08.08.16.0861
Time Stamp: Fri Aug 09 2024 08:08:16 GMT-0700 (Pacific Daylight Time)
Mounted: No
Policy: Pol_NFSDS04
VMware snapshot: Yes

Entities

The following entities are included in the backup:RG_NFSDS04_08-09-2024_08.08.16.0861

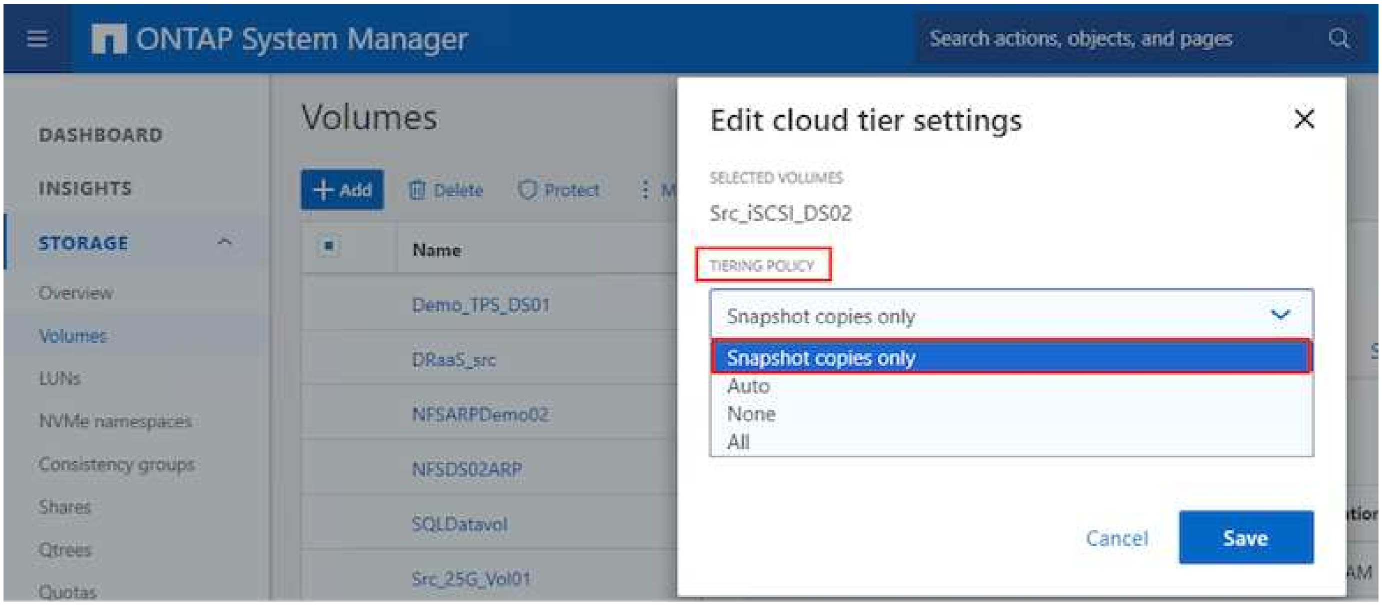
Select an entity and click Restore to restore it

Entity Name	Quiesced	UUID	Location
NFS_DemoB_VM02	Yes	50121565-4678-a71d-2121-77000008a62f	[Src_NFS_DS04] NFS_DemoB_VM02/NFS_DemoB_VM02.vmx
NFS_DemoB_VM01	Yes	50128ad9-70c4-216e-92db-e48014833b60	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_DemoB_VM01.vmx
NFS_DemoB_VM03	Yes	50126688-a05b-84fc-767a-4ba43a991520	[Src_NFS_DS04] NFS_DemoB_VM03/NFS_DemoB_VM03.vmx
NFS_DemoB_VM05	Yes	5012ab69-ee28-b633-28c9-9f3137a6591f	[Src_NFS_DS04] NFS_DemoB_VM05/NFS_DemoB_VM05.vmx
NFS_DemoB_VM04	Yes	50125d7a-e4ec-a03f-5253-292b7f4a8f16	[Src_NFS_DS04] NFS_DemoB_VM04/NFS_DemoB_VM04.vmx
Src_NFS_DS04	No	netfs://172.21.168.161//Src_NFS_DS04	svm_NFS:/vol/Src_NFS_DS04

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

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

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



Edit cloud tier settings

SELECTED VOLUMES

Src_iSCSI_DS02

TIERING POLICY

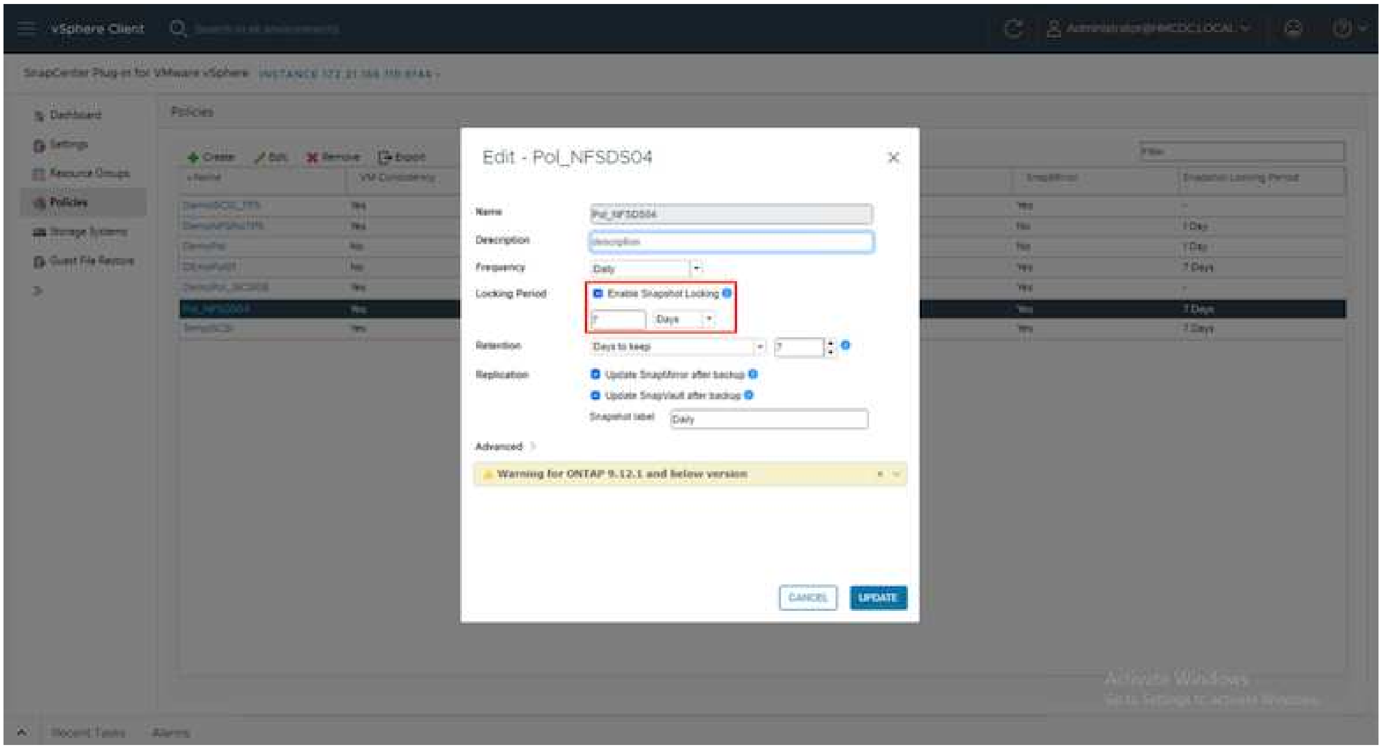
Snapshot copies only

View detailed guidance for VMware vSphere with ONTAP.

Ransomware Protection

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

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



Edit - Pol_NFSDS04

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

Warning for ONTAP 9.12.1 and below version

CANCEL UPDATE

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

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

Migration

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

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

- View detailed guidance for Migrate Workloads to FSx 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 NetApp Disaster Recovery for VMFS Datastores

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

For those customers looking to use VMware Cloud on any hyperscalar as the disaster recovery target, ONTAP storage powered datastores (Azure NetApp Files, FSx 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 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.

Use nConnect on NFS v3 datastores to improve datastore performance

Use the NFS nConnect feature to improve datastore performance in VMware vSphere 8 environments. This procedure includes hosting VMs per NFS datastore, boosting NFS datastore performance, and configuring a higher tier for VM and container based applications.

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

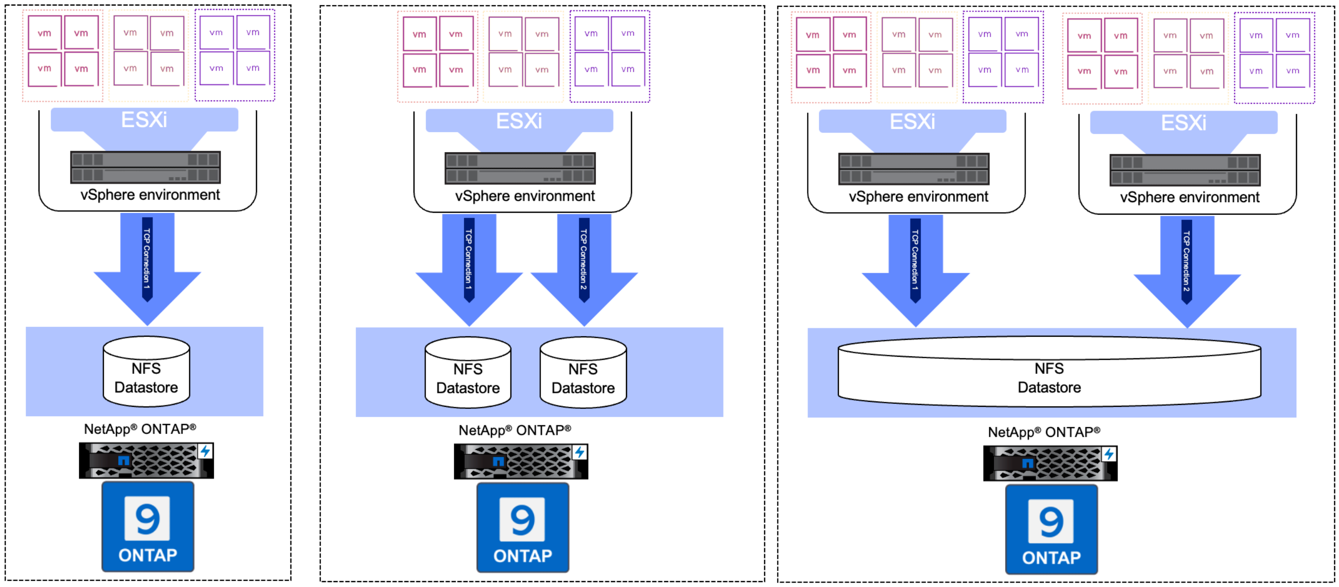
- Host more virtual machines per NFS datastore on the same host.
- Boost NFS datastore performance.
- Provide an option to offer service at a higher tier for VM and Container based applications.

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

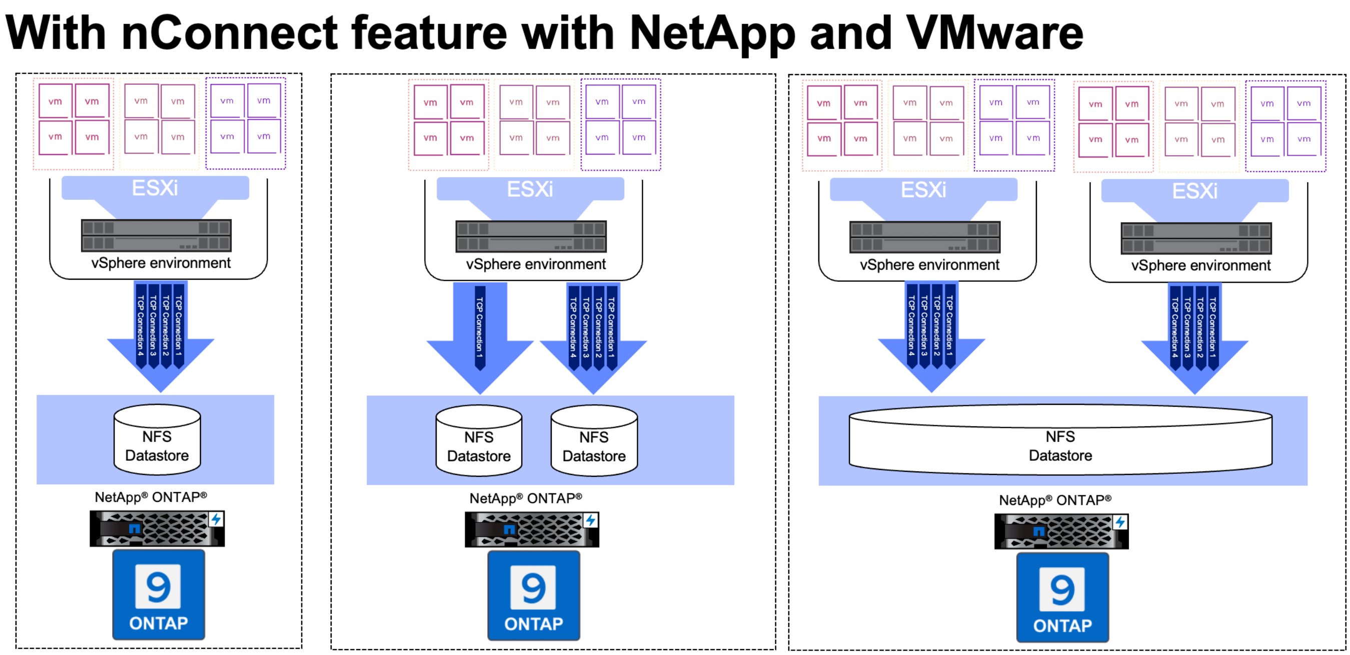
To address the performance limitations of single connection of NFS datastore, additional datastores are mounted or additional hosts are added to increase the connection.



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.



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. Have to unmount the datastore to decrease the 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.

Configure NFS datastores for vSphere 8 using ONTAP tools for VMware vSphere

Deploy ONTAP tools for VMware vSphere 10 to configure NFS datastores in a vSphere 8 environment. This procedure includes creating SVMs and LIFs for NFS traffic, setting up ESXi host networking, and registering ONTAP tools with your vSphere cluster.

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

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

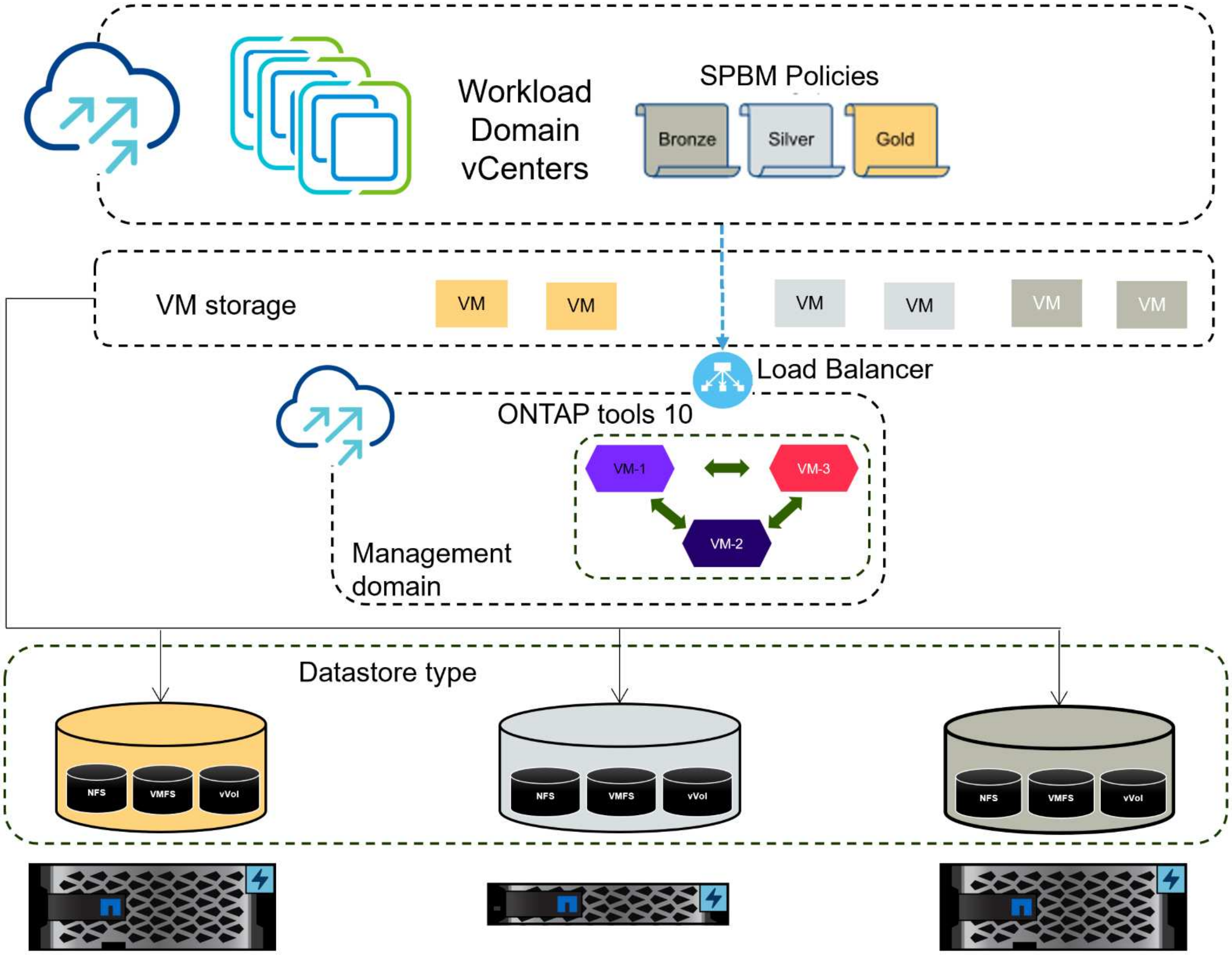
Solution Overview

This scenario covers the following high level steps:

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

Architecture

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



Prerequisites

This solution requires the following components and configurations:

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

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

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

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

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

Deployment Steps

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

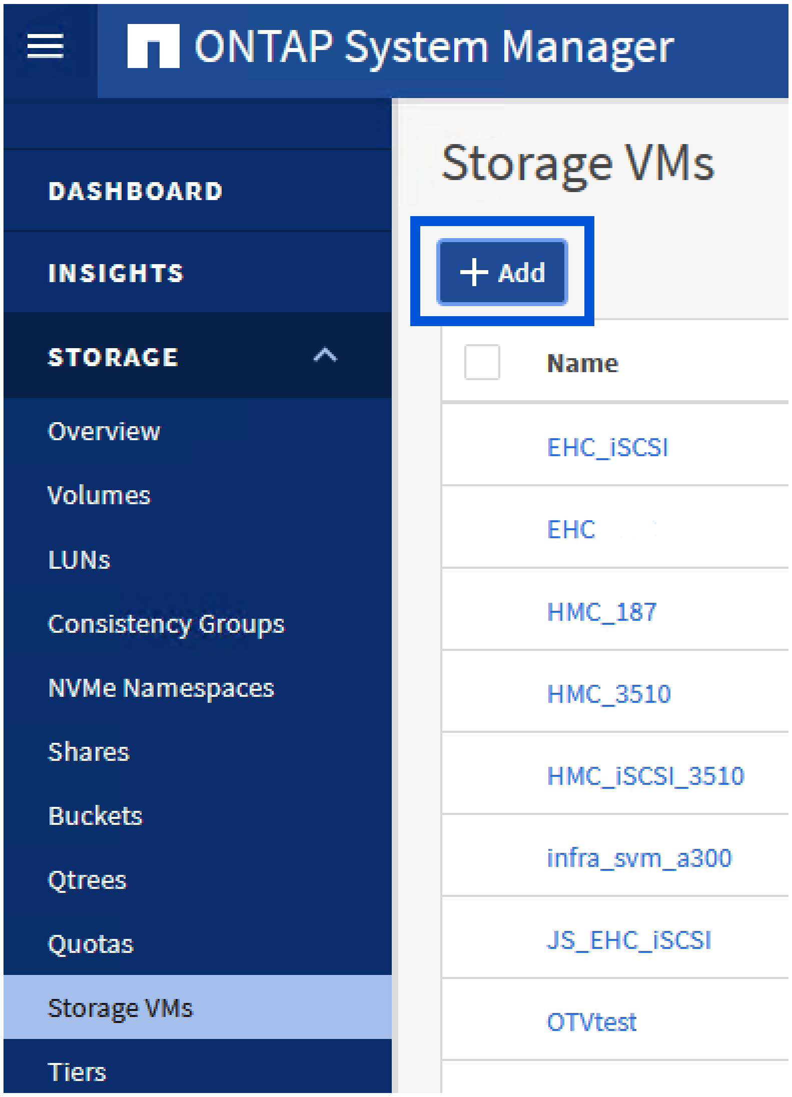
Create SVM and LIFs on ONTAP storage system

The following step is performed in ONTAP System Manager.

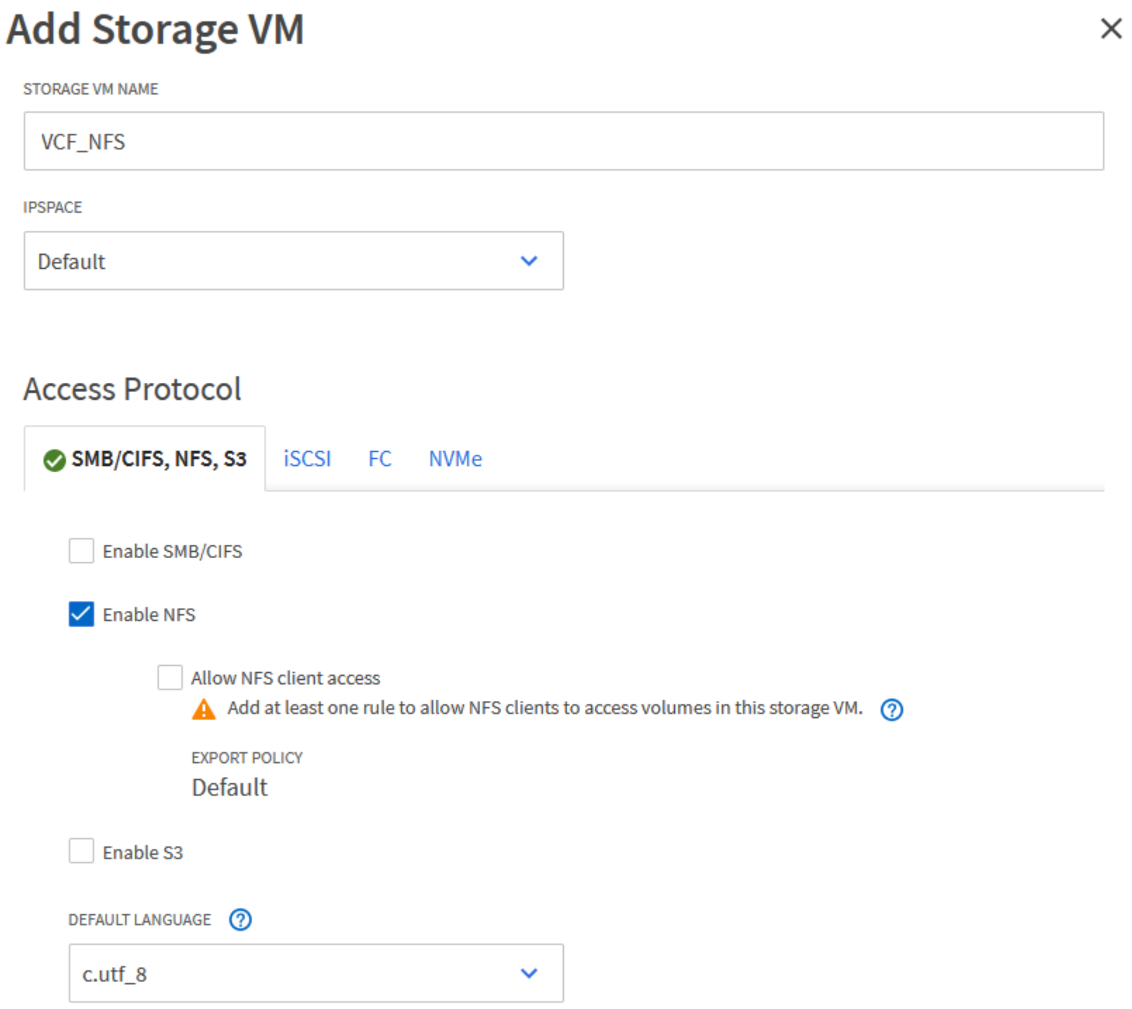
Create the storage VM and LIFs

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

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



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



Add Storage VM

STORAGE VM NAME

VCF_NFS

IPSPACE

Default

Access Protocol

□ Enable SMB/CIFS

☑ Enable NFS

□ Allow NFS client access

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

EXPORT POLICY

Default

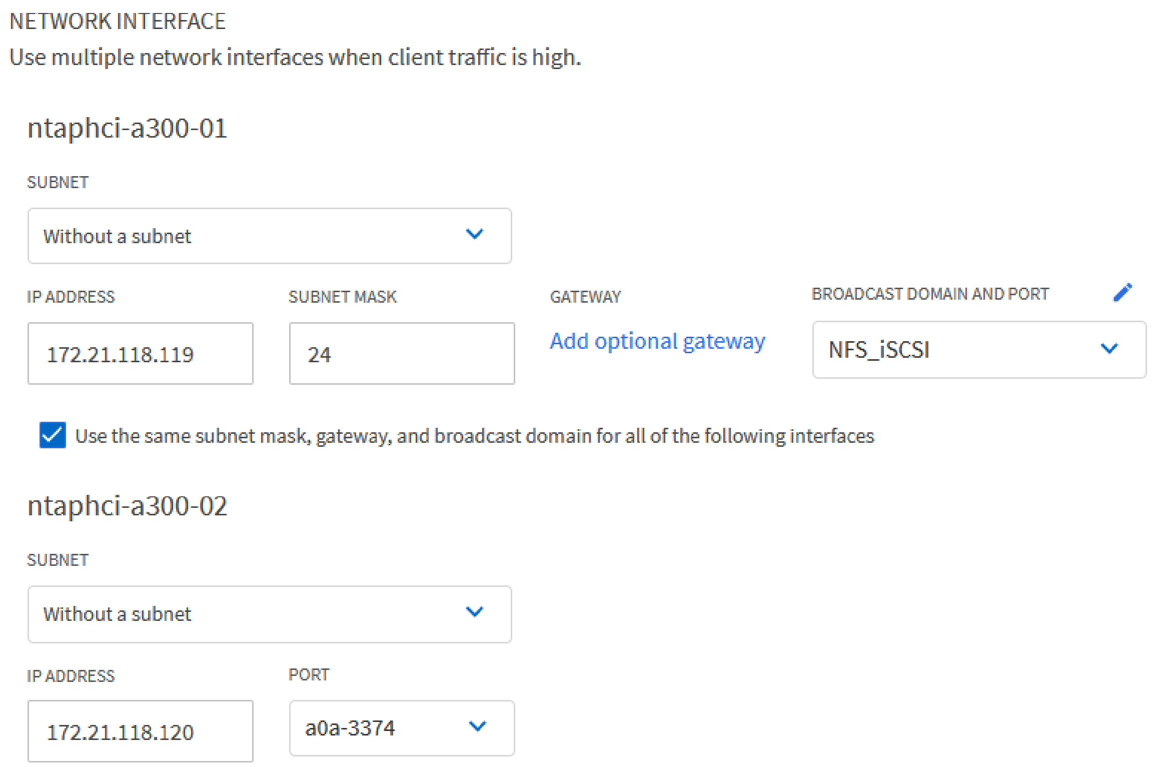
□ Enable S3

DEFAULT LANGUAGE

c.utf_8

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

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



NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET: Without a subnet

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

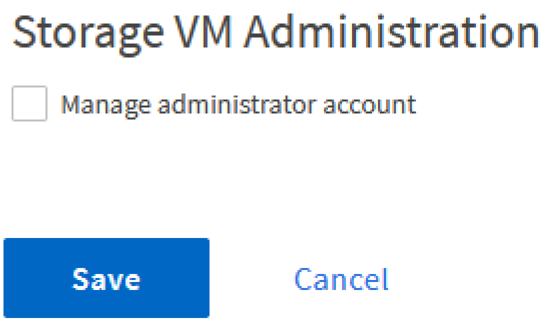
☑ Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

ntaphci-a300-02

SUBNET: Without a subnet

IP ADDRESS	PORT
172.21.118.120	a0a-3374

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



Storage VM Administration

□ Manage administrator account

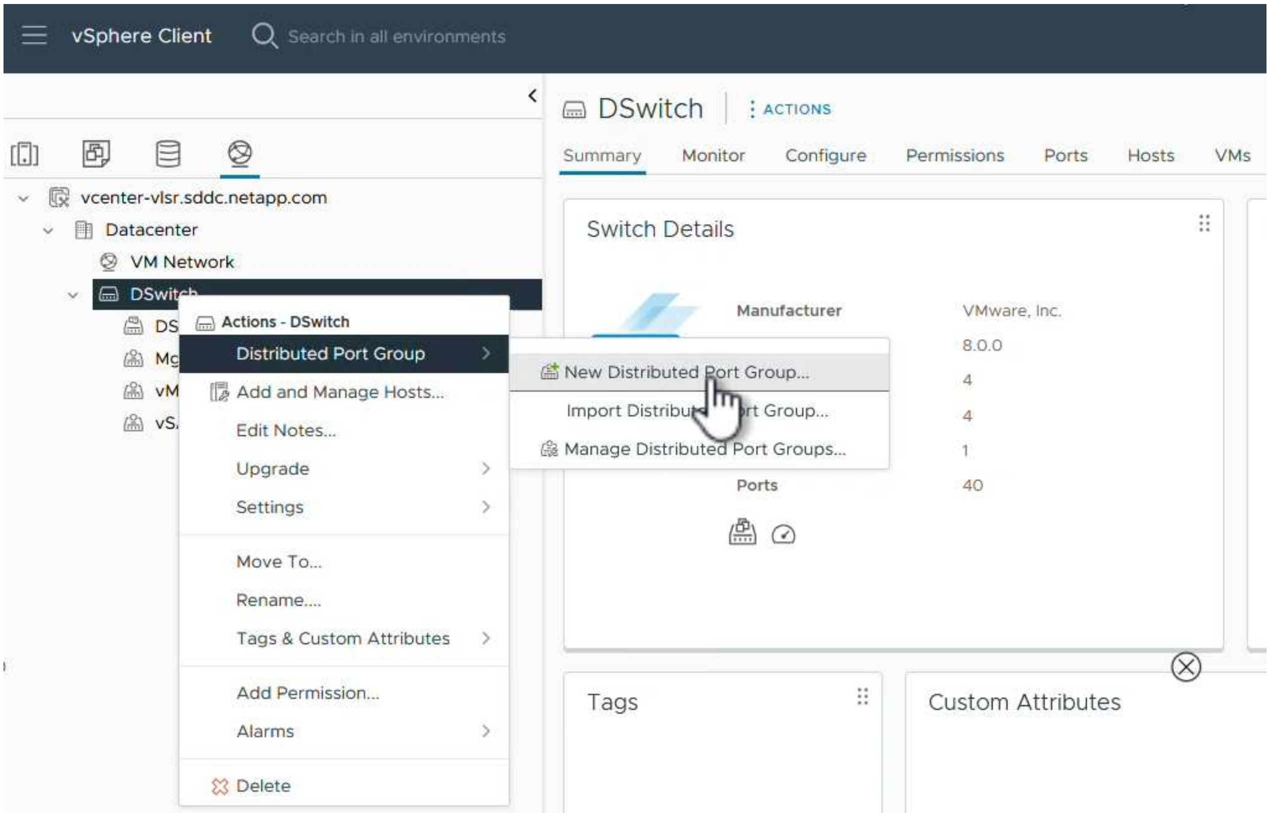
Set up networking for NFS on ESXi hosts

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

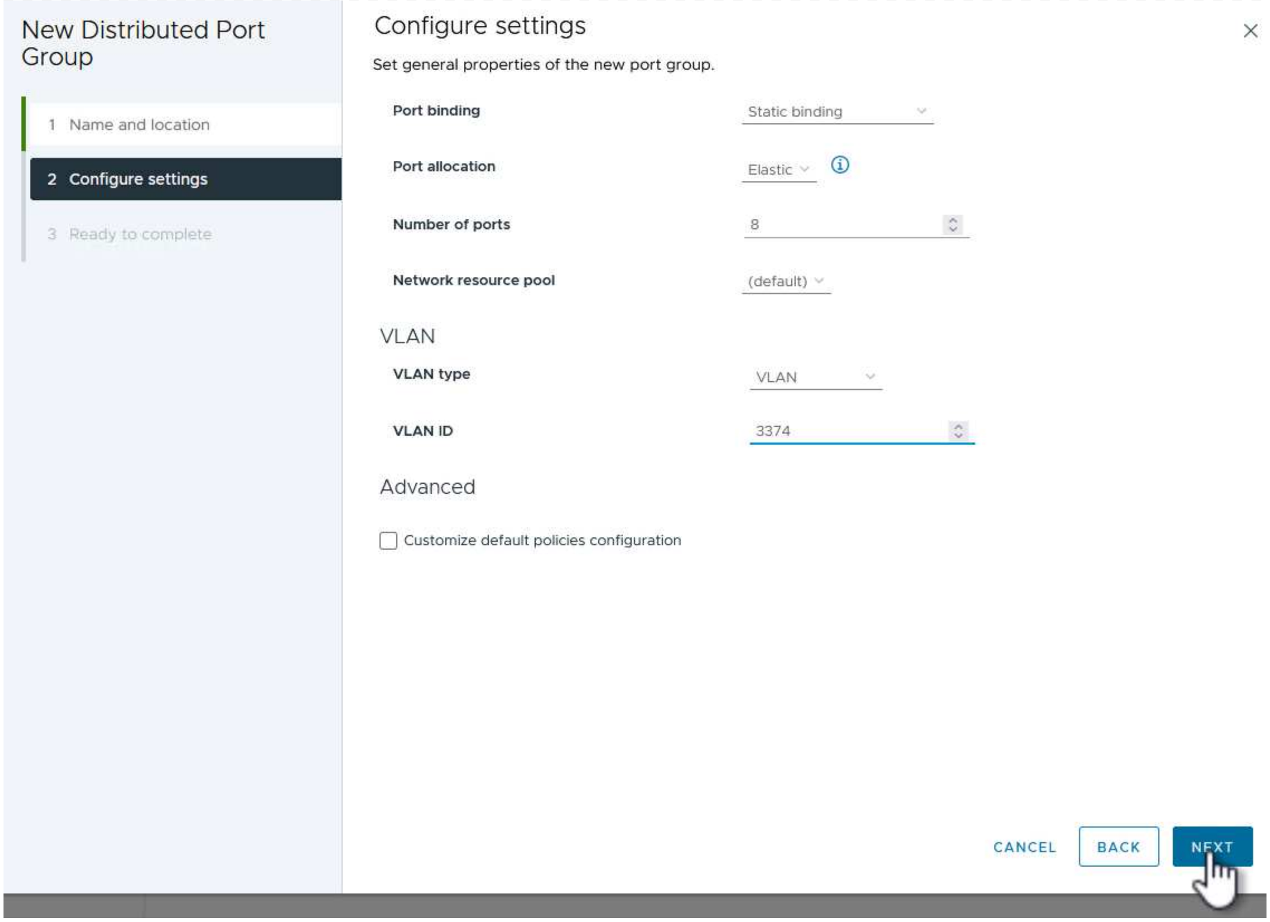
Create a Distributed Port Group for NFS traffic

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

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



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



New Distributed Port Group

Configure settings

Set general properties of the new port group.

Port binding: Static binding

Port allocation: Elastic

Number of ports: 8

Network resource pool: (default)

VLAN

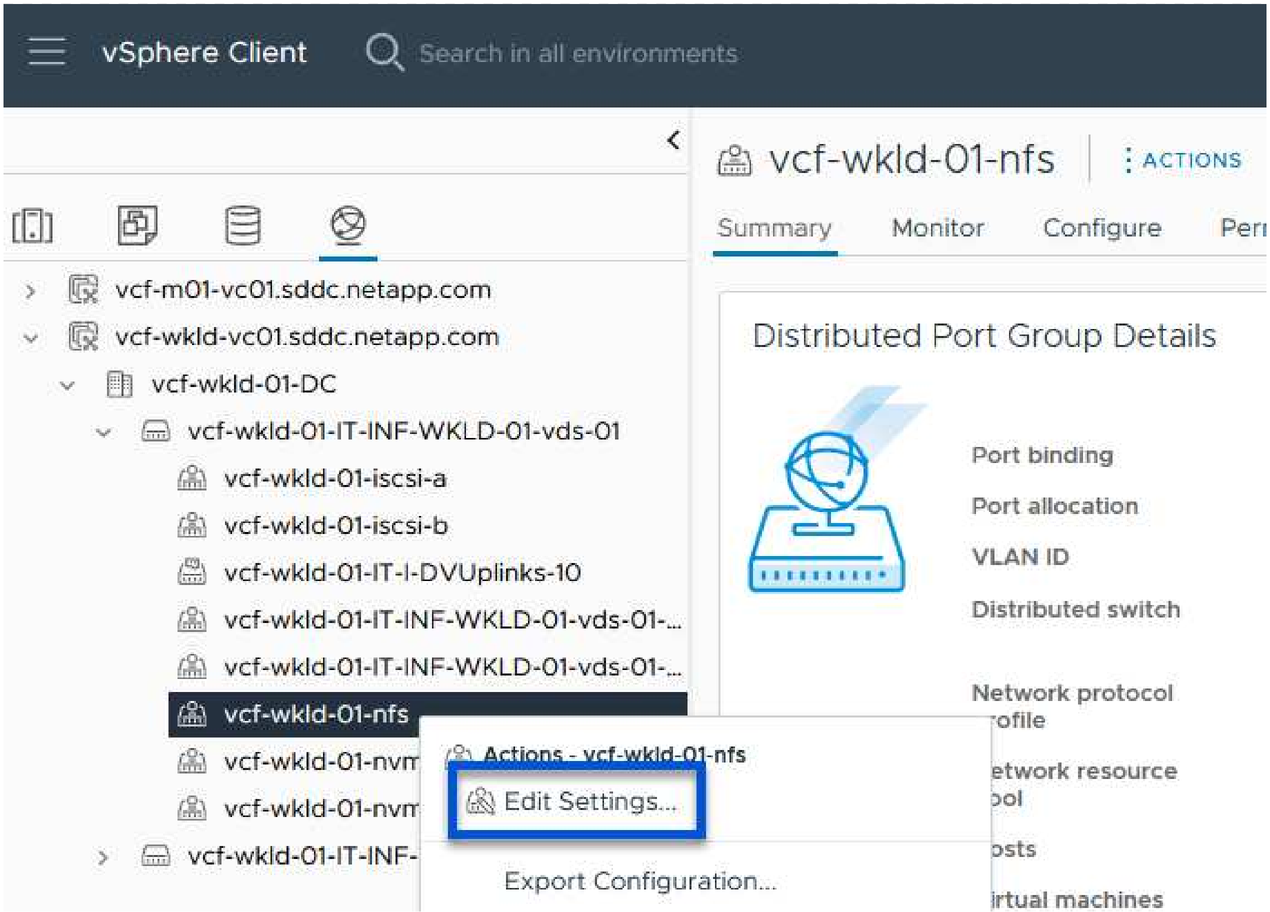
VLAN type: VLAN

VLAN ID: 3374

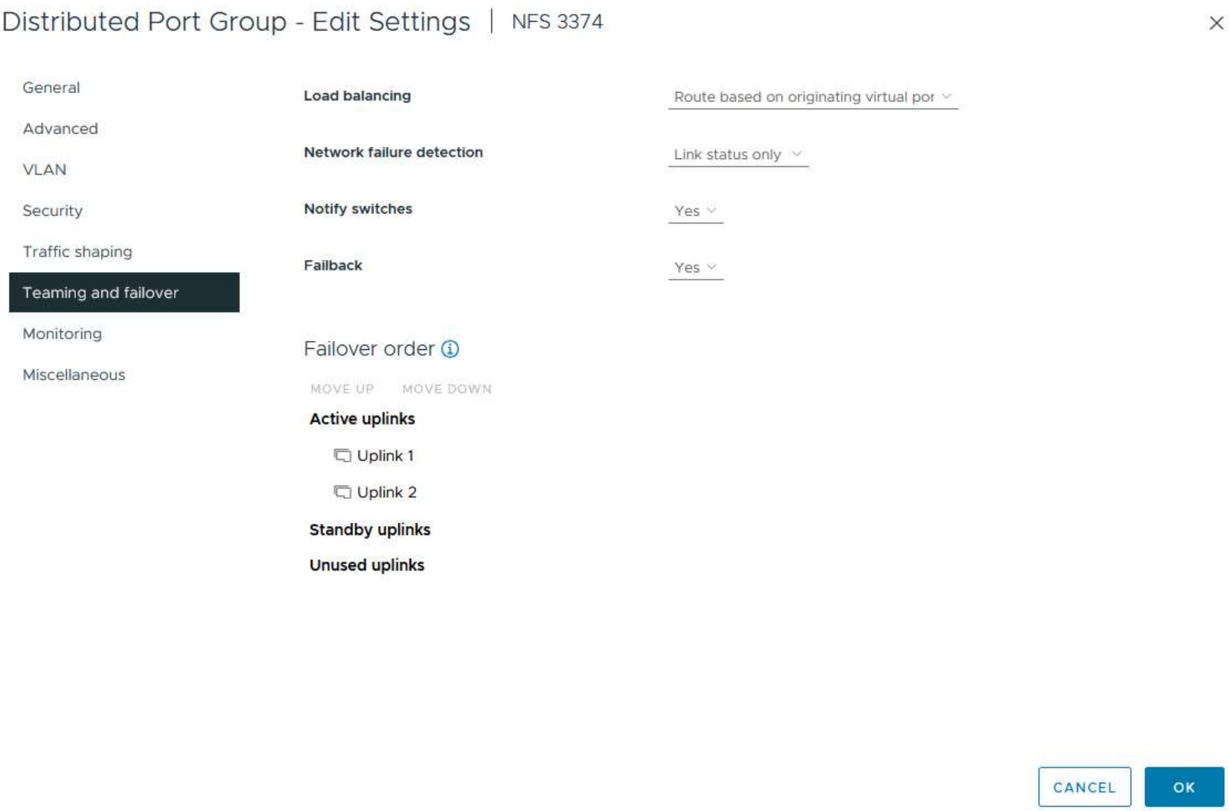
Advanced

□ Customize default policies configuration

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



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



Distributed Port Group - Edit Settings | NFS 3374

Load balancing: Route based on originating virtual por

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

Failover order

Active uplinks

- Uplink 1
- Uplink 2

Standby uplinks

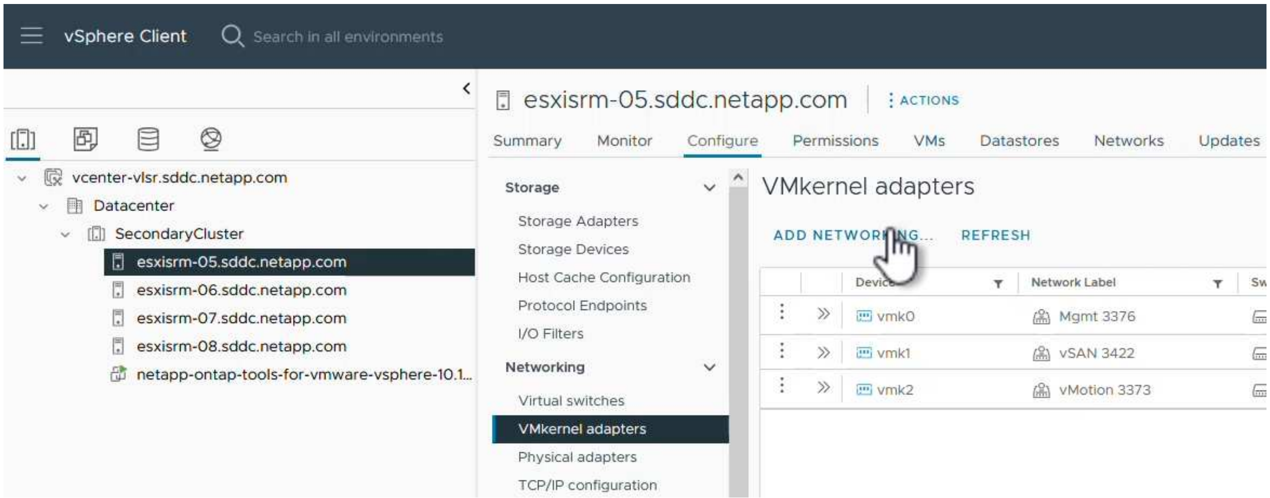
Unused uplinks

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

Create a VMkernel adapter on each ESXi host

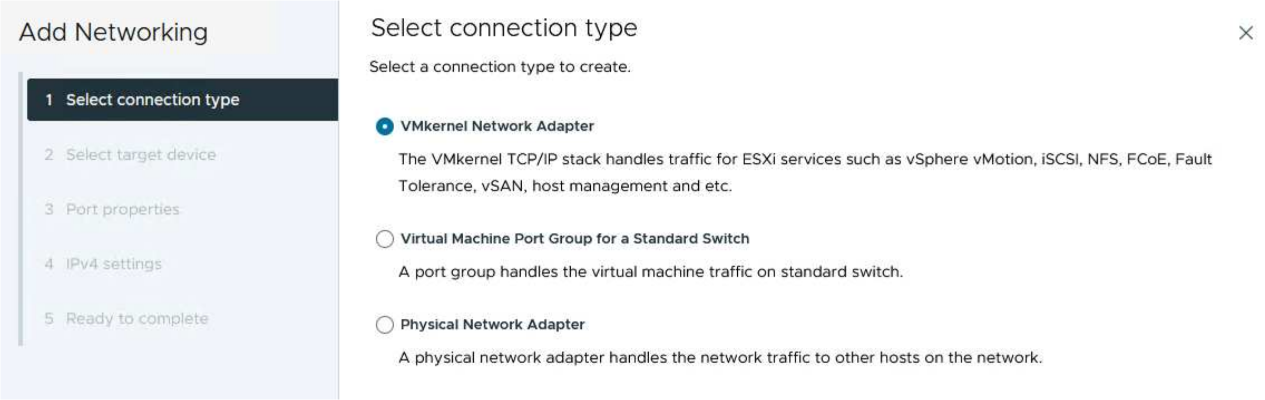
Repeat this process on each ESXi host in the workload domain.

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



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

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



Select connection type

Select a connection type to create.

● VMkernel Network Adapter

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

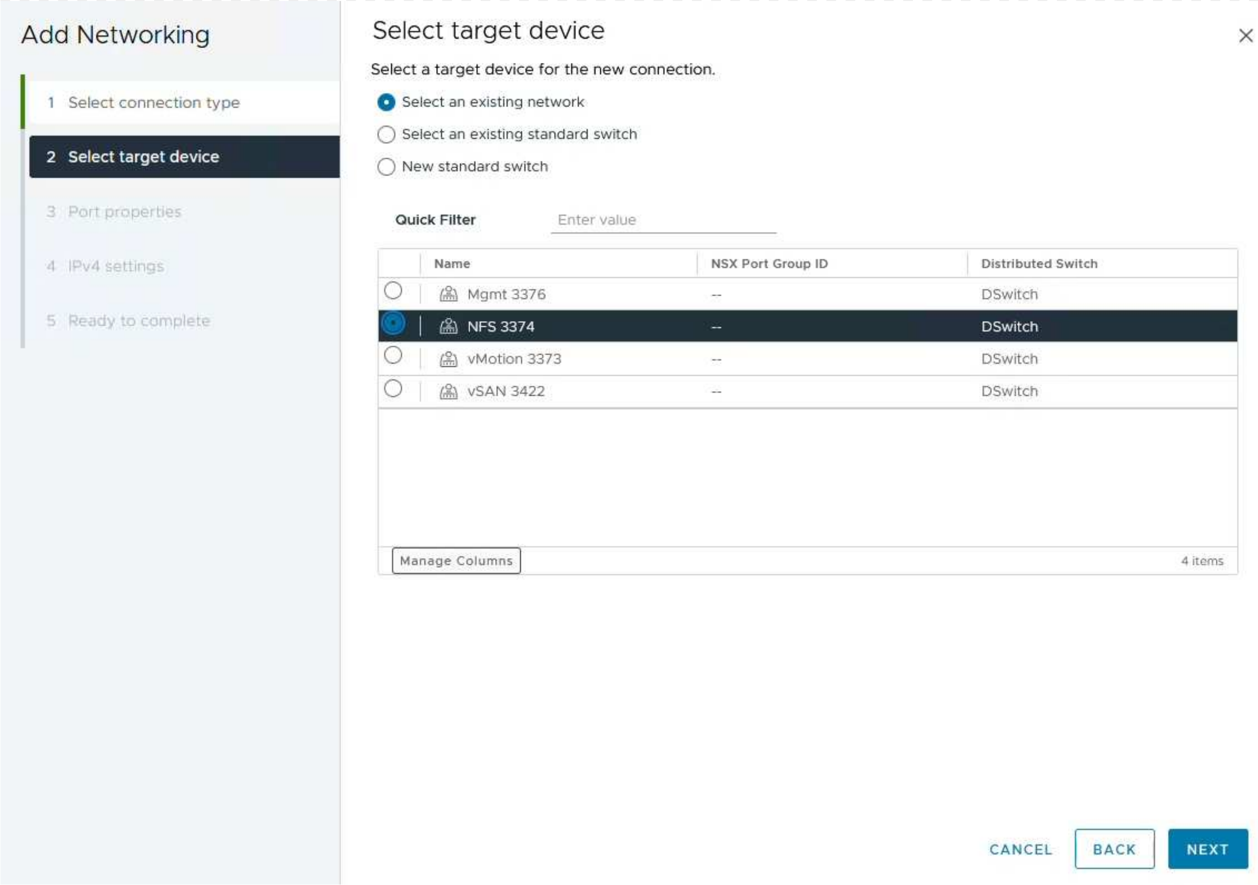
○ Virtual Machine Port Group for a Standard Switch

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

○ Physical Network Adapter

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

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



Select target device

Select a target device for the new connection.

● Select an existing network

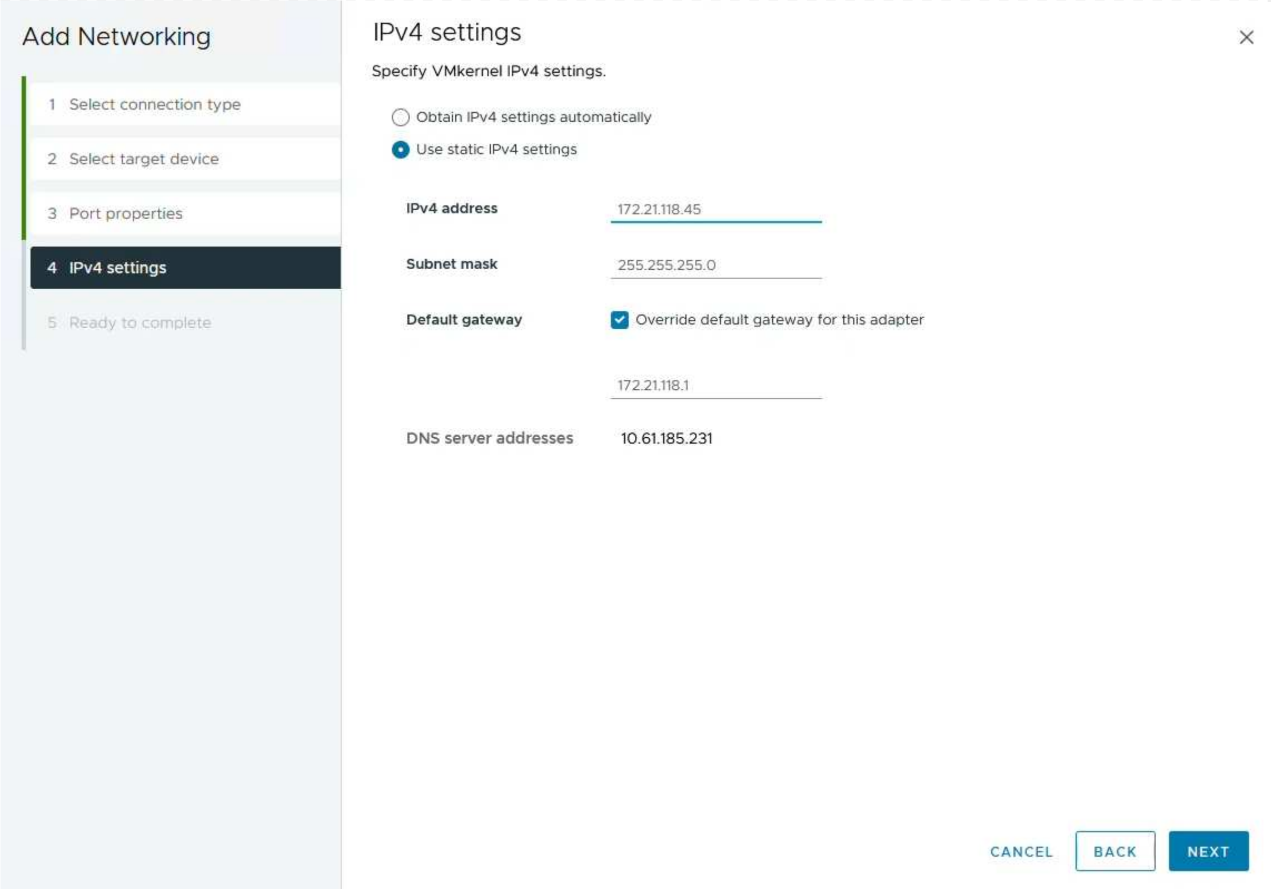
○ Select an existing standard switch

○ New standard switch

Quick Filter: Enter value

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

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.



IPv4 settings

Specify VMkernel IPv4 settings.

○ Obtain IPv4 settings automatically

● Use static IPv4 settings

IPv4 address 172.21.118.45

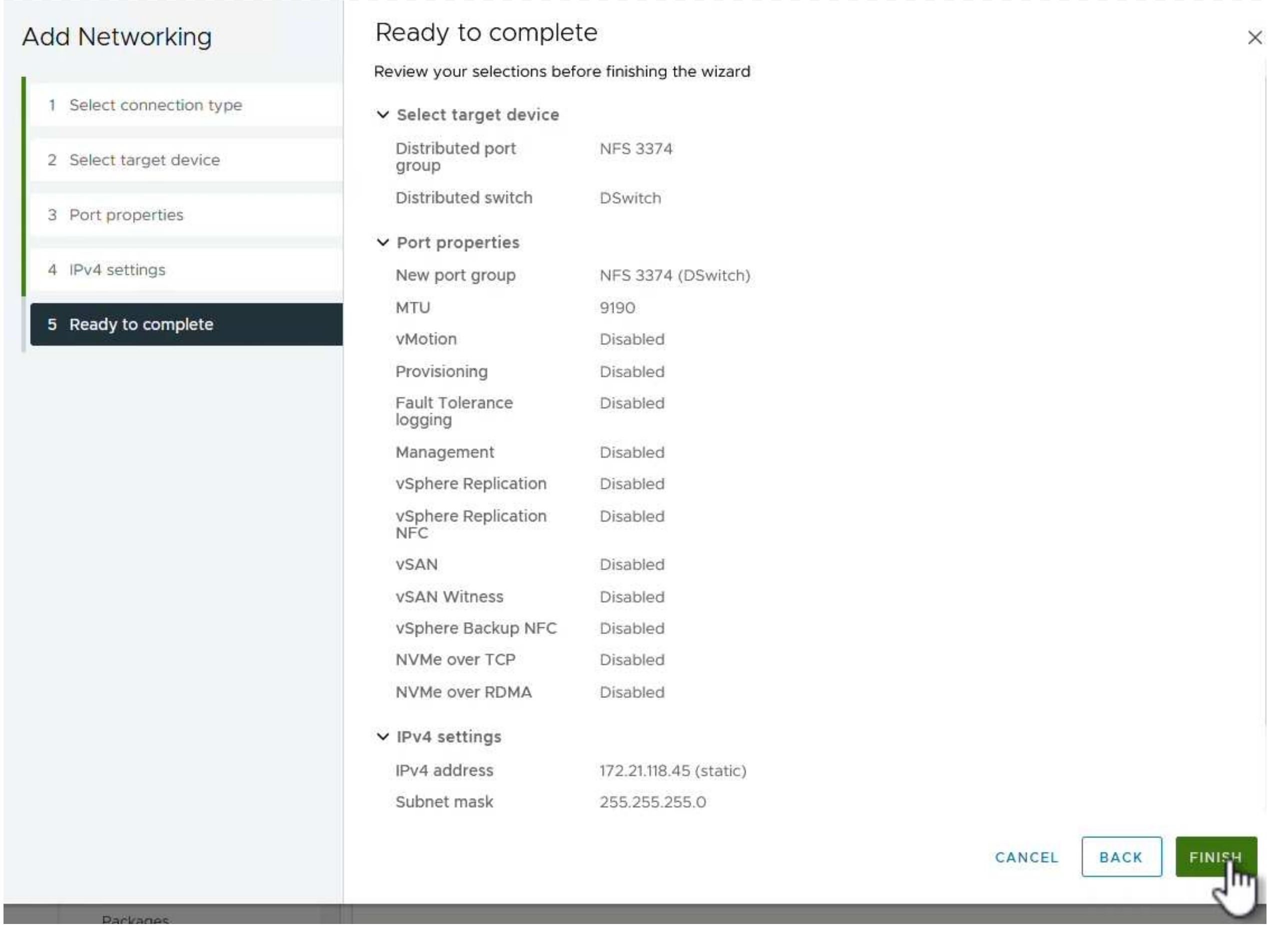
Subnet mask 255.255.255.0

Default gateway ☑ Override default gateway for this adapter

172.21.118.1

DNS server addresses 10.61.185.231

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



Ready to complete

Review your selections before finishing the wizard

Select target device

Distributed port group	NFS 3374
Distributed switch	DSwitch

Port properties

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

IPv4 settings

IPv4 address	172.21.118.45 (static)
Subnet mask	255.255.255.0

Deploy and use ONTAP tools 10 to configure storage

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

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

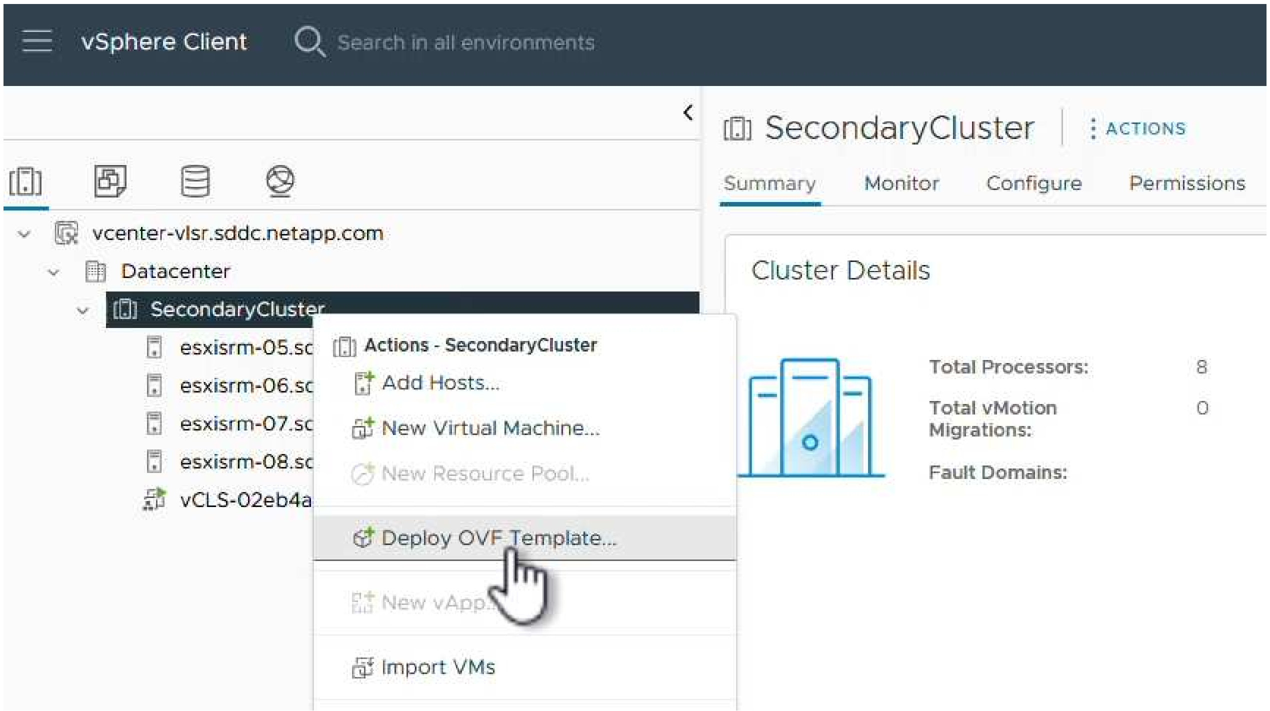
Deploy ONTAP tools for VMware vSphere 10

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

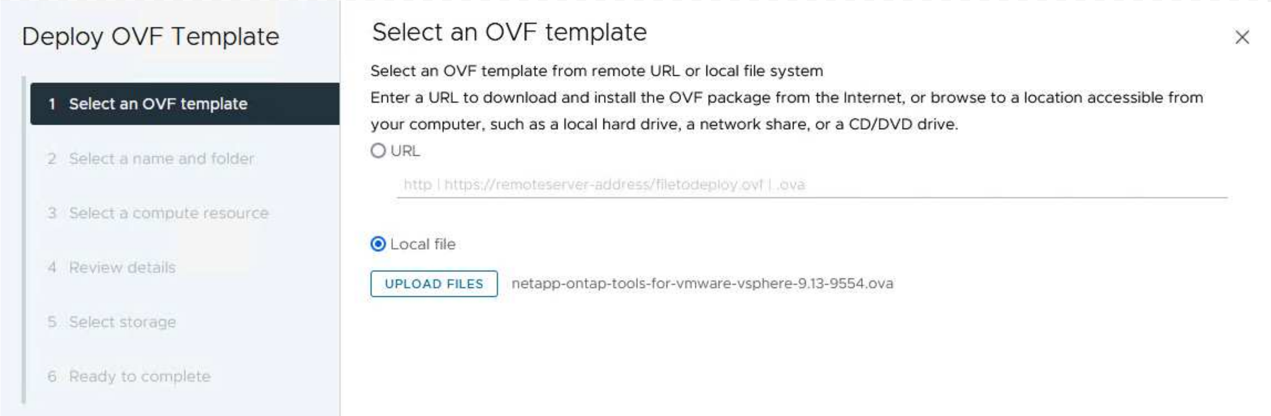
> ⓘ In a non-HA deployment scenario, three available IP addresses are required. One IP address is allocated for the load balancer, another for the Kubernetes control plane, and the remaining one for the node. In an HA deployment, two additional IP addresses are necessary for the second and third nodes,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

Complete the following to Deploy ONTAP tools for VMware vSphere:

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



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



Deploy OVF Template

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

Select an OVF template

Select an OVF template from remote URL or local file system

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

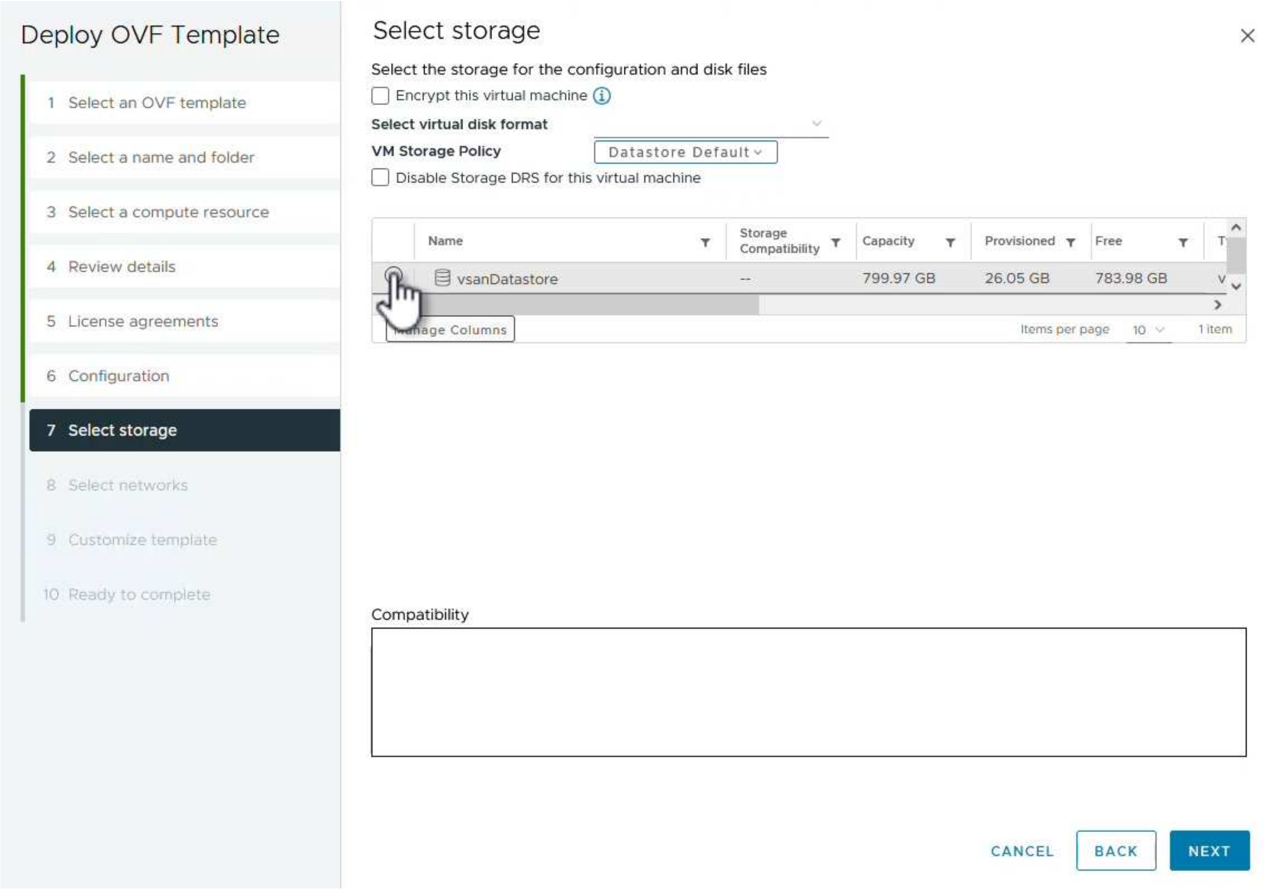
○ URL

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

● Local file

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

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



Deploy OVF Template

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

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine

Select virtual disk format

VM Storage Policy: Datastore Default

□ Disable Storage DRS for this virtual machine

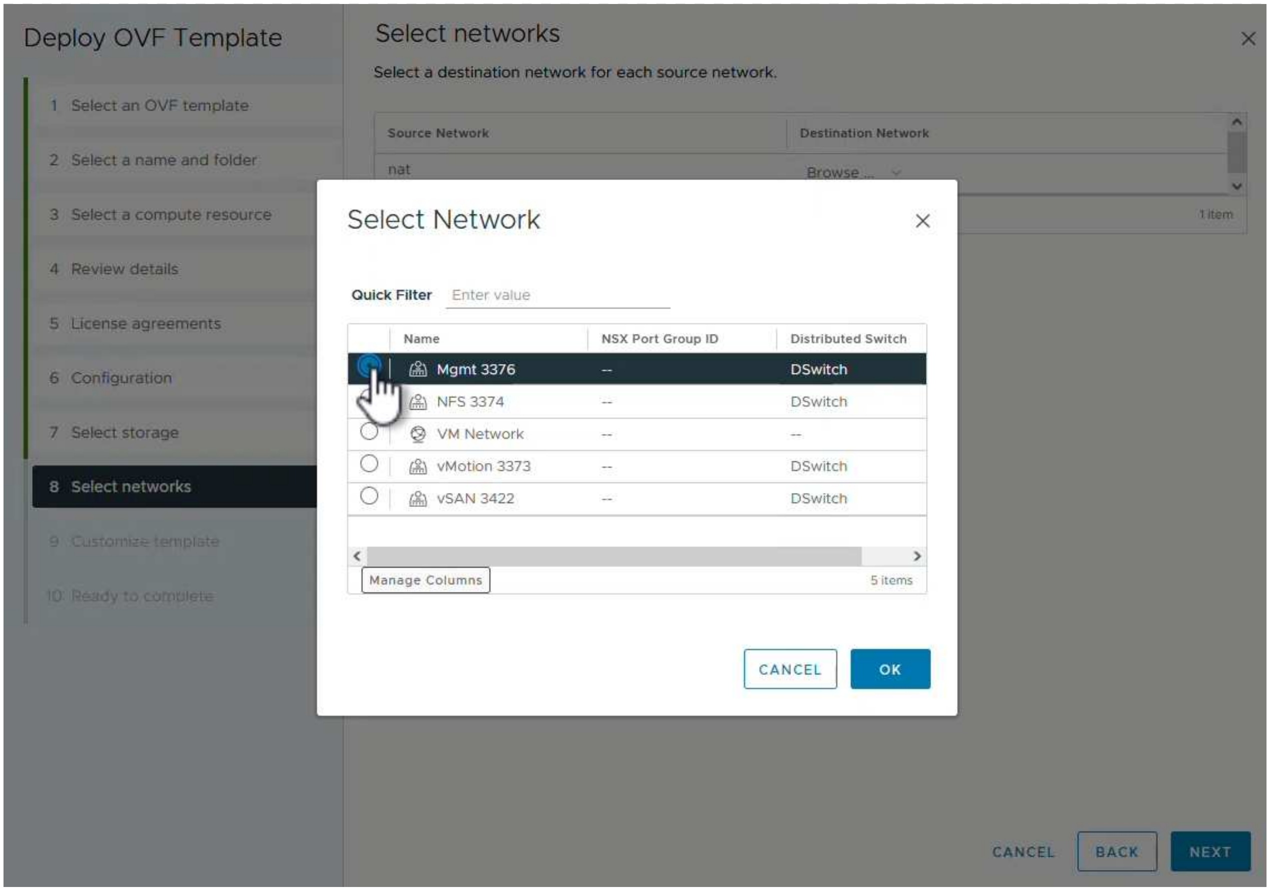
	Name	Storage Compatibility	Capacity	Provisioned	Free	T
○	vsanDatastore	--	799.97 GB	26.05 GB	783.98 GB	V

Manage Columns Items per page 10 1 item

Compatibility

CANCEL BACK NEXT

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



Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	Browse ...

1 item

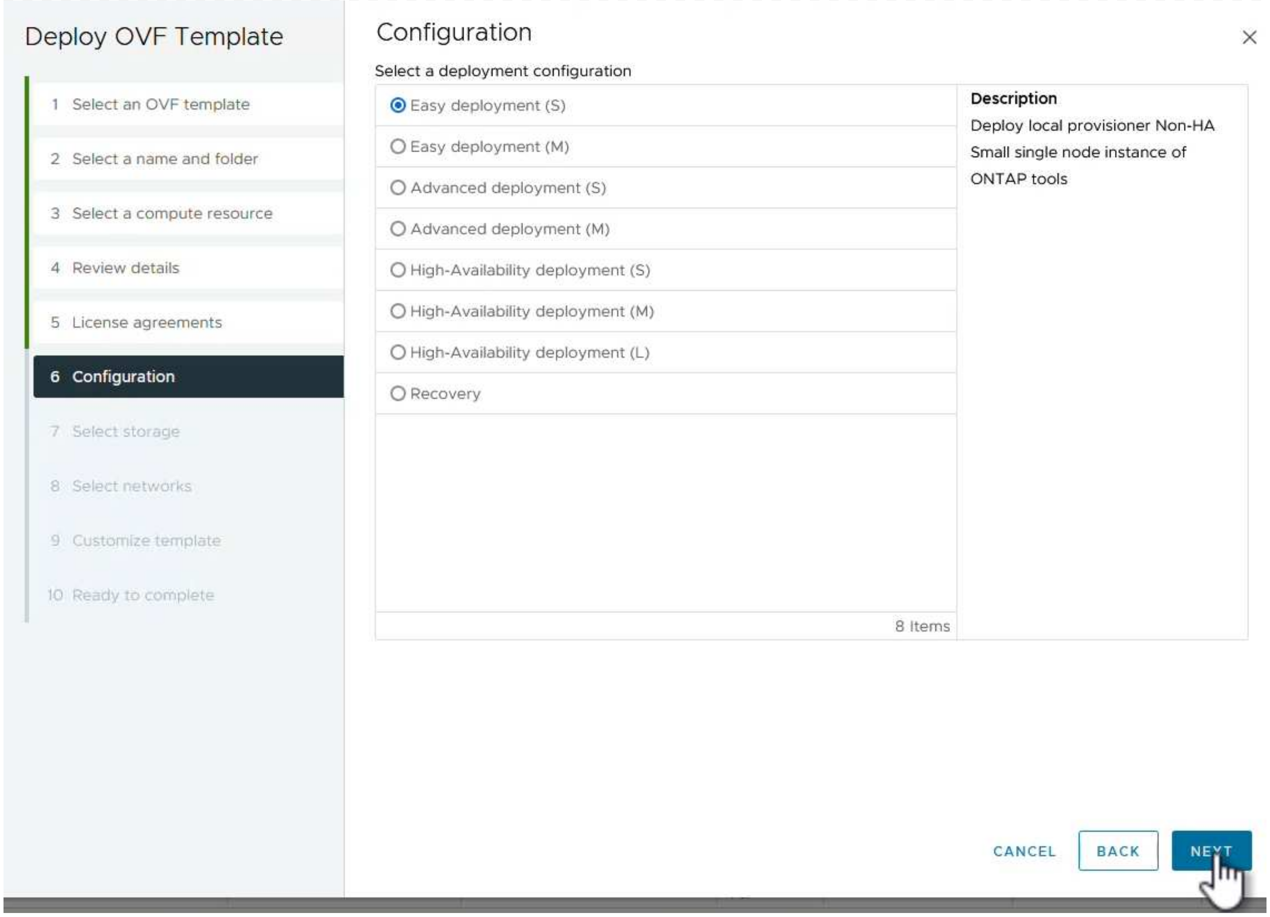
Select Network

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

5 items

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

> ONTAP Tools 10 features multiple deployment configurations including high-availability deployments using multiple nodes. For documentation on all deployment configurations and prerequisites, refer to Prerequisites for deploying ONTAP tools for VMware vSphere.



Deploy OVF Template

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

Configuration

Select a deployment configuration

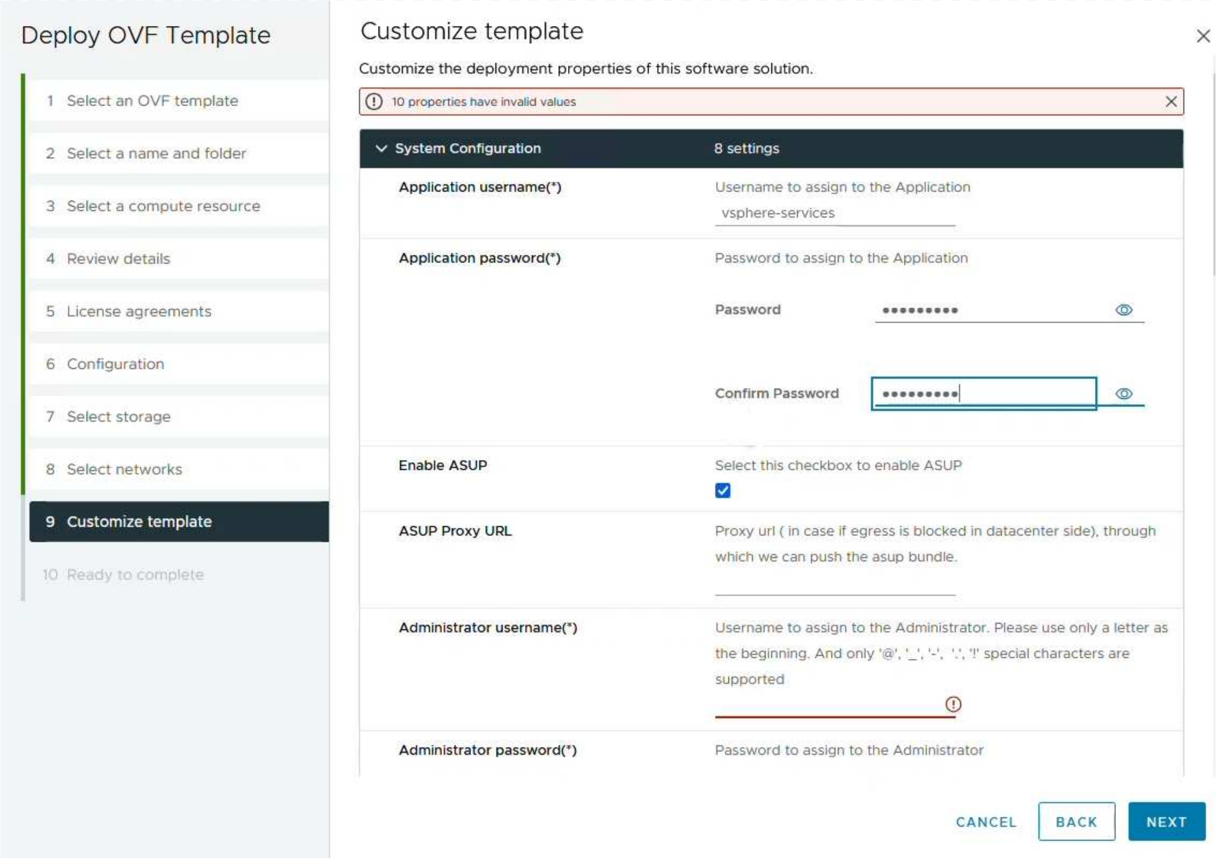
● Easy deployment (S)
○ Easy deployment (M)
○ Advanced deployment (S)
○ Advanced deployment (M)
○ High-Availability deployment (S)
○ High-Availability deployment (M)
○ High-Availability deployment (L)
○ Recovery

8 Items

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

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

     Click on **Next** to continue.



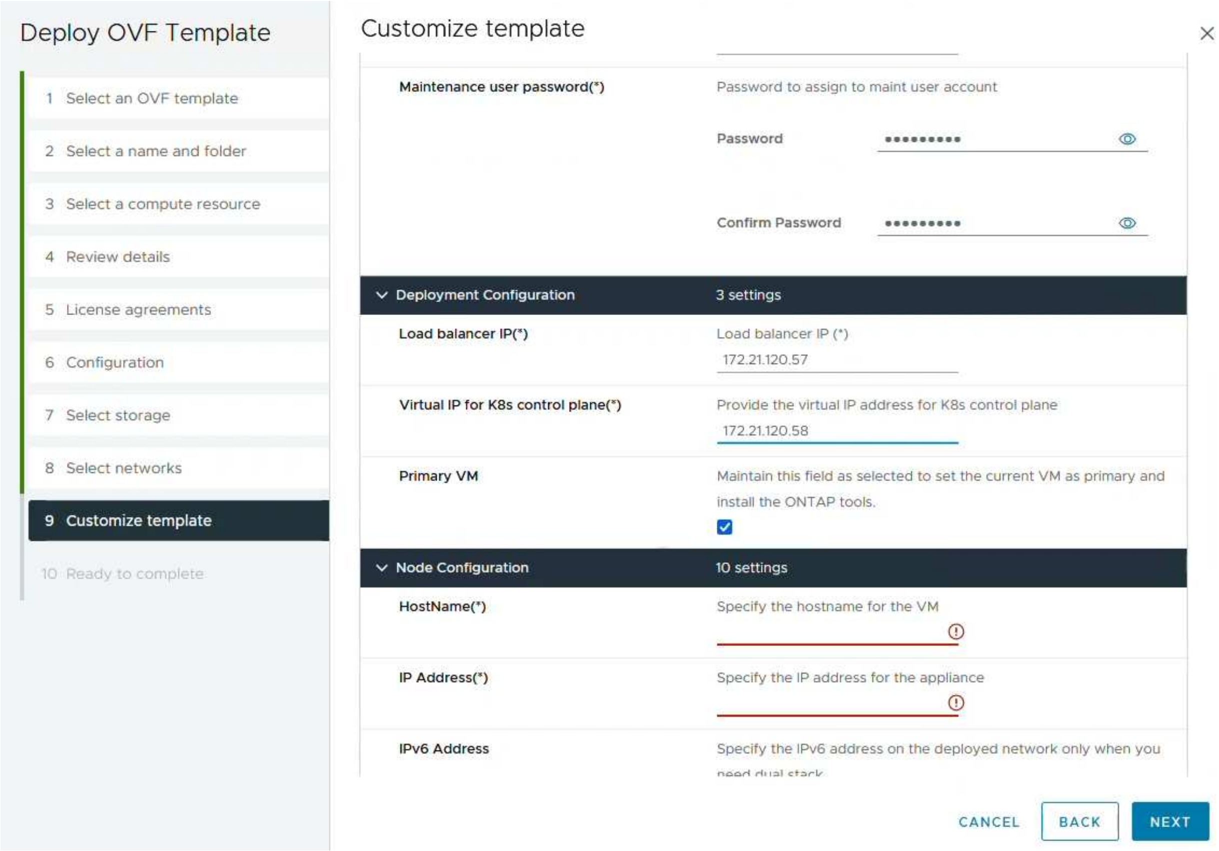
Customize template

Customize the deployment properties of this software solution.

ⓘ 10 properties have invalid values

System Configuration — 8 settings

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



Customize template

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

Deployment Configuration — 3 settings

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

Node Configuration — 10 settings

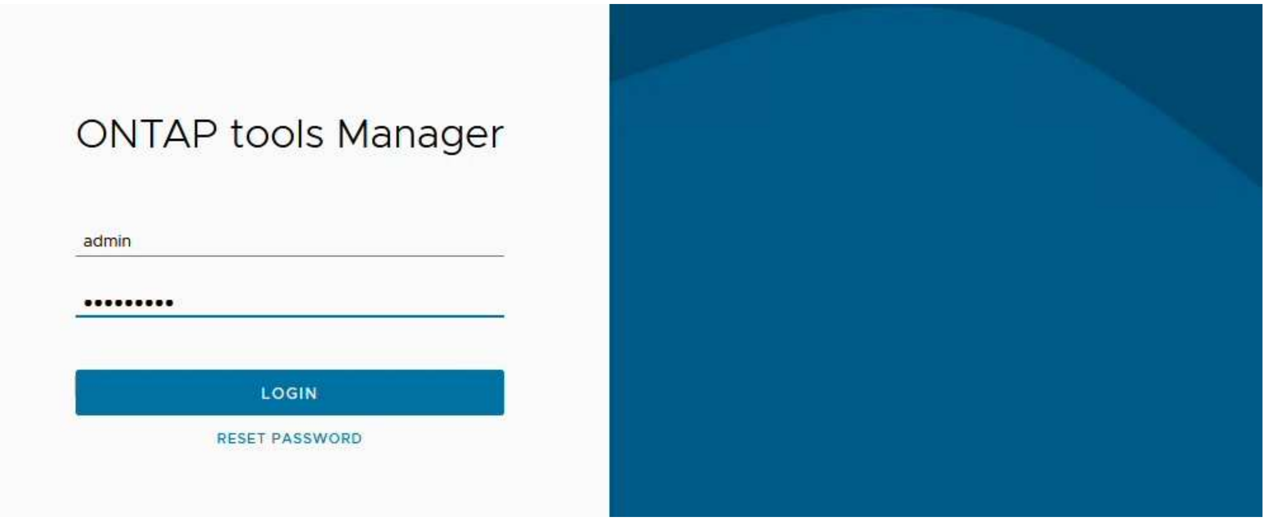
HostName(*)	Specify the hostname for the VM
IP Address(*)	Specify the IP address for the appliance
IPv6 Address	Specify the IPv6 address on the deployed network only when you need dual stack

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

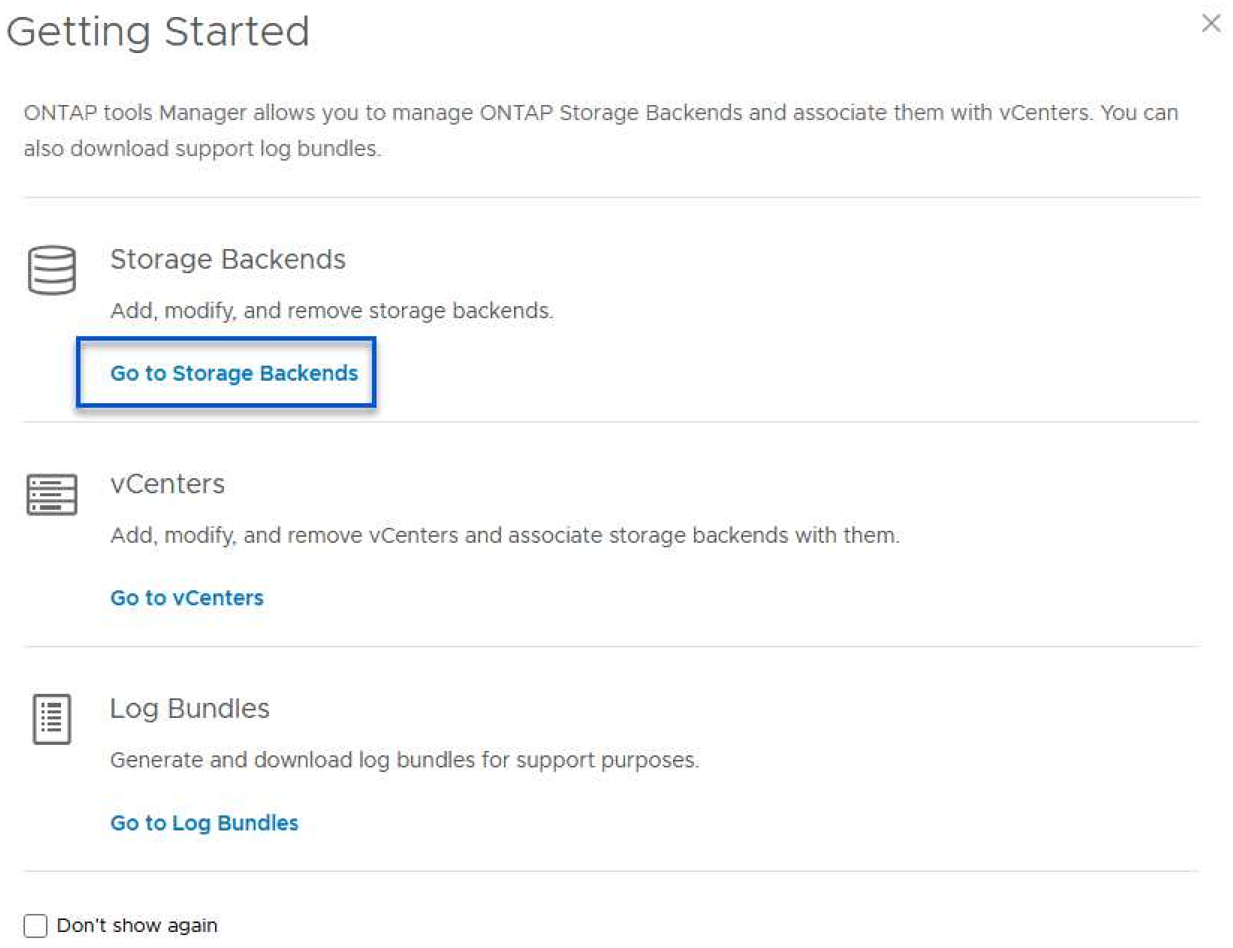
Connect Storage Backend and vCenter Server to ONTAP tools 10.

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

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



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



Getting Started

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

Storage Backends

Add, modify, and remove storage backends.

Go to Storage Backends

vCenters

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

Go to vCenters

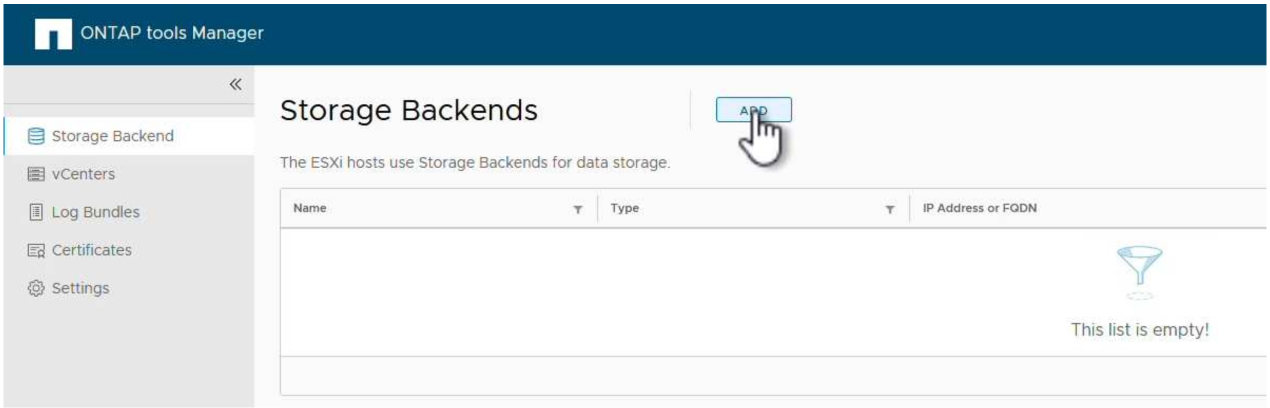
Log Bundles

Generate and download log bundles for support purposes.

Go to Log Bundles

□ Don't show again

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



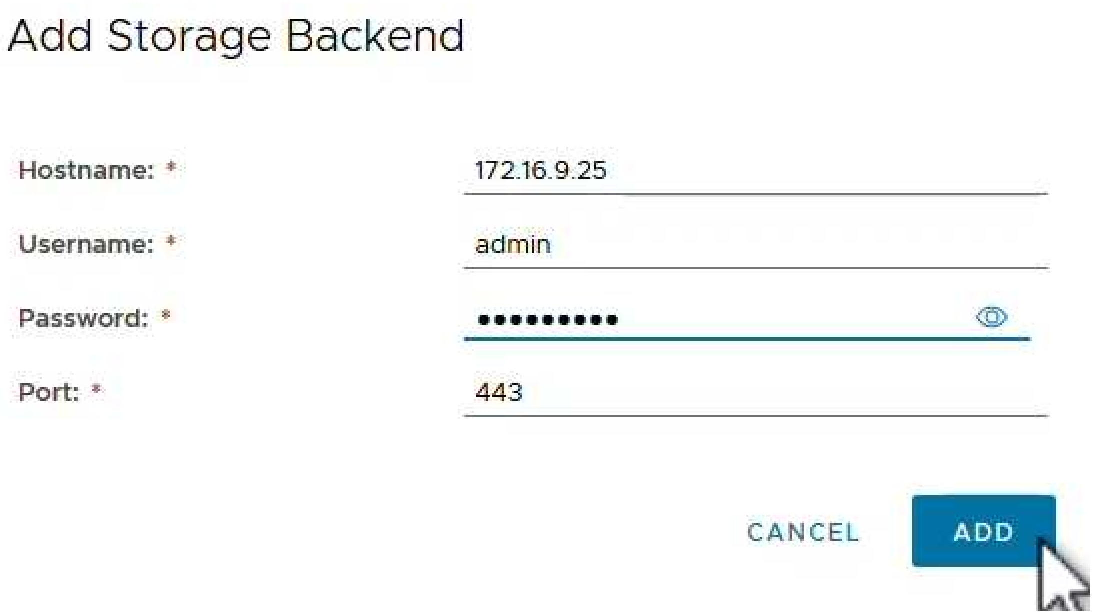
Storage Backends

The ESXi hosts use Storage Backends for data storage.

Name	Type	IP Address or FQDN

This list is empty!

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


Add Storage Backend

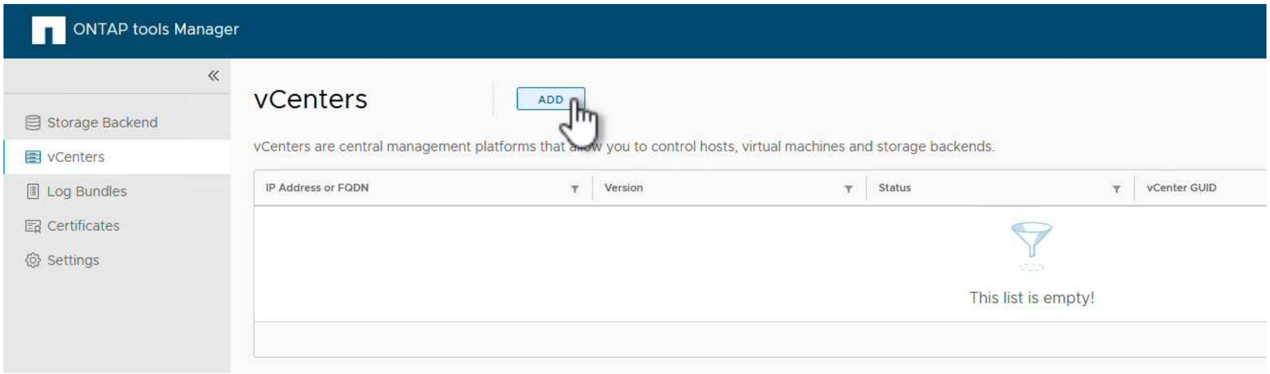
Hostname: * 172.16.9.25

Username: * admin

Password: * ●●●●●●●●●●

Port: * 443

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



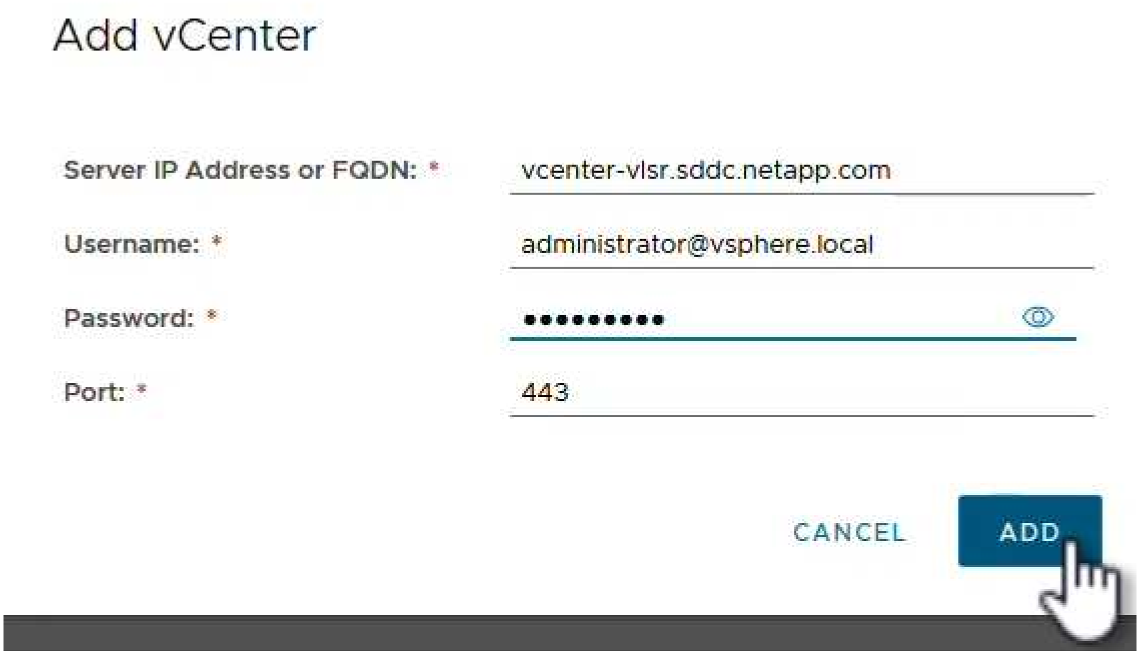
vCenters

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

IP Address or FQDN	Version	Status	vCenter GUID

This list is empty!

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



Add vCenter

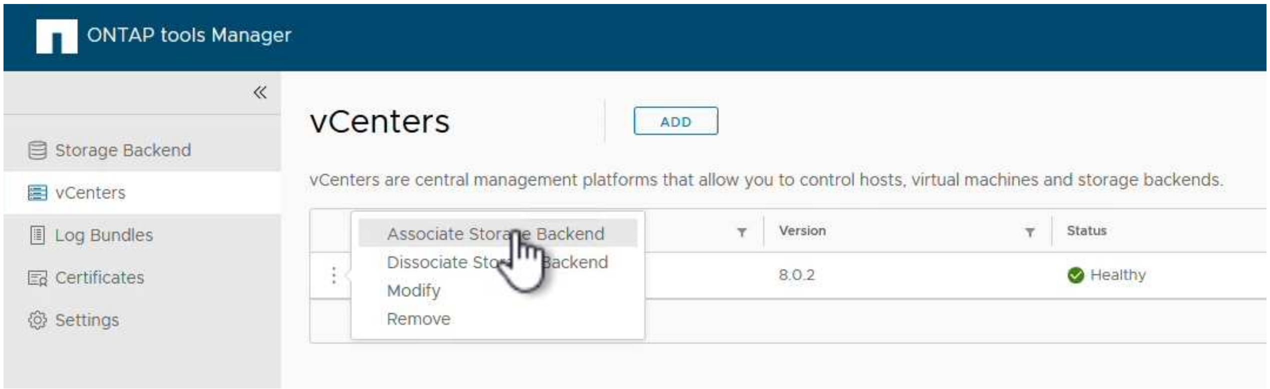
Server IP Address or FQDN: * vcenter-vlsr.sddc.netapp.com

Username: * administrator@vsphere.local

Password: * ••••••••••

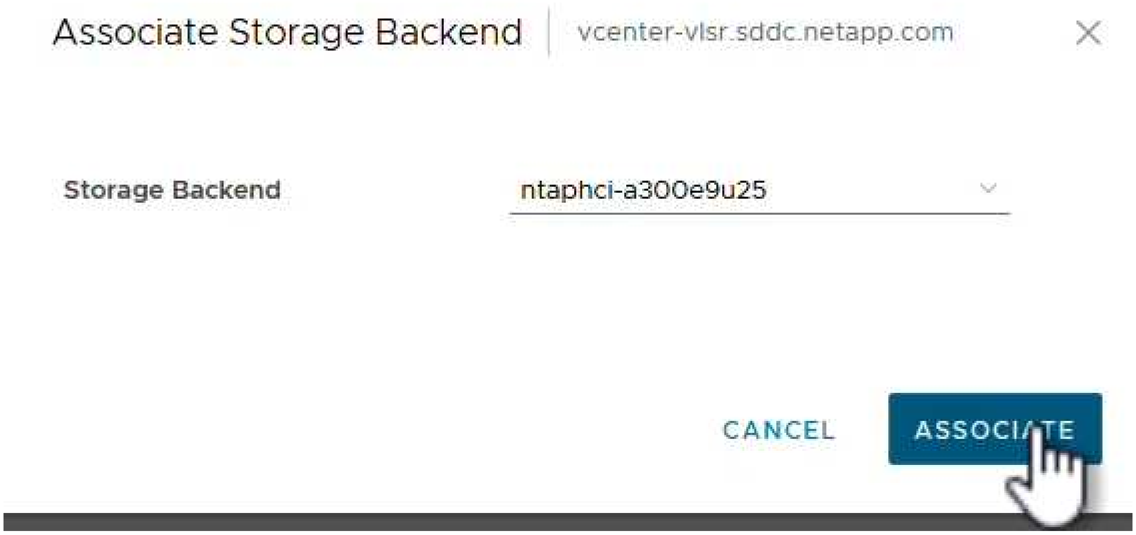
Port: * 443

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



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

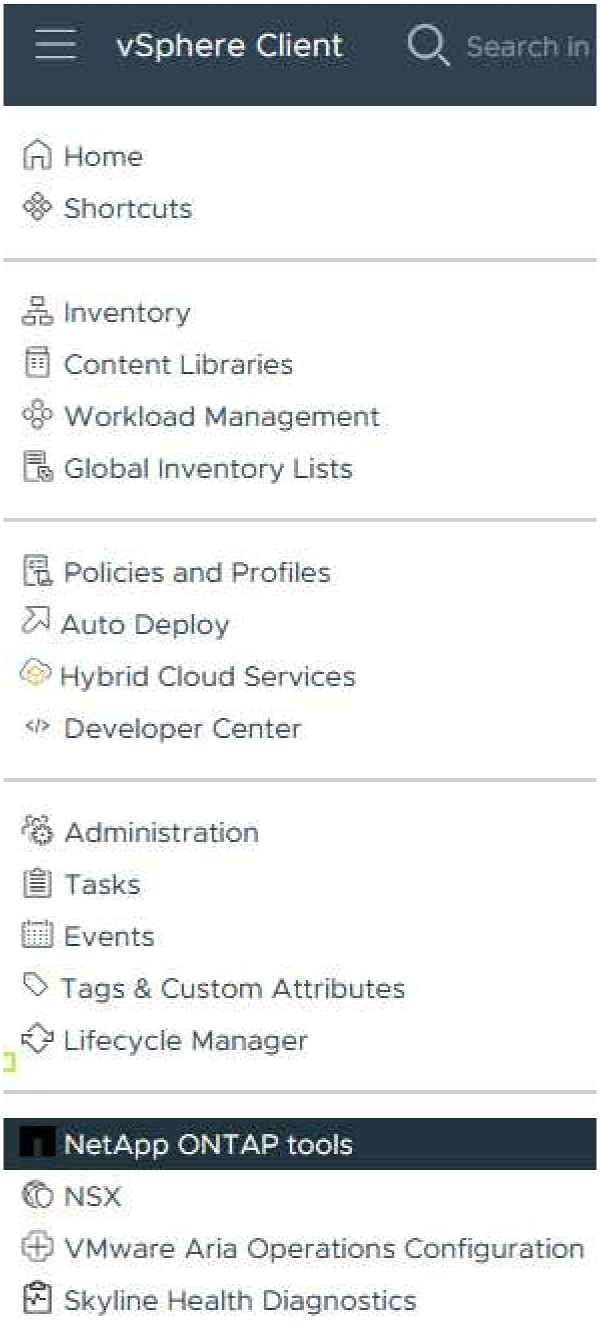
8. On the **Associate Storage Backend** box, select the ONTAP storage system to associated with the vCenter server and click on **Associate** to complete the action.



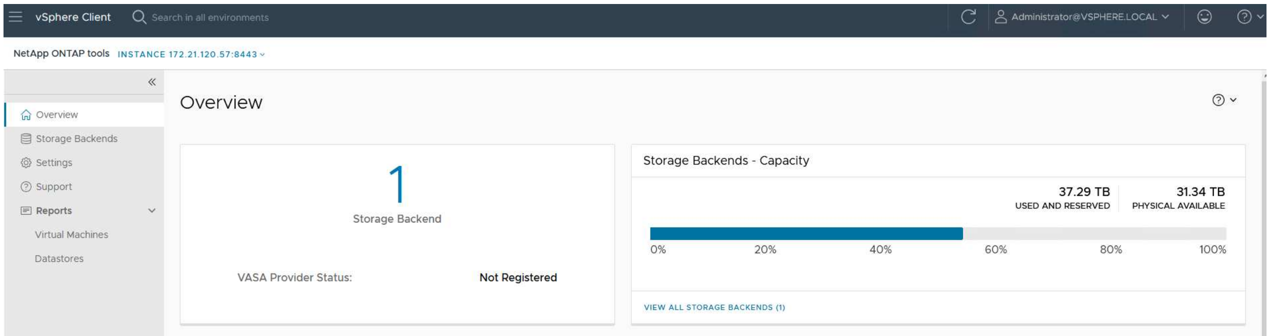
Associate Storage Backend | vcenter-vlsr.sddc.netapp.com

Storage Backend: ntaphci-a300e9u25

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



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


vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
NetApp ONTAP tools
INSTANCE 172.21.120.57:8443
Overview
Storage Backends
Settings
Support
Reports
Virtual Machines
Datastores
Overview
Storage Backends - Capacity
0%
20%
40%
60%
80%
100%
VIEW ALL STORAGE BACKENDS (1)

1 Storage Backend

VASA Provider Status: Not Registered

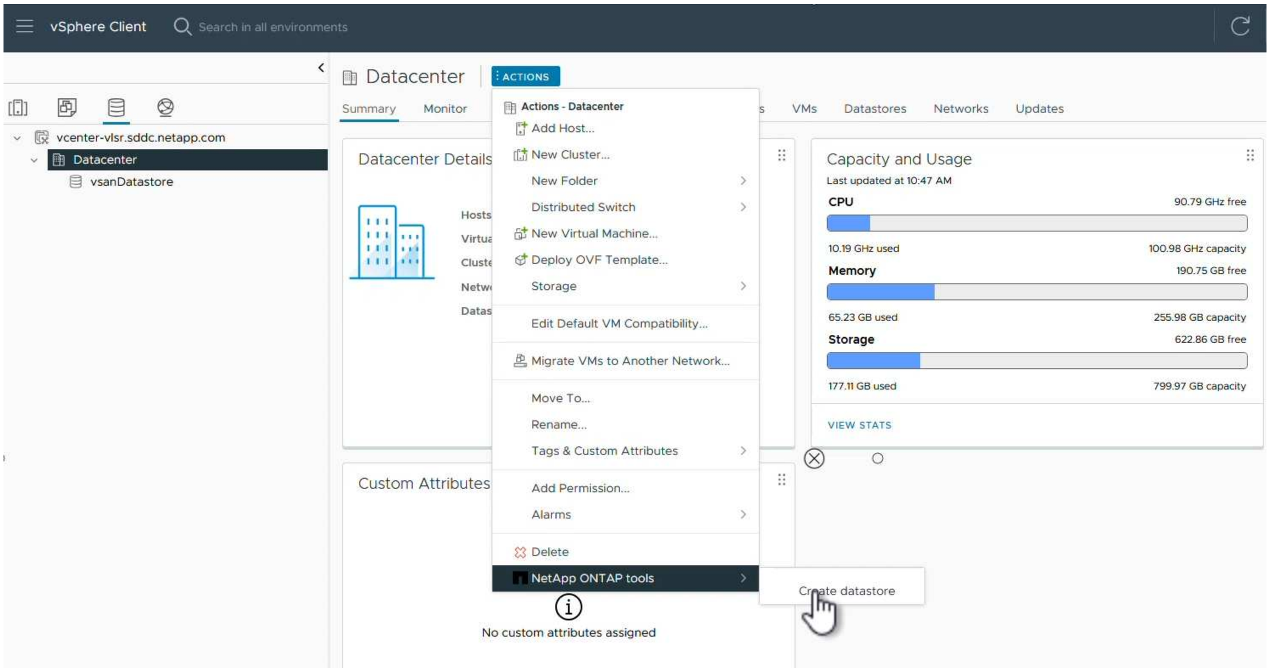
37.29 TB USED AND RESERVED

31.34 TB PHYSICAL AVAILABLE

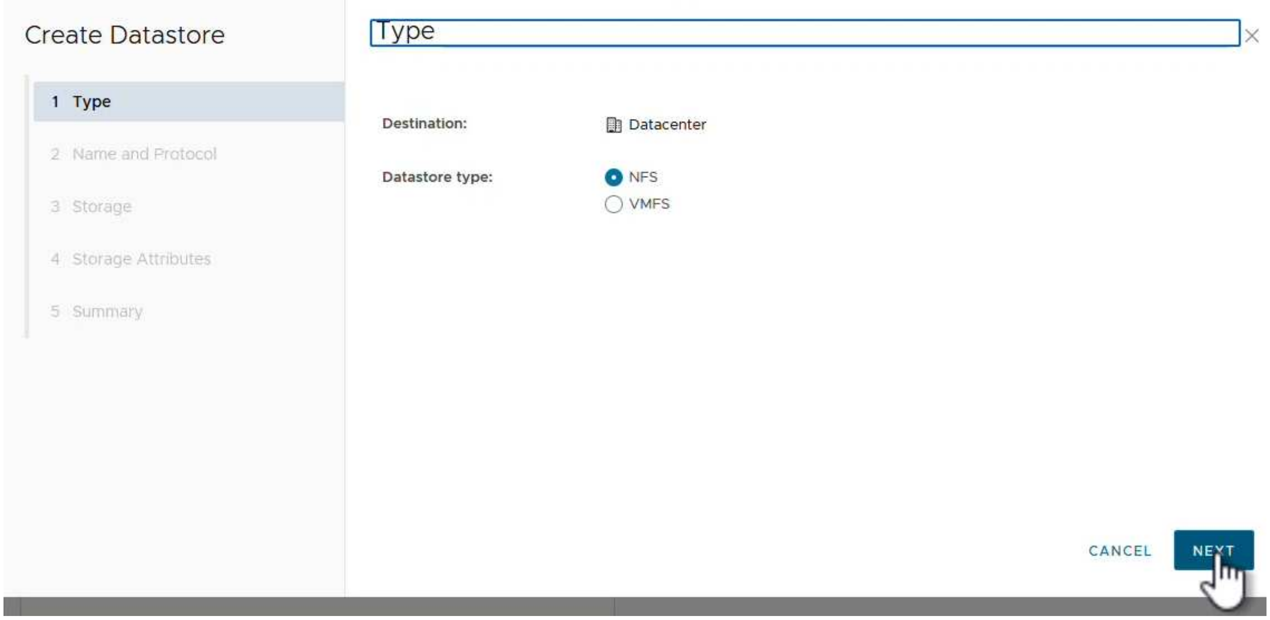
Create an NFS datastore using ONTAP tools 10

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

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



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

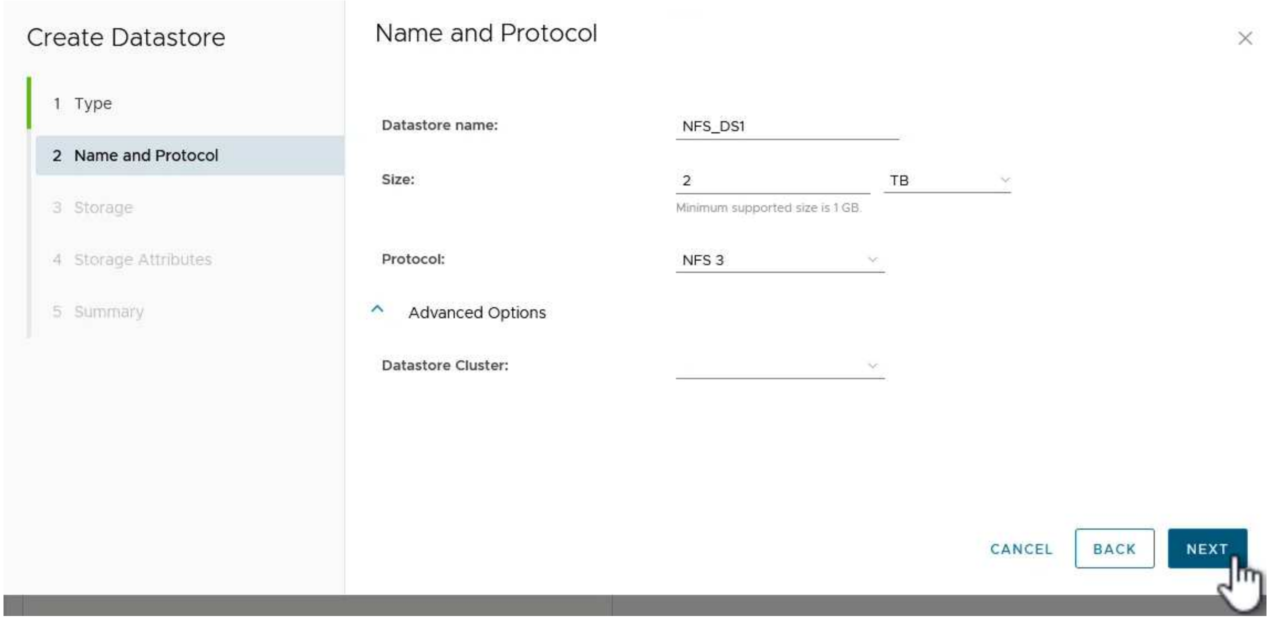


Destination: Datacenter

Datastore type: ● NFS ○ VMFS

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

to continue.


Create Datastore

1 Type

2 Name and Protocol

3 Storage

4 Storage Attributes

5 Summary

Name and Protocol

Datastore name: NFS_DS1

Size: 2 TB

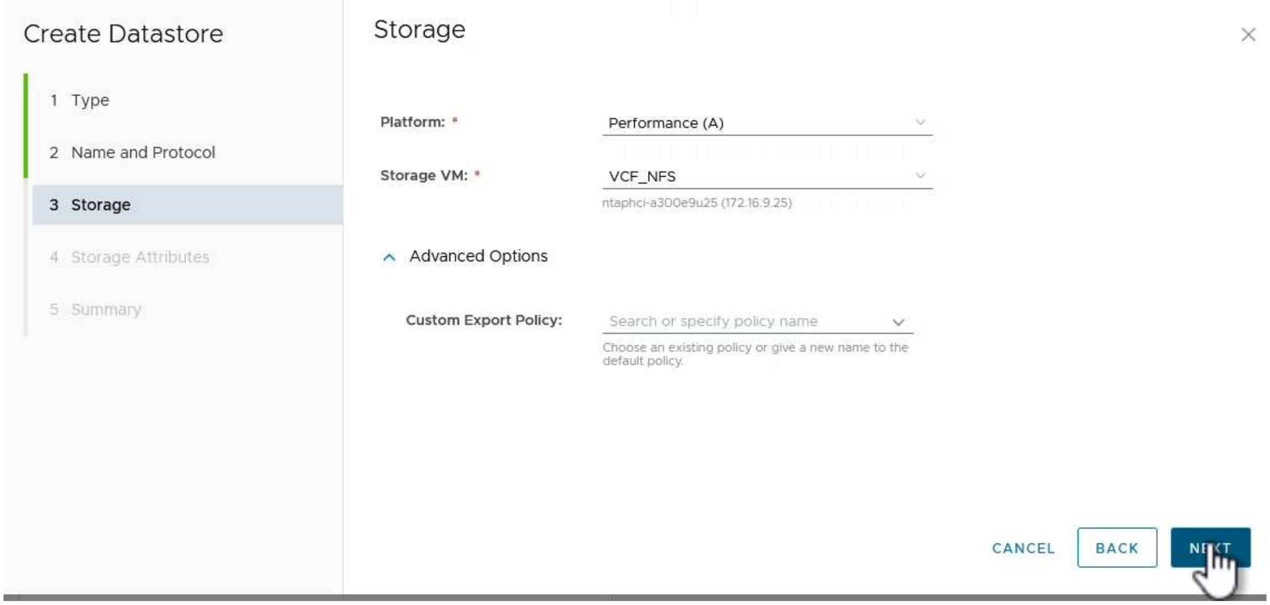
Minimum supported size is 1 GB.

Protocol: NFS 3

Advanced Options

Datastore Cluster:

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


Create Datastore

1 Type

2 Name and Protocol

3 Storage

4 Storage Attributes

5 Summary

Storage

Platform: * Performance (A)

Storage VM: * VCF_NFS

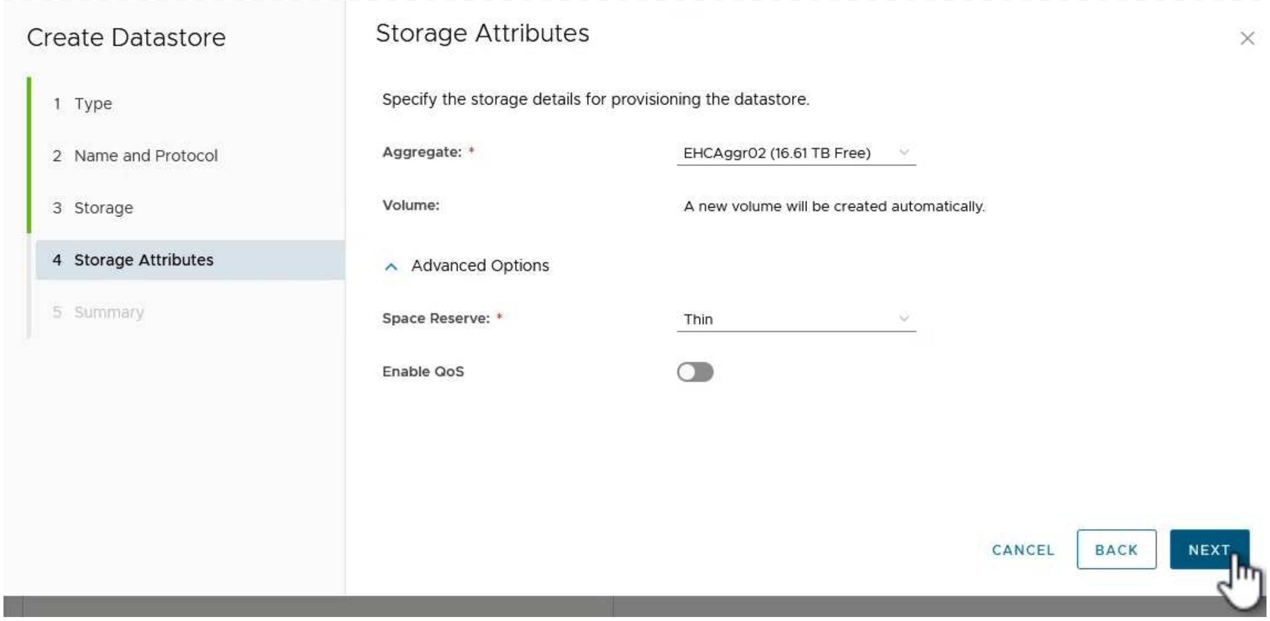
ntaphci-a300e9u25 (172.16.9.25)

Advanced Options

Custom Export Policy: Search or specify policy name

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

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



Create Datastore

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)

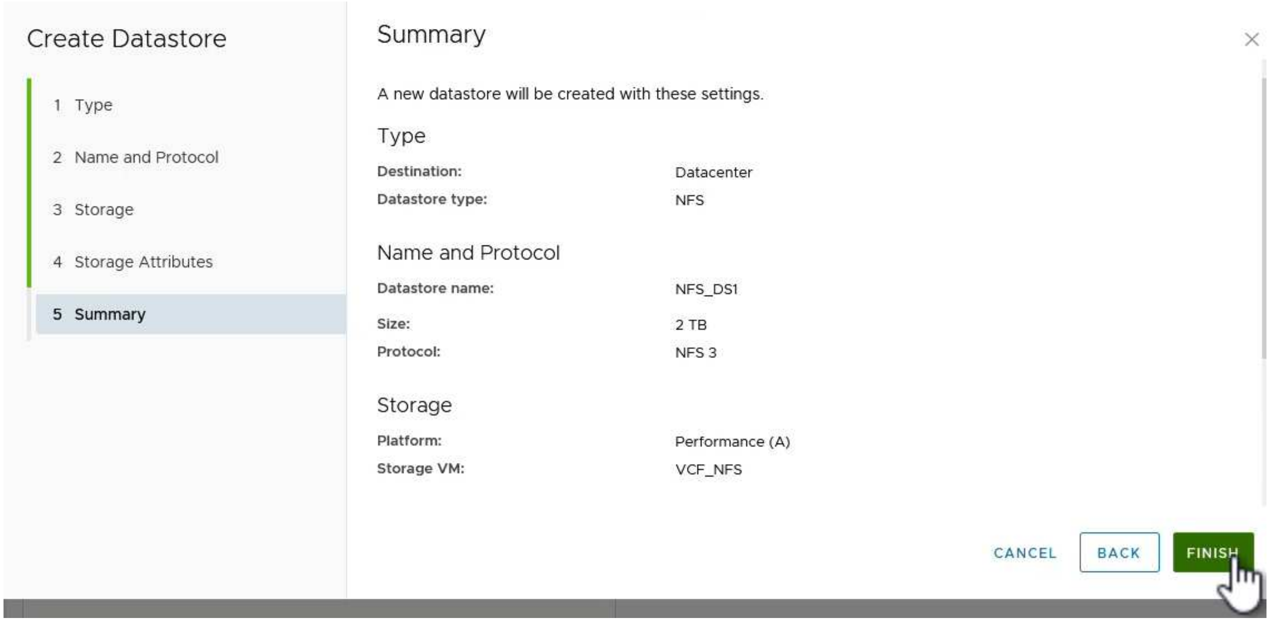
Volume: A new volume will be created automatically.

Advanced Options

Space Reserve: * Thin

Enable QoS

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

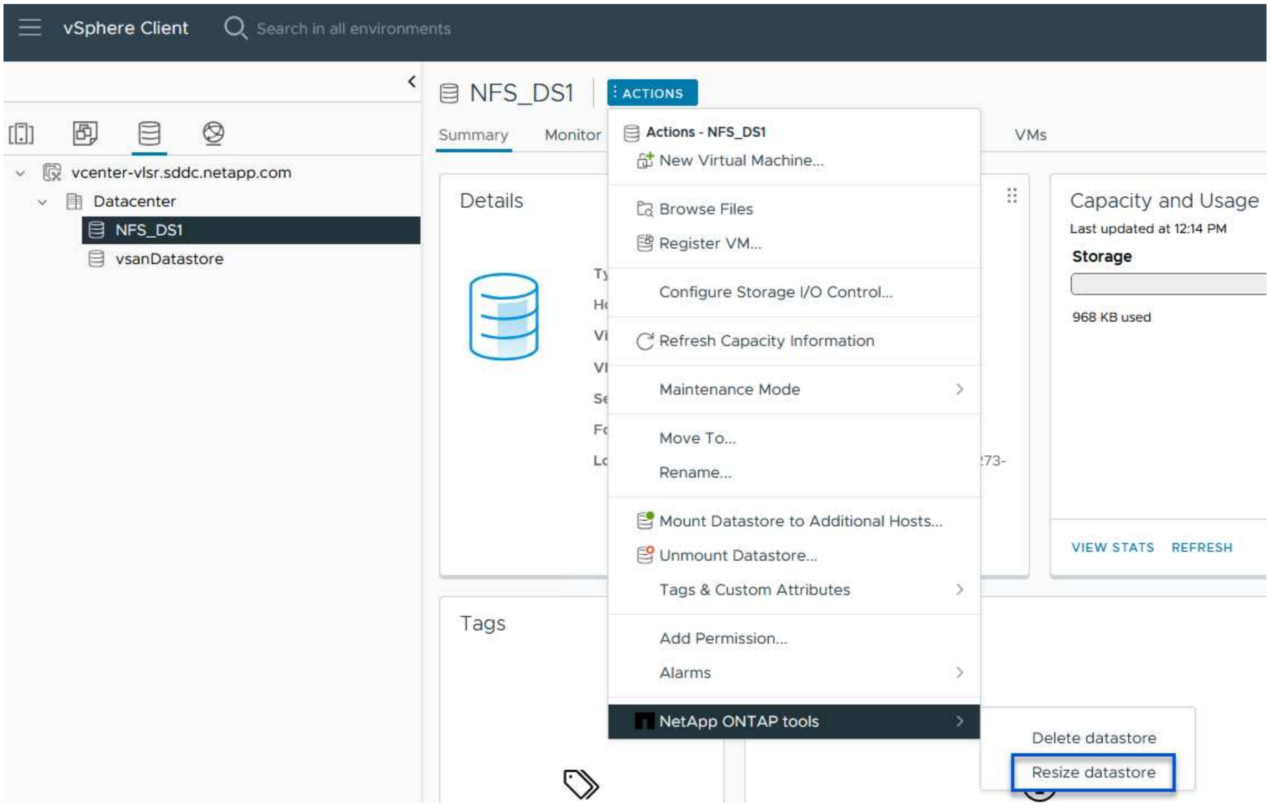
Storage

Platform: Performance (A)
Storage VM: VCF_NFS

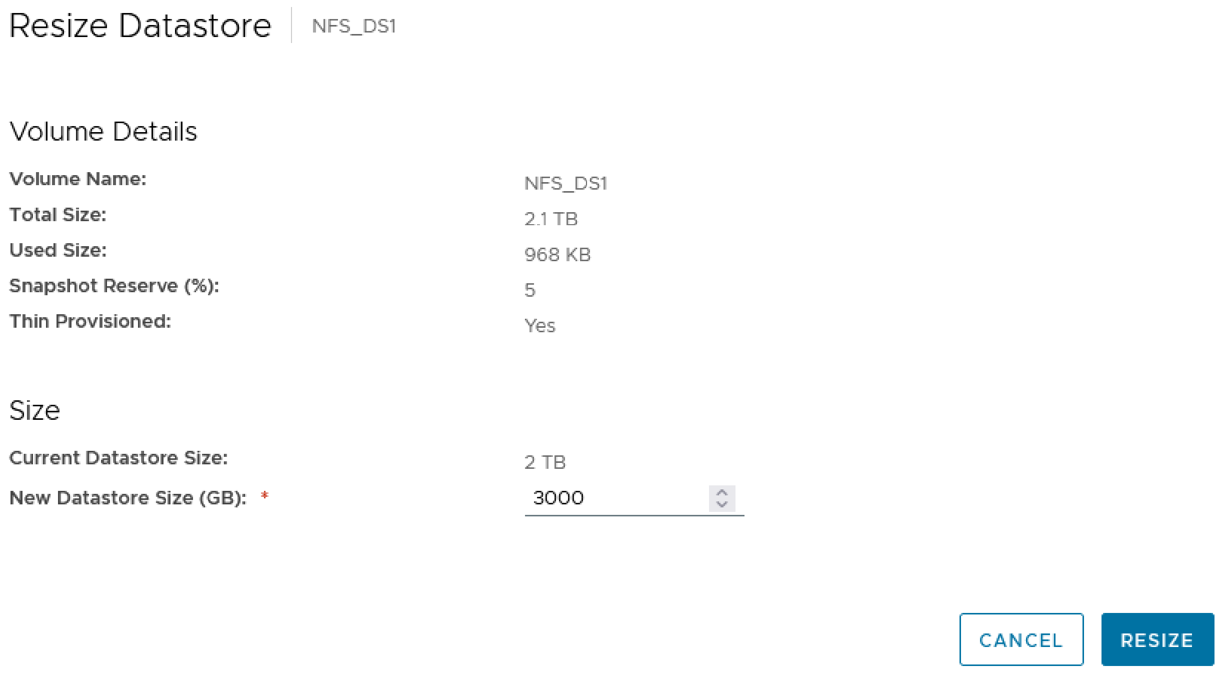
Resize an NFS datastore using ONTAP tools 10

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

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



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



Resize Datastore | NFS_DS1

Volume Details

Volume Name: NFS_DS1

Total Size: 2.1 TB

Used Size: 968 KB

Snapshot Reserve (%): 5

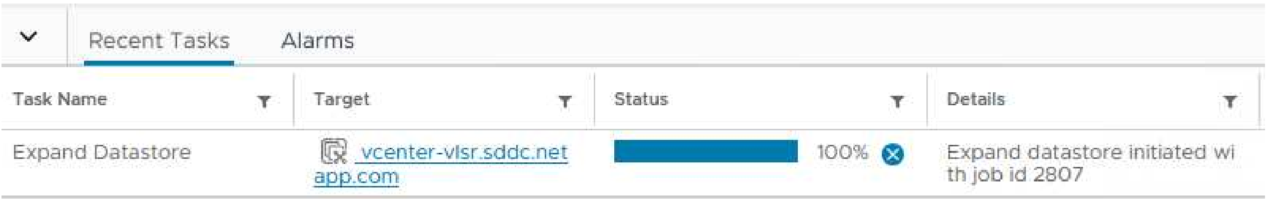
Thin Provisioned: Yes

Size

Current Datastore Size: 2 TB

New Datastore Size (GB): * 3000

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



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

Additional information

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

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

Configure disaster recovery for NFS datastores using VMware Site Recovery Manager

Implement disaster recovery for NFS datastores using VMware Site Recovery Manager (SRM) and ONTAP tools for VMware vSphere 10. This procedure includes configuring SRM with vCenter servers at primary and secondary sites, installing the ONTAP Storage Replication Adapter (SRA), establishing SnapMirror relationships between ONTAP storage systems, and setting up site recovery for SRM.

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

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

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

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

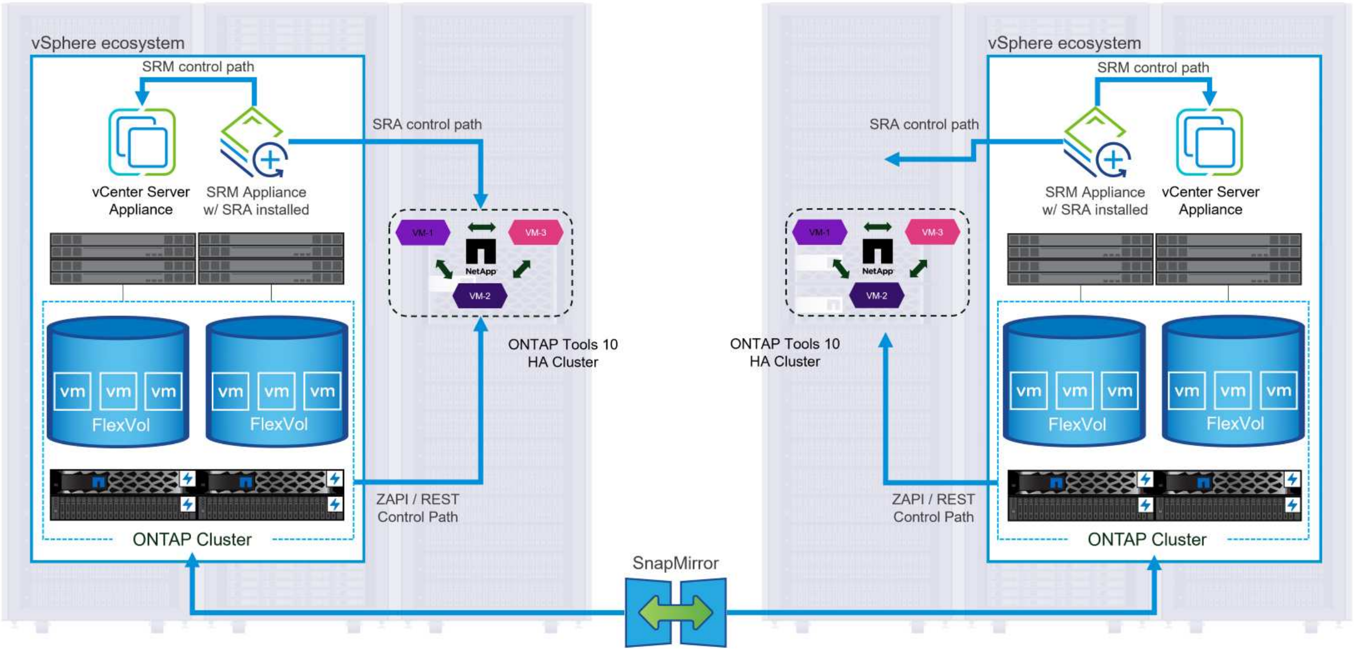
Scenario Overview

This scenario covers the following high level steps:

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

Architecture

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



Prerequisites

This scenario requires the following components and configurations:

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

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

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

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

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

Deployment Steps

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

Create SnapMirror relationship between ONTAP storage systems

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

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

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

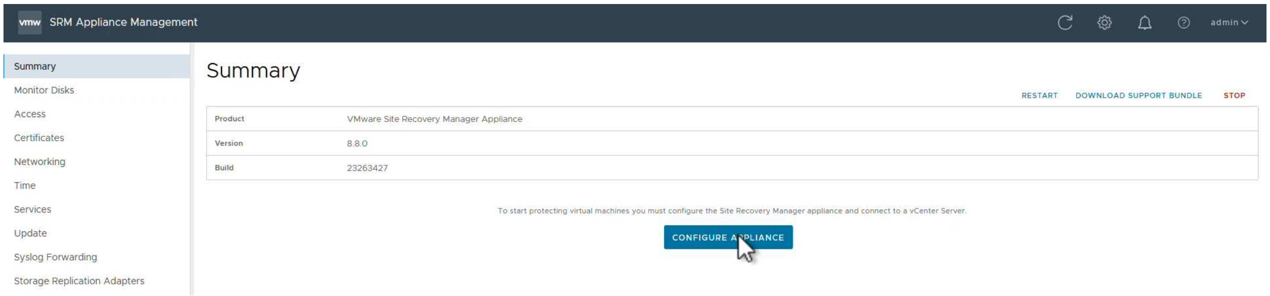
Configure the SRM appliance

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

Connect the SRM appliance for primary and secondary sites

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

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

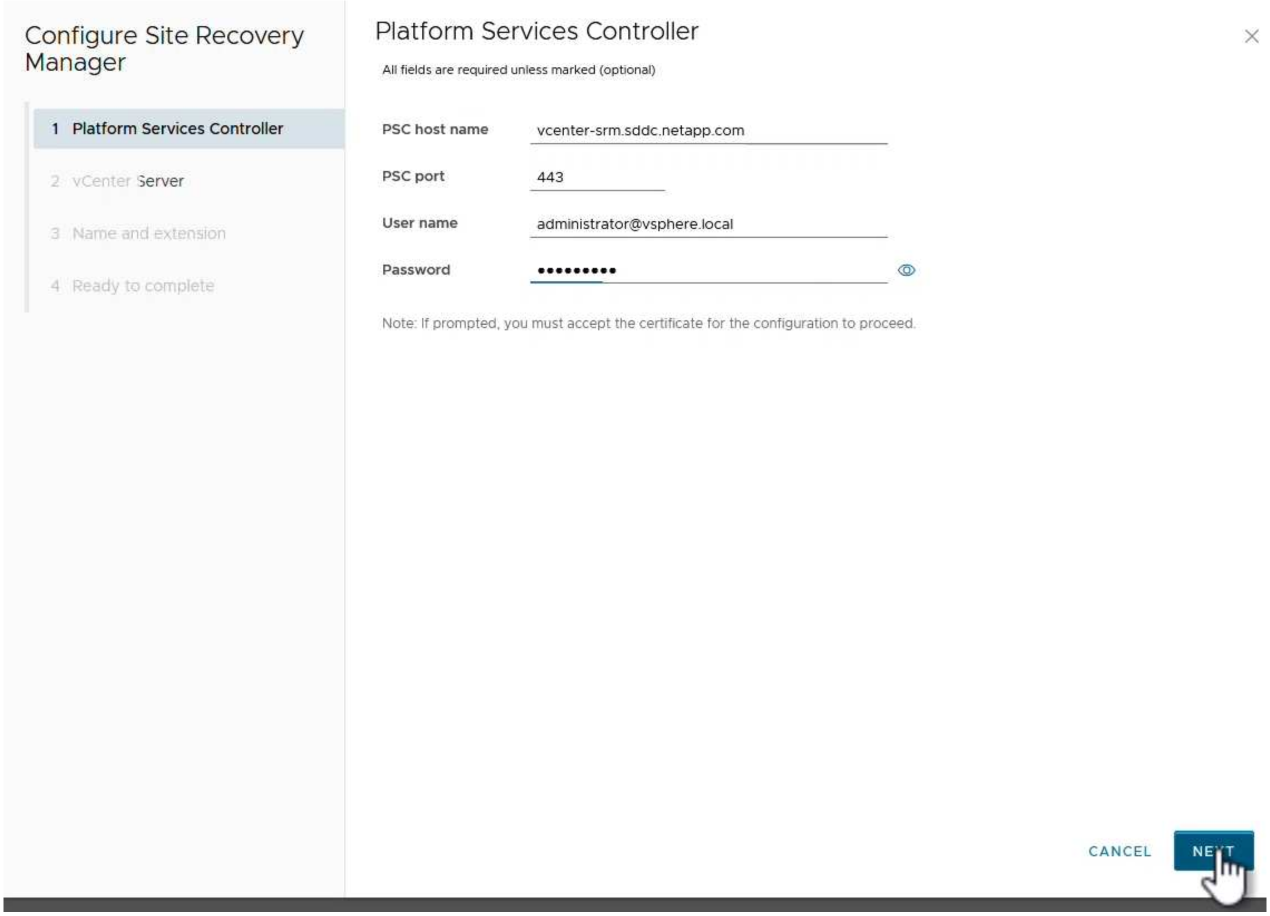
   

   Summary

Product	VMware Site Recovery Manager Appliance
Version	8.8.0
Build	23263427

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

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

   Platform Services Controller

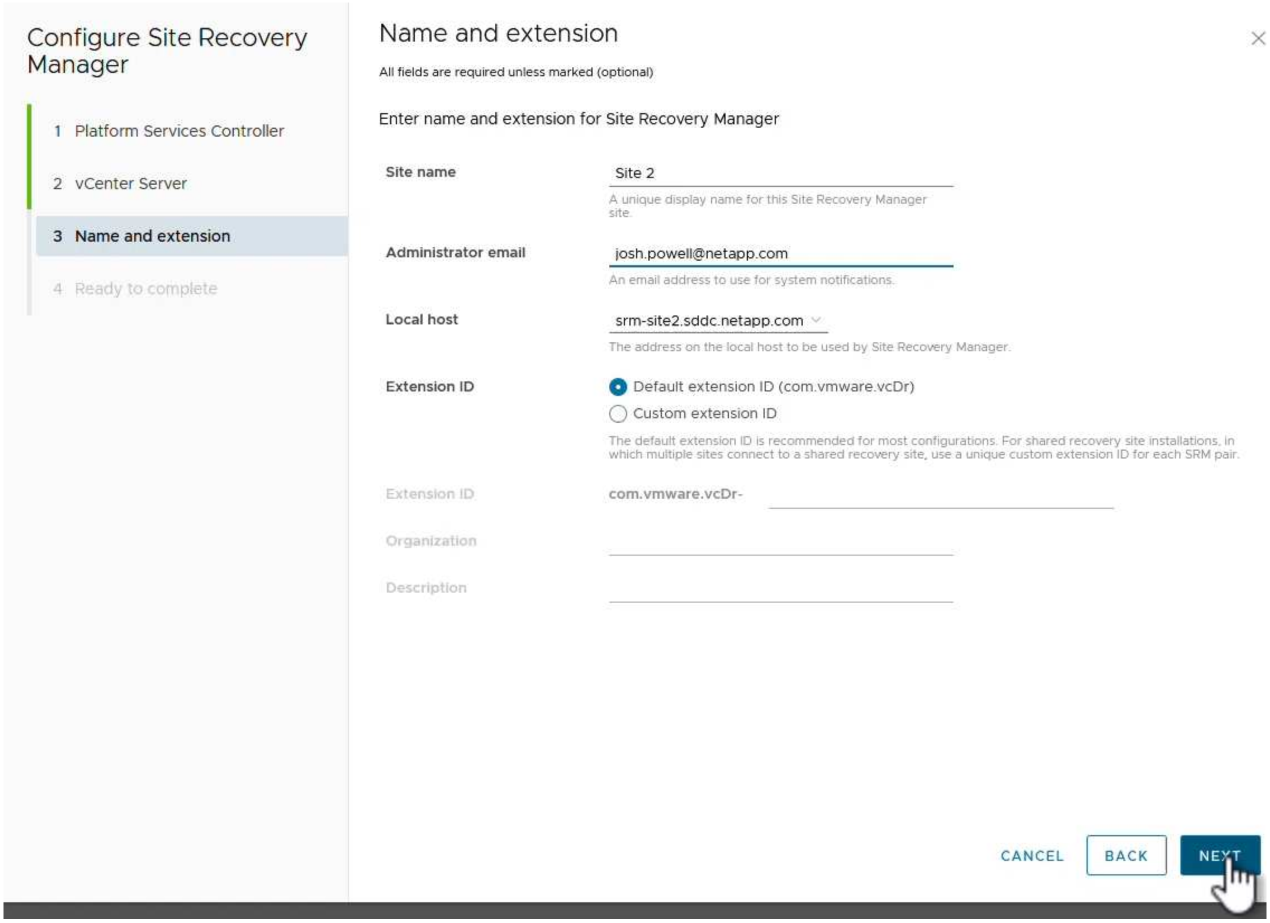
   All fields are required unless marked (optional)

PSC host name	vcenter-srm.sddc.netapp.com
PSC port	443
User name	administrator@vsphere.local
Password	••••••••••

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

3. On the **vCenter Server** page, view the connected vServer and click on **Next** to continue.

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


Configure Site Recovery Manager

1 Platform Services Controller

2 vCenter Server

3 Name and extension

4 Ready to complete

Name and extension

All fields are required unless marked (optional)

Enter name and extension for Site Recovery Manager

Site name: Site 2

A unique display name for this Site Recovery Manager site.

Administrator email: josh.powell@netapp.com

An email address to use for system notifications.

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

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

Extension ID:

● Default extension ID (com.vmware.vcDr)

○ Custom extension ID

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

Extension ID: com.vmware.vcDr-

Organization

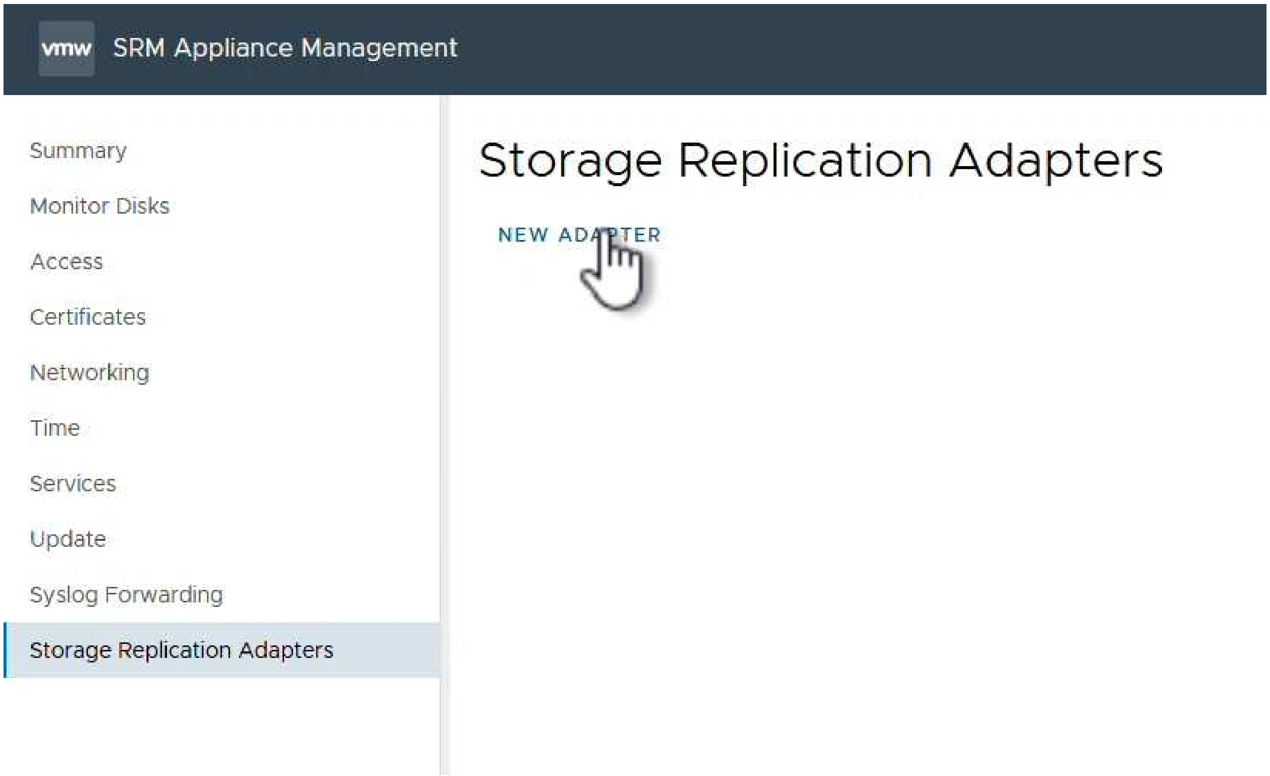
Description

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

Configure SRA on the SRM appliance

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

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



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

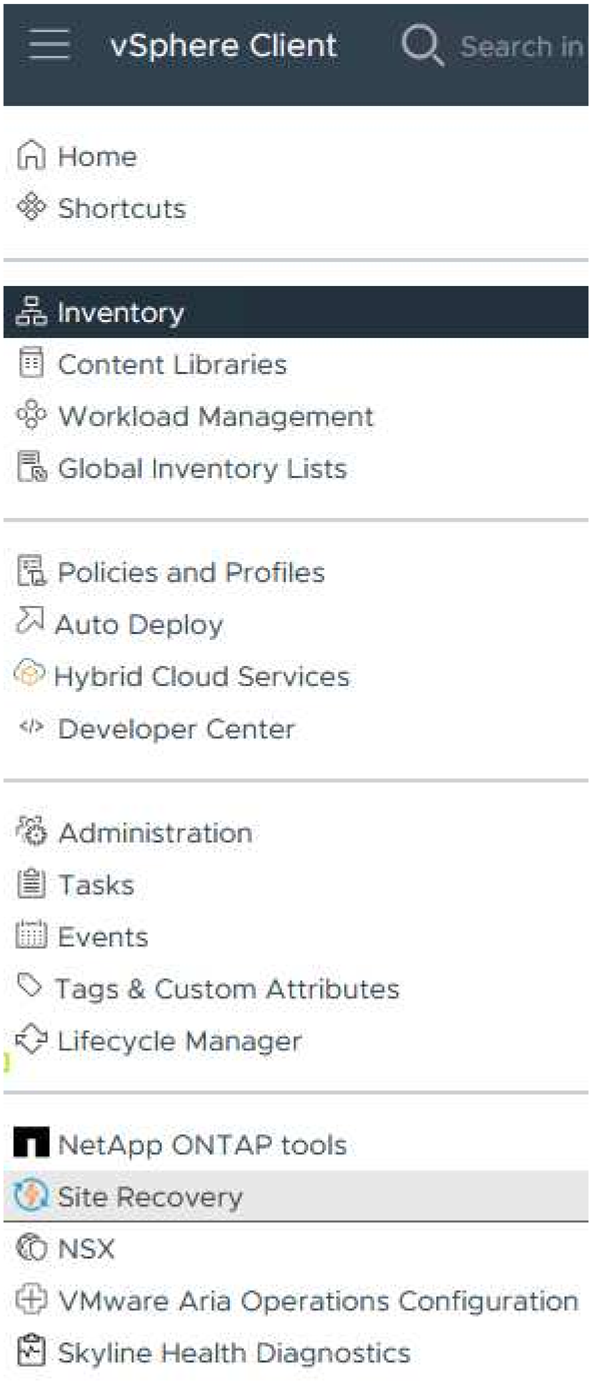
Configure Site Recovery for SRM

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

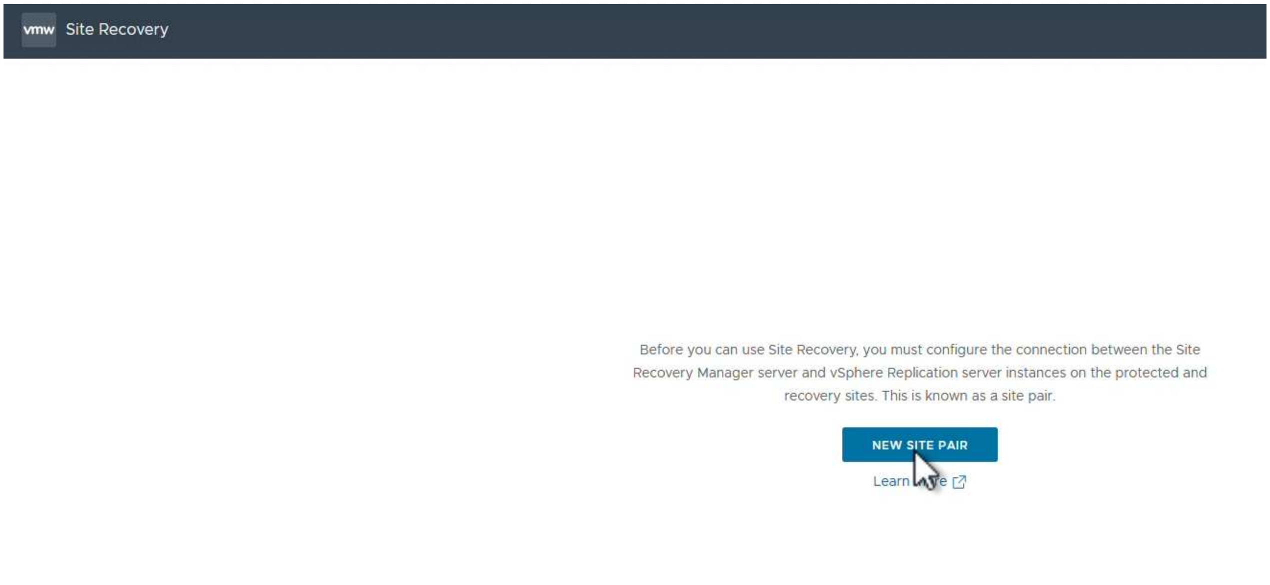
Configure Site Pairing for SRM

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

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

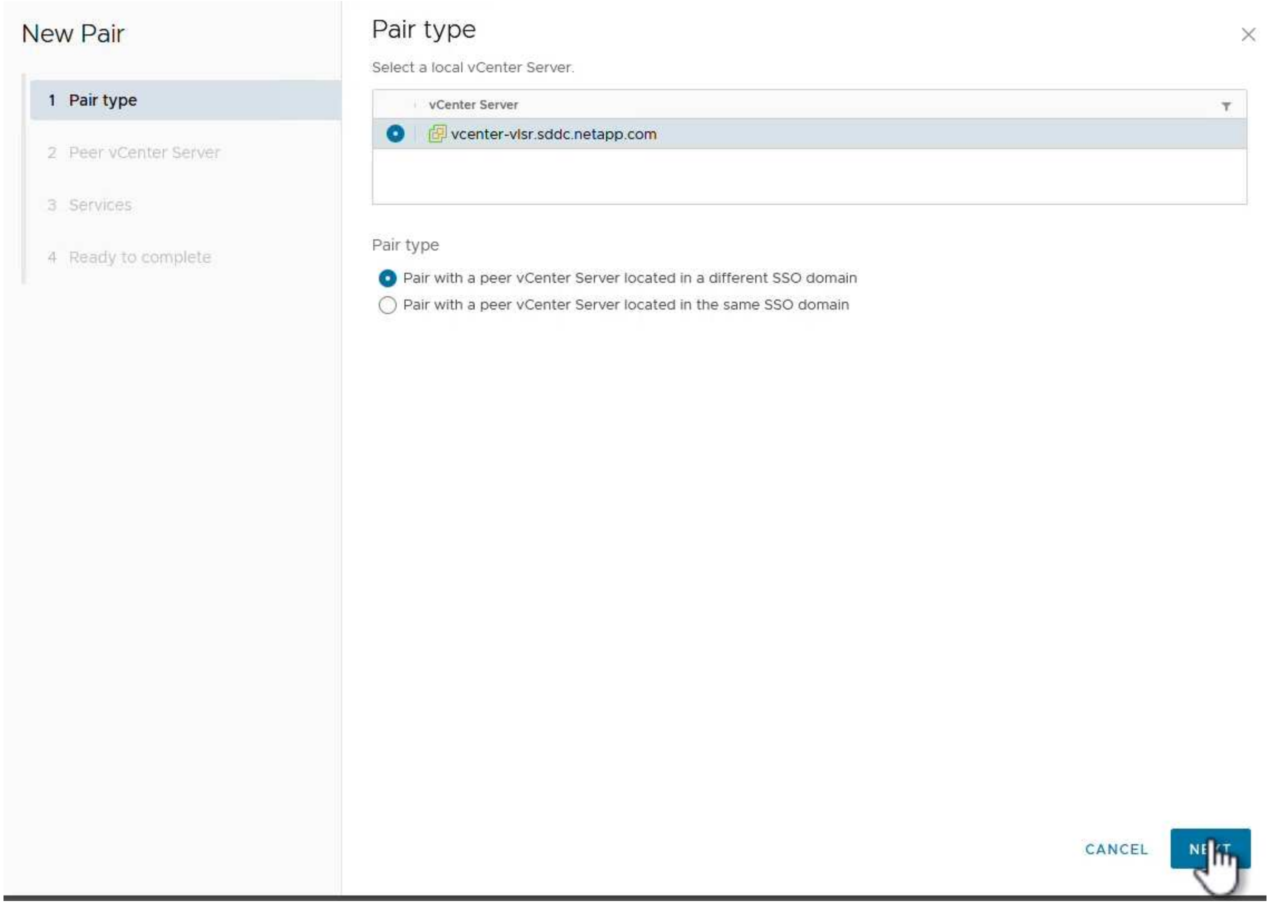


2. On the **Site Recovery** page, click on **NEW SITE PAIR**.



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

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



Pair type

Select a local vCenter Server.

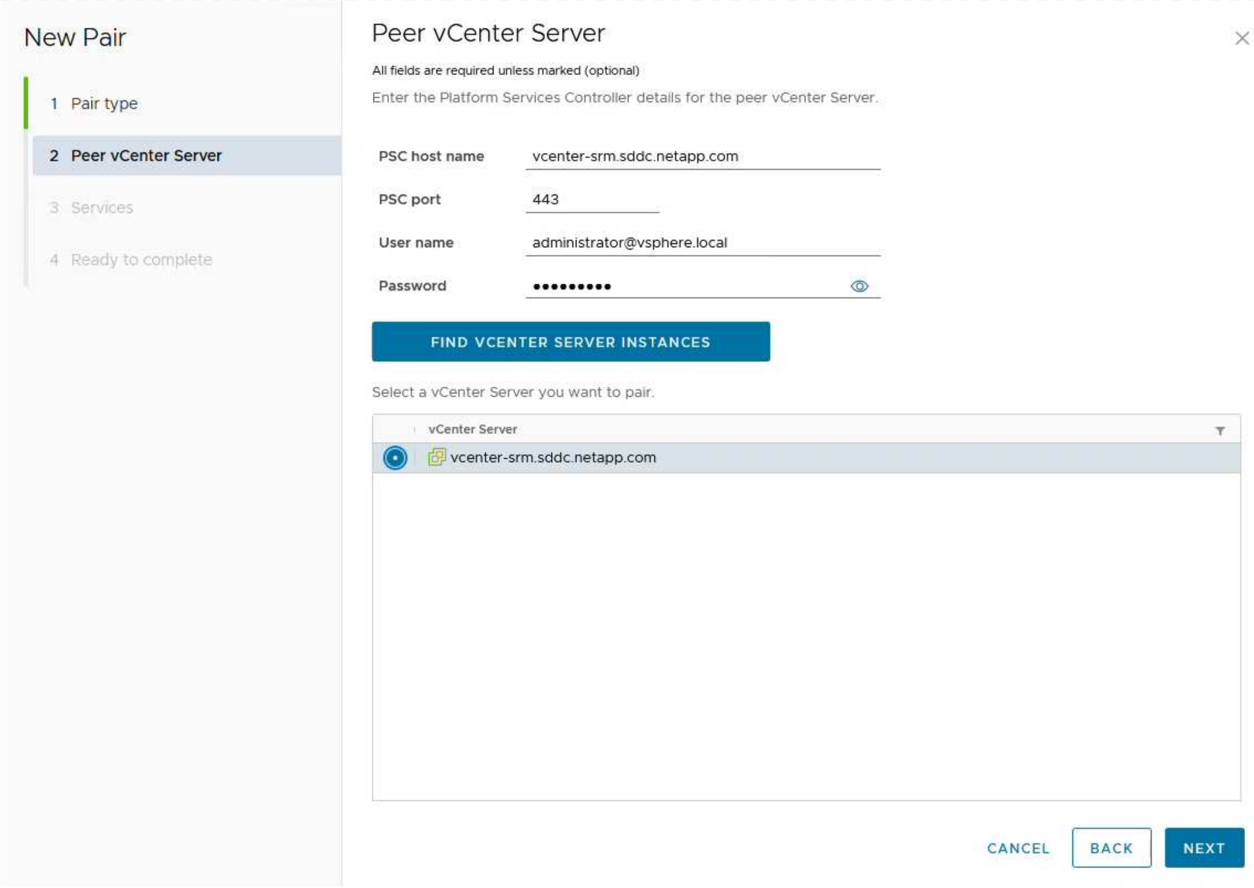
	vCenter Server
●	vcenter-vlsr.sddc.netapp.com

Pair type

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

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

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


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: vcenter-srm.sddc.netapp.com

PSC port: 443

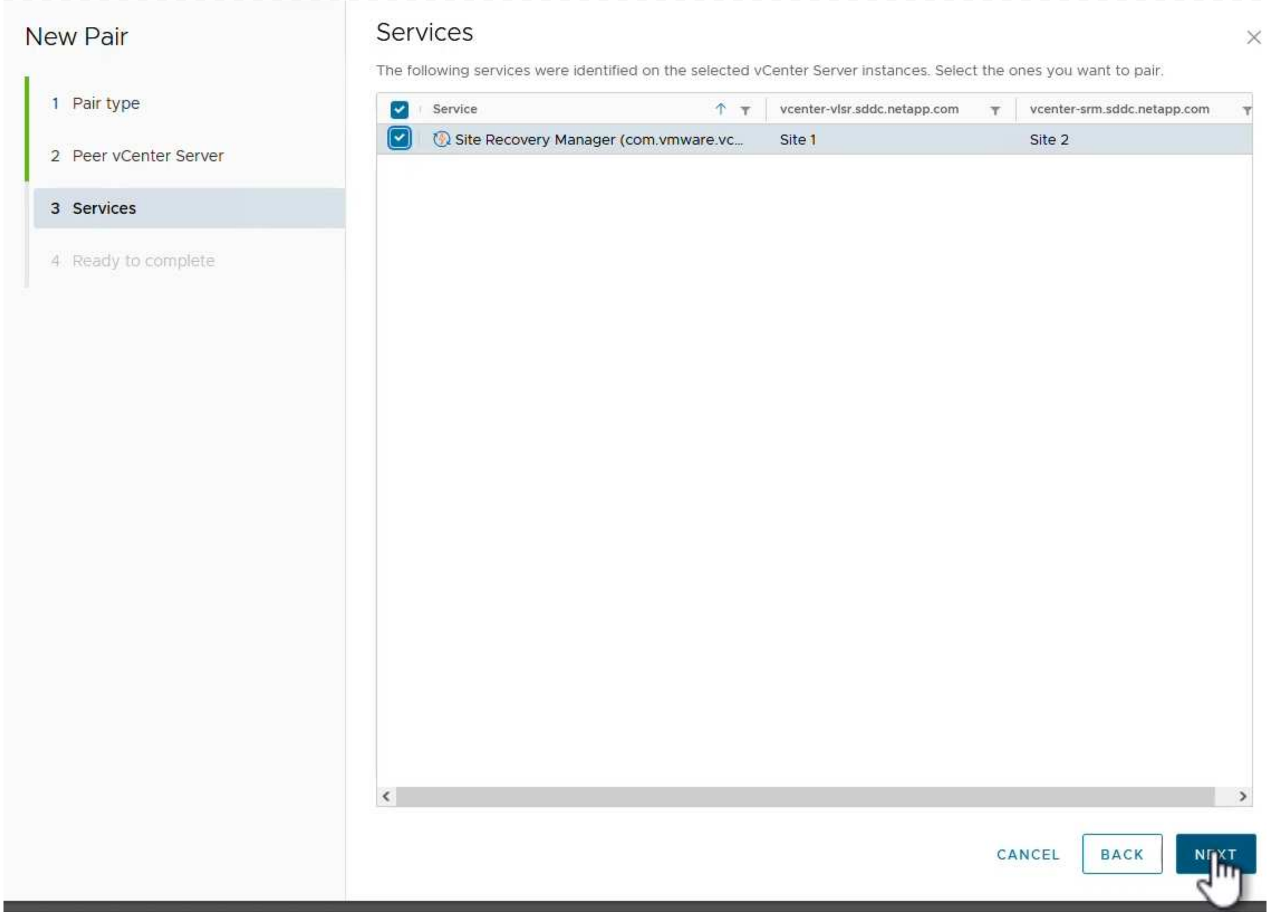
User name: administrator@vsphere.local

Password: ••••••••••

Select a vCenter Server you want to pair.

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

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

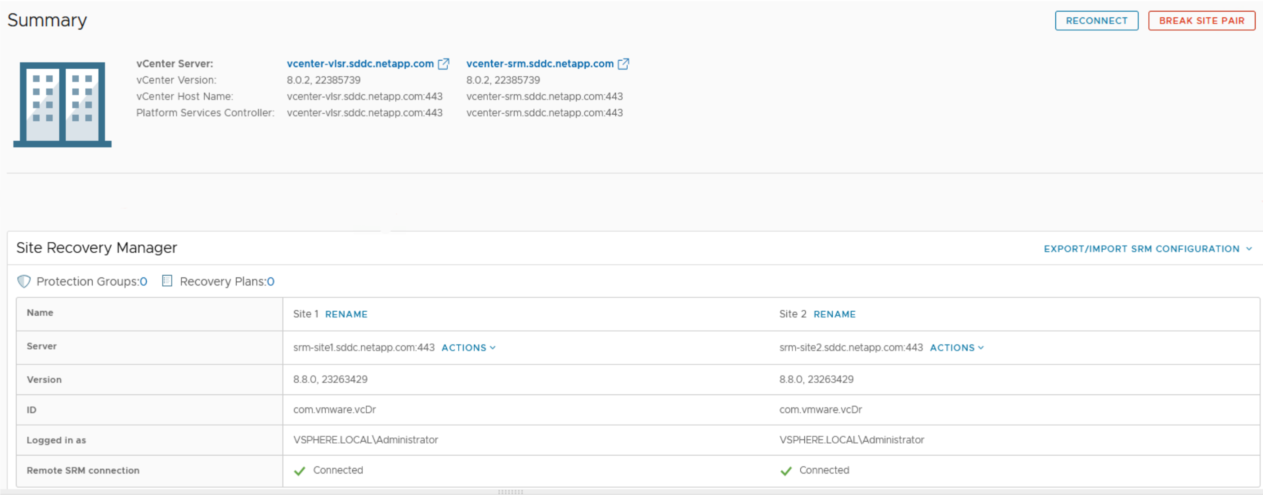


Services

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

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

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



Summary

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

Site Recovery Manager

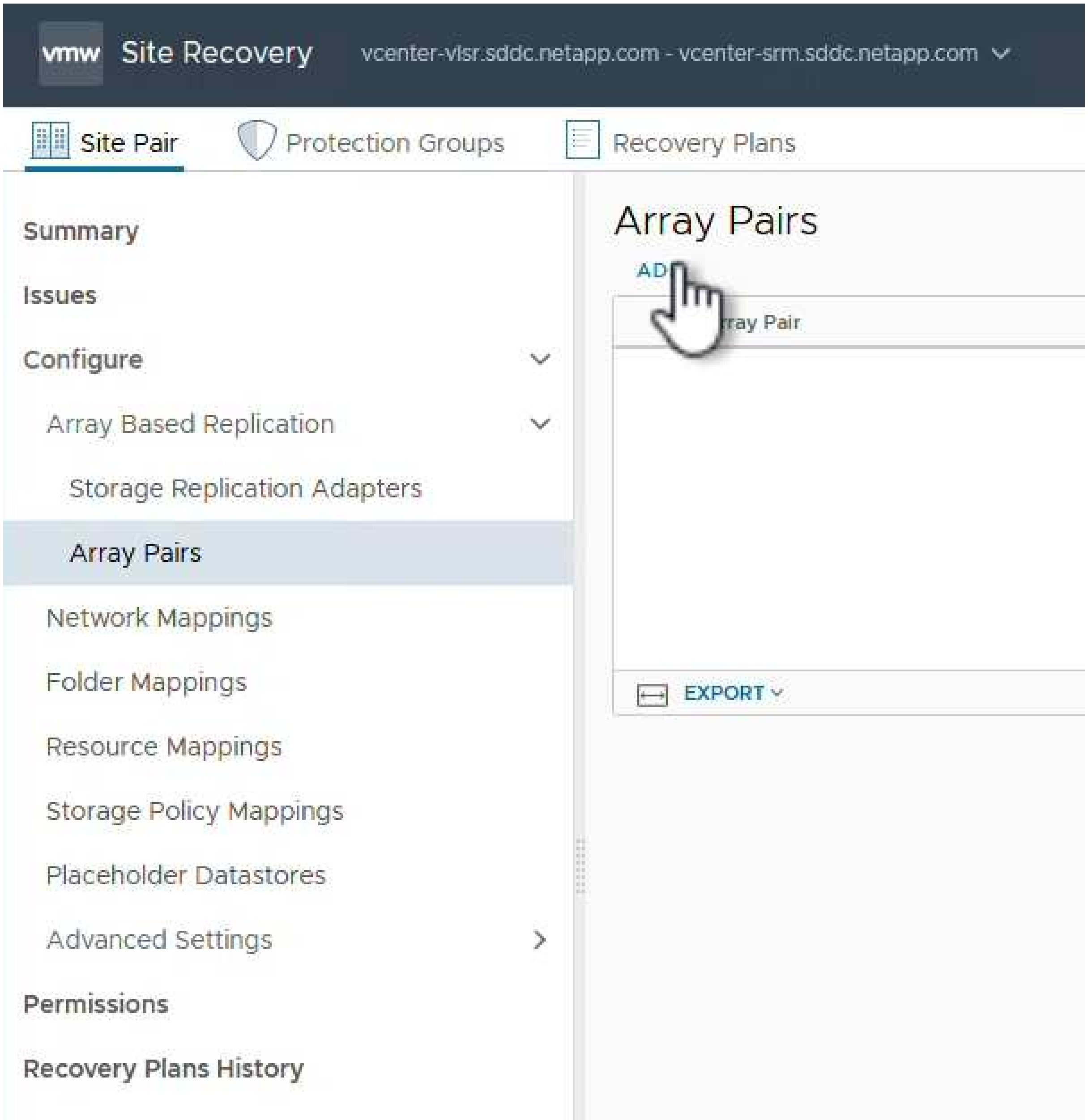
Protection Groups:0 Recovery Plans:0

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

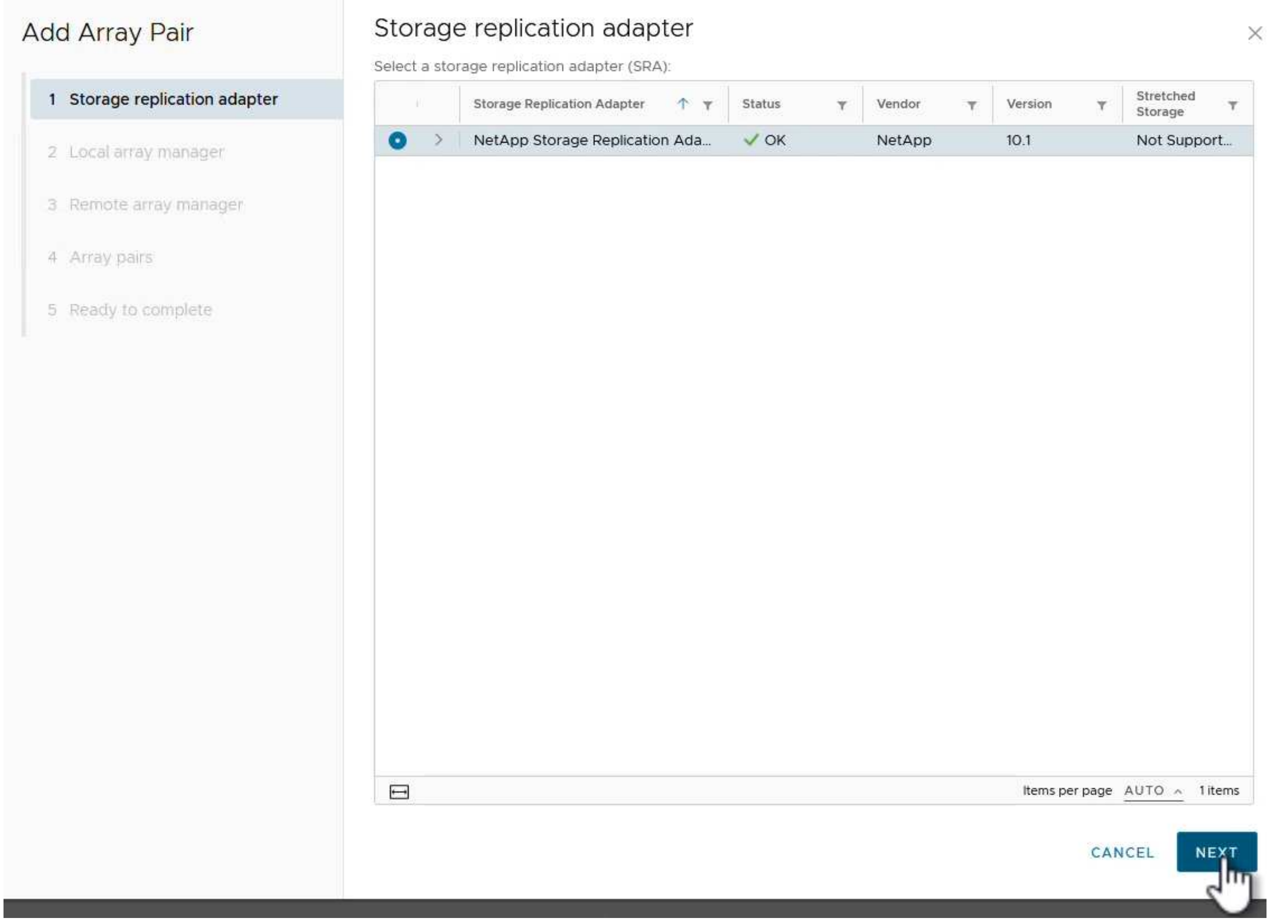
Add an Array Pair for SRM

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

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



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



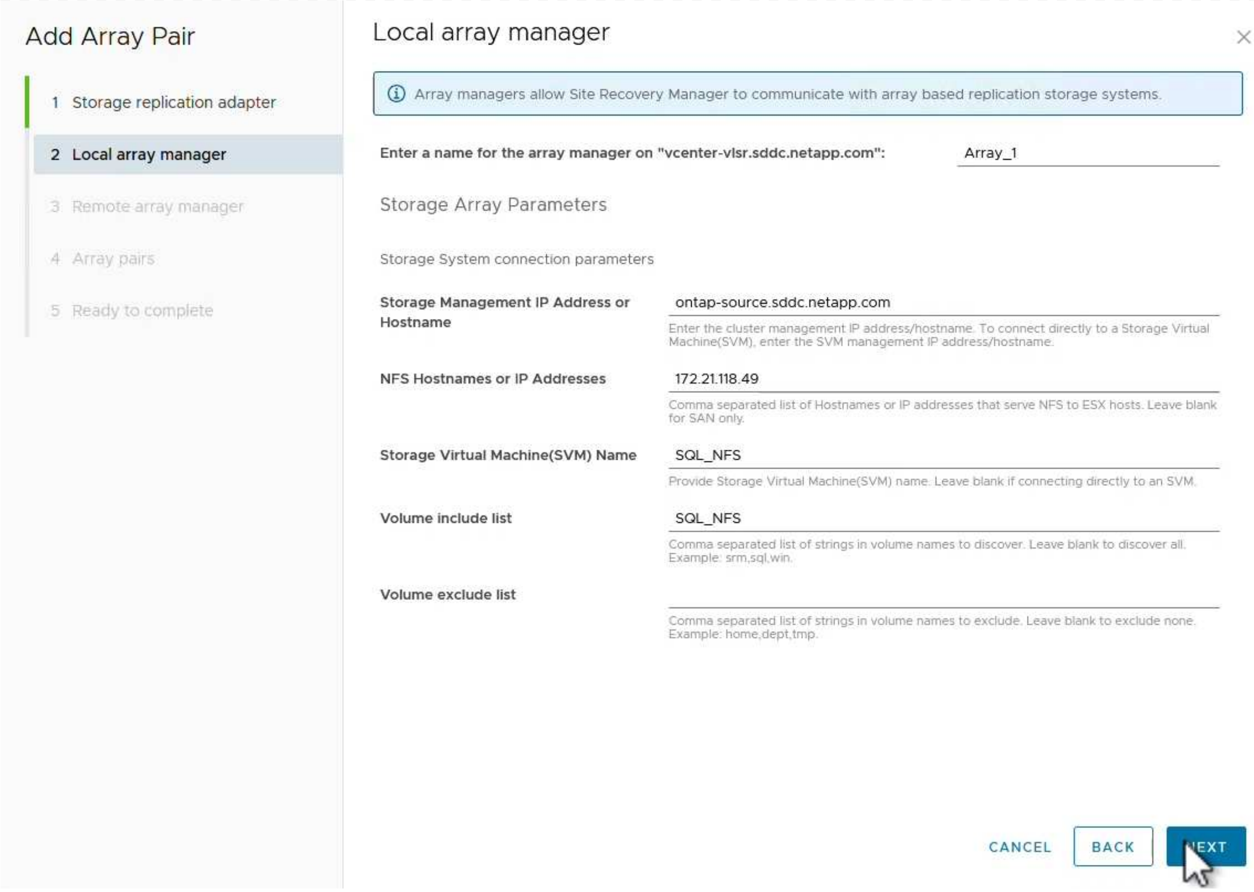
Storage replication adapter

Select a storage replication adapter (SRA):

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

Items per page AUTO 1 items

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



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": Array_1

Storage Array Parameters

Storage System connection parameters

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

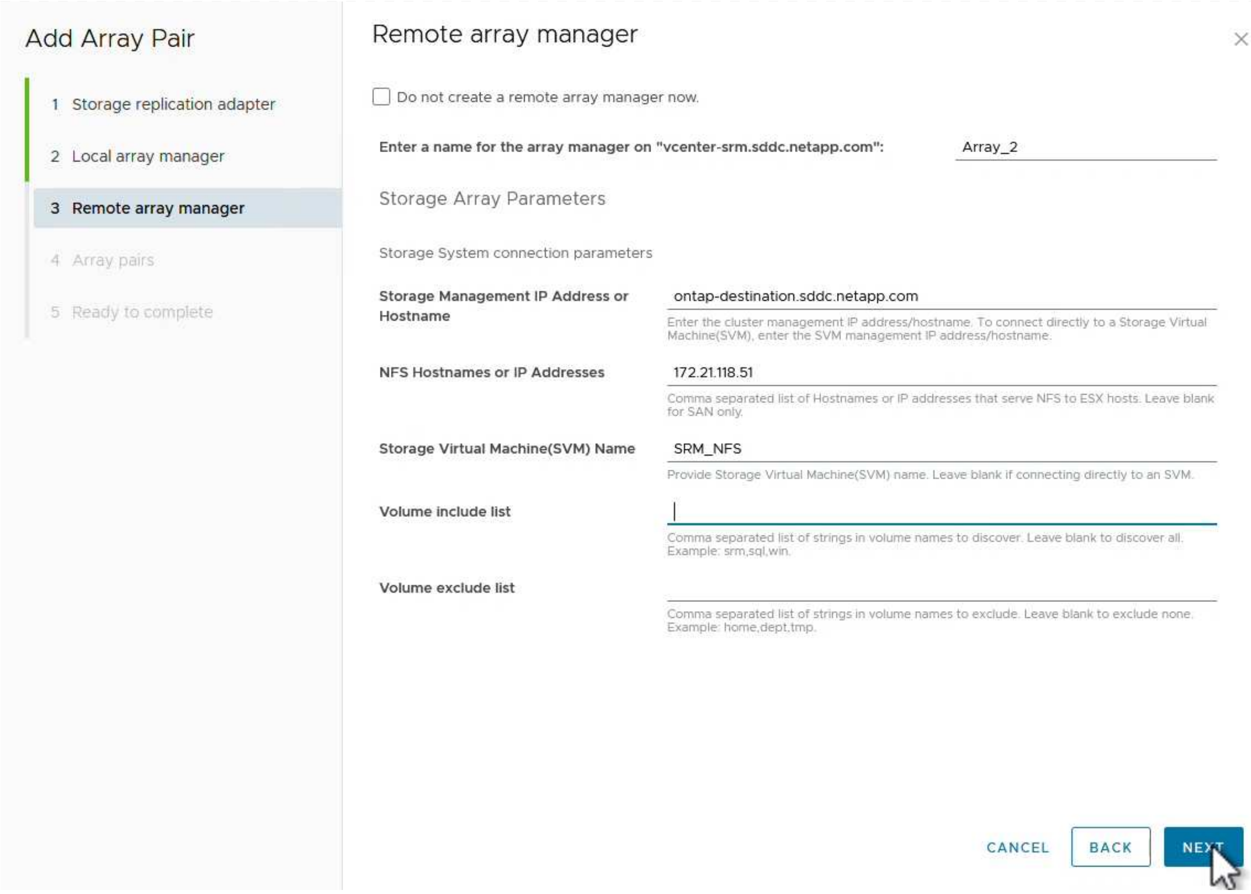
NFS Hostnames or IP Addresses: 172.21.118.49
Comma separated list of Hostnames or IP addresses that serve NFS to ESX hosts. Leave blank for SAN only.

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

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

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

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


Add Array Pair

Remote array manager

☐ Do not create a remote array manager now.

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

Storage Array Parameters

Storage System connection parameters

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

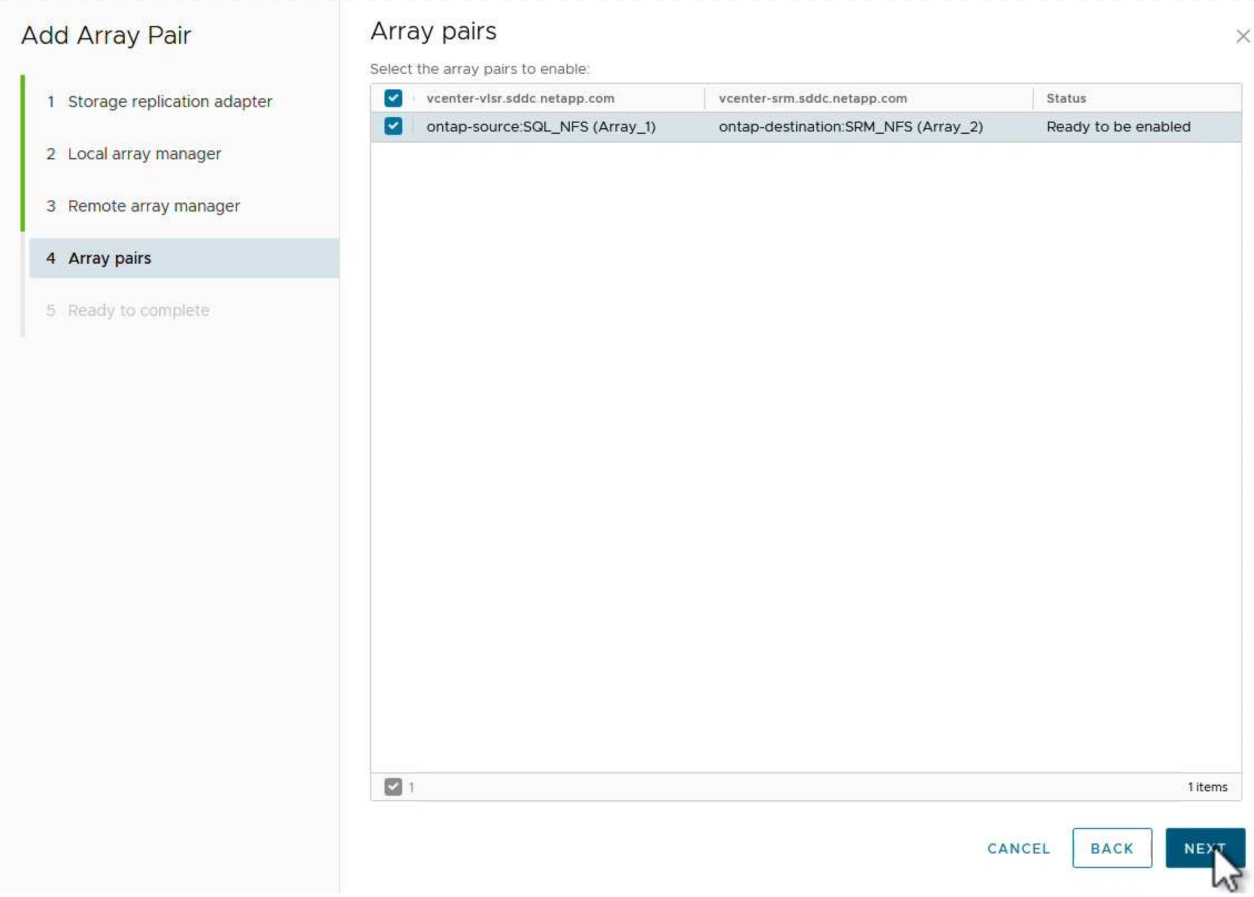
NFS Hostnames or IP Addresses: 172.21.118.51
Comma separated list of Hostnames or IP addresses that serve NFS to ESX hosts. Leave blank for SAN only.

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

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

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

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



Array pairs

Select the array pairs to enable:

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

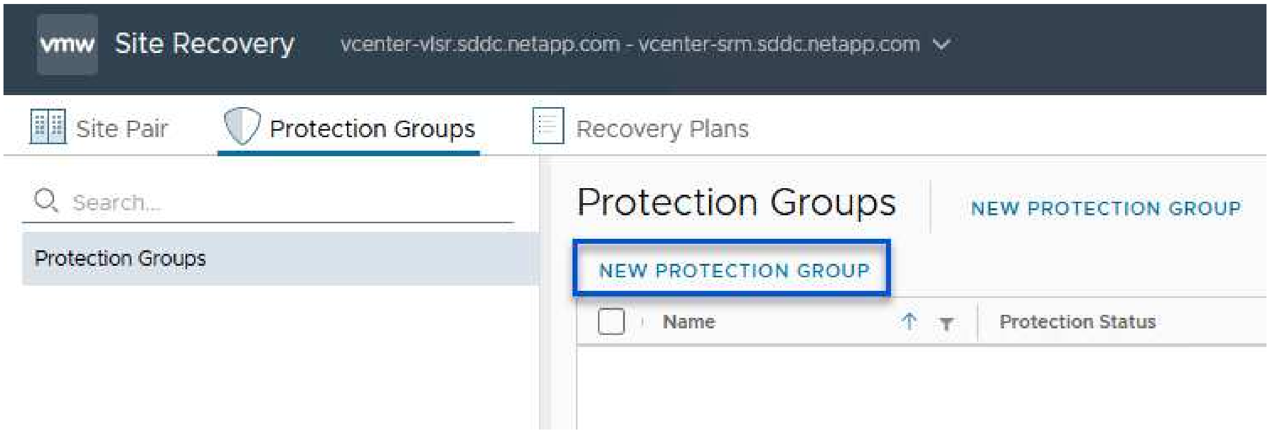
☑ 1 1 items

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

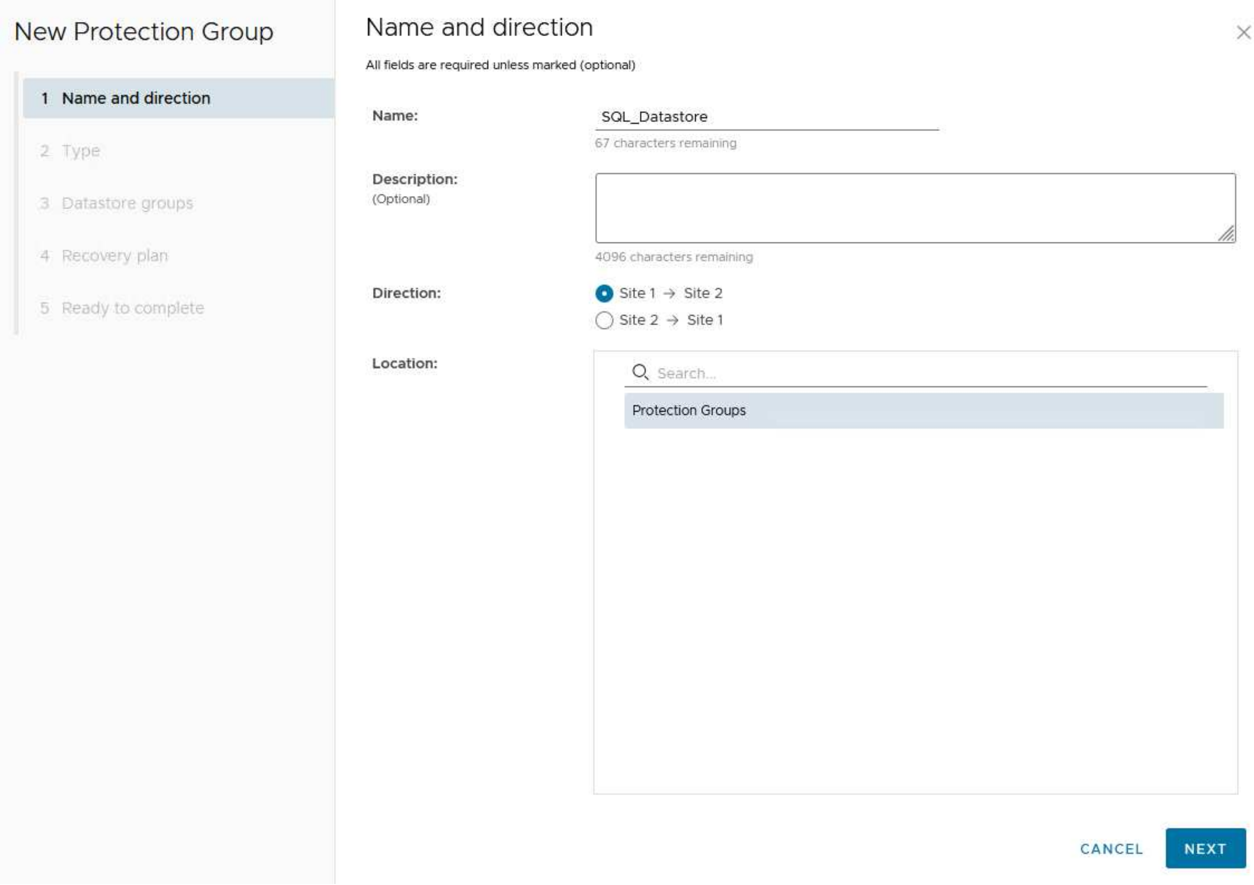
Configure Protection Groups for SRM

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

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



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



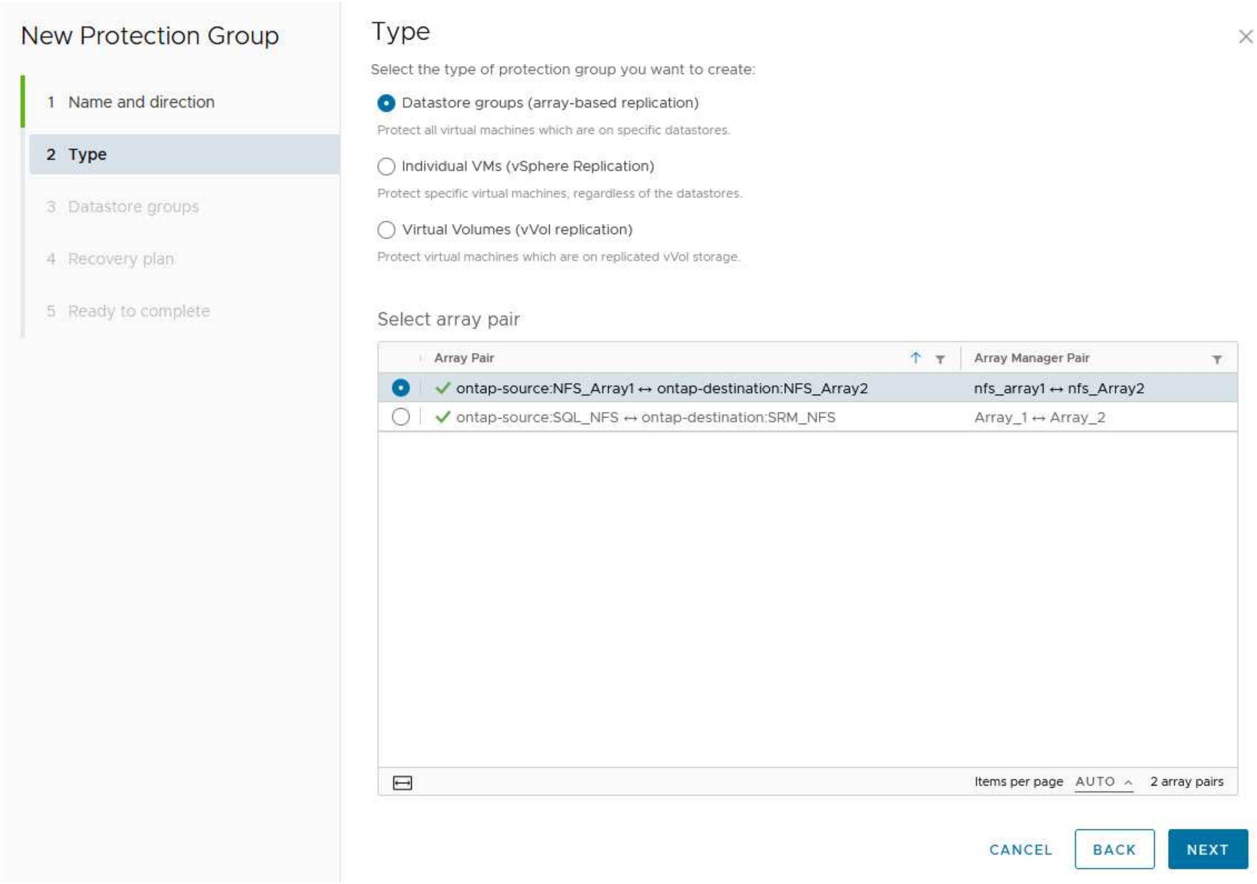
Name: SQL_Datastore
67 characters remaining

Description: (Optional)
4096 characters remaining

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

Location: Protection Groups

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



New Protection Group

1 Name and direction

2 Type

3 Datastore groups

4 Recovery plan

5 Ready to complete

Type

Select the type of protection group you want to create:

● Datastore groups (array-based replication)

Protect all virtual machines which are on specific datastores.

○ Individual VMs (vSphere Replication)

Protect specific virtual machines, regardless of the datastores.

○ Virtual Volumes (vVol replication)

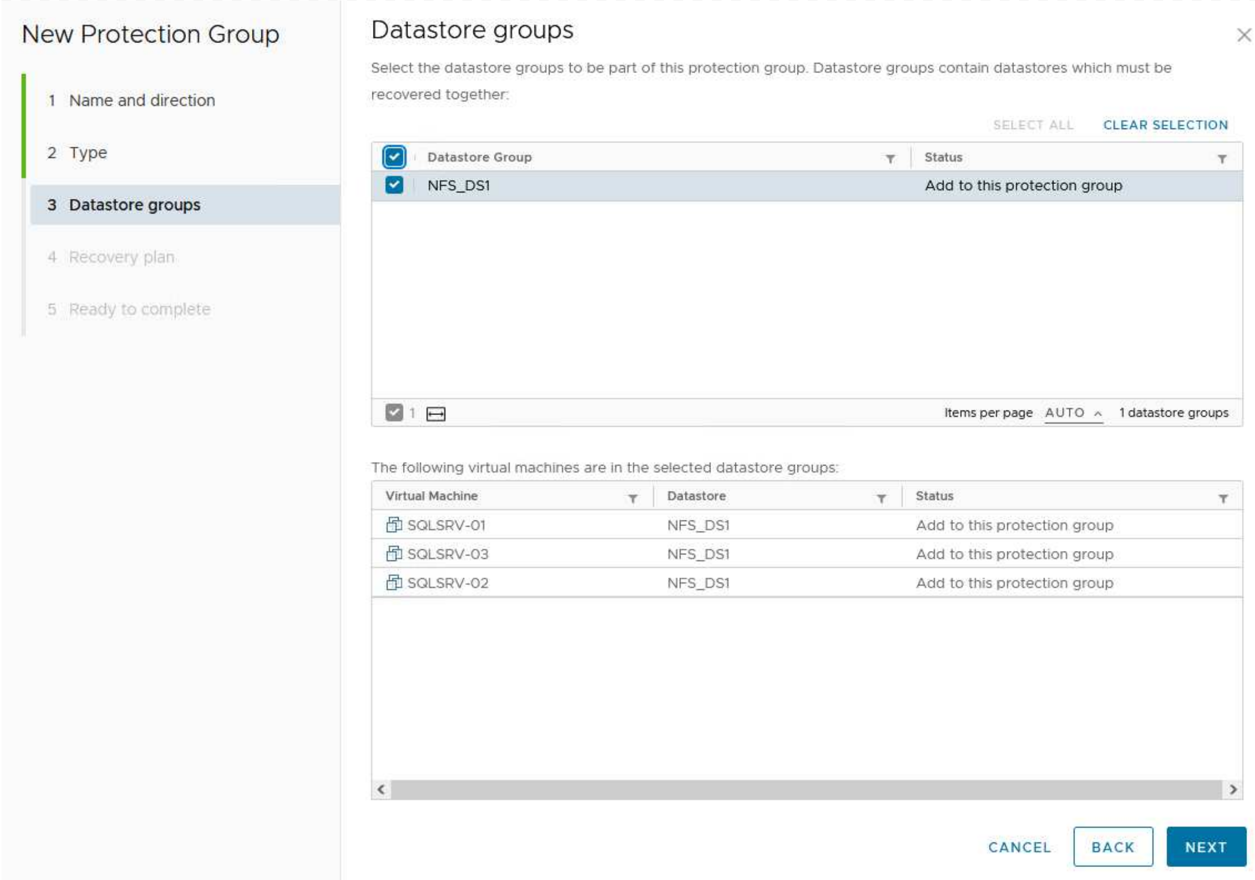
Protect virtual machines which are on replicated vVol storage.

Select array pair

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

Items per page AUTO 2 array pairs

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


New Protection Group

1 Name and direction

2 Type

3 Datastore groups

4 Recovery plan

5 Ready to complete

Datastore groups

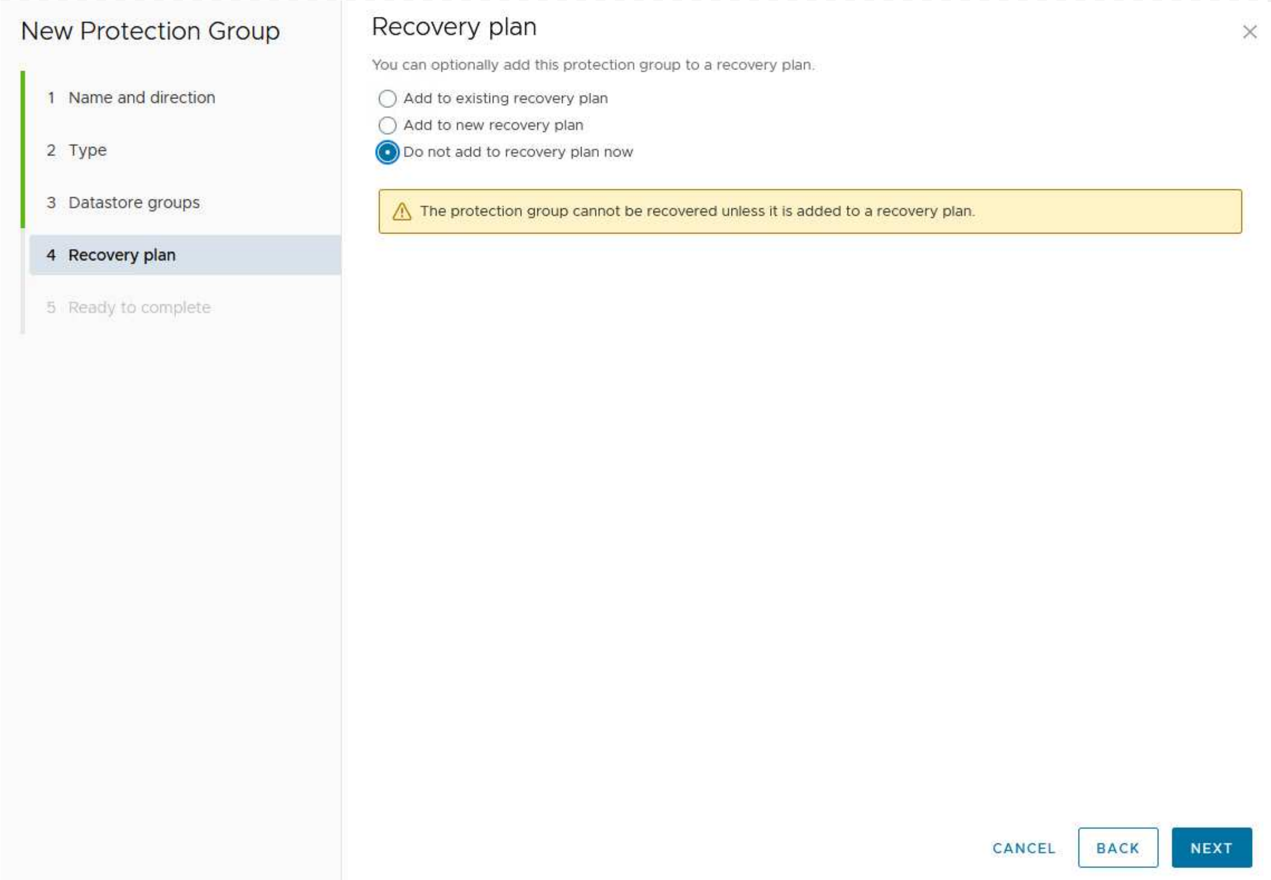
Select the datastore groups to be part of this protection group. Datastore groups contain datastores which must be recovered together:

☑	Datastore Group	Status
☑	NFS_DS1	Add to this protection group

The following virtual machines are in the selected datastore groups:

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

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



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.

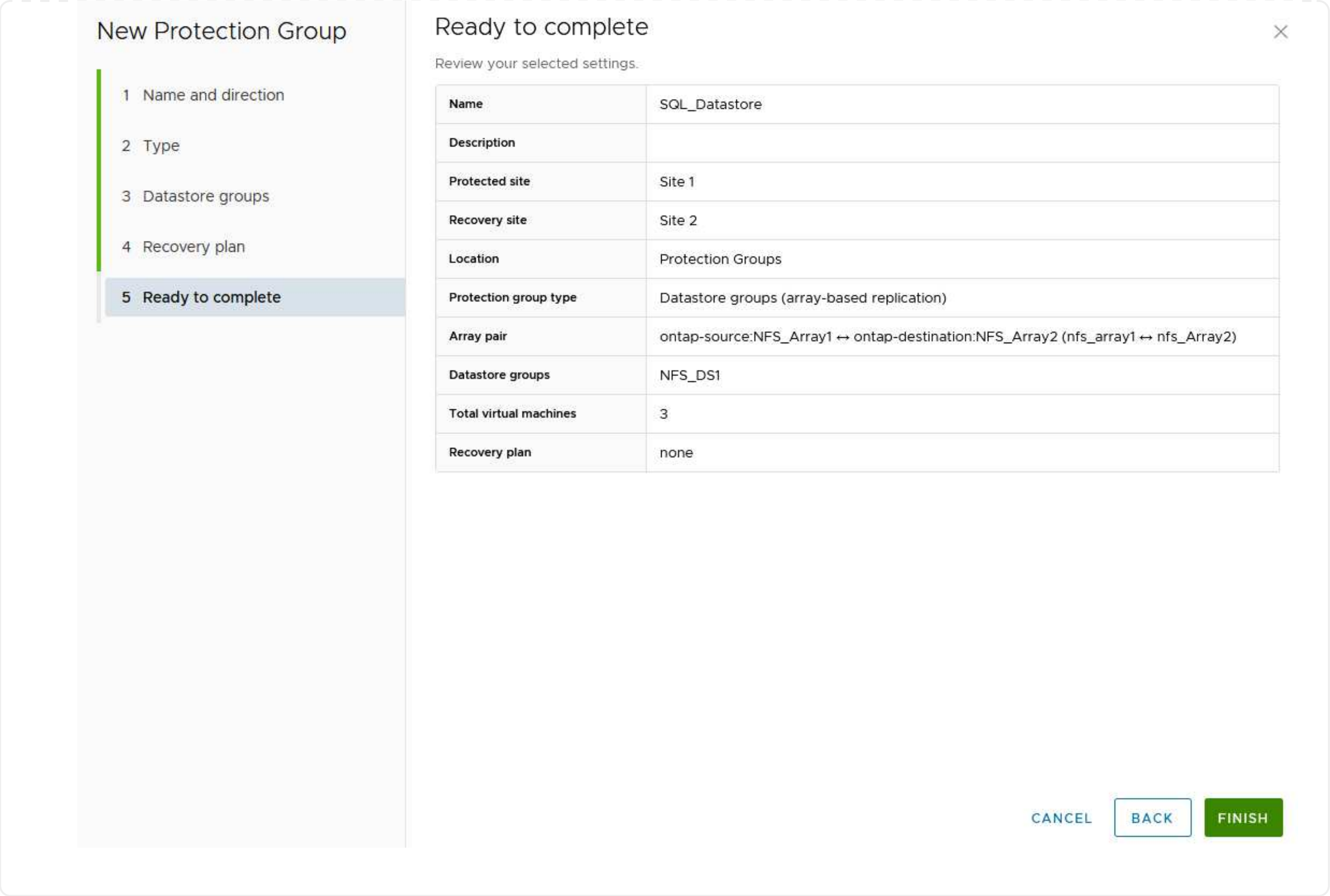
○ Add to existing recovery plan

○ 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.

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



Ready to complete

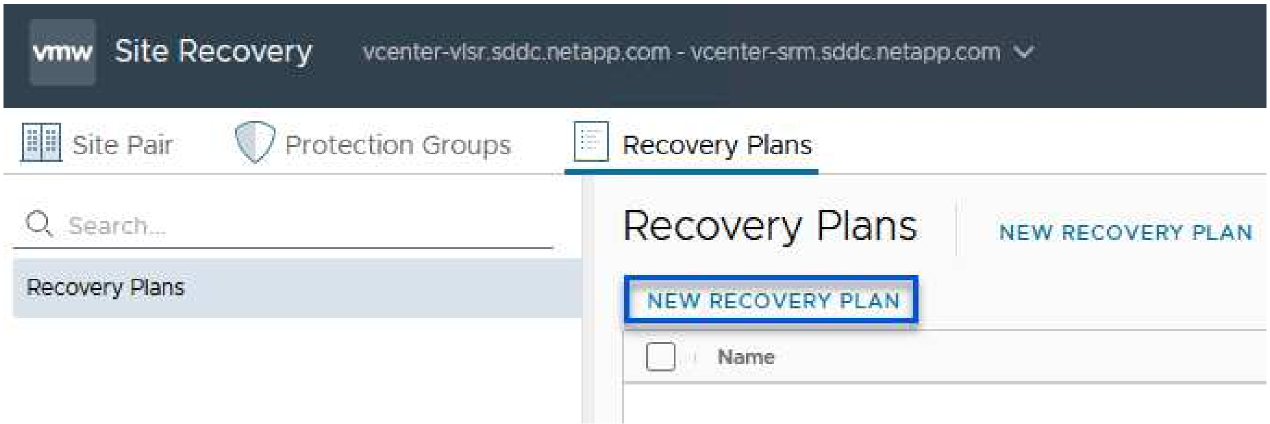
Review your selected settings.

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

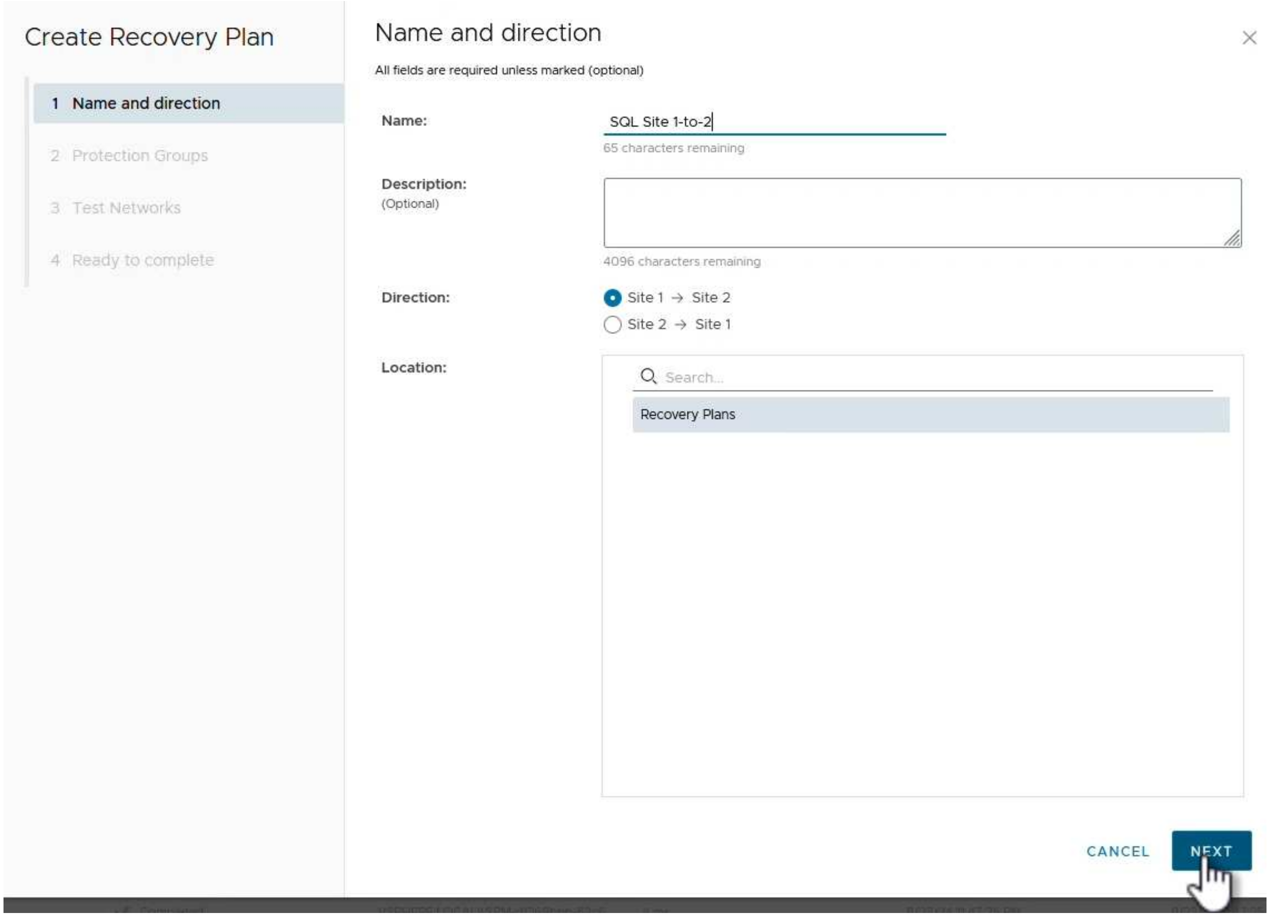
Configure Recovery Plan for SRM

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

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



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



All fields are required unless marked (optional)

Name: SQL Site 1-to-2

65 characters remaining

Description: (Optional)

4096 characters remaining

Direction:

● Site 1 → Site 2

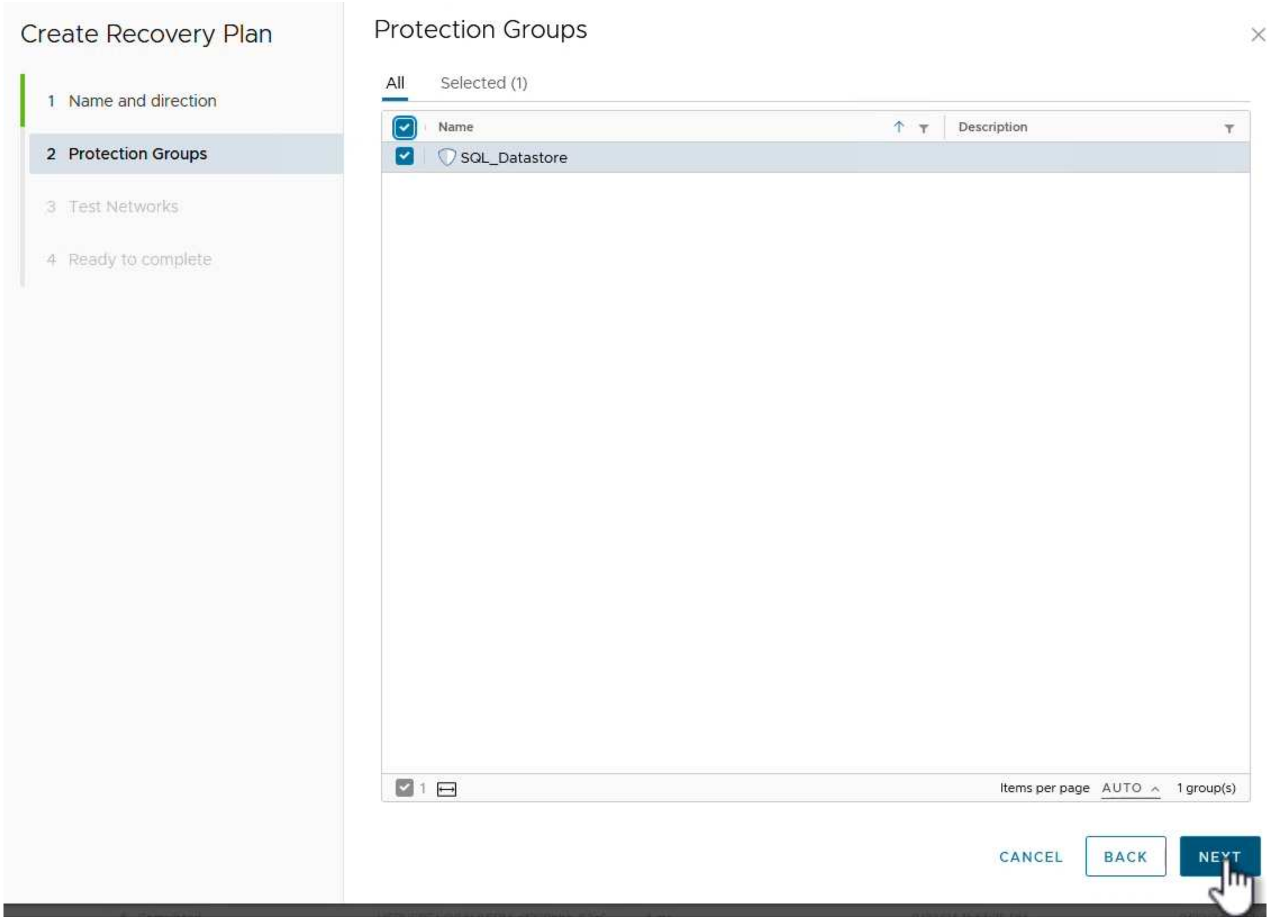
○ Site 2 → Site 1

Location:

Search...

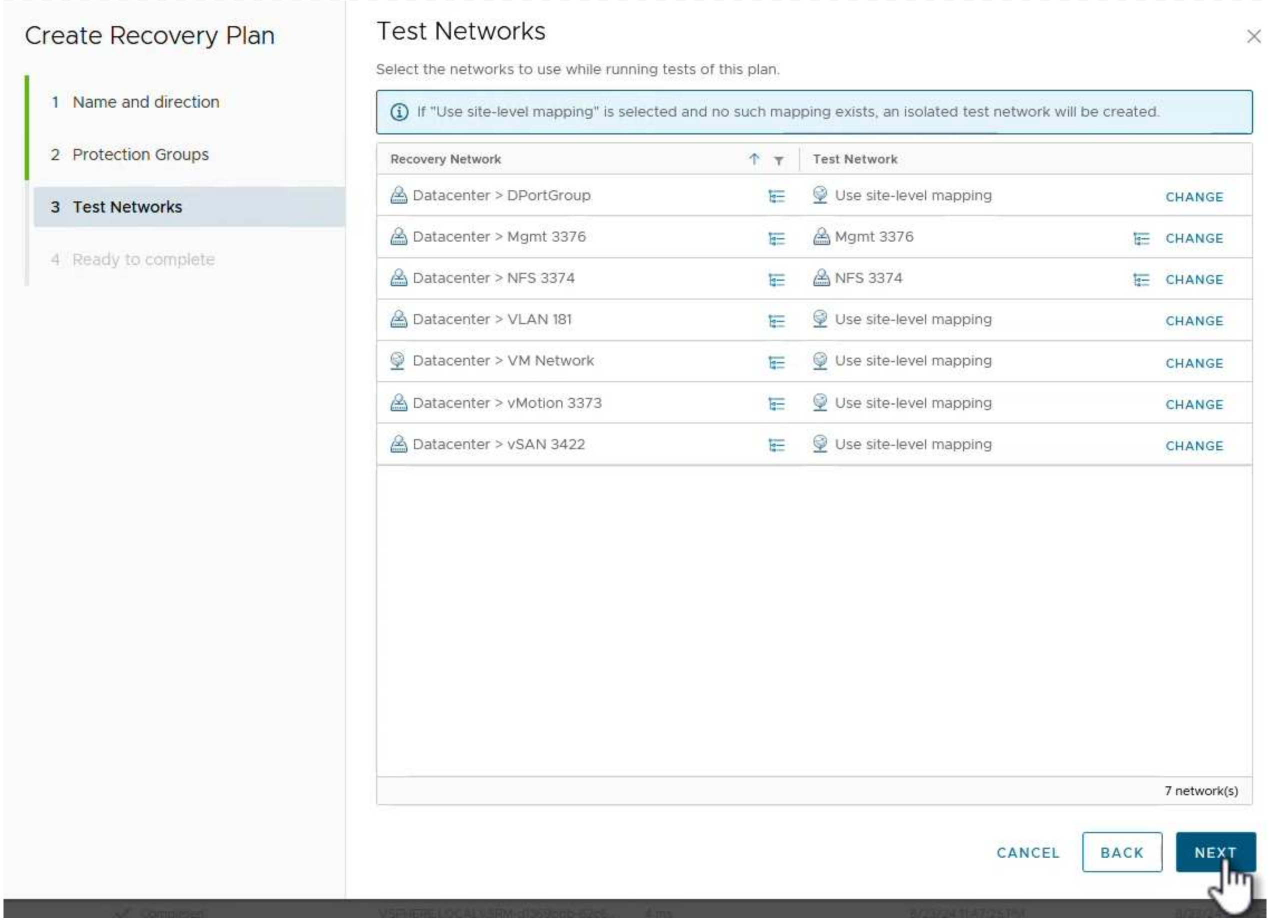
Recovery Plans

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



☑ SQL_Datastore

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



Create Recovery Plan

1 Name and direction

2 Protection Groups

3 Test Networks

4 Ready to complete

Test Networks

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

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

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

7 network(s)

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

Disaster recovery operations with SRM

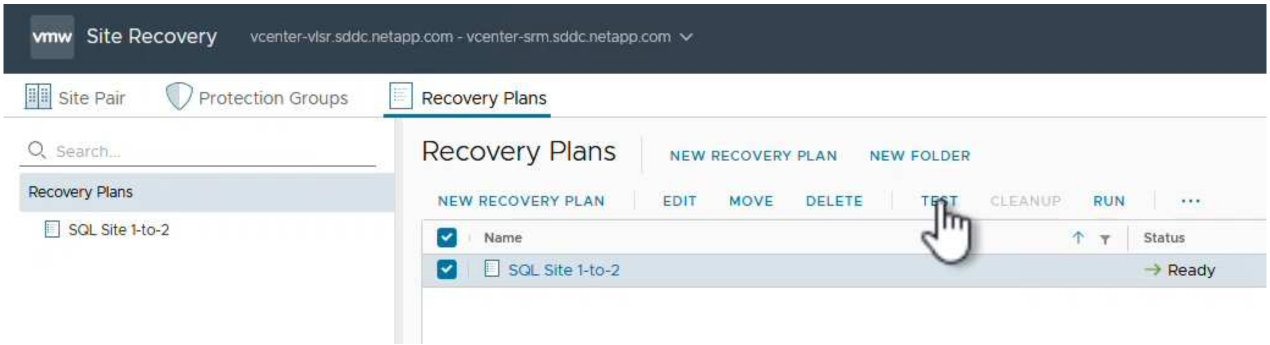
In this section various functions of using disaster recovery with SRM will be covered including, testing failover, performing failover, performing reprotection and failback.

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

Testing failover with SRM

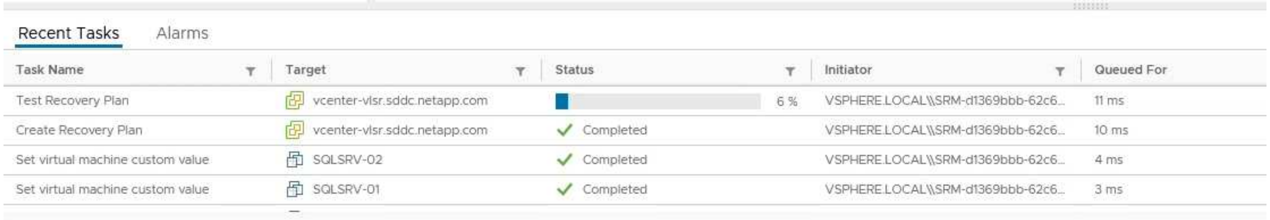
The following step is completed in the Site Recovery interface.

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



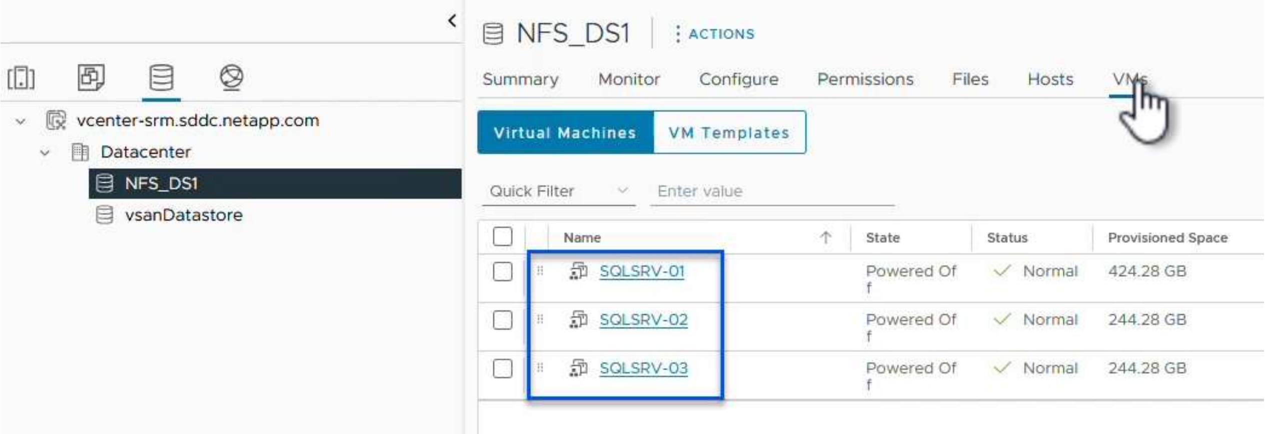
☑	Name	Status
☑	SQL Site 1-to-2	→ Ready

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



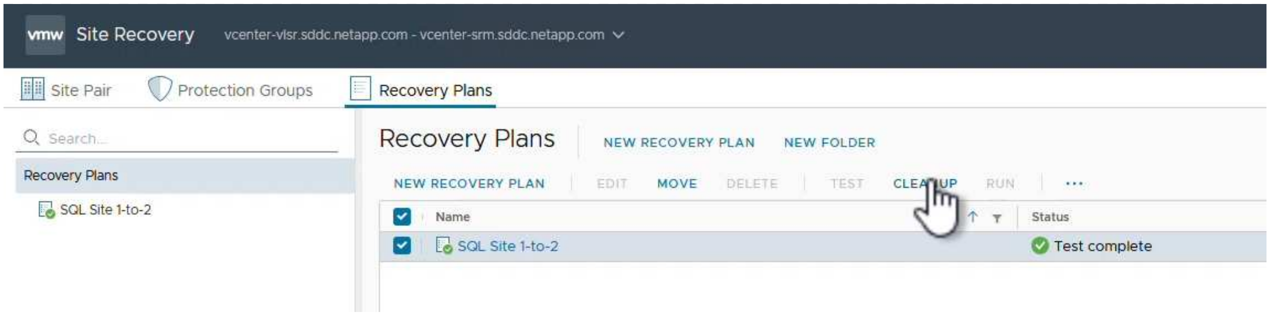
Task Name	Target	Status	Initiator	Queued For
Test Recovery Plan	vcenter-vlsr.sddc.netapp.com	6 %	VSPHERE.LOCAL\\SRM-d1369bbb-62c6...	11 ms
Create Recovery Plan	vcenter-vlsr.sddc.netapp.com	✓ Completed	VSPHERE.LOCAL\\SRM-d1369bbb-62c6...	10 ms
Set virtual machine custom value	SQLSRV-02	✓ Completed	VSPHERE.LOCAL\\SRM-d1369bbb-62c6...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

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



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

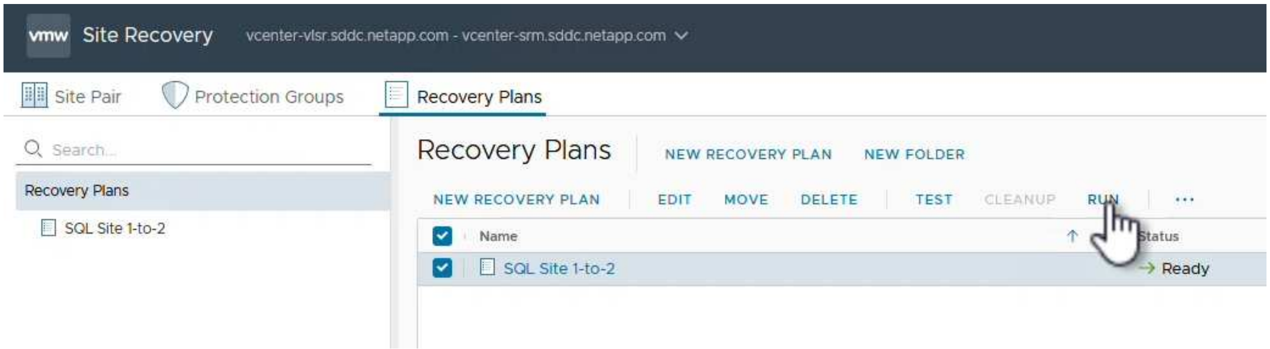
4. Once the test has completed, click on **Cleanup** to unmount the datastore and revert back to the original environment.



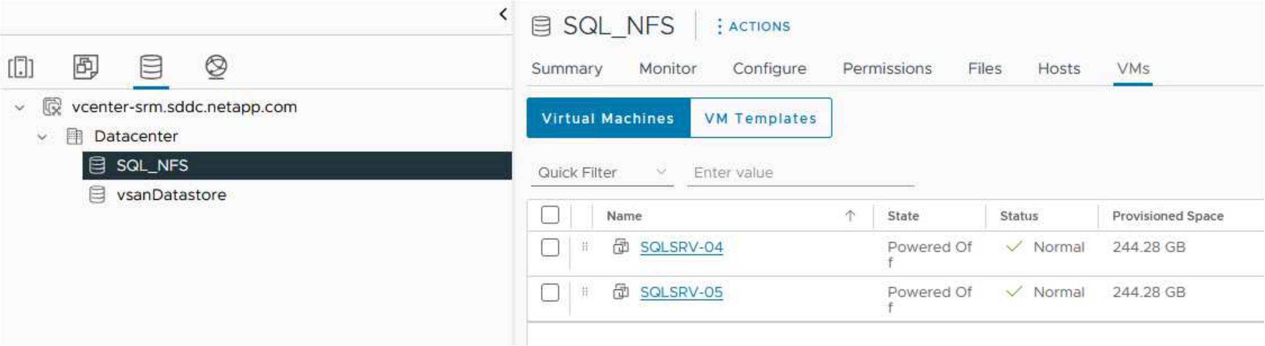
Run Recovery Plan with SRM

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.



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

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

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

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

Additional information

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

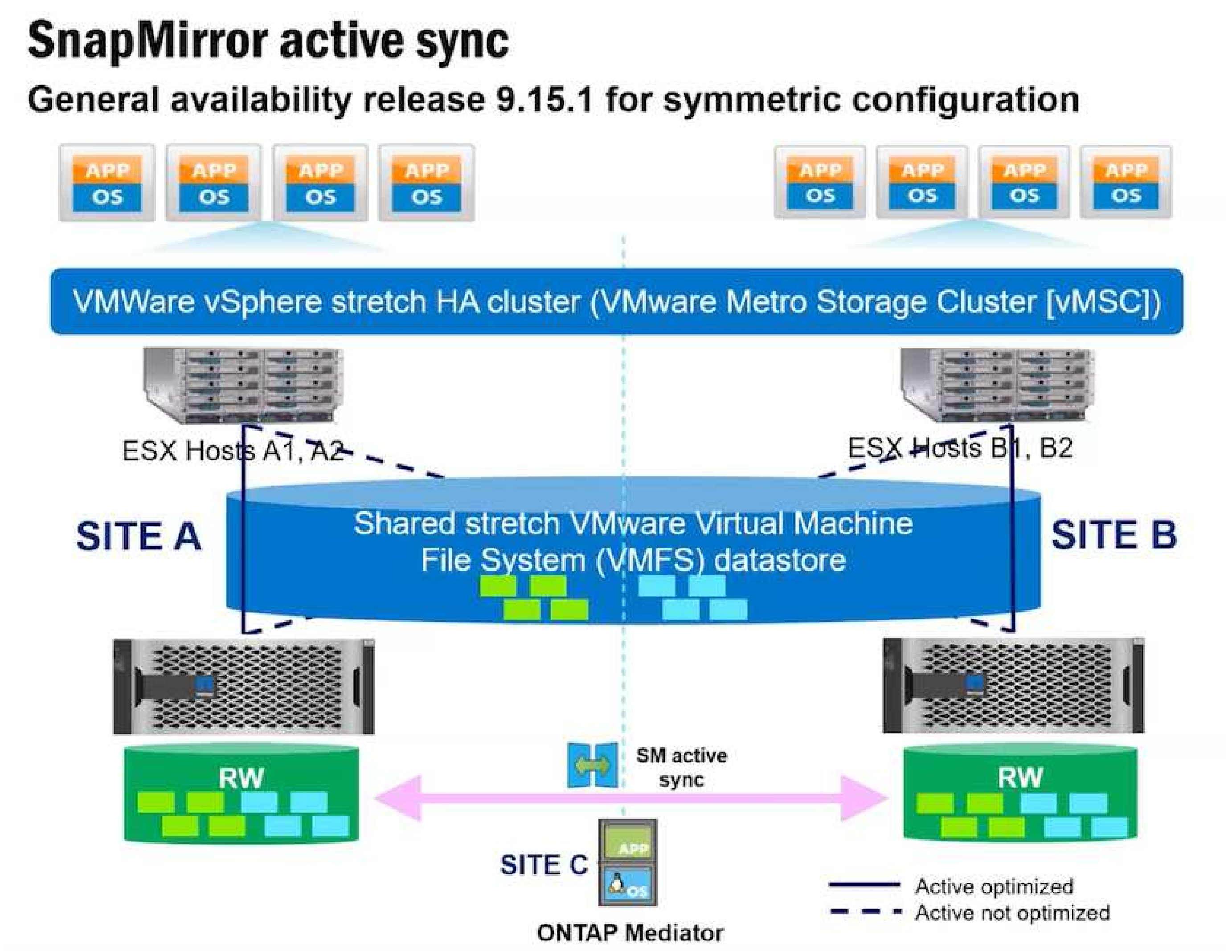
For information on configuring ONTAP storage systems refer to the ONTAP 9 Documentation center.

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

VMware vSphere Metro Storage Cluster with SnapMirror active sync

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

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



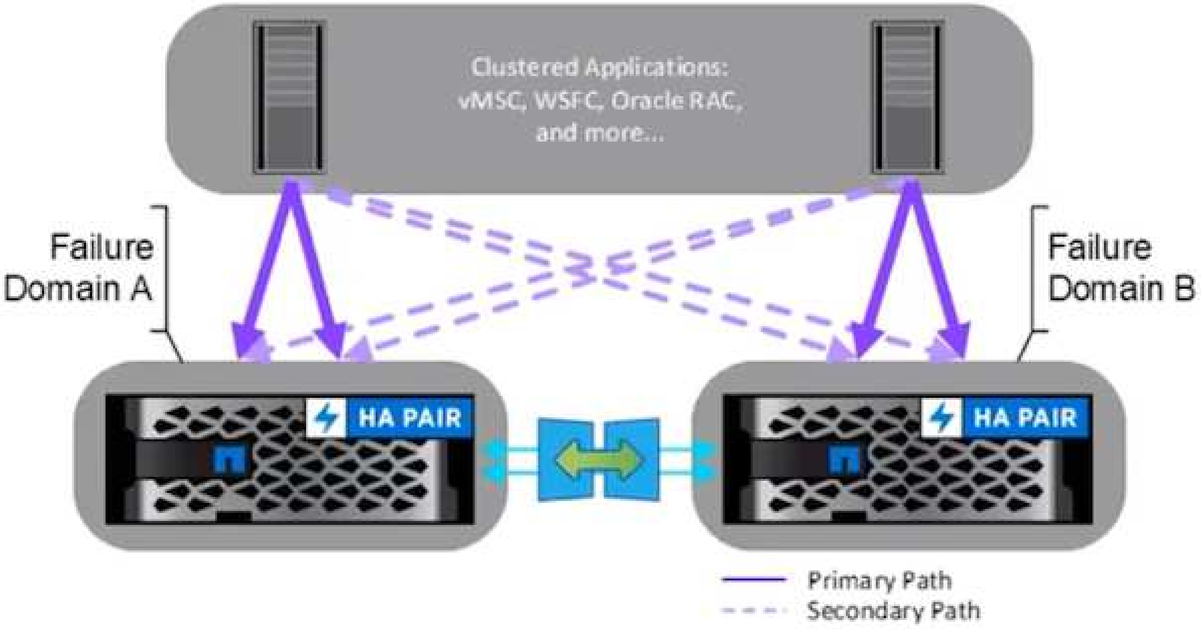
SnapMirror active sync

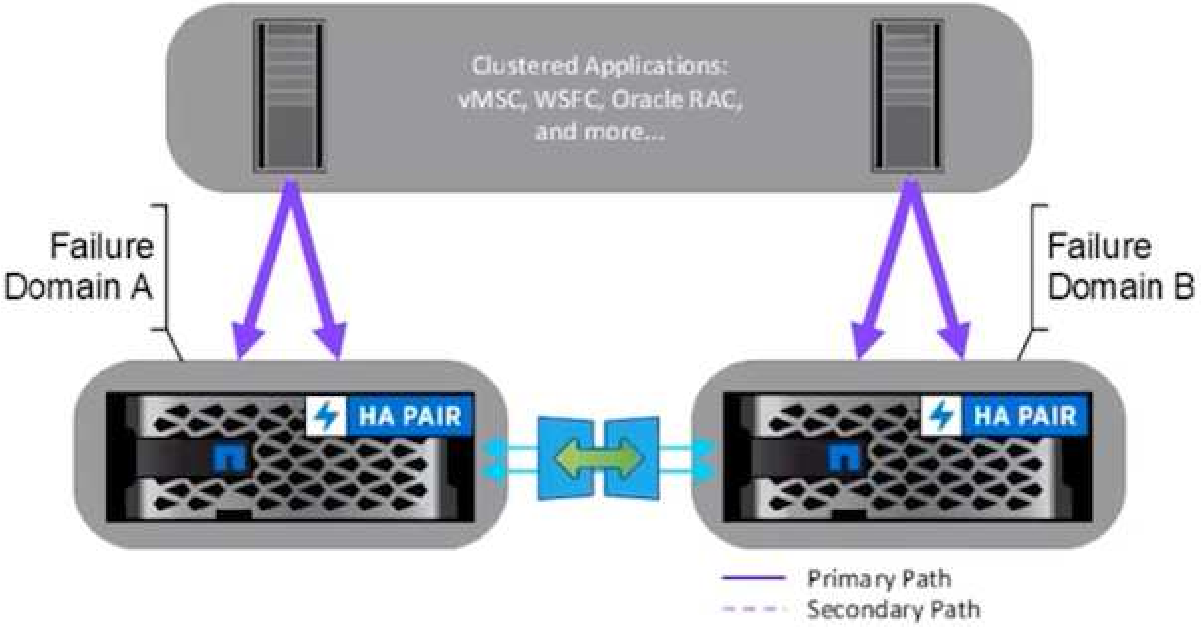
General availability release 9.15.1 for symmetric configuration

APP
OS
VMWare vSphere stretch HA cluster (VMware Metro Storage Cluster [vMSC])
ESX Hosts A1, A2
ESX Hosts B1, B2
SITE A
SITE B
Shared stretch VMware Virtual Machine File System (VMFS) datastore
RW
RW
SM active sync
SITE C
APP
OS
ONTAP Mediator
Active optimized
Active not optimized

SnapMirror active sync supports ASA, AFF and FAS storage arrays. It is recommended to use same type (Performance/Capacity models) on both fault domains. Currently, only block protocols like FC and iSCSI are supported. For further support guidelines, refer Interoperability Matrix Tool and Hardware Universe

vMSC supports two different deployment models named Uniform host access and Non-uniform host access. In Uniform host access configuration, every host on the cluster has access to LUN on both fault domains. It is typically used in different availability zones in same datacenter.





In Non-Uniform host access configuration, host has access only to local fault domain. It is typically used in different sites where running multiple cables across the fault domains are restrictive option.

In Non-Uniform host access mode, the VMs will be restarted in other fault domain by vSphere HA. Application availability will be impacted based on its design. Non-Uniform host access mode is supported only with ONTAP 9.15 onwards.

Prerequisites

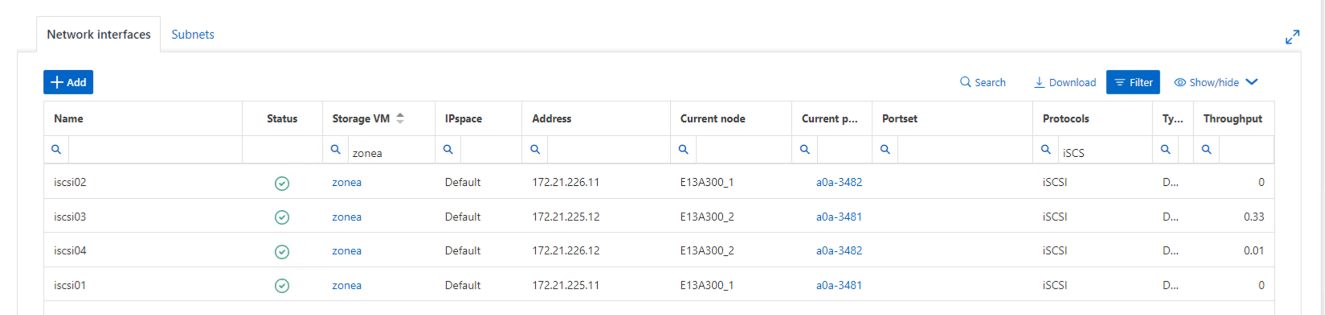
- VMware vSphere hosts deployed with dual storage fabric (Two HBAs or Dual VLAN for iSCSI) per host.
- Storage Arrays are deployed with link aggregation for data ports (for iSCSI).
- Storage VM and LIFs are available
- Inter-Cluster latency round trip time must be less than 10 milliseconds.
- ONTAP Mediator VM is deployed on different fault domain
- Cluster Peer relationship is established
- SVM Peer relationship is established
- ONTAP Mediator registered to ONTAP cluster

If using self-signed certificate, the CA certificate can be retrieved from the <installation path>/ontap_mediator/server_config/ca.crt on mediator VM.

vMSC non-uniform host access with ONTAP System Manager UI.

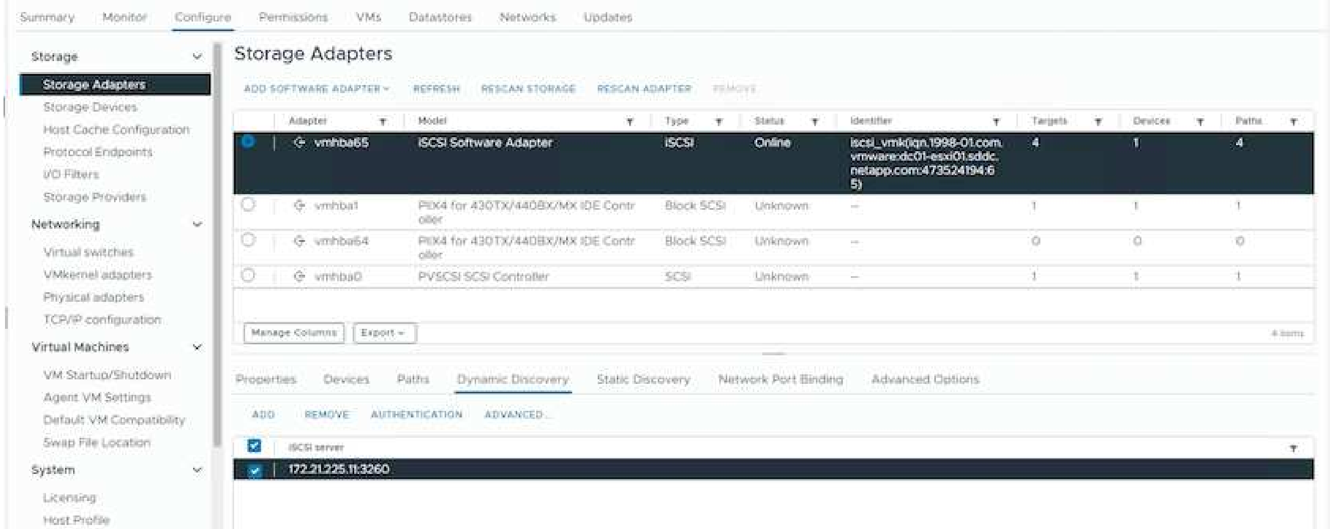
Note: ONTAP Tools 10.2 or above can be used to provision stretched datastore with non-uniform host access mode without switching multiple user interfaces. This section is just for reference if ONTAP Tools is not used.

1. Note down one of the iSCSI data lif IP address from the local fault domain storage array.



Name	Status	Storage VM	IPspace	Address	Current node	Current p...	Portset	Protocols	Ty...	Throughput
		zonea						iSCS		
iscsi02	✓	zonea	Default	172.21.226.11	E13A300_1	a0a-3482		iSCSI	D...	0
iscsi03	✓	zonea	Default	172.21.225.12	E13A300_2	a0a-3481		iSCSI	D...	0.33
iscsi04	✓	zonea	Default	172.21.226.12	E13A300_2	a0a-3482		iSCSI	D...	0.01
iscsi01	✓	zonea	Default	172.21.225.11	E13A300_1	a0a-3481		iSCSI	D...	0

2. On vSphere host iSCSI Storage Adapter, add that iSCSI IP under the Dynamic Discovery tab.

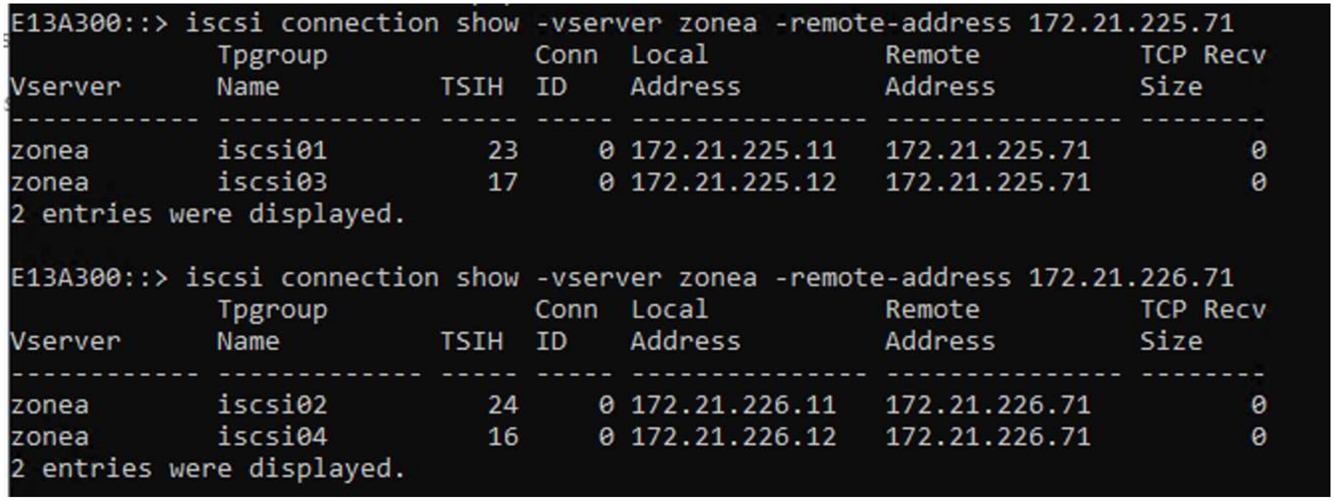


	Adapter	Model	Type	Status	Identifier	Targets	Devices	Paths
●	vmhba65	iSCSI Software Adapter	iSCSI	Online	iscsi_vmk(iqn.1998-01.com.vmware:dc01-esxi01.sddc.netapp.com:473524194:65)	4	1	4
○	vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	1	1	1
○	vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	0	0	0
○	vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	1	1	1

☑	iSCSI server
☑	172.21.225.11:3260

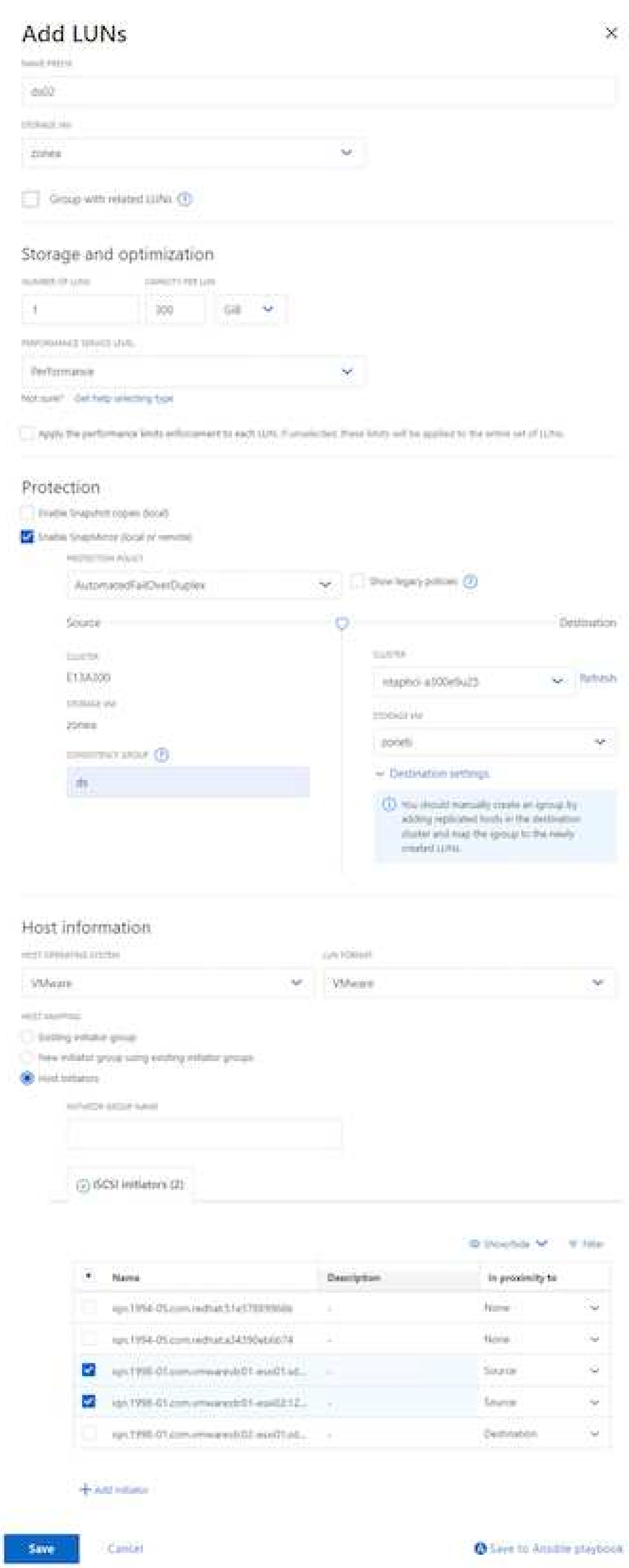
For Uniform access mode, need to provide the source and target fault domain iSCSI data lif address.

3. Repeat the above step on vSphere hosts for the other fault domain adding its local iSCSI data lif IP on Dynamic Discovery tab.
4. With proper network connectivity, four iSCSI connection should exist per vSphere host that has two iSCSI VMKernel nics and two iSCSI data lifs per storage controller.



```
E13A300::> iscsi connection show -vserver zonea -remote-address 172.21.225.71
             Tpgroup              Conn  Local            Remote           TCP Recv
Vserver      Name           TSIH  ID    Address          Address          Size
------------ -------------- ----- ----- ---------------  ---------------  --------
zonea        iscsi01           23     0 172.21.225.11    172.21.225.71           0
zonea        iscsi03           17     0 172.21.225.12    172.21.225.71           0
2 entries were displayed.

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

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



Add LUNs

NAME PREFIX
ds02

STORAGE VM
zonea

☐ Group with related LUNs

Storage and optimization

NUMBER OF LUNS: 1
CAPACITY PER LUN: 300 GiB

PERFORMANCE SERVICE LEVEL
Performance

Not sure? Get help selecting type

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

Protection

☐ Enable Snapshot copies (local)
☑ Enable SnapMirror (local or remote)

PROTECTION POLICY
AutomatedFailOverDuplex
☐ Show legacy policies

Source

CLUSTER
E13A300

STORAGE VM
zonea

CONSISTENCY GROUP
ds

Destination

CLUSTER
ntaphci-a300e9u25
Refresh

STORAGE VM
zoneb

Destination settings

You should manually create an igroup by adding replicated hosts in the destination cluster and map the igroup to the newly created LUNs.

Host information

HOST OPERATING SYSTEM
VMware

LUN FORMAT
VMware

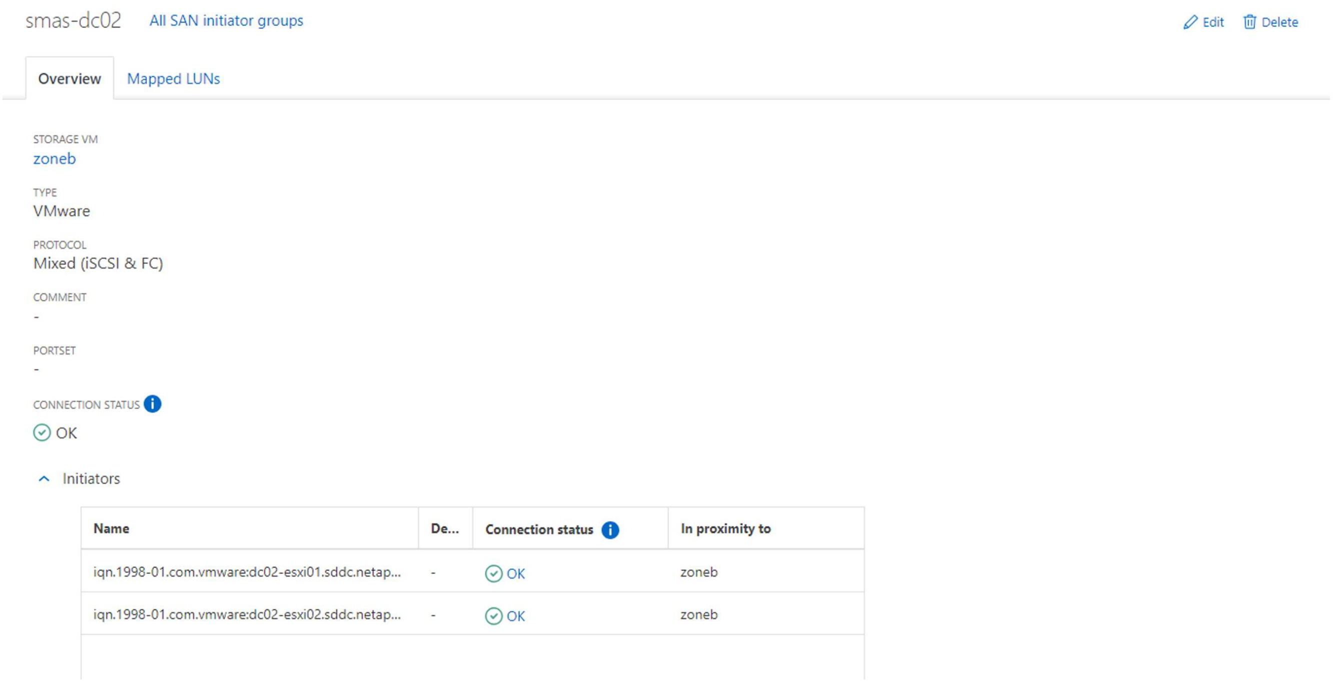
HOST MAPPING
○ Existing initiator group
○ New initiator group using existing initiator groups
● Host initiators

INITIATOR GROUP NAME

iSCSI initiators (2)

	Name	Description	In proximity to
☐	iqn.1994-05.com.redhat:51a57939...	-	None
☐	iqn.1994-05.com.redhat:a34290ebf674	-	None
☑	iqn.1998-01.com.vmware:sb01-esxi01.ad...	-	Source
☑	iqn.1998-01.com.vmware:sb01-esxi02.12...	-	Source
☐	iqn.1998-01.com.vmware:sb02-esxi01.ad...	-	Destination

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



STORAGE VM
zoneb

TYPE
VMware

PROTOCOL
Mixed (iSCSI & FC)

COMMENT
-

PORTSET
-

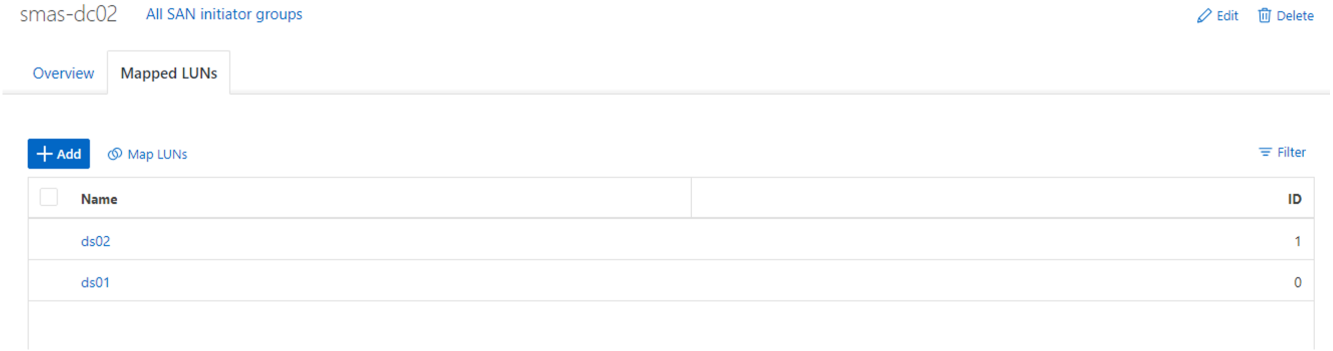
CONNECTION STATUS
OK

Initiators

Name	De...	Connection status	In proximity to
iqn.1998-01.com.vmware:dc02-esxi01.sddc.netap...	-	OK	zoneb
iqn.1998-01.com.vmware:dc02-esxi02.sddc.netap...	-	OK	zoneb

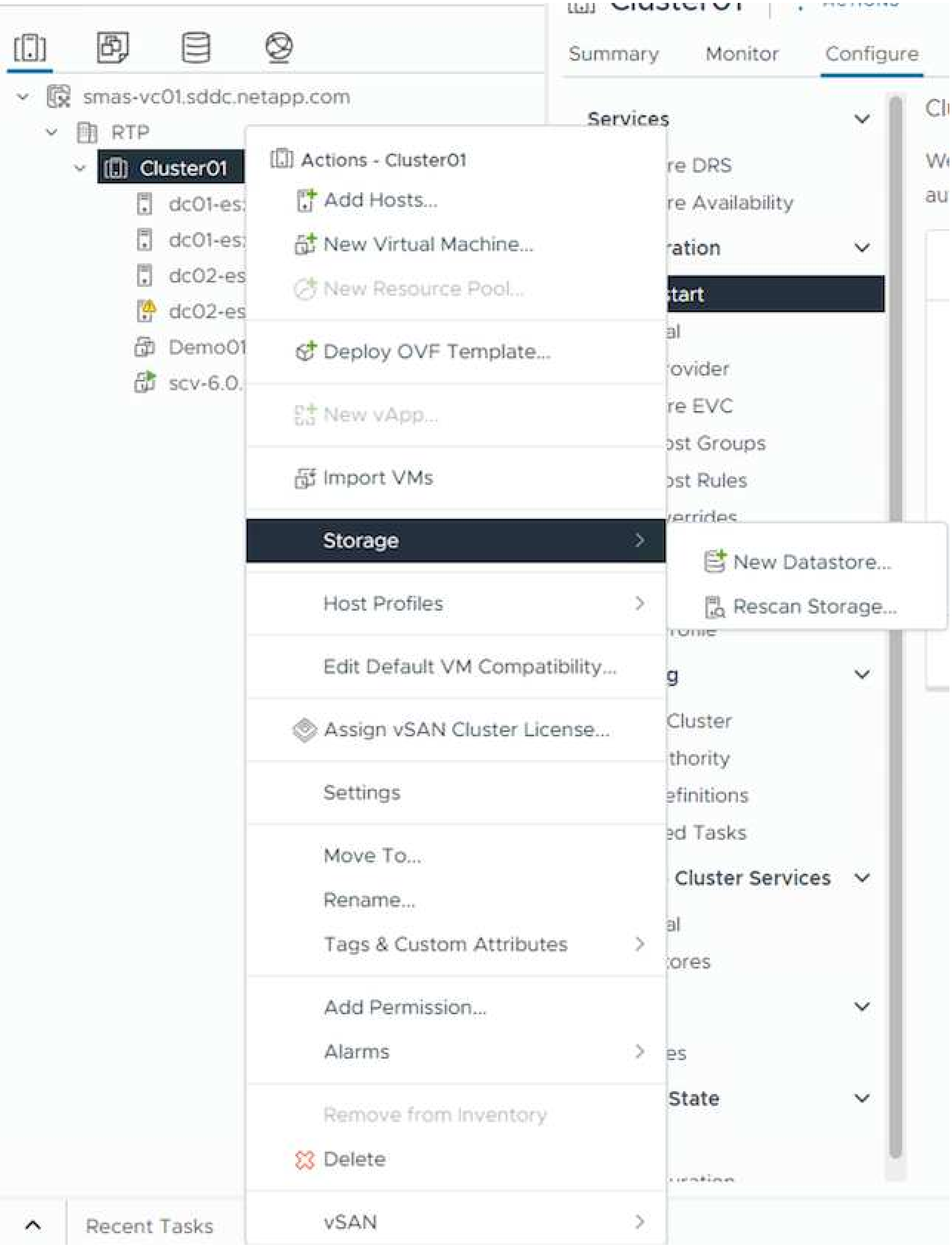
For Uniform access mode, the igroup can be replicated from source fault domain.

7. Map the replicated LUN with same mapping ID as in source fault domain.

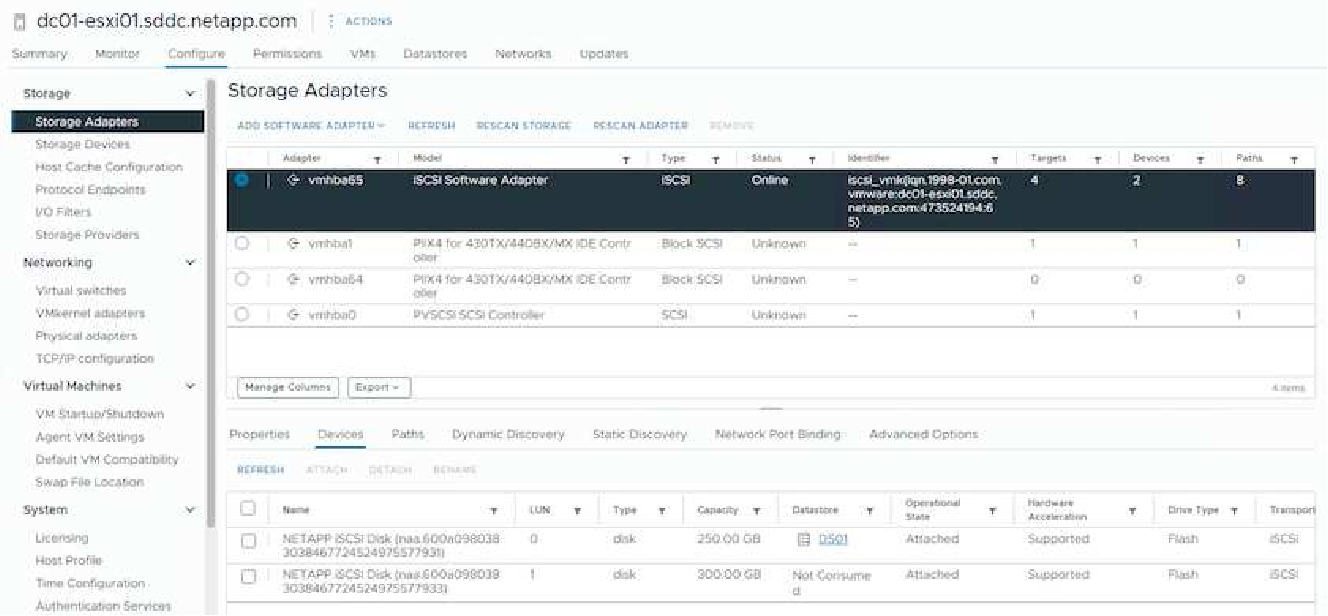


Name	ID
ds02	1
ds01	0

8. On vCenter, right click on vSphere Cluster and select Rescan Storage option.



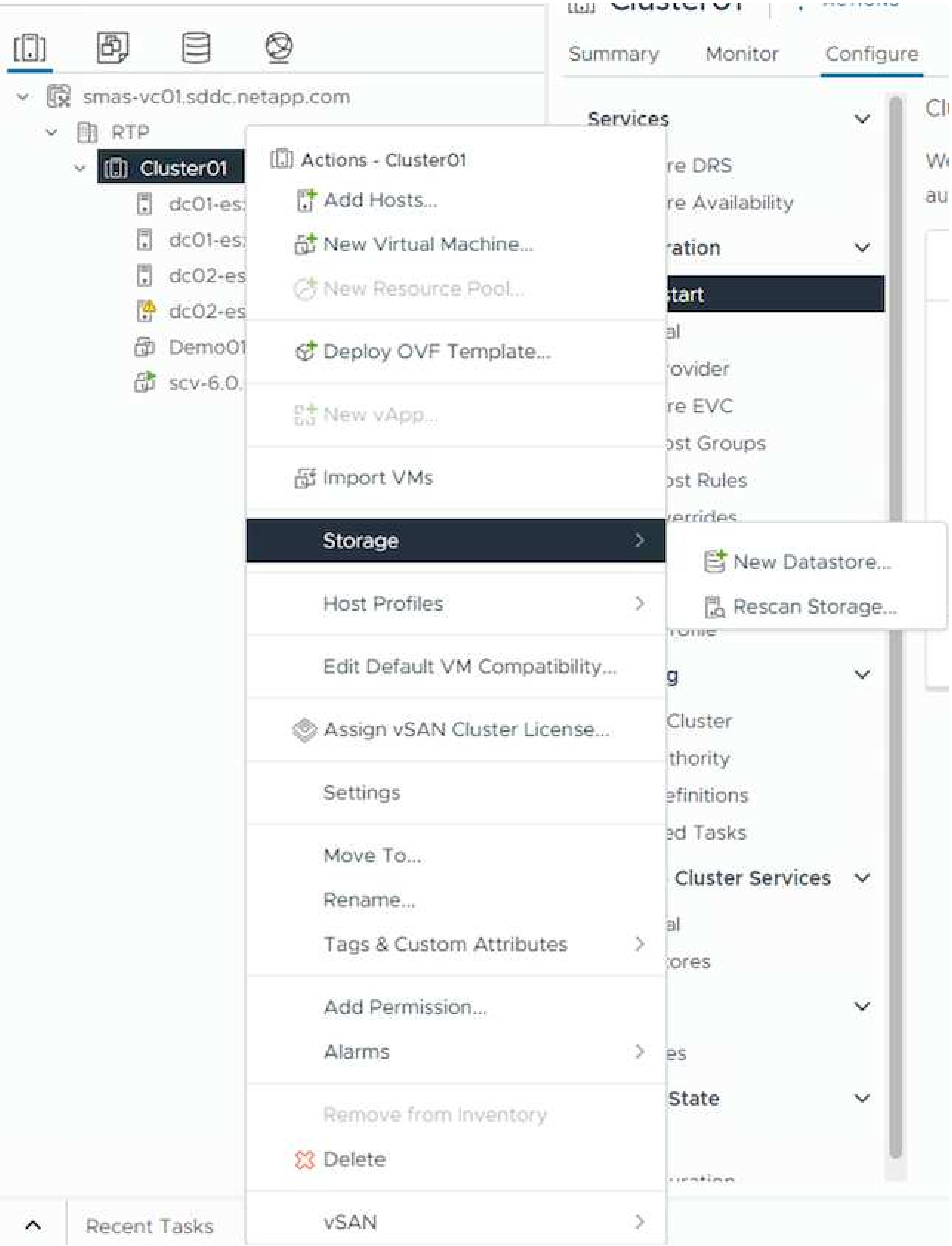
9. On one of the vSphere host in the cluster, check the newly created device shows up with datastore showing Not Consumed.



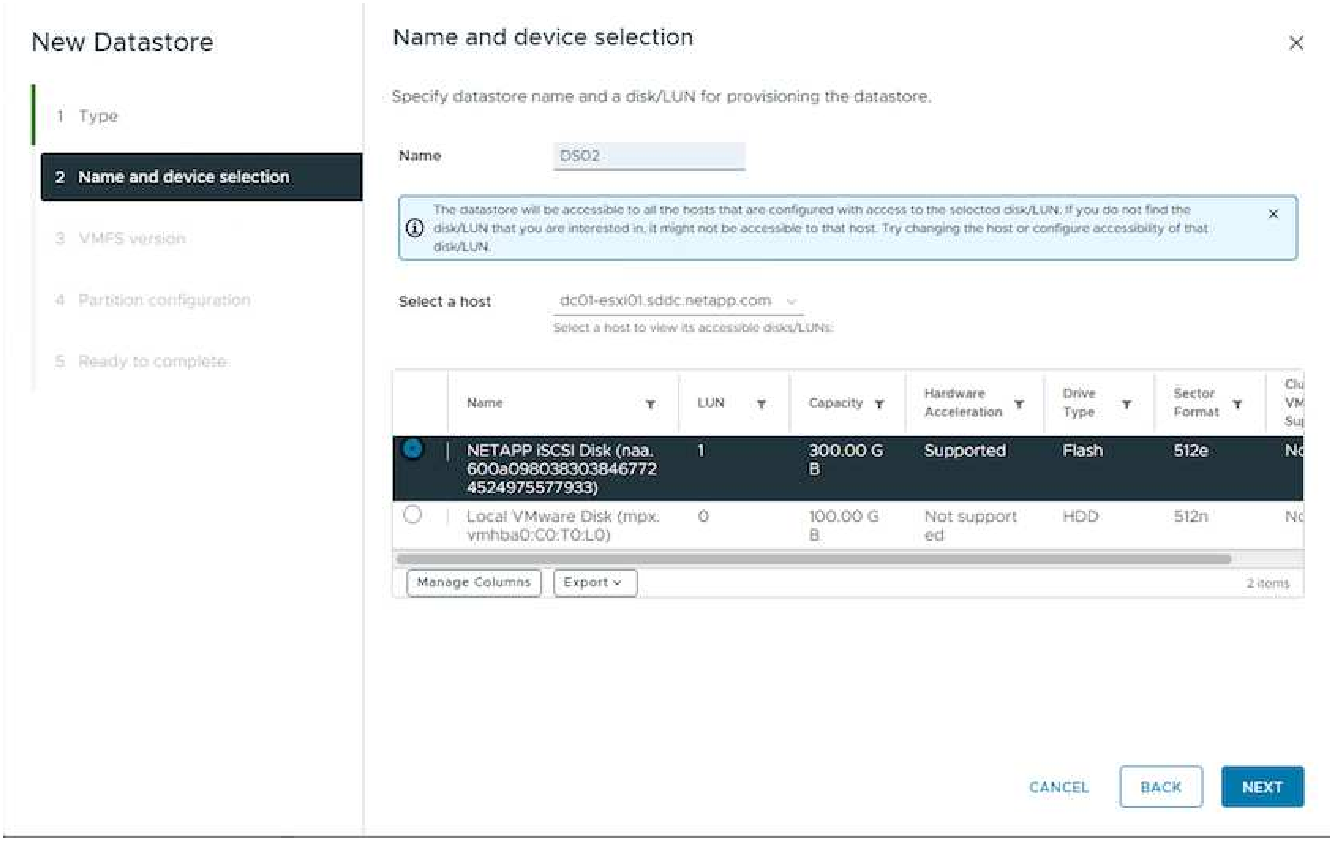
	Adapter	Model	Type	Status	Identifier	Targets	Devices	Paths
●	vmhba65	iSCSI Software Adapter	iSCSI	Online	iscsi_vmk(iqn.1998-01.com.vmware:dc01-esxi01.sddc.netapp.com:473524194:65)	4	2	8
○	vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	1	1	1
○	vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	0	0	0
○	vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	1	1	1

□	Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type	Transport
□	NETAPP iSCSI Disk (naa.600a098038303846772452497557793 1)	0	disk	250.00 GB	DS01	Attached	Supported	Flash	iSCSI
□	NETAPP iSCSI Disk (naa.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.



Name and device selection

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

Name: DS02

The datastore will be accessible to all the hosts that are configured with access to the selected disk/LUN. If you do not find the disk/LUN that you are interested in, it might not be accessible to that host. Try changing the host or configure accessibility of that disk/LUN.

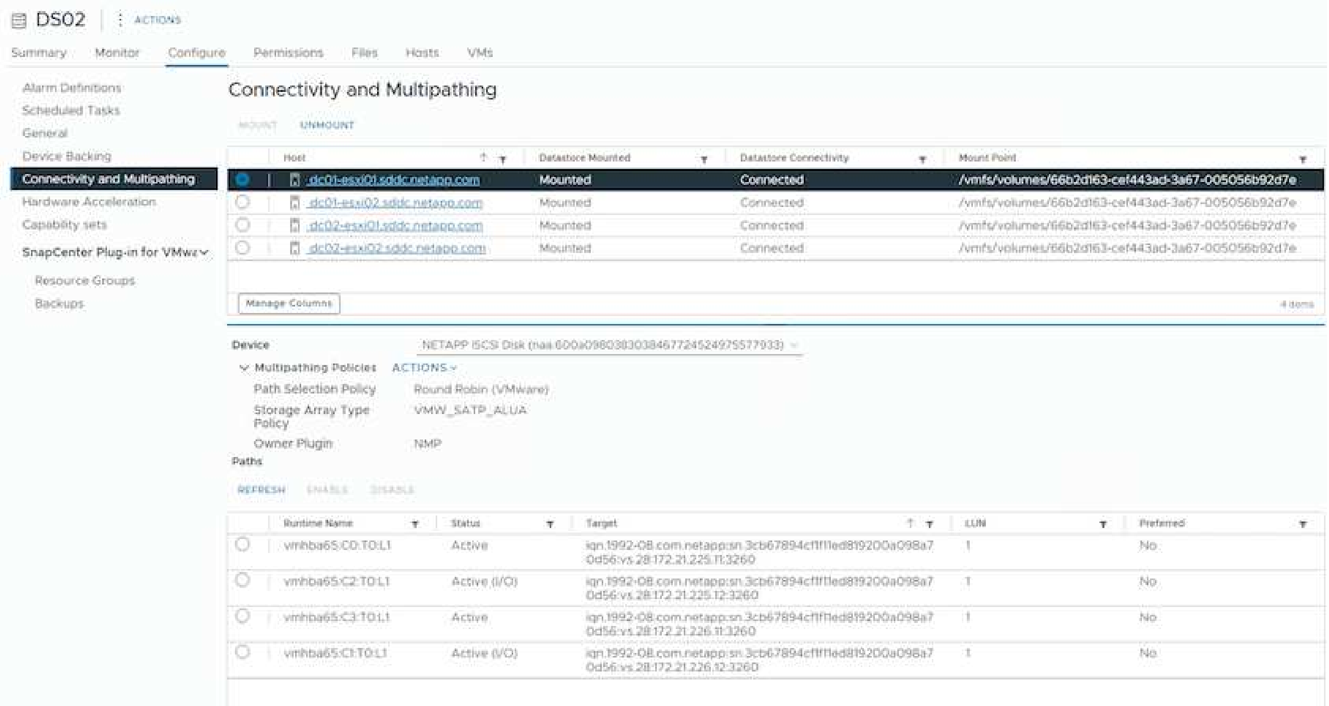
Select a host: dc01-esxi01.sddc.netapp.com

Select a host to view its accessible disks/LUNs:

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format	Clu VM Su
●	NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)	1	300.00 GB	Supported	Flash	512e	No
○	Local VMware Disk (mpx.vmhba0:C0:T0:L0)	0	100.00 GB	Not supported	HDD	512n	No

2 items

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



Connectivity and Multipathing

	Host	Datastore Mounted	Datastore Connectivity	Mount Point
●	dc01-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
○	dc01-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
○	dc02-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
○	dc02-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e

4 items

Device: NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)

Multipathing Policies ACTIONS

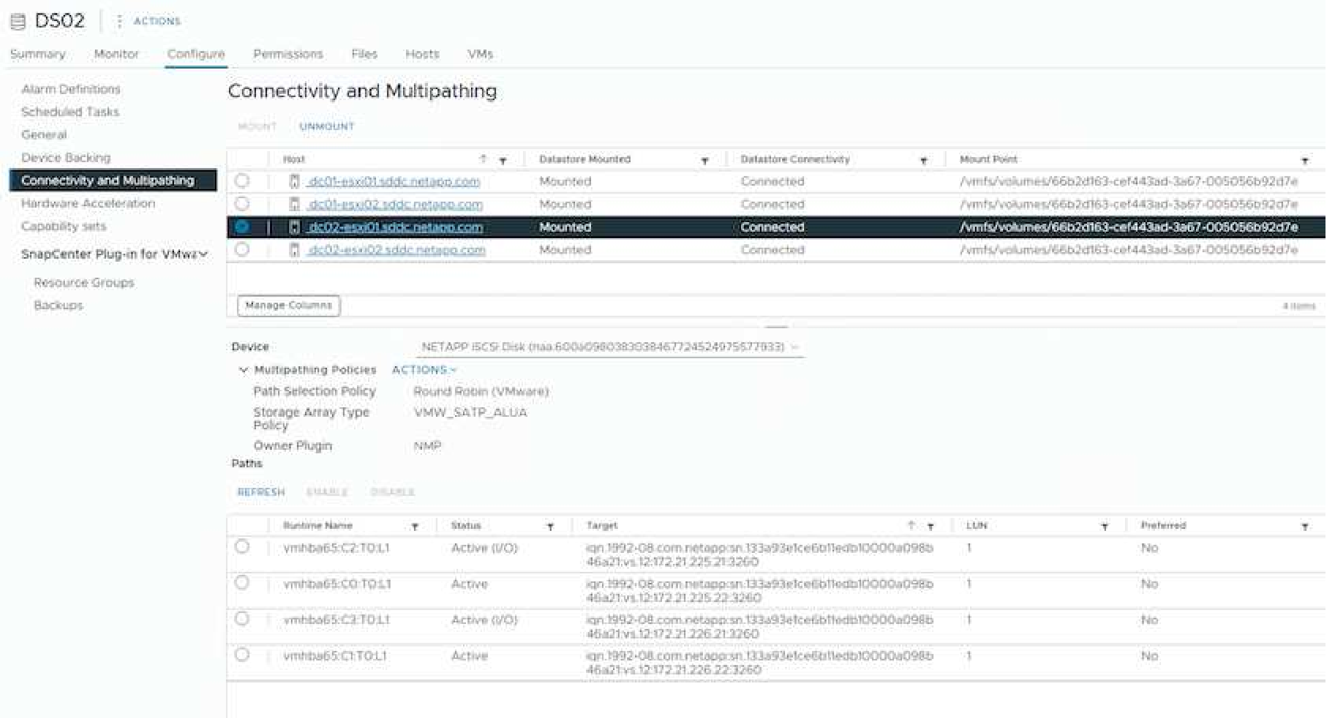
Path Selection Policy: Round Robin (VMware)

Storage Array Type Policy: VMW_SATP_ALUA

Owner Plugin: NMP

Paths

	Runtime Name	Status	Target	LUN	Preferred
○	vmhba65:C0:T0:L1	Active	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.225.11:3260	1	No
○	vmhba65:C2:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.225.12:3260	1	No
○	vmhba65:C3:T0:L1	Active	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.226.11:3260	1	No
○	vmhba65:C1:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.226.12:3260	1	No



DS02 ⋮ ACTIONS

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 VMwa
Resource Groups
Backups

Connectivity and Multipathing

MOUNT UNMOUNT

	Host	Datastore Mounted	Datastore Connectivity	Mount Point
○	dc01-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
○	dc01-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
●	dc02-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
○	dc02-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e

Manage Columns 4 items

Device NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)

Multipathing Policies ACTIONS

Path Selection Policy: Round Robin (VMware)
Storage Array Type Policy: VMW_SATP_ALUA
Owner Plugin: NMP

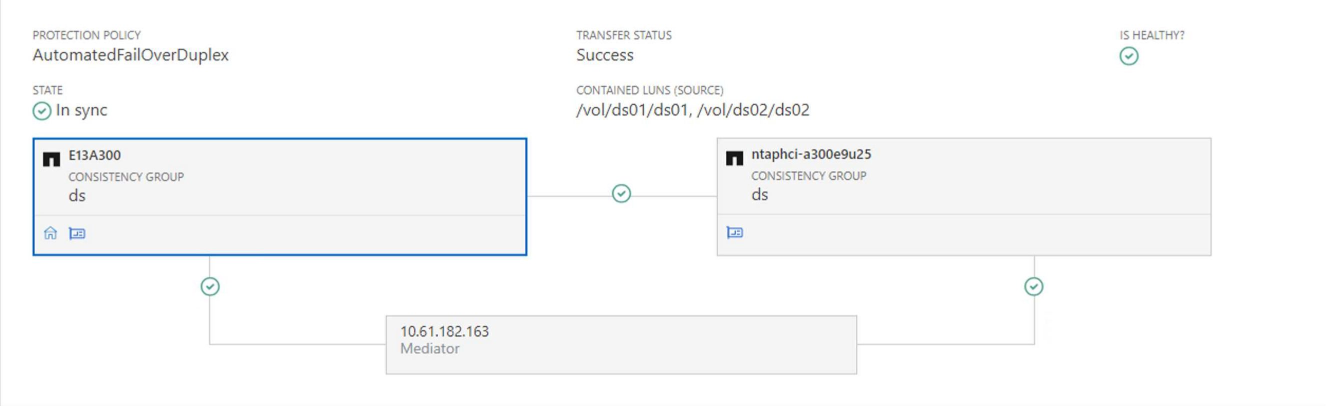
Paths

REFRESH ENABLE DISABLE

	Runtime Name	Status	Target	LUN	Preferred
○	vmhba65:C2:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.225.21:3260	1	No
○	vmhba65:C0:T0:L1	Active	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.225.22:3260	1	No
○	vmhba65:C3:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.226.21:3260	1	No
○	vmhba65:C1:T0:L1	Active	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.226.22:3260	1	No

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

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



PROTECTION POLICY: AutomatedFailOverDuplex

TRANSFER STATUS: Success

IS HEALTHY? ✓

STATE: ✓ In sync

CONTAINED LUNS (SOURCE): /vol/ds01/ds01, /vol/ds02/ds02

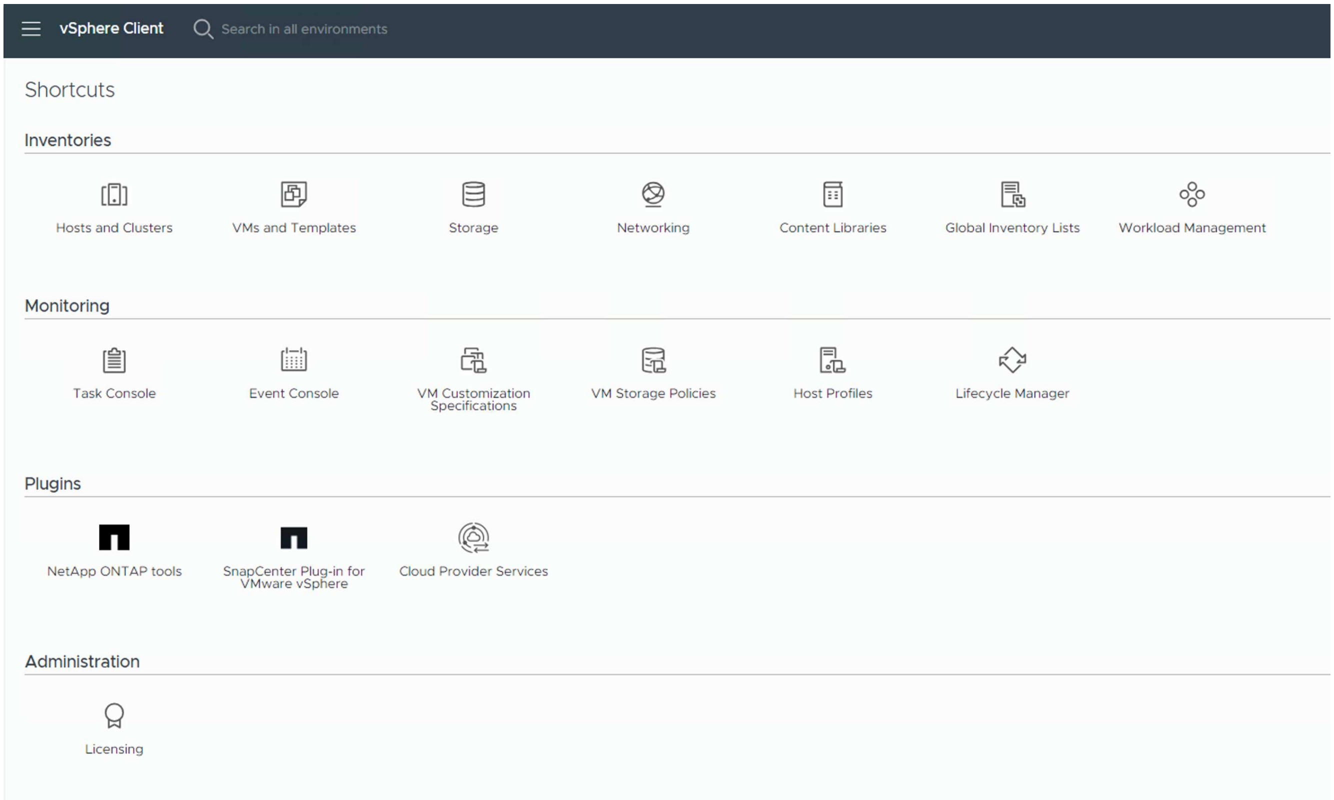
E13A300
CONSISTENCY GROUP
ds

ntaphci-a300e9u25
CONSISTENCY GROUP
ds

10.61.182.163
Mediator

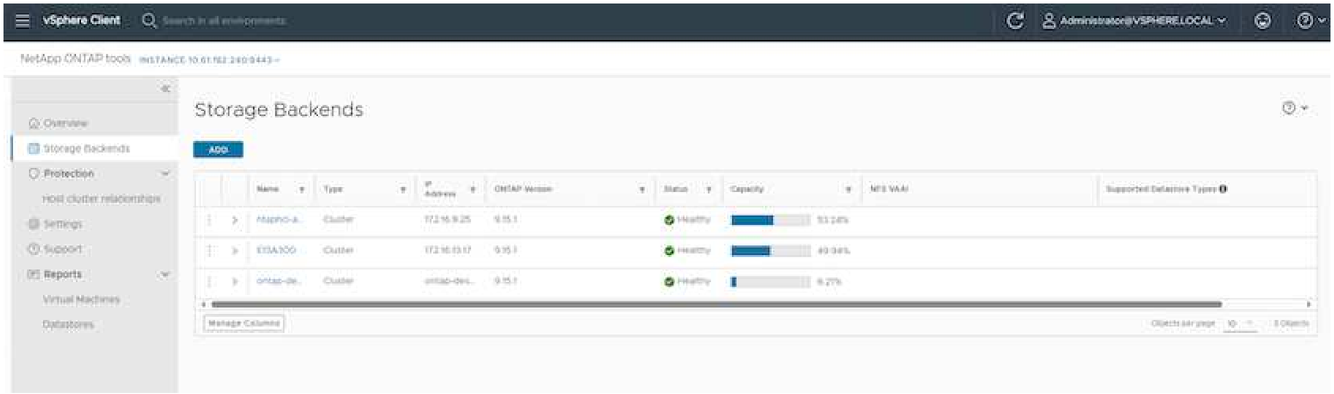
vMSC uniform host access mode with ONTAP Tools.

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



If not, follow ONTAP Tools deployment and Add a vCenter server instance

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

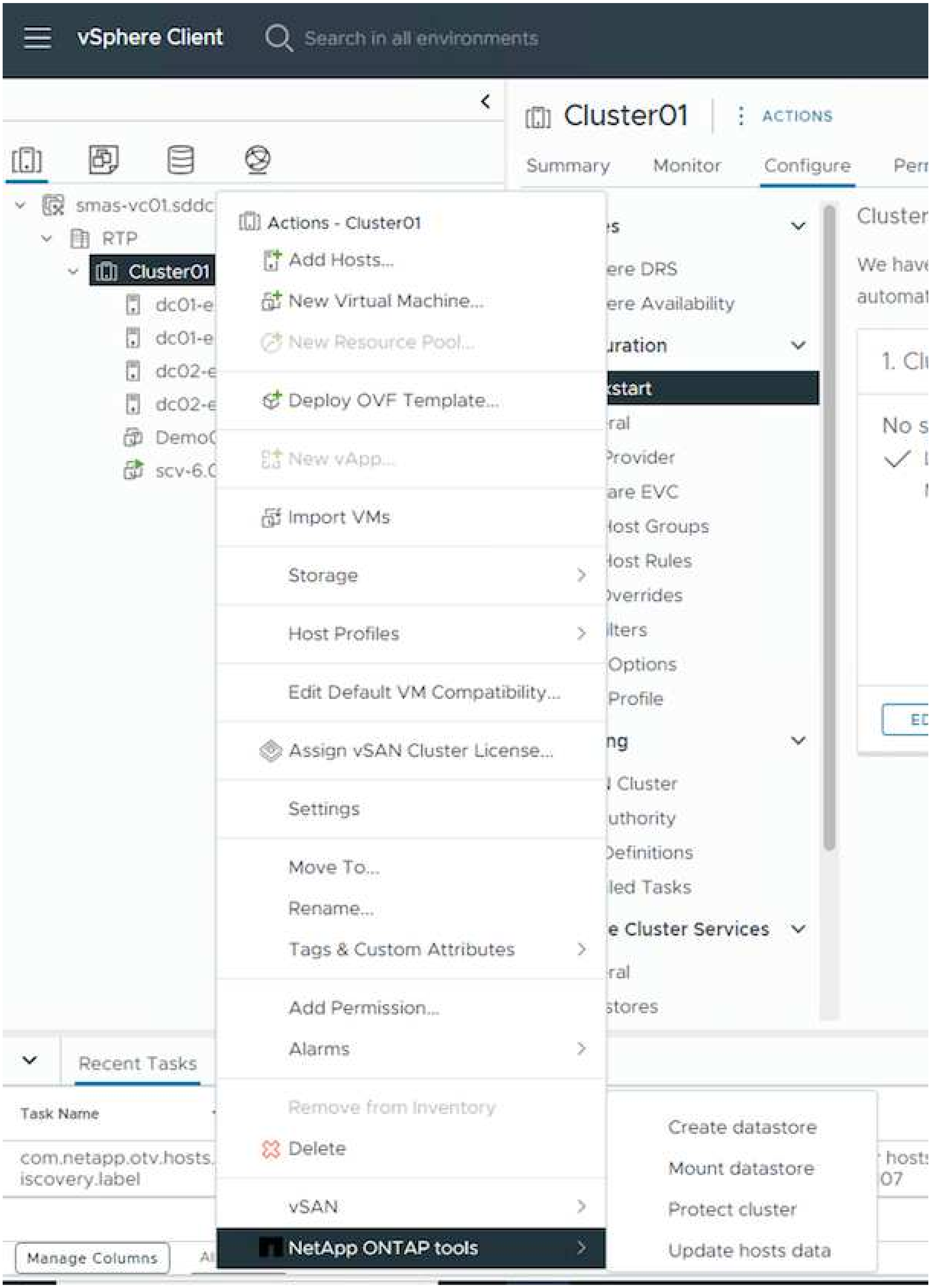


Storage Backends

Name	Type	IP Address	ONTAP Version	Status	Capacity	NFS VAAI	Supported Datastore Types
Hbapho-a...	Cluster	172.16.9.25	9.15.1	Healthy	53.24%		
E13A300	Cluster	172.16.13.17	9.15.1	Healthy	49.94%		
ontap-de...	Cluster	ontap-des...	9.15.1	Healthy	6.27%		

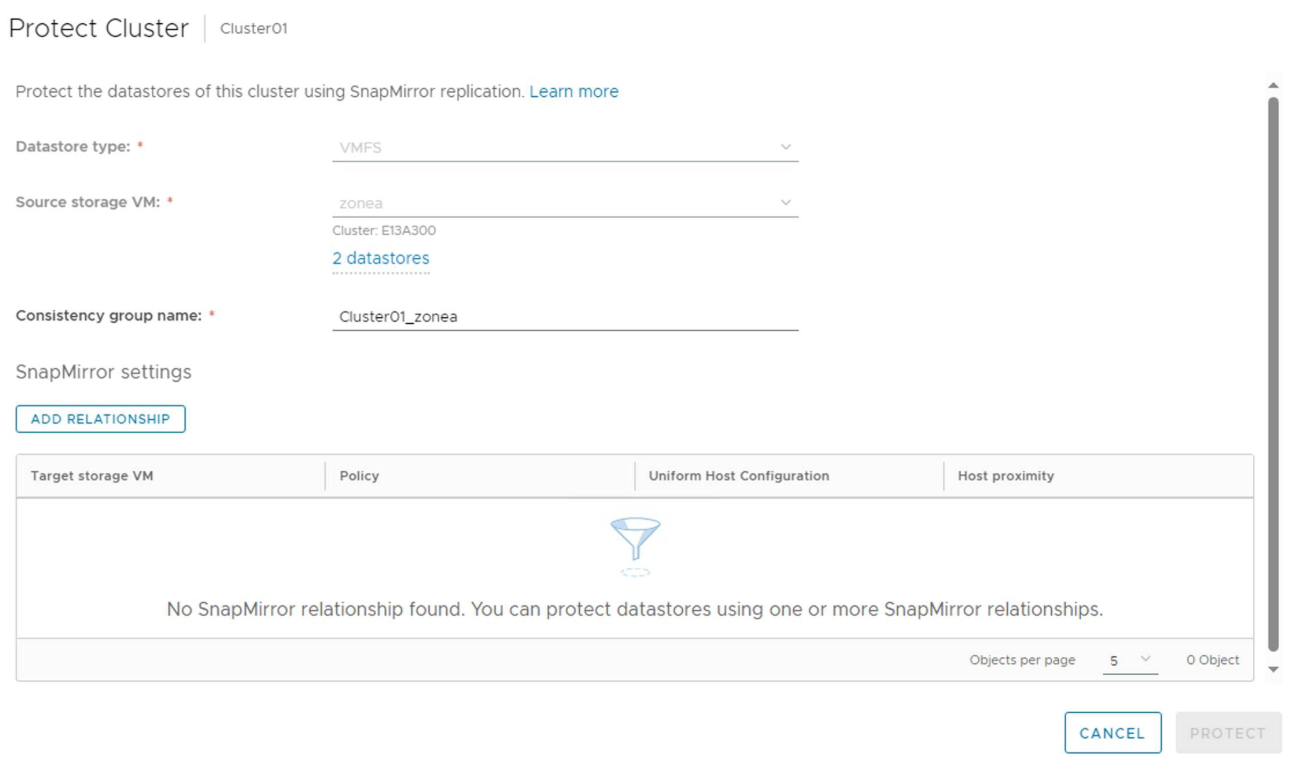
If not, follow Add storage backend using vSphere client UI

3. Update hosts data to sync with ONTAP Tools and then, create a datastore.



4. To enable SM-as, right click on vSphere cluster and pick Protect cluster on NetApp ONTAP Tools (refer above screenshot)

5. It will show existing datastores for that cluster along with SVM details. The default CG name is <vSphere Cluster name>_<SVM name>. Click on Add Relationship button.



Protect Cluster | Cluster01

Protect the datastores of this cluster using SnapMirror replication. Learn more

Datastore type: * VMFS

Source storage VM: * zonea

Cluster: E13A300

2 datastores

Consistency group name: * Cluster01_zonea

SnapMirror settings

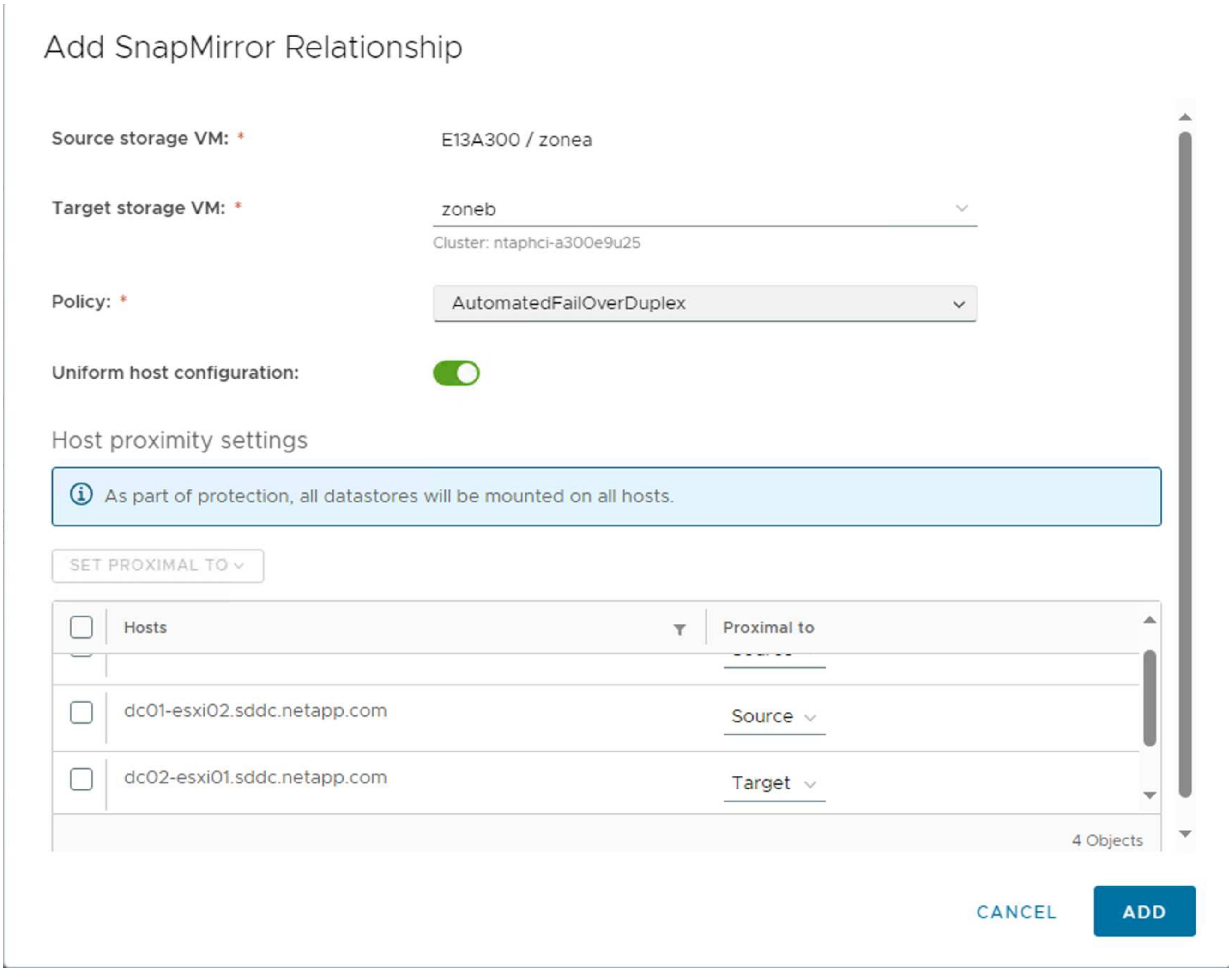
ADD RELATIONSHIP

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 5 0 Object

6. Pick the target SVM and set the policy to AutomatedFailOverDuplex for SM-as. There is a toggle switch for Uniform host configuration. Set the proximity for each host.



Add SnapMirror Relationship

Source storage VM: * E13A300 / zonea

Target storage VM: * zoneb

Cluster: ntaphci-a300e9u25

Policy: * AutomatedFailOverDuplex

Uniform host configuration: ●

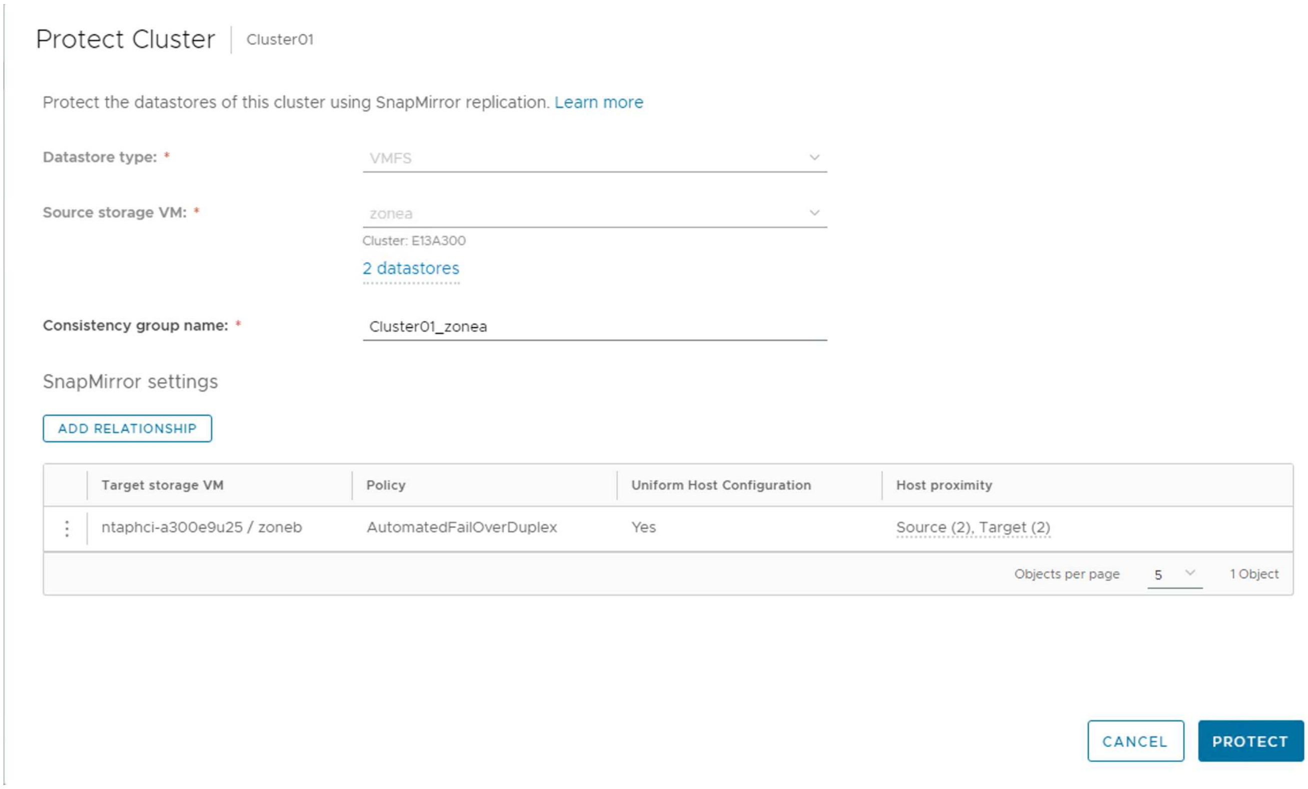
Host proximity settings

As part of protection, all datastores will be mounted on all hosts.

□	Hosts	Proximal to
□	dc01-esxi02.sddc.netapp.com	Source
□	dc02-esxi01.sddc.netapp.com	Target

4 Objects

7. Verify the host promity info and other details. Add another relationship to third site with replication policy of Asynchronous if required. Then, click on Protect.



Protect Cluster | Cluster01

Protect the datastores of this cluster using SnapMirror replication. Learn more

Datastore type: * VMFS

Source storage VM: * zonea
Cluster: E13A300
2 datastores

Consistency group name: * Cluster01_zonea

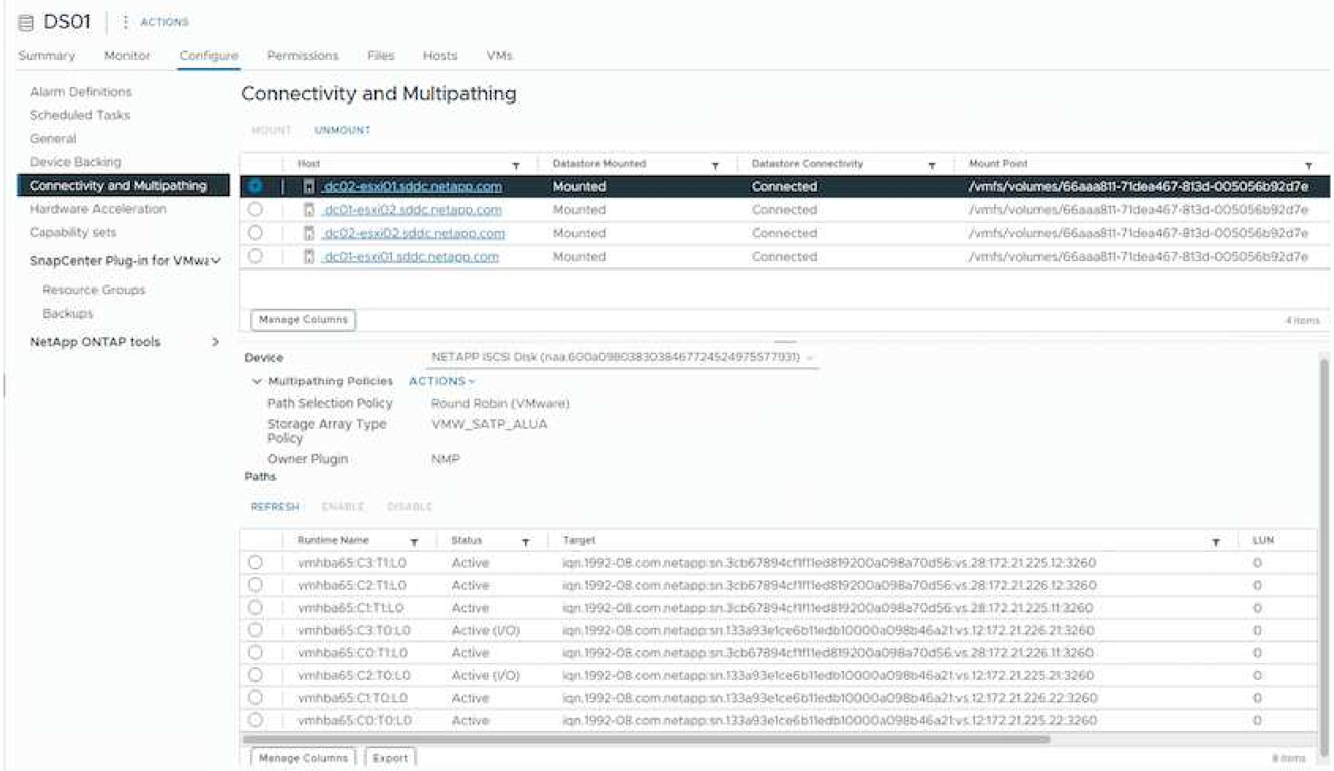
SnapMirror settings

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

Objects per page 5 1 Object

NOTE: If plan to use SnapCenter Plug-in for VMware vSphere 6.0, the replication needs to be setup at volume level rather than at Consistency Group level.

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



Connectivity and Multipathing

Host	Datastore Mounted	Datastore Connectivity	Mount Point
dc02-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e
dc01-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e
dc02-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e
dc01-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e

4 items

Device NETAPP iSCSI Disk (naa.600a098038303846772452497557793l)

Multipathing Policies ACTIONS
Path Selection Policy Round Robin (VMware)
Storage Array Type Policy VMW_SATP_ALUA
Owner Plugin NMP

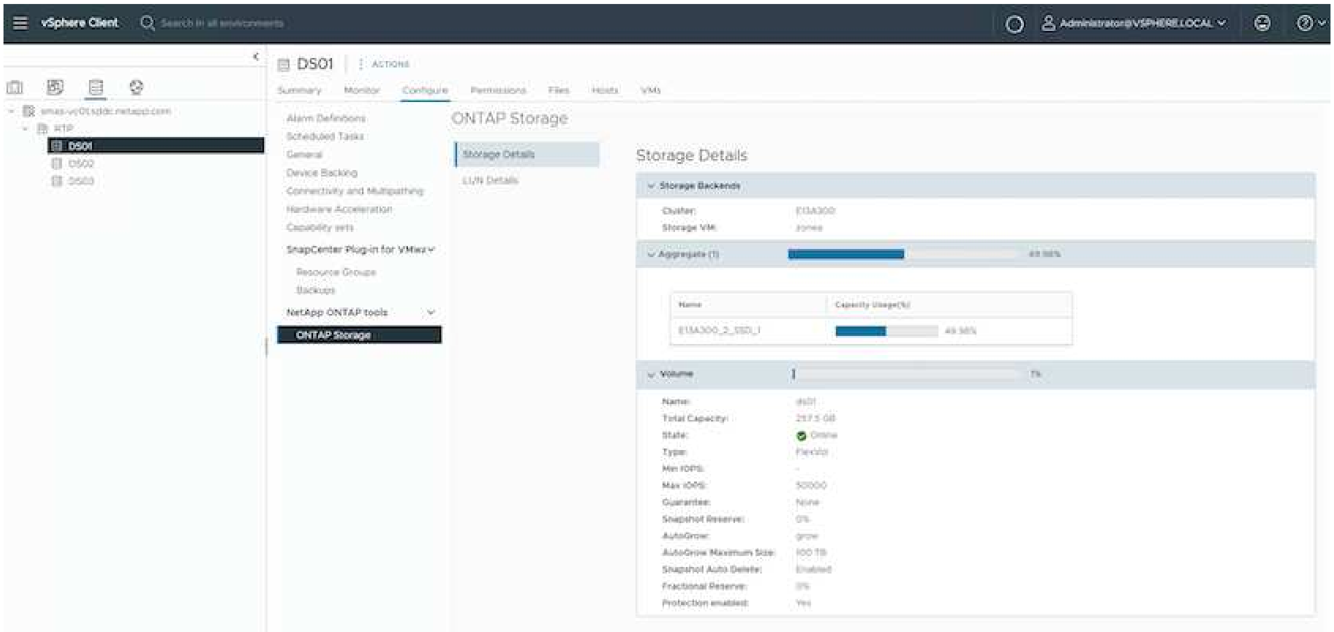
Paths

Runtime Name	Status	Target	LUN
vmhba65:C3:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.225.12:3260	0
vmhba65:C2:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.226.12:3260	0
vmhba65:C1:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.225.11:3260	0
vmhba65:C3:T0:L0	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.226.21:3260	0
vmhba65:C0:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894cf1f11ed819200a098a70d56:vs.28:172.21.226.11:3260	0
vmhba65:C2:T0:L0	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.225.21:3260	0
vmhba65:C1:T0:L0	Active	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.226.22:3260	0
vmhba65:C0:T0:L0	Active	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12:172.21.225.22:3260	0

8 items

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

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



Storage Details

Storage Backends

Cluster: E13A300
Storage VM: zonea

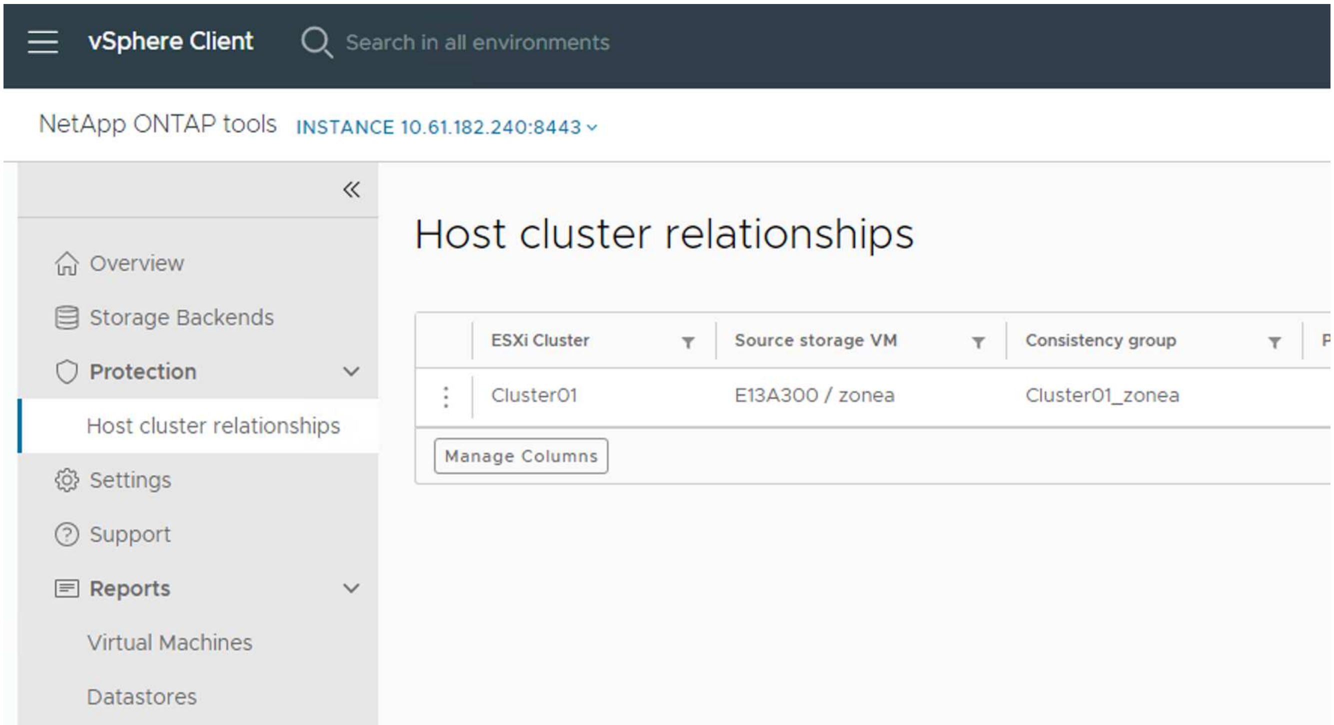
Aggregate (1) 49.98%

Name	Capacity Usage(%)
E13A300_2_SSD_1	49.98%

Volume 1%

Name: ds01
Total Capacity: 257.5 GB
State: ✓ Online
Type: FlexVol
Min IOPS: -
Max IOPS: 50000
Guarantee: None
Snapshot Reserve: 0%
AutoGrow: grow
AutoGrow Maximum Size: 100 TB
Snapshot Auto Delete: Enabled
Fractional Reserve: 0%
Protection enabled: Yes

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

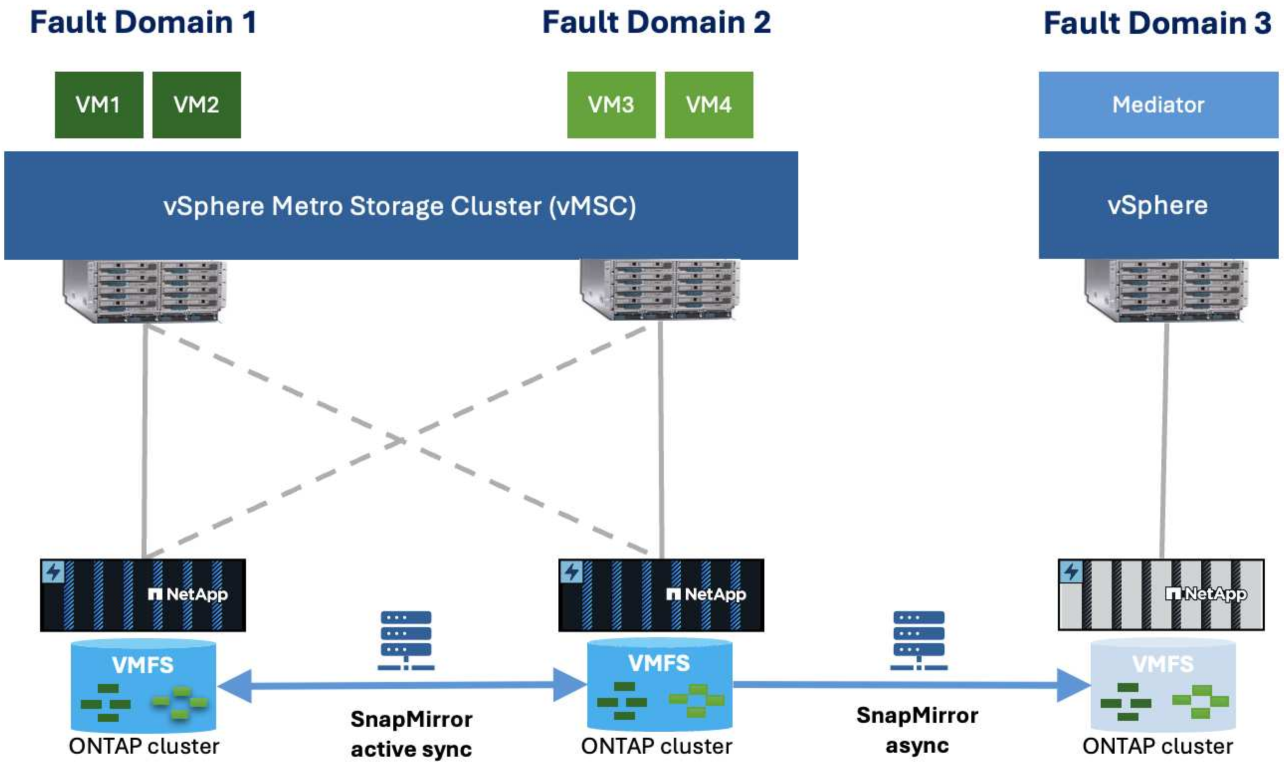


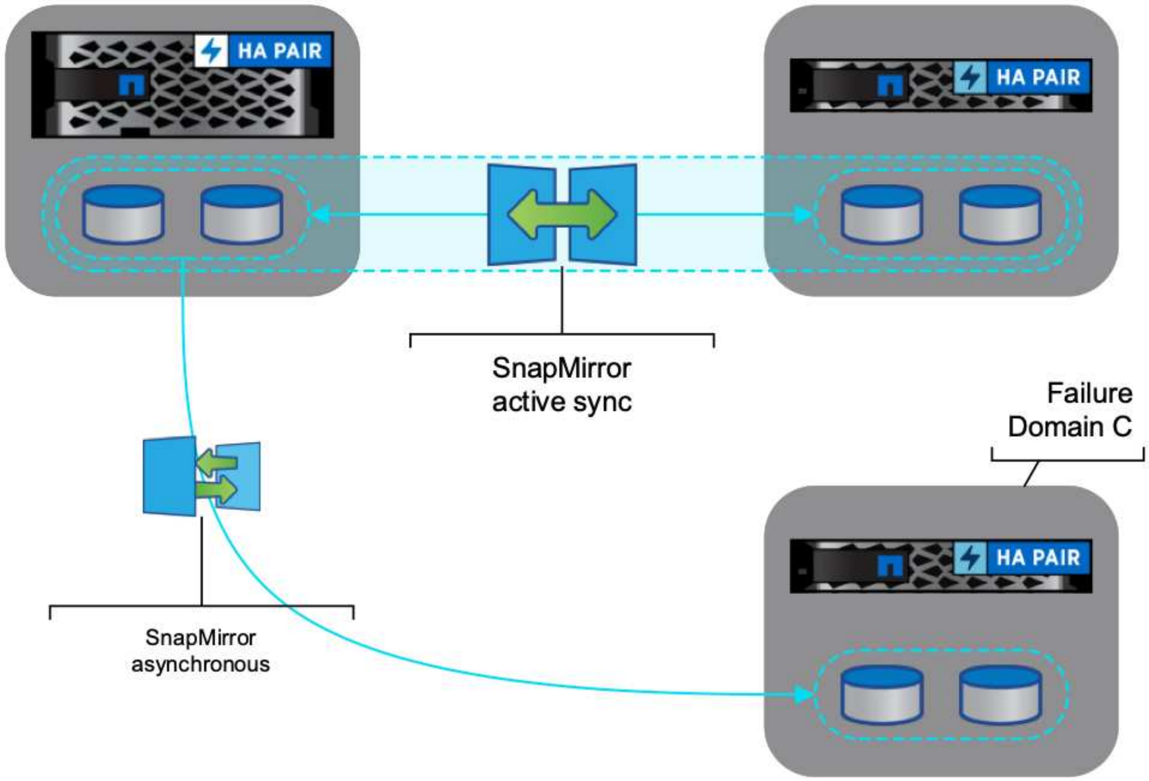
Host cluster relationships

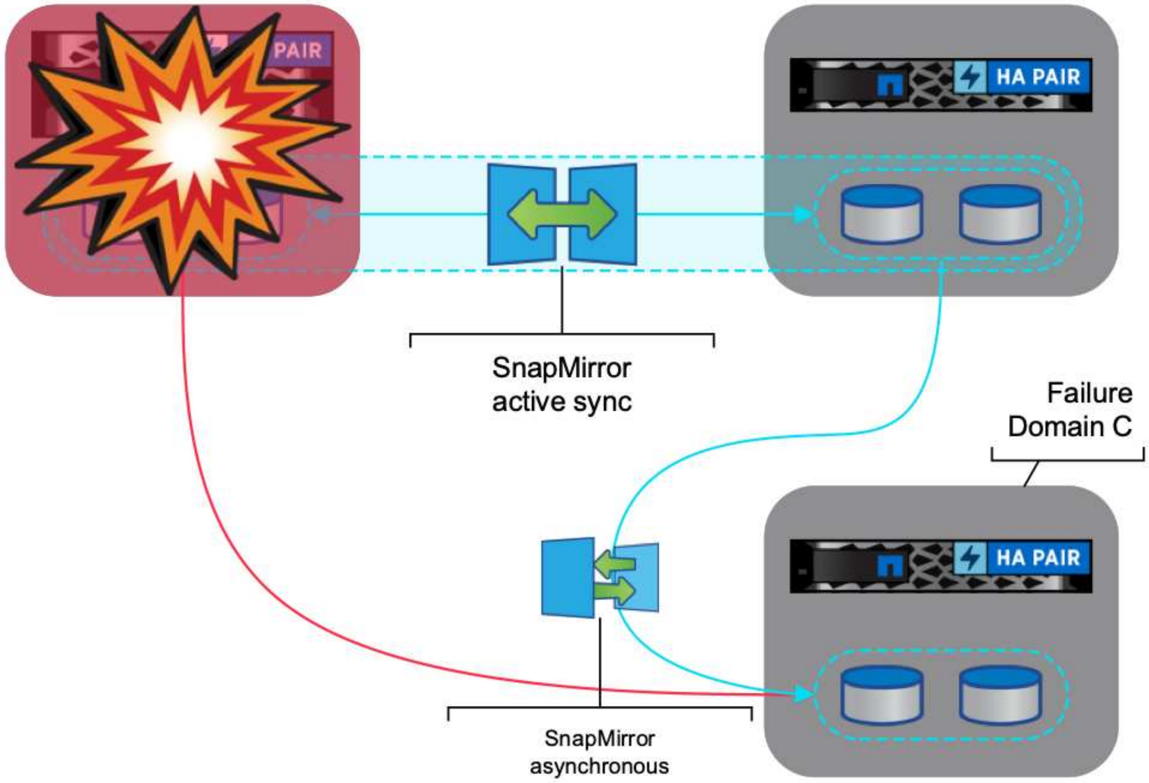
ESXi Cluster	Source storage VM	Consistency group	P
Cluster01	E13A300 / zonea	Cluster01_zonea	

VM protection with SnapCenter plug-in for VMware vSphere.

SnapCenter Plug-in for VMware vSphere (SCV) 6.0 or above supports SnapMirror active sync and also in combination with SnapMirror Async to replicate to third fault domain.

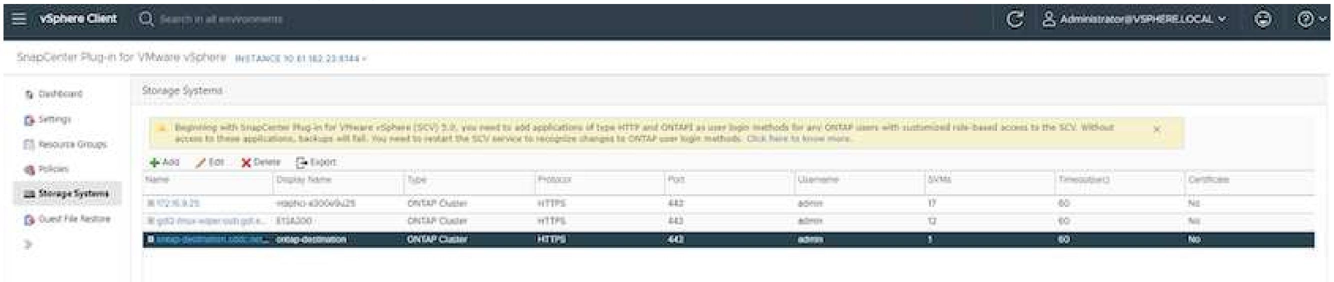

Fault Domain 1
Fault Domain 2
Fault Domain 3
VM1
VM2
VM3
VM4
Mediator
vSphere Metro Storage Cluster (vMSC)
vSphere
NetApp
NetApp
NetApp
VMFS
VMFS
VMFS
ONTAP cluster
SnapMirror
active sync
ONTAP cluster
SnapMirror
async
ONTAP cluster


HA PAIR
HA PAIR
SnapMirror
active sync
Failure
Domain C
HA PAIR
SnapMirror
asynchronous


PAIR
HA PAIR
SnapMirror
active sync
Failure
Domain C
HA PAIR
SnapMirror
asynchronous

Supported use-cases include:
* Backup and Restore the VM or Datastore from either of fault domains with SnapMirror active sync.
* Restore resources from third fault domain.

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



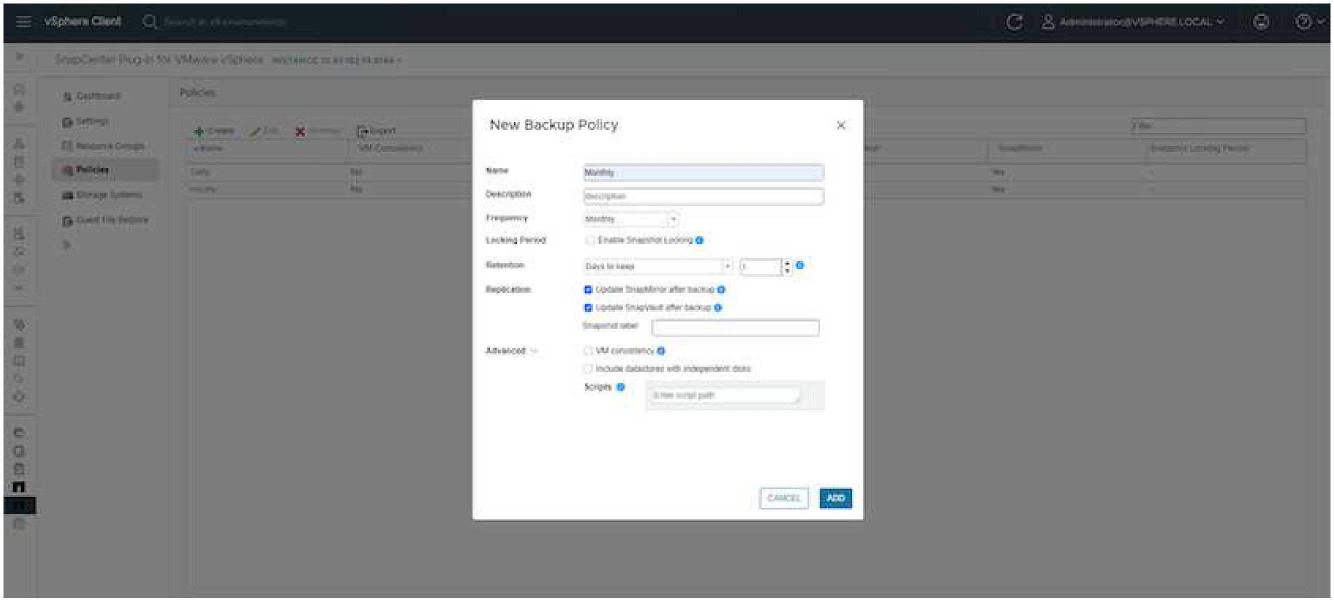
SnapCenter Plug-in for VMware vSphere INSTANCE 10.61.182.23:8144

Storage Systems

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

Name	Display Name	Type	Protocol	Port	Username	SVMs	Timeout(sec)	Certificate
172.16.9.25	[illegible]	ONTAP Cluster	HTTPS	443	admin	17	60	No
[illegible]	E13A300	ONTAP Cluster	HTTPS	443	admin	12	60	No
[illegible]	ontap-destination	ONTAP Cluster	HTTPS	443	admin	1	60	No

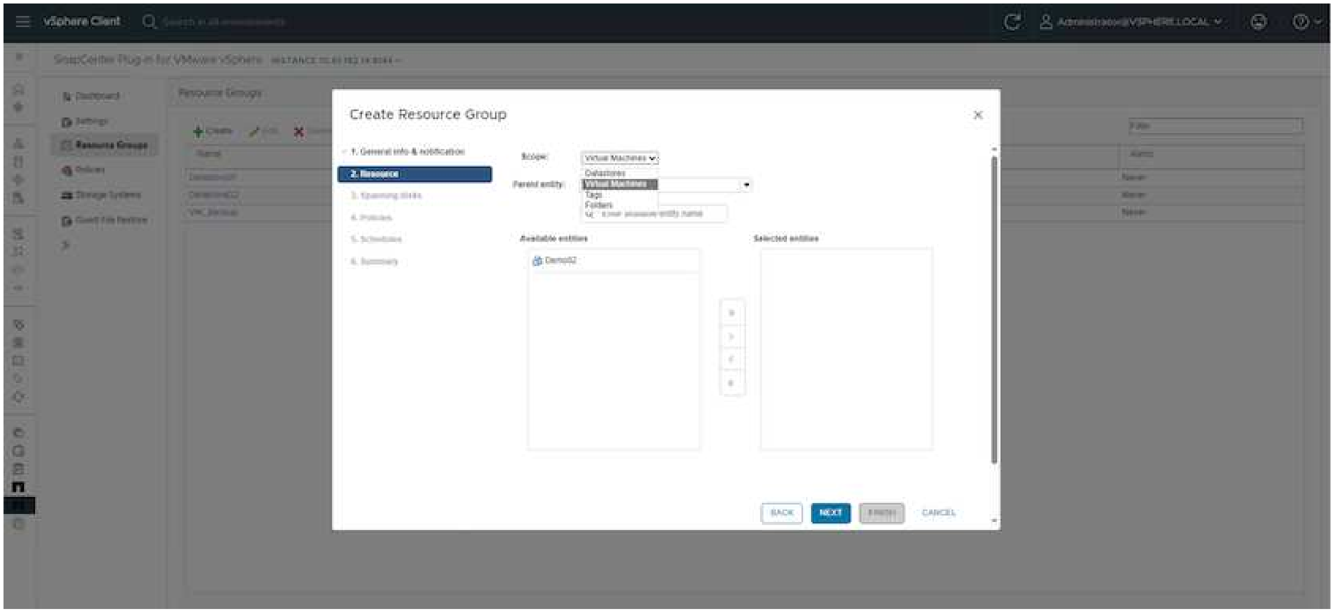
2. Create Policy. Ensure Update SnapMirror after backup is checked for SM-as and also Update SnapVault after backup for Async replication to third fault domain.



New Backup Policy

Name: Monthly
Description: Description
Frequency: Monthly
Locking Period: ☐ Enable Snapshot Locking
Retention: Days to keep 1
Replication: ☑ Update SnapMirror after backup
☑ Update SnapVault after backup
Snapshot label:
Advanced: ☐ VM consistency
☐ Include datastores with independent disks
Scripts: Enter script path

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



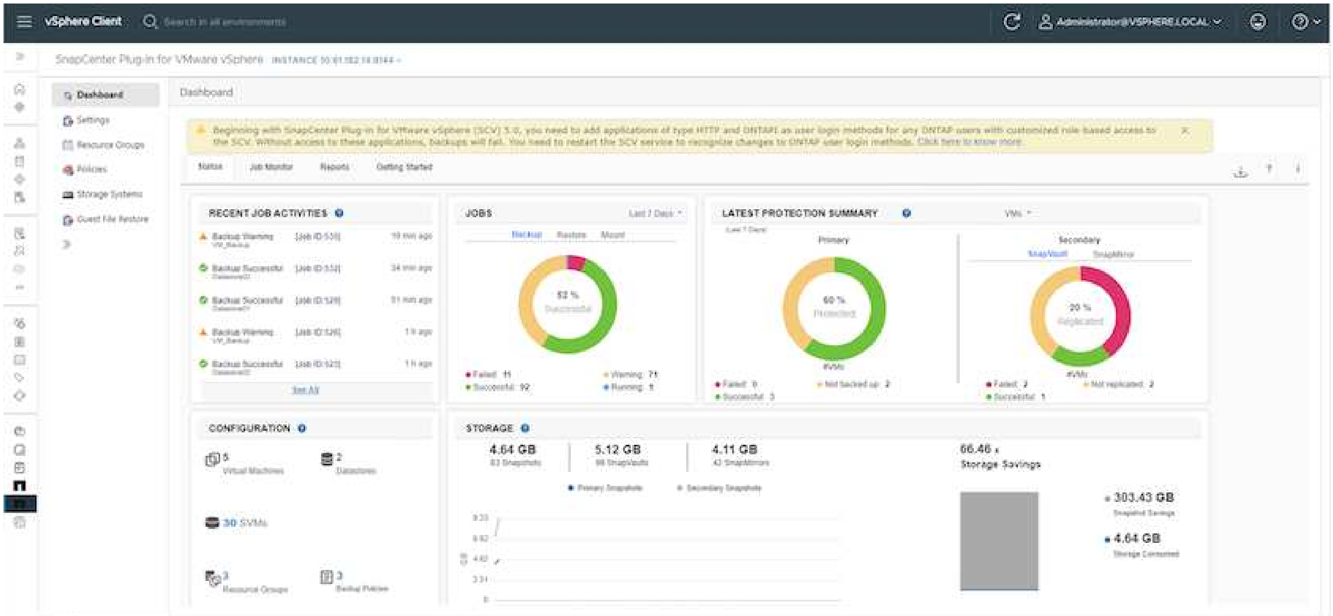
Create Resource Group

1. General info & notification
2. Resource
3. Spanning disks
4. Policies
5. Schedules
6. Summary

Scope: Virtual Machines
Parent entity: Virtual Machines
Available entities: Demo02
Selected entities:

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

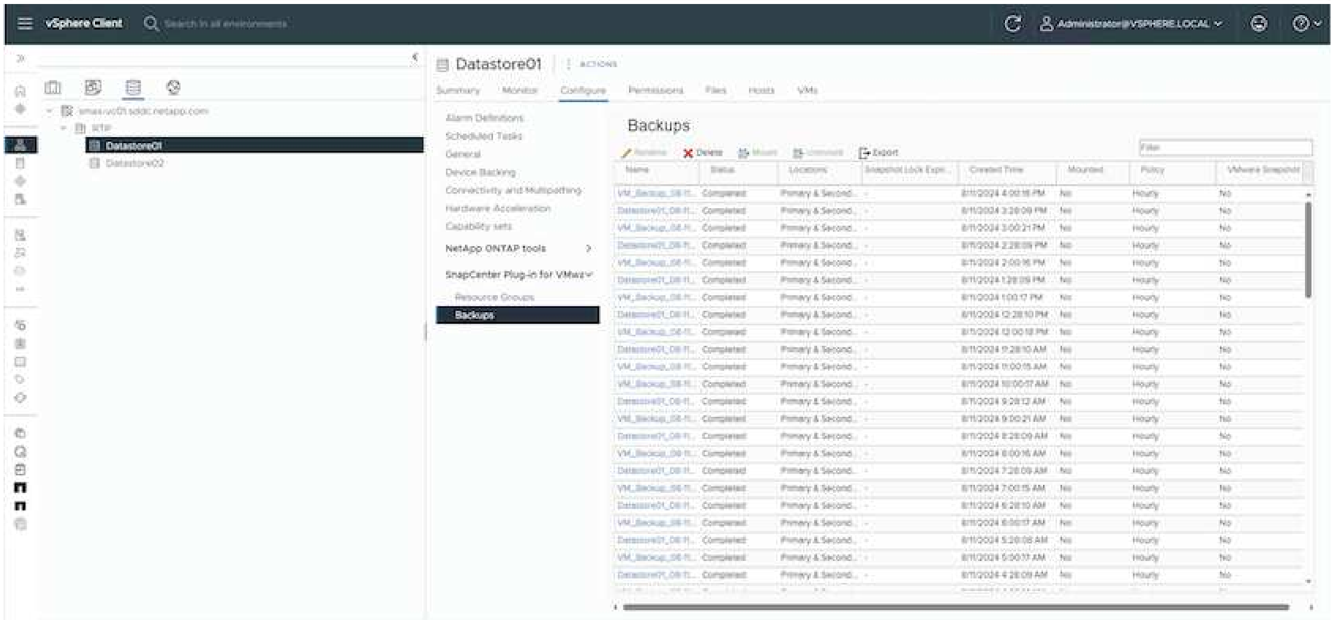
4. Backups occur at scheduled time based on Policy associated to Resource Group. Jobs can be monitored from the Dashboard job monitor or from the backup info on those resources.



SnapCenter Plug-in for VMware vSphere

Dashboard

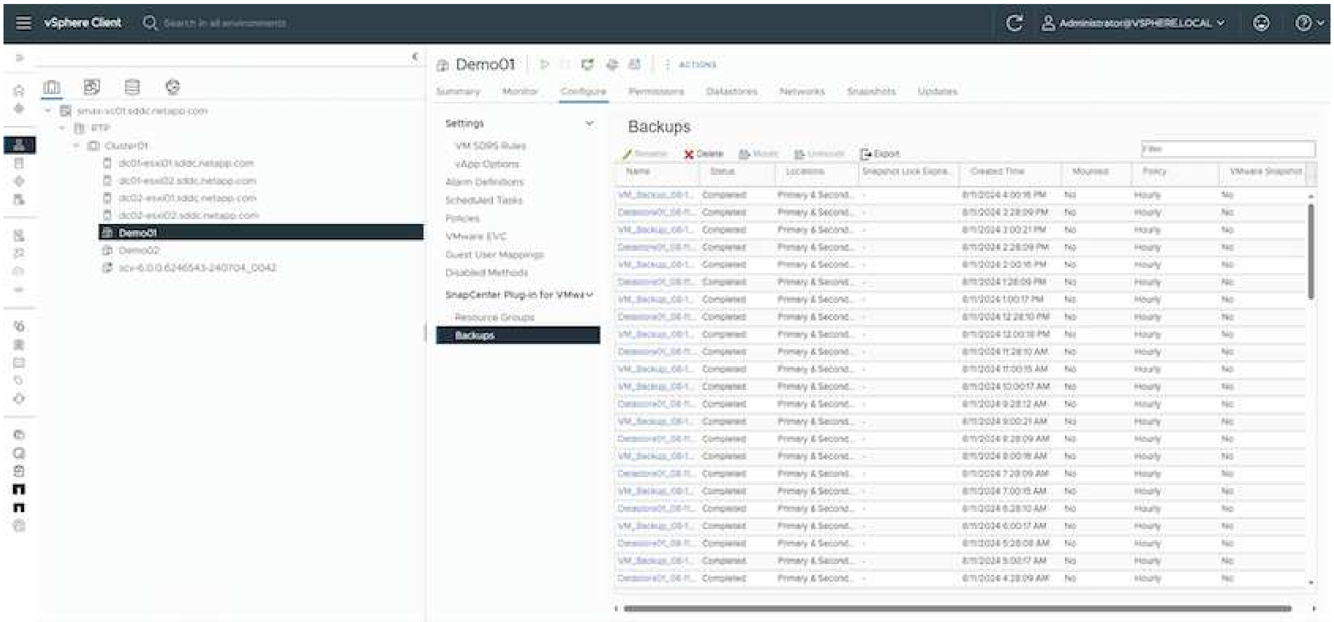
Beginning with SnapCenter Plug-in for VMware vSphere (SCV) 5.0, you need to add applications of type HTTP and ONTAPI as user login methods for any ONTAP users with customized role-based access to the SCV. Without access to these applications, backups will fail. You need to restart the SCV service to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



Datastore01

Backups

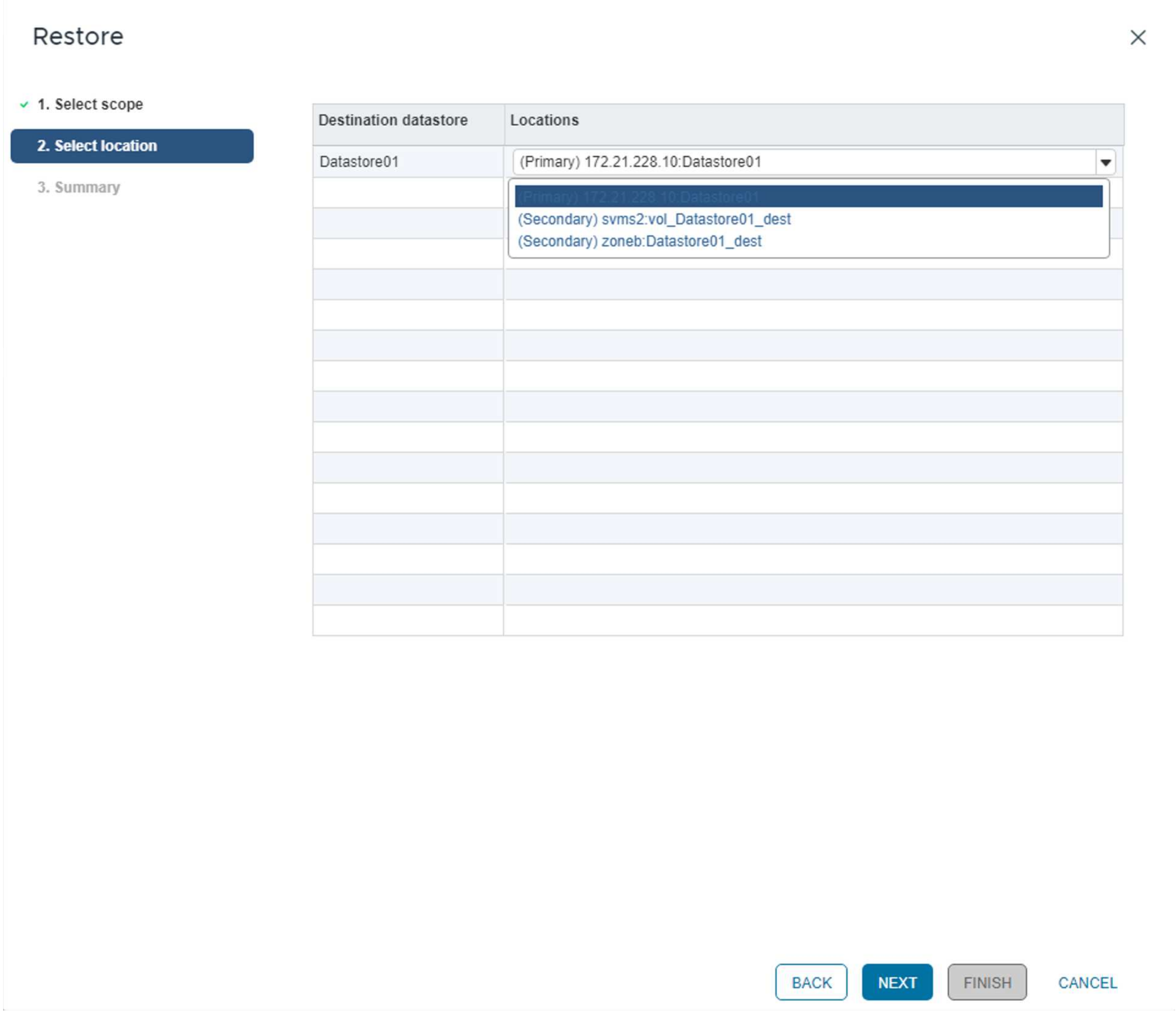
Name	Status	Locations	Snapshot Lock Expi...	Created Time	Mounted	Policy	VMware Snapshot
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 4:00:16 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 3:28:09 PM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 3:00:21 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 2:28:09 PM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 2:00:16 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 1:28:09 PM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 1:00:17 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 12:28:10 PM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 12:00:18 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 11:28:10 AM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 11:00:15 AM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 10:00:17 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 9:28:12 AM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 9:00:21 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 8:28:09 AM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 8:00:16 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 7:28:09 AM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 7:00:15 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 6:28:10 AM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 6:00:17 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 5:28:08 AM	No	Hourly	No
VM_Backup_08-11...	Completed	Primary & Second...	-	8/11/2024 5:00:17 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 4:28:09 AM	No	Hourly	No



Backups

Name	Status	Locations	Snapshot Lock Expira...	Created Time	Mounted	Policy	VMware Snapshot
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 4:00:16 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 2:28:09 PM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 3:00:21 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 2:28:09 PM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 2:00:16 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 1:28:09 PM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 1:00:17 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 12:28:10 PM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 12:00:18 PM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 11:28:10 AM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 11:00:15 AM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 10:00:17 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 9:28:12 AM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 9:00:21 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 8:28:09 AM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 8:00:18 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 7:28:09 AM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 7:00:15 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 6:28:10 AM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 6:00:17 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 5:28:08 AM	No	Hourly	No
VM_Backup_08-1...	Completed	Primary & Second...	-	8/11/2024 5:00:17 AM	No	Hourly	No
Datastore01_08-11...	Completed	Primary & Second...	-	8/11/2024 4:28:09 AM	No	Hourly	No

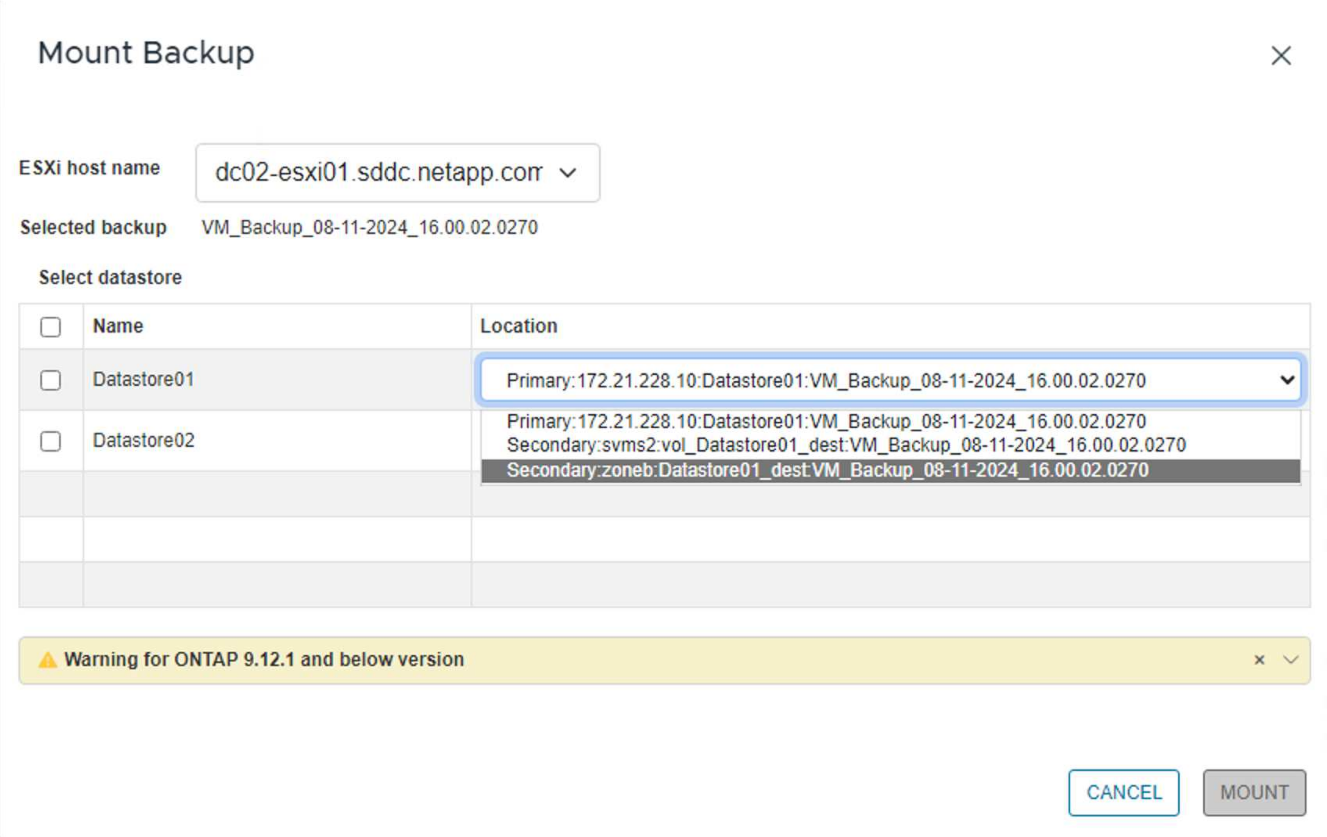
5. VMs can be restored to same or alternate vCenter from the SVM on Primary fault domain or from one of the secondary locations.



Destination datastore	Locations
Datastore01	(Primary) 172.21.228.10:Datastore01

(Primary) 172.21.228.10:Datastore01
(Secondary) svms2:vol_Datastore01_dest
(Secondary) zoneb:Datastore01_dest

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



Mount Backup

ESXi host name: dc02-esxi01.sddc.netapp.com

Selected backup: VM_Backup_08-11-2024_16.00.02.0270

Select datastore

□	Name	Location
□	Datastore01	Primary:172.21.228.10:Datastore01:VM_Backup_08-11-2024_16.00.02.0270
□	Datastore02	

Primary:172.21.228.10:Datastore01:VM_Backup_08-11-2024_16.00.02.0270
Secondary:svms2:vol_Datastore01_dest:VM_Backup_08-11-2024_16.00.02.0270
Secondary:zoneb:Datastore01_dest:VM_Backup_08-11-2024_16.00.02.0270

⚠ Warning for ONTAP 9.12.1 and below version

For assistance with additional operations with SCV, refer SnapCenter Plug-in for VMware vSphere documentation

Convert SM active sync from asymmetric to symmetric active/active with VMware vSphere Metro Storage Cluster

This article details how to convert SnapMirror active sync from asymmetric to symmetric active/active with VMware vSphere Metro Storage Cluster (VMSC).

Overview

NetApp Snapmirror active sync (SM active sync) is a robust solution for achieving zero Recovery Time Objective (RTO) and zero Recovery Point Objective (RPO) in a virtualized environment.

VMware vSphere Metro Storage Cluster (vMSC) is a stretched cluster solution across different fault domains and allows virtual machines (VMs) to be distributed across two geographically separated sites, providing continuous availability even if one site fails.

Combining vMSC with SM active sync ensures data consistency and immediate failover capabilities between two sites. This setup is particularly crucial for mission-critical applications where any data loss or downtime is unacceptable.

SM active sync, previously known as SnapMirror Business Continuity (SMBC), enables business services to continue operating even through a complete site failure, supporting applications to fail over transparently using a secondary copy. Beginning with ONTAP 9.15.1, SM active sync supports a symmetric active/active capability. Symmetric active/active enables read and write I/O operations from both copies of a protected LUN with bidirectional synchronous replication so that both LUN copies can serve I/O operations locally.

This document shows you the steps of how to convert SM active sync asymmetric active/active to SM active sync symmetric active/active in a VMware stretch cluster environment, in other words converts a SM active sync from an automated failover policy to automated failover-duplex policy. For the details of how to setup the vMSC with SnapMirror active sync (SM-as) utilizing System Manager and ONTAP Tools, check VMware vSphere Metro Storage Cluster with SnapMirror active sync.

Prerequisites

- NetApp storage systems: ensure you have two NetApp storage clusters (source and destination) with Snapmirror licenses.
- Network connectivity: verify low-latency network connectivity between the source and destination systems.
- Cluster and SVM peering: set up cluster peering and Storage Virtual Machine (SVM) peering between the source and destination clusters.
- ONTAP Version: ensure both clusters are running a version of ONTAP that supports synchronous replication. For SM active sync, ONTAP 9.15.1 and onward, is required.
- VMware vMSC infrastructure: a stretched cluster enables the subsystems to span geographies, presenting a single and common base infrastructure set of resources to the vSphere cluster at both sites. It stretches network and storage between sites.
- Use ONTAP tools 10.2 onwards for ease of use for NetApp SnapMirror, more details check ONTAP tools for VMware vSphere 10.
- A zero RPO Snapmirror synchronous relationship must exist between the primary and secondary cluster.
- All LUNs on the destination volume must be unmapped before the zero RTO Snapmirror relationship can be created.
- Snapmirror active sync only supports SAN protocols (not NFS/CIFS). Ensure no constituent of the consistency group is mounted for NAS access.

Steps to convert from asymmetric to symmetric SM active sync

In the example below, selectrz1 is the primary site and selectrz2 is the secondary site.

1. From the secondary site, perform a SnapMirror update on the existing relationship.

   ```
   selectrz2::> snapmirror update -destination-path site2:/cg/CGsite1_dest
   ```

2. Verify that the SnapMirror update completed successfully.

   ```
   selectrz2::> snapmirror show
   ```

3. Pause each of the zero RPO synchronous relationships.

   ```
    selectrz2::> snapmirror quiesce -destination-path
   site2:/cg/CGsite1_dest
   ```

4. Delete each of the zero RPO synchronous relationships.

```
selectrz2::> snapmirror delete -destination-path site2:/cg/CGsite1_dest
```

5. Release the source SnapMirror relationship but retain the common snapshots.

```
selectrz1::> snapmirror release -relationship-info-only  true
-destination-path svm0.1:/cg/CGsite1_dest
".
```

6. Create a zero RTO SnapMirror synchronous relationship with the AutomatedFailoverDuplex policy.

```
selectrz2::> snapmirror create -source-path svm0.1:/cg/CGsite1
-destination-path site2:/cg/CGsite1_dest -cg-item-mappings
site1lun1:@site1lun1_dest -policy AutomatedFailOverDuplex
```

7. If the existing hosts are local the primary cluster, add the host to the secondary cluster and establish connectivity with respective access to each cluster.
8. On the secondary site, delete the LUN maps on the igroups associated with remote hosts.

```
selectrz2::> lun mapping delete -vserver svm0 -igroup wlkd01 -path
/vol/wkld01/wkld01
```

9. On the primary site, modify the initiator configuration for existing hosts to set the proximal path for initiators on the local cluster.

```
selectrz1::> set -privilege advanced
selectrz1::*> igroup initiator add-proximal-vserver -vserver site1
-initiator iqn.1998-01.com.vmware:vcf-wkld-
esx01.sddc.netapp.com:575556728:67 -proximal-vserver site1
```

10. Add a new igroup and initiator for the new hosts and set the host proximity for host affinity to its local site. Enable igroup replication to replicate the configuration and invert the host locality on the remote cluster.

```
selectrz1::*> igroup modify -vserver site1  -igroup smbc2smas
-replication-peer svm0.1
selectrz1::*> igroup initiator add-proximal-vserver -vserver site1
-initiator iqn.1998-01.com.vmware:vcf-wkld-
esx01.sddc.netapp.com:575556728:67 -proximal-vserver svm0.1
```

11. Discover the paths on the hosts and verify the hosts have an Active/Optimized path to the storage LUN

from the preferred cluster.

12. Deploy the application and distribute the VM workloads across clusters.
13. Resynchronize the consistency group.

```
selectrz2::> snapmirror resync -destination-path site2:/cg/CGsite1_dest
```

14. Rescan host LUN I/O paths to restore all paths to the LUNs.

Learn about using VMware Virtual Volumes (vVols) with ONTAP storage

Learn about the benefits of VMware Virtual Volumes (vVols), provisioning of ONTAP tools for VMware vSphere, data protection strategies, and VM migration guidelines.

Overview

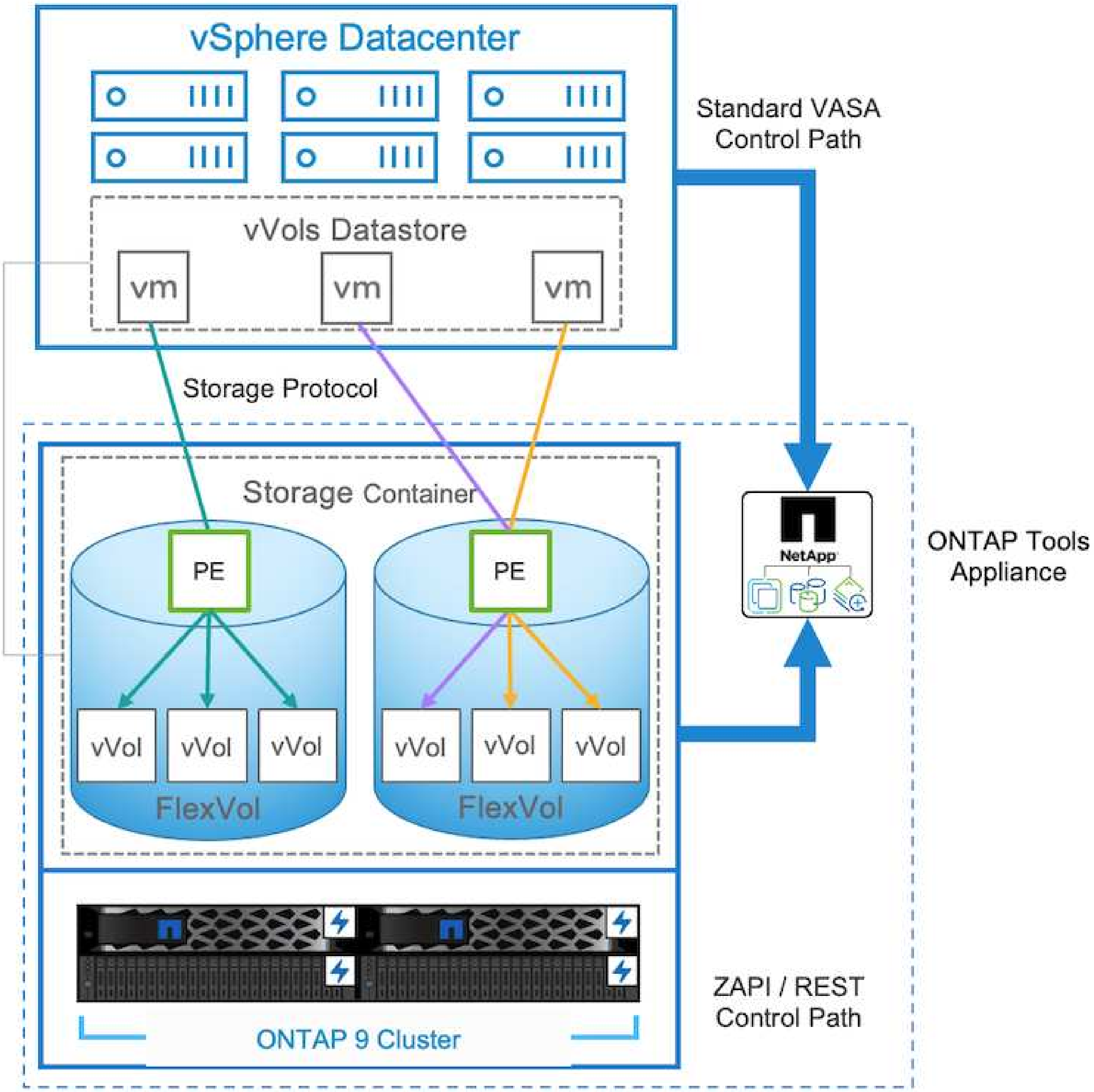
The vSphere API for Storage Awareness (VASA) make it easy for a VM administrator to use whatever storage capabilities are needed to provision VMs without having to interact with their storage team. Prior to VASA, VM administrators could define VM storage policies, but had to work with their storage administrators 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 VCF Automation (formerly known as Aria or vRealize) Automation or VMware vSphere Kubernetes Service to automatically select storage from an assigned policy. This approach is known as storage policy based management. While storage capability profiles and policies may also be used with traditional datastores, our focus here is on vVols datastores. The VASA provider for ONTAP is included as part of ONTAP tools for VMware vSphere.

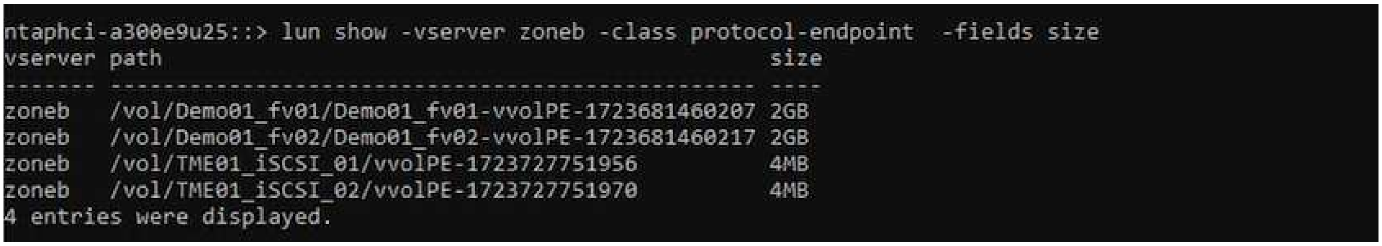
The advantages of having VASA Provider out of Storage Array, includes:

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

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

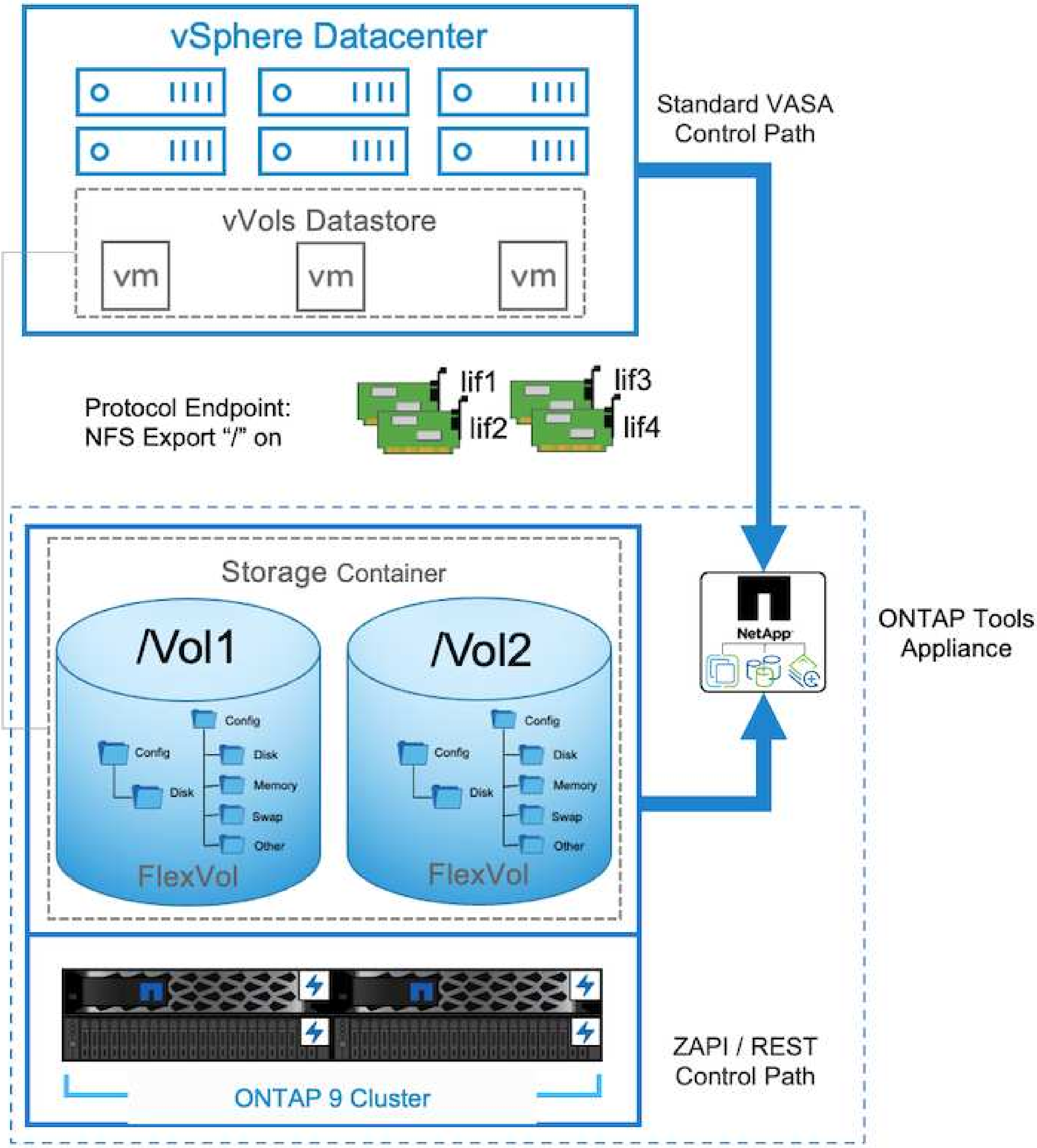
The Protocol Endpoint (PE) is mostly managed by ONTAP tools. In case of iSCSI based vVols, one PE is created for every ONTAP volume that is part of that storage container or vVol datastore. The PE for iSCSI is a small sized LUN (4MiB for 9.x and 2GiB for 10.x) that is presented to vSphere host and multipathing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

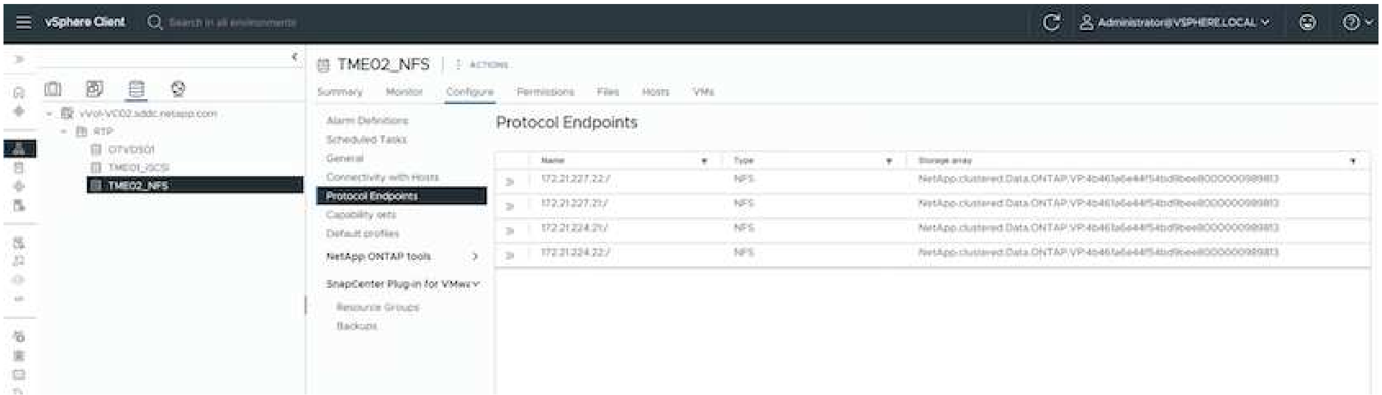




```
ntaphci-a300e9u25::> lun show -vserver zoneb -class protocol-endpoint  -fields size
vserver path                                                   size
------- ------------------------------------------------------ ----
zoneb   /vol/Demo01_fv01/Demo01_fv01-vvolPE-1723681460207 2GB
zoneb   /vol/Demo01_fv02/Demo01_fv02-vvolPE-1723681460217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

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





Protocol Endpoints

Name	Type	Storage array
172.21.227.22:/	NFS	NetApp.clustered.Data.ONTAP.VP:4b461a6e44f54bd9bee800000989813
172.21.227.21:/	NFS	NetApp.clustered.Data.ONTAP.VP:4b461a6e44f54bd9bee800000989813
172.21.224.21:/	NFS	NetApp.clustered.Data.ONTAP.VP:4b461a6e44f54bd9bee800000989813
172.21.224.22:/	NFS	NetApp.clustered.Data.ONTAP.VP:4b461a6e44f54bd9bee800000989813

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

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

ONTAP tools 9.x

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

ONTAP tools 10.x

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

Why vVols?

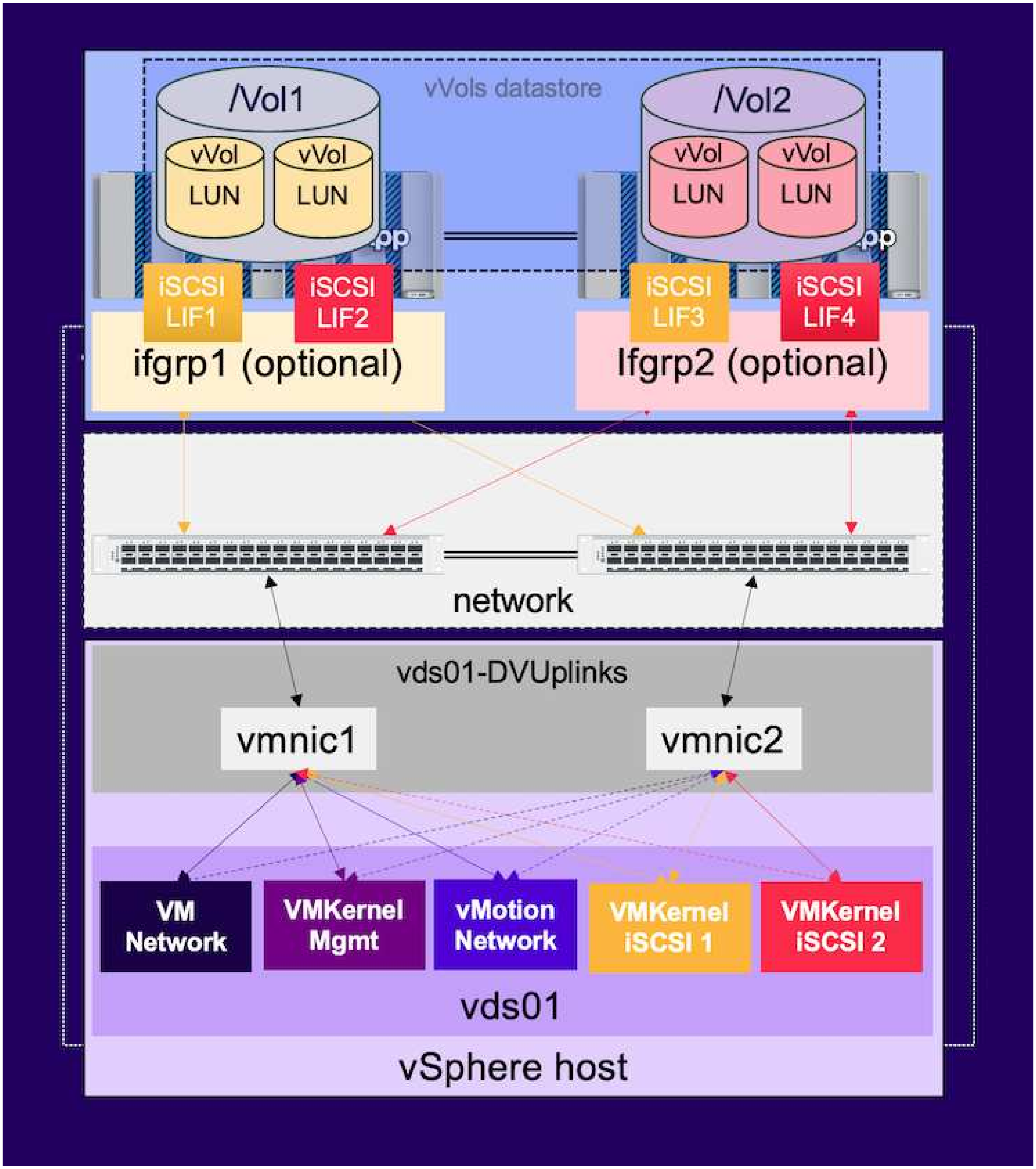
VMware Virtual Volumes (vVols) provides the following benefits:

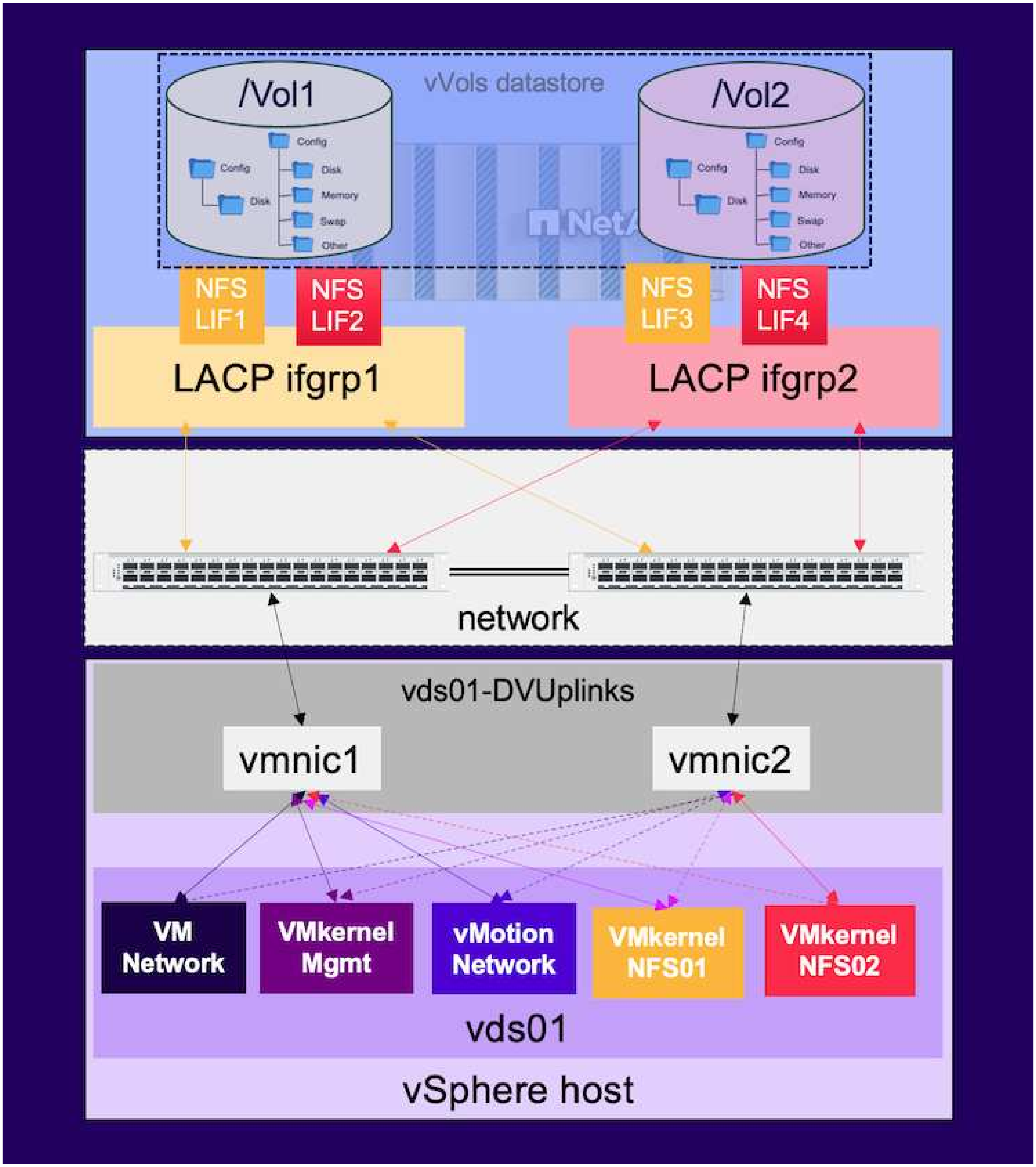
- Simplified provisioning (No need to worry about Maximum LUN limits per vSphere host or need to create the NFS exports for each volume)
- Minimizes the number of iSCSI/FC paths (For block SCSI based vVol)
- Snapshots, Clones & other Storage operations are typically offloaded to storage array and performs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

Connectivity options

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

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



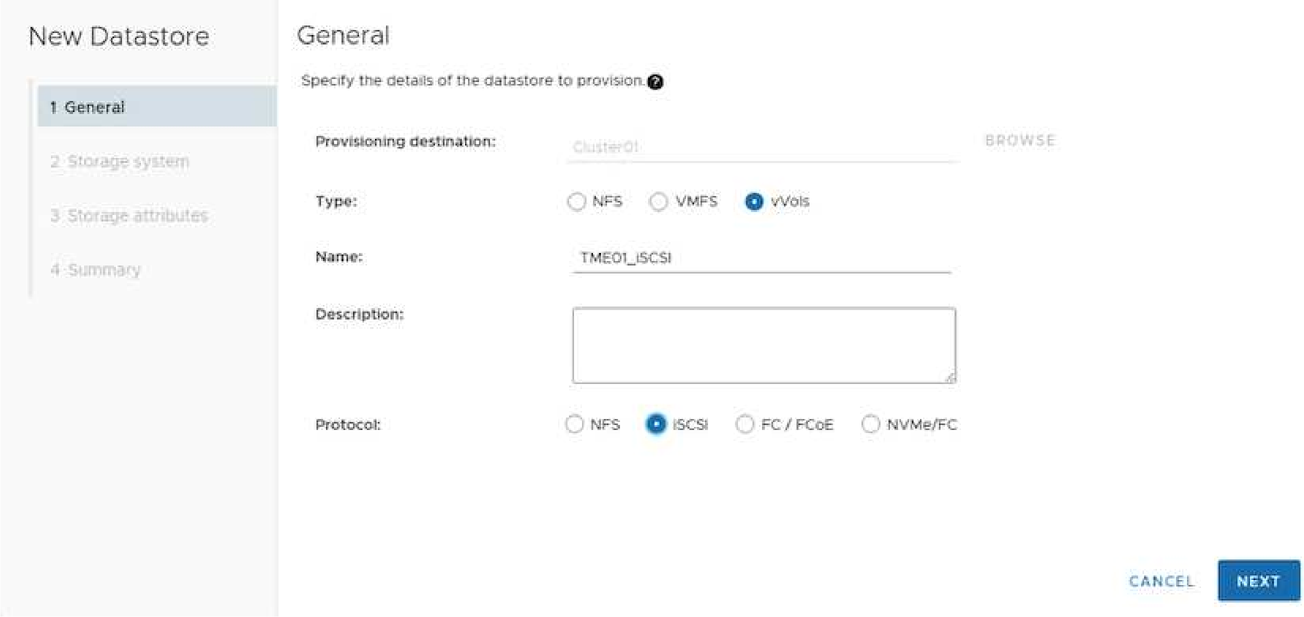


Provisioning using ONTAP tools for VMware vSphere

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

With ONTAP tools 9.13

1. Right click on vSphere cluster or host and select Provision Datastore under NetApp ONTAP tools.
2. Keep the type as vVols, provide name for the datastore and select the desired protocol



New Datastore

General

Specify the details of the datastore to provision.

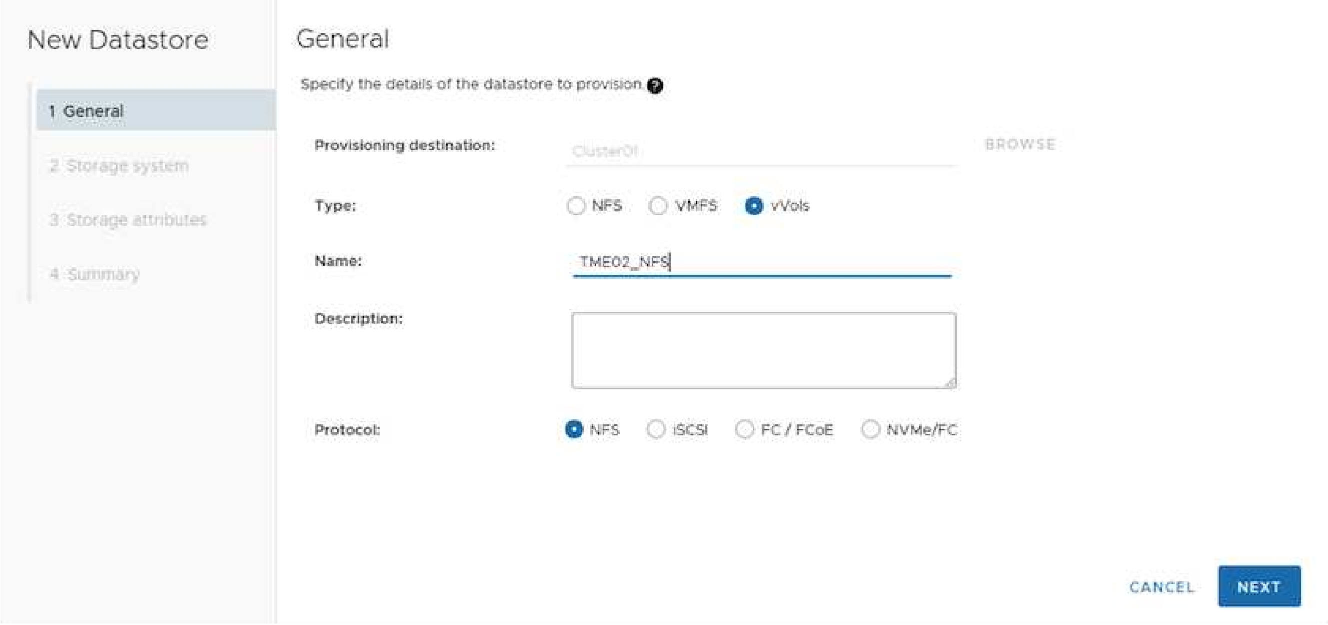
Provisioning destination: Cluster01

Type: ○ NFS ○ VMFS ● vVols

Name: TME01_iSCSI

Description:

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



New Datastore

General

Specify the details of the datastore to provision.

Provisioning destination: Cluster01

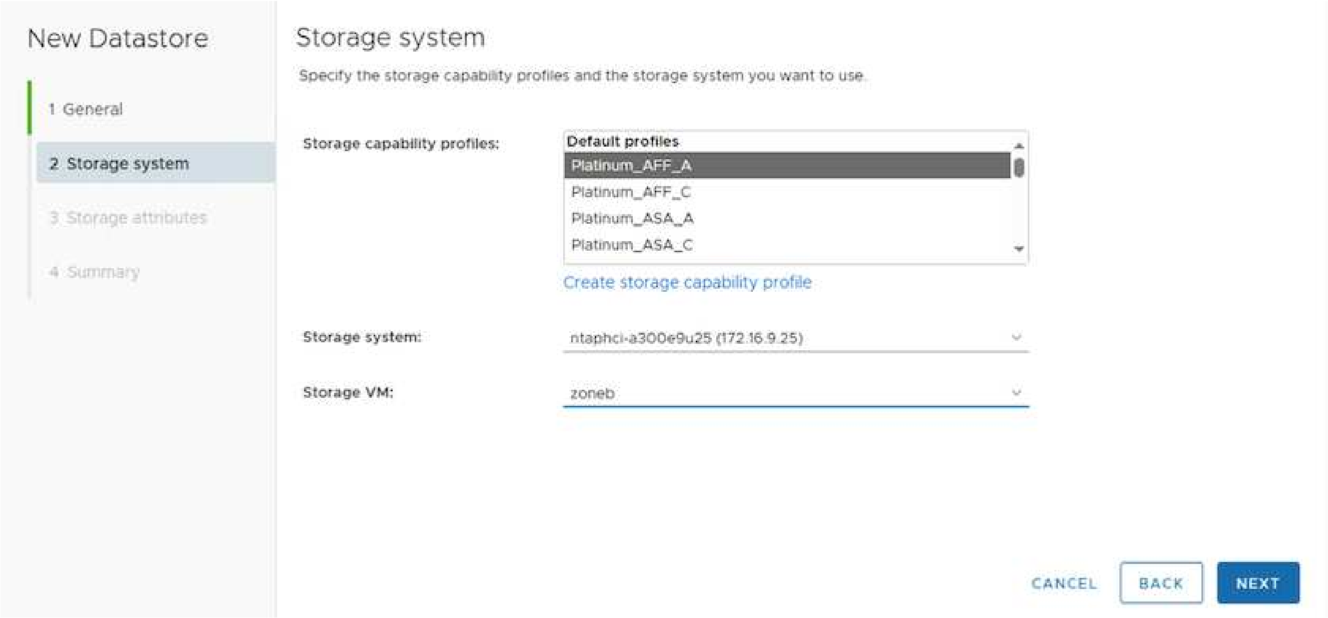
Type: ○ NFS ○ VMFS ● vVols

Name: TME02_NFS

Description:

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

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



New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

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

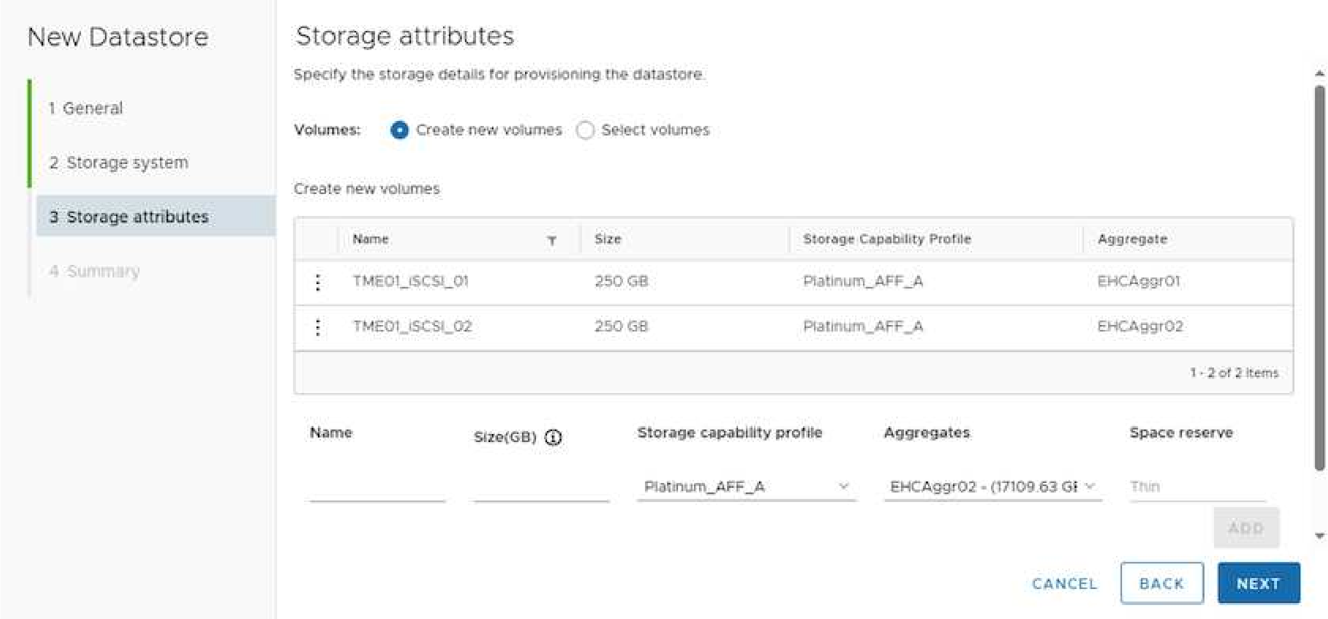
Storage capability profiles: Default profiles: Platinum_AFF_A (selected), Platinum_AFF_C, Platinum_ASA_A, Platinum_ASA_C

Create storage capability profile

Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: zoneb

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



New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: ● Create new volumes ○ Select volumes

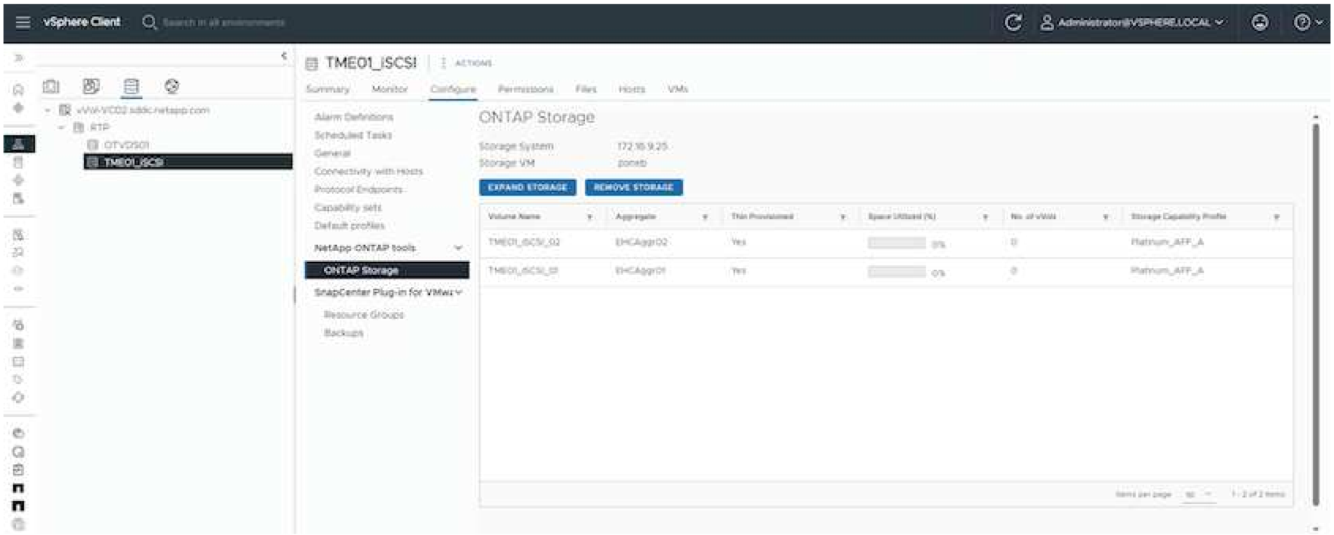
Create new volumes

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

1 - 2 of 2 items

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

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



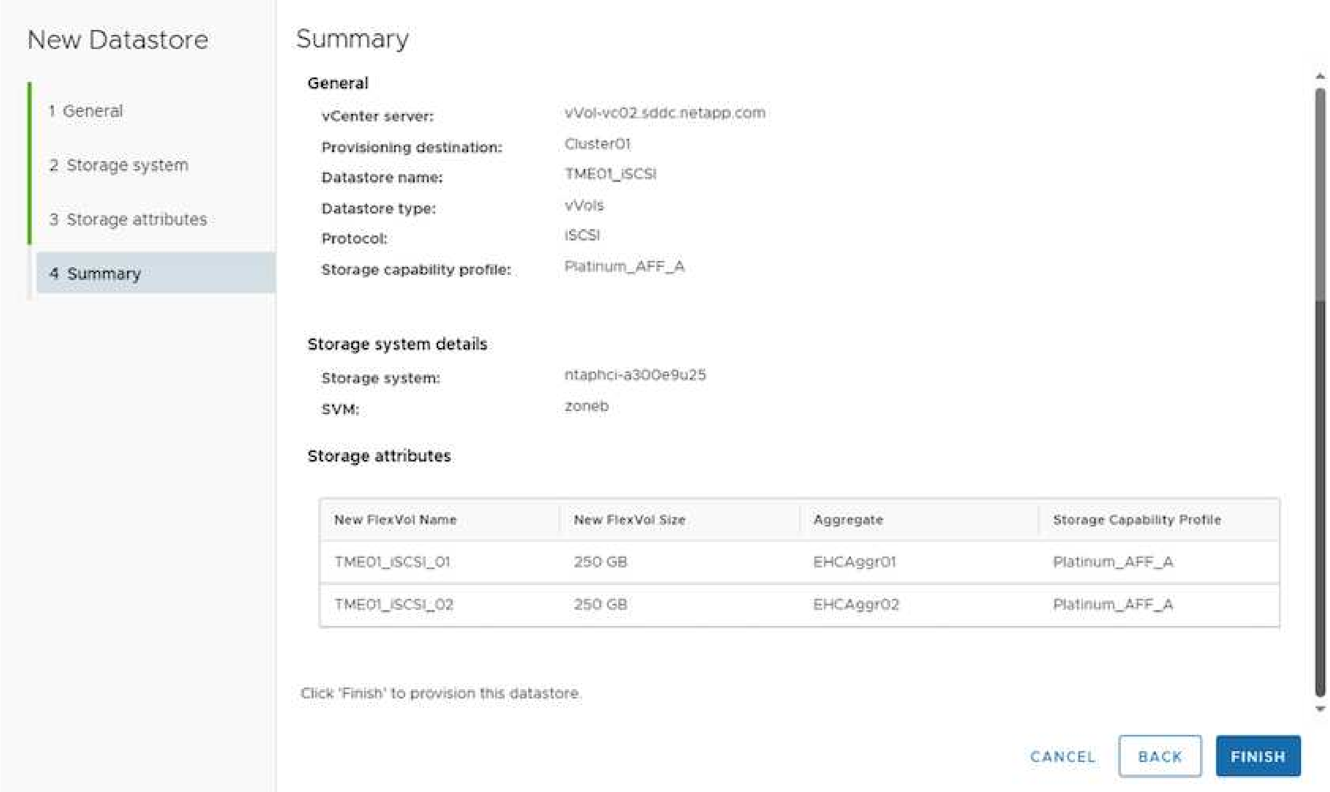
TME01_iSCSI

ONTAP Storage

Storage System 172.16.9.25
Storage VM zoneb

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

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



Summary

General

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

Storage system details

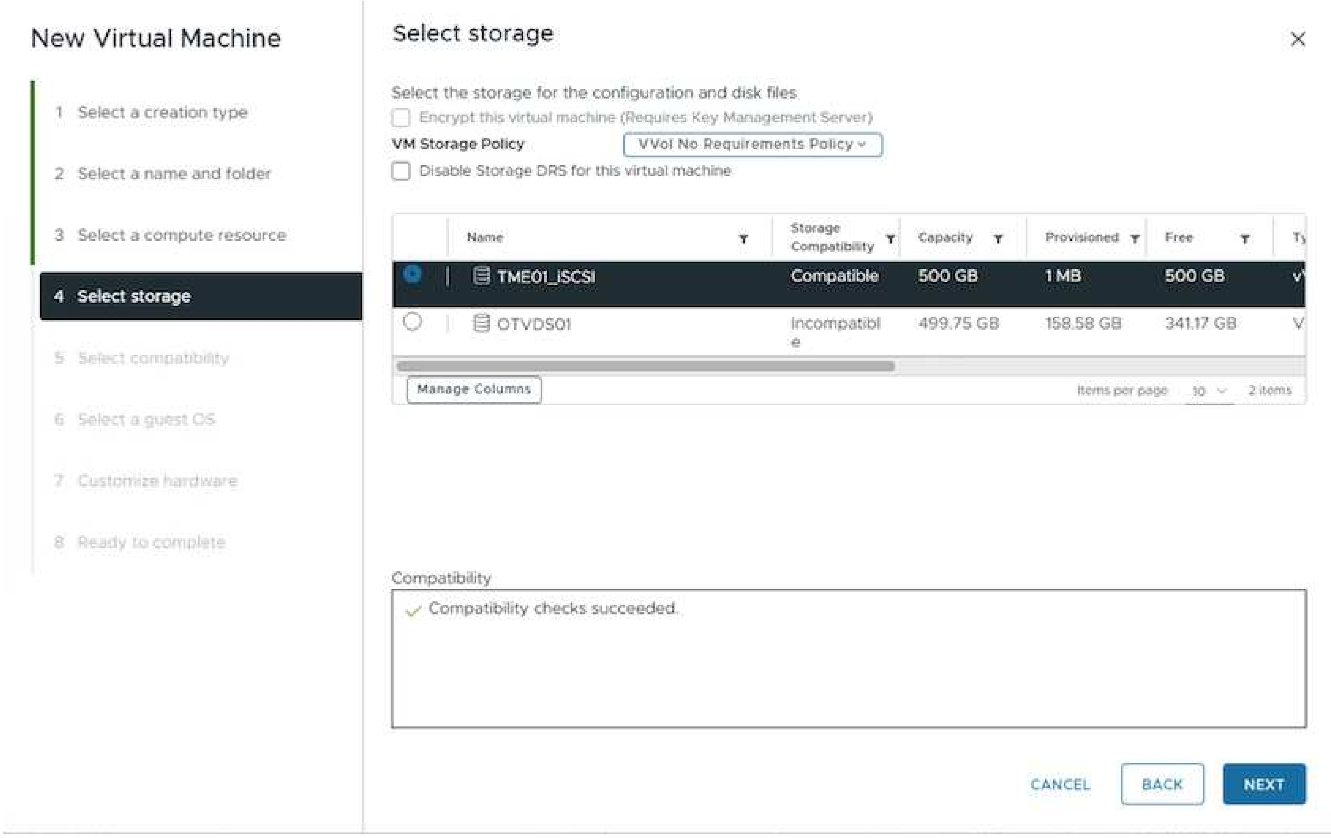
Storage system:	ntaphci-a300e9u25
SVM:	zoneb

Storage attributes

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

Click 'Finish' to provision this datastore.

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



Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

VM Storage Policy: VVol No Requirements Policy

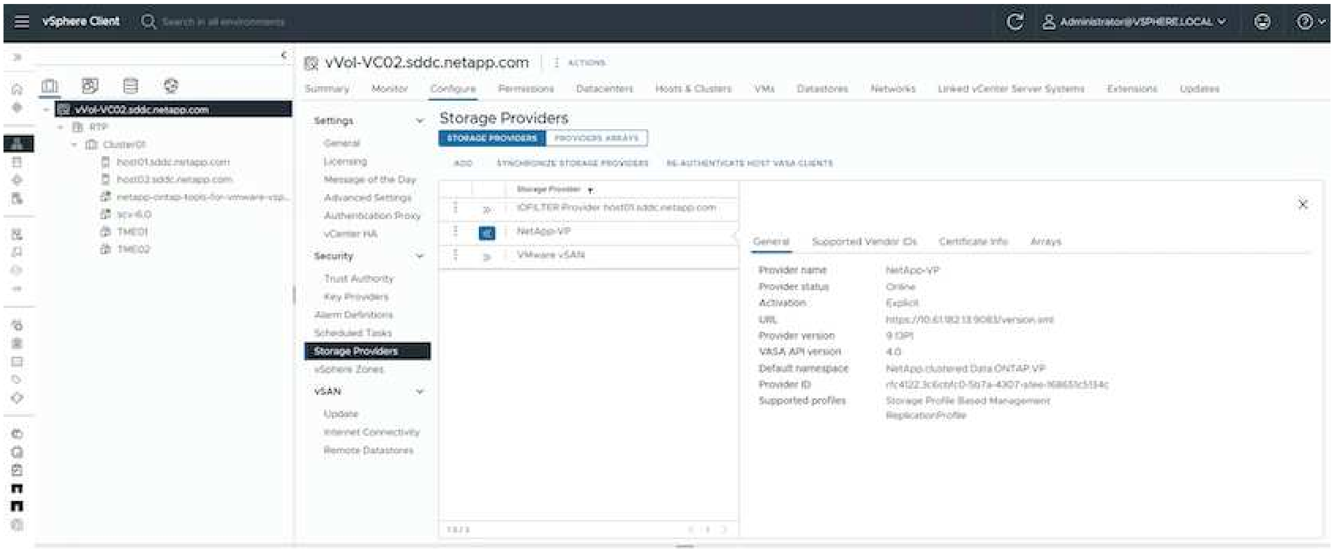
□ Disable Storage DRS for this virtual machine

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

Compatibility

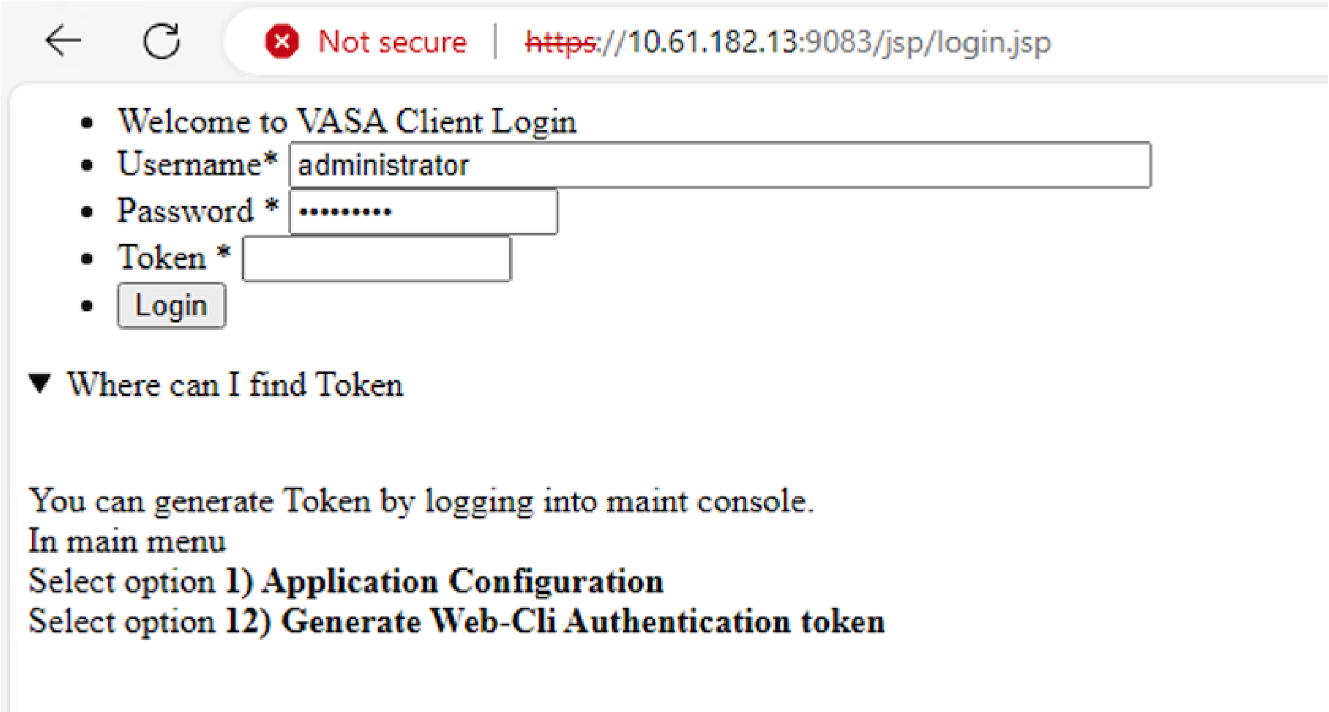
✓ Compatibility checks succeeded.

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



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

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

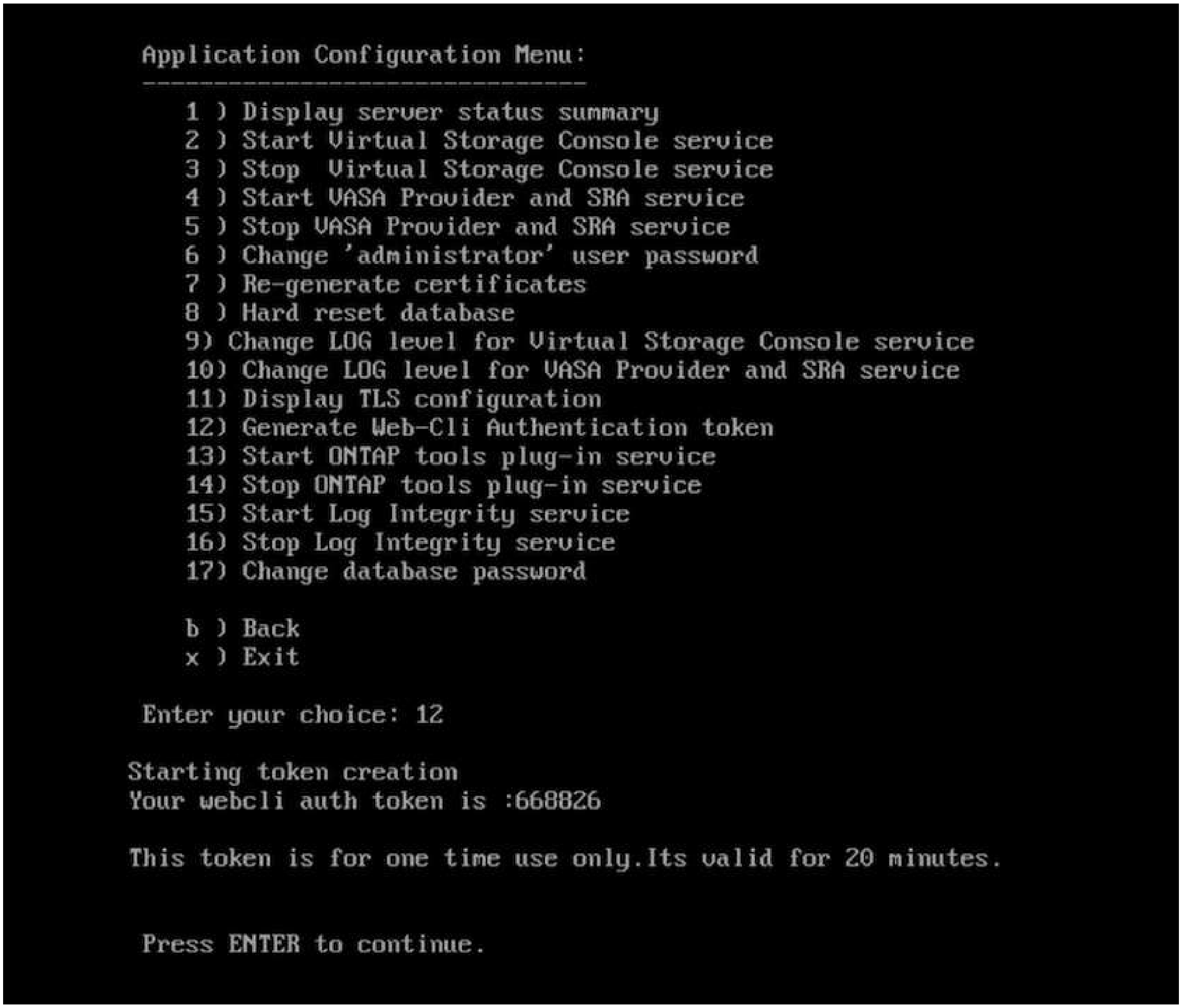


- Welcome to VASA Client Login
- Username* administrator
- Password * •••••••••
- Token *
- Login

▼ Where can I find Token

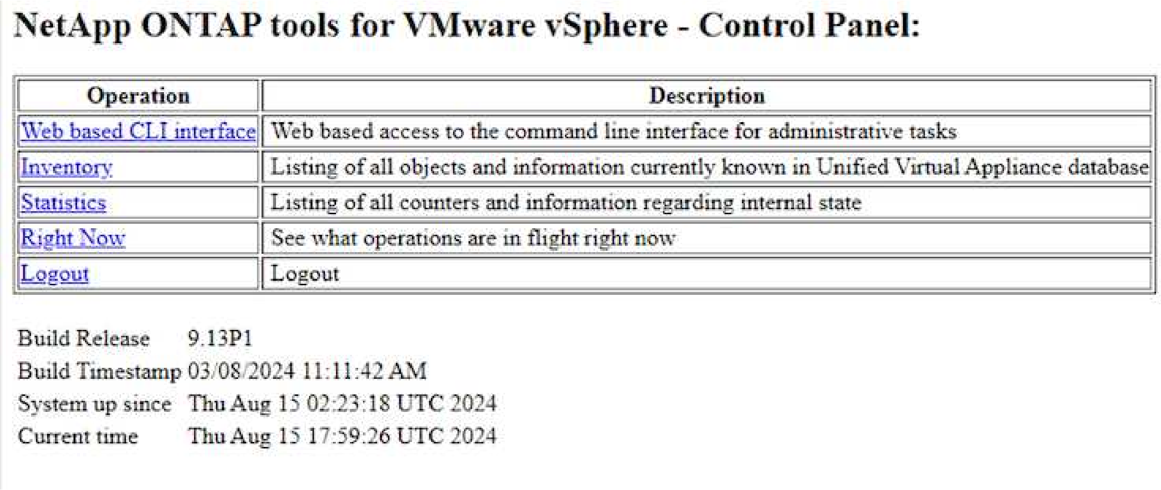
You can generate Token by logging into maint console.
In main menu
Select option **1) Application Configuration**
Select option **12) Generate Web-Cli Authentication token**

or use updated password with ONTAP tools maintenance console.



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

    b ) Back
    x ) Exit

 Enter your choice: 12

Starting token creation
Your webcli auth token is :668826

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


 Press ENTER to continue.
```

Select Web based CLI interface.

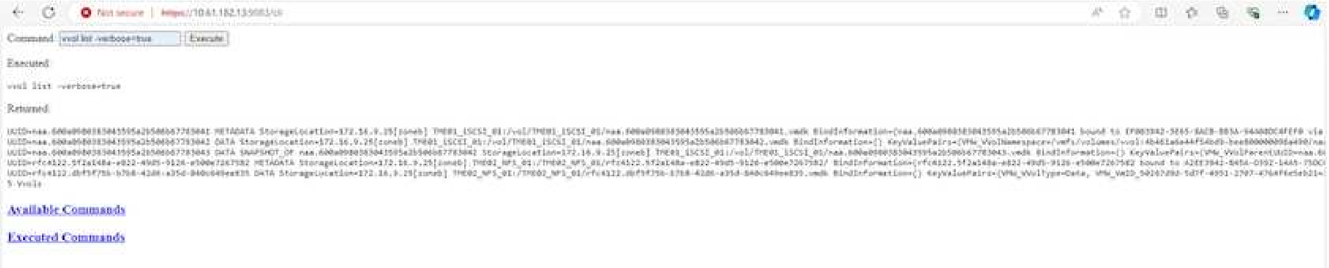


NetApp ONTAP tools for VMware vSphere - Control Panel:

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

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

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



Command: vvol list -verbose=true Execute

Executed

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

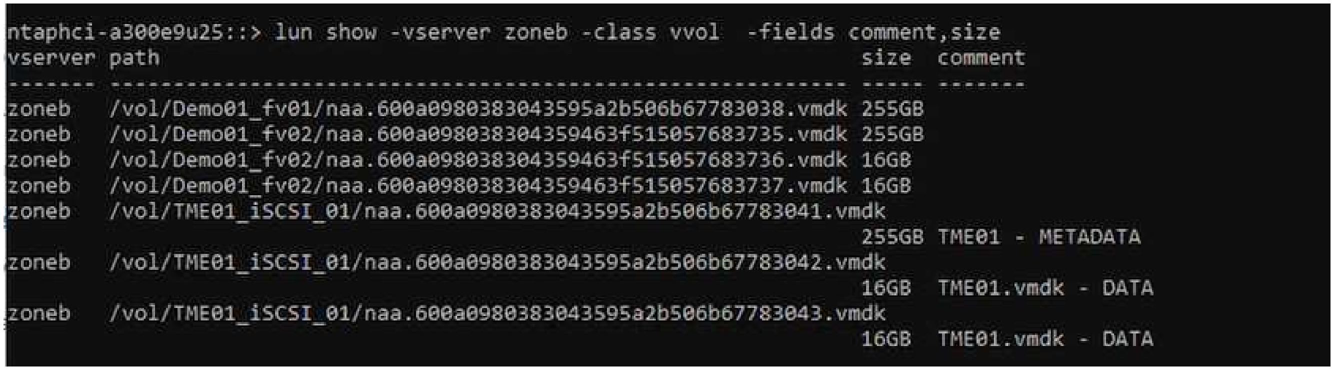
Returned

```
UUID=naa.600a0980383043595a2b506b67783041 METADATA StorageLocation=172.16.9.25[zoneb] TME01_iSCSI_01:/vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783041.vmdk BindInformation={naa.600a0980383043595a2b506b67783041 bound to EF003942-3E65-8ACB-8B5A-94A0DC4FEFF0 via
UUID=naa.600a0980383043595a2b506b67783042 DATA StorageLocation=172.16.9.25[zoneb] TME01_iSCSI_01:/vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783042.vmdk BindInformation={} KeyValuePairs={VMW_VVolNamespace=/vmfs/volumes/vvol:4b461a6a44f54bd9-bee800000000a490/na
UUID=naa.600a0980383043595a2b506b67783043 DATA SNAPSHOT_OF naa.600a0980383043595a2b506b67783042 StorageLocation=172.16.9.25[zoneb] TME01_iSCSI_01:/vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783043.vmdk BindInformation={} KeyValuePairs={VMW_VVolParentUUID=naa.6
UUID=rfc4122.5f2a148a-e822-49d5-9126-e500e7267582 METADATA StorageLocation=172.16.9.25[zoneb] TME02_NFS_01:/TME02_NFS_01/rfc4122.5f2a148a-e822-49d5-9126-e500e7267582/ BindInformation={rfc4122.5f2a148a-e822-49d5-9126-e500e7267582 bound to A2EF3942-B456-D392-14A5-75DC
UUID=rfc4122.dbf9f756-b768-42d6-a35d-840c649ea835 DATA StorageLocation=172.16.9.25[zoneb] TME02_NFS_01:/TME02_NFS_01/rfc4122.dbf9f756-1768-42d6-a35d-840c649ea835.vmdk BindInformation={} KeyValuePairs={VMW_VVolType=Data, VMW_VmID_50267d92-5d7f-4951-2797-476af6e5ab21=
5 Vvols
```

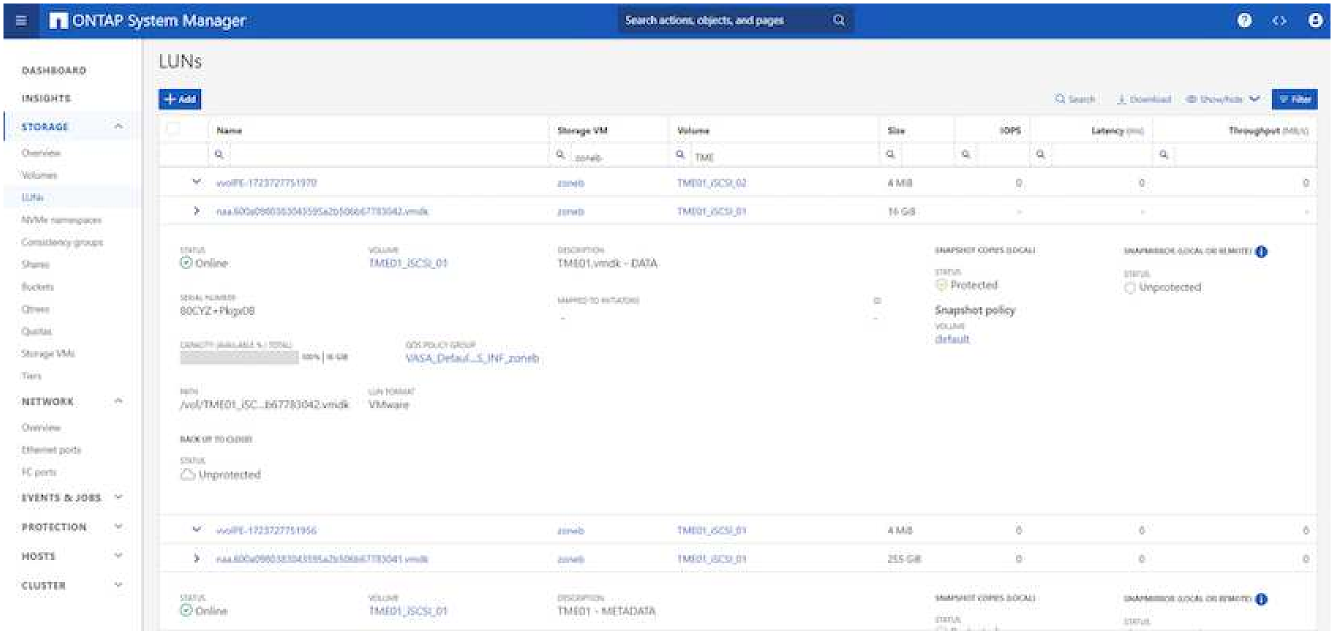
Available Commands

Executed Commands

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



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



LUNs

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

STATUS
Online

VOLUME
TME01_iSCSI_01

DESCRIPTION
TME01.vmdk - DATA

SERIAL NUMBER
80CYZ+Pkgx08

MAPPED TO INITIATORS
-

ID
-

CAPACITY (AVAILABLE % / TOTAL)
100% | 16 GiB

QOS POLICY GROUP
VASA_Defaul..._S_INF_zoneb

PATH
/vol/TME01_iSC...b67783042.vmdk

LUN FORMAT
VMware

BACK UP TO CLOUD
STATUS
Unprotected

SNAPSHOT COPIES (LOCAL)
STATUS
Protected

Snapshot policy
VOLUME
default

SNAPMIRROR (LOCAL OR REMOTE)
STATUS
Unprotected

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

STATUS
Online

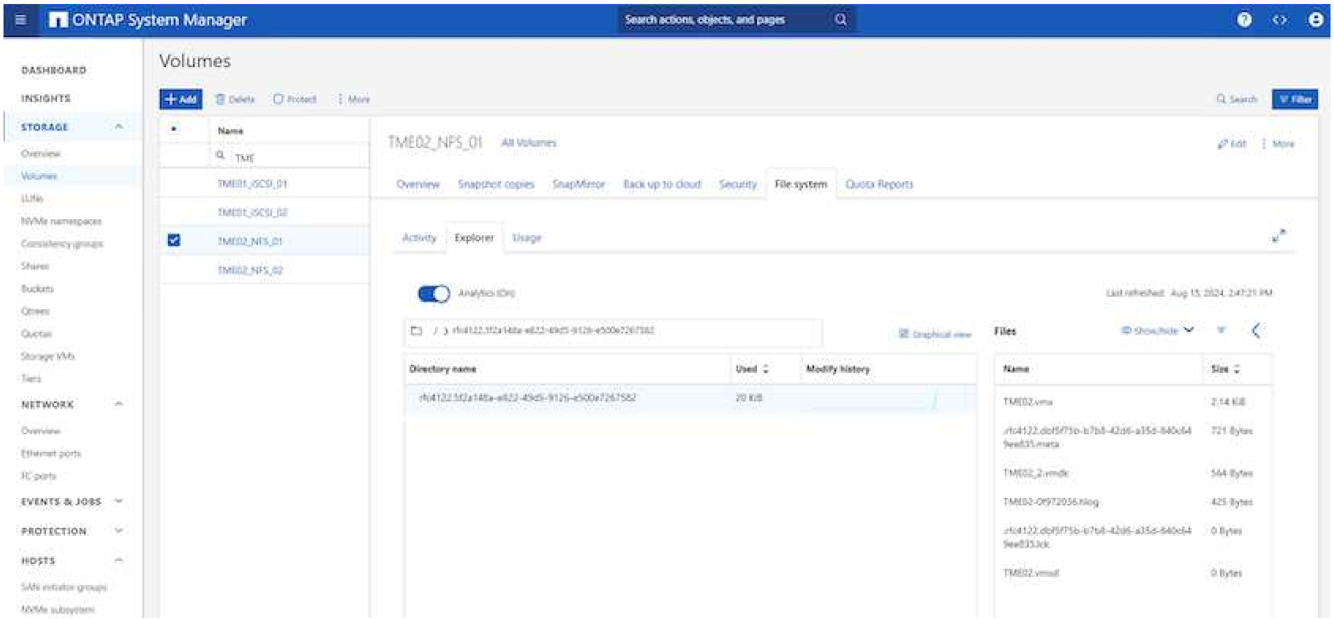
VOLUME
TME01_iSCSI_01

DESCRIPTION
TME01 - METADATA

SNAPSHOT COPIES (LOCAL)
STATUS

SNAPMIRROR (LOCAL OR REMOTE)
STATUS

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

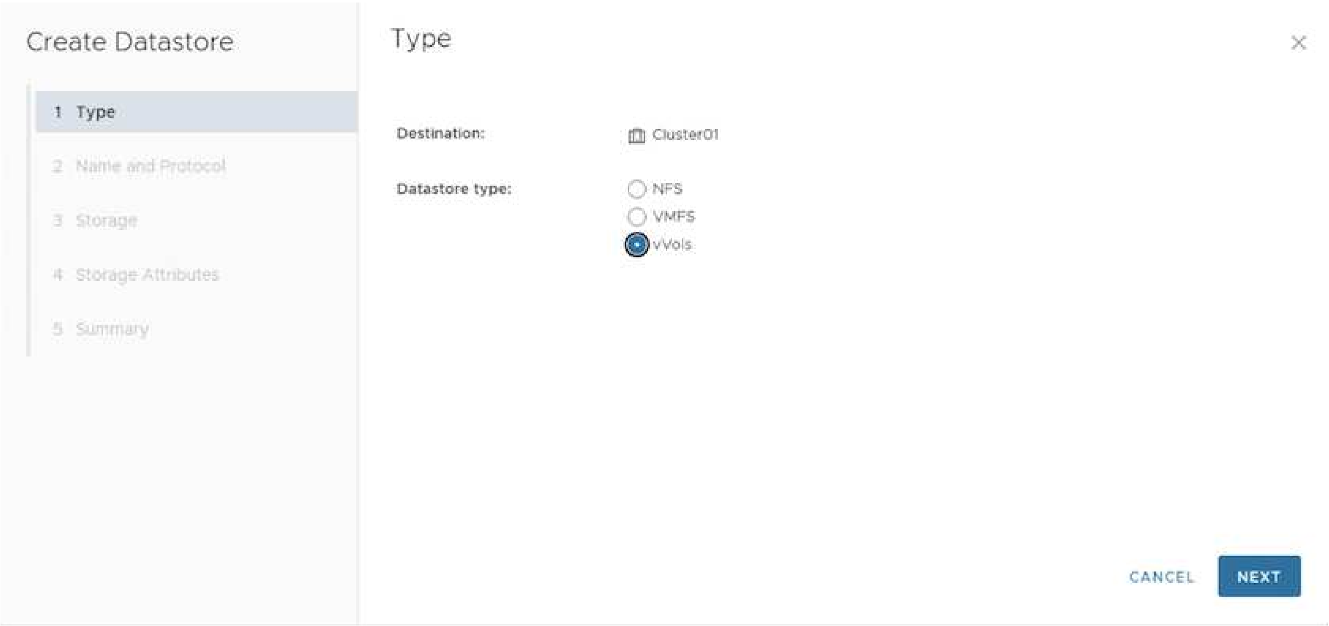


Directory name	Used	Modify history
rfc4122.5f2a148a-e822-49d5-9126-e500e7267582	20 KiB	

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

With ONTAP tools 10.1

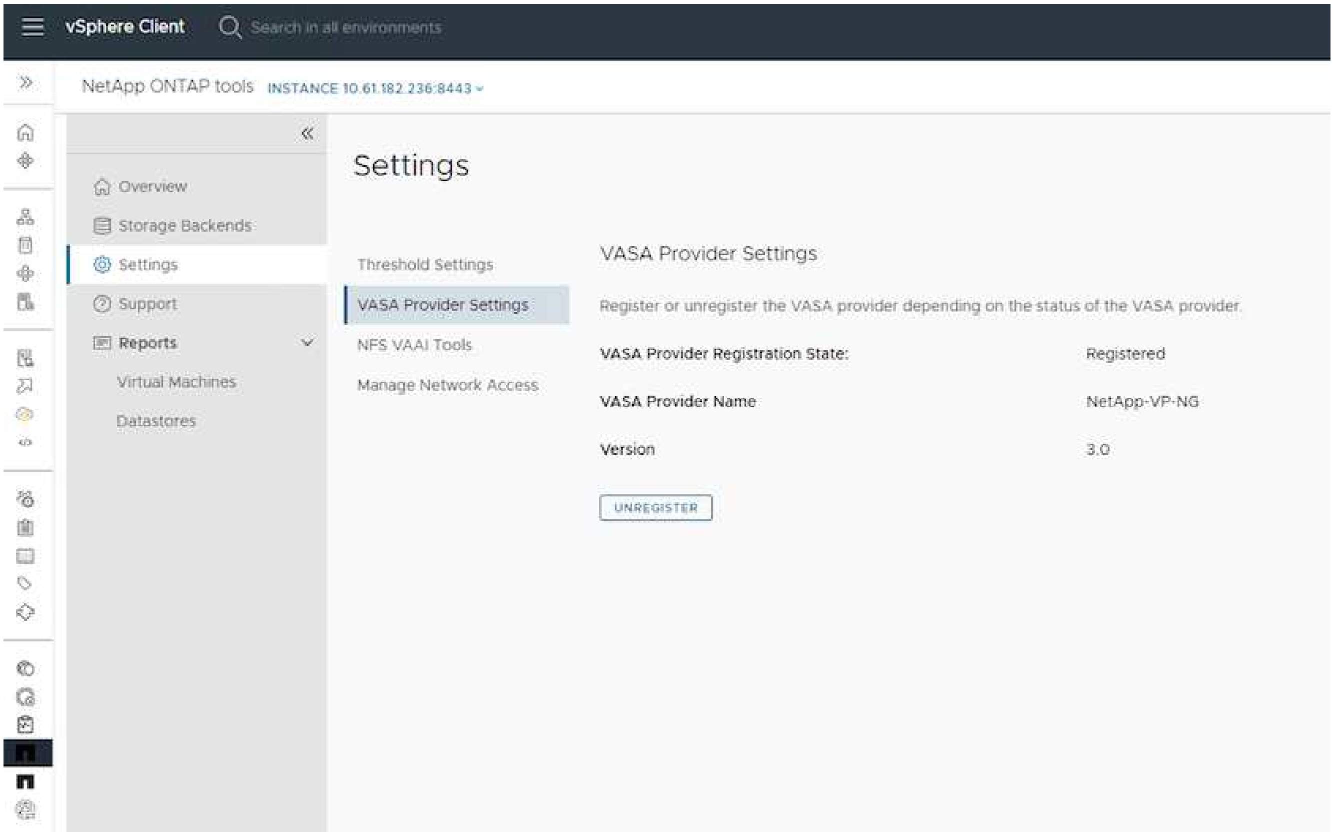
1. Right click on vSphere cluster or host and select Create Datastore (10.1) under NetApp ONTAP tools.
2. Select the datastore type as vVols.



Destination: Cluster01

Datastore type: ○ NFS ○ VMFS ● vVols

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



Settings

VASA Provider Settings

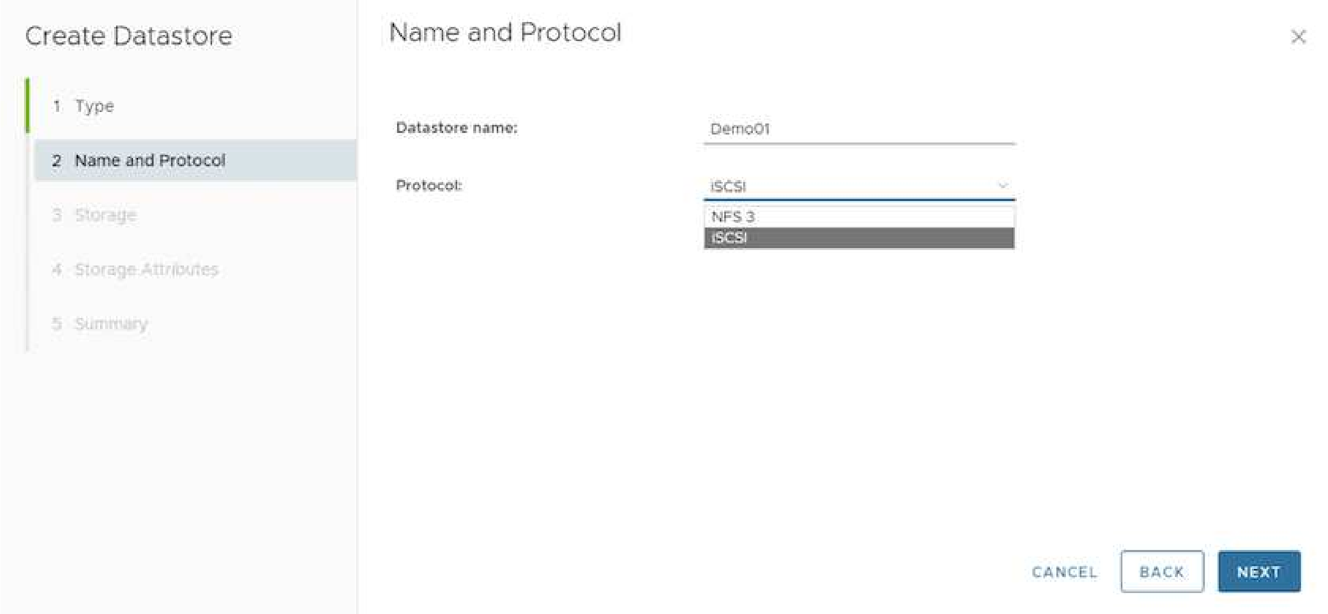
Register or unregister the VASA provider depending on the status of the VASA provider.

VASA Provider Registration State: Registered

VASA Provider Name: NetApp-VP-NG

Version: 3.0

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

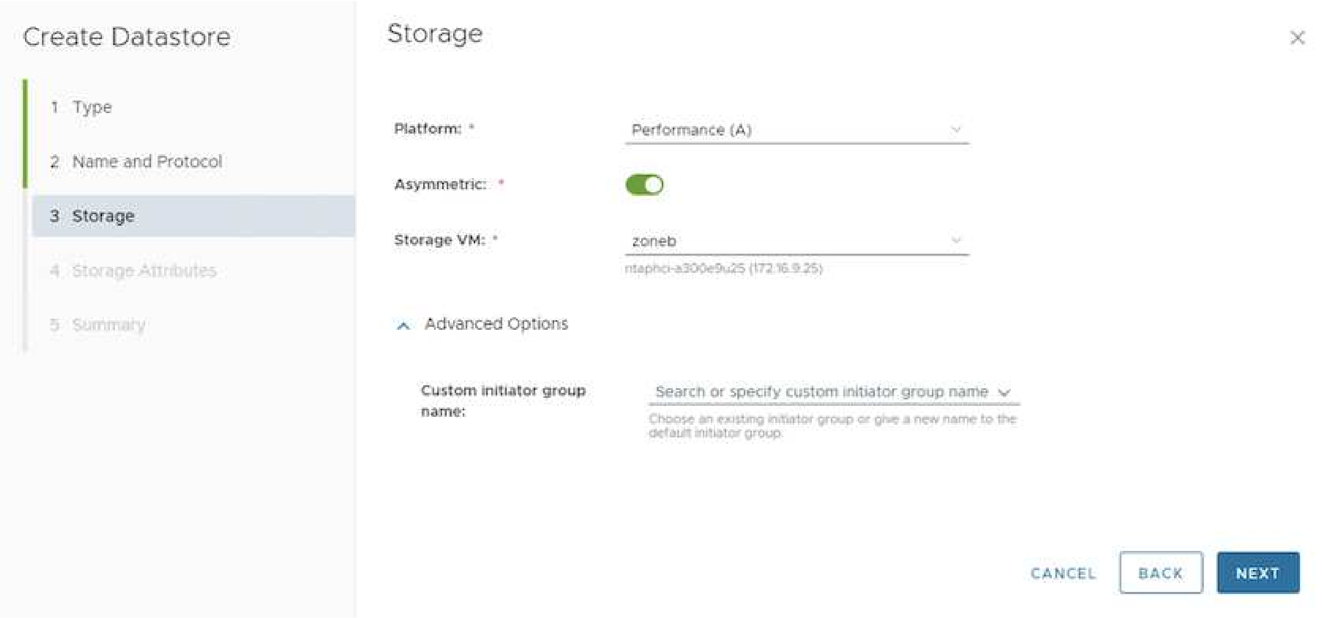


Name and Protocol

Datastore name: Demo01

Protocol: iSCSI

4. Select platform and Storage VM.



Create Datastore

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

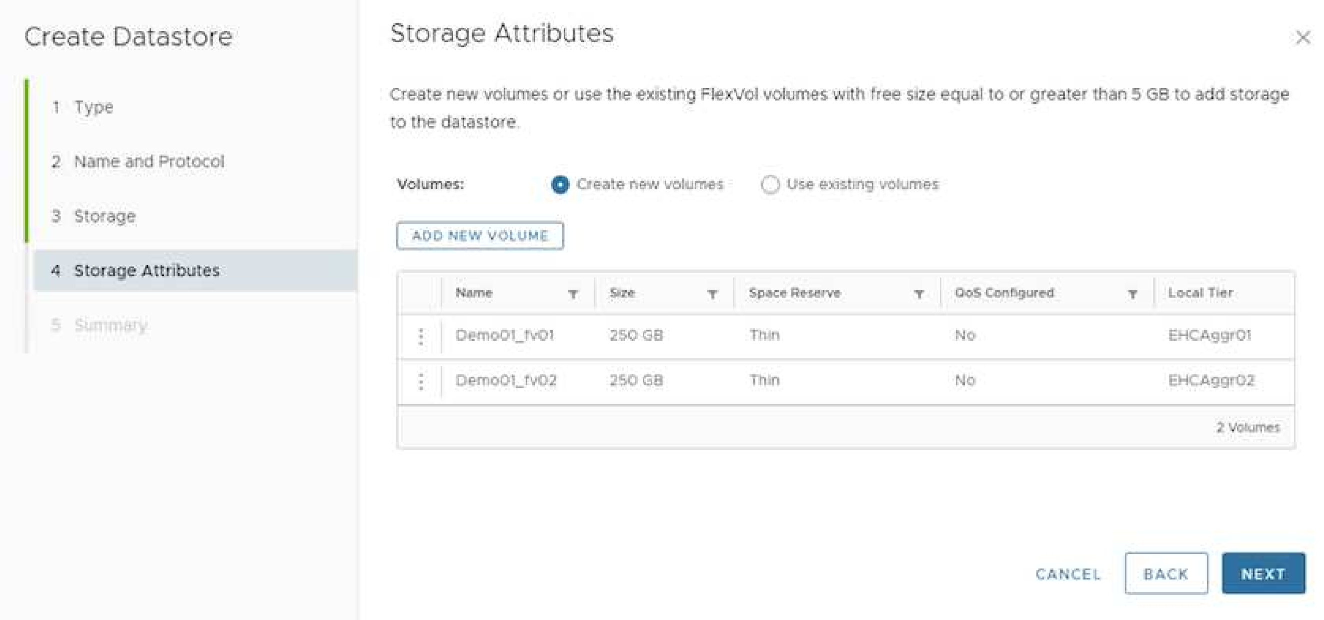
Storage

Platform: *	Performance (A)
Asymmetric: *	●
Storage VM: *	zoneb ntaphci-a300e9u25 (172.16.9.25)

Advanced Options

Custom initiator group name: Search or specify custom initiator group name
Choose an existing initiator group or give a new name to the default initiator group.

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



Create Datastore

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

Storage Attributes

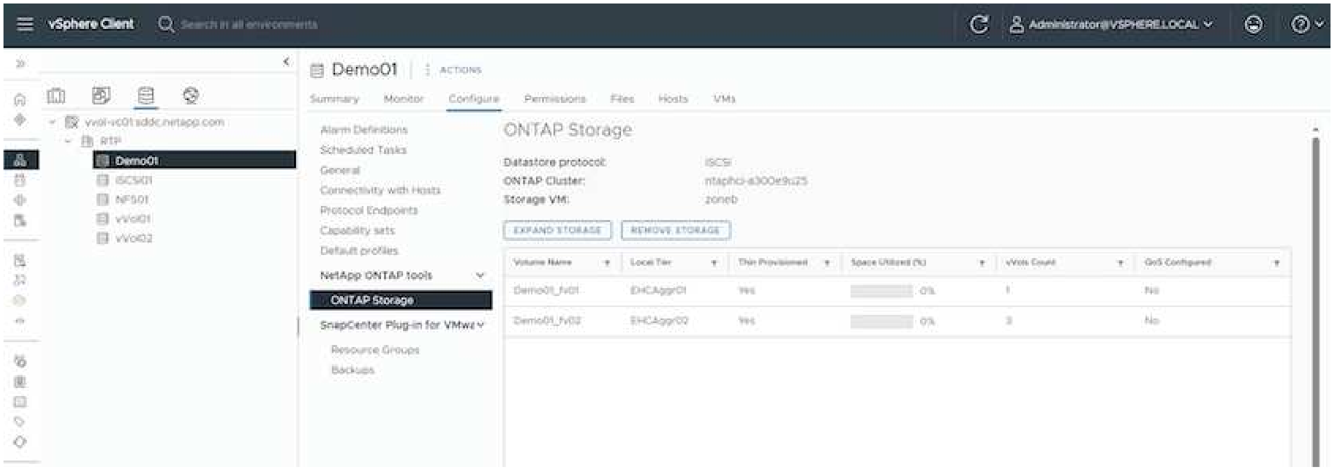
Create new volumes or use the existing FlexVol volumes with free size equal to or greater than 5 GB to add storage to the datastore.

Volumes: ● Create new volumes ○ Use existing volumes

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

2 Volumes

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



Demo01

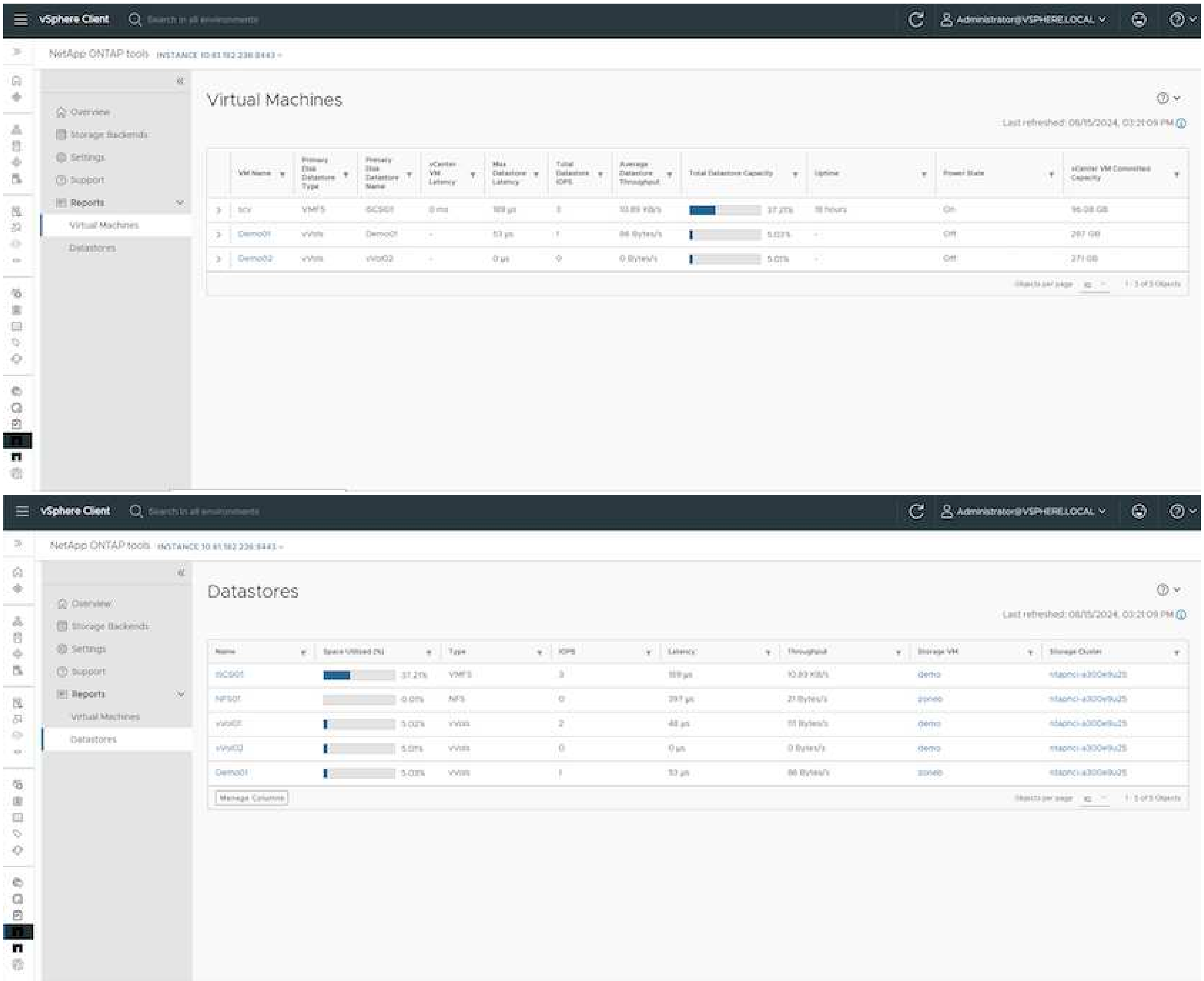
ONTAP Storage

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

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

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

7. ONTAP tools provide the VM and Datastore report.



Virtual Machines

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

VM Name	Primary Disk Datastore Type	Primary Disk Datastore Name	vCenter VM Latency	Max Datastore Latency	Total Datastore IOPS	Average Datastore Throughput	Total Datastore Capacity	Uptime	Power State	vCenter VM Committed Capacity
scv	VMFS	iSCSI01	0 ms	169 µs	3	10.89 KB/s	37.21%	18 hours	On	96.08 GB
Demo01	vVols	Demo01	-	53 µs	1	86 Bytes/s	5.03%	-	Off	287 GB
Demo02	vVols	vVol02	-	0 µs	0	0 Bytes/s	5.01%	-	Off	271 GB

Objects per page 10 1 - 3 of 3 Objects

Datastores

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

Name	Space Utilized (%)	Type	IOPS	Latency	Throughput	Storage VM	Storage Cluster
iSCSI01	37.21%	VMFS	3	169 µs	10.83 KB/s	demo	ntaphci-a300e9u25
NFS01	0.01%	NFS	0	397 µs	21 Bytes/s	zoneb	ntaphci-a300e9u25
vVol01	5.02%	vVols	2	48 µs	111 Bytes/s	demo	ntaphci-a300e9u25
vVol02	5.01%	vVols	0	0 µs	0 Bytes/s	demo	ntaphci-a300e9u25
Demo01	5.03%	vVols	1	53 µs	86 Bytes/s	zoneb	ntaphci-a300e9u25

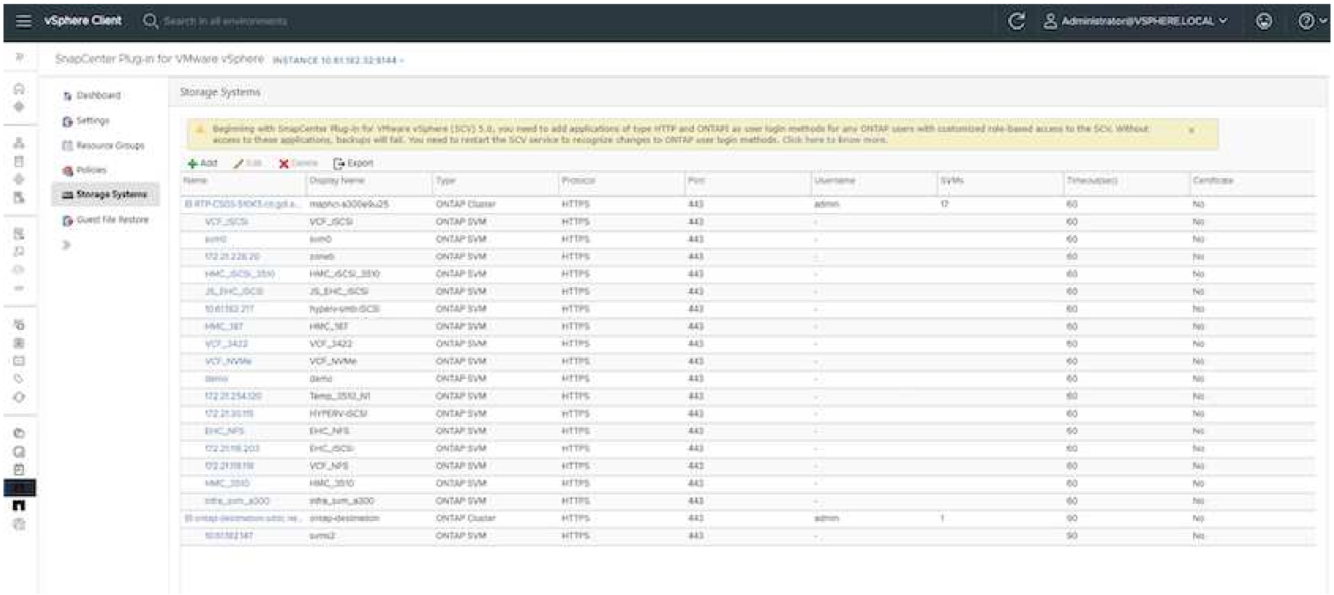
Manage Columns

Objects per page 10 1 - 5 of 5 Objects

Data Protection of VMs on vVol datastore

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

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



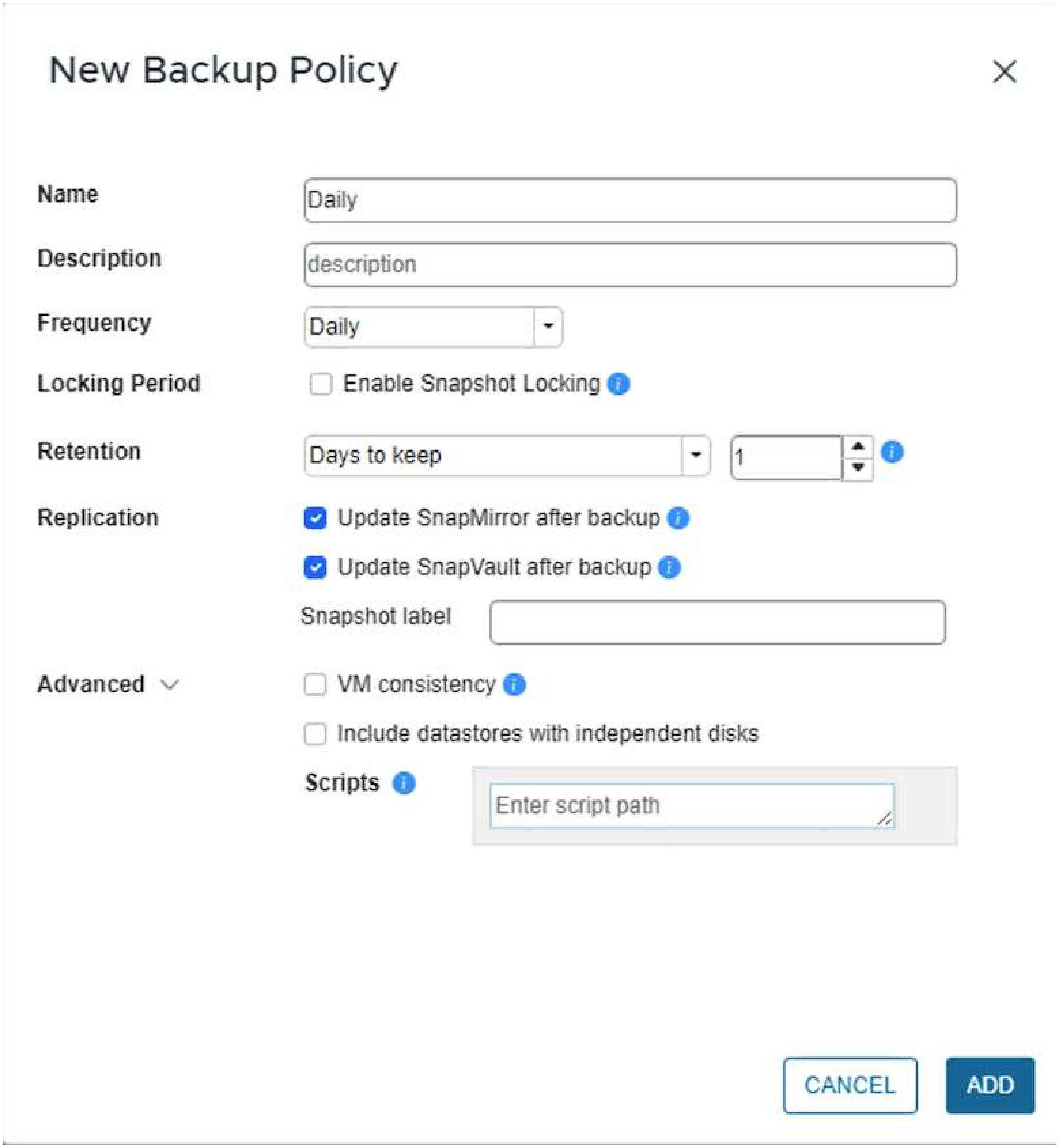
vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
SnapCenter Plug-in for VMware vSphere
INSTANCE 10.61.182.32:8144
Dashboard
Settings
Resource Groups
Policies
Storage Systems
Guest File Restore
Add
Edit
Delete
Export

Storage Systems

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

Name	Display Name	Type	Protocol	Port	Username	SVMs	Timeout(sec)	Certificate
RTP-CS05-SVOK5.rtp.gdl.a...	mapho-a300e9u25	ONTAP Cluster	HTTPS	443	admin	17	60	No
VCF_iSCSI	VCF_iSCSI	ONTAP SVM	HTTPS	443	-		60	No
svm0	svm0	ONTAP SVM	HTTPS	443	-		60	No
172.21.228.20	zoneb	ONTAP SVM	HTTPS	443	-		60	No
HMC_iSCSI_3510	HMC_iSCSI_3510	ONTAP SVM	HTTPS	443	-		60	No
JS_EHC_iSCSI	JS_EHC_iSCSI	ONTAP SVM	HTTPS	443	-		60	No
10.61.182.217	hyperv-smb-iSCSI	ONTAP SVM	HTTPS	443	-		60	No
HMC_187	HMC_187	ONTAP SVM	HTTPS	443	-		60	No
VCF_3422	VCF_3422	ONTAP SVM	HTTPS	443	-		60	No
VCF_NVMe	VCF_NVMe	ONTAP SVM	HTTPS	443	-		60	No
demo	demo	ONTAP SVM	HTTPS	443	-		60	No
172.21.254.120	Temp_3510_N1	ONTAP SVM	HTTPS	443	-		60	No
172.21.30.115	HYPERV-iSCSI	ONTAP SVM	HTTPS	443	-		60	No
EHC_NFS	EHC_NFS	ONTAP SVM	HTTPS	443	-		60	No
172.21.118.203	EHC_iSCSI	ONTAP SVM	HTTPS	443	-		60	No
172.21.118.118	VCF_NFS	ONTAP SVM	HTTPS	443	-		60	No
HMC_3510	HMC_3510	ONTAP SVM	HTTPS	443	-		60	No
infra_svm_a300	infra_svm_a300	ONTAP SVM	HTTPS	443	-		60	No
ontap-destination.sddc.ne...	ontap-destination	ONTAP Cluster	HTTPS	443	admin	1	90	No
10.61.182.147	svm2	ONTAP SVM	HTTPS	443	-		90	No

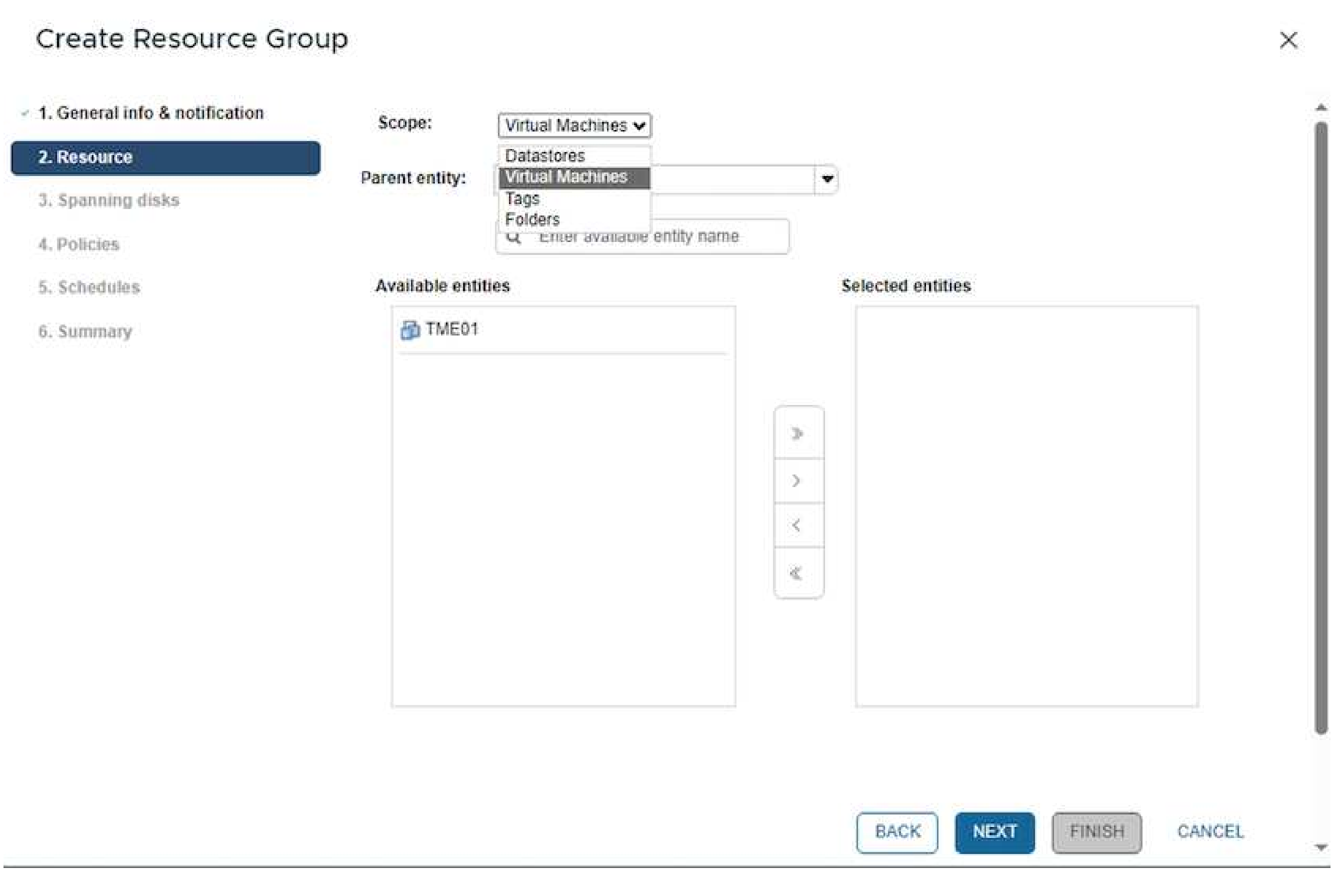
2. Create a policy with required attributes.



New Backup Policy

Name	Daily
Description	description
Frequency	Daily
Locking Period	□ Enable Snapshot Locking
Retention	Days to keep 1
Replication	☑ Update SnapMirror after backup ☑ Update SnapVault after backup Snapshot label
Advanced	□ VM consistency □ Include datastores with independent disks Scripts: Enter script path

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



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

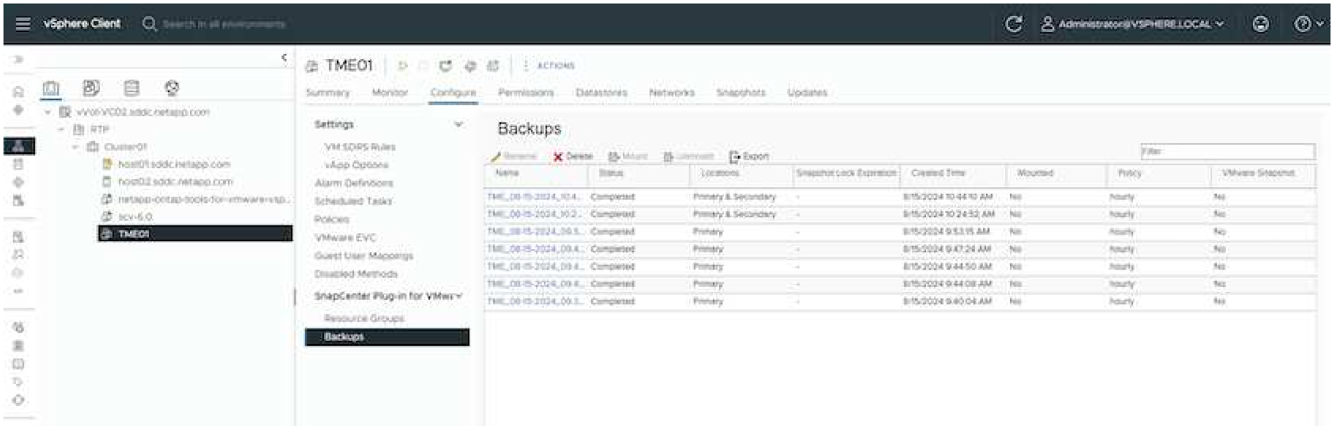
Available entities

TME01

Selected entities

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.



Backups

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

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

Refer SnapCenter plug-in documentation for additional use cases.

VM migration from traditional datastores to vVol datastore

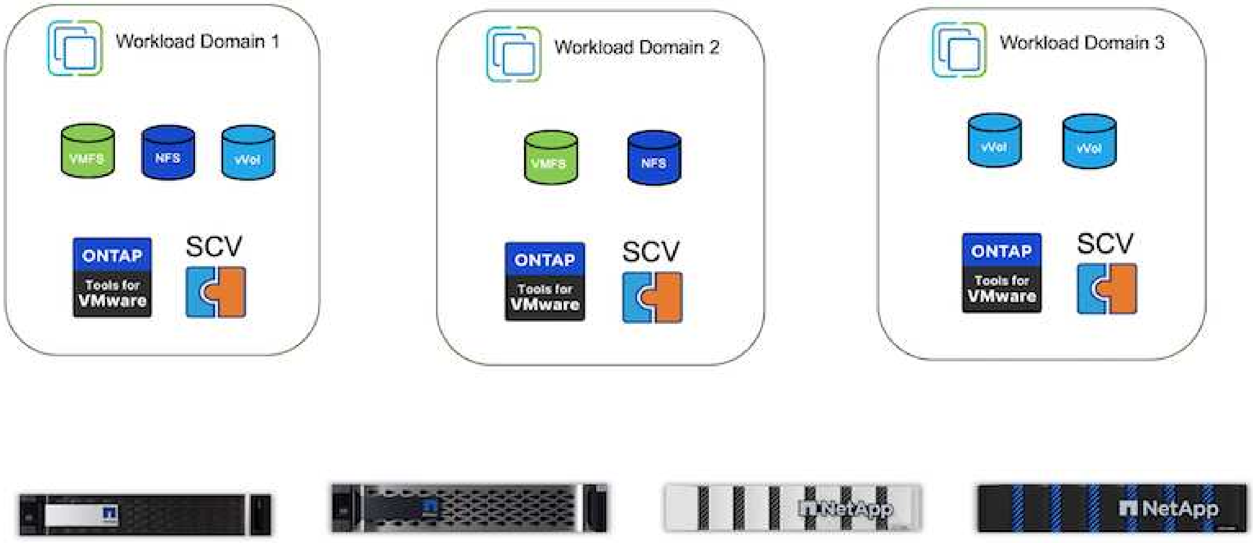
To migrate VMs from other datastores to a vVol datastore, various options are available based on the scenario. It can vary from a simple storage vMotion operation to migration using HCX. Refer migrate vms to ONTAP datastore for more details.

VM migration between vVol datastores

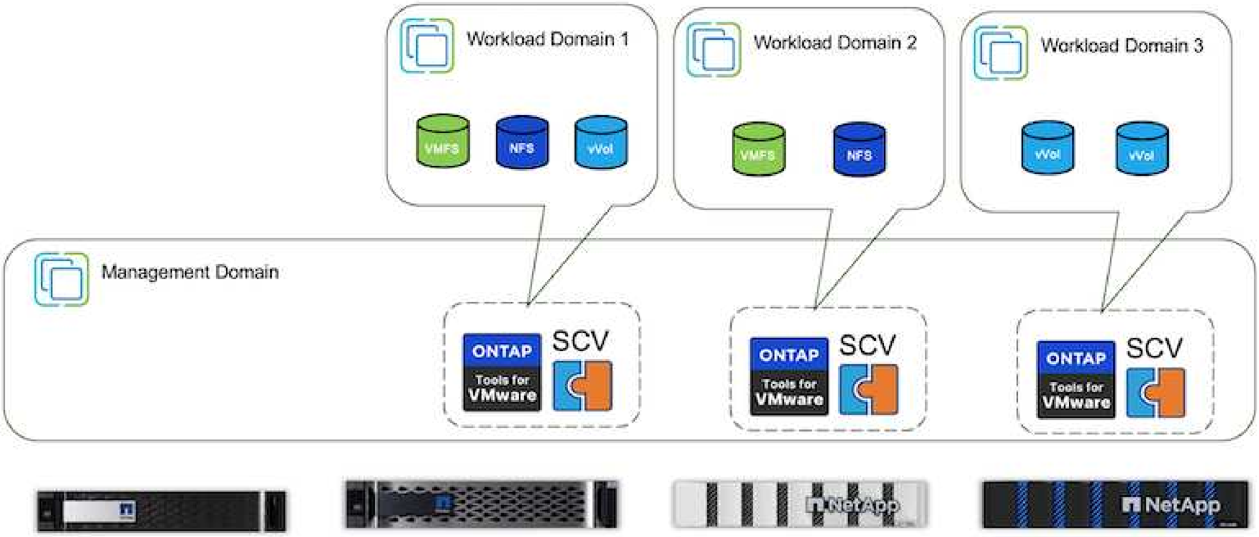
For bulk migration of VMs between vVol datastores, please check migrate vms to ONTAP datastore.

Sample Reference architecture

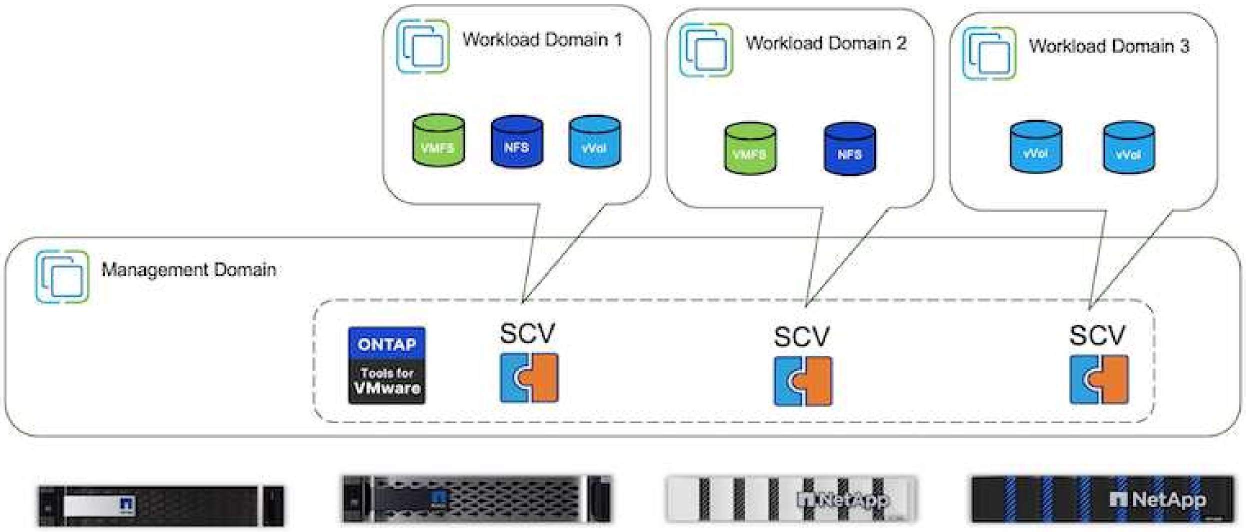
ONTAP tools for VMware vSphere and SCV can be installed on same vCenter it is managing or on different vCenter server. It is better to avoid to host on vVol datastore it is managing.



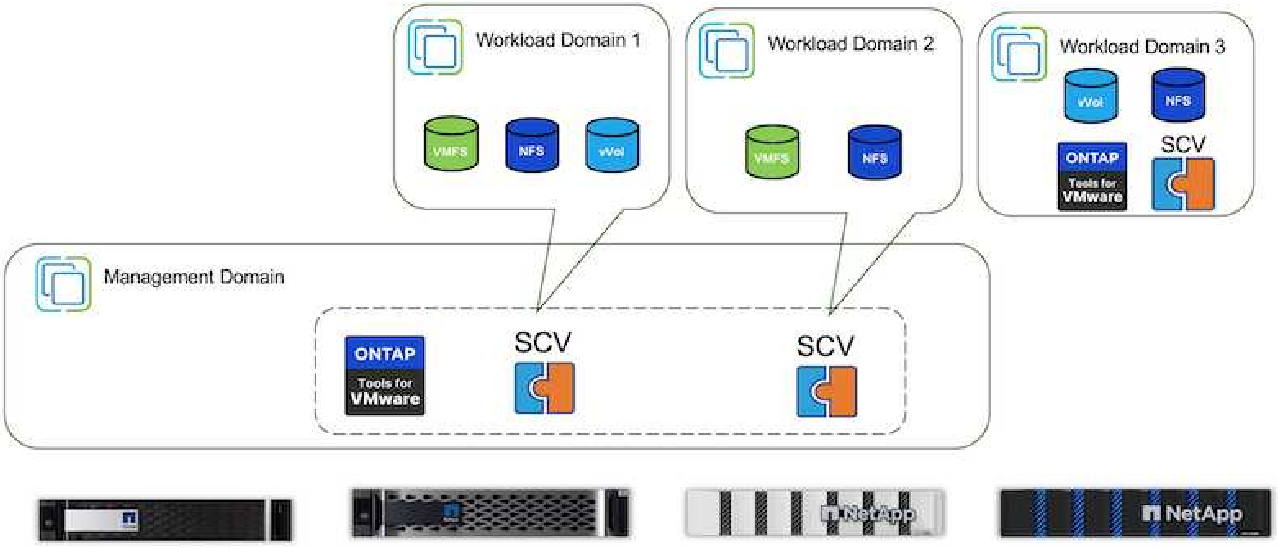
As many customers host their vCenter servers on different one rather than it is managing, similar approach is adviced for ONTAP tools & SCV too.



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



Mix of dedicated and shared model is also supported.



How to get started

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

Collect data with the Virtual Machine Data Collector

Learn about assessing your VMware infrastructure using the Virtual Machine Data Collector

The Virtual Machine Data Collector (VMDC) is a free, lightweight tool with a GUI designed for VMware environments. It gathers inventory and performance data on VMs, hosts, storage, and networks, offering insights for resource optimization and capacity planning.

Introduction

Virtual Machine Data Collector (VMDC) is a free, lightweight, simple GUI based toolkit for VMware environments that allows users to collect detailed inventory information about their virtual machines (VMs), hosts, storage, and networks.

For more information on Virtual Machine Data Collector, see Virtual Machine Data Collector Documentation.

VMDC Capabilities

VMDC is just a stepping stone to collect quick and instant statistics for projecting optimization possibilities for VMWare core licensing along with vCPU and RAM. NetApp Data Infrastructure Insights which requires installation of AUs and data collectors should be the obvious next step for understanding detailed VM topology, grouping of VMs using annotation so as to right size the workloads and future proof the infrastructure.

Sampling of the metrics gathered with VMDC:

- VM information
  - VM name
  - VM power state
  - VM CPU information
  - VM memory information
  - VM location
  - VM network information
  - and more
- VM performance
  - Performance data for VMs at selected interval
  - VM read / write information
  - VM IOPS information
  - VM latency
  - and more
- ESXi host information
  - Host datacenter information
  - Host cluster information
  - Host model information
  - Host CPU information
  - Host memory information
  - and more

Virtual Machine Data Collector (VMDC)

The Virtual Machine Data Collector (VMDC) is a free, lightweight, simple GUI based toolkit for VMware environments that allows users to collect detailed inventory information about their virtual machines (VMs), hosts, storage, and networks.

This is a preview release of VMDC.

Overview

The main function of VMDC is reporting on the configuration of vCenter, ESXi servers, and the virtual machines (VMs) that reside on a vSphere environment, including cluster configuration, networking, storage and performance data. Once comprehensive environmental data has been collected, it can be utilized to produce insightful information on the infrastructure. The reporting output display is a spreadsheet-style GUI with multiple tabs to its various sections. It provides easy-to-read reports and helps in optimizing resource usage, and planning for capacity.

VMDC is just a stepping stone to collect quick and instant statistics for projecting optimization possibilities for VMWare core licensing along with vCPU and RAM. NetApp Data Infrastructure Insights which requires installation of AUs and data collectors should be the obvious next step for understanding detailed VM topology, grouping of VMs using annotation so as to right size the workloads and future proof the infrastructure.

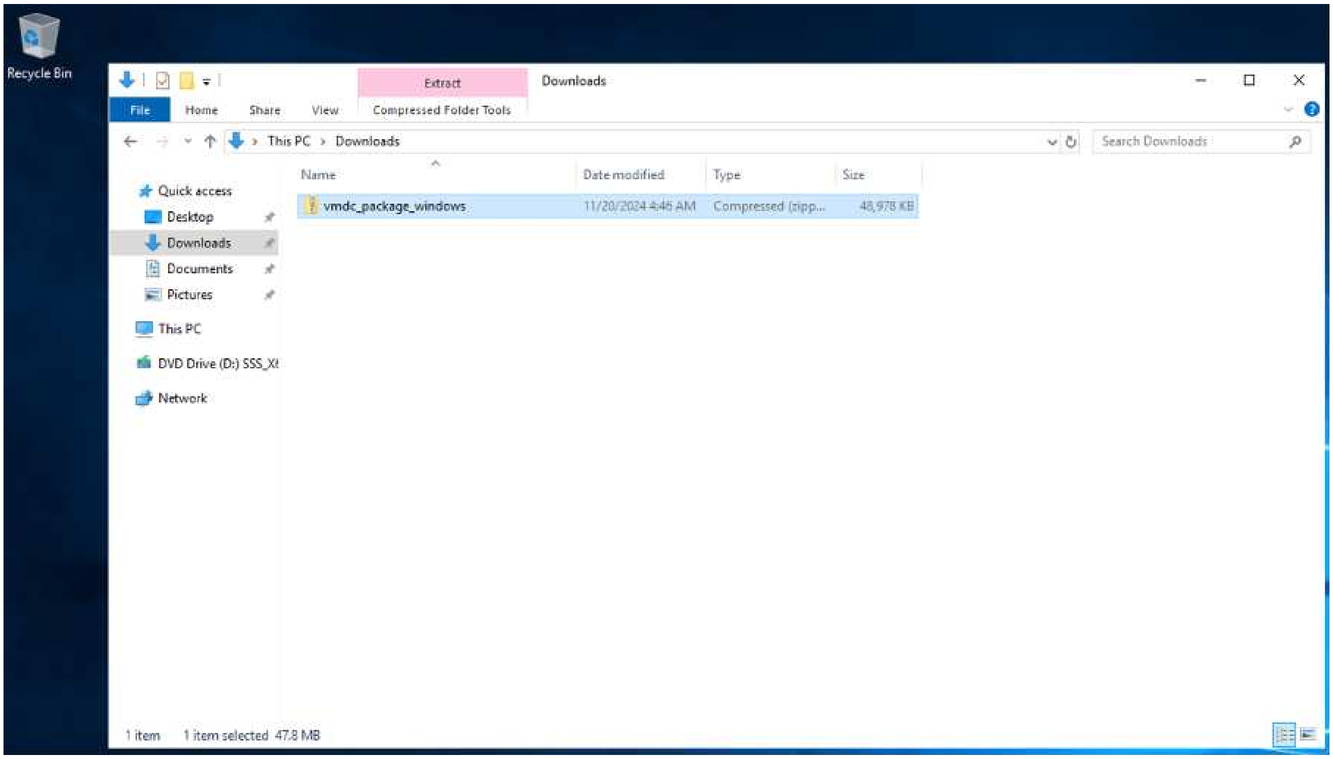
VMDC can be downloaded here and is available for Windows Systems only.

Installing and Setting Up VMDC

VMDC can be run on Windows 2019, 2022 version. The pre-requisite is to have network connectivity from VMDC instance to the designated vCenter servers. Once verified, download the VMDC package from NetApp Toolchest and then unzip the package and run the batch file to install and start the service.

Once VMDC has been installed, access the UI using the IP address mentioned during the installation. This will bring up the VMDC log-in interface, where the vCenter’s can be added by entering the IP address or DNS name and credentials of a vCenter Server.

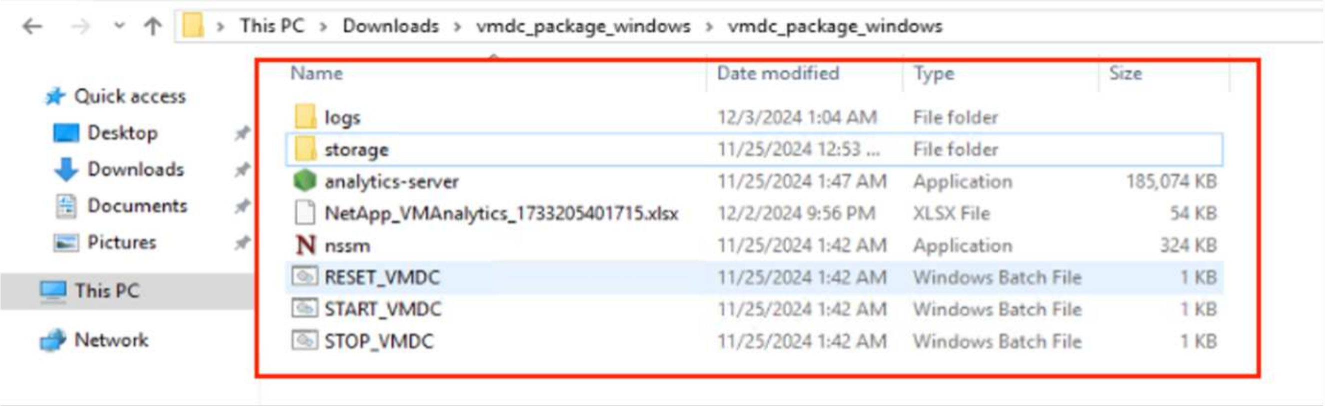
1. Download VMDC package.



Name	Date modified	Type	Size
vmdc_package_windows	11/20/2024 4:46 AM	Compressed (zipp...	48,978 KB

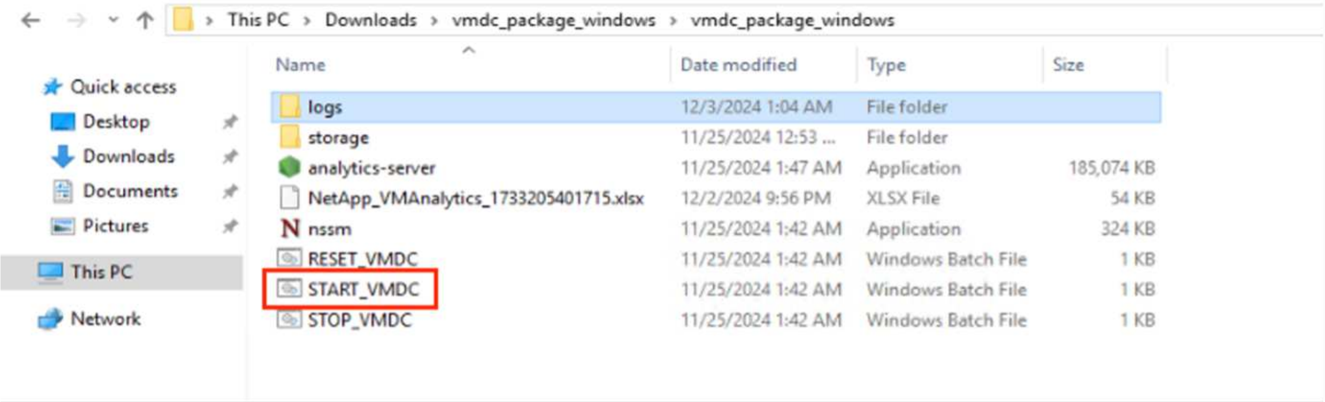
1 item   1 item selected 47.8 MB

2. Extract the package to the designated folder.


This PC › Downloads › vmdc_package_windows › vmdc_package_windows
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network

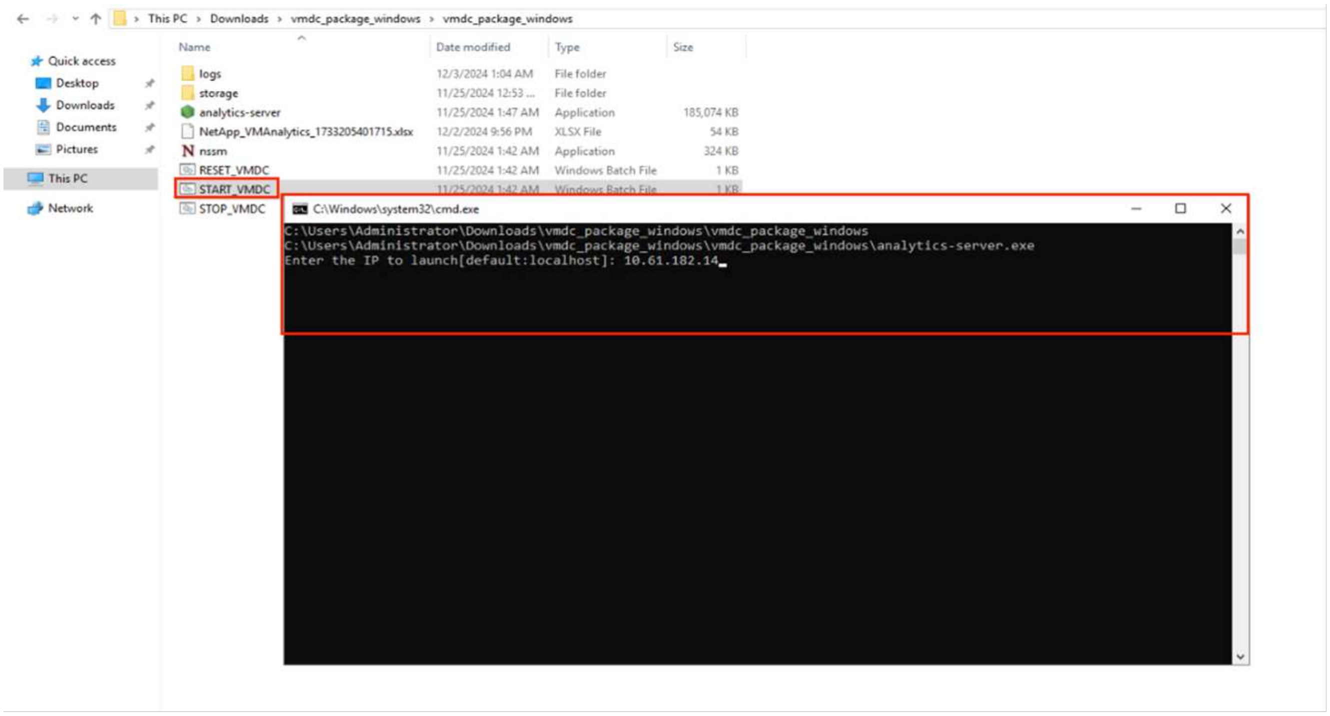
Name	Date modified	Type	Size
logs	12/3/2024 1:04 AM	File folder	
storage	11/25/2024 12:53 ...	File folder	
analytics-server	11/25/2024 1:47 AM	Application	185,074 KB
NetApp_VMAnalytics_1733205401715.xlsx	12/2/2024 9:56 PM	XLSX File	54 KB
nssm	11/25/2024 1:42 AM	Application	324 KB
RESET_VMDC	11/25/2024 1:42 AM	Windows Batch File	1 KB
START_VMDC	11/25/2024 1:42 AM	Windows Batch File	1 KB
STOP_VMDC	11/25/2024 1:42 AM	Windows Batch File	1 KB

3. Run the VMDC package by clicking on Start_VMDC batch file. This will open the command prompt and will prompt to enter the IP address.


This PC › Downloads › vmdc_package_windows › vmdc_package_windows
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network

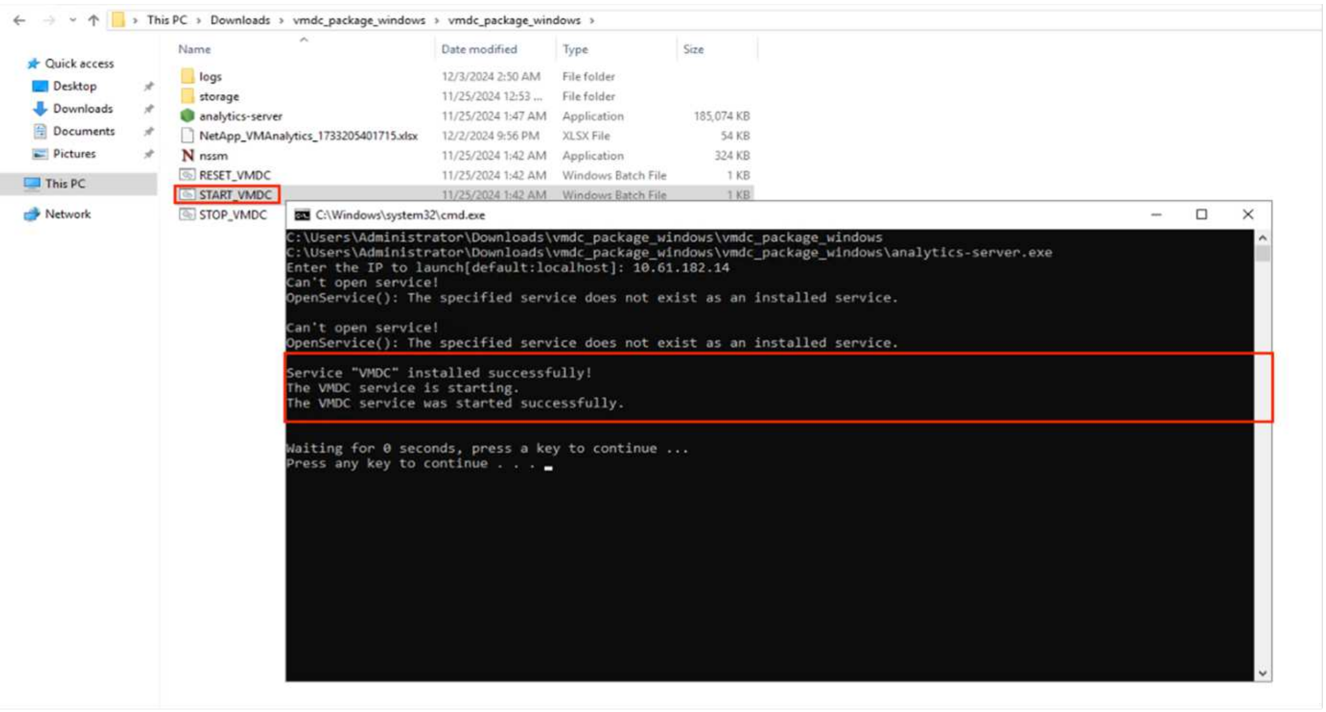
Name	Date modified	Type	Size
logs	12/3/2024 1:04 AM	File folder	
storage	11/25/2024 12:53 ...	File folder	
analytics-server	11/25/2024 1:47 AM	Application	185,074 KB
NetApp_VMAnalytics_1733205401715.xlsx	12/2/2024 9:56 PM	XLSX File	54 KB
nssm	11/25/2024 1:42 AM	Application	324 KB
RESET_VMDC	11/25/2024 1:42 AM	Windows Batch File	1 KB
START_VMDC	11/25/2024 1:42 AM	Windows Batch File	1 KB
STOP_VMDC	11/25/2024 1:42 AM	Windows Batch File	1 KB

4. The installer will begin the installation process and start the VMDC service.


This PC › Downloads › vmdc_package_windows › vmdc_package_windows
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
C:\Windows\system32\cmd.exe

Name	Date modified	Type	Size
logs	12/3/2024 1:04 AM	File folder	
storage	11/25/2024 12:53 ...	File folder	
analytics-server	11/25/2024 1:47 AM	Application	185,074 KB
NetApp_VMAnalytics_1733205401715.xlsx	12/2/2024 9:56 PM	XLSX File	54 KB
nssm	11/25/2024 1:42 AM	Application	324 KB
RESET_VMDC	11/25/2024 1:42 AM	Windows Batch File	1 KB
START_VMDC	11/25/2024 1:42 AM	Windows Batch File	1 KB
STOP_VMDC			

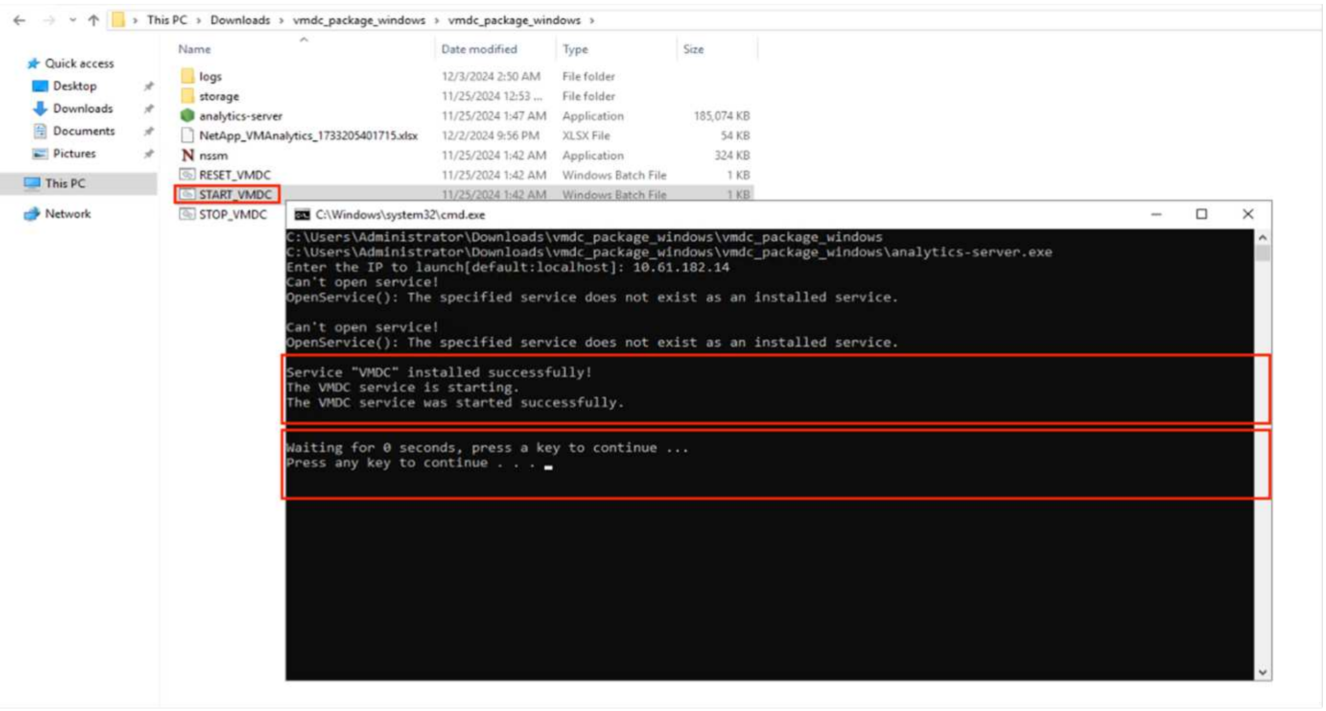
```
C:\Users\Administrator\Downloads\vmdc_package_windows\vmdc_package_windows
C:\Users\Administrator\Downloads\vmdc_package_windows\vmdc_package_windows\analytics-server.exe
Enter the IP to launch[default:localhost]: 10.61.182.14_
```


This PC › Downloads › vmdc_package_windows › vmdc_package_windows
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
C:\Windows\system32\cmd.exe

Name	Date modified	Type	Size
logs	12/3/2024 2:50 AM	File folder	
storage	11/25/2024 12:53 ...	File folder	
analytics-server	11/25/2024 1:47 AM	Application	185,074 KB
NetApp_VMAnalytics_1733205401715.xlsx	12/2/2024 9:56 PM	XLSX File	54 KB
nssm	11/25/2024 1:42 AM	Application	324 KB
RESET_VMDC	11/25/2024 1:42 AM	Windows Batch File	1 KB
START_VMDC	11/25/2024 1:42 AM	Windows Batch File	1 KB
STOP_VMDC			

```
C:\Users\Administrator\Downloads\vmdc_package_windows\vmdc_package_windows
C:\Users\Administrator\Downloads\vmdc_package_windows\vmdc_package_windows\analytics-server.exe
Enter the IP to launch[default:localhost]: 10.61.182.14
Can't open service!
OpenService(): The specified service does not exist as an installed service.

Can't open service!
OpenService(): The specified service does not exist as an installed service.

Service "VMDC" installed successfully!
The VMDC service is starting.
The VMDC service was started successfully.

Waiting for 0 seconds, press a key to continue ...
Press any key to continue . . .
```

5. Once done, "Press any key to continue" to close the command prompt.

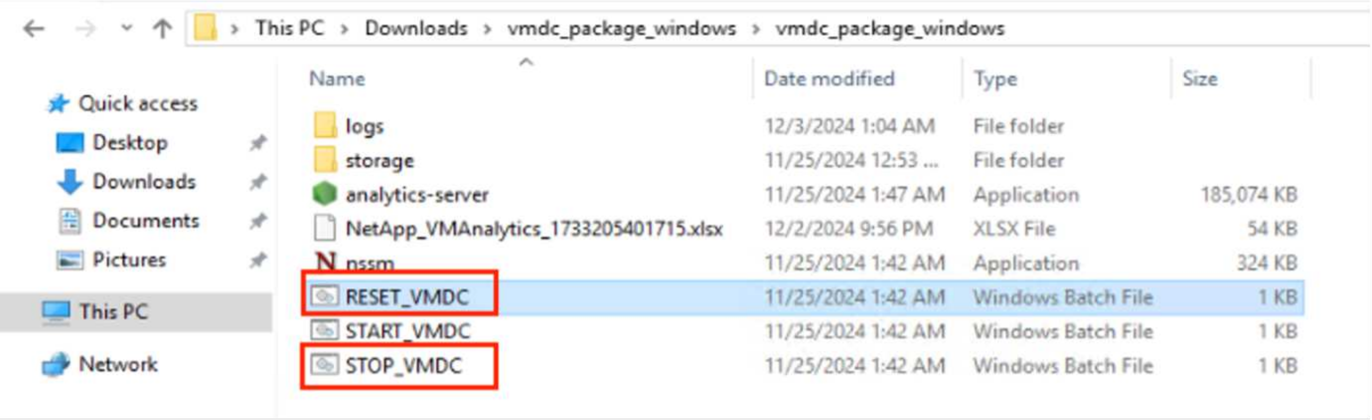

This PC › Downloads › vmdc_package_windows › vmdc_package_windows
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
C:\Windows\system32\cmd.exe

Name	Date modified	Type	Size
logs	12/3/2024 2:50 AM	File folder	
storage	11/25/2024 12:53 ...	File folder	
analytics-server	11/25/2024 1:47 AM	Application	185,074 KB
NetApp_VMAnalytics_1733205401715.xlsx	12/2/2024 9:56 PM	XLSX File	54 KB
nssm	11/25/2024 1:42 AM	Application	324 KB
RESET_VMDC	11/25/2024 1:42 AM	Windows Batch File	1 KB
START_VMDC	11/25/2024 1:42 AM	Windows Batch File	1 KB
STOP_VMDC			

```
C:\Users\Administrator\Downloads\vmdc_package_windows\vmdc_package_windows
C:\Users\Administrator\Downloads\vmdc_package_windows\vmdc_package_windows\analytics-server.exe
Enter the IP to launch[default:localhost]: 10.61.182.14
Can't open service!
OpenService(): The specified service does not exist as an installed service.

Can't open service!
OpenService(): The specified service does not exist as an installed service.

Service "VMDC" installed successfully!
The VMDC service is starting.
The VMDC service was started successfully.

Waiting for 0 seconds, press a key to continue ...
Press any key to continue . . .
```

ⓘ To stop data collection, click on Stop_VMDC batch file.

ⓘ To remove the collected data and reset VMDC, run reset_VMDC batch file. Keep in mind, running reset bat file will delete all the existing data and start from the scratch.

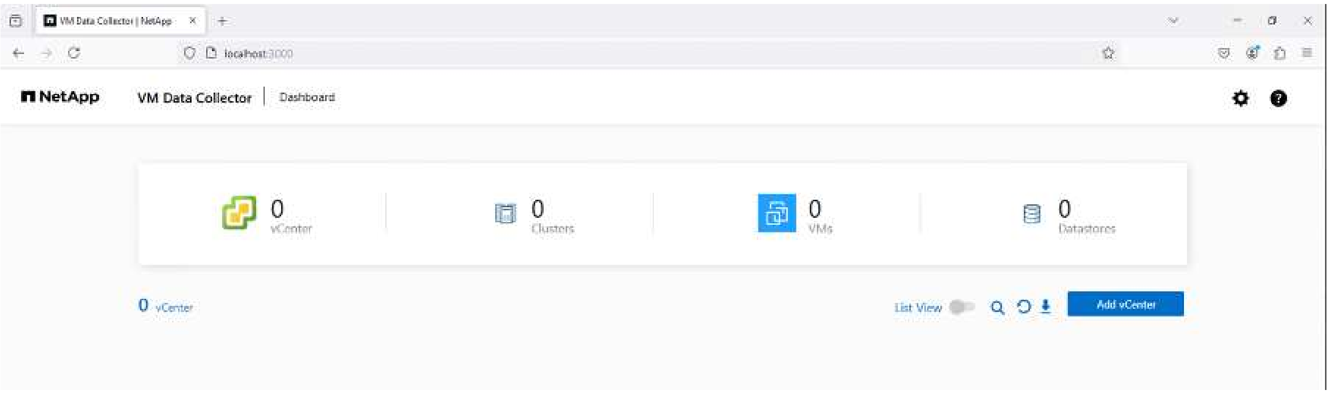

This PC › Downloads › vmdc_package_windows › vmdc_package_windows
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network

Name	Date modified	Type	Size
logs	12/3/2024 1:04 AM	File folder	
storage	11/25/2024 12:53 ...	File folder	
analytics-server	11/25/2024 1:47 AM	Application	185,074 KB
NetApp_VMAnalytics_1733205401715.xlsx	12/2/2024 9:56 PM	XLSX File	54 KB
nssm	11/25/2024 1:42 AM	Application	324 KB
RESET_VMDC	11/25/2024 1:42 AM	Windows Batch File	1 KB
START_VMDC	11/25/2024 1:42 AM	Windows Batch File	1 KB
STOP_VMDC	11/25/2024 1:42 AM	Windows Batch File	1 KB

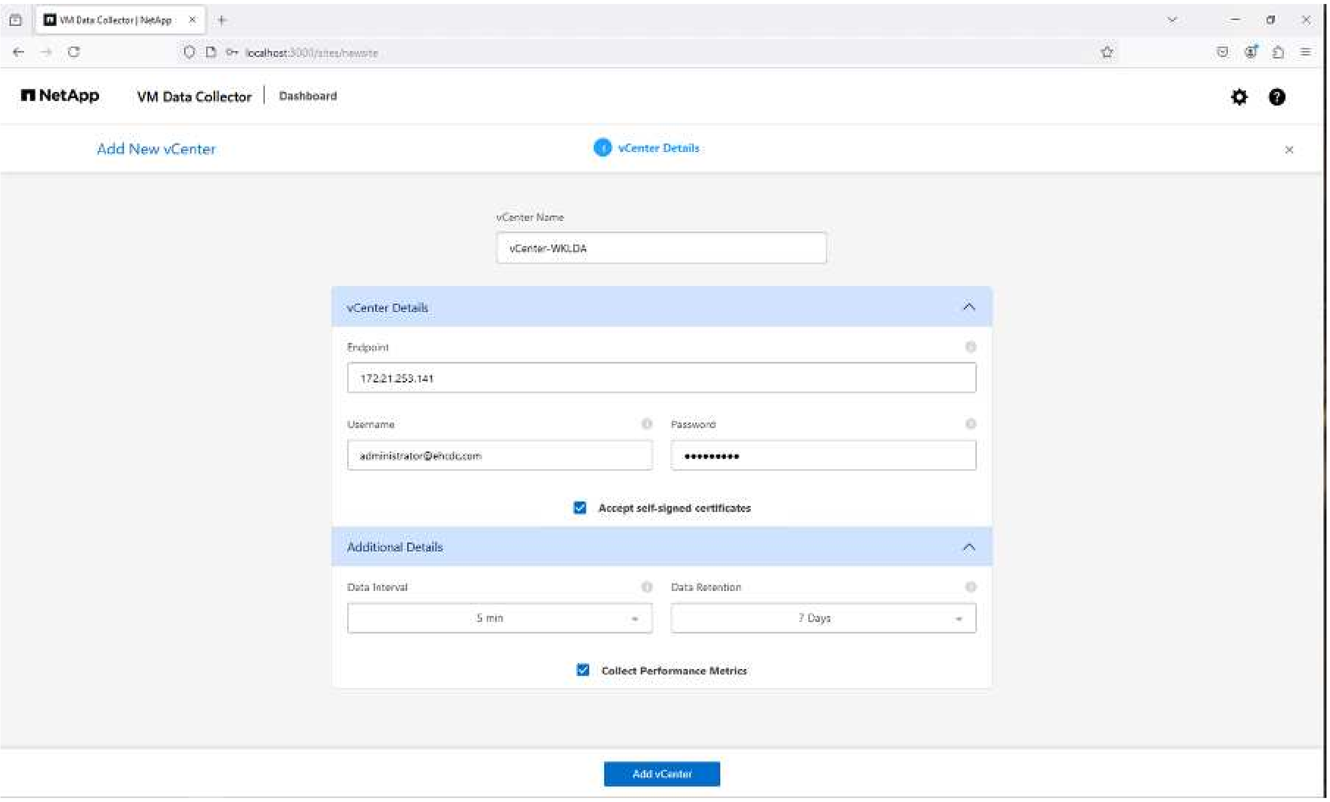
Using the GUI

Run VMDC

- Using the browser, access VMDC UI



- Add the designated vCenter using "Add vCenter" option
  - vCenter Name - Provide a name for the vCenter
  - Endpoint - Enter the IP address or FQDN of the vCenter server
  - Username - username to access the vCenter (in UPN format: username@domain.com)
  - Password
- Modify the "Additional Details" as per the requirements
  - Data Interval time – Specifies the sample aggregation time range. Default is 5 mins, however, can be modified to 30sec or 1 min as needed.
  - Data Retention – Specifies the retention period to store the historical metrics.
  - Collect Performance Metrics – When enabled, collects the performance metrics for each VM. If not selected, VMDC provides functionality like RVtools by just providing the VM, host and datastore details.
- Once done, Click on "Add vCenter"



vCenter Name: vCenter-WKLDA

vCenter Details

Endpoint: 172.21.253.141

Username: administrator@ehcdc.com

Password: ••••••••••

☑ Accept self-signed certificates

Additional Details

Data Interval: 5 min

Data Retention: 7 Days

☑ Collect Performance Metrics

> The data collection starts immediately once the vCenter is added. There is no need to schedule a time for collection as the process would fetch the data available in the vCenter database and start aggregating them based on the "data interval time" specified.

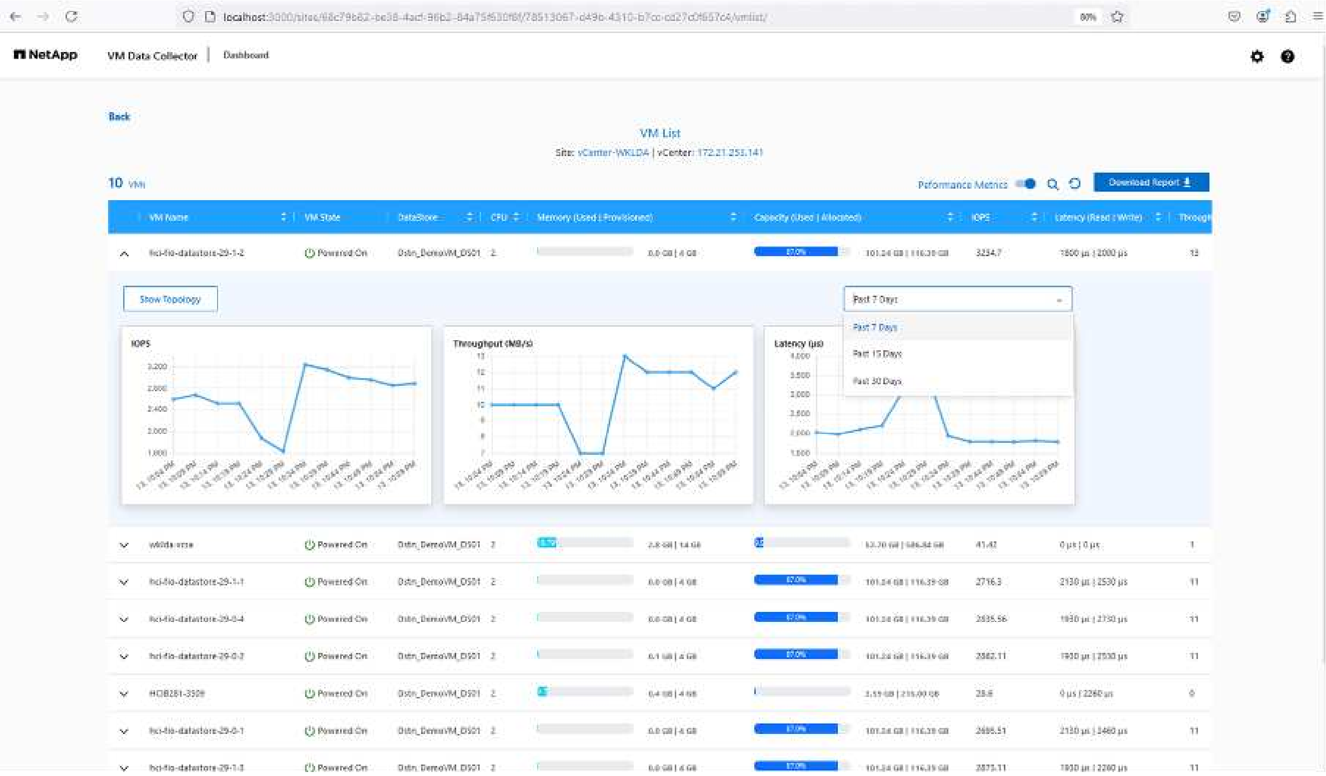
To view the data for a specific vCenter, go to the dashboard, click on "View Inventory" against the appropriate vCenter name. The page will display the VM inventory along with the VM attributes. By default, "Performance Metrics" is disabled in the UI, however it can be turned ON by using the toggle option. Once performance metrics is enabled, the perf data against each VM will be displayed. For live performance information, click on the refresh button.

View VM topology

VMDC provides "Show Topology" option for each VM which provides an interactive interface to view resources and their relationships wrt VM disk, VM, ESXi host, Datastores and networks. It helps to manage and monitor with insights from the gathered performance data. Topology helps to perform basic diagnosis and troubleshoot issues using the current data. For detailed troubleshooting and quick MTTR, use NetApp Data Infrastructure Insights which provides detailed topology view with end to end dependency mapping.

To access the topology view, follow the below steps:

- Access the VMDC dashboard.
- Select the vCenter name and click on "View Inventory".



NetApp VM Data Collector | Dashboard

Back

VM List

Site: vCenter-WKLDA | vCenter: 172.21.253.141

10 VMs

Performance Metrics

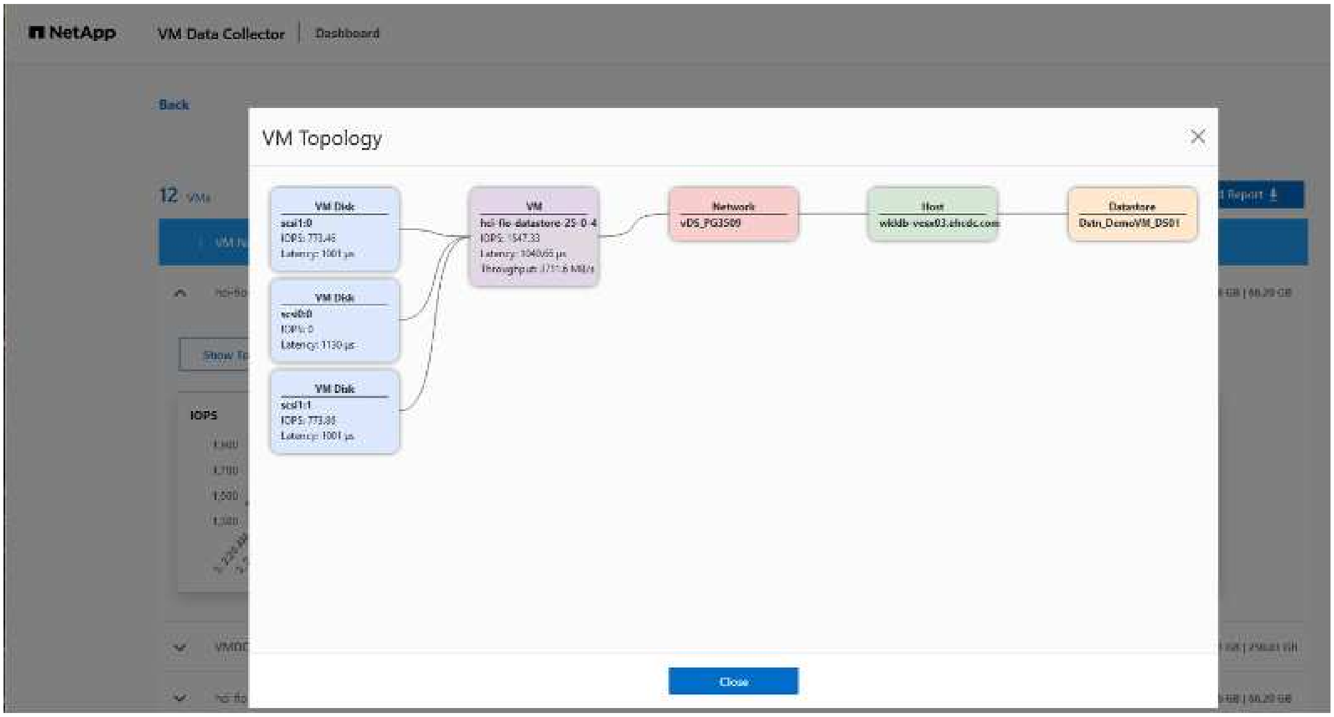
Download Report

VM Name	VM State	DataStore	CPU	Memory (Used | Provisioned)	Capacity (Used | Allocated)	IOPS	Latency (Read | Write)	Throughput
hci-fio-datastore-29-1-2	Powered On	Dstn_DemoVM_DS01	2	0.0 GB | 4 GB	87.0% 101.24 GB | 116.39 GB	3234.7	1800 µs | 2000 µs	13
wkldx-vrse	Powered On	Dstn_DemoVM_DS01	2	2.8 GB | 14 GB	53.70 GB | 586.84 GB	41.42	0 µs | 0 µs	1
hci-fio-datastore-29-1-1	Powered On	Dstn_DemoVM_DS01	2	0.0 GB | 4 GB	87.0% 101.24 GB | 116.39 GB	2716.3	2130 µs | 2530 µs	11
hci-fio-datastore-29-0-4	Powered On	Dstn_DemoVM_DS01	2	0.0 GB | 4 GB	87.0% 101.24 GB | 116.39 GB	2635.56	1930 µs | 2730 µs	11
hci-fio-datastore-29-0-2	Powered On	Dstn_DemoVM_DS01	2	0.1 GB | 4 GB	87.0% 101.24 GB | 116.39 GB	2682.11	1900 µs | 2530 µs	11
HCIB281-3509	Powered On	Dstn_DemoVM_DS01	2	0.4 GB | 4 GB	3.59 GB | 215.00 GB	28.6	0 µs | 2260 µs	0
hci-fio-datastore-29-0-1	Powered On	Dstn_DemoVM_DS01	2	0.0 GB | 4 GB	87.0% 101.24 GB | 116.39 GB	2695.51	2120 µs | 2460 µs	11
hci-fio-datastore-29-1-3	Powered On	Dstn_DemoVM_DS01	2	0.0 GB | 4 GB	87.0% 101.24 GB | 116.39 GB	2873.11	1900 µs | 2260 µs	11

Show Topology

Past 7 Days

- Select the VM and click on "Show Topology".



VM Topology

VM Disk
scsi1:0
IOPS: 773.46
Latency: 1001 µs

VM Disk
scsi0:0
IOPS: 0
Latency: 1130 µs

VM Disk
scsi1:1
IOPS: 773.86
Latency: 1001 µs

VM
hci-fio-datastore-25-0-4
IOPS: 1547.33
Latency: 1040.65 µs
Throughput: 1711.6 MB/s

Network
vDS_PG3509

Host
wkldb-vesx03.ehcdc.com

Datastore
Dstn_DemoVM_DS01

Close

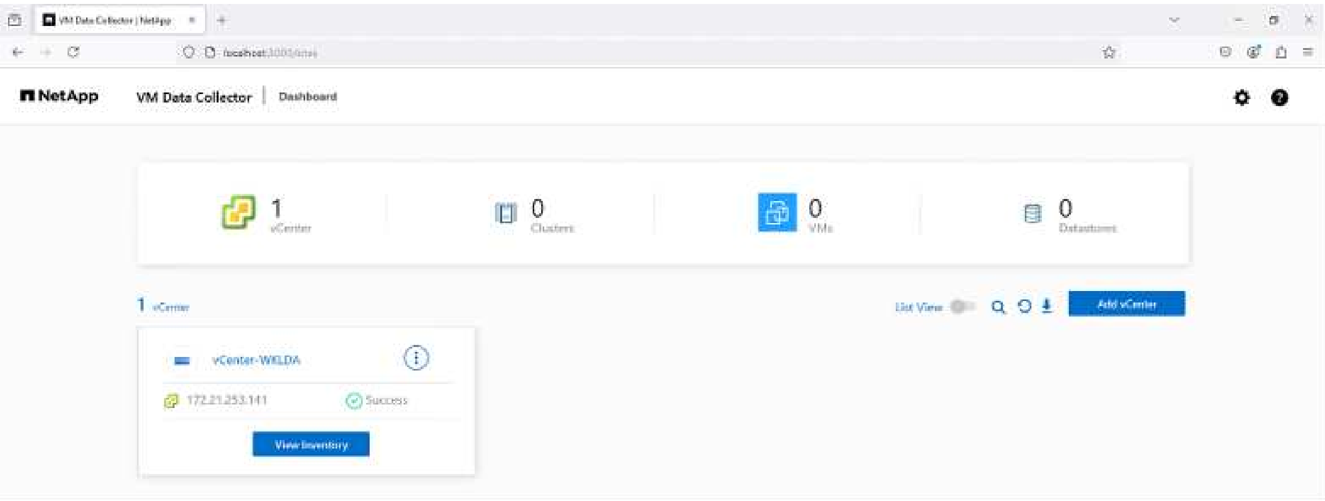
Export to Excel

To capture the collected in a usable format, use "Download Report" option to download the XLSX file.

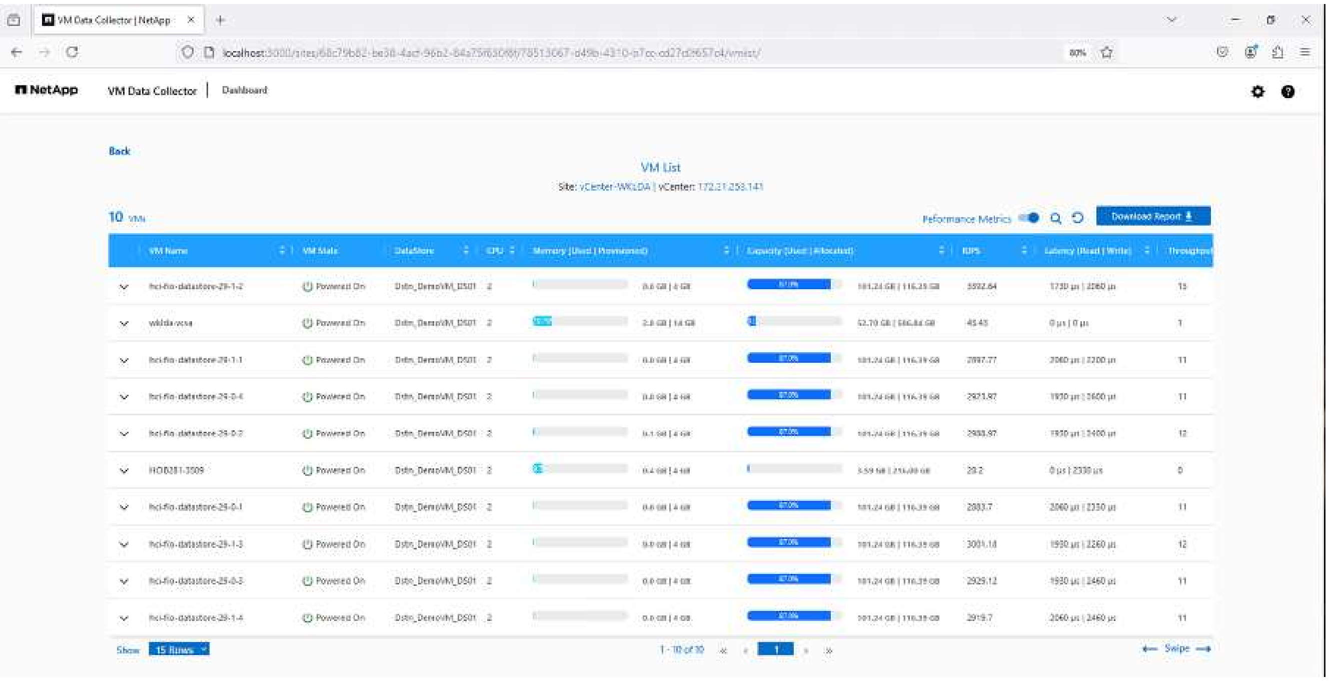
To download the report, follow the below steps:

- Access the VMDC dashboard.

- Select the vCenter name and click on "View Inventory".



- Select "Download Report" option


VM Data Collector | NetApp
localhost:3000/sites/68c79b82-be38-4acf-96b2-84a75f630f6f/78513067-d49b-4310-a7cc-cd27cdf657c4/vmlist/
80%
NetApp
VM Data Collector
Dashboard
Back
Performance Metrics
Download Report
Show
15 Rows
1 - 10 of 10
1
Swipe

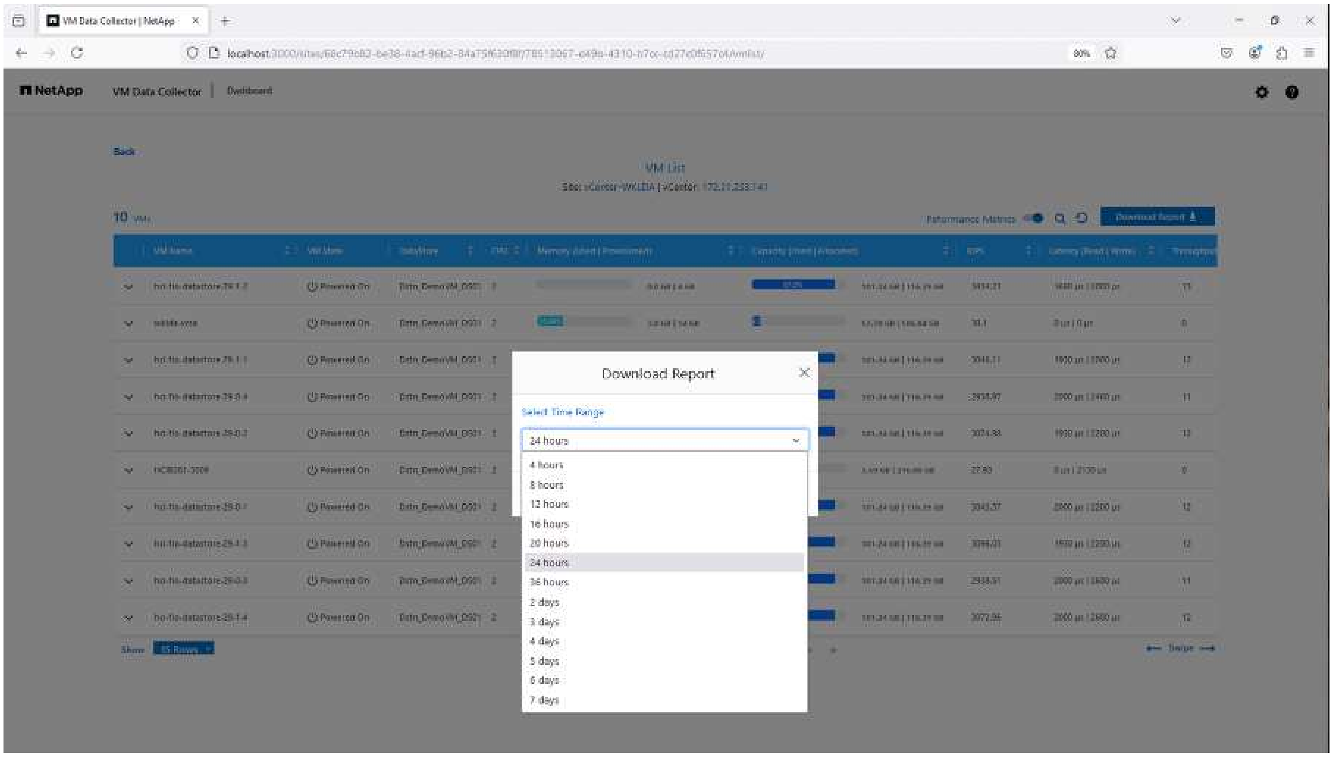
VM List

Site: vCenter-WKLDA | vCenter: 172.21.253.141

10 VMs

VM Name	VM State	DataStore	CPU	Memory (Used | Provisioned)	Capacity (Used | Allocated)		IOPS	Latency (Read | Write)	Throughput
hci-fio-datastore-29-1-2	Powered On	Dstn_DemoVM_DS01	2	0.6 GB | 4 GB	87.0%	101.24 GB | 116.35 GB	3332.64	1730 µs | 2060 µs	13
wklda-vcsa	Powered On	Dstn_DemoVM_DS01	2	2.8 GB | 14 GB		52.70 GB | 566.84 GB	45.45	0 µs | 0 µs	1
hci-fio-datastore-29-1-1	Powered On	Dstn_DemoVM_DS01	2	0.0 GB | 4 GB	87.0%	101.24 GB | 116.39 GB	2897.77	2060 µs | 2200 µs	11
hci-fio-datastore-29-0-4	Powered On	Dstn_DemoVM_DS01	2	0.0 GB | 4 GB	87.0%	101.24 GB | 116.39 GB	2971.97	1930 µs | 2600 µs	11
hci-fio-datastore-29-0-2	Powered On	Dstn_DemoVM_DS01	2	0.1 GB | 4 GB	87.0%	101.24 GB | 116.39 GB	2988.97	1930 µs | 2400 µs	12
HOB281-3509	Powered On	Dstn_DemoVM_DS01	2	0.4 GB | 4 GB		3.59 GB | 214.00 GB	20.2	0 µs | 2330 µs	0
hci-fio-datastore-29-0-1	Powered On	Dstn_DemoVM_DS01	2	0.6 GB | 4 GB	87.0%	101.24 GB | 116.39 GB	2983.7	2060 µs | 2330 µs	11
hci-fio-datastore-29-1-3	Powered On	Dstn_DemoVM_DS01	2	0.0 GB | 4 GB	87.0%	101.24 GB | 116.39 GB	3001.18	1930 µs | 2260 µs	12
hci-fio-datastore-29-0-3	Powered On	Dstn_DemoVM_DS01	2	0.0 GB | 4 GB	87.0%	101.24 GB | 116.39 GB	2929.12	1930 µs | 2460 µs	11
hci-fio-datastore-29-1-4	Powered On	Dstn_DemoVM_DS01	2	0.0 GB | 4 GB	87.0%	101.24 GB | 116.39 GB	2919.7	2060 µs | 2460 µs	11

- Select the time range. The time range provides multiple options starting from 4 hours to 7 days.



Select Time Range: 24 hours

For example, if the data required is for last 4 hours, choose 4 or choose the appropriate value to capture the data for that given period. The data generated is aggregated on a continuous basis. So, select the time range to ensure the report generated captures the necessary workload statistics.

VMDC Data Counters

Once downloaded, the first sheet that VMDC displays is "VM Info", a sheet that contains information regarding the VMs that reside in the vSphere environment. This shows generic information about the virtual machines: VM Name, Power State, CPUs, Memory Provisioned (MB), Memory Utilized (MB), Capacity Provisioned (GB), Capacity Utilized (GB), VMware tools version, OS Version, Environment Type, Datacenter, Cluster, Host, Folder, Primary Datastore, Disks, NICs, VM ID and VM UUID.

The 'VM Performance' tab captures the performance data for each VM sampled at selected interval level (default is 5 mins). The sample of each virtual machine covers: Average Read IOPS, Average Write IOPS, Total Average IOPS, Peak Read IOPS, Peak Write IOPS, Total Peak IOPS, Average Read Throughput (KB/s), Average Write Throughput (KB/s), Total Average Throughput (KB/s), Peak Read Throughput (KB/s), Peak Write Throughput (KB/s), Total Peak Throughput (KB/s), Average Read Latency (ms), Average Write Latency (ms), Total Average Latency (ms), Peak Read Latency (ms), Peak Write Latency (ms) and Total Peak Latency (ms).

The "ESXi Host Info" tab captures for each host: Datacenter, vCenter, Cluster, OS, Manufacturer, Model, CPU Sockets, CPU Cores, Net Clock Speed (GHz), CPU Clock Speed (GHz), CPU Threads, Memory (GB), Memory Used (%), CPU usage (%), Guest VM Count and Number of NICs.

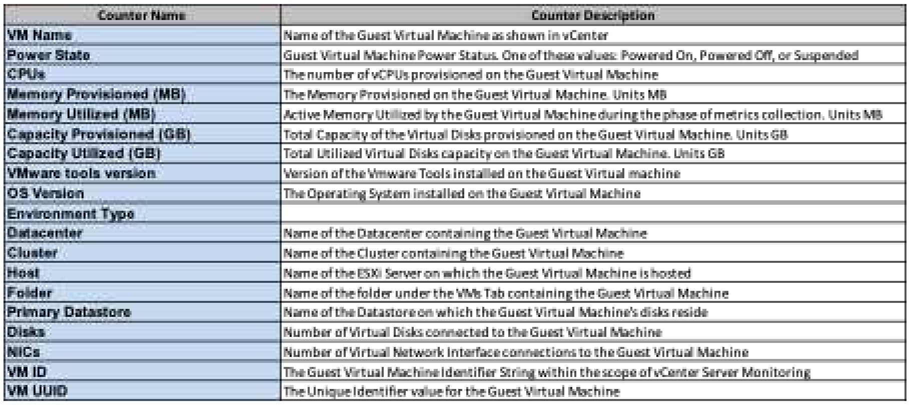
Next Steps

Use the downloaded XLSX file for optimization and refactoring exercises.

VMDC Attributes Description

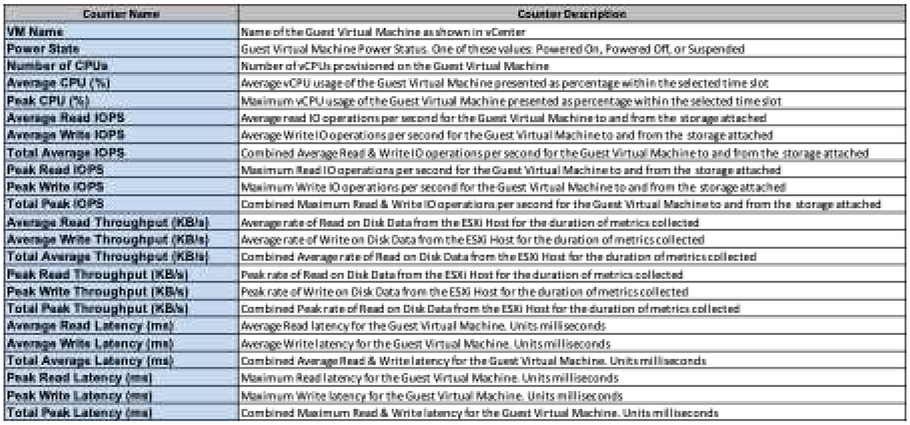
This section of the document covers the definition of each counter used in the excel sheet.

VM Info sheet



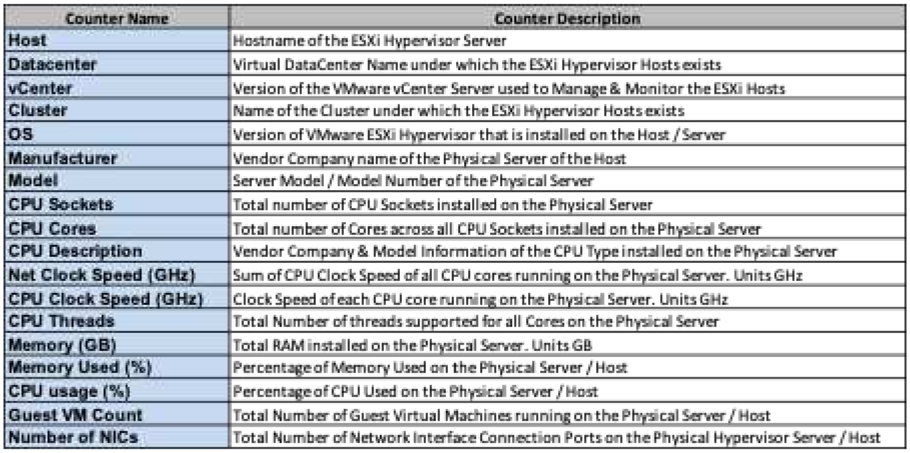
Counter Name	Counter Description
VM Name	Name of the Guest Virtual Machine as shown in vCenter
Power State	Guest Virtual Machine Power Status. One of these values: Powered On, Powered Off, or Suspended
CPUs	The number of vCPUs provisioned on the Guest Virtual Machine
Memory Provisioned (MB)	The Memory Provisioned on the Guest Virtual Machine. Units MB
Memory Utilized (MB)	Active Memory Utilized by the Guest Virtual Machine during the phase of metrics collection. Units MB
Capacity Provisioned (GB)	Total Capacity of the Virtual Disks provisioned on the Guest Virtual Machine. Units GB
Capacity Utilized (GB)	Total Utilized Virtual Disks capacity on the Guest Virtual Machine. Units GB
VMware tools version	Version of the Vmware Tools installed on the Guest Virtual machine
OS Version	The Operating System installed on the Guest Virtual Machine
Environment Type	
Datacenter	Name of the Datacenter containing the Guest Virtual Machine
Cluster	Name of the Cluster containing the Guest Virtual Machine
Host	Name of the ESXi Server on which the Guest Virtual Machine is hosted
Folder	Name of the folder under the VMs Tab containing the Guest Virtual Machine
Primary Datastore	Name of the Datastore on which the Guest Virtual Machine's disks reside
Disks	Number of Virtual Disks connected to the Guest Virtual Machine
NICs	Number of Virtual Network Interface connections to the Guest Virtual Machine
VM ID	The Guest Virtual Machine Identifier String within the scope of vCenter Server Monitoring
VM UUID	The Unique Identifier value for the Guest Virtual Machine

VM Performance sheet



Counter Name	Counter Description
VM Name	Name of the Guest Virtual Machine as shown in vCenter
Power State	Guest Virtual Machine Power Status. One of these values: Powered On, Powered Off, or Suspended
Number of CPUs	Number of vCPUs provisioned on the Guest Virtual Machine
Average CPU (%)	Average vCPU usage of the Guest Virtual Machine presented as percentage within the selected time slot
Peak CPU (%)	Maximum vCPU usage of the Guest Virtual Machine presented as percentage within the selected time slot
Average Read IOPS	Average read IO operations per second for the Guest Virtual Machine to and from the storage attached
Average Write IOPS	Average Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Total Average IOPS	Combined Average Read & Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Peak Read IOPS	Maximum Read IO operations per second for the Guest Virtual Machine to and from the storage attached
Peak Write IOPS	Maximum Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Total Peak IOPS	Combined Maximum Read & Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Average Read Throughput (KB/s)	Average rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Average Write Throughput (KB/s)	Average rate of Write on Disk Data from the ESXi Host for the duration of metrics collected
Total Average Throughput (KB/s)	Combined Average rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Peak Read Throughput (KB/s)	Peak rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Peak Write Throughput (KB/s)	Peak rate of Write on Disk Data from the ESXi Host for the duration of metrics collected
Total Peak Throughput (KB/s)	Combined Peak rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Average Read Latency (ms)	Average Read latency for the Guest Virtual Machine. Units milliseconds
Average Write Latency (ms)	Average Write latency for the Guest Virtual Machine. Units milliseconds
Total Average Latency (ms)	Combined Average Read & Write latency for the Guest Virtual Machine. Units milliseconds
Peak Read Latency (ms)	Maximum Read latency for the Guest Virtual Machine. Units milliseconds
Peak Write Latency (ms)	Maximum Write latency for the Guest Virtual Machine. Units milliseconds
Total Peak Latency (ms)	Combined Maximum Read & Write latency for the Guest Virtual Machine. Units milliseconds

ESXi Host Info



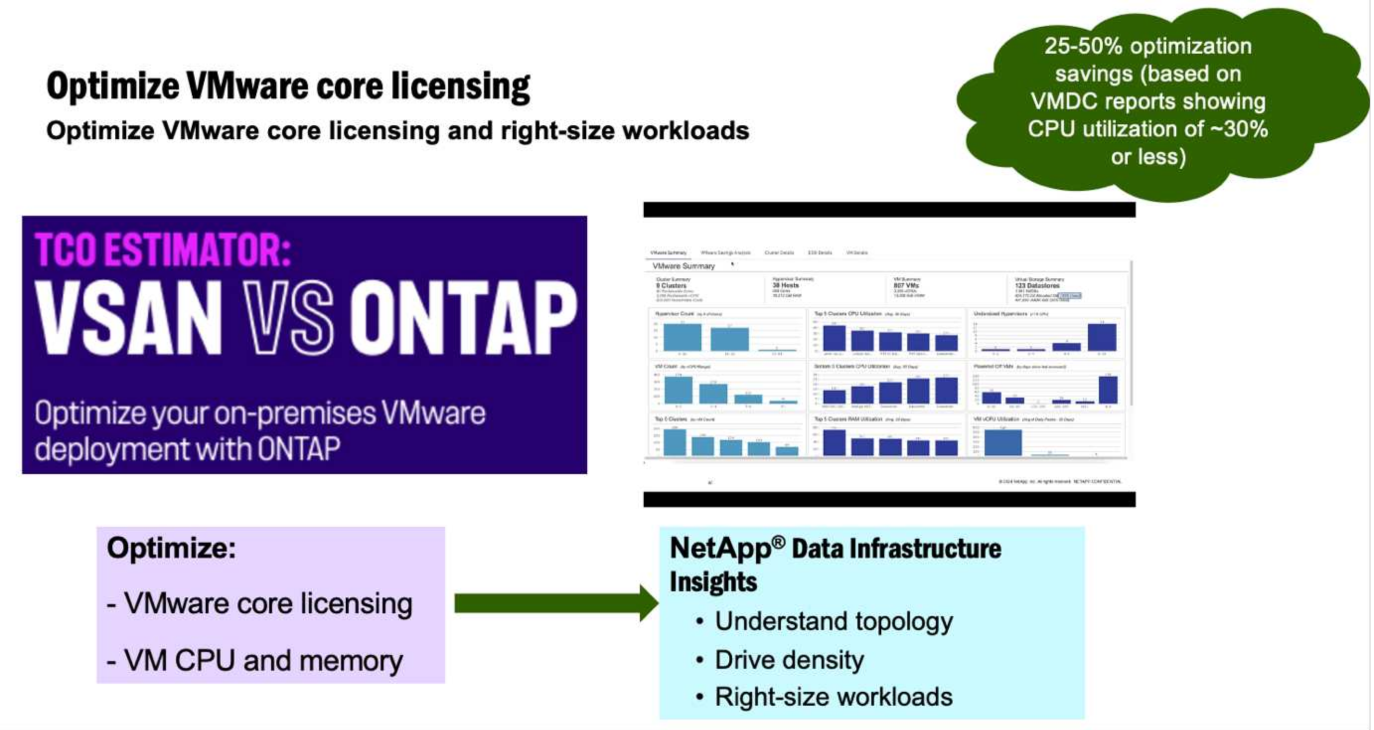
Counter Name	Counter Description
Host	Hostname of the ESXi Hypervisor Server
Datacenter	Virtual DataCenter Name under which the ESXi Hypervisor Hosts exists
vCenter	Version of the VMware vCenter Server used to Manage & Monitor the ESXi Hosts
Cluster	Name of the Cluster under which the ESXi Hypervisor Hosts exists
OS	Version of VMware ESXi Hypervisor that is installed on the Host / Server
Manufacturer	Vendor Company name of the Physical Server of the Host
Model	Server Model / Model Number of the Physical Server
CPU Sockets	Total number of CPU Sockets installed on the Physical Server
CPU Cores	Total number of Cores across all CPU Sockets installed on the Physical Server
CPU Description	Vendor Company & Model Information of the CPU Type installed on the Physical Server
Net Clock Speed (GHz)	Sum of CPU Clock Speed of all CPU cores running on the Physical Server. Units GHz
CPU Clock Speed (GHz)	Clock Speed of each CPU core running on the Physical Server. Units GHz
CPU Threads	Total Number of threads supported for all Cores on the Physical Server
Memory (GB)	Total RAM installed on the Physical Server. Units GB
Memory Used (%)	Percentage of Memory Used on the Physical Server / Host
CPU usage (%)	Percentage of CPU Used on the Physical Server / Host
Guest VM Count	Total Number of Guest Virtual Machines running on the Physical Server / Host
Number of NICs	Total Number of Network Interface Connection Ports on the Physical Hypervisor Server / Host

Conclusion

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. VMDC provides the ability to swiftly collect VM data that can be sliced to report and optimize the existing environment.

Using VMDC, conduct quick assessment to pinpoint underutilized resources and then use NetApp Data Infrastructure Insights (DII) to provide detailed analysis and recommendations for VM reclamation. This enables customers to understand the potential cost savings and optimization while NetApp Data Infrastructure Insights (DII) is deployed and configured. NetApp Data Infrastructure Insights (DII) 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, VMDC and DII as a detailed analysis mechanism 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 these two tools to make rational, strategic decisions that balance cost optimization with operational efficiency and productivity.

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



Optimize VMware core licensing

Optimize VMware core licensing and right-size workloads

25-50% optimization savings (based on VMDC reports showing CPU utilization of ~30% or less)

TCO ESTIMATOR:
VSAN VS ONTAP
Optimize your on-premises VMware deployment with ONTAP

Optimize:
- VMware core licensing
- VM CPU and memory

NetApp® Data Infrastructure Insights
- Understand topology
- Drive density
- Right-size workloads

Next Steps

Download VMDC package and gather the data and use vSAN TCO Estimator for easy projection and then use DII to continuously provides the intelligence, impacting IT now and in the future to ensure it can adapt as new needs arise.

Copyright information

Trademark information