VMware Cloud Foundation on NetApp

NetApp virtualization solutions

NetApp
January 15, 2026

Table of Contents

VMware Cloud Foundation on NetApp

Simplify hybrid cloud experience with VMware Cloud Foundation and ONTAP

NetApp ONTAP integrates with VMware Cloud Foundation (VCF) to deliver a unified storage solution supporting both block and file protocols. This integration simplifies hybrid cloud deployments, improves data management and performance, and ensures consistent data services across on-premises and cloud environments.

Introduction

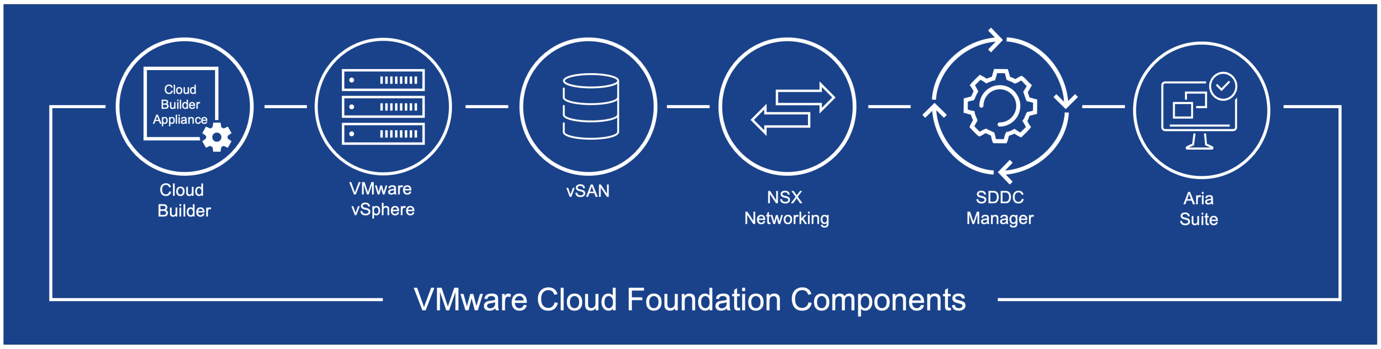
Using NetApp with VCF enhances data management and storage efficiency through NetApp's advanced features like deduplication, compression, and snapshots. This combination provides seamless integration, high performance, and scalability for virtualized environments. Additionally, it simplifies hybrid cloud deployments by enabling consistent data services and management across on-premises and cloud infrastructures.

Introduction to NetApp ONTAP

NetApp ONTAP is a comprehensive data management software that delivers advanced storage features across a wide product line. ONTAP is available as software defined storage, as a first party service through the major cloud providers and as the storage OS for NetApp ASA (All San Array), AFF (All-flash FAS) and FAS (Fabric-Attached Storage) platforms. ONTAP delivers high-performance and low-latency for a variety of use cases including VMware virtualization, without creating silos.

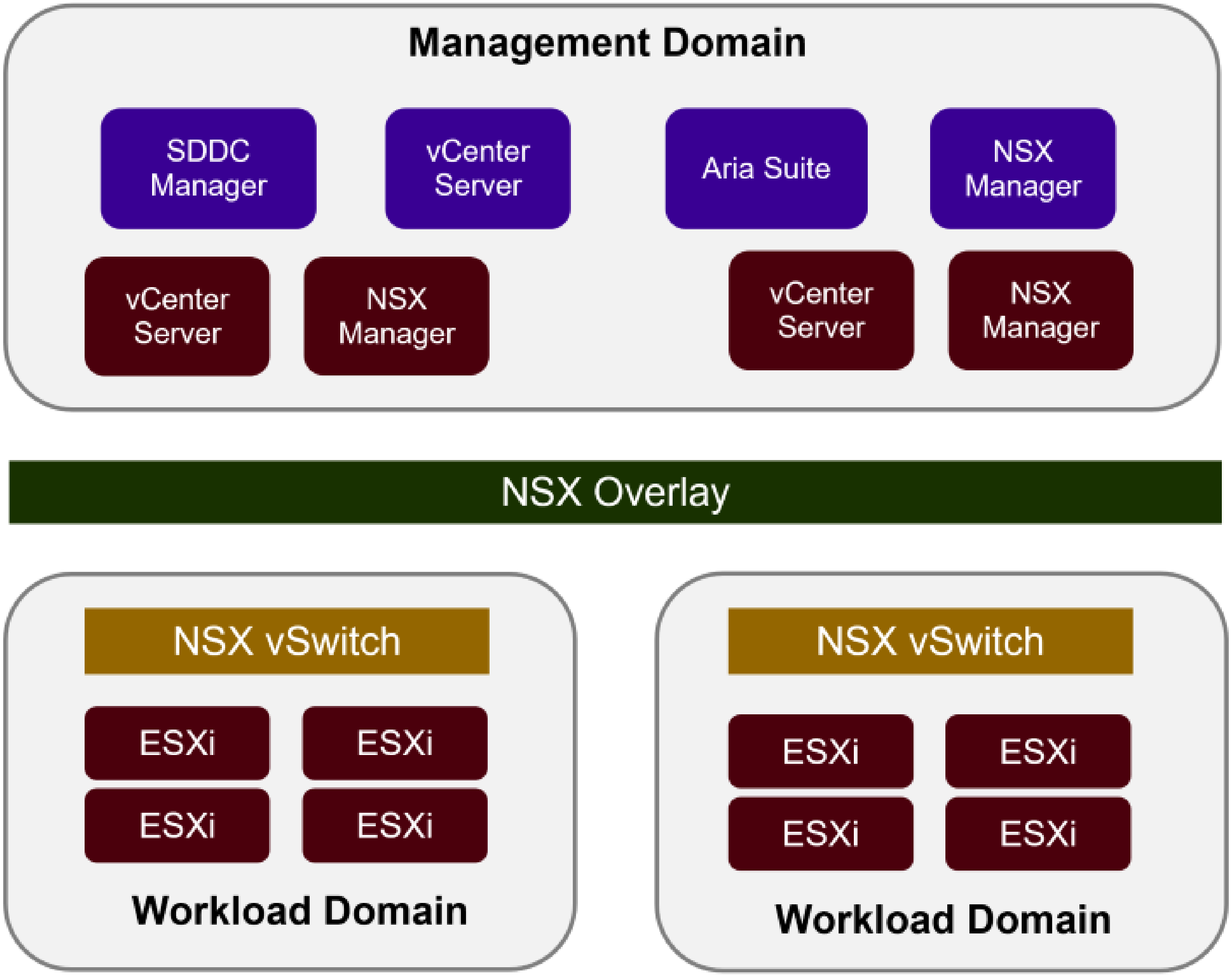
Introduction to VMware Cloud Foundation

VCF integrates compute, network and storage offerings with VMware products and 3rd party integrations, facilitating both native Kubernetes and virtual machine-based workloads. This software platform includes key components such as VMware vSphere, NSX, Aria Suite Enterprise, Vmware vSphere Kubernetes Service, HCX Enterprise, SDDC Manager and storage-capacity linked to host CPU cores via vSAN. NetApp ONTAP integrates seamlessly with a variety of VCF deployment models both on-premises and in the public cloud.



VCF Domains

Domains are a foundational construct within VCF that enable the organization of resources into distinct, independent groupings. Domains help organize the infrastructure more effectively, ensuring resources are utilized efficiently. Each domain is deployed with its own compute, network and storage elements.



There are two primary types of domains with VCF:

- **Management Domain** – The management domain includes components responsible for the core functions of the VCF environment. The components handle essential tasks such as resource provisioning, monitoring, maintenance and include 3rd party plug-in integrations such as NetApp ONTAP Tools for VMware. Management domains can be deployed using the Cloud Builder Appliance to ensure best practices are followed, or an existing vCenter environment can be converted into a VCF management domain.
- **Virtual Infrastructure Workload Domain** – Virtual Infrastructure Workload domains are designed to be pools of resources dedicated to a specific operational need, workload or organization. Workload domains are deployed easily via the SDDC Manager, helping to automate a series of complex tasks. Up to 24 workload domains can be provisioned within a VCF environment, with each representing a unit of application-ready infrastructure.

Storage with VCF

Central to the functionality of domains is the storage that they consume. While VCF includes CPU-core based vSAN capacity for hyper-converged use cases, it also supports a wide range of external storage solutions. This flexibility is crucial for enterprises that have significant investments in existing storage arrays or need to support protocols beyond what vSAN affords. VMware supports multiple storage types with VCF.

There are two primary types of storage with VCF:

- **Principal storage** – This storage type is allocated during the initial creation of the domain. For management domains, this storage houses the VCF administrative and operations components. For workload domains, this storage is designed to support the workloads, VMs or containers for which the domain was deployed.
- **Supplemental storage** – Supplemental storage can be added to any workload domain after deployment. This storage type helps organizations leverage existing investments in storage infrastructure and integrate various storage technologies to optimize performance, scalability, and cost-efficiency.

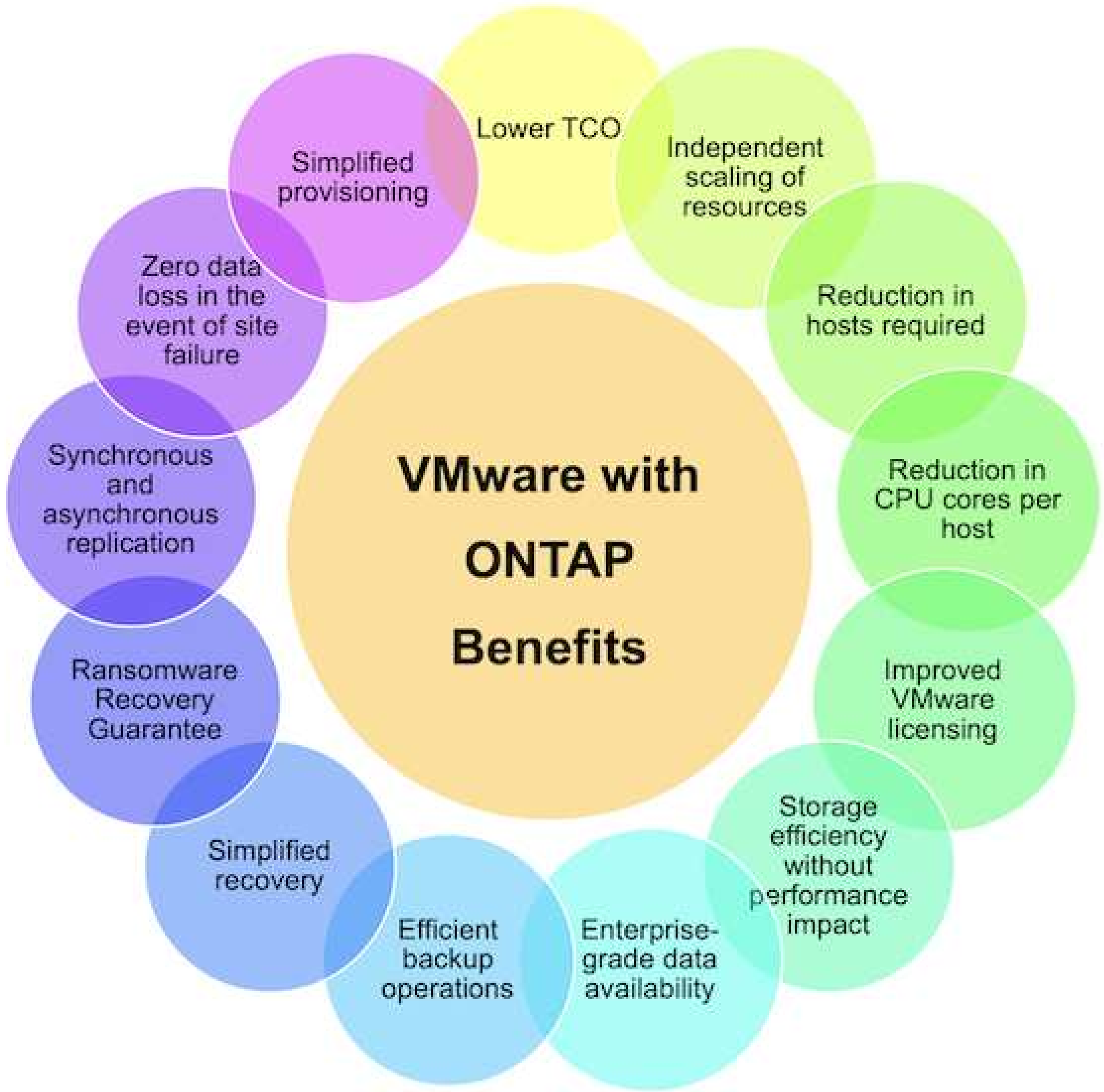
Support VCF Storage types

Domain Type	Principal Storage	Supplemental Storage
Management Domain	vSAN FC* NFS*	vVols (FC, iSCSI, or NFS) FC NFS iSCSI NVMe/TCP NVMe/FC NVMe/RDMA
Virtual Infrastructure Workload Domain	vSAN vVols (FC, iSCSI, or NFS) FC NFS	vVols (FC, iSCSI, or NFS) FC NFS iSCSI NVMe/TCP NVMe/FC NVMe/RDMA

Note: * Specific protocol support provided when using VCF Import Tool with existing vSphere environments.

Why ONTAP for VCF

In addition to use cases involving investment protection and multi-protocol support, there are many additional reasons to take advantage of external shared storage within a VCF workload domain. It may be assumed that storage provisioned for a workload domain is merely a repository to host VMs and container. However, organization needs often outgrow the capabilities of the licensed-capacity and require enterprise storage. Storage provided by ONTAP, allocated to domains within VCF, is easy to deploy and offers a future-proof shared storage solution.


VMware with ONTAP Benefits
Lower TCO
Independent scaling of resources
Reduction in hosts required
Reduction in CPU cores per host
Improved VMware licensing
Storage efficiency without performance impact
Enterprise-grade data availability
Efficient backup operations
Simplified recovery
Ransomware Recovery Guarantee
Synchronous and asynchronous replication
Zero data loss in the event of site failure
Simplified provisioning

For more information regarding the top ONTAP Benefits for VMware VCF identified below see Why ONTAP for VMware.

- Flexibility on day 1 and as you scale
- Offload storage tasks to ONTAP
- Best in class storage efficiency
- Enterprise-grade data availability
- Efficient backup and recovery operations
- Wholistic business continuity capabilities

Additional information:

- NetApp Storage Options
- vSphere Metro Storage Cluster (vMSC) support
- ONTAP Tools for VMware vSphere
- VMware Automation with ONTAP

- NetApp SnapCenter
- Hybrid Multicloud with VMware and NetApp
- Security and ransomware protection
- Easy migration of VMware workloads to NetApp
- NetApp Disaster Recovery
- Data Insfrastructure Insights
- VM Data Collector

Summary

ONTAP provides a platform that addresses all workload requirements, offering customized block storage solutions and unified offerings to enable faster results for VMs and applications in a reliable and secure manner. ONTAP incorporates advanced data reduction and movement techniques to minimize the data center footprint, while ensuring enterprise-level availability to keep critical workloads online. Additionally, the AWS, Azure and Google support NetApp-powered external storage to enhance vSAN storage in VMware cloud-based clusters as part of their VMware-in-the-Cloud offerings. Overall, NetApp's superior capabilities make it a more effective choice for VMware Cloud Foundation deployments.

Documentation resources

For detailed information on NetApp offerings for VMware Cloud Foundation, refer to the following the following:

VMware Cloud Foundation Documentation

- VMware Cloud Foundation Documentation

Four (4) part blog series on VCF with NetApp

- NetApp and VMware Cloud Foundation made easy Part 1: Getting started
- NetApp and VMware Cloud Foundation made easy Part 2: VCF and ONTAP principal storage
- NetApp and VMware Cloud Foundation made easy Part 3: VCF and Element principal storage
- NetApp and VMware Cloud Foundation made easy - Part 4: ONTAP Tools for VMware and supplemental storage

VMware Cloud Foundation with NetApp All-Flash SAN Arrays

- VCF with NetApp ASA arrays, Introduction and Technology Overview
- Use ONTAP with FC as principal storage for management domains
- Use ONTAP with FC as principal storage for VI workload domains domains
- Use Ontap Tools to deploy iSCSI datastores in a VCF management domain
- Use Ontap Tools to deploy FC datastores in a VCF management domain
- Use Ontap Tools to deploy vVols (iSCSI) datastores in a VI workload domain
- Configure NVMe over TCP datastores for use in a VI workload domain
- Deploy and use the SnapCenter Plug-in for VMware vSphere to protect and restore VMs in a VI workload domain
- Deploy and use the SnapCenter Plug-in for VMware vSphere to protect and restore VMs in a VI workload

domain (NVMe/TCP datastores)

VMware Cloud Foundation with NetApp All-Flash AFF Arrays

- VCF with NetApp AFF arrays, Introduction and Technology Overview
- Use ONTAP with NFS as principal storage for management domains
- Use ONTAP with NFS as principal storage for VI workload domains
- Use ONTAP Tools to deploy vVols (NFS) datastores in a VI workload domain

NetApp FlexPod solutions for VMware Cloud Foundation

- Expanding FlexPod hybrid cloud with VMware Cloud Foundation
- FlexPod as a Workload Domain for VMware Cloud Foundation
- FlexPod as a Workload Domain for VMware Cloud Foundation Design Guide

Design options with VMware Cloud Foundation and ONTAP

You can start fresh with VCF 9 or reuse existing deployments to create a Private Cloud environment using VCF 9 and ONTAP. Learn about popular design blueprints for VCF 9 and how NetApp products add value.

Storage options

VMware Cloud Foundation with ONTAP supports a variety of storage configurations to meet different performance, scalability, and availability requirements. The following tables summarize principal and supplemental storage options available for your environment.

Table 1. Principal storage options

Product Family	VMFS on FC	NFSv3
ASA A-Series and C-Series	Yes	No
AFF A-Series and C-Series	Yes	Yes
FAS	Yes	Yes

Table 2. Supplemental storage options

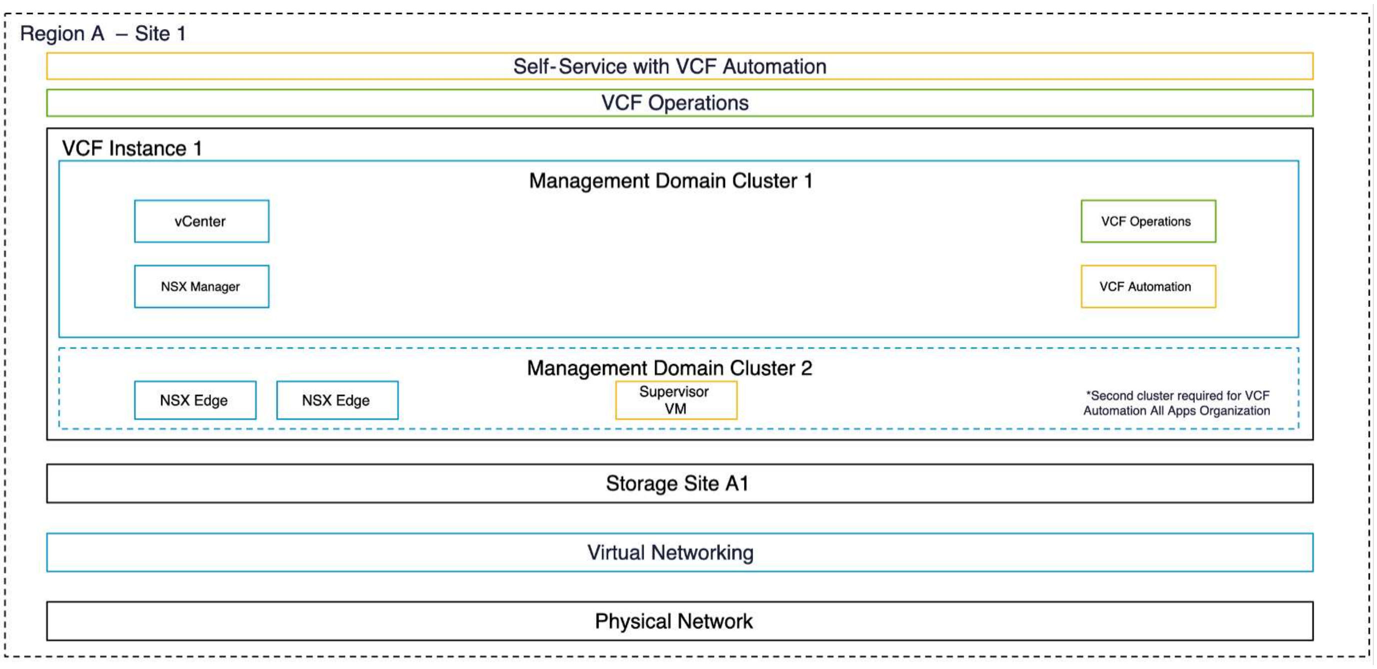
Product Family	VMFS on FC	VMFS on iSCSI	VMFS on NVMe-oF	NFSv3	NFSv4.1
ASA A-Series and C-Series	Yes	Yes	Yes	No	No
AFF A-Series and C-Series	Yes	Yes	Yes	Yes	Yes
FAS	Yes	Yes	Yes	Yes	Yes

Blueprints

The following blueprints illustrate common deployment models for VMware Cloud Foundation and ONTAP in various site and resource scenarios.

VCF fleet in a single site with minimal footprint

This design blueprint is for deploying Management and Workload components in a Single vSphere Cluster with minimal resources. It supports VMFS and NFSv3 Principal Datastores and a simple deployment option with a two-node configuration. If you plan to use VCF Automation with the All Apps Organization model, you need a second cluster to deploy vSphere Supervisor and NSX Edge nodes.



To minimize resource consumption, use an existing ONTAP tools instance if possible. If unavailable, a single node with a Small profile is suitable. The SnapCenter Plug-in for VMware vSphere protects virtual machines and Datastores using native snapshots and replication to another ONTAP storage array.

ⓘ If you lack resources to explore VCF, many Cloud Providers offer VCF as a service, and ONTAP is available as a first-party service from cloud providers.

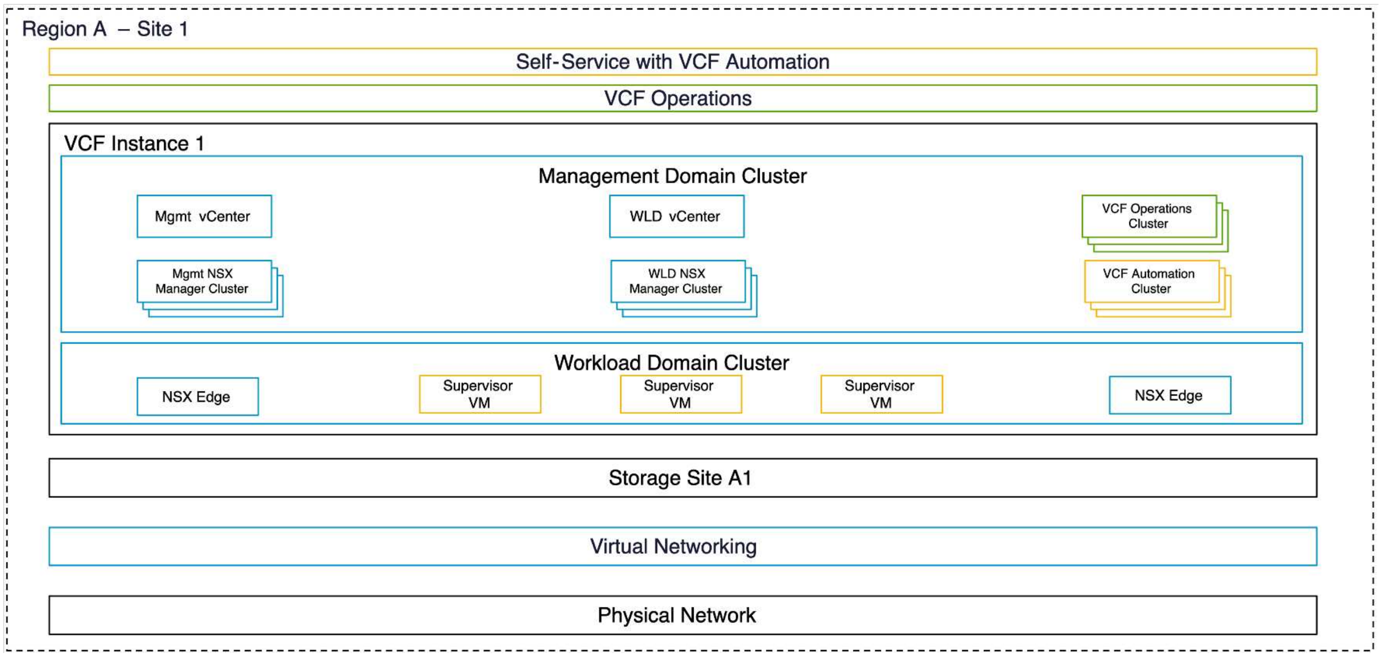
For more details on this design, refer to the Broadcom Technical Documentation on VCF Fleet in a Single Site with Minimal Footprint.

VCF fleet in a single site

This design blueprint is for customers with a single Primary Datacenter relying on application High Availability. Typically, it involves a single VCF environment. You can use ASA for block workloads and AFF for file/unified workloads.

Content Repository shares VM templates and container registries across VCF Domains. When hosted on FlexGroup Volume, FlexCache feature is available for subscription datastore.

! Hosting VMs on FlexCache Datastore is not supported.



A single instance of ONTAP tools in HA mode can manage all vCenters in the VCF Fleet. Refer to the Configuration Limits of ONTAP tools for more info. ONTAP tools integrate with VCF SSO and VCF OPS smart grouping for multi-vCenter access in the same UI.

VCF Supplemental Datastore with ONTAP Tools

You must deploy the SnapCenter Plug-in on each vCenter instance for VM and Datastore protection.

Storage policy-based Management is used with vSphere Supervisor to host control VMs of VKS. Tags are centrally managed at VCF Ops. NetApp Trident CSI is used with VKS for application backup protection using native array features. When you use vSphere CSI, persistent volume details appear on VCF Automation.

For more details on this blueprint, refer to the Broadcom Technical Documentation on VCF Fleet in a Single Site.

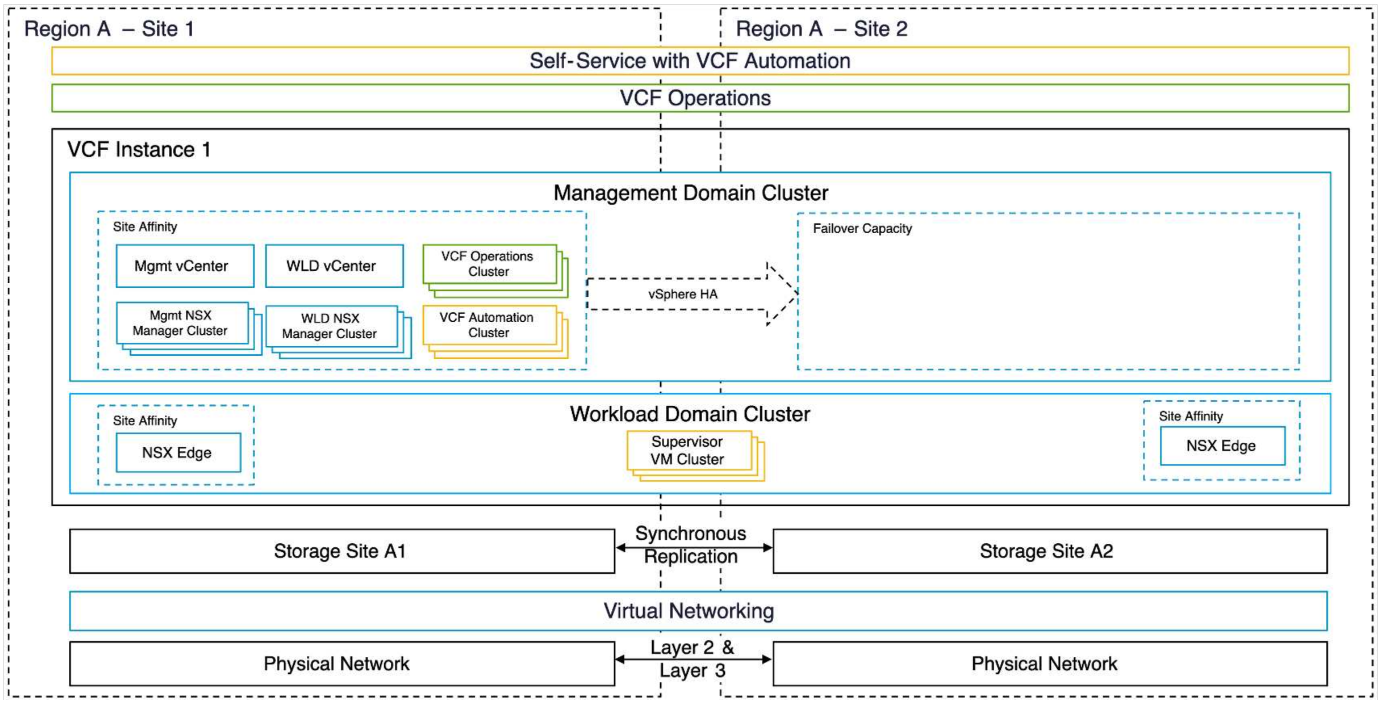
VCF fleet with multiple sites in a single region

This design is for customers providing cloud-like services with higher availability by spreading workloads across different fault domains.

For VMFS datastores, SnapMirror active sync provides an active-active storage unit for use with vSphere Metro Storage Cluster. Uniform access mode offers transparent storage failover, while Non-Uniform access mode requires VM restart on fault domain failure.

For NFS datastores, ONTAP MetroCluster with vSphere Metro Storage Cluster ensures high availability. A mediator avoids split-brain scenarios and can now be hosted on NetApp Console.

VM placement rules control VMs within the same fault domain for Management Domain components.



ONTAP tools provide a UI to set up SnapMirror active sync relationships. Storage Systems of both fault domains must be registered in ONTAP tools and SnapCenter Plug-in for VMware vSphere.

You can implement 3-2-1 backup policies using NetApp Backup and Recovery for VMs via SnapMirror and SnapMirror to Cloud. You can perform restores from any of the three locations.

Trident Protect or NetApp Backup and Recovery for Kubernetes protect VKS Cluster Applications.

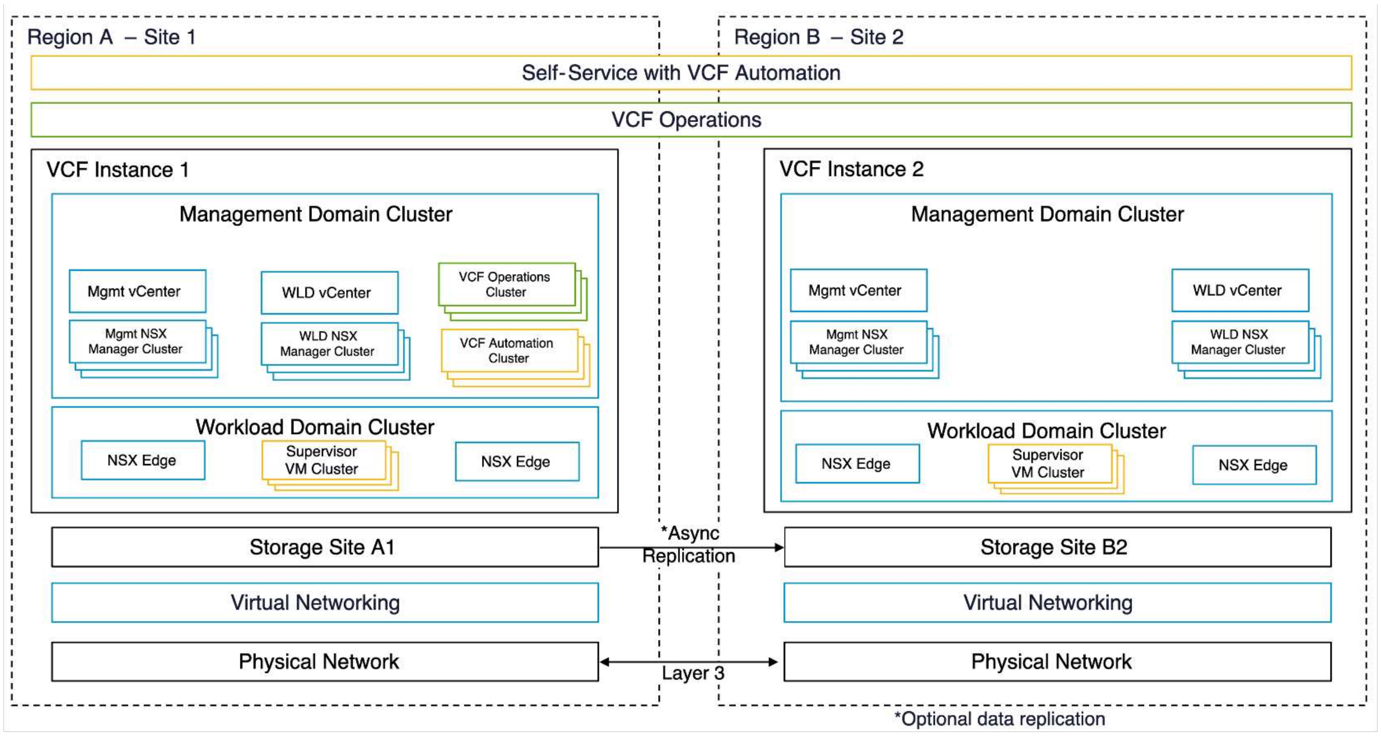
For more info, check the Broadcom Technical Documentation on VCF Fleet with Multiple Sites in a Single Region.

VCF fleet with multiple sites across multiple regions

This design is for customers spread globally, providing services in close proximity and disaster recovery solutions.

You can manage Disaster Recovery for VMs with VMware Live Site Recovery or NetApp Disaster Recovery. ONTAP tools offer the SRA (Storage Replication Adapter) to orchestrate storage operations with ONTAP.

Product Family	SnapMirror active sync	MetroCluster
ASA A-Series and C-Series	Yes	Yes
AFF A-Series and C-Series	Yes	Yes
FAS	No	Yes



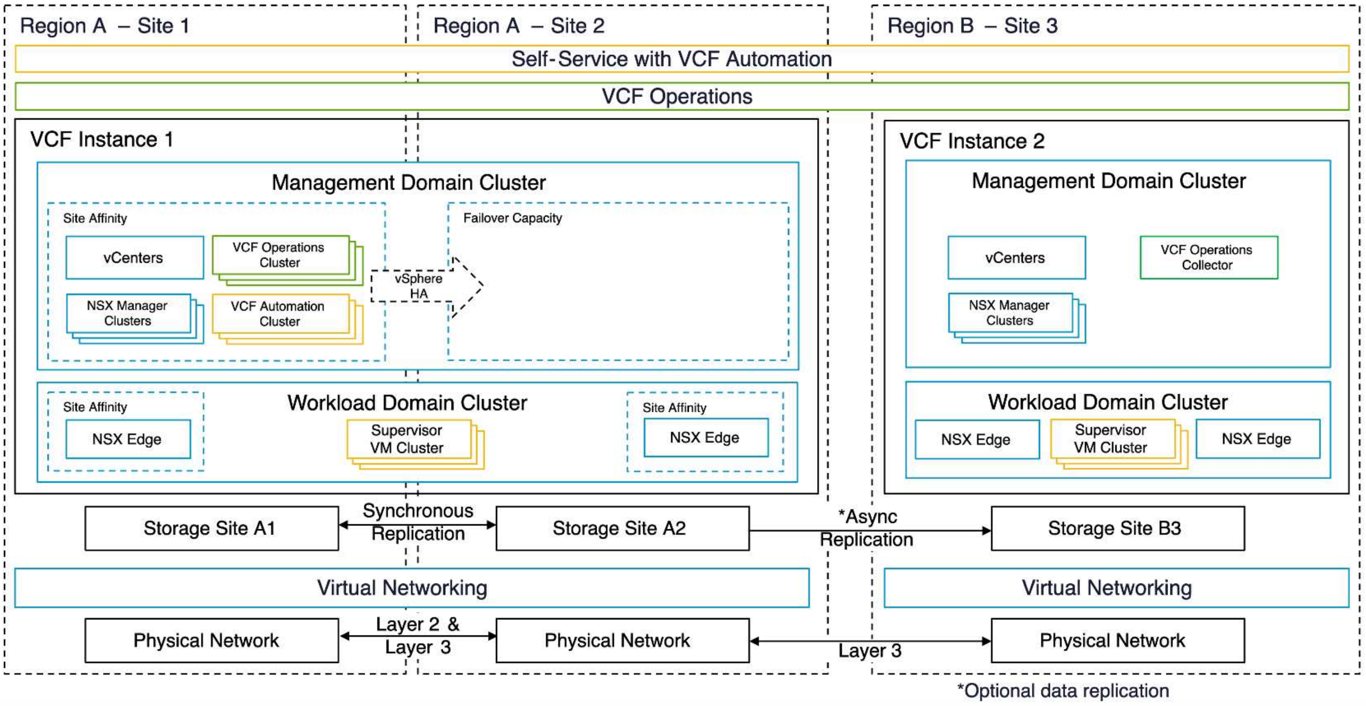
ONTAP tools provide a UI for datastore replication setup. NetApp Console can also be used for replication between storage arrays. SnapCenter Plug-in for VMware vSphere utilizes existing SnapMirror relationships for SnapShots.

For more info, check the Broadcom Technical Documentation on VCF Fleet with Multiple Sites Across Multiple Regions.

VCF fleet with multiple sites in a single region plus additional regions

This design addresses both availability and disaster recovery of VMs and VKS applications.

ASA, AFF, and FAS support this design option.



You can use ONTAP tools or NetApp Console to set up the replication relationship.

For more information, see the Broadcom Technical Documentation on VCF Fleet with Multiple Sites in a Single Region plus Additional Regions.

Set up private cloud environments with VMware Cloud Foundation and ONTAP

Deploy, converge, or upgrade VMware Cloud Foundation 9 environments with ONTAP. Learn how to set up new VCF 9.0 environments, converge existing vCenter instances and ONTAP datastores, and upgrade earlier VCF deployments.

Deploy a new VCF 9 instance

Use this workflow to deploy a clean VMware Cloud Foundation (VCF) 9.0 environment. After deployment, you can migrate workloads or begin provisioning applications and provide infrastructure services.

For high-level steps, see the Build Journey – Install a new VMware Cloud Foundation deployment.

Steps

1. Follow the Broadcom VCF 9 deployment steps.
2. In the deployment preparation step, complete the tasks for your principal storage option.

VMFS on FC

1. Collect the WWPNs for all ESXi hosts. You can run `esxcli storage san fc list`, use the ESXi Host Client, or use PowerCLI.
2. Configure zoning. See Recommended FC zoning configurations for ONTAP systems.

   > Use the WWPNs of the SVM logical interfaces (LIFs), not the physical adapter WWPNs.

3. Create a LUN and map it to the hosts by WWPN using System Manager, the ONTAP CLI, or the API.
4. Rescan the storage adapter on ESXi and create the VMFS datastore.

NFSv3

1. Create a VMkernel interface on one ESXi host.
2. Ensure the SVM has NFS enabled and vStorage over NFS is enabled.
3. Create a volume and export it with a policy that allows the ESXi hosts.
4. Adjust permissions as needed.
5. Deploy the ONTAP NFS VAAI VIB and include it in the vLCM image. For example: `esxcli software vib install -d /NetAppNasPlugin2.0.1.zip`. (Download the ZIP from the NetApp Support Site.)
6. Mount the NFS volume on the host where you created the VMkernel interface. For example: `esxcli storage nfs add -c 4 -H 192.168.122.210 -s /use1_m01_nfs01 -v use1-m01-cl01-nfs01`.

   > The `nConnect` session count is per host. Update other hosts after deployment as needed.

3. At the end of **Verify deployment summary and review next steps** in the **Deploy VCF Fleet** phase, complete the following:

   a. Deploy ONTAP tools

      - Download ONTAP tools 10.x from the NetApp Support Site.
      - Create DNS records for ONTAP tools Manager, node(s), and the virtual IP used for internal communication.
      - Deploy the OVA to the management vCenter Server.
      - Register the management domain vCenter with ONTAP tools Manager.
      - Add the storage backend using the vSphere Client UI.
      - Create a supplemental datastore (include one for the content registry).
      - Create the content registry if you plan an HA deployment.
      - Enable HA in ONTAP tools Manager.

   b. Deploy the SnapCenter Plug-in

      - Deploy the SnapCenter Plug-in for VMware vSphere.
      - Add the storage backend.

      - Create backup policies.
      - Create resource groups.
   c. Deploy the NetApp Console agent
      - Review what you can do without a Console agent.
      - Agent deployment modes.
   d. Use NetApp Backup and Recovery
      - Protect VM workloads.
      - Protect VKS workloads.
4. After you import vCenter as a workload domain in the VCF instance, complete the following:
   a. Register ONTAP tools
      - Register the workload domain vCenter with ONTAP tools Manager.
      - Add the storage backend using the vSphere Client UI.
      - Create a supplemental datastore.
   b. Deploy the SnapCenter Plug-in for VMware vSphere
      - Deploy the SnapCenter Plug-in for VMware vSphere.
      - Add the storage backend.
      - Create backup policies.
      - Create resource groups.
   c. Use NetApp Backup and Recovery
      - Protect VM workloads.
      - Protect VKS workloads.

You can reuse these steps whenever you create a new workload domain.

Converge existing components into VCF 9

You may already have some components of the VCF fleet and prefer to reuse them. When you reuse a vCenter instance, datastores are frequently provisioned with ONTAP tools, which can serve as the principal storage for VCF.

Prerequisites

- Confirm existing vCenter instances are functional.
- Verify ONTAP-provisioned datastores are available.
- Ensure access to the Interoperability Matrix.

Steps

1. Review the supported scenarios to converge to VCF.
2. Converge a vCenter instance with ONTAP-provisioned datastores as principal storage.
3. Verify supported versions using the Interoperability Matrix.
4. Upgrade ONTAP tools if required.
5. Upgrade the SnapCenter Plugin for VMware vSphere if required.

Upgrade an existing VCF environment to VCF 9

Upgrade an earlier VCF deployment to version 9.0 using the standard upgrade process. The outcome is a VCF environment running version 9.0 with upgraded management and workload domains.

Prerequisites

- Back up the management domain and workload domains.
- Verify compatibility of ONTAP tools and SnapCenter Plug-in with VCF 9.0. Follow the Interoperability Matrix to upgrade ONTAP tools and SnapCenter Plugin for VMware vSphere that are supported for VCF 9.

Steps

1. Upgrade the VCF management domain. See Upgrade VCF Management Domain to VCF 9 for instructions.
2. Upgrade any VCF 5.x workload domains. See Upgrade VCF 5.x Workload Domain to VCF 9 for instructions.

Implementing Disaster Recovery with NetApp Disaster Recovery

VCF disaster recovery solution for NFS datastore with NetApp SnapMirror and NetApp Disaster Recovery

Block-level replication from a production site to a disaster recovery (DR) site offers a resilient and cost-effective strategy for protecting workloads against site outages and data corruption events, including ransomware attacks. NetApp SnapMirror replication enables VMware VCF 9 workload domains running on on-premises ONTAP systems—using either NFS or VMFS datastores—to be replicated to a secondary ONTAP system located in a designated recovery datacenter where VMware is also deployed.

For more information, see the following NetApp Disaster Recovery documentation.

This section outlines the configuration of NetApp Disaster Recovery to establish DR for on-premises VMware virtual machines.

The setup includes:

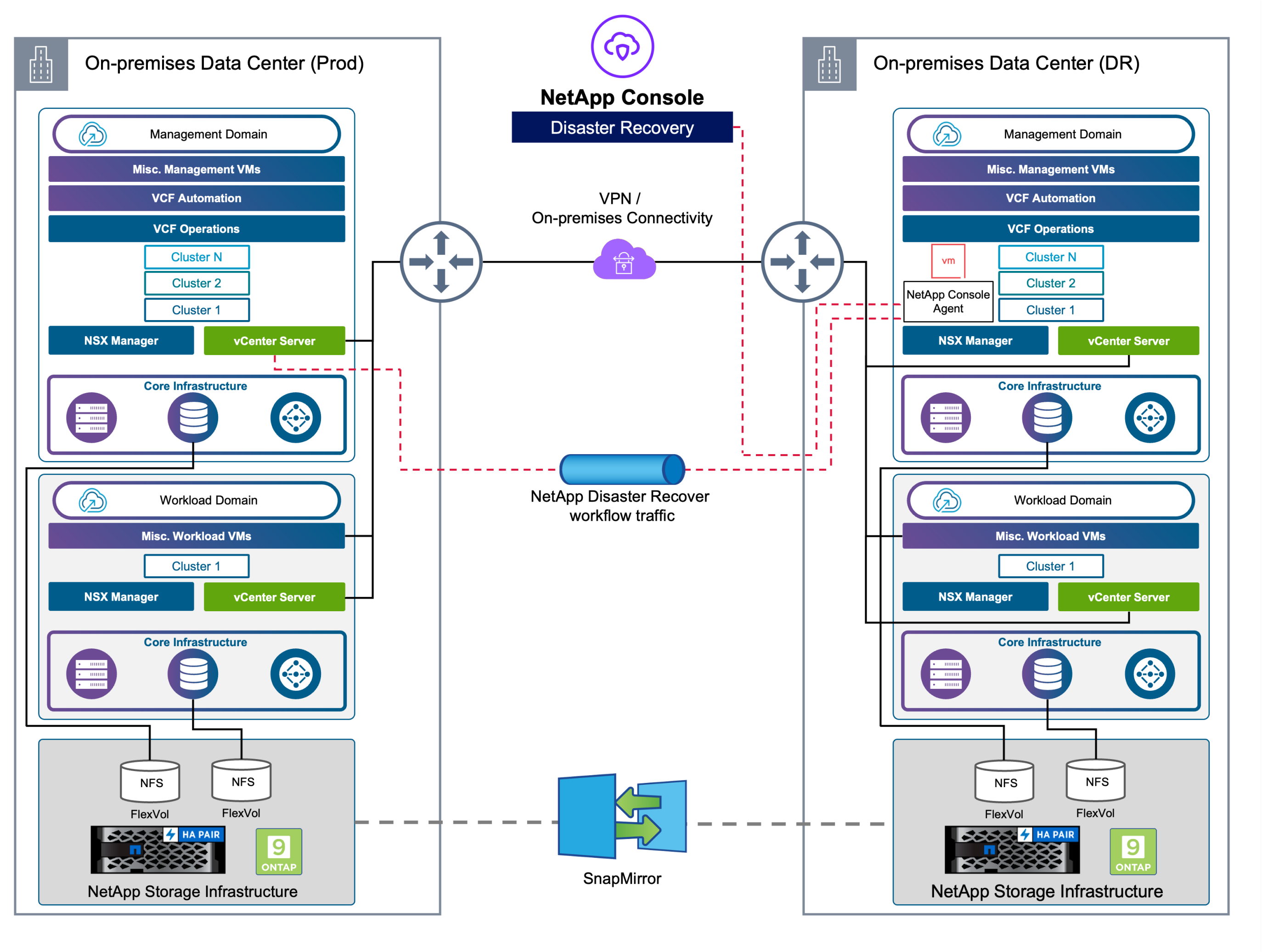
- Creating a NetApp Console account and deploying an agent.
- Adding ONTAP arrays to the NetApp Console to systems under Management to facilitate communication between VMware vCenter and ONTAP storage.
- Configuring replication between sites using SnapMirror.
- Setting up and testing a recovery plan to validate failover readiness.

NetApp Disaster Recovery, integrated within the NetApp Console, enables organizations to seamlessly discover their on-premises VMware vCenters and ONTAP storage systems. Once discovered, administrators can define resource groupings, create disaster recovery plans, associate them with the appropriate resources, and initiate or test failover and failback operations.
NetApp SnapMirror provides efficient block-level replication, ensuring that the DR site remains synchronized with the production environment through incremental updates. This enables a Recovery Point Objective (RPO) as low as five minutes.

NetApp Disaster Recovery also supports non-disruptive disaster recovery testing. Leveraging ONTAP’s FlexClone technology, it creates space-efficient, temporary copies of the NFS datastore from the most recent replicated Snapshot—without impacting production workloads or incurring additional storage costs. After testing, the environment can be easily torn down, preserving the integrity of the replicated data.

In the event of an actual failover, NetApp Console orchestrates the recovery process, automatically bringing up protected virtual machines at the designated DR site with minimal user intervention. When the primary site is restored, the service reverses the SnapMirror relationship and replicates any changes back to the original site, enabling a smooth and controlled failback.

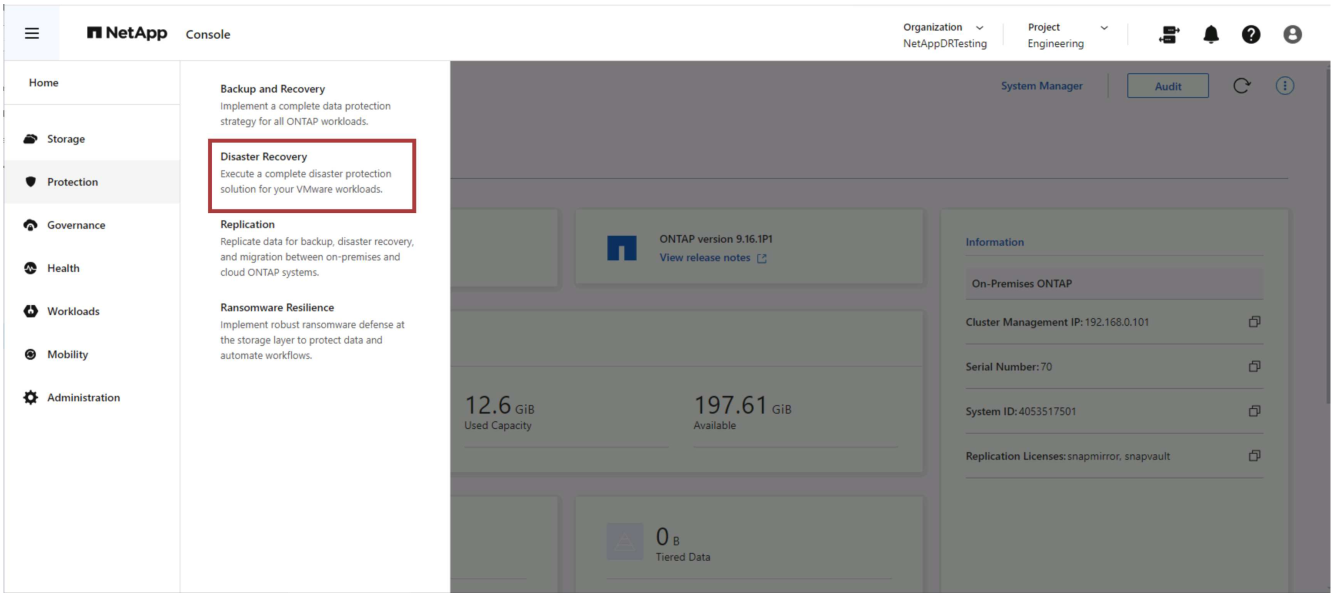
All these capabilities are delivered at a significantly lower cost compared to traditional disaster recovery solutions.



Getting started

To get started with NetApp Disaster Recovery, use NetApp Console and then access the service.

1. Log in to NetApp Console.
2. From the NetApp Console left navigation, select Protection > Disaster Recovery.
3. The NetApp Disaster Recovery Dashboard appears.



Backup and Recovery
Implement a complete data protection strategy for all ONTAP workloads.

Disaster Recovery
Execute a complete disaster protection solution for your VMware workloads.

Replication
Replicate data for backup, disaster recovery, and migration between on-premises and cloud ONTAP systems.

Ransomware Resilience
Implement robust ransomware defense at the storage layer to protect data and automate workflows.

ONTAP version 9.16.1P1
View release notes

Information

On-Premises ONTAP

Cluster Management IP: 192.168.0.101

Serial Number: 70

System ID: 4053517501

Replication Licenses: snapmirror, snapvault

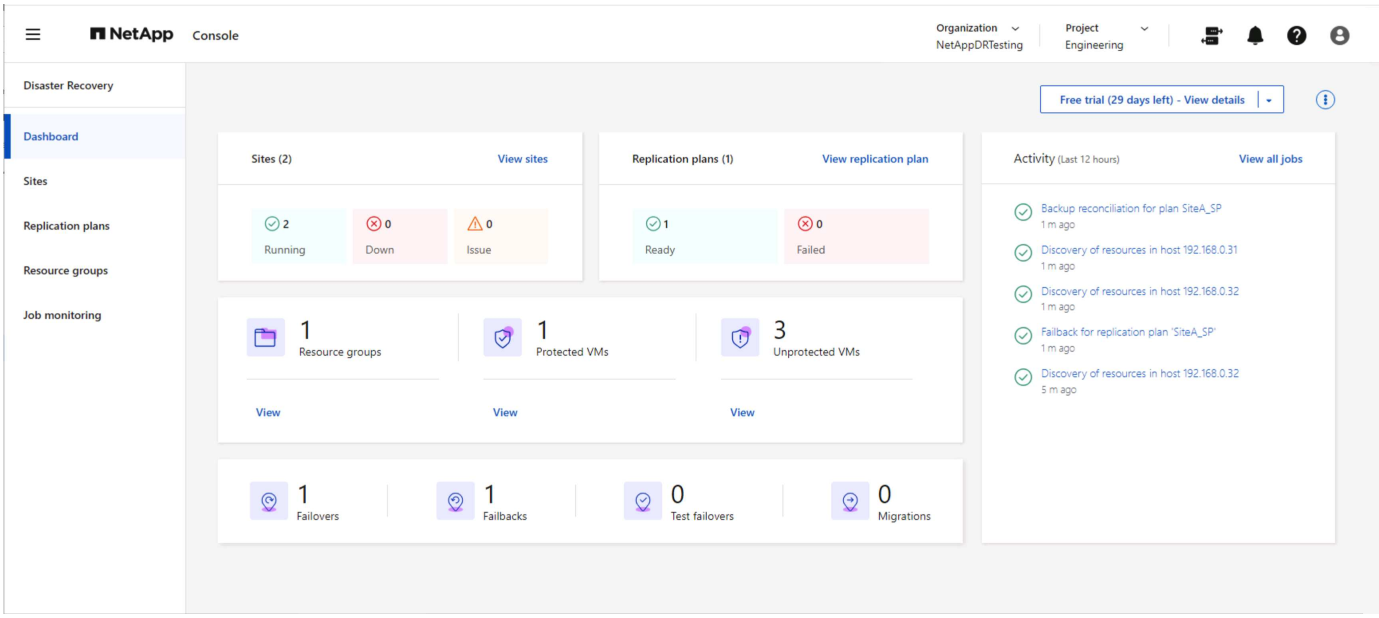
Before configuring the disaster recovery plan, ensure the following pre-requisites are met:

- The Console agent is set up in NetApp Console.
- The agent instance have connectivity to the source and destination workload domain vCenter and storage systems.
- NetApp Data ONTAP cluster to provide storage NFS or VMFS datastores.
- On-premises NetApp storage systems hosting NFS or VMFS datastores for VMware are added in NetApp Console.
- DNS resolution should be in place when using DNS names. Otherwise, use IP addresses for the vCenter.
- SnapMirror replication is configured for the designated NFS or VMFS based datastore volumes.
- Make sure that the environment has supported versions of vCenter Server and ESXi servers.

Once the connectivity is established between the source and destination sites, proceed with configuration steps, which should take couple of clicks and about 3 to 5 minutes.

Note: NetApp recommends deploying the Console agent in the destination site or in a third site, so that the agent can communicate through the network with source and destination resources.

In this demonstration, the workload domains are configured with ONTAP NFS storage. The steps in terms of workflow remains the same for VMFS based datastores.



Backup reconciliation for plan SiteA_SP
1 m ago

Discovery of resources in host 192.168.0.31
1 m ago

Discovery of resources in host 192.168.0.32
1 m ago

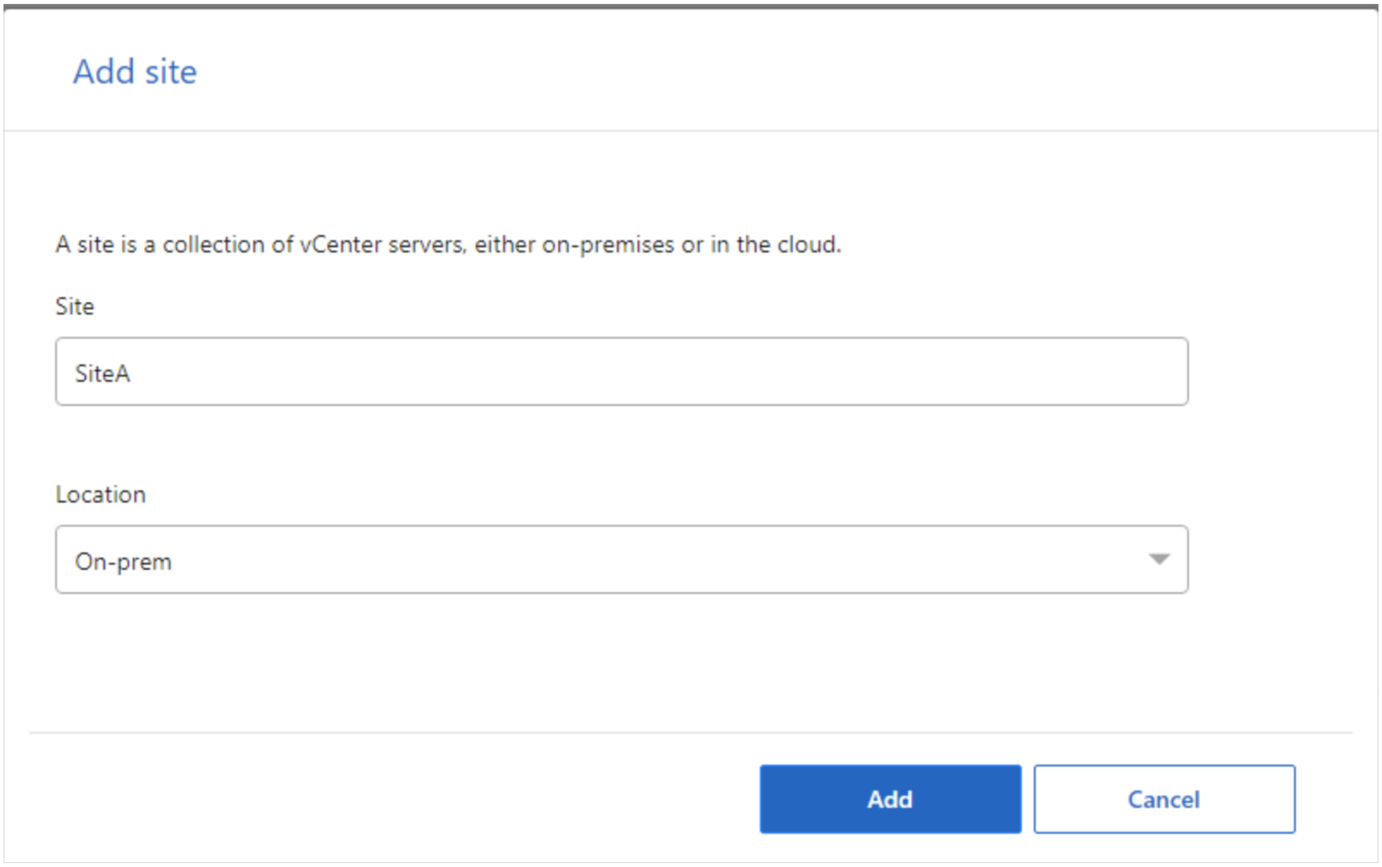
Failback for replication plan 'SiteA_SP'
1 m ago

Discovery of resources in host 192.168.0.32
5 m ago

NetApp Disaster Recovery configuration

The first step in preparing for disaster recovery is to discover and add the source vCenter and storage resources to NetApp Disaster Recovery.

Open NetApp Console and select Protection > Disaster Recovery from left navigation. Select Sites and then choose Add. Enter a name for the new source site and its locations. Repeat the step to add the destination site and location.



Add site

A site is a collection of vCenter servers, either on-premises or in the cloud.

Site: SiteA

Location: On-prem

Add the following platforms:

- Source workload domain vCenter
- Destination workload domain vCenter.

Once the vCenters are added, automated discovery is triggered.

Configuring storage replication between source site array and destination site array

SnapMirror provides data replication in a NetApp environment. Built on NetApp Snapshot® technology, SnapMirror replication is extremely efficient because it replicates only the blocks that have been changed or added since the previous update. SnapMirror is easily configured by using either NetApp OnCommand® System Manager or the ONTAP CLI. NetApp Disaster Recovery also creates the SnapMirror relationship provided cluster and SVM peering is configured beforehand.

For cases in which the primary storage is not completely lost, SnapMirror provides an efficient means of resynchronizing the primary and DR sites. SnapMirror can resynchronize the two sites, transferring only changed or new data back to the primary site from the DR site by simply reversing the SnapMirror relationships. This means replication plans in NetApp Disaster Recovery can be resynchronized in either direction after a failover without recopying the entire volume. If a relationship is resynchronized in the reverse direction, only new data that was written since the last successful synchronization of the Snapshot copy is sent back to the destination.

> ⓘ If SnapMirror relationship is already configured for the volume via CLI or System Manager, NetApp Disaster Recovery picks up the relationship and continues with the rest of the workflow operations.

How to setup replication relationships for NetApp Disaster Recovery

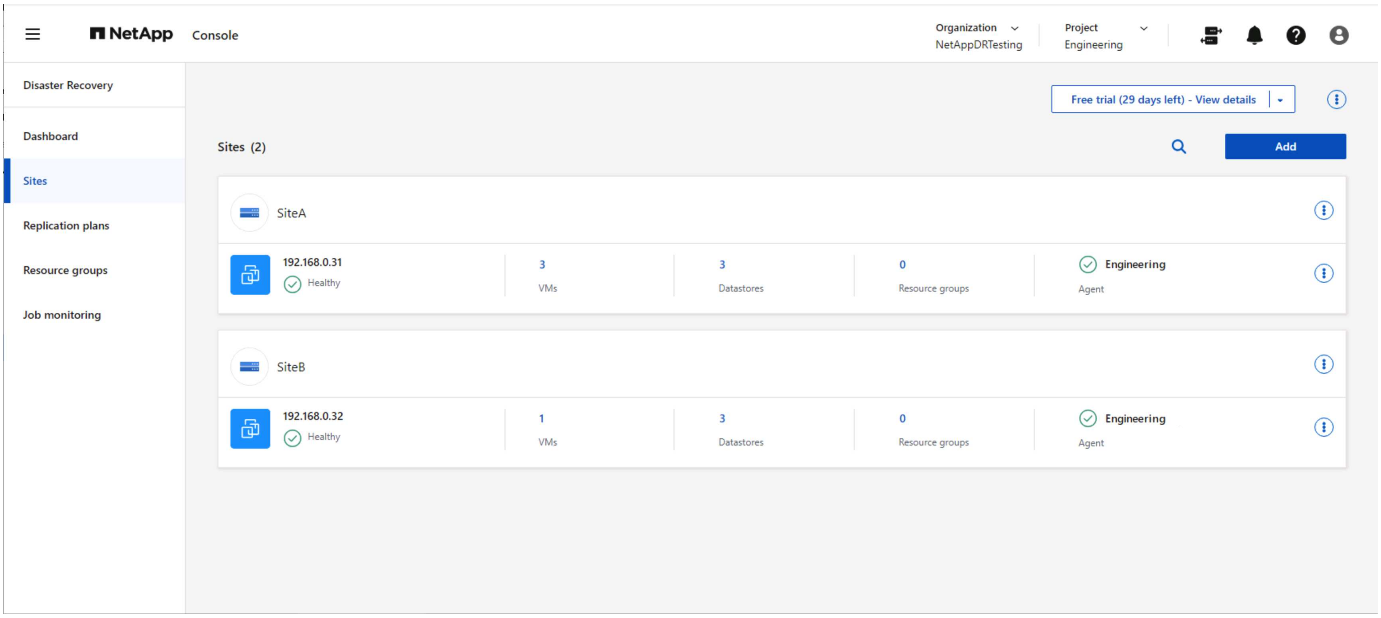
The underlying process to create SnapMirror replication remains the same for any given application. The process can be manual or automated. The easiest way is to leverage NetApp Disaster Recovery which will automate the replication workflow provided the following two criteria are met:

- Source and destination clusters have a peer relationship.
- Source SVM and destination SVM have a peer relationship.

NetApp Console also provides an alternate option to configure SnapMirror replication by using simple drag & drop of the source ONTAP system in the environment onto the destination to trigger the wizard that guides through the rest of the process.

What can NetApp Disaster Recovery do for you?

After the source and destination sites are added, NetApp Disaster Recovery performs automatic deep discovery and displays the VMs along with associated metadata. NetApp Disaster Recovery also automatically detects the networks and port groups used by the VMs and populates them.



NetApp Console

Organization: NetAppDRTesting

Project: Engineering

Disaster Recovery

- Dashboard
- Sites
- Replication plans
- Resource groups
- Job monitoring

Free trial (29 days left) - View details

Sites (2)

Add

SiteA

192.168.0.31 Healthy	3 VMs	3 Datastores	0 Resource groups	Engineering Agent

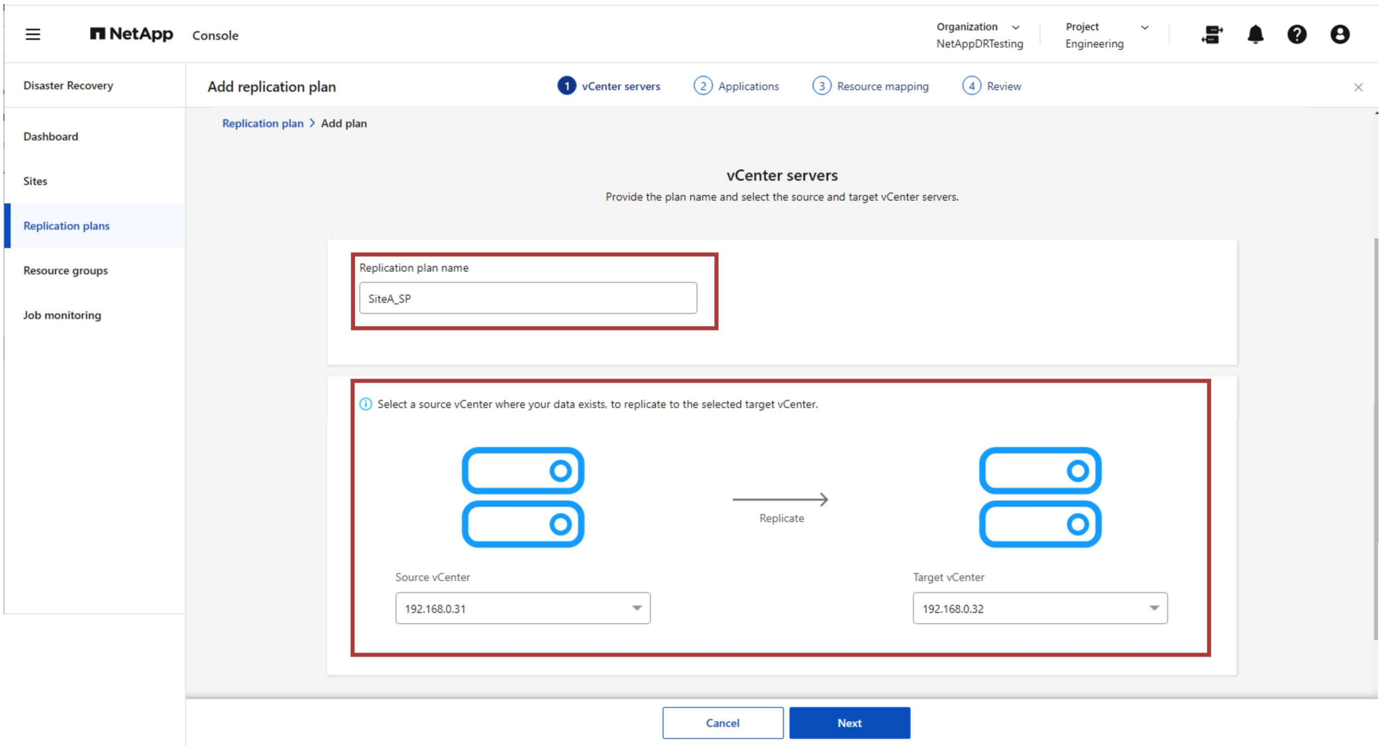
SiteB

192.168.0.32 Healthy	1 VMs	3 Datastores	0 Resource groups	Engineering Agent

After the sites have been added, configure the replication plan by selecting the source and destination vCenter platforms and pick the resource groups to be included in the plan, along with the grouping of how applications should be restored and powered on and mapping of clusters and networks. To define the recovery plan, navigate to the **Replication plans** tab and click **Add**.

In this step, the VMs can be grouped into resource groups. NetApp Disaster Recovery resource groups allow you to group a set of dependent VMs into logical groups that contain their boot orders and boot delays that can be executed upon recovery. Resource groups can be during the creation of the replication plan or by using the Resource group tab on the left navigation.

First, name the replication plan and select the source vCenter and destination vCenter.



NetApp Console

Organization: NetAppDRTesting

Project: Engineering

Disaster Recovery

- Dashboard
- Sites
- Replication plans
- Resource groups
- Job monitoring

Add replication plan

1 vCenter servers — 2 Applications — 3 Resource mapping — 4 Review

Replication plan > Add plan

vCenter servers

Provide the plan name and select the source and target vCenter servers.

Replication plan name: SiteA_SP

Select a source vCenter where your data exists, to replicate to the selected target vCenter.

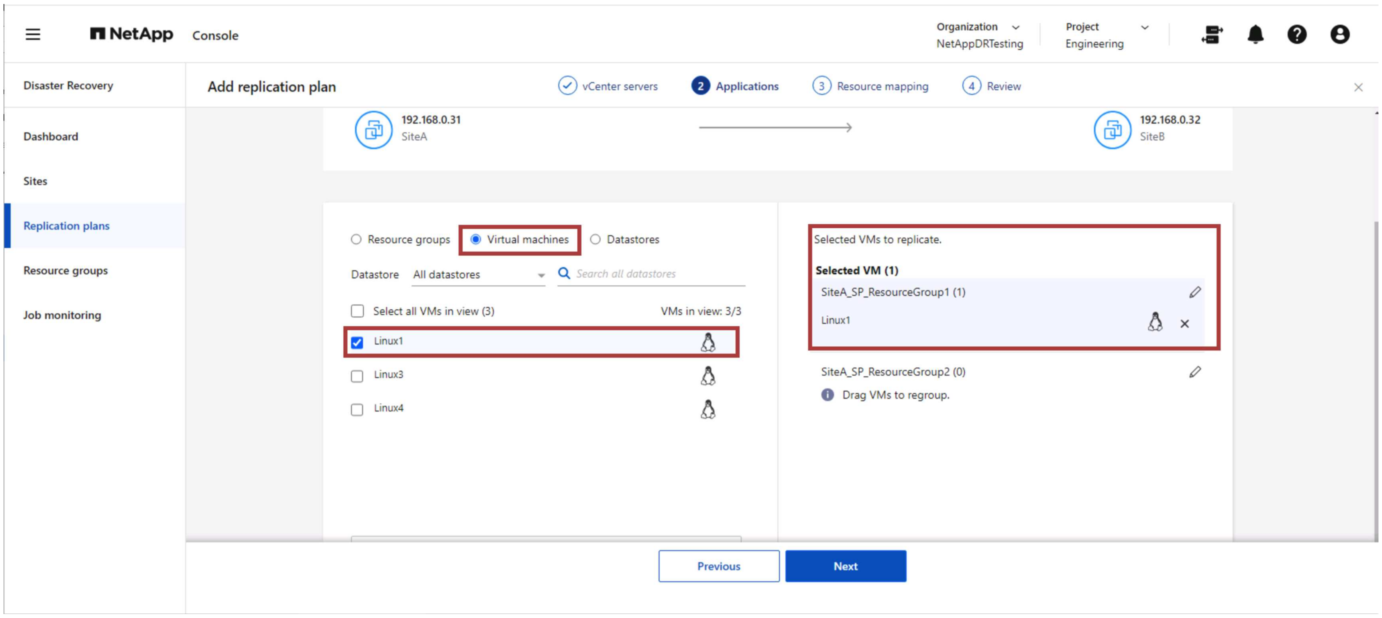
Replicate

Source vCenter: 192.168.0.31

Target vCenter: 192.168.0.32

Cancel | Next

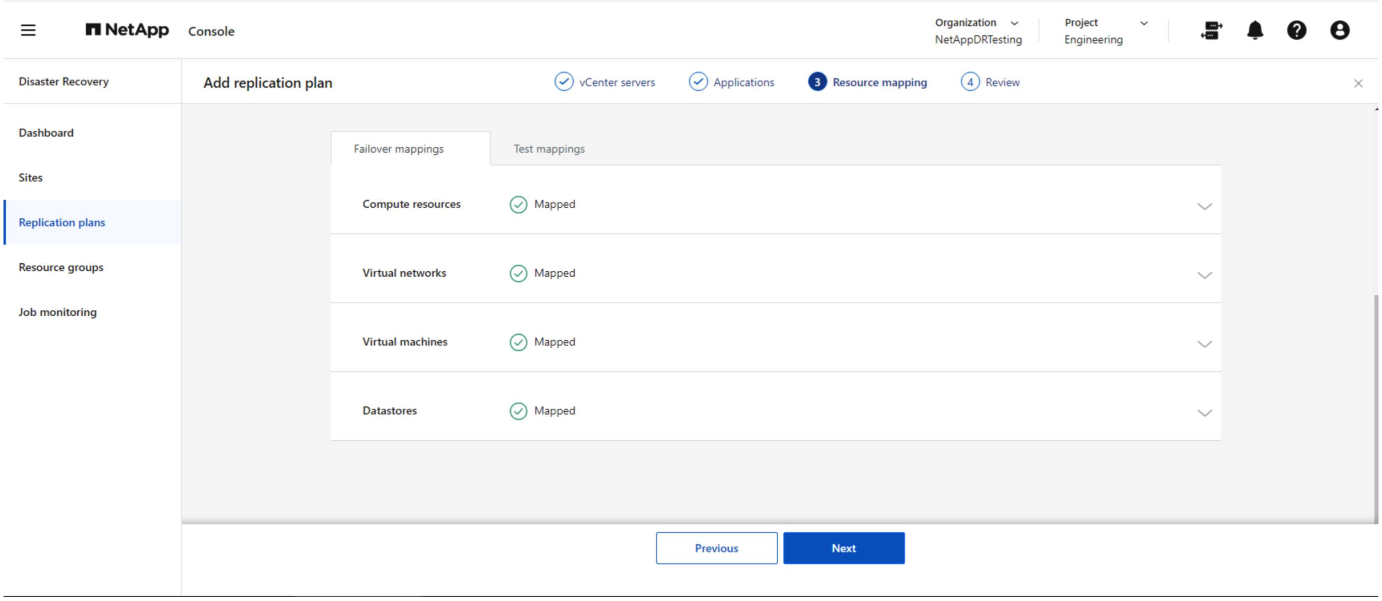
The next step is to choose whether you are creating a replication plan with Resource groups, virtual machines or datastores. Select an existing resource group and if no resource groups are created, then the wizard helps to group the required virtual machines (basically create functional resource groups) based on the recovery objectives. This also helps define the operation sequence of how application virtual machines should be restored.



Resource group allows to set boot order using the drag and drop functionality. It can be used to easily modify the order in which the VMs would be powered on during the recovery process.

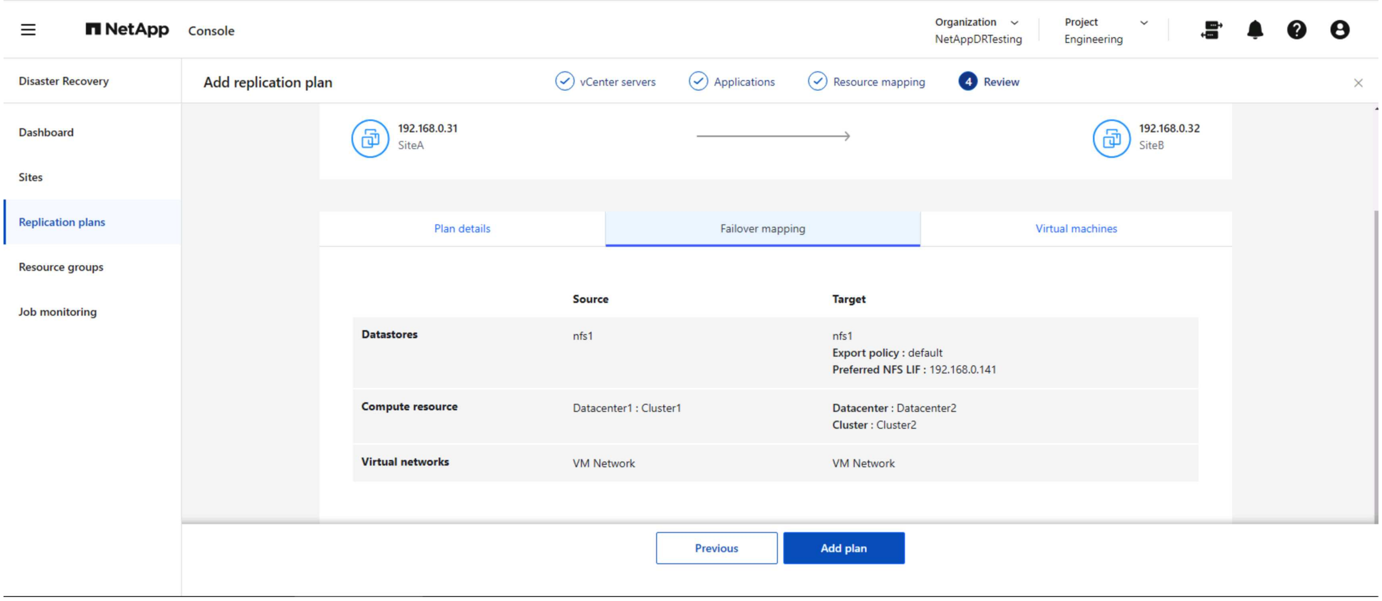
Once the resource groups are created via replication plan, the next step is to create the mapping to recover virtual machines and applications in the event of a disaster. In this step, specify how the resources from the source environment map to the destination. This includes compute resources, virtual networks, IP customization, pre- and post-scripts, boot delays, application consistency and so on. For detailed information, refer to Create a replication plan. As mentioned in the prerequisites, SnapMirror replication can be configured beforehand or DRaaS can configure it using the RPO and retention count specified during creation of the replication plan.

Note: By default, the same mapping parameters are used for both test and failover operations. To set different mappings for test environment, select the Test mapping option after unchecking the checkbox “Use same mappings for failover and test mappings”. Once the resource mapping is complete, click Next.



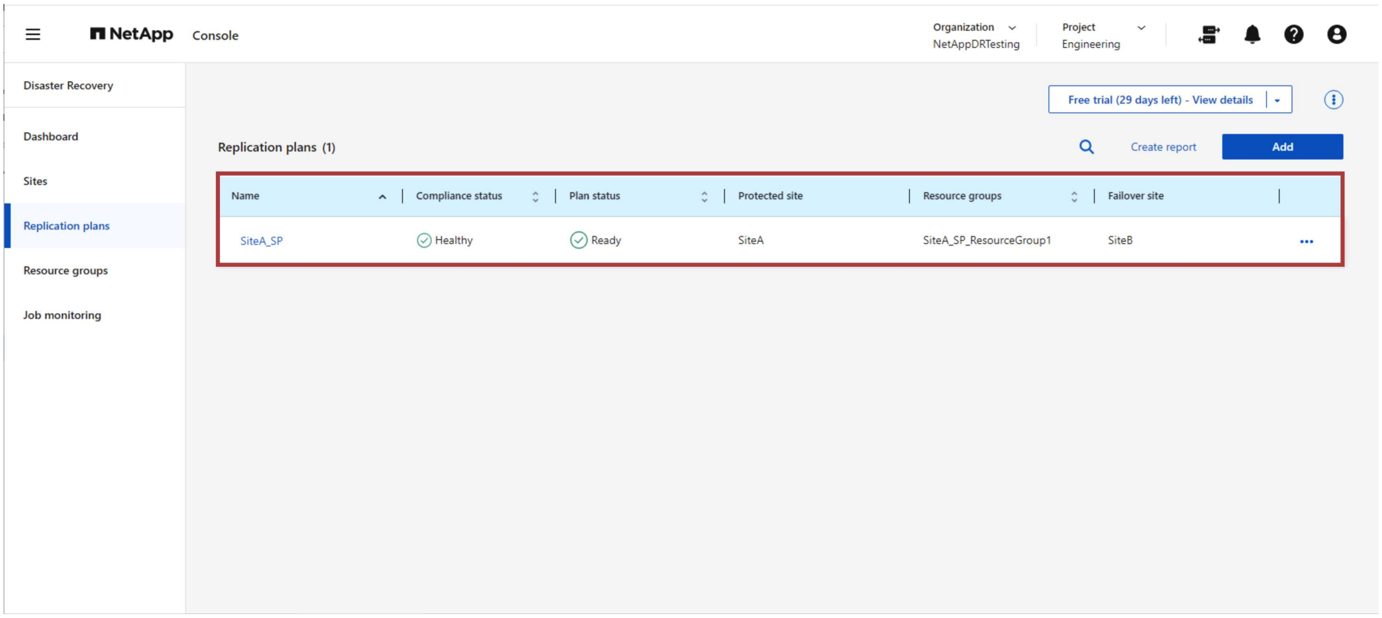
Compute resources	✓ Mapped
Virtual networks	✓ Mapped
Virtual machines	✓ Mapped
Datastores	✓ Mapped

Once done, review the created mappings and then click on Add plan.



	Source	Target
Datastores	nfs1	nfs1 **Export policy :** default **Preferred NFS LIF :** 192.168.0.141
Compute resource	Datacenter1 : Cluster1	**Datacenter :** Datacenter2 **Cluster :** Cluster2
Virtual networks	VM Network	VM Network

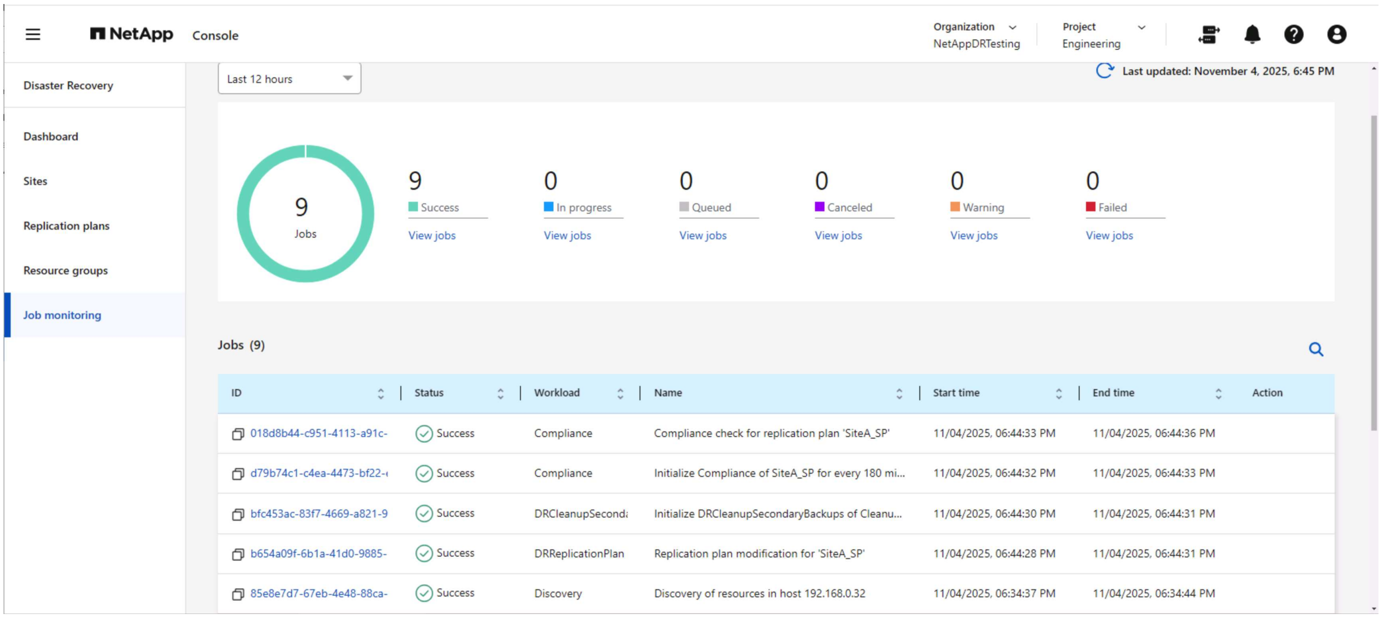
VMs from different volumes and SVMs can be included in a replication plan. Depending on the VM placement (be it on same volume or separate volume within the same SVM, separate volumes on different SVMs), NetApp Disaster Recovery creates a Consistency Group Snapshot.



Replication plans (1)

Name	Compliance status	Plan status	Protected site	Resource groups	Failover site
SiteA_SP	✓ Healthy	✓ Ready	SiteA	SiteA_SP_ResourceGroup1	SiteB

As soon as the plan is created, a series of validations are triggered and SnapMirror replication and schedules are configured as per the selection.



Last updated: November 4, 2025, 6:45 PM

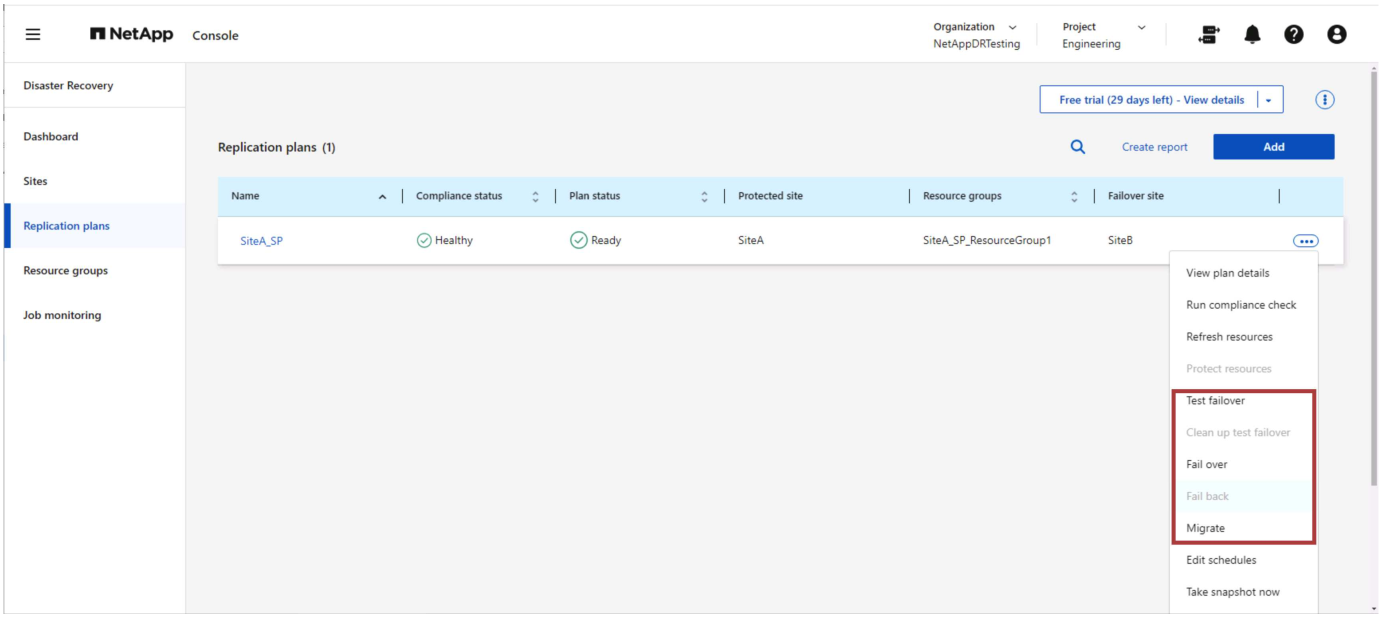
9	0	0	0	0	0
Success	In progress	Queued	Canceled	Warning	Failed

Jobs (9)

ID	Status	Workload	Name	Start time	End time	Action
018d8b44-c951-4113-a91c-	✓ Success	Compliance	Compliance check for replication plan 'SiteA_SP'	11/04/2025, 06:44:33 PM	11/04/2025, 06:44:36 PM	
d79b74c1-c4ea-4473-bf22-‹	✓ Success	Compliance	Initialize Compliance of SiteA_SP for every 180 mi...	11/04/2025, 06:44:32 PM	11/04/2025, 06:44:33 PM	
bfc453ac-83f7-4669-a821-9	✓ Success	DRCleanupSecond:	Initialize DRCleanupSecondaryBackups of Cleanu...	11/04/2025, 06:44:30 PM	11/04/2025, 06:44:31 PM	
b654a09f-6b1a-41d0-9885-	✓ Success	DRReplicationPlan	Replication plan modification for 'SiteA_SP'	11/04/2025, 06:44:28 PM	11/04/2025, 06:44:31 PM	
85e8e7d7-67eb-4e48-88ca-	✓ Success	Discovery	Discovery of resources in host 192.168.0.32	11/04/2025, 06:34:37 PM	11/04/2025, 06:34:44 PM	

NetApp Disaster Recovery consists of the following workflows:

- Test failover (including periodic automated simulations)
- Cleanup failover test
- Failover:
  - Planned migration (extend the usecase for one time failover)
  - Disaster recovery
- Failback

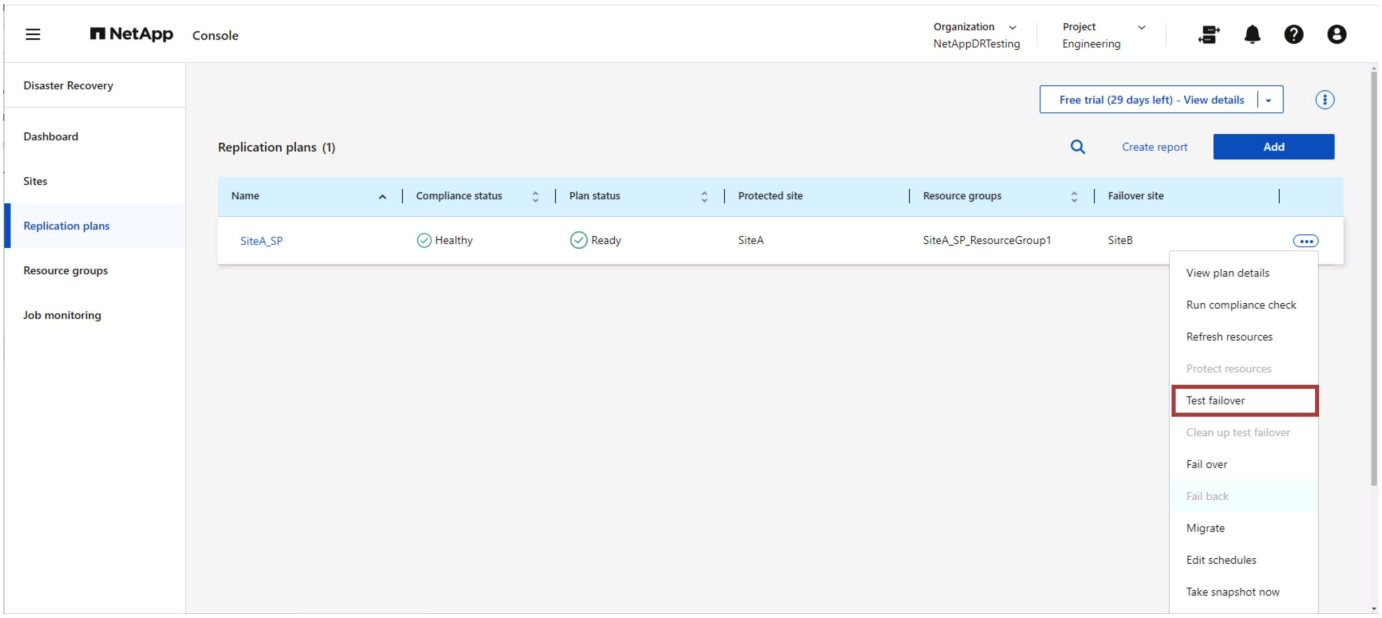


Replication plans (1)

Name	Compliance status	Plan status	Protected site	Resource groups	Failover site
SiteA_SP	Healthy	Ready	SiteA	SiteA_SP_ResourceGroup1	SiteB

Test failover

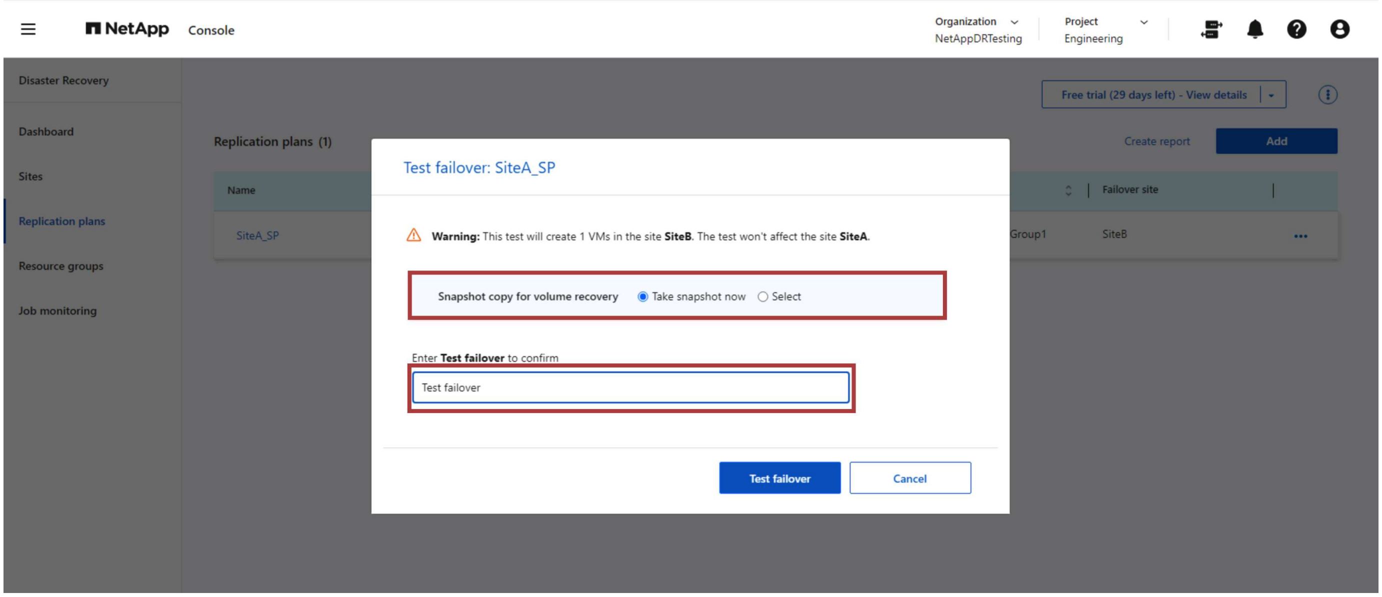
Test failover in NetApp Disaster Recovery is an operational procedure that allows VMware administrators to fully validate their recovery plans without disrupting their production environments.



Replication plans (1)

Name	Compliance status	Plan status	Protected site	Resource groups	Failover site
SiteA_SP	Healthy	Ready	SiteA	SiteA_SP_ResourceGroup1	SiteB

NetApp Disaster Recovery incorporates the ability to select the snapshot as an optional capability in the test failover operation. This capability allows the VMware administrator to verify that any changes that were recently made in the environment are replicated to the destination site and thus are present during the test. Such changes include patches to the VM guest operating system.



Test failover: SiteA_SP

⚠ **Warning:** This test will create 1 VMs in the site **SiteB**. The test won't affect the site **SiteA**.

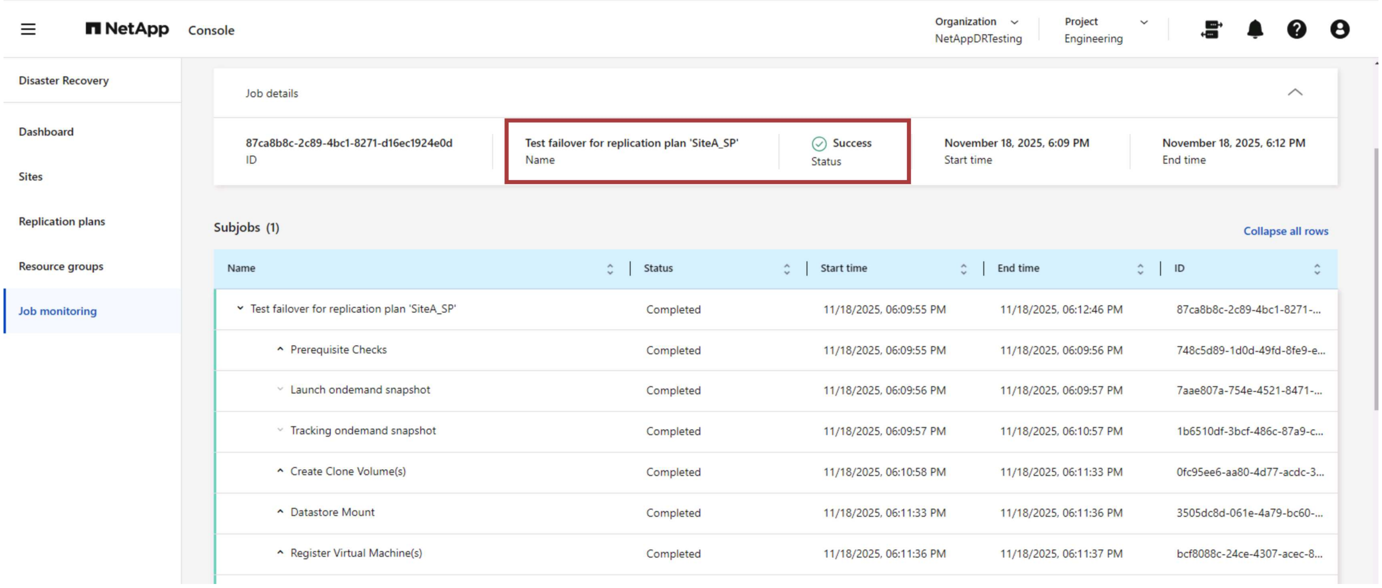
Snapshot copy for volume recovery ● Take snapshot now ○ Select

Enter **Test failover** to confirm

Test failover

When the VMware administrator runs a test failover operation, NetApp Disaster Recovery automates the following tasks:

- Triggering SnapMirror relationships to update storage at the destination site with any recent changes that were made at the production site.
- Creating NetApp FlexClone volumes of the FlexVol volumes on the DR storage array.
- Connecting the datastores in the FlexClone volumes to the ESXi hosts at the DR site.
- Connecting the VM network adapters to the test network specified during the mapping.
- Reconfiguring the VM guest operating system network settings as defined for the network at the DR site.
- Executing any custom commands that have been stored in the replication plan.
- Powering on the VMs in the order that is defined in the replication plan.



Job details

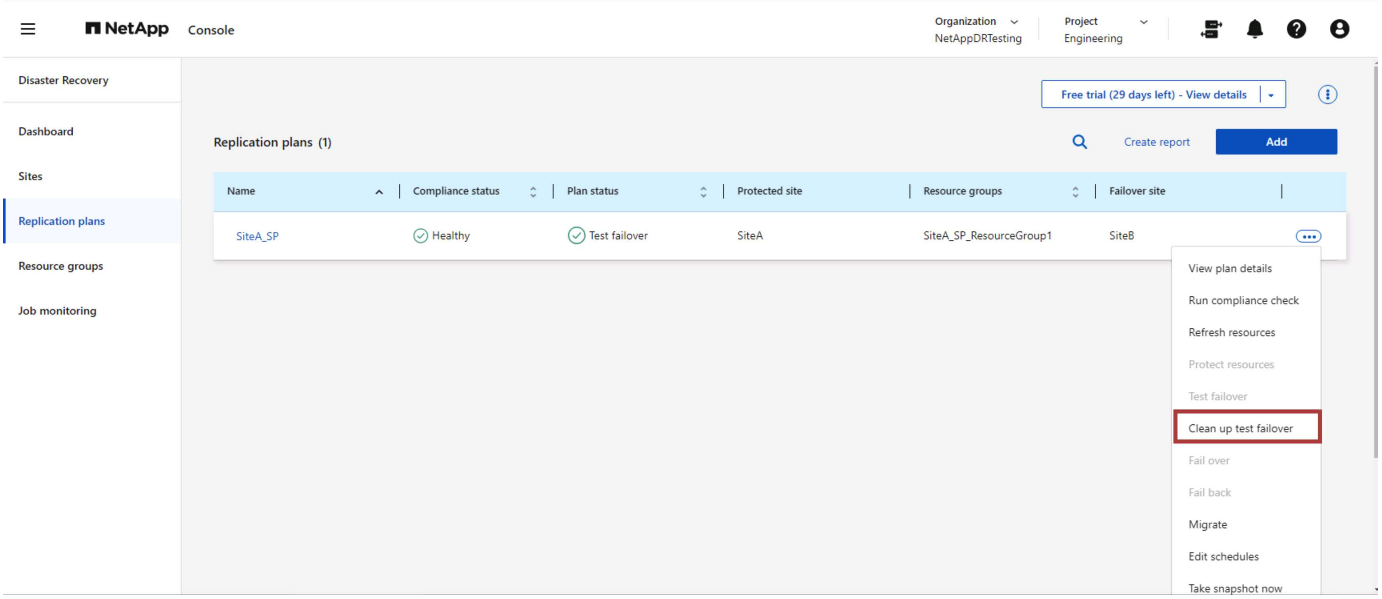
ID	Name	Status	Start time	End time
87ca8b8c-2c89-4bc1-8271-d16ec1924e0d	Test failover for replication plan 'SiteA_SP'	Success	November 18, 2025, 6:09 PM	November 18, 2025, 6:12 PM

Subjobs (1)

Name	Status	Start time	End time	ID
Test failover for replication plan 'SiteA_SP'	Completed	11/18/2025, 06:09:55 PM	11/18/2025, 06:12:46 PM	87ca8b8c-2c89-4bc1-8271-...
Prerequisite Checks	Completed	11/18/2025, 06:09:55 PM	11/18/2025, 06:09:56 PM	748c5d89-1d0d-49fd-8fe9-e...
Launch ondemand snapshot	Completed	11/18/2025, 06:09:56 PM	11/18/2025, 06:09:57 PM	7aae807a-754e-4521-8471-...
Tracking ondemand snapshot	Completed	11/18/2025, 06:09:57 PM	11/18/2025, 06:10:57 PM	1b6510df-3bcf-486c-87a9-c...
Create Clone Volume(s)	Completed	11/18/2025, 06:10:58 PM	11/18/2025, 06:11:33 PM	0fc95ee6-aa80-4d77-acdc-3...
Datastore Mount	Completed	11/18/2025, 06:11:33 PM	11/18/2025, 06:11:36 PM	3505dc8d-061e-4a79-bc60-...
Register Virtual Machine(s)	Completed	11/18/2025, 06:11:36 PM	11/18/2025, 06:11:37 PM	bcf8088c-24ce-4307-acec-8...

Cleanup failover test Operation

The cleanup failover test operation occurs after the replication plan test has been completed and the VMware administrator responds to the cleanup prompt.



Replication plans (1)

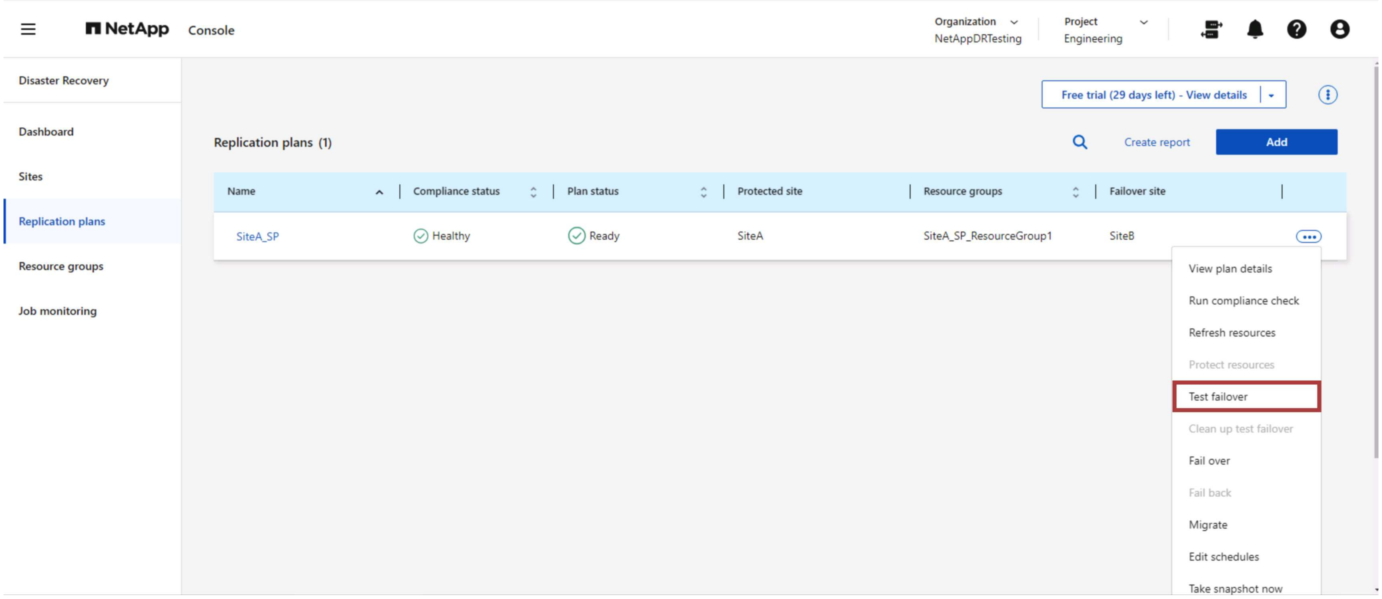
Name	Compliance status	Plan status	Protected site	Resource groups	Failover site
SiteA_SP	Healthy	Test failover	SiteA	SiteA_SP_ResourceGroup1	SiteB

This action will reset the virtual machines (VMs) and the status of the replication plan to the ready state. When the VMware administrator performs a recovery operation, NetApp Disaster Recovery completes the following process:

1. It powers off each recovered VM in the FlexClone copy that was used for testing.
2. It deletes the FlexClone volume that was used to present the recovered VMs during the test.

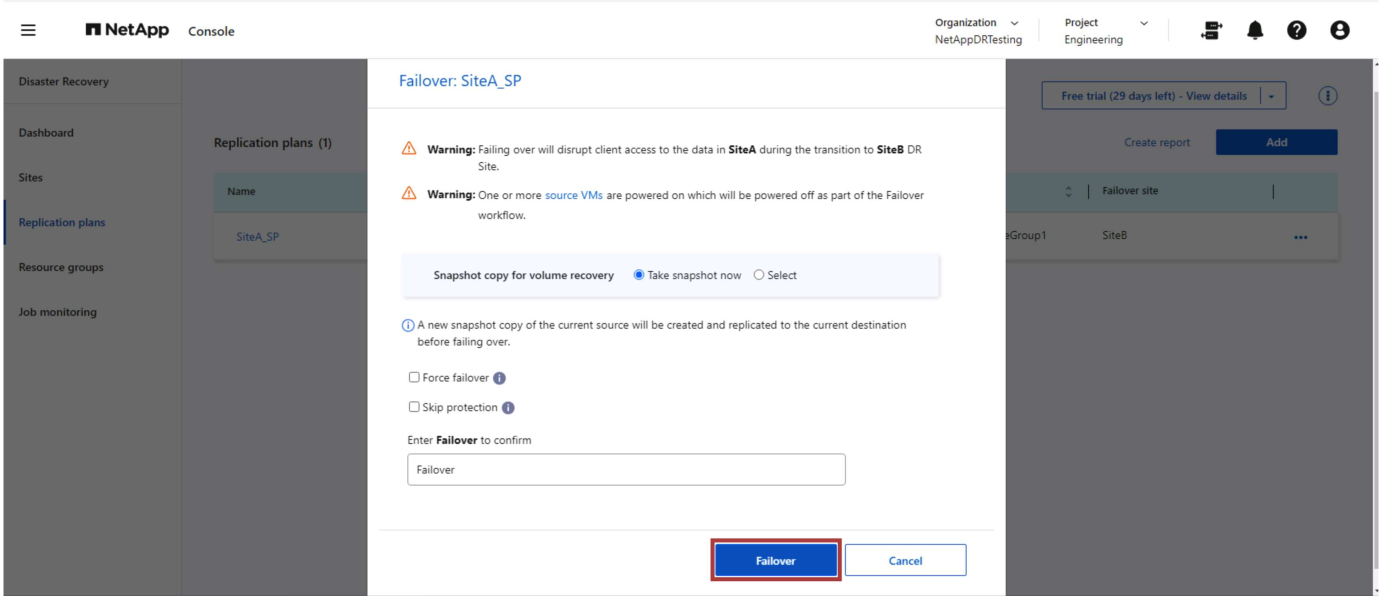
Planned Migration and Fail over

NetApp Disaster Recovery has two methods for performing a real failover: planned migration and fail over. The first method, planned migration, incorporates VM shutdown and storage replication synchronization into the process to recover or effectively move the VMs to the destination site. Planned migration requires access to the source site. The second method, failover, is a planned/unplanned failover in which the VMs are recovered at the destination site from the last storage replication interval that was able to complete. Depending on the RPO that was designed into the solution, some amount of data loss can be expected in the DR scenario.



Replication plans (1)

Name	Compliance status	Plan status	Protected site	Resource groups	Failover site
SiteA_SP	Healthy	Ready	SiteA	SiteA_SP_ResourceGroup1	SiteB



Failover: SiteA_SP

⚠ **Warning:** Failing over will disrupt client access to the data in **SiteA** during the transition to **SiteB** DR Site.

⚠ **Warning:** One or more source VMs are powered on which will be powered off as part of the Failover workflow.

Snapshot copy for volume recovery ● Take snapshot now ○ Select

ⓘ A new snapshot copy of the current source will be created and replicated to the current destination before failing over.

□ Force failover

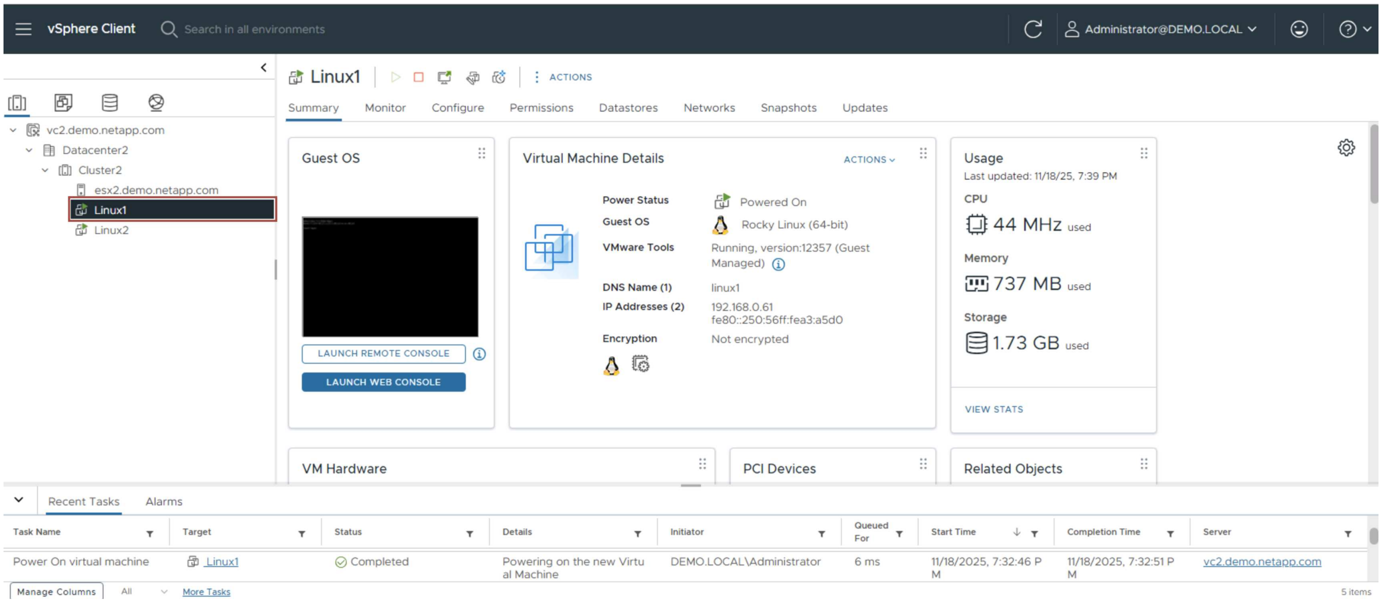
□ Skip protection

Enter **Failover** to confirm

Failover

When the VMware administrator performs a failover operation, NetApp Disaster Recovery automates the following tasks:

- Break and fail over the NetApp SnapMirror relationships.
- Connect the replicated datastores to the ESXi hosts at the DR site.
- Connect the VM network adapters to the appropriate destination site network.
- Reconfigure the VM guest operating system network settings as defined for the network at the destination site.
- Execute any custom commands (if any) that have been stored in the replication plan.
- Power on the VMs in the order that was defined in the replication plan.



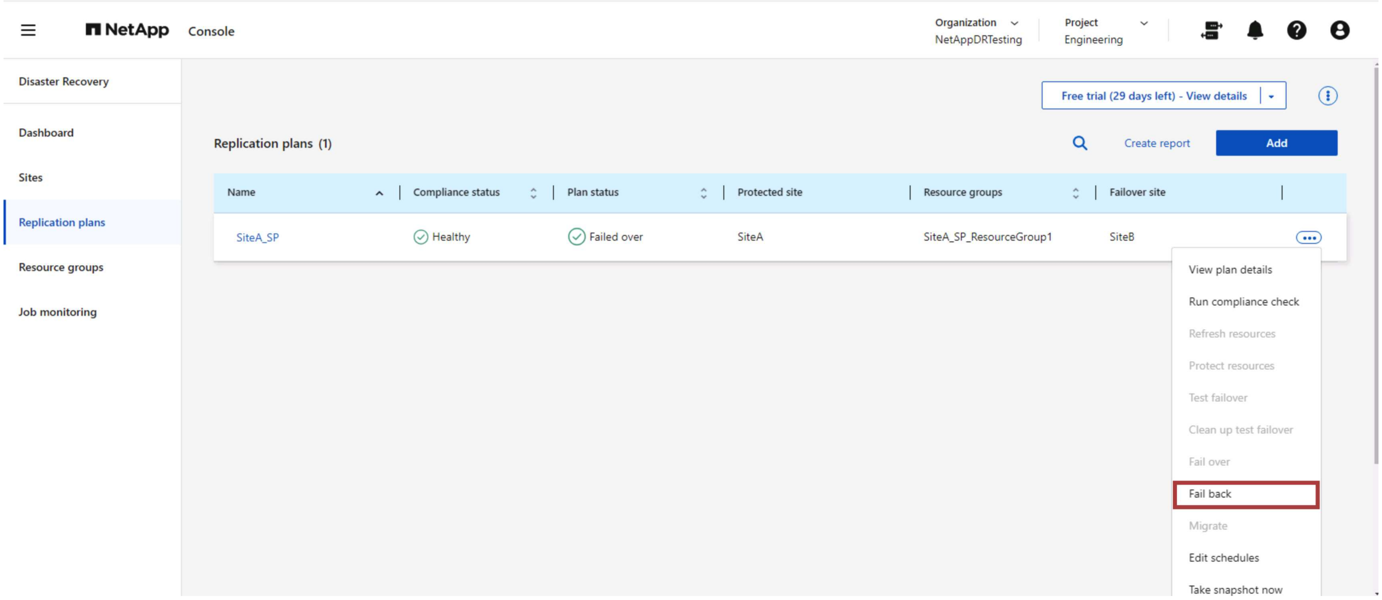
Power Status: Powered On
Guest OS: Rocky Linux (64-bit)
VMware Tools: Running, version:12357 (Guest Managed)
DNS Name (1): linux1
IP Addresses (2): 192.168.0.61, fe80::250:56ff:fea3:a5d0
Encryption: Not encrypted

Last updated: 11/18/25, 7:39 PM
CPU: 44 MHz used
Memory: 737 MB used
Storage: 1.73 GB used

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Power On virtual machine	Linux1	Completed	Powering on the new Virtual Machine	DEMO.LOCAL\Administrator	6 ms	11/18/2025, 7:32:46 PM	11/18/2025, 7:32:51 PM	vc2.demo.netapp.com

Failback

A failback is an optional procedure that restores the original configuration of the source and destination sites after a recovery.



Replication plans (1)

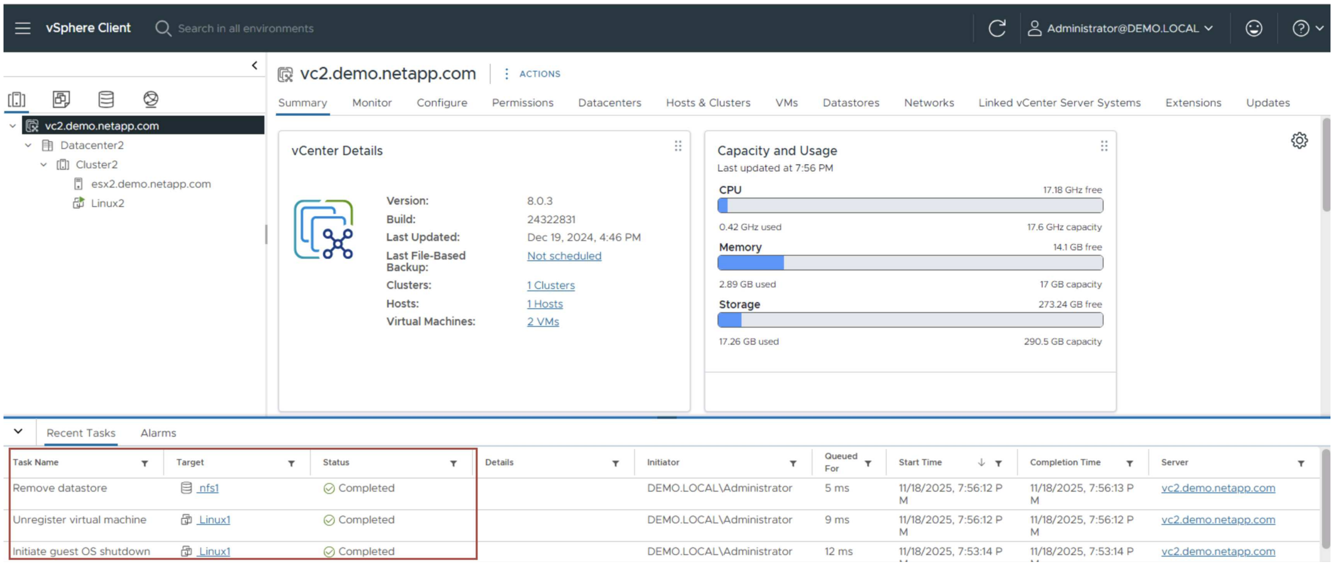
Name	Compliance status	Plan status	Protected site	Resource groups	Failover site
SiteA_SP	Healthy	Failed over	SiteA	SiteA_SP_ResourceGroup1	SiteB

VMware administrators can configure and run a failback procedure when they are ready to restore services to the original source site.

NetApp Disaster Recovery replicates (resyncs) any changes back to the original source virtual machine before reversing the replication direction.

This process starts from a relationship that has completed failing over to a target and involves the following steps:

- Power off and unregister the virtual machines and volumes on the destination site are unmounted.



vc2.demo.netapp.com

vCenter Details

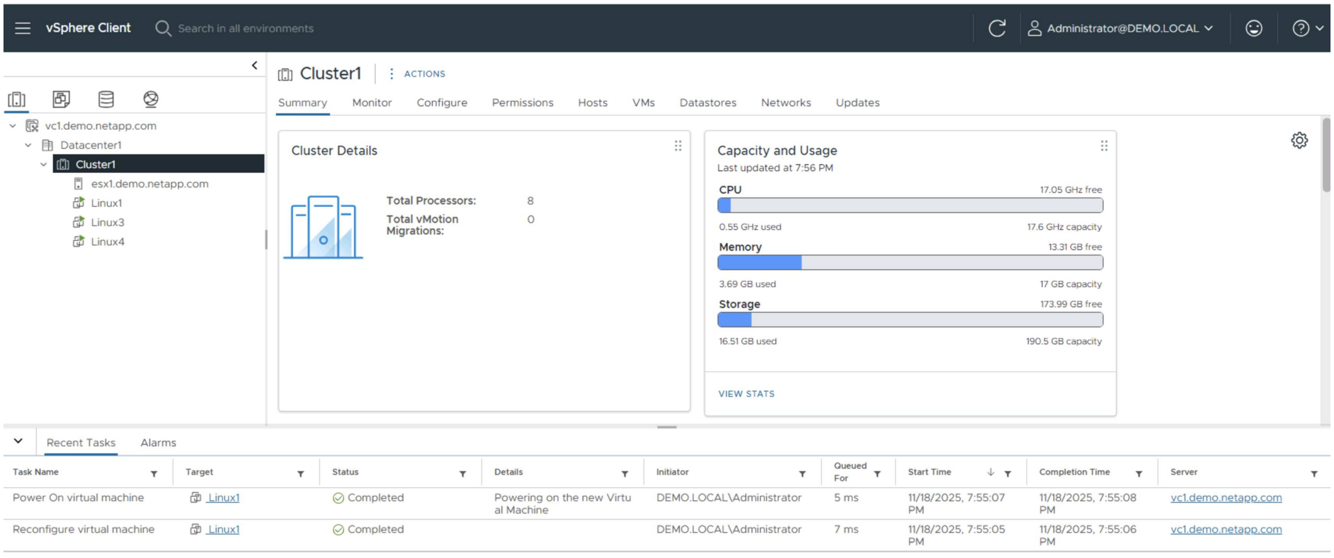
Version: 8.0.3
Build: 24322831
Last Updated: Dec 19, 2024, 4:46 PM
Last File-Based Backup: Not scheduled
Clusters: 1 Clusters
Hosts: 1 Hosts
Virtual Machines: 2 VMs

Capacity and Usage
Last updated at 7:56 PM

CPU: 17.18 GHz free; 0.42 GHz used; 17.6 GHz capacity
Memory: 14.1 GB free; 2.89 GB used; 17 GB capacity
Storage: 273.24 GB free; 17.26 GB used; 290.5 GB capacity

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Remove datastore	nfs1	Completed		DEMO.LOCAL\Administrator	5 ms	11/18/2025, 7:56:12 PM	11/18/2025, 7:56:13 PM	vc2.demo.netapp.com
Unregister virtual machine	Linux1	Completed		DEMO.LOCAL\Administrator	9 ms	11/18/2025, 7:56:12 PM	11/18/2025, 7:56:12 PM	vc2.demo.netapp.com
Initiate guest OS shutdown	Linux1	Completed		DEMO.LOCAL\Administrator	12 ms	11/18/2025, 7:53:14 P	11/18/2025, 7:53:14 P	vc2.demo.netapp.com

- Break the SnapMirror relationship on the original source is broken to make it read/write.
- Resynchronize the SnapMirror relationship to reverse the replication.
- Mount the volume on the source, power on and register the source virtual machines.



Total Processors: 8
Total vMotion Migrations: 0

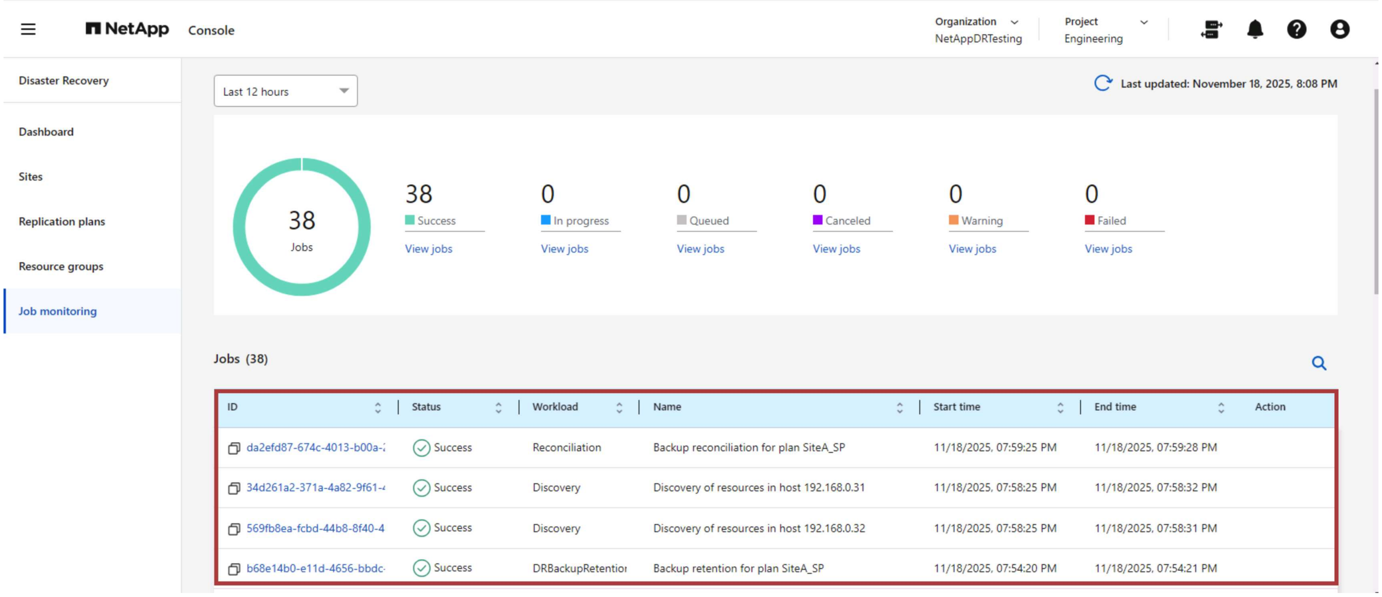
CPU		17.05 GHz free
0.55 GHz used		17.6 GHz capacity
Memory		13.31 GB free
3.69 GB used		17 GB capacity
Storage		173.99 GB free
16.51 GB used		190.5 GB capacity

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Power On virtual machine	Linux1	✓ Completed	Powering on the new Virtual Machine	DEMO.LOCAL\Administrator	5 ms	11/18/2025, 7:55:07 PM	11/18/2025, 7:55:08 PM	vc1.demo.netapp.com
Reconfigure virtual machine	Linux1	✓ Completed		DEMO.LOCAL\Administrator	7 ms	11/18/2025, 7:55:05 PM	11/18/2025, 7:55:06 PM	vc1.demo.netapp.com

For more details about accessing and configuring NetApp Disaster Recovery, see the Learn about NetApp Disaster Recovery for VMware.

Monitoring and Dashboard

From NetApp Disaster Recovery or the ONTAP CLI, you can monitor the replication health status for the appropriate datastore volumes, and the status of a failover or test failover can be tracked via Job Monitoring.



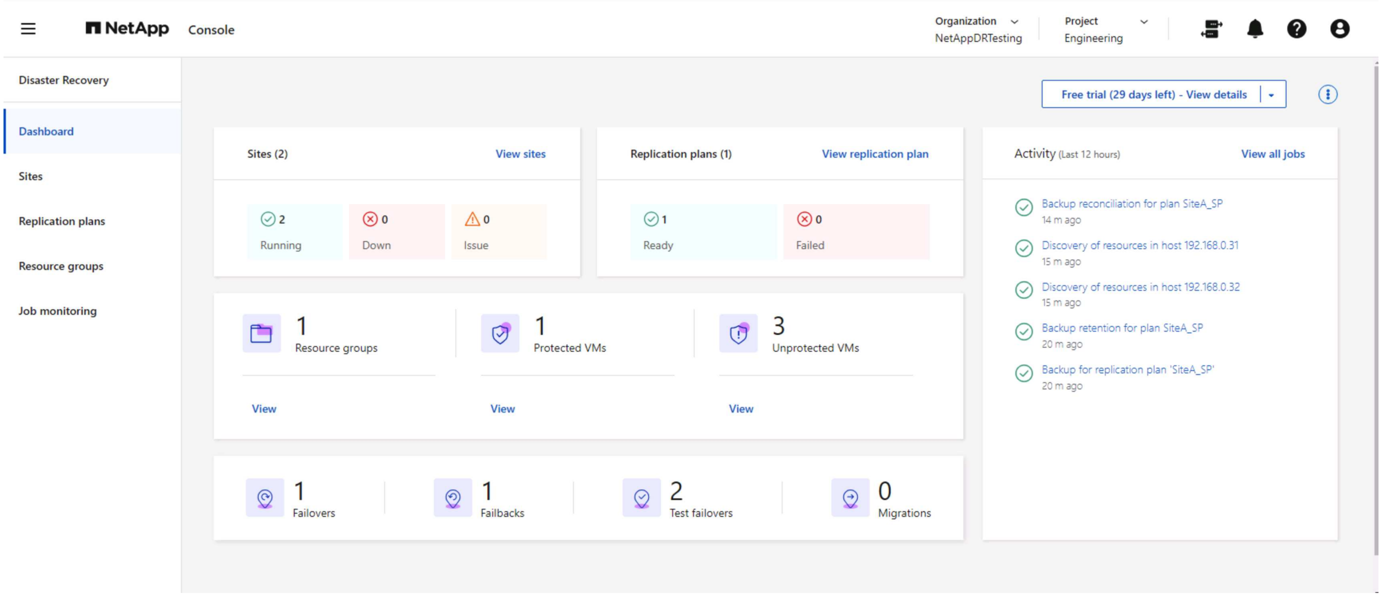
38	0	0	0	0	0
🟩 Success	🟦 In progress	⬜ Queued	🟪 Canceled	🟧 Warning	🟥 Failed

Jobs (38)

ID	Status	Workload	Name	Start time	End time	Action
da2efd87-674c-4013-b00a-:	✓ Success	Reconciliation	Backup reconciliation for plan SiteA_SP	11/18/2025, 07:59:25 PM	11/18/2025, 07:59:28 PM	
34d261a2-371a-4a82-9f61-4	✓ Success	Discovery	Discovery of resources in host 192.168.0.31	11/18/2025, 07:58:25 PM	11/18/2025, 07:58:32 PM	
569fb8ea-fcbd-44b8-8f40-4	✓ Success	Discovery	Discovery of resources in host 192.168.0.32	11/18/2025, 07:58:25 PM	11/18/2025, 07:58:31 PM	
b68e14b0-e11d-4656-bbdc-	✓ Success	DRBackupRetentior	Backup retention for plan SiteA_SP	11/18/2025, 07:54:20 PM	11/18/2025, 07:54:21 PM	

> If a job is currently in progress or queued, and you wish to stop it, there is an option to cancel it.

With the NetApp Disaster Recovery dashboard, confidently evaluate the status of disaster recovery sites and replication plans. This enables administrators to swiftly identify healthy, disconnected, or degraded sites and plans.



Backup reconciliation for plan SiteA_SP
14 m ago

Discovery of resources in host 192.168.0.31
15 m ago

Discovery of resources in host 192.168.0.32
15 m ago

Backup retention for plan SiteA_SP
20 m ago

Backup for replication plan 'SiteA_SP'
20 m ago

This provides a powerful solution to handle a tailored and customized disaster recovery plan. Failover can be done as planned failover or failover with a click of a button when disaster occurs and decision is made to activate the DR site.

Convert existing vSphere clusters to VCF

Learn about converting a vSphere environment with existing datastores to a VCF management domain

Converting a vSphere environment with existing Fibre Channel or NFS datastores on ONTAP involves integrating the current infrastructure into a modern private cloud architecture.

Solution overview

This solution demonstrates how existing FC or NFS datastores in vSphere become principal storage when the cluster is converted to a VCF management domain.

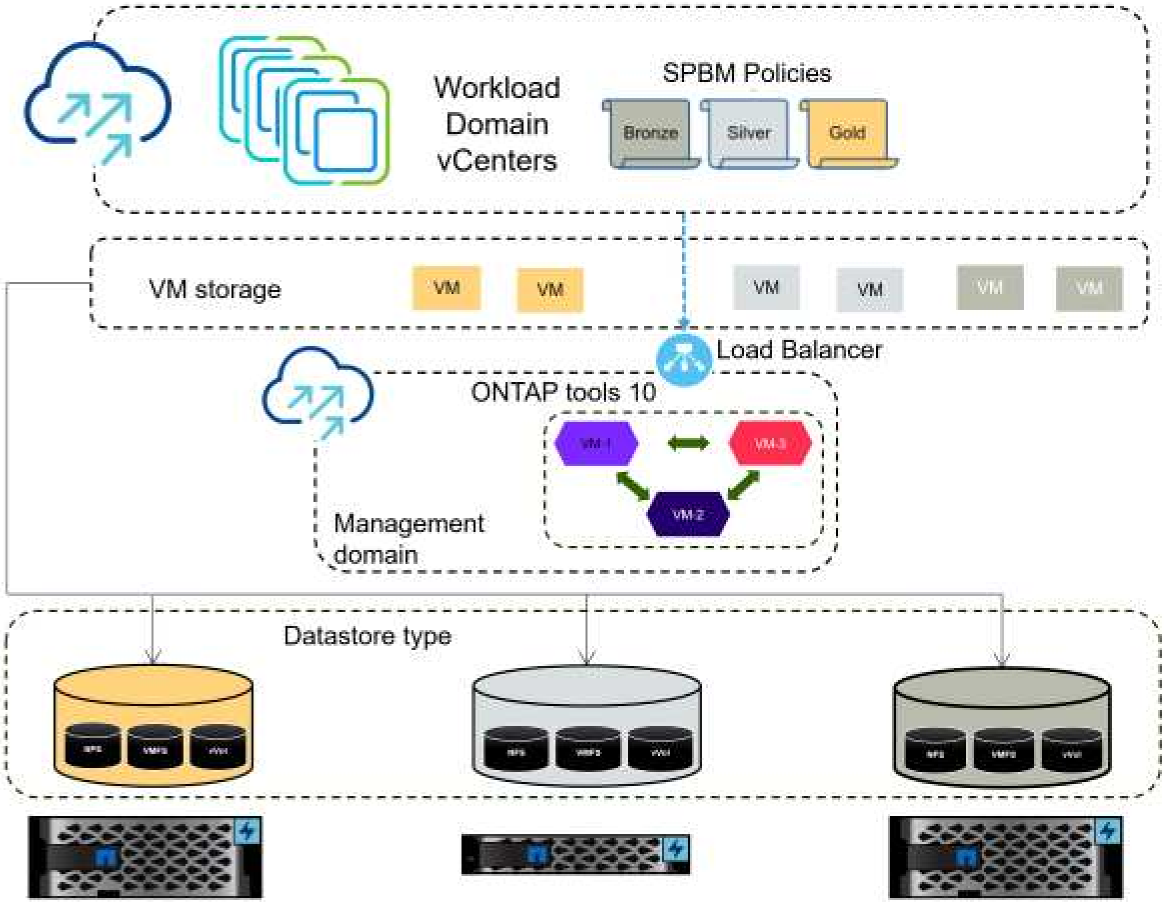
This process benefits from the robustness and flexibility of ONTAP storage to ensure seamless data access and management. After a VCF management domain is established through the conversion process, administrators can efficiently import additional vSphere environments, including those using both FC and NFS datastores, into the VCF ecosystem.

This integration not only enhances resource usage but also simplifies the management of private cloud infrastructure, ensuring a smooth transition with minimal disruption to existing workloads.

Architecture overview

The architecture of ONTAP tools integrates seamlessly with VMware environments, leveraging a modular and scalable framework that includes the ONTAP tools services, vSphere plug-in, and REST APIs to enable efficient storage management, automation, and data protection.

ONTAP tools for VMware vSphere can be installed in either HA or non-HA configurations.



Supported solutions for converting a vSphere environment

Refer to the following solutions for the technical details to convert a vCenter instance.

- Convert a vCenter instance to the VCF management domain (NFS datastore)
- Convert vCenter instance to the VCF management domain (FC datastore)

Additional information

- For video demos of these solutions, refer to VMware datastore provisioning with ONTAP.
- For an overview of the conversion process, refer to the Convert a vSphere environment to a management domain or Import a vSphere environment as a VI workload domain in VMware Cloud Foundation.
- For information on configuring ONTAP storage systems, refer to ONTAP 9 documentation.
- For information on configuring VCF, refer to VMware Cloud Foundation documentation.
- For supported storage and other considerations to convert or import vSphere to VCF 5.2, refer to Considerations before converting or importing existing vSphere environments into VMware Cloud Foundation.

Deployment workflow for converting vCenter server instances to VCF management domains with NFS datastores

Convert an existing vSphere 8 cluster with NetApp ONTAP NFS datastores to a VMware

Cloud Foundation management domain. You’ll review configuration requirements, deploy ONTAP tools and provision NFS datastores, and use the VCF Import Tool to validate and convert the cluster.

For an overview of the conversion process, refer to the VMware documentation: Convert a vSphere environment to a management domain or Import a vSphere environment as a VI workload domain in VMware Cloud Foundation.

① **Review the configuration requirements**

Review the key requirements for converting vCenter server instances to VCF management domains using NFS datastores.

② **Deploy ONTAP tools and provision an NFS datastore**

Deploy ONTAP tools for VMware vSphere and provision an NFS datastore.

③ **Convert vSphere cluster to VCF management domain**

Use the VCF Import Tool to validate and convert the vSphere 8 to the VCF management domain.

Deployment workflow for converting vCenter server instances to VCF management domains with Fibre Channel datastores

Convert an existing vSphere 8 cluster with NetApp ONTAP Fibre Channel (FC) datastores to a VMware Cloud Foundation management domain. You’ll review configuration requirements, deploy ONTAP tools and provision FC datastores, and use the VCF Import Tool to validate and convert the cluster.

For an overview of the conversion process, refer to the VMware documentation: Convert a vSphere environment to a management domain or Import a vSphere environment as a VI workload domain in VMware Cloud Foundation.

① **Review the configuration requirements**

Review the key requirements for converting vCenter server instances to VCF management domains using FC datastores.

② **Deploy ONTAP tools and provision a FC datastore**

Deploy ONTAP tools for VMware vSphere and provision a FC datastore.

③ **Convert vSphere cluster to VCF management domain**

Use the VCF Import Tool to validate and convert the vSphere 8 cluster to the VCF management domain.

Provision VCF with principal storage

Provision a VCF environment with ONTAP as the principal storage solution

NetApp ONTAP storage is an ideal primary storage solution for VMware Cloud Foundation (VCF) management and Virtual Infrastructure (VI) workload domains. ONTAP delivers high performance, scalability, advanced data management, and seamless integration to improve operational efficiency and data protection.

Please refer to the following solutions for the technical details of provisioning a VCF environment in the appropriate domain and with the appropriate protocol.

- Management Domain with FC
- Management Domain with NFS
- Virtual Infrastructure Workload Domain with FC
- Virtual Infrastructure Workload Domain with NFS

Use an FC-based VMFS datastore on ONTAP as principal storage for VCF management domain

In this use case we outline the procedure to use an existing FC-based VMFS datastore on ONTAP as the primary storage for VMware Cloud Foundation (VCF) management domains. This procedure summarizes the required components, configurations, and deployment steps.

Introduction

Where appropriate we will refer to external documentation for the steps that must be performed in VCF's SDDC Manager, and reference those steps that are specific to the storage configuration portion.

For information on converting an existing FC-based vSphere environment with ONTAP, refer to Convert vSphere Environment (FC datastore) to VCF Management Domain.

> ⓘ VCF release 5.2 introduced the the capability to convert an existing vSphere 8 environment to a VCF management domain or import as VCF VI workload domains. Prior to this release, VMware vSAN was the only option for principal storage for the VCF management domain.

> ⓘ This solution is applicable for ONTAP platforms supporting FC storage including NetApp ASA, AFF and FAS.

Prerequisites

The following components and configurations are used in this scenario:

- NetApp storage system with a storage virtual machine (SVM) configured to allow FC traffic.
- Logical interfaces (LIF) have been created on the FC fabric that is to carry FC traffic and is associated with the SVM.
- Zoning has been configured to use single initiator-target zoning on FC switches for host HBAs and storage

targets.

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

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

Deployment Steps

Management Domain - Default Cluster

FC Principal storage on the initial cluster is only supported with VCF brownfield import tool. If VCF is deployed with Cloud Builder tool (priort to release version 5.2.x), only vSAN is supported.

For more information on using an existing vSphere environment, refer to converting existing vSphere environment to management domain for more info.

Management Domain - Additional Cluster

The additional vSphere cluster on management domain can be deployed with following options:

- Have additional cluster in vSphere environment and use the VCF brownfield import tool to convert the vSphere environment to Management domain. ONTAP tools for VMware vSphere System Manager or ONTAP API can be used to deploy the VMFS datastore to vSphere cluster.
- Use SDDC API to deploy additional cluster. The vSphere hosts should have the VMFS datastore configured. Use System Manager or ONTAP API to deploy LUN to vSphere hosts.
- Use SDDC Manager UI to deploy additional cluster. But this option only creates VSAN datastore till version 5.2.x.

Additional information

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

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

Use an NFS datastore on ONTAP as principal storage for VCF management domain

In this use case we outline the procedure to use an existing NFS datastore on ONTAP as the primary storage for VMware Cloud Foundation (VCF) management domains. This procedure summarizes the required components, configuration steps, and deployment process.

Introduction

Where appropriate we will refer to external documentation for the steps that must be performed in VCF's SDDC Manager, and reference those steps that are specific to the storage configuration portion.

For information on converting an existing NFS-based vSphere environment with ONTAP, refer to Convert vSphere Environment (NFS datastore) to VCF Management Domain.

> ⓘ VCF release 5.2 introduced the the capability to convert an existing vSphere 8 environment to a VCF management domain or import as VCF VI workload domains. Prior to this release, VMware vSAN was the only option for principal storage for the VCF management domain.

This solution is applicable for ONTAP platforms supporting NFS storage including NetApp AFF and FAS.

Prerequisites

The following components and configurations are used in this scenario:

- NetApp storage system with a storage virtual machine (SVM) configured to allow NFS traffic.
- Logical interface (LIF) has been created on the IP network that is to carry NFS traffic and is associated with the SVM.
- A vSphere 8 cluster with 4 x ESXi hosts and a vCenter appliance colocated on the cluster.
- Distributed port group configured for vMotion and NFS storage traffic on the VLANs or network segments established for this purpose.
- Download software required for the VCF conversion.

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

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

Deployment Steps

Management Domain - Default Cluster

NFS Principal storage on the initial cluster is only supported with VCF brownfield import tool. If VCF is deployed with Cloud Builder tool (till version 5.2.x), only VSAN is supported.

For more information on using an existing vSphere environment, refer to converting existing vSphere environment to management domain for more info.

Management Domain - Additional Cluster

The additional vSphere cluster on management domain can be deployed with following options:

- Have additional cluster in vSphere environment and use the VCF brownfield import tool to convert the vSphere environment to Management domain. ONTAP tools for VMware vSphere System Manager or ONTAP API can be used to deploy the NFS datastore to vSphere cluster.
- Use SDDC API to deploy additional cluster. The vSphere hosts should have the NFS datastore configured. Use System Manager or ONTAP API to deploy LUN to vSphere hosts.
- Use SDDC Manager UI to deploy additional cluster. But this option only creates vSAN datastore with releases prior to 5.2.x.

Additional information

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

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

Use an FC-based VMFS datastore on ONTAP as principal storage for a VI workload domain

In this use case we outline the procedure to set up a Fibre Channel (FC) VMFS datastore on ONTAP as the primary storage solution for a VMware Cloud Foundation (VCF) Virtual Infrastructure (VI) workload domain. This procedure summarizes the required components, configuration steps, and deployment process.

Benefits of Fibre Channel

High Performance: FC provides high-speed data transfer rates, making it ideal for applications requiring fast and reliable access to large amounts of data.

Low Latency: Very low latency, which is crucial for performance-sensitive applications like databases and virtualized environments.

Reliability: FC networks are known for their robustness and reliability, with features like built-in redundancy and error correction.

Dedicated Bandwidth: FC provides dedicated bandwidth for storage traffic, reducing the risk of network congestion.

For more information on using Fibre Channel with NetApp storage systems, refer to SAN Provisioning with FC.

Scenario Overview

This scenario covers the following high level steps:

- Create a storage virtual machine (SVM) with logical interfaces (LIFs) for FC traffic.
- Collect WWPN information of hosts to be deployed and create corresponding initiator groups on the ONTAP storage system.
- Create an FC volume on the ONTAP storage system.
- Map initiator groups to create FC volume
- Utilize single initiator-target zoning on FC switches. Create one zone for each initiator (single initiator zone).
    - For each zone, include a target that is the ONTAP FC logical interface (WWPN) for the SVMs. There should be at least two logical interfaces per node per SVM. Do not use the WWPN of the physical ports.
- Create a Network Pool for vMotion traffic in SDDC Manager.
- Commission hosts in VCF for use in a VI Workload Domain.
- Deploy a VI Workload Domain in VCF using an FC datastore as principal storage.

> ⓘ This solution is applicable for ONTAP platforms supporting NFS storage including NetApp AFF and FAS.

Prerequisites

The following components and configurations are used in this scenario:

- An ONTAP AFF or ASA storage system with FC ports connected to FC switches.
- SVM created with FC lifs.
- vSphere with FC HBAs connected to FC switches.

- Single initiator-target zoning is configured on FC switches.

NetApp recommends multipath for FC LUNs.

Deployment Steps

Management Domain - Default Cluster

FC Principal storage on initial cluster is only supported with the VCF brownfield import tool. If VCF is deployed with the cloudbuilder tool (till version 5.2.x), only VSAN is supported. Refer converting existing vSphere environment to management domain for more info.

Management Domain - Additional Cluster

The additional vSphere cluster on management domain can be deployed with following options:
* Have additional cluster in vSphere environment and use the VCF brownfield import tool to convert the vSphere environment to Management domain. ONTAP tools for VMware vSphere, System Manager or ONTAP API can be used to deploy the VMFS datastore to vSphere cluster.
* Use SDDC API to deploy additional cluster. The vSphere hosts should have the VMFS datastore configured. Use System Manager or ONTAP API to deploy LUN to vSphere hosts.
* Use SDDC Manager UI to deploy additional cluster. But this option only creates VSAN datastore till version 5.2.x.

VI Workload Domain - Default Cluster

After the management domain is up and running, VI Workload domain can be created:

- Using SDDC Manager UI. The vSphere hosts should have the VMFS datastore configured. Use System Manager or ONTAP API to deploy LUN to vSphere hosts.
- Import an existing vSphere environment as new VI workload domain. ONTAP tools for VMware vSphere, System Manager or ONTAP API can be used to deploy the VMFS datastore to vSphere cluster.

VI Workload Domain - Additional Cluster

Once VI workload is up and running, additional clusters can be deployed with VMFS on FC LUN using the following options.

- Additional clusters in vSphere environment imported using VCF brownfield import tool. ONTAP tools for VMware vSphere, System Manager or ONTAP API can be used to deploy the VMFS datastore to vSphere cluster.
- Using SDDC Manager UI or API to deploy additional cluster. The vSphere hosts should have the VMFS datastore configured. Use System Manager or ONTAP API to deploy LUN to vSphere hosts.

Additional information

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

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

Use an NFS datastore on ONTAP as principal storage for a VI workload domain

In this use case we outline the procedure to configure an NFS datastore on ONTAP as the primary storage solution for a VMware Cloud Foundation (VCF) Virtual Infrastructure

(VI) workload domain. This procedure summarizes the required components, configuration steps, and deployment process.

Benefits of NFS

Simplicity and Ease of Use: NFS is straightforward to set up and manage, making it an excellent choice for environments that require quick and easy file sharing.

Scalability: ONTAP’s architecture allows NFS to scale efficiently, supporting growing data needs without significant changes to the infrastructure.

Flexibility: NFS supports a wide range of applications and workloads, making it versatile for various use cases, including virtualized environments.

For more information, refer to the NFS v3 Reference Guide for vSphere 8.

For more information on using Fibre Channel with NetApp storage systems, refer to NFS v3 Reference Guide for vSphere 8.

Scenario Overview

This scenario covers the following high level steps:

- Create a storage virtual machine (SVM) with logical interface (LIFs) for NFS straffic
- Verify networking for the ONTAP storage virtual machine (SVM) and that a logical interface (LIF) is present to carry NFS traffic.
- Create an export policy to allow the ESXi hosts access to the NFS volume.
- Create an NFS volume on the ONTAP storage system.
- Create a Network Pool for NFS and vMotion traffic in SDDC Manager.
- Commission hosts in VCF for use in a VI Workload Domain.
- Deploy a VI Workload Domain in VCF using an NFS datastore as principal storage.
- Install NetApp NFS Plug-in for VMware VAAI

> ⓘ This solution is applicable for ONTAP platforms supporting NFS storage including NetApp AFF and FAS.

Prerequisites

The following components and configurations are used in this scenario:

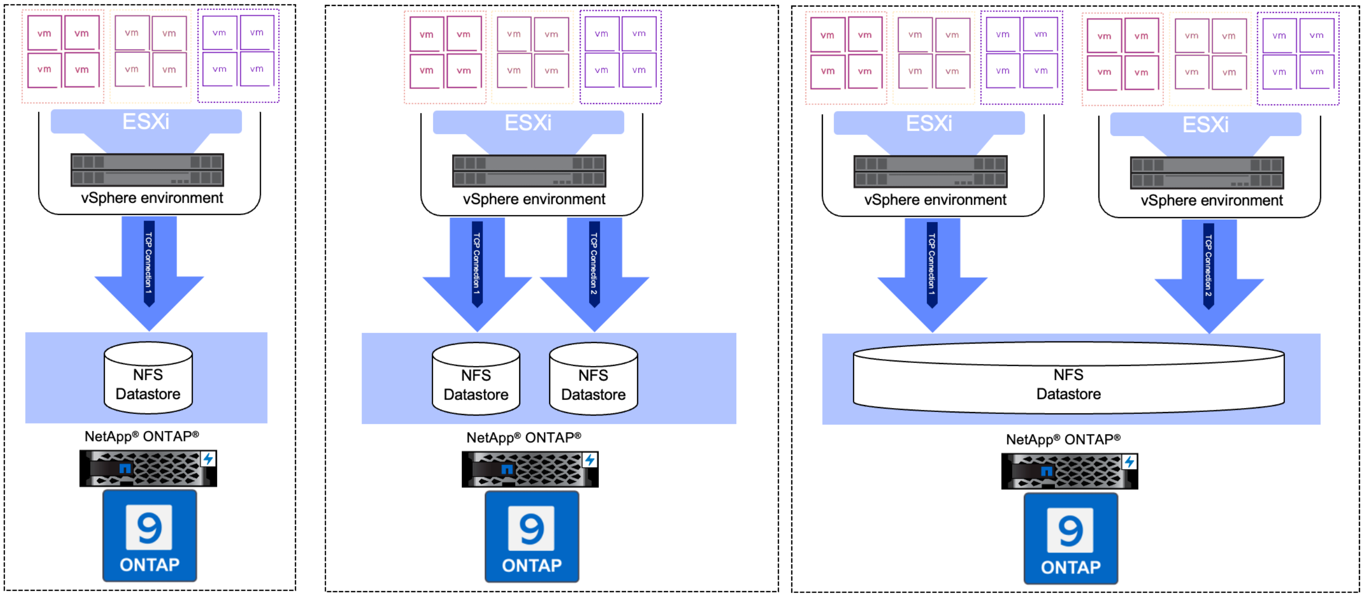
- NetApp AFF storage system with a storage virtual machine (SVM) configured to allow NFS traffic.
- Logical interface (LIF) has been created on the IP network that is to carry NFS traffic and is associated with the SVM.
- VCF management domain deployment is complete and the SDDC Manager interface is accessible.
- 4 x ESXi hosts configured for communication on the VCF management network.
- IP addresses reserved for vMotion and NFS storage traffic on the VLAN or network segment established for this purpose.

> When deploying a VI Workload Domain, VCF validates connectivity to the NFS Server. This is done using the management adapter on the ESXi hosts before any additional vmkernel adapter is added with the NFS IP address. Therefore, it is necessary to ensure that either 1) the management network is routable to the NFS Server, or 2) a LIF for the management network has been added to the SVM hosting the NFS datastore volume, to ensure that the validation can proceed.

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

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

For more information on using NFS with vSphere clusters, refer to the NFS v3 Reference Guide for vSphere 8.



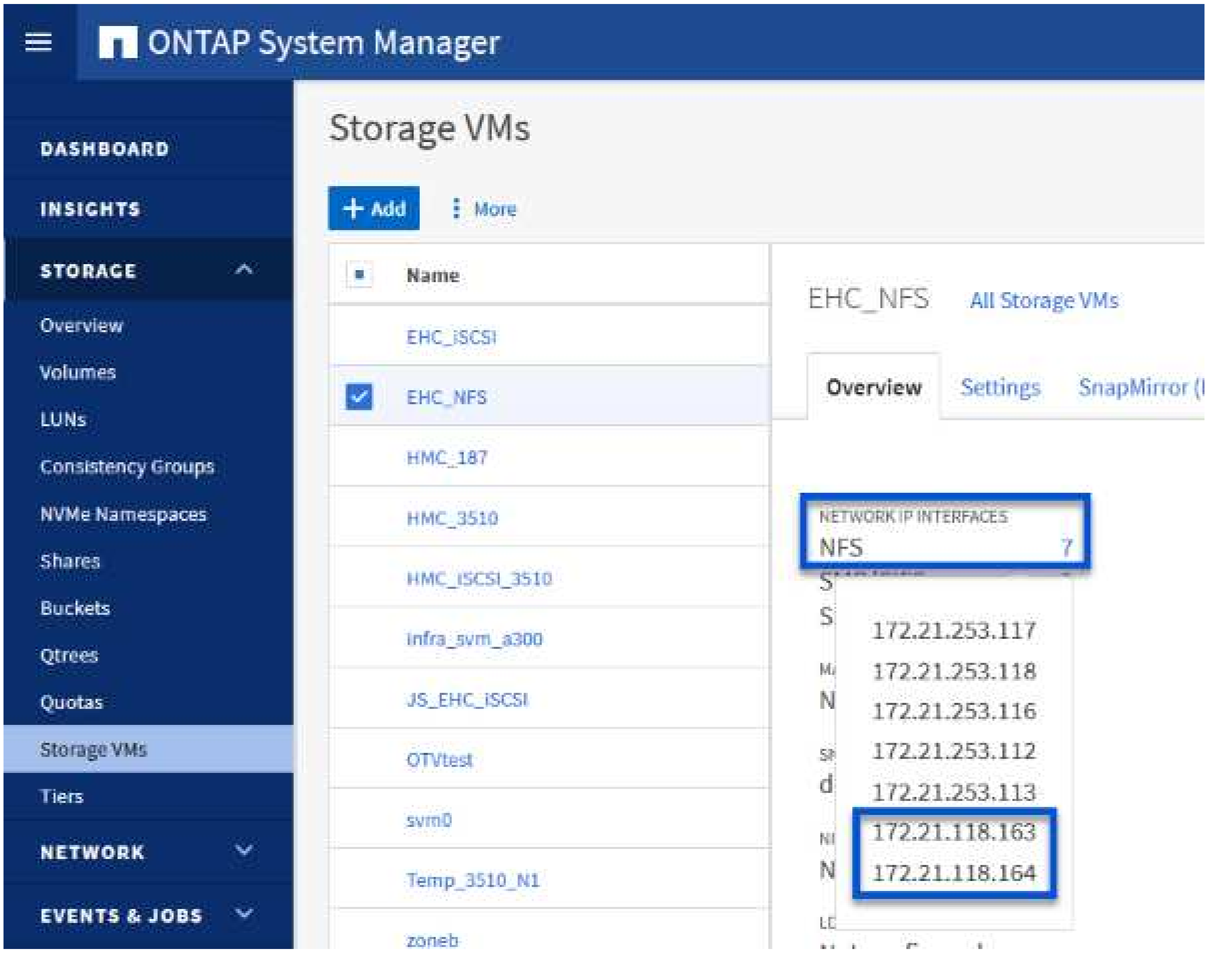
Deployment Steps

To deploy a VI Workload Domain with an NFS datastore as principal storage, complete the following steps:

Verify networking for ONTAP SVM

Verify that the required logical interfaces have been established for the network that will carry NFS traffic between the ONTAP storage cluster and VI Workload Domain.

1. From ONTAP System Manager navigate to **Storage VMs** in the left-hand menu and click on the SVM to be used for NFS traffic. On the **Overview** tab, under **NETWORK IP INTERFACES**, click on the numeric to the right of **NFS**. In the list verify that the required LIF IP addresses are listed.



Alternately, verify the LIFs associated with an SVM from the ONTAP CLI with the following command:

```
network interface show -vserver <SVM_NAME>
```

1. Verify that the ESXi hosts can communicate to the ONTAP NFS Server. Log into the ESXi host via SSH and ping the SVM LIF:

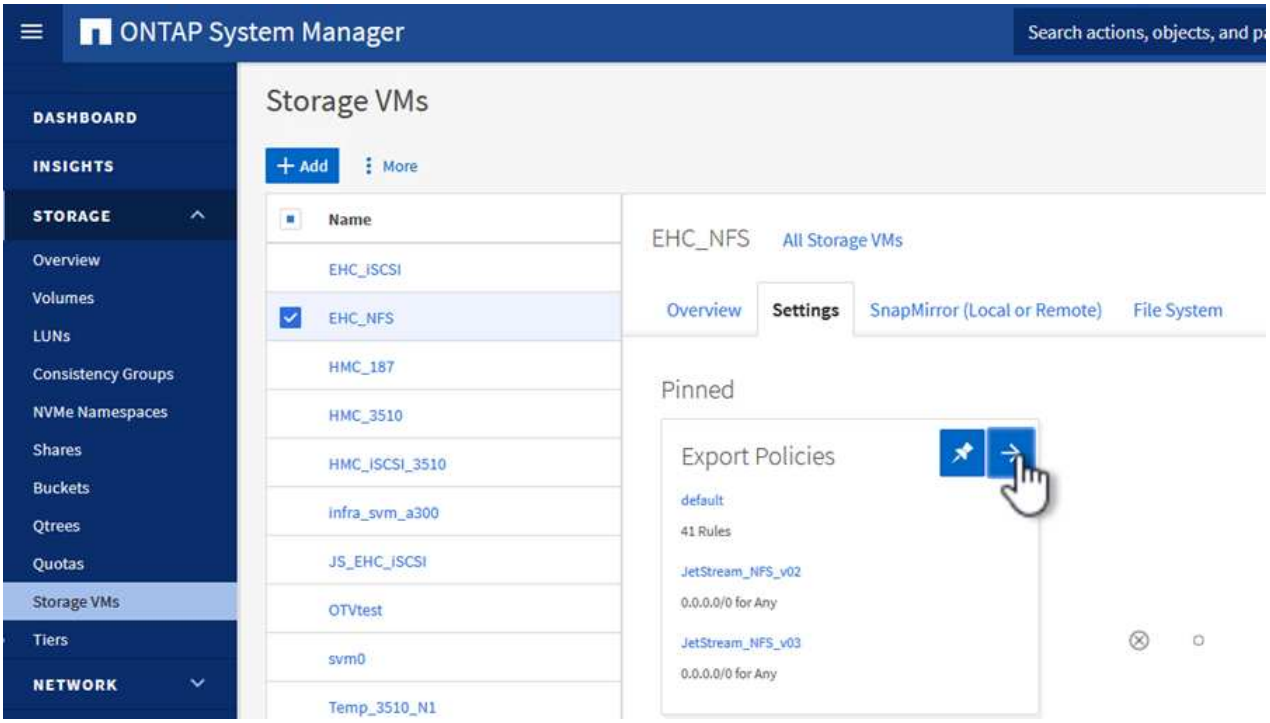
```
vmkping <IP Address>
```

When deploying a VI Workload Domain, VCF validates connectivity to the NFS Server. This is done using the management adapter on the ESXi hosts before any additional vmkernel adapter is added with the NFS IP address. Therefore, it is necessary to ensure that either 1) the management network is routable to the NFS Server, or 2) a LIF for the management network has been added to the SVM hosting the NFS datastore volume, to ensure that the validation can proceed.

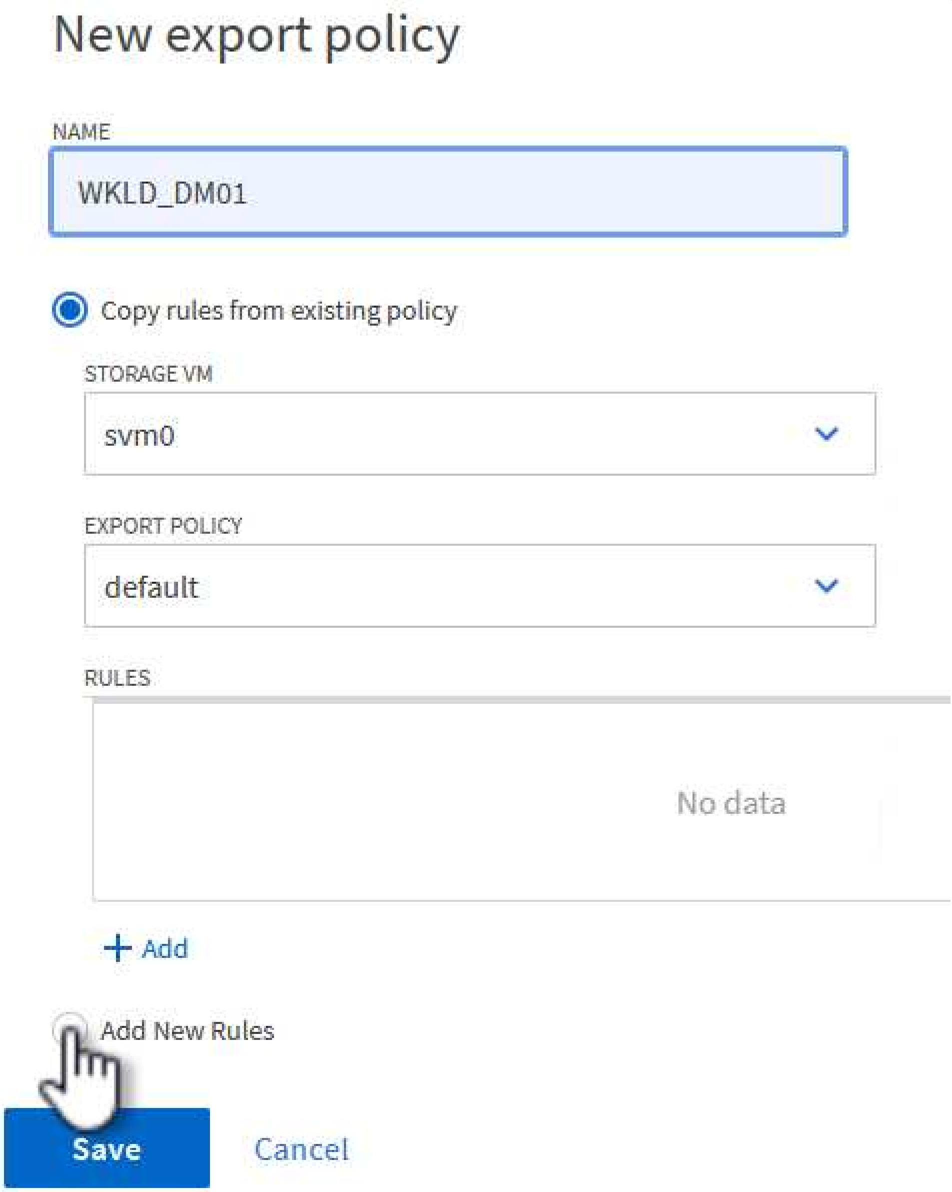
Create Export Policy for sharing NFS volume

Create an export policy in ONTAP System Manager to define access control for NFS volumes.

1. In ONTAP System Manager click on **Storage VMs** in the left-hand menu and select an SVM from the list.
2. On the **Settings** tab locate **Export Policies** and click on the arrow to access.



3. In the **New export policy** window add a name for the policy, click on the **Add new rules** button and then on the **+Add** button to begin adding a new rule.



New export policy

NAME

WKLD_DM01

● Copy rules from existing policy

STORAGE VM

svm0

EXPORT POLICY

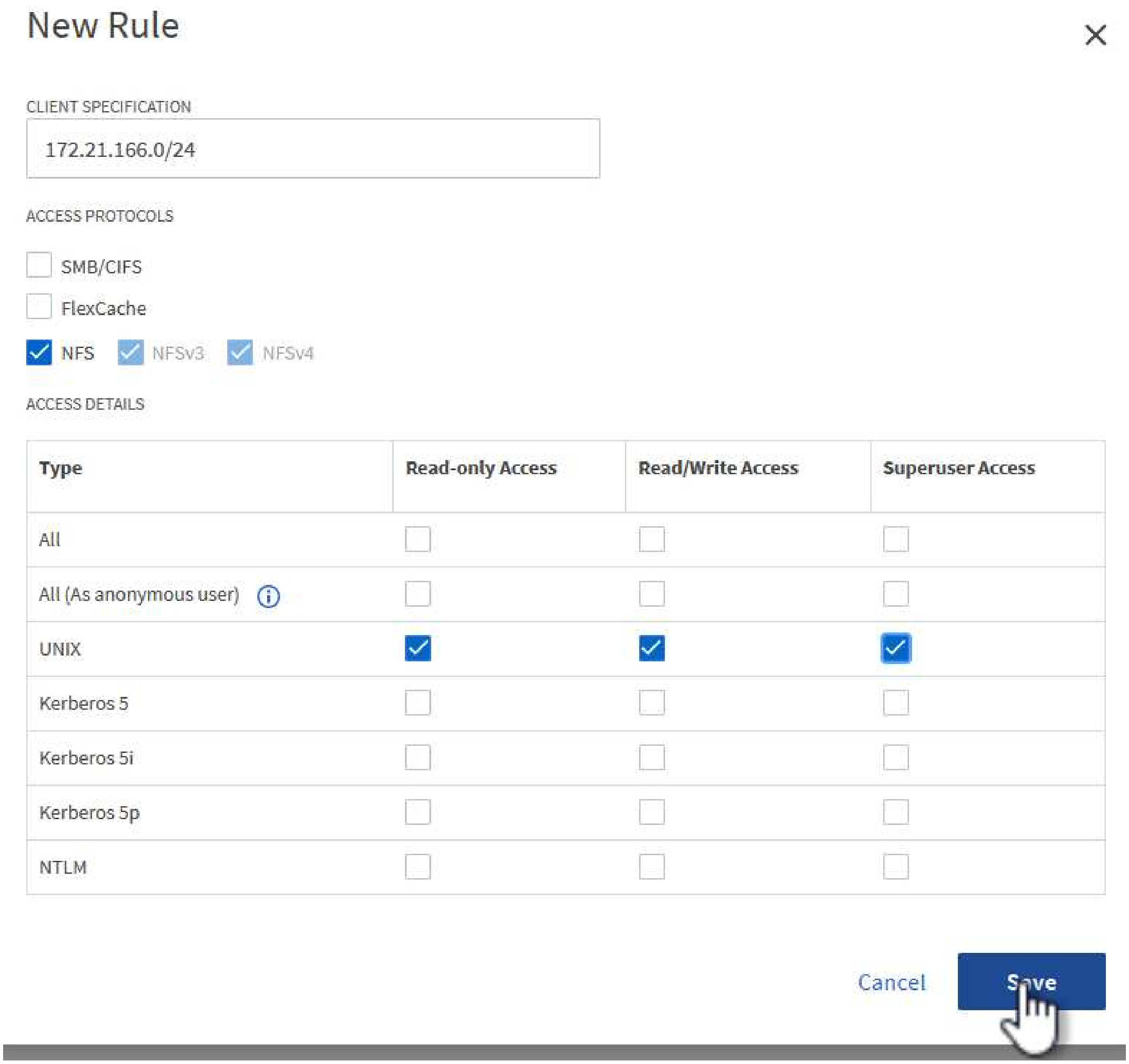
default

RULES

No data

○ Add New Rules

4. Fill in the IP Addresses, IP address range, or network that you wish to include in the rule. Uncheck the **SMB/Cifs** and **FlexCache** boxes and make selections for the access details below. Selecting the UNIX boxes is sufficient for ESXi host access.



New Rule

CLIENT SPECIFICATION

172.21.166.0/24

ACCESS PROTOCOLS

□ SMB/CIFS

□ FlexCache

☑ NFS ☑ NFSv3 ☑ NFSv4

ACCESS DETAILS

Type	Read-only Access	Read/Write Access	Superuser Access
All	□	□	□
All (As anonymous user)	□	□	□
UNIX	☑	☑	☑
Kerberos 5	□	□	□
Kerberos 5i	□	□	□
Kerberos 5p	□	□	□
NTLM	□	□	□

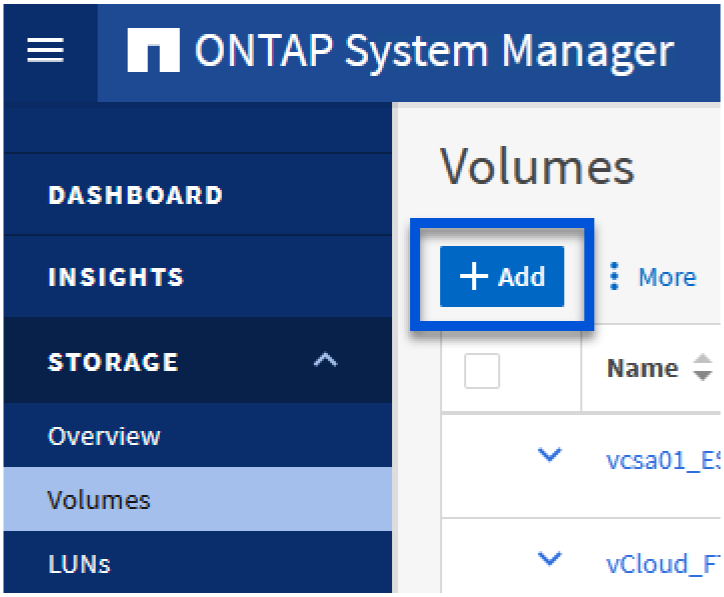
> When deploying a VI Workload Domain, VCF validates connectivity to the NFS Server. This is done using the management adapter on the ESXi hosts before any additional vmkernel adapter is added with the NFS IP address. Therefore, it is necessary to ensure that the export policy includes the VCF management network in order to allow the validation to proceed.

5. Once all rules have been entered click on the **Save** button to save the new Export Policy.
6. Alternately, you can create export policies and rules in the ONTAP CLI. Refer to the steps for creating an export policy and adding rules in the ONTAP documentation.
   - Use the ONTAP CLI to Create an export policy.
   - Use the ONTAP CLI to Add a rule to an export policy.

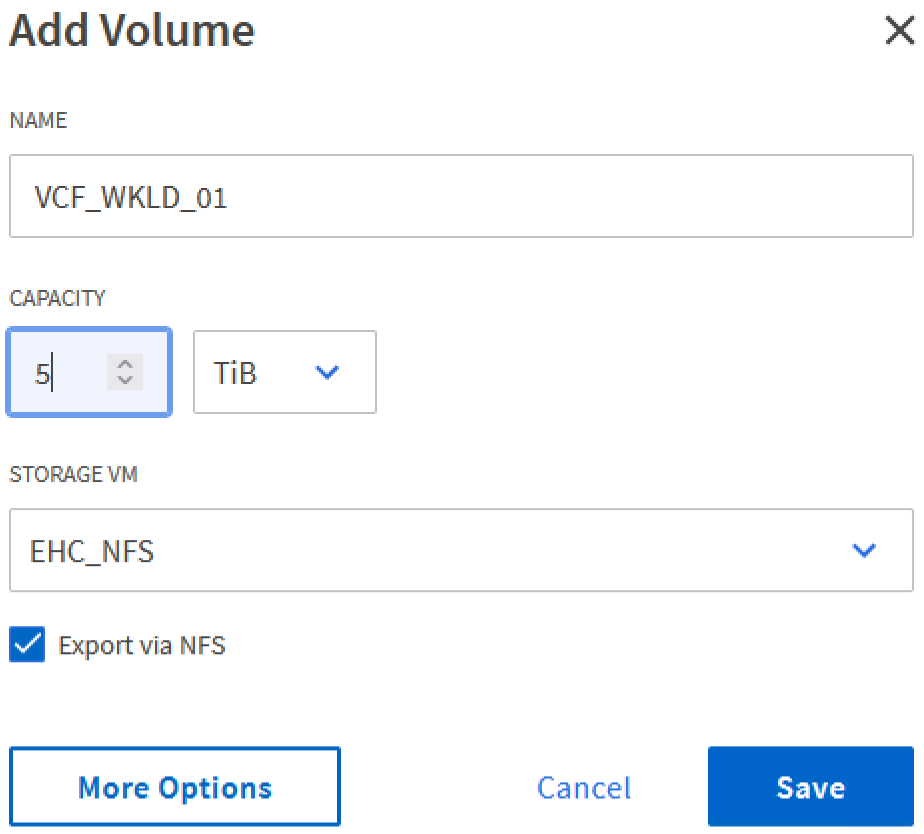
Create NFS volume

Create an NFS volume on the ONTAP storage system to be used as a datastore in the Workload Domain deployment.

1. From ONTAP System Manager navigate to **Storage > Volumes** in the left-hand menu and click on **+Add** to create a new volume.



2. Add a name for the volume, fill out the desired capacity and selection the storage VM that will host the volume. Click on **More Options** to continue.



Add Volume

NAME

VCF_WKLD_01

CAPACITY

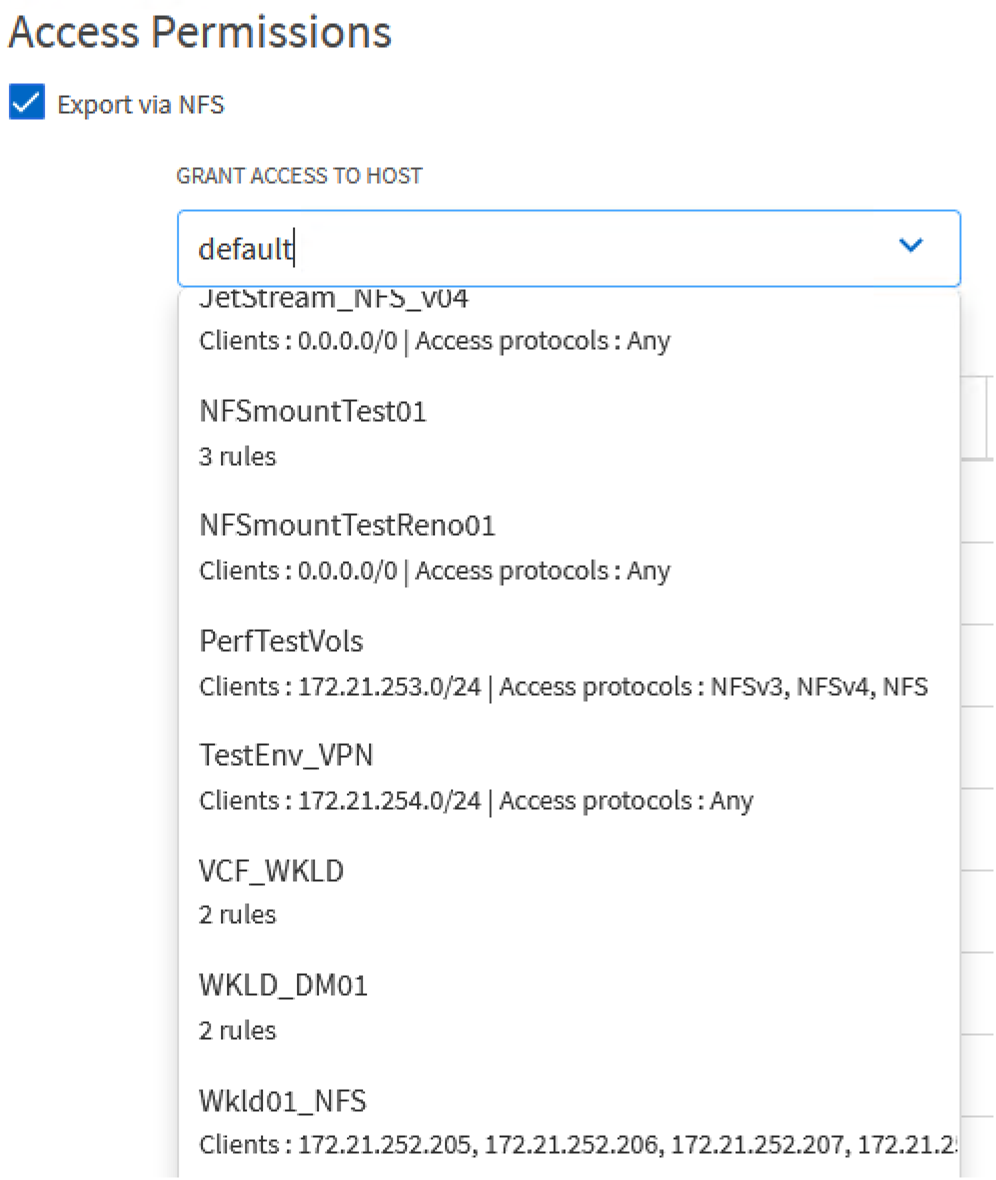
5 TiB

STORAGE VM

EHC_NFS

☑ Export via NFS

3. Under Access Permissions, select the Export Policy which includes the VCF management network or IP address and NFS network IP addresses that will be used for both validation of the NFS Server and NFS traffic.



Access Permissions

☑ Export via NFS

GRANT ACCESS TO HOST

default

JetStream_NFS_v04
Clients : 0.0.0.0/0 | Access protocols : Any

NFSmountTest01
3 rules

NFSmountTestReno01
Clients : 0.0.0.0/0 | Access protocols : Any

PerfTestVols
Clients : 172.21.253.0/24 | Access protocols : NFSv3, NFSv4, NFS

TestEnv_VPN
Clients : 172.21.254.0/24 | Access protocols : Any

VCF_WKLD
2 rules

WKLD_DM01
2 rules

Wkld01_NFS
Clients : 172.21.252.205, 172.21.252.206, 172.21.252.207, 172.21.2

+

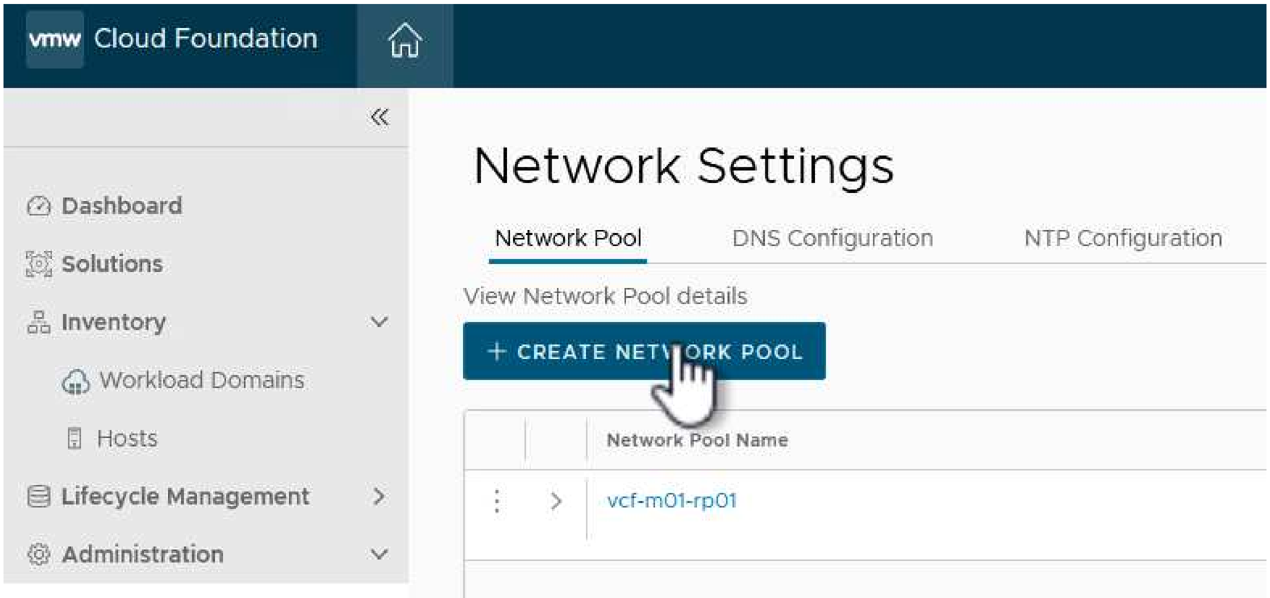
When deploying a VI Workload Domain, VCF validates connectivity to the NFS Server. This is done using the management adapter on the ESXi hosts before any additional vmkernel adapter is added with the NFS IP address. Therefore, it is necessary to ensure that either 1) the management network is routable to the NFS Server, or 2) a LIF for the management network has been added to the SVM hosting the NFS datastore volume, to ensure that the validation can proceed.

4. Alternately, ONTAP Volumes can be created in the ONTAP CLI. For more information refer to the lun create command in the ONTAP commands documentation.

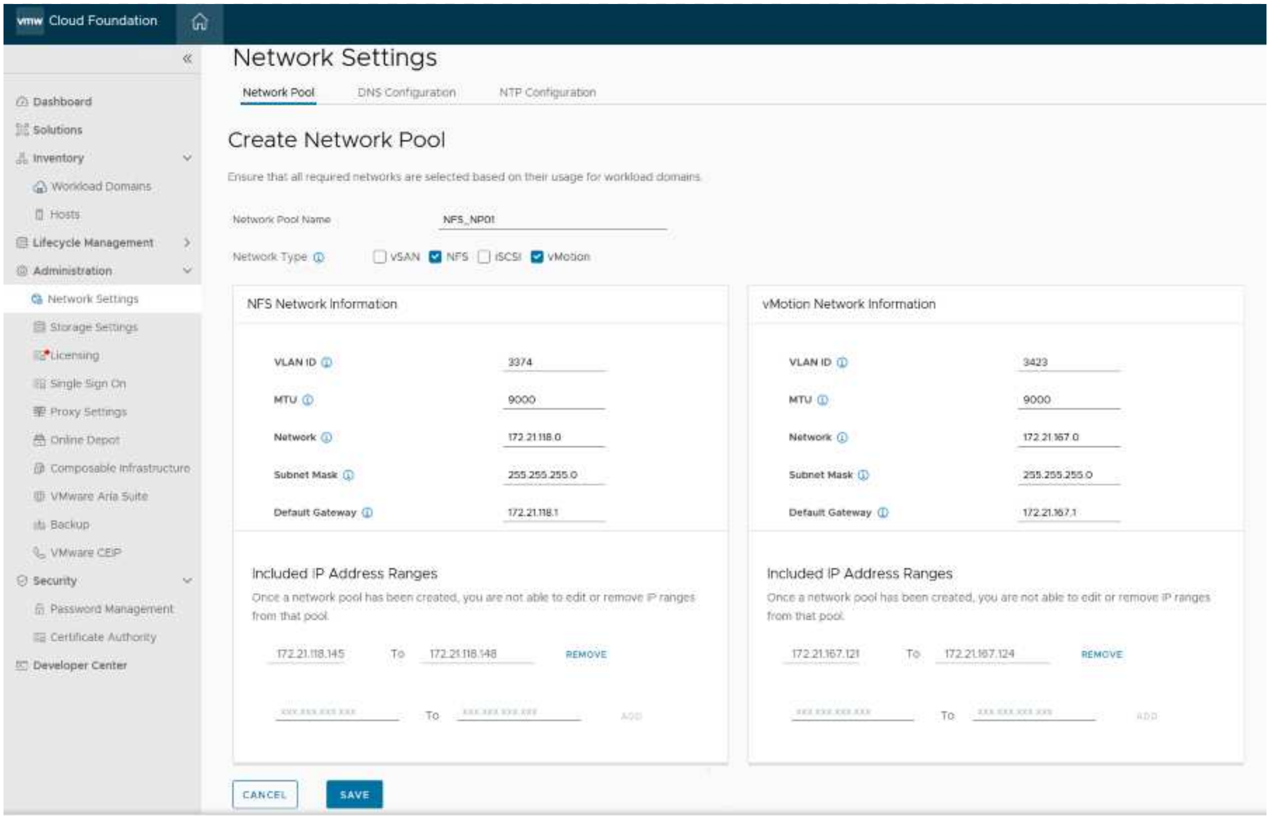
Create Network Pool in SDDC Manager

ANetwork Pool must be created in SDDC Manager before commissioning the ESXi hosts, as preparation for deploying them in a VI Workload Domain. The Network Pool must include the network information and IP address range(s) for VMkernel adapters to be used for communication with the NFS server.

1. From the SDDC Manager web interface navigate to **Network Settings** in the left-hand menu and click on the **+ Create Network Pool** button.



2. Fill out a name for the Network Pool, select the check box for NFS and fill out all networking details. Repeat this for the vMotion network information.



Network Settings

Create Network Pool

Ensure that all required networks are selected based on their usage for workload domains.

Network Pool Name: NFS_NP01

Network Type: □ vSAN ☑ NFS □ iSCSI ☑ vMotion

NFS Network Information

VLAN ID	3374
MTU	9000
Network	172.21.118.0
Subnet Mask	255.255.255.0
Default Gateway	172.21.118.1

Included IP Address Ranges

Once a network pool has been created, you are not able to edit or remove IP ranges from that pool.

172.21.118.145 To 172.21.118.148 REMOVE

xxx.xxx.xxx.xxx To xxx.xxx.xxx.xxx ADD

vMotion Network Information

VLAN ID	3423
MTU	9000
Network	172.21.167.0
Subnet Mask	255.255.255.0
Default Gateway	172.21.167.1

Included IP Address Ranges

Once a network pool has been created, you are not able to edit or remove IP ranges from that pool.

172.21.167.121 To 172.21.167.124 REMOVE

xxx.xxx.xxx.xxx To xxx.xxx.xxx.xxx ADD

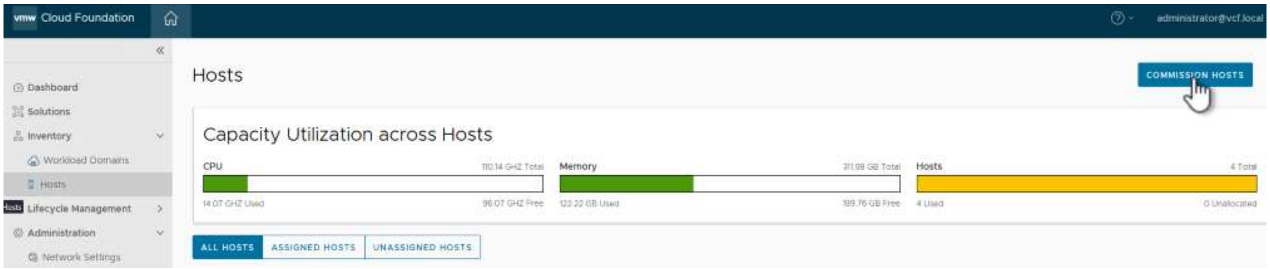
3. Click the **Save** button to complete creating the Network Pool.

Commission Hosts

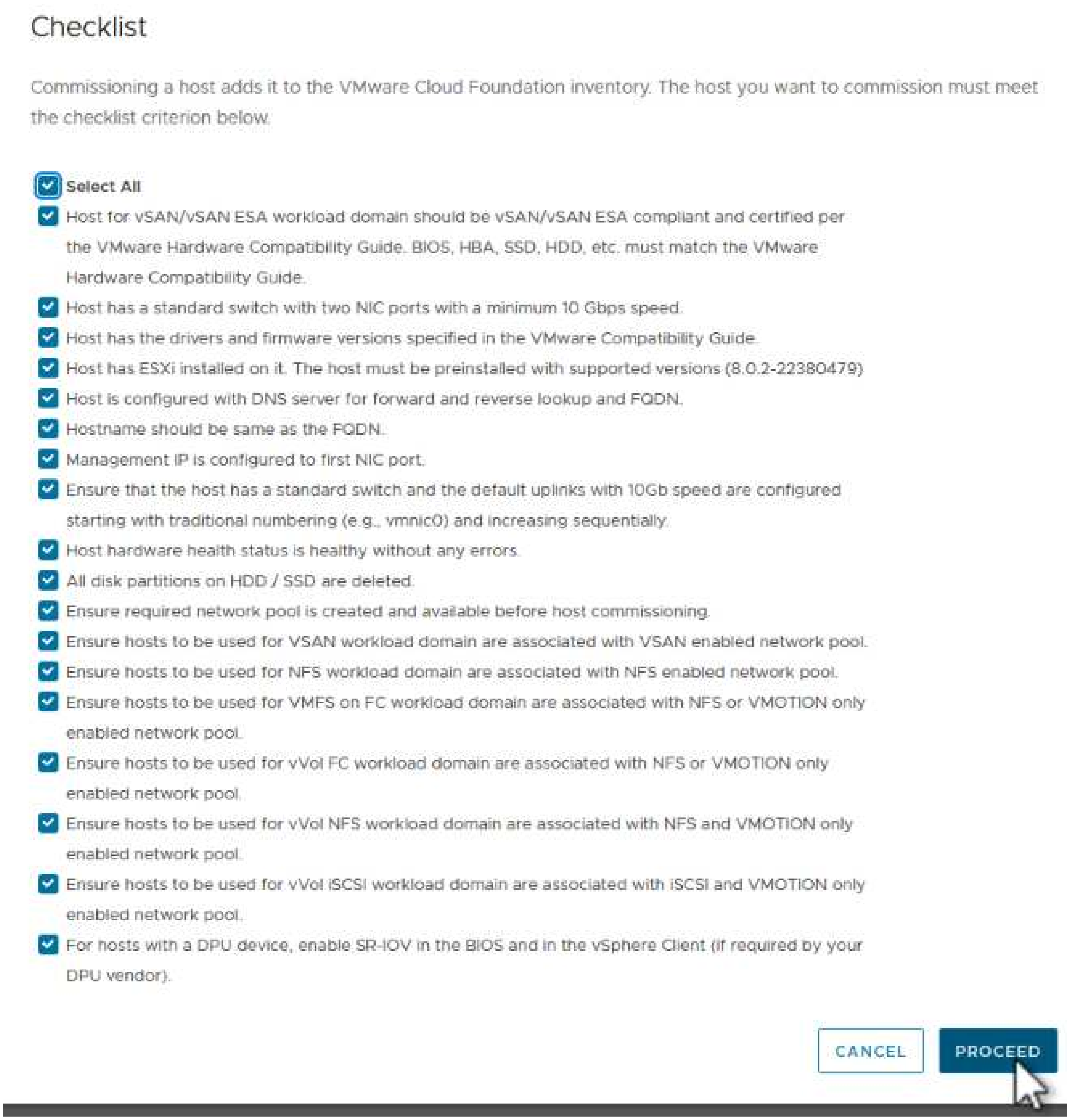
Before ESXi hosts can be deployed as a workload domain they must be added to the SDDC Manager inventory. This involves providing the required information, passing validation and starting the commissioning process.

For more information see Commission Hosts in the VCF Administration Guide.

1. From the SDDC Manager interface navigate to **Hosts** in the left-hand menu and click on the **Commission Hosts** button.



2. The first page is a prerequisite checklist. Double-check all prerequisites and select all checkboxes to proceed.

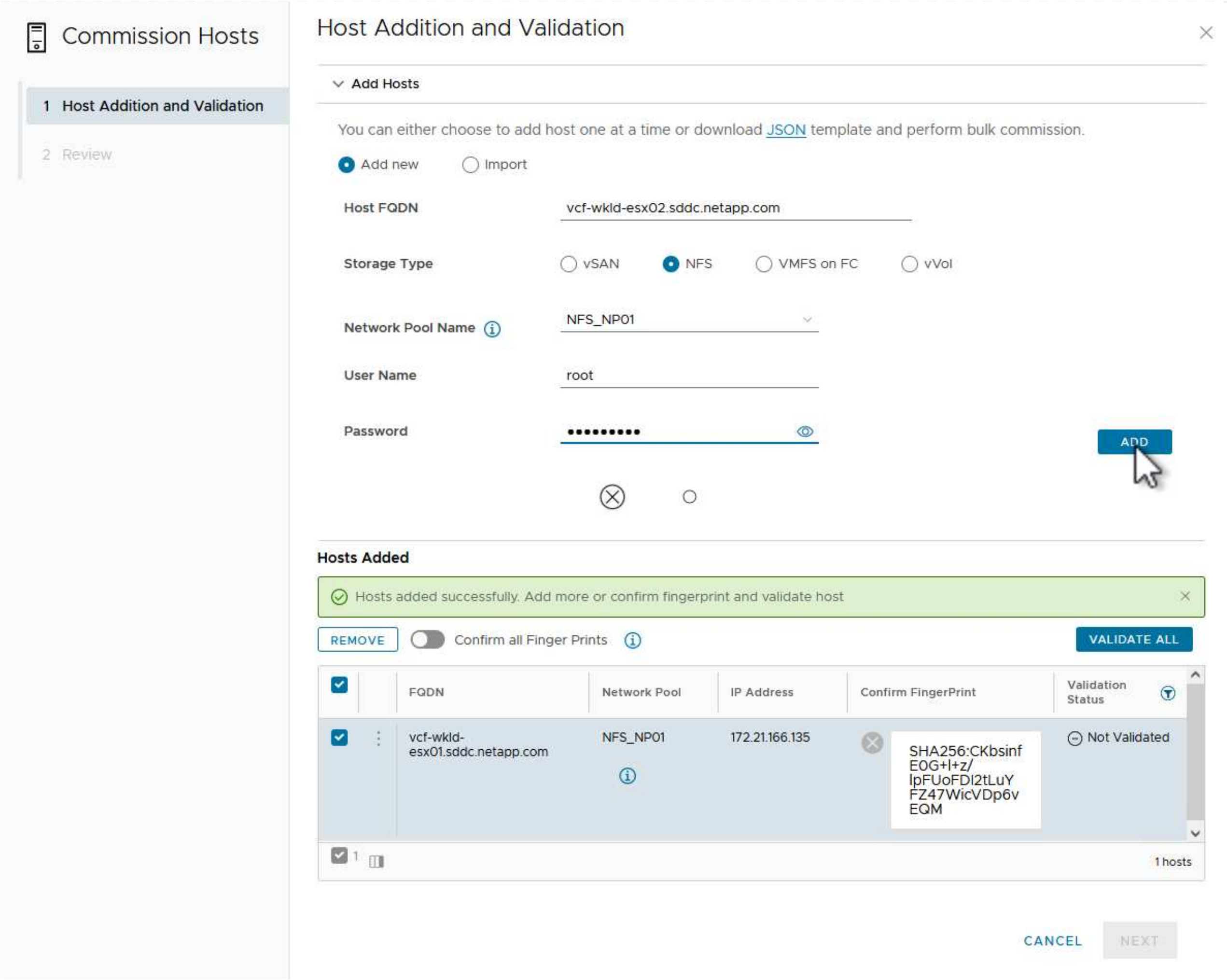


Checklist

Commissioning a host adds it to the VMware Cloud Foundation inventory. The host you want to commission must meet the checklist criterion below.

- ☑ **Select All**
- ☑ Host for vSAN/vSAN ESA workload domain should be vSAN/vSAN ESA compliant and certified per the VMware Hardware Compatibility Guide. BIOS, HBA, SSD, HDD, etc. must match the VMware Hardware Compatibility Guide.
- ☑ Host has a standard switch with two NIC ports with a minimum 10 Gbps speed.
- ☑ Host has the drivers and firmware versions specified in the VMware Compatibility Guide.
- ☑ Host has ESXi installed on it. The host must be preinstalled with supported versions (8.0.2-22380479)
- ☑ Host is configured with DNS server for forward and reverse lookup and FQDN.
- ☑ Hostname should be same as the FQDN.
- ☑ Management IP is configured to first NIC port.
- ☑ Ensure that the host has a standard switch and the default uplinks with 10Gb speed are configured starting with traditional numbering (e.g., vmnic0) and increasing sequentially.
- ☑ Host hardware health status is healthy without any errors.
- ☑ All disk partitions on HDD / SSD are deleted.
- ☑ Ensure required network pool is created and available before host commissioning.
- ☑ Ensure hosts to be used for VSAN workload domain are associated with VSAN enabled network pool.
- ☑ Ensure hosts to be used for NFS workload domain are associated with NFS enabled network pool.
- ☑ Ensure hosts to be used for VMFS on FC workload domain are associated with NFS or VMOTION only enabled network pool.
- ☑ Ensure hosts to be used for vVol FC workload domain are associated with NFS or VMOTION only enabled network pool.
- ☑ Ensure hosts to be used for vVol NFS workload domain are associated with NFS and VMOTION only enabled network pool.
- ☑ Ensure hosts to be used for vVol iSCSI workload domain are associated with iSCSI and VMOTION only enabled network pool.
- ☑ For hosts with a DPU device, enable SR-IOV in the BIOS and in the vSphere Client (if required by your DPU vendor).

3. In the **Host Addition and Validation** window fill out the **Host FQDN**, **Storage Type**, The **Network Pool** name that includes the vMotion and NFS storage IP addresses to be used for the workload domain, and the credentials to access the ESXi host. Click on **Add** to add the host to the group of hosts to be validated.



Commission Hosts

1 Host Addition and Validation

2 Review

Host Addition and Validation

Add Hosts

You can either choose to add host one at a time or download JSON template and perform bulk commission.

● Add new ○ Import

Host FQDN: vcf-wkld-esx02.sddc.netapp.com

Storage Type: ○ vSAN ● NFS ○ VMFS on FC ○ vVol

Network Pool Name: NFS_NP01

User Name: root

Password: ●●●●●●●●●●

ADD

Hosts Added

Hosts added successfully. Add more or confirm fingerprint and validate host

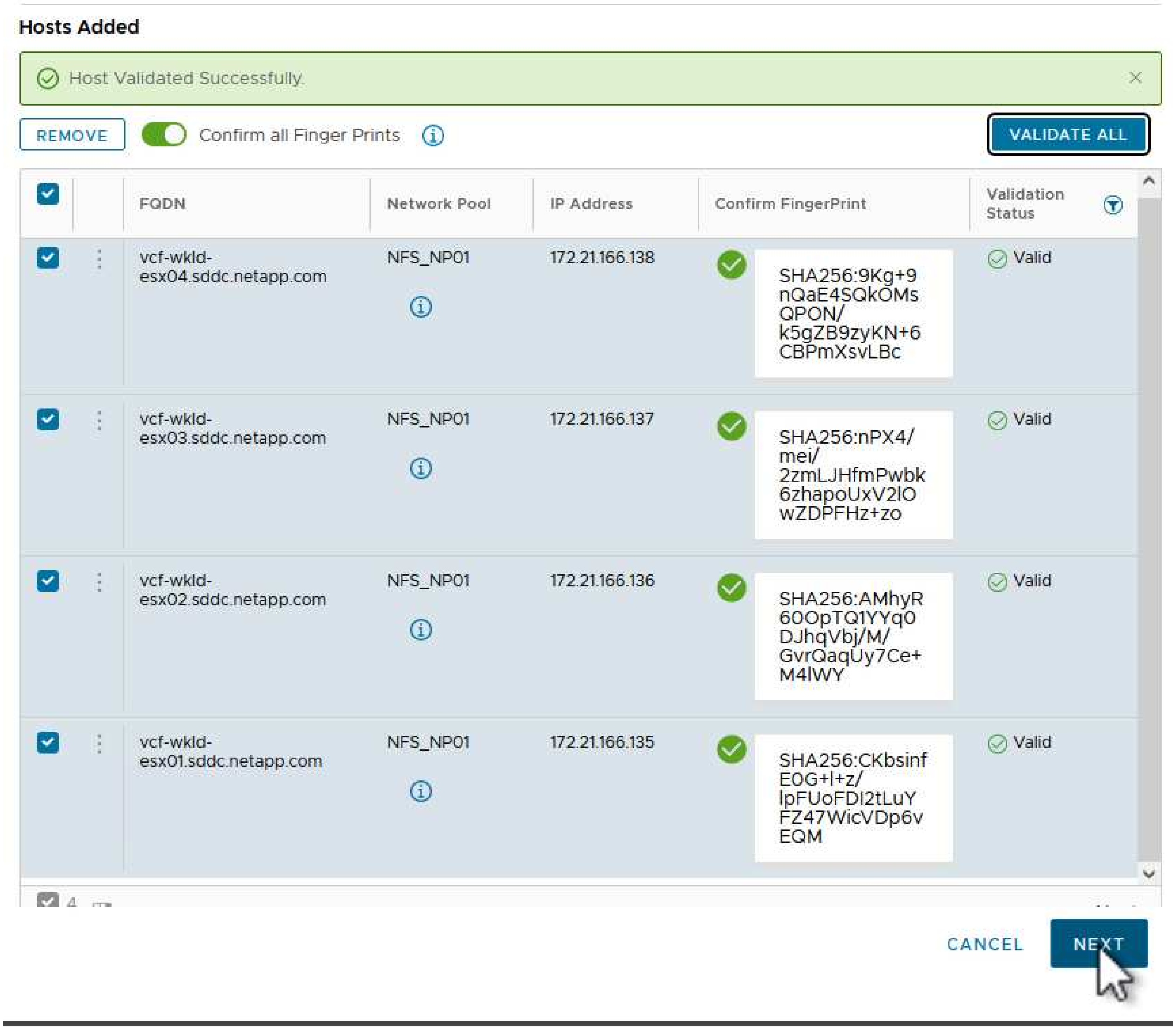
REMOVE | Confirm all Finger Prints | VALIDATE ALL

☑		FQDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
☑	⋮	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01	172.21.166.135	SHA256:CKbsinfE0G+l+z/lpFUoFDI2tLuYFZ47WicVDp6vEQM	Not Validated

1 hosts

CANCEL NEXT

4. Once all hosts to be validated have been added, click on the **Validate All** button to continue.
5. Assuming all hosts are validated, click on **Next** to continue.



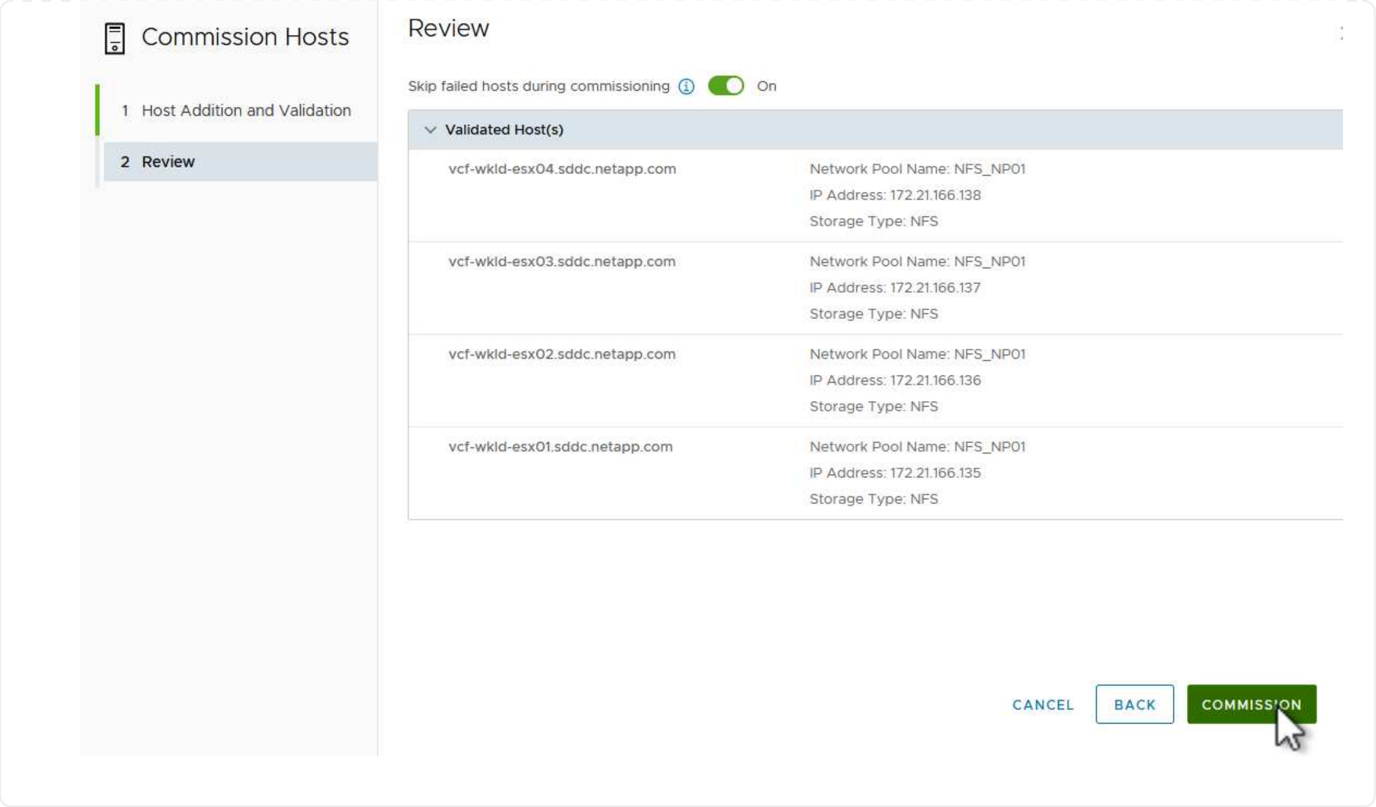
Hosts Added

Host Validated Successfully.

Confirm all Finger Prints: on

☑	FQDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
☑	vcf-wkld-esx04.sddc.netapp.com	NFS_NP01	172.21.166.138	✓ SHA256:9Kg+9nQaE4SQkOMsQPON/k5gZB9zyKN+6CBPmXsvLBc	✓ Valid
☑	vcf-wkld-esx03.sddc.netapp.com	NFS_NP01	172.21.166.137	✓ SHA256:nPX4/mei/2zmLJHfmPwbk6zhapoUxV2lOwZDPFHz+zo	✓ Valid
☑	vcf-wkld-esx02.sddc.netapp.com	NFS_NP01	172.21.166.136	✓ SHA256:AMhyR60OpTQ1YYq0DJhqVbj/M/GvrQaqUy7Ce+M4lWY	✓ Valid
☑	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01	172.21.166.135	✓ SHA256:CKbsinfE0G+l+z/lpFUoFDI2tLuYFZ47WicVDp6vEQM	✓ Valid

6. Review the list of hosts to be commissioned and click on the **Commission** button to start the process. Monitor the commissioning process from the Task pane in SDDC manager.



Review

Skip failed hosts during commissioning On

Validated Host(s)

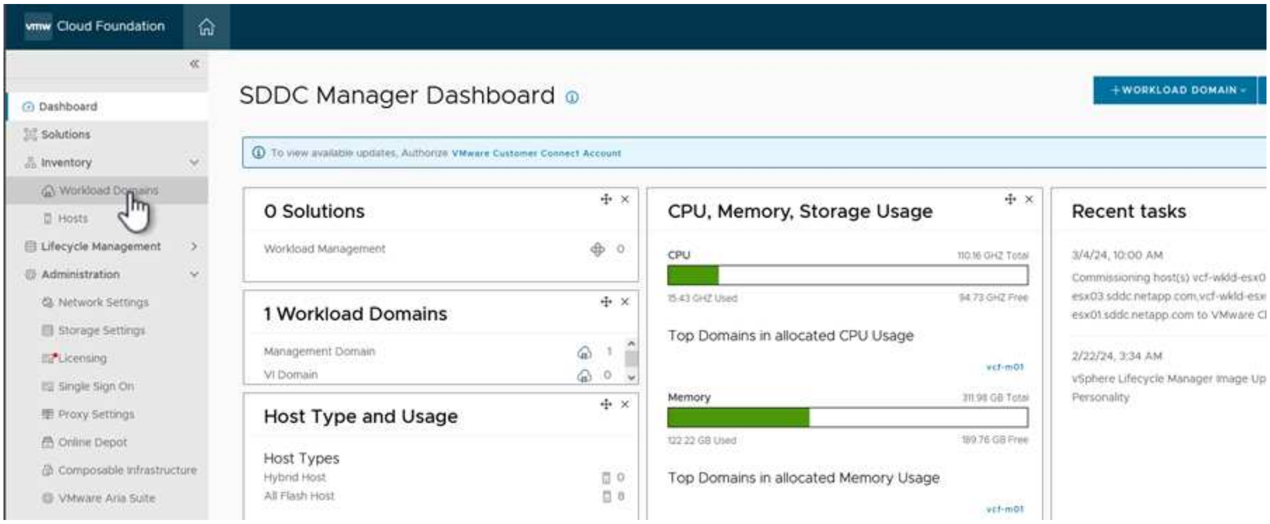
vcf-wkld-esx04.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.138 Storage Type: NFS
vcf-wkld-esx03.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.137 Storage Type: NFS
vcf-wkld-esx02.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.136 Storage Type: NFS
vcf-wkld-esx01.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.135 Storage Type: NFS

Deploy VI Workload Domain

Deploying VI workload domains is accomplished using the VCF Cloud Manager interface. Only the steps related to the storage configuration will be presented here.

For step-by-step instructions on deploying a VI workload domain refer to Deploy a VI Workload Domain Using the SDDC Manager UI.

1. From the SDDC Manager Dashboard click on **+ Workload Domain** in the upper right hand corner to create a new Workload Domain.



SDDC Manager Dashboard

To view available updates, Authorize VMware Customer Connect Account

0 Solutions
Workload Management 0

1 Workload Domains
Management Domain 1
VI Domain 0

Host Type and Usage
Host Types
Hybrid Host 0
All Flash Host 8

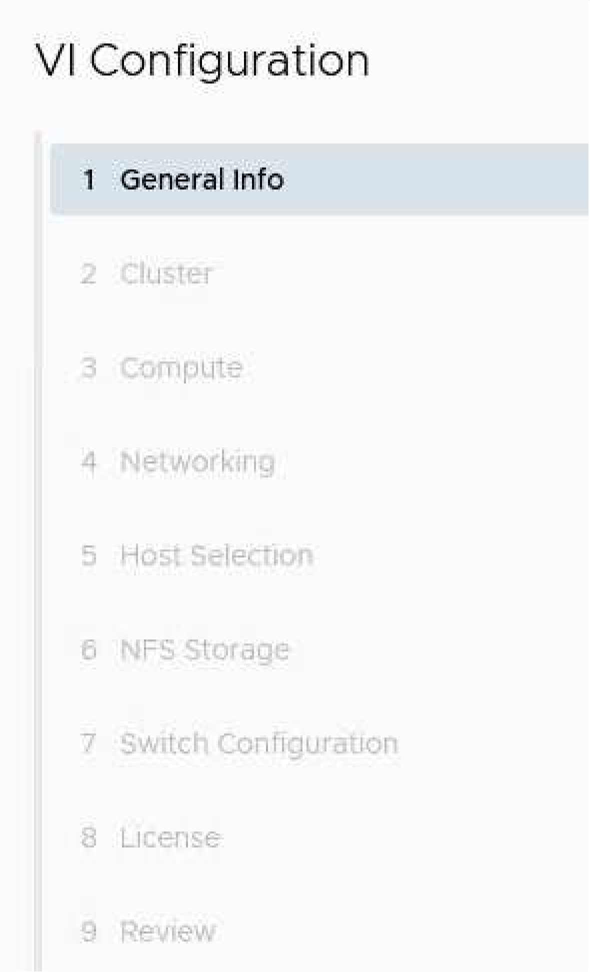
CPU, Memory, Storage Usage
CPU 110.16 GHZ Total
15.43 GHZ Used 94.73 GHZ Free
Top Domains in allocated CPU Usage
vcf-m01
Memory 311.98 GB Total
122.22 GB Used 189.76 GB Free
Top Domains in allocated Memory Usage
vcf-m01

Recent tasks
3/4/24, 10:00 AM
Commissioning host(s) vcf-wkld-esx0 esx03.sddc.netapp.com,vcf-wkld-esx esx01.sddc.netapp.com to VMware Cl
2/22/24, 3:34 AM
vSphere Lifecycle Manager Image Up Personality

2. In the VI Configuration wizard fill out the sections for **General Info, Cluster, Compute, Networking**, and **Host Selection** as required.

For information on filling out the information required in the VI Configuration wizard refer to Deploy a VI Workload Domain Using the SDDC Manager UI.

+



VI Configuration

1 General Info

2 Cluster

3 Compute

4 Networking

5 Host Selection

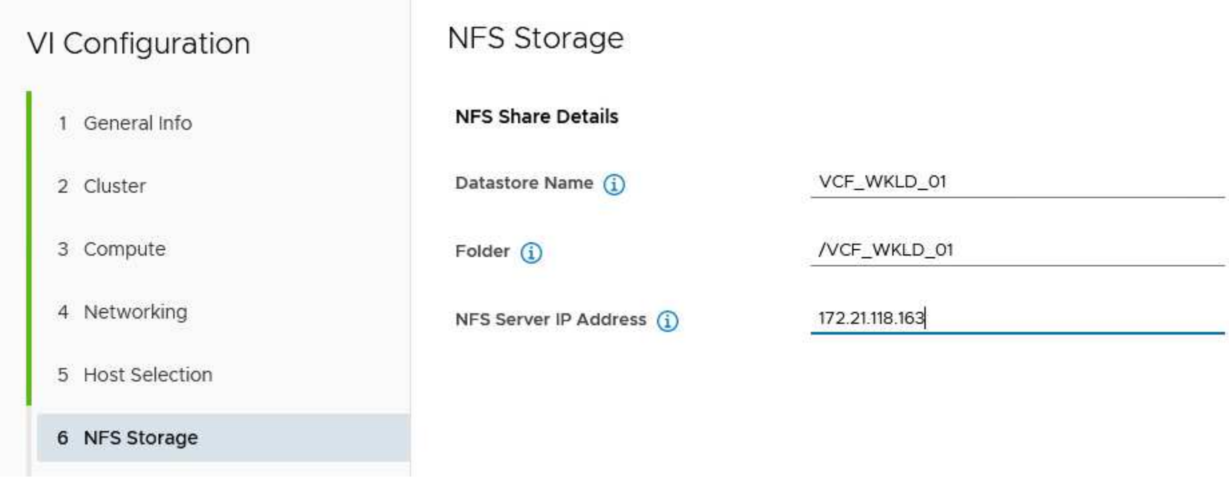
6 NFS Storage

7 Switch Configuration

8 License

9 Review

1. In the NFS Storage section fill out the Datastore Name, the folder mount point of the NFS volume and the IP address of the ONTAP NFS storage VM LIF.



NFS Storage

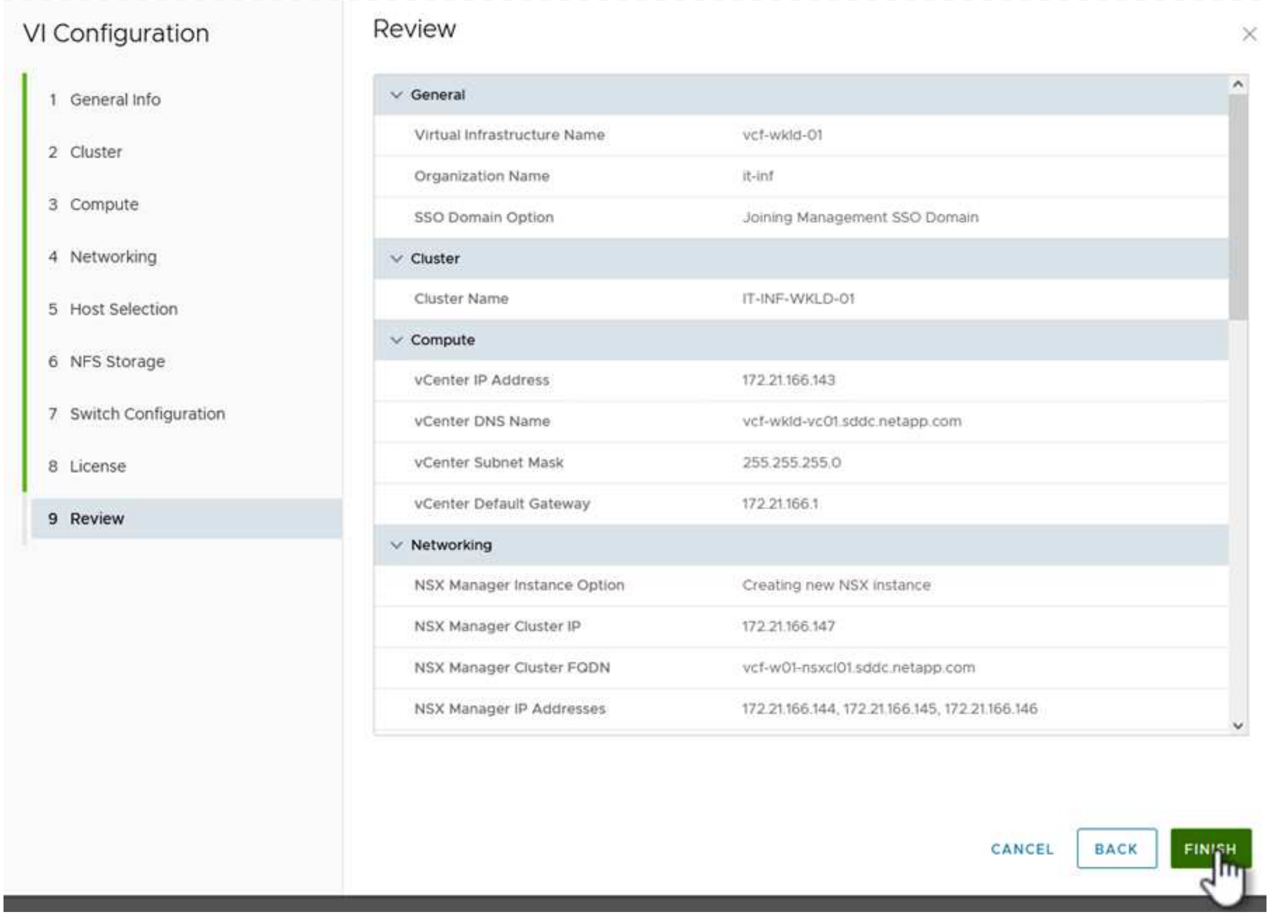
NFS Share Details

Datastore Name: VCF_WKLD_01

Folder: /VCF_WKLD_01

NFS Server IP Address: 172.21.118.163

2. In the VI Configuration wizard complete the Switch Configuration and License steps, and then click on **Finish** to start the Workload Domain creation process.



General	
Virtual Infrastructure Name	vcf-wkld-01
Organization Name	it-inf
SSO Domain Option	Joining Management SSO Domain
Cluster	
Cluster Name	IT-INF-WKLD-01
Compute	
vCenter IP Address	172.21.166.143
vCenter DNS Name	vcf-wkld-vc01.sddc.netapp.com
vCenter Subnet Mask	255.255.255.0
vCenter Default Gateway	172.21.166.1
Networking	
NSX Manager Instance Option	Creating new NSX instance
NSX Manager Cluster IP	172.21.166.147
NSX Manager Cluster FQDN	vcf-w01-nsxcl01.sddc.netapp.com
NSX Manager IP Addresses	172.21.166.144, 172.21.166.145, 172.21.166.146

3. Monitor the process and resolve any validation issues that arise during the process.

Install NetApp NFS Plug-in for VMware VAAI

The NetApp NFS Plug-in for VMware VAAI integrates the VMware Virtual Disk Libraries installed on the ESXi host and provides higher performance cloning operations that finish faster. This is a recommended procedure when using ONTAP storage systems with VMware vSphere.

For step-by-step instructions on deploying the NetApp NFS Plug-in for VMware VAAI following the instructions at Install NetApp NFS Plug-in for VMware VAAI.

Video demo for this solution

NFS Datastores as Principal Storage for VCF Workload Domains

Additional information

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

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

Expand VCF with supplemental storage

Learn about expanding storage for a VCF environment using supplemental storage

VMware Cloud Foundation (VCF) supports a wide range of supplemental storage options to expand storage on VCF management domains and Virtual Infrastructure (VI) workload domains.

NetApp's ONTAP tools for VMware vSphere provide an efficient solution for this expansion by integrating NetApp storage seamlessly into the VCF environment.

ONTAP tools simplifies the setup and management of datastores, allowing administrators to provision and manage storage directly from the vSphere Client. ONTAP's advanced features, such as snapshots, cloning, and data protection, enhance storage performance, efficiency, and scalability within the VCF environment.

Supported protocols for expanding storage

VCF environments can be expanded using several storage protocols, each offering unique benefits and use cases.

You can use the following protocols to expand storage in VCF management domains and VI workload domains. Choose the best option for your environment to seamlessly integrate supplemental storage into your VCF deployment.

iSCSI

Block-based protocol that uses standard Ethernet networks. Ideal for environments that require high performance, flexibility, and cost-effective scaling.

iSCSI is widely used for VMFS datastores and supports advanced ONTAP features, such as snapshots and cloning.

- **High Performance:** Offers high performance to deliver fast, efficient data transfer rates and low latency. Ideal for demanding enterprise applications and virtualized environments.
- **Ease of Management:** Simplifies storage management by using familiar IP-based tools and protocols.
- **Cost Effective:** Uses existing Ethernet infrastructure, reducing the need for specialized hardware and allowing organizations to achieve reliable and scalable storage solutions.

For more information on using iSCSI with NetApp storage systems, refer to SAN Provisioning with iSCSI.

Fibre Channel (FC)

High-speed, low-latency protocol that uses dedicated FC networks. FC is preferred for mission-critical workloads that demand reliability, dedicated bandwidth, and robust error correction. It is commonly used for VMFS datastores in enterprise environments.

- **High Performance:** FC provides high-speed data transfer rates, making it ideal for applications requiring fast and reliable access to large amounts of data.
- **Low Latency:** Very low latency, which is crucial for performance-sensitive applications like databases and virtualized environments.
- **Reliability:** FC networks are known for their robustness and reliability, with features like built-in redundancy and error correction.

- **Dedicated Bandwidth:** FC provides dedicated bandwidth for storage traffic, reducing the risk of network congestion.

For more information on using Fibre Channel with NetApp storage systems, refer to SAN Provisioning with FC.

NFS (Network File System)

File-based protocol that enables easy sharing and management of files across hosts. NFS is simple to set up and scales efficiently, making it suitable for virtualized workloads and environments that require flexible file access.

NFS datastores are supported by ONTAP and vSphere for both management and workload domains.

- **Simplicity and ease of use:** NFS is straightforward to set up and manage, making it an excellent choice for environments that require quick and easy file sharing.
- **Scalability:** ONTAP's architecture allows NFS to scale efficiently, supporting growing data needs without significant changes to the infrastructure.
- **Flexibility:** NFS supports a wide range of applications and workloads, making it versatile for various use cases, including virtualized environments.

For more information, refer to the NFS v3 Reference Guide for vSphere 8.

NVMe/TCP

Modern protocol that delivers high performance and low latency over standard Ethernet networks using TCP/IP. NVMe/TCP is ideal for demanding applications and large-scale data operations, providing scalability and cost efficiency without requiring specialized hardware.

- **High Performance:** Delivers exceptional performance with low latency and high data transfer rates. This is crucial for demanding applications and large-scale data operations.
- **Scalability:** Supports scalable configurations, allowing IT administrators to expand their infrastructure seamlessly as data requirements grow.
- **Cost Effective:** Runs over standard Ethernet switches and is encapsulated inside TCP datagrams. No special equipment required to implement.

For more information on the benefits of NVMe, refer to What is NVME?.

Use cases for adding supplemental storage

The following use cases demonstrate how to add supplemental storage to VCF management domains and Virtual Infrastructure (VI) workload domains using different protocols and configurations.

- Management Domain with iSCSI
- Management Domain with FC
- Virtual Infrastructure Workload Domain with vVols (iSCSI)
- Virtual Infrastructure Workload Domain with vVols (NFS)
- Virtual Infrastructure Workload Domain with NVMe/TCP
- Virtual Infrastructure Workload Domain with FC

Expand management domains with iSCSI

Deployment workflow for adding an iSCSI datastore as supplemental storage in a VCF management domain

Get started with adding an iSCSI datastore as supplemental storage for a VMware Cloud Foundation (VCF) management domain. You'll set up a Storage Virtual Machine (SVM) with logical interfaces (LIFs) for iSCSI, configure iSCSI networking on ESXi hosts, deploy ONTAP tools for VMware vSphere, and create a VMFS datastore.

1 **Review the deployment requirements**

Review the requirements for adding iSCSI datastores as supplemental storage to VCF management domain.

2 **Create the SVM and LIFs**

Create an SVM with multiple LIFs for iSCSI traffic.

3 **Configure networking**

Set up networking for iSCSI on ESXi hosts.

4 **Configure storage**

Deploy and use ONTAP tools to configure storage.

Deployment requirements for adding an iSCSI datastore to a VCF management domain

Review the requirements for adding iSCSI datastores as supplemental storage to a VMware Cloud Foundation (VCF) management domain.

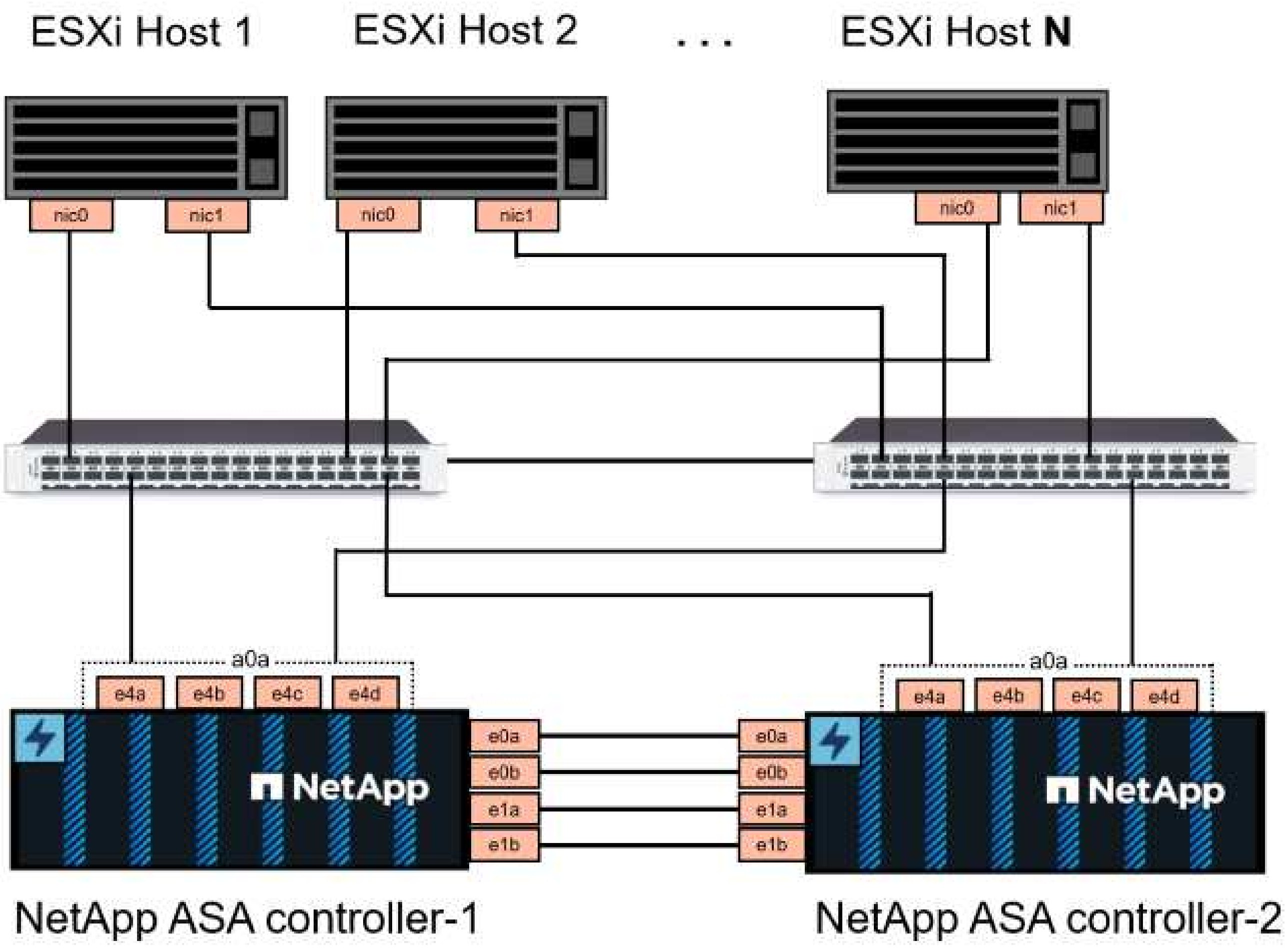
Infrastructure requirements

Make sure the following components and configurations are in place.

- An ONTAP AFF or ASA storage system with physical data ports on Ethernet switches dedicated to storage traffic.
- VCF management domain deployment is complete and the vSphere client is accessible.

Recommended iSCSI network design

You should configure fully redundant network designs for iSCSI. The following diagram shows an example of a redundant configuration, providing fault tolerance for storage systems, switches, networks adapters and host systems. Refer to the NetApp SAN configuration reference for additional information.



For multipathing and failover across multiple paths, create a minimum of two LIFs per storage node in separate Ethernet networks for all SVMs in iSCSI configurations.

> In situations where multiple VMkernel adapters are configured on the same IP network, it is recommended to use software iSCSI port binding on the ESXi hosts to ensure that load balancing across the adapters occurs. Refer to KB article Considerations for using software iSCSI port binding in ESX/ESXi.

What's next?

After reviewing the deployment requirements, create the SVM and LIFs.

Create SVM and LIFs for iSCSI datastores in a VCF management domain

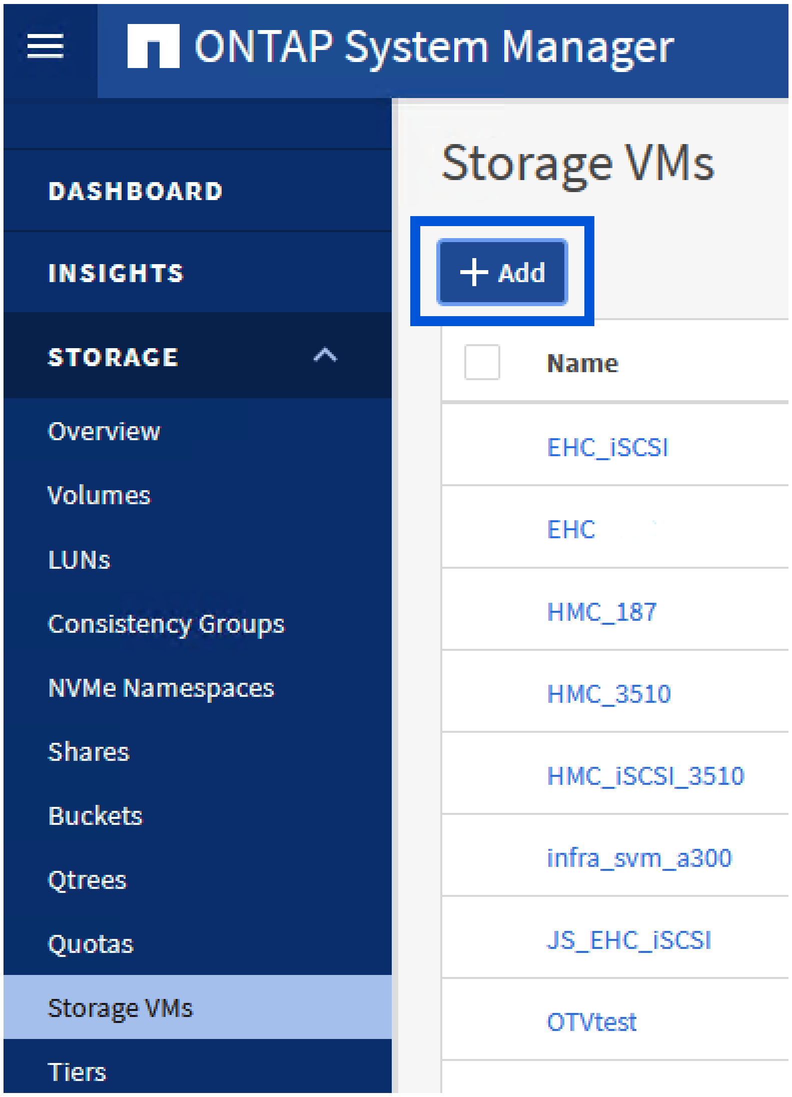
Create a Storage Virtual Machine (SVM) with multiple Logical Interfaces (LIFs) to provide iSCSI connectivity for VMware Cloud Foundation management domains. You'll configure the SVM with iSCSI protocol support and set up multiple LIFs across separate Ethernet networks to enable multipathing and failover for optimal performance and availability.

To add new LIFs to an existing SVM, refer to the ONTAP documentation: Create ONTAP LIFs.

Steps

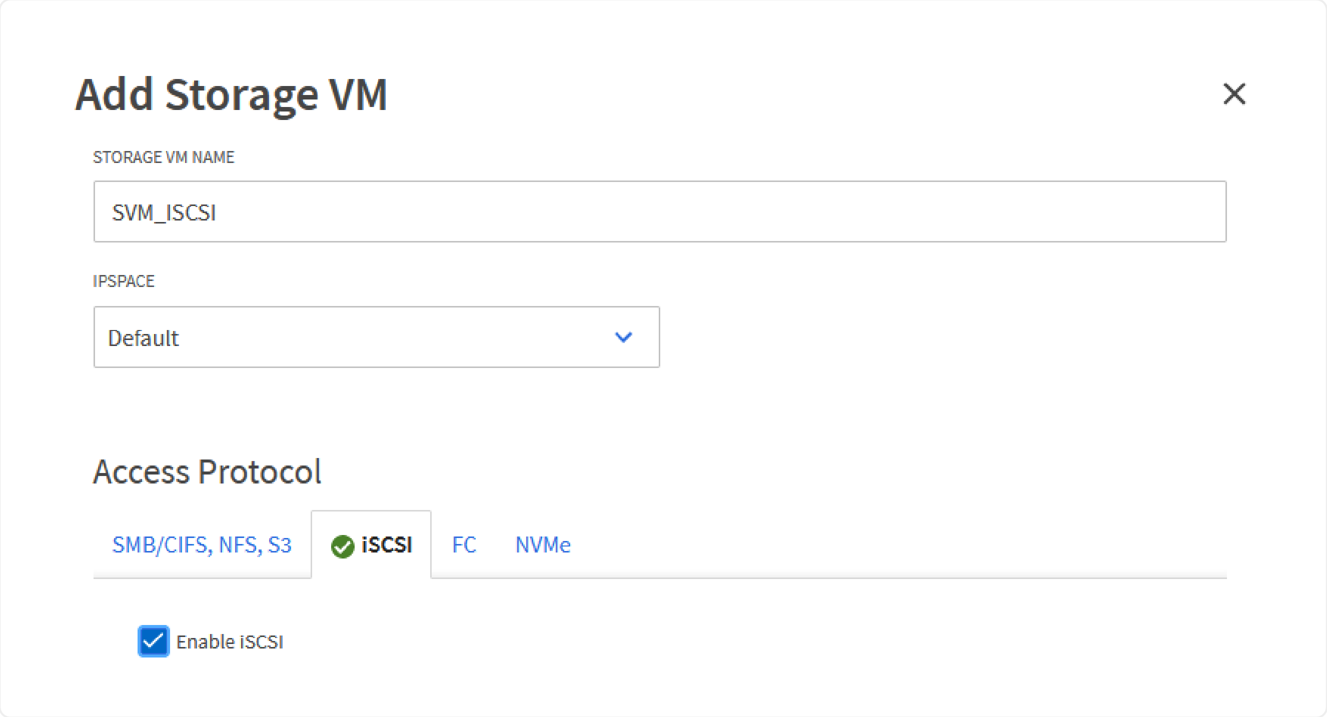
1. From ONTAP System Manager navigate to **Storage VMs** in the left-hand menu and click **+ Add** to start.

Show example



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

Show example



Add Storage VM

STORAGE VM NAME

SVM_ISCSI

IPSPACE

Default

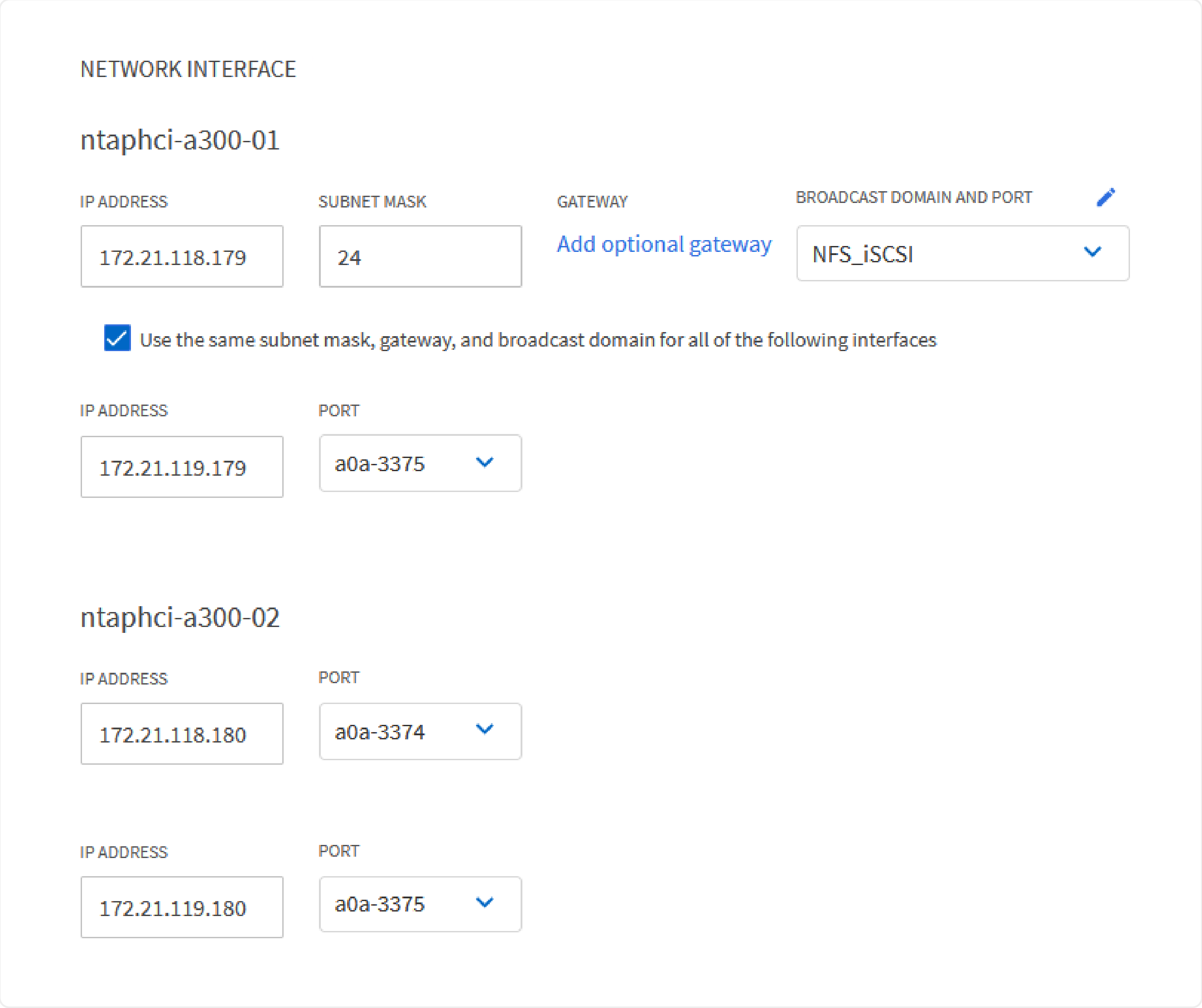
Access Protocol

☑ Enable iSCSI

3. In the **Network Interface** section fill in the **IP address**, **Subnet Mask**, and **Broadcast Domain and Port** for the first LIF. For subsequent LIFs, you can either use individual settings or enable the checkbox to use common settings across all remaining LIFs.

   For multipathing and failover across multiple paths, create a minimum of two LIFs per storage node in separate Ethernet networks for all SVMs in iSCSI configurations.

Show example



NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS: 172.21.118.179

SUBNET MASK: 24

GATEWAY: Add optional gateway

BROADCAST DOMAIN AND PORT: NFS_iSCSI

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

IP ADDRESS: 172.21.119.179

PORT: a0a-3375

ntaphci-a300-02

IP ADDRESS: 172.21.118.180

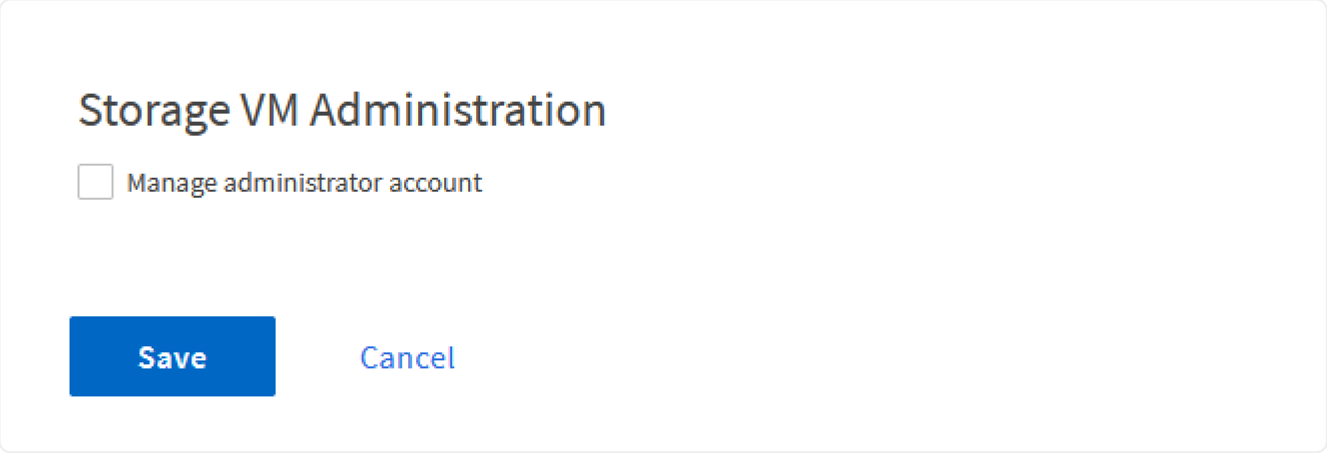
PORT: a0a-3374

IP ADDRESS: 172.21.119.180

PORT: a0a-3375

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

Show example



Storage VM Administration

□ Manage administrator account

What’s next?

After you create the SVM and LIFs, configure networking for iSCSI on ESXi hosts.

Configure networking for iSCSI on ESXi hosts in a VCF management domain

Configure iSCSI networking on ESXi hosts in VMware Cloud Foundation management domains to enable connectivity to ONTAP storage systems. You’ll create distributed port groups with VLAN separation, configure uplink teaming for redundancy, and set up VMkernel adapters on each ESXi host to establish dedicated iSCSI paths for failover capabilities.

Perform these steps on the VCF management domain cluster using the vSphere client.

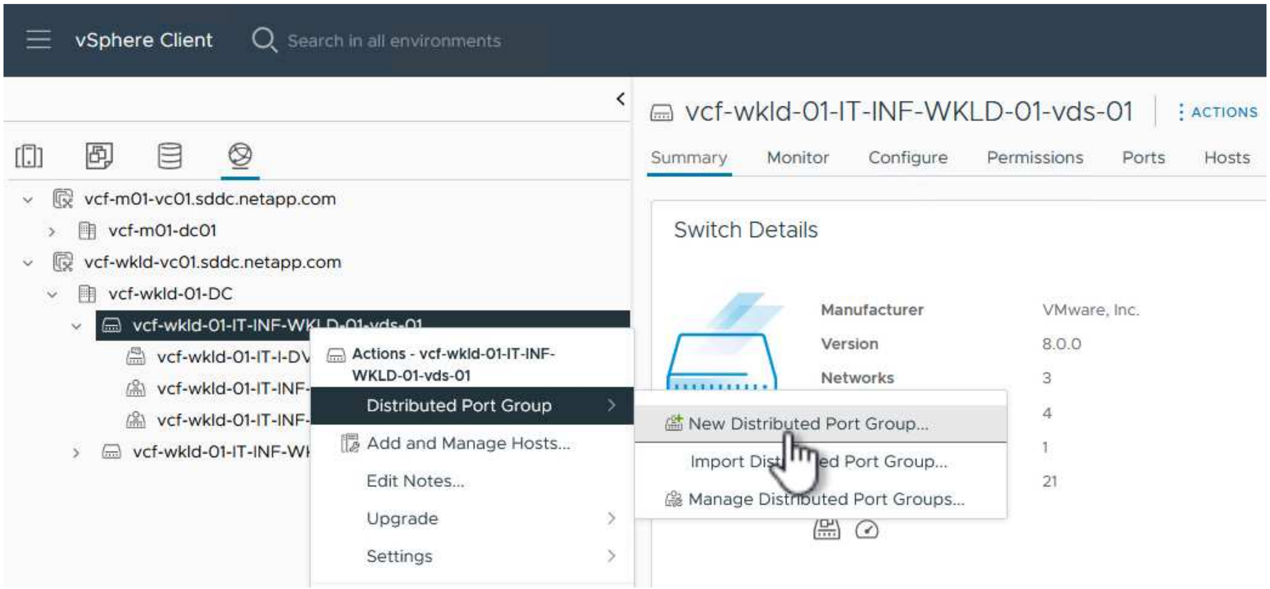
Step 1: Create distributed port groups for iSCSI traffic

Complete the following steps to create a new distributed port group for each iSCSI network:

Steps

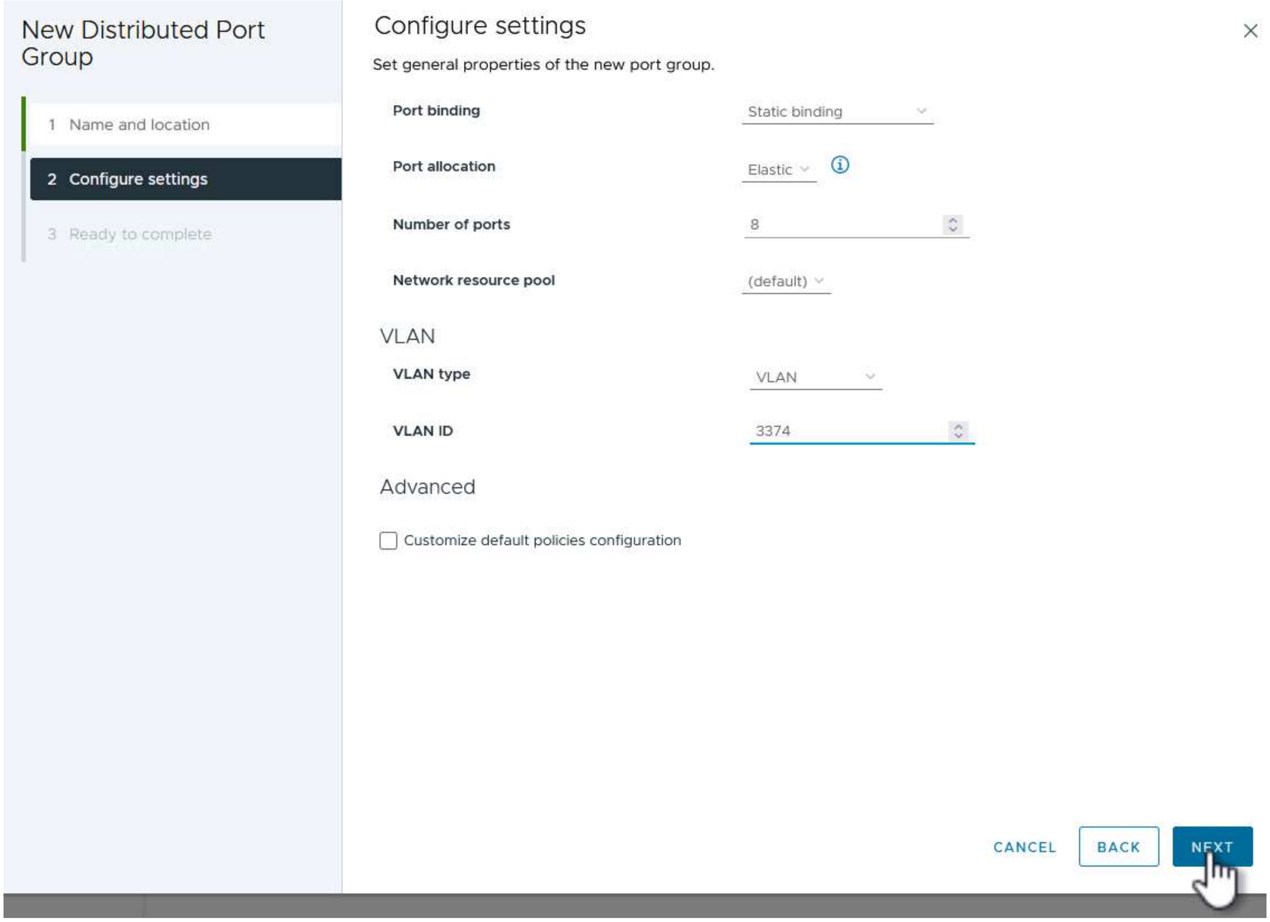
1. From the vSphere client , navigate to **Inventory > Networking** for the workload domain. Navigate to the existing Distributed Switch and choose the action to create a new **Distributed Port Group….**

   Show example



2. In the **New Distributed Port Group** wizard, fill in a name for the new port group and then click **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 **Next** to continue.

Show example



New Distributed Port Group

1 Name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding: Static binding

Port allocation: Elastic

Number of ports: 8

Network resource pool: (default)

VLAN

VLAN type: VLAN

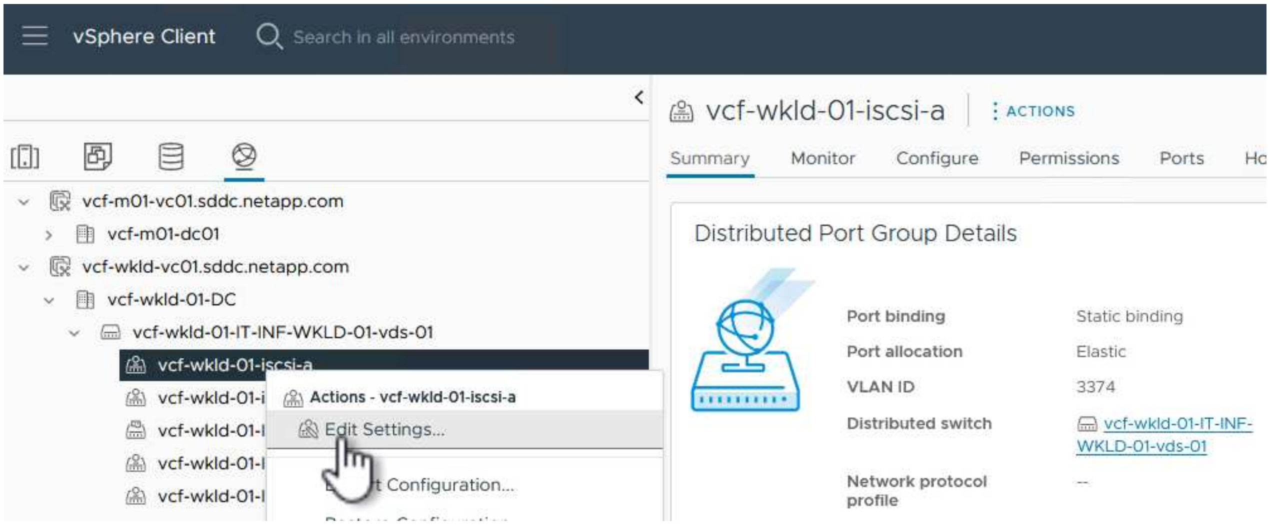
VLAN ID: 3374

Advanced

□ Customize default policies configuration

4. On the **Ready to complete** page, review the changes and click **Finish** to create the new distributed port group.
5. Repeat this process to create a distributed port group for the second iSCSI network being used and ensure you have input the correct **VLAN ID**.
6. Once both port groups have been created, navigate to the first port group and select the action to **Edit settings…**.

Show example

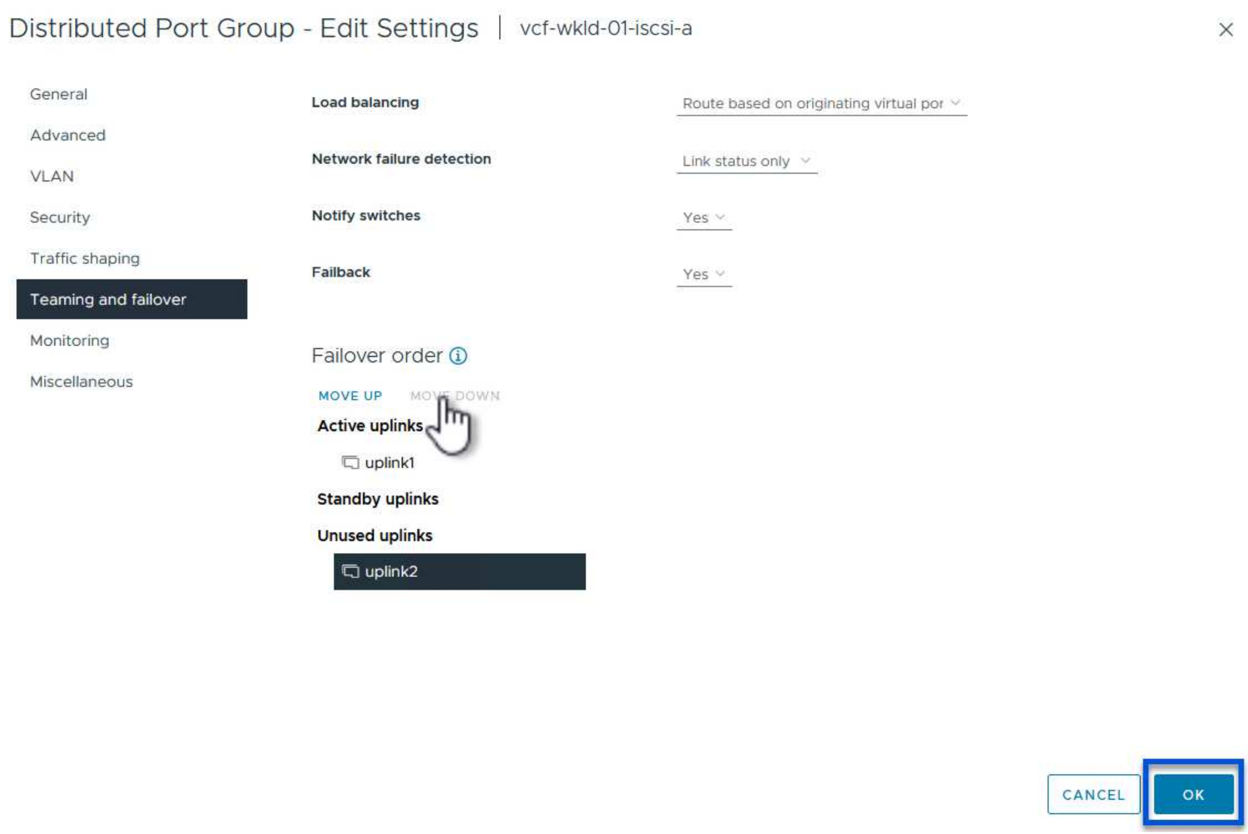


Distributed Port Group Details

Port binding	Static binding
Port allocation	Elastic
VLAN ID	3374
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01
Network protocol profile	--

7. On **Distributed Port Group - Edit Settings** page, navigate to **Teaming and failover** in the left-hand menu and click **uplink2** to move it down to **Unused uplinks**.

Show example



Load balancing	Route based on originating virtual por
Network failure detection	Link status only
Notify switches	Yes
Failback	Yes

Failover order

Active uplinks

- uplink1

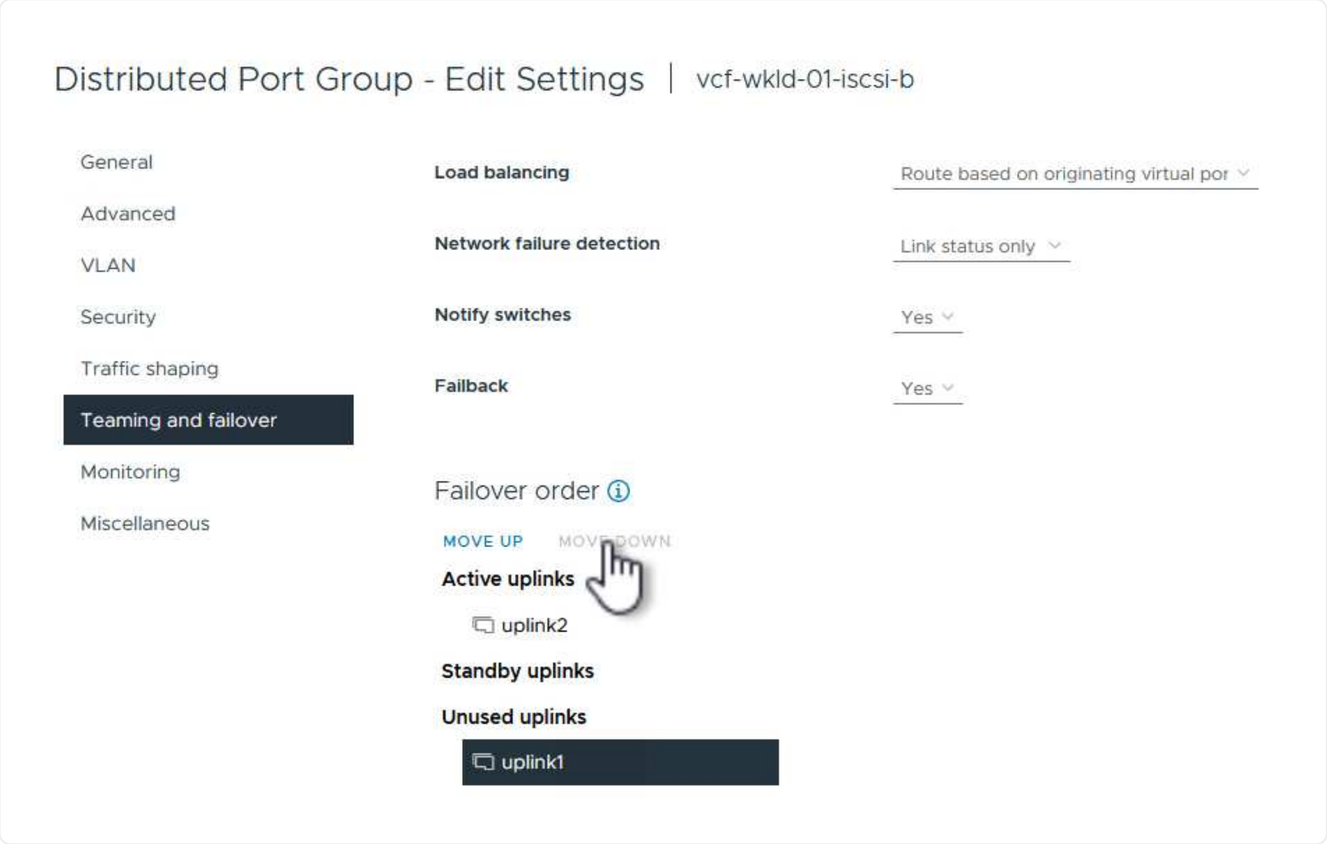
Standby uplinks

Unused uplinks

- uplink2

8. Repeat this step for the second iSCSI port group. However, this time move **uplink1** down to **Unused uplinks**.

Show example


Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-b

Load balancing: Route based on originating virtual por

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

Failover order

Active uplinks
- uplink2

Standby uplinks

Unused uplinks
- uplink1

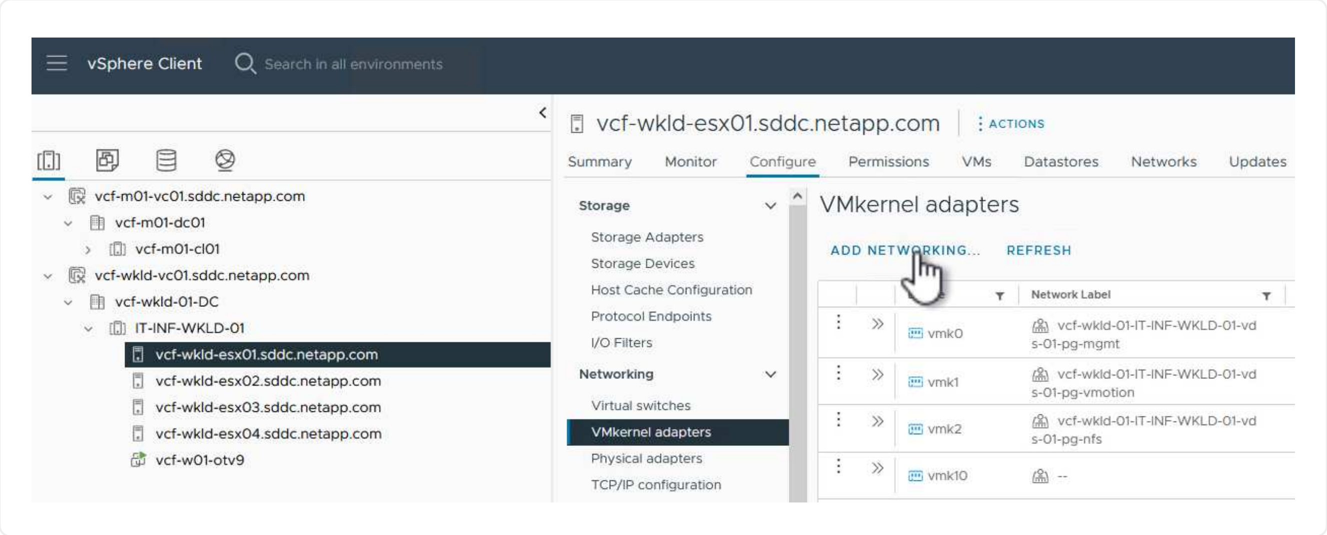
Step 2: Create VMkernel adapters on each ESXi host

Create VMkernel adapters on each ESXi host in the management domain.

Steps

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 **Add Networking…** to start.

   Show example

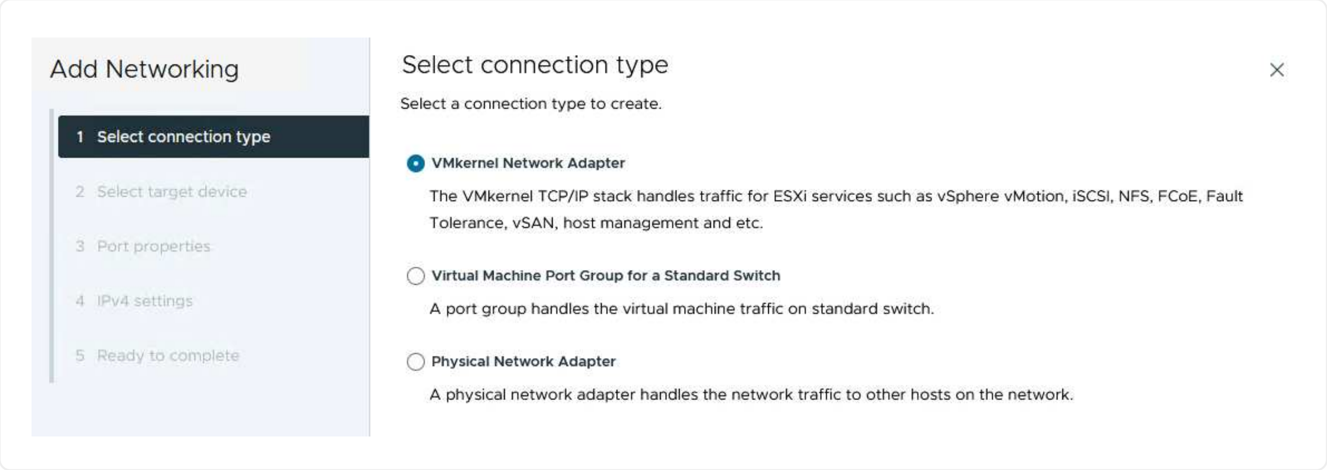


VMkernel adapters

	Network Label
vmk0	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt
vmk1	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion
vmk2	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs
vmk10	--

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

Show example



Select connection type

Select a connection type to create.

● **VMkernel Network Adapter**

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

○ **Virtual Machine Port Group for a Standard Switch**

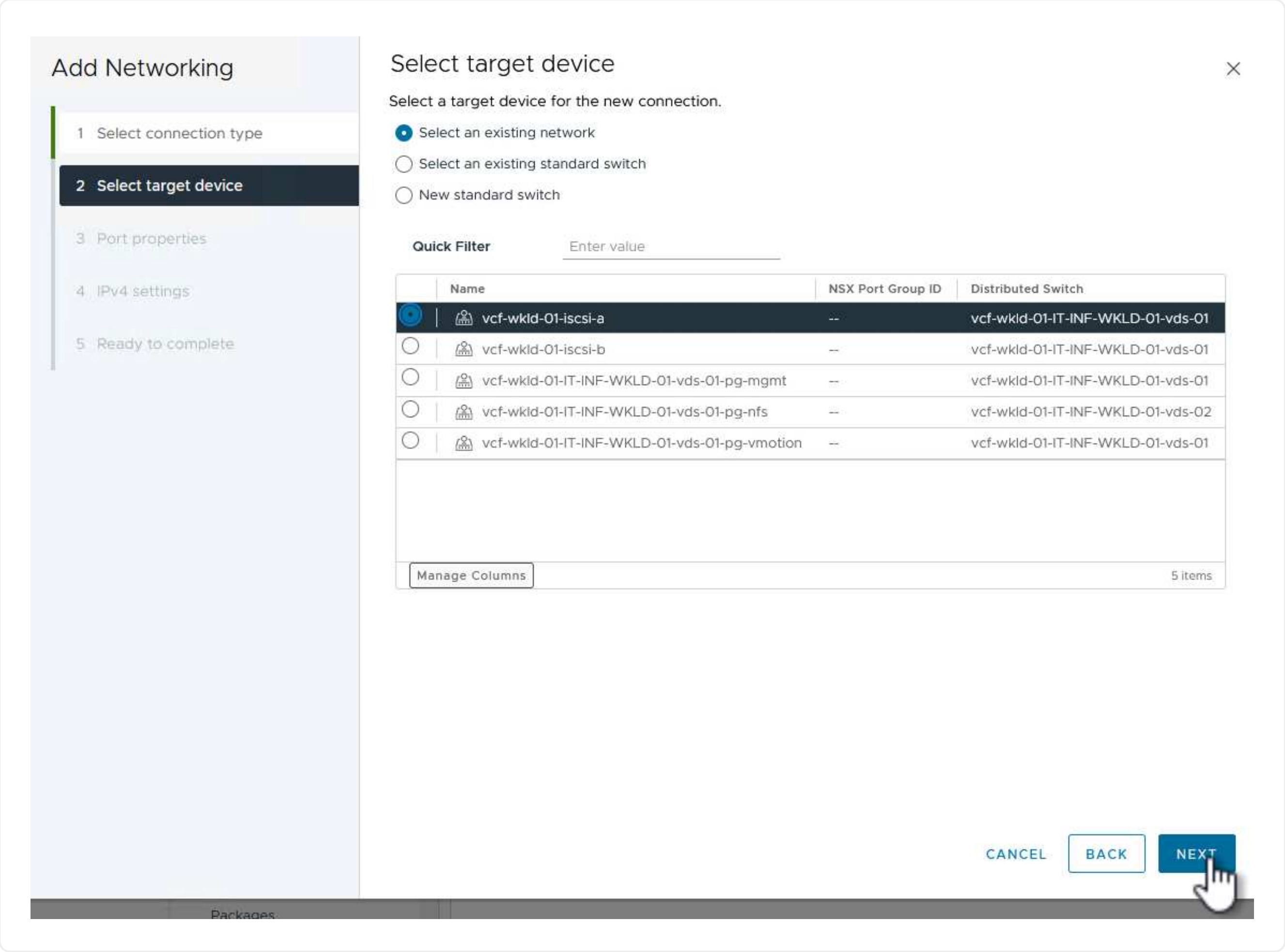
A port group handles the virtual machine traffic on standard switch.

○ **Physical Network Adapter**

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

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

Show example



Select target device

Select a target device for the new connection.

● Select an existing network

○ Select an existing standard switch

○ New standard switch

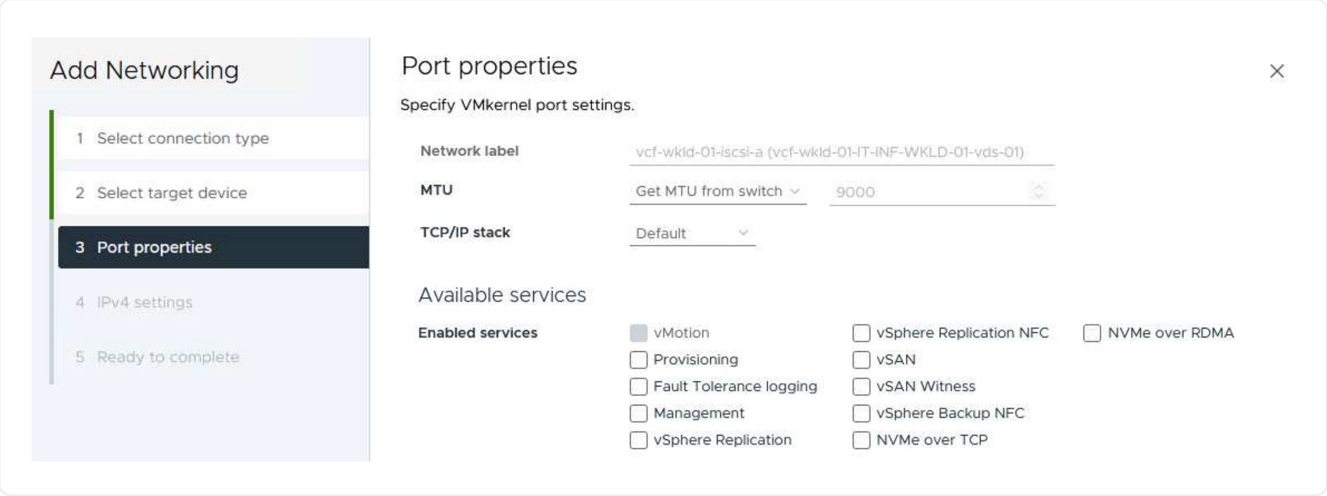
Quick Filter Enter value

	Name	NSX Port Group ID	Distributed Switch
●	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

5 items

4. On the **Port properties** page, keep the defaults and click **Next** to continue.

Show example



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label	vcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	Get MTU from switch 9000
TCP/IP stack	Default

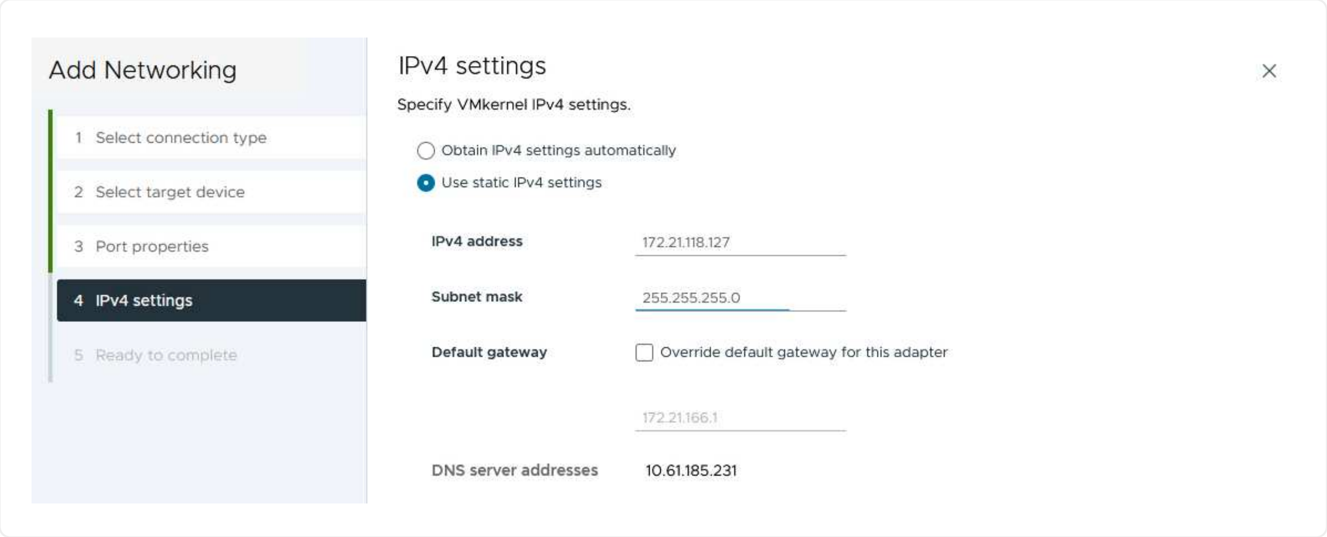
Available services

Enabled services

☐ vMotion	☐ vSphere Replication NFC	☐ NVMe over RDMA
☐ Provisioning	☐ vSAN	
☐ Fault Tolerance logging	☐ vSAN Witness	
☐ Management	☐ vSphere Backup NFC	
☐ vSphere Replication	☐ NVMe over TCP	

5. On the **IPv4 settings** page, fill in the **IP address**, **Subnet mask**, and provide a new Gateway IP address (only if required). Click **Next** to continue.

Show example



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

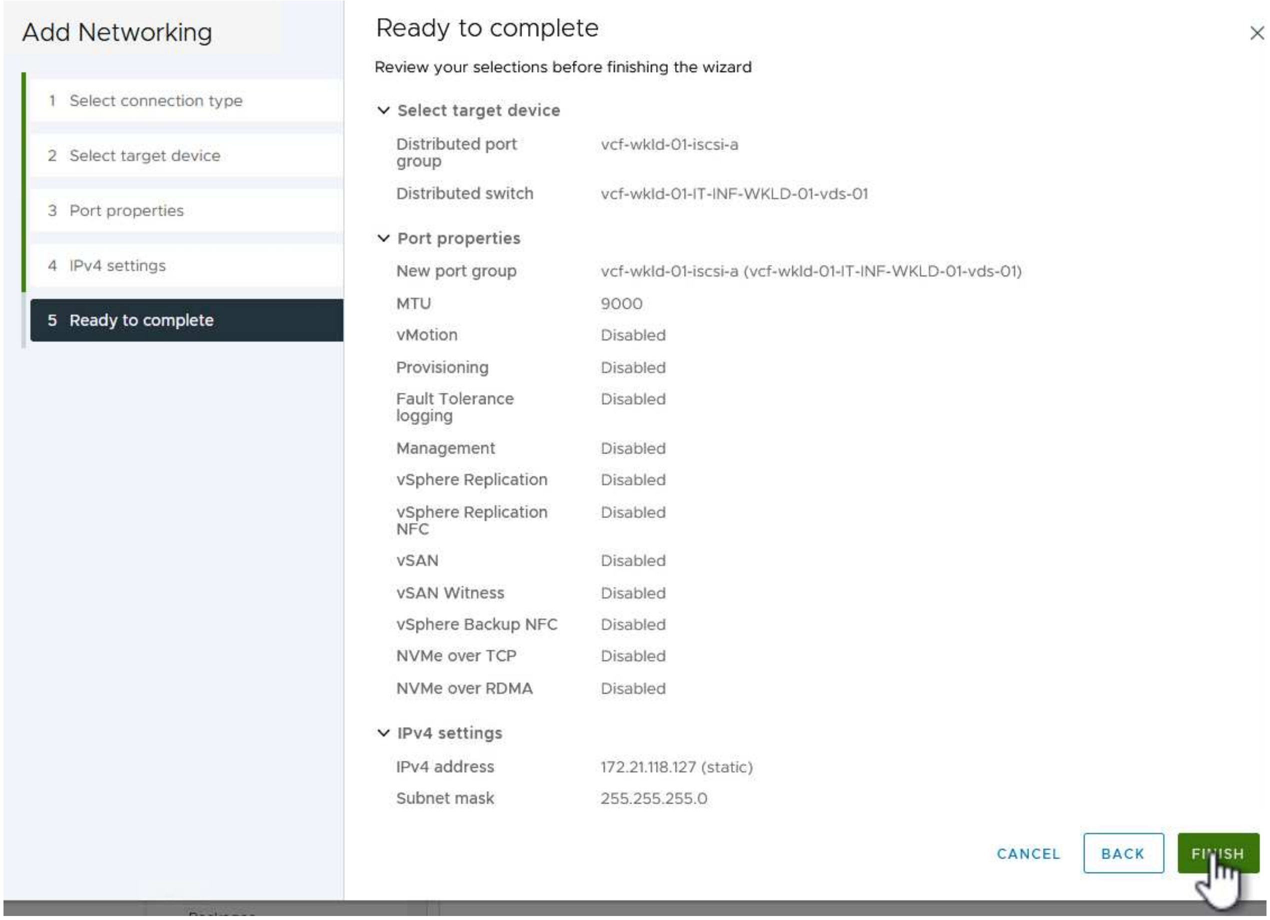
○ Obtain IPv4 settings automatically

● Use static IPv4 settings

IPv4 address	172.21.118.127
Subnet mask	255.255.255.0
Default gateway	☐ Override default gateway for this adapter
	172.21.166.1
DNS server addresses	10.61.185.231

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

Show example



Ready to complete

Review your selections before finishing the wizard

Select target device

Distributed port group	vcf-wkld-01-iscsi-a
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Port properties

New port group	vcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Disabled
NVMe over RDMA	Disabled

IPv4 settings

IPv4 address	172.21.118.127 (static)
Subnet mask	255.255.255.0

7. Repeat this process to create a VMkernel adapter for the second iSCSI network.

What’s next?

After you configure networking for iSCSI on all ESXi hosts in the workload domain, configure storage for iSCSI on ESXi hosts.

Configure iSCSI storage in a VCF management domain using ONTAP tools

Set up supplemental iSCSI storage to expand VMware Cloud Foundation management domains. You’ll deploy ONTAP tools, configure an iSCSI datastore on the management domain, and migrate management VMs to the new datastore.

Perform the following steps on the VCF management domain cluster using the vSphere client.

Step 1: Deploy ONTAP tools for VMware vSphere

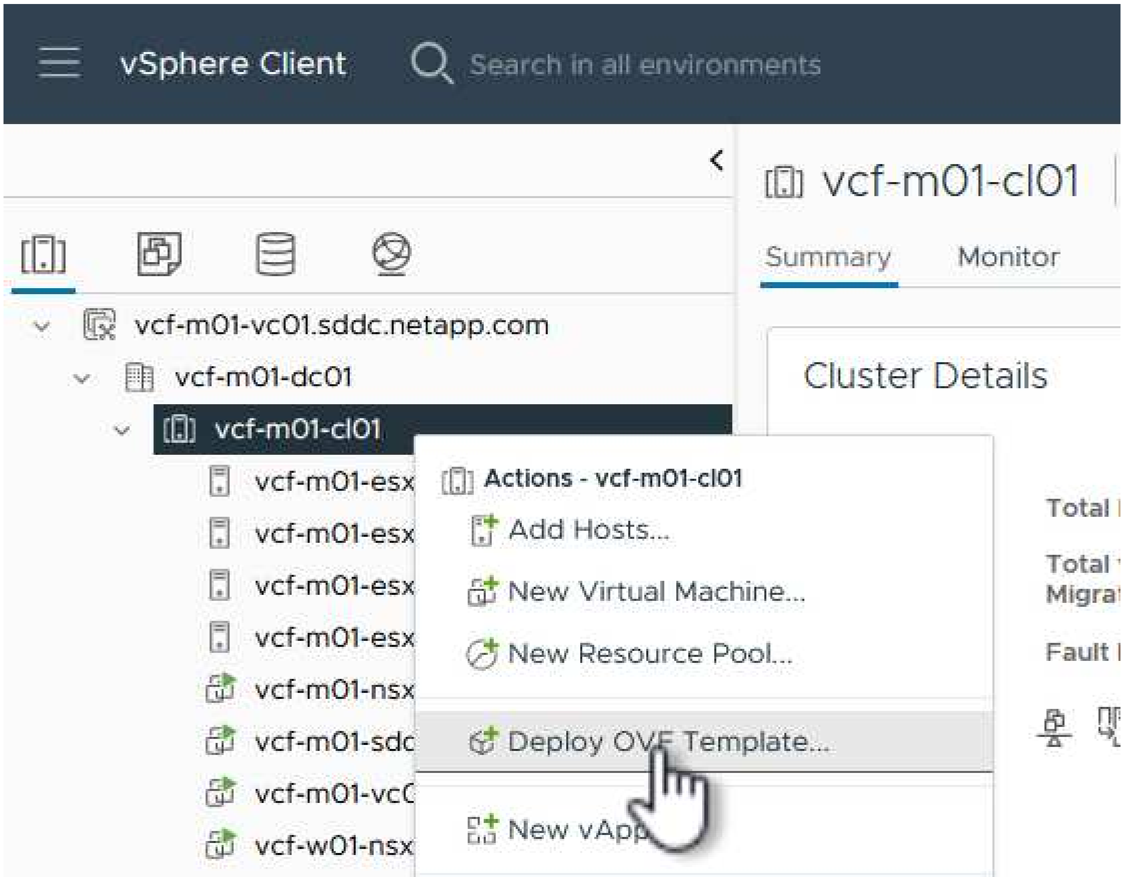
ONTAP tools for VMware vSphere (OTV) is deployed as a VM appliance and provides an integrated vCenter UI for managing ONTAP storage.

Steps

1. Obtain the ONTAP tools OVA image from the NetApp Support site and download it to a local folder.

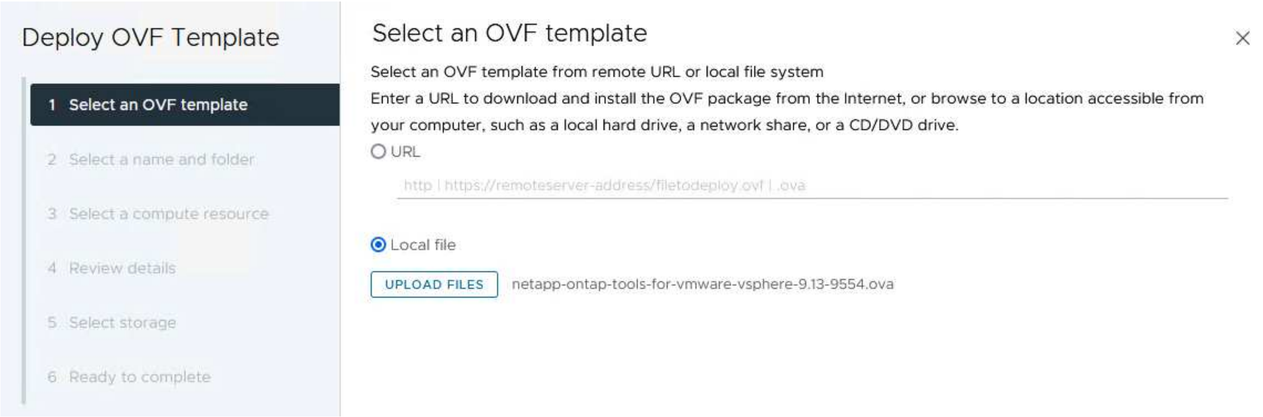
2. Log into the vCenter appliance for the VCF management domain.
3. From the vCenter appliance interface right-click the management cluster and select **Deploy OVF Template…**

Show example



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

Show example



Select an OVF template from remote URL or local file system

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

○ URL

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

● Local file

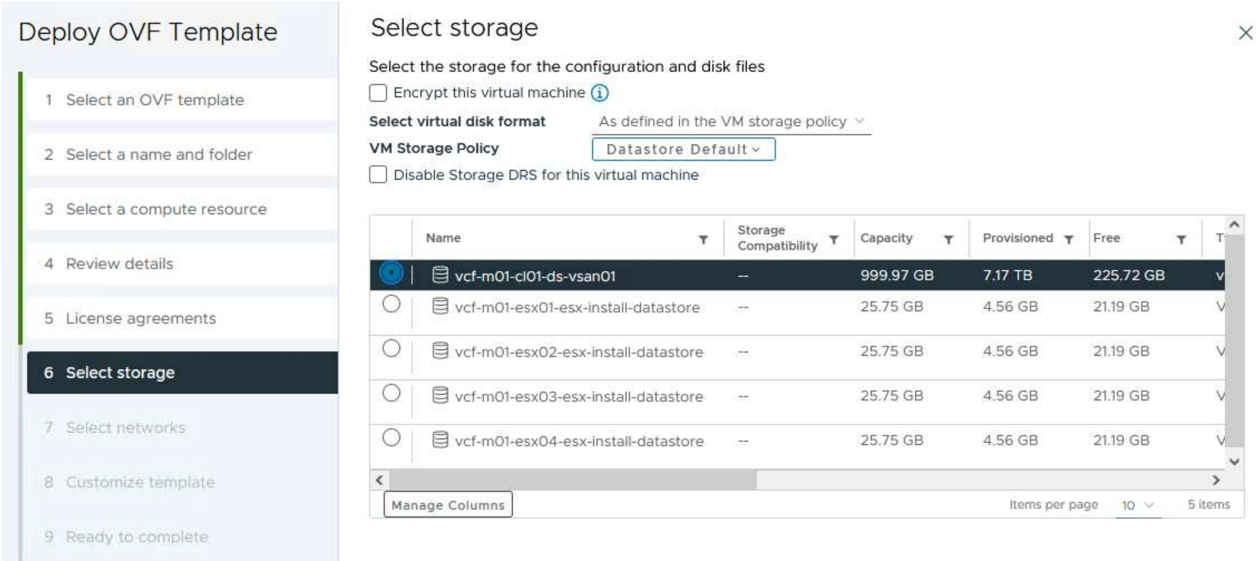
UPLOAD FILES netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. For steps 2 through 5 of the wizard, select a name and folder for the VM, select the compute resource,

review the details, and accept the license agreement.

6. For the storage location of the configuration and disk files, select the vSAN datastore of the VCF management domain cluster.

Show example



Deploy OVF Template

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

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine

Select virtual disk format As defined in the VM storage policy

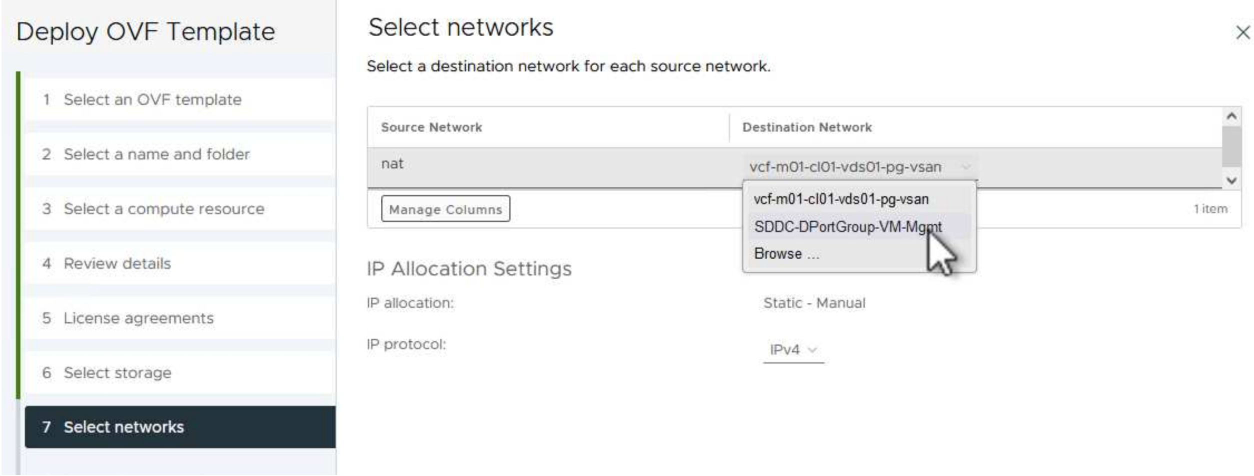
VM Storage Policy Datastore Default

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	v
○	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V

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

Show example



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks

Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	vcf-m01-cl01-vds01-pg-vsan

IP Allocation Settings

IP allocation: Static - Manual

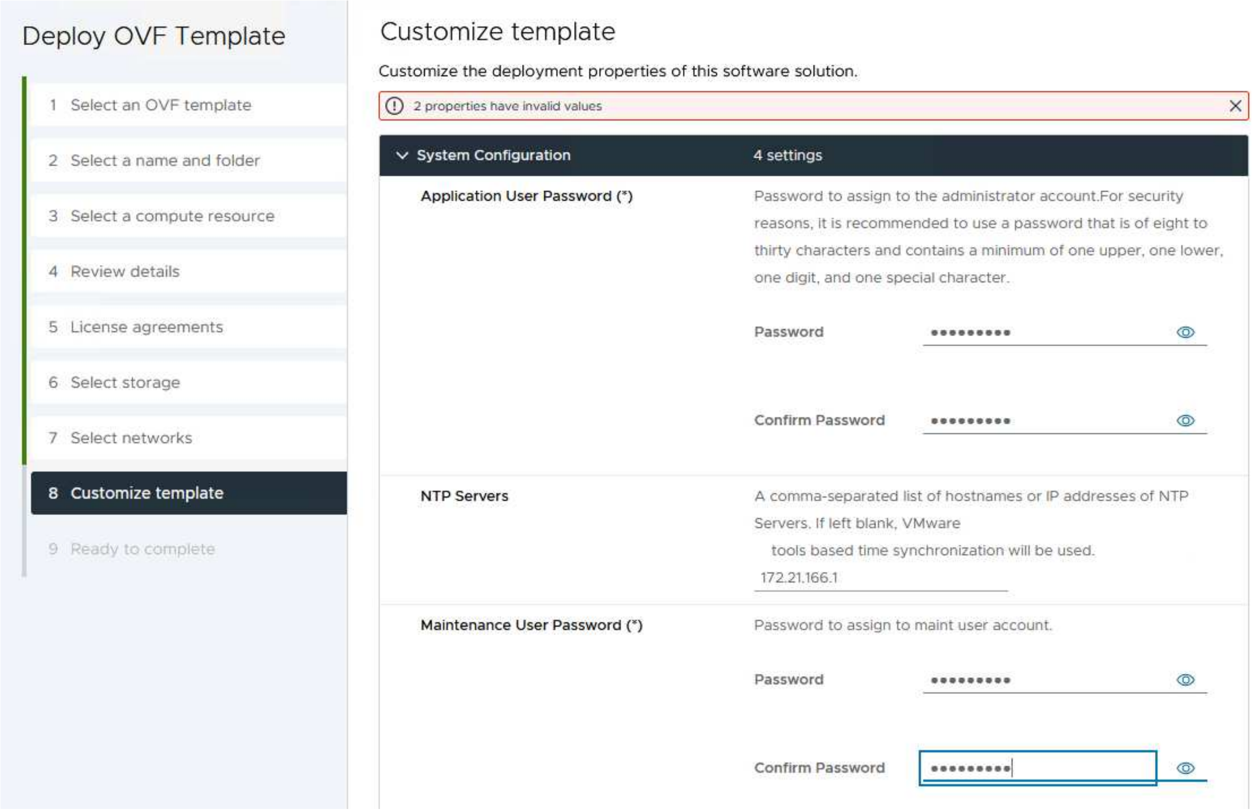
IP protocol: IPv4

8. On the **Customize template** page, enter all required information:
   - Password to be used for administrative access to ONTAP tools.
   - NTP server IP address.
   - ONTAP tools maintenance account password.
   - ONTAP tools Derby DB password.
   - Do not check the box to **Enable VMware Cloud Foundation (VCF)**. VCF mode is not required for deploying supplemental storage.

    - FQDN or IP address of the vCenter appliance for the **VI Workload Domain**
    - Credentials for the vCenter appliance of the **VI Workload Domain**
    - Required network properties.

9. Click **Next** to continue.

Show example



Deploy OVF Template

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

Customize template

Customize the deployment properties of this software solution.

ⓘ 2 properties have invalid values ✕

System Configuration — 4 settings

Application User Password (*) — Password to assign to the administrator account.For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.

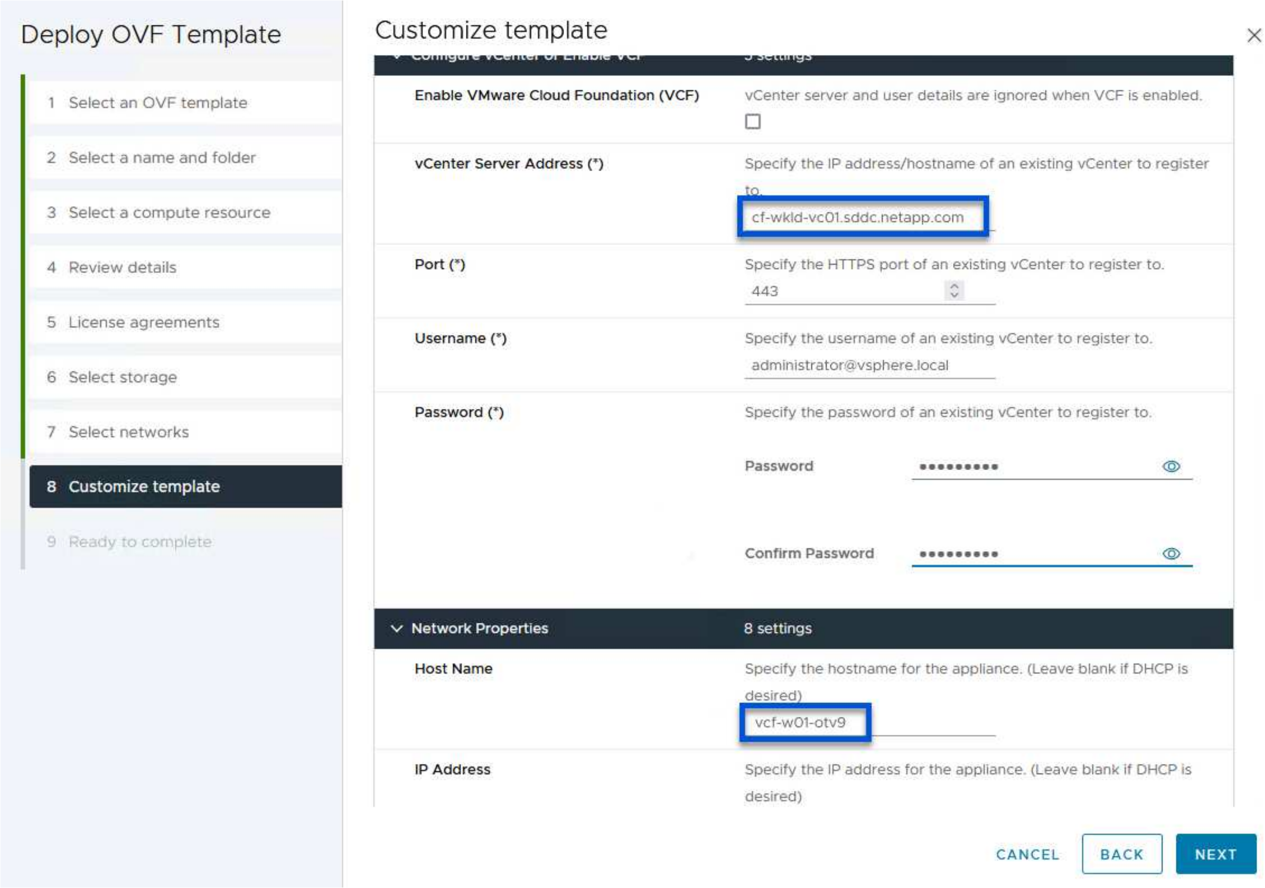
Password: ●●●●●●●●●
Confirm Password: ●●●●●●●●●

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

172.21.166.1

Maintenance User Password (*) — Password to assign to maint user account.

Password: ●●●●●●●●●
Confirm Password: ●●●●●●●●●



Deploy OVF Template

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

Customize template ✕

Configure vCenter or Enable VCF — 3 settings

Enable VMware Cloud Foundation (VCF) — vCenter server and user details are ignored when VCF is enabled.

□

vCenter Server Address (*) — Specify the IP address/hostname of an existing vCenter to register to.

cf-wkld-vc01.sddc.netapp.com

Port (*) — Specify the HTTPS port of an existing vCenter to register to.

443

Username (*) — Specify the username of an existing vCenter to register to.

administrator@vsphere.local

Password (*) — Specify the password of an existing vCenter to register to.

Password: ●●●●●●●●●
Confirm Password: ●●●●●●●●●

Network Properties — 8 settings

Host Name — Specify the hostname for the appliance. (Leave blank if DHCP is desired)

vcf-w01-otv9

IP Address — Specify the IP address for the appliance. (Leave blank if DHCP is desired)

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

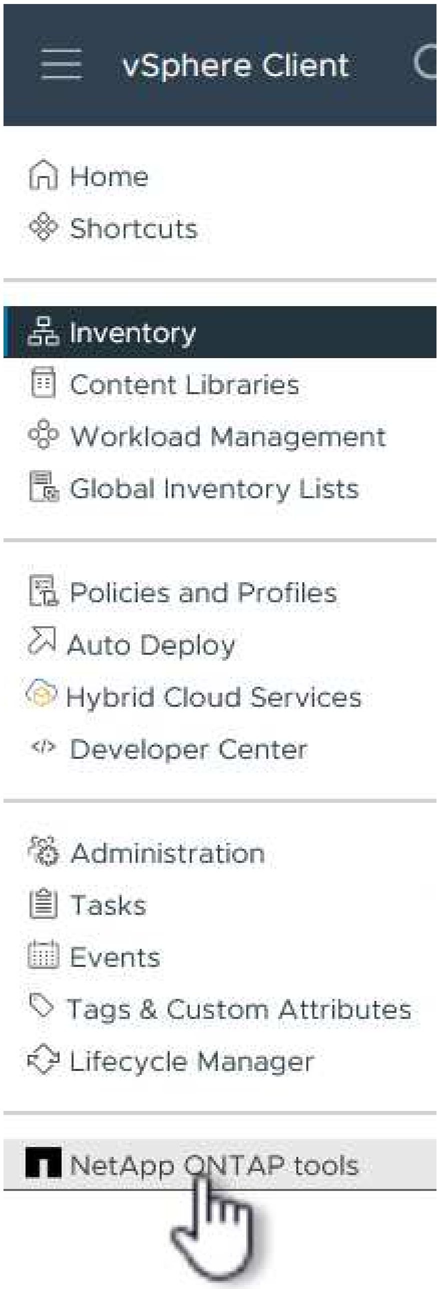
Step 2: Add a storage system

Perform the following steps to add a storage system using ONTAP tools.

Steps

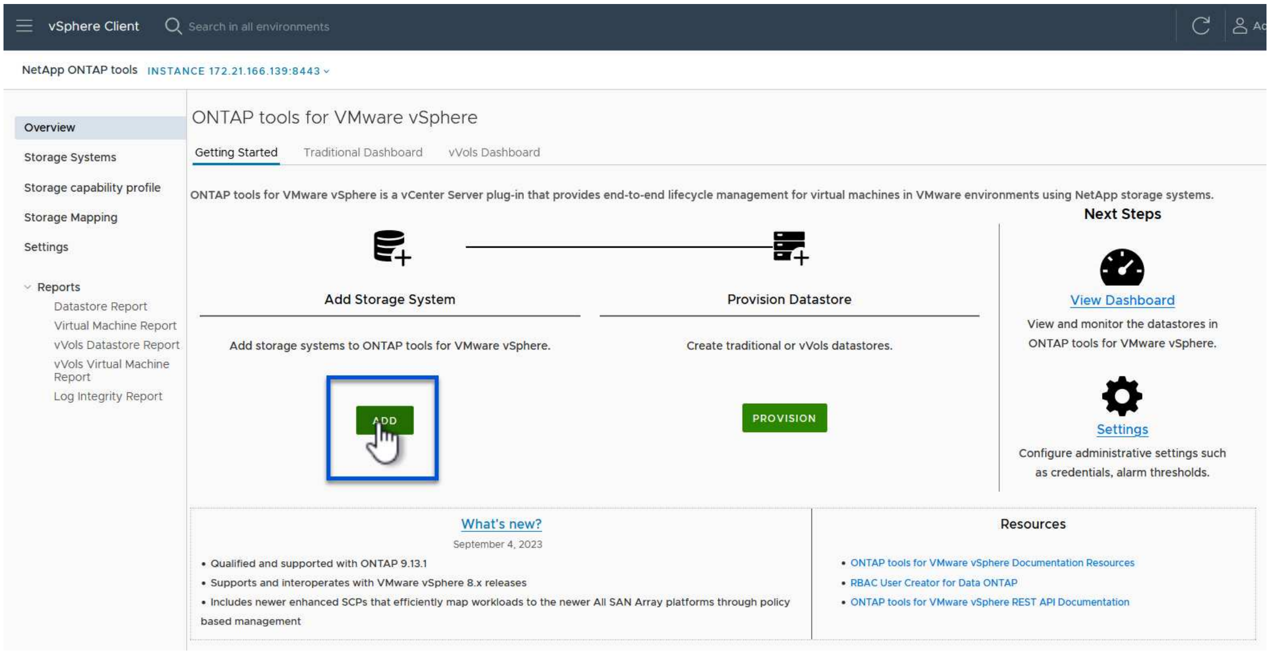
1. In the vSphere client navigate to the main menu and select **NetApp ONTAP tools**.

   Show example



2. Once in **ONTAP tools**, from the Getting Started page (or from **Storage Systems**), click **Add** to add a new storage system.

Show example



ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.

Add storage systems to ONTAP tools for VMware vSphere.

Create traditional or vVols datastores.

View and monitor the datastores in ONTAP tools for VMware vSphere.

Configure administrative settings such as credentials, alarm thresholds.

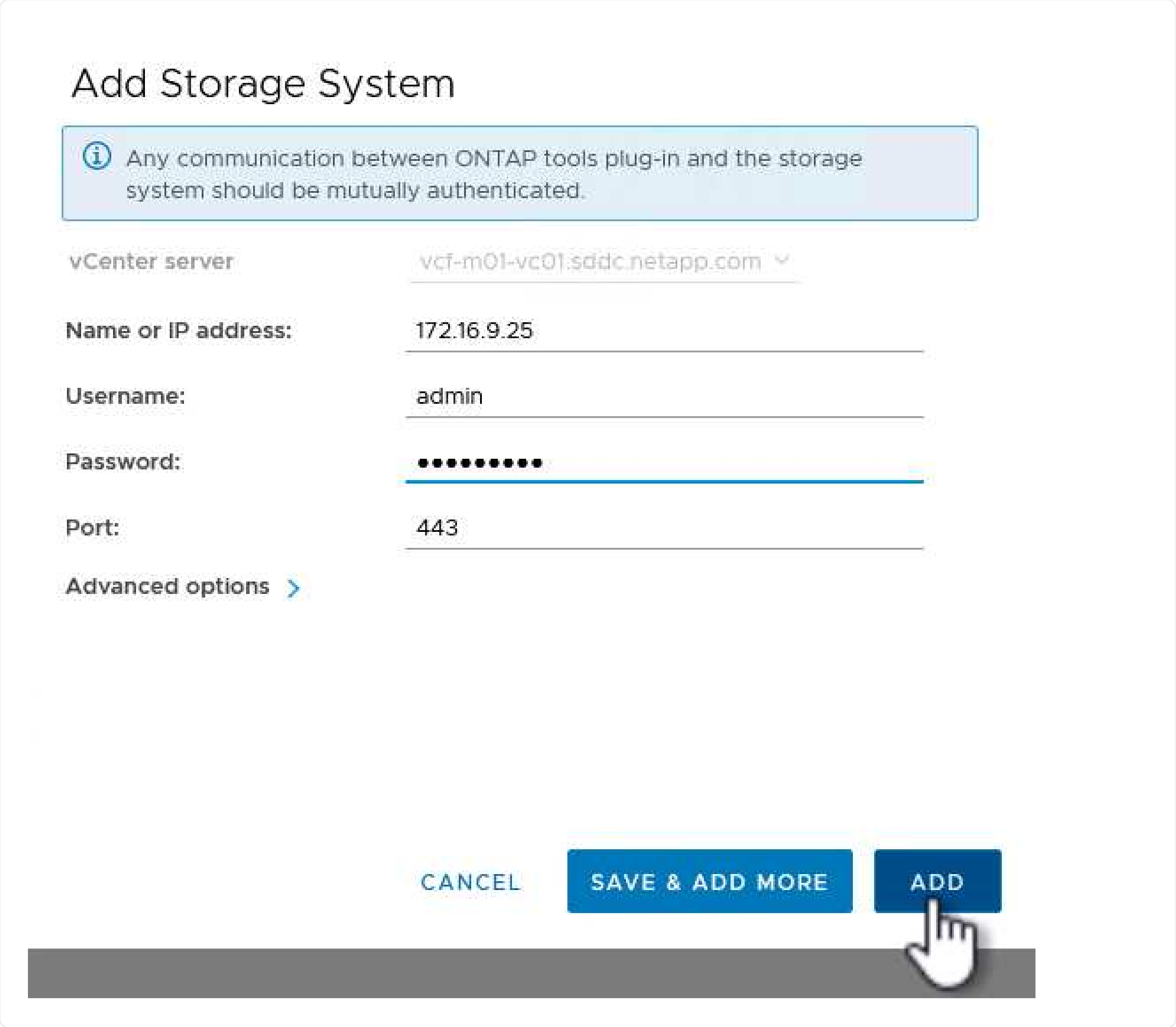
September 4, 2023

- Qualified and supported with ONTAP 9.13.1
- Supports and interoperates with VMware vSphere 8.x releases
- Includes newer enhanced SCPs that efficiently map workloads to the newer All SAN Array platforms through policy based management

- ONTAP tools for VMware vSphere Documentation Resources
- RBAC User Creator for Data ONTAP
- ONTAP tools for VMware vSphere REST API Documentation

3. Provide the IP address and credentials of the ONTAP storage system and click **Add**.

Show example



Add Storage System

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

vCenter server: vcf-m01-vc01.sddc.netapp.com

Name or IP address: 172.16.9.25

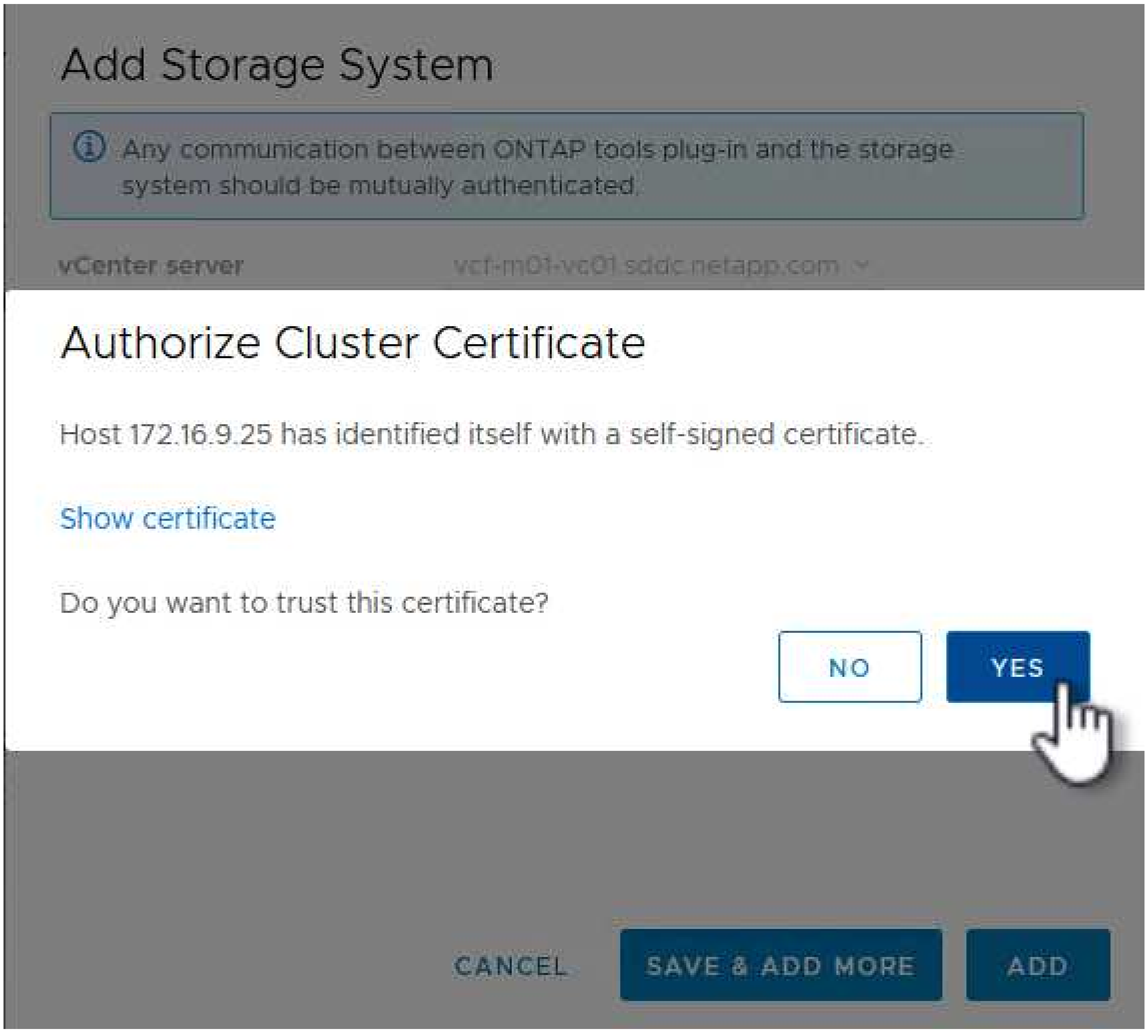
Username: admin

Password: ●●●●●●●●●●

Port: 443

4. Click **Yes** to authorize the cluster certificate and add the storage system.

Show example



Add Storage System

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

vCenter server vcf-m01-vc01.sddc.netapp.com

Authorize Cluster Certificate

Host 172.16.9.25 has identified itself with a self-signed certificate.

Show certificate

Do you want to trust this certificate?

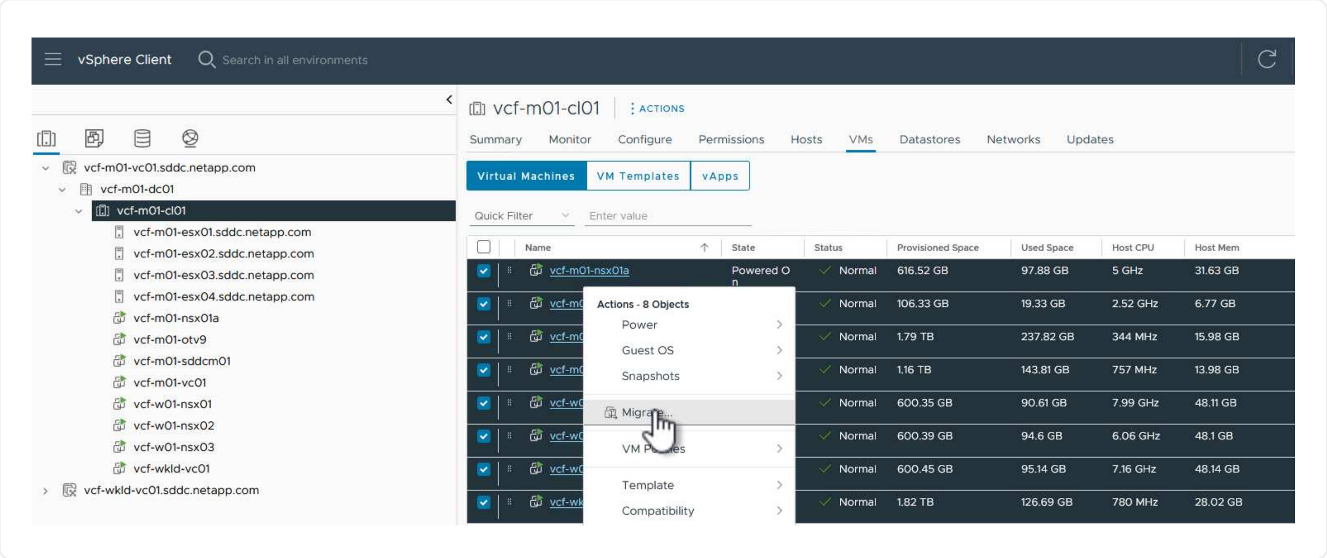
Optional: Migrate management VMs to the iSCSI datastore

In cases where you prefer to use ONTAP storage to protect the VCF management VMs, use vMotion to migrate the VMs to the newly created iSCSI datastore.

Steps

1. From the vSphere Client navigate to the management domain cluster and click the **VMs** tab.
2. Select the VMs to be migrated to the iSCSI datastore, right click and select **Migrate..**.

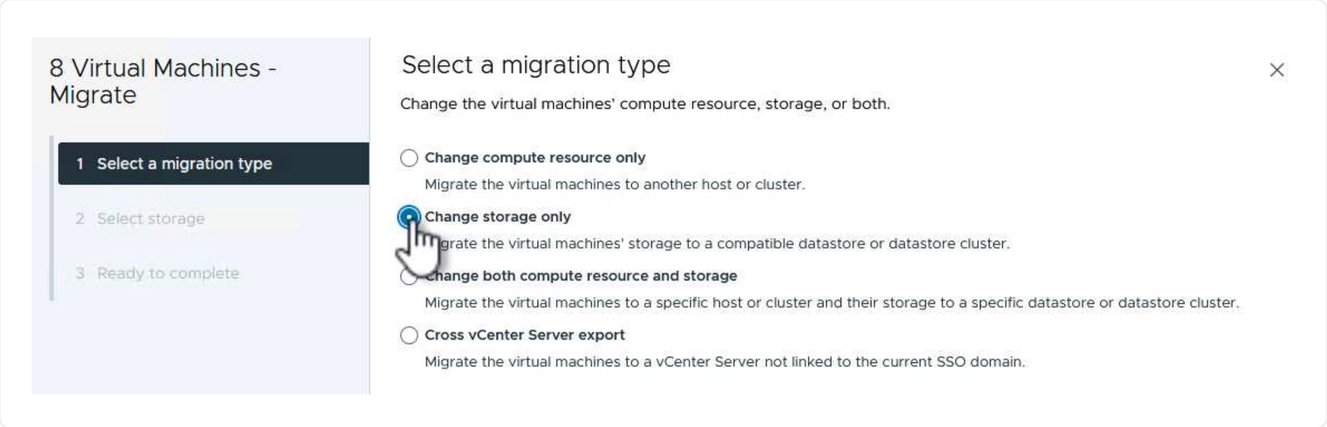
Show example



☑	Name	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
☑	vcf-m01-nsx01a	Powered On	✓ Normal	616.52 GB	97.88 GB	5 GHz	31.63 GB
☑	vcf-m0		✓ Normal	106.33 GB	19.33 GB	2.52 GHz	6.77 GB
☑	vcf-m0		✓ Normal	1.79 TB	237.82 GB	344 MHz	15.98 GB
☑	vcf-m0		✓ Normal	1.16 TB	143.81 GB	757 MHz	13.98 GB
☑	vcf-w0		✓ Normal	600.35 GB	90.61 GB	7.99 GHz	48.11 GB
☑	vcf-w0		✓ Normal	600.39 GB	94.6 GB	6.06 GHz	48.1 GB
☑	vcf-w0		✓ Normal	600.45 GB	95.14 GB	7.16 GHz	48.14 GB
☑	vcf-wk		✓ Normal	1.82 TB	126.69 GB	780 MHz	28.02 GB

3. In the **Virtual Machines - Migrate** wizard, select **Change storage only** as the migration type and click **Next** to continue.

Show example



Select a migration type

Change the virtual machines' compute resource, storage, or both.

○ **Change compute resource only**
Migrate the virtual machines to another host or cluster.

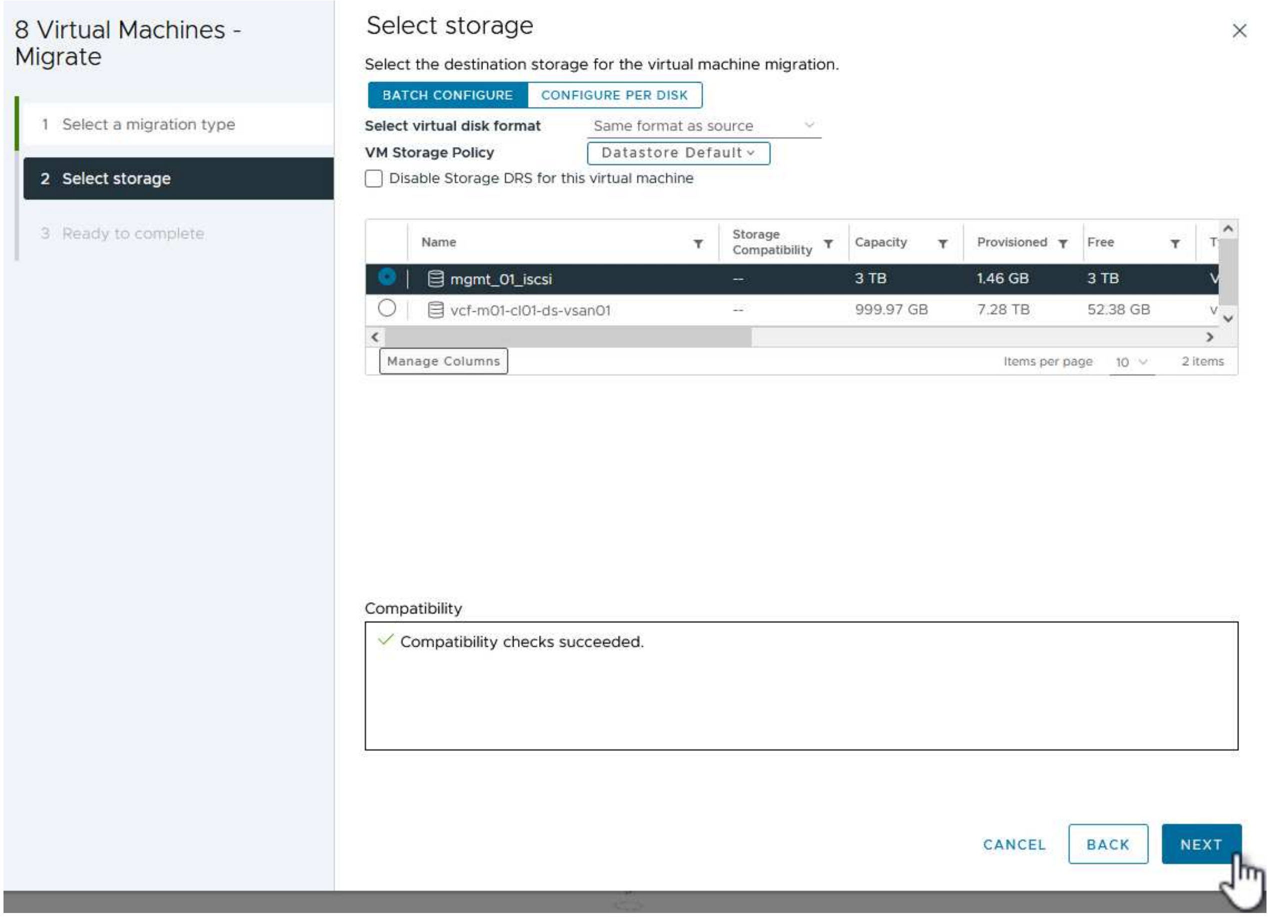
● **Change storage only**
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

○ **Change both compute resource and storage**
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

○ **Cross vCenter Server export**
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

4. On the **Select storage** page, select the iSCSi datastore and select **Next** to continue.

Show example



8 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE | CONFIGURE PER DISK

Select virtual disk format: Same format as source

VM Storage Policy: Datastore Default

□ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	mgmt_01_iscsi	--	3 TB	1.46 GB	3 TB	V
○	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.28 TB	52.38 GB	V

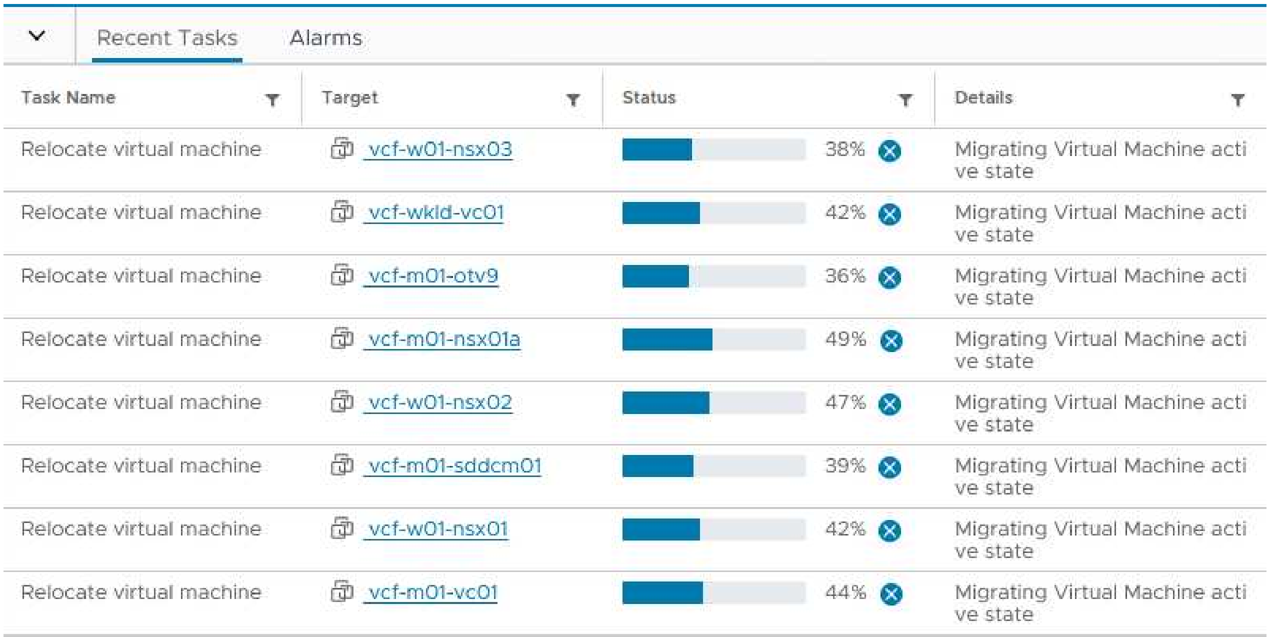
Manage Columns — Items per page 10 — 2 items

Compatibility

✓ Compatibility checks succeeded.

5. Review the selections and click **Finish** to start the migration.
6. The relocation status can be viewed from the **Recent Tasks** pane.

Show example



Task Name	Target	Status	Details
Relocate virtual machine	vcf-w01-nsx03	38%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-wkld-vc01	42%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-otv9	36%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-nsx01a	49%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-w01-nsx02	47%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-sddcm01	39%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-w01-nsx01	42%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-vc01	44%	Migrating Virtual Machine active state

Additional information

- For information on configuring ONTAP storage systems, refer to ONTAP 9 documentation.
- For information on configuring VCF, refer to VMware Cloud Foundation documentation.
- For information on using VMFS iSCSI datastores with VMware, refer to vSphere VMFS datastore - iSCSI storage backend with ONTAP.
- For video demos of this solution, refer to VMware datastore provisioning.

Add an FC-based VMFS datastore as supplemental storage for a management domain using ONTAP tools for VMware vSphere

In this use case we outline how to configure a VMFS datastore over Fibre Channel (FC) as supplemental storage for the VMware Cloud Foundation (VCF) management domain. This procedure summarizes the steps to deploy ONTAP tools on the management domain, add a storage backend, and provision the datastore.

Before you begin

Make sure the following components and configurations are in place.

- An ONTAP storage system with FC ports connected to FC switches.
- SVM created with FC LIFs.
- vSphere with FC HBAs connected to FC switches.
- Single initiator-target zoning is configured on FC switches.

- ◦ Use SVM FC logical interface in zone configuration rather than physical FC ports on ONTAP systems.
- ◦ Use multipath for FC LUNs.

Steps

1. Deploy ONTAP tools on the management domain by following the instructions in the ONTAP tools for VMware vSphere documentation: Deploy ONTAP tools on management domain.

   The ONTAP tools for VMware vSphere appliance is deployed as a small-sized single node with core services to support NFS and VMFS datastores.

2. Add a storage backend using the vSphere client interface by following the instructions in the ONTAP tools for VMware vSphere documentation: Define Storage backend using vSphere client interface.

   Adding a storage backend enables you to onboard an ONTAP cluster.

3. Provision VMFS on FC by following the instructions in the ONTAP tools for VMware vSphere documentation: Provision VMFS on FC.

Additional information

- For information about configuring ONTAP storage systems, refer to ONTAP 9 documentation.
- For information about configuring VCF, refer to the VMware Cloud Foundation documentation.
- For information about configuring Fibre Channel on ONTAP storage systems, refer to the ONTAP 9 documentation SAN storage management.
- For more information about using VMFS with ONTAP storage systems, refer to the Deployment guide for VMFS.
- For video demos of this solution, refer to VMware datastore provisioning.

Expand VI workload domains with vVols iSCSI

Deployment workflow for adding an iSCSI vVols datastore as supplemental storage in a VI workload domain

Get started with configuring a iSCI vVols datastore as supplemental storage in a VMware Cloud Foundation (VCF) Virtual Infrastructure (VI) workload domain. You’ll create the SVM and LIFs, set up iSCSI networking, deploy ONTAP tools for VMware vSphere, and configure storage.

1 **Review the deployment requirements**

Review the requirements to deploy iSCSI vVols in a VMware Cloud Foundation VI workload domain.

2 **Create the SVM and LIFs**

Create an SVM with multiple LIFs for iSCSI traffic.

3 **Configure networking**

Set up networking for iSCSI on ESXi hosts.

4 **Configure storage**

Deploy and use ONTAP tools to configure storage.

Deployment requirements for iSCSI vVols in a VI workload domain

Review the recommended network design and infrastructure requirements to deploy iSCSI vVols in a VMware Cloud Foundation VI workload domain. You need a fully configured ONTAP AFF or ASA storage system, a completed VCF management domain, and an existing VI workload domain.

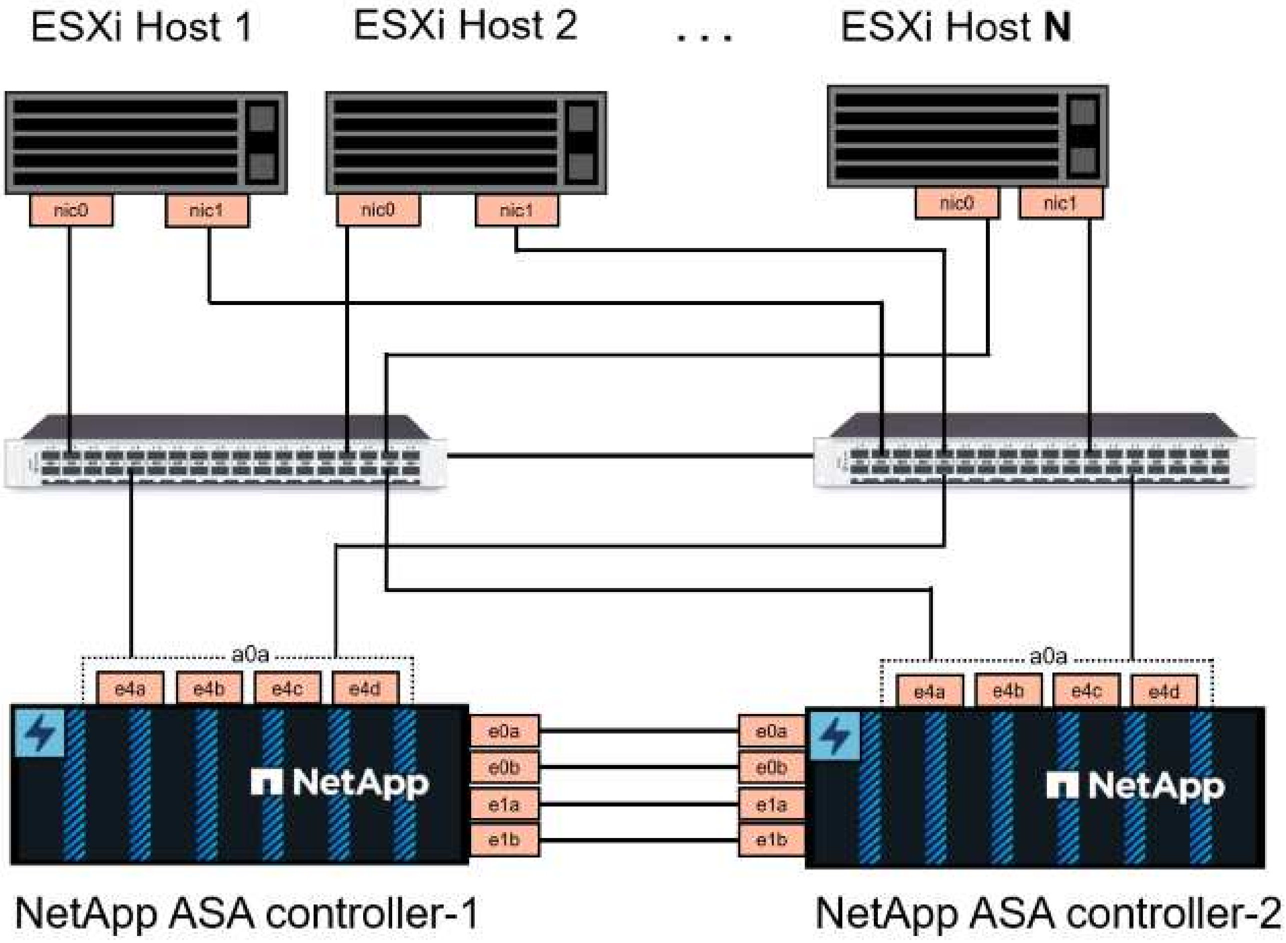
Infrastructure requirements

Make sure the following components and configurations are in place.

- An ONTAP AFF or ASA storage system with physical data ports on Ethernet switches dedicated to storage traffic.
- The VCF management domain deployment is complete and the vSphere client is accessible.
- A VI workload domain has been previously deployed.

Recommended iSCSI network design

You should configure fully redundant network designs for iSCSI. The following diagram illustrates an example of a redundant configuration. It provides fault tolerance for storage systems, switches, networks adapters, and host systems. For additional information, refer to the NetApp SAN configuration reference.



For multipathing and failover across multiple paths, create a minimum of two LIFs per storage node in separate Ethernet networks for all SVMs in iSCSI configurations.

> In situations where multiple VMkernel adapters are configured on the same IP network, use software iSCSI port binding on the ESXi hosts to ensure that load balancing across the adapters occurs. Refer to KB article Considerations for using software iSCSI port binding in ESX/ESXi.

What's next?

After reviewing the deployment requirements, create the SVM and LIFs.

Create SVM and LIFs for iSCSI vVols datastores in a VCF VI workload domain

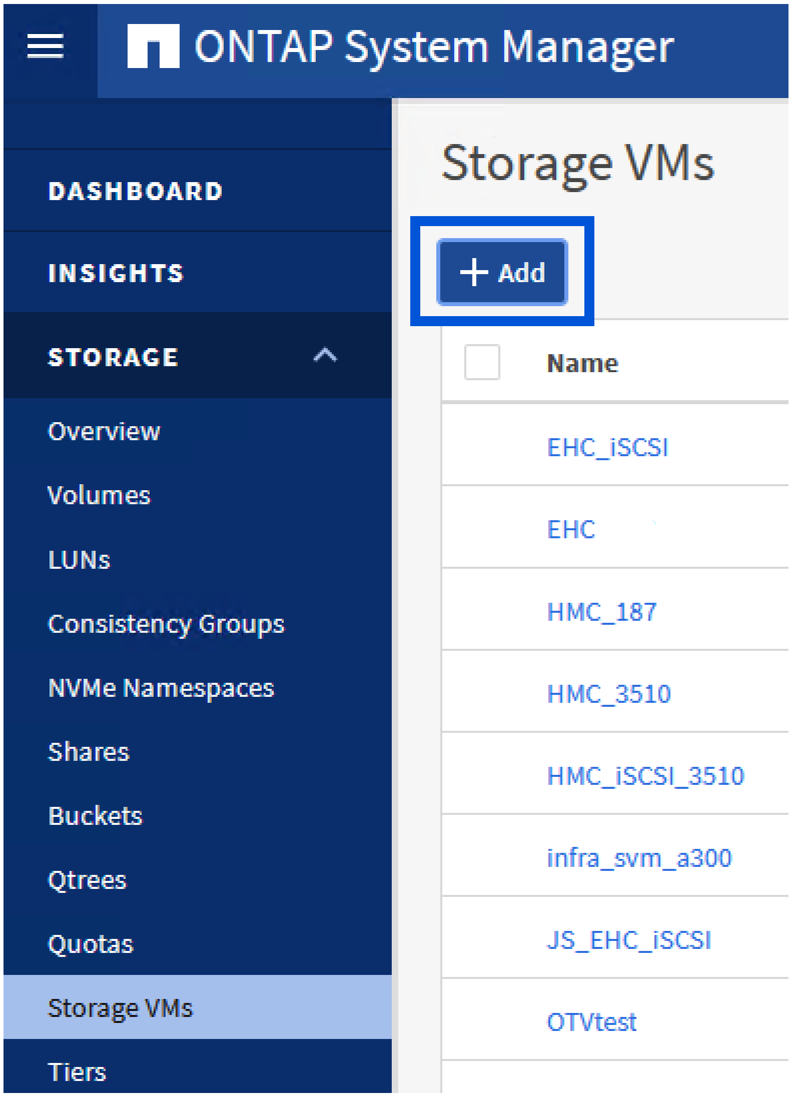
Create a Storage Virtual Machine (SVM) and multiple logical interfaces (LIFs) on an ONTAP system to support iSCSI traffic for vVols datastores in a VMware Cloud Foundation VI workload domain. You'll add a new SVM, enable iSCSI, configure LIFs, and optionally enable the Storage VM Administration account.

To add new LIFs to an existing SVM, refer to the ONTAP documentation: Create ONTAP LIFs.

Steps

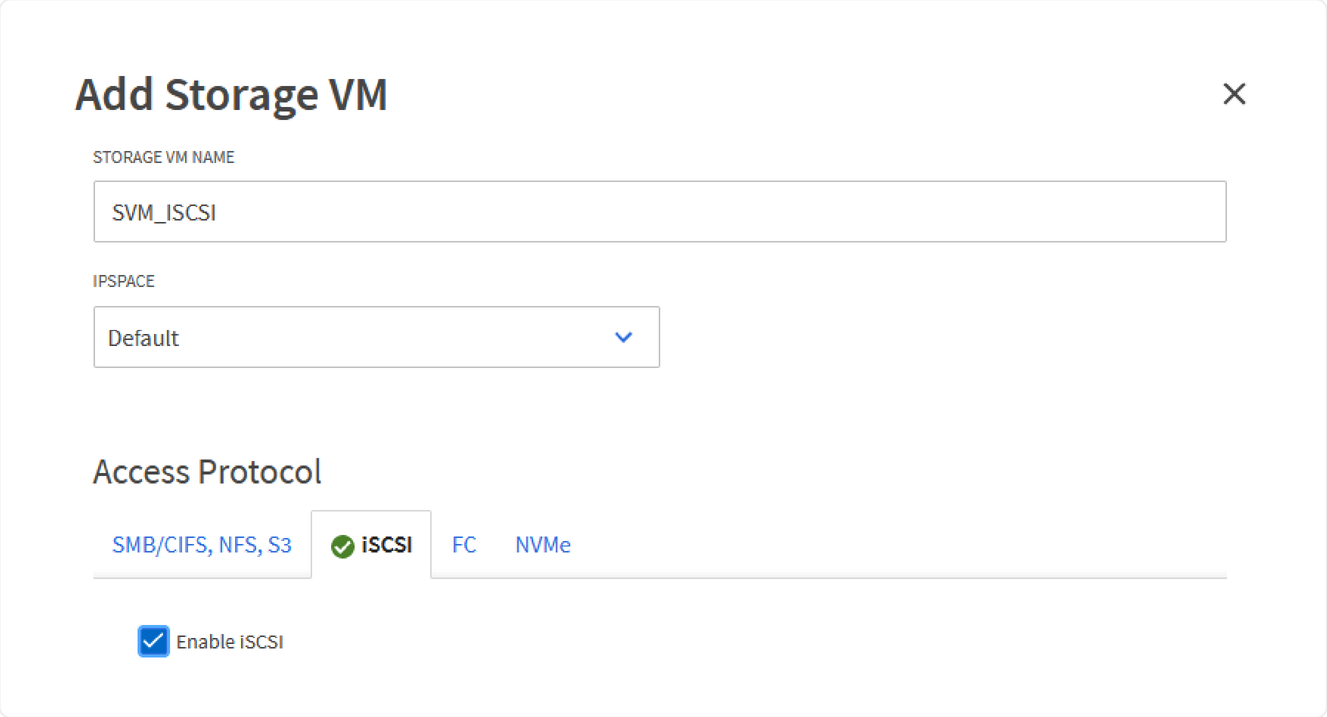
1. From ONTAP System Manager navigate to **Storage VMs** in the left-hand menu and click **+ Add** to start.

Show example



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

Show example



Add Storage VM

STORAGE VM NAME

SVM_ISCSI

IPSPACE

Default

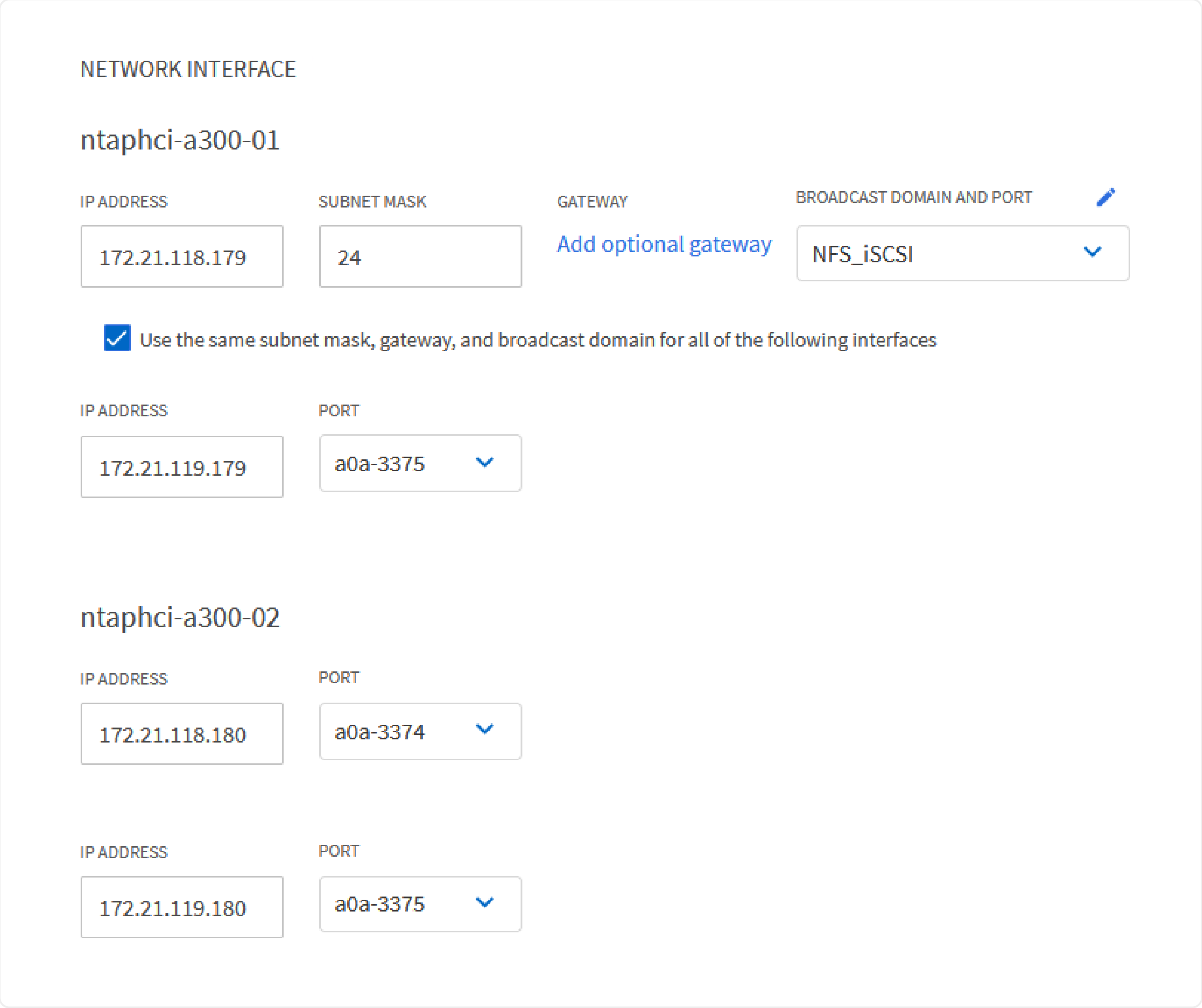
Access Protocol

☑ Enable iSCSI

3. In the **Network Interface** section fill in the **IP address**, **Subnet Mask**, and **Broadcast Domain and Port** for the first LIF. For subsequent LIFs, you can either use individual settings or enable the checkbox to use common settings across all remaining LIFs.

> ⓘ For multipathing and failover across multiple paths, create a minimum of two LIFs per storage node in separate Ethernet networks for all SVMs in iSCSI configurations.

Show example



NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS	SUBNET MASK	GATEWAY	BROADCAST DOMAIN AND PORT
172.21.118.179	24	Add optional gateway	NFS_iSCSI

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

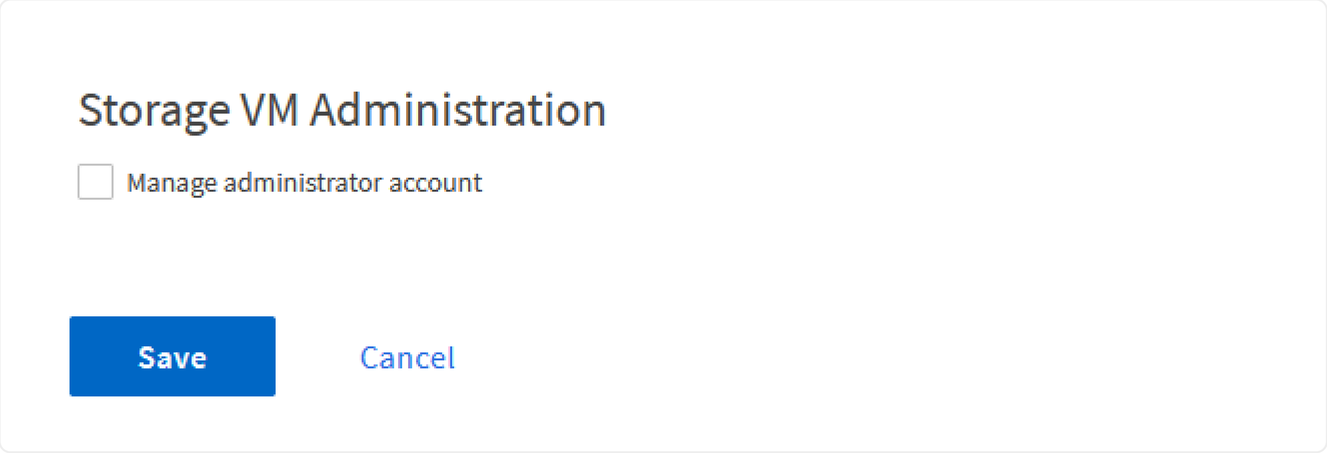
IP ADDRESS	PORT
172.21.119.179	a0a-3375

ntaphci-a300-02

IP ADDRESS	PORT
172.21.118.180	a0a-3374
172.21.119.180	a0a-3375

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

Show example



Storage VM Administration

□ Manage administrator account

What’s next?

After you create the SVM and LIFs, configure networking for iSCSI on ESXi hosts.

Configure networking for iSCSI on ESXi hosts in a VCF VI workload domain

Configure networking for iSCSI storage on ESXi hosts in a VI workload domain. You’ll create distributed port groups for iSCSI traffic and set up VMkernel adapters using the vSphere client to enable reliable connectivity and multipathing.

Use the vSphere client with vCenter Single Sign-On to perform these steps on the VI Workload Domain cluster. The same vSphere client manages both the management and workload domains.

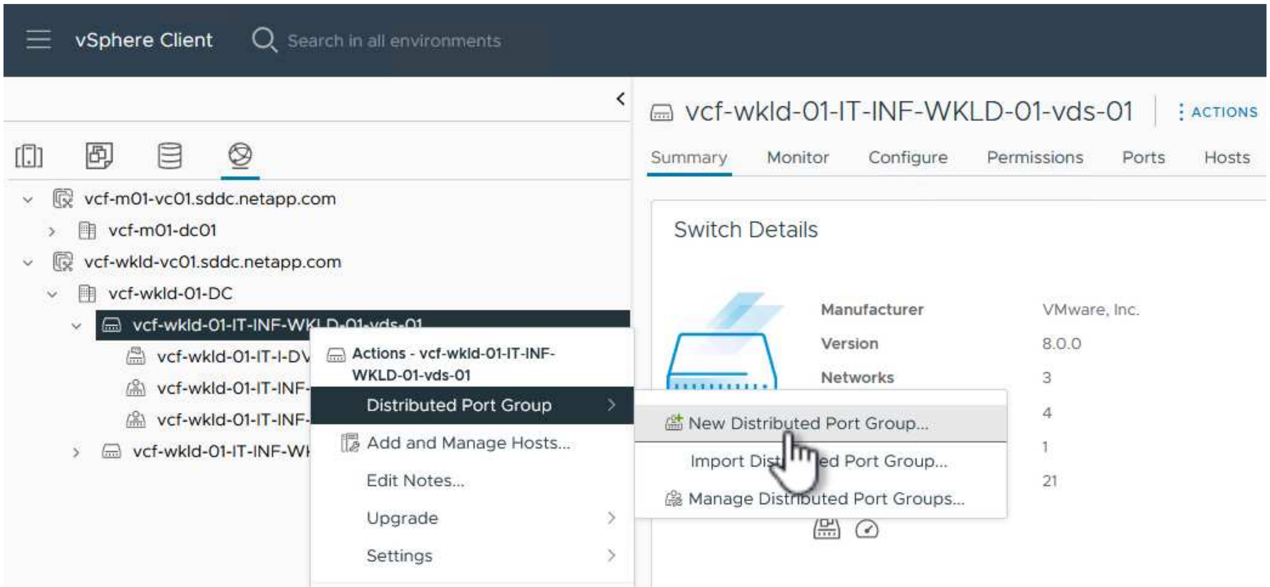
Step 1: Create distributed port groups for iSCSI traffic

Complete the following steps to create a new distributed port group for each iSCSI network.

Steps

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 a new **Distributed Port Group…**.

   Show example

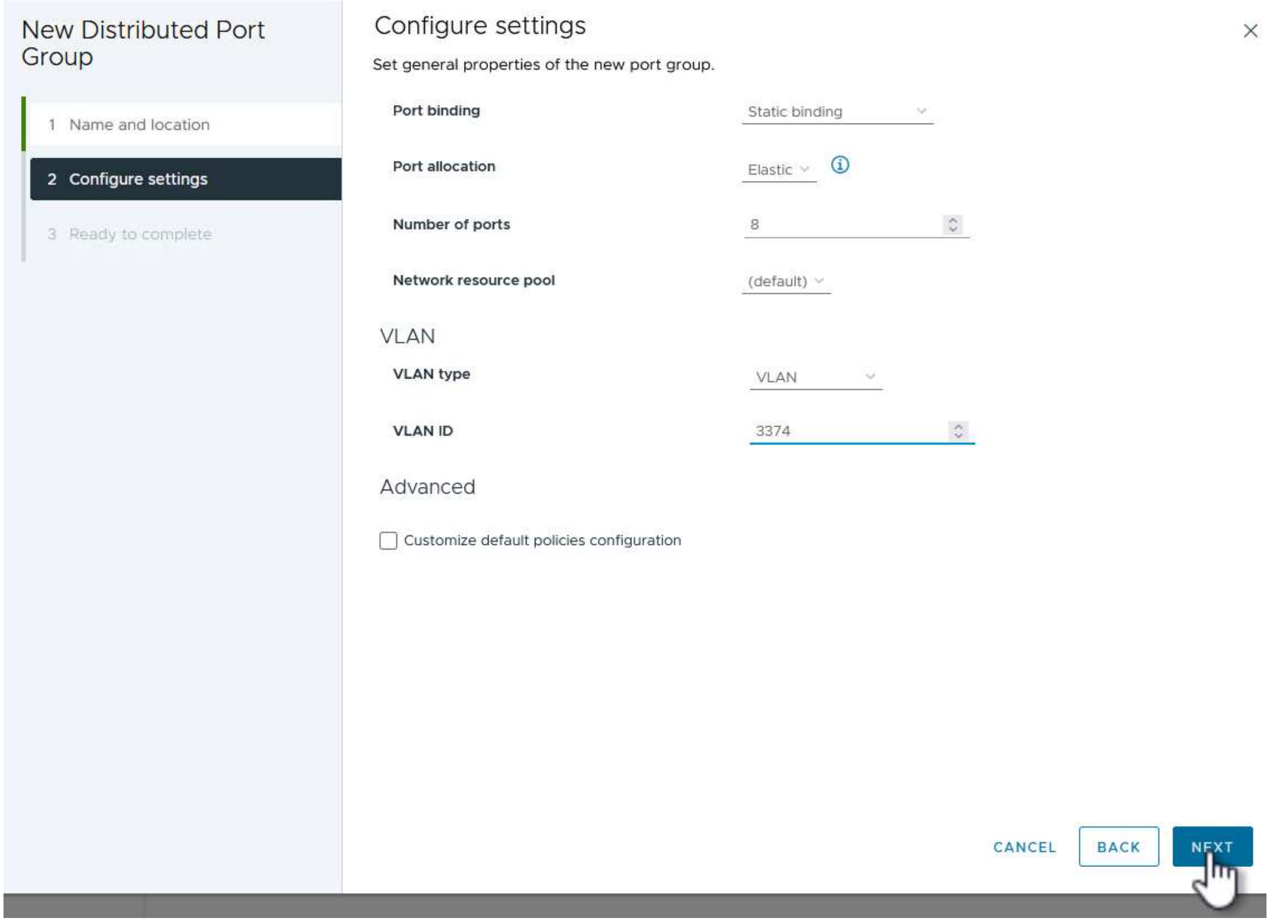

vSphere Client
Search in all environments
vcf-wkld-01-IT-INF-WKLD-01-vds-01
ACTIONS
Summary
Monitor
Configure
Permissions
Ports
Hosts
vcf-m01-vc01.sddc.netapp.com
vcf-m01-dc01
vcf-wkld-vc01.sddc.netapp.com
vcf-wkld-01-DC
vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-IT-I-DV
vcf-wkld-01-IT-INF-
vcf-wkld-01-IT-INF-
vcf-wkld-01-IT-INF-WI
Actions - vcf-wkld-01-IT-INF-WKLD-01-vds-01
Distributed Port Group
Add and Manage Hosts...
Edit Notes...
Upgrade
Settings
New Distributed Port Group...
Import Distributed Port Group...
Manage Distributed Port Groups...
Switch Details

Manufacturer	VMware, Inc.
Version	8.0.0
Networks	3
	4
	1
	21

2. In the **New Distributed Port Group** wizard, fill in a name for the new port group and then click **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 **Next** to continue.

Show example



New Distributed Port Group

1 Name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

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

VLAN

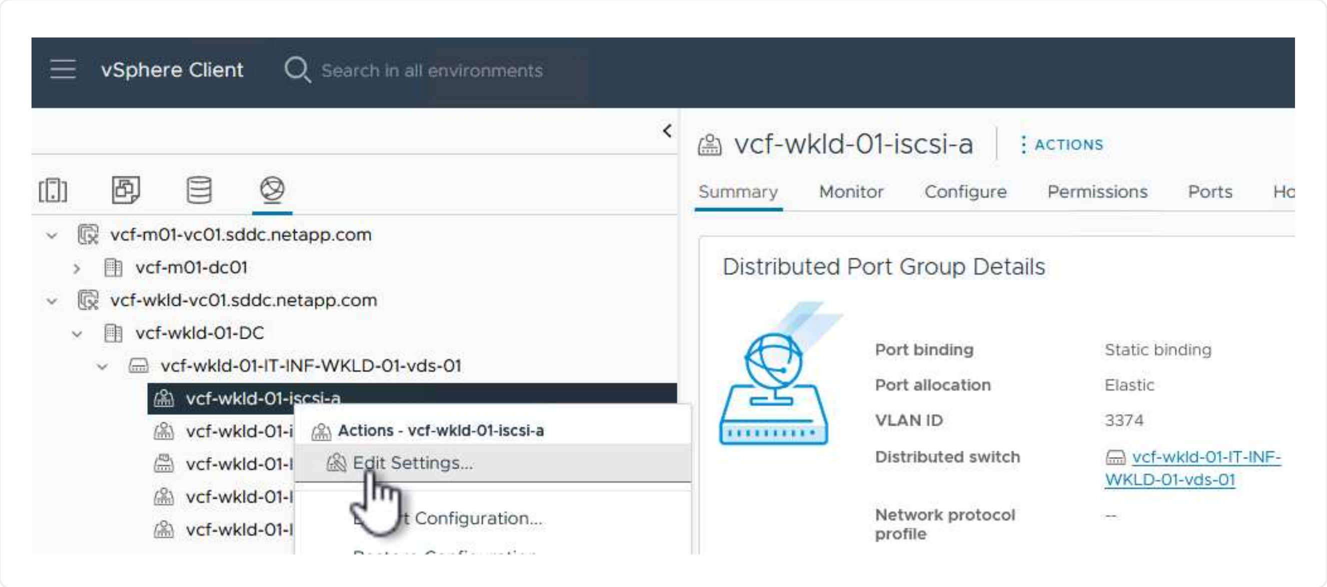
VLAN type	VLAN
VLAN ID	3374

Advanced

□ Customize default policies configuration

4. On the **Ready to complete** page, review the changes and click **Finish** to create the new distributed port group.
5. Repeat this process to create a distributed port group for the second iSCSI network being used and ensure you have input the correct **VLAN ID**.
6. Once both port groups have been created, navigate to the first port group and select the action to **Edit settings…**.

Show example

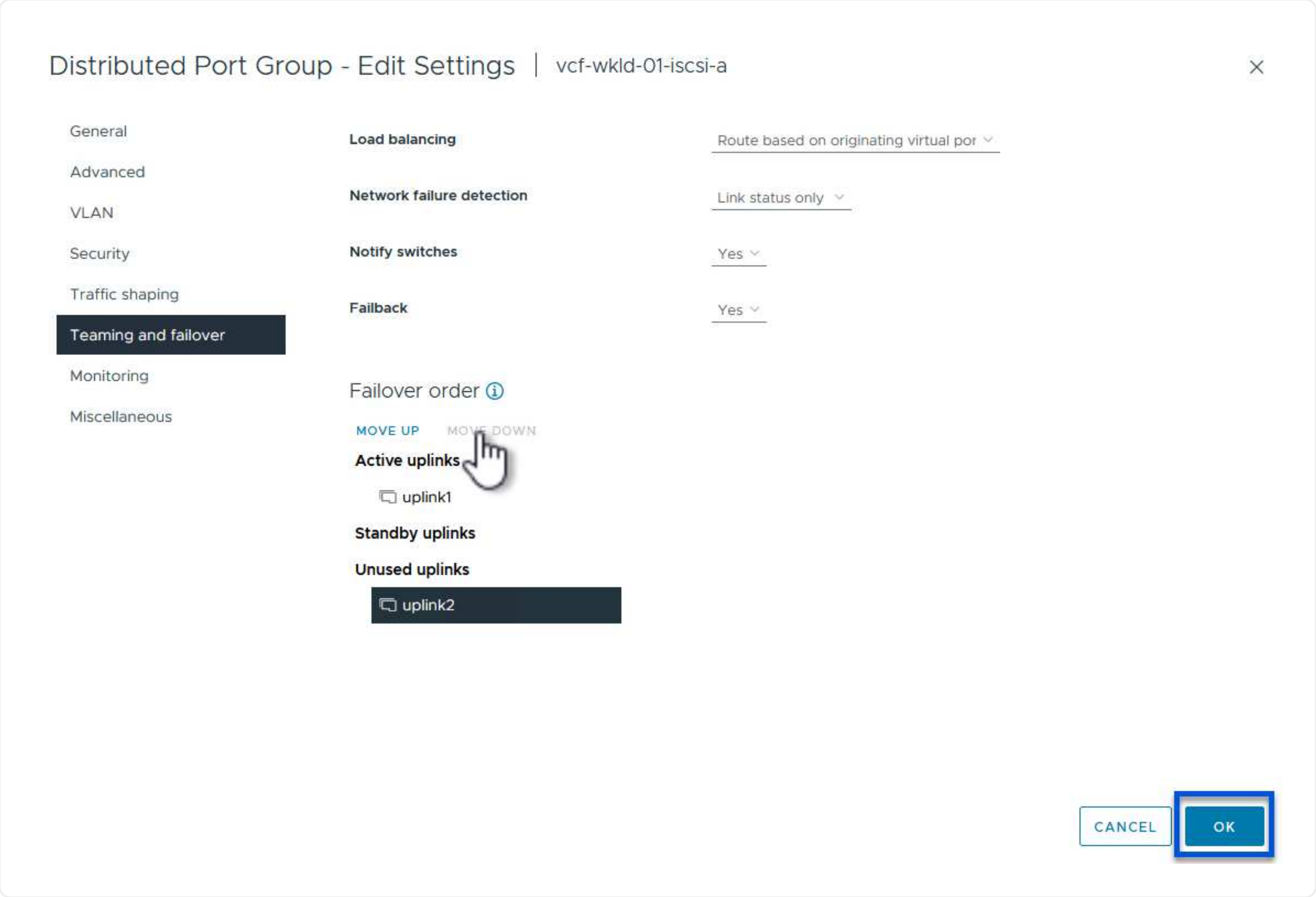


Distributed Port Group Details

Port binding	Static binding
Port allocation	Elastic
VLAN ID	3374
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01
Network protocol profile	--

7. On **Distributed Port Group - Edit Settings** page, navigate to **Teaming and failover** in the left-hand menu and click **uplink2** to move it down to **Unused uplinks**.

Show example



Load balancing	Route based on originating virtual por
Network failure detection	Link status only
Notify switches	Yes
Failback	Yes

Failover order

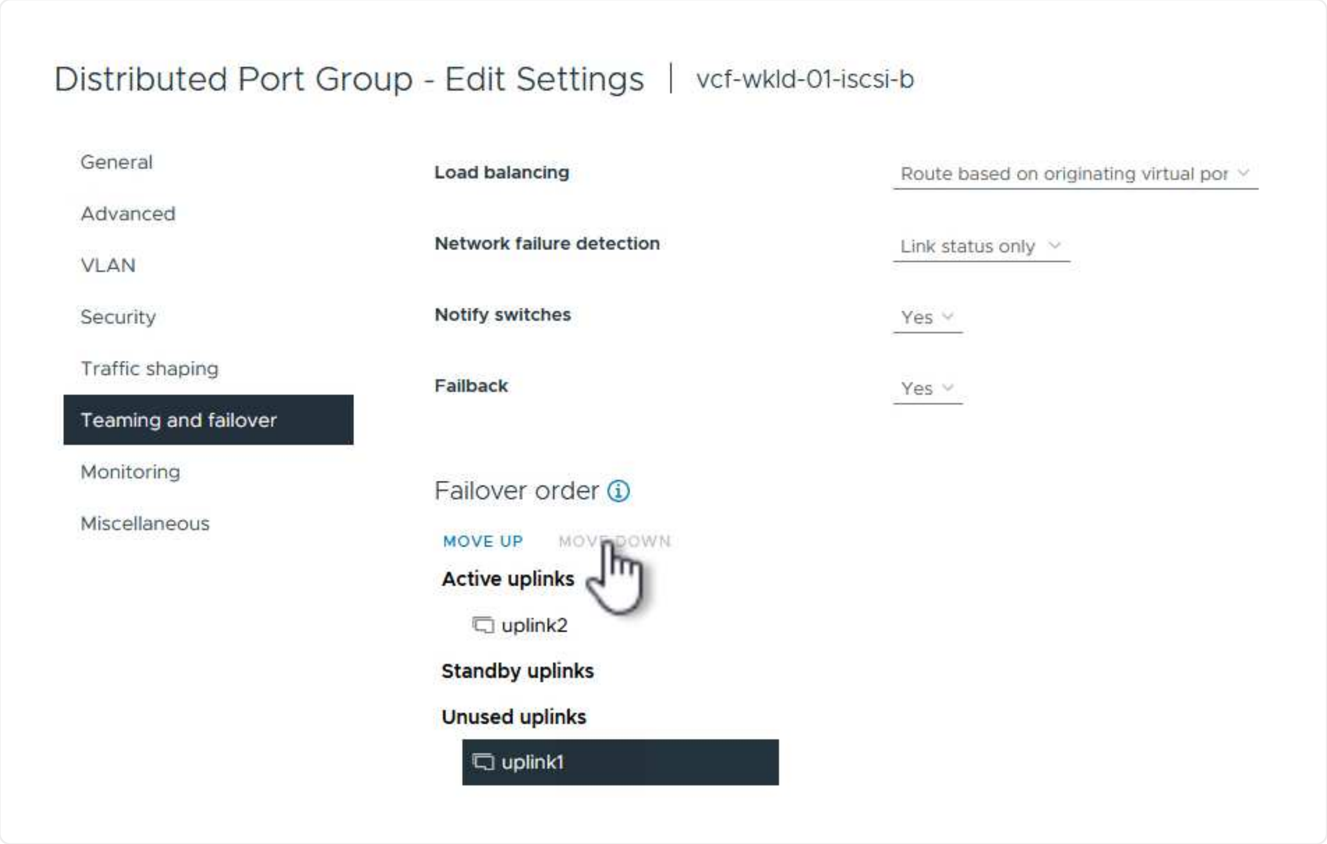
Active uplinks
- uplink1

Standby uplinks

Unused uplinks
- uplink2

8. Repeat this step for the second iSCSI port group. However, this time move **uplink1** down to **Unused uplinks**.

Show example



Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-b

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing: Route based on originating virtual por

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

Failover order

MOVE UP MOVE DOWN

Active uplinks

uplink2

Standby uplinks

Unused uplinks

uplink1

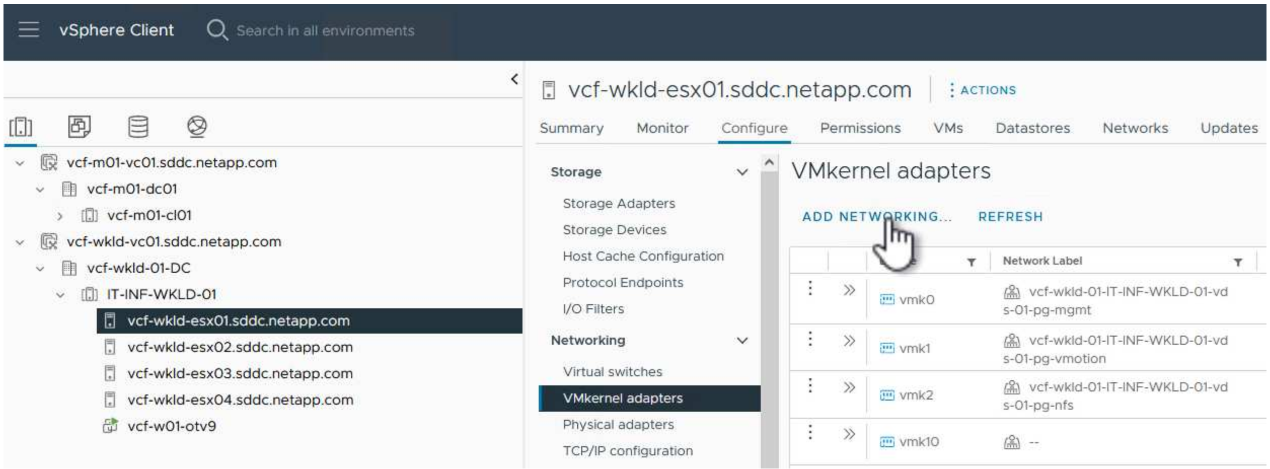
Step 2: Create VMkernel adapters on each ESXi host

Perform the following steps on each ESXi host in the workload domain using the vSphere client.

Steps

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 **Add Networking…** to start.

   Show example



vSphere Client   Search in all environments

- vcf-m01-vc01.sddc.netapp.com
  - vcf-m01-dc01
    - vcf-m01-cl01
- vcf-wkld-vc01.sddc.netapp.com
  - vcf-wkld-01-DC
    - IT-INF-WKLD-01
      - vcf-wkld-esx01.sddc.netapp.com
      - vcf-wkld-esx02.sddc.netapp.com
      - vcf-wkld-esx03.sddc.netapp.com
      - vcf-wkld-esx04.sddc.netapp.com
      - vcf-w01-otv9

vcf-wkld-esx01.sddc.netapp.com   ACTIONS

Summary   Monitor   Configure   Permissions   VMs   Datastores   Networks   Updates

Storage: Storage Adapters, Storage Devices, Host Cache Configuration, Protocol Endpoints, I/O Filters

Networking: Virtual switches, VMkernel adapters, Physical adapters, TCP/IP configuration

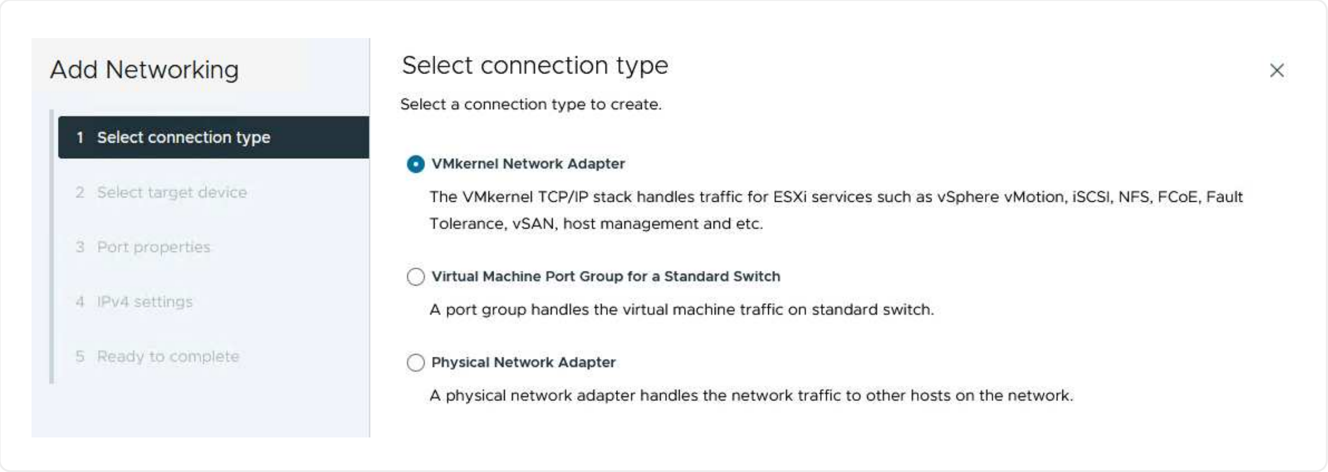
VMkernel adapters

ADD NETWORKING...   REFRESH

Device	Network Label
vmk0	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt
vmk1	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion
vmk2	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs
vmk10	--

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

Show example



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select connection type

Select a connection type to create.

● **VMkernel Network Adapter**

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

○ **Virtual Machine Port Group for a Standard Switch**

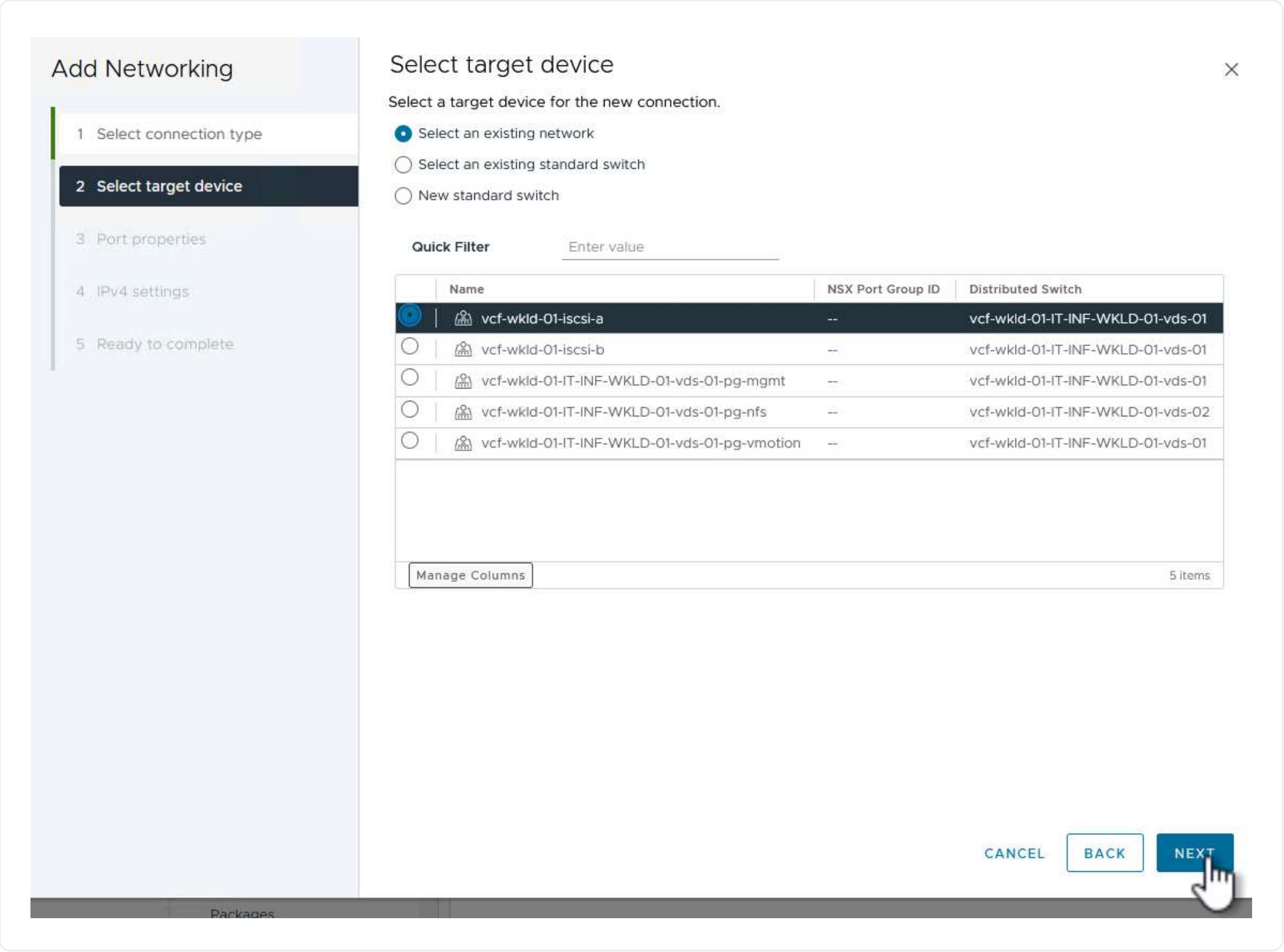
A port group handles the virtual machine traffic on standard switch.

○ **Physical Network Adapter**

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

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

Show example



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

● Select an existing network

○ Select an existing standard switch

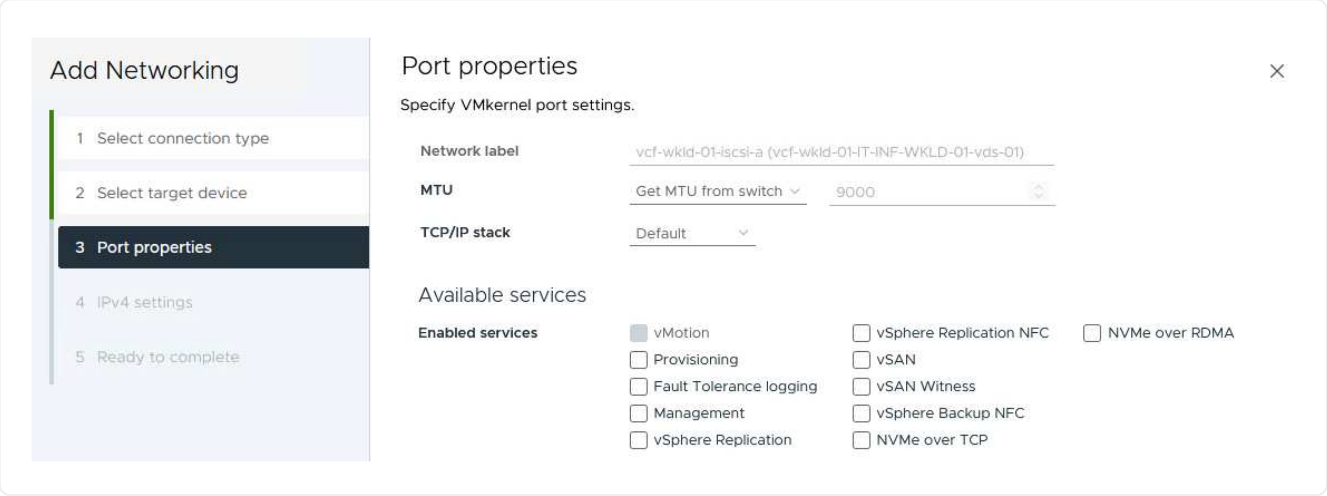
○ New standard switch

Quick Filter Enter value

	Name	NSX Port Group ID	Distributed Switch
●	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

4. On the **Port properties** page, keep the defaults and click **Next** to continue.

Show example



Add Networking

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

Port properties

Specify VMkernel port settings.

Network label: vcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)

MTU: Get MTU from switch 9000

TCP/IP stack: Default

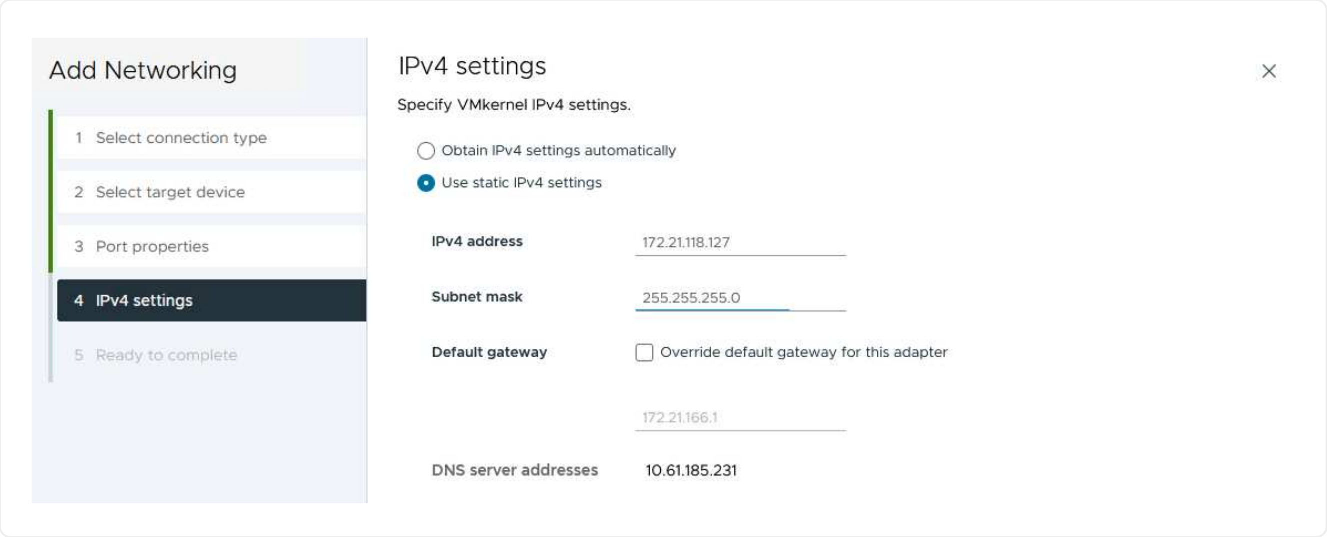
Available services

Enabled services

□ vMotion
□ Provisioning
□ Fault Tolerance logging
□ Management
□ vSphere Replication
□ vSphere Replication NFC
□ vSAN
□ vSAN Witness
□ vSphere Backup NFC
□ NVMe over TCP
□ NVMe over RDMA

5. On the **IPv4 settings** page, fill in the **IP address**, **Subnet mask**, and provide a new Gateway IP address (only if required). Click **Next** to continue.

Show example



Add Networking

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

IPv4 settings

Specify VMkernel IPv4 settings.

○ Obtain IPv4 settings automatically

● Use static IPv4 settings

IPv4 address: 172.21.118.127

Subnet mask: 255.255.255.0

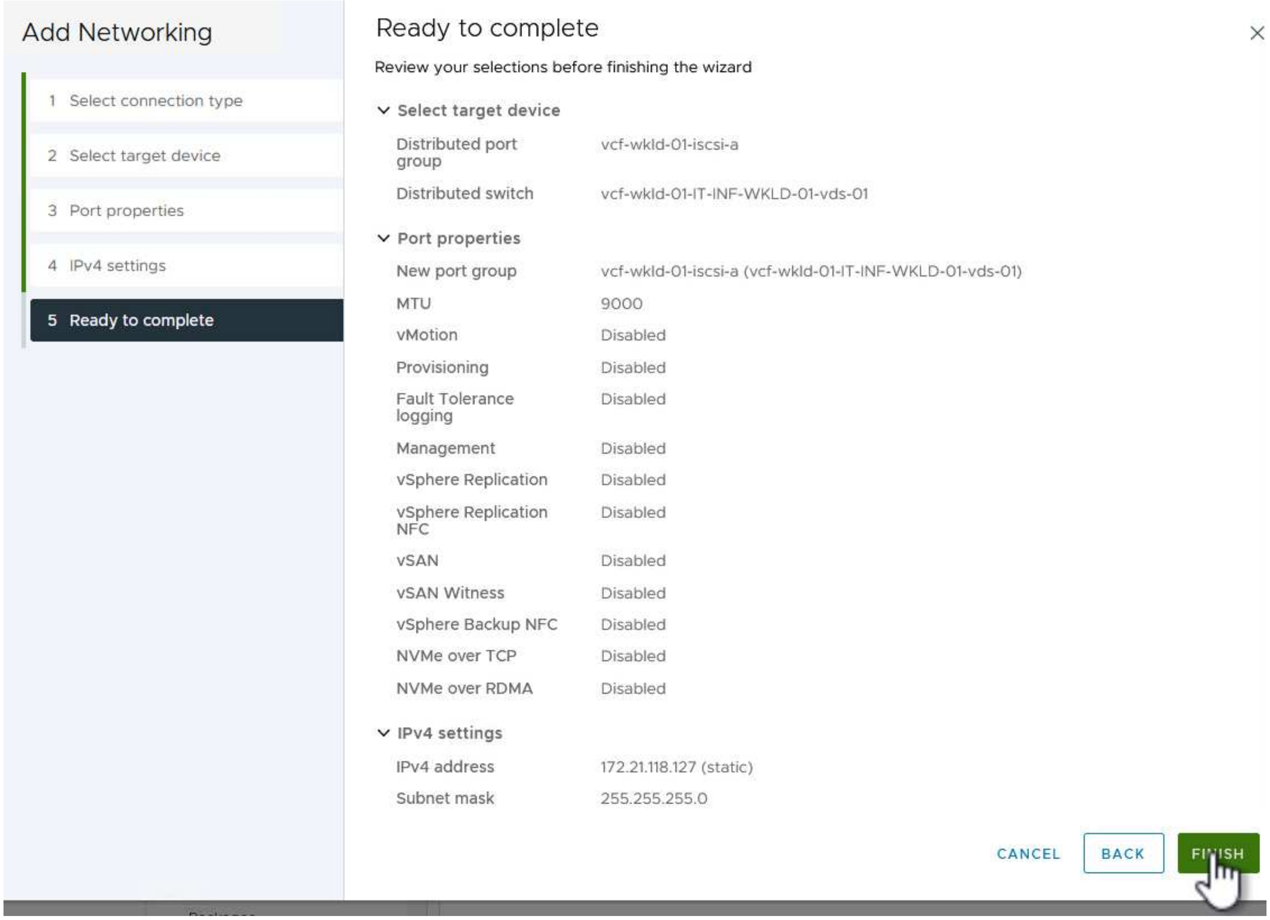
Default gateway: □ Override default gateway for this adapter

172.21.166.1

DNS server addresses: 10.61.185.231

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

Show example



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

Select target device

Distributed port group	vcf-wkld-01-iscsi-a
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Port properties

New port group	vcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Disabled
NVMe over RDMA	Disabled

IPv4 settings

IPv4 address	172.21.118.127 (static)
Subnet mask	255.255.255.0

7. Repeat this process to create a VMkernel adapter for the second iSCSI network.

What’s next?

After you configure networking for iSCSI on all ESXi hosts in the workload domain, configure storage for iSCSI vVols.

Configure iSCSI vVols storage in a VCF VI workload domain using ONTAP tools

Configure iSCSI vVols storage in a VI workload domain using ONTAP tools. You’ll deploy ONTAP tools for VMware vSphere, register a storage system, create a storage capability profile, and provision a vVols datastore in the vSphere client.

Step 1: Deploy ONTAP tools for VMware vSphere

For VI workload domains, ONTAP tools is installed to the VCF Management Cluster but registered with the vCenter associated with the VI workload domain.

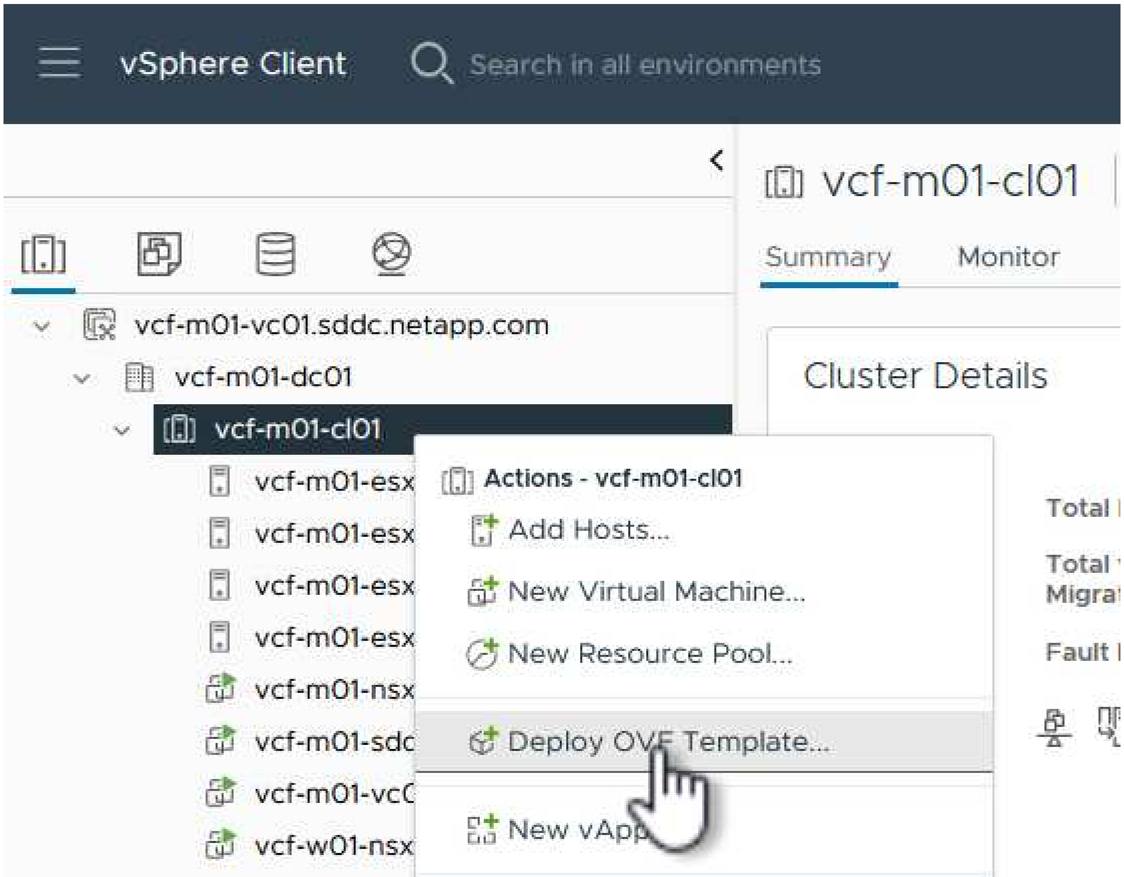
ONTAP tools for VMware vSphere is deployed as a VM appliance and provides an integrated vCenter UI for managing ONTAP storage.

Steps

1. Obtain the ONTAP tools OVA image from the NetApp Support site and download it to a local folder.

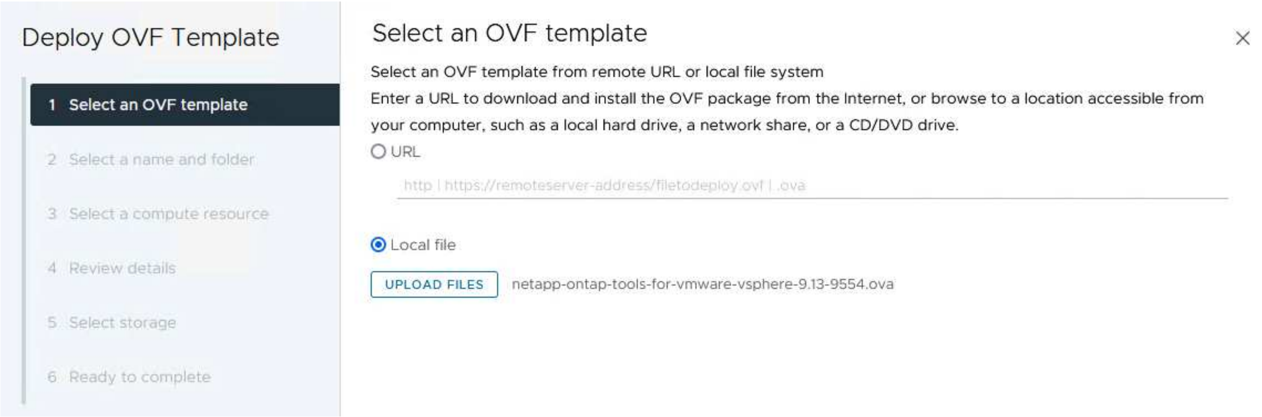
2. Log into the vCenter appliance for the VCF management domain.
3. From the vCenter appliance interface right-click the management cluster and select **Deploy OVF Template…**

   Show example



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

   Show example


Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

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

○ URL

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

● Local file

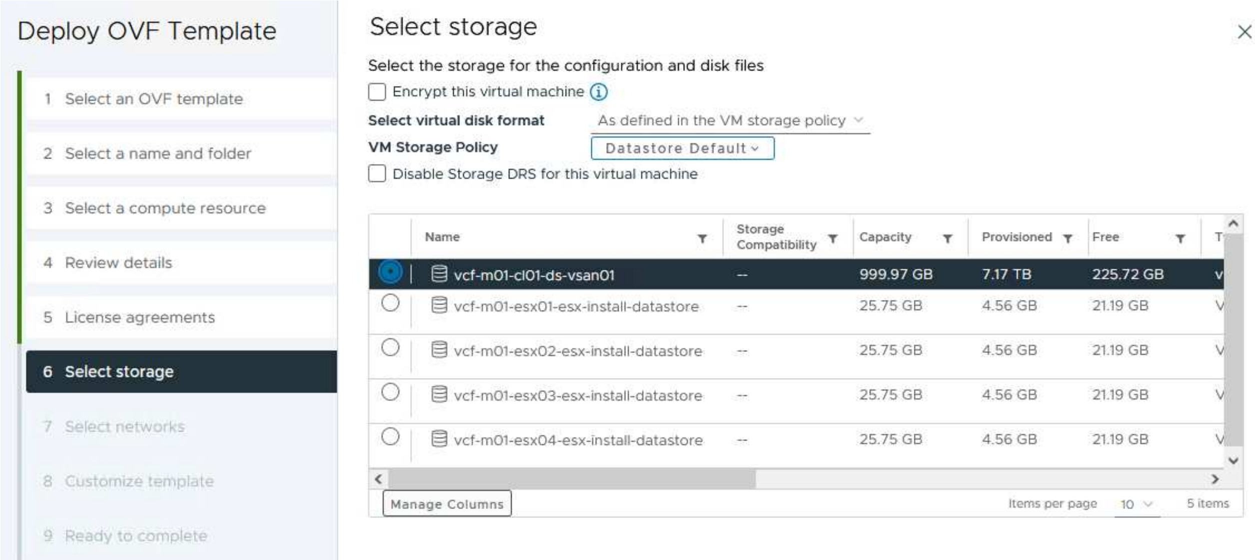
UPLOAD FILES netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. For steps 2 through 5 of the wizard, select a name and folder for the VM, select the compute resource,

review the details, and accept the license agreement.

6. For the storage location of the configuration and disk files, select the vSAN datastore of the VCF management domain cluster.

Show example



Deploy OVF Template

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

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine

Select virtual disk format As defined in the VM storage policy

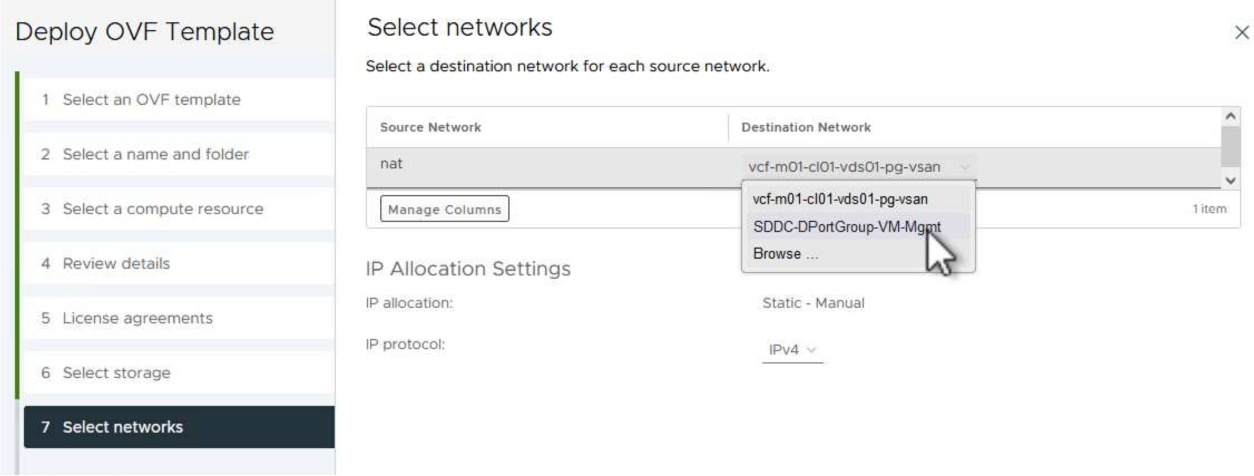
VM Storage Policy Datastore Default

□ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	v
○	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V

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

Show example



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks

Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	vcf-m01-cl01-vds01-pg-vsan

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

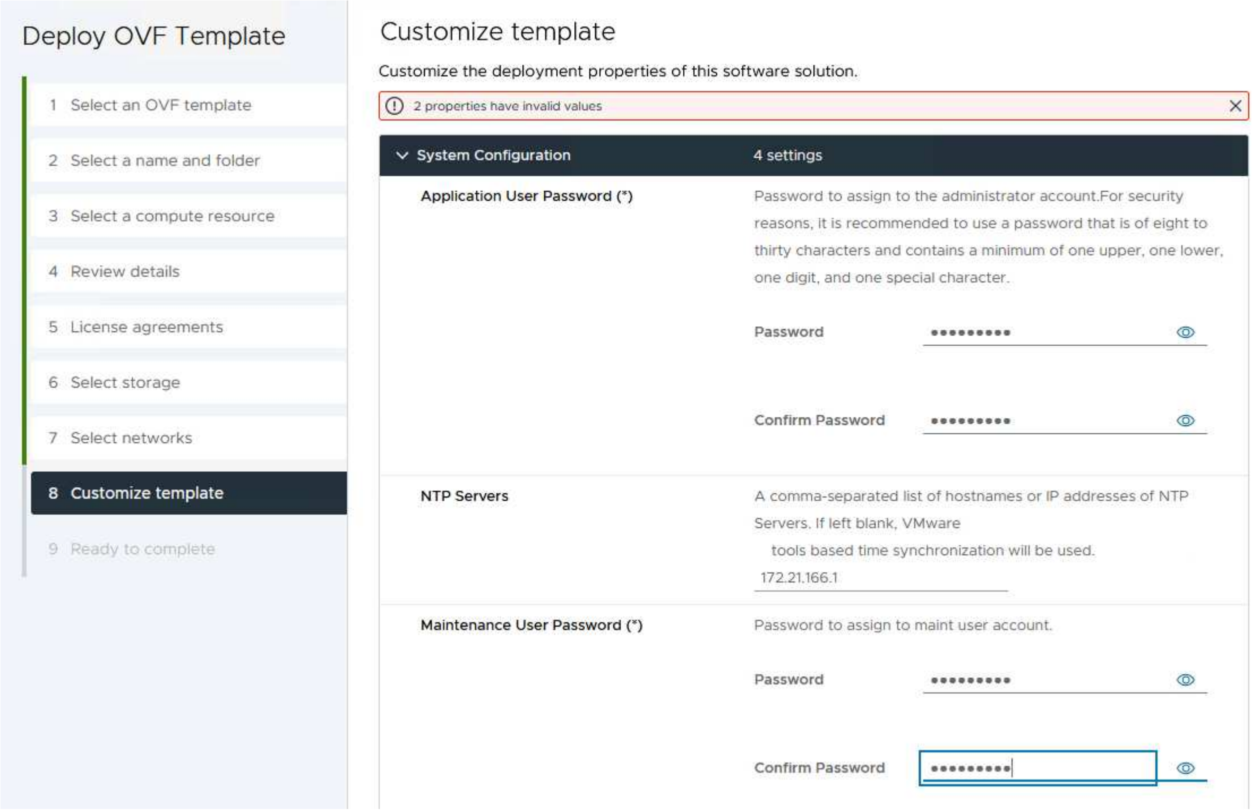
8. On the **Customize template** page, enter all required information:

    - Password to be used for administrative access to ONTAP tools.
    - NTP server IP address.
    - ONTAP tools maintenance account password.
    - ONTAP tools Derby DB password.
    - Do not check the box to **Enable VMware Cloud Foundation (VCF)**. VCF mode is not required for deploying supplemental storage.

- FQDN or IP address of the vCenter appliance for the **VI Workload Domain**
- Credentials for the vCenter appliance of the **VI Workload Domain**
- Required network properties.

9. Click **Next** to continue.

Show example



Deploy OVF Template

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

Customize template

Customize the deployment properties of this software solution.

ⓘ 2 properties have invalid values

System Configuration — 4 settings

Application User Password (*) — Password to assign to the administrator account.For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.

Password: ●●●●●●●●●

Confirm Password: ●●●●●●●●●

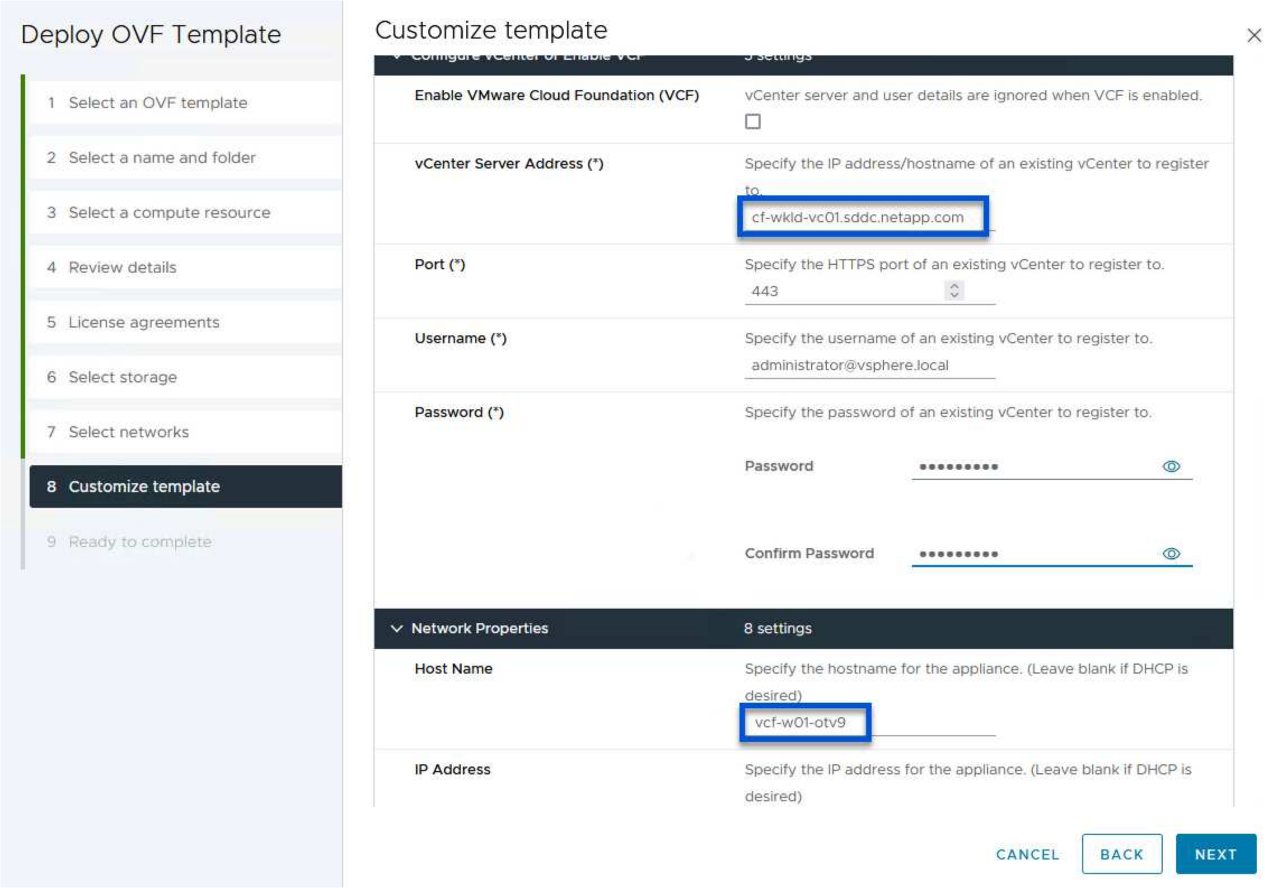
NTP Servers — A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used.

172.21.166.1

Maintenance User Password (*) — Password to assign to maint user account.

Password: ●●●●●●●●●

Confirm Password: ●●●●●●●●●



Deploy OVF Template

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

Customize template

Configure vCenter or Enable VCF — 5 settings

Enable VMware Cloud Foundation (VCF) — vCenter server and user details are ignored when VCF is enabled.

☐

vCenter Server Address (*) — Specify the IP address/hostname of an existing vCenter to register to.

cf-wkld-vc01.sddc.netapp.com

Port (*) — Specify the HTTPS port of an existing vCenter to register to.

443

Username (*) — Specify the username of an existing vCenter to register to.

administrator@vsphere.local

Password (*) — Specify the password of an existing vCenter to register to.

Password: ●●●●●●●●●

Confirm Password: ●●●●●●●●●

Network Properties — 8 settings

Host Name — Specify the hostname for the appliance. (Leave blank if DHCP is desired)

vcf-w01-otv9

IP Address — Specify the IP address for the appliance. (Leave blank if DHCP is desired)

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

Step 2: Add a storage system

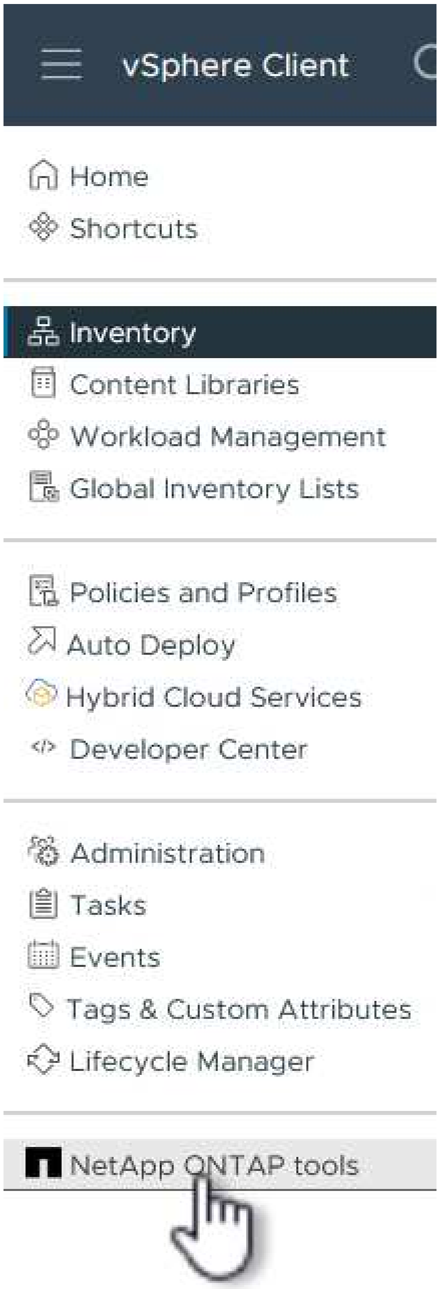
Perform the following steps to add a storage system using ONTAP tools.

> ⓘ vVol requires ONTAP cluster credentials rather than SVM credentials. For more information, refer to the ONTAP tools for VMware vSphere documentation: Add storage systems.

Steps

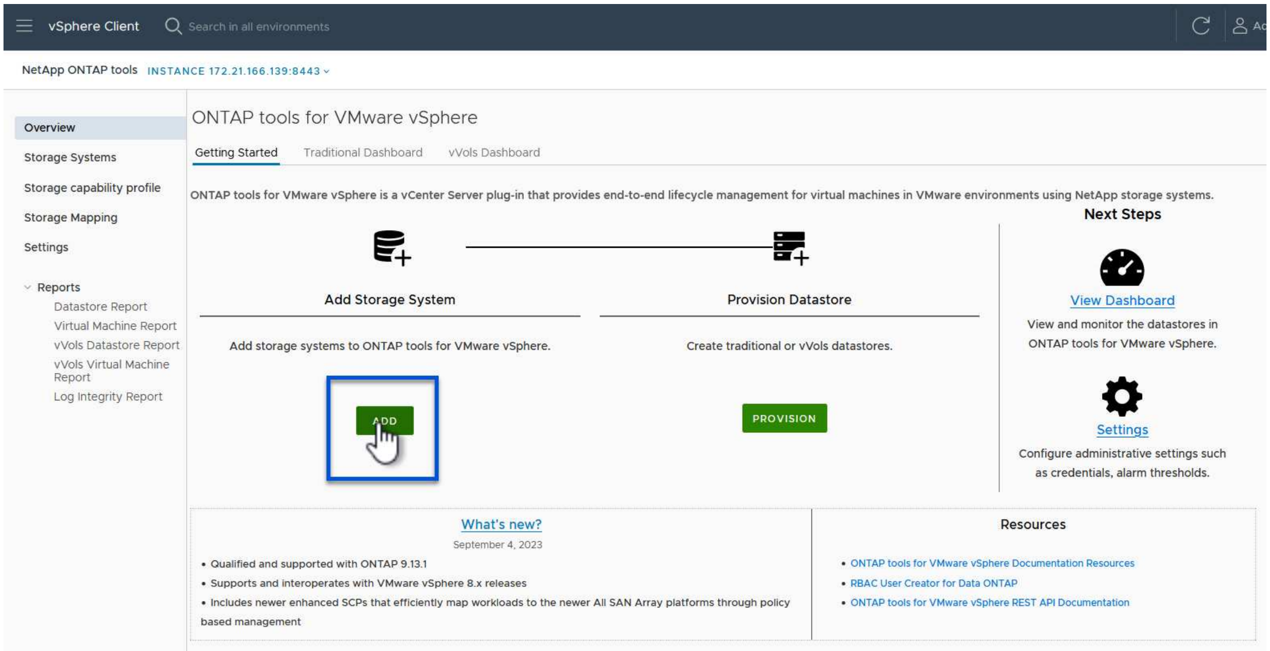
1. In the vSphere client navigate to the main menu and select **NetApp ONTAP tools**.

Show example



2. Once in **ONTAP tools**, from the Getting Started page (or from **Storage Systems**), click **Add** to add a new storage system.

   Show example



ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.

Add storage systems to ONTAP tools for VMware vSphere.

Create traditional or vVols datastores.

View and monitor the datastores in ONTAP tools for VMware vSphere.

Configure administrative settings such as credentials, alarm thresholds.

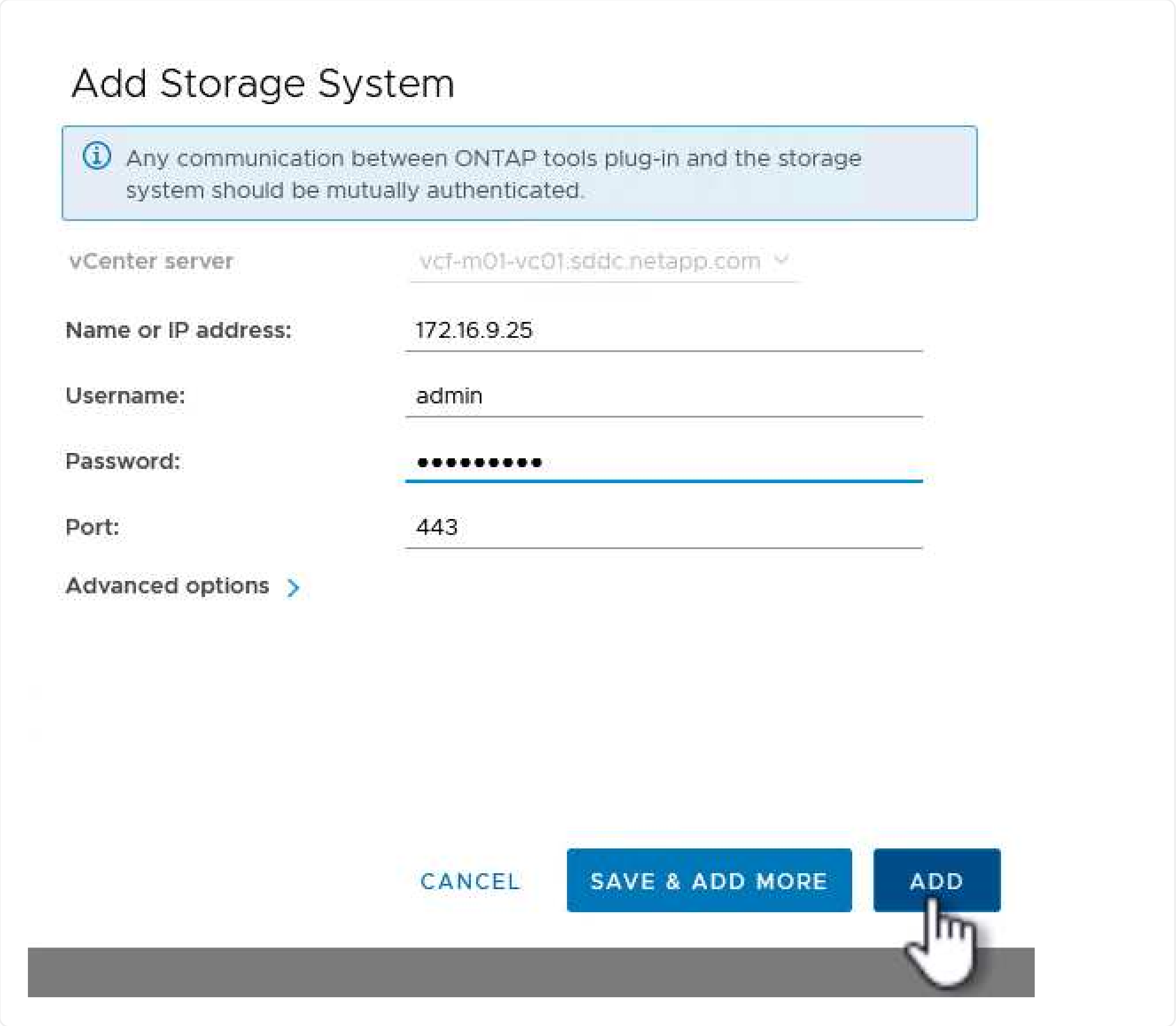
September 4, 2023

- Qualified and supported with ONTAP 9.13.1
- Supports and interoperates with VMware vSphere 8.x releases
- Includes newer enhanced SCPs that efficiently map workloads to the newer All SAN Array platforms through policy based management

- ONTAP tools for VMware vSphere Documentation Resources
- RBAC User Creator for Data ONTAP
- ONTAP tools for VMware vSphere REST API Documentation

3. Provide the IP address and credentials of the ONTAP storage system and click **Add**.

Show example



Add Storage System

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

vCenter server: vcf-m01-vc01.sddc.netapp.com

Name or IP address: 172.16.9.25

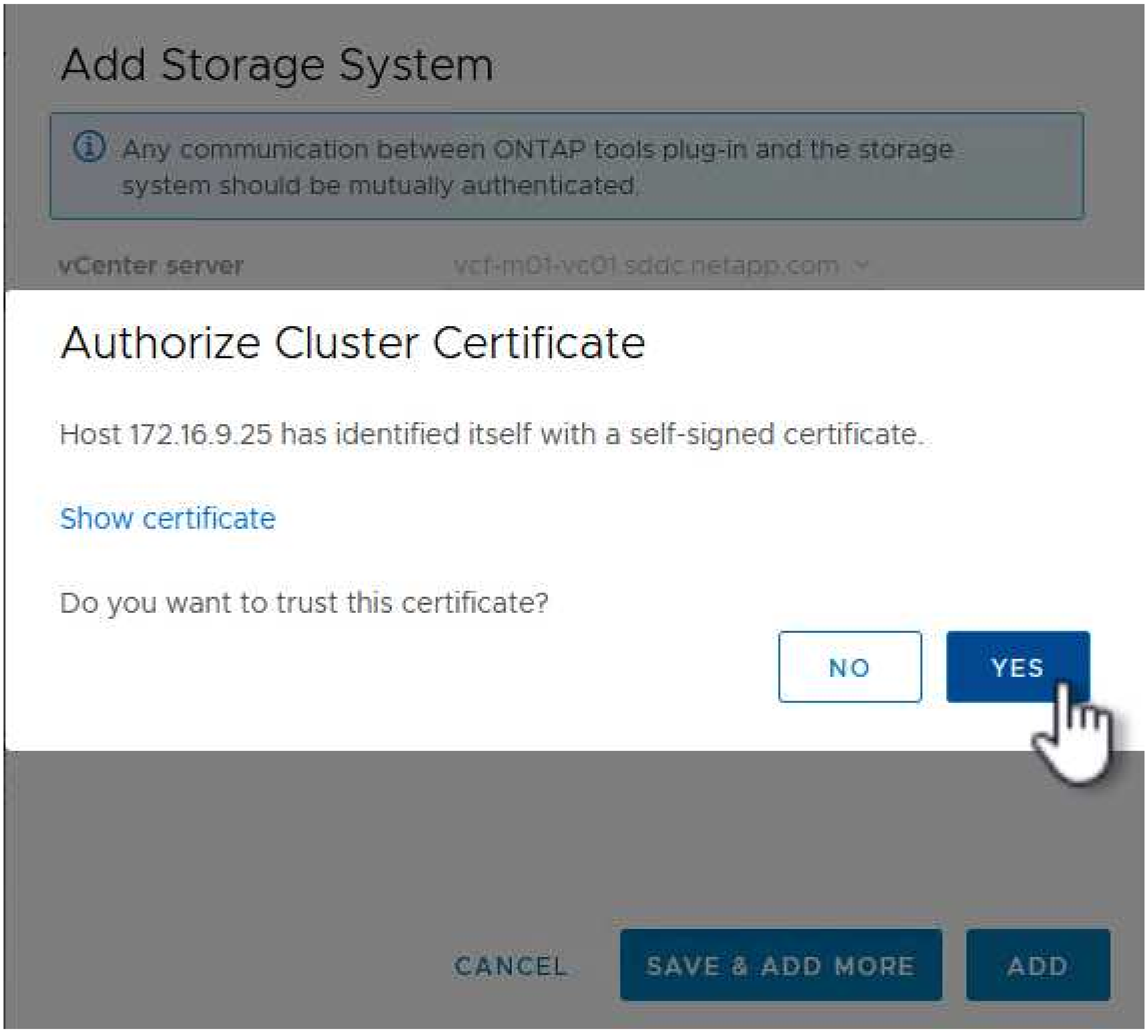
Username: admin

Password: ●●●●●●●●●●

Port: 443

4. Click **Yes** to authorize the cluster certificate and add the storage system.

Show example



Add Storage System

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

vCenter server vcf-m01-vc01.sddc.netapp.com

Authorize Cluster Certificate

Host 172.16.9.25 has identified itself with a self-signed certificate.

Show certificate

Do you want to trust this certificate?

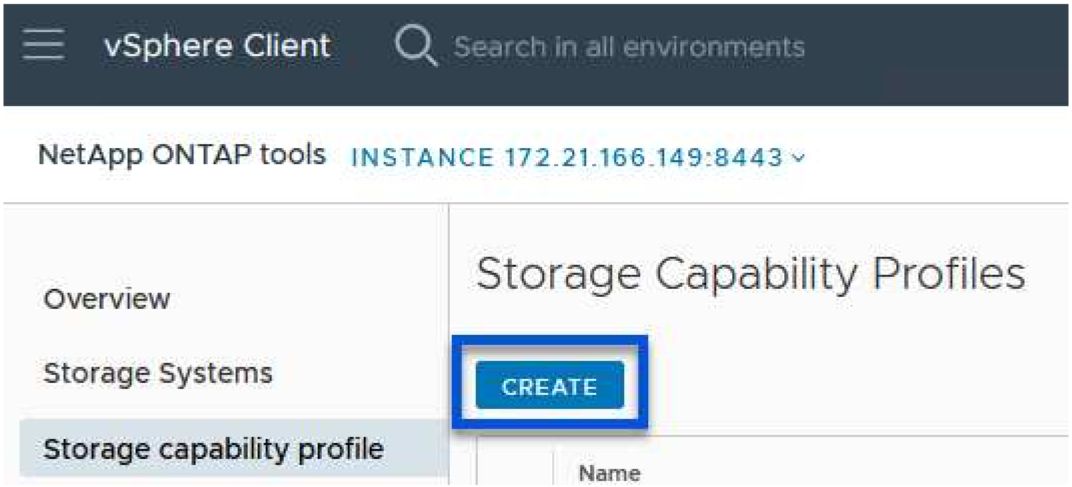
Step 3: Create a storage capability profile in ONTAP tools

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

Steps

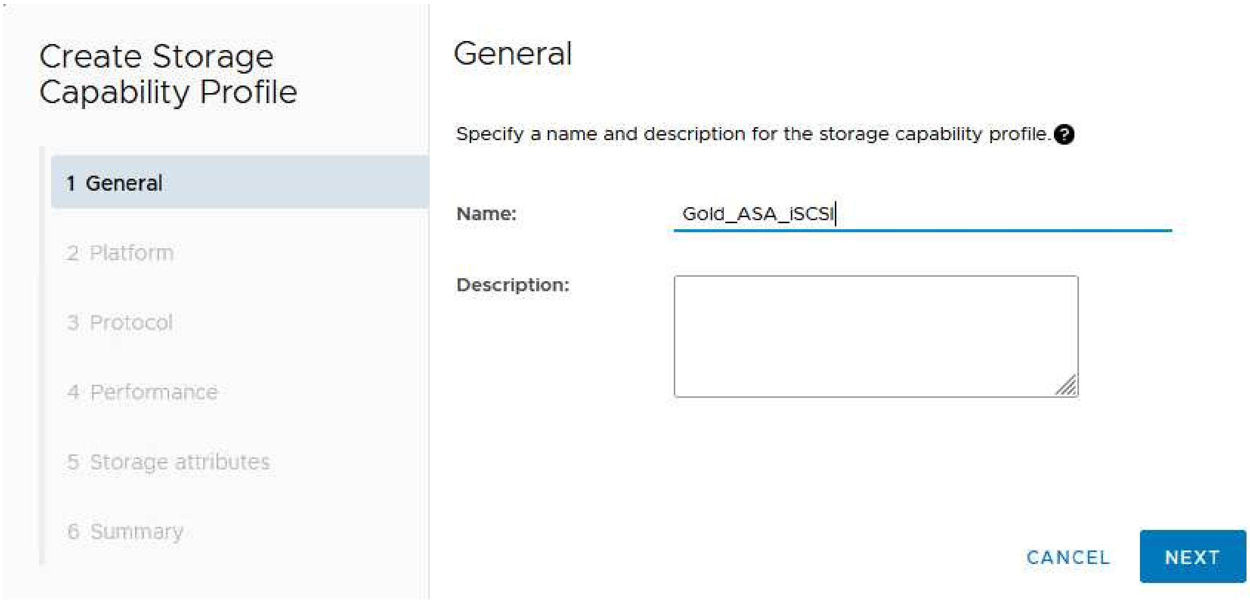
1. In ONTAP tools, select **Storage capability profile** from the left-hand menu and then press **Create**.

Show example


vSphere Client
Search in all environments
NetApp ONTAP tools
INSTANCE 172.21.166.149:8443
Overview
Storage Systems
Storage capability profile
Storage Capability Profiles
CREATE
Name

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

Show example



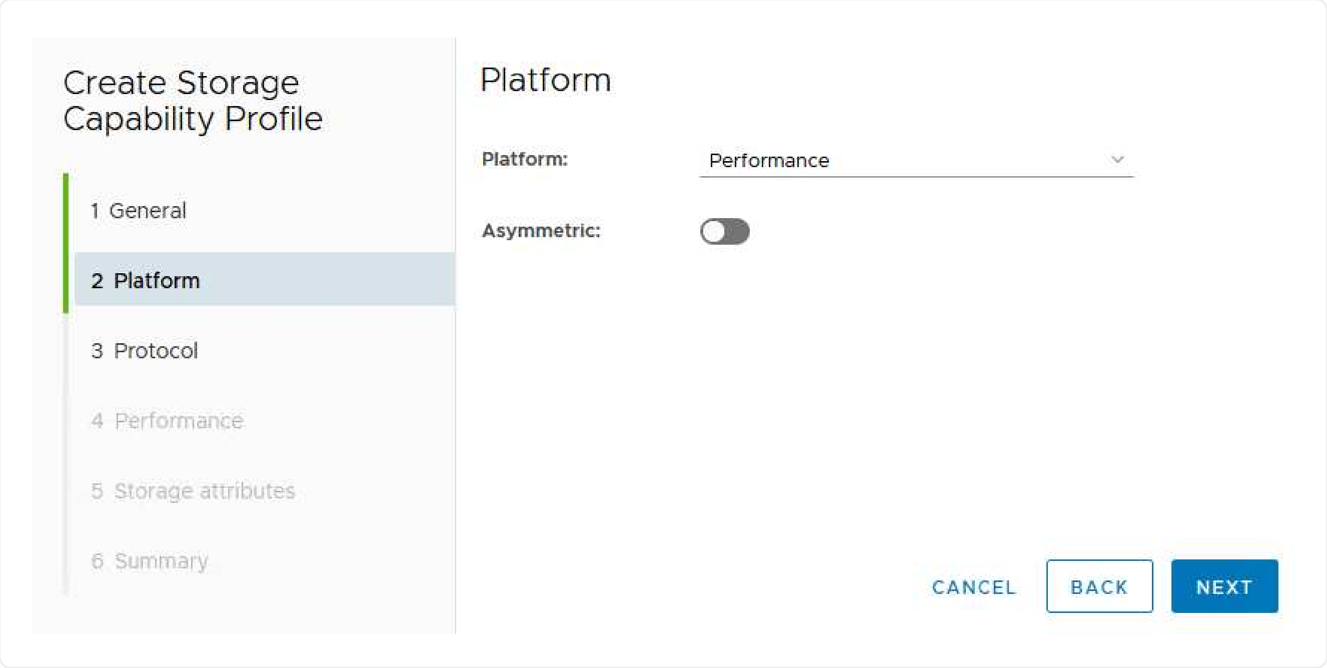
Specify a name and description for the storage capability profile.

Name: Gold_ASA_iSCSI

Description:

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

Show example



Create Storage Capability Profile

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

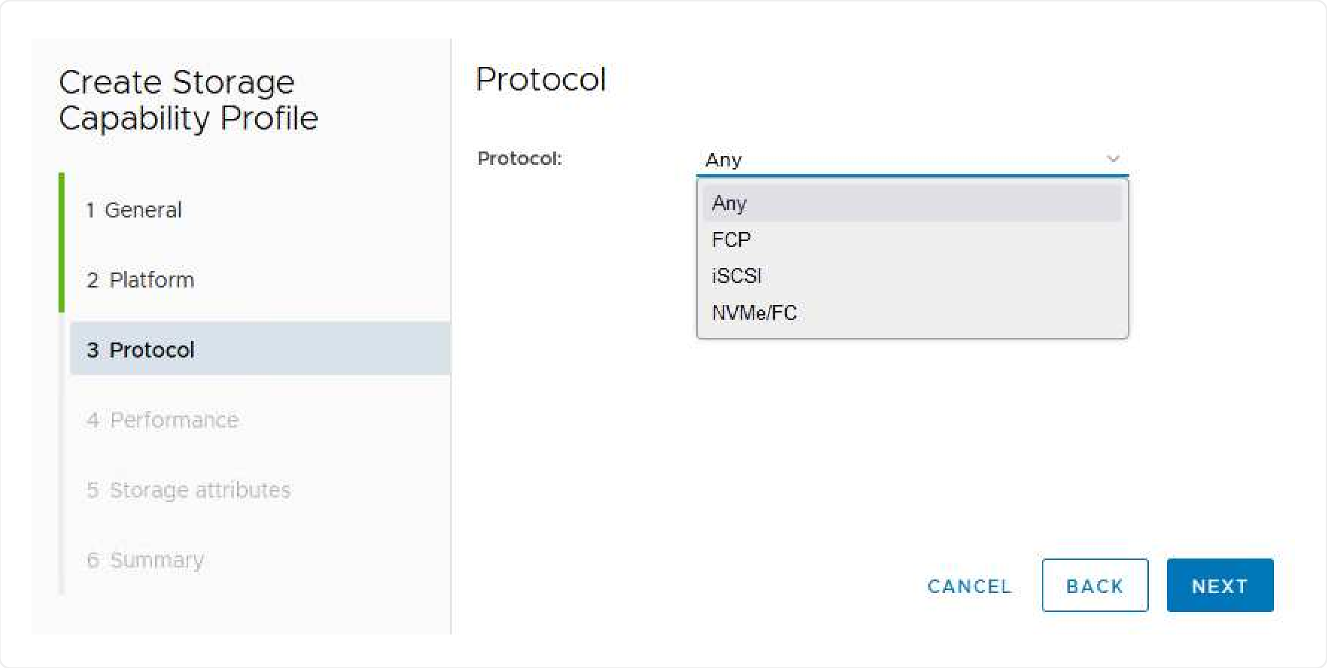
Platform

Platform: Performance

Asymmetric:

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

Show example



Create Storage Capability Profile

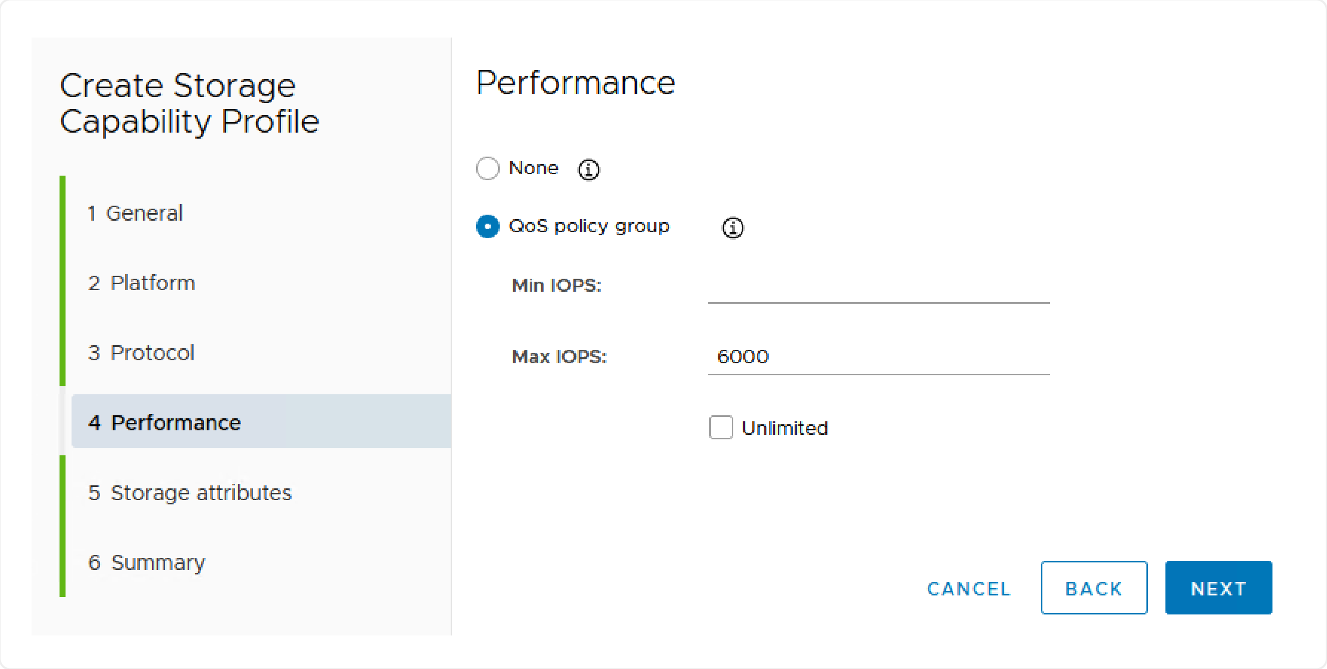
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary

Protocol

Protocol: Any

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

Show example



Create Storage Capability Profile

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

Performance

○ None

● QoS policy group

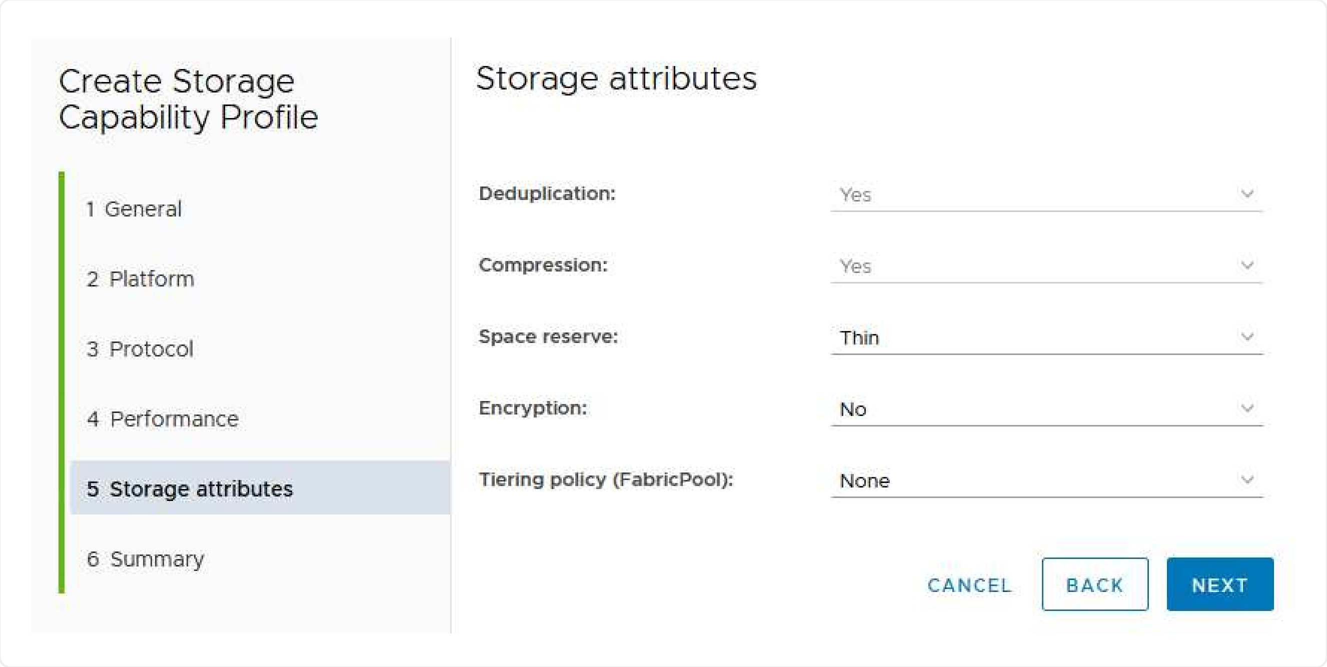
Min IOPS:

Max IOPS: 6000

□ Unlimited

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

Show example



Create Storage Capability Profile

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

Storage attributes

Deduplication: Yes

Compression: Yes

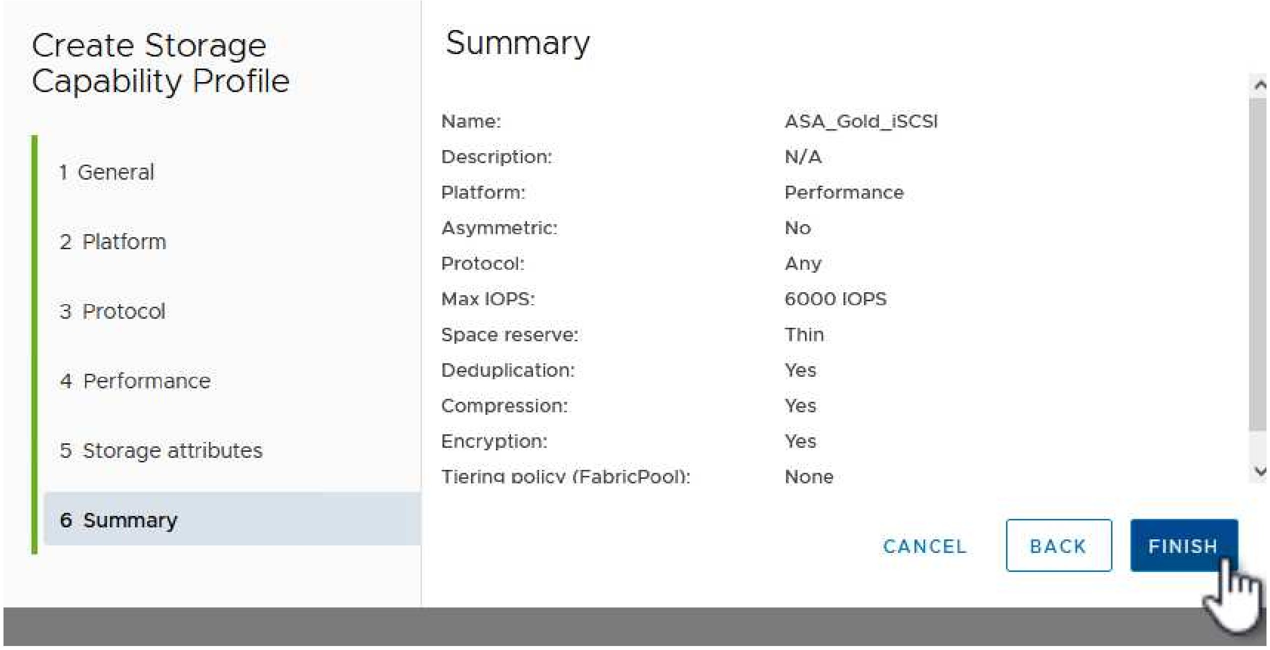
Space reserve: Thin

Encryption: No

Tiering policy (FabricPool): None

8. Review the summary and click **Finish** to create the profile.

Show example



Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Summary

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

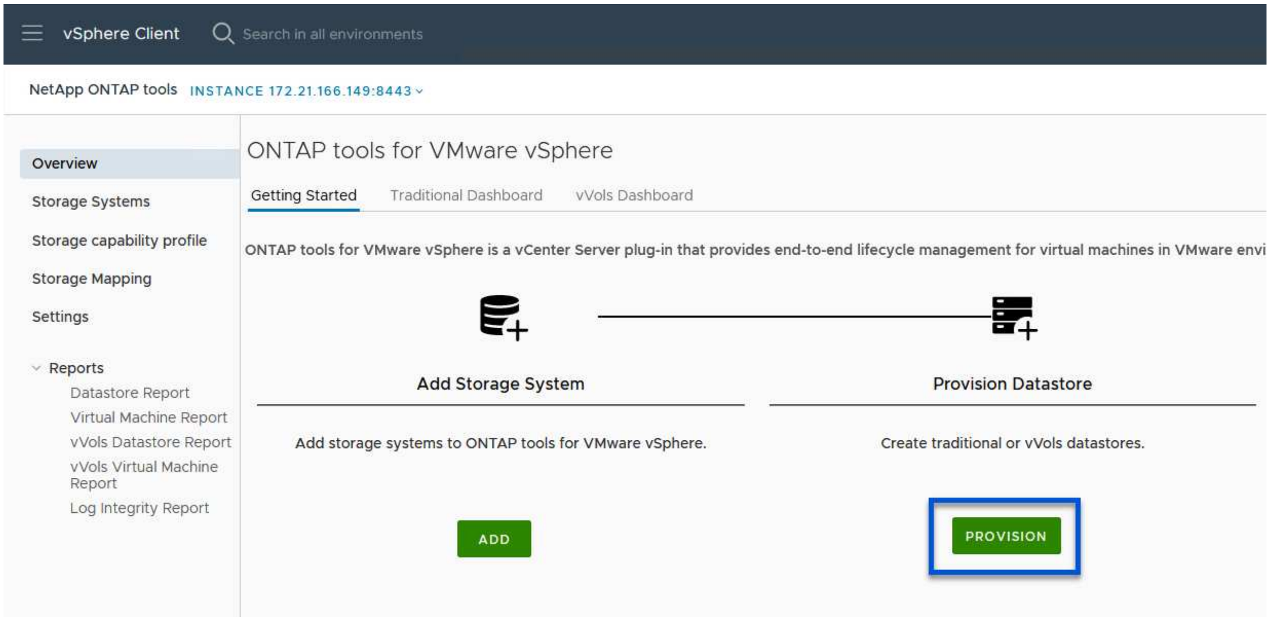
Step 4: Create a vVols datastore in ONTAP tools

To create a vVols datastore in ONTAP tools complete the following steps.

Steps

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

   Show example



ONTAP tools for VMware vSphere

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

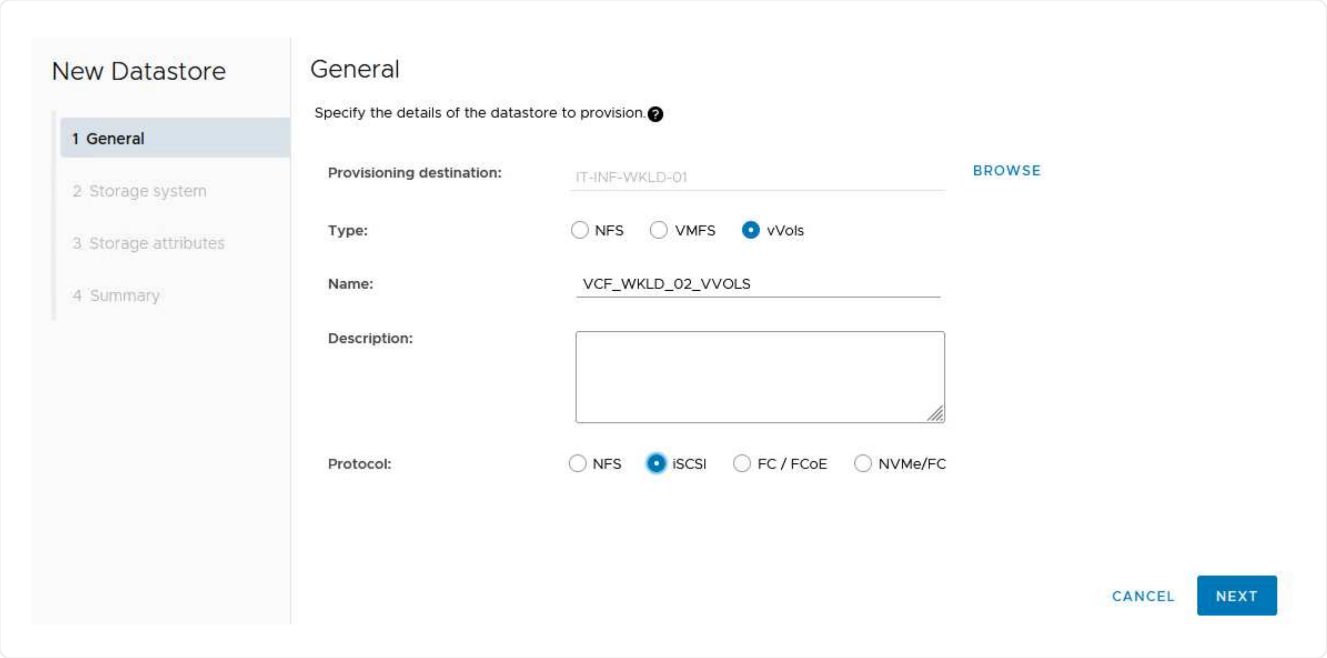
Add storage systems to ONTAP tools for VMware vSphere.

Create traditional or vVols datastores.

2. On the **General** page of the New Datastore wizard, select the vSphere datacenter or cluster destination.

3. Select **vVols** as the datastore type, enter a name for the datastore, and select **iSCSI** as the protocol.
4. Click **Next** to continue.

Show example



New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

General

Specify the details of the datastore to provision.

Provisioning destination: IT-INF-WKLD-01 BROWSE

Type: ○ NFS ○ VMFS ● vVols

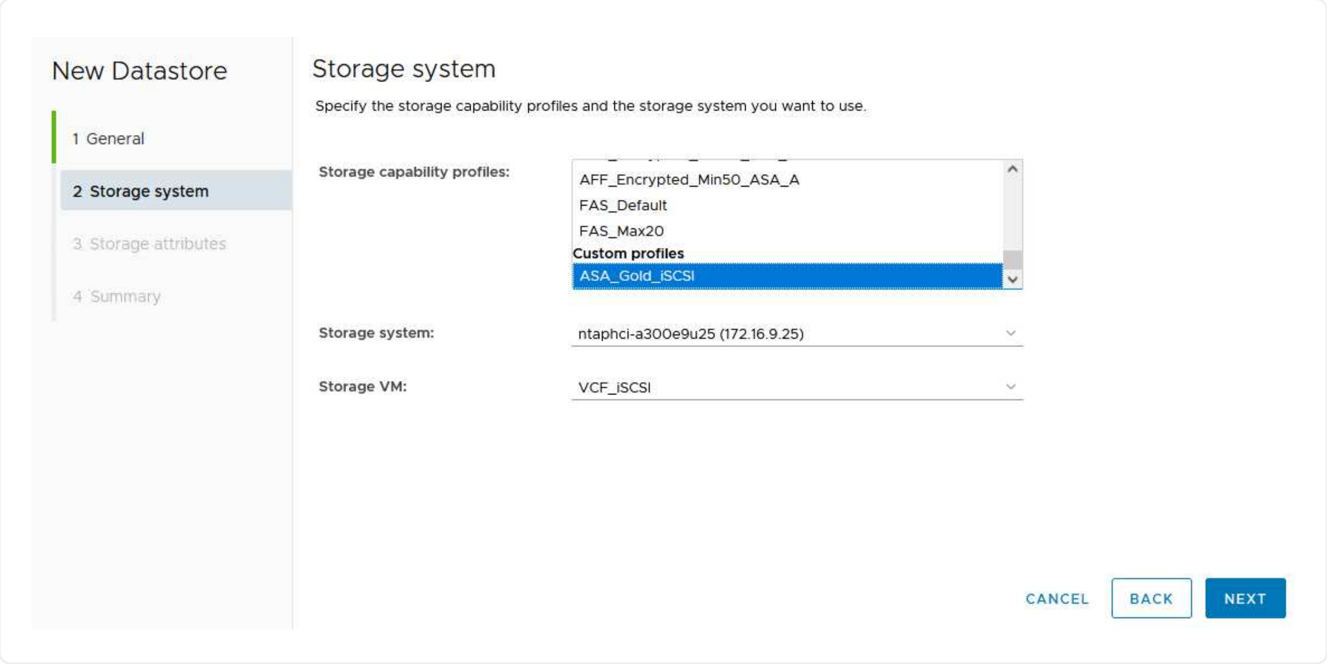
Name: VCF_WKLD_02_VVOLS

Description:

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

5. On the **Storage system** page, select a storage capability profile, the storage system, and the VM.
6. Click **Next** to continue.

Show example



New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

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

Storage capability profiles:

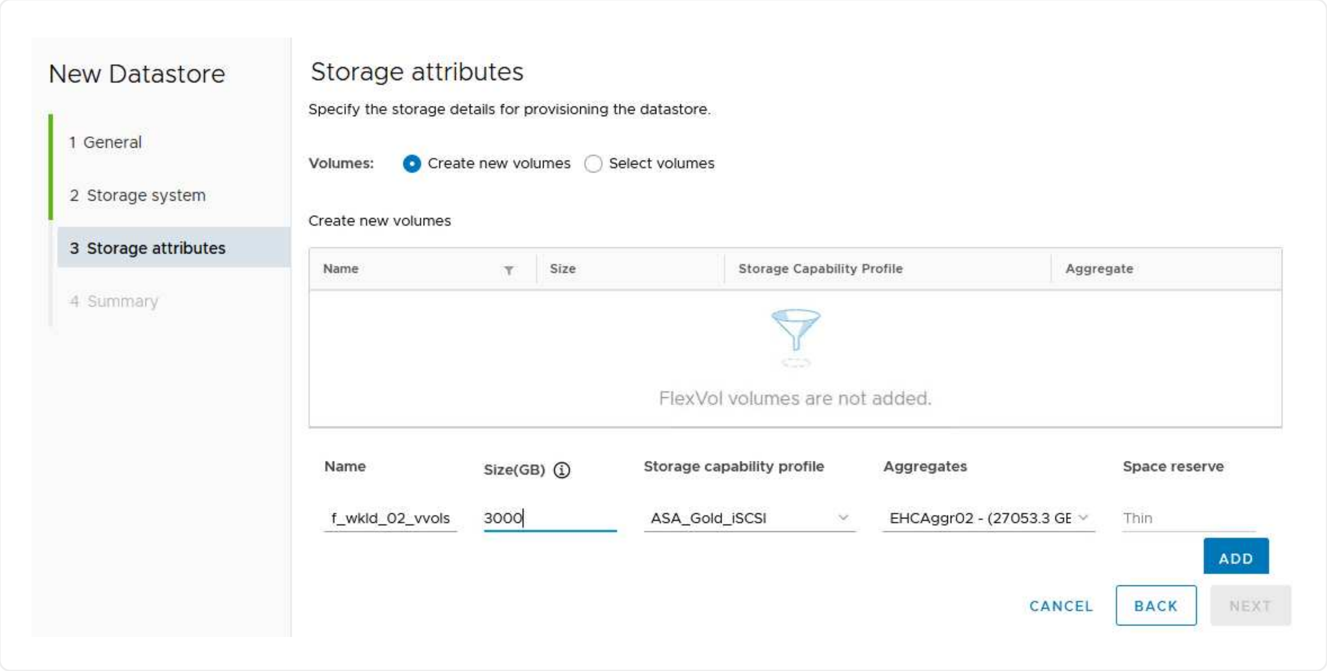
AFF_Encrypted_Min50_ASA_A
FAS_Default
FAS_Max20
Custom profiles
ASA_Gold_iSCSI

Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: VCF_iSCSI

7. On the **Storage attributes** page, select to create a new volume for the datastore and enter the storage attributes of the volume you want to create.
8. Click **Add** to create the volume and then **Next** to continue.

Show example



Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: ● Create new volumes ○ Select volumes

Create new volumes

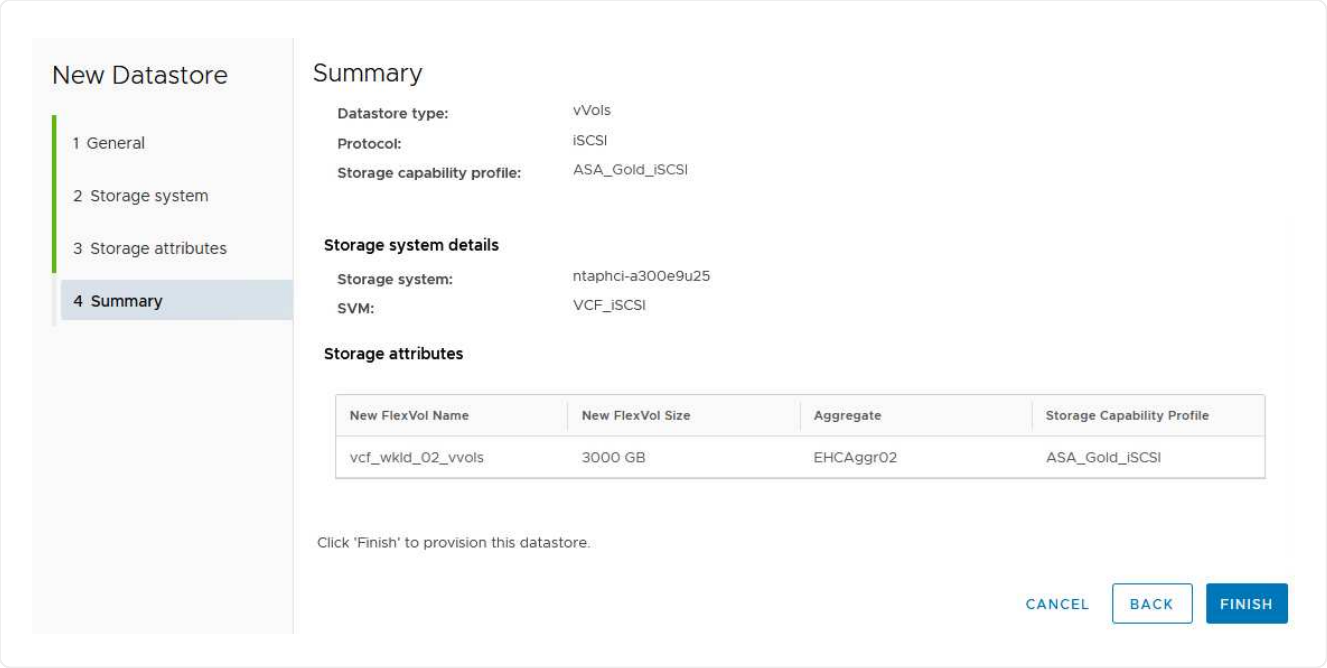
Name	Size	Storage Capability Profile	Aggregate

FlexVol volumes are not added.

Name	Size(GB)	Storage capability profile	Aggregates	Space reserve
f_wkld_02_vvols	3000	ASA_Gold_iSCSI	EHCAggr02 - (27053.3 GE	Thin

9. Review the summary and click **Finish** to start the vVol datastore creation process.

Show example



Summary

Datastore type: vVols
Protocol: iSCSI
Storage capability profile: ASA_Gold_iSCSI

Storage system details

Storage system: ntaphci-a300e9u25
SVM: VCF_iSCSI

Storage attributes

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile
vcf_wkld_02_vvols	3000 GB	EHCAggr02	ASA_Gold_iSCSI

Click 'Finish' to provision this datastore.

Additional information

- For information on configuring ONTAP storage systems, refer to ONTAP 9 documentation.
- For information on configuring VCF, refer to VMware Cloud Foundation documentation.
- For information on using VMFS iSCSI datastores with VMware, refer to vSphere VMFS datastore - iSCSI storage backend with ONTAP.
- For video demos of this solution, refer to VMware datastore provisioning.

Expand VI workload domains with vVols NFS

Deployment workflow for adding NFS vVols datastores as supplemental storage in a VI workload domain

Get started with adding NFS vVols datastores as supplemental storage in a VI workload domains using ONTAP tools for VMware vSphere. You'll review the deployment requirements, deploy ONTAP tools for VMware vSphere, configure the SVM with logical interfaces, and configure storage.

1 **Review the deployment requirements**

Review the requirements to deploy NFS vVols in a VMware Cloud Foundation management domain.

2 **Create the SVM and LIFs**

Create an SVM with multiple LIFs for NFS traffic.

3 **Configure networking**

Set up networking for NFS on ESXi hosts.

4 **Configure storage**

Deploy and use ONTAP tools to configure storage.

Deployment requirements for adding NFS vVols in a VI workload domain

Review the recommended network design and infrastructure requirements to deploy NFS vVols in a VMware Cloud Foundation VI workload domain. You need a fully configured ONTAP AFF or ASA storage system, a completed VCF management domain, and an existing VI workload domain.

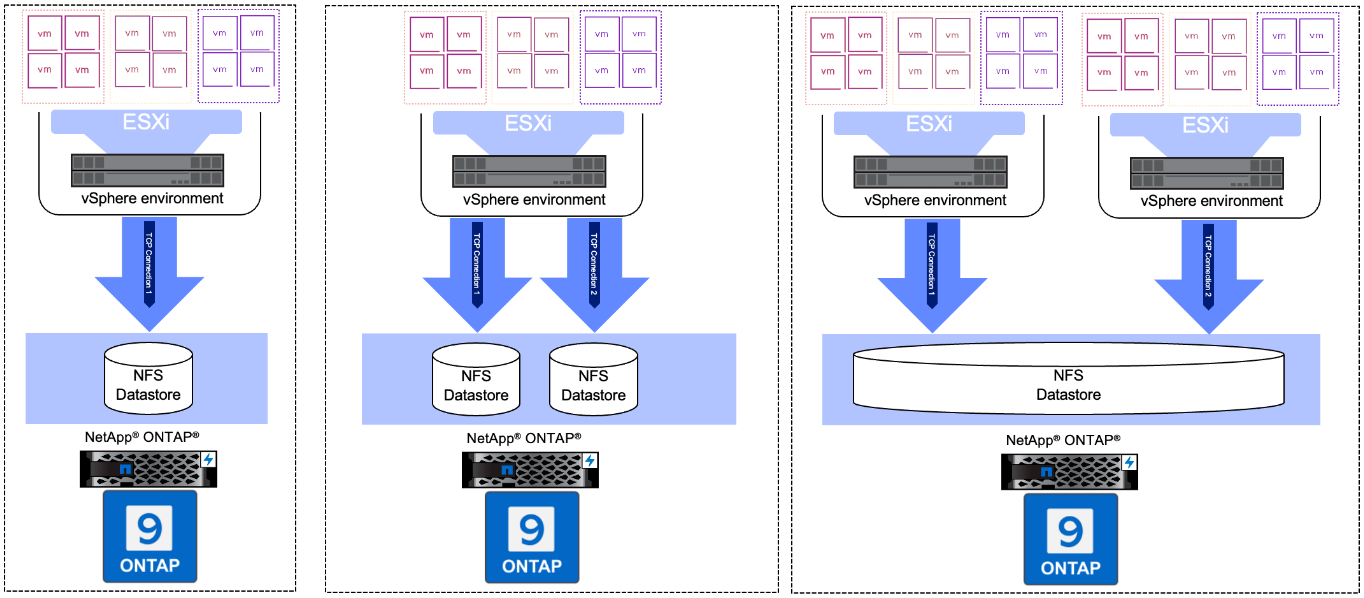
Infrastructure requirements

Make sure the following components and configurations are in place.

- An ONTAP AFF or FAS storage system with physical data ports on Ethernet switches dedicated to storage traffic.
- VCF management domain deployment is complete and the vSphere client is accessible.
- A VI workload domain has been previously deployed.

Recommended NFS network design

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



Additional information

- For detailed information specific to VMware vSphere, refer to Best Practices For Running NFS with VMware vSphere.
- For network guidance on using ONTAP with VMware vSphere refer to the Network configuration - NFS section of the NetApp enterprise applications documentation.

  This documentation demonstrates the process of creating a new SVM and specifying the IP address information to create multiple LIFs for NFS traffic. To add new LIFs to an existing SVM refer to Create a LIF (network interface).
- For complete information on using NFS with vSphere clusters, refer to the NFS v3 Reference Guide for vSphere 8.

What's next?

After reviewing the requirements, create the SVM and LIFs.

Create SVM and LIFs for NFS vVols datastores in a VCF VI workload domain

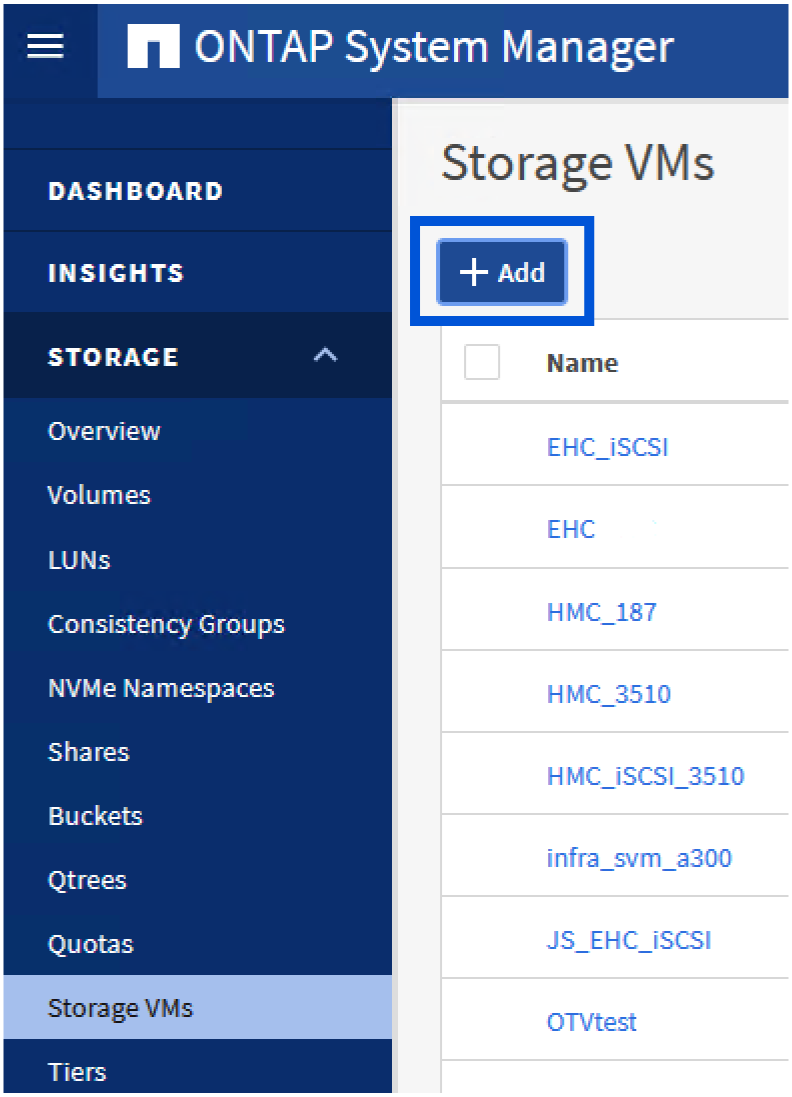
Create a Storage Virtual Machine (SVM) and multiple logical interfaces (LIFs) on an ONTAP system to support NFS traffic for vVols datastores in a VMware Cloud Foundation VI workload domain.

To add new LIFs to an existing SVM, refer to the ONTAP documentation: Create ONTAP LIFs.

Steps

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

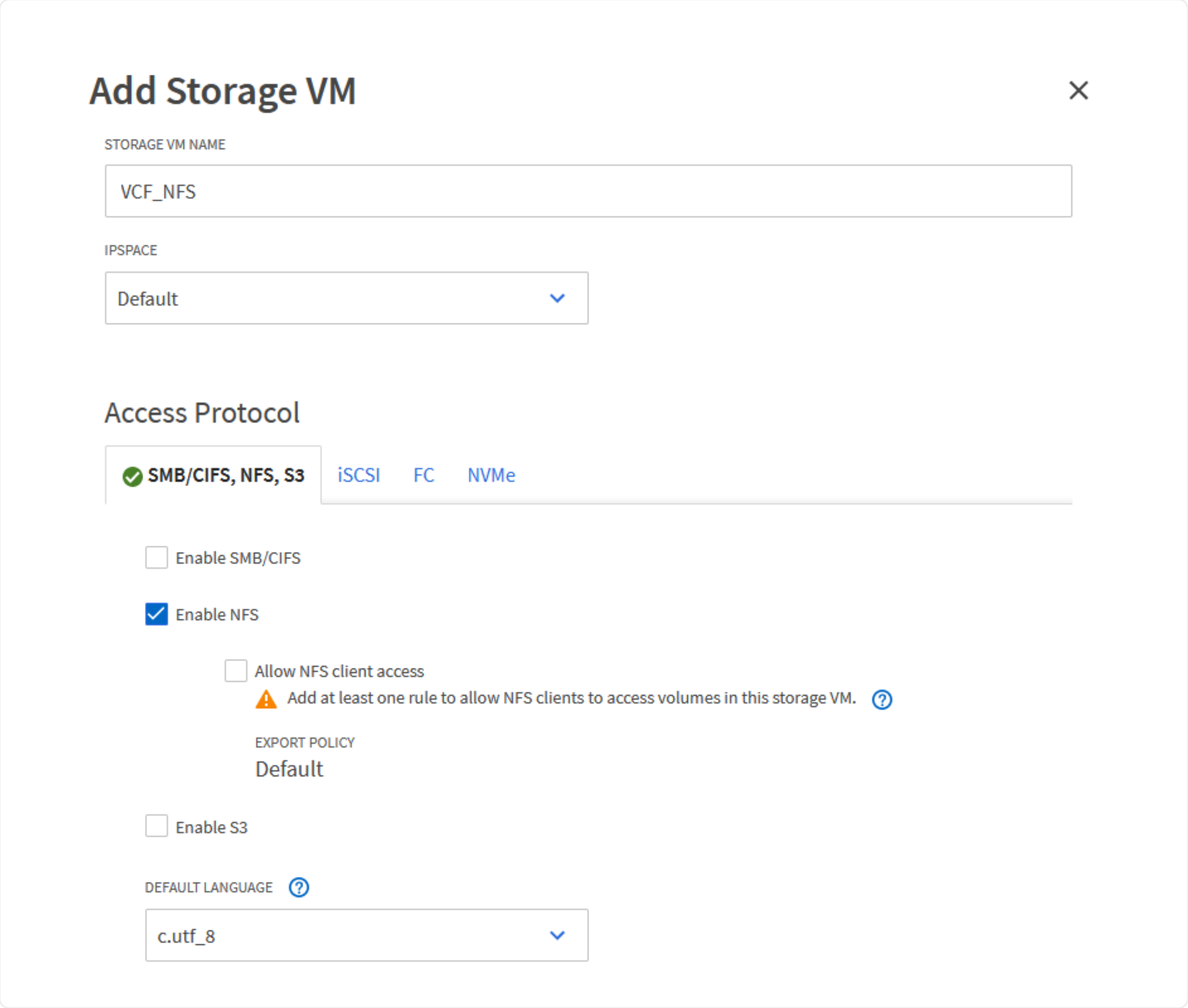
Show example



□	Name
	EHC_iSCSI
	EHC
	HMC_187
	HMC_3510
	HMC_iSCSI_3510
	infra_svm_a300
	JS_EHC_iSCSI
	OTVtest

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

Show example



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

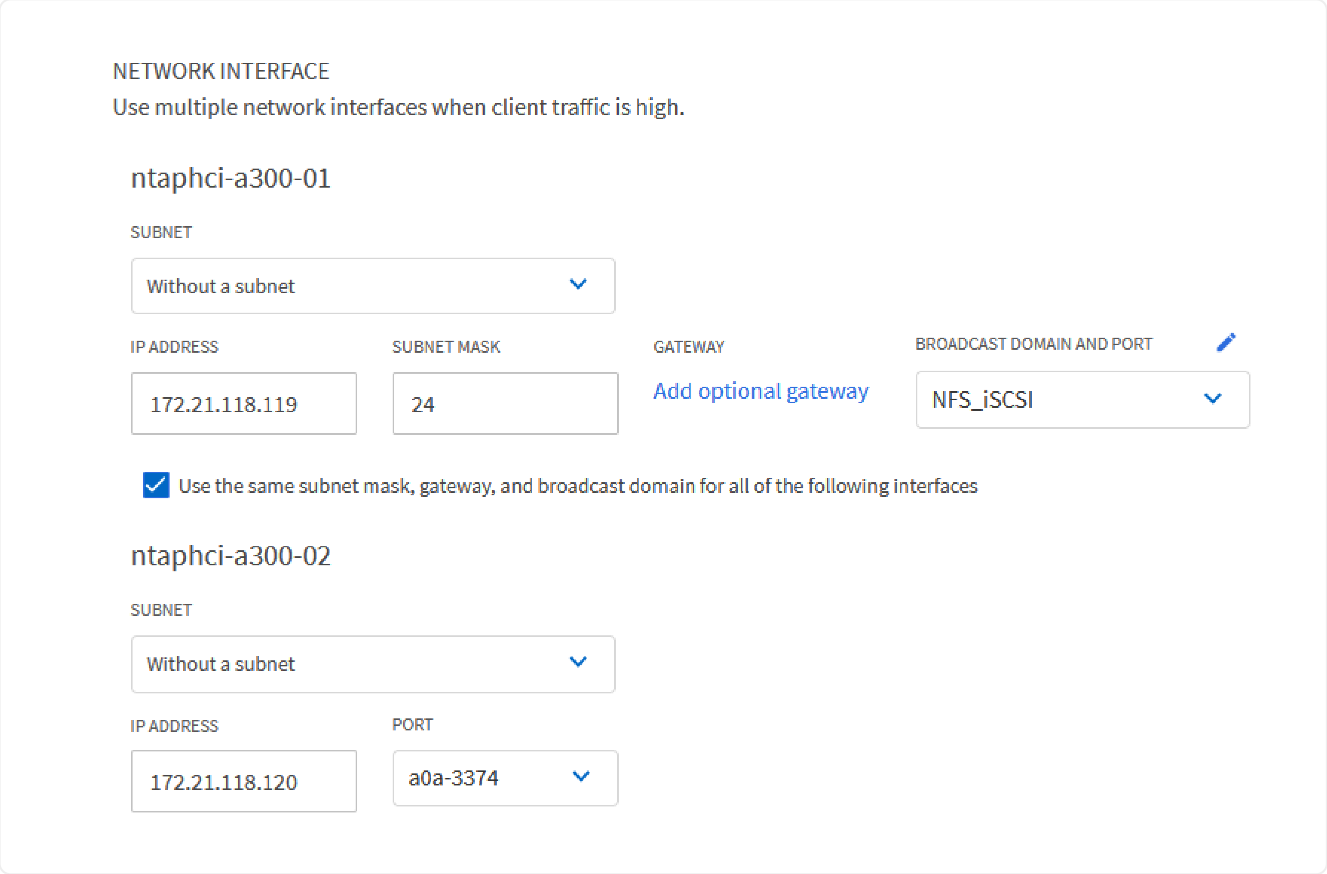
DEFAULT LANGUAGE

c.utf_8

> You don’t need to check the **Allow NFS client access** checkbox. ONTAP tools for VMware vSphere will be used to automate the datastore deployment process, which 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, you can either use individual settings or enable the checkbox to use common settings across all remaining LIFs.

Show example



NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET: Without a subnet

IP ADDRESS: 172.21.118.119

SUBNET MASK: 24

GATEWAY: Add optional gateway

BROADCAST DOMAIN AND PORT: NFS_iSCSI

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

ntaphci-a300-02

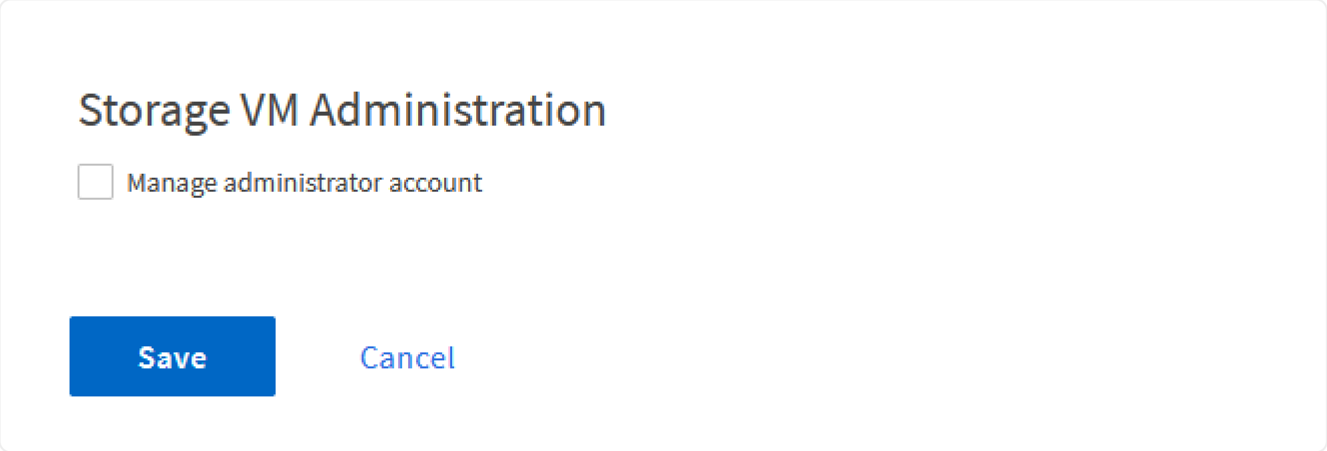
SUBNET: Without a subnet

IP ADDRESS: 172.21.118.120

PORT: a0a-3374

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

Show example



Storage VM Administration

□ Manage administrator account

What’s next?

After creating the SVM and LIFs, configure networking for NFS on ESXi hosts.

Configure networking for NFS on ESXi hosts in a VCF VI workload domain

Configure NFS networking on ESXi hosts in VMware Cloud Foundation management domains to enable connectivity to ONTAP storage systems. You’ll create distributed port groups with VLAN separation, configure uplink teaming for redundancy, and set up VMkernel adapters on each ESXi host to establish dedicated NFS paths for failover capabilities.

Perform the following steps 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.

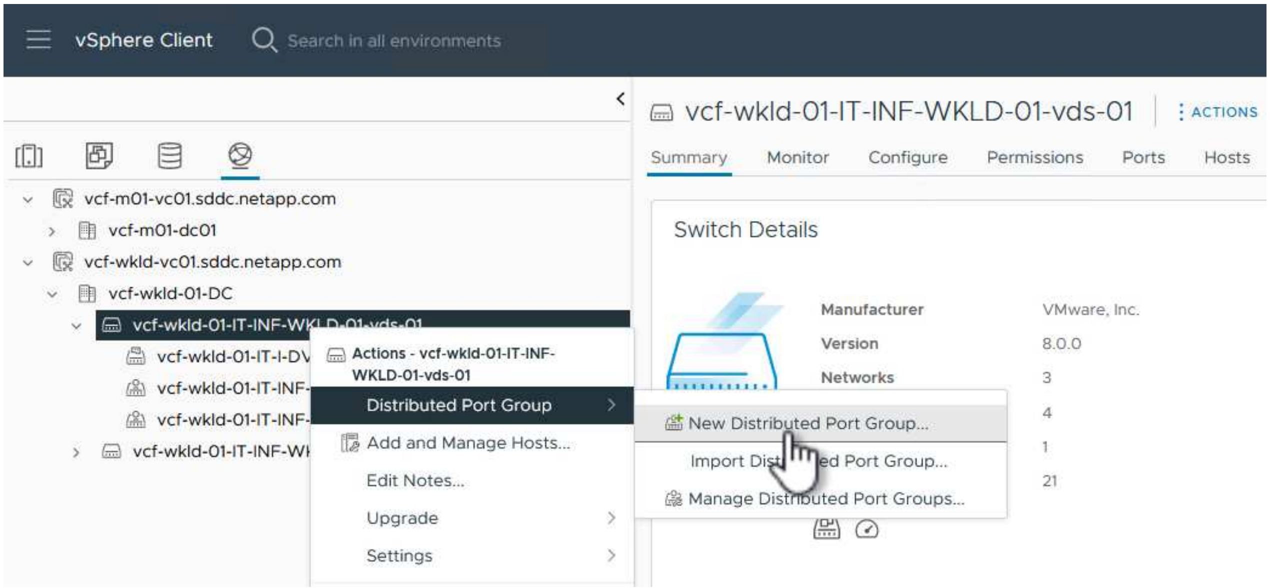
Step 1: Create a distributed port group for NFS traffic

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

Steps

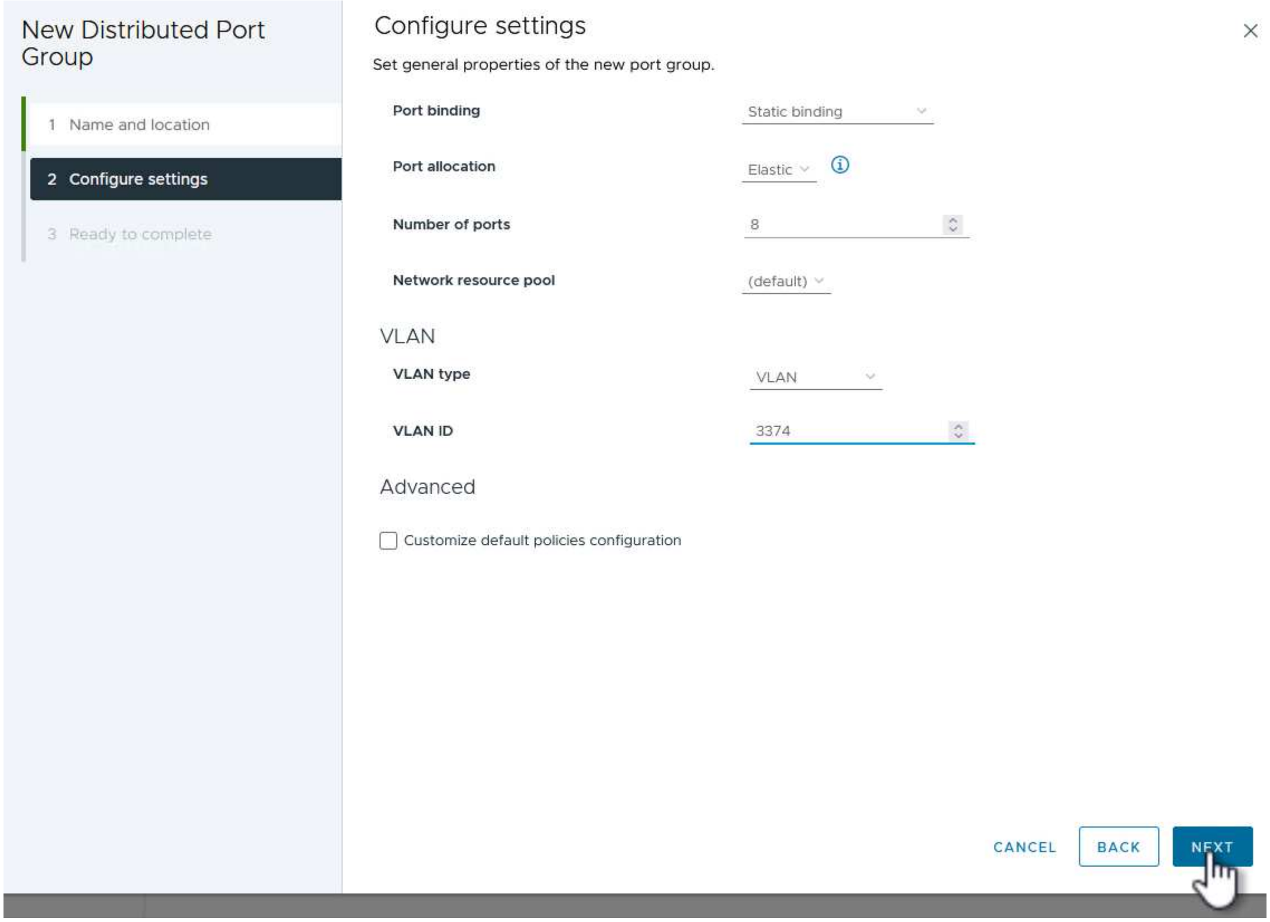
1. From the vSphere client , navigate to **Inventory > Networking** for the workload domain. Navigate to the existing Distributed Switch and choose the action to create **New Distributed Port Group…**.

   Show example



2. In the **New Distributed Port Group** wizard, fill in a name for the new port group and click **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 **Next** to continue.

Show example



New Distributed Port Group

1 Name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding: Static binding

Port allocation: Elastic

Number of ports: 8

Network resource pool: (default)

VLAN

VLAN type: VLAN

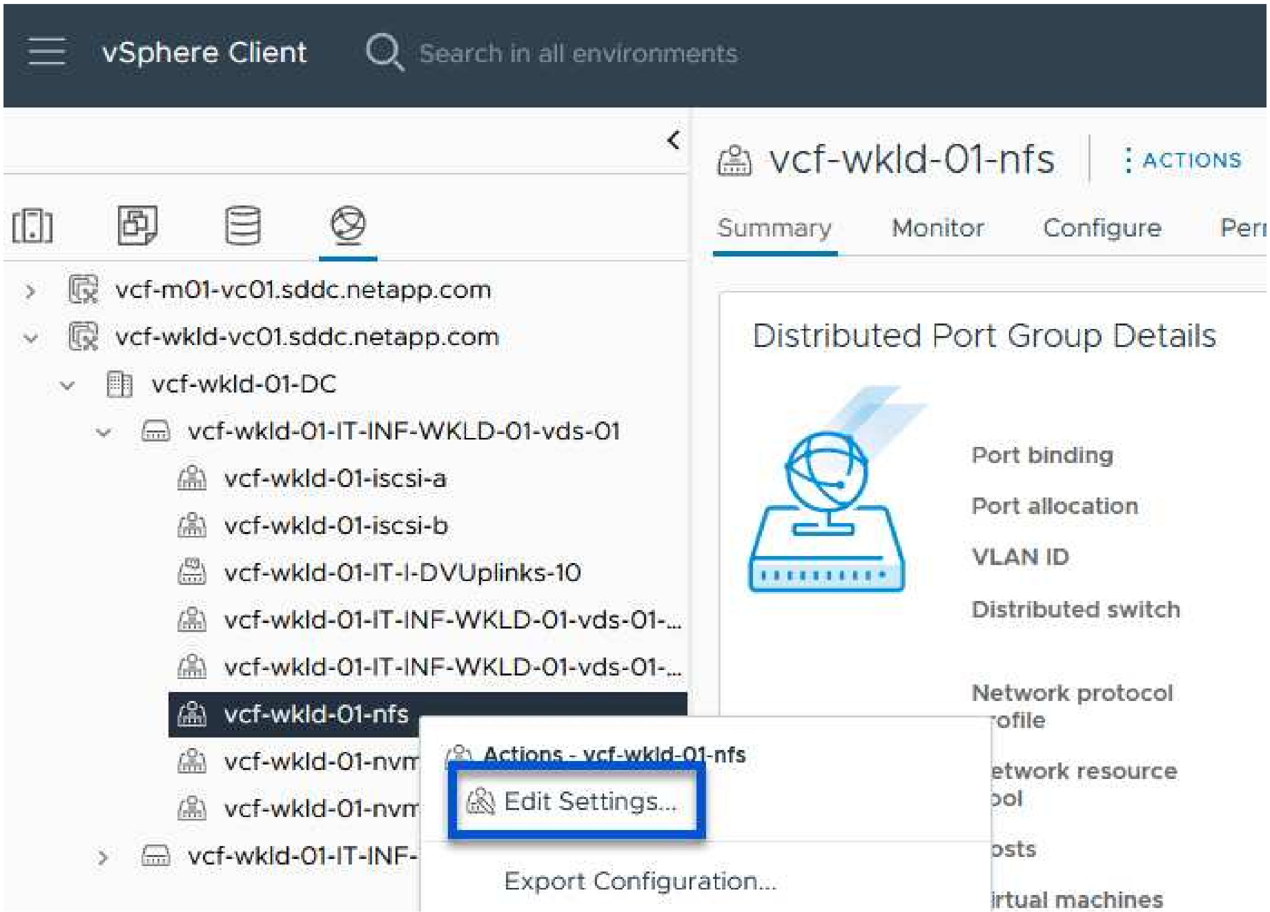
VLAN ID: 3374

Advanced

□ Customize default policies configuration

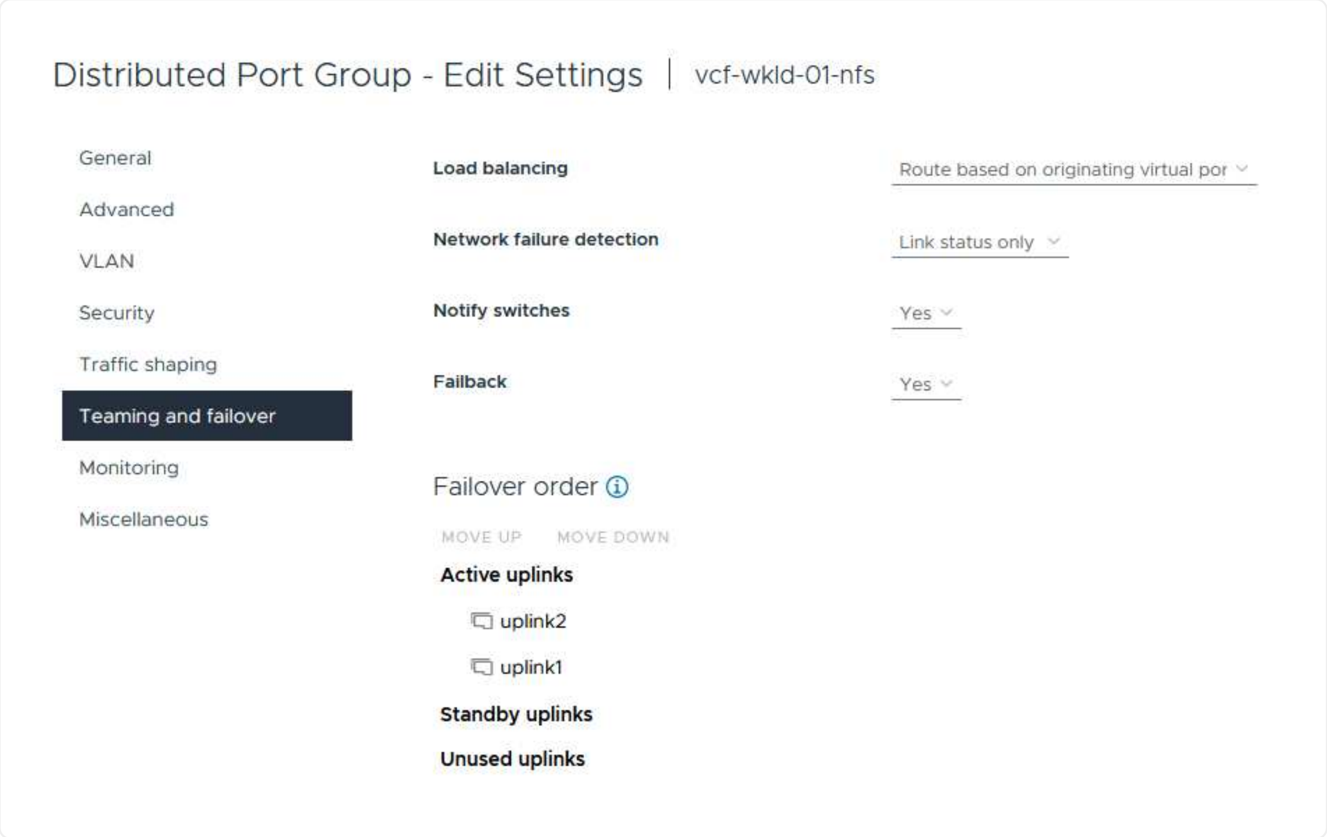
4. On the **Ready to complete** page, review the changes and click **Finish** to create the new distributed port group.
5. Once the port group has been created, navigate to the port group and select the action to **Edit settings…**.

Show example



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**.

Show example



Distributed Port Group - Edit Settings | vcf-wkld-01-nfs

Load balancing: Route based on originating virtual por

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

Failover order

Active uplinks
- uplink2
- uplink1

Standby uplinks

Unused uplinks

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

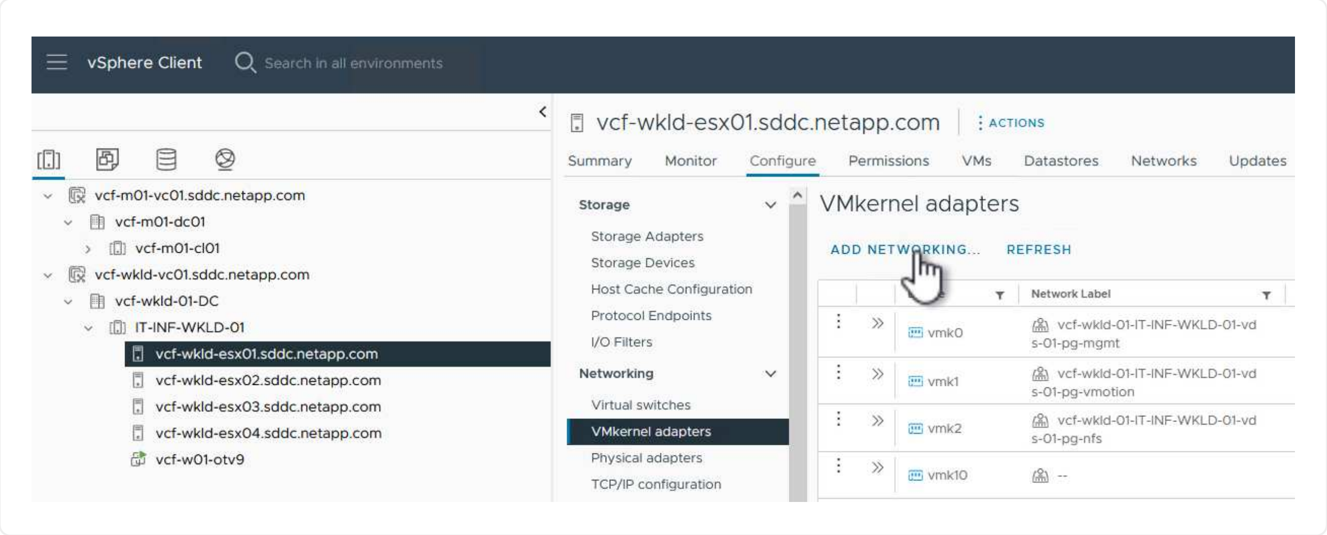
Step 2: Create a VMkernel adapter on each ESXi host

Create a VMkernel adapter on each ESXi host in the workload domain.

Steps

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 **Add Networking…** to start.

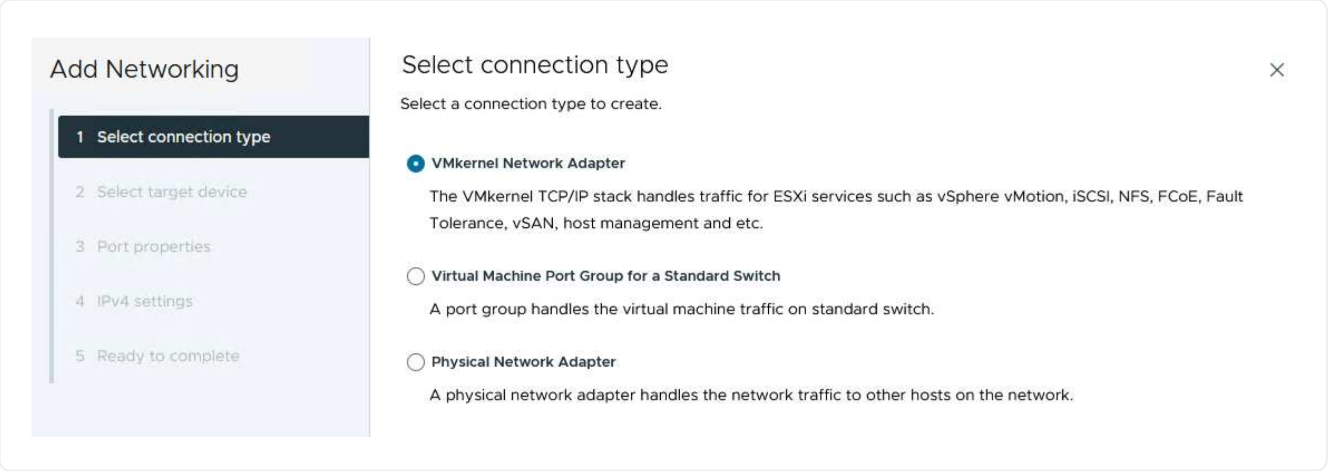
Show example



	Network Label
vmk0	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt
vmk1	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion
vmk2	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs
vmk10	--

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

Show example



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**

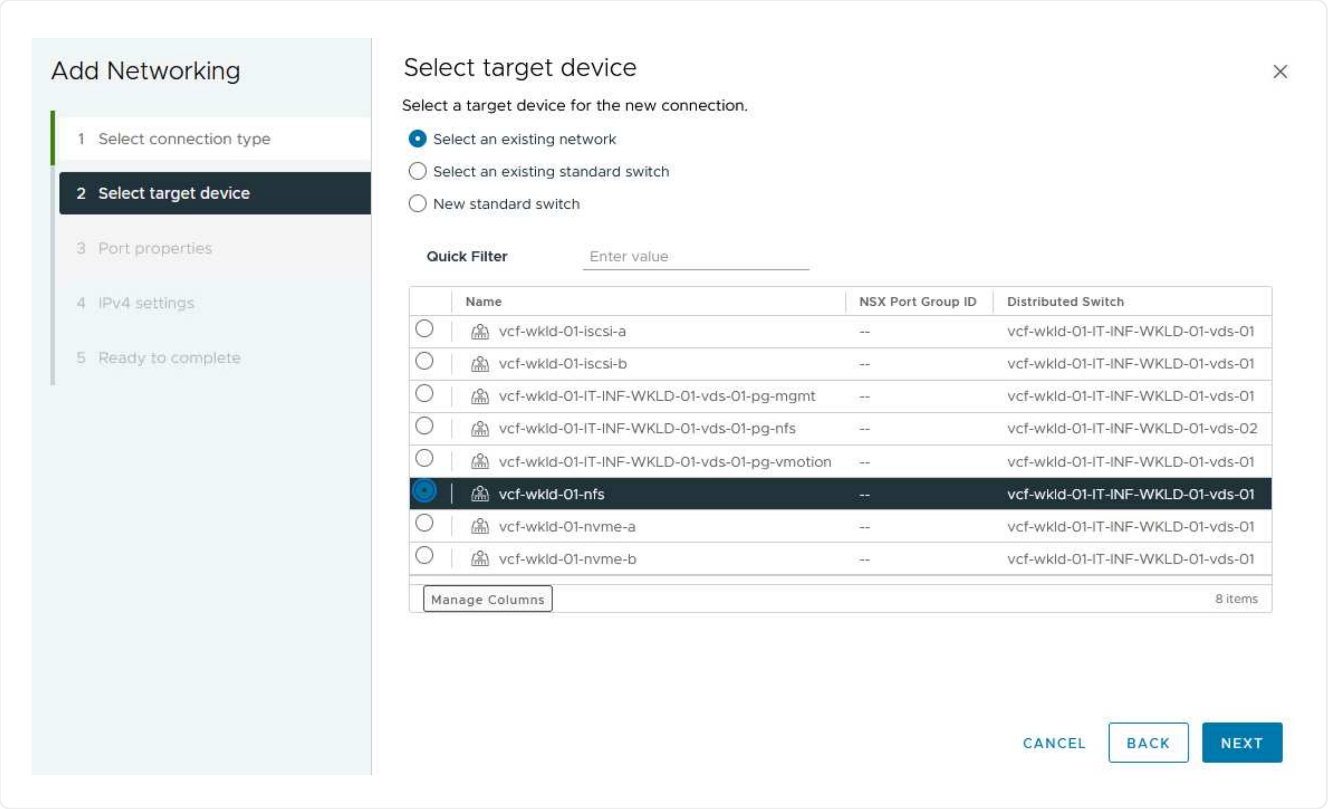
A port group handles the virtual machine traffic on standard switch.

○ **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.

Show example



Select target device

Select a target device for the new connection.

● Select an existing network

○ Select an existing standard switch

○ New standard switch

Quick Filter Enter value

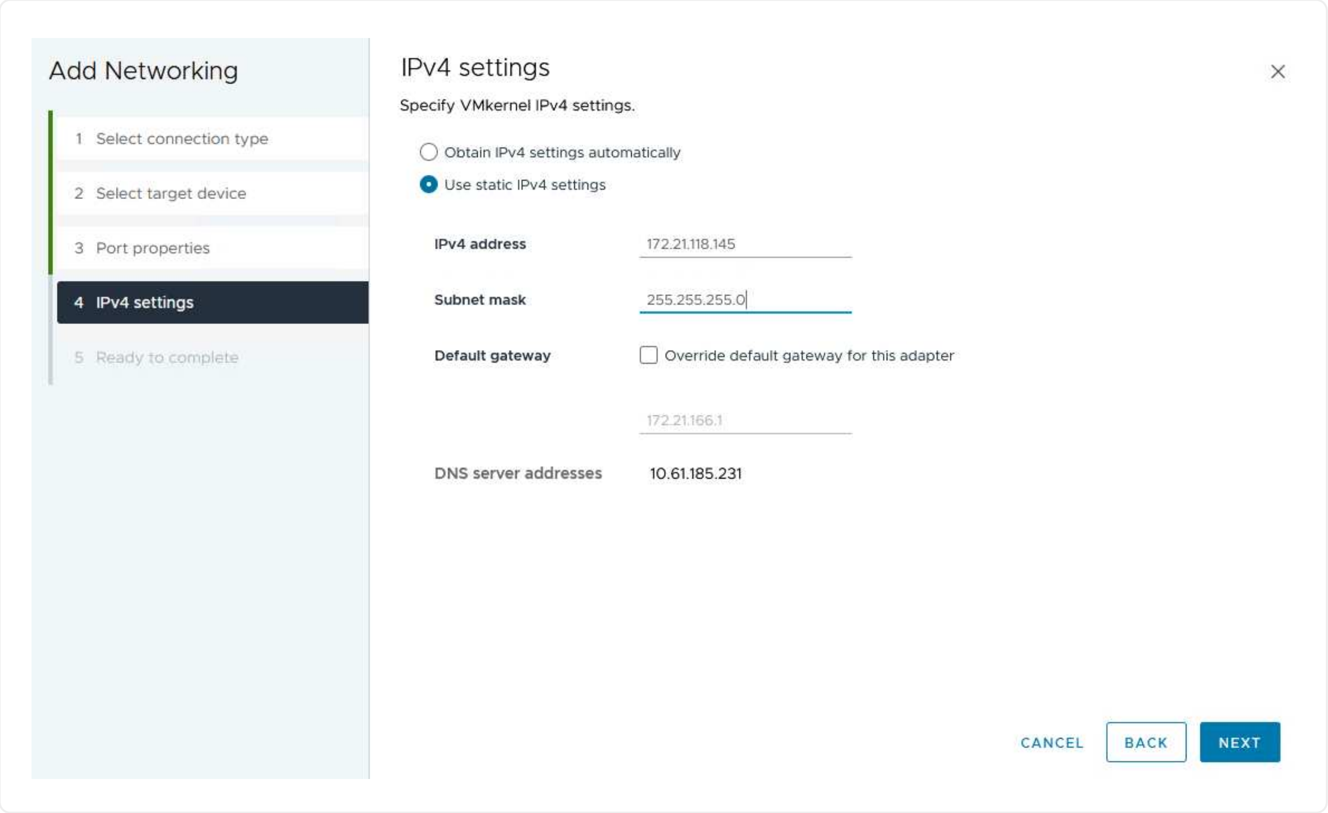
	Name	NSX Port Group ID	Distributed Switch
○	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
●	vcf-wkld-01-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

8 items

4. On the **Port properties** page, keep the defaults (no enabled services) and click **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 **Next** to continue.

Show example



Add Networking

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

IPv4 settings

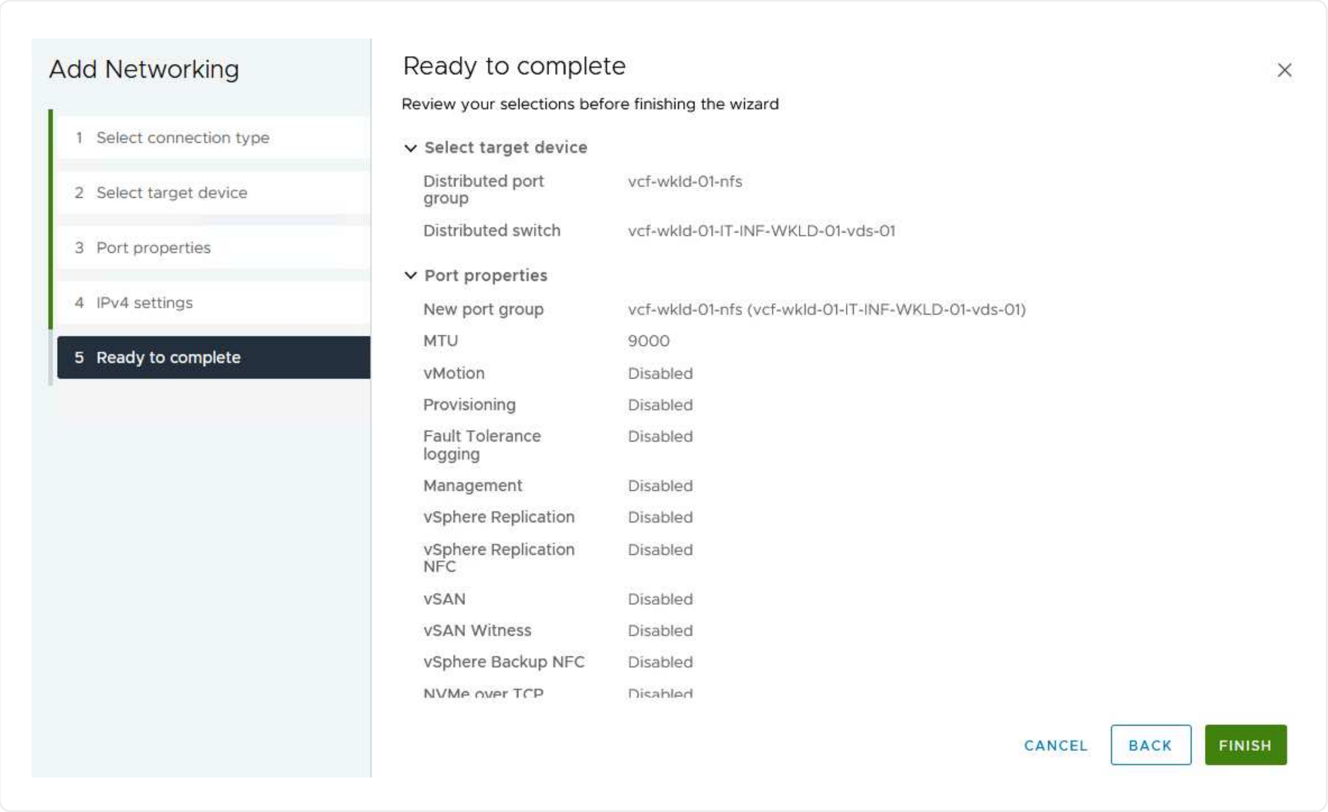
Specify VMkernel IPv4 settings.

○ Obtain IPv4 settings automatically
● Use static IPv4 settings

IPv4 address	172.21.118.145
Subnet mask	255.255.255.0
Default gateway	□ Override default gateway for this adapter
	172.21.166.1
DNS server addresses	10.61.185.231

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

Show example



Add Networking

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

Ready to complete

Review your selections before finishing the wizard

Select target device

Distributed port group	vcf-wkld-01-nfs
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Port properties

New port group	vcf-wkld-01-nfs (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Disabled

What’s next?

After you configure networking for NFS on all ESXi hosts in the workload domain, configure storage for NFS vVols.

Configure NFS vVols storage in a VCF VI workload domain using ONTAP tools

Configure NFS vVols storage in a VI workload domain. After you deploy ONTAP tools for VMware vSphere, you’ll use the vSphere client interface to add the storage system, create a storage capability profile, and provision a vVols datastore.

Step 1: Deploy ONTAP tools for VMware vSphere

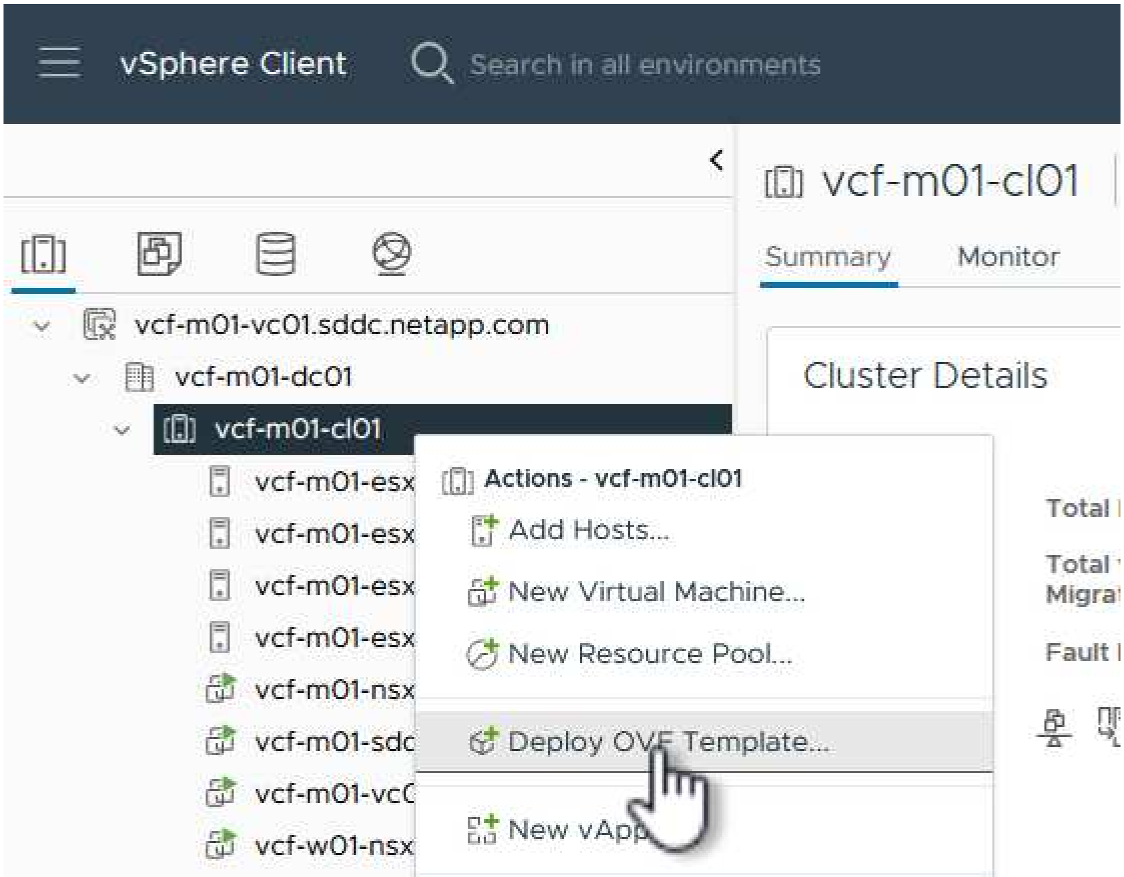
For VI workload domains, ONTAP tools is installed to the VCF Management Cluster but registered with the vCenter associated with the VI workload domain.

ONTAP tools for VMware vSphere is deployed as a VM appliance and provides an integrated vCenter UI for managing ONTAP storage.

Steps

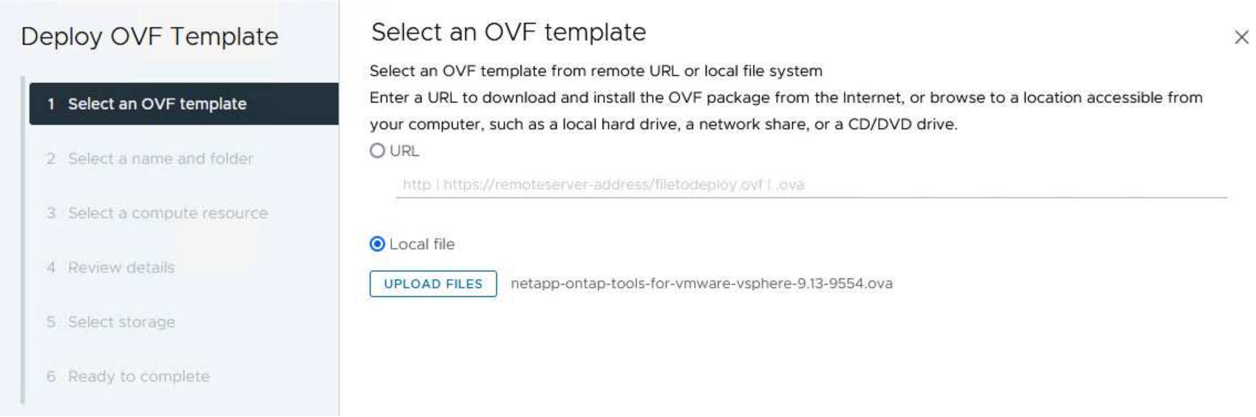
1. Obtain the ONTAP tools OVA image from the NetApp Support site and download it to a local folder.
2. Log into the vCenter appliance for the VCF management domain.
3. From the vCenter appliance interface right-click the management cluster and select **Deploy OVF Template…**

Show example



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

   Show example



Select an OVF template

Select an OVF template from remote URL or local file system

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

○ URL

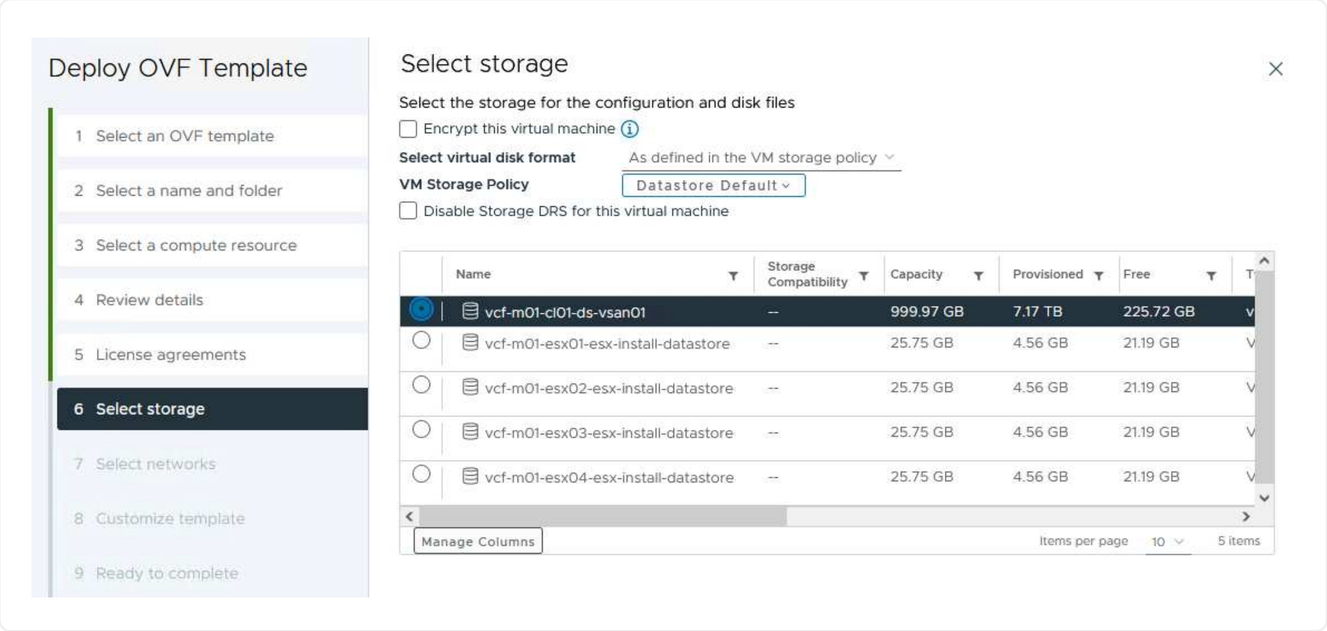
http | https://remoteserver-address/filetodeploy.ovf | .ova

● Local file

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

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

Show example



Deploy OVF Template

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

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine

Select virtual disk format: As defined in the VM storage policy

VM Storage Policy: Datastore Default

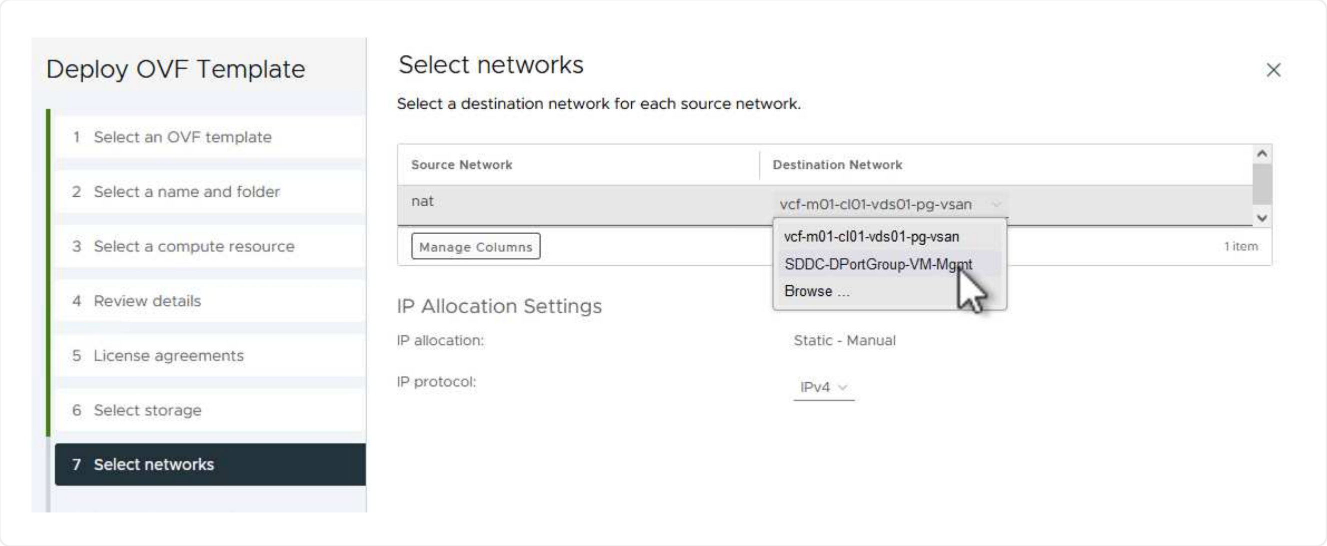
□ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	v
○	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
○	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V

Manage Columns | Items per page 10 | 5 items

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

Show example



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks

Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	vcf-m01-cl01-vds01-pg-vsan

Manage Columns | 1 item

IP Allocation Settings

IP allocation: Static - Manual

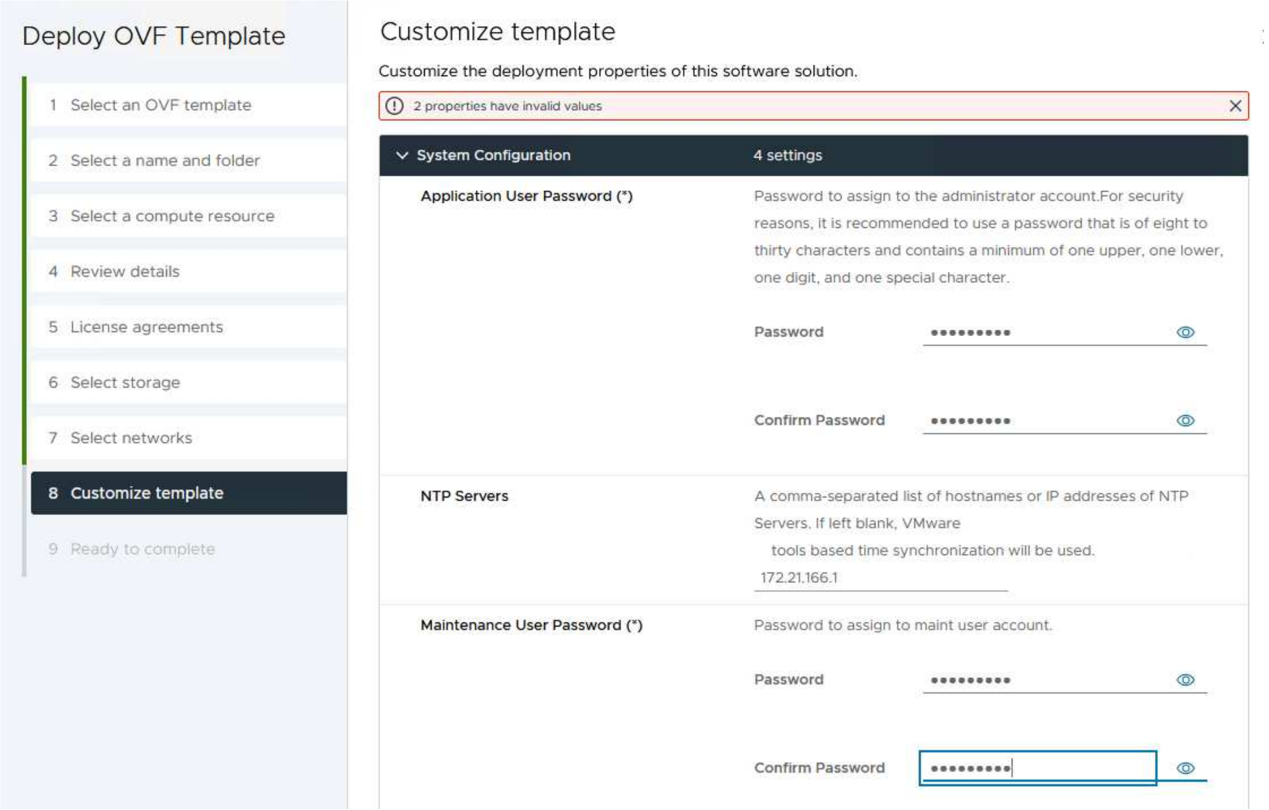
IP protocol: IPv4

8. On the **Customize template** page, enter all required information:

   - Password to be used for administrative access to ONTAP tools.
   - NTP server IP address.
   - ONTAP tools maintenance account password.
   - ONTAP tools Derby DB password.
   - Do not check the box to **Enable VMware Cloud Foundation (VCF)**. VCF mode is not required for deploying supplemental storage.
   - FQDN or IP address of the vCenter appliance for the **VI Workload Domain**
   - Credentials for the vCenter appliance of the **VI Workload Domain**
   - Required network properties.

9. Click **Next** to continue.

Show example



Deploy OVF Template

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

Customize template

Customize the deployment properties of this software solution.

ⓘ 2 properties have invalid values ✕

∨ System Configuration — 4 settings

Application User Password (*) — Password to assign to the administrator account.For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.

Password: •••••••••

Confirm Password: •••••••••

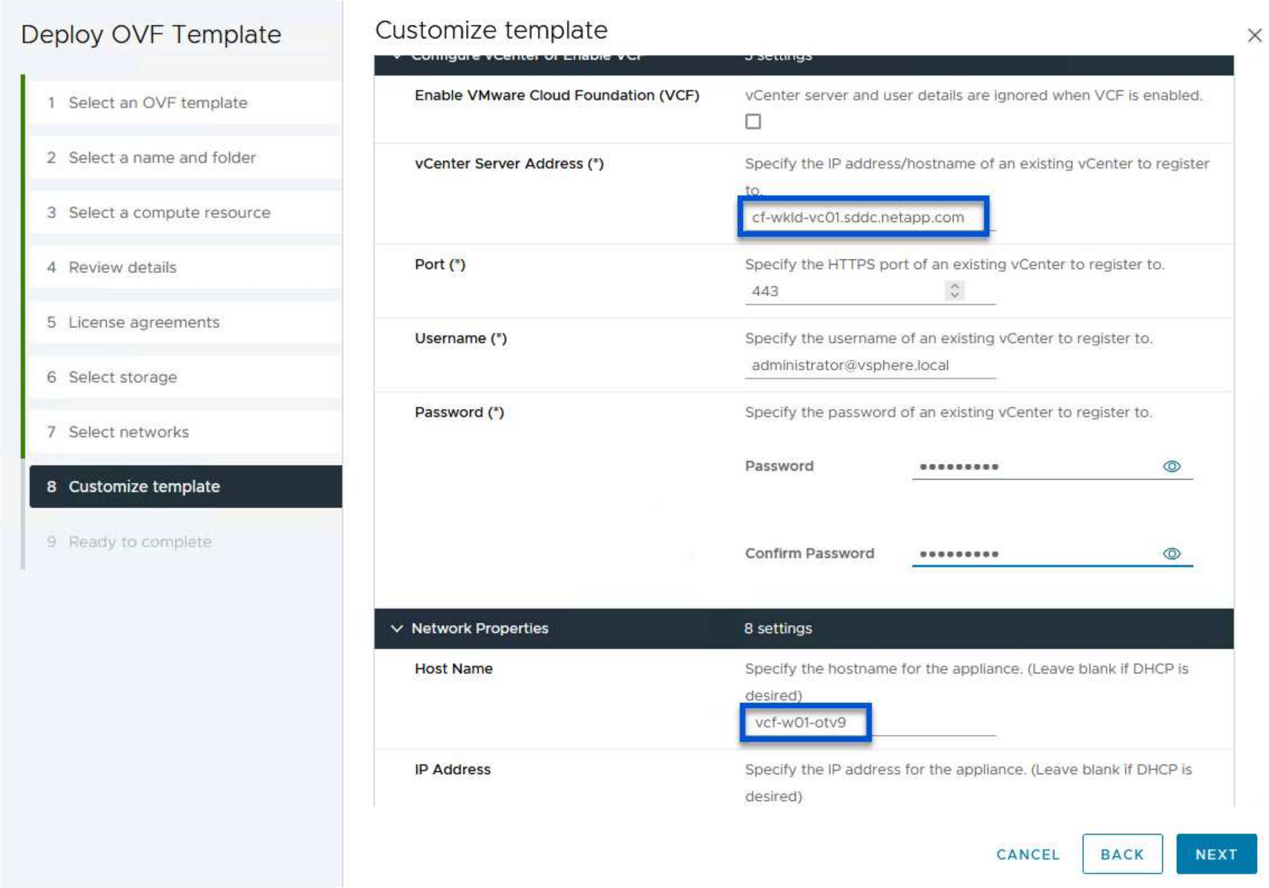
NTP Servers — A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used.

172.21.166.1

Maintenance User Password (*) — Password to assign to maint user account.

Password: •••••••••

Confirm Password: •••••••••



Deploy OVF Template

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

Customize template ✕

∨ Configure vCenter or Enable VCF — 5 settings

Enable VMware Cloud Foundation (VCF) — vCenter server and user details are ignored when VCF is enabled.

☐

vCenter Server Address (*) — Specify the IP address/hostname of an existing vCenter to register to.

cf-wkld-vc01.sddc.netapp.com

Port (*) — Specify the HTTPS port of an existing vCenter to register to.

443

Username (*) — Specify the username of an existing vCenter to register to.

administrator@vsphere.local

Password (*) — Specify the password of an existing vCenter to register to.

Password: •••••••••

Confirm Password: •••••••••

∨ Network Properties — 8 settings

Host Name — Specify the hostname for the appliance. (Leave blank if DHCP is desired)

vcf-w01-otv9

IP Address — Specify the IP address for the appliance. (Leave blank if DHCP is desired)

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

Step 2: Add a storage system

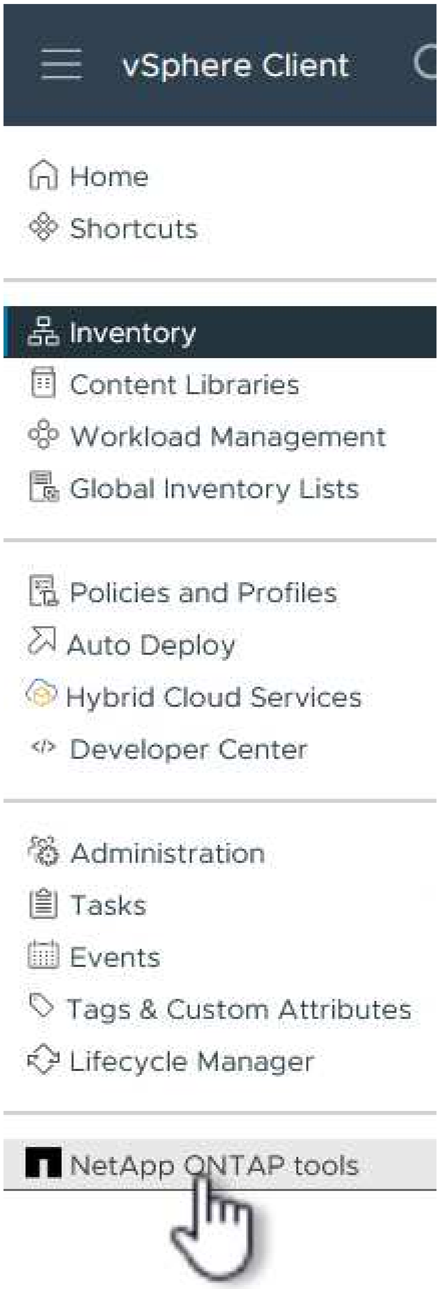
Perform the following steps to add a storage system using ONTAP tools.

> vVol requires ONTAP cluster credentials rather than SVM credentials. For more information, refer to the ONTAP tools for VMware vSphere documentation: Add storage systems.

Steps

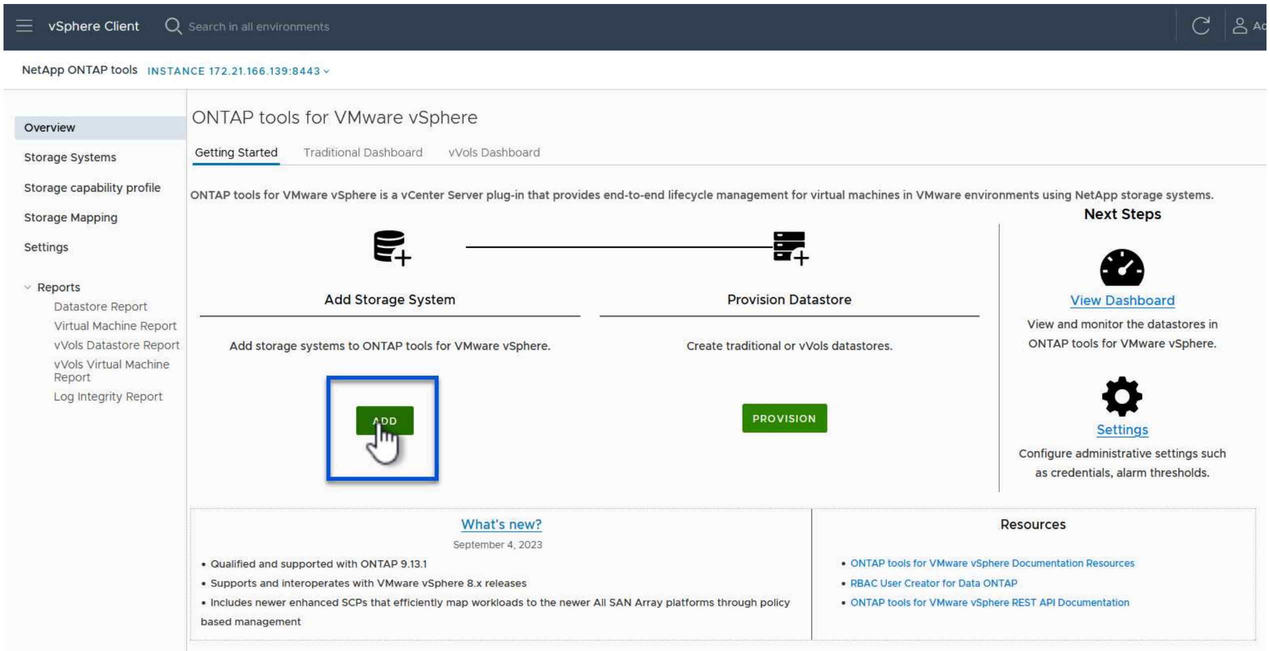
1. In the vSphere client navigate to the main menu and select **NetApp ONTAP tools**.

Show example



2. Once in **ONTAP tools**, from the Getting Started page (or from **Storage Systems**), click **Add** to add a new storage system.

Show example



ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.

Add storage systems to ONTAP tools for VMware vSphere.

Create traditional or vVols datastores.

View and monitor the datastores in ONTAP tools for VMware vSphere.

Configure administrative settings such as credentials, alarm thresholds.

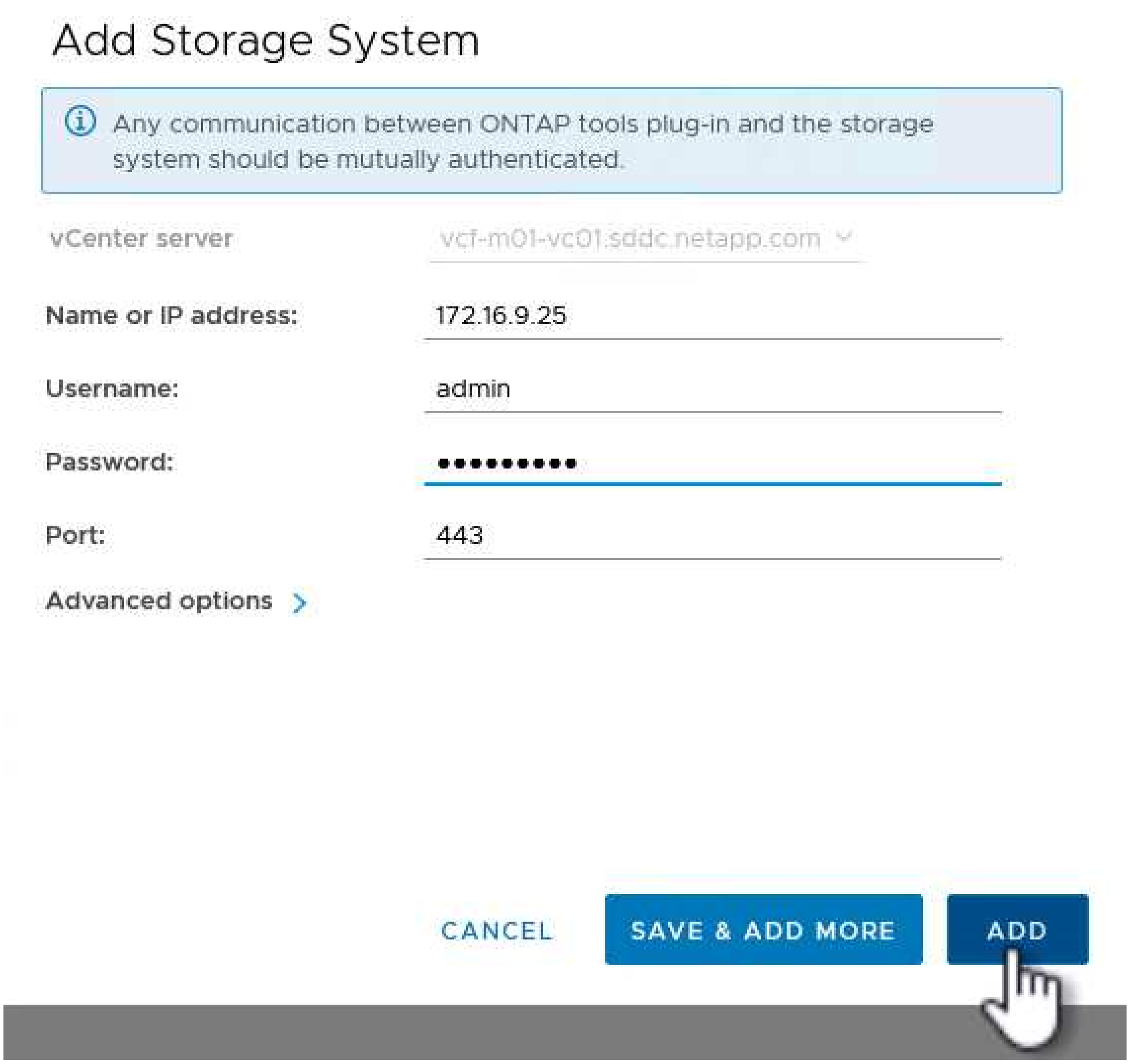
September 4, 2023

- Qualified and supported with ONTAP 9.13.1
- Supports and interoperates with VMware vSphere 8.x releases
- Includes newer enhanced SCPs that efficiently map workloads to the newer All SAN Array platforms through policy based management

- ONTAP tools for VMware vSphere Documentation Resources
- RBAC User Creator for Data ONTAP
- ONTAP tools for VMware vSphere REST API Documentation

3. Provide the IP address and credentials of the ONTAP storage system and click **Add**.

Show example



Add Storage System

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

vCenter server: vcf-m01-vc01.sddc.netapp.com

Name or IP address: 172.16.9.25

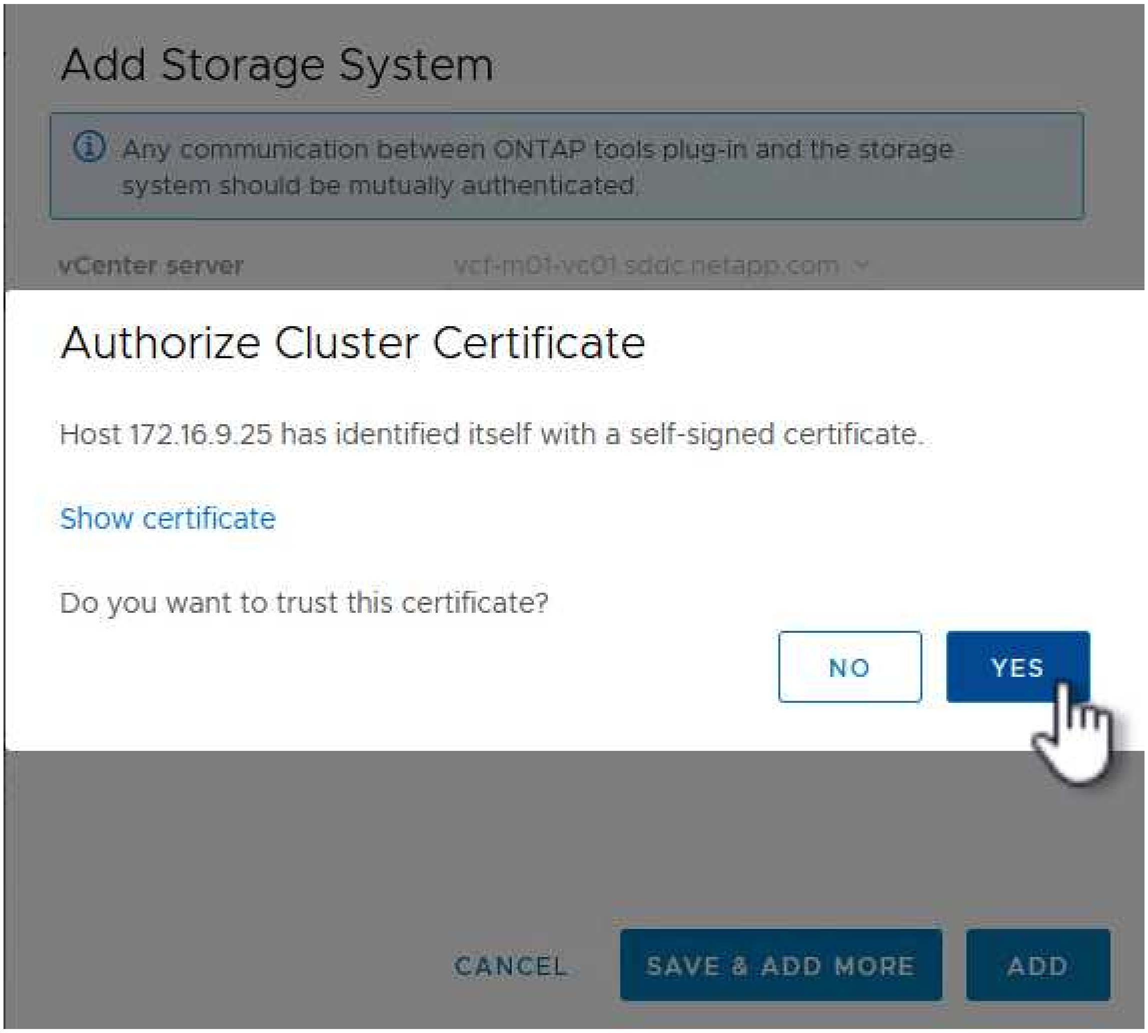
Username: admin

Password: ••••••••••

Port: 443

4. Click **Yes** to authorize the cluster certificate and add the storage system.

Show example



Add Storage System

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

vCenter server vcf-m01-vc01.sddc.netapp.com

Authorize Cluster Certificate

Host 172.16.9.25 has identified itself with a self-signed certificate.

Show certificate

Do you want to trust this certificate?

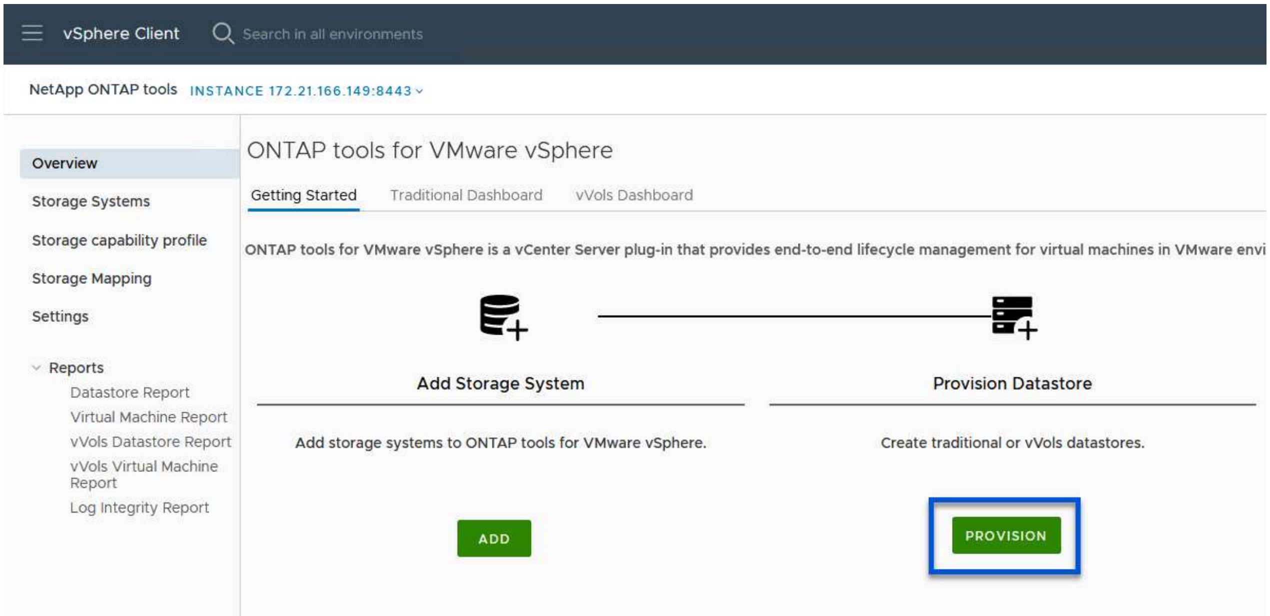
Step 3: Create an NFS datastore in ONTAP tools

Complete the following steps to deploy an ONTAP datastore running on NFS. Use ONTAP tools.

Steps

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

Show example



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

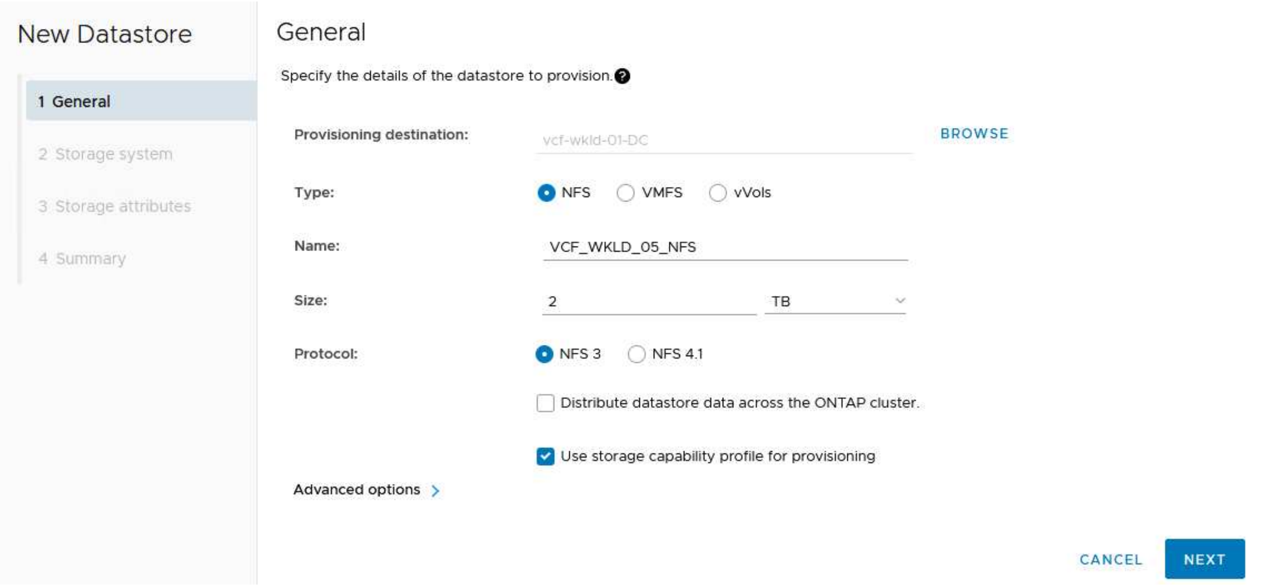
Add storage systems to ONTAP tools for VMware vSphere.

Create traditional or vVols datastores.

2. On the **General** page of the New Datastore wizard, select the vSphere datacenter or cluster destination.
3. Select **NFS** as the datastore type, enter a name for the datastore, and select the protocol.
4. Choose whether to use FlexGroup volumes and whether to use a storage capability file for provisioning.
5. Click **Next** to continue.

> Selecting to **Distribute datastore data across the cluster** will create the underlying volume as a FlexGroup volume, which precludes the use of Storage Capability Profiles. Refer to Supported and unsupported configurations for FlexGroup volumes for more information on using FlexGroup Volumes.

Show example



Specify the details of the datastore to provision.

Provisioning destination: vcf-wkld-01-DC

Type: ● NFS ○ VMFS ○ vVols

Name: VCF_WKLD_05_NFS

Size: 2 TB

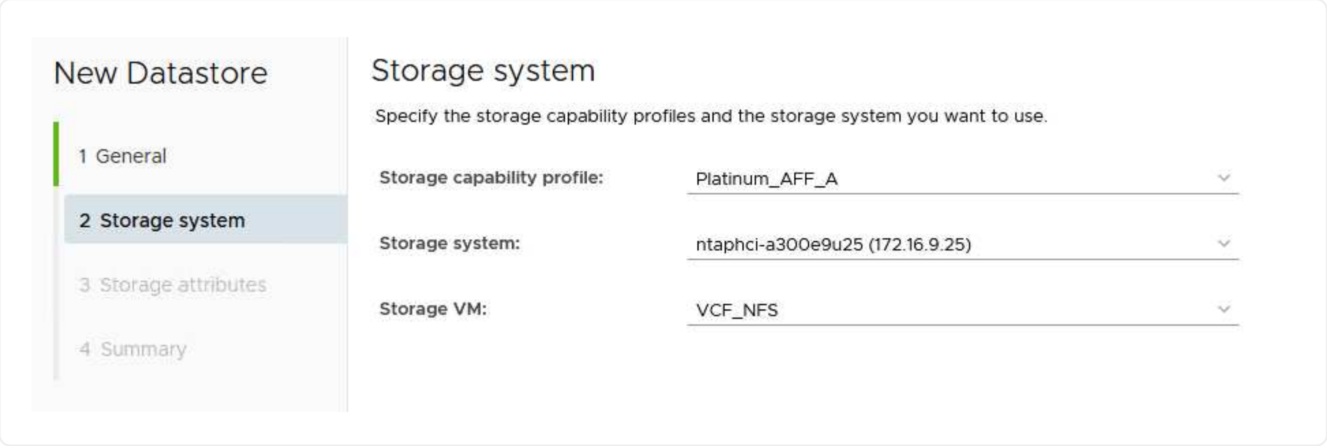
Protocol: ● NFS 3 ○ NFS 4.1

☐ Distribute datastore data across the ONTAP cluster.

☑ Use storage capability profile for provisioning

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

   Show example

   New Datastore

   1 General
   2 Storage system
   3 Storage attributes
   4 Summary

   Storage system

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

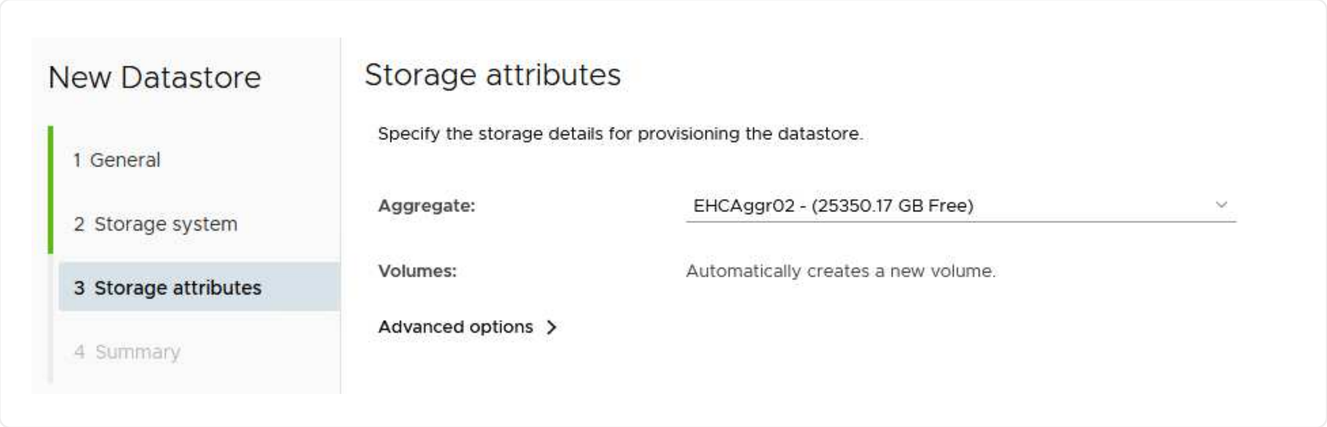
   Storage capability profile: Platinum_AFF_A

   Storage system: ntaphci-a300e9u25 (172.16.9.25)

   Storage VM: VCF_NFS

7. On the **Storage attributes** page, select the aggregate to use and then click **Next** to continue.

   Show example

   New Datastore

   1 General
   2 Storage system
   3 Storage attributes
   4 Summary

   Storage attributes

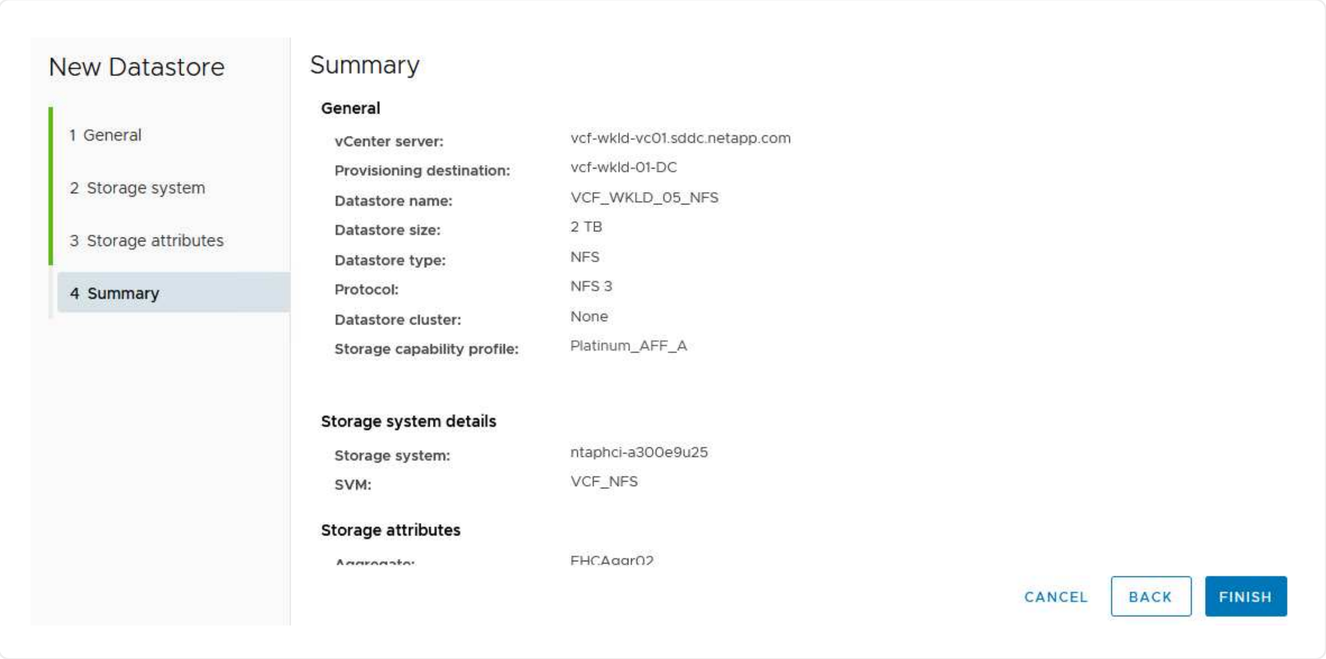
   Specify the storage details for provisioning the datastore.

   Aggregate: EHCAggr02 - (25350.17 GB Free)

   Volumes: Automatically creates a new volume.

8. Review the **Summary** and click **Finish** to begin creating the NFS datastore.

Show example



New Datastore

1 General
2 Storage system
3 Storage attributes
4 Summary

Summary

General

vCenter server:	vcf-wkld-vc01.sddc.netapp.com
Provisioning destination:	vcf-wkld-01-DC
Datastore name:	VCF_WKLD_05_NFS
Datastore size:	2 TB
Datastore type:	NFS
Protocol:	NFS 3
Datastore cluster:	None
Storage capability profile:	Platinum_AFF_A

Storage system details

Storage system:	ntaphci-a300e9u25
SVM:	VCF_NFS

Storage attributes

Aggregate:	EHCAggr02

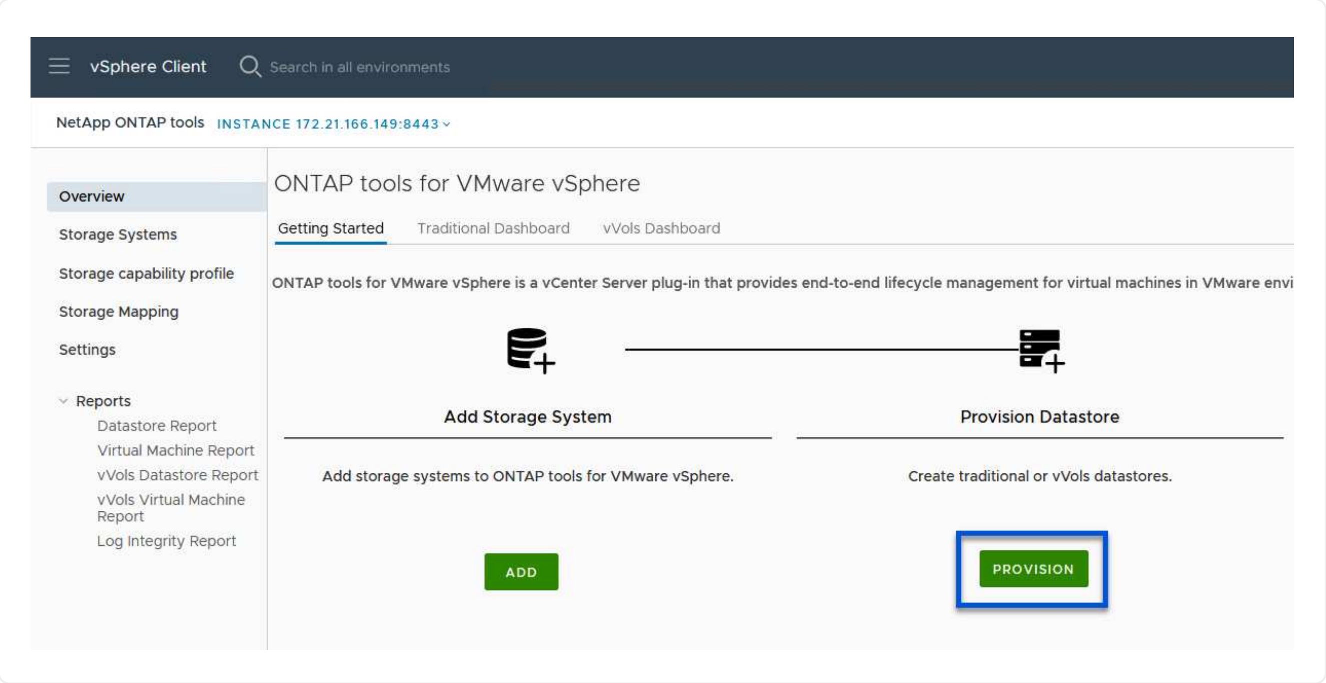
Step 4: Create a vVols datastore in ONTAP tools

To create a vVols datastore in ONTAP tools, complete the following steps.

Steps

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

   Show example



ONTAP tools for VMware vSphere

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

Add Storage System

Add storage systems to ONTAP tools for VMware vSphere.

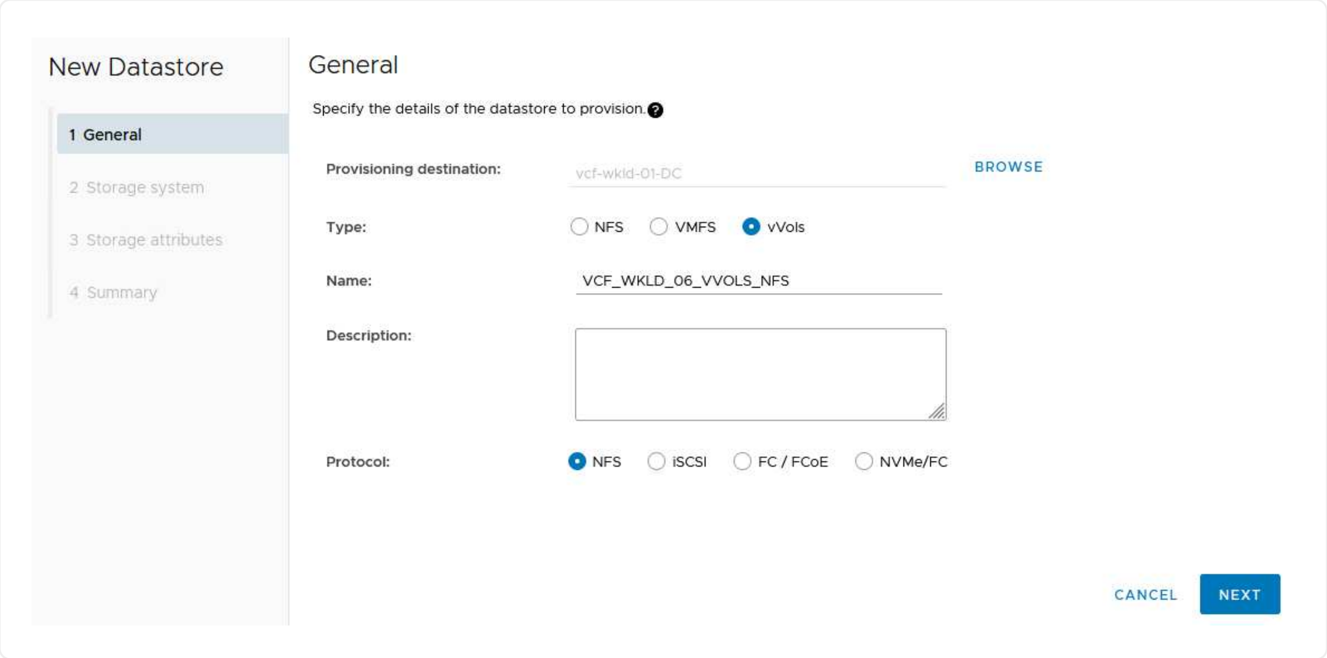
Provision Datastore

Create traditional or vVols datastores.

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

4. Click **Next** to continue.

Show example



General

Specify the details of the datastore to provision.

Provisioning destination: vcf-wkld-01-DC

Type: ○ NFS ○ VMFS ● vVols

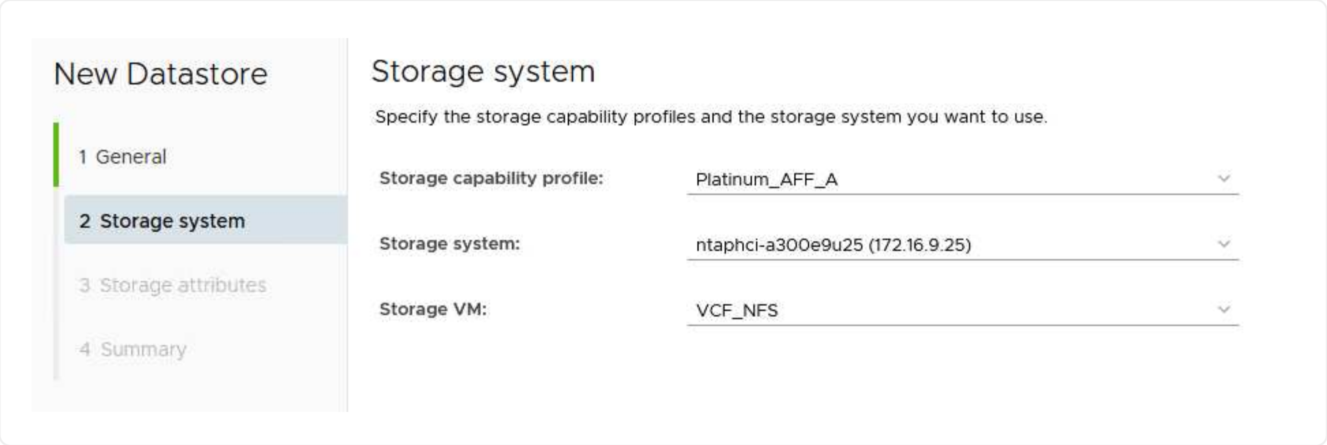
Name: VCF_WKLD_06_VVOLS_NFS

Description:

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

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

Show example



Storage system

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

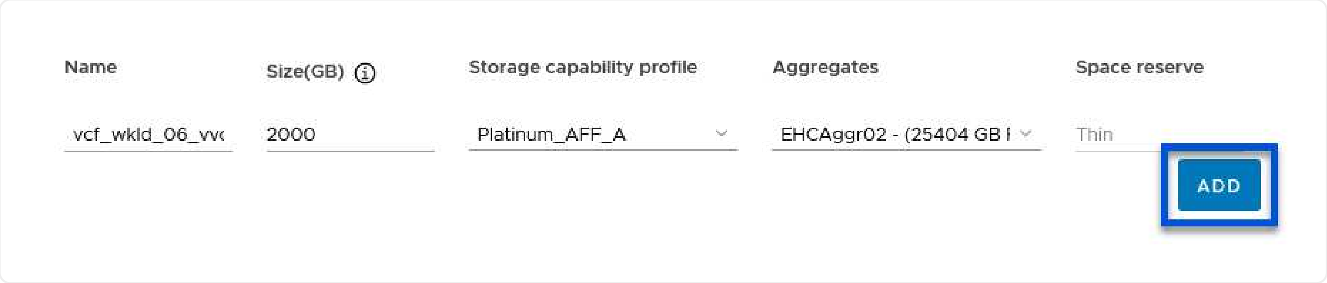
Storage capability profile: Platinum_AFF_A

Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: VCF_NFS

7. On the **Storage attributes** page, select **Create a new volumes** and enter the storage attributes of the volume to be created.

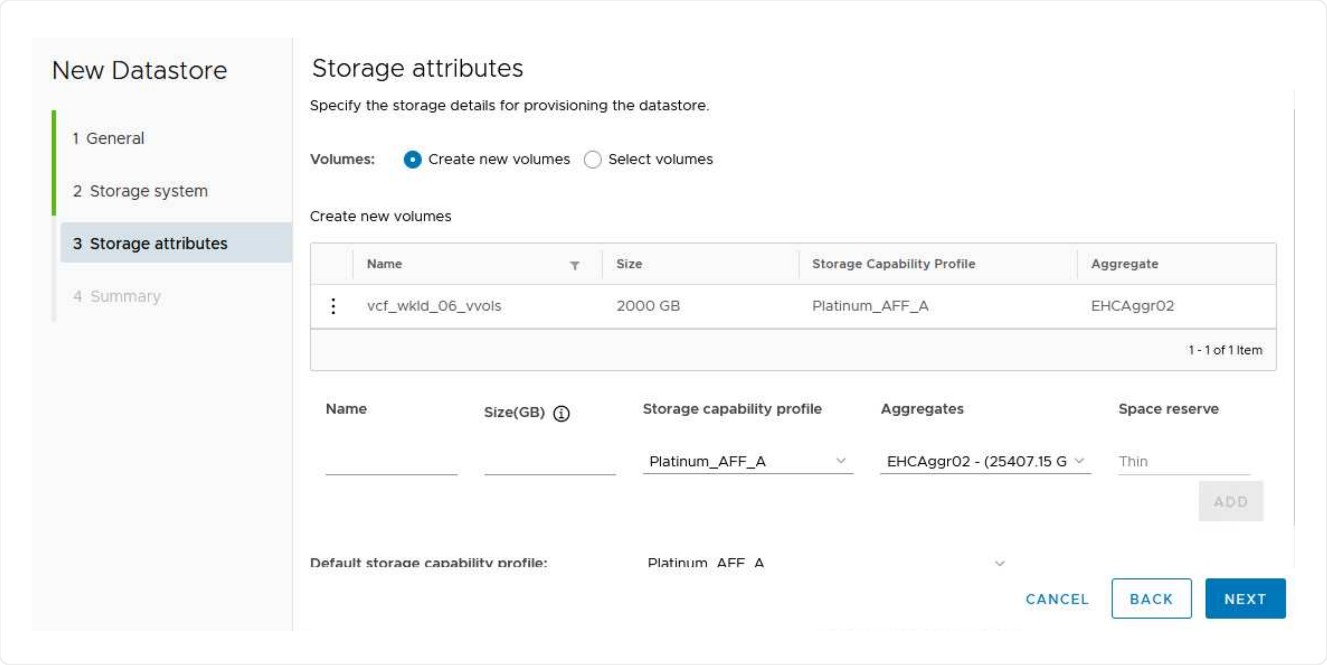
Show example



Name	Size(GB)	Storage capability profile	Aggregates	Space reserve
vcf_wkld_06_vvc	2000	Platinum_AFF_A	EHCAggr02 - (25404 GB I	Thin

8. Click **Add** to create the volume and then **Next** to continue.

Show example



New Datastore

1 General
2 Storage system
3 Storage attributes
4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: ● Create new volumes ○ Select volumes

Create new volumes

	Name	Size	Storage Capability Profile	Aggregate
⋮	vcf_wkld_06_vvols	2000 GB	Platinum_AFF_A	EHCAggr02

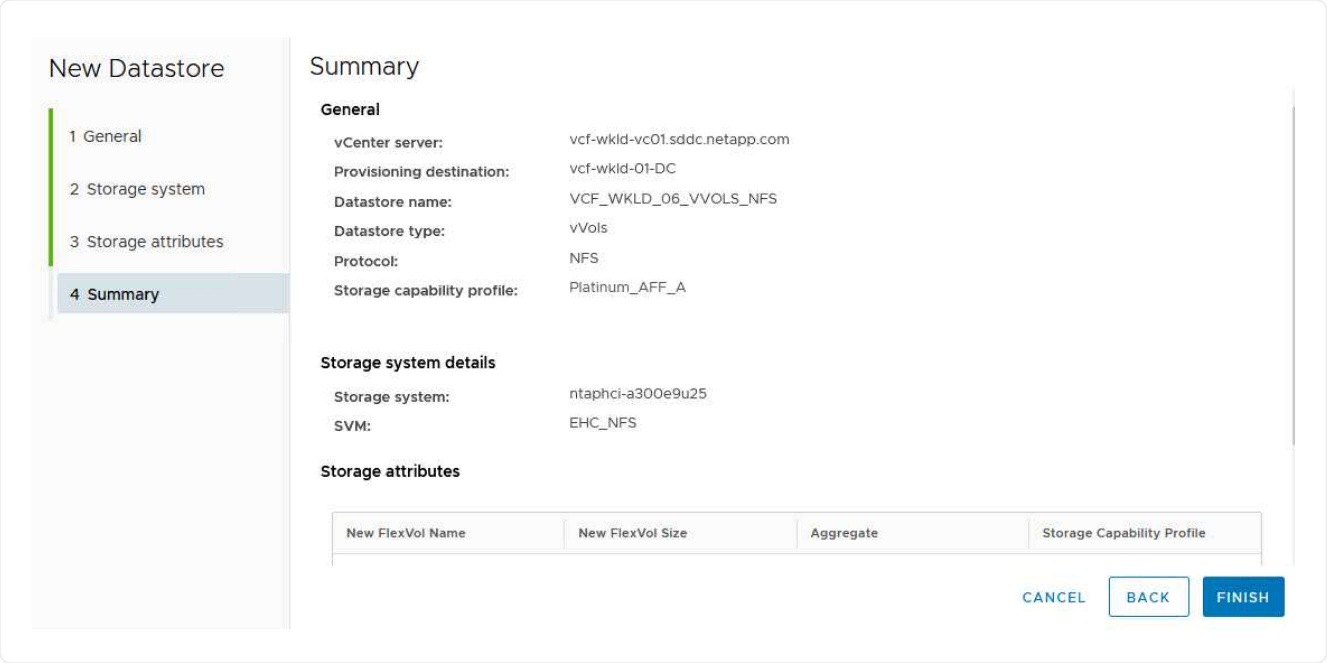
1 - 1 of 1 Item

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
		Platinum_AFF_A	EHCAggr02 - (25407.15 G	Thin

Default storage capability profile: Platinum_AFF_A

9. Review the **Summary** page and click **Finish** to start the vVol datastore creation process.

Show example



New Datastore

1 General
2 Storage system
3 Storage attributes
4 Summary

Summary

General

vCenter server:	vcf-wkld-vc01.sddc.netapp.com
Provisioning destination:	vcf-wkld-01-DC
Datastore name:	VCF_WKLD_06_VVOLS_NFS
Datastore type:	vVols
Protocol:	NFS
Storage capability profile:	Platinum_AFF_A

Storage system details

Storage system:	ntaphci-a300e9u25
SVM:	EHC_NFS

Storage attributes

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile

Additional information

- For information on configuring ONTAP storage systems, refer to the ONTAP 9 documentation.
- For information on configuring VCF, refer to the VMware Cloud Foundation documentation.
- For information on deploying and using ONTAP tools in multiple vCenter environments, refer to the Requirements for registering ONTAP tools in multiple vCenter server environments.

- For video demos of this solution, refer to VMware datastore provisioning.

Expand VI workload domains with NVMe/TCP

Deployment workflow for adding vVols NVMe datastores as supplemental storage in a VI workload domain

Get started with adding NVMe/TCP vVols datastores as supplemental storage for a VMware Cloud Foundation (VCF) Virtual Infrastructure (VI) workload domain. You'll review the deployment requirements, set up an NVMe/TCP-enabled SVMs and LIFs, configure ESXi host networking, and deploy the NVMe/TCP datastore.

1 **Review the deployment requirements**

Review the requirements to deploy NVMe/TCP datastore in a VMware Cloud Foundation VI workload domain.

2 **Create the SVM and LIFs and the NVMe namespace**

Create a storage virtual machine with logical interfaces and the NVMe namespace for NVMe/TCP traffic.

3 **Configure networking**

Create distributed port groups and vmkernel adapters on the ESXi hosts for the VI workload domain.

4 **Configure storage**

Deploy the NVMe/TCP datastore.

Deployment requirements for NVMe vVols in a VI workload domain

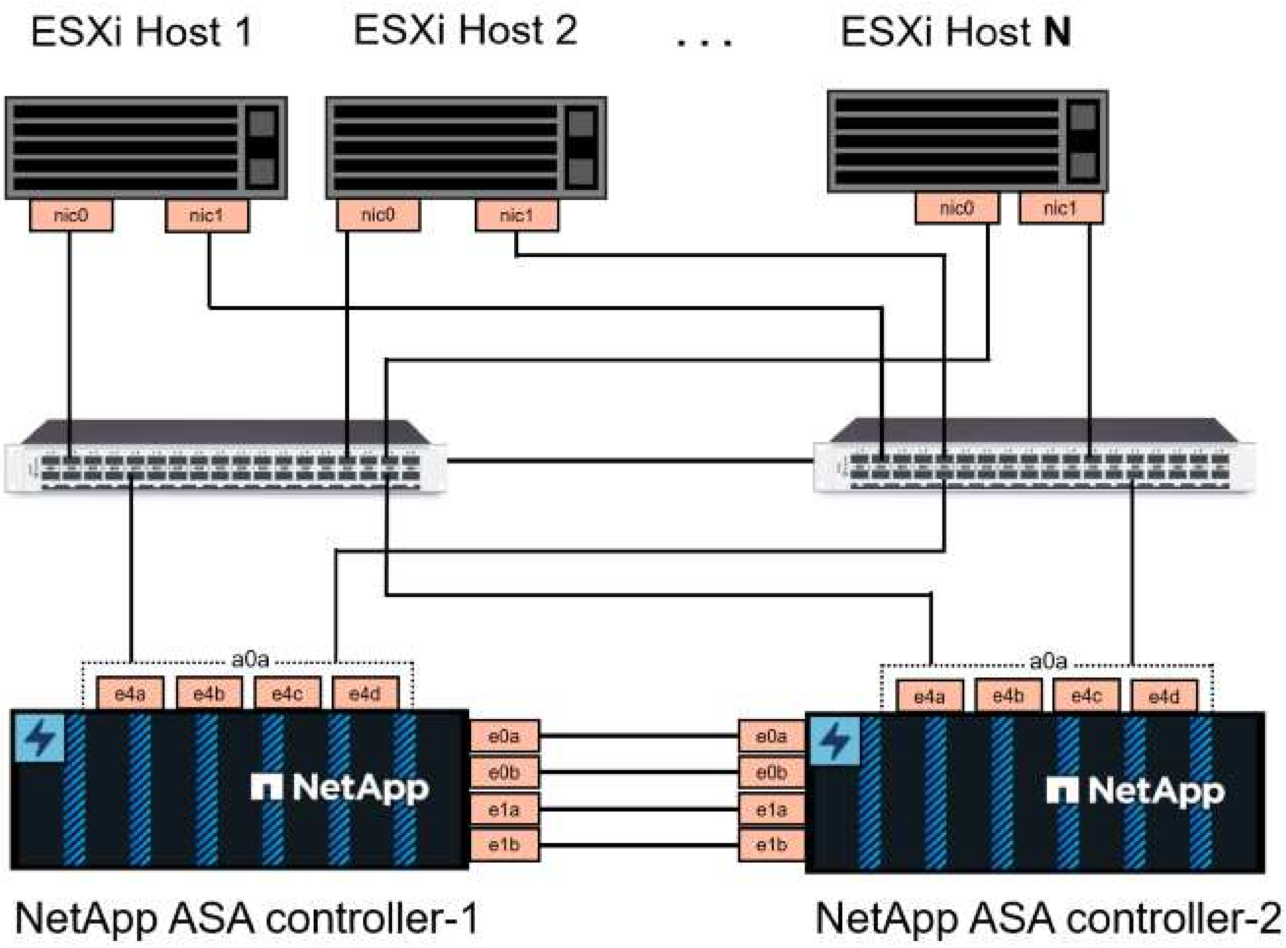
Review the recommended network design and infrastructure requirements to deploy NVMe vVols in a VMware Cloud Foundation VI workload domain. You need a fully configured ONTAP AFF or ASA storage system, a deployed VCF management domain, and an existing VI workload domain.

Infrastructure requirements

- An ONTAP AFF or ASA storage system with physical data ports on Ethernet switches dedicated to storage traffic.
- VCF management domain deployment is complete and the vSphere client is accessible.
- A VI workload domain has been previously deployed.

Recommended NVMe/TCP network design

NetApp recommends fully redundant network designs for NVMe/TCP. The following diagram illustrates an example of a redundant configuration, providing fault tolerance for storage systems, switches, networks adapters and host systems.



For multipathing and failover across multiple paths, configure a minimum of two LIFs per storage node in separate Ethernet networks for all SVMs in NVMe/TCP configurations.

What’s next?

After reviewing the deployment requirements, create the SVM and LIFs.

Create SVM and LIFs and the NVMe namespace for NVMe/TCP vVols datastores in a VCF VI workload domain

Create a Storage Virtual Machine (SVM) with multiple Logical Interfaces (LIFs) to provide NVMe connectivity for VMware Cloud Foundation workload domains. This procedure summarizes setting up an NVMe/TCP-enabled SVM and LIFs and creating the NVMe namespaces.

Step 1: Create the SVMs and LIFs

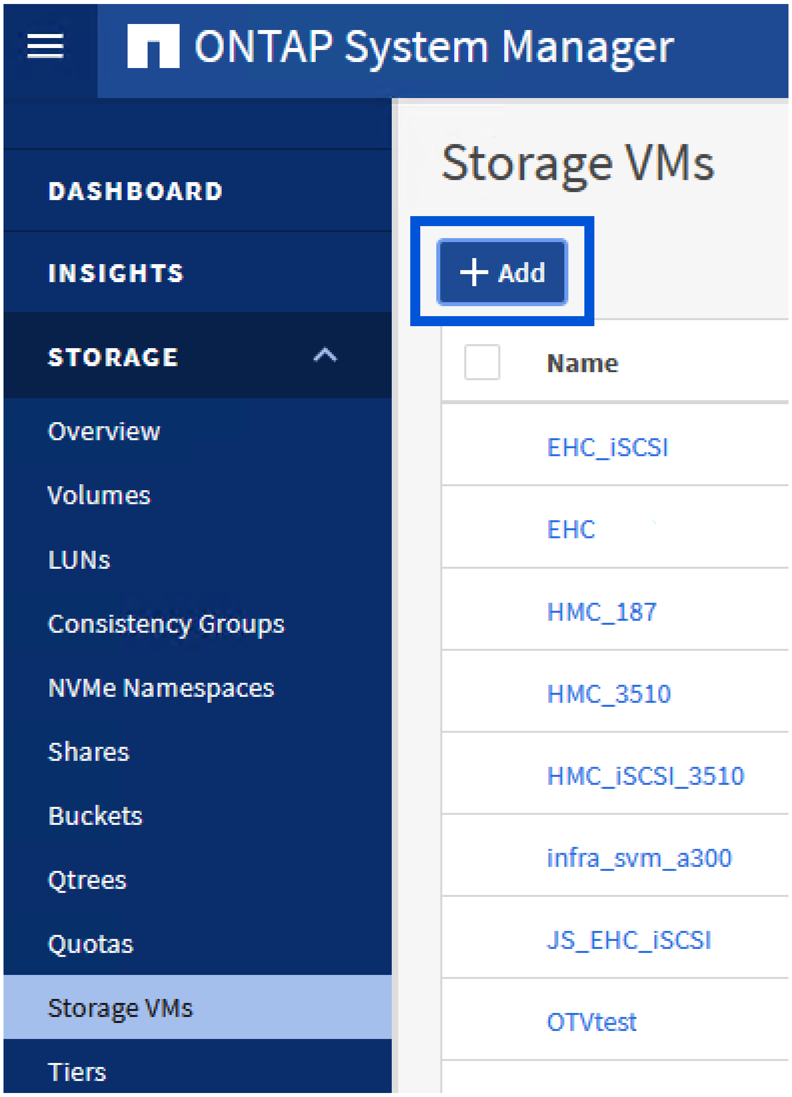
Complete the following steps to create an SVM with multiple LIFs for NVMe/TCP traffic.

To add new LIFs to an existing SVM, refer to the ONTAP documentation: Create ONTAP LIFs.

Steps

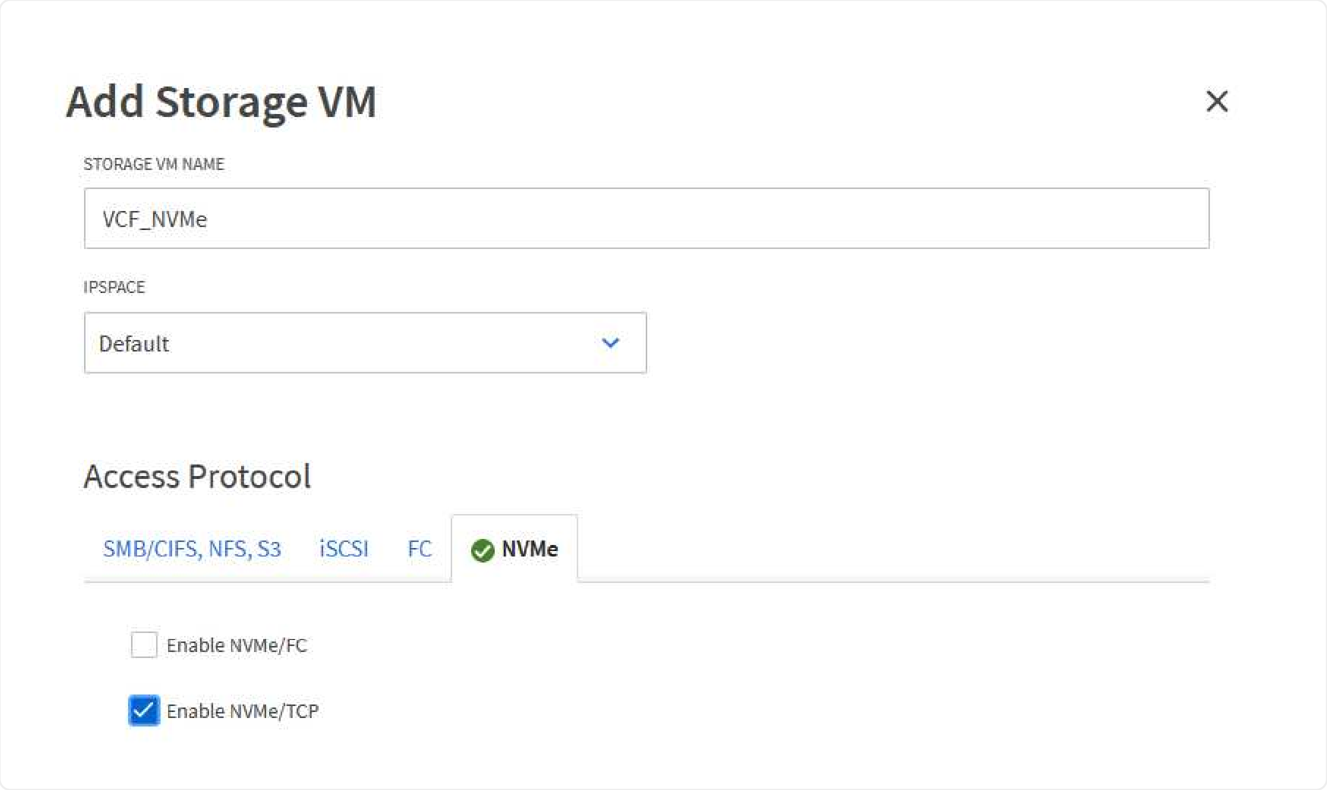
1. From ONTAP System Manager, navigate to **Storage VMs** in the left-hand menu and click **+ Add**.

Show example



2. In the **Add Storage VM** wizard, enter a **Name** for the SVM, select the **IP Space** and then, under **Access Protocol**, click the **NVMe** tab and check the box to **Enable NVMe/TCP**.

Show example



Add Storage VM

STORAGE VM NAME: VCF_NVMe

IPSPACE: Default

Access Protocol

□ Enable NVMe/FC

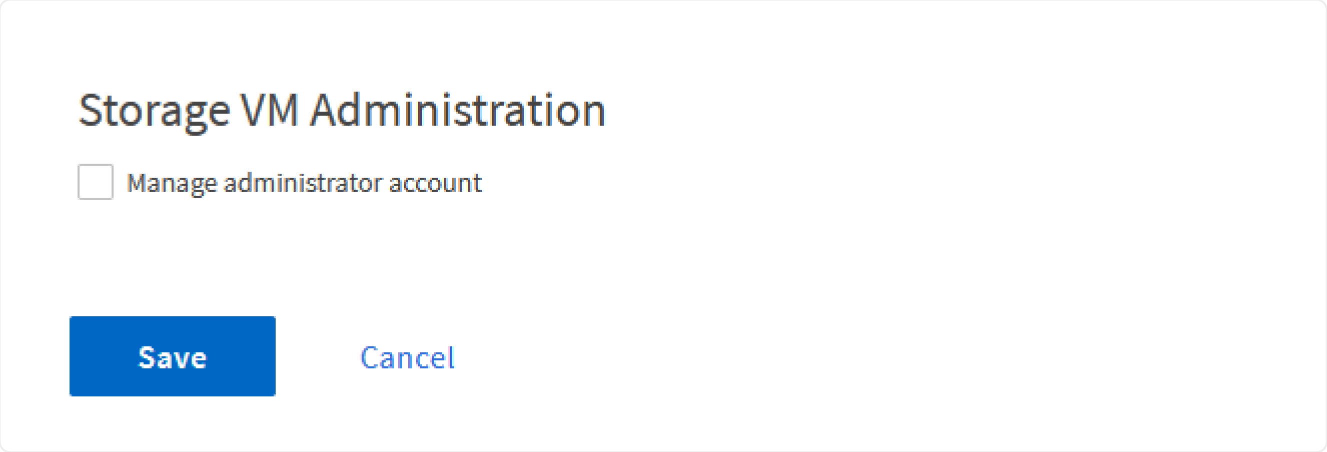
☑ Enable NVMe/TCP

3. In the **Network Interface** section, enter the **IP address**, **Subnet Mask**, and **Broadcast Domain and Port** for the first LIF. For subsequent LIFs, you can either use individual settings or enable the checkbox to use common settings across all remaining LIFs.

   > For multipathing and failover across multiple paths, create a minimum of two LIFs per storage node in separate Ethernet networks for all SVMs in NVMe/TCP configurations.

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

Show example



Storage VM Administration

□ Manage administrator account

Step 2: Create the NVMe Namespace

NVMe namespaces are analogous to LUNs for iSCSi or FC. You must create the NVMe Namespace before a

VMFS datastore can be deployed from the vSphere Client.

To create the NVMe namespace, get the NVMe Qualified Name (NQN) from each ESXi host in the cluster. ONTAP uses the NQN to provide access control for the namespace.

Steps

1. Open an SSH session with an ESXi host in the cluster to obtain its NQN. Use the following command from the CLI:

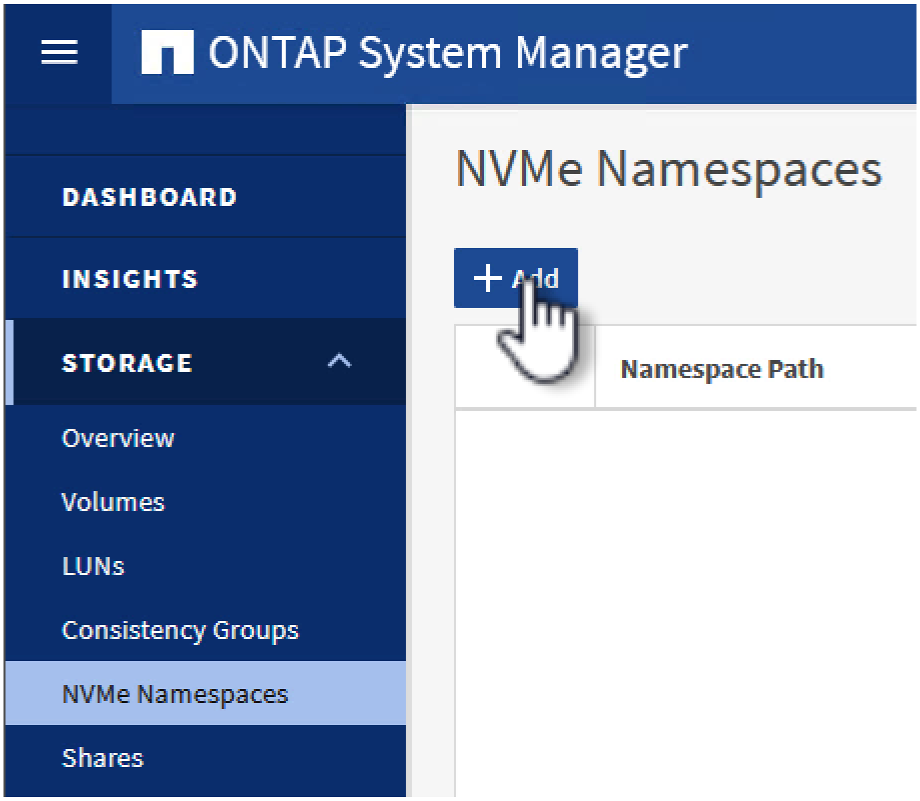
   ```
   esxcli nvme info get
   ```

   An output similar to the following example should be displayed:

   ```
   Host NQN: nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-esx01
   ```

2. Record the NQN for each ESXi host in the cluster.
3. From ONTAP System Manager, navigate to **NVMe Namespaces** in the left-hand menu and click **+ Add** to start.

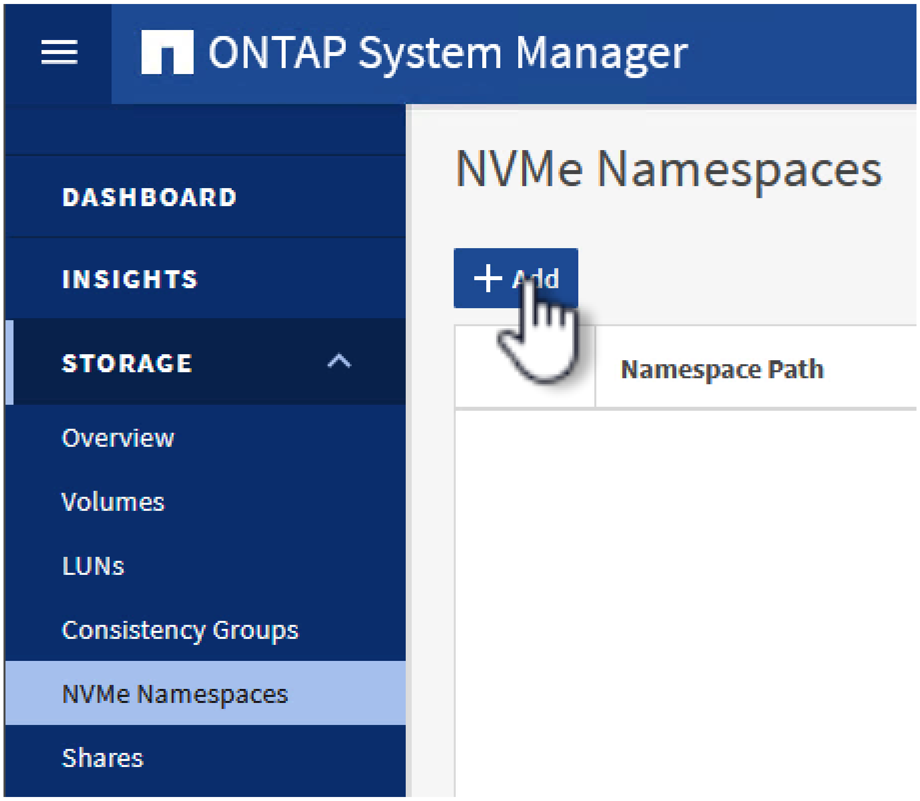
   Show example



4. On the **Add NVMe Namespace** page, fill in a name prefix, the number of namespaces to create, the size of the namespace, and the host operating system that will be accessing the namespace.
5. In the **Host NQN** section, create a comma separated list of the NQN's previously collected from the ESXi hosts that will be accessing the namespaces.

6. Click **More Options** to configure additional items, such as the snapshot protection policy.
7. Finally, click **Save** to create the NVMe Namespace.

   Show example



What’s next?

After creating the SVM and LIFs, configure networking for NVMe/TCP (NVMe/TCP) vVols.

Configure networking for NVMe/TCP on ESXi hosts in a VCF VI workload domain

Configure networking for NVMe over TCP (NVMe/TCP) storage on ESXi hosts in a VI workload domain. You’ll create distributed port groups for NVMe traffic, set up VMkernel adapters on each ESXi host, and add an NVMe/TCP adapter to enable reliable connectivity and multipathing.

Perform the following steps on the VI workload domain cluster using the vSphere client. In this case vCenter Single Sign-On is being used so the vSphere client is common to both the management and workload domains.

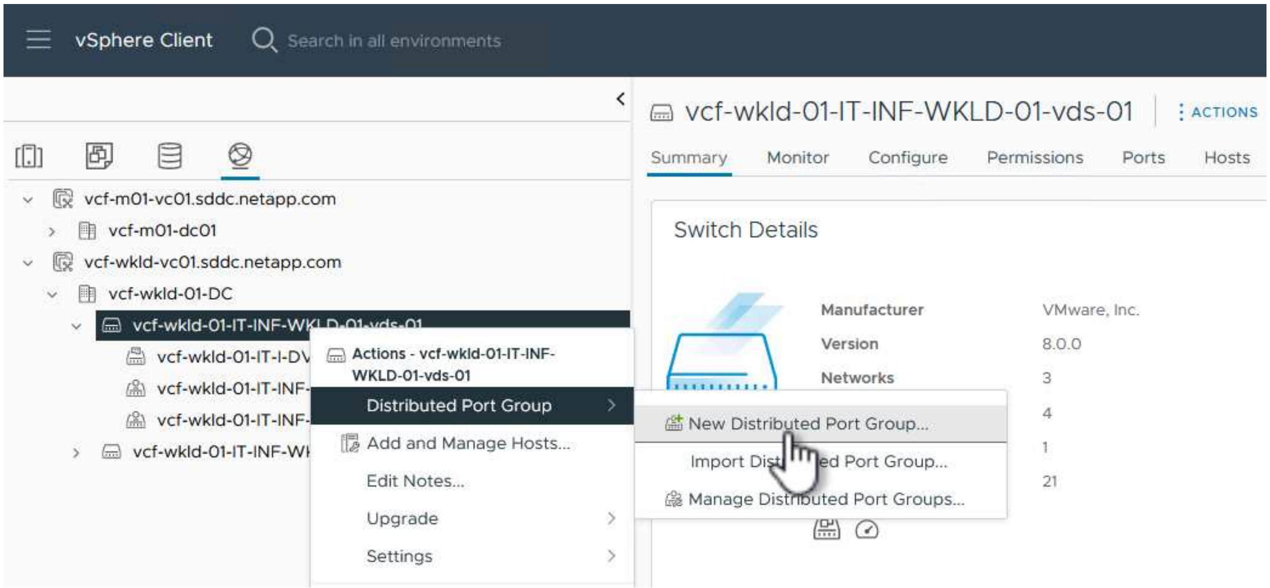
Step 1: Create distributed port groups for NVME/TCP traffic

Complete the following steps to create a new distributed port group for each NVMe/TCP network.

Steps

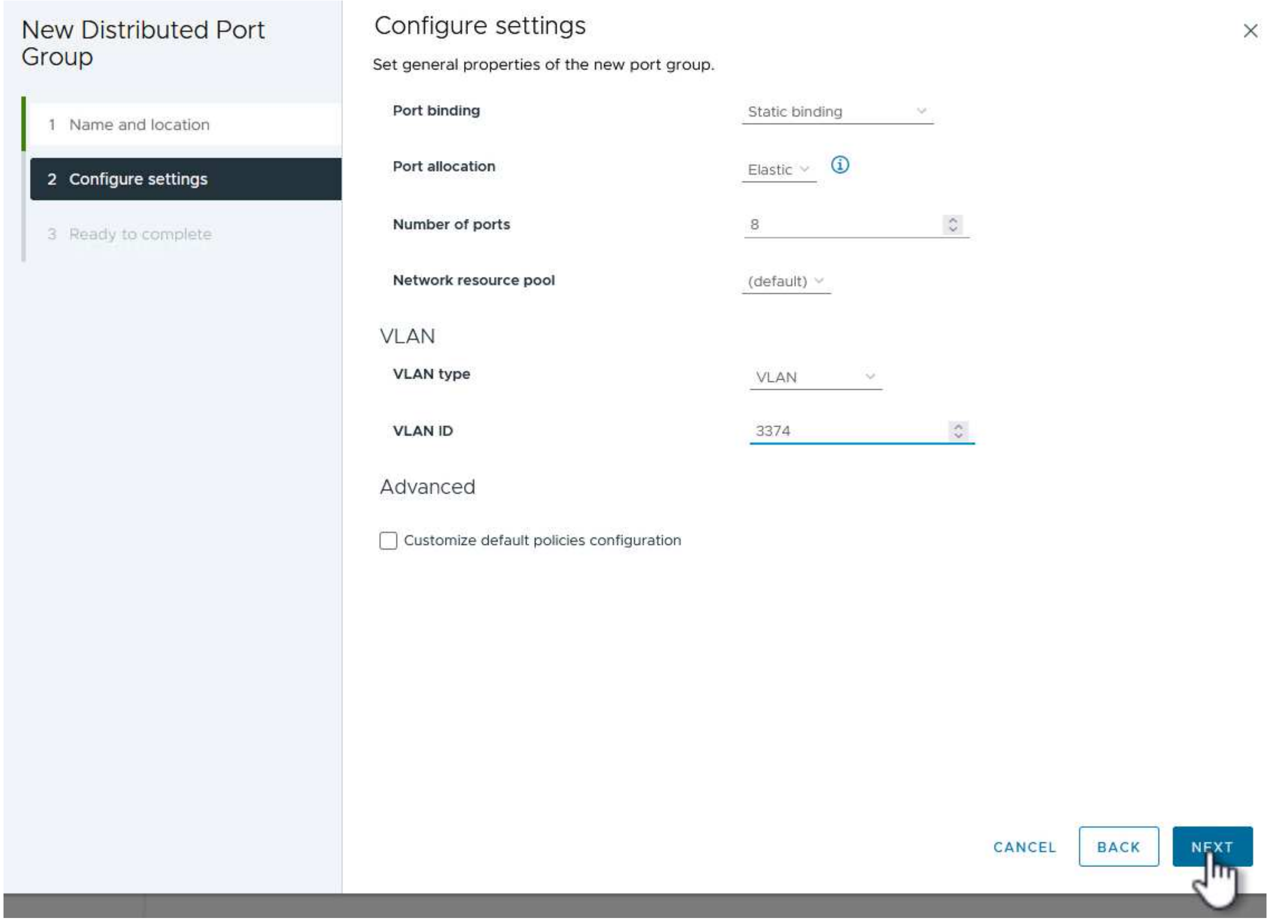
1. From the vSphere client , navigate to **Inventory > Networking** for the workload domain. Navigate to the existing Distributed Switch and choose the action to create **New Distributed Port Group…**.

Show example



2. In the **New Distributed Port Group** wizard, fill in a name for the new port group and click **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 **Next** to continue.

Show example



New Distributed Port Group

1 Name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding: Static binding

Port allocation: Elastic

Number of ports: 8

Network resource pool: (default)

VLAN

VLAN type: VLAN

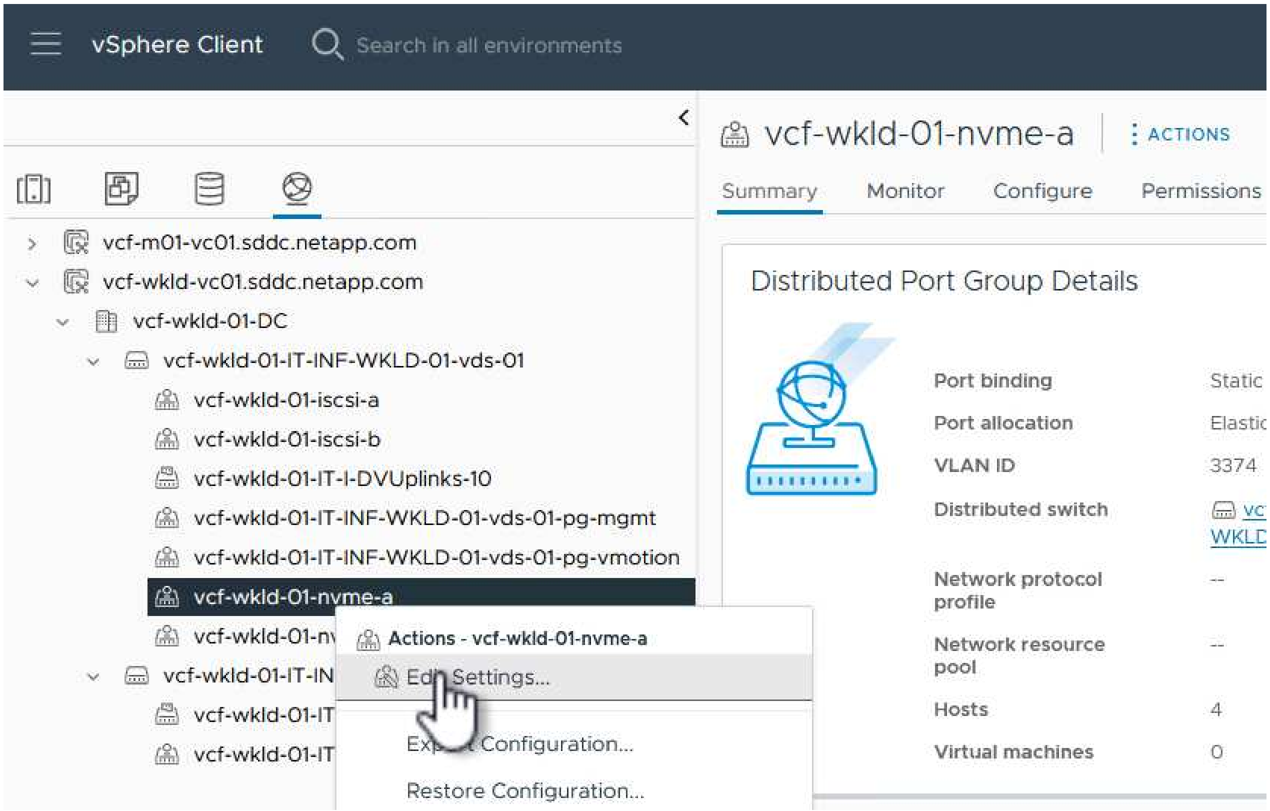
VLAN ID: 3374

Advanced

☐ Customize default policies configuration

4. On the **Ready to complete** page, review the changes and click **Finish** to create the new distributed port group.
5. Repeat this process to create a distributed port group for the second NVMe/TCP network being used and ensure you have input the correct **VLAN ID**.
6. When both port groups have been created, navigate to the first port group and select the action to **Edit settings…**.

Show example

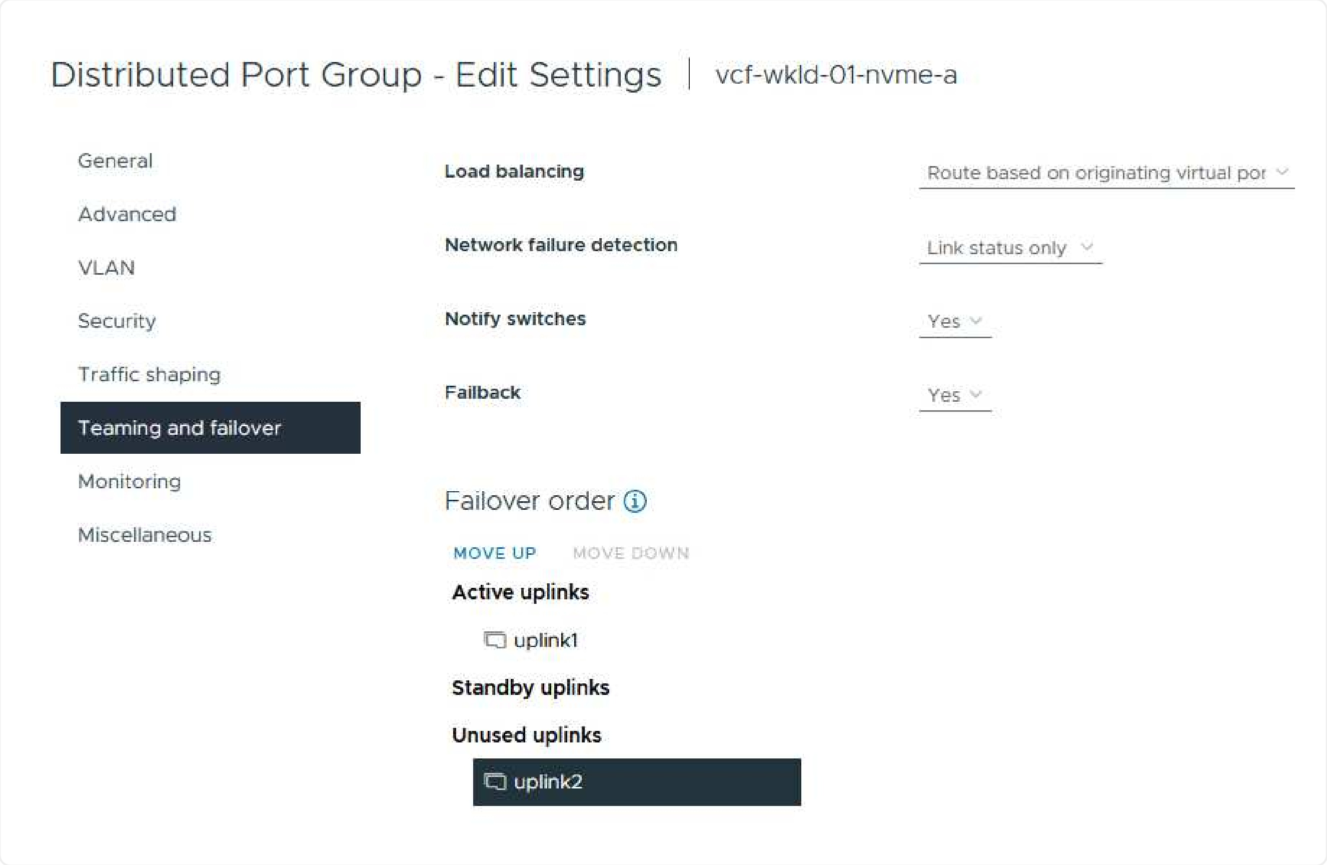


vSphere Client
Search in all environments
vcf-m01-vc01.sddc.netapp.com
vcf-wkld-vc01.sddc.netapp.com
vcf-wkld-01-DC
vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-iscsi-a
vcf-wkld-01-iscsi-b
vcf-wkld-01-IT-I-DVUplinks-10
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion
vcf-wkld-01-nvme-a
vcf-wkld-01-nv
vcf-wkld-01-IT-IN
vcf-wkld-01-IT
vcf-wkld-01-IT
Actions - vcf-wkld-01-nvme-a
Edit Settings...
Export Configuration...
Restore Configuration...
vcf-wkld-01-nvme-a
ACTIONS
Summary
Monitor
Configure
Permissions
Distributed Port Group Details

Port binding	Static
Port allocation	Elastic
VLAN ID	3374
Distributed switch	vc WKLD
Network protocol profile	--
Network resource pool	--
Hosts	4
Virtual machines	0

7. On the **Distributed Port Group - Edit Settings** page, navigate to **Teaming and failover** in the left-hand menu and click **uplink2** to move it down to **Unused uplinks**.

Show example



Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-a

Load balancing: Route based on originating virtual por

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

Failover order

Active uplinks

uplink1

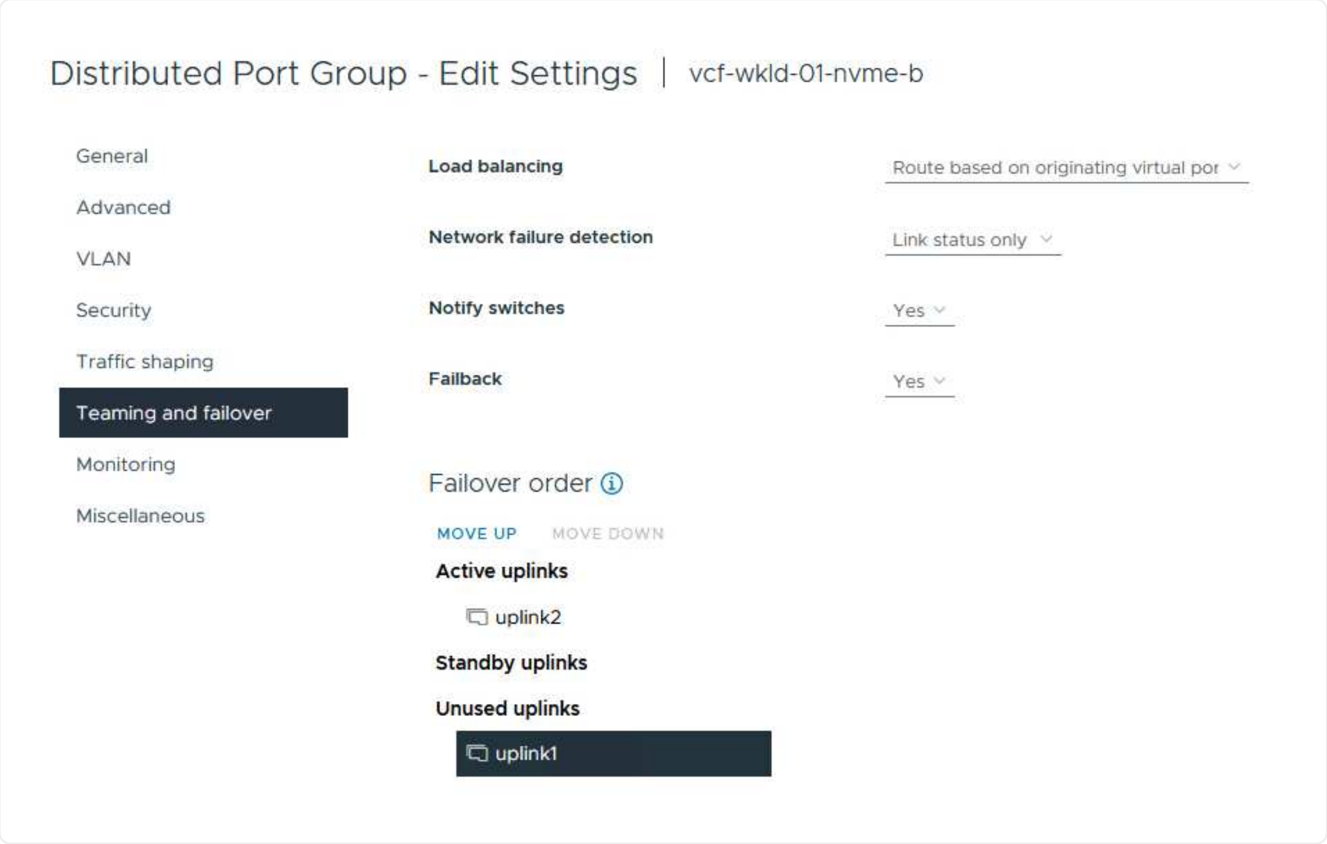
Standby uplinks

Unused uplinks

uplink2

8. Repeat this step for the second NVMe/TCP port group. This time, move **uplink1** down to **Unused uplinks**.

Show example



Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-b

Load balancing	Route based on originating virtual por
Network failure detection	Link status only
Notify switches	Yes
Failback	Yes

Failover order

Active uplinks

uplink2

Standby uplinks

Unused uplinks

uplink1

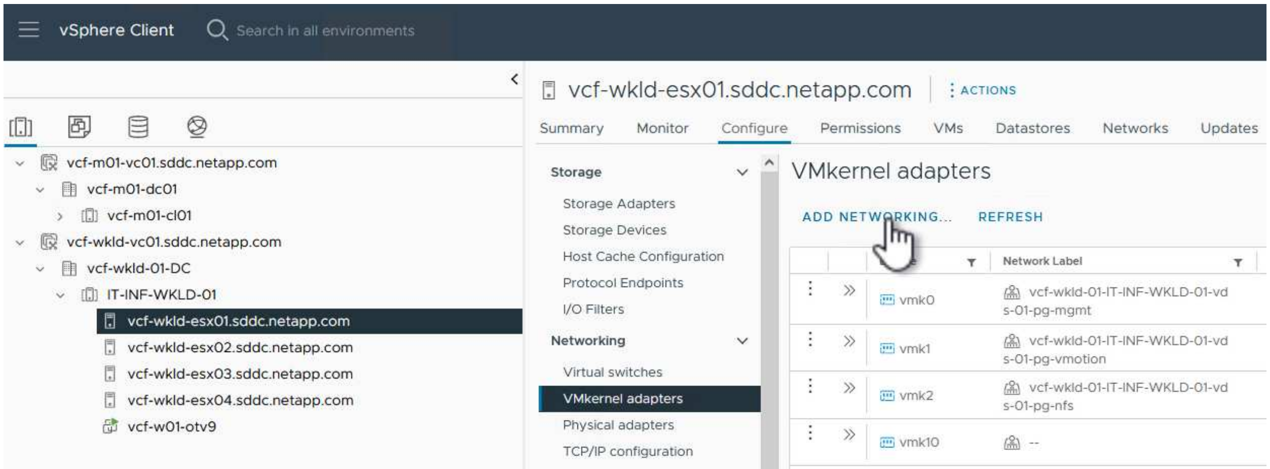
Step 2: Create the VMkernel adapters on each ESXi host

Create the VMkernel adapters on each ESXi host in the workload domain.

Steps

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 **Add Networking…** to start.

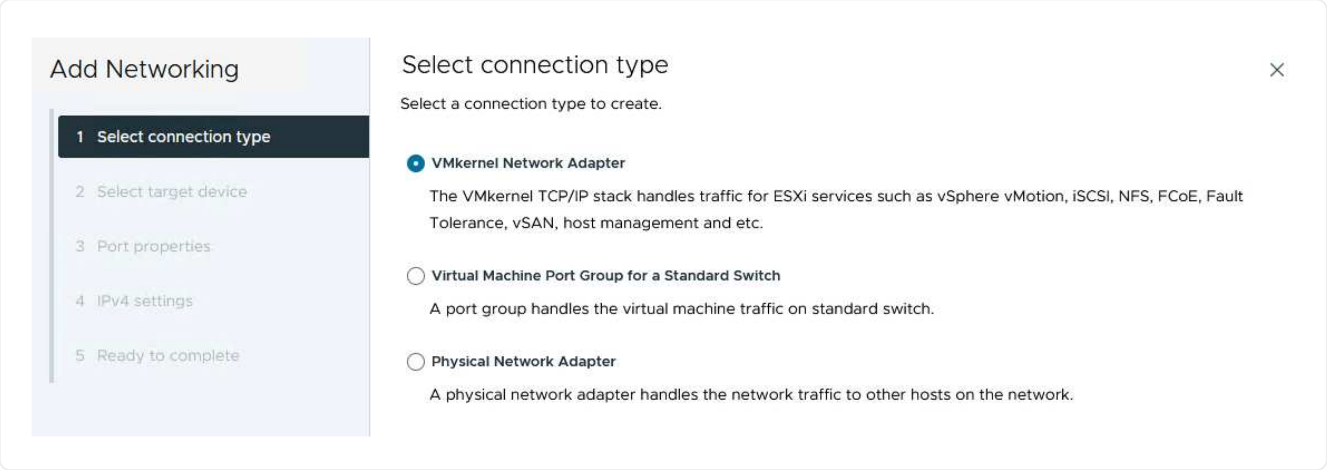
   Show example



	Network Label
vmk0	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt
vmk1	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion
vmk2	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs
vmk10	--

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

Show example



Add Networking

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

Select connection type

Select a connection type to create.

● **VMkernel Network Adapter**

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

○ **Virtual Machine Port Group for a Standard Switch**

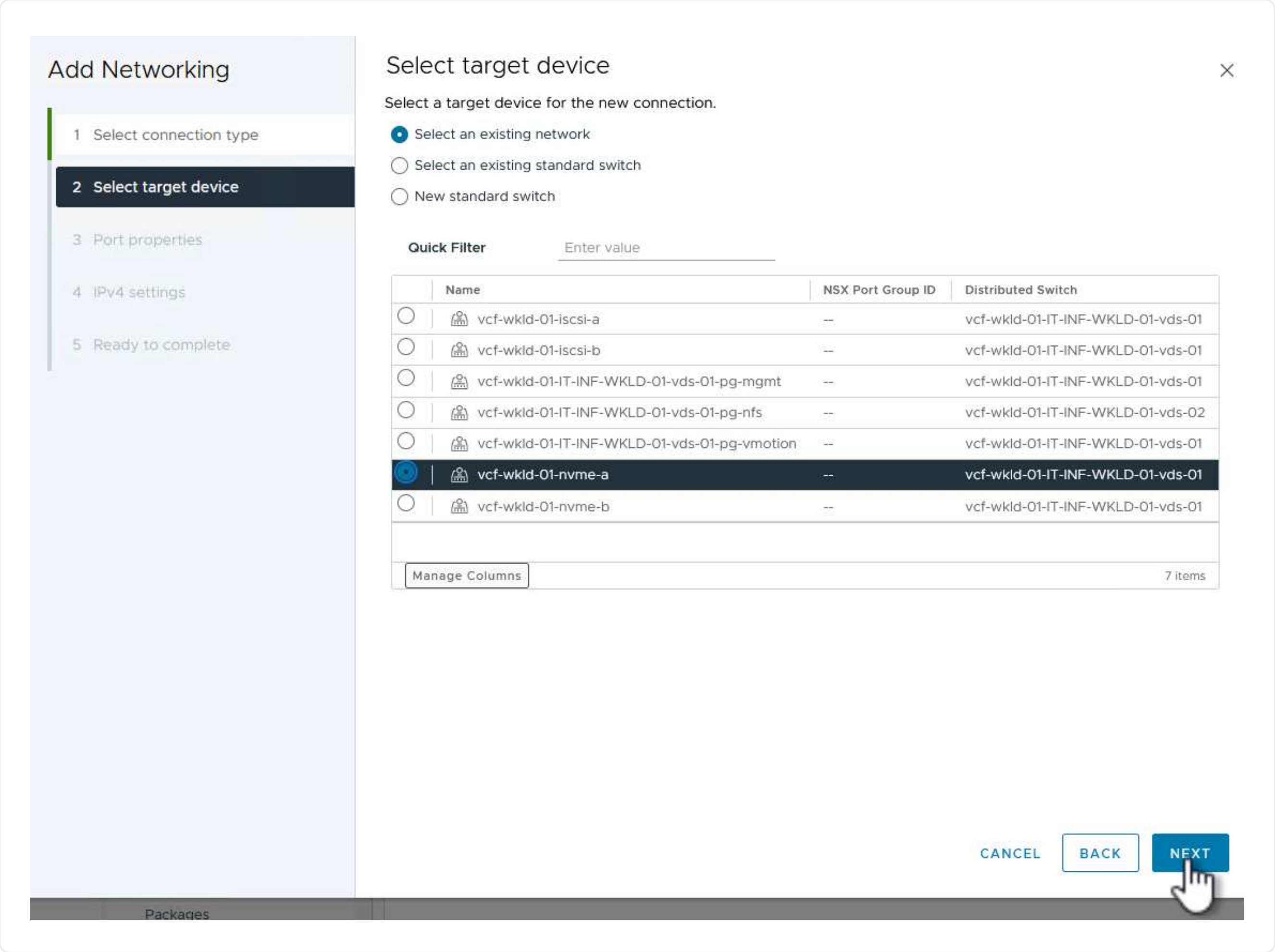
A port group handles the virtual machine traffic on standard switch.

○ **Physical Network Adapter**

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

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

Show example



Add Networking

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

Select target device

Select a target device for the new connection.

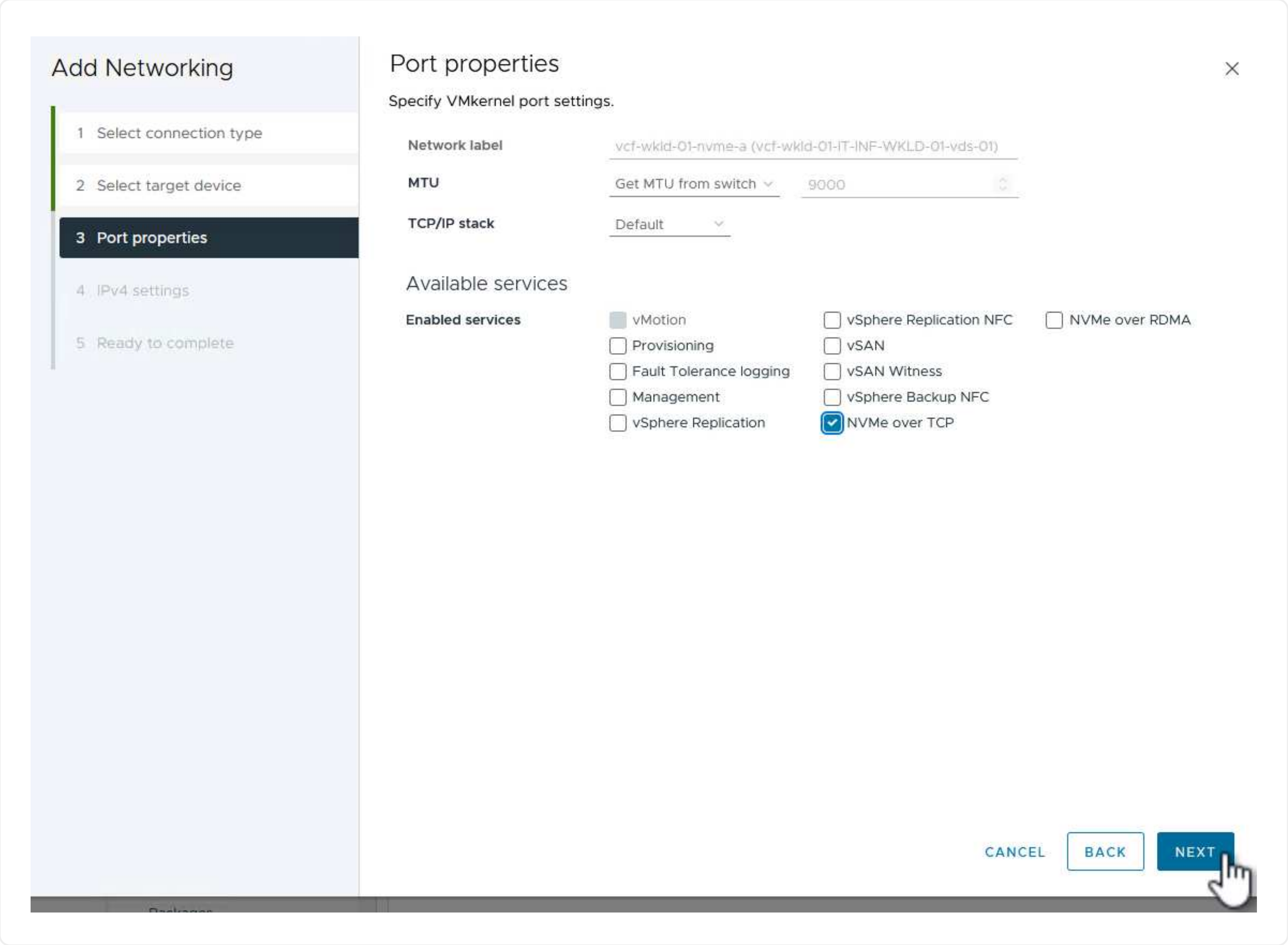
● Select an existing network
○ Select an existing standard switch
○ New standard switch

Quick Filter: Enter value

	Name	NSX Port Group ID	Distributed Switch
○	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
○	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
●	vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
○	vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

4. On the **Port properties** page, click the box for **NVMe/TCP** and click **Next** to continue.

Show example



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label vcf-wkld-01-nvme-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)

MTU Get MTU from switch 9000

TCP/IP stack Default

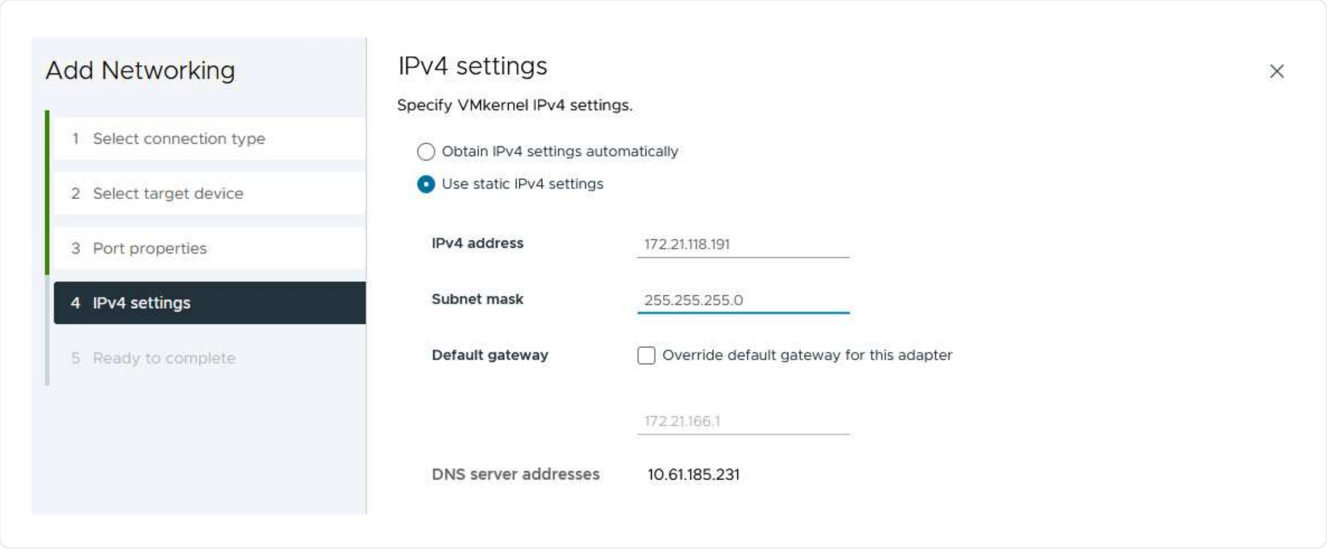
Available services

Enabled services

□ vMotion	□ vSphere Replication NFC	□ NVMe over RDMA
□ Provisioning	□ vSAN	
□ Fault Tolerance logging	□ vSAN Witness	
□ Management	□ vSphere Backup NFC	
□ vSphere Replication	☑ NVMe over TCP	

5. On the **IPv4 settings** page, fill in the **IP address** and **Subnet mask** and provide a new gateway IP address (only if required). Click **Next** to continue.

Show example



Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

○ Obtain IPv4 settings automatically

● Use static IPv4 settings

IPv4 address 172.21.118.191

Subnet mask 255.255.255.0

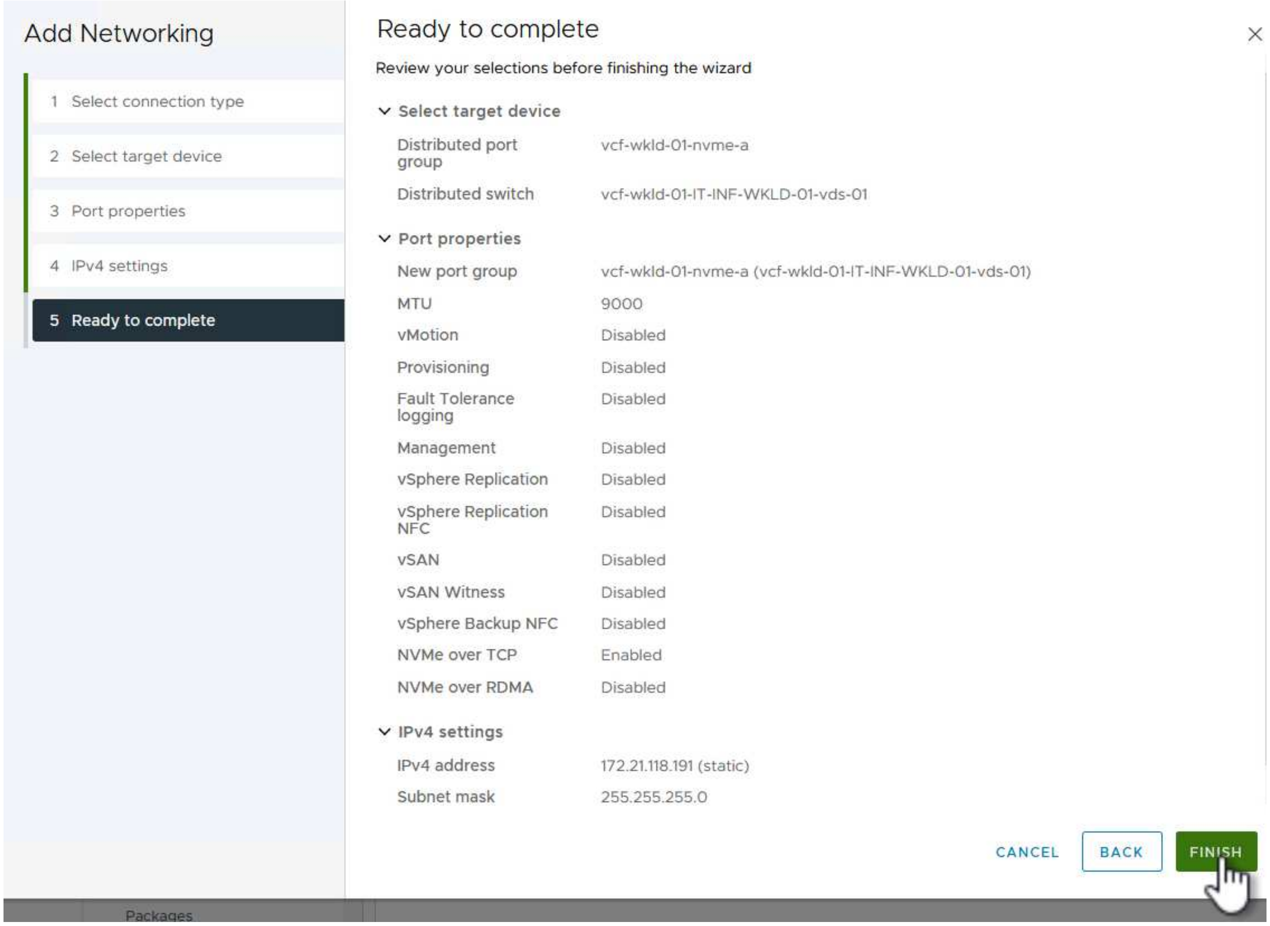
Default gateway □ Override default gateway for this adapter

172.21.166.1

DNS server addresses 10.61.185.231

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

Show example



Ready to complete

Review your selections before finishing the wizard

Select target device

Distributed port group	vcf-wkld-01-nvme-a
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Port properties

New port group	vcf-wkld-01-nvme-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Enabled
NVMe over RDMA	Disabled

IPv4 settings

IPv4 address	172.21.118.191 (static)
Subnet mask	255.255.255.0

7. Repeat this process to create a VMkernel adapter for the second iSCSI network.

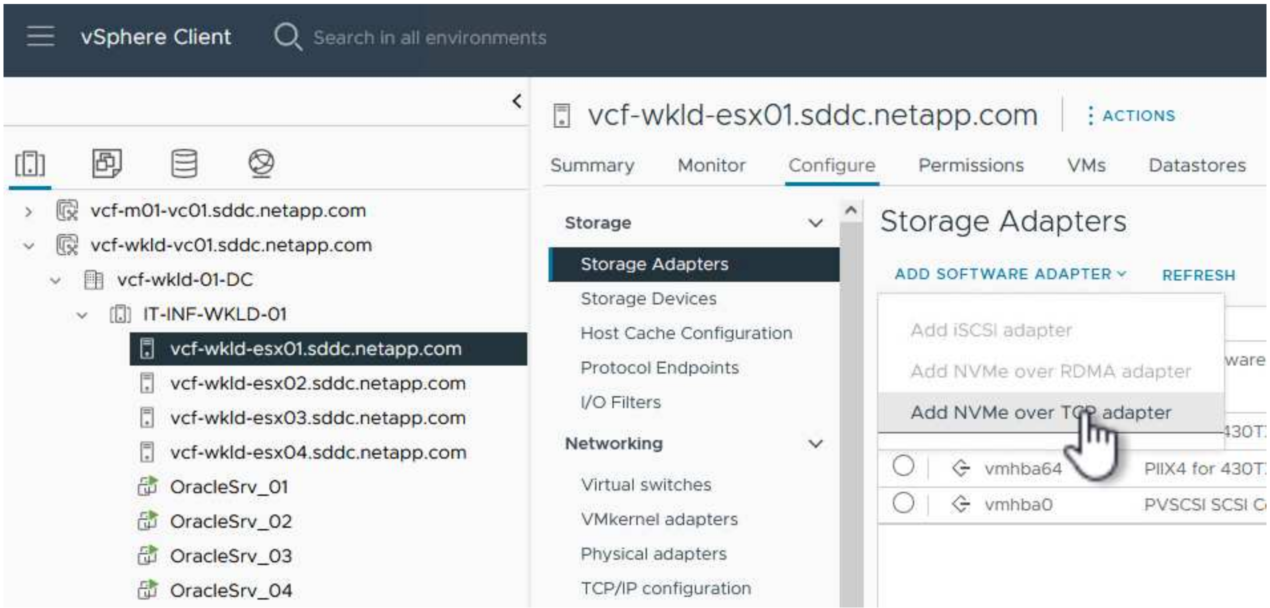
Step 3: Add NVMe/TCP adapter

Each ESXi host in the workload domain cluster must have an NVMe/TCP software adapter installed for every established NVMe/TCP network dedicated to storage traffic.

To install NVMe/TCP adapters and discover the NVMe controllers, complete the following steps.

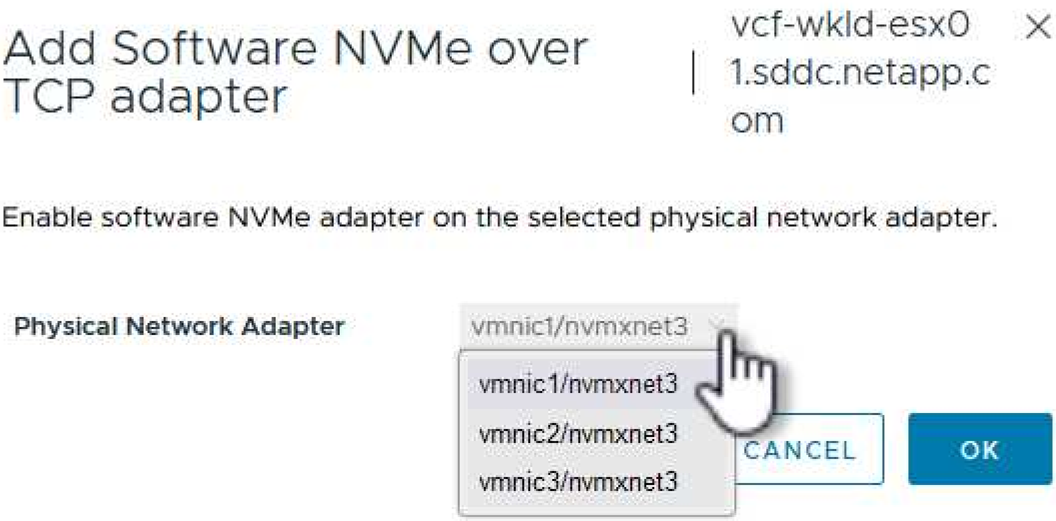
1. In the vSphere client, navigate to one of the ESXi hosts in the workload domain cluster. From the **Configure** tab, click **Storage Adapters** in the menu.
2. From the **Add Software Adapter** drop-down menu, select **Add NVMe over TCP adapter**.

Show example



3. In the **Add Software NVMe over TCP adapter** window, access the **Physical Network Adapter** drop-down menu and select the correct physical network adapter on which to enable the NVMe adapter.

Show example

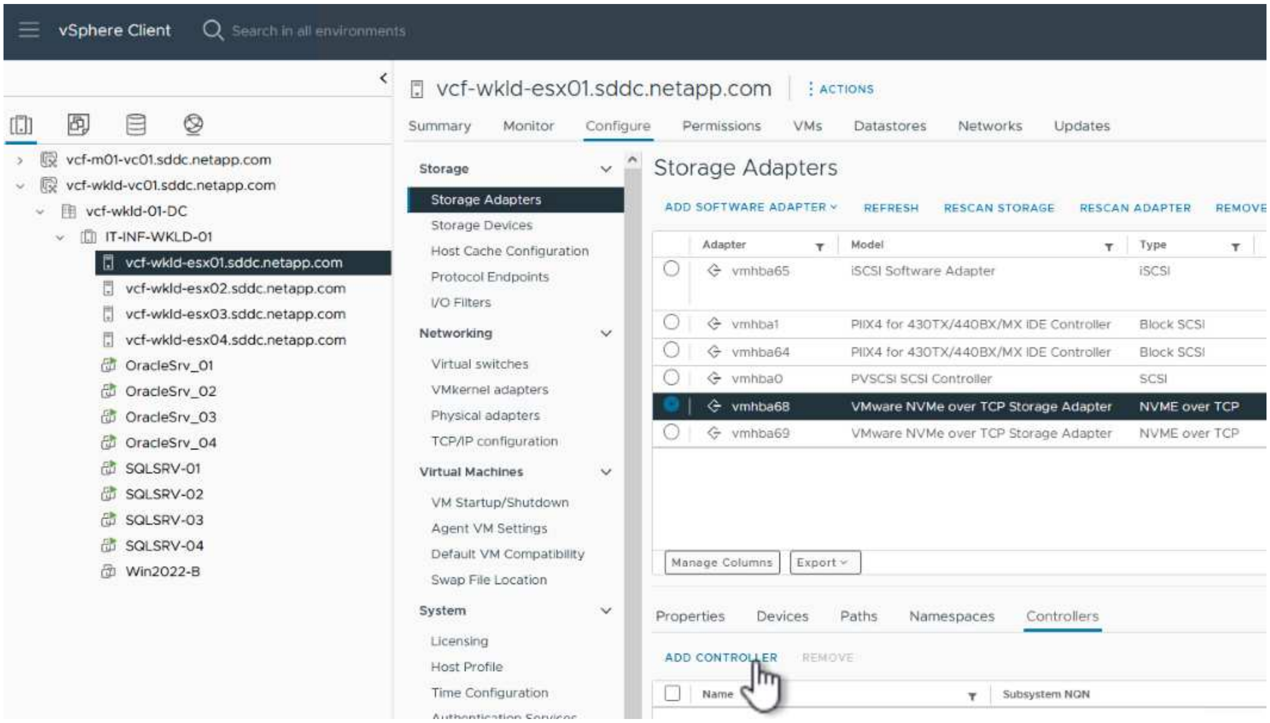

Add Software NVMe over TCP adapter | vcf-wkld-esx01.sddc.netapp.com

Enable software NVMe adapter on the selected physical network adapter.

Physical Network Adapter: vmnic1/nvmxnet3

4. Repeat this process for the second network assigned to NVMe/TCP traffic, assigning the correct physical adapter.
5. Select one of the newly installed NVMe/TCP adapters. On the **Controllers** tab, select **Add Controller**.

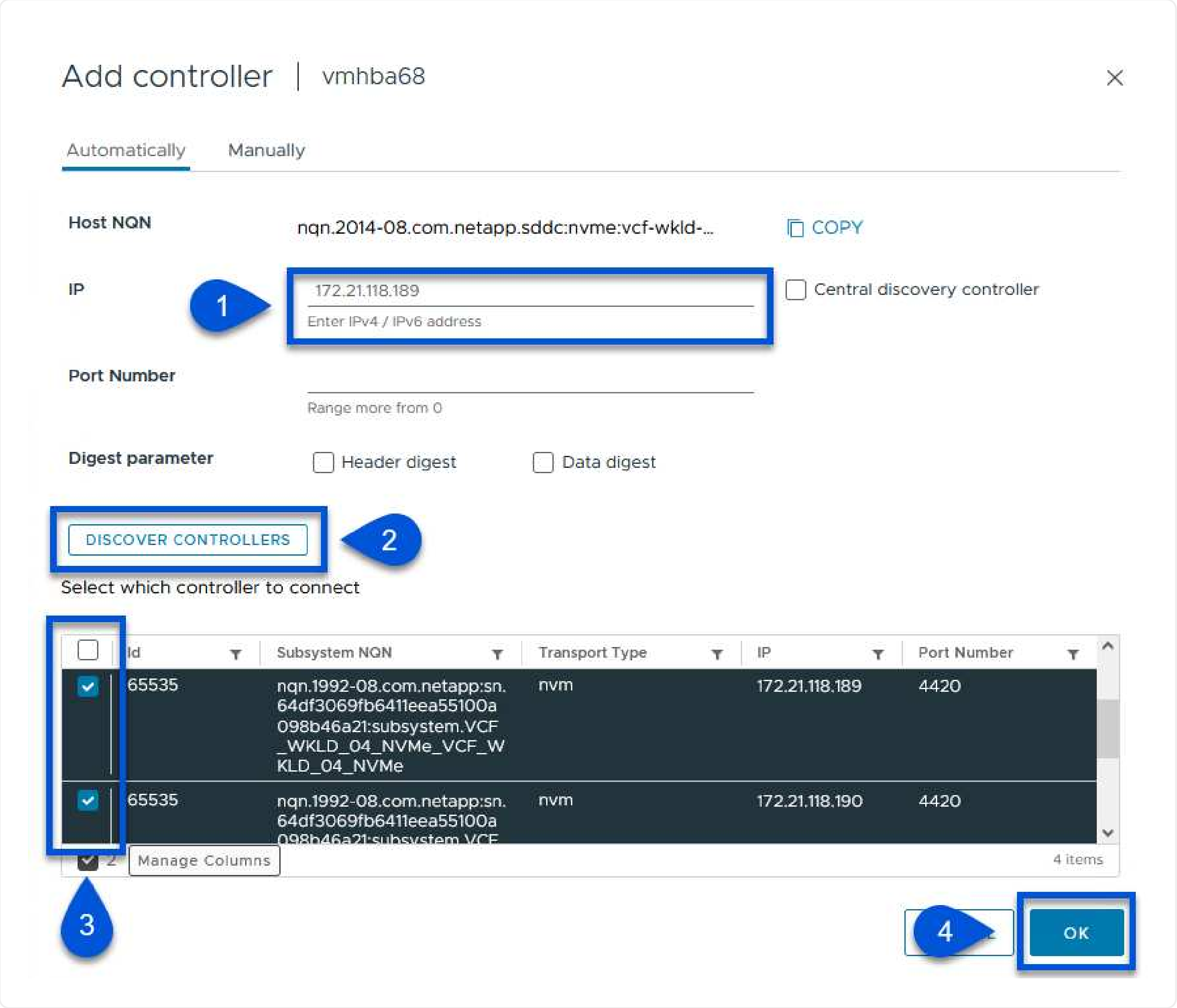
Show example



	Adapter	Model	Type
○	vmhba65	iSCSI Software Adapter	iSCSI
○	vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI
○	vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI
○	vmhba0	PVSCSI SCSI Controller	SCSI
●	vmhba68	VMware NVMe over TCP Storage Adapter	NVME over TCP
○	vmhba69	VMware NVMe over TCP Storage Adapter	NVME over TCP

6. In the **Add controller** window, select the **Automatically** tab and complete the following steps.
   a. Enter an IP address for one of the SVM logical interfaces on the same network as the physical adapter assigned to this NVMe/TCP adapter.
   b. Click the **Discover Controllers** button.
   c. From the list of discovered controllers, click the checkbox for the two controllers with network addresses aligned with this NVMe/TCP adapter.
7. Click **OK** to add the selected controllers.

Show example



Add controller | vmhba68

Automatically | Manually

Host NQN: nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-...

IP: 172.21.118.189 (Enter IPv4 / IPv6 address)

□ Central discovery controller

Port Number: (Range more from 0)

Digest parameter: □ Header digest □ Data digest

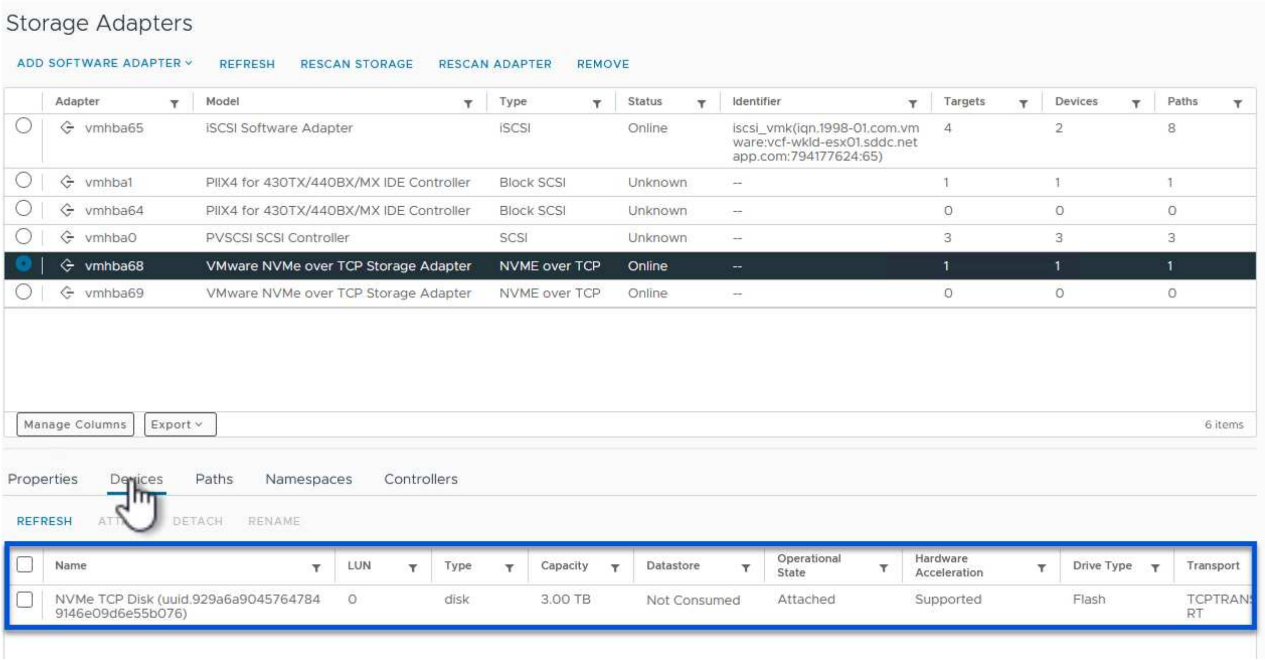
Select which controller to connect

	Id	Subsystem NQN	Transport Type	IP	Port Number
☑	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF_WKLD_04_NVMe_VCF_WKLD_04_NVMe	nvm	172.21.118.189	4420
☑	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF	nvm	172.21.118.190	4420

2 | 4 items

8. After a few seconds you should see the NVMe namespace appear on the Devices tab.

Show example



	Adapter	Model	Type	Status	Identifier	Targets	Devices	Paths
○	vmhba65	iSCSI Software Adapter	iSCSI	Online	iscsi_vmk(iqn.1998-01.com.vmware:vcf-wkld-esx01.sddc.netapp.com:794177624:65)	4	2	8
○	vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	1	1	1
○	vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	0	0	0
○	vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	3	3	3
●	vmhba68	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	1	1	1
○	vmhba69	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	0	0	0

□	Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type	Transport
□	NVMe TCP Disk (uuid.929a6a90457647849146e09d6e55b076)	0	disk	3.00 TB	Not Consumed	Attached	Supported	Flash	TCPTRANSRT

9. Repeat this procedure to create an NVMe/TCP adapter for the second network established for NVMe/TCP traffic.

What’s next?

After configuring networking, configure storage for NVMe vVols.

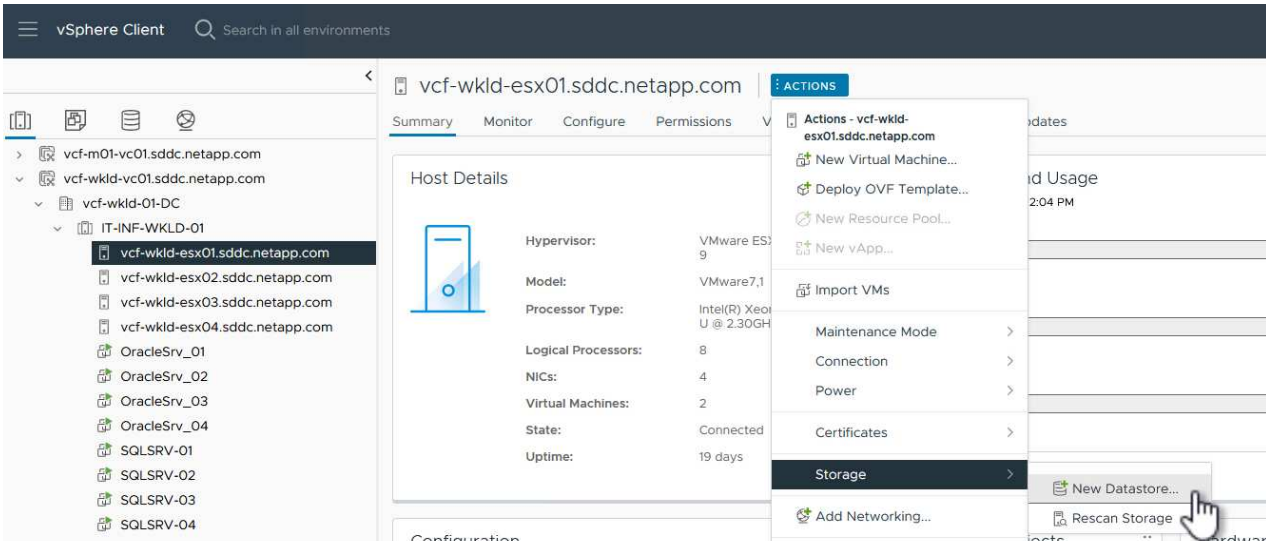
Configure NVMe/TCP vVols storage in a VCF VI workload domain

Configure NVMe/TCP vVols storage in a VMware Cloud Foundation VI workload domain. You’ll deploy ONTAP tools, register a storage system, create a storage capability profile, and provision a vVols datastore in the vSphere client.

Steps

1. In the vSphere client, navigate to one of the ESXi hosts in the workload domain cluster. From the **Actions** menu select **Storage > New Datastore…**.

Show example



Hypervisor: VMware ESX 9

Model: VMware7,1

Processor Type: Intel(R) Xeon U @ 2.30GH

Logical Processors: 8

NICs: 4

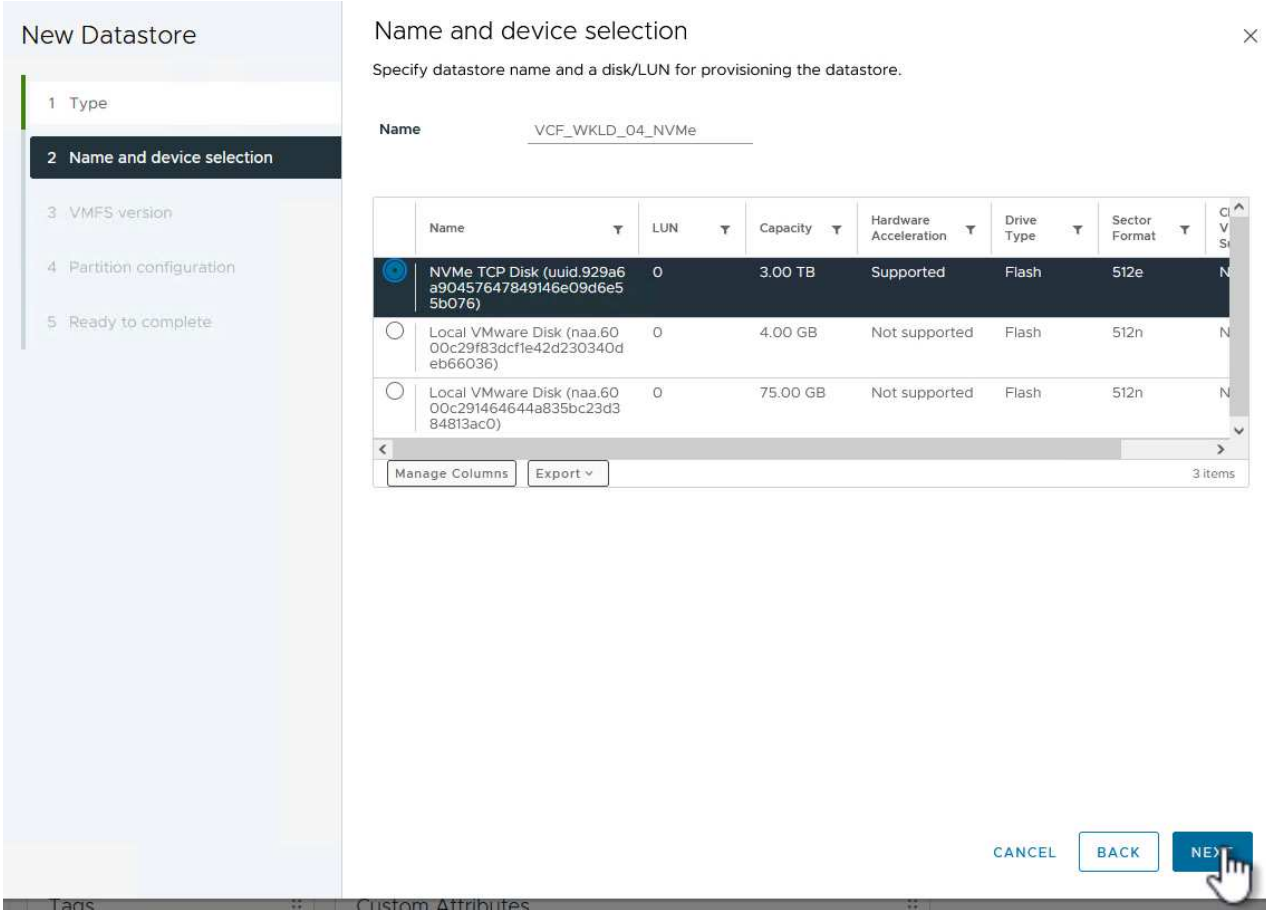
Virtual Machines: 2

State: Connected

Uptime: 19 days

2. In the **New Datastore** wizard, select **VMFS** as the type. Click **Next** to continue.
3. On the **Name and device selection** page, provide a name for the datastore and select the NVMe namespace from the list of available devices.

Show example



Name and device selection

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

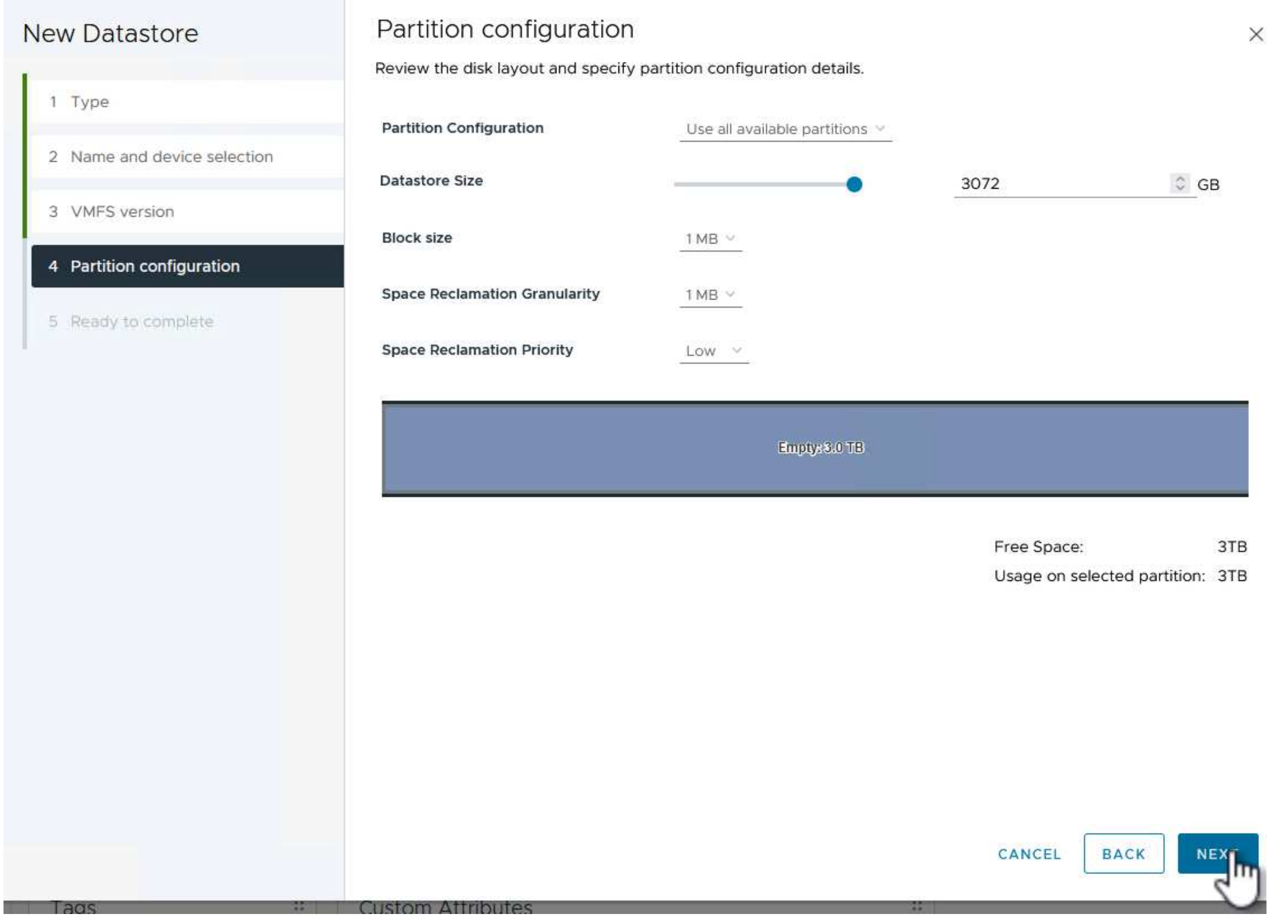
Name VCF_WKLD_04_NVMe

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format
●	NVMe TCP Disk (uuid.929a6a90457647849146e09d6e55b076)	0	3.00 TB	Supported	Flash	512e
○	Local VMware Disk (naa.6000c29f83dcf1e42d230340deb66036)	0	4.00 GB	Not supported	Flash	512n
○	Local VMware Disk (naa.6000c291464644a835bc23d384813ac0)	0	75.00 GB	Not supported	Flash	512n

3 items

4. On the **VMFS version** page, select the version of VMFS for the datastore.
5. On the **Partition configuration** page, make any desired changes to the default partition scheme. Click **Next** to continue.

Show example



New Datastore

1 Type
2 Name and device selection
3 VMFS version
4 Partition configuration
5 Ready to complete

Partition configuration

Review the disk layout and specify partition configuration details.

Partition Configuration: Use all available partitions

Datastore Size: 3072 GB

Block size: 1 MB

Space Reclamation Granularity: 1 MB

Space Reclamation Priority: Low

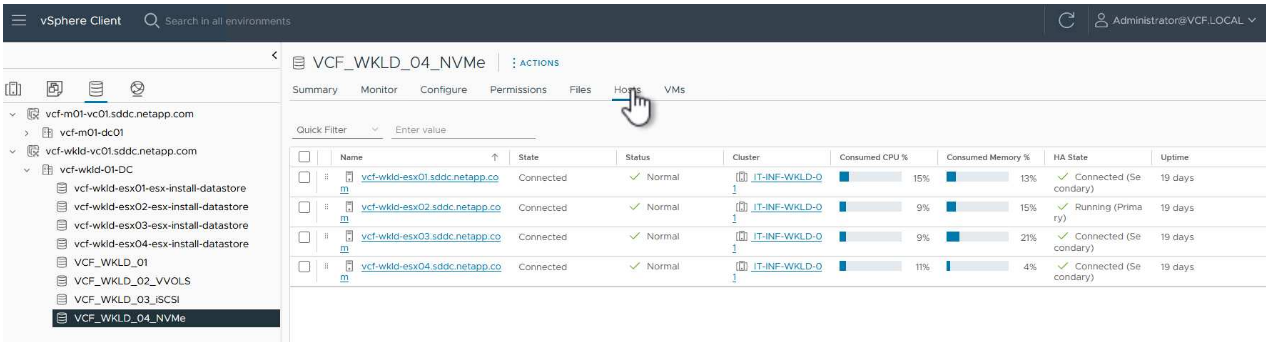
Empty: 3.0 TB

Free Space: 3TB

Usage on selected partition: 3TB

6. On the **Ready to complete** page, review the summary and click **Finish** to create the datastore.
7. Navigate to the new datastore in inventory and click the **Hosts** tab. If configured correctly, all ESXi hosts in the cluster should be listed and have access to the new datastore.

Show example



vSphere Client
Search in all environments
Administrator@VCF.LOCAL
vcf-m01-vc01.sddc.netapp.com
vcf-m01-dc01
vcf-wkld-vc01.sddc.netapp.com
vcf-wkld-01-DC
vcf-wkld-esx01-esx-install-datastore
vcf-wkld-esx02-esx-install-datastore
vcf-wkld-esx03-esx-install-datastore
vcf-wkld-esx04-esx-install-datastore
VCF_WKLD_01
VCF_WKLD_02_VVOLS
VCF_WKLD_03_iSCSI
VCF_WKLD_04_NVMe
VCF_WKLD_04_NVMe
ACTIONS
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
Quick Filter
Enter value

Name	State	Status	Cluster	Consumed CPU %	Consumed Memory %	HA State	Uptime
vcf-wkld-esx01.sddc.netapp.com	Connected	✓ Normal	IT-INF-WKLD-01	15%	13%	✓ Connected (Secondary)	19 days
vcf-wkld-esx02.sddc.netapp.com	Connected	✓ Normal	IT-INF-WKLD-01	9%	15%	✓ Running (Primary)	19 days
vcf-wkld-esx03.sddc.netapp.com	Connected	✓ Normal	IT-INF-WKLD-01	9%	21%	✓ Connected (Secondary)	19 days
vcf-wkld-esx04.sddc.netapp.com	Connected	✓ Normal	IT-INF-WKLD-01	11%	4%	✓ Connected (Secondary)	19 days

Additional information

- For more information on configuring SAN for redundancy, refer to the NetApp SAN configuration reference.
- For additional information on NVMe design considerations for ONTAP storage systems, refer to NVMe configuration, support and limitations.
- For information on configuring ONTAP storage systems, refer to the ONTAP 9 documentation.
- For information on configuring VCF, refer to the VMware Cloud Foundation documentation.

Add an FC-based VMFS datastore as supplemental storage to a VI workload domains

In this use case we outline the procedure to configure a VMFS datastore using Fiber Channel (FC) as supplemental storage for a VMware Cloud Foundation (VCF) Virtual Infrastructure (VI) workload domain. This procedure summarizes deploying ONTAP Tools for VMware vSphere, registering the VI workload vCenter server, defining the storage backend, and provisioning the FC datastore.

Before you begin

Make sure the following components and configurations are in place.

- An ONTAP AFF or ASA storage system with FC ports connected to FC switches.
- SVM created with FC LIFs.
- vSphere with FC HBAs connected to FC switches.
- Single initiator-target zoning is configured on FC switches.

> - Use SVM FC logical interface in zone configuration rather than physical FC ports on ONTAP systems.
> - Use multipath for FC LUNs.

Steps

1. Register the VI workload vCenter by following the instructions in the ONTAP tools for VMware vSphere documentation:
   Register VI workload vCenter.

   Registering the VI workload vCenter enables the vCenter plugin.

2. Add a storage backend using the vSphere client interface by following the instructions in the ONTAP tools for VMware vSphere documentation: Define Storage backend using vSphere client interface.

   Adding a storage backend enables you to onboard an ONTAP cluster.

3. Provision VMFS on Fibre Channel (FC)by following the instructions in the ONTAP tools for VMware vSphere documentation: Provision VMFS on FC.

Additional information

- For information on configuring ONTAP storage systems, refer to the ONTAP 9 documentation.
- For information on configuring VCF, refer to the VMware Cloud Foundation documentation.

- For information on configuring Fibre Channel on ONTAP storage systems, refer to the SAN storage management in the ONTAP 9 documentation.
- For information on using VMFS with ONTAP storage systems, refer to the Deployment guide for VMFS.
- For video demos of this solution, refer to VMware datastore provisioning.

Protect VCF with SnapCenter

Learn about protecting VCF workload domains with SnapCenter plug-in for VMware vSphere

Learn about the NetApp solutions you can use to protect VMware Cloud Foundation (VCF) workloads with SnapCenter Plug-in for VMware vSphere. This plug-in simplifies backup and recovery, ensuring application-consistent backups, and optimizing storage with NetApp's efficiency technologies.

It supports automated workflows, and scalable operations while providing seamless integration with the vSphere client. With SnapMirror replication providing secondary backup on-premises or to the cloud, it offers robust data protection and operational efficiency in virtualized environments.

Please refer to the following solutions for more details.

- Protect VCF Workload Domain
- Protect VCF Multiple Workload Domains
- Protect VCF Workload Domain with NVMe

Protect a VCF workload domain with SnapCenter plug-in for VMware vSphere

In this use case we outline the procedure to use the SnapCenter plug-in for VMware vSphere to back up and restore VMs and datastores in a VMware Cloud Foundation (VCF) workload domain. This procedure summarizes deploying SnapCenter plug-in for VMware vSphere, adding storage systems, creating backup policies, and performing restores of VMs and files.

iSCSI is used as the storage protocol for the VMFS datastore in this solution.

Scenario Overview

This scenario covers the following high level steps:

- Deploy the SnapCenter Plug-in for VMware vSphere (SCV) on the VI workload domain.
- Add storage systems to SCV.
- Create backup policies in SCV.
- Create Resource Groups in SCV.
- Use SCV to backup datastores or specific VMs.
- Use SCV to restores VMs to an alternate location in the cluster.
- Use SCV to restores files to a windows file system.

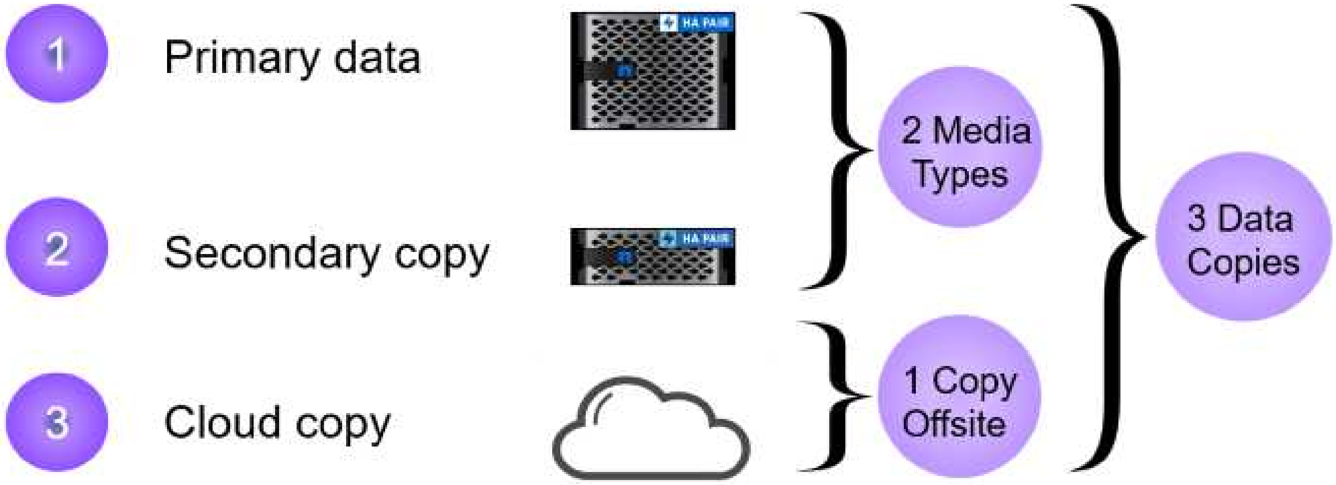
Prerequisites

This scenario requires the following components and configurations:

- An ONTAP ASA storage system with iSCSI VMFS datastores allocated to the workload domain cluster.
- A secondary ONTAP storage system configured to received secondary backups using SnapMirror.
- VCF management domain deployment is complete and the vSphere client is accessible.
- A VI workload domain has been previously deployed.
- Virtual machines are present on the cluster SCV is designated to protect.

For information on configuring iSCSI VMFS datastores as supplemental storage refer to **iSCSI as supplemental storage for Management Domains using ONTAP Tools for VMware** in this documentation. The process for using OTV to deploy datastores is identical for management and workload domains.

> In addition to replicating backups taken with SCV to secondary storage, offsite copies of data can be made to object storage on one of the three (3) leading cloud providers using NetApp Backup and Recovery for VMs. For more information refer to this offering NetApp Backup and Recovery Documentation.



Deployment Steps

To deploy the SnapCenter Plug-in and use it to create backups, and restore VMs and datastores, complete the following steps:

Deploy and use SCV to protect data in a VI workload domain

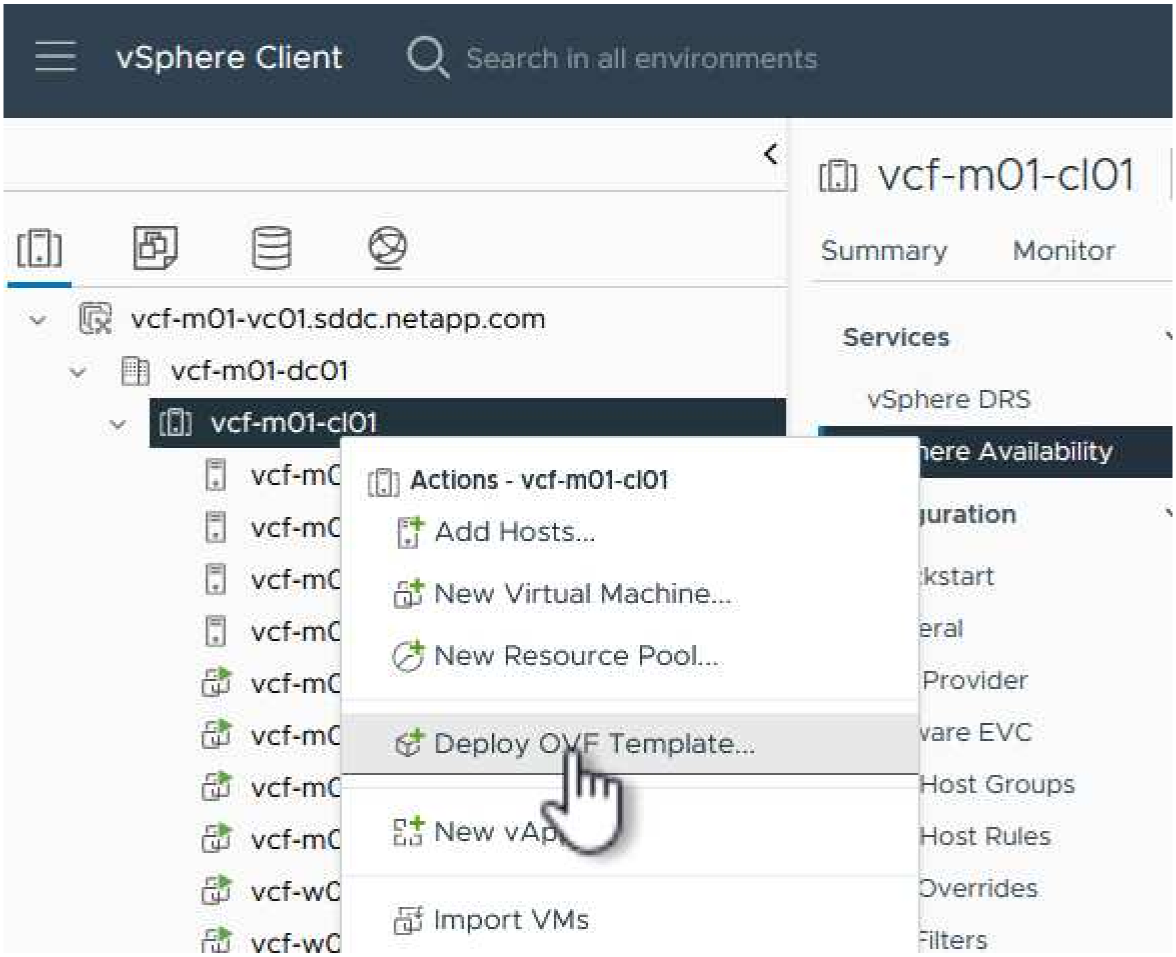
Complete the following steps to deploy, configure, and use SCV to protect data in a VI workload domain:

Deploy the SnapCenter Plug-in for VMware vSphere

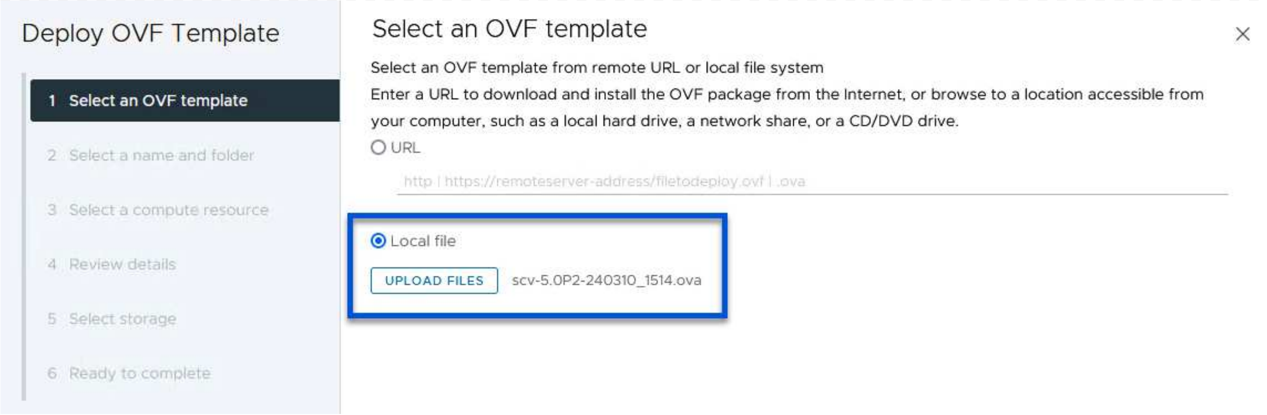
The SnapCenter Plug-in is hosted on the VCF management domain but registered to the vCenter for the VI workload domain. One SCV instance is required for each vCenter instance and, keep in mind that, a Workload domain can include multiple clusters managed by a single vCenter instance.

Complete the following steps from the vCenter client to deploy SCV to the VI workload domain:

1. Download the OVA file for the SCV deployment from the download area of the NetApp support site **HERE**.
2. From the management domain vCenter Client, select to **Deploy OVF Template…**.



3. In the **Deploy OVF Template** wizard, click on the **Local file** radio button and then select to upload the previously downloaded OVF template. Click on **Next** to continue.



Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

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

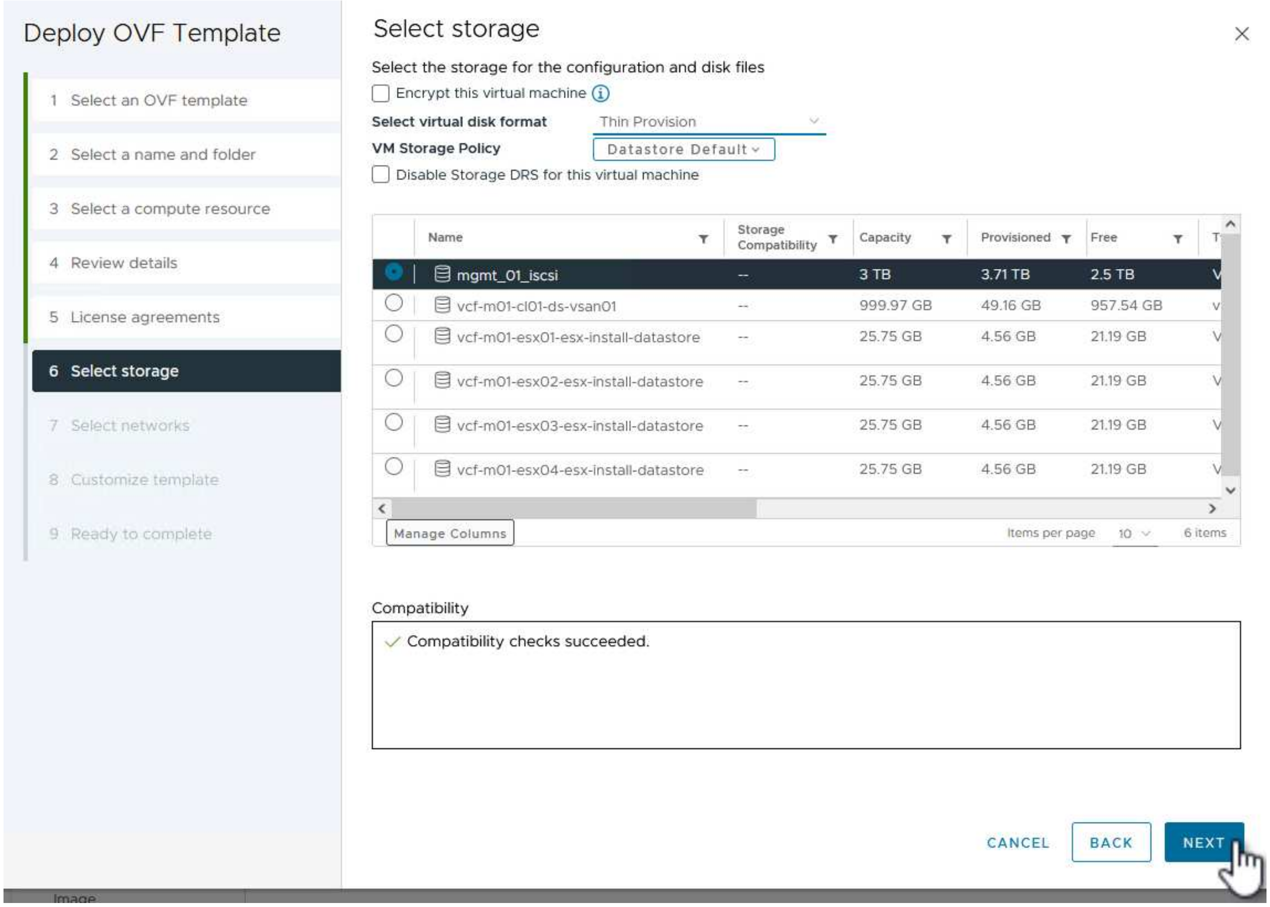
○ URL

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

● Local file

UPLOAD FILES scv-5.0P2-240310_1514.ova

4. On the **Select name and folder** page, provide a name for the SCV data broker VM and a folder on the management domain. Click on **Next** to continue.
5. On the **Select a compute resource** page, select the management domain cluster or specific ESXi host within the cluster to install the VM to.
6. Review information pertaining to the OVF template on the **Review details** page and agree to the licensing terms on the **Licensing agreements** page.
7. On the **Select storage** page choose the datastore which the VM will be installed to and select the **virtual disk format** and **VM Storage Policy**. In this solution, the VM will be installed on an iSCSI VMFS datastore located on an ONTAP storage system, as previously deployed in a separate section of this documentation. Click on **Next** to continue.



Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine

Select virtual disk format: Thin Provision

VM Storage Policy: Datastore Default

□ Disable Storage DRS for this virtual machine

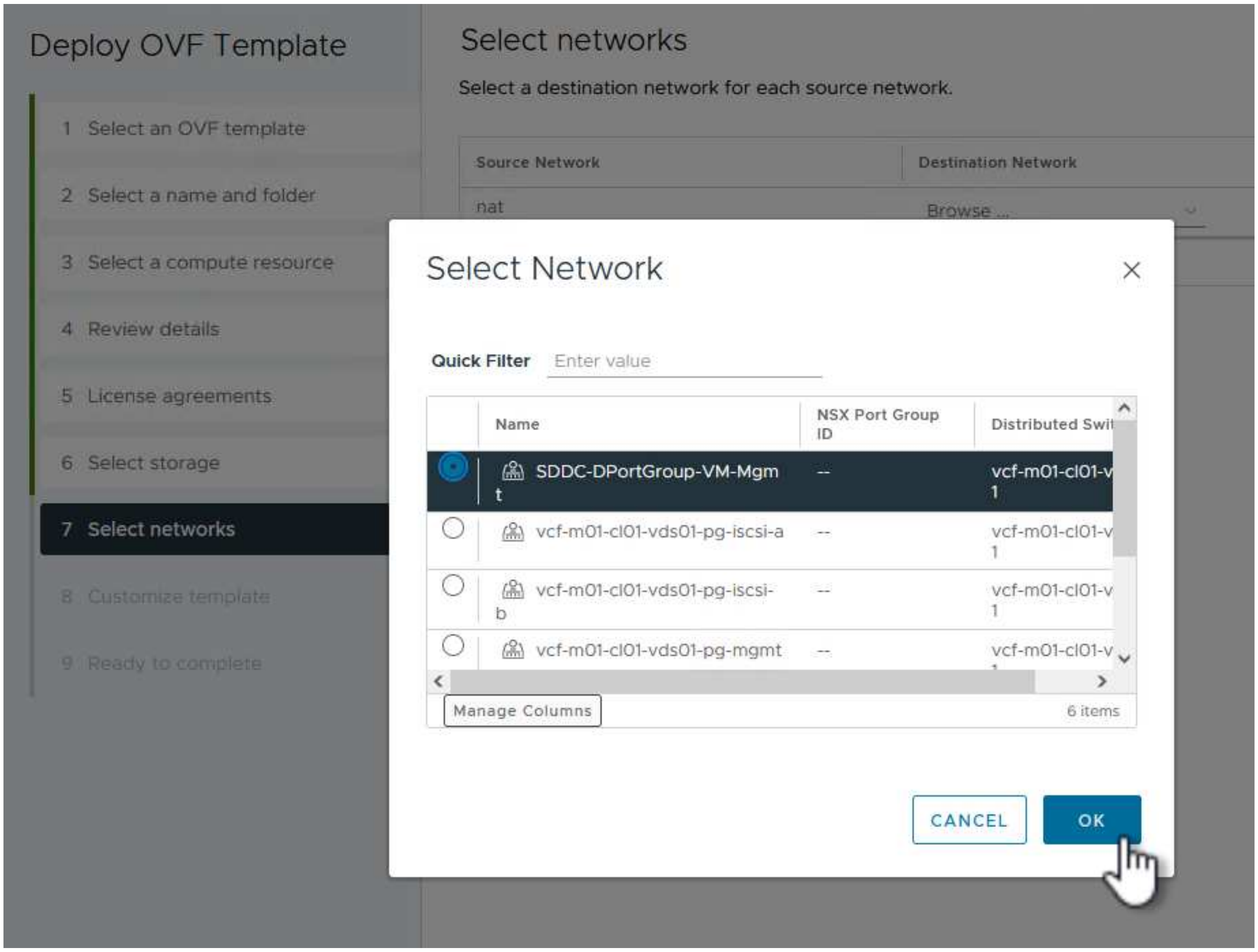
	Name	Storage Compatibility	Capacity	Provisioned	Free
●	mgmt_01_iscsi	--	3 TB	3.71 TB	2.5 TB
○	vcf-m01-cl01-ds-vsan01	--	999.97 GB	49.16 GB	957.54 GB
○	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB
○	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB
○	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB
○	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB

Manage Columns   Items per page 10   6 items

Compatibility

✓ Compatibility checks succeeded.

8. On the **Select network** page, select the management network that is able to communicate with the workload domain vCenter appliance and both the primary and secondary ONTAP storage systems.



Deploy OVF Template

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

Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	Browse ...

Select Network

Quick Filter Enter value

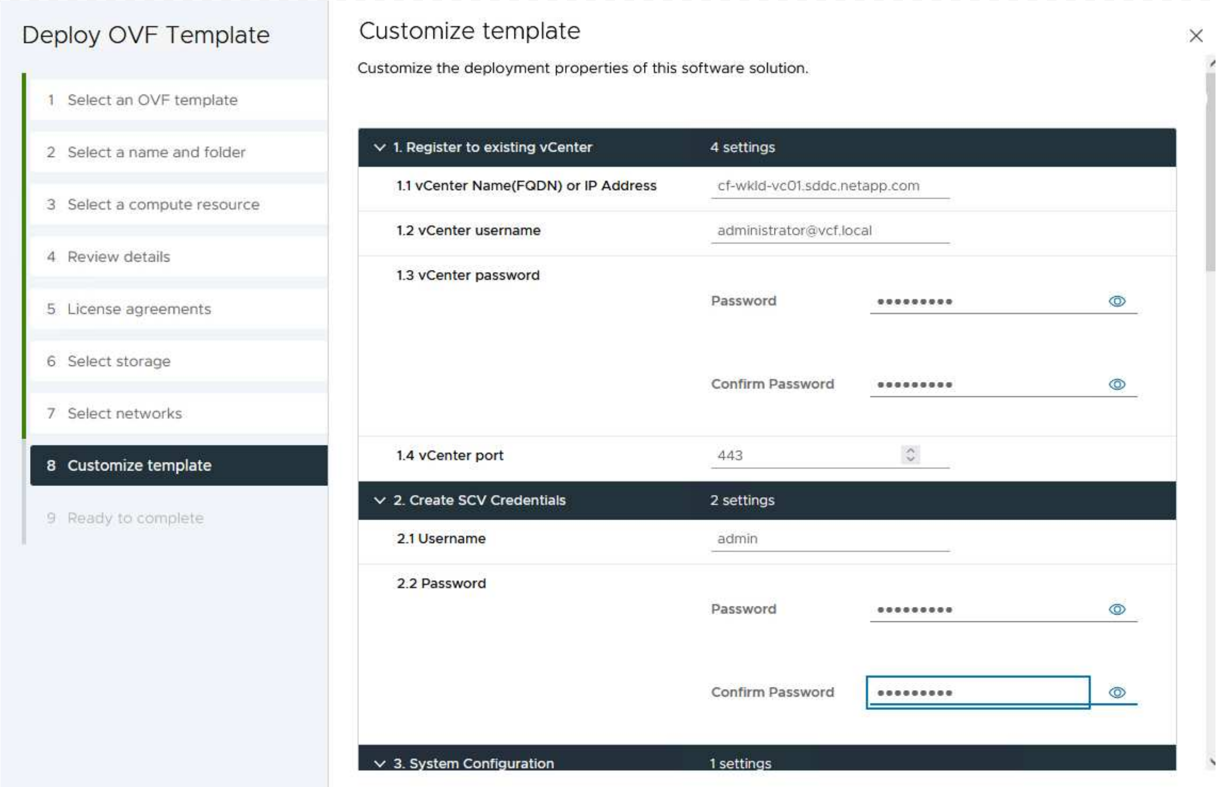
	Name	NSX Port Group ID	Distributed Swi
●	SDDC-DPortGroup-VM-Mgmt	--	vcf-m01-cl01-v 1
○	vcf-m01-cl01-vds01-pg-iscsi-a	--	vcf-m01-cl01-v 1
○	vcf-m01-cl01-vds01-pg-iscsi-b	--	vcf-m01-cl01-v 1
○	vcf-m01-cl01-vds01-pg-mgmt	--	vcf-m01-cl01-v

Manage Columns 6 items

CANCEL OK

9. On the **Customize template** page fill out all information required for the deployment:
   - FQDN or IP, and credentials for the workload domain vCenter appliance.
   - Credentials for the SCV administrative account.
   - Credentials for the SCV maintenance account.
   - IPv4 Network Properties details (IPv6 can also be used).
   - Date and Time settings.

   Click on **Next** to continue.



Customize template

Customize the deployment properties of this software solution.

1. Register to existing vCenter — 4 settings

1.1 vCenter Name(FQDN) or IP Address: cf-wkld-vc01.sddc.netapp.com

1.2 vCenter username: administrator@vcf.local

1.3 vCenter password
Password: •••••••••
Confirm Password: •••••••••

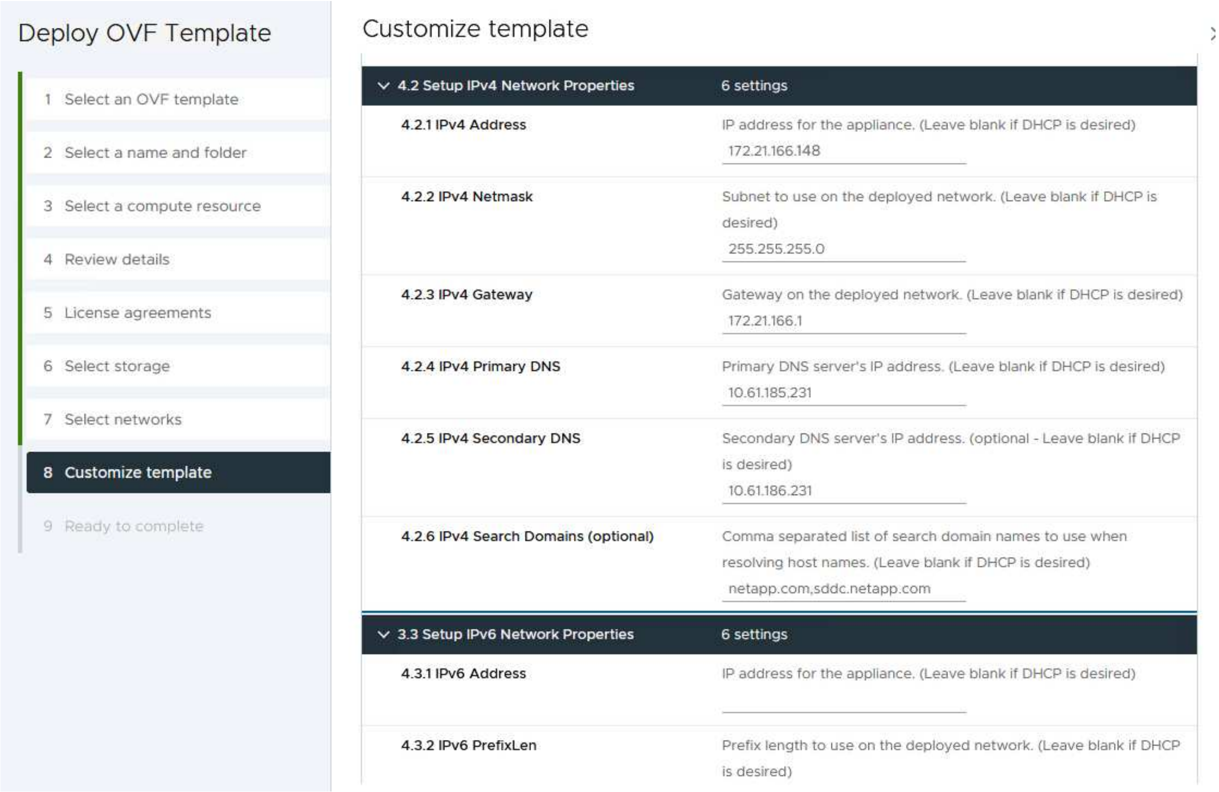
1.4 vCenter port: 443

2. Create SCV Credentials — 2 settings

2.1 Username: admin

2.2 Password
Password: •••••••••
Confirm Password: •••••••••

3. System Configuration — 1 settings



Customize template

4.2 Setup IPv4 Network Properties — 6 settings

4.2.1 IPv4 Address: IP address for the appliance. (Leave blank if DHCP is desired)
172.21.166.148

4.2.2 IPv4 Netmask: Subnet to use on the deployed network. (Leave blank if DHCP is desired)
255.255.255.0

4.2.3 IPv4 Gateway: Gateway on the deployed network. (Leave blank if DHCP is desired)
172.21.166.1

4.2.4 IPv4 Primary DNS: Primary DNS server's IP address. (Leave blank if DHCP is desired)
10.61.185.231

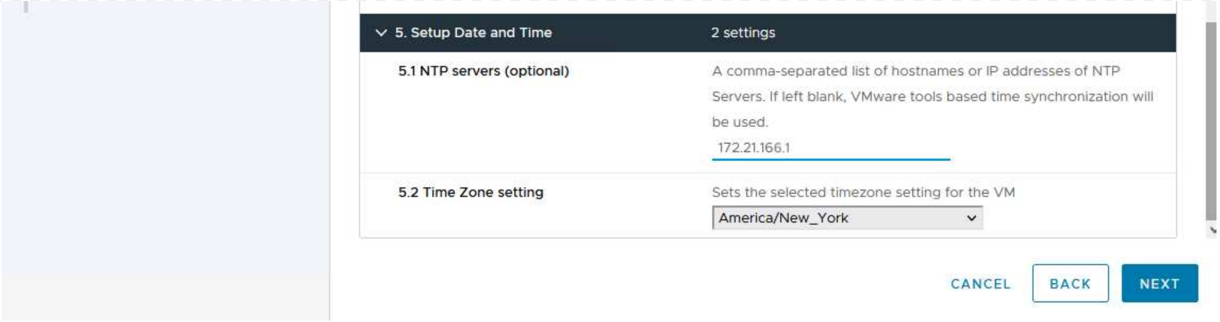
4.2.5 IPv4 Secondary DNS: Secondary DNS server's IP address. (optional - Leave blank if DHCP is desired)
10.61.186.231

4.2.6 IPv4 Search Domains (optional): Comma separated list of search domain names to use when resolving host names. (Leave blank if DHCP is desired)
netapp.com,sddc.netapp.com

3.3 Setup IPv6 Network Properties — 6 settings

4.3.1 IPv6 Address: IP address for the appliance. (Leave blank if DHCP is desired)

4.3.2 IPv6 PrefixLen: Prefix length to use on the deployed network. (Leave blank if DHCP is desired)



5. Setup Date and Time — 2 settings

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

172.21.166.1

5.2 Time Zone setting — Sets the selected timezone setting for the VM

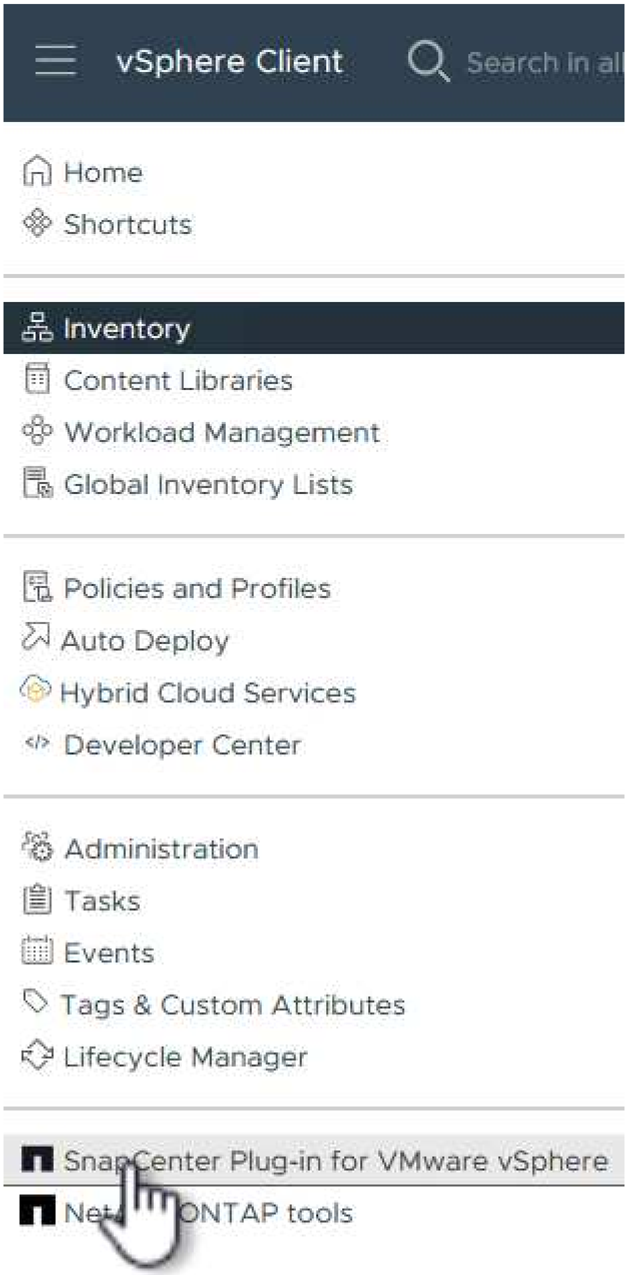
America/New_York

10. Finally, on the **Ready to complete page**, review all settings and click on Finish to start the deployment.

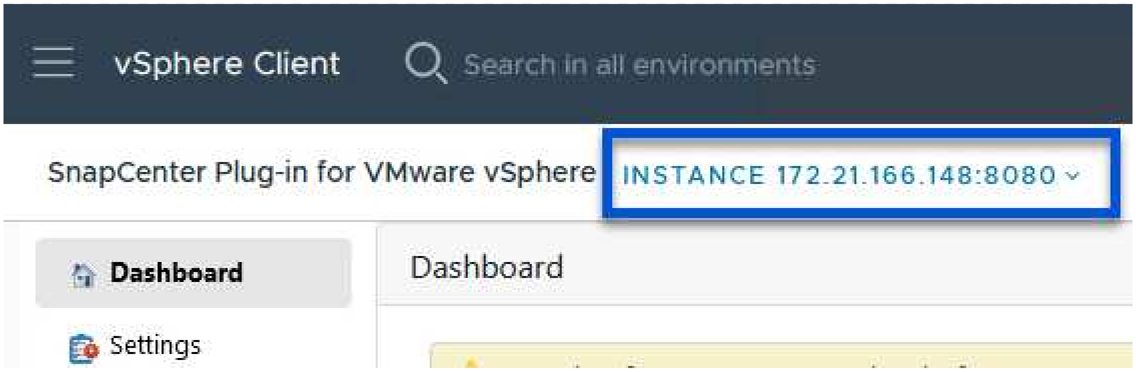
Add Storage Systems to SCV

Once the SnapCenter Plug-in is installed complete the following steps to add storage systems to SCV:

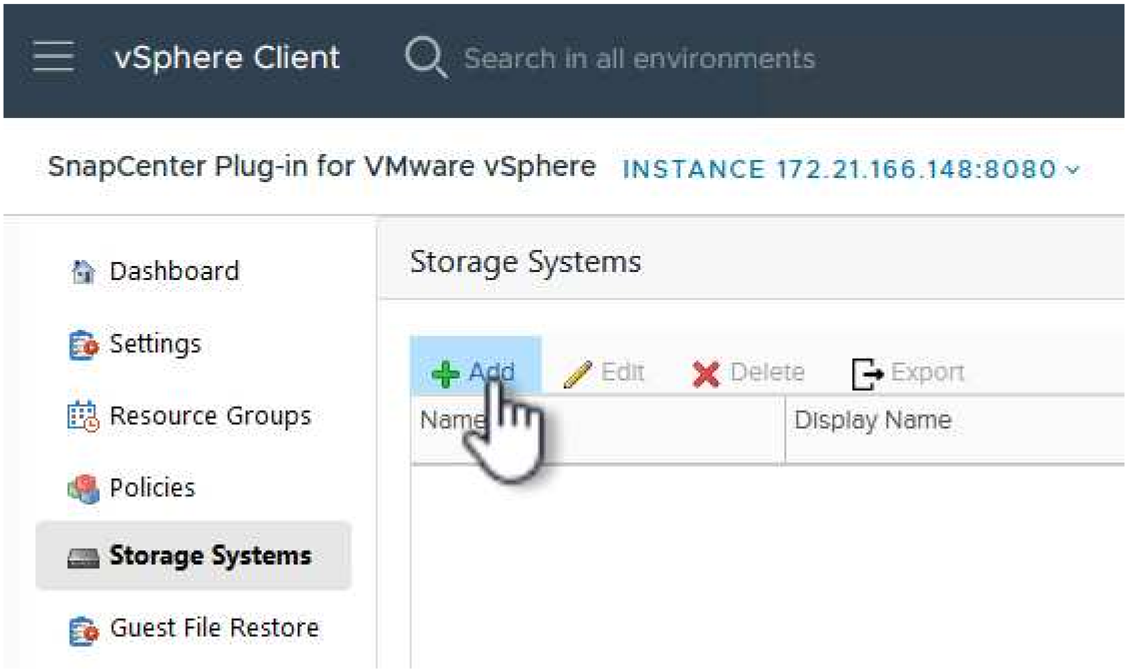
1. SCV can be accessed from the main menu in the vSphere Client.



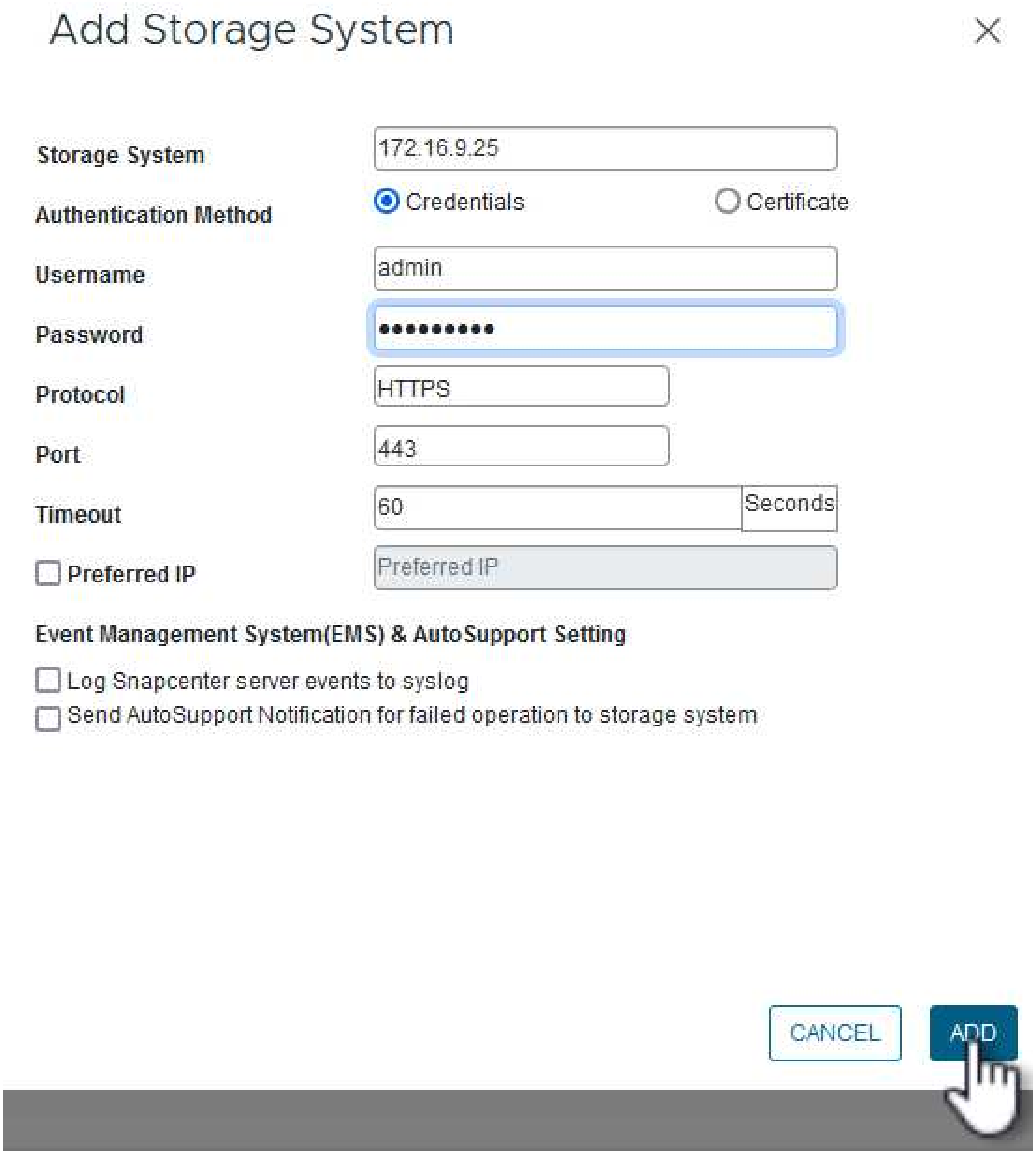
2. At the top of the SCV UI interface, select the correct SCV instance that matches the vSphere cluster to be protected.


vSphere Client
Search in all environments
SnapCenter Plug-in for VMware vSphere
INSTANCE 172.21.166.148:8080
Dashboard
Settings
Dashboard

3. Navigate to **Storage Systems** in the left-hand menu and click on **Add** to get started.



4. On the **Add Storage System** form, fill in the IP address and credentials of the ONTAP storage system to be added, and click on **Add** to complete the action.



Add Storage System

Storage System	172.16.9.25
Authentication Method	● Credentials ○ Certificate
Username	admin
Password	••••••••••
Protocol	HTTPS
Port	443
Timeout	60 Seconds
□ Preferred IP	Preferred IP

Event Management System(EMS) & AutoSupport Setting

□ Log Snapcenter server events to syslog

□ Send AutoSupport Notification for failed operation to storage system

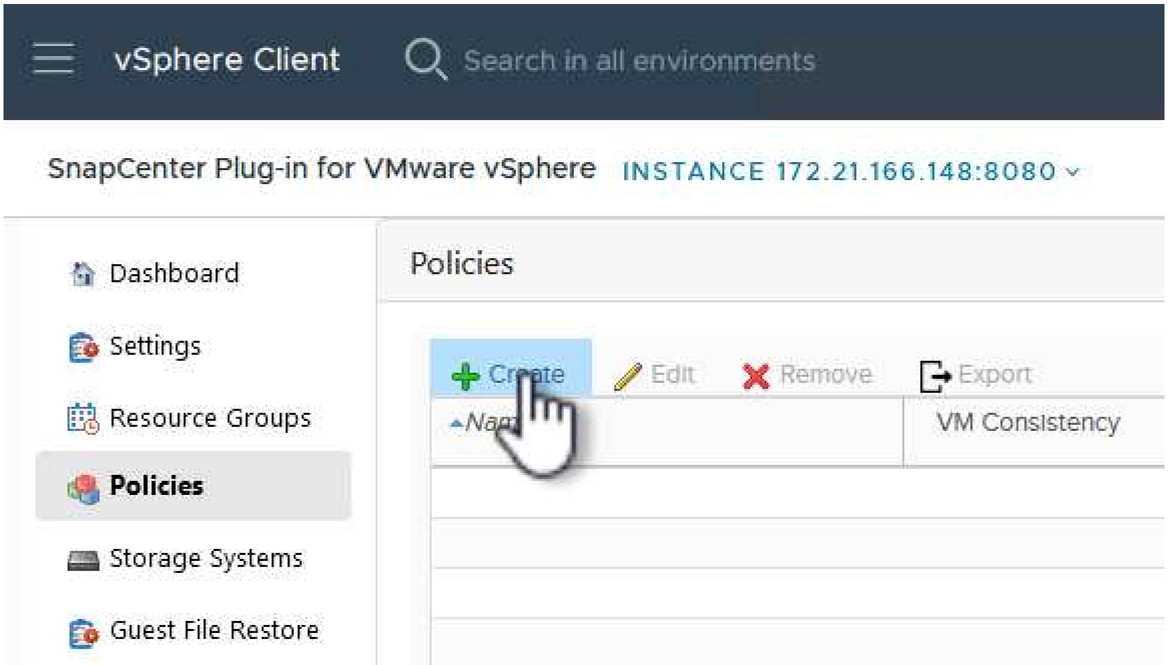
5. Repeat this procedure for any additional storage systems to be managed, including any systems to be used as secondary backup targets.

Configure backup policies in SCV

For more information on creating SCV backup policies refer to Create backup policies for VMs and datastores.

Complete the following steps to create a new backup policy:

1. From the left-hand menu select **Policies** and click on **Create** to begin.



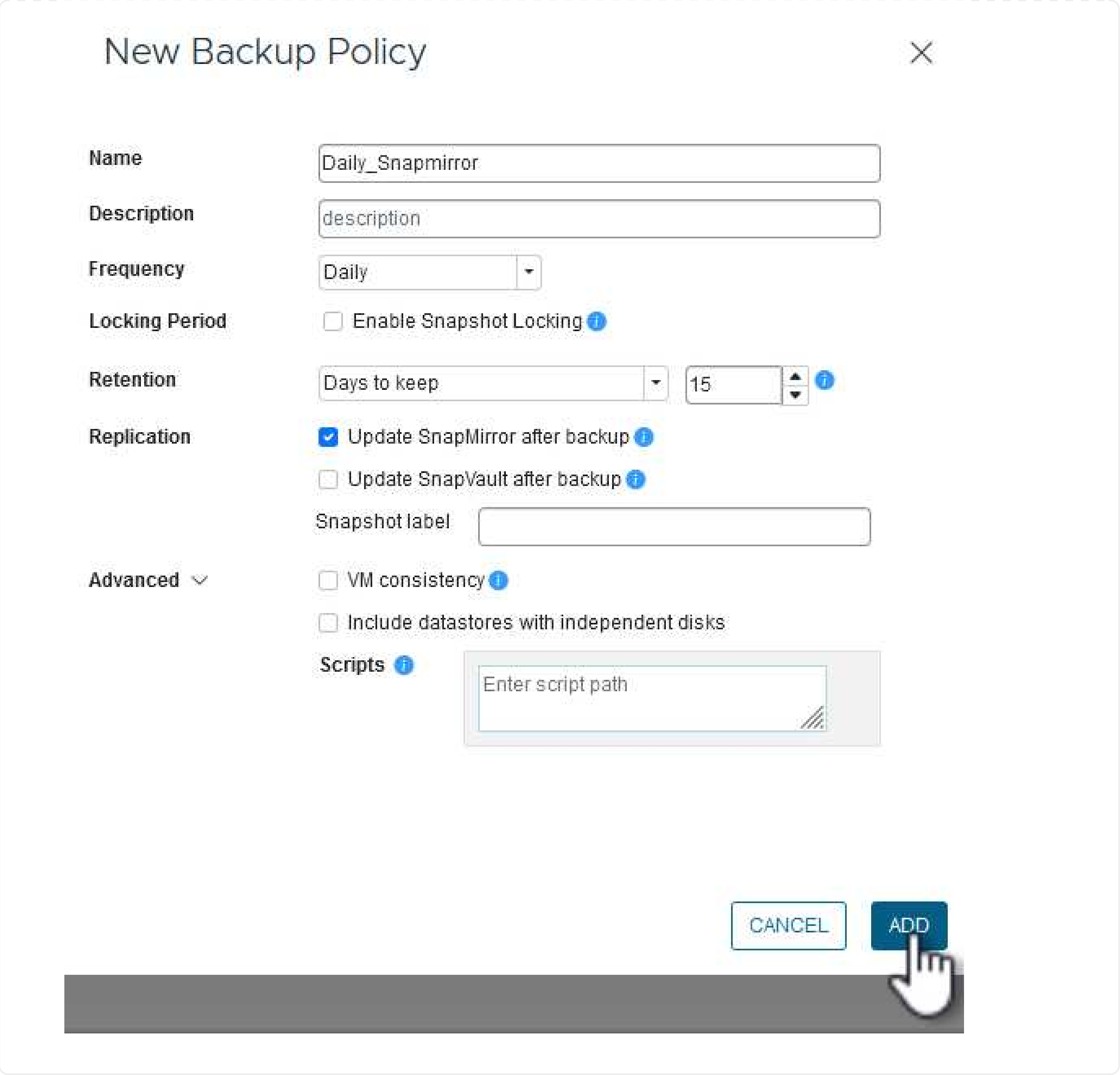
2. On the **New Backup Policy** form, provide a **Name** and **Description** for the policy, the **Frequency** at which the backups will take place, and the **Retention** period which specifies how long the backup is retained.

   Locking Period enables the ONTAP SnapLock feature to create tamper proof snapshots and allows configuration of the locking period.

   For **Replication** Select to update the underlying SnapMirror or SnapVault relationships for the ONTAP storage volume.

   > SnapMirror and SnapVault replication are similar in that they both utilize ONTAP SnapMirror technology to asynchronously replicate storage volumes to a secondary storage system for increased protection and security. For SnapMirror relationships, the retention schedule specified in the SCV backup policy will govern retention for both the primary and secondary volume. With SnapVault relationships, a separate retention schedule can be established on the secondary storage system for longer term or differing retention schedules. In this case the snapshot label is specified in the SCV backup policy and in the policy associated with the secondary volume, to identify which volumes to apply the independent retention schedule to.

   Choose any additional advanced options and click on **Add** to create the policy.



New Backup Policy

Name: Daily_Snapmirror

Description: description

Frequency: Daily

Locking Period: □ Enable Snapshot Locking

Retention: Days to keep 15

Replication: ☑ Update SnapMirror after backup

□ Update SnapVault after backup

Snapshot label:

Advanced: □ VM consistency

□ Include datastores with independent disks

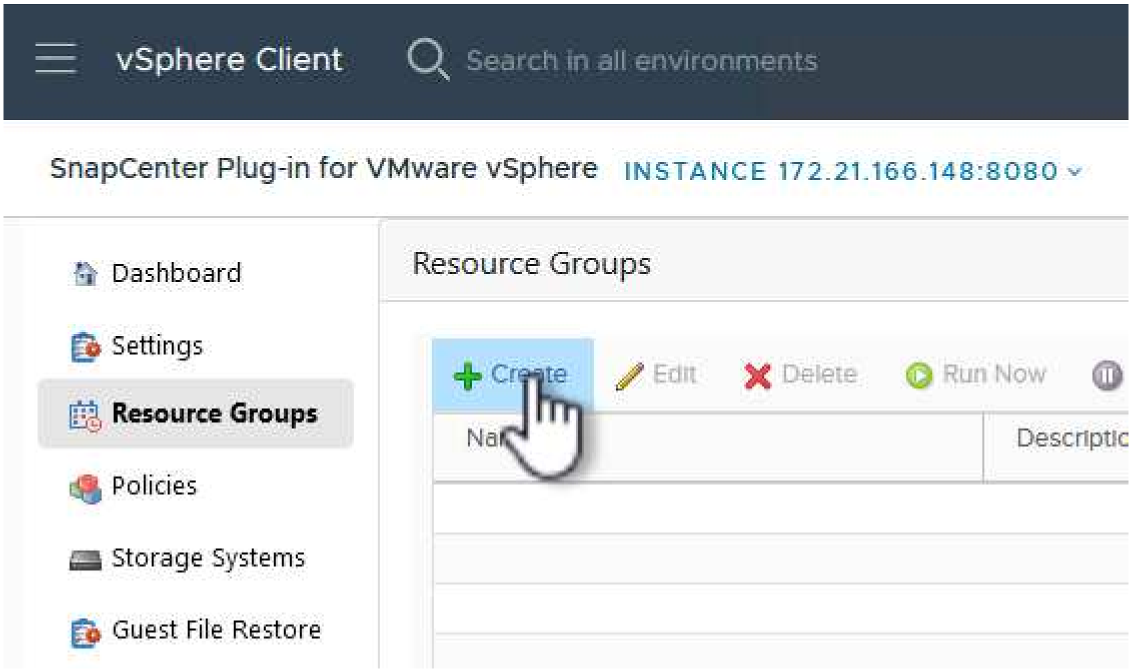
Scripts: Enter script path

Create resource groups in SCV

For more information on creating SCV Resource Groups refer to Create resource groups.

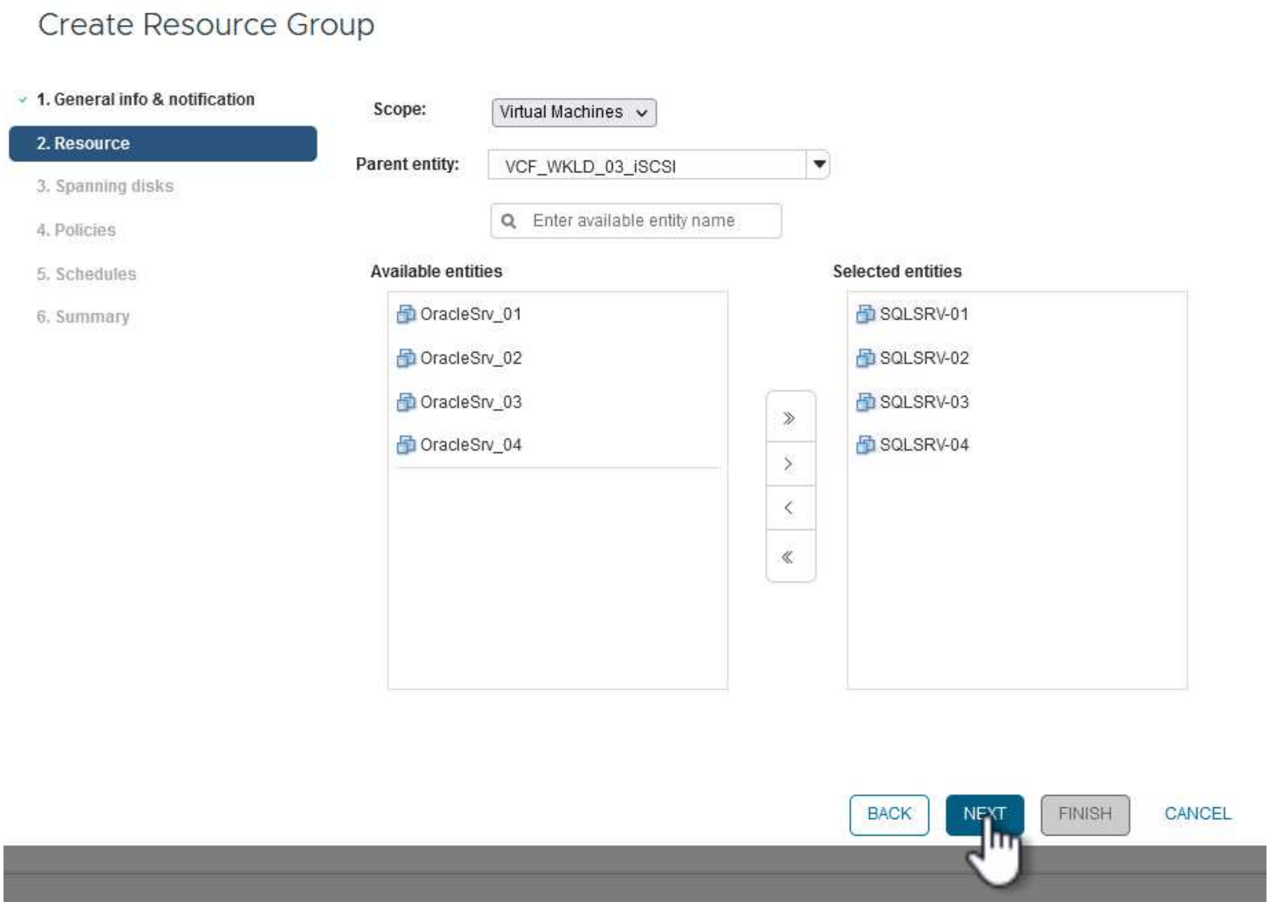
Complete the following steps to create a new resource group:

1. From the left-hand menu select **Resource Groups** and click on **Create** to begin.



2. On the **General info & notification** page, provide a name for for the resource group, notification settings, and any additional options for the naming of the snapshots.
3. On the **Resource** page select the datastores and VM's to be protected in the resource group. Click on **Next** to continue.

> Even when only specific VMs are selected, the entire datastore is always backed up. This is because ONTAP takes snapshots of the volume hosting the datastore. However, note that selecting only specific VMs for backup limits the ability to restore to only those VMs.



Create Resource Group

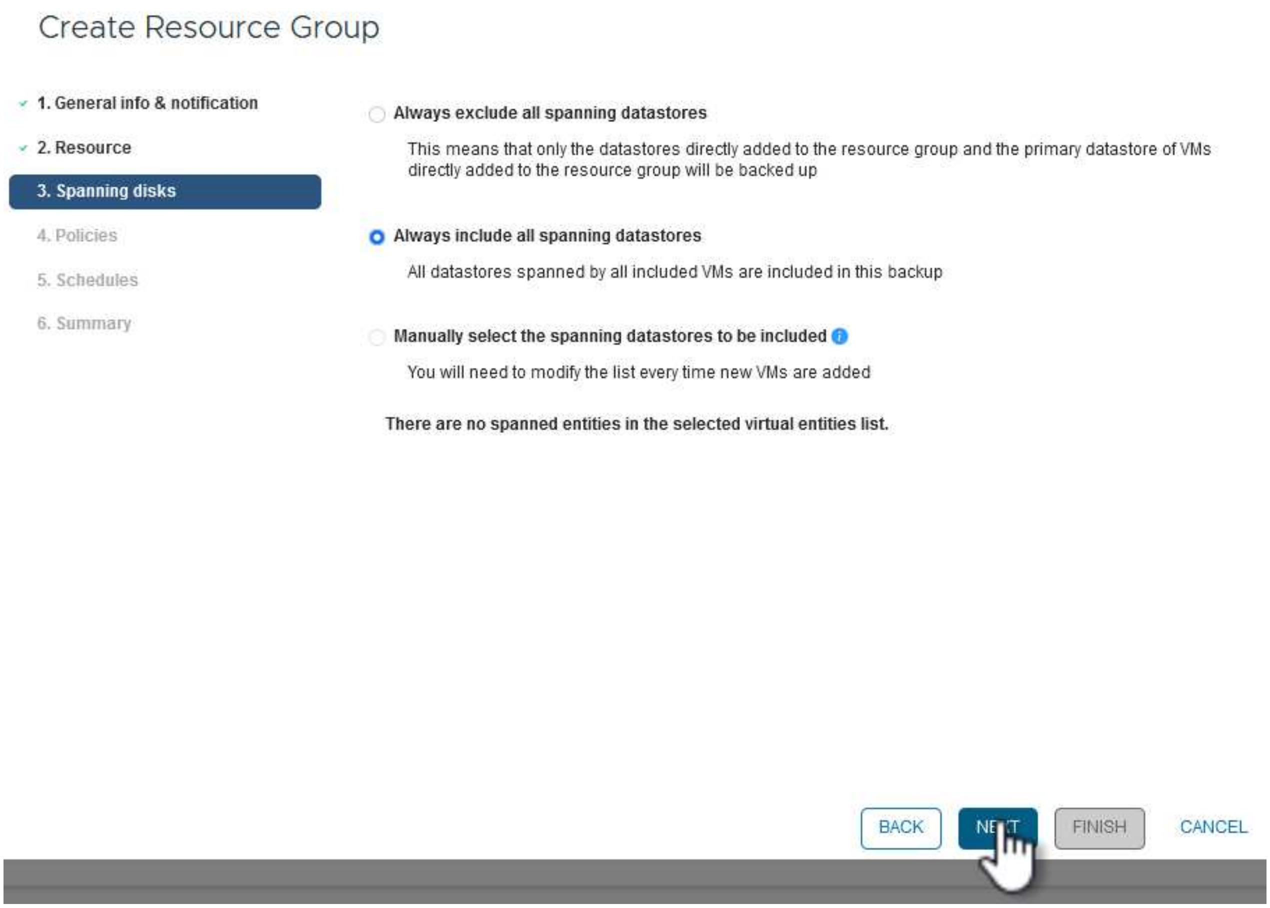
Scope: Virtual Machines

Parent entity: VCF_WKLD_03_iSCSI

Enter available entity name

Available entities	Selected entities
OracleSrv_01	SQLSRV-01
OracleSrv_02	SQLSRV-02
OracleSrv_03	SQLSRV-03
OracleSrv_04	SQLSRV-04

4. On the **Spanning disks** page select the option for how to handle VMs with VMDK’s that span multiple datastores. Click on **Next** to continue.



Create Resource Group

○ **Always exclude all spanning datastores**

This means that only the datastores directly added to the resource group and the primary datastore of VMs directly added to the resource group will be backed up

● **Always include all spanning datastores**

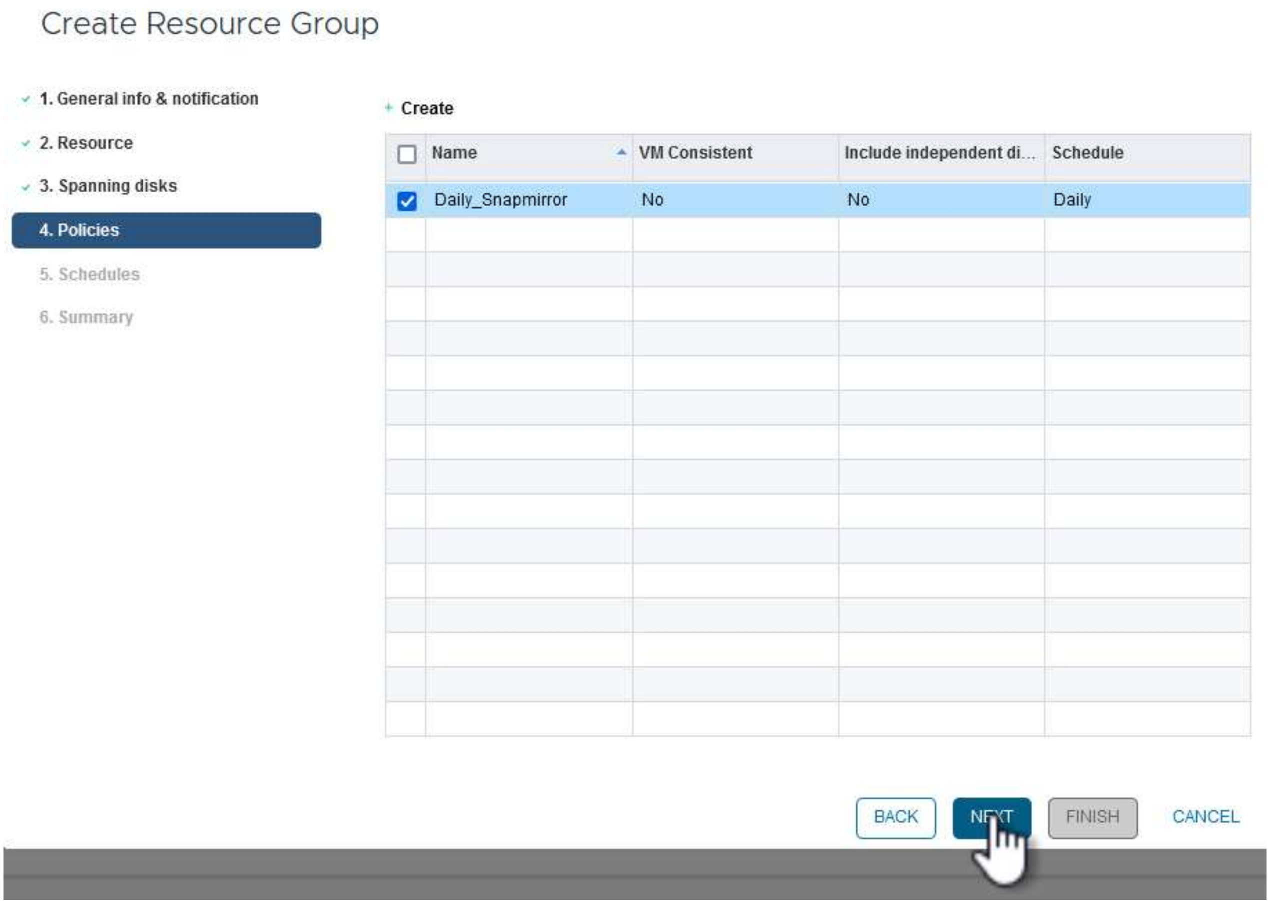
All datastores spanned by all included VMs are included in this backup

○ **Manually select the spanning datastores to be included**

You will need to modify the list every time new VMs are added

There are no spanned entities in the selected virtual entities list.

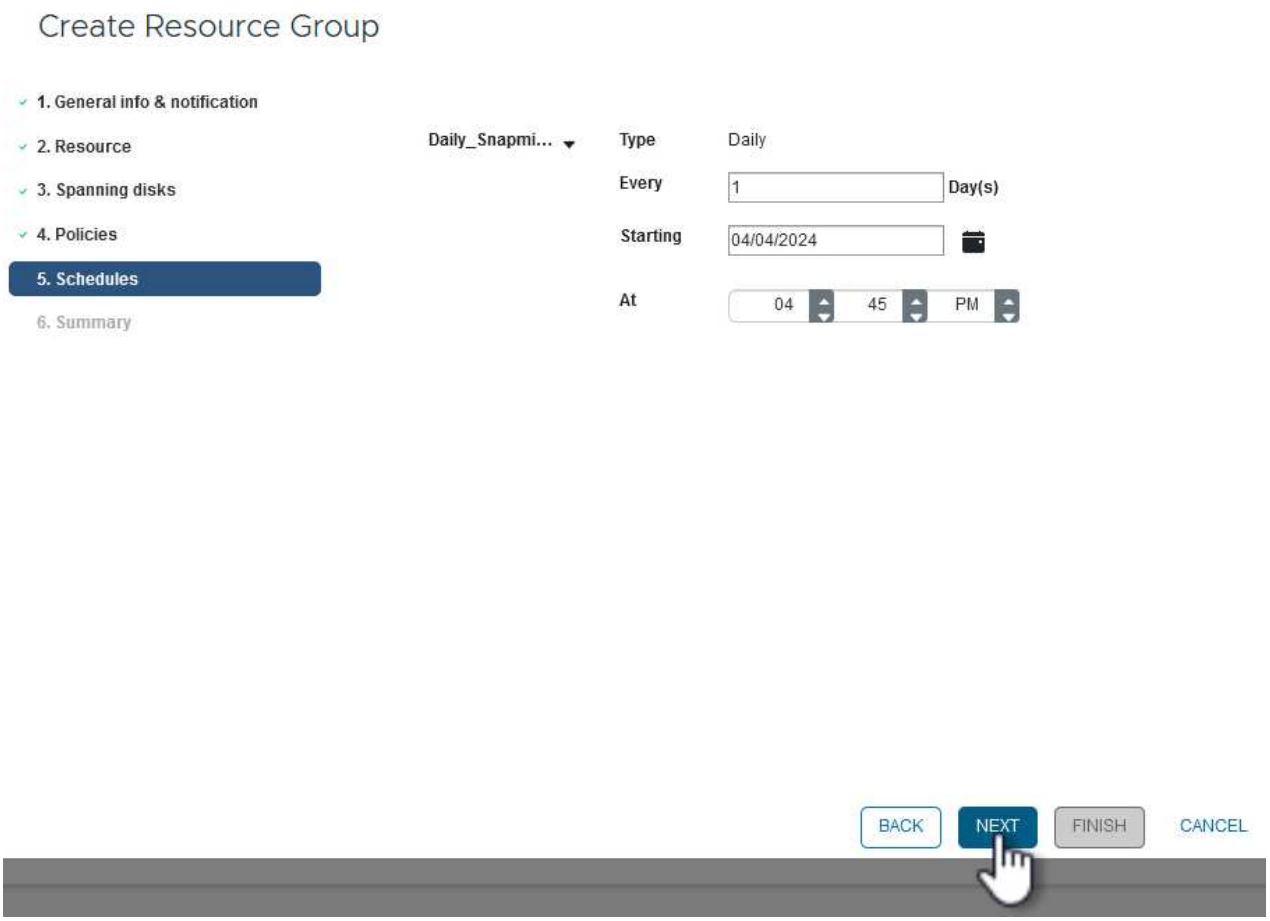
5. On the **Policies** page select a previously created policy or multiple policies that will be used with this resource group. Click on **Next** to continue.



Create Resource Group

☐	Name	VM Consistent	Include independent di...	Schedule
☑	Daily_Snapmirror	No	No	Daily

6. On the **Schedules** page establish for when the backup will run by configuring the recurrence and time of day. Click on **Next** to continue.



Create Resource Group

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

Daily_Snapmi...

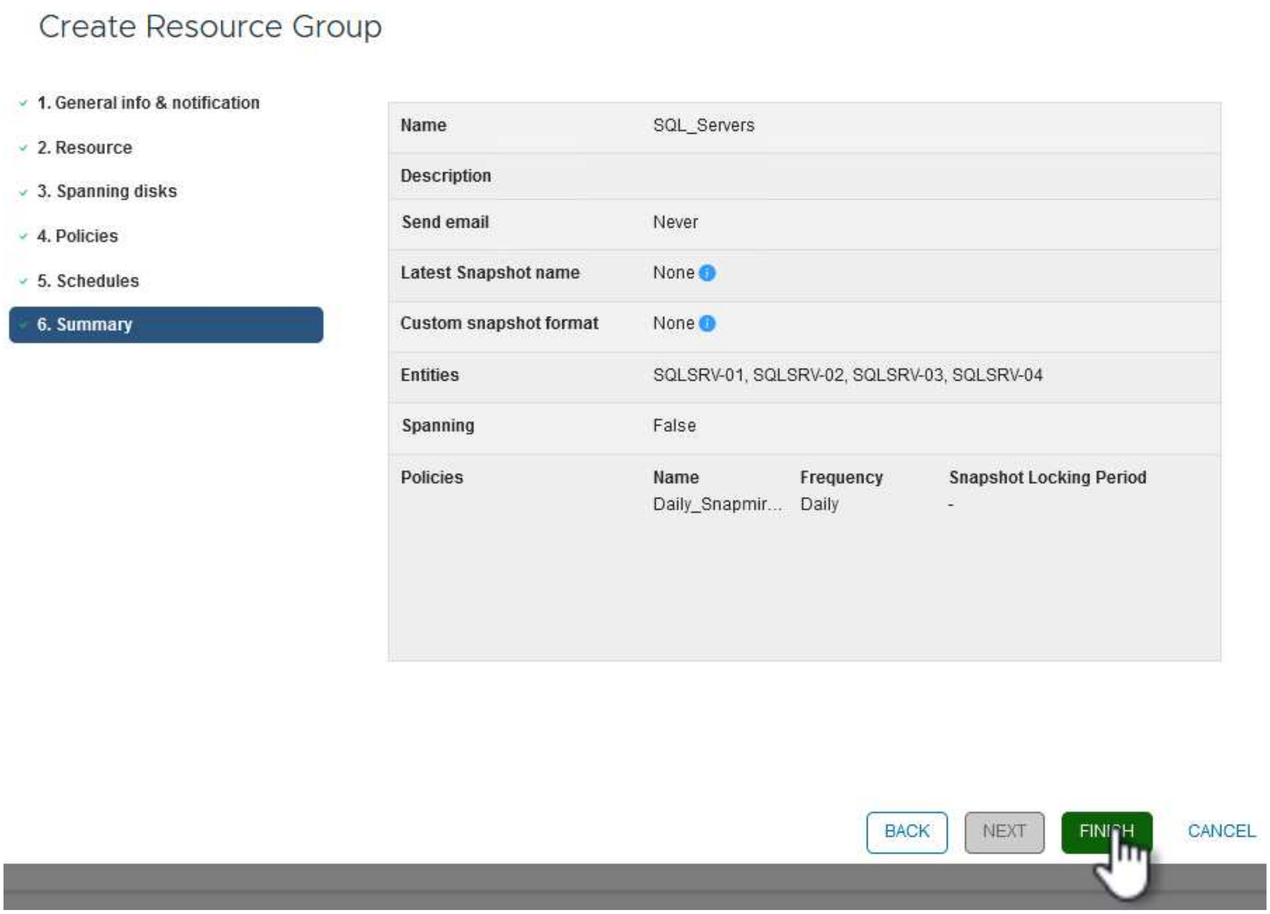
Type: Daily

Every: 1 Day(s)

Starting: 04/04/2024

At: 04 45 PM

7. Finally review the **Summary** and click on **Finish** to create the resource group.

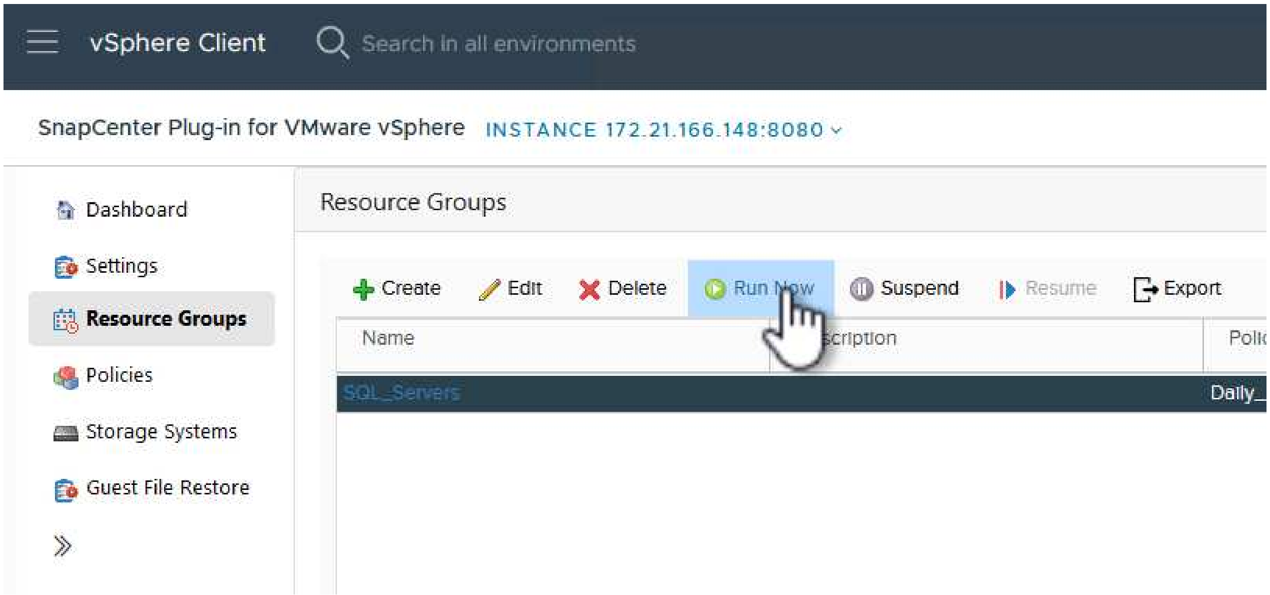


Create Resource Group

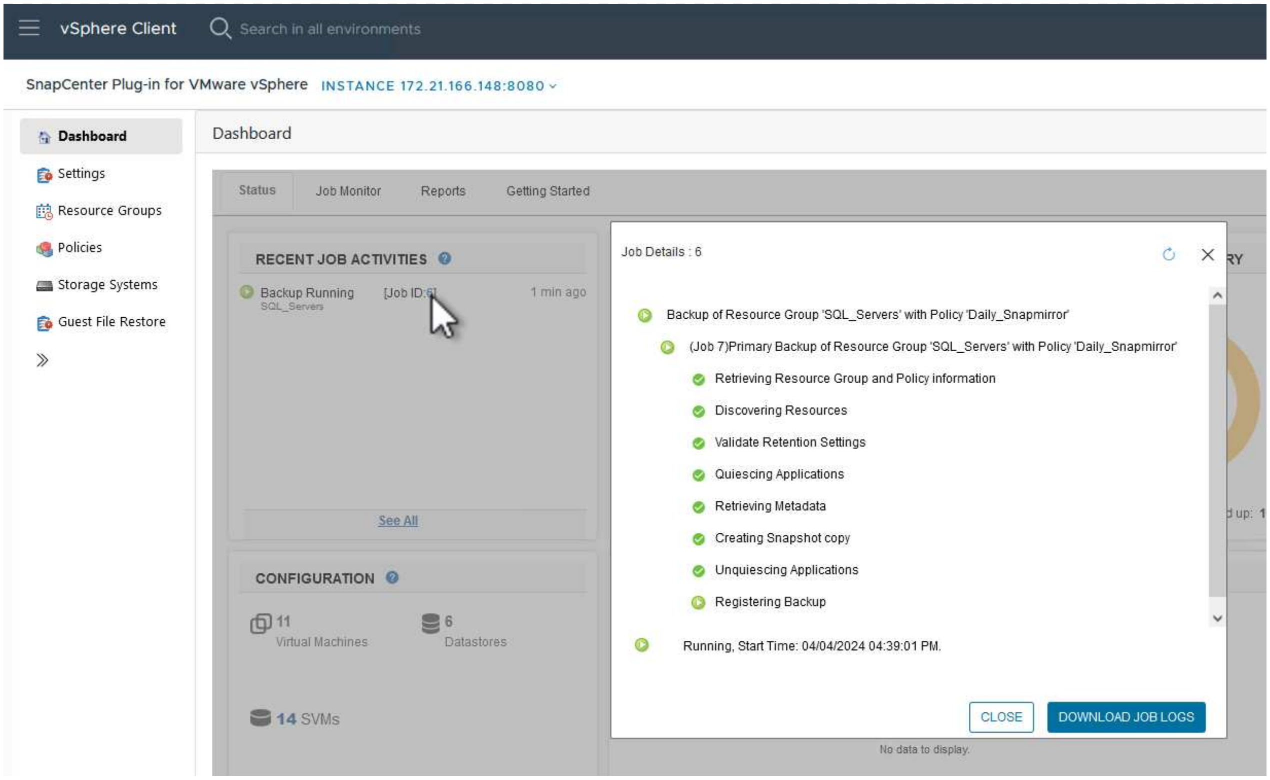
- ✓ 1. General info & notification
- ✓ 2. Resource
- ✓ 3. Spanning disks
- ✓ 4. Policies
- ✓ 5. Schedules
- ✓ 6. Summary

Name	SQL_Servers		
Description			
Send email	Never		
Latest Snapshot name	None		
Custom snapshot format	None		
Entities	SQLSRV-01, SQLSRV-02, SQLSRV-03, SQLSRV-04		
Spanning	False		
Policies	Name Daily_Snapmir...	Frequency Daily	Snapshot Locking Period -

8. With the resource group created click on the **Run Now** button to run the first backup.



9. Navigate to the **Dashboard** and, under **Recent Job Activities** click on the number next to **Job ID** to open the job monitor and view the progress of the running job.



Backup Running [Job ID:6] 1 min ago
SQL_Servers

11 Virtual Machines
6 Datastores
14 SVMs

Job Details : 6

- Backup of Resource Group 'SQL_Servers' with Policy 'Daily_Snapmirror'
  - (Job 7)Primary Backup of Resource Group 'SQL_Servers' with Policy 'Daily_Snapmirror'
    - Retrieving Resource Group and Policy information
    - Discovering Resources
    - Validate Retention Settings
    - Quiescing Applications
    - Retrieving Metadata
    - Creating Snapshot copy
    - Unquiescing Applications
    - Registering Backup

Running, Start Time: 04/04/2024 04:39:01 PM.

No data to display.

Use SCV to restore VMs, VMDKs and files

The SnapCenter Plug-in allows restores of VMs, VMDKs, files, and folders from primary or secondary backups.

VMs can be restored to the original host, or to an alternate host in the same vCenter Server, or to an alternate ESXi host managed by the same vCenter or any vCenter in linked mode.

vVol VMs can be restored to the original host.

VMDKs in traditional VMs can be restored to either the original or to an alternate datastore.

VMDKs in vVol VMs can be restored to the original datastore.

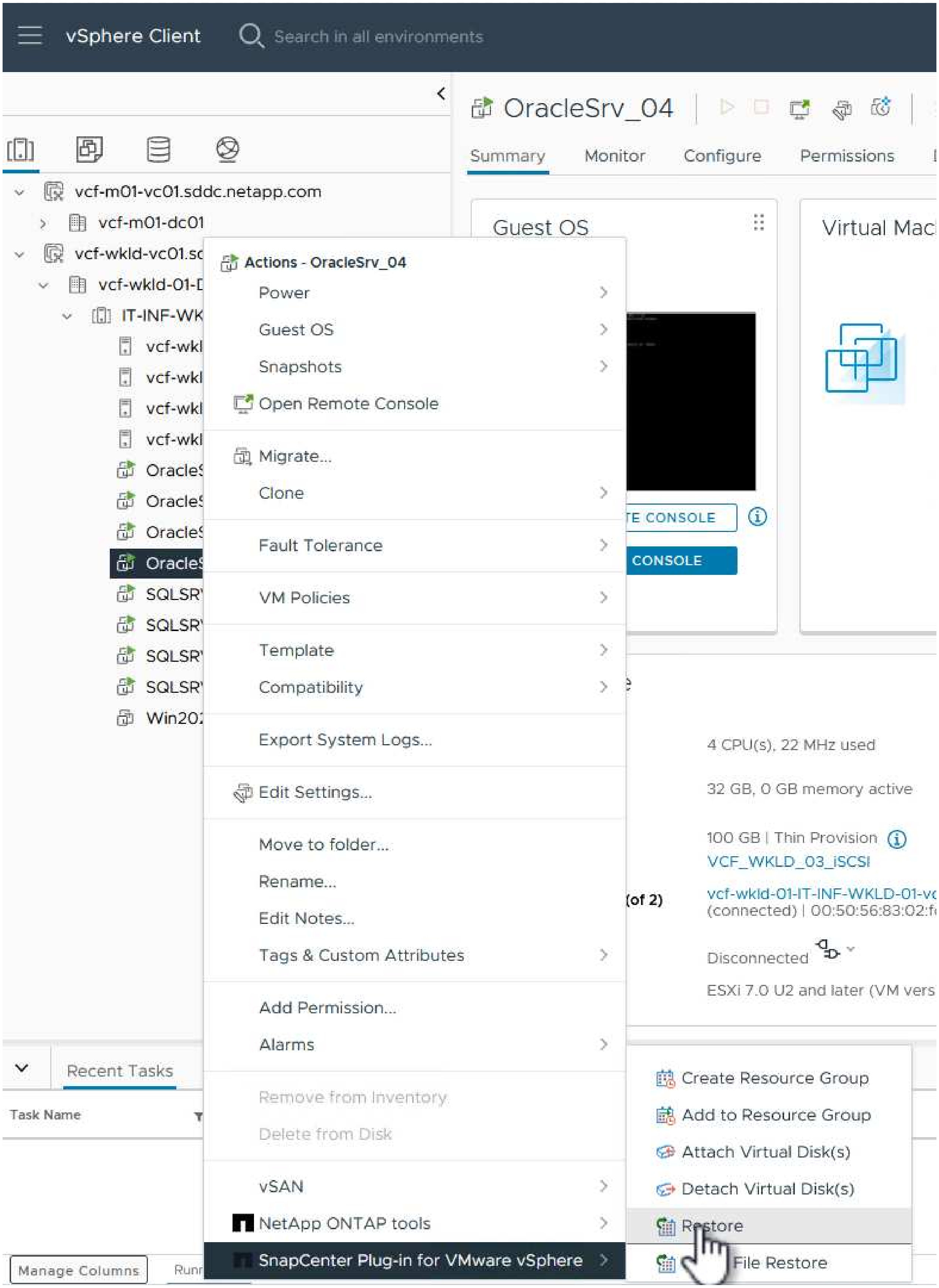
Individual files and folders in a guest file restore session can be restored, which attaches a backup copy of a virtual disk and then restores the selected files or folders.

Complete the following steps to restore VMs, VMDKs or individual folders.

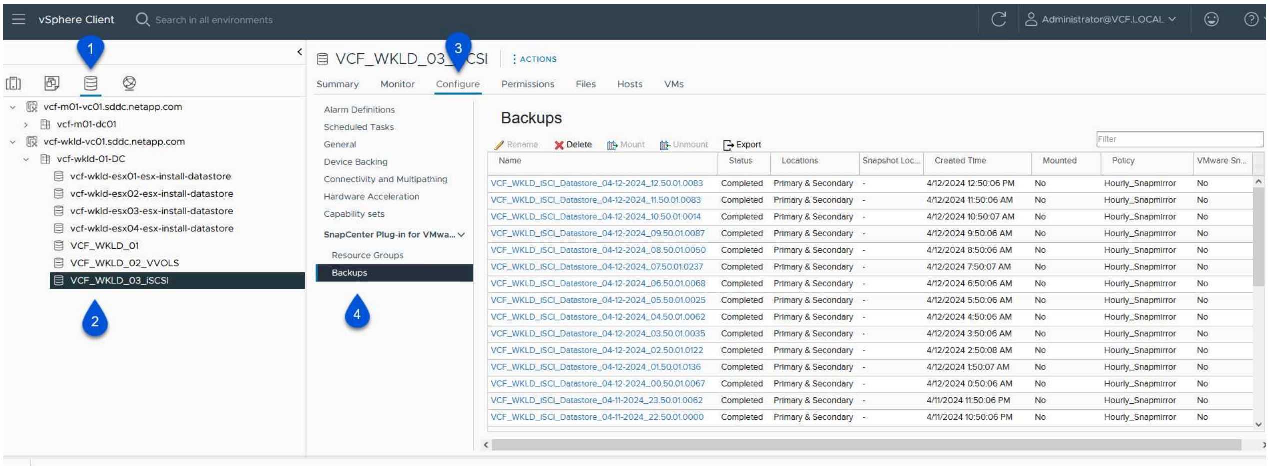
Restore VMs using SnapCenter Plug-in

Complete the following steps to restore a VM with SCV:

1. Navigate to the VM to be restored in the vSphere client, right click and navigate to **SnapCenter Plug-in for VMware vSphere**. Select **Restore** from the sub-menu.


vSphere Client
Search in all environments
vcf-m01-vc01.sddc.netapp.com
vcf-m01-dc01
vcf-wkld-vc01.sc
vcf-wkld-01-D
IT-INF-WK
vcf-wkl
vcf-wkl
vcf-wkl
vcf-wkl
OracleS
OracleS
OracleS
OracleS
SQLSR
SQLSR
SQLSR
SQLSR
Win20
OracleSrv_04
Summary
Monitor
Configure
Permissions
Guest OS
Virtual Mac
TE CONSOLE
CONSOLE
4 CPU(s), 22 MHz used
32 GB, 0 GB memory active
100 GB | Thin Provision
VCF_WKLD_03_iSCSI
(of 2)
vcf-wkld-01-IT-INF-WKLD-01-vc
(connected) | 00:50:56:83:02:f
Disconnected
ESXi 7.0 U2 and later (VM vers
Recent Tasks
Task Name
Manage Columns
Runr
Actions - OracleSrv_04
Power
Guest OS
Snapshots
Open Remote Console
Migrate...
Clone
Fault Tolerance
VM Policies
Template
Compatibility
Export System Logs...
Edit Settings...
Move to folder...
Rename...
Edit Notes...
Tags & Custom Attributes
Add Permission...
Alarms
Remove from Inventory
Delete from Disk
vSAN
NetApp ONTAP tools
SnapCenter Plug-in for VMware vSphere
Create Resource Group
Add to Resource Group
Attach Virtual Disk(s)
Detach Virtual Disk(s)
Restore
File Restore

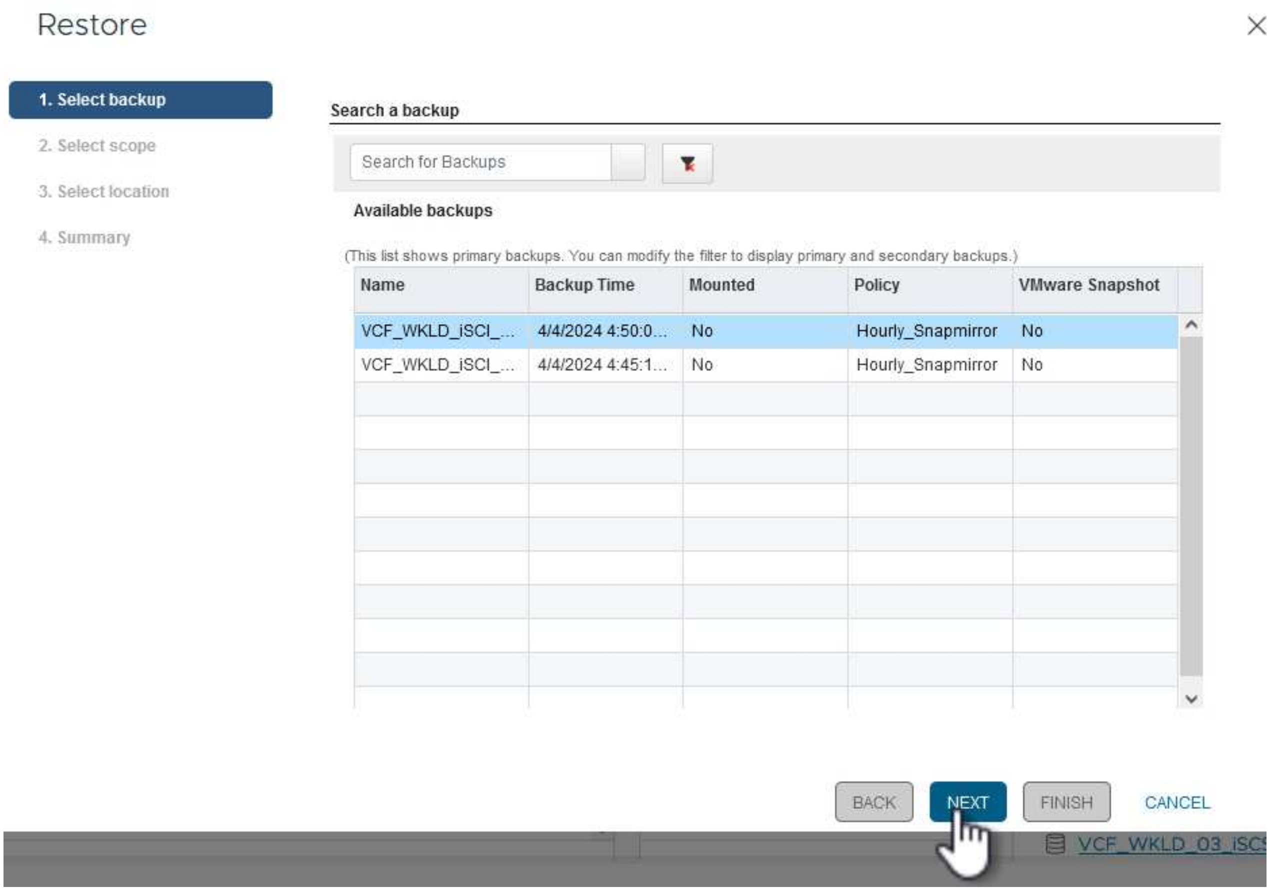
An alternative is to navigate to the datastore in inventory and then under the **Configure** tab go to **SnapCenter Plug-in for VMware vSphere > Backups**. From the chosen backup, select the VMs to be restored.



Backups

Name	Status	Locations	Snapshot Loc...	Created Time	Mounted	Policy	VMware Sn...
VCF_WKLD_iSCI_Datastore_04-12-2024_12.50.01.0083	Completed	Primary & Secondary	-	4/12/2024 12:50:06 PM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_11.50.01.0083	Completed	Primary & Secondary	-	4/12/2024 11:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_10.50.01.0014	Completed	Primary & Secondary	-	4/12/2024 10:50:07 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_09.50.01.0087	Completed	Primary & Secondary	-	4/12/2024 9:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_08.50.01.0050	Completed	Primary & Secondary	-	4/12/2024 8:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_07.50.01.0237	Completed	Primary & Secondary	-	4/12/2024 7:50:07 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_06.50.01.0068	Completed	Primary & Secondary	-	4/12/2024 6:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_05.50.01.0025	Completed	Primary & Secondary	-	4/12/2024 5:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_04.50.01.0062	Completed	Primary & Secondary	-	4/12/2024 4:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_03.50.01.0035	Completed	Primary & Secondary	-	4/12/2024 3:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_02.50.01.0122	Completed	Primary & Secondary	-	4/12/2024 2:50:08 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_01.50.01.0136	Completed	Primary & Secondary	-	4/12/2024 1:50:07 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-12-2024_00.50.01.0067	Completed	Primary & Secondary	-	4/12/2024 0:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-11-2024_23.50.01.0062	Completed	Primary & Secondary	-	4/11/2024 11:50:06 PM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-11-2024_22.50.01.0000	Completed	Primary & Secondary	-	4/11/2024 10:50:06 PM	No	Hourly_Snapmirror	No

2. In the **Restore** wizard select the backup to be used. Click on **Next** to continue.



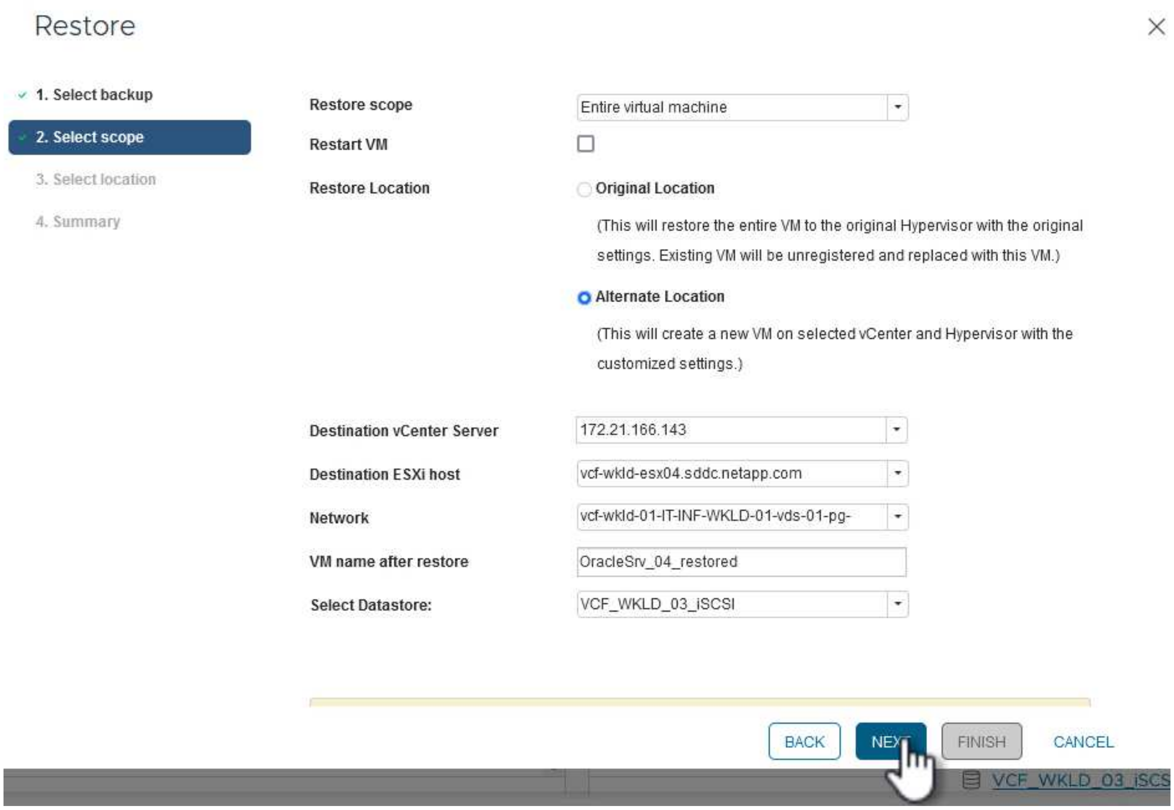
Available backups

(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF_WKLD_iSCI_...	4/4/2024 4:50:0...	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_...	4/4/2024 4:45:1...	No	Hourly_Snapmirror	No

3. On the **Select scope** page fill out all required fields:

- **Restore scope** - Select to restore the entire virtual machine.
- **Restart VM** - Choose whether to start the VM after the restore.
- **Restore Location** - Choose to restore to the original location or to an alternate location. When choosing alternate location select the options from each of the fields:
    - **Destination vCenter Server** - local vCenter or alternate vCenter in linked mode
    - **Destination ESXi host**
    - **Network**
    - **VM name after restore**
    - **Select datastore:**



Restore

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

Restore scope: Entire virtual machine

Restart VM: □

Restore Location:

○ Original Location

(This will restore the entire VM to the original Hypervisor with the original settings. Existing VM will be unregistered and replaced with this VM.)

● Alternate Location

(This will create a new VM on selected vCenter and Hypervisor with the customized settings.)

Destination vCenter Server: 172.21.166.143

Destination ESXi host: vcf-wkld-esx04.sddc.netapp.com

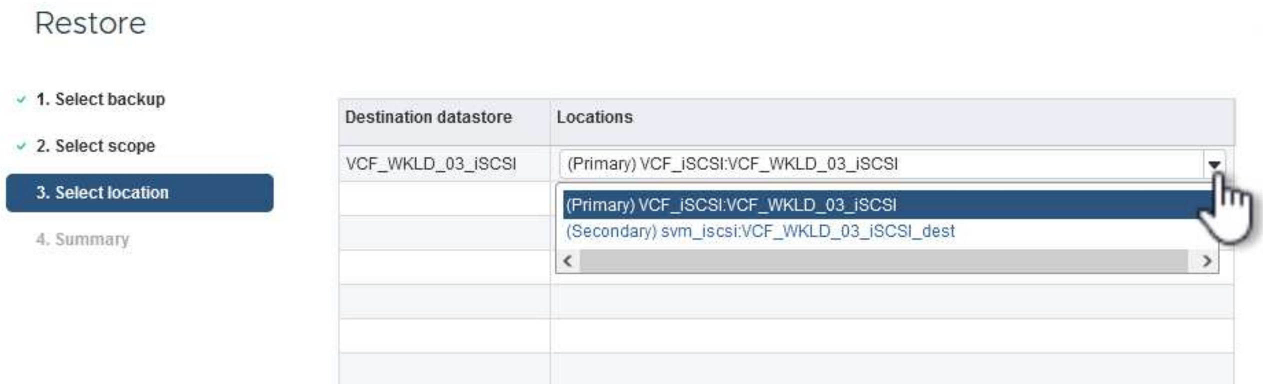
Network: vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-

VM name after restore: OracleSrv_04_restored

Select Datastore: VCF_WKLD_03_iSCSI

Click on **Next** to continue.

4. On the **Select location** page, choose to restore the VM from the primary or secondary ONTAP storage system. Click on **Next** to continue.



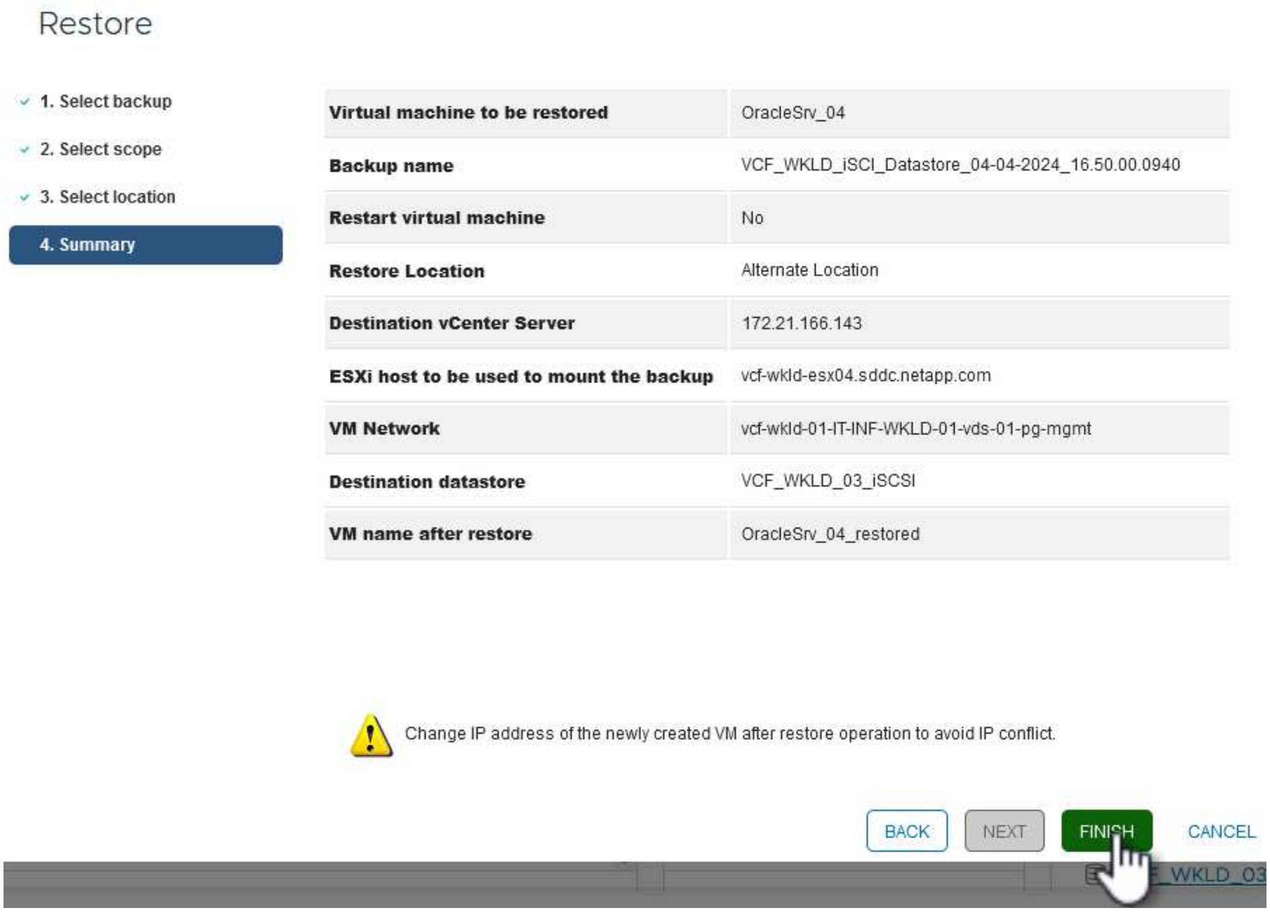
Restore

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

Destination datastore	Locations
VCF_WKLD_03_iSCSI	(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI

(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI
(Secondary) svm_iscsi:VCF_WKLD_03_iSCSI_dest

5. Finally, review the **Summary** and click on **Finish** to start the restore job.



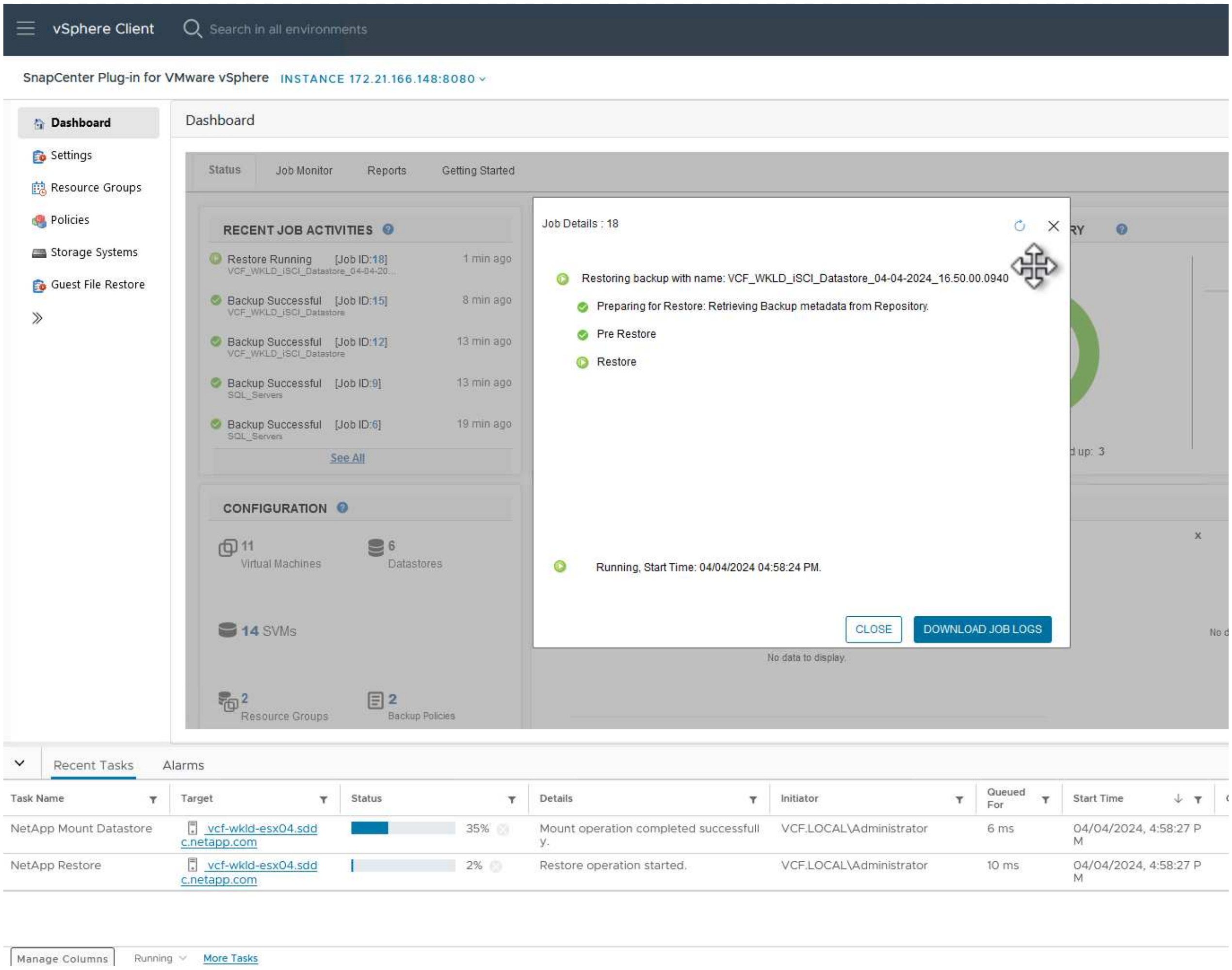
Restore

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

Virtual machine to be restored	OracleSrv_04
Backup name	VCF_WKLD_iSCI_Datastore_04-04-2024_16.50.00.0940
Restart virtual machine	No
Restore Location	Alternate Location
Destination vCenter Server	172.21.166.143
ESXi host to be used to mount the backup	vcf-wkld-esx04.sddc.netapp.com
VM Network	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt
Destination datastore	VCF_WKLD_03_iSCSI
VM name after restore	OracleSrv_04_restored

Change IP address of the newly created VM after restore operation to avoid IP conflict.

6. The restore job progress can be monitored from the **Recent Tasks** pane in the vSphere Client and from the job monitor in SCV.



Restore Running [Job ID:18] 1 min ago
VCF_WKLD_iSCI_Datastore_04-04-20...

Backup Successful [Job ID:15] 8 min ago
VCF_WKLD_iSCI_Datastore

Backup Successful [Job ID:12] 13 min ago
VCF_WKLD_iSCI_Datastore

Backup Successful [Job ID:9] 13 min ago
SQL_Servers

Backup Successful [Job ID:6] 19 min ago
SQL_Servers

Job Details : 18

Restoring backup with name: VCF_WKLD_iSCI_Datastore_04-04-2024_16.50.00.0940

- Preparing for Restore: Retrieving Backup metadata from Repository.
- Pre Restore
- Restore

Running, Start Time: 04/04/2024 04:58:24 PM.

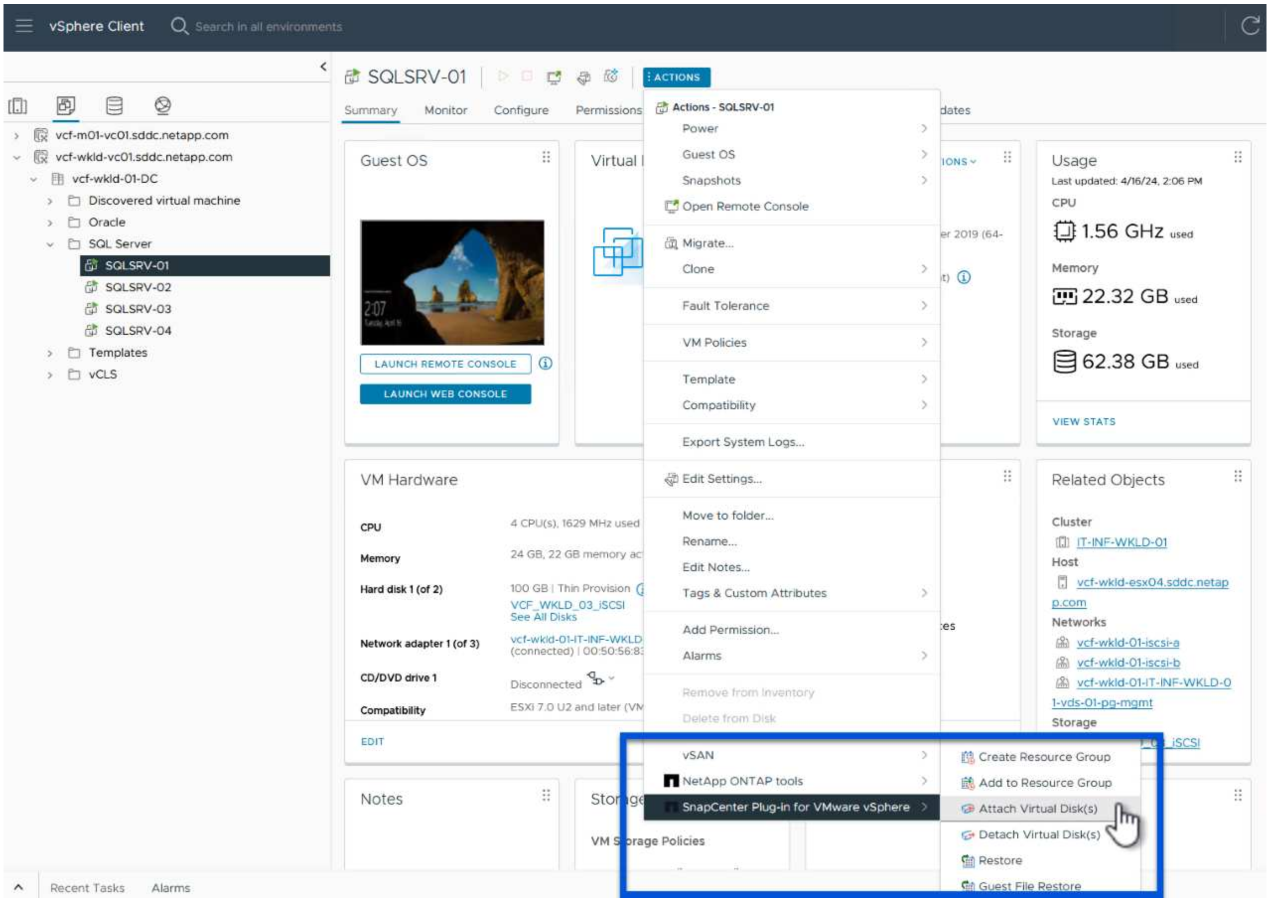
Task Name	Target	Status	Details	Initiator	Queued For	Start Time
NetApp Mount Datastore	vcf-wkld-esx04.sddc.netapp.com	35%	Mount operation completed successfully.	VCF.LOCAL\Administrator	6 ms	04/04/2024, 4:58:27 PM
NetApp Restore	vcf-wkld-esx04.sddc.netapp.com	2%	Restore operation started.	VCF.LOCAL\Administrator	10 ms	04/04/2024, 4:58:27 PM

Restore VMDKs using SnapCenter Plug-in

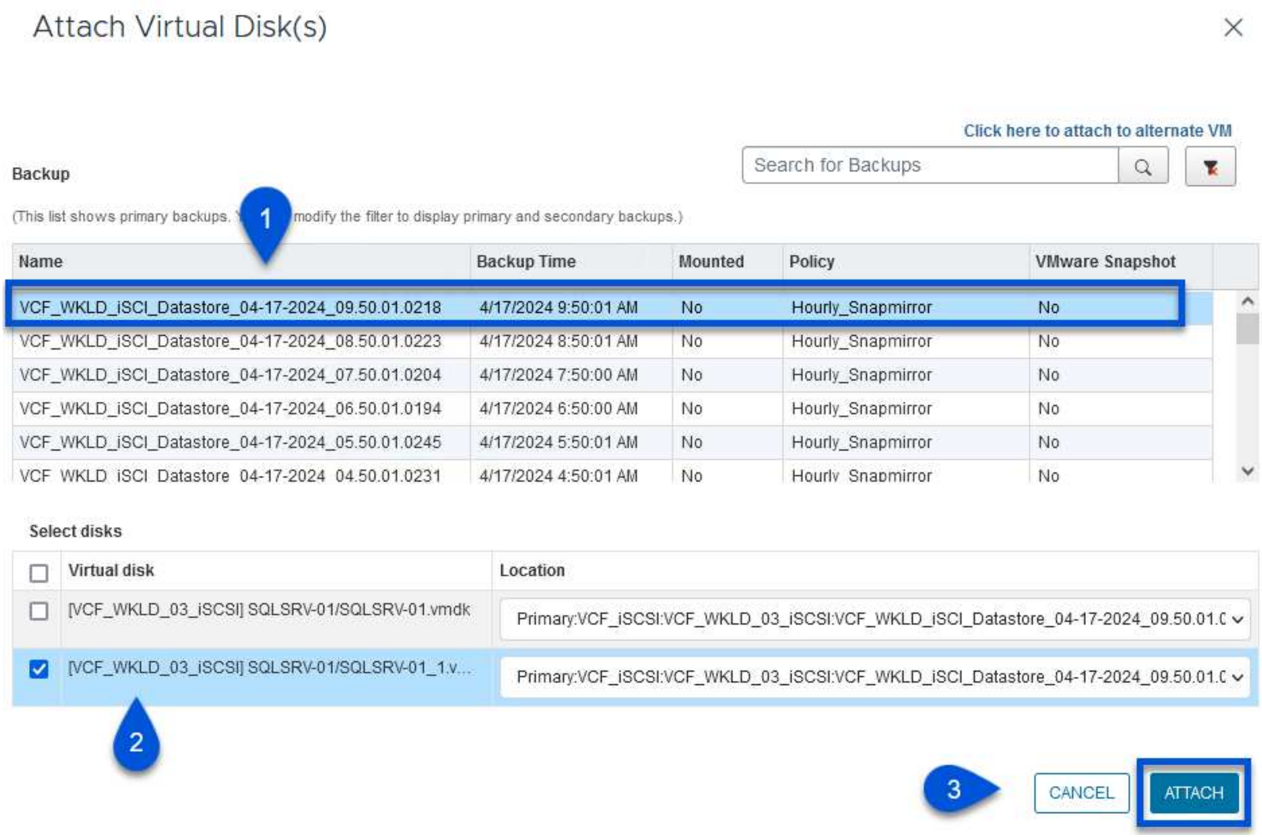
ONTAP Tools allows full restore of VMDK’s to their original location or the ability to attach a VMDK as a new disk to a host system. In this scenario a VMDK will be attached to a Windows host in order to access the file system.

To attach a VMDK from a backup, complete the following steps:

1. In the vSphere Client navigate to a VM and, from the **Actions** menu, select **SnapCenter Plug-in for VMware vSphere > Attach Virtual Disk(s)**.



2. In the **Attach Virtual Disk(s)** wizard, select the backup instance to be used and the particular VMDK to be attached.



Attach Virtual Disk(s)

Click here to attach to alternate VM

Search for Backups

Backup

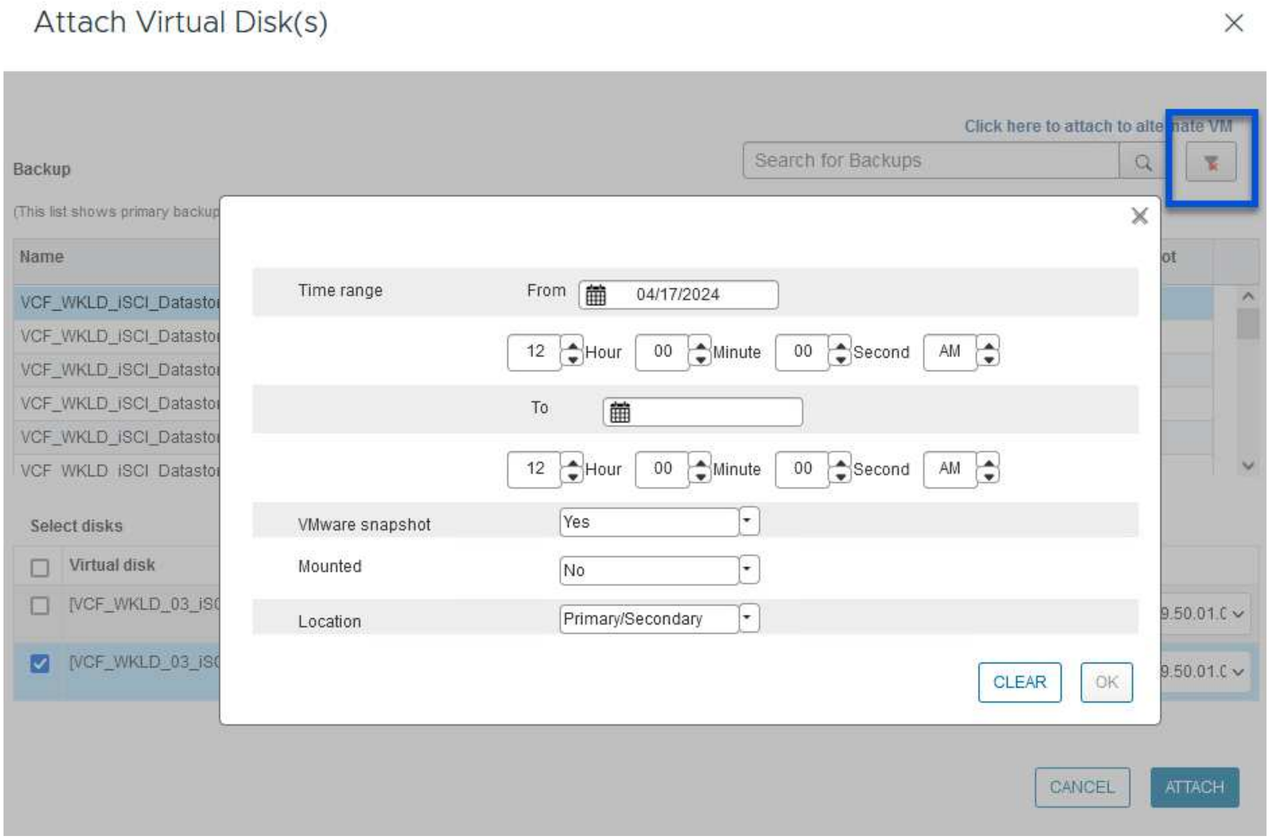
(This list shows primary backups. Y modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF_WKLD_iSCI_Datastore_04-17-2024_09.50.01.0218	4/17/2024 9:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-17-2024_08.50.01.0223	4/17/2024 8:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-17-2024_07.50.01.0204	4/17/2024 7:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-17-2024_06.50.01.0194	4/17/2024 6:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-17-2024_05.50.01.0245	4/17/2024 5:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCI_Datastore_04-17-2024_04.50.01.0231	4/17/2024 4:50:01 AM	No	Hourly_Snapmirror	No

Select disks

☐	Virtual disk	Location
☐	[VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCI_Datastore_04-17-2024_09.50.01.C
☑	[VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.v...	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCI_Datastore_04-17-2024_09.50.01.C

Filter options can be used to locate backups and to display backups from both primary and secondary storage systems.



Attach Virtual Disk(s)

Click here to attach to alternate VM

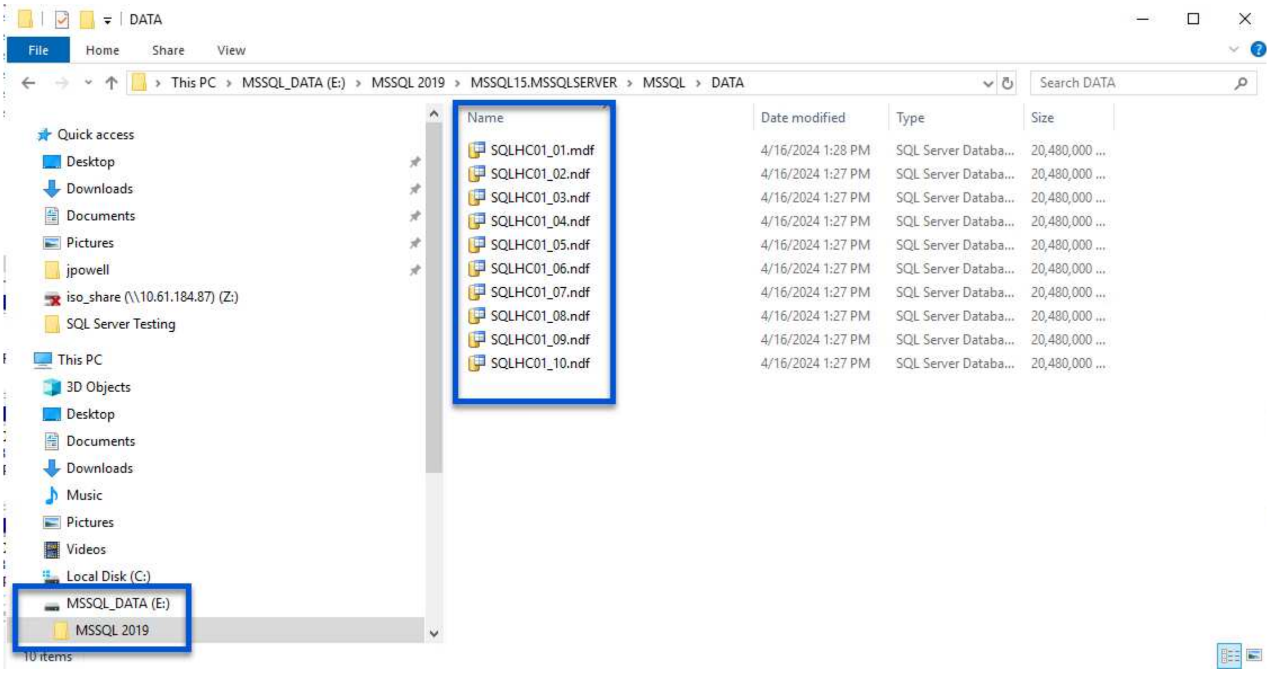
Search for Backups

Backup

(This list shows primary backup

Time range	From	04/17/2024
		12 Hour 00 Minute 00 Second AM
	To	
		12 Hour 00 Minute 00 Second AM
VMware snapshot		Yes
Mounted		No
Location		Primary/Secondary

3. After selecting all options, click on the **Attach** button to begin the restore process and attached the VMDK to the host.
4. Once the attach procedure is complete the disk can be accessed from the OS of the host system. In this case SCV attached the disk with its NTFS file system to the E: drive of our Windows SQL Server and the SQL database files on the file system are accessible through File Explorer.



Name	Date modified	Type	Size
SQLHC01_01.mdf	4/16/2024 1:28 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_02.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_03.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_04.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_05.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_06.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_07.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_08.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_09.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...
SQLHC01_10.ndf	4/16/2024 1:27 PM	SQL Server Databa...	20,480,000 ...

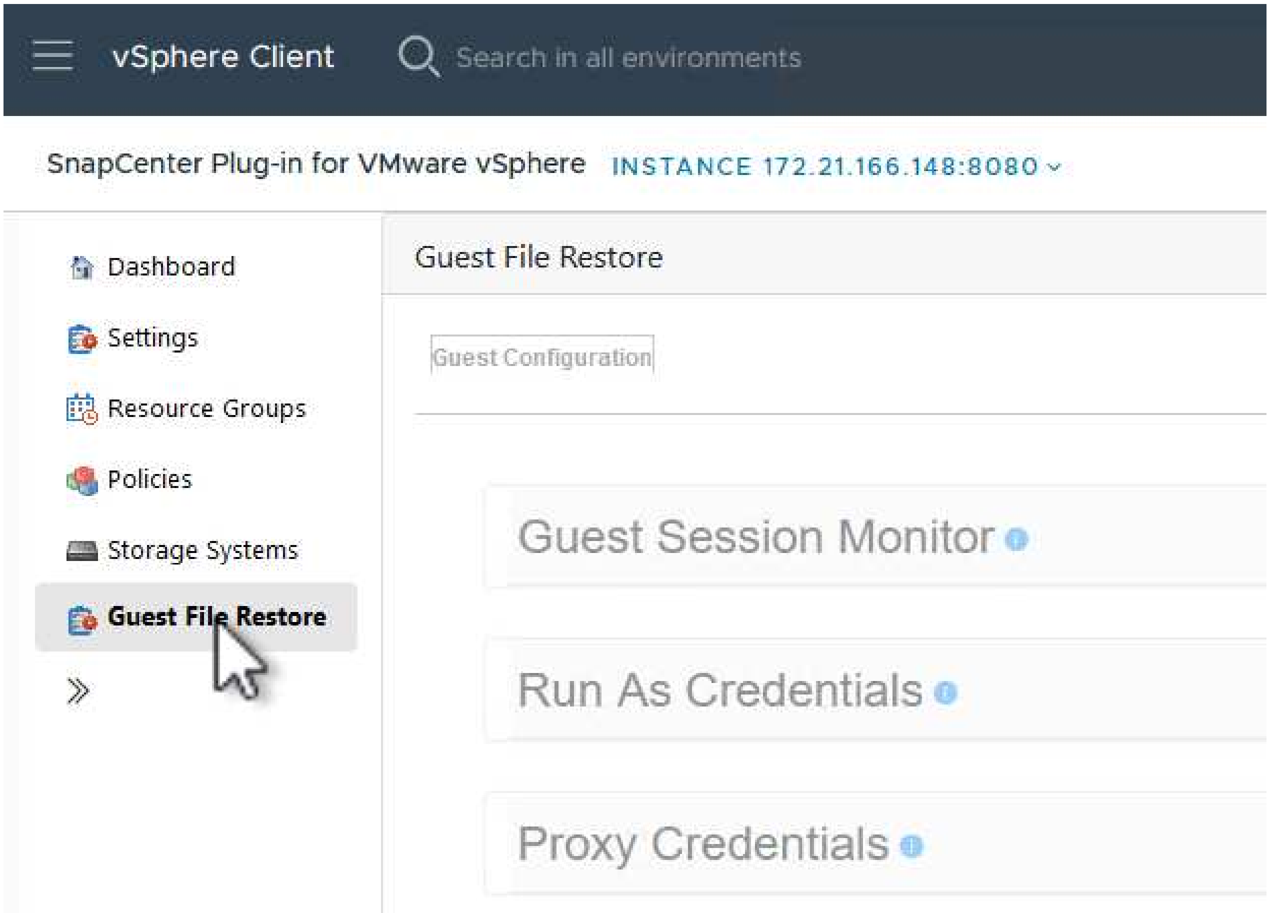
Guest File System Restore using SnapCenter Plug-in

ONTAP Tools features guest file system restores from a VMDK on Windows Server OSes. This is preformed centrally from the SnapCenter Plug-in interface.

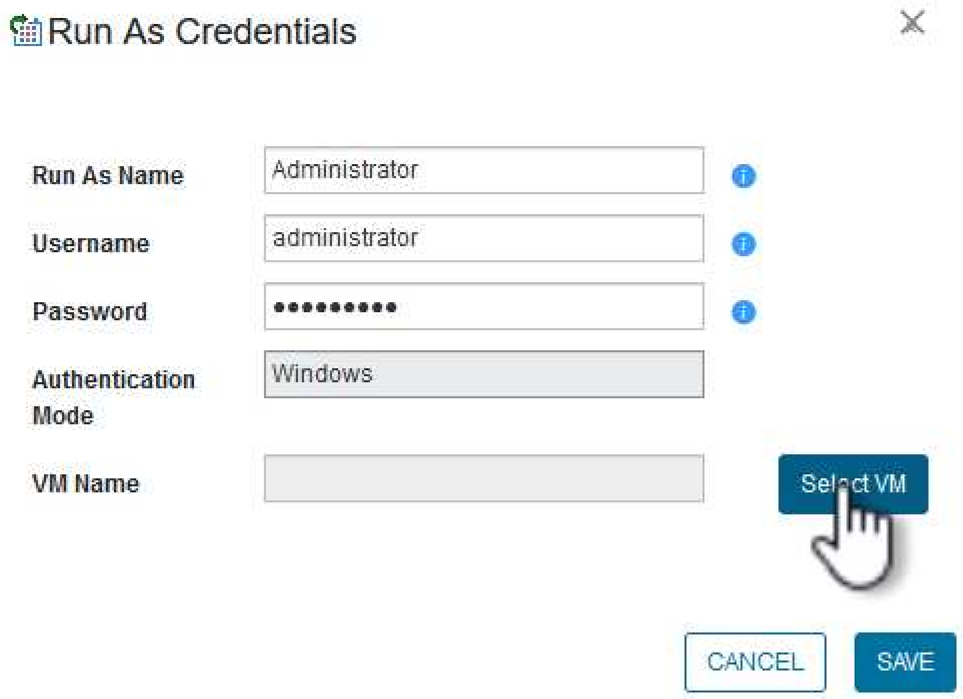
For detailed information refer to Restore guest files and folders at the SCV documentation site.

To perform a guest file system restore for a Windows system, complete the following steps:

1. The first step is to create Run As credentials to provide access to the Windows host system. In the vSphere Client navigate to the CSV plug-in interface and click on **Guest File Restore** in the main menu.



2. Under **Run As Credentials** click on the **+** icon to open the **Run As Credentials** window.
3. Fill in a name for the credentials record, an administrator username and password for the Windows system, and then click on the **Select VM** button to select an optional Proxy VM to be used for the restore.



Run As Credentials

Run As Name: Administrator

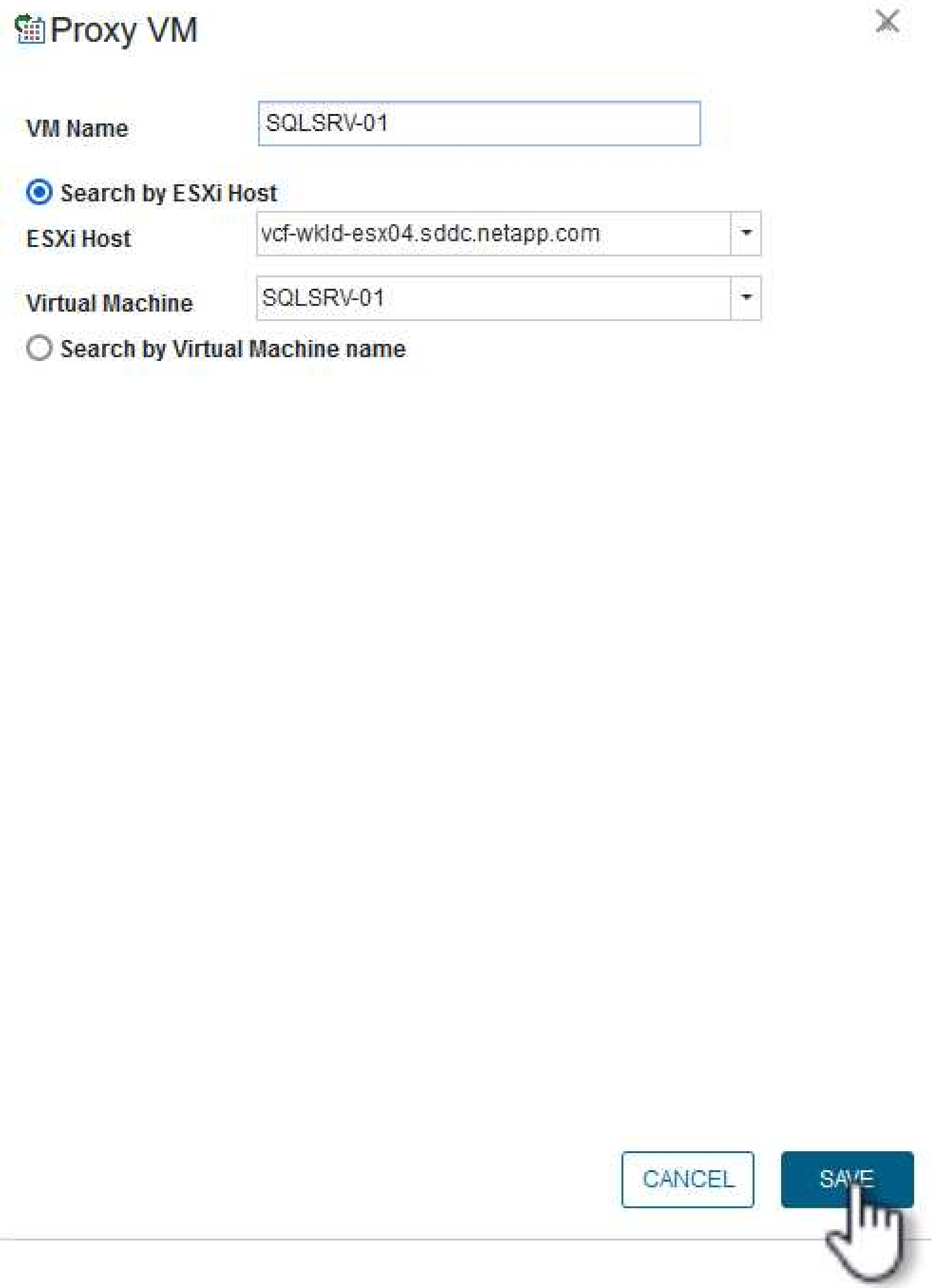
Username: administrator

Password: ••••••••••

Authentication Mode: Windows

VM Name:

4. On the Proxy VM page provide a name for the VM and locate it by searching by ESXi host or by name. Once selected, click on **Save**.



Proxy VM

VM Name: SQLSRV-01

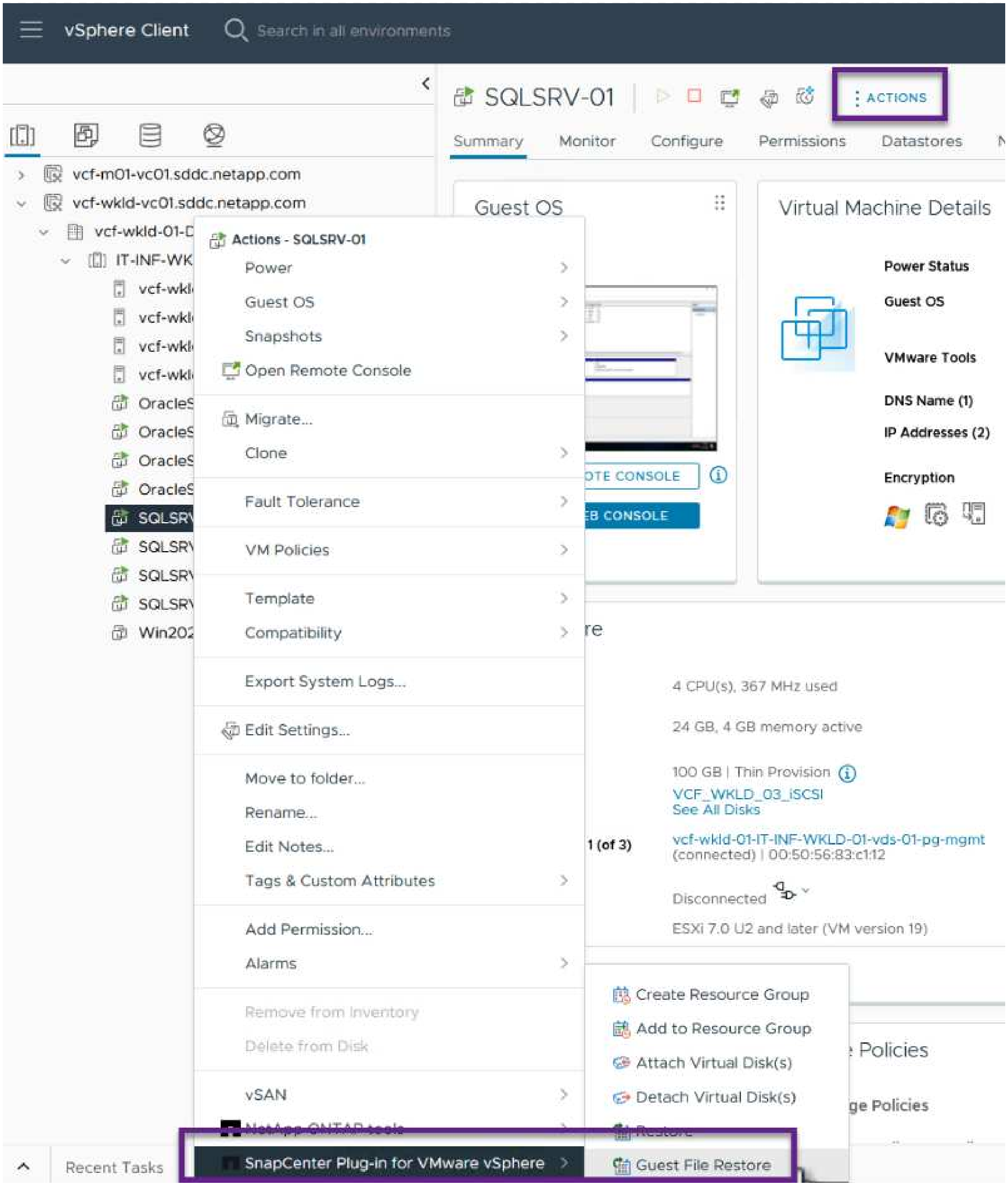
● Search by ESXi Host

ESXi Host: vcf-wkld-esx04.sddc.netapp.com

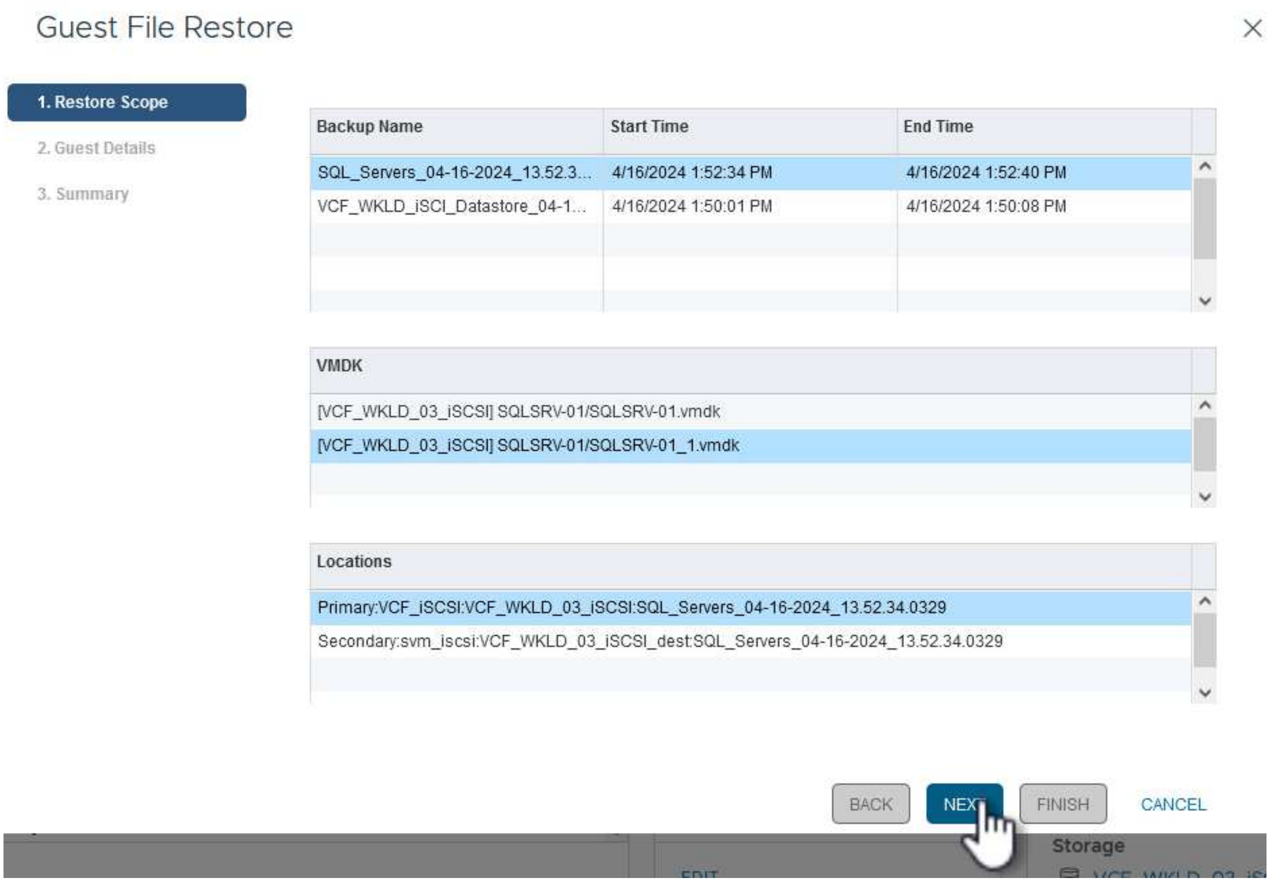
Virtual Machine: SQLSRV-01

○ Search by Virtual Machine name

5. Click on **Save** again in the **Run As Credentials** window to complete saving the record.
6. Next, navigate to a VM in the inventory. From the **Actions** menu, or by right-clicking on the VM, select **SnapCenter Plug-in for VMware vSphere > Guest File Restore**.



7. On the **Restore Scope** page of the **Guest File Restore** wizard, select the backup to restore from, the particular VMDK, and the location (primary or secondary) to restore the VMDK from. Click on **Next** to continue.



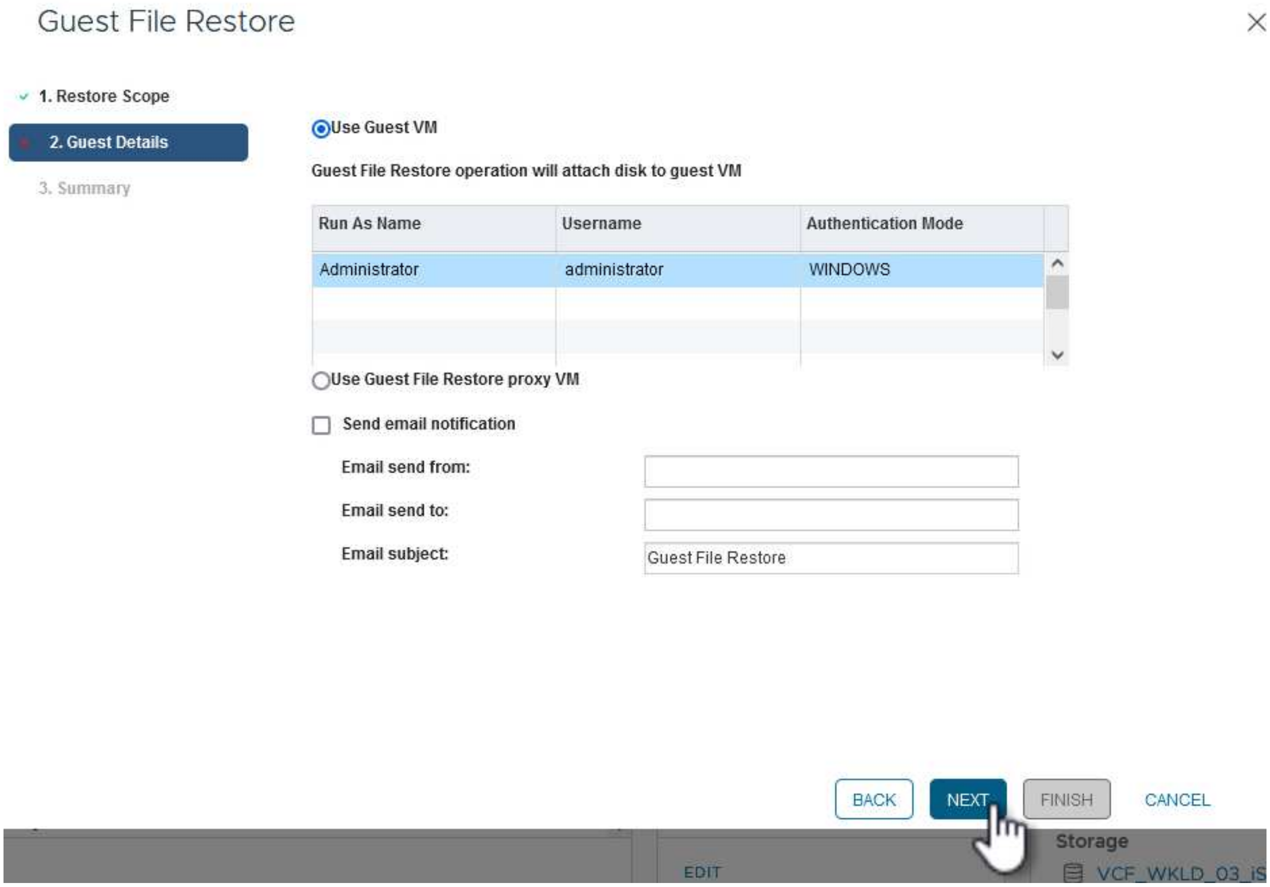
Guest File Restore

Backup Name	Start Time	End Time
SQL_Servers_04-16-2024_13.52.3...	4/16/2024 1:52:34 PM	4/16/2024 1:52:40 PM
VCF_WKLD_iSCI_Datastore_04-1...	4/16/2024 1:50:01 PM	4/16/2024 1:50:08 PM

VMDK
[VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk
[VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.vmdk

Locations
Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:SQL_Servers_04-16-2024_13.52.34.0329
Secondary:svm_iscsi:VCF_WKLD_03_iSCSI_dest:SQL_Servers_04-16-2024_13.52.34.0329

8. On the **Guest Details** page, select to use **Guest VM** or **Use Gues File Restore proxy VM** for the restore. Also, fill out email notification settings here if desired. Click on **Next** to continue.



Guest File Restore

- ✓ 1. Restore Scope
- 2. Guest Details
- 3. Summary

● Use Guest VM

Guest File Restore operation will attach disk to guest VM

Run As Name	Username	Authentication Mode
Administrator	administrator	WINDOWS

○ Use Guest File Restore proxy VM

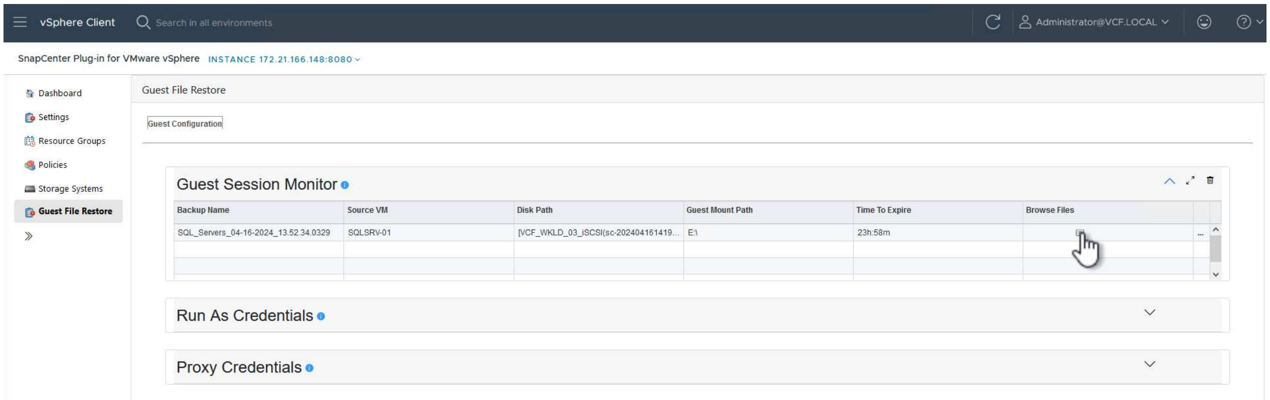
□ Send email notification

Email send from:

Email send to:

Email subject: Guest File Restore

9. Finally, review the **Summary** page and click on **Finish** to begin the Guest File System Restore session.
10. Back in the SnapCenter Plug-in interface, navigate to **Guest File Restore** again and view the running session under **Guest Session Monitor**. Click on the icon under **Browse Files** to continue.



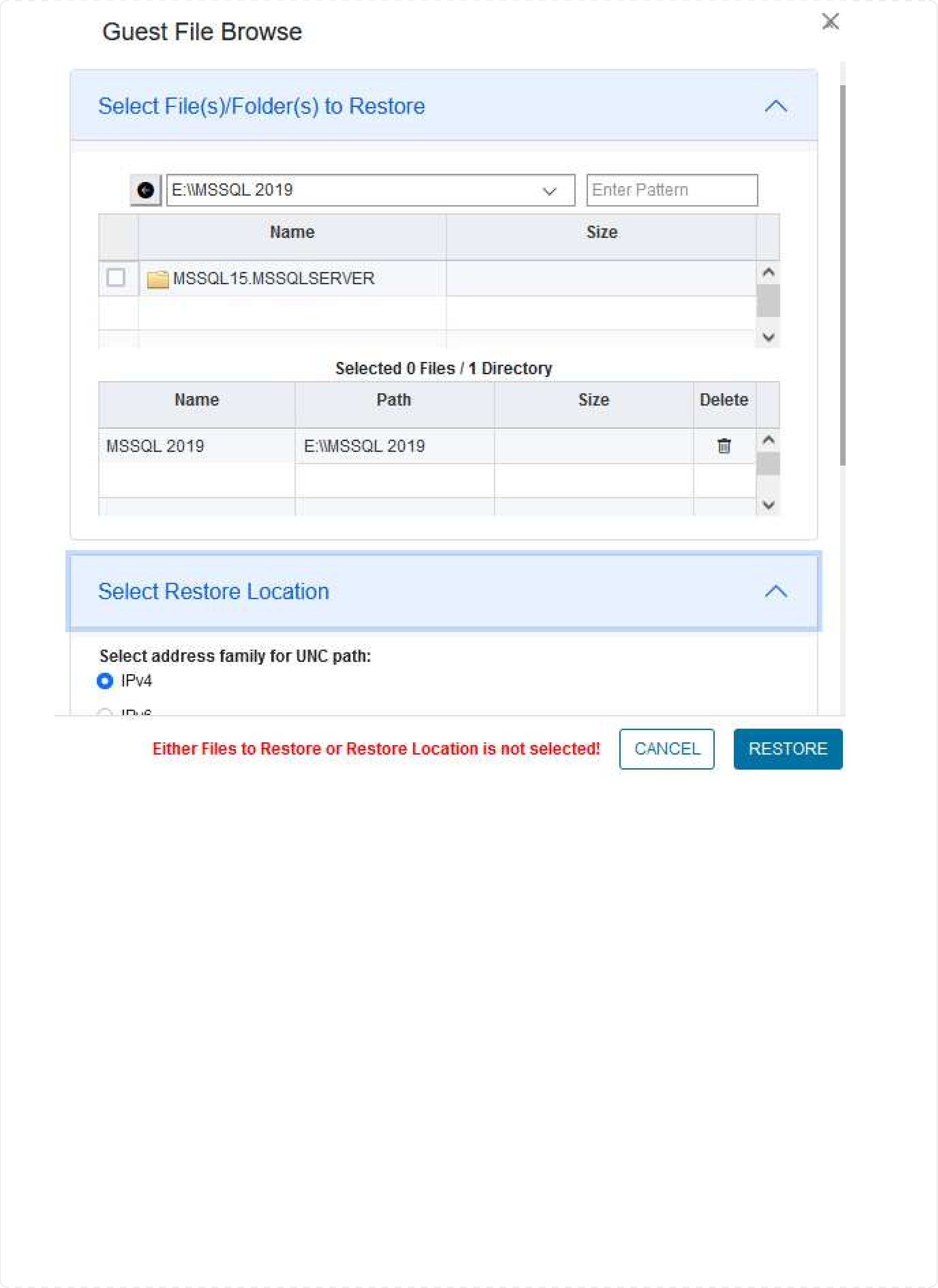
SnapCenter Plug-in for VMware vSphere INSTANCE 172.21.166.148:8080

Guest File Restore

Guest Session Monitor

Backup Name	Source VM	Disk Path	Guest Mount Path	Time To Expire	Browse Files
SQL_Servers_04-16-2024_13.52.34.0329	SQLSRV-01	[VCF_WKLD_03_iSCSI(sc-202404161419...	E:\	23h:58m	

11. In the **Guest File Browse** wizard select the folder or files to restore and the file system location to restore them to. Finally, click on **Restore** to start the **Restore** process.



Guest File Browse

Select File(s)/Folder(s) to Restore

E:\\MSSQL 2019

Enter Pattern

	Name	Size
□	MSSQL15.MSSQLSERVER	

Selected 0 Files / 1 Directory

Name	Path	Size	Delete
MSSQL 2019	E:\\MSSQL 2019		🗑

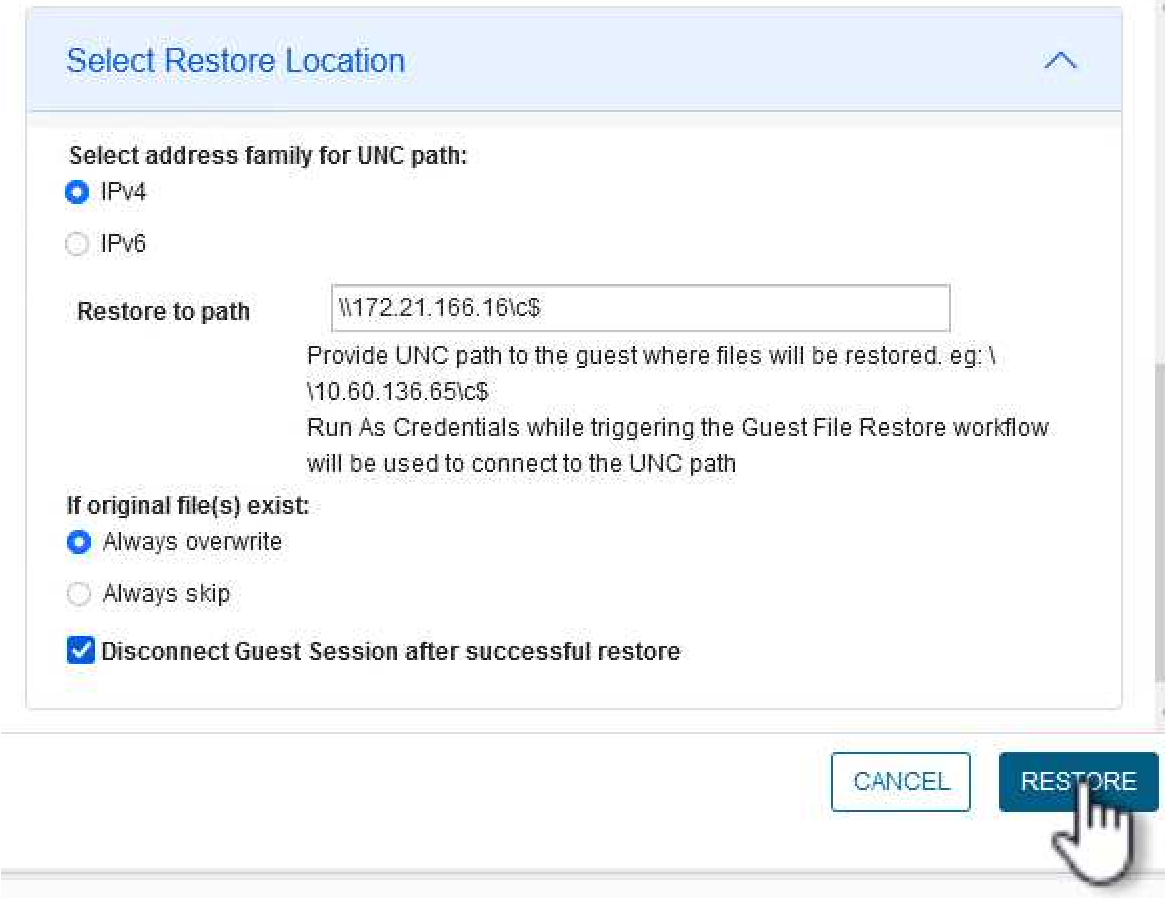
Select Restore Location

Select address family for UNC path:

● IPv4

○ IPv6

Either Files to Restore or Restore Location is not selected!



Select Restore Location

Select address family for UNC path:

● IPv4

○ IPv6

Restore to path: \\172.21.166.16\c$

Provide UNC path to the guest where files will be restored. eg: \\10.60.136.65\c$
Run As Credentials while triggering the Guest File Restore workflow will be used to connect to the UNC path

If original file(s) exist:

● Always overwrite

○ Always skip

☑ Disconnect Guest Session after successful restore

12. The restore job can be monitored from the vSphere Client task pane.

Additional information

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

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

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

Protect a VCF management and workload domains using SnapCenter plug-in for VMware vSphere

Use SnapCenter Plug-in for VMware vSphere to protect multiple VCF domains. This procedure includes setting up the plug-in for each domain, configuring backup policies and performing restore operations.

VMware Cloud Foundation (VCF) workload domains enable organizations to logically separate resources into different domains to group different workloads, enhance security and fault tolerance.

Introduction

Domains can scale independently, meet specific compliances and provide multitenancy. Data Protection for VMware Cloud Foundation (VCF) is a critical aspect to ensure the availability, integrity, and recoverability of data across the management domain and workload domains. NetApp SnapCenter Plug-in for VMware vSphere (SCV) is a powerful tool that integrates NetApp's data protection capabilities into VMware environments. It simplifies backup, restore, and cloning of VMware vSphere virtual machines (VMs) hosted on NetApp storage.

This document provides deployment steps on how to protect VCF multiple domains with SCV.

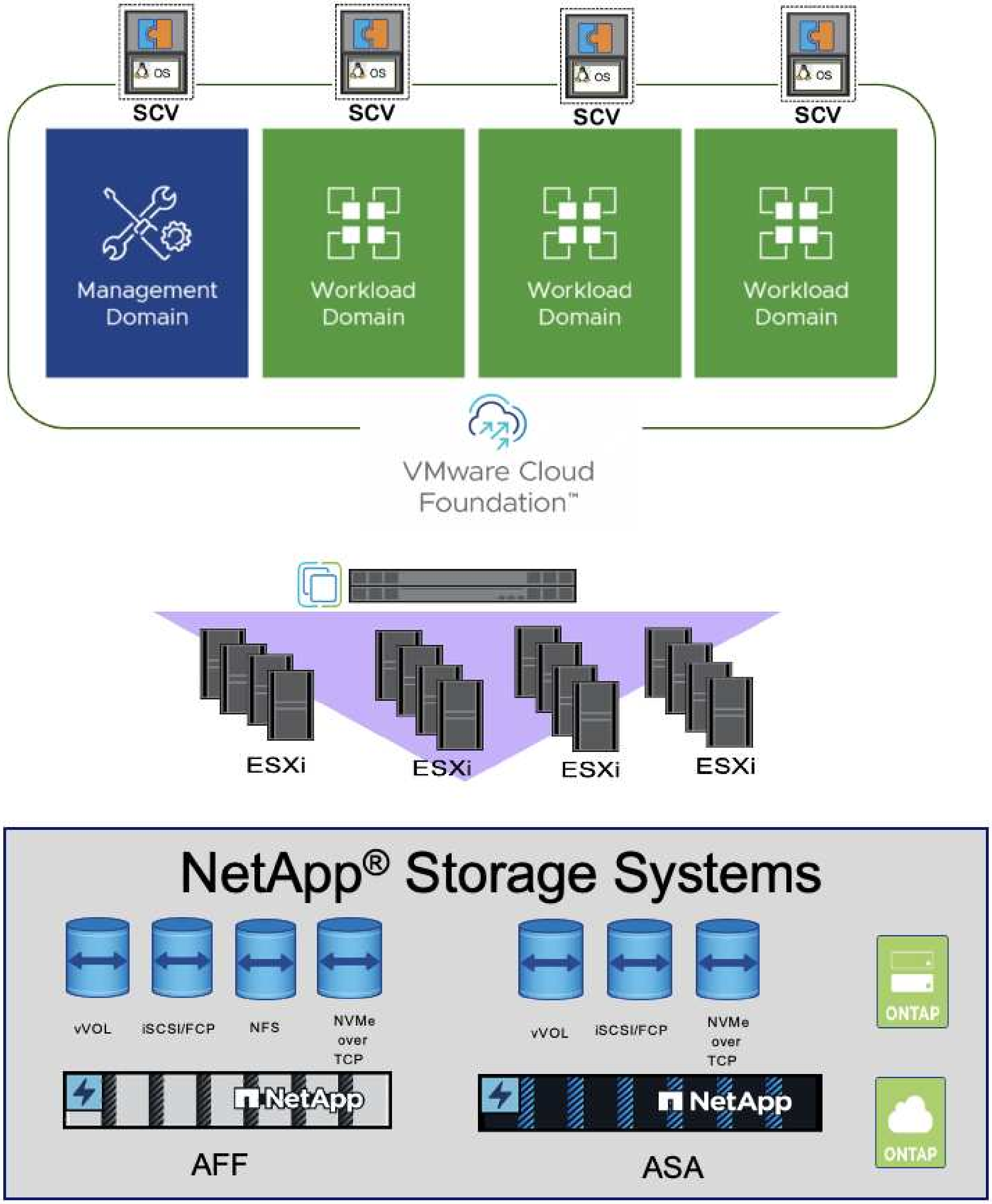
Audience

Solution architects or storage administrators ensuring data protection and disaster recovery for VMware VCF workload domains.

Architecture Overview

SCV is deployed as a Linux virtual appliance using an OVA file to provide fast, space-efficient, crash-consistent, and VM-consistent backup and restore operations for VMs, datastores, and files and folders. SCV uses a remote plug-in architecture. There were multiple SCVs deployed and hosted on VCF management domain vCenter. SCV and VCF domain is one to one relationship thus VCF management domain and each workload domain requires one SCV.

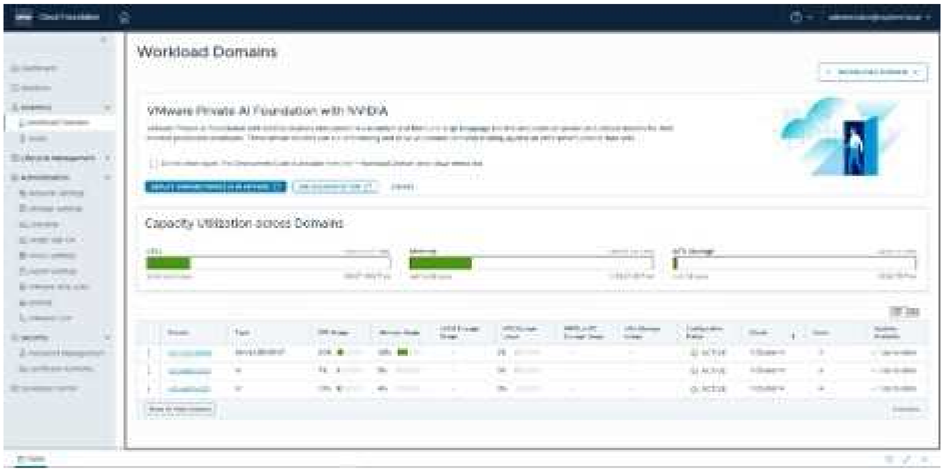
Data that is on ONTAP FAS, AFF, or All SAN Array (ASA) primary systems and replicated to ONTAP FAS, AFF, or ASA secondary systems. SCV also works with SnapCenter Server to support application-based backup and restore operations in VMware environments for SnapCenter application-specific plug-ins. For more information check, SnapCenter Plug-in for VMware vSphere documentation.



The 3-2-1 backup rule is a data protection strategy that involves making three copies of data, storing them on two different types of media, and keeping one copy off-site. NetApp Backup and Recovery is a cloud based tool for data management that provides a single control plane for a wide range of backup and recovery operations across both on-premises and cloud environments. For more details, check NetApp Backup and Recovery Documentation.

Deploy a VCF with Management Domain and Multiple Workload Domains

A VCF workload domain is a group ESXi hosts with one or more vSphere clusters, provisioned by SDDC Manager and application ready. In a VCF example below, one management domain and two workload domains were deployed. For more details on how to deploy VCF with NetApp storage, check NetApp VCF deployment documentation.



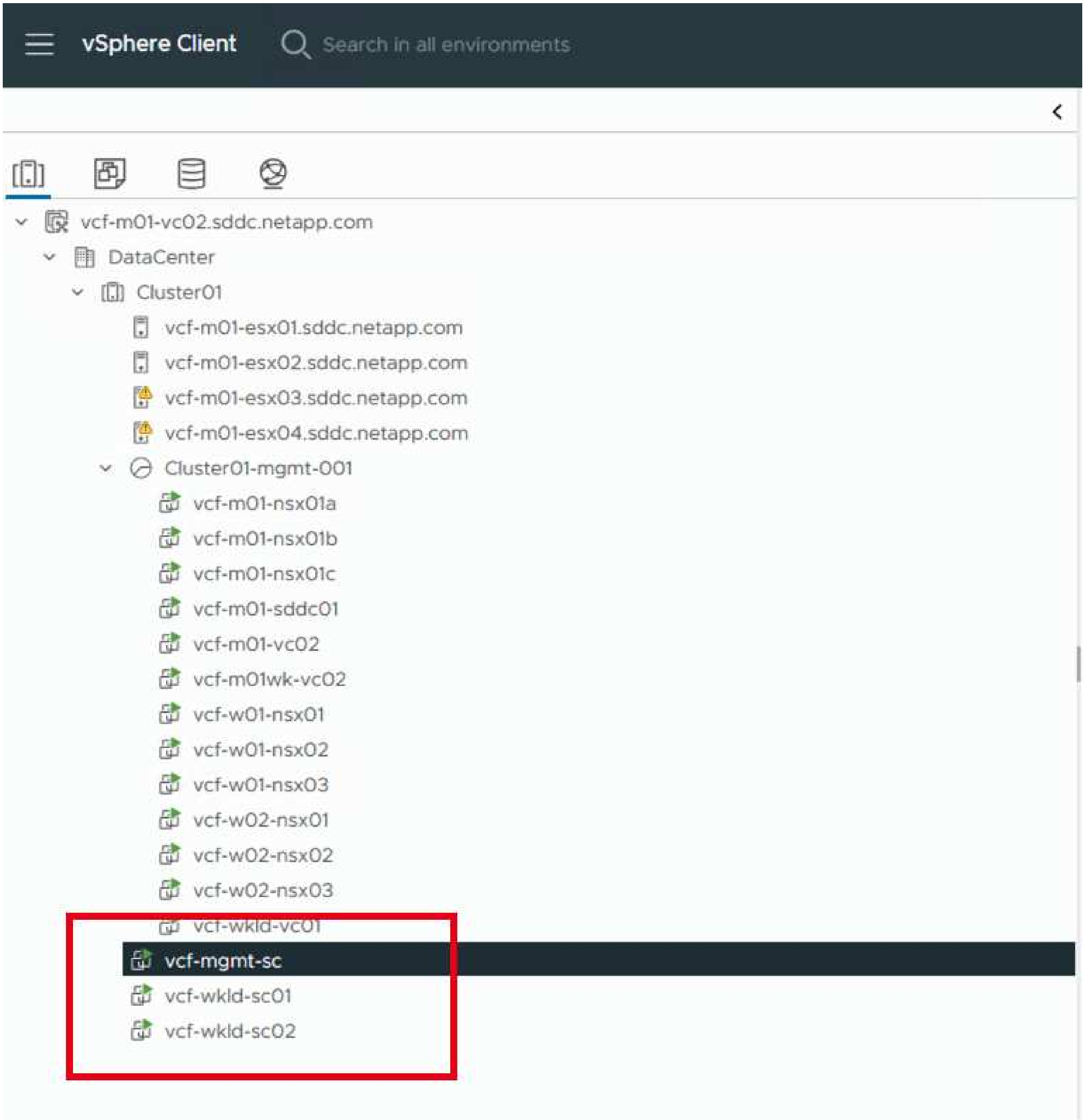
Workload Domains

VMware Private AI Foundation with NVIDIA

Capacity Utilization across Domains

SCV Deployment, Configuration and Restoration Steps

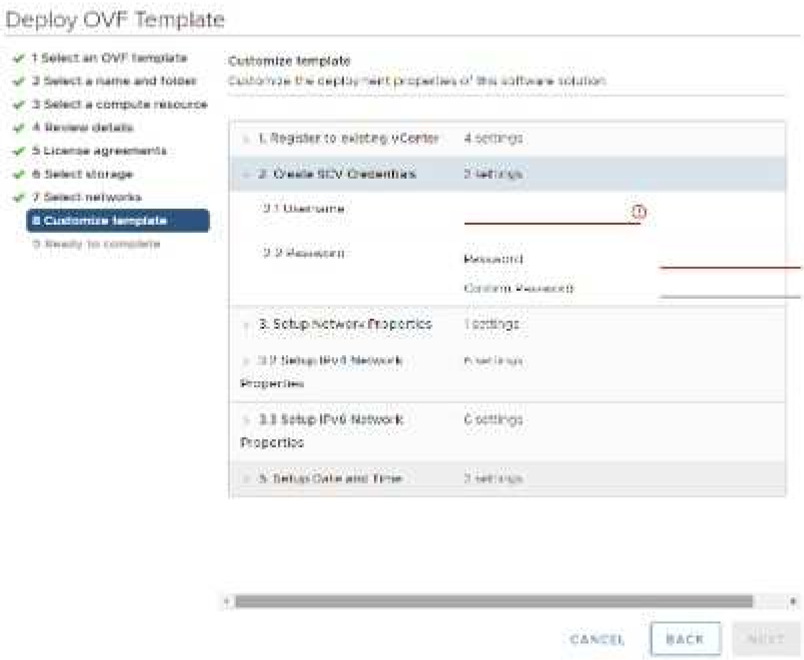
Based the number of workload domains and plus the management domain, multiple SCVs need to be deployed. With two workload domains and one management domain, the example below shows three SCVs are deployed on VCF management domain vCenter.



- vcf-m01-vc02.sddc.netapp.com
  - DataCenter
    - Cluster01
      - vcf-m01-esx01.sddc.netapp.com
      - vcf-m01-esx02.sddc.netapp.com
      - vcf-m01-esx03.sddc.netapp.com
      - vcf-m01-esx04.sddc.netapp.com
      - Cluster01-mgmt-001
        - vcf-m01-nsx01a
        - vcf-m01-nsx01b
        - vcf-m01-nsx01c
        - vcf-m01-sddc01
        - vcf-m01-vc02
        - vcf-m01wk-vc02
        - vcf-w01-nsx01
        - vcf-w01-nsx02
        - vcf-w01-nsx03
        - vcf-w02-nsx01
        - vcf-w02-nsx02
        - vcf-w02-nsx03
        - vcf-wkld-vc01
      - vcf-mgmt-sc
      - vcf-wkld-sc01
      - vcf-wkld-sc02

Deploy SCV for management domain and each workload domain

1. Download the Open Virtual Appliance (OVA).
2. Log in with the vSphere Client to the vCenter Server. Navigate to Administration > Certificates > Certificate Management. Add Trusted Root Certificates and install each certificate in the certs folder. Once the certificates are installed, OVA can be verified and deployed.
3. Log in to the VCF workload domain vCenter and deploy OVF Template to start the VMware deploy wizard.



Deploy OVF Template

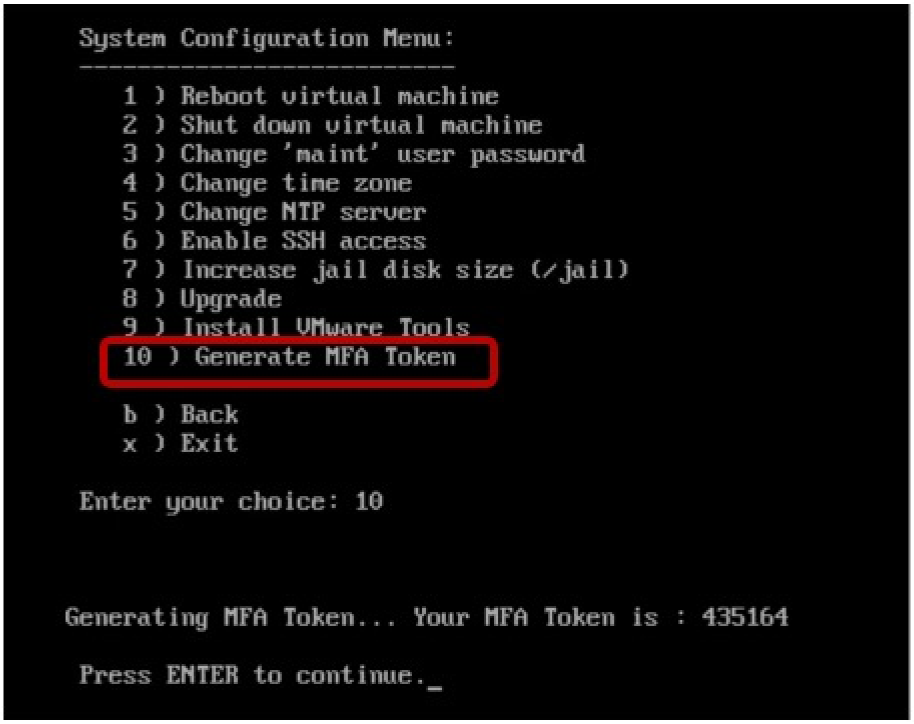
- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Select storage
- ✓ 7 Select networks
- 8 Customize template
- 9 Ready to complete

Customize template

Customize the deployment properties of this software solution.

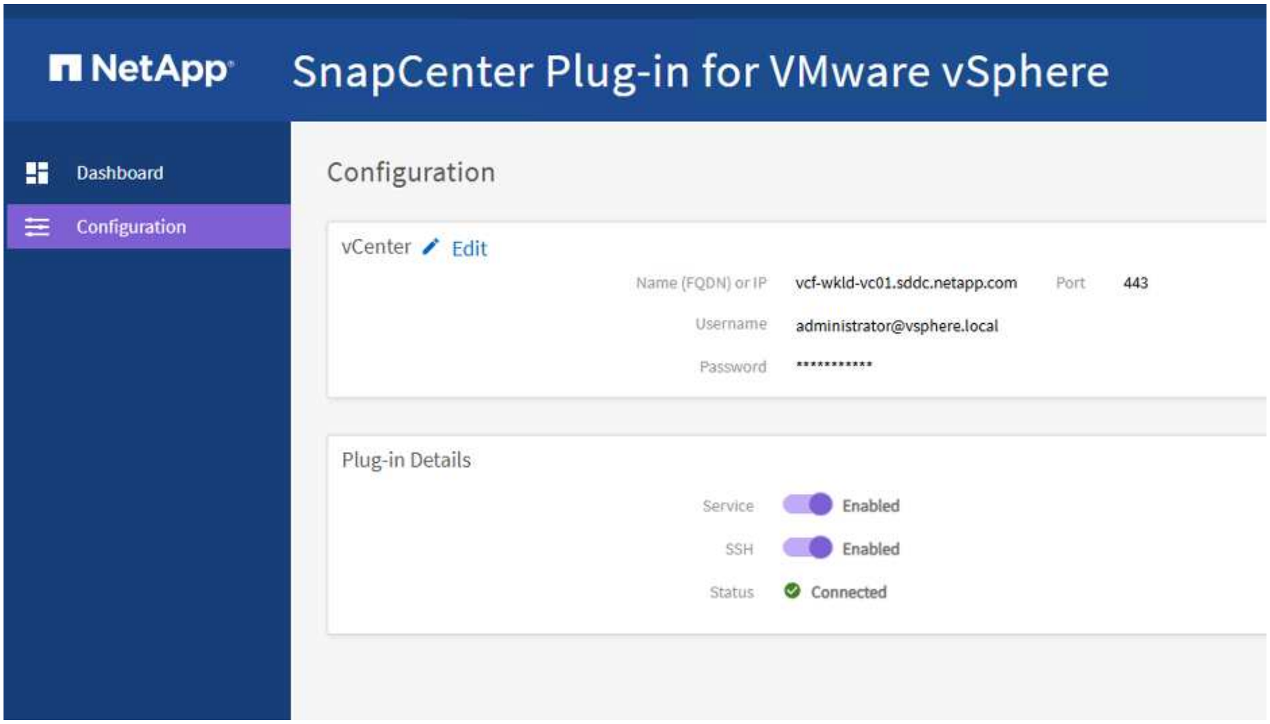
1. Register to existing vCenter	4 settings
2. Create SCV Credentials	2 settings
2.1 Username	
2.2 Password	Password Confirm Password
3. Setup Network Properties	1 settings
3.2 Setup IPv4 Network Properties	6 settings
3.3 Setup IPv6 Network Properties	6 settings
5. Setup Date and Time	2 settings

4. Power on OVA to start SCV and then click Install VMware tools.
5. Generate the MFA token from the OVA console, system configuration menu.



```
System Configuration Menu:
--------------------------
   1 ) Reboot virtual machine
   2 ) Shut down virtual machine
   3 ) Change 'maint' user password
   4 ) Change time zone
   5 ) Change NTP server
   6 ) Enable SSH access
   7 ) Increase jail disk size (/jail)
   8 ) Upgrade
   9 ) Install VMware Tools
   10 ) Generate MFA Token

   b ) Back
   x ) Exit

Enter your choice: 10


Generating MFA Token... Your MFA Token is : 435164

Press ENTER to continue._
```

6. Log in to the SCV management GUI with the admin username and password set at the time of deployment and the MFA token generated using the maintenance console. `https://<appliance-IP-address>:8080` to access the management GUI.



Configuration

vCenter Edit

Name (FQDN) or IP: vcf-wkld-vc01.sddc.netapp.com Port: 443

Username: administrator@vsphere.local

Password: ***********

Plug-in Details

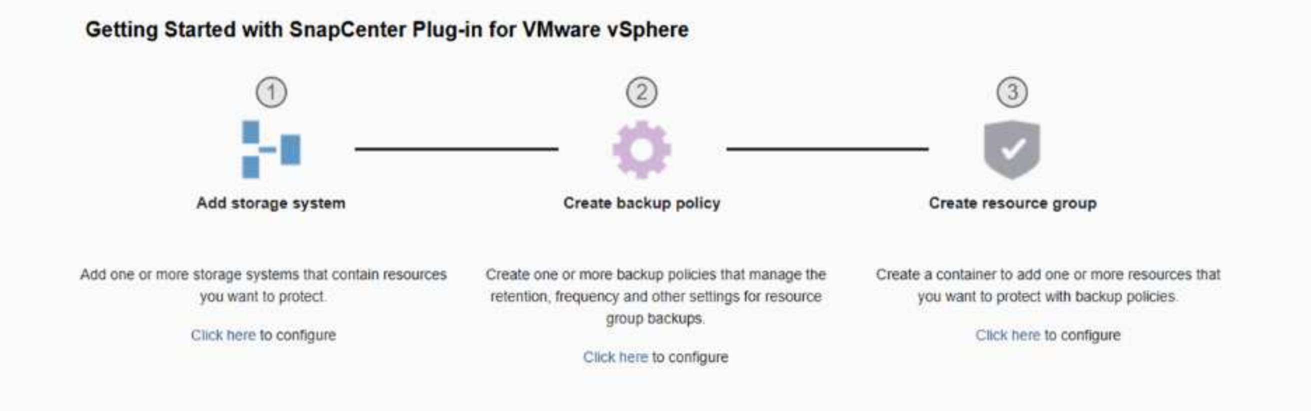
Service: Enabled

SSH: Enabled

Status: ✓ Connected

Configure SCV

To backup or restore VMs, first add the storage clusters or VMs hosting the datastores,then create backup policies for retention and frequency, and set up a resource group to protect the resources.



Getting Started with SnapCenter Plug-in for VMware vSphere

1 Add storage system

Add one or more storage systems that contain resources you want to protect.

Click here to configure

2 Create backup policy

Create one or more backup policies that manage the retention, frequency and other settings for resource group backups.

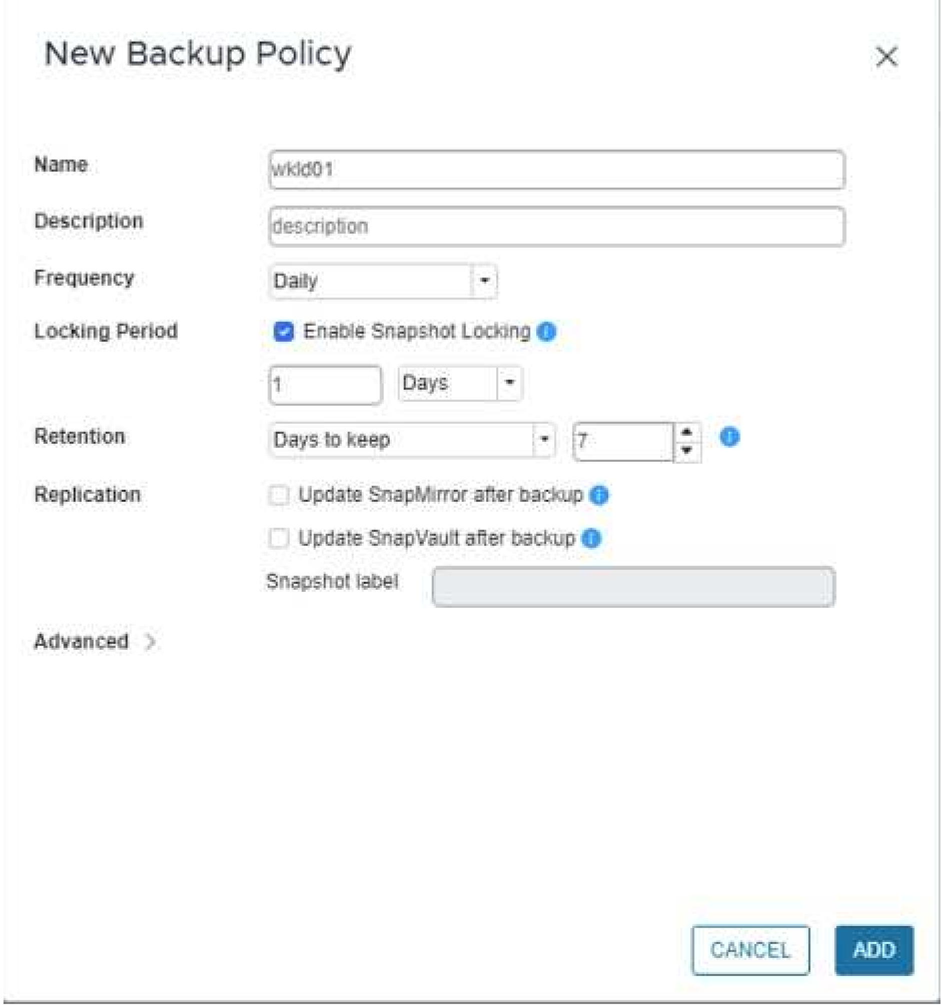
Click here to configure

3 Create resource group

Create a container to add one or more resources that you want to protect with backup policies.

Click here to configure

1. Log in to vCenter web client and click Menu in the toolbar and select SnapCenter Plug-in for VMware vSphere and Add a storage. In the left navigator pane of the SCV plug-in, click Storage Systems and then select Add option. On the Add Storage System dialog box, enter the basic SVM or cluster information, and select Add. Enter NetApp storage IP address and login.
2. To create a new backup policy, in the left navigator pane of the SCV plug-in, click Policies, and select New Policy. On the New Backup Policy page, enter the policy configuration information, and click Add.



New Backup Policy

Name: wkld01

Description: description

Frequency: Daily

Locking Period: ☑ Enable Snapshot Locking

1 Days

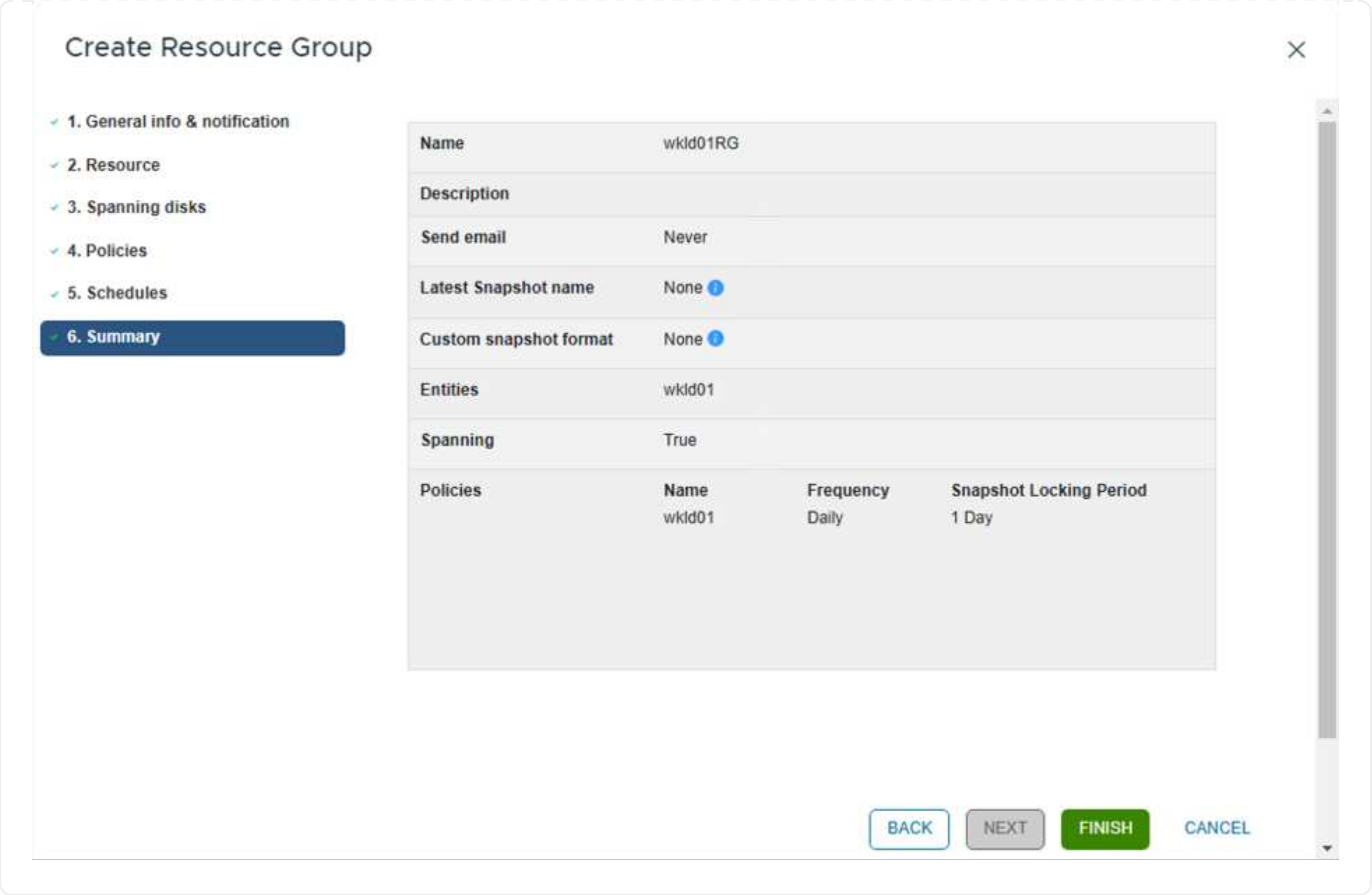
Retention: Days to keep 7

Replication: □ Update SnapMirror after backup

□ Update SnapVault after backup

Snapshot label

3. In the left navigator pane of the SCV plug-in, click Resource Groups, and then select Create. Enter the required information on each page of the Create Resource Group wizard, select VMs and datastores to be included in the resource group, and then select the backup policies to be applied to the resource group and specify the backup schedule.



Create Resource Group

Name	wkld01RG
Description	
Send email	Never
Latest Snapshot name	None
Custom snapshot format	None
Entities	wkld01
Spanning	True

Policies

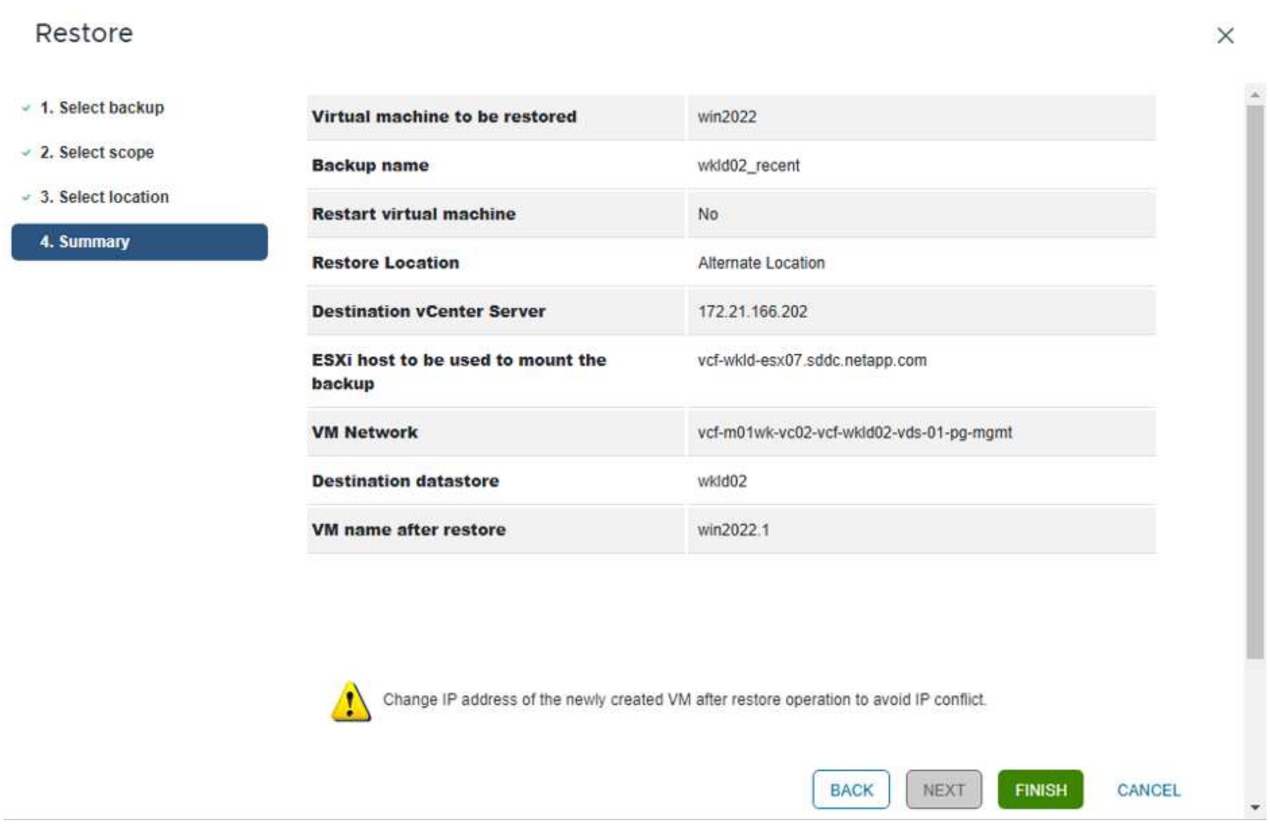
Name	Frequency	Snapshot Locking Period
wkld01	Daily	1 Day

Restore VM and files or folders backup

VMs, VMDKs, files, and folders from backups can be restored. VM can be restored to the original host or an alternate host in the same vCenter Server, or to an alternate ESXi host managed by the same vCenter. You can mount a traditional datastore from a backup if you want to access files in the backup. You can either mount the backup to the same ESXi host where the backup was created or to an alternate ESXi host that has the same type of VM and host configurations. You can mount a datastore multiple times on a host. Individual files and folders can also be restored in a guest file restore session, which attaches a backup copy of a virtual disk and then restores the selected files or folders. Files and folders can also be restored.

VM Restore Steps

1. In the VMware vSphere client GUI, click Menu in the toolbar and select VMs and Templates from the drop-down list, right click a VM, and select SnapCenter Plug-in for VMware vSphere in the drop-down list, and then select Restore in the secondary drop-down list to start the wizard.
2. In the Restore wizard, select the backup Snapshot that you want to restore and select Entire virtual machine in the Restore scope field, select the restore location, and then enter the destination information where the backup should be mounted. On the Select Location page, select the location for the restored datastore. Review the Summary page and click Finish.



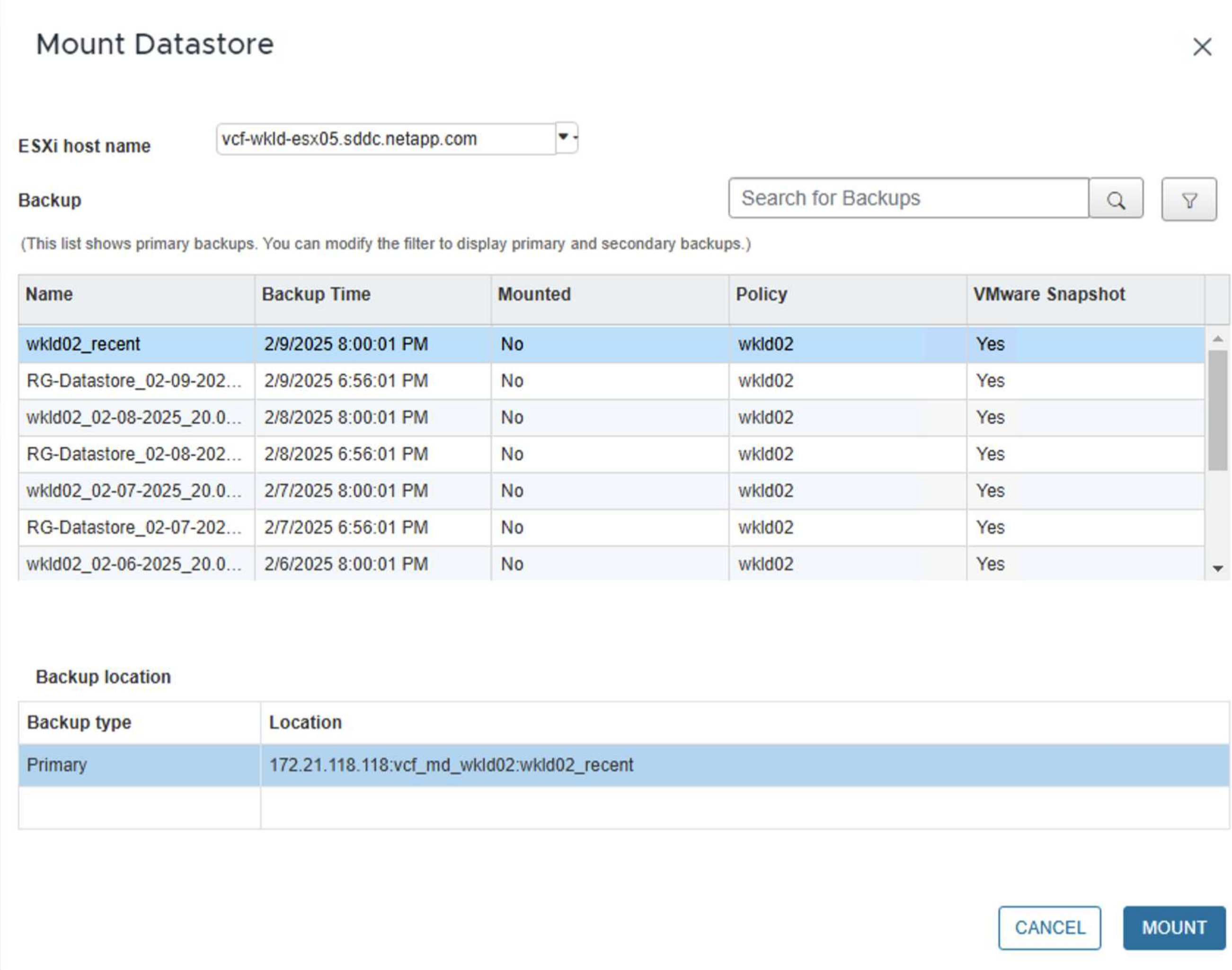
Virtual machine to be restored	win2022
Backup name	wkld02_recent
Restart virtual machine	No
Restore Location	Alternate Location
Destination vCenter Server	172.21.166.202
ESXi host to be used to mount the backup	vcf-wkld-esx07.sddc.netapp.com
VM Network	vcf-m01wk-vc02-vcf-wkld02-vds-01-pg-mgmt
Destination datastore	wkld02
VM name after restore	win2022.1

Change IP address of the newly created VM after restore operation to avoid IP conflict.

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

Datastore Restore Steps

1. Right-click a datastore and select SnapCenter Plug-in for VMware vSphere > Mount Backup.
2. On the Mount Datastore page, select a backup and a backup location (primary or secondary), and then click Mount.



Mount Datastore

ESXi host name: vcf-wkld-esx05.sddc.netapp.com

Backup

(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

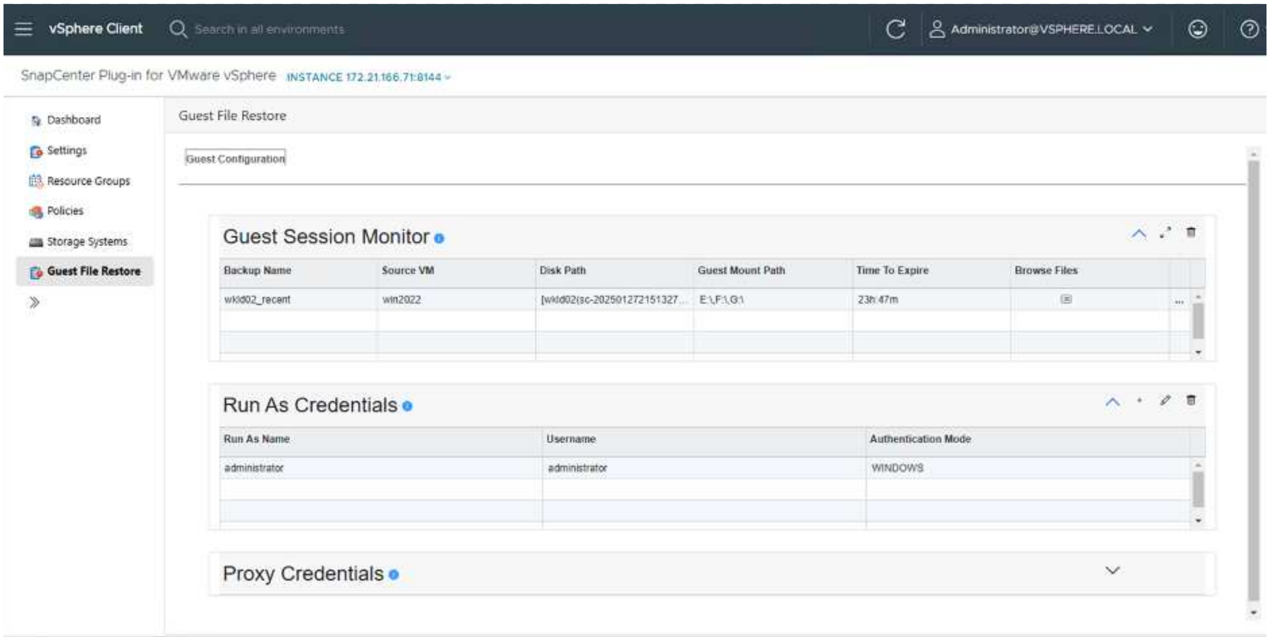
Name	Backup Time	Mounted	Policy	VMware Snapshot
wkld02_recent	2/9/2025 8:00:01 PM	No	wkld02	Yes
RG-Datastore_02-09-202...	2/9/2025 6:56:01 PM	No	wkld02	Yes
wkld02_02-08-2025_20.0...	2/8/2025 8:00:01 PM	No	wkld02	Yes
RG-Datastore_02-08-202...	2/8/2025 6:56:01 PM	No	wkld02	Yes
wkld02_02-07-2025_20.0...	2/7/2025 8:00:01 PM	No	wkld02	Yes
RG-Datastore_02-07-202...	2/7/2025 6:56:01 PM	No	wkld02	Yes
wkld02_02-06-2025_20.0...	2/6/2025 8:00:01 PM	No	wkld02	Yes

Backup location

Backup type	Location
Primary	172.21.118.118:vcf_md_wkld02:wkld02_recent

Files and Folders Restore Steps

1. When you a virtual attach disk for guest file or folder restore operations, the target VM for the attach must have credentials configured before you restore. From SnapCenter Plug-in for VMware vSphere under plug-ins, select Guest File Restore and Run As Credentials section, enter the User credentials. For Username, you must enter "Administrator".



vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
SnapCenter Plug-in for VMware vSphere
INSTANCE 172.21.166.71:8144
Dashboard
Settings
Resource Groups
Policies
Storage Systems
Guest File Restore
Guest Configuration

Guest File Restore

Guest Session Monitor

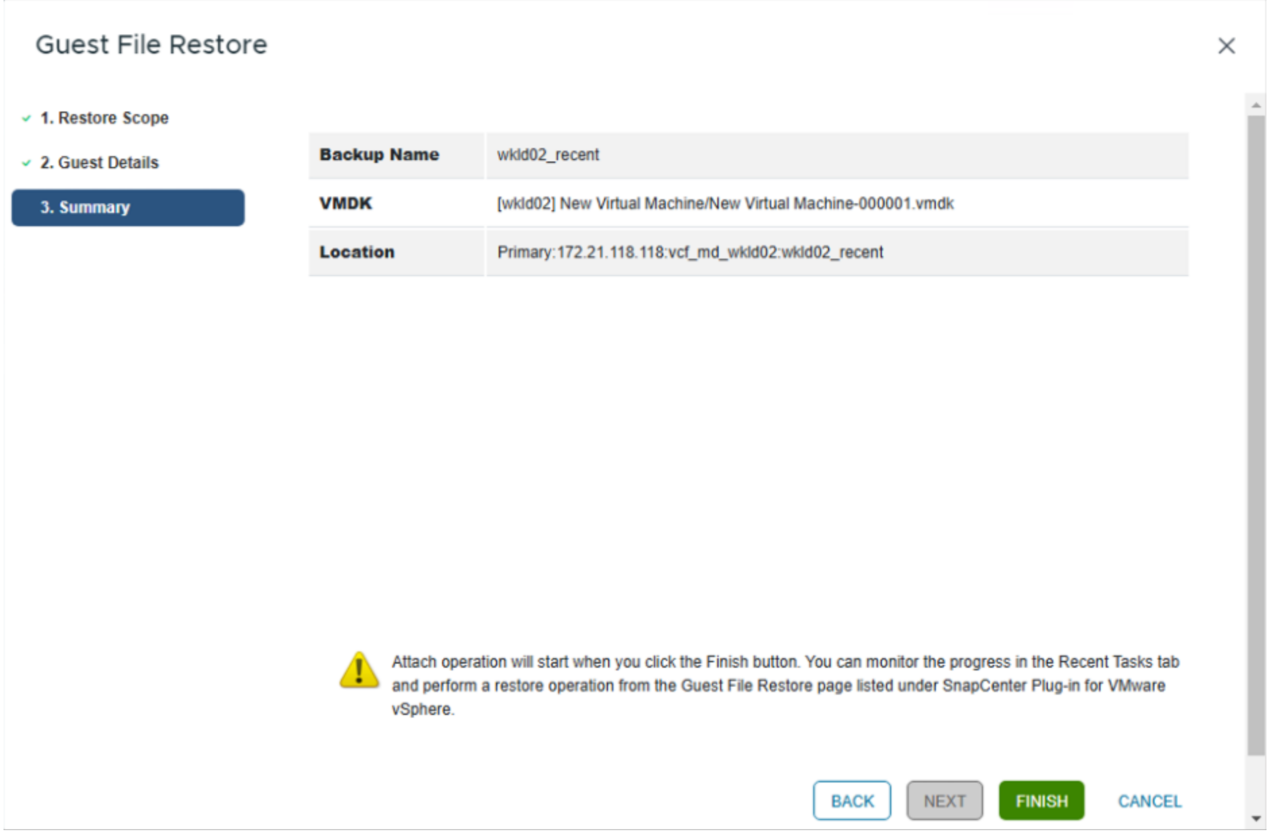
Backup Name	Source VM	Disk Path	Guest Mount Path	Time To Expire	Browse Files
wkld02_recent	win2022	[wkld02(sc-202501272151327...	E:\,F:\,G:\	23h:47m	

Run As Credentials

Run As Name	Username	Authentication Mode
administrator	administrator	WINDOWS

Proxy Credentials

2. Right-click on the VM from the vSphere client and select SnapCenter Plug-in for VMware vSphere > Guest File Restore. On the Restore Scope page, specify Backup Name, VMDK virtual disk and Location – primary or secondary. Click Summery to confirm.



Guest File Restore

Backup Name	wkld02_recent
VMDK	[wkld02] New Virtual Machine/New Virtual Machine-000001.vmdk
Location	Primary:172.21.118.118:vcf_md_wkld02:wkld02_recent

Attach operation will start when you click the Finish button. You can monitor the progress in the Recent Tasks tab and perform a restore operation from the Guest File Restore page listed under SnapCenter Plug-in for VMware vSphere.

NetApp SnapCenter for VCP multi-domain centralizes data protection, efficiently reduces the time and storage space required for backups using NetApp snapshots, supports large-scale VMware environments with robust backup and replication features and allows granular recovery of entire VMs, specific VMDKs, or individual files.

Video Demo for Protect VCF Multiple Domains with SCV

Protect VMware VCF multiple domains with NetApp SCV

Protect VCF workload domains with NVMe over TCP storage and SnapCenter plug-in for VMware vSphere

Use SnapCenter Plug-in for VMware vSphere to protect VCF workload domains with NVMe. This procedure includes setting up the plug-in, configuring NVMe over TCP for optimal performance, and performing backup, restore, or cloning operations.

NVMe (Non-Volatile Memory Express) over TCP is a cutting-edge network protocol that facilitates high-speed data transfer between VMware Cloud Foundation ESXi servers and NetApp storage, including All Flash FAS (AFF) and All SAN Array (ASA).

Introduction

Leveraging NVMe over TCP provides low latency and high throughput for demanding workloads. The integration of NVMe over TCP with NetApp SnapCenter Plug-in for VMware vSphere (SCV) offers a powerful combination for efficient data management, enhancing backup, restore, and cloning operations within VMware environments.

Benefits of NVMe over TCP

- High Performance: Delivers exceptional performance with low latency and high data transfer rates. This is crucial for demanding applications and large-scale data operations.
- Scalability: Supports scalable configurations, allowing IT administrators to expand their infrastructure seamlessly as data requirements grow.
- Efficiency: Enables faster backup and restore operations, reducing downtime and improving overall system availability.

This document provides steps on deploying and managing SCV in VMware Cloud Foundation (VCF) environments, with a focus on leveraging NVMe over TCP for optimal performance.

Audience

Solution architects or storage administrators ensuring data protection and disaster recovery for VMware VCF workload domains.

Architecture overview

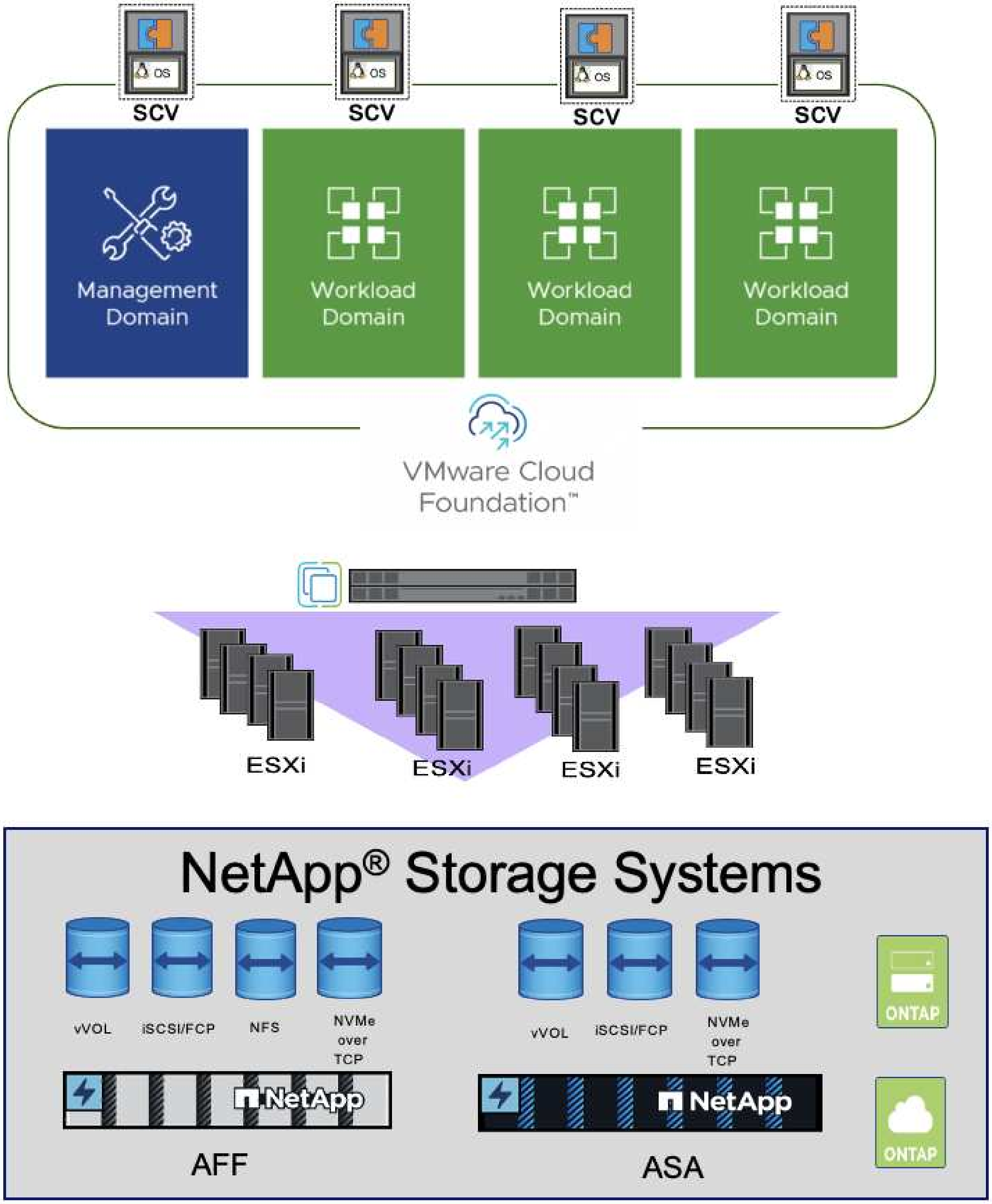
SCV is a powerful tool designed to facilitate fast, space-efficient, crash-consistent, and VM-consistent backup and restore operations for VMs, datastores, and files and folders in VMware environments. SCV is deployed as a Linux virtual appliance using an OVA file and leverages a remote plug-in architecture.

SCV deployment architecture

- Virtual Appliance Deployment: SCV is deployed as a Linux virtual appliance using an OVA file. This deployment method ensures a streamlined and efficient setup process.
- Remote Plug-in Architecture: SCV uses a remote plug-in architecture, allowing for scalability and flexibility in managing multiple instances.
- One-to-One Relationship: Each VCF domain requires a dedicated SCV instance, ensuring isolated and

efficient backup and restore operations.

With ONTAP 9.10.1 and later versions, NetApp AFF and ASA support NVMe over TCP. Data that is on AFF, or ASA primary systems and can replicate to ONTAP AFF, or ASA secondary systems. SCV also works with SnapCenter Server to support application-based backup and restore operations in VMware environments for SnapCenter application-specific plug-ins. For more information check, SnapCenter Plug-in for VMware vSphere documentation and Protect Workloads with SnapCenter



The 3-2-1 backup rule is a data protection strategy that involves making three copies of data, storing them on two different types of media, and keeping one copy off-site. NetApp Backup and Recovery is a cloud based tool for data management that provides a single control plane for a wide range of backup and recovery operations across both on-premises and cloud environments. For more details, check NetApp Backup and Recovery Documentation.

SCV for VCF on NVMe deployment steps

The ONTAP tools for VMware vSphere (OTV) provides a powerful and efficient solution for managing NetApp storage in VMware environments. By integrating directly with the vCenter Server, OTV simplifies storage management, enhances data protection, and optimizes performance. While optional, deploying OTV can significantly improve the management capabilities and overall efficiency of VMware environments.

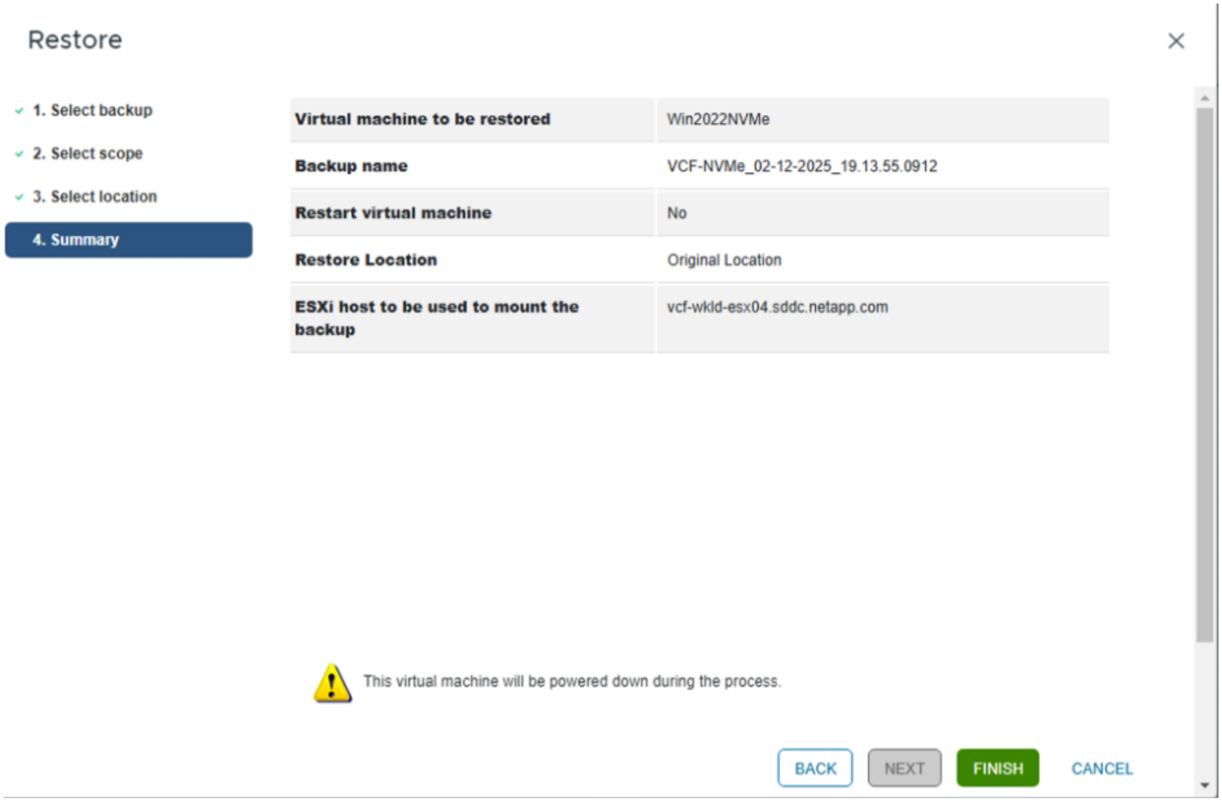
- Create a NVMe/TCP storage for VCF workload domains
- Configure NetApp SnapCenter for VMware vSphere (SCV)

Restore VM, datastore, virtual disk and files or folders

SCV provides comprehensive backup and restore capabilities for VMware environments. For VMFS environments, SCV uses clone and mount operations in conjunction with Storage VMotion to perform restore operations. This ensures efficient and seamless restoration of data. For more details check how the restore operations are performed.

- VM restore
  You can restore the VM to its original host within the same vCenter Server or to an alternate ESXi host managed by the same vCenter Server.

  1. Right click a VM and select SnapCenter Plug-in for VMware vSphere in the drop-down list, and then select Restore in the secondary drop-down list to start the wizard.
  2. In the Restore wizard, select the backup Snapshot that you want to restore and select Entire virtual machine in the Restore scope field, select the restore location, and then enter the destination information where the backup should be mounted. On the Select Location page, select the location for the restored datastore. Review the Summary page and click Finish.

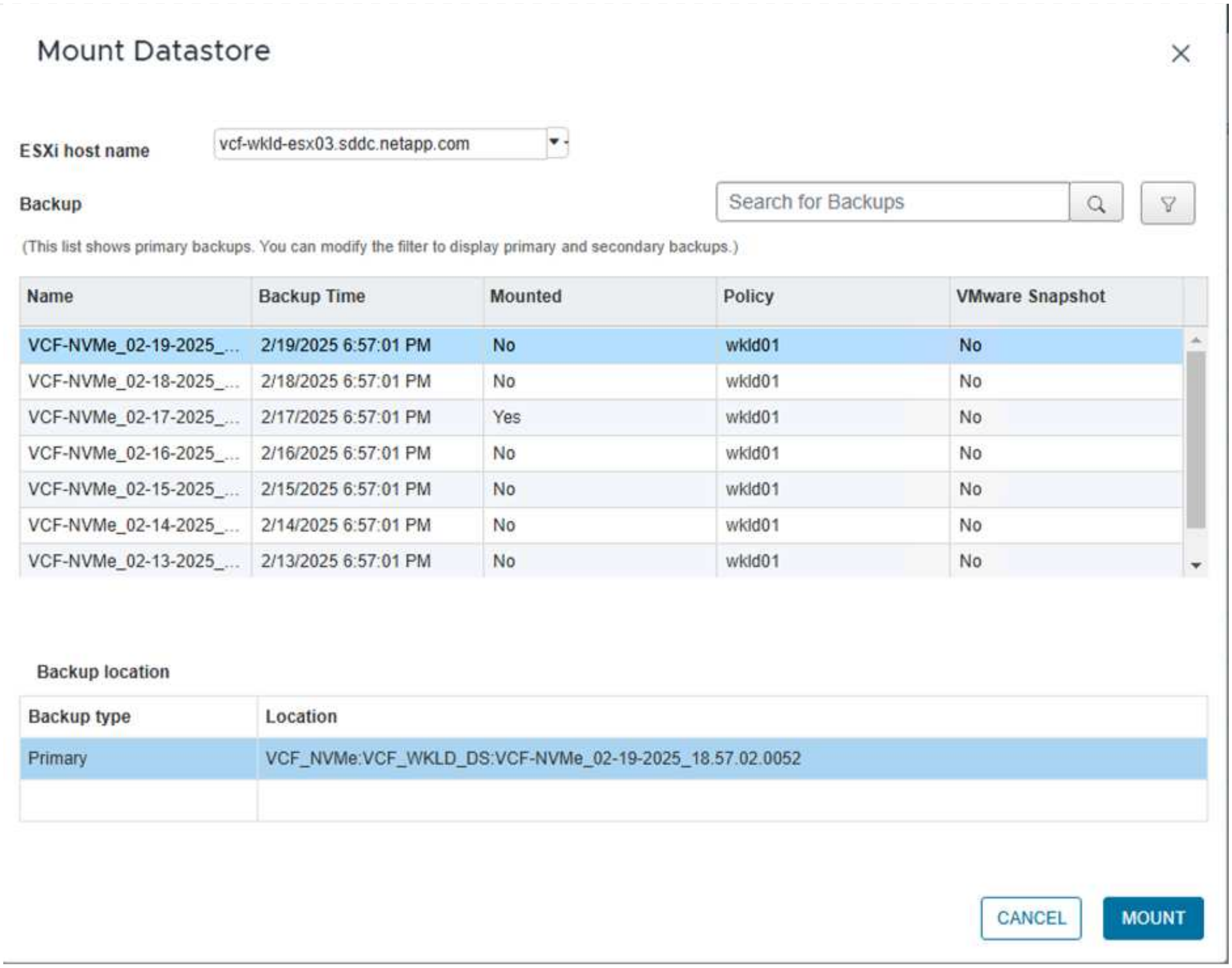


Virtual machine to be restored	Win2022NVMe
Backup name	VCF-NVMe_02-12-2025_19.13.55.0912
Restart virtual machine	No
Restore Location	Original Location
ESXi host to be used to mount the backup	vcf-wkld-esx04.sddc.netapp.com

This virtual machine will be powered down during the process.

- Mount a datastore
  You can mount a traditional datastore from a backup if you want to access files in the backup. You can either mount the backup to the same ESXi host where the backup was created or to an alternate ESXi host that has the same type of VM and host configurations. You can mount a datastore multiple times on a host.

  1. Right-click a datastore and select select SnapCenter Plug-in for VMware vSphere > Mount Backup.
  2. On the Mount Datastore page, select a backup and a backup location (primary or secondary), and then click Mount.



Mount Datastore

ESXi host name: vcf-wkld-esx03.sddc.netapp.com

Backup

(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

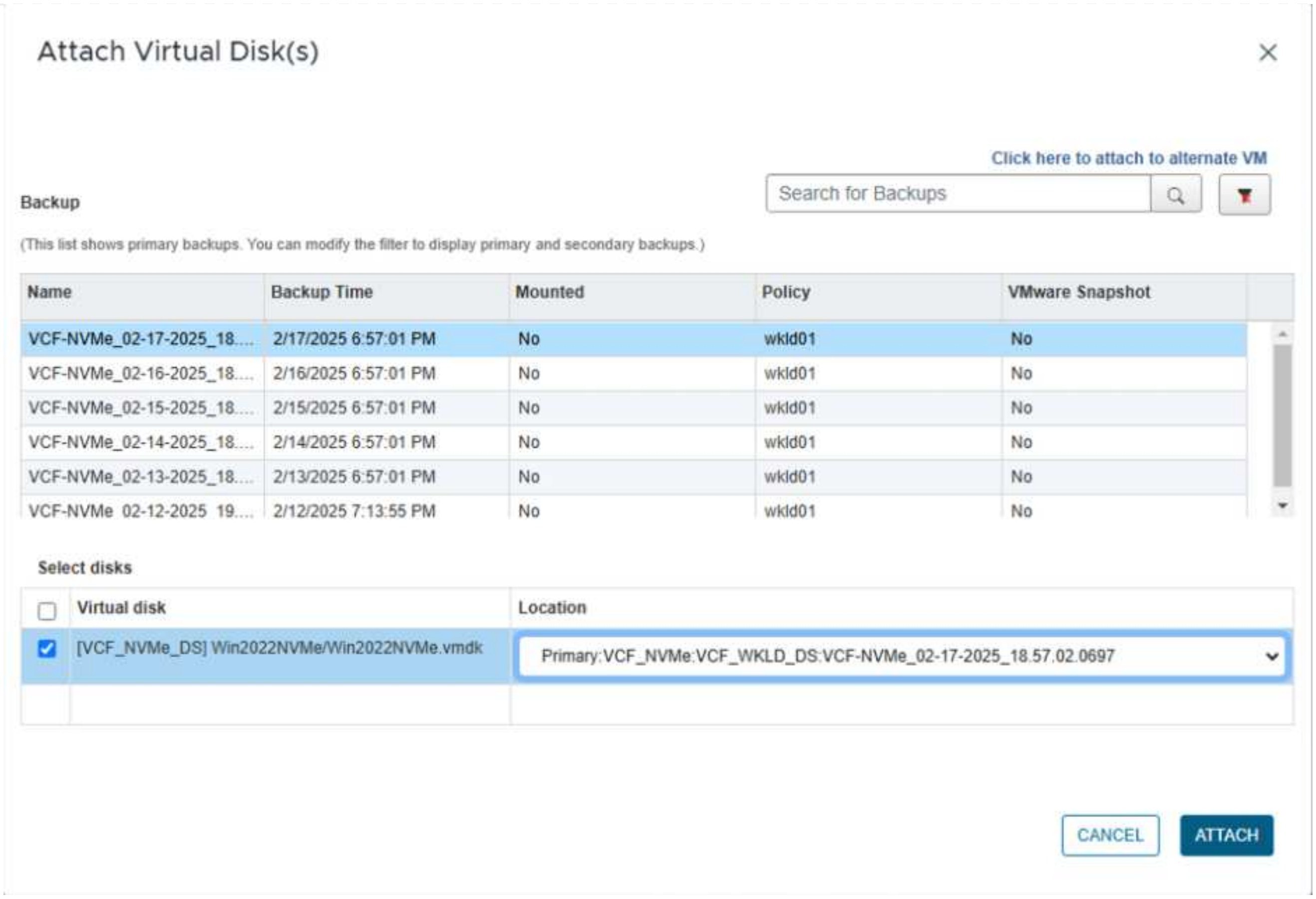
Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF-NVMe_02-19-2025_...	2/19/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-18-2025_...	2/18/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-17-2025_...	2/17/2025 6:57:01 PM	Yes	wkld01	No
VCF-NVMe_02-16-2025_...	2/16/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-15-2025_...	2/15/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-14-2025_...	2/14/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-13-2025_...	2/13/2025 6:57:01 PM	No	wkld01	No

Backup location

Backup type	Location
Primary	VCF_NVMe:VCF_WKLD_DS:VCF-NVMe_02-19-2025_18.57.02.0052

- Attach a virtual disk
  You can attach one or more VMDKs from a backup to the parent VM, or to an alternate VM on the same ESXi host, or to an alternate VM on an alternate ESXi host managed by the same vCenter or a different vCenter in linked mode.

  1. Right click a VM, select SnapCenter Plug-in for VMware vSphere > Attach virtual disk(s).
  2. On the Attach Virtual Disk window, select a backup and select one or more disks you want to attach and the location you want to attach from (primary or secondary). By default, the selected virtual disks are attached to the parent VM. To attach the selected virtual disks to an alternate VM in the same ESXi host, select Click here to attach to alternate VM and specify the alternate VM. Click Attach.



Attach Virtual Disk(s)

Click here to attach to alternate VM

Backup

Search for Backups

(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

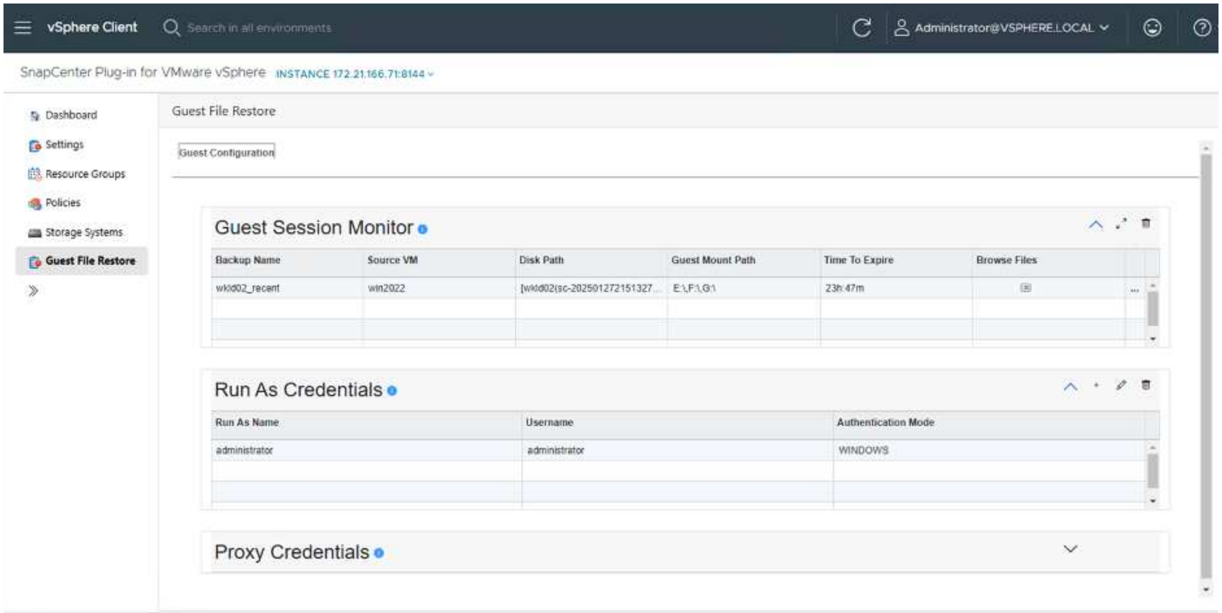
Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF-NVMe_02-17-2025_18....	2/17/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-16-2025_18....	2/16/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-15-2025_18....	2/15/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-14-2025_18....	2/14/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-13-2025_18....	2/13/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-12-2025_19....	2/12/2025 7:13:55 PM	No	wkld01	No

Select disks

□	Virtual disk	Location
☑	[VCF_NVMe_DS] Win2022NVMe/Win2022NVMe.vmdk	Primary:VCF_NVMe:VCF_WKLD_DS:VCF-NVMe_02-17-2025_18.57.02.0697

- Files and folders restore steps
  Individual files and folders can be restored in a guest file restore session, which attaches a backup copy of a virtual disk and then restores the selected files or folders. Files and folders can also be restored. More details check SnapCenter file and folder restore.

  1. When you a virtual attach disk for guest file or folder restore operations, the target VM for the attach must have credentials configured before you restore. From SnapCenter Plug-in for VMware vSphere under plug-ins, select Guest File Restore and Run As Credentials section, enter the User credentials. For Username, you must enter "Administrator".



vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
SnapCenter Plug-in for VMware vSphere
INSTANCE 172.21.166.71:8144
Dashboard
Settings
Resource Groups
Policies
Storage Systems
Guest File Restore
Guest Configuration

Guest File Restore

Guest Session Monitor

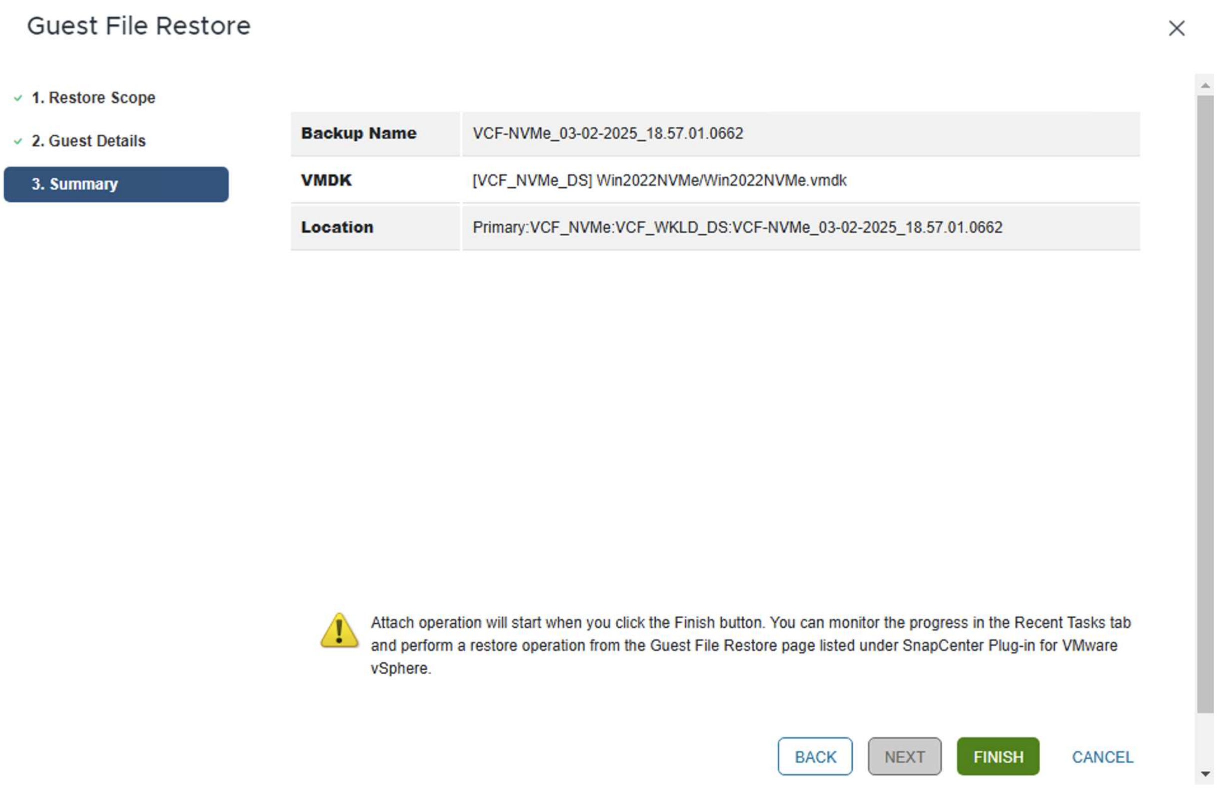
Backup Name	Source VM	Disk Path	Guest Mount Path	Time To Expire	Browse Files
wkld02_recent	win2022	[wkld02(sc-202501272151327...	E:\,F:\,G:\	23h:47m	

Run As Credentials

Run As Name	Username	Authentication Mode
administrator	administrator	WINDOWS

Proxy Credentials

2. Right-click on the VM from the vSphere client and select SnapCenter Plug-in for VMware vSphere > Guest File Restore. On the Restore Scope page, specify Backup Name, VMDK virtual disk and Location – primary or secondary. Click Summery to confirm.

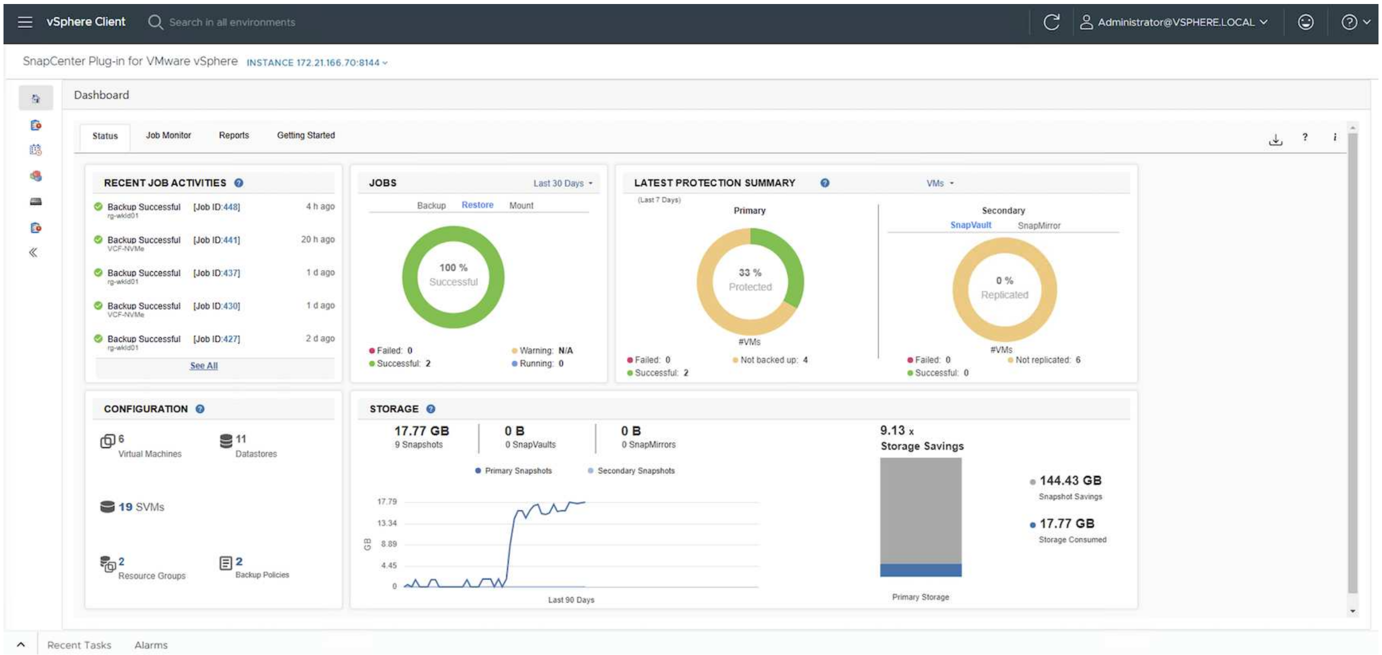


Backup Name	VCF-NVMe_03-02-2025_18.57.01.0662
VMDK	[VCF_NVMe_DS] Win2022NVMe/Win2022NVMe.vmdk
Location	Primary:VCF_NVMe:VCF_WKLD_DS:VCF-NVMe_03-02-2025_18.57.01.0662

Attach operation will start when you click the Finish button. You can monitor the progress in the Recent Tasks tab and perform a restore operation from the Guest File Restore page listed under SnapCenter Plug-in for VMware vSphere.

Monitor and report

SCV provides robust monitoring and reporting capabilities to help administrators manage backup and restore operations efficiently.
You can view status information, monitor jobs, download job logs, access reports, for more details check SnapCenter plug-in for VMware vSphere Monitor and Report.



By harnessing the power of NVMe over TCP and NetApp SnapCenter Plug-in for VMware vSphere, organizations can achieve high-performance data protection and disaster recovery for VMware Cloud Foundation workload domains. This approach ensures rapid, reliable backup and restore operations, minimizing downtime and safeguarding critical data.

Protect workloads with vSphere Metro Storage Cluster

Learn about integrating ONTAP high availability with VMware vSphere Metro Storage Cluster (vMSC)

Learn about the NetApp solutions you can use to integrate NetApp ONTAP high availability with VMware vSphere Metro Storage Cluster (vMSC). This provides a robust solutions for VMware Cloud Foundation (VCF) management and VI workload domains.

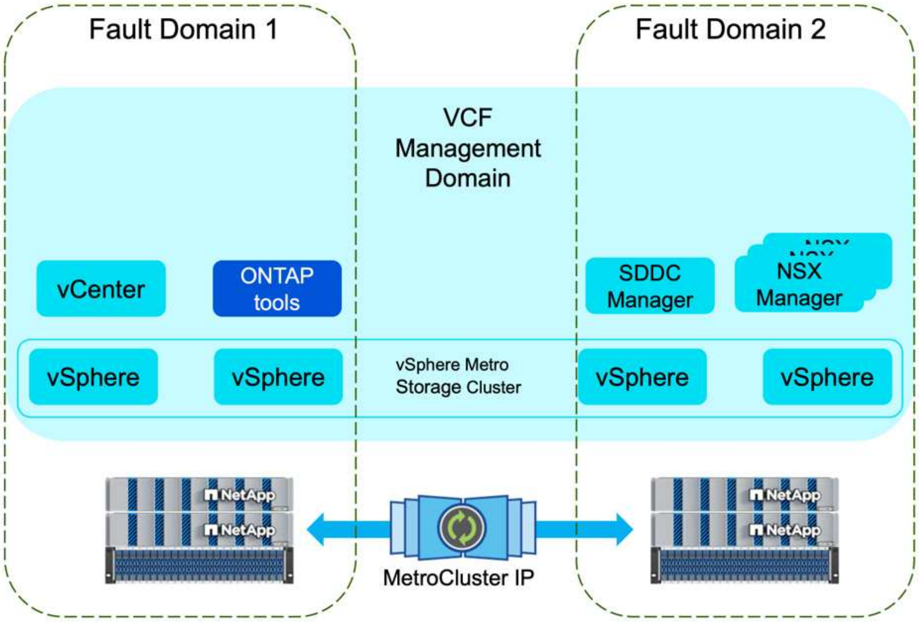
This combination ensures continuous data availability, seamless failover, and disaster recovery across geographically dispersed sites, enhancing resilience and operational continuity for critical workloads. SnapMirror active sync, enables business services to continue operating even through a complete site failure, supporting applications to fail over transparently using a secondary copy. There is no manual intervention or custom scripting required to trigger a failover with SnapMirror active sync.

Please refer to the following solutions for more details.

- Stretch Cluster for Management Domain using SnapMirror active sync
- Stretch Cluster for Management Domain using MetroCluster
- Stretch Cluster for VI Workload Domain using SnapMirror active sync
- Stretch Cluster for VI Workload Domain using MetroCluster

Configure a stretch cluster for a VCF management domain using MetroCluster

In this use case we outline the procedure to configure a stretch cluster for the VMware Cloud Foundation (VCF) management domain using ONTAP MetroCluster with NFS as the primary datastore. This procedure includes deploying vSphere hosts and vCenter Server, provisioning NFS datastores, validating the cluster with the VCF Import Tool, configuring NSX settings, and converting the environment into a VCF management domain.



Introduction

In this solution we will demonstrate how to implement Stretched VCF Management Domain with NFS as Principal Datastore using ONTAP MetroCluster.

Scenario Overview

This scenario covers the following high level steps:

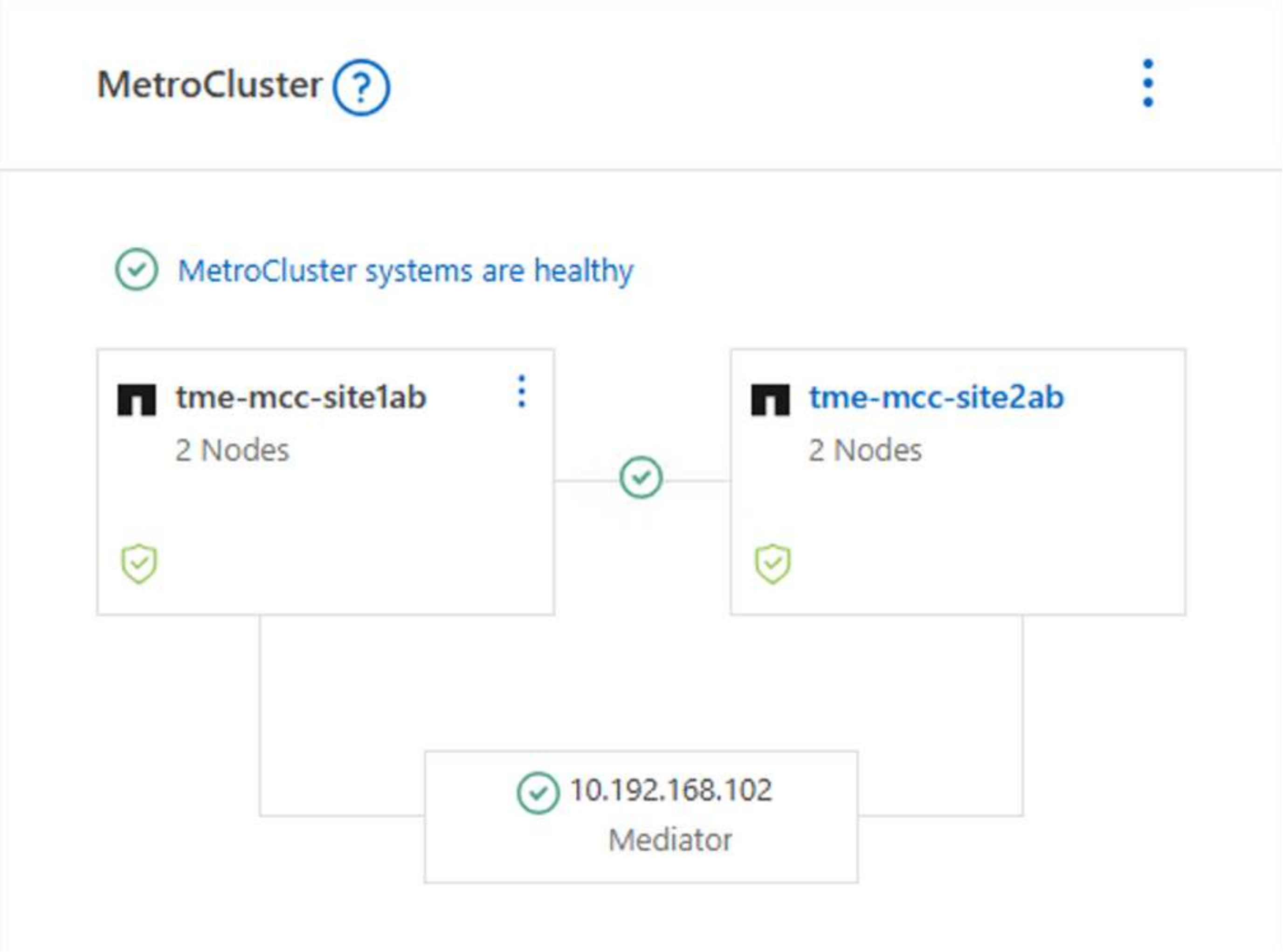
- Deploy vSphere hosts and vCenter server.
- Provision NFS datastore to vSphere hosts.
- Deploy the SDDC Manager in the vSphere cluster.
- Use the VCF Import Tool to validate the vSphere cluster.
- Configure a JSON file for create an NSX during the VCF conversion.
- Use the VCF Import Tool to convert the vSphere 8 environment to VCF management domain.

Prerequisites

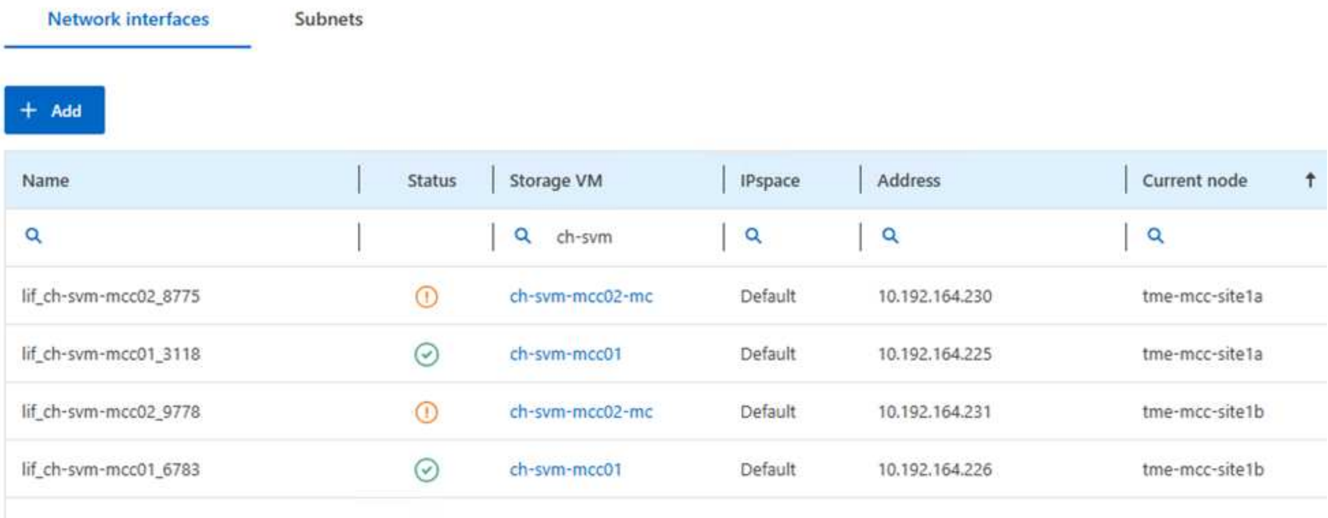
This scenario requires the following components and configurations:

- Supported ONTAP MetroCluster configuration
- Storage virtual machine (SVM) configured to allow NFS traffic.
- Logical interface (LIF) has been created on the IP network that is to carry NFS traffic and is associated with the SVM.
- A vSphere 8 cluster with 4 x ESXi hosts connected to network switch.
- Download software required for the VCF conversion.

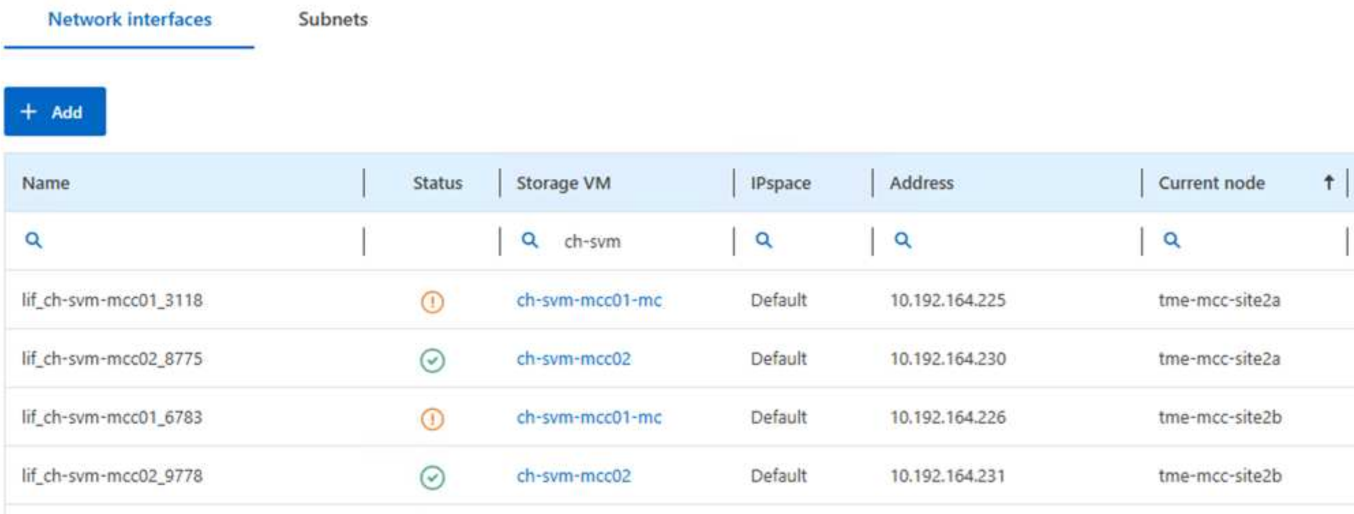
Here is the sample screenshot from System Manager showing MetroCluster configuration.



and here is the SVM Network interfaces from both fault domains.

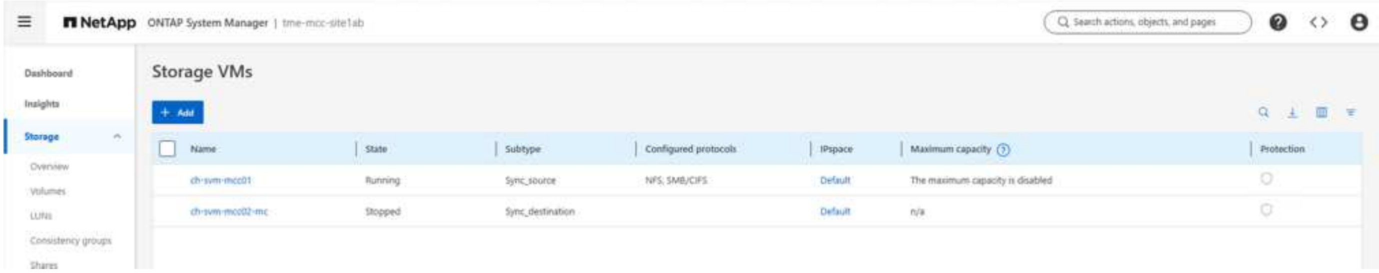


Name	Status	Storage VM	IPspace	Address	Current node ↑
		ch-svm			
lif_ch-svm-mcc02_8775	!	ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a
lif_ch-svm-mcc01_3118	✓	ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a
lif_ch-svm-mcc02_9778	!	ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b
lif_ch-svm-mcc01_6783	✓	ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b



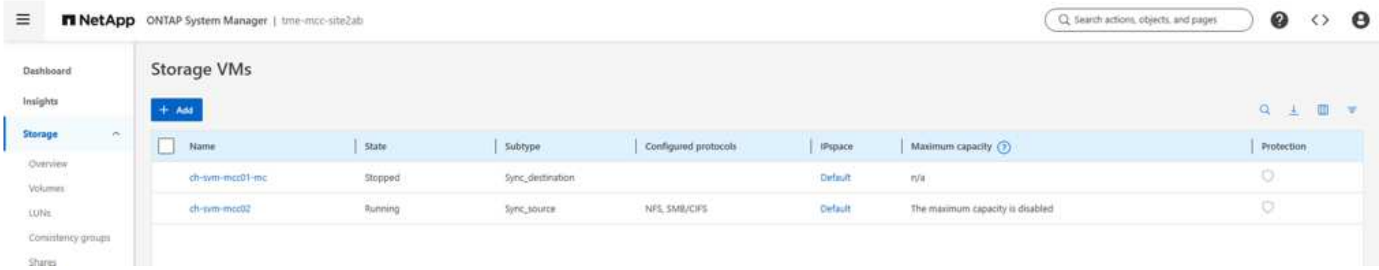
Name	Status	Storage VM	IPspace	Address	Current node ↑
		ch-svm			
lif_ch-svm-mcc01_3118	ⓘ	ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a
lif_ch-svm-mcc02_8775	✓	ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a
lif_ch-svm-mcc01_6783	ⓘ	ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b
lif_ch-svm-mcc02_9778	✓	ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b

[NOTE] SVM will be active on one of the fault domains in MetroCluster.


NetApp ONTAP System Manager | tme-mcc-site1ab
Search actions, objects, and pages
Dashboard
Insights
Storage
Overview
Volumes
LUNs
Consistency groups
Shares
+ Add

Storage VMs

Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
ch-svm-mcc01	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	
ch-svm-mcc02-mc	Stopped	Sync_destination		Default	n/a	


NetApp ONTAP System Manager | tme-mcc-site2ab
Search actions, objects, and pages
Dashboard
Insights
Storage
Overview
Volumes
LUNs
Consistency groups
Shares
+ Add

Storage VMs

Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
ch-svm-mcc01-mc	Stopped	Sync_destination		Default	n/a	
ch-svm-mcc02	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	

Refer vMSC with MetroCluster.

For supported storage and other considerations for converting or importing vSphere to VCF 5.2, refer to Considerations Before Converting or Importing Existing vSphere Environments into VMware Cloud Foundation.

Before creating vSphere Cluster that will be converted to VCF Management Domain, refer NSX consideration on vSphere Cluster

For required software refer to Download Software for Converting or Importing Existing vSphere Environments.

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

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

Deployment Steps

To deploy VCF Stretched Management Domain with NFS as Principal Datastore,

Complete the following steps:

- Deploy vSphere hosts and vCenter.
- Create vSphere Cluster.
- Provision NFS datastore.
- Copy the VCF Import Tool to the vCenter appliance.
- Run a pre-check on the vCenter appliance using the VCF Import Tool.
- Deploy the SDDC manager VM on the vCenter cluster.
- Create a JSON file for an NSX cluster to deployed during the conversion process.
- Upload the required software to the SDDC manager.
- Convert the vSphere cluster into VCF Management Domain.

For an overview of the conversion process, refer to Convert a vSphere Environment to a Management Domain or Import a vSphere Environment as a VI Workload Domain in VMware Cloud Foundation.

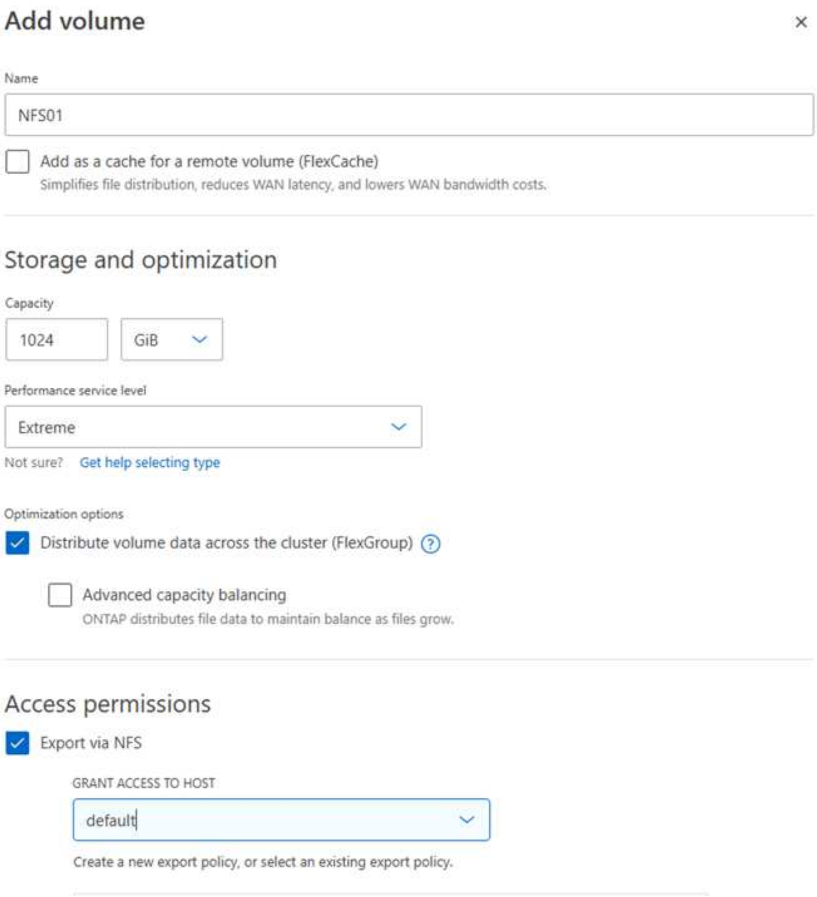
Deploy vSphere hosts and vCenter

Deploy vSphere on hosts using ISO downloaded from Broadcom support portal or use existing deployment option for vSphere host.

Mount NFS Datastore to host VMs

In this step, We create the NFS volume and mount it as Datastore to host VMs.

1. Using System Manager, Create a volume and attach to export policy that includes the IP subnet of the vSphere host.



Add volume ×

Name

NFS01

☐ Add as a cache for a remote volume (FlexCache)
Simplifies file distribution, reduces WAN latency, and lowers WAN bandwidth costs.

Storage and optimization

Capacity

1024 GiB

Performance service level

Extreme

Not sure? Get help selecting type

Optimization options

☑ Distribute volume data across the cluster (FlexGroup) ?

☐ Advanced capacity balancing
ONTAP distributes file data to maintain balance as files grow.

Access permissions

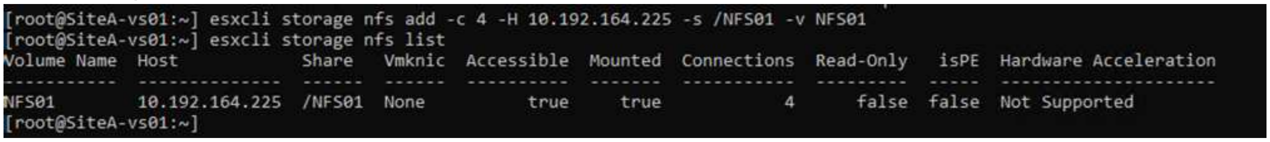
☑ Export via NFS

GRANT ACCESS TO HOST

default

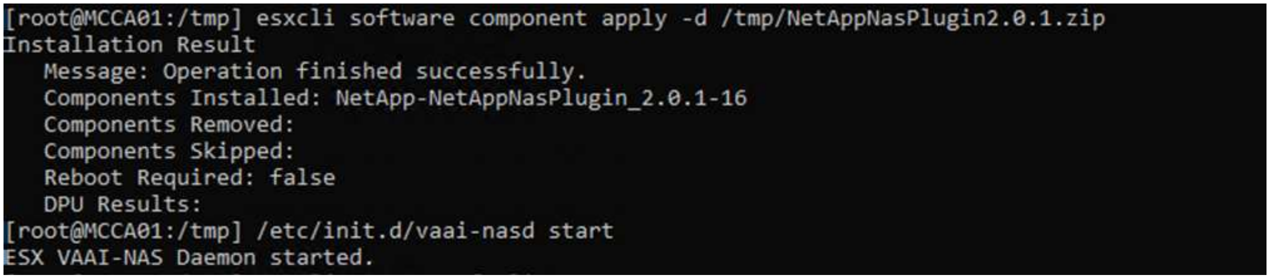
Create a new export policy, or select an existing export policy.

2. SSH to vSphere host and mount the NFS Datastore.



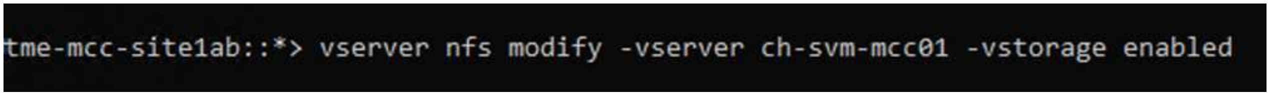
```
[root@SiteA-vs01:~] esxcli storage nfs add -c 4 -H 10.192.164.225 -s /NFS01 -v NFS01
[root@SiteA-vs01:~] esxcli storage nfs list
Volume Name  Host            Share   Vmknic  Accessible  Mounted  Connections  Read-Only  isPE   Hardware Acceleration
-----------  --------------  ------  ------  ----------  -------  -----------  ---------  -----  --------------------
NFS01        10.192.164.225  /NFS01  None          true     true            4      false  false  Not Supported
[root@SiteA-vs01:~]
```

[NOTE] If hardware acceleration is shown as not supported, ensure latest NFS VAAI component (downloaded from NetApp Support portal) is installed on the vSphere host



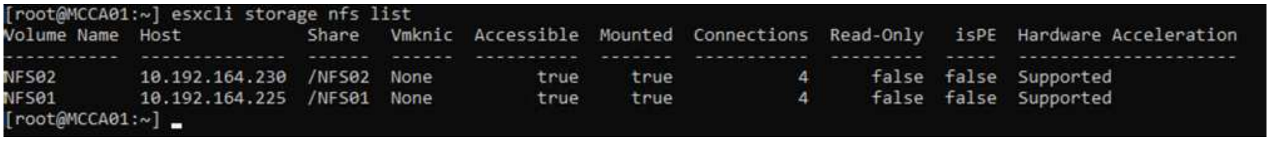
```
[root@MCCA01:/tmp] esxcli software component apply -d /tmp/NetAppNasPlugin2.0.1.zip
Installation Result
   Message: Operation finished successfully.
   Components Installed: NetApp-NetAppNasPlugin_2.0.1-16
   Components Removed:
   Components Skipped:
   Reboot Required: false
   DPU Results:
[root@MCCA01:/tmp] /etc/init.d/vaai-nasd start
ESX VAAI-NAS Daemon started.
```

and vStorage is enabled on the SVM that hosts the volume.



```
tme-mcc-site1ab::*> vserver nfs modify -vserver ch-svm-mcc01 -vstorage enabled
```

3. Repeat above steps for additional datastore need and ensure the hardware acceleration is supported.



```
[root@MCCA01:~] esxcli storage nfs list
Volume Name  Host            Share   Vmknic  Accessible  Mounted  Connections  Read-Only   isPE  Hardware Acceleration
-----------  --------------  ------  ------  ----------  -------  -----------  ---------  -----  ---------------------
NFS02        10.192.164.230  /NFS02  None          true     true            4      false  false  Supported
NFS01        10.192.164.225  /NFS01  None          true     true            4      false  false  Supported
[root@MCCA01:~] ▂
```

Deploy vCenter on NFS Datastore. Ensure SSH and Bash shell is enabled on vCenter appliance.

Create vSphere Cluster

1. Login to vSphere web client, Create the DataCenter and vSphere Cluster by adding one of the host where NFS VAAI is deployed. We opted to Manage all hosts in the cluster with single image option.
   [TIP] Do not select Manage configuration at cluster level.
   For additional details, refer NSX consideration on vSphere Cluster. For vMSC best practices with ONTAP MetroCluster, check vMSC Design and Implementation Guidelines
2. Add other vSphere hosts to Cluster.
3. Create Distributed Switch and add the port groups.
4. Migrate networking from standard vSwitch to distributed switch.

Convert vSphere environment to VCF Management Domain

The following section covers the steps to deploy the SDDC manager and convert the vSphere 8 cluster to a VCF 5.2 management domain. Where appropriate, VMware documentation will be referred to for additional detail.

The VCF Import Tool, from VMware by Broadcom is a utility that is used on both the vCenter appliance and SDDC manager to validate configurations and provide conversion and import services for vSphere and VCF environments.

For more information, refer to VCF Import Tool Options and Parameters.

Copy and extract VCF Import Tool

The VCF Import Tool is used on the vCenter appliance to validate that the vSphere cluster is in a healthy state for the VCF conversion or import process.

Complete the following steps:

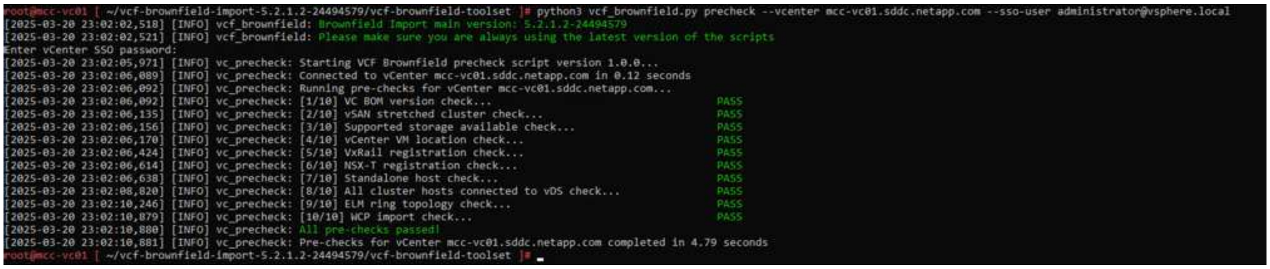
1. Follow the steps at Copy the VCF Import Tool to the Target vCenter Appliance at VMware Docs to copy the VCF Import Tool to the correct location.
2. Extract the bundle using the following command:

   ```
   tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
   ```

Validate the vCenter appliance

Use the VCF Import tool to validate the vCenter appliance before the conversion.

1. Follow the steps at Run a Pre-check on the Target vCenter Before Conversion to run the validation.
2. The following output shows that the vCenter appliance has passed the pre-check.

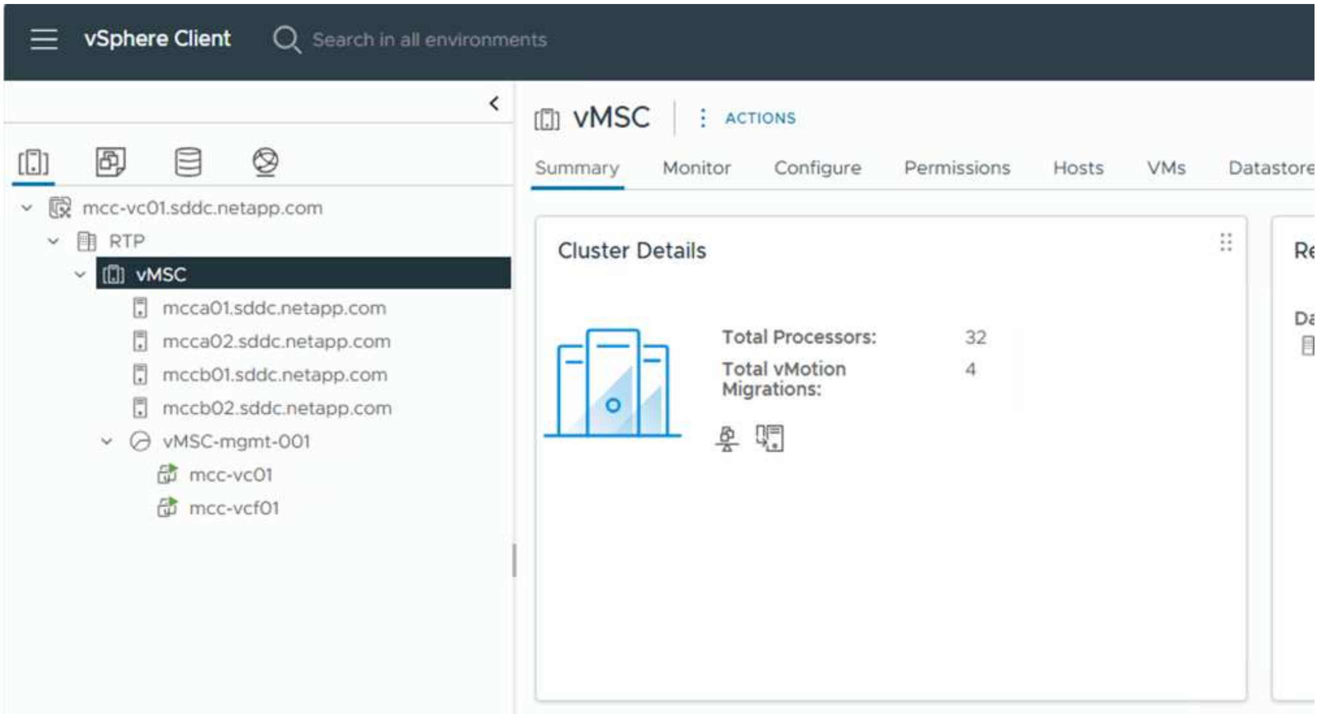


```
root@mcc-vc01 [ ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter mcc-vc01.sddc.netapp.com --sso-user administrator@vsphere.local
[2025-03-20 23:02:02,518] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.2-24494579
[2025-03-20 23:02:02,521] [INFO] vcf_brownfield: Please make sure you are always using the latest version of the scripts
Enter vCenter SSO password:
[2025-03-20 23:02:05,971] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2025-03-20 23:02:06,089] [INFO] vc_precheck: Connected to vCenter mcc-vc01.sddc.netapp.com in 0.12 seconds
[2025-03-20 23:02:06,092] [INFO] vc_precheck: Running pre-checks for vCenter mcc-vc01.sddc.netapp.com...
[2025-03-20 23:02:06,092] [INFO] vc_precheck: [1/10] VC BOM version check...                                     PASS
[2025-03-20 23:02:06,135] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...                             PASS
[2025-03-20 23:02:06,156] [INFO] vc_precheck: [3/10] Supported storage available check...                        PASS
[2025-03-20 23:02:06,170] [INFO] vc_precheck: [4/10] vCenter VM location check...                                PASS
[2025-03-20 23:02:06,424] [INFO] vc_precheck: [5/10] VxRail registration check...                                PASS
[2025-03-20 23:02:06,614] [INFO] vc_precheck: [6/10] NSX-T registration check...                                 PASS
[2025-03-20 23:02:06,638] [INFO] vc_precheck: [7/10] Standalone host check...                                    PASS
[2025-03-20 23:02:08,820] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...                 PASS
[2025-03-20 23:02:10,246] [INFO] vc_precheck: [9/10] ELM ring topology check...                                  PASS
[2025-03-20 23:02:10,879] [INFO] vc_precheck: [10/10] WCP import check...                                        PASS
[2025-03-20 23:02:10,880] [INFO] vc_precheck: All pre-checks passed!
[2025-03-20 23:02:10,881] [INFO] vc_precheck: Pre-checks for vCenter mcc-vc01.sddc.netapp.com completed in 4.79 seconds
root@mcc-vc01 [ ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]#
```

Deploy the SDDC Manager

The SDDC manager must be colocated on the vSphere cluster that will be converted to a VCF management domain.

Follow the deployment instructions at VMware Docs to complete the deployment.



Total Processors: 32

Total vMotion Migrations: 4

Refer to Deploy the SDDC Manager Appliance on the Target vCenter.

Create a JSON file for NSX deployment

To deploy NSX Manager while importing or converting a vSphere environment into VMware Cloud Foundation, create an NSX deployment specification. NSX deployment requires a minimum of 3 hosts.

> When deploying an NSX Manager cluster in a convert or import operation, NSX VLAN backed segment is used. For details on the limitations of NSX-VLAN backed segment, refer to the section "Considerations Before Converting or Importing Existing vSphere Environments into VMware Cloud Foundation. For information about NSX-VLAN networking limitations, refer to Considerations Before Converting or Importing Existing vSphere Environments into VMware Cloud Foundation.

The following is an example of a JSON file for NSX deployment:

```
{
  "deploy_without_license_keys": true,
  "form_factor": "small",
  "admin_password": "******************",
  "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-
133764.zip",
  "cluster_ip": "10.61.185.114",
  "cluster_fqdn": "mcc-nsx.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "mcc-nsxa.sddc.netapp.com",
    "name": "mcc-nsxa",
    "ip_address": "10.61.185.111",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-nsxb.sddc.netapp.com",
    "name": "mcc-nsxb",
    "ip_address": "10.61.185.112",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-nsxc.sddc.netapp.com",
    "name": "mcc-nsxc",
    "ip_address": "10.61.185.113",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Copy the JSON file to vcf user home folder on the SDDC Manager.

Upload software to SDDC Manager

Copy the VCF Import Tool to home folder of vcf user and the NSX deployment bundle to /nfs/vmware/vcf/nfs-mount/bundle/ folder on the SDDC Manager.

See Upload the Required Software to the SDDC Manager Appliance for detailed instructions.

Detailed Check on vCenter before conversion

Before you perform a management domain convert operation or a VI workload domain import operation, you must perform a detailed check to ensure that the existing vSphere environment's configuration is supported for convert or import.
. SSH to the SDDC Manager appliance as user vcf.
. Navigate to the directory where you copied the VCF Import Tool.
. Run the following command to check that the vSphere environment can be converted

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '********' --local-admin-password
'****************' --accept-trust
```

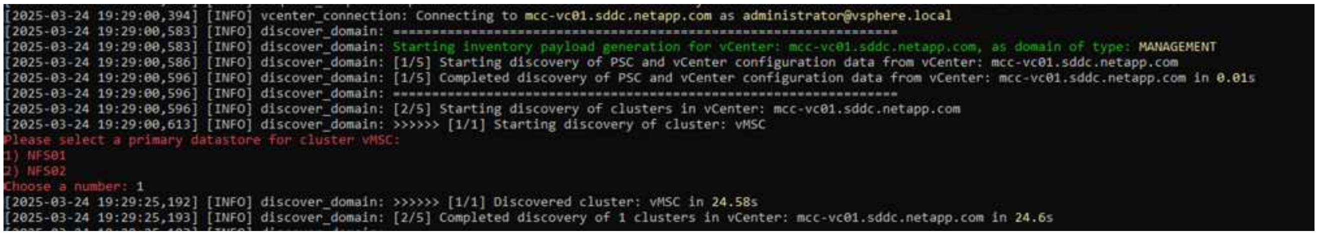
Convert vSphere cluster to VCF management domain

The VCF Import Tool is used to conduct the conversion process.

The following command is run to convert the vSphere cluster to a VCF management domain and deploy the NSX cluster:

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '******' --vcenter-root-password '********'
--local-admin-password '****************' --backup-password
'****************' --domain-name '<Mgmt-domain-name>' --accept-trust
--nsx-deployment-spec-path /home/vcf/nsx.json
```

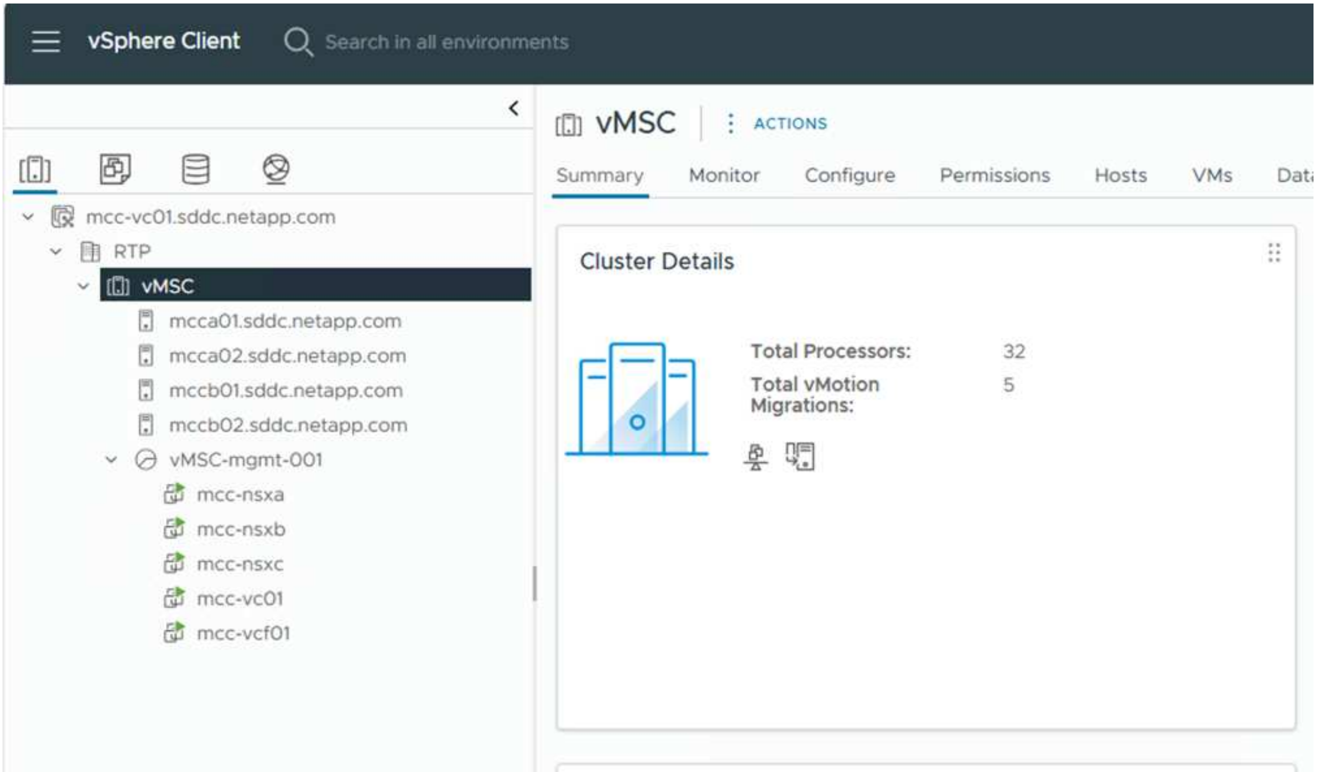
When multiple Datastores are available on vSphere host, it prompts which Datastore that needs to be considered as Primary Datastore on which NSX VMs will be deployed by default.



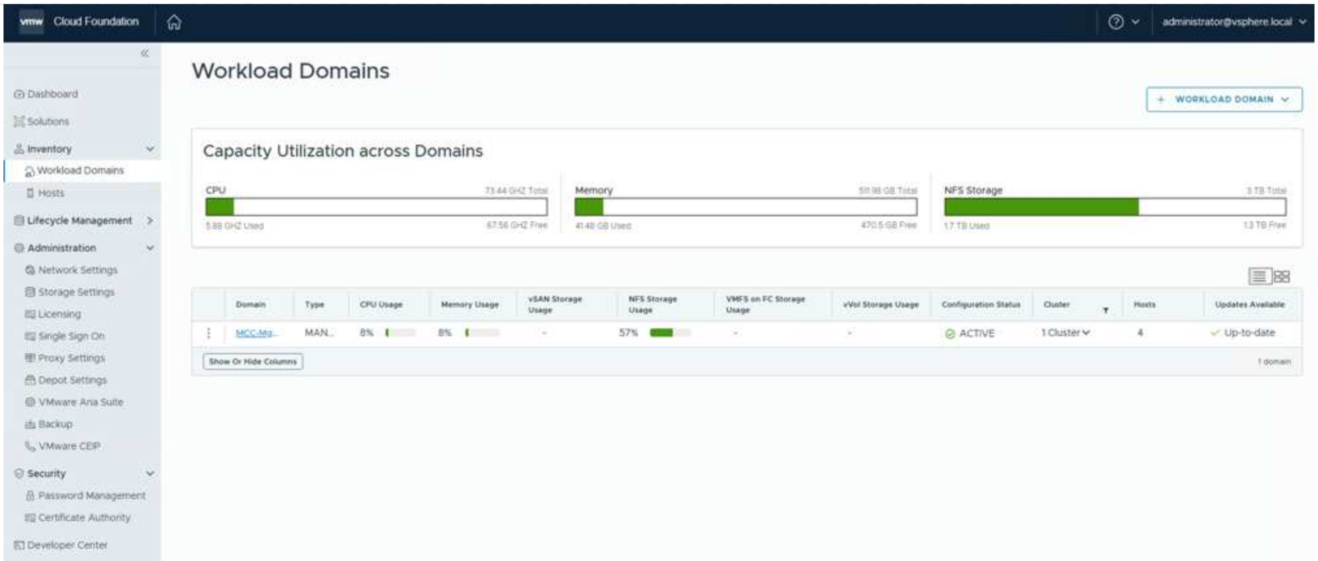
```
[2025-03-24 19:29:00,394] [INFO] vcenter_connection: Connecting to mcc-vc01.sddc.netapp.com as administrator@vsphere.local
[2025-03-24 19:29:00,583] [INFO] discover_domain: ============================================================
[2025-03-24 19:29:00,583] [INFO] discover_domain: Starting inventory payload generation for vCenter: mcc-vc01.sddc.netapp.com, as domain of type: MANAGEMENT
[2025-03-24 19:29:00,586] [INFO] discover_domain: [1/5] Starting discovery of PSC and vCenter configuration data from vCenter: mcc-vc01.sddc.netapp.com
[2025-03-24 19:29:00,596] [INFO] discover_domain: [1/5] Completed discovery of PSC and vCenter configuration data from vCenter: mcc-vc01.sddc.netapp.com in 0.01s
[2025-03-24 19:29:00,596] [INFO] discover_domain: ============================================================
[2025-03-24 19:29:00,596] [INFO] discover_domain: [2/5] Starting discovery of clusters in vCenter: mcc-vc01.sddc.netapp.com
[2025-03-24 19:29:00,613] [INFO] discover_domain: >>>>>> [1/1] Starting discovery of cluster: vMSC
Please select a primary datastore for cluster vMSC:
1) NFS01
2) NFS02
Choose a number: 1
[2025-03-24 19:29:25,192] [INFO] discover_domain: >>>>>> [1/1] Discovered cluster: vMSC in 24.58s
[2025-03-24 19:29:25,193] [INFO] discover_domain: [2/5] Completed discovery of 1 clusters in vCenter: mcc-vc01.sddc.netapp.com in 24.6s
```

For complete instructions, refer to VCF Convert Procedure.

NSX VMs will be deployed to vCenter.



SDDC Manager shows the Management domain created with the name that was provided and NFS as Datastore.



Workload Domains

Capacity Utilization across Domains

CPU 73.44 GHZ Total
5.88 GHZ Used 67.56 GHZ Free

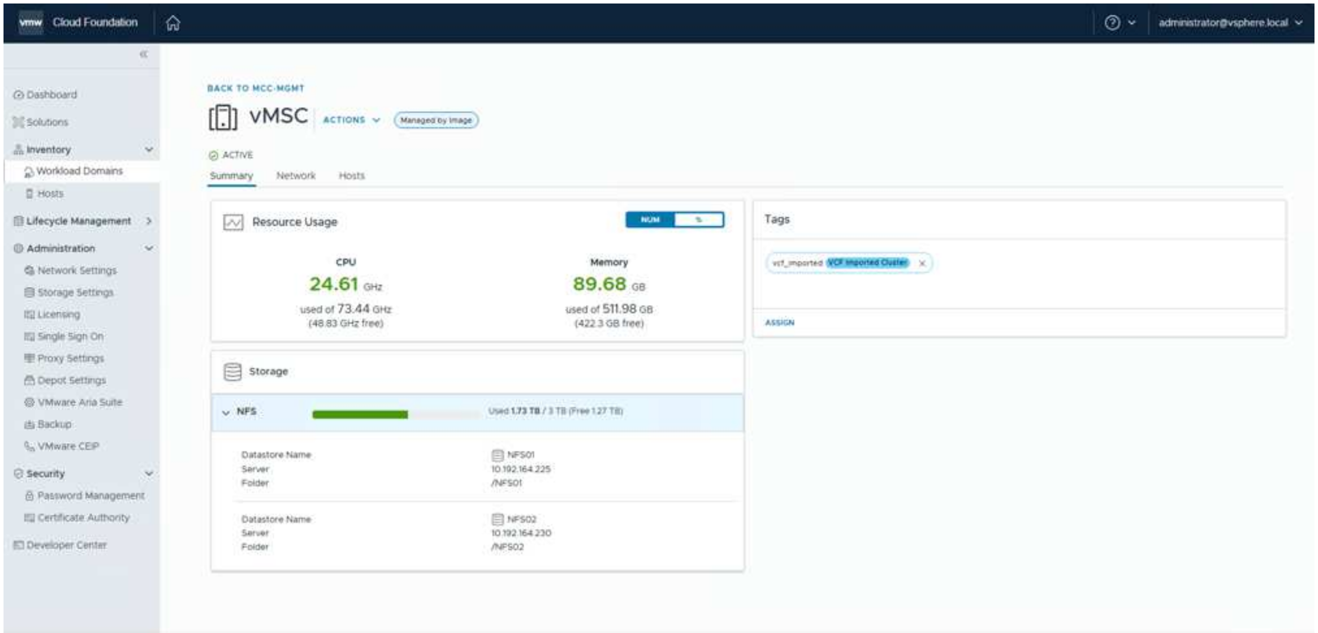
Memory 511.98 GB Total
41.48 GB Used 470.5 GB Free

NFS Storage 3 TB Total
1.7 TB Used 1.3 TB Free

Domain	Type	CPU Usage	Memory Usage	vSAN Storage Usage	NFS Storage Usage	VMFS on FC Storage Usage	vVol Storage Usage	Configuration Status	Cluster	Hosts	Updates Available
MCC-Mg...	MAN...	8%	8%	-	57%	-	-	ACTIVE	1 Cluster	4	Up-to-date

1 domain

On Inspecting the cluster, it provides the information of NFS Datastore.



vMSC

ACTIVE

Resource Usage

CPU
24.61 GHz
used of 73.44 GHz
(48.83 GHz free)

Memory
89.68 GB
used of 511.98 GB
(422.3 GB free)

Tags

vcf_imported VCF Imported Cluster

Storage

NFS Used 1.73 TB / 3 TB (Free 1.27 TB)

Datastore Name NFS01
Server 10.192.164.225
Folder /NFS01

Datastore Name NFS02
Server 10.192.164.230
Folder /NFS02

Add licensing to VCF

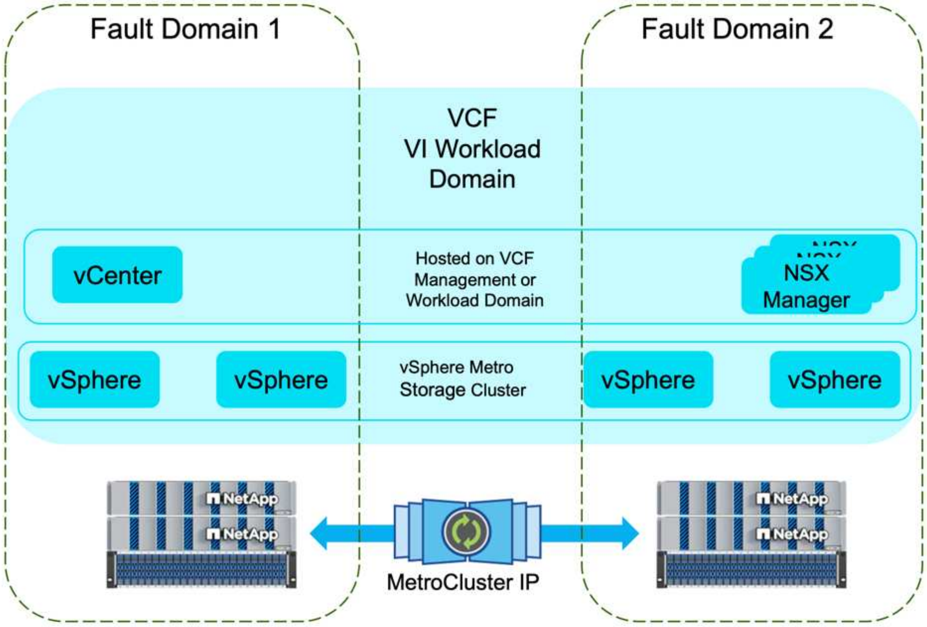
After completing the conversion, licensing must be added to the environment.

1. Log in to the SDDC Manager UI.
2. Navigate to **Administration > Licensing** in the navigation pane.
3. Click on **+ License Key**.
4. Choose a product from the drop-down menu.
5. Enter the license key.
6. Provide a description for the license.
7. Click **Add**.
8. Repeat these steps for each license.

Configure a stretch cluster for a VI workload domain using MetroCluster

In this use case we outline the procedure to configure stretched VCF VI workload domain with NFS as principal datastore using ONTAP MetroCluster. This procedure includes deploying vSphere hosts and vCenter Server, provisioning NFS datastores, validating the vSphere cluster, configuring NSX during the VCF conversion, and importing the vSphere environment into an existing VCF Management Domain.

The Workloads on VCF is protected by vSphere Metro Storage Cluster (vMSC). ONTAP MetroCluster with either FC or IP deployment is typically utilized to provide fault tolerance of VMFS and NFS Datastores.



Introduction

In this solution we will demonstrate how to implement Stetched VCF VI Workload Domain with NFS as Principal Datastore using ONTAP MetroCluster. The VI Workload Domain can be deployed using SDDC Manager or import an existing vSphere environment as VI Workload Domain.

Scenario Overview

This scenario covers the following high level steps:

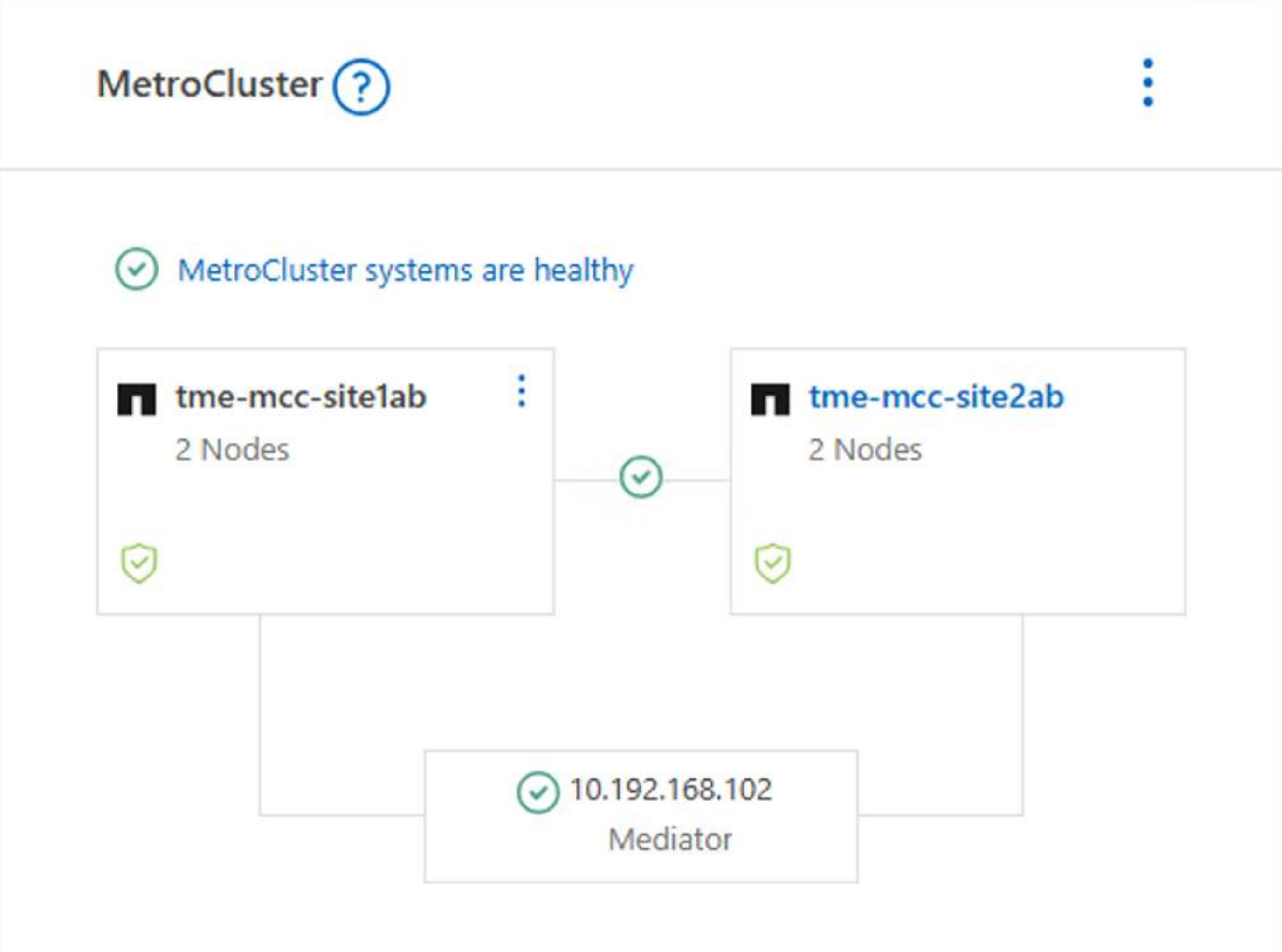
- Deploy vSphere hosts and vCenter server.
- Provision NFS datastore to vSphere hosts.
- Use the VCF Import Tool to validate the vSphere cluster.
- Configure a JSON file for create an NSX during the VCF conversion.
- Use the VCF Import Tool to import the vSphere 8 environment as VCF VI Workload domain to an existing VCF Management Domain.

Prerequisites

This scenario requires the following components and configurations:

- Supported ONTAP MetroCluster configuration
- Storage virtual machine (SVM) configured to allow NFS traffic.
- Logical interface (LIF) has been created on the IP network that is to carry NFS traffic and is associated with the SVM.
- A vSphere 8 cluster with 4 x ESXi hosts connected to network switch.
- Download software required for the VCF conversion.

Here is the sample screenshot from System Manager showing MetroCluster configuration.



MetroCluster

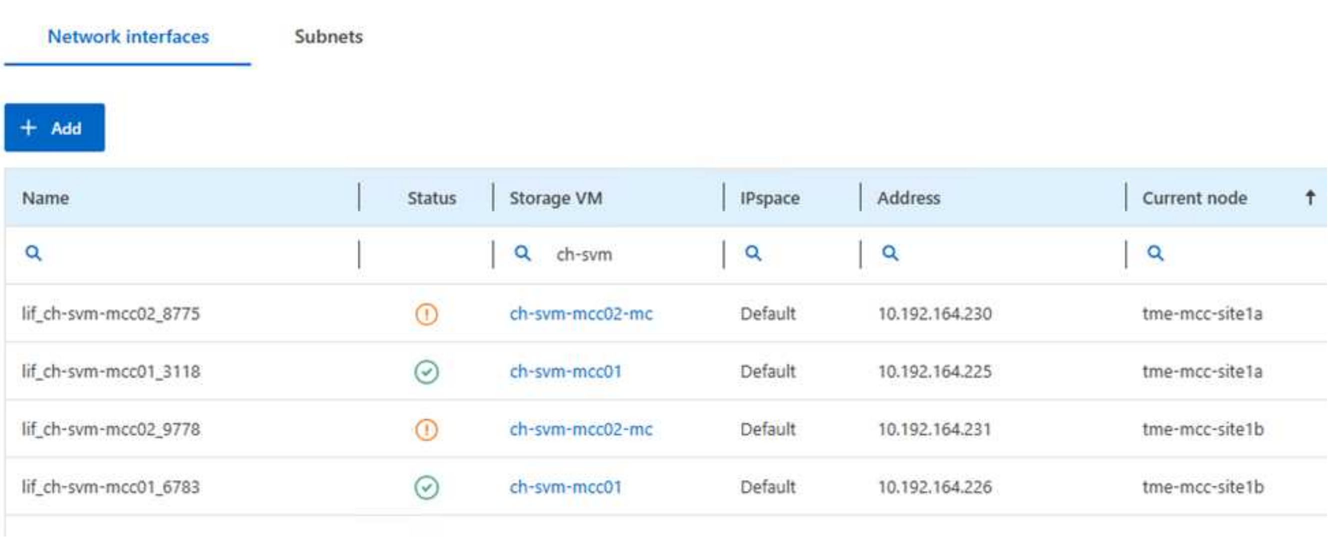
MetroCluster systems are healthy

tme-mcc-site1ab
2 Nodes

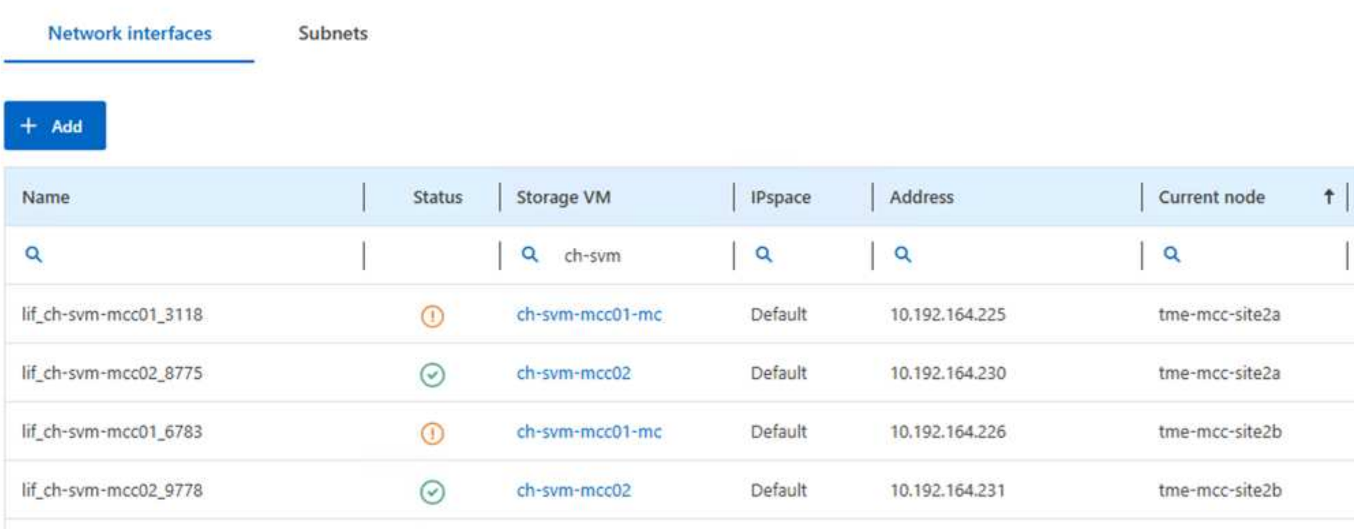
tme-mcc-site2ab
2 Nodes

10.192.168.102
Mediator

and here is the SVM Network interfaces from both fault domains.

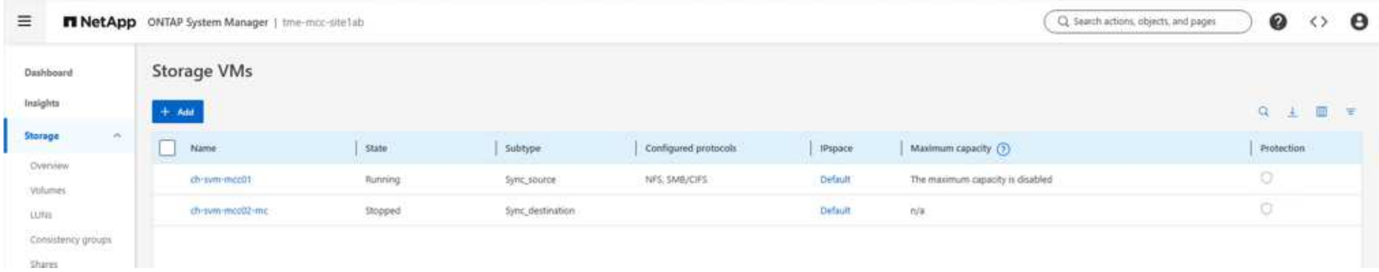


Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc02_8775	!	ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a
lif_ch-svm-mcc01_3118	✓	ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a
lif_ch-svm-mcc02_9778	!	ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b
lif_ch-svm-mcc01_6783	✓	ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b



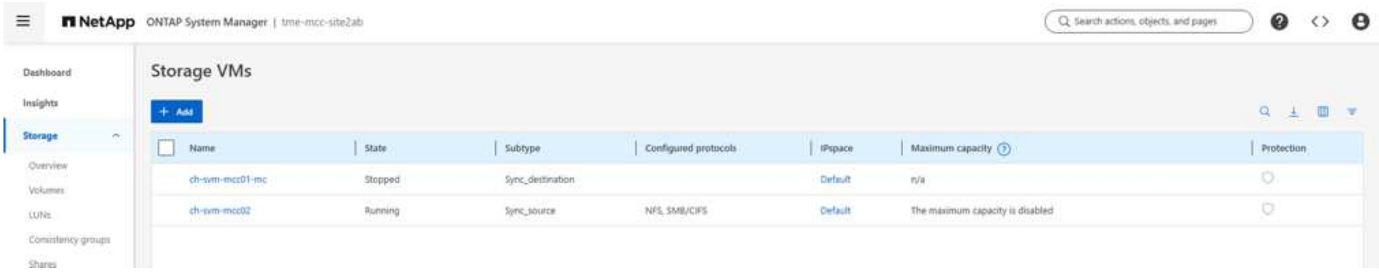
Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc01_3118	!	ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a
lif_ch-svm-mcc02_8775	✓	ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a
lif_ch-svm-mcc01_6783	!	ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b
lif_ch-svm-mcc02_9778	✓	ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b

[NOTE] SVM will be active on one of the fault domains in MetroCluster.


NetApp ONTAP System Manager | tme-mcc-site1ab
Search actions, objects, and pages
Dashboard
Insights
Storage
Overview
Volumes
LUNs
Consistency groups
Shares
+ Add

Storage VMs

☐	Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
	ch-svm-mcc01	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	○
	ch-svm-mcc02-mc	Stopped	Sync_destination		Default	n/a	○


NetApp ONTAP System Manager | tme-mcc-site2ab
Search actions, objects, and pages
Dashboard
Insights
Storage
Overview
Volumes
LUNs
Consistency groups
Shares
+ Add

Storage VMs

☐	Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
	ch-svm-mcc01-mc	Stopped	Sync_destination		Default	n/a	○
	ch-svm-mcc02	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	○

Refer vMSC with MetroCluster.

For supported storage and other considerations for converting or importing vSphere to VCF 5.2, refer to Considerations Before Converting or Importing Existing vSphere Environments into VMware Cloud Foundation.

Before creating vSphere Cluster that will be converted to VCF Management Domain, refer NSX consideration on vSphere Cluster

For required software refer to Download Software for Converting or Importing Existing vSphere Environments.

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

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

Deployment Steps

To deploy VCF Stretched Management Domain with NFS as Principal Datastore,

Complete the following steps:

- Deploy vSphere hosts and vCenter.
- Create vSphere Cluster.
- Provision NFS datastore.
- Copy the VCF Import Tool to the vCenter appliance.
- Run a precheck on the vCenter appliance using the VCF Import Tool.
- Create a JSON file for an NSX cluster to deployed during the import process.
- Upload the required software to the SDDC manager.
- Convert the vSphere cluster into VCF VI Workload Domain.

For an overview of the conversion process, refer to Convert a vSphere Environment to a Management Domain or Import a vSphere Environment as a VI Workload Domain in VMware Cloud Foundation.

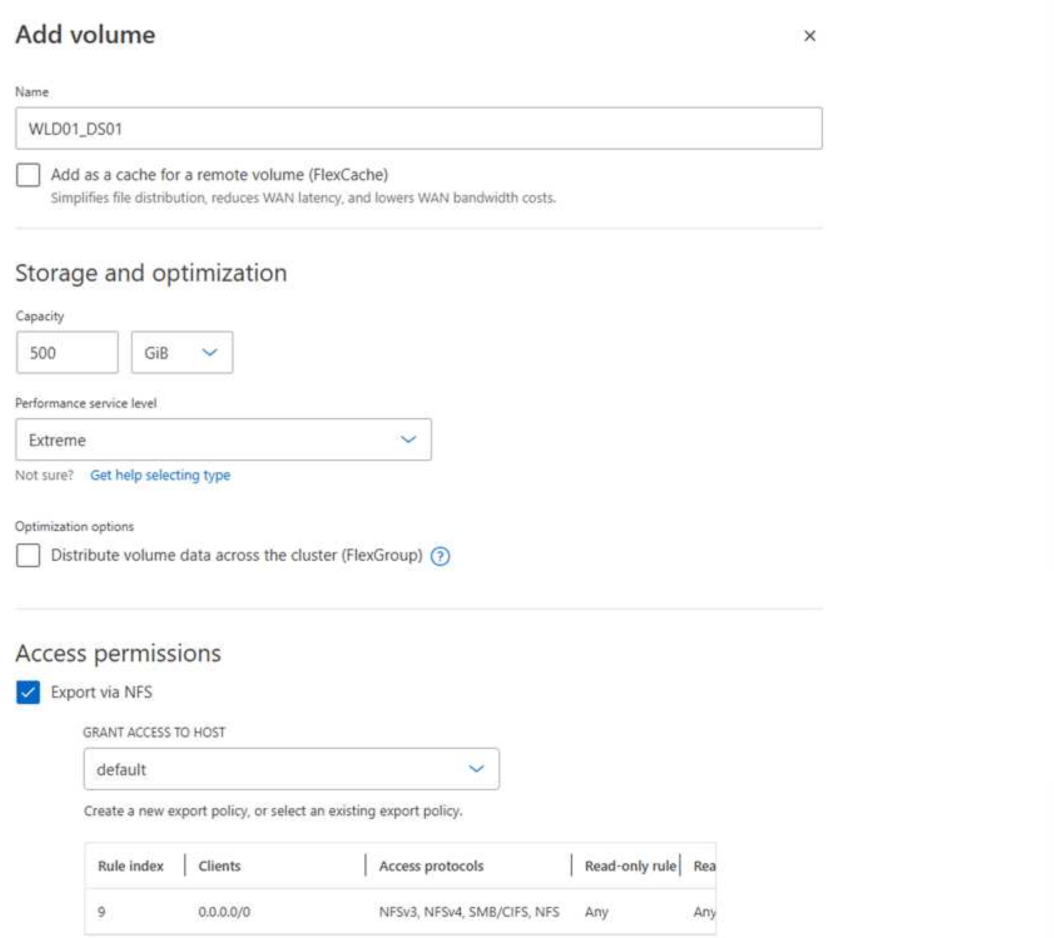
Deploy vSphere hosts and vCenter

Deploy vSphere on hosts using ISO downloaded from Broadcom support portal or use existing deployment option for vSphere host.

Mount NFS Datastore to host VMs

In this step, We create the NFS volume and mount it as Datastore to host VMs.

1. Using System Manager, Create a volume and attach to export policy that includes the IP subnet of the vSphere host.



Add volume ×

Name

WLD01_DS01

□ Add as a cache for a remote volume (FlexCache)
Simplifies file distribution, reduces WAN latency, and lowers WAN bandwidth costs.

Storage and optimization

Capacity

500 GiB

Performance service level

Extreme

Not sure? Get help selecting type

Optimization options

□ Distribute volume data across the cluster (FlexGroup)

Access permissions

☑ Export via NFS

GRANT ACCESS TO HOST

default

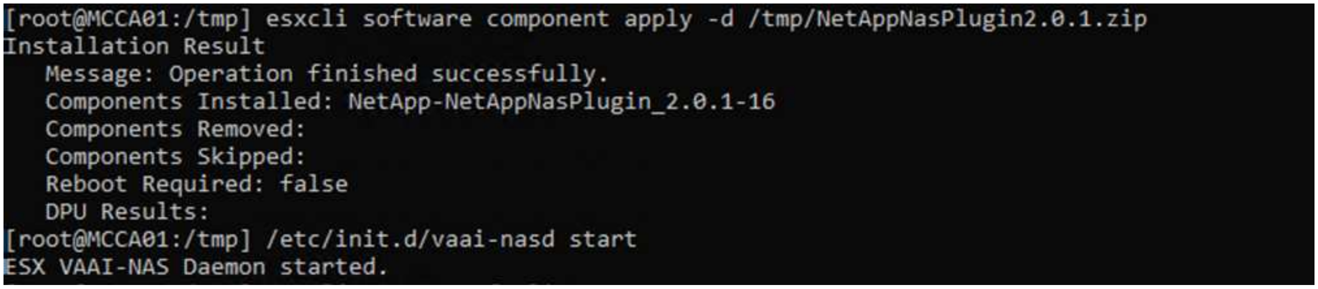
Create a new export policy, or select an existing export policy.

Rule index	Clients	Access protocols	Read-only rule	Rea
9	0.0.0.0/0	NFSv3, NFSv4, SMB/CIFS, NFS	Any	Any

2. SSH to vSphere host and mount the NFS Datastore.

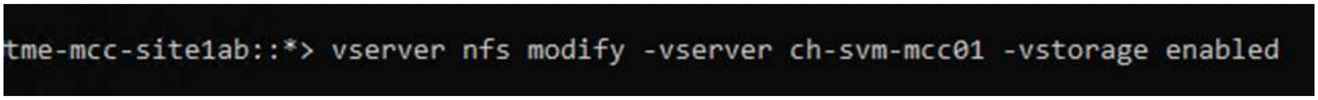
```
esxcli storage nfs add -c 4 -H 10.192.164.225 -s /WLD01_DS01 -v DS01
esxcli storage nfs add -c 4 -H 10.192.164.230 -s /WLD01_DS02 -v DS02
esxcli storage nfs list
```

[NOTE] If hardware acceleration is shown as not supported, ensure latest NFS VAAI component (downloaded from NetApp Support portal) is installed on the vSphere host



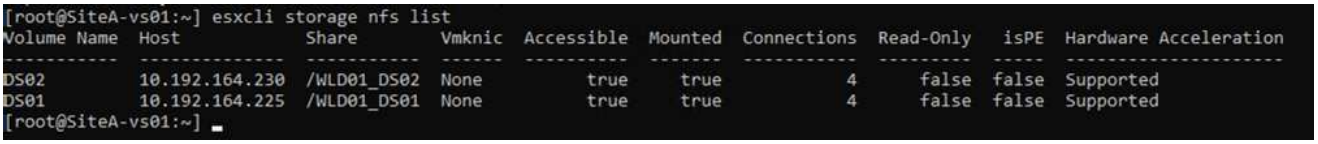
```
[root@MCCA01:/tmp] esxcli software component apply -d /tmp/NetAppNasPlugin2.0.1.zip
Installation Result
   Message: Operation finished successfully.
   Components Installed: NetApp-NetAppNasPlugin_2.0.1-16
   Components Removed:
   Components Skipped:
   Reboot Required: false
   DPU Results:
[root@MCCA01:/tmp] /etc/init.d/vaai-nasd start
ESX VAAI-NAS Daemon started.
```

and vStorage is enabled on the SVM that hosts the volume.



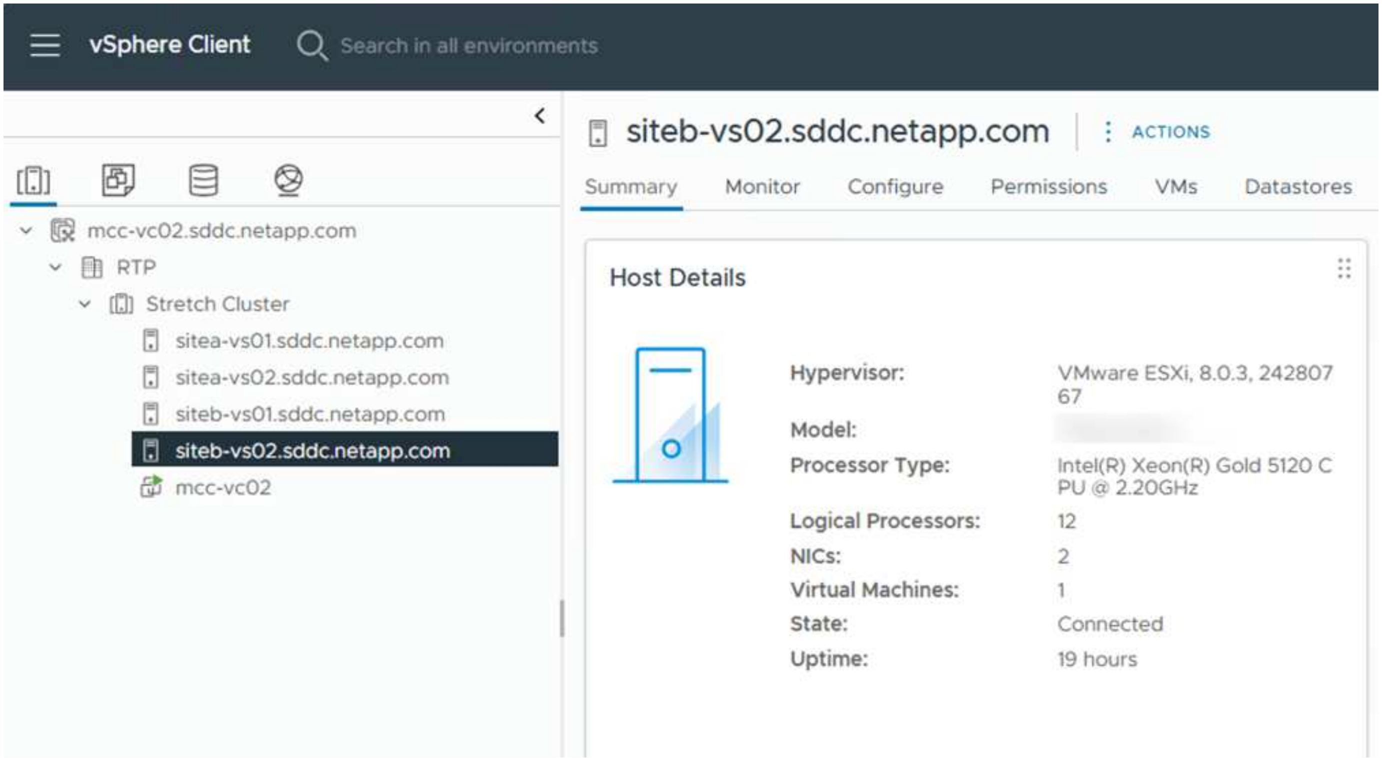
```
tme-mcc-site1ab::*> vserver nfs modify -vserver ch-svm-mcc01 -vstorage enabled
```

. Repeat above steps for additional datastore need and ensure the hardware acceleration is supported.



```
[root@SiteA-vs01:~] esxcli storage nfs list
Volume Name  Host            Share        Vmknic  Accessible  Mounted  Connections  Read-Only   isPE  Hardware Acceleration
-----------  --------------  -----------  ------  ----------  -------  -----------  ---------  -----  ---------------------
DS02         10.192.164.230  /WLD01_DS02  None          true     true            4      false  false  Supported
DS01         10.192.164.225  /WLD01_DS01  None          true     true            4      false  false  Supported
[root@SiteA-vs01:~] _
```

Deploy vCenter on NFS Datastore. Ensure SSH and Bash shell is enabled on vCenter appliance.


vSphere Client
Search in all environments
mcc-vc02.sddc.netapp.com
RTP
Stretch Cluster
sitea-vs01.sddc.netapp.com
sitea-vs02.sddc.netapp.com
siteb-vs01.sddc.netapp.com
siteb-vs02.sddc.netapp.com
mcc-vc02
siteb-vs02.sddc.netapp.com
ACTIONS
Summary
Monitor
Configure
Permissions
VMs
Datastores

Host Details

Hypervisor: VMware ESXi, 8.0.3, 24280767
Model: [redacted]
Processor Type: Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz
Logical Processors: 12
NICs: 2
Virtual Machines: 1
State: Connected
Uptime: 19 hours

Create vSphere Cluster

1. Login to vSphere webclient, Create the DataCenter and vSphere Cluster by adding one of the host where NFS VAAI is deployed. We opted to Manage all hosts in the cluster with single image option.
   [TIP] Do not select Manage configuration at cluster level.
   For additional details, refer NSX consideration on vSphere Cluster. For vMSC best practices with ONTAP MetroCluster, check vMSC Design and Implementation Guidelines
2. Add other vSphere hosts to Cluster.
3. Create Distributed Switch and add the port groups.
4. Migrate networking from standard vSwitch to distributed switch.

Convert vSphere environment to VCF VI Workload Domain

The following section covers the steps to deploy the SDDC manager and convert the vSphere 8 cluster to a VCF 5.2 management domain. Where appropriate, VMware documentation will be referred to for additional detail.

The VCF Import Tool, from VMware by Broadcom is a utility that is used on both the vCenter appliance and SDDC manager to validate configurations and provide conversion and import services for vSphere and VCF environments.

For more information, refer to VCF Import Tool Options and Parameters.

Copy and extract VCF Import Tool

The VCF Import Tool is used on the vCenter appliance to validate that the vSphere cluster is in a healthy state for the VCF conversion or import process.

Complete the following steps:

1. Follow the steps at Copy the VCF Import Tool to the Target vCenter Appliance at VMware Docs to copy the VCF Import Tool to the correct location.
2. Extract the bundle using the following command:

   ```
   tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
   ```

Validate the vCenter appliance

Use the VCF Import tool to validate the vCenter appliance before the import as VI Workload Domain.

1. Follow the steps at Run a Precheck on the Target vCenter Before Conversion to run the validation.

Create a JSON file for NSX deployment

To deploy NSX Manager while importing or converting a vSphere environment into VMware Cloud Foundation, create an NSX deployment specification. NSX deployment requires a minimum of 3 hosts.

> When deploying an NSX Manager cluster in a convert or import operation, NSX VLAN backed segment is used. For details on the limitations of NSX-VLAN backed segment, refer to the section "Considerations Before Converting or Importing Existing vSphere Environments into VMware Cloud Foundation. For information about NSX-VLAN networking limitations, refer to Considerations Before Converting or Importing Existing vSphere Environments into VMware Cloud Foundation.

The following is an example of a JSON file for NSX deployment:

```
{
  "deploy_without_license_keys": true,
  "form_factor": "small",
  "admin_password": "****************",
  "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-
133764.zip",
  "cluster_ip": "10.61.185.105",
  "cluster_fqdn": "mcc-wld01-nsx.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "mcc-wld01-nsxa.sddc.netapp.com",
    "name": "mcc-wld01-nsxa",
    "ip_address": "10.61.185.106",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-wld01-nsxb.sddc.netapp.com",
    "name": "mcc-wld01-nsxb",
    "ip_address": "10.61.185.107",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-wld01-nsxc.sddc.netapp.com",
    "name": "mcc-wld01-nsxc",
    "ip_address": "10.61.185.108",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Copy the JSON file to vcf user home folder on the SDDC Manager.

Upload software to SDDC Manager

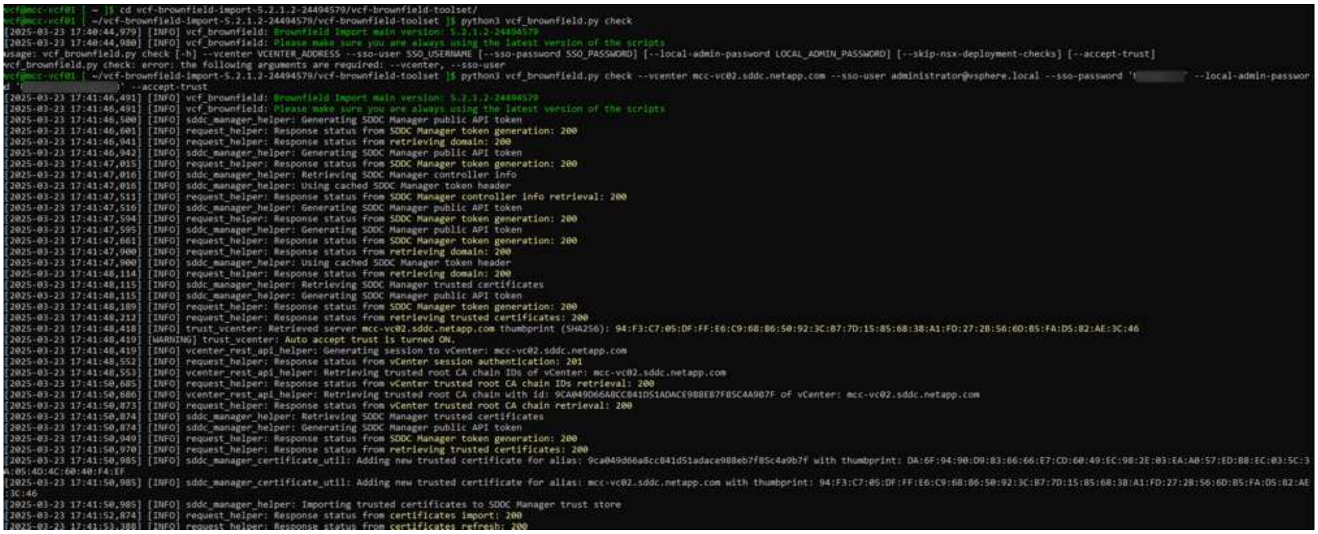
Copy the VCF Import Tool to home folder of vcf user and the NSX deployment bundle to /nfs/vmware/vcf/nfs-mount/bundle/ folder on the SDDC Manager.

See Upload the Required Software to the SDDC Manager Appliance for detailed instructions.

Detailed Check on vCenter before conversion

Before you perform a management domain convert operation or a VI workload domain import operation, you must perform a detailed check to ensure that the existing vSphere environment’s configuration is supported for convert or import.
. SSH to the SDDC Manager appliance as user vcf.
. Navigate to the directory where you copied the VCF Import Tool.
. Run the following command to check that the vSphere environment can be converted

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '********' --local-admin-password
'****************' --accept-trust
```



```
vcf@mcc-vcf01 [ ~ ]$ cd vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset/
vcf@mcc-vcf01 [ ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]$ python3 vcf_brownfield.py check
[2025-03-23 17:40:44,979] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.2-24494579
[2025-03-23 17:40:44,980] [INFO] vcf_brownfield: Please make sure you are always using the latest version of the scripts
usage: vcf_brownfield.py check [-h] --vcenter VCENTER_ADDRESS --sso-user SSO_USERNAME [--sso-password SSO_PASSWORD] [--local-admin-password LOCAL_ADMIN_PASSWORD] [--skip-nsx-deployment-checks] [--accept-trust]
vcf_brownfield.py check: error: the following arguments are required: --vcenter, --sso-user
vcf@mcc-vcf01 [ ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]$ python3 vcf_brownfield.py check --vcenter mcc-vc02.sddc.netapp.com --sso-user administrator@vsphere.local --sso-password '[redacted]' --local-admin-passwor
d '[redacted]' --accept-trust
[2025-03-23 17:41:46,491] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.2-24494579
[2025-03-23 17:41:46,491] [INFO] vcf_brownfield: Please make sure you are always using the latest version of the scripts
[2025-03-23 17:41:46,500] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:46,601] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:46,941] [INFO] request_helper: Response status from retrieving domain: 200
[2025-03-23 17:41:46,942] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:47,015] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:47,016] [INFO] sddc_manager_helper: Retrieving SDDC Manager controller info
[2025-03-23 17:41:47,016] [INFO] sddc_manager_helper: Using cached SDDC Manager token header
[2025-03-23 17:41:47,511] [INFO] request_helper: Response status from SDDC Manager controller info retrieval: 200
[2025-03-23 17:41:47,516] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:47,594] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:47,595] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:47,661] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:47,900] [INFO] request_helper: Response status from retrieving domain: 200
[2025-03-23 17:41:47,900] [INFO] sddc_manager_helper: Using cached SDDC Manager token header
[2025-03-23 17:41:48,114] [INFO] request_helper: Response status from retrieving domain: 200
[2025-03-23 17:41:48,115] [INFO] sddc_manager_helper: Retrieving SDDC Manager trusted certificates
[2025-03-23 17:41:48,115] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:48,189] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:48,212] [INFO] request_helper: Response status from retrieving trusted certificates: 200
[2025-03-23 17:41:48,418] [INFO] trust_vcenter: Retrieved server mcc-vc02.sddc.netapp.com thumbprint (SHA256): 94:F3:C7:05:DF:FF:E6:C9:68:86:50:92:3C:87:7D:15:85:68:38:A1:FD:27:28:56:6D:85:FA:D5:82:AE:3C:46
[2025-03-23 17:41:48,419] [WARNING] trust_vcenter: Auto accept trust is turned ON.
[2025-03-23 17:41:48,419] [INFO] vcenter_rest_api_helper: Generating session to vCenter: mcc-vc02.sddc.netapp.com
[2025-03-23 17:41:48,552] [INFO] request_helper: Response status from vCenter session authentication: 201
[2025-03-23 17:41:48,553] [INFO] vcenter_rest_api_helper: Retrieving trusted root CA chain IDs of vCenter: mcc-vc02.sddc.netapp.com
[2025-03-23 17:41:50,685] [INFO] request_helper: Response status from vCenter trusted root CA chain IDs retrieval: 200
[2025-03-23 17:41:50,686] [INFO] vcenter_rest_api_helper: Retrieving trusted root CA chain with id: 9CA049D66A8CC841D51ADACE988EB7F85C4A9B7F of vCenter: mcc-vc02.sddc.netapp.com
[2025-03-23 17:41:50,873] [INFO] request_helper: Response status from vCenter trusted root CA chain retrieval: 200
[2025-03-23 17:41:50,874] [INFO] sddc_manager_helper: Retrieving SDDC Manager trusted certificates
[2025-03-23 17:41:50,874] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:50,949] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:50,970] [INFO] request_helper: Response status from retrieving trusted certificates: 200
[2025-03-23 17:41:50,985] [INFO] sddc_manager_certificate_util: Adding new trusted certificate for alias: 9ca049d66a8cc841d51adace988eb7f85c4a9b7f with thumbprint: DA:6F:94:90:D9:83:66:66:E7:CD:60:49:EC:98:2E:03:EA:A0:57:ED:88:EC:03:5C:3
A:05:4D:4C:60:40:F4:EF
[2025-03-23 17:41:50,985] [INFO] sddc_manager_certificate_util: Adding new trusted certificate for alias: mcc-vc02.sddc.netapp.com with thumbprint: 94:F3:C7:05:DF:FF:E6:C9:68:86:50:92:3C:87:7D:15:85:68:38:A1:FD:27:28:56:6D:85:FA:D5:82:AE
:3C:46
[2025-03-23 17:41:50,985] [INFO] sddc_manager_helper: Importing trusted certificates to SDDC Manager trust store
[2025-03-23 17:41:52,874] [INFO] request_helper: Response status from certificates import: 200
[2025-03-23 17:41:53,388] [INFO] request_helper: Response status from certificates refresh: 200
```

Convert vSphere cluster to VCF VI Workload domain

The VCF Import Tool is used to conduct the conversion process.

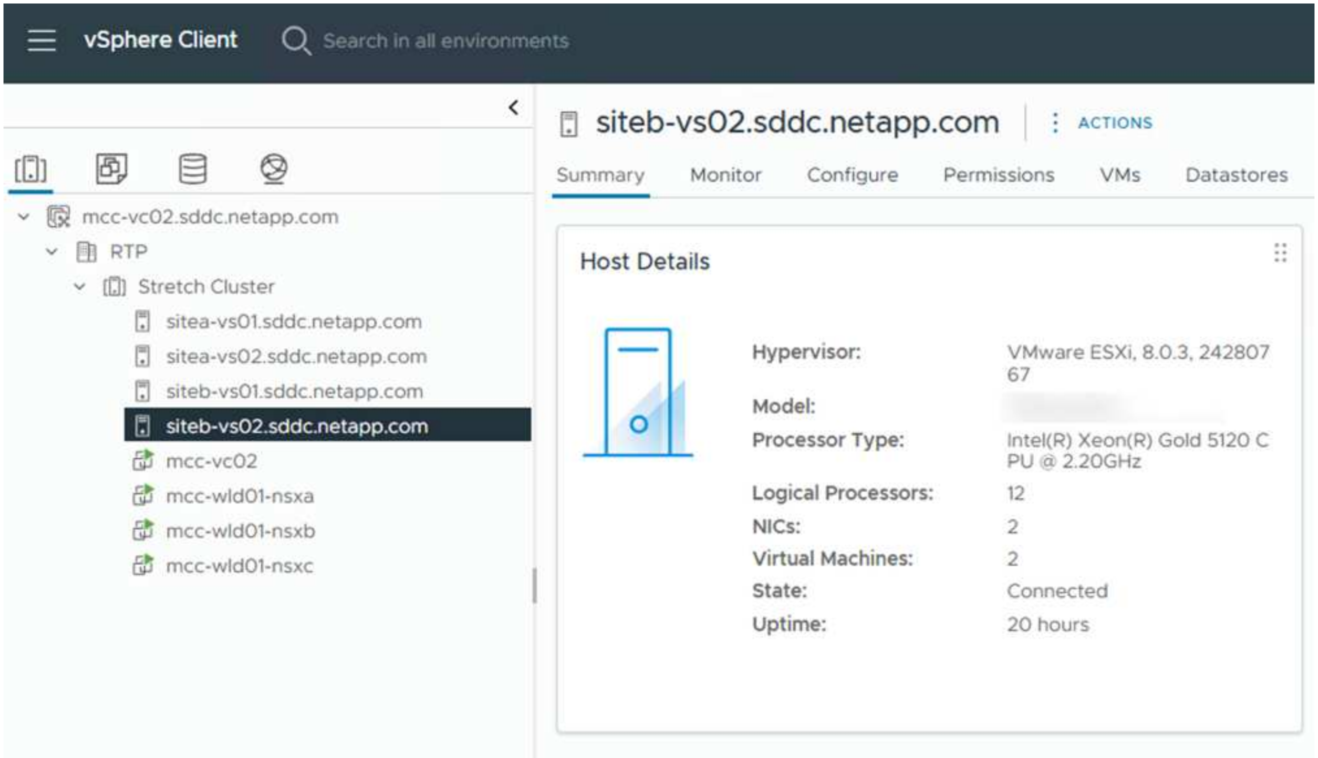
The following command is run to convert the vSphere cluster to a VCF management domain and deploy the NSX cluster:

```
python3 vcf_brownfield.py import --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '******' --vcenter-root-password '********'
--local-admin-password '****************' --backup-password
'****************' --domain-name '<Mgmt-domain-name>' --accept-trust
--nsx-deployment-spec-path /home/vcf/nsx.json
```

Even multiple Datastores are available on vSphere host, there is no need to prompt which Datastore that needs to be considered as Primary Datastore.

For complete instructions, refer to VCF Convert Procedure.

NSX VMs will be deployed to vCenter.



Host Details

Hypervisor: VMware ESXi, 8.0.3, 24280767

Model: [redacted]

Processor Type: Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz

Logical Processors: 12

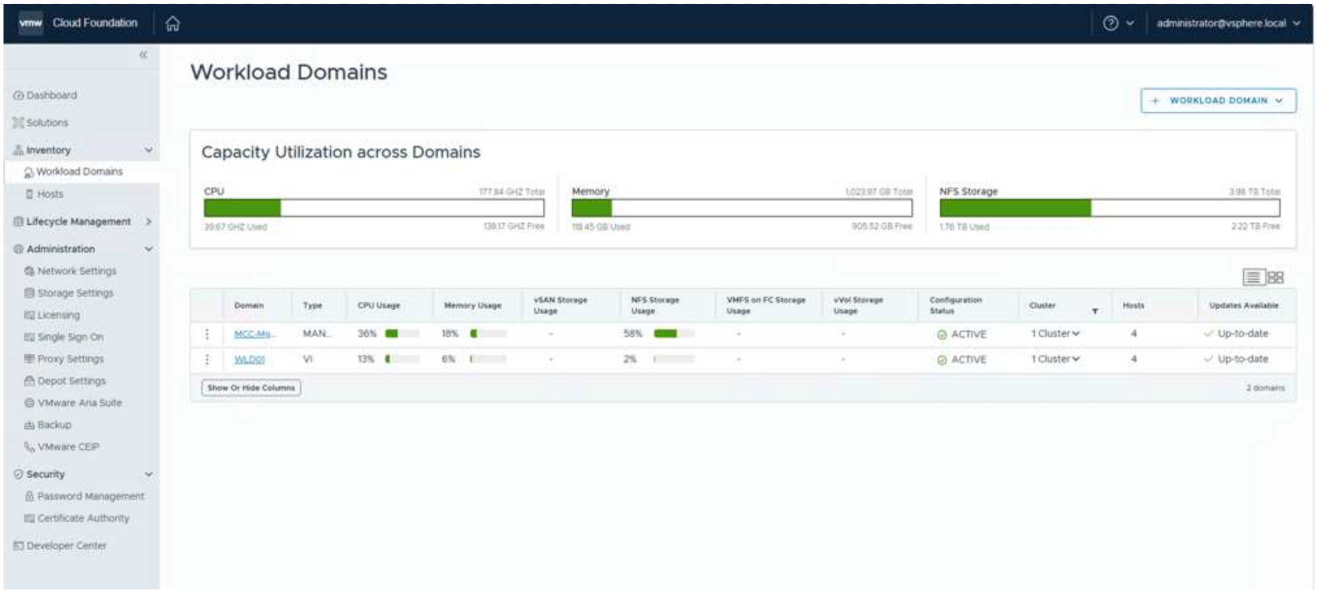
NICs: 2

Virtual Machines: 2

State: Connected

Uptime: 20 hours

SDDC Manager shows the VI Workload domain created with the name that was provided and NFS as Datastore.



Workload Domains

Capacity Utilization across Domains

CPU 177.84 GHZ Total, 39.67 GHZ Used, 138.17 GHZ Free

Memory 1,023.97 GB Total, 118.45 GB Used, 905.52 GB Free

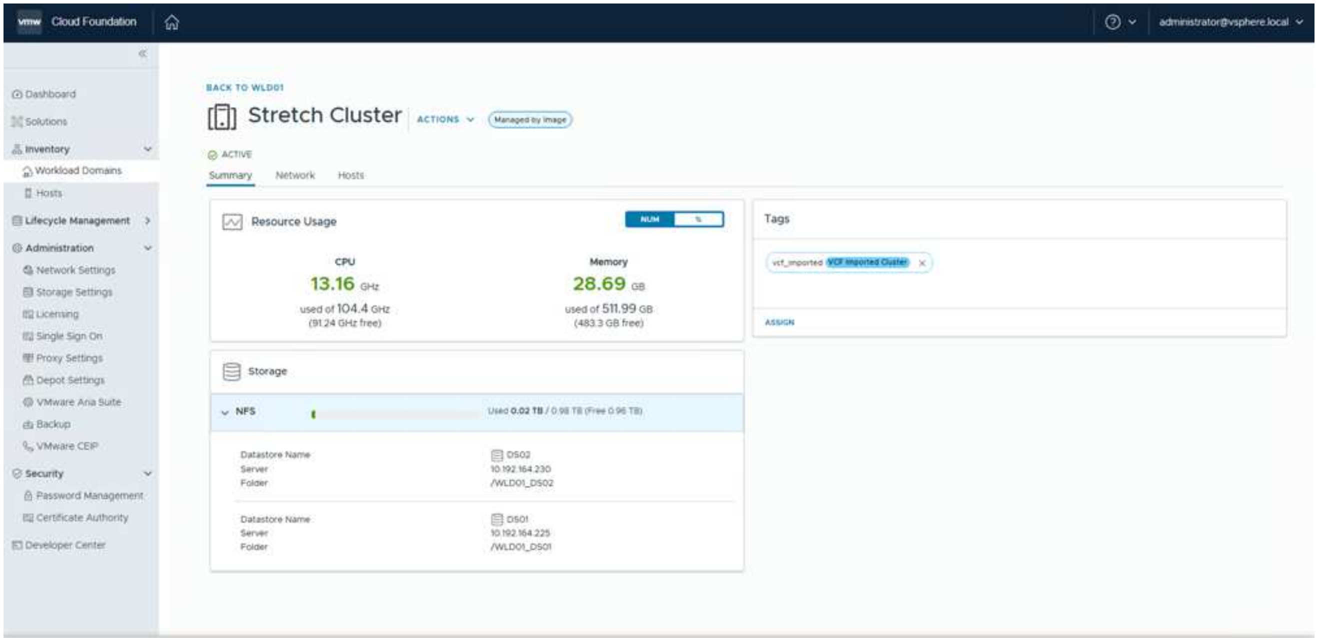
NFS Storage 3.98 TB Total, 1.76 TB Used, 2.22 TB Free

Domain	Type	CPU Usage	Memory Usage	vSAN Storage Usage	NFS Storage Usage	VMFS on FC Storage Usage	vVol Storage Usage	Configuration Status	Cluster	Hosts	Updates Available
MCC-Mg...	MAN...	36%	18%	-	58%	-	-	ACTIVE	1 Cluster	4	Up-to-date
WLD01	VI	13%	6%	-	2%	-	-	ACTIVE	1 Cluster	4	Up-to-date

Show Or Hide Columns

2 domains

On Inspecting the cluster, it provides the information of NFS Datastores.



Stretch Cluster

ACTIVE

Resource Usage

CPU 13.16 GHz used of 104.4 GHz (91.24 GHz free)

Memory 28.69 GB used of 511.99 GB (483.3 GB free)

Tags

vcf_imported VCF Imported Cluster

Storage

NFS Used 0.02 TB / 0.98 TB (Free 0.96 TB)

Datastore Name	DS02
Server	10.192.164.230
Folder	/WLD01_DS02
Datastore Name	DS01
Server	10.192.164.225
Folder	/WLD01_DS01

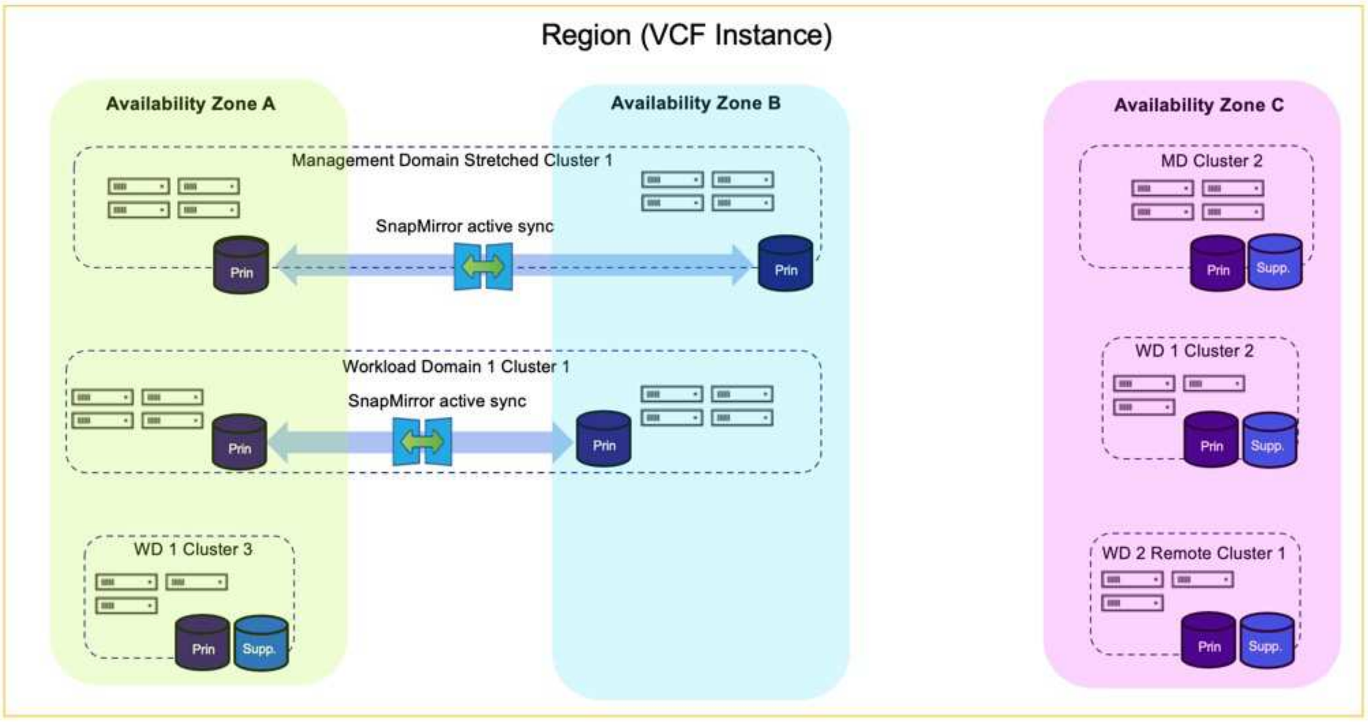
Add licensing to VCF

After completing the conversion, licensing must be added to the environment.

1. Log in to the SDDC Manager UI.
2. Navigate to **Administration > Licensing** in the navigation pane.
3. Click on **+ License Key**.
4. Choose a product from the drop-down menu.
5. Enter the license key.
6. Provide a description for the license.
7. Click **Add**.
8. Repeat these steps for each license.

Configure a stretch cluster for a VCF management domain using SnapMirror Active Sync

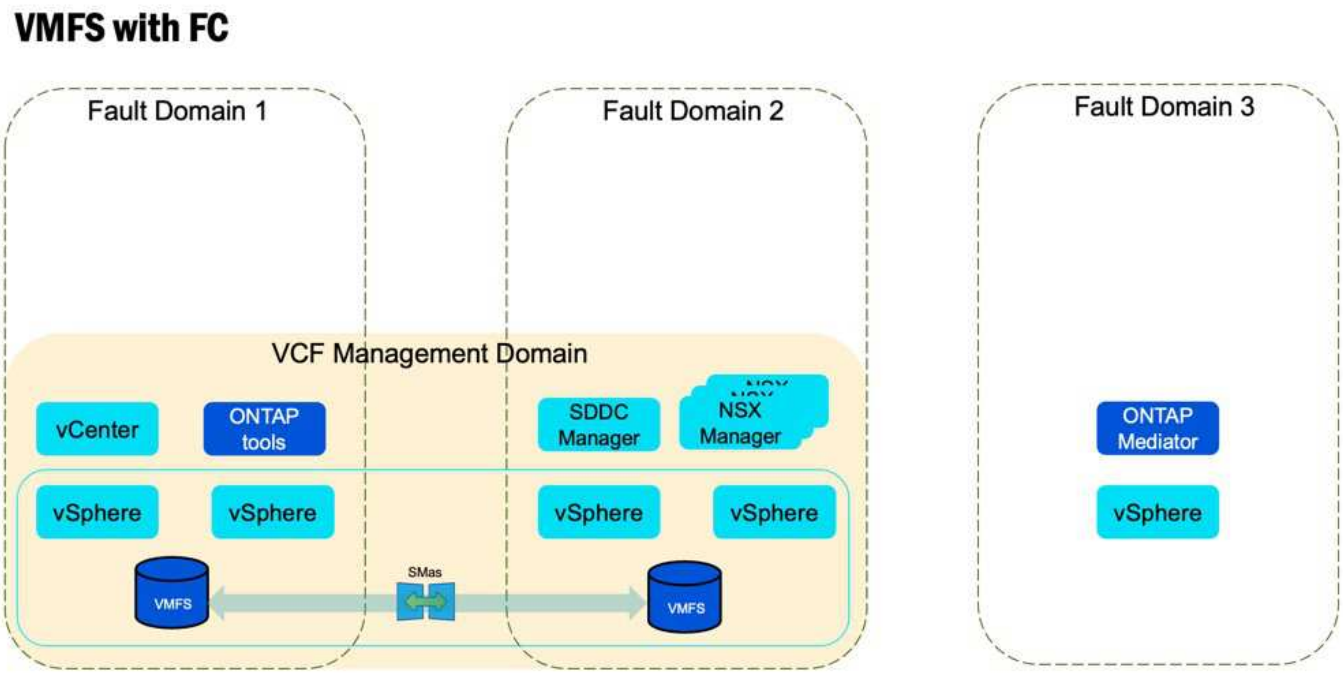
In this use case we outline the procedure to use ONTAP tools for VMware vSphere to configure a stretch cluster for a VCF management domain. This procedure includes deploying vSphere hosts and vCenter Server, installing ONTAP tools, protecting datastores with SnapMirror Active Sync, migrating VMs to protected datastores, and configuring supplemental storage.



Scenario Overview

The stretch cluster solution can be implemented on default cluster or on additional cluster in VCF management or workload domains. VMFS on FC is supported on both principal datastore and supplemental datastores.

VMFS on iSCSI is only supported with supplemental datastores. Refer IMT for support of VMFS on NVMe-oF with SnapMirror active sync.



Principal storage on Management Domain

With VCF 5.2 onwards managment domain can be deployed without VSAN using the VCF import Tool. The convert option of VCF import tool allows an existing vCenter deployment into a management domain. All the clusters in vCenter will become part of management domain.

1. Deploy vSphere hosts
2. Deploy vCenter server on local datastore (vCenter needs to co-exist on vSphere hosts that will be converted into management domain)
3. Deploy ONTAP tools for VMware vSphere
4. Deploy SnapCenter Plugin for VMware vSphere (optional)
5. Create datastore (FC zone configuration should be in place)
6. Protect the vSphere cluster
7. Migrate VMs to newly created datastore

ⓘ Whenever the cluster is expanded or shrank, need to update the Host Cluster relationship on ONTAP tools for the cluster to indicate the changes made to source or target.

Supplemental storage on Management Domain

Once the management domain is up and running, additional datastores can be created using ONTAP tools which will trigger the consistency group expansion.

> If a vSphere cluster is protected, all the datastores in the cluster will be protected.

If VCF environment is deployed with Cloud Builder tool, to create the supplemental storage with iSCSI, deploy ONTAP tools to create the iSCSI datastore and protect the vSphere cluster.

> Whenever the cluster is expanded or shrank, need to update the Host Cluster relationship on ONTAP tools for the cluster to indicate the changes made to source or target.

Additional information

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

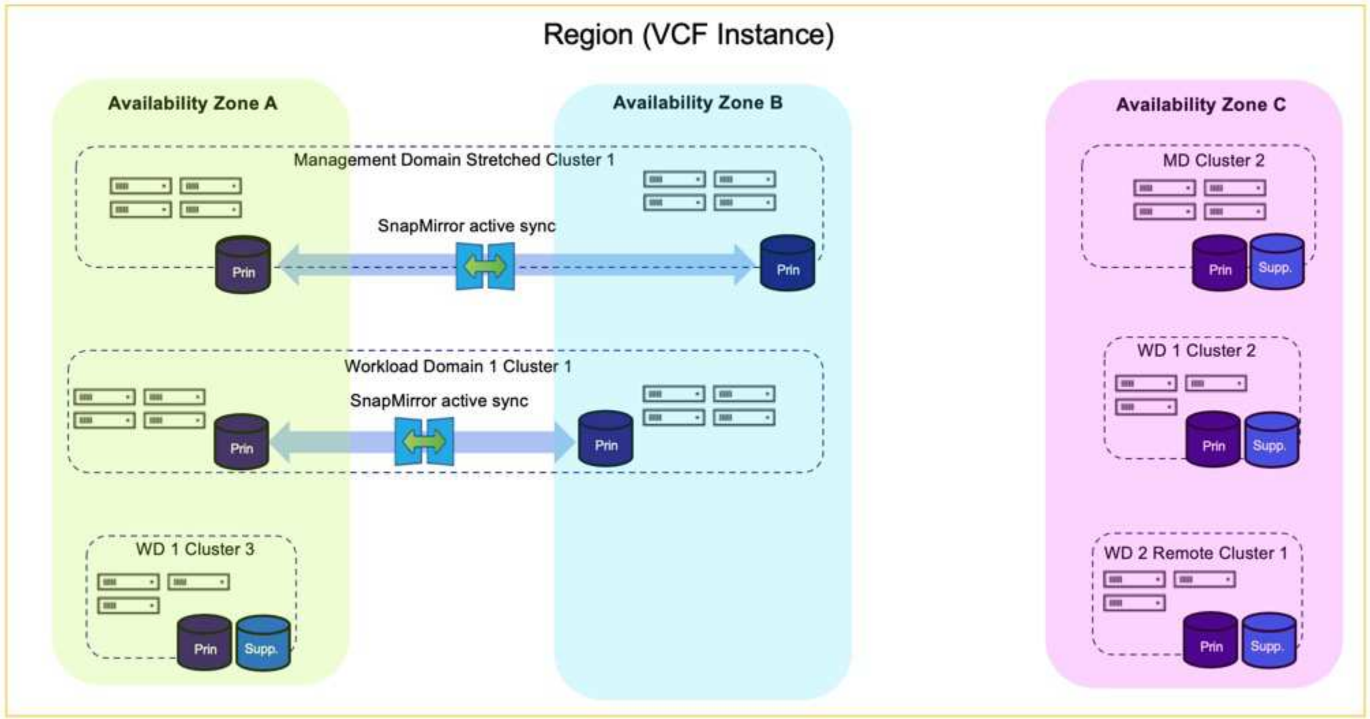
For information on configuring VCF refer to VMware Cloud Foundation 5.2 Documentation.

Video demo for this solution

Stretch cluster for VCF with ONTAP tools

Configure a stretch cluster for a VI workload domain using SnapMirror Active Sync

In this use case we outline the procedure to configure a stretch cluster for a Virtual Infrastructure (VI) workload domain using SnapMirror Active Sync with ONTAP tools for VMware vSphere. This procedure includes creating a VCF Workload Domain with VMFS on Fibre Channel, registering the vCenter with ONTAP tools, registering storage systems, and protecting the vSphere cluster.



Scenario Overview

The datastores on VCF Workload domain can be protected with SnapMirror active sync to provide stretch cluster solution. The protection is enabled at vSphere cluster level and all ONTAP block datastores in the cluster will be protected.

Principal storage on Workload Domain

Workload domain can be created either importing using the VCF import tool or deploy using the SDDC manager. Deploying with SDDC manager will provide more networking options than importing an existing environment.

1. Create Workload domain with VMFS on FC
2. Register workload domain vCenter to ONTAP tools manager to deploy vCenter plugin
3. Register storage systems on ONTAP tools
4. Protect the vSphere cluster

Whenever the cluster is expanded or shrank, need to update the Host Cluster relationship on ONTAP tools for the cluster to indicate the changes made to source or target.

Supplemental storage on Workload Domain

Once the workload domain is up and running, additional datastores can be created using ONTAP tools which will trigger the consistency group expansion.

If a vSphere cluster is protected, all the datastores in the cluster will be protected.

Additional information

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

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

Video demo for this solution

Stretch cluster for VCF with ONTAP tools

Migrate VMs from VMware vSphere to ONTAP datastores

VMware vSphere environments can significantly benefit from migrating virtual machines to NetApp ONTAP-backed datastores. Whether you’re moving from vSAN, third-party storage systems, or upgrading your existing infrastructure, explore various vMotion scenarios and migration strategies to seamlessly transition your VMs to ONTAP datastores. This ensures business continuity while leveraging ONTAP’s enterprise-class storage features.

VMware vSphere by Broadcom supports VMFS, NFS, and vVol datastores for hosting virtual machines. Customers have the option to create those datastores with hyper converged infrastructures or with centralized shared storage systems.

Customers often see the value with hosting on ONTAP based storage systems to provide space efficient snapshots and clones of Virtual machines, flexibility to choose various deployment models across the datacenters and clouds, operational efficiency with monitoring and alerting tools, security, governance and optional compliance tools to inspect VM data, and so on.

VMs hosted on ONTAP datastores can be protected using SnapCenter Plugin for VMware vSphere (SCV). SCV creates storage based snapshots and also replicates to remote ONTAP storage system. Restores can be performed either from Primary or Secondary storage systems.

Customers has flexibility to choose Cloud Insights or Aria Operations or combination of both or other third party tools that use ONTAP api to troubleshoot, performance monitoring, reporting and alert notification features.

Customers can easily provision datastore using ONTAP Tools vCenter Plug-in or its API and VMs can be migrated to ONTAP datastores even while it is powered on.

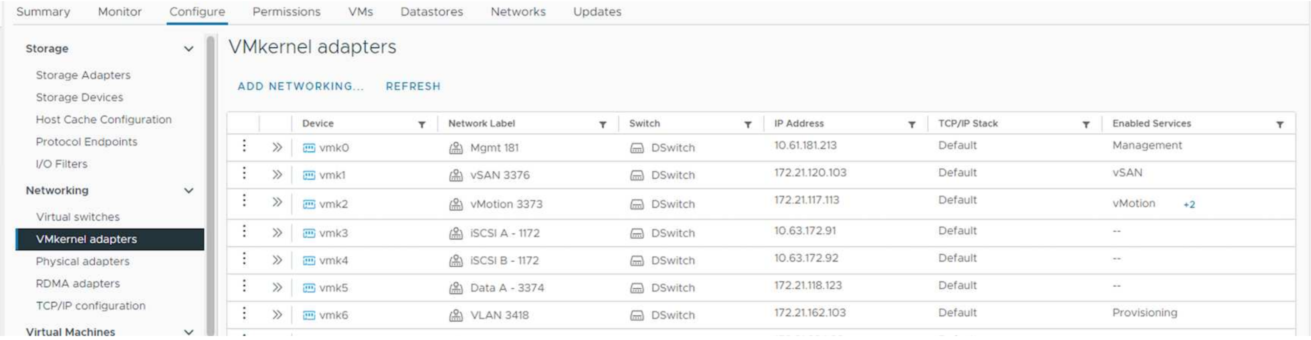
> Some VMs which are deployed with external management tool like VCF Automation, vSphere Supervisor (or other Kubernetes flavors) are usually depends on VM storage policy. If migrating between the datastores within same VM storage policy, it should be of less impact for the applications. Check with Application owners to properly migrate those VMs to new datastore. vSphere 8 introduced vSphere vMotion Notifications for Latency Sensitive Applications to prepare applications for vMotion.

Network Requirements

VM migration with vMotion

It is assumed that dual storage network is already in place for the ONTAP datastore to provide connectivity, fault tolerance and performance boost.

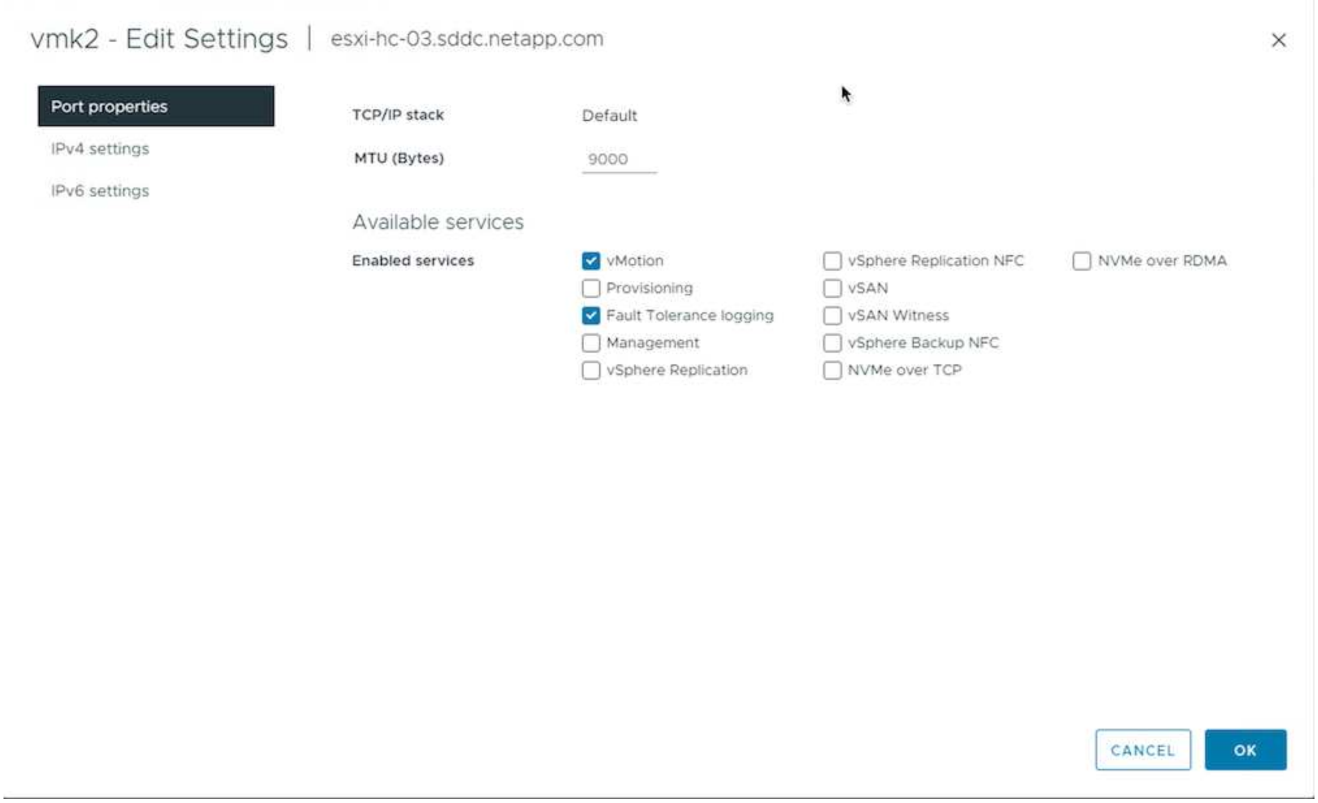
Migration of VMs across the vSphere hosts are also handled by the VMKernel interface of the vSphere host. For hot migration (powered on VMs), VMKernel interface with vMotion enabled service is used and for cold migration (powered off VMs), VMKernel interface with Provisioning service enabled is consumed to move the data. If no valid interface was found, it will use the management interface to move the data which may not be desirable for certain use cases.



VMkernel adapters

Device	Network Label	Switch	IP Address	TCP/IP Stack	Enabled Services
vmk0	Mgmt 181	DSwitch	10.61.181.213	Default	Management
vmk1	vSAN 3376	DSwitch	172.21.120.103	Default	vSAN
vmk2	vMotion 3373	DSwitch	172.21.117.113	Default	vMotion +2
vmk3	iSCSI A - 1172	DSwitch	10.63.172.91	Default	--
vmk4	iSCSI B - 1172	DSwitch	10.63.172.92	Default	--
vmk5	Data A - 3374	DSwitch	172.21.118.123	Default	--
vmk6	VLAN 3418	DSwitch	172.21.162.103	Default	Provisioning

When you edit the VMKernel interface, here is the option to enable the required services.



vmk2 - Edit Settings | esxi-hc-03.sddc.netapp.com

TCP/IP stack: Default

MTU (Bytes): 9000

Available services

Enabled services

☑ vMotion
☐ Provisioning
☑ Fault Tolerance logging
☐ Management
☐ vSphere Replication
☐ vSphere Replication NFC
☐ vSAN
☐ vSAN Witness
☐ vSphere Backup NFC
☐ NVMe over TCP
☐ NVMe over RDMA

Ensure at least two high-speed active uplink nics are available for the portgroup used by vMotion and Provisioning VMkernel interfaces.

VM Migration Scenarios

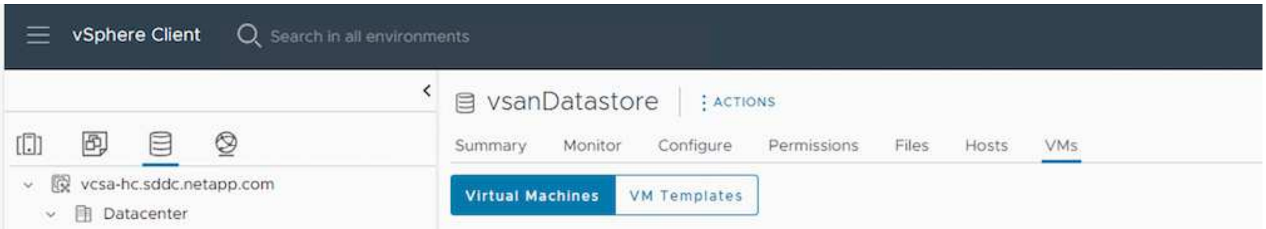
vMotion is often used to migrate the VMs irrespective of its power state. Additional considerations and migration procedure for specific scenarios is available below.

> ⓘ Understand VM Conditions and Limitation of vSphere vMotion before proceeding with any VM migration options.

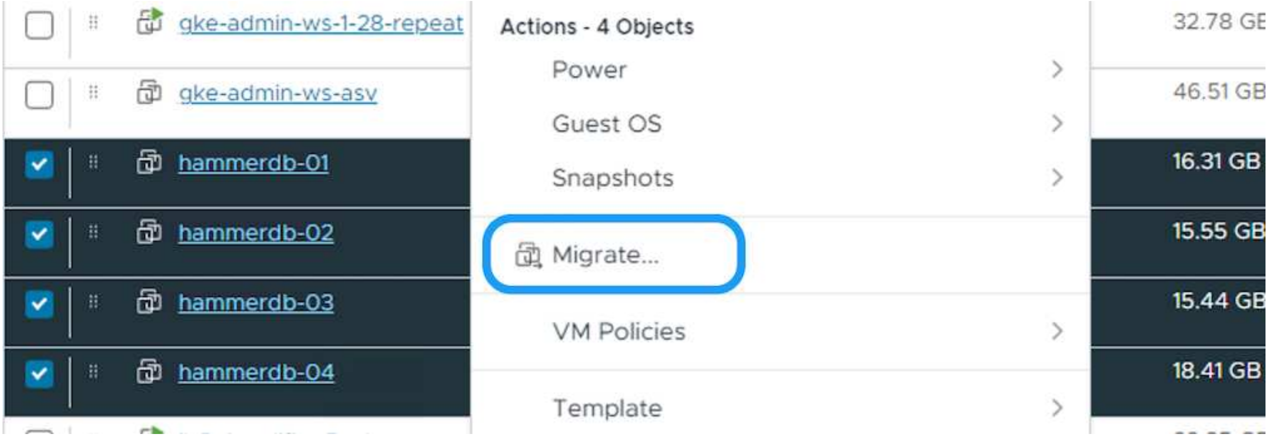
Migration of VMs from specific vSphere Datastore

Follow the procedure below to migrate VMs to new Datastore using UI.

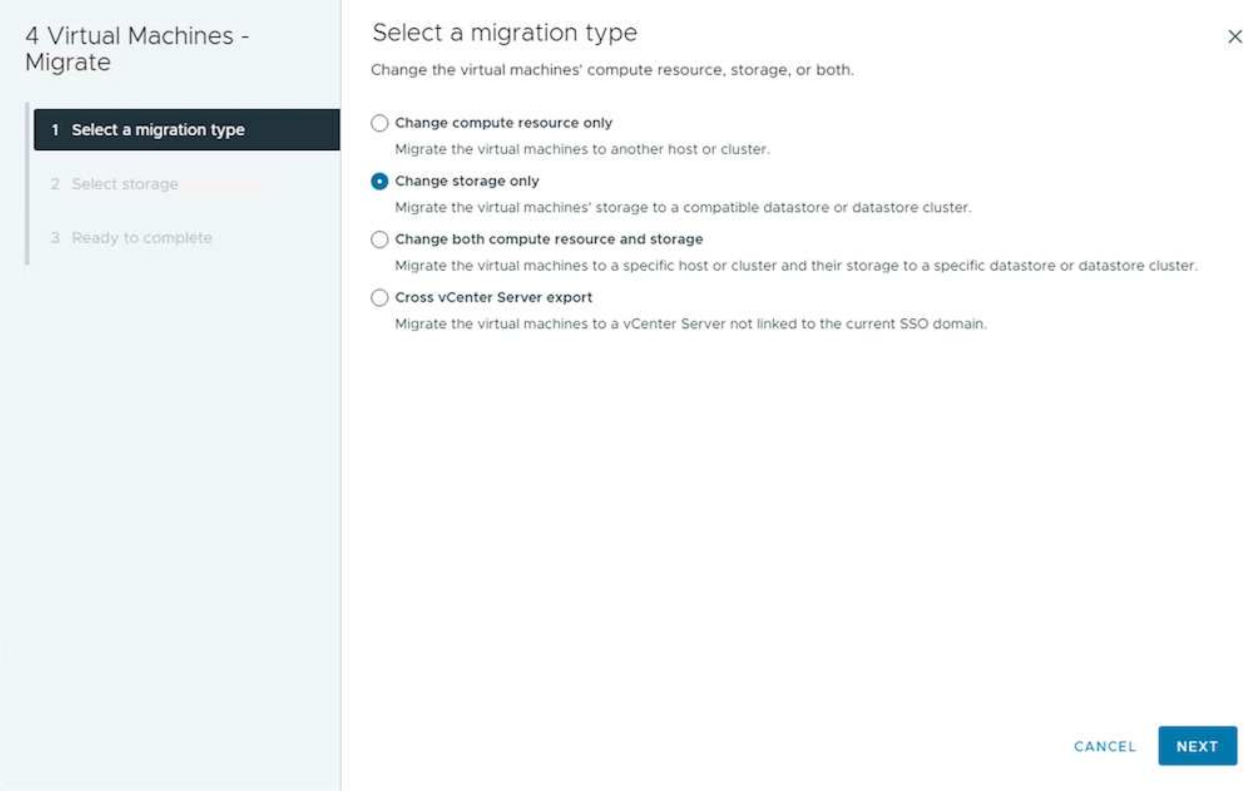
1. With vSphere Web Client, select the Datastore from the storage inventory and click on VMs tab.



2. Select the VMs that needs to be migrated and right click to select Migrate option.



3. Choose option to change storage only, Click Next



Select a migration type

Change the virtual machines' compute resource, storage, or both.

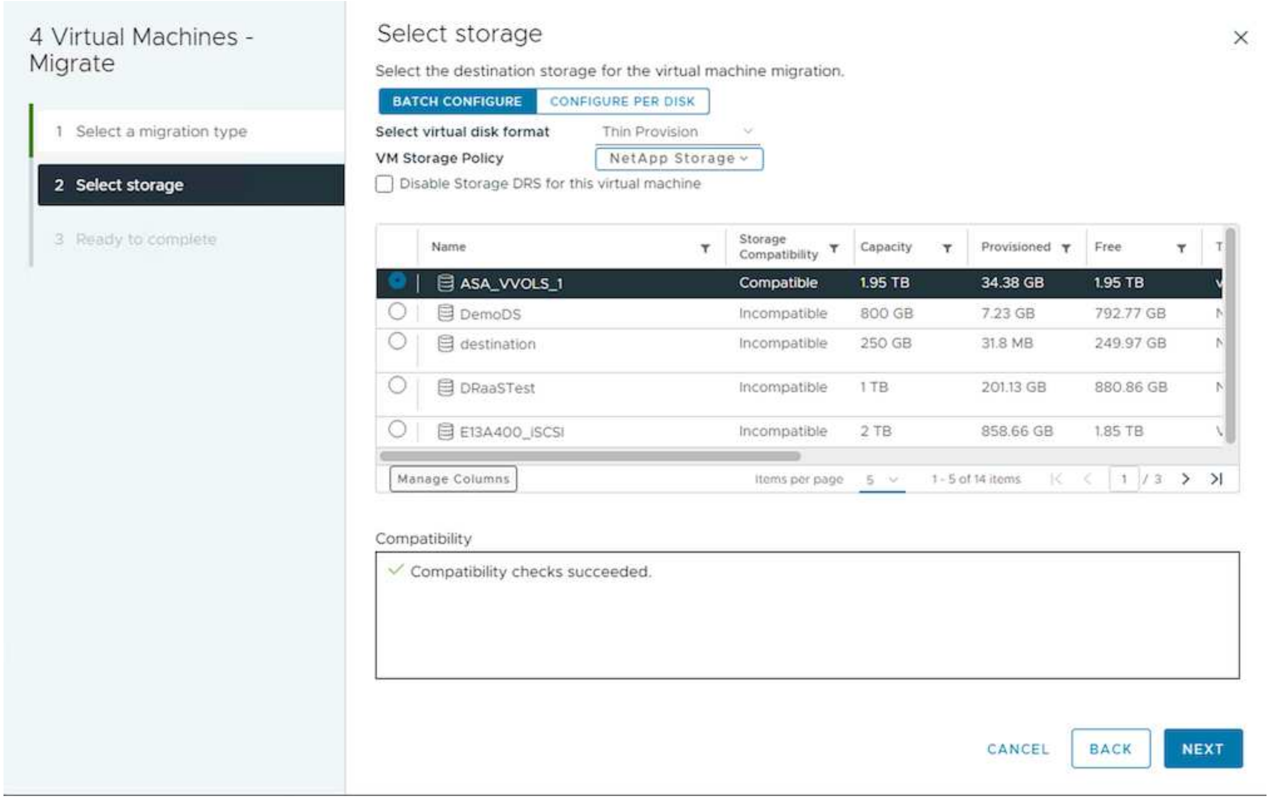
○ Change compute resource only
Migrate the virtual machines to another host or cluster.

● Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

○ Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

○ Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

4. Select the desired VM Storage Policy and pick the datastore that is compatible. Click Next.



4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE | CONFIGURE PER DISK

Select virtual disk format: Thin Provision

VM Storage Policy: NetApp Storage

□ Disable Storage DRS for this virtual machine

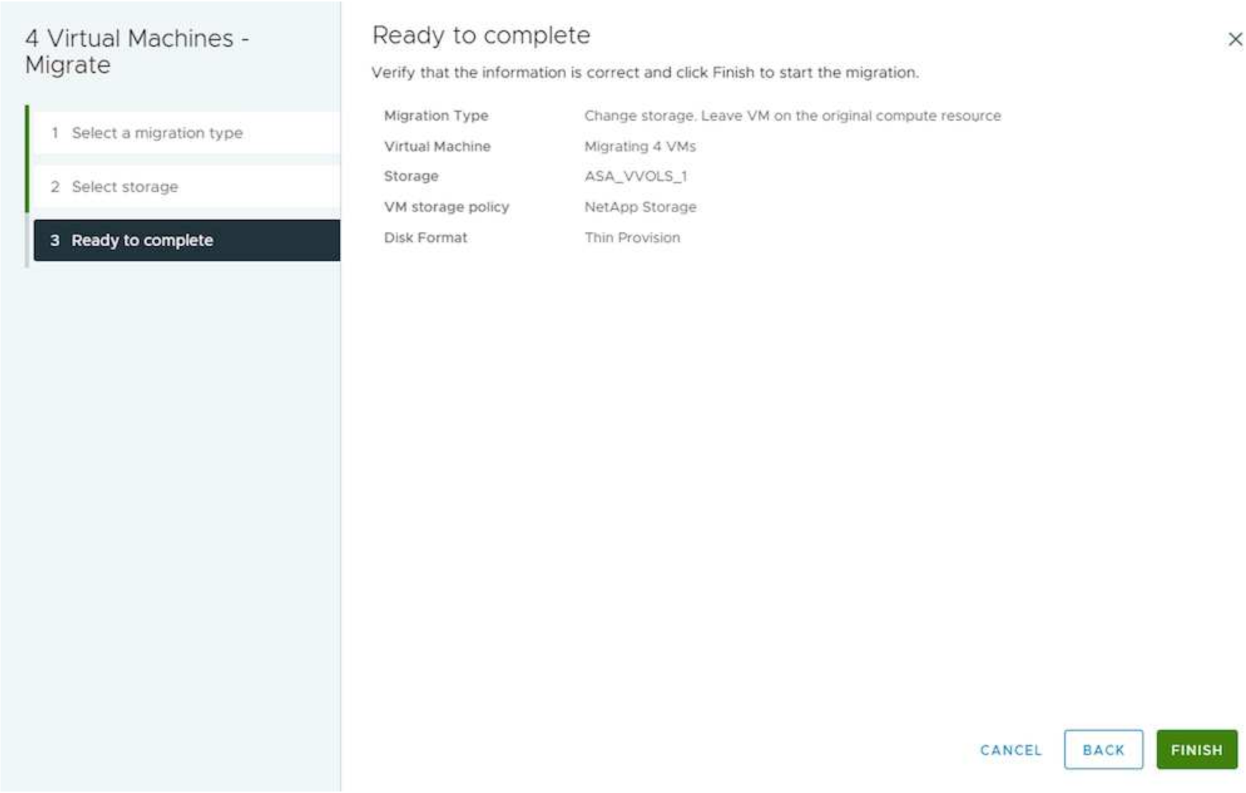
	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB	V
○	DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB	N
○	destination	Incompatible	250 GB	31.8 MB	249.97 GB	N
○	DRaaSTest	Incompatible	1 TB	201.13 GB	880.86 GB	N
○	E13A400_iSCSI	Incompatible	2 TB	858.66 GB	1.85 TB	V

Manage Columns   Items per page 5   1 - 5 of 14 items   1 / 3

Compatibility

✓ Compatibility checks succeeded.

5. Review and click on Finish.



4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

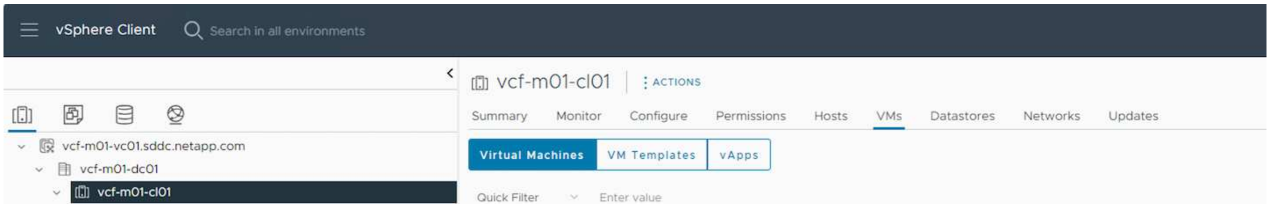
To migrate VMs using PowerCLI, here is the sample script.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific datastore
$vm = Get-DataStore 'vSanDatastore' | Get-VM Har*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

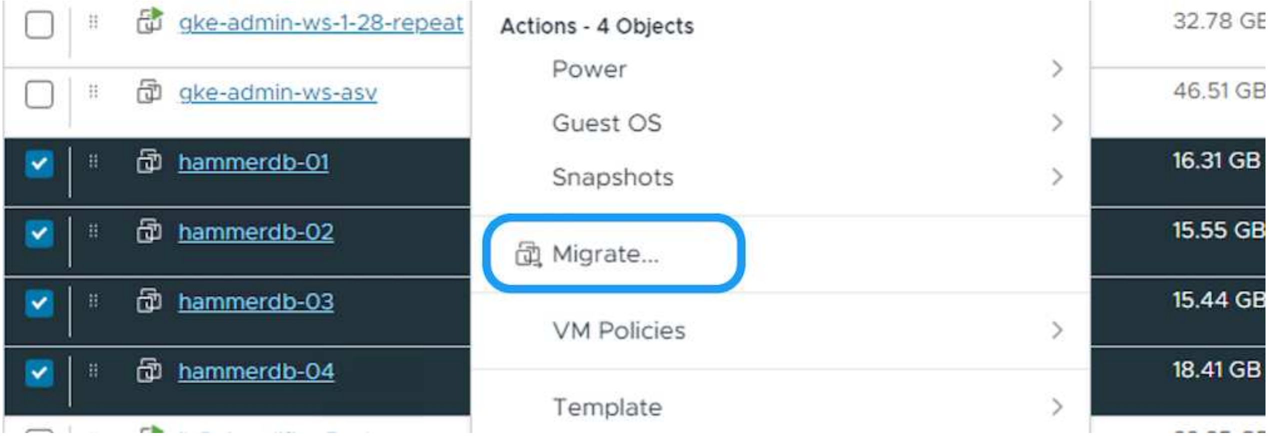
Migration of VMs in same vSphere cluster

Follow the procedure below to migrate VMs to new Datastore using UI.

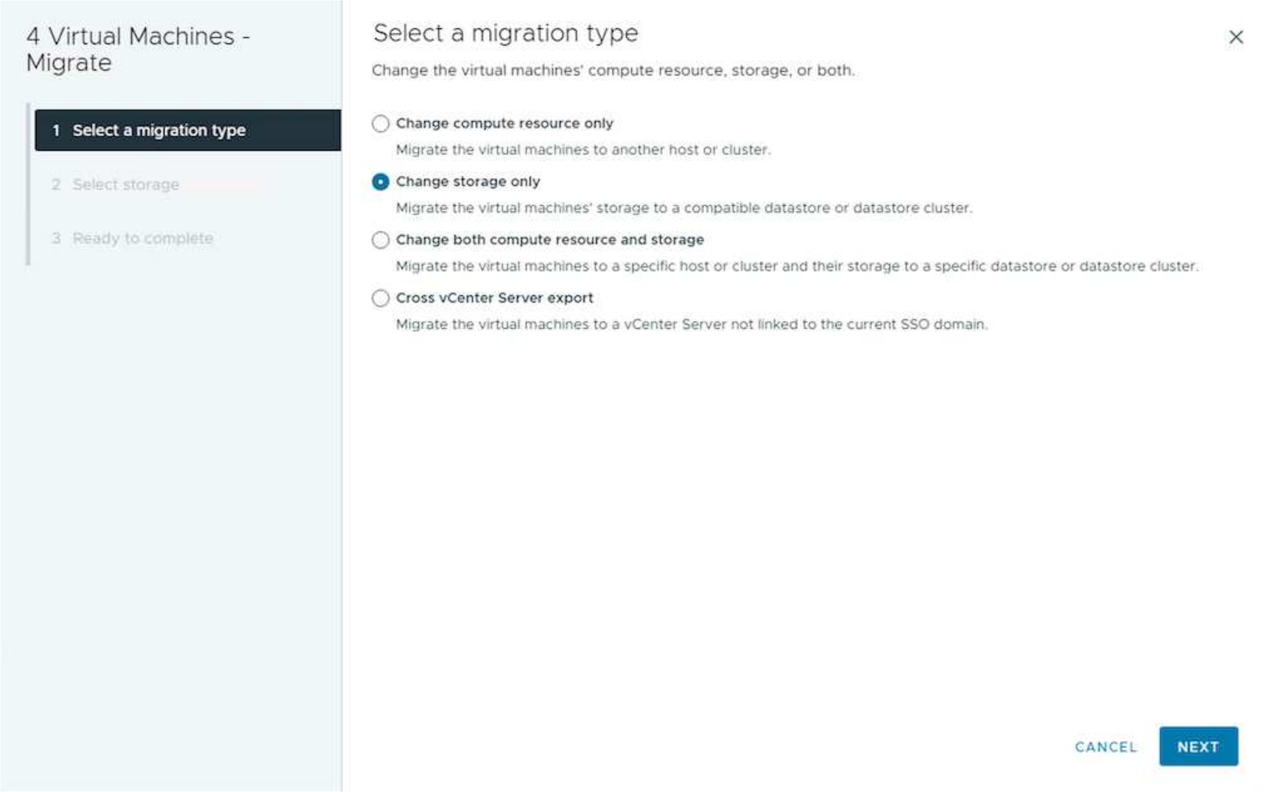
1. With vSphere Web Client, select the Cluster from the Host and Cluster inventory and click on VMs tab.



2. Select the VMs that needs to be migrated and right click to select Migrate option.



3. Choose option to change storage only, Click Next



Select a migration type

Change the virtual machines' compute resource, storage, or both.

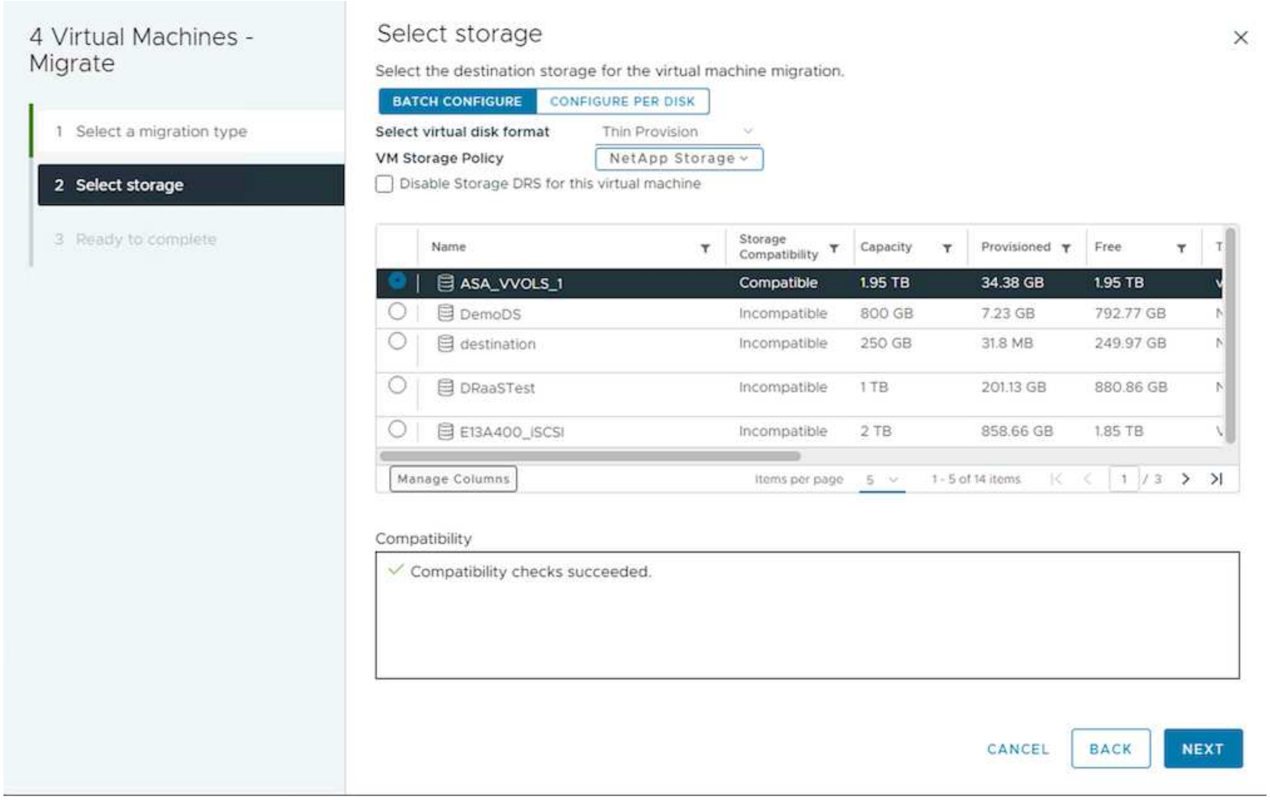
○ Change compute resource only
Migrate the virtual machines to another host or cluster.

● Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

○ Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

○ Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

4. Select the desired VM Storage Policy and pick the datastore that is compatible. Click Next.



4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE | CONFIGURE PER DISK

Select virtual disk format: Thin Provision

VM Storage Policy: NetApp Storage

□ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB	V
○	DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB	N
○	destination	Incompatible	250 GB	31.8 MB	249.97 GB	N
○	DRaaSTest	Incompatible	1 TB	201.13 GB	880.86 GB	N
○	E13A400_iSCSI	Incompatible	2 TB	858.66 GB	1.85 TB	V

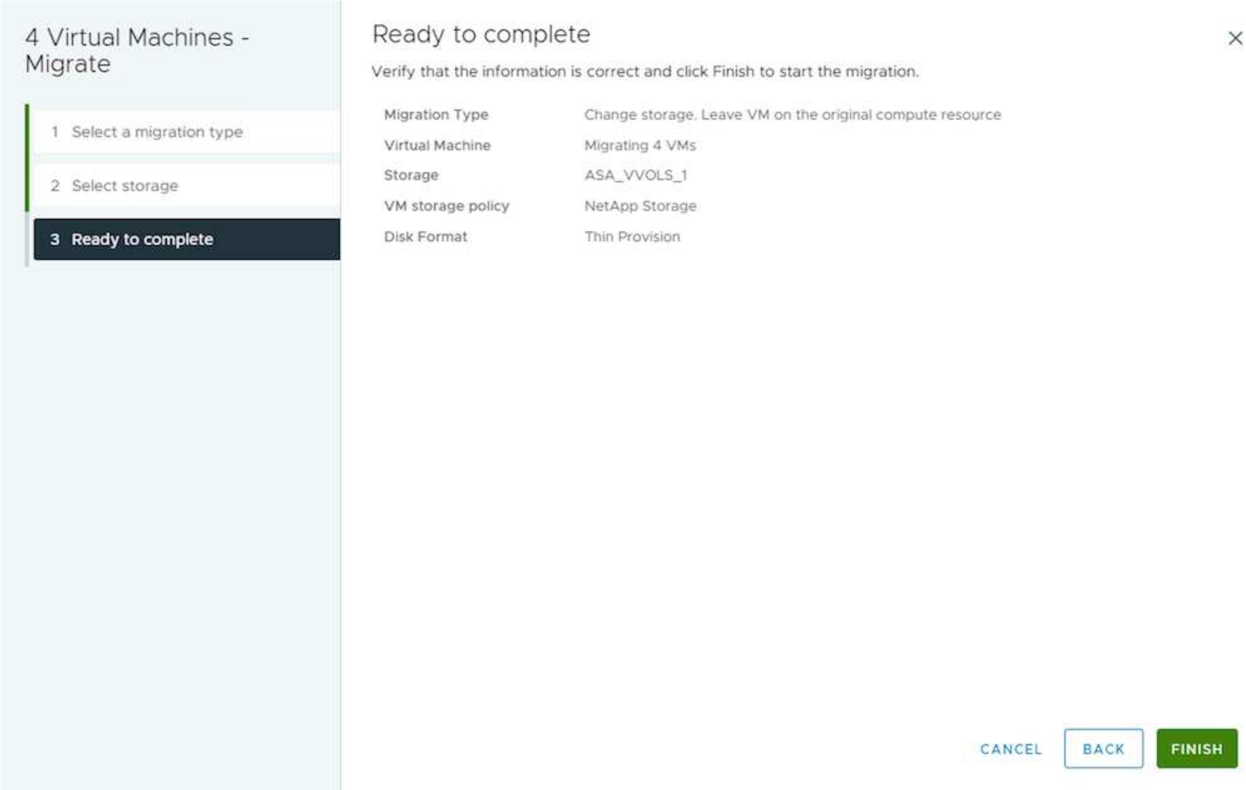
Manage Columns   Items per page 5   1 - 5 of 14 items   1 / 3

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

5. Review and click on Finish.



4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL BACK FINISH

To migrate VMs using PowerCLI, here is the sample script.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

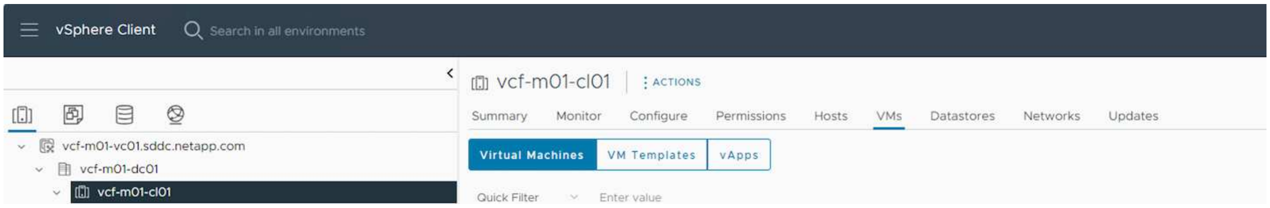
When Datastore Cluster is in use with fully automated storage DRS (Dynamic Resource Scheduling) and both (source & target) datastores are of same type (VMFS/NFS/vVol), Keep both datastores in same storage cluster and migrate VMs from source datastore by enabling maintenance mode on the source. Experience will be similar to how compute hosts are handled for maintenance.

Migration of VMs across multiple vSphere clusters

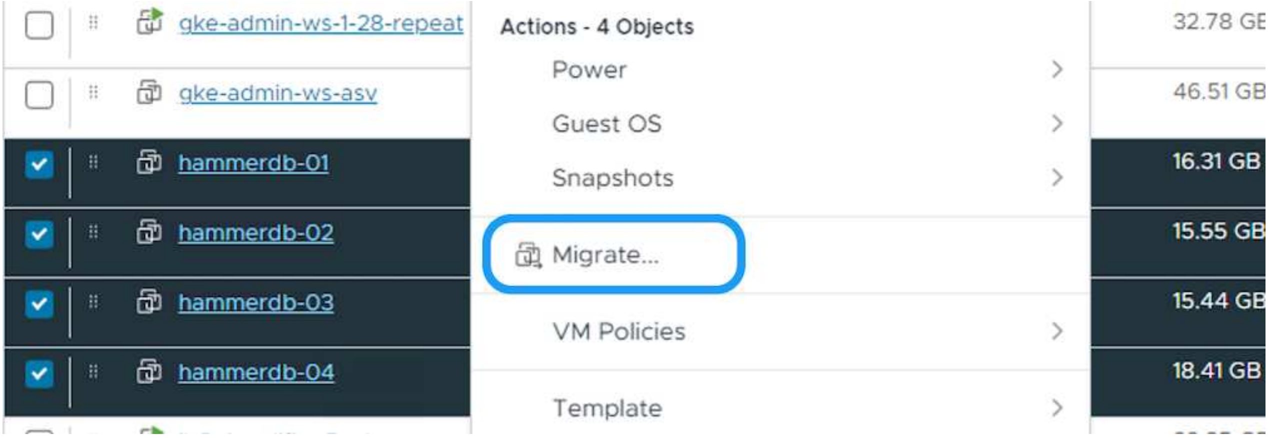
Refer CPU Compatibility and vSphere Enhanced vMotion Compatibility when source and target hosts are of different CPU family or model.

Follow the procedure below to migrate VMs to new Datastore using UI.

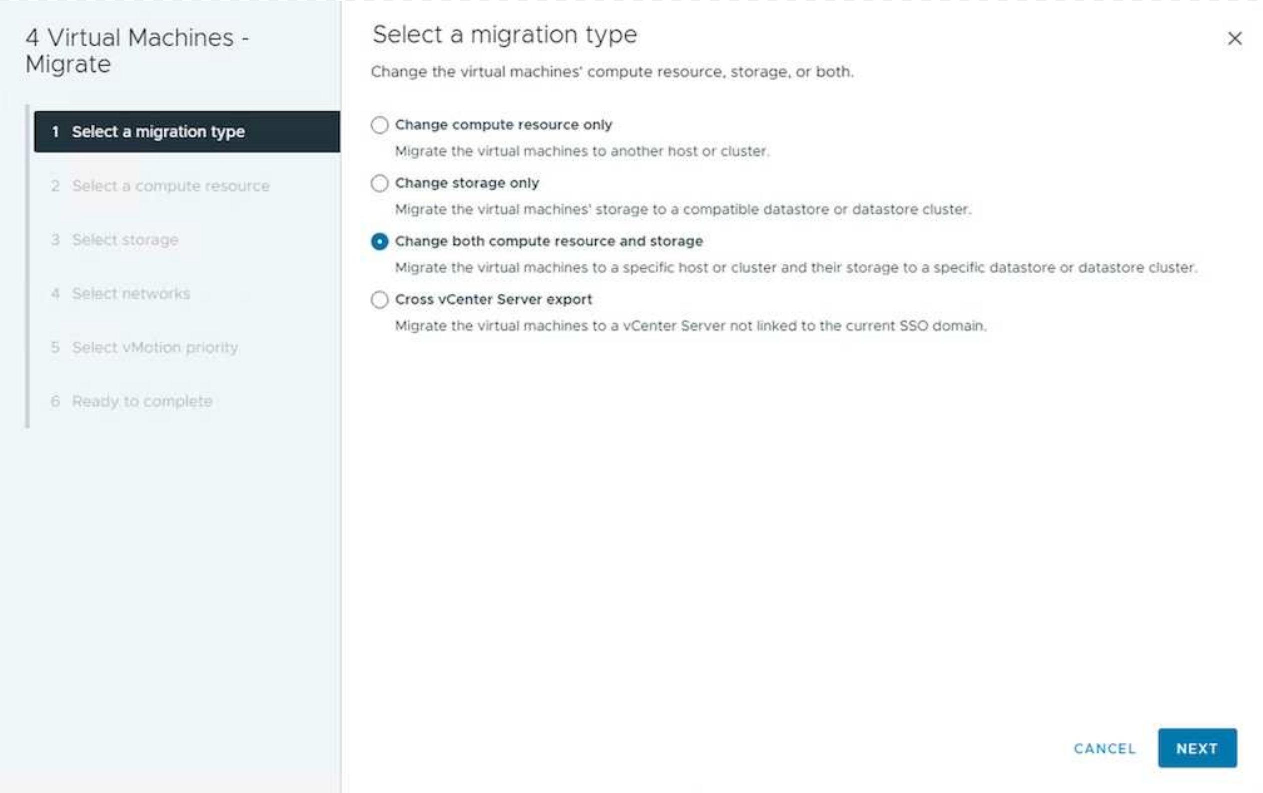
1. With vSphere Web Client, select the Cluster from the Host and Cluster inventory and click on VMs tab.



2. Select the VMs that needs to be migrated and right click to select Migrate option.



3. Choose option to change compute resource and storage, Click Next



4 Virtual Machines - Migrate

1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select networks
5 Select vMotion priority
6 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

○ Change compute resource only

Migrate the virtual machines to another host or cluster.

○ Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

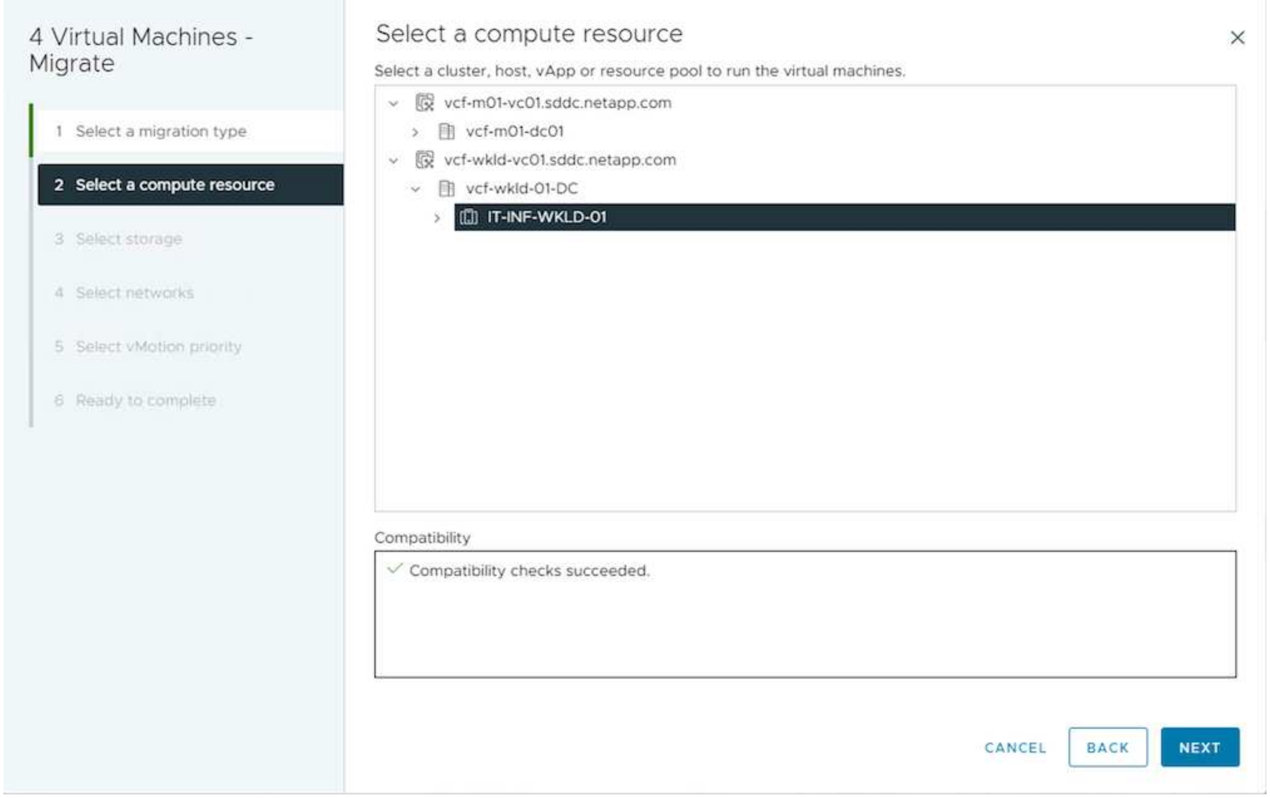
● Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

○ Cross vCenter Server export

Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

4. Navigate and pick the right cluster to migrate.



4 Virtual Machines - Migrate

1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select networks
5 Select vMotion priority
6 Ready to complete

Select a compute resource

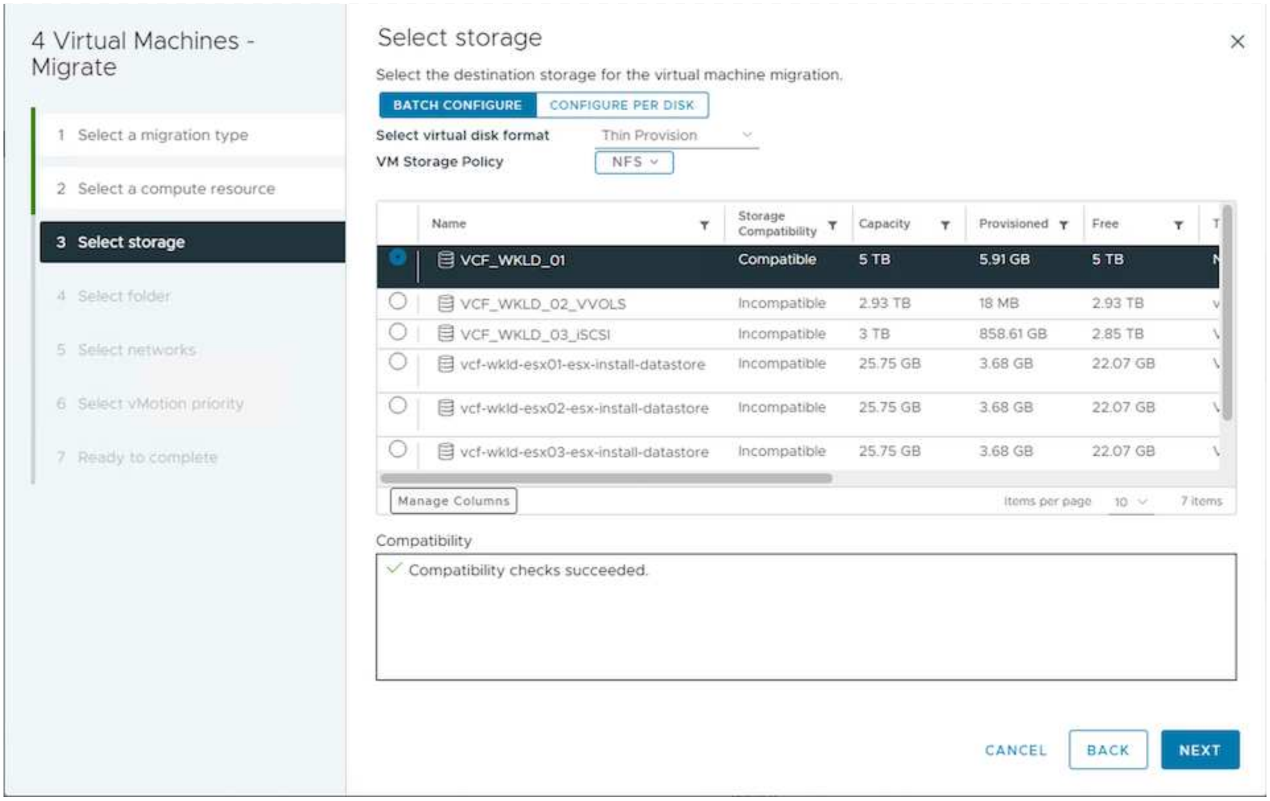
Select a cluster, host, vApp or resource pool to run the virtual machines.

vcf-m01-vc01.sddc.netapp.com
vcf-m01-dc01
vcf-wkld-vc01.sddc.netapp.com
vcf-wkld-01-DC
IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

5. Select the desired VM Storage Policy and pick the datastore that is compatible. Click Next.



4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select folder

5 Select networks

6 Select vMotion priority

7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE | CONFIGURE PER DISK

Select virtual disk format: Thin Provision

VM Storage Policy: NFS

	Name	Storage Compatibility	Capacity	Provisioned	Free
●	VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB
○	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB
○	VCF_WKLD_03_iSCSI	Incompatible	3 TB	858.61 GB	2.85 TB
○	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB
○	vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB
○	vcf-wkld-esx03-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB

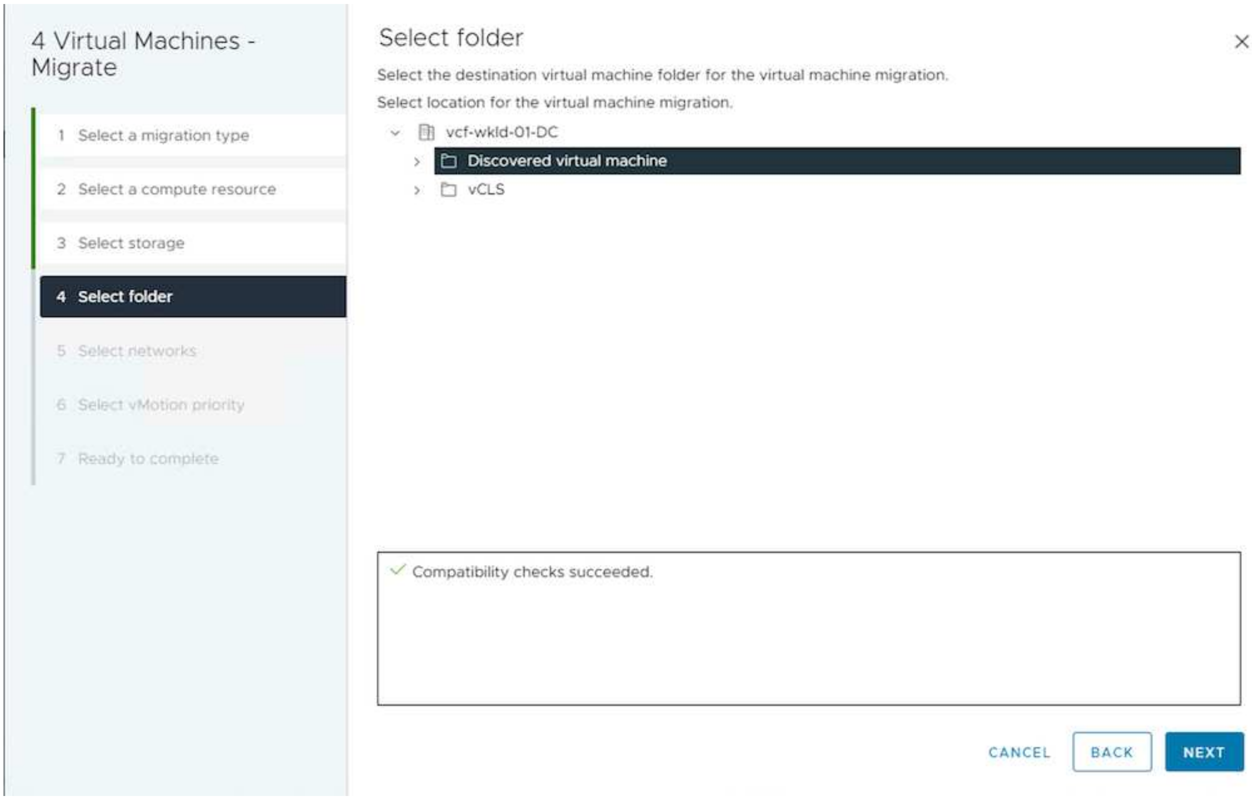
Manage Columns | Items per page 10 | 7 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL | BACK | NEXT

6. Pick the VM folder to place the target VMs.



4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select folder

5 Select networks

6 Select vMotion priority

7 Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration.

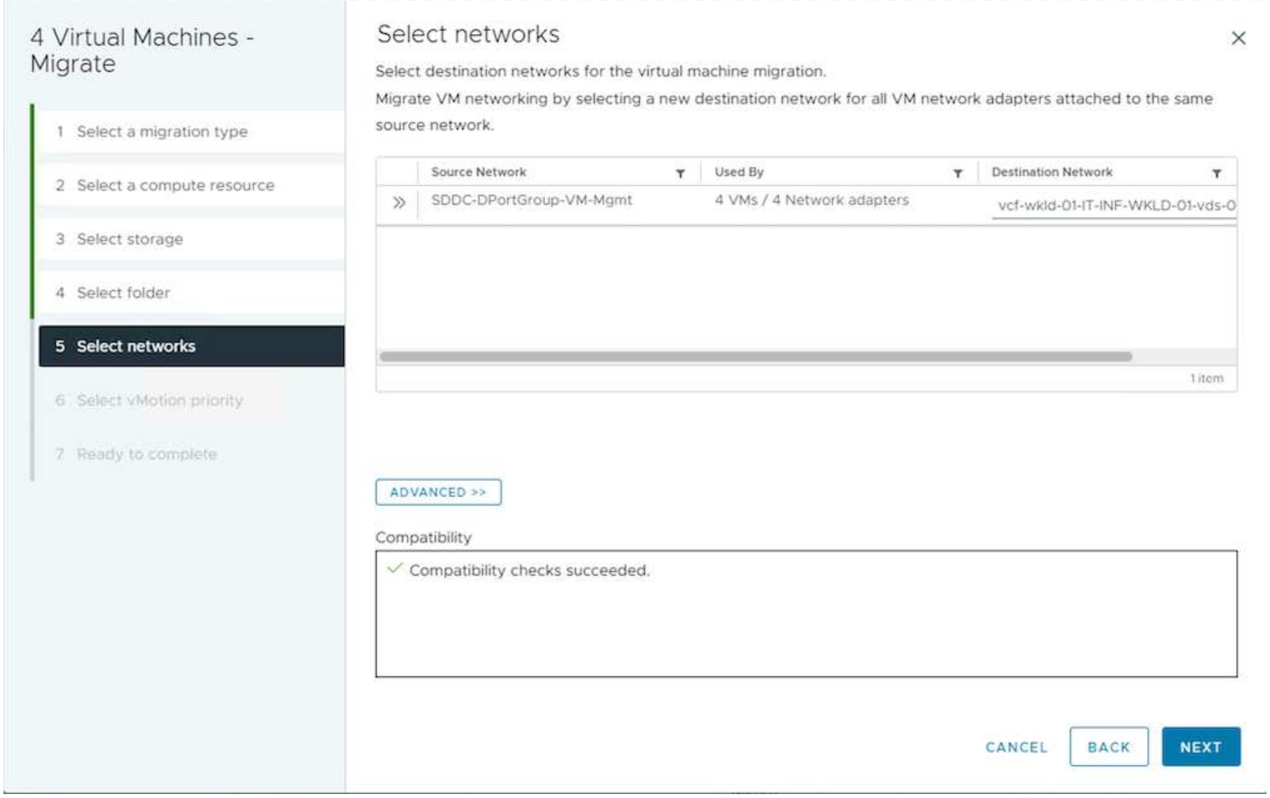
Select location for the virtual machine migration.

- vcf-wkld-01-DC
  - Discovered virtual machine
  - vCLS

✓ Compatibility checks succeeded.

CANCEL | BACK | NEXT

7. Select the target port group.


4 Virtual Machines - Migrate
1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select folder
5 Select networks
6 Select vMotion priority
7 Ready to complete
ADVANCED >>
CANCEL
BACK
NEXT

Select networks

Select destination networks for the virtual machine migration.

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

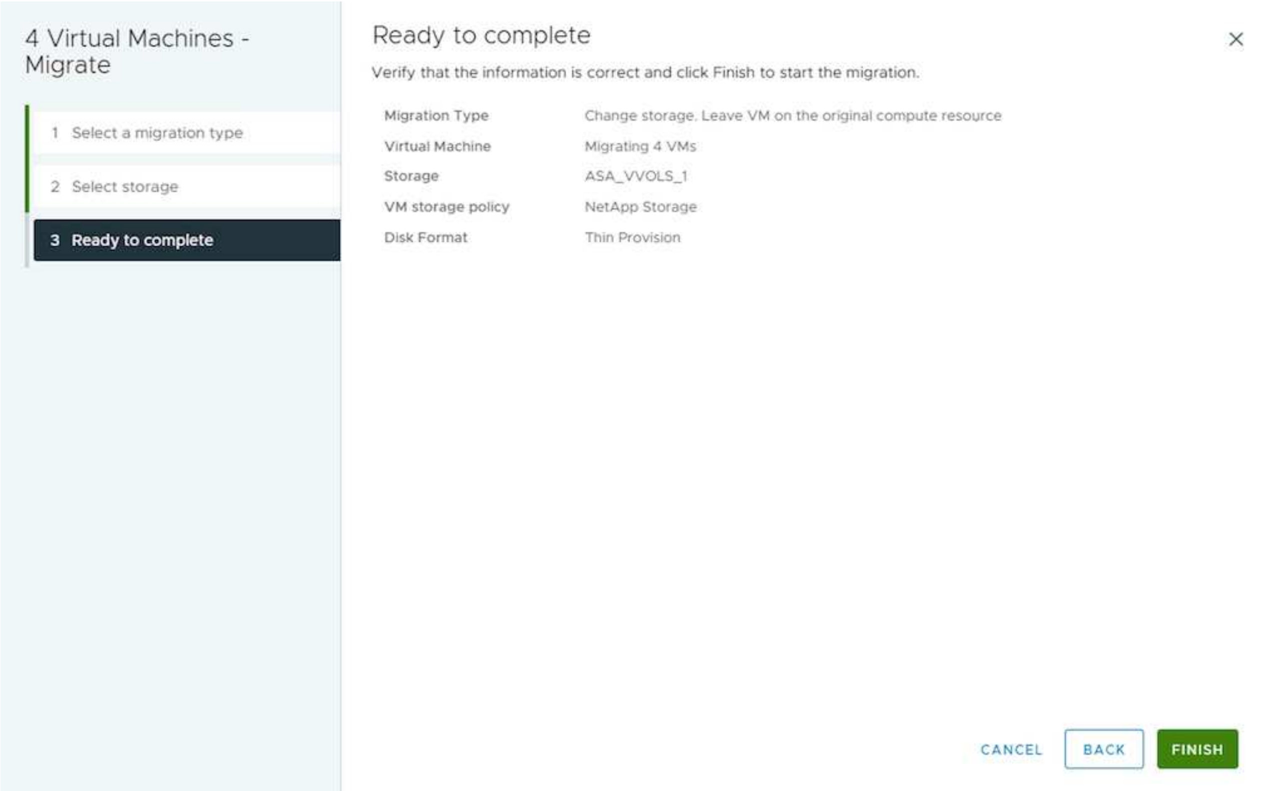
Source Network	Used By	Destination Network
SDDC-DPortGroup-VM-Mgmt	4 VMs / 4 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-0

1 item

Compatibility

✓ Compatibility checks succeeded.

8. Review and click on Finish.



Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

To migrate VMs using PowerCLI, here is the sample script.

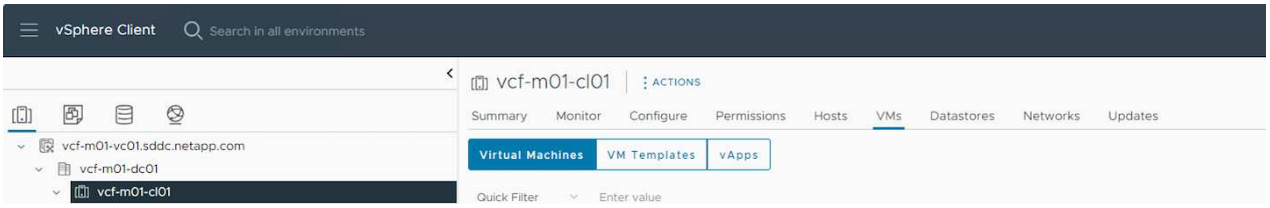
```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to another cluster and Datastore specified by Policy
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy)

#When Portgroup is specific to each cluster, replace the above command
with
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy) -PortGroup
(Get-VirtualPortGroup 'VLAN 101')

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

Migration of VMs across vCenter servers in same SSO domain

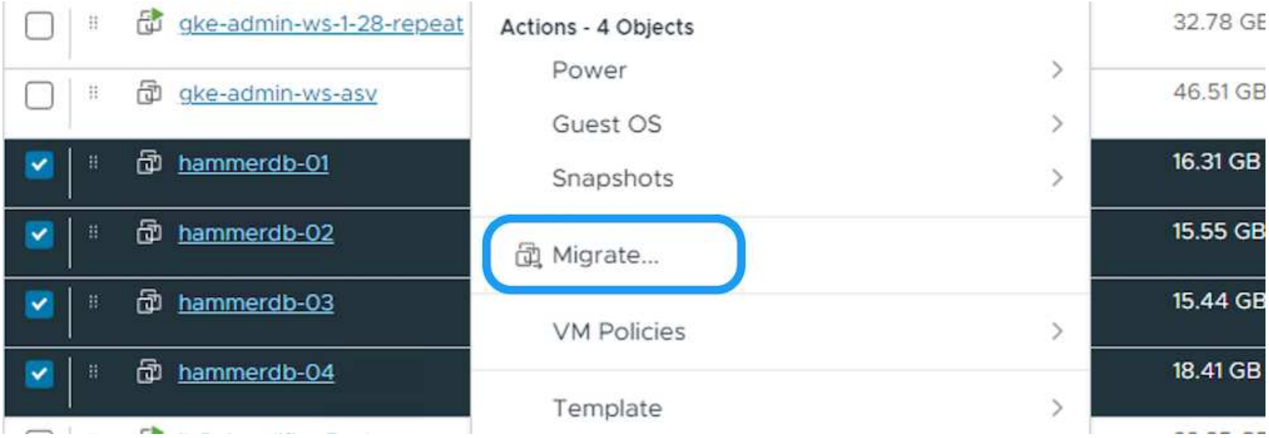
Follow the procedure below to migrate VMs to new vCenter server which is listed on same vSphere Client UI.

For additional requirements like source and target vCenter versions,etc., check vSphere documentation on requirements for vMotion between vCenter server instances

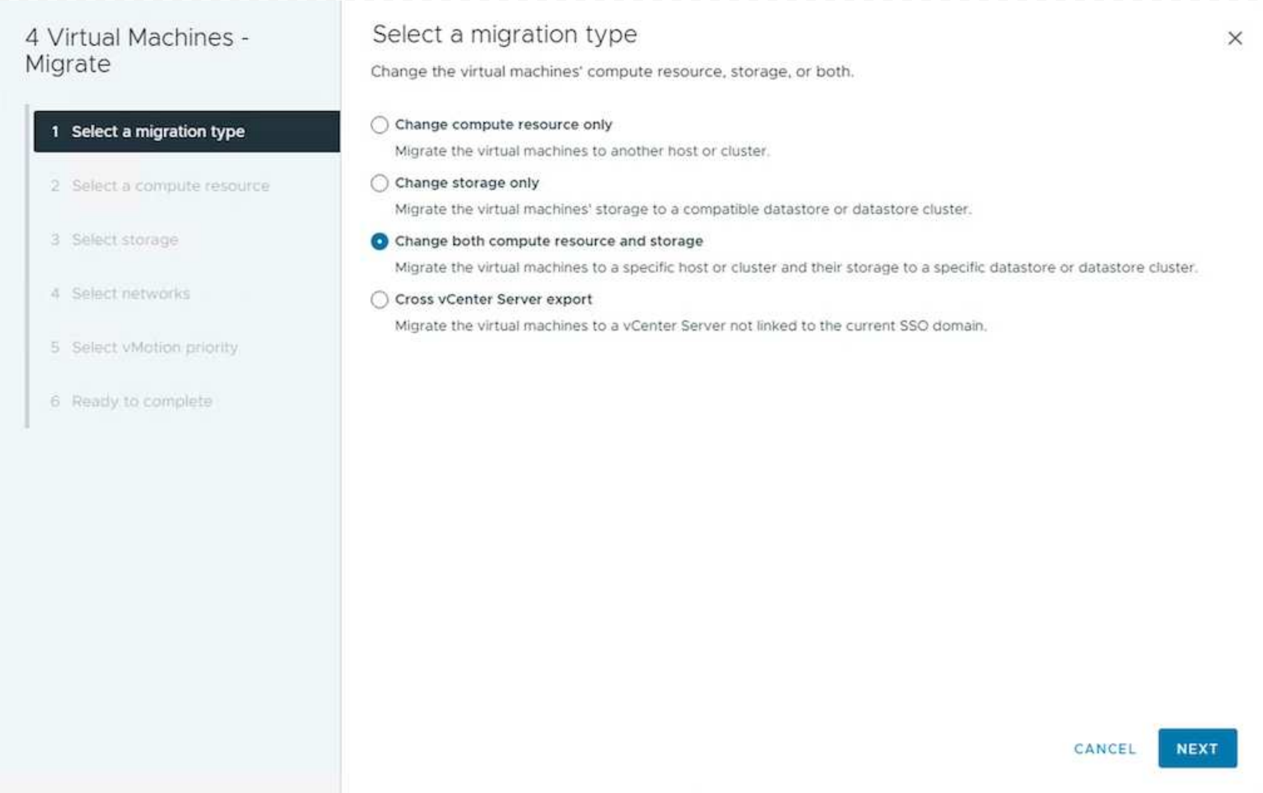
1. With vSphere Web Client, select the Cluster from the Host and Cluster inventory and click on VMs tab.



2. Select the VMs that needs to be migrated and right click to select Migrate option.



3. Choose option to change compute resource and storage, Click Next


4 Virtual Machines - Migrate
1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select networks
5 Select vMotion priority
6 Ready to complete
CANCEL
NEXT

Select a migration type

Change the virtual machines' compute resource, storage, or both.

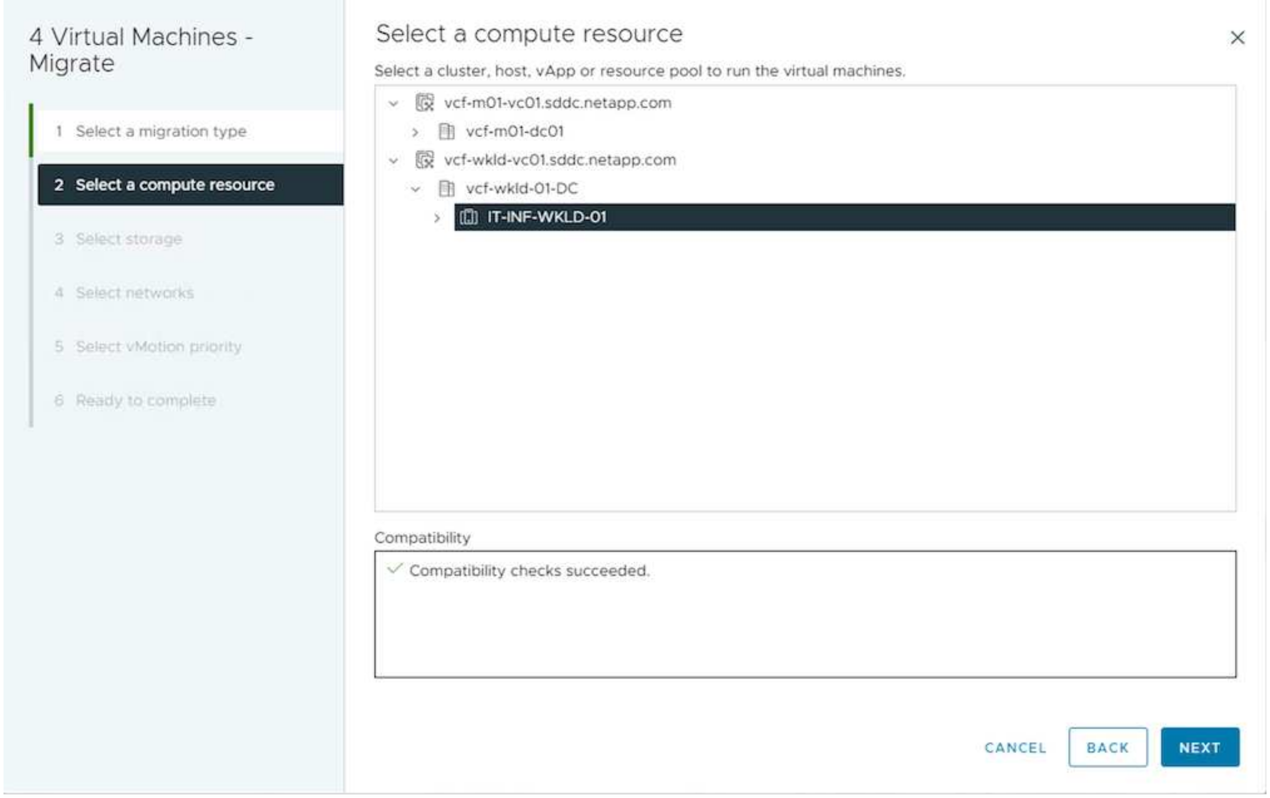
○ Change compute resource only
Migrate the virtual machines to another host or cluster.

○ Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

● Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

○ Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

4. Select the target cluster in target vCenter server.


4 Virtual Machines - Migrate
1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select networks
5 Select vMotion priority
6 Ready to complete
CANCEL
BACK
NEXT

Select a compute resource

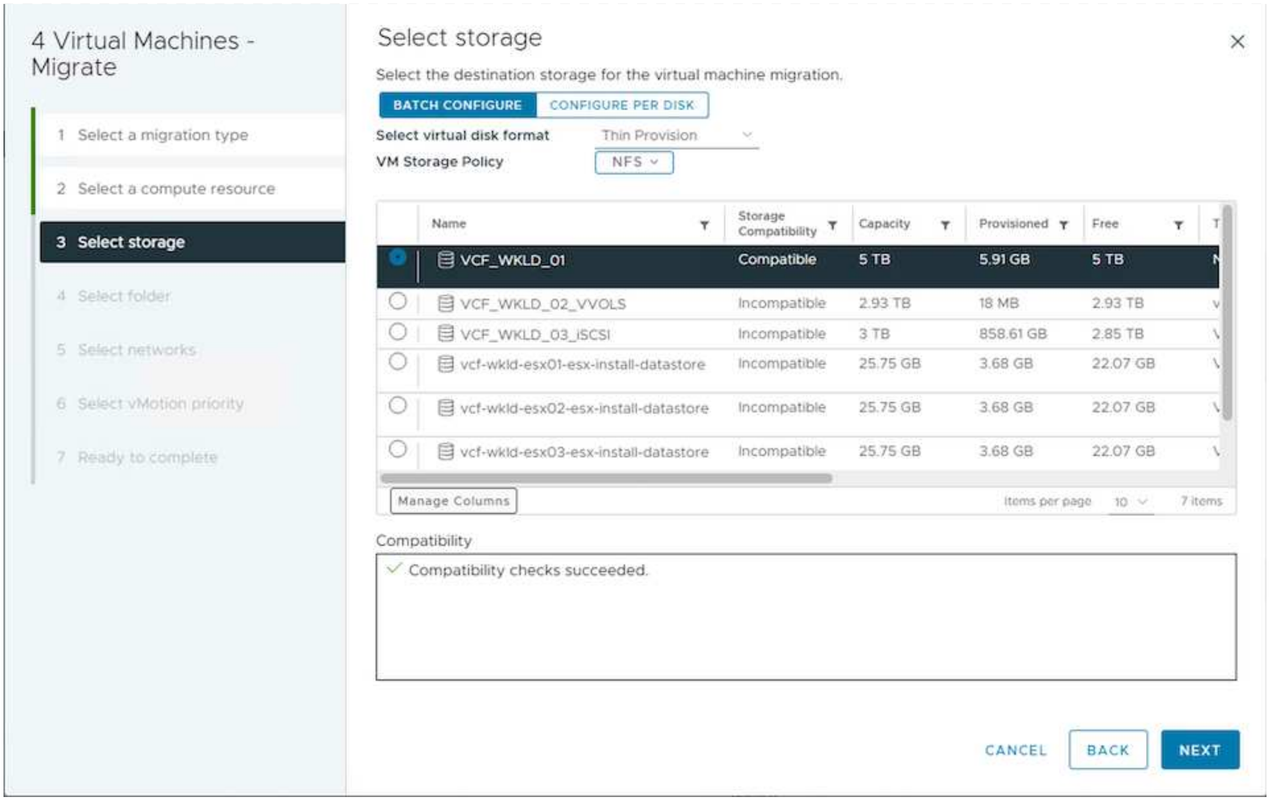
Select a cluster, host, vApp or resource pool to run the virtual machines.

- vcf-m01-vc01.sddc.netapp.com
  - vcf-m01-dc01
- vcf-wkld-vc01.sddc.netapp.com
  - vcf-wkld-01-DC
    - IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

5. Select the desired VM Storage Policy and pick the datastore that is compatible. Click Next.



4 Virtual Machines - Migrate

1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select folder
5 Select networks
6 Select vMotion priority
7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE | CONFIGURE PER DISK

Select virtual disk format: Thin Provision

VM Storage Policy: NFS

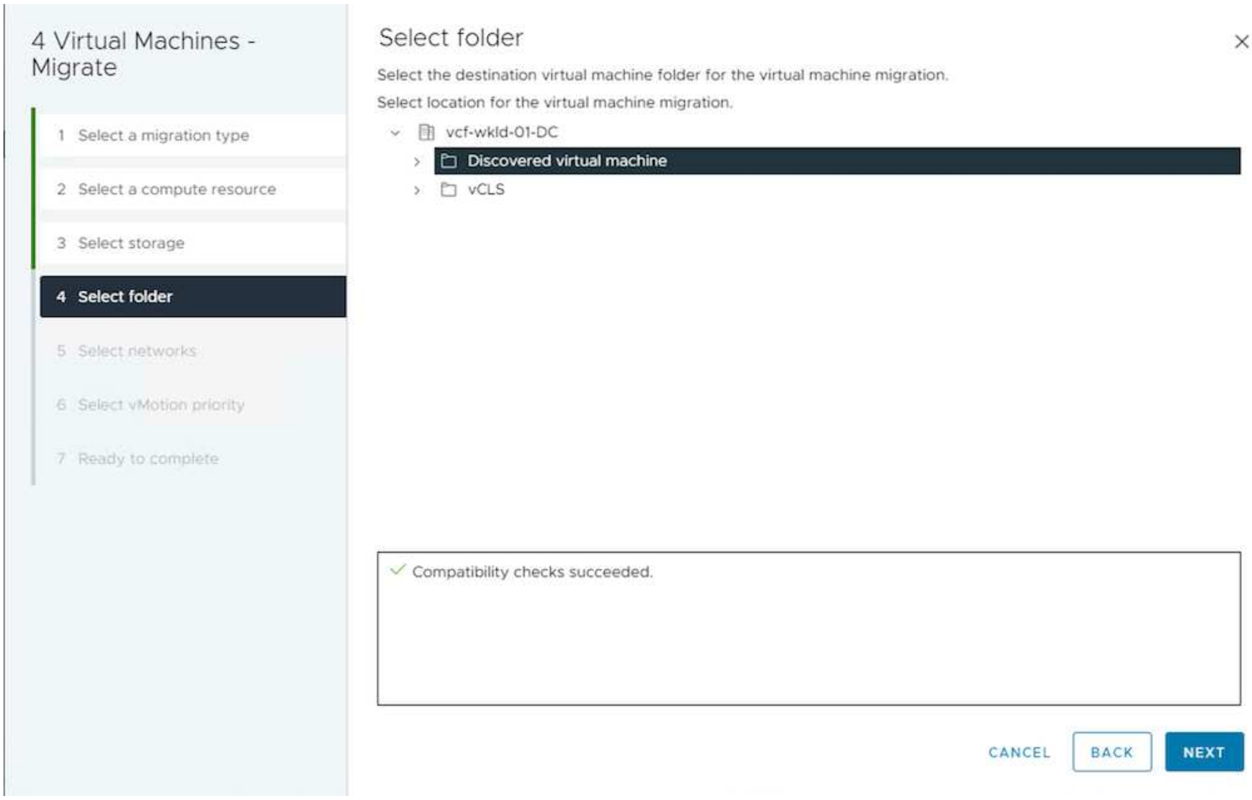
	Name	Storage Compatibility	Capacity	Provisioned	Free	T
●	VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB	N
○	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB	V
○	VCF_WKLD_03_iSCSI	Incompatible	3 TB	858.61 GB	2.85 TB	V
○	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	V
○	vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	V
○	vcf-wkld-esx03-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	V

Manage Columns | Items per page 10 | 7 items

Compatibility

✓ Compatibility checks succeeded.

6. Pick the VM folder to place the target VMs.



4 Virtual Machines - Migrate

1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select folder
5 Select networks
6 Select vMotion priority
7 Ready to complete

Select folder

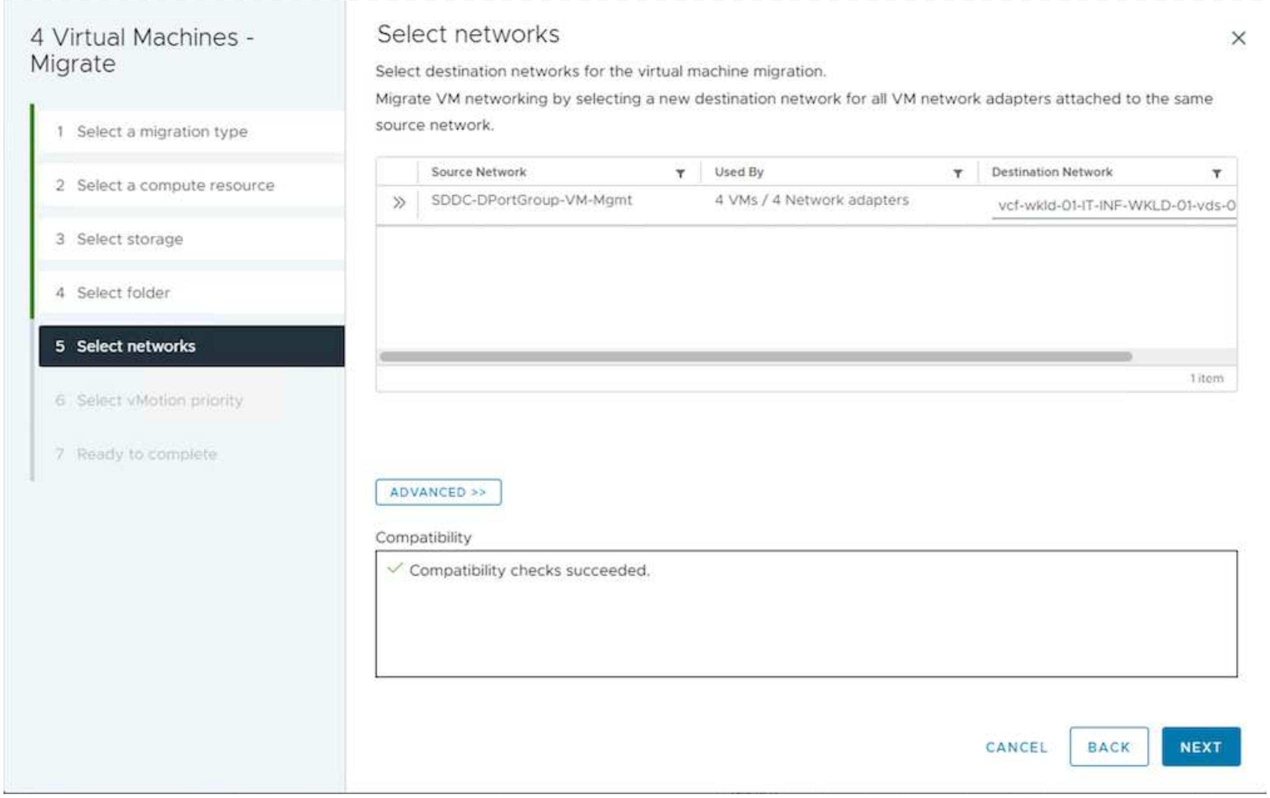
Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

- vcf-wkld-01-DC
  - Discovered virtual machine
  - vCLS

✓ Compatibility checks succeeded.

7. Select the target port group.


4 Virtual Machines - Migrate
1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select folder
5 Select networks
6 Select vMotion priority
7 Ready to complete
ADVANCED >>
CANCEL
BACK
NEXT

Select networks

Select destination networks for the virtual machine migration.

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

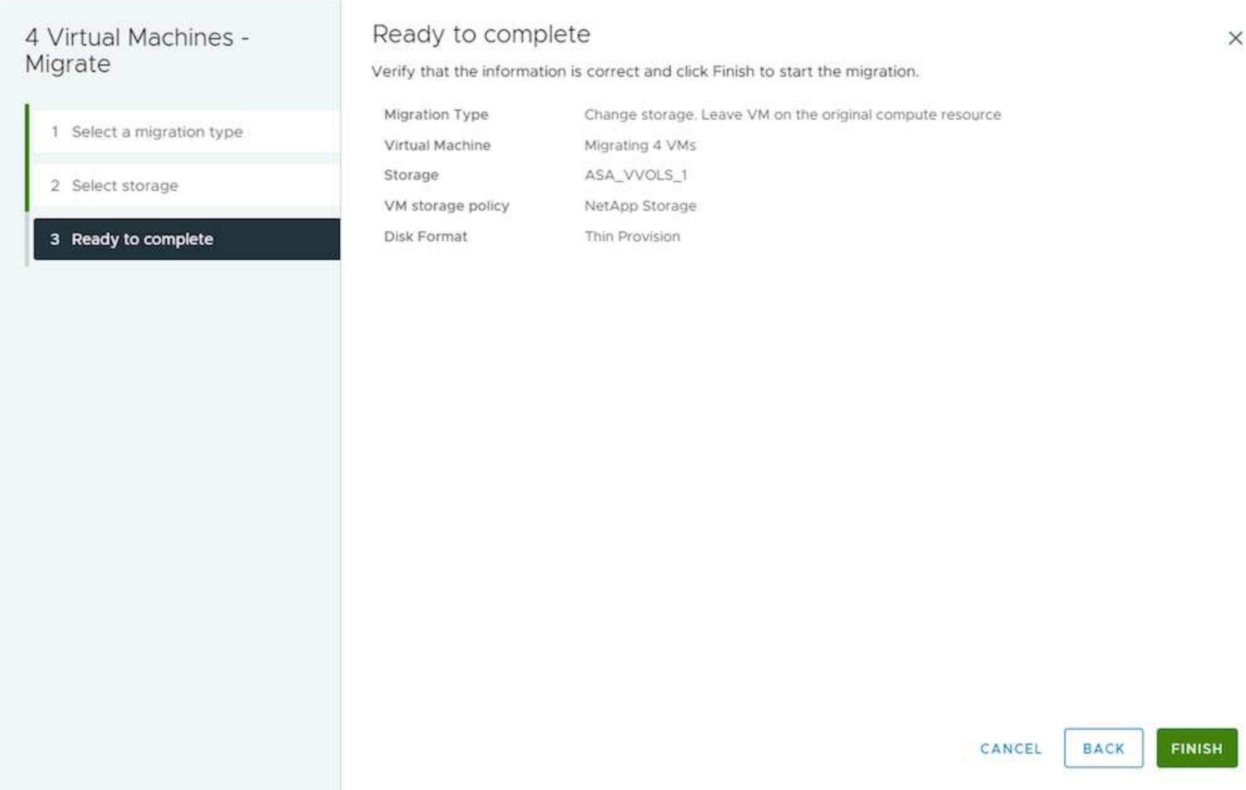
	Source Network	Used By	Destination Network
»	SDDC-DPortGroup-VM-Mgmt	4 VMs / 4 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-0

1 item

Compatibility

✓ Compatibility checks succeeded.

8. Review the migration options and click Finish.



Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

To migrate VMs using PowerCLI, here is the sample script.

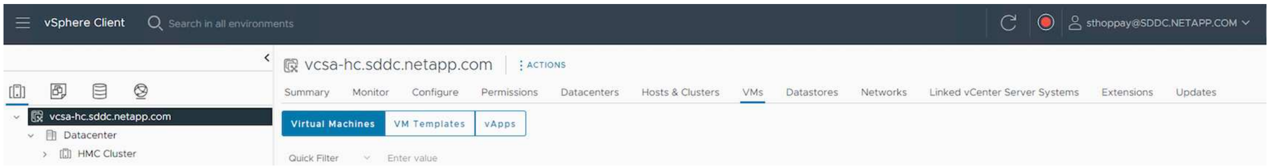
```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

Migration of VMs across vCenter servers in different SSO domain

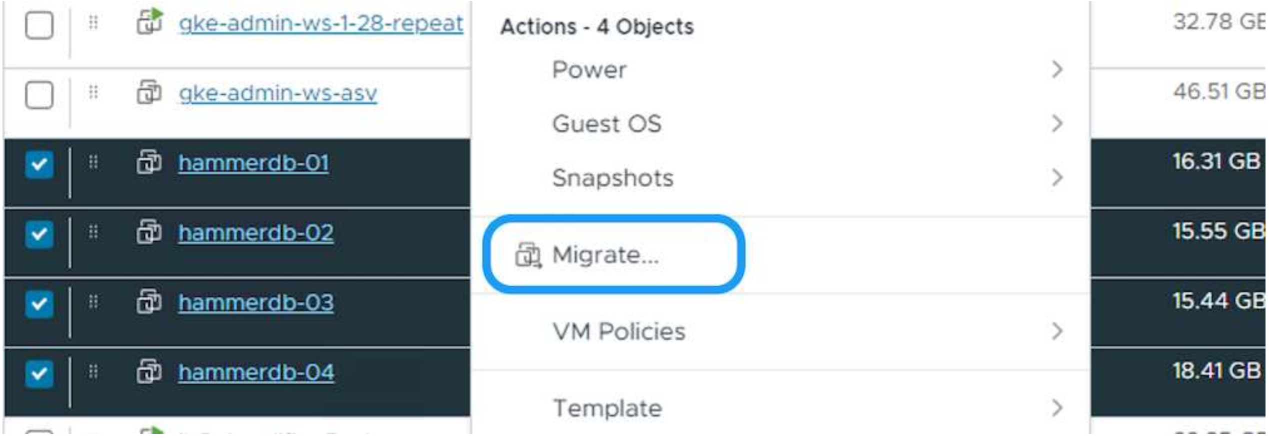
This scenario assumes the communication exists between the vCenter servers. Otherwise check the across datacenter location scenario listed below. For prerequisites, check vSphere documentation on Advanced Cross vCenter vMotion

Follow the procedure below to migrate VMs to differnt vCenter server using UI.

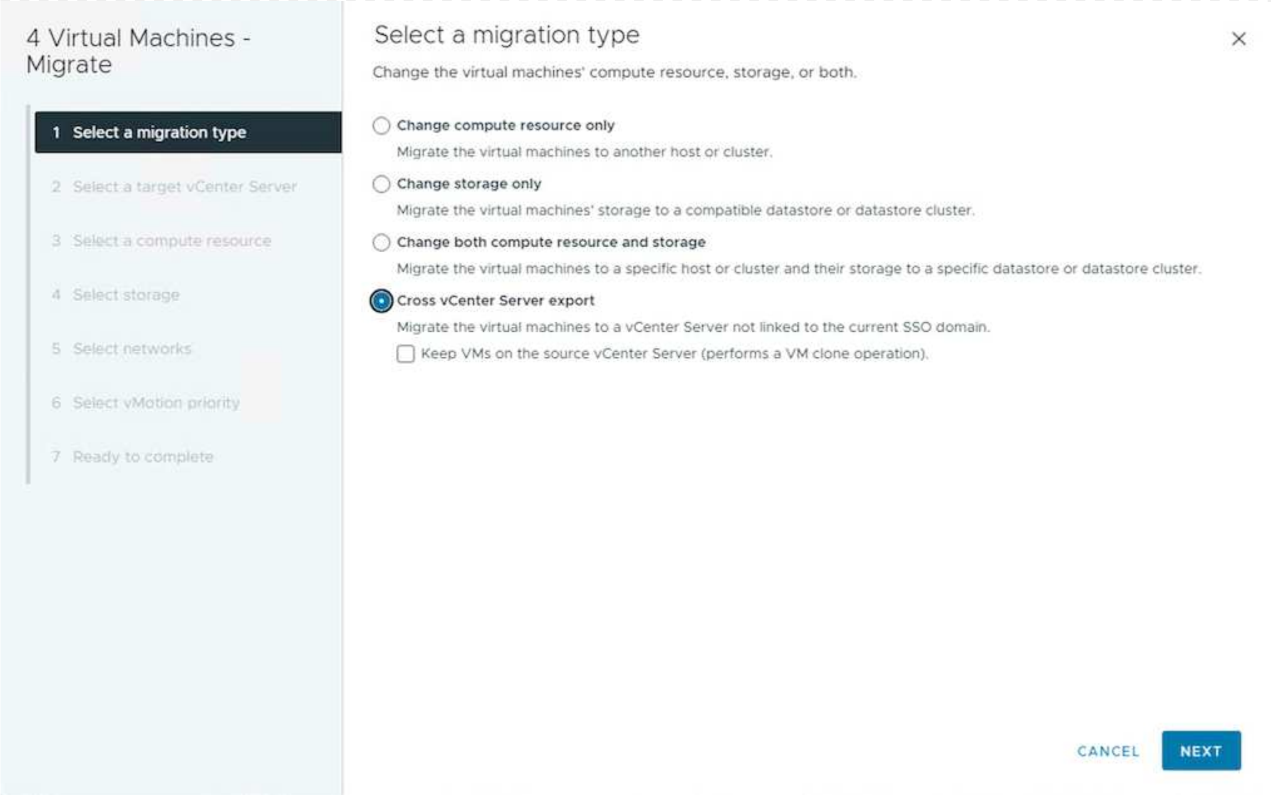
1. With vSphere Web Client, select the source vCenter server and click on VMs tab.



2. Select the VMs that needs to be migrated and right click to select Migrate option.



3. Choose option Cross vCenter Server export, Click Next


4 Virtual Machines - Migrate
1 Select a migration type
2 Select a target vCenter Server
3 Select a compute resource
4 Select storage
5 Select networks
6 Select vMotion priority
7 Ready to complete
CANCEL
NEXT

Select a migration type

Change the virtual machines' compute resource, storage, or both.

○ Change compute resource only
Migrate the virtual machines to another host or cluster.

○ Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

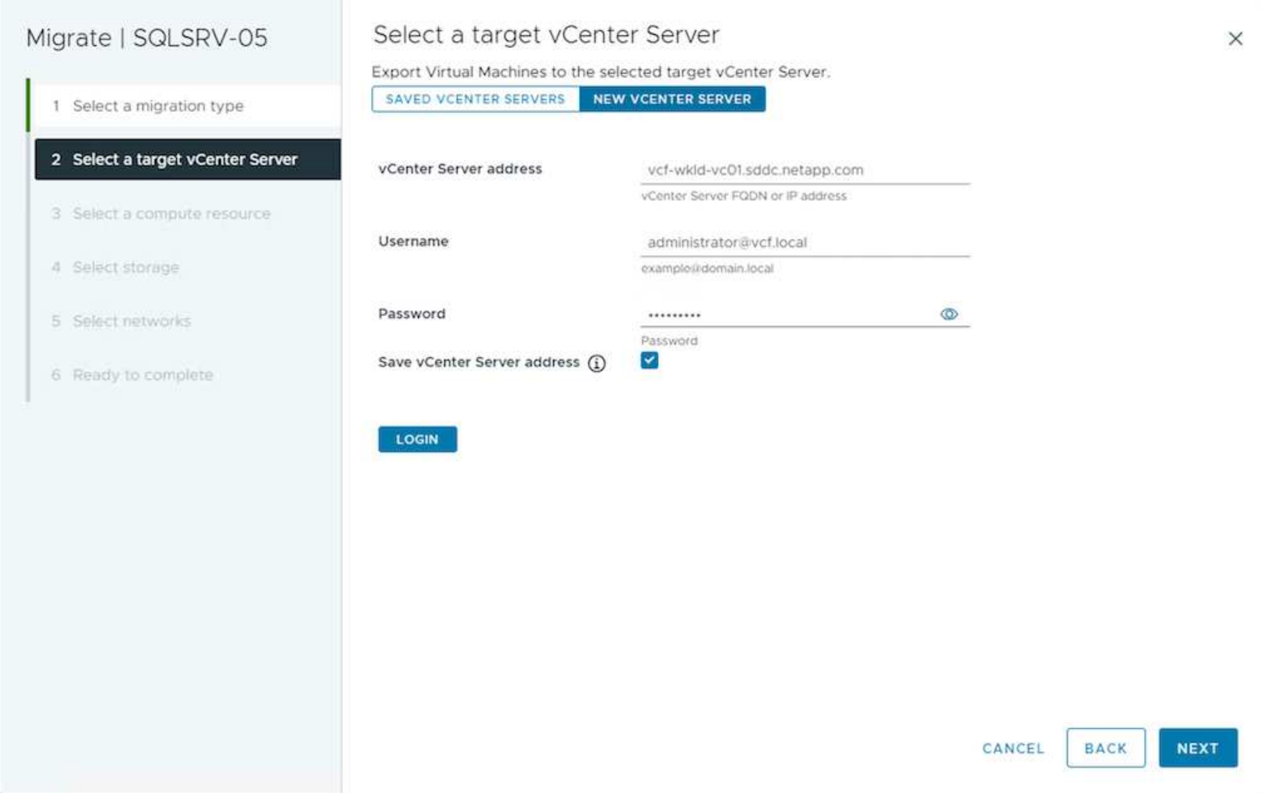
○ Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

● Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

□ Keep VMs on the source vCenter Server (performs a VM clone operation).

VM can also be imported from the target vCenter server. For that procedure, check Import or Clone a Virtual Machine with Advanced Cross vCenter vMotion

4. Provide vCenter credential details and click Login.



Select a target vCenter Server

Export Virtual Machines to the selected target vCenter Server.

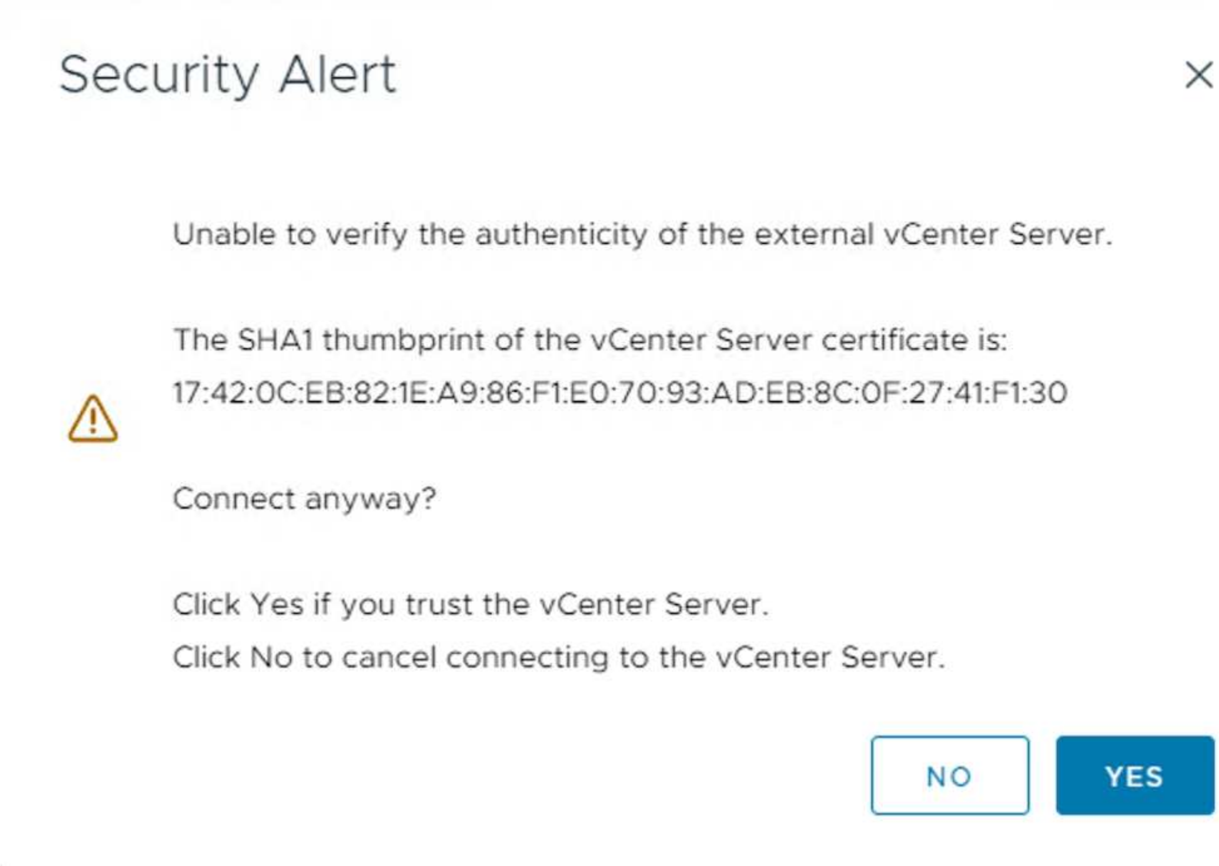
vCenter Server address: vcf-wkld-vc01.sddc.netapp.com
vCenter Server FQDN or IP address

Username: administrator@vcf.local
example@domain.local

Password: •••••••••
Password

Save vCenter Server address ☑

5. Confirm and Accept the SSL certificate thumbprint of vCenter server



Security Alert

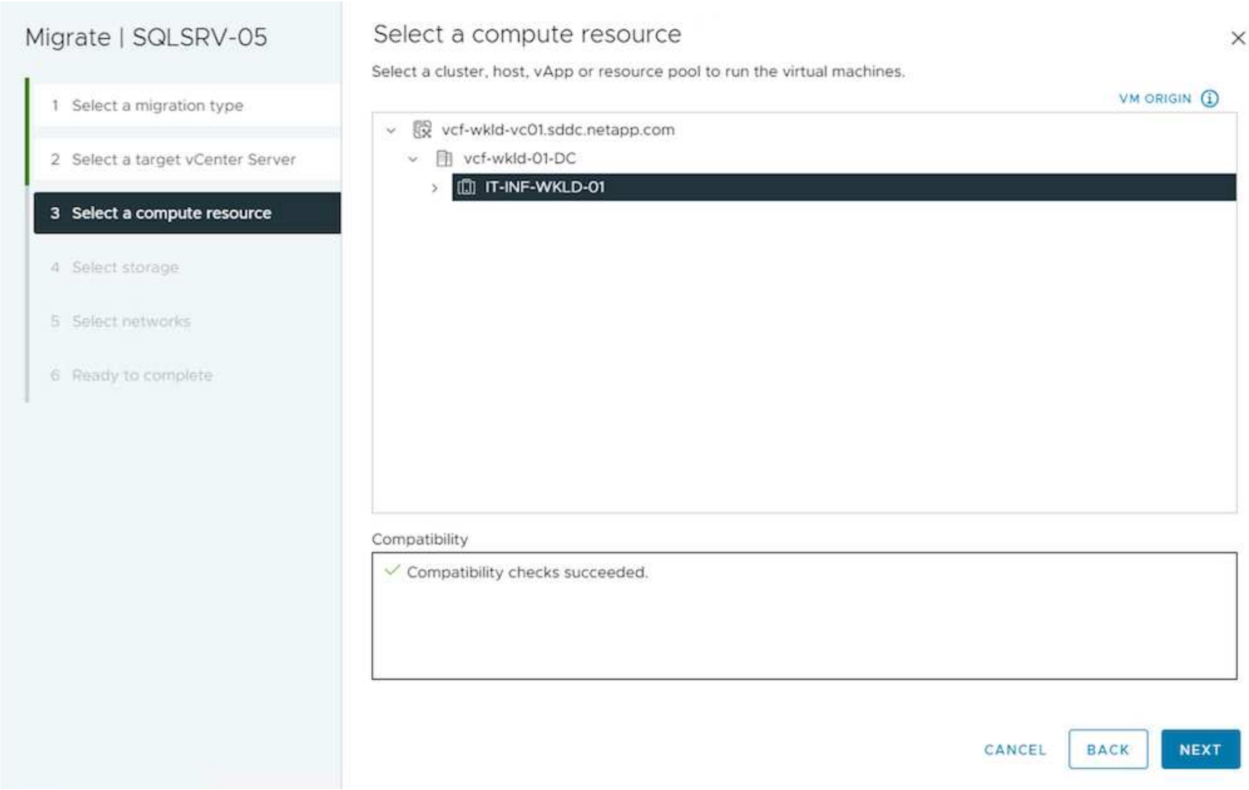
Unable to verify the authenticity of the external vCenter Server.

The SHA1 thumbprint of the vCenter Server certificate is:
17:42:0C:EB:82:1E:A9:86:F1:E0:70:93:AD:EB:8C:0F:27:41:F1:30

Connect anyway?

Click Yes if you trust the vCenter Server.
Click No to cancel connecting to the vCenter Server.

6. Expand target vCenter and select the target compute cluster.



Migrate | SQLSRV-05

1 Select a migration type
2 Select a target vCenter Server
3 Select a compute resource
4 Select storage
5 Select networks
6 Ready to complete

Select a compute resource

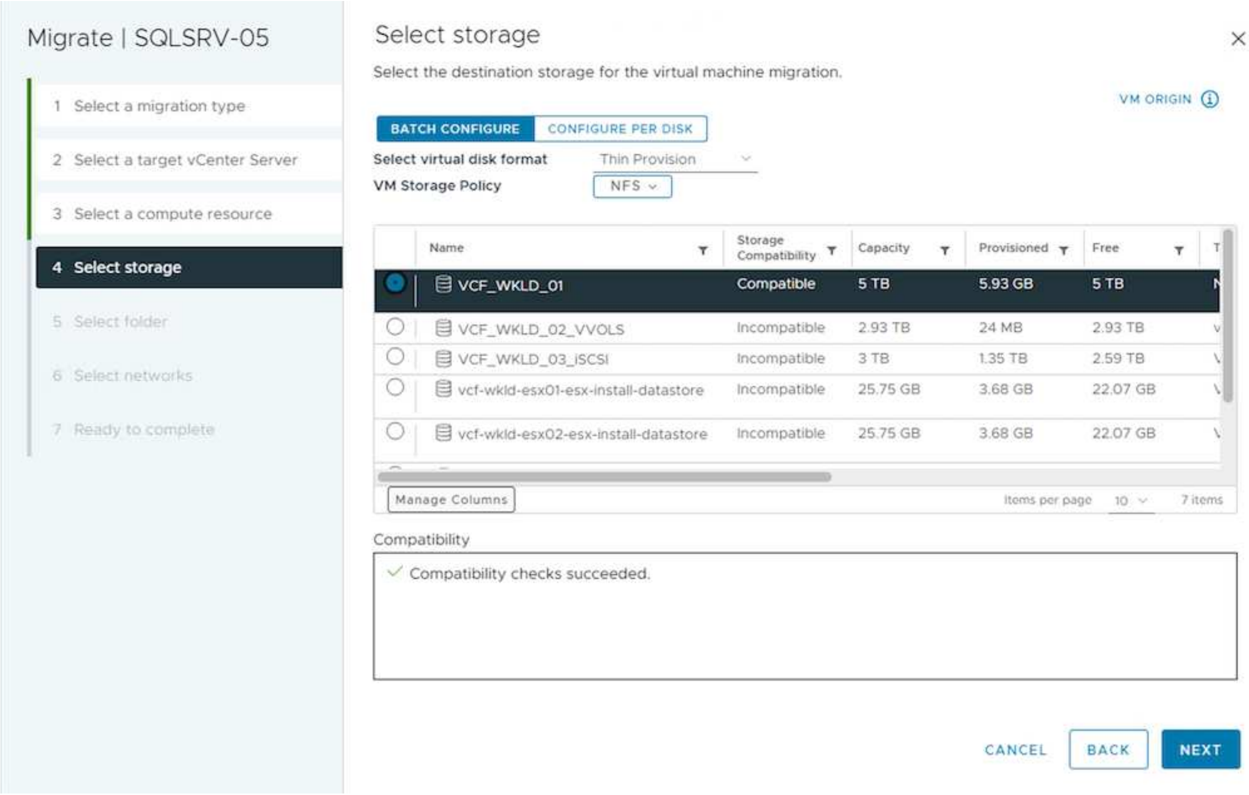
Select a cluster, host, vApp or resource pool to run the virtual machines.

- vcf-wkld-vc01.sddc.netapp.com
  - vcf-wkld-01-DC
    - IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

7. Select the target datastore based on the VM Storage Policy.



Select storage

Select the destination storage for the virtual machine migration.

Select virtual disk format: Thin Provision

VM Storage Policy: NFS

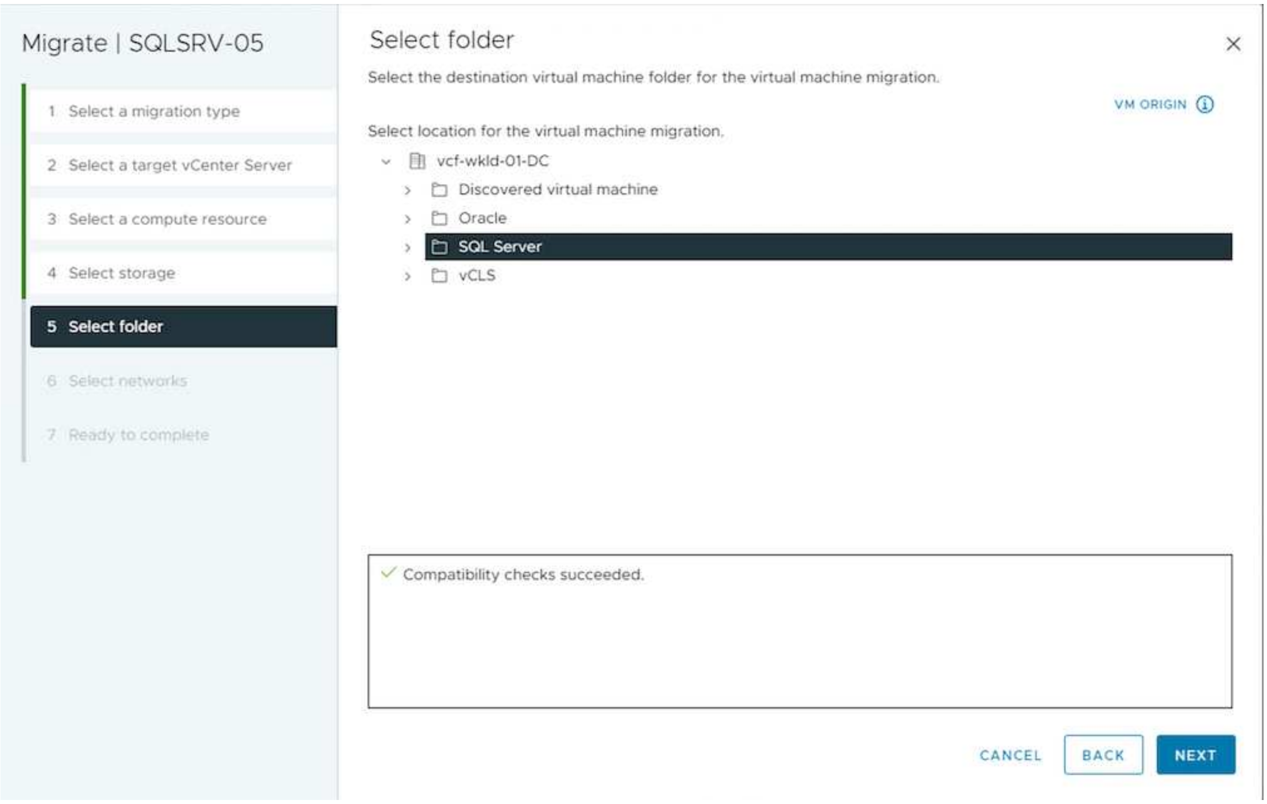
	Name	Storage Compatibility	Capacity	Provisioned	Free
●	VCF_WKLD_01	Compatible	5 TB	5.93 GB	5 TB
○	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	24 MB	2.93 TB
○	VCF_WKLD_03_iSCSI	Incompatible	3 TB	1.35 TB	2.59 TB
○	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB
○	vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB

Items per page 10 7 items

Compatibility

✓ Compatibility checks succeeded.

8. Select the target VM folder.



Select folder

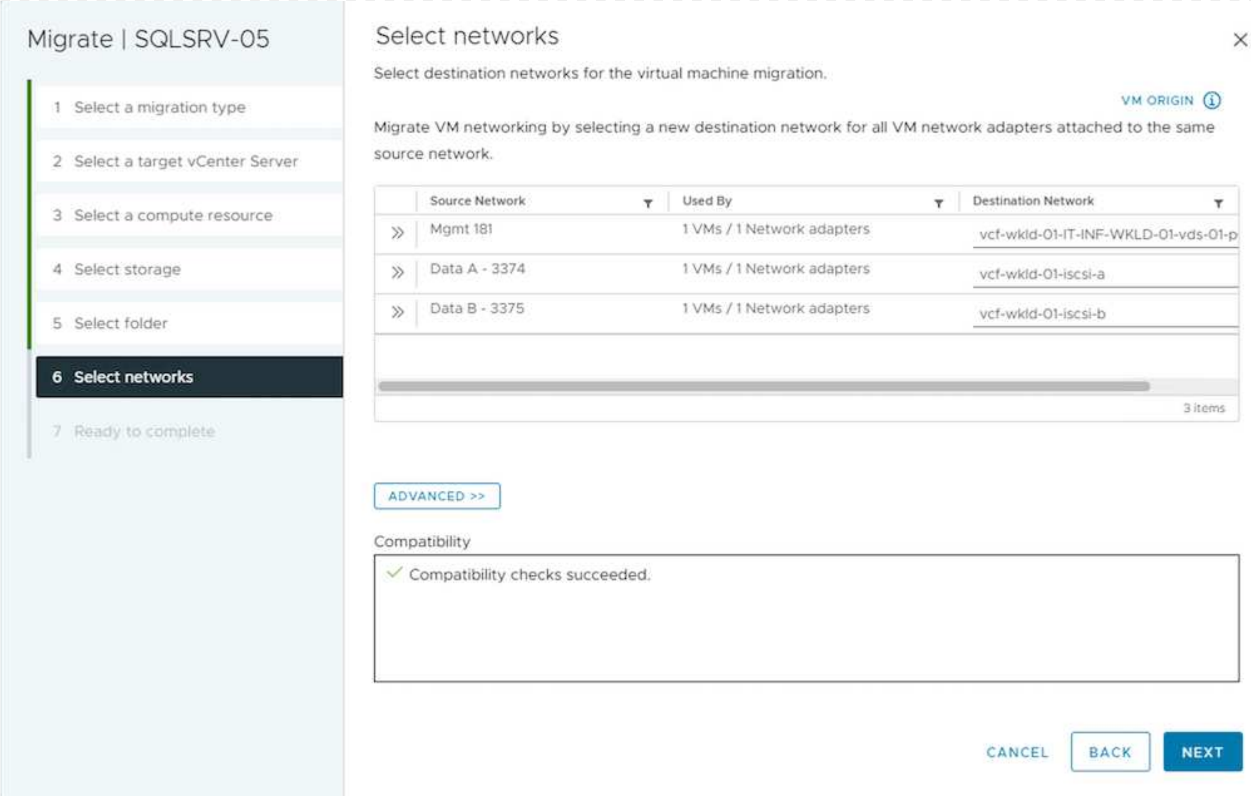
Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

- vcf-wkld-01-DC
  - Discovered virtual machine
  - Oracle
  - SQL Server
  - vCLS

✓ Compatibility checks succeeded.

9. Pick the VM portgroup for each network interface card mapping.



Migrate | SQLSRV-05

1 Select a migration type

2 Select a target vCenter Server

3 Select a compute resource

4 Select storage

5 Select folder

6 Select networks

7 Ready to complete

Select networks

Select destination networks for the virtual machine migration.

VM ORIGIN

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

	Source Network	Used By	Destination Network
»	Mgmt 181	1 VMs / 1 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-01-p
»	Data A - 3374	1 VMs / 1 Network adapters	vcf-wkld-01-iscsi-a
»	Data B - 3375	1 VMs / 1 Network adapters	vcf-wkld-01-iscsi-b

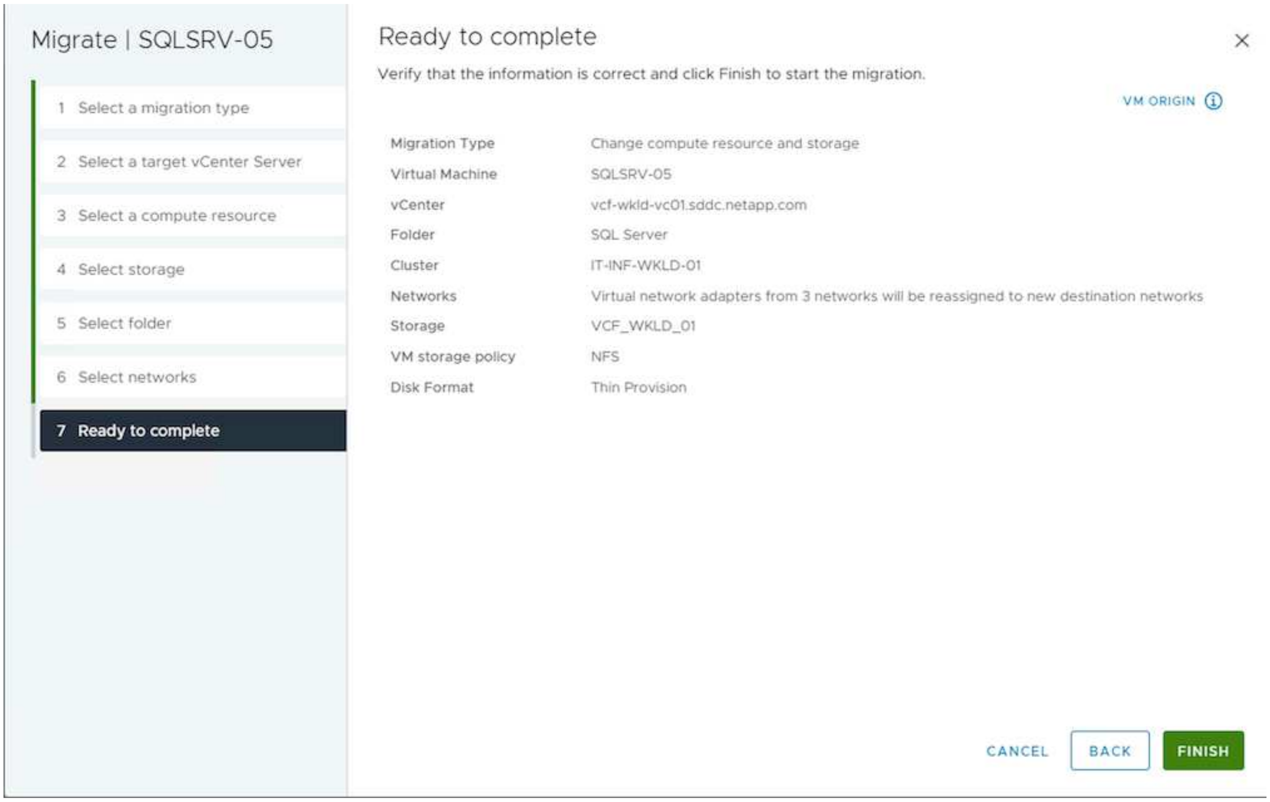
3 items

ADVANCED >>

Compatibility

✓ Compatibility checks succeeded.

10. Review and click Finish to start the vMotion across the vCenter servers.



Migrate | SQLSRV-05

1 Select a migration type

2 Select a target vCenter Server

3 Select a compute resource

4 Select storage

5 Select folder

6 Select networks

7 Ready to complete

Ready to complete

Verify that the information is correct and click Finish to start the migration.

VM ORIGIN

Migration Type	Change compute resource and storage
Virtual Machine	SQLSRV-05
vCenter	vcf-wkld-vc01.sddc.netapp.com
Folder	SQL Server
Cluster	IT-INF-WKLD-01
Networks	Virtual network adapters from 3 networks will be reassigned to new destination networks
Storage	VCF_WKLD_01
VM storage policy	NFS
Disk Format	Thin Provision

To migrate VMs using PowerCLI, here is the sample script.

```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'Source Cluster'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

Migration of VMs across datacenter locations

- When Layer 2 traffic is stretched across datacenters either by using NSX Federation or other options, follow the procedure for migrating VMs across vCenter servers.
- HCX provides various migration types including Replication Assisted vMotion across the datacenters to move VM without any downtime.
- Site Recovery Manager (SRM) is typically meant for Disaster Recovery purposes and also often used for planned migration utilizing storage array based replication.
- Continous Data Protection (CDP) products use vSphere API for IO (VAIO) to intercept the data and send a copy to remote location for near zero RPO solution.
- Backup and Recovery products can also be utilized. But often results in longer RTO.
- NetApp Disater Recovery utilizes storage array based replication and automates certain tasks to recover the VMs at target site.

Migration of VMs in hybrid cloud environment

- Configure Hybrid Linked Mode and follow the procedure of Migration of VMs across vCenter servers in same SSO domain
- HCX provides various migration types including Replication Assisted vMotion across the datacenters to move VM while it is powered on.
  - TR 4942: Migrate Workloads to FSx ONTAP datastore using VMware HCX
  - TR-4940: Migrate workloads to Azure NetApp Files datastore using VMware HCX - Quickstart guide
  - Migrate workloads to Google Cloud NetApp Volumes datastore on Google Cloud VMware Engine using VMware HCX - Quickstart guide
- NetApp Disaster Recovery utilizes storage array based replication and automates certain tasks to recover the VMs at target site.
- With supported Continous Data Protection (CDP) products that use vSphere API for IO (VAIO) to intercept the data and send a copy to remote location for near zero RPO solution.

> When the source VM resides on block vVol datastore, it can be replicated with SnapMirror to Amazon FSx ONTAP or Cloud Volumes ONTAP (CVO) at other supported cloud providers and consume as iSCSI volume with cloud native VMs.

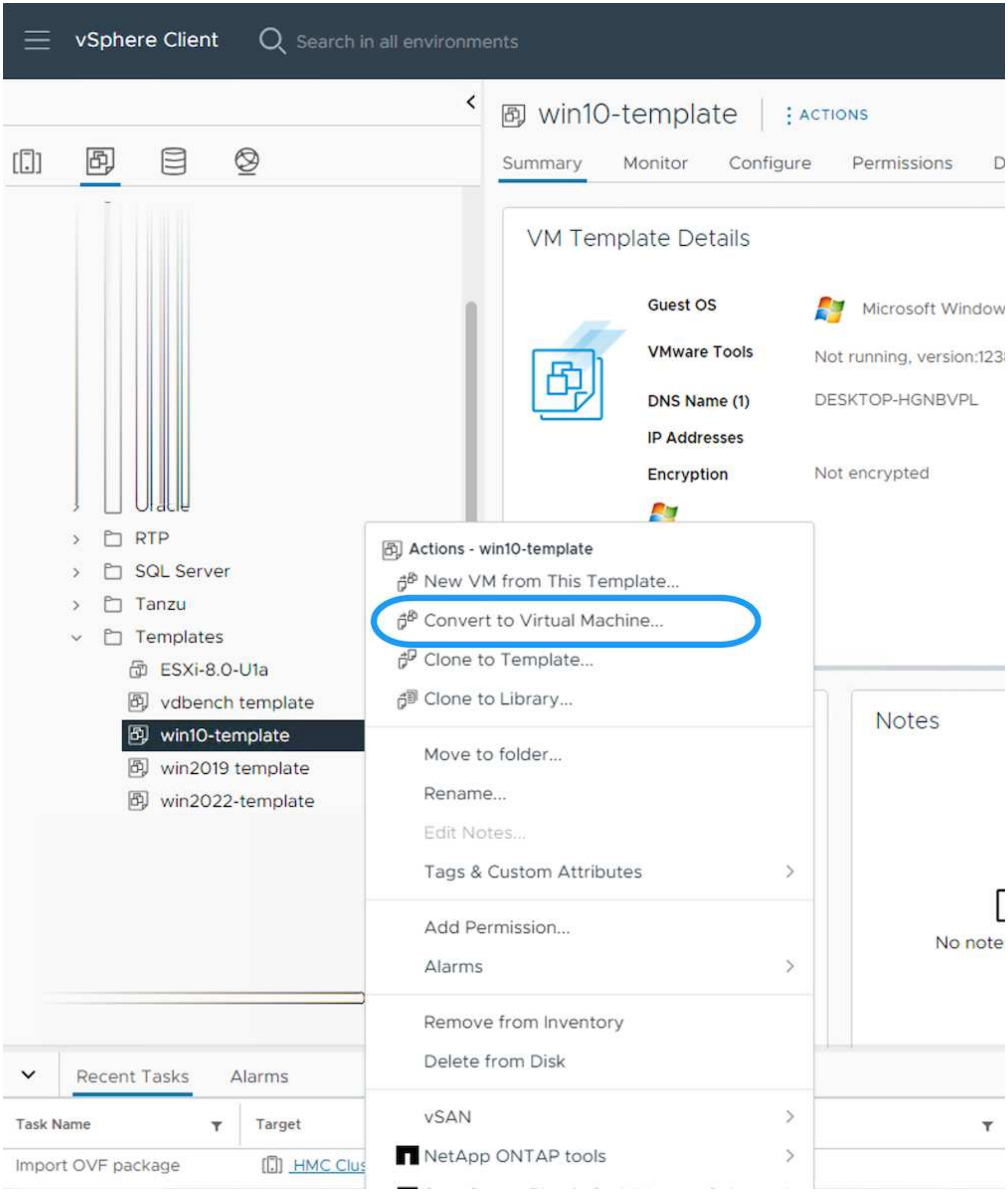
VM Template Migration Scenarios

VM Templates can be managed by vCenter Server or by a content library. Distribution of VM templates, OVF and OVA templates, other types of files are handled by publishing it in local content library and remote content libraries can subscribe to it.

- VM templates stored on vCenter inventory can be converted to VM and use the VM migration options.
- OVF and OVA templates, other types of files stored on content library can be cloned to other content libraries.
- Content library VM Templates can be hosted on any datastore and needs to be added into new content library.

Migration of VM templates hosted on datastore

1. In vSphere Web Client, right click on the VM template under VM and Templates folder view and select option to convert to VM.



Guest OS: Microsoft Window

VMware Tools: Not running, version:123

DNS Name (1): DESKTOP-HGNBVPL

IP Addresses

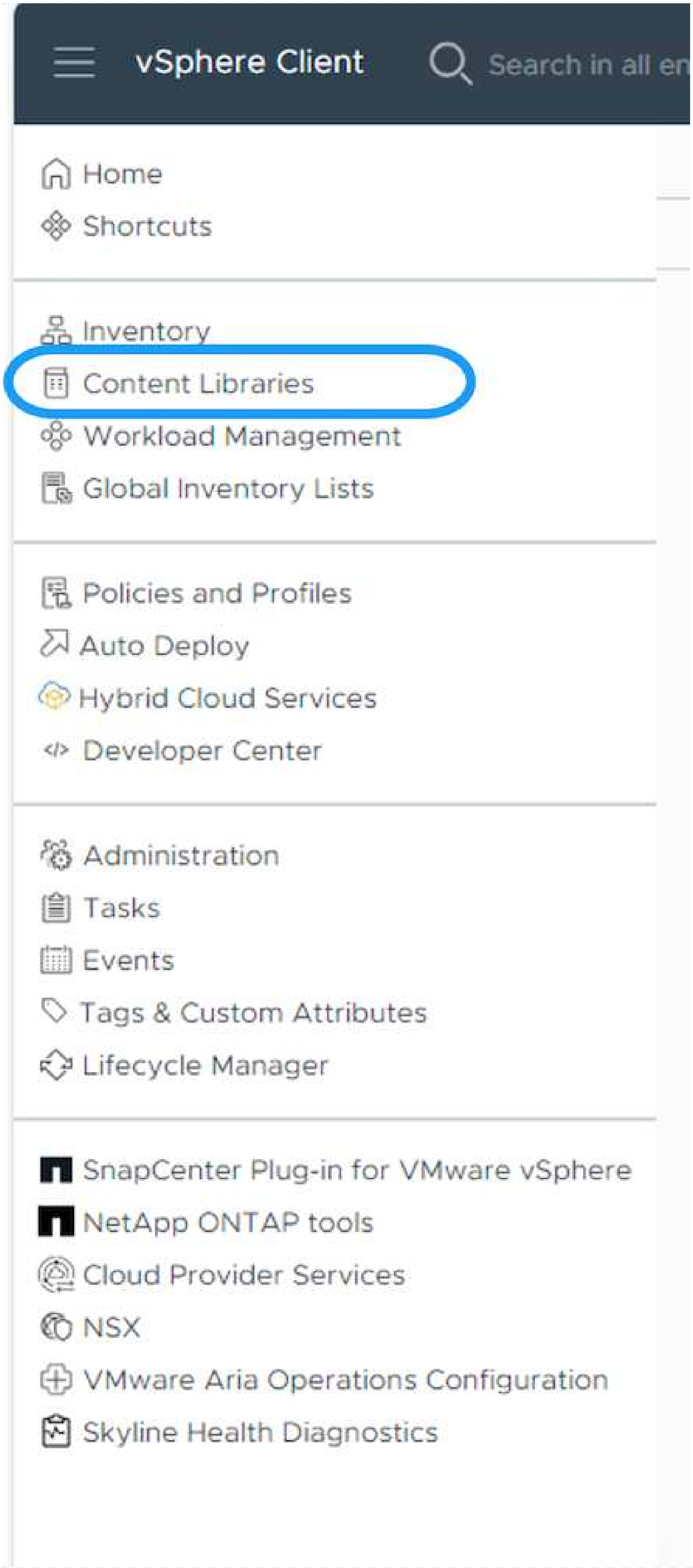
Encryption: Not encrypted

Import OVF package | HMC Clus

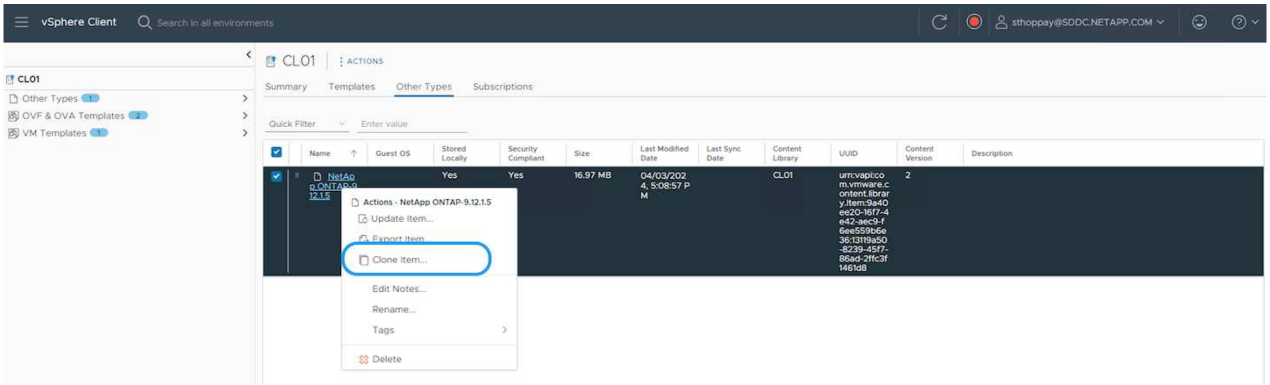
2. Once it is converted as VM, follow the VM migration options.

Clone of Content Library items

1. In vSphere Web Client, select Content Libraries


vSphere Client
Search in all en
Home
Shortcuts
Inventory
Content Libraries
Workload Management
Global Inventory Lists
Policies and Profiles
Auto Deploy
Hybrid Cloud Services
Developer Center
Administration
Tasks
Events
Tags & Custom Attributes
Lifecycle Manager
SnapCenter Plug-in for VMware vSphere
NetApp ONTAP tools
Cloud Provider Services
NSX
VMware Aria Operations Configuration
Skyline Health Diagnostics

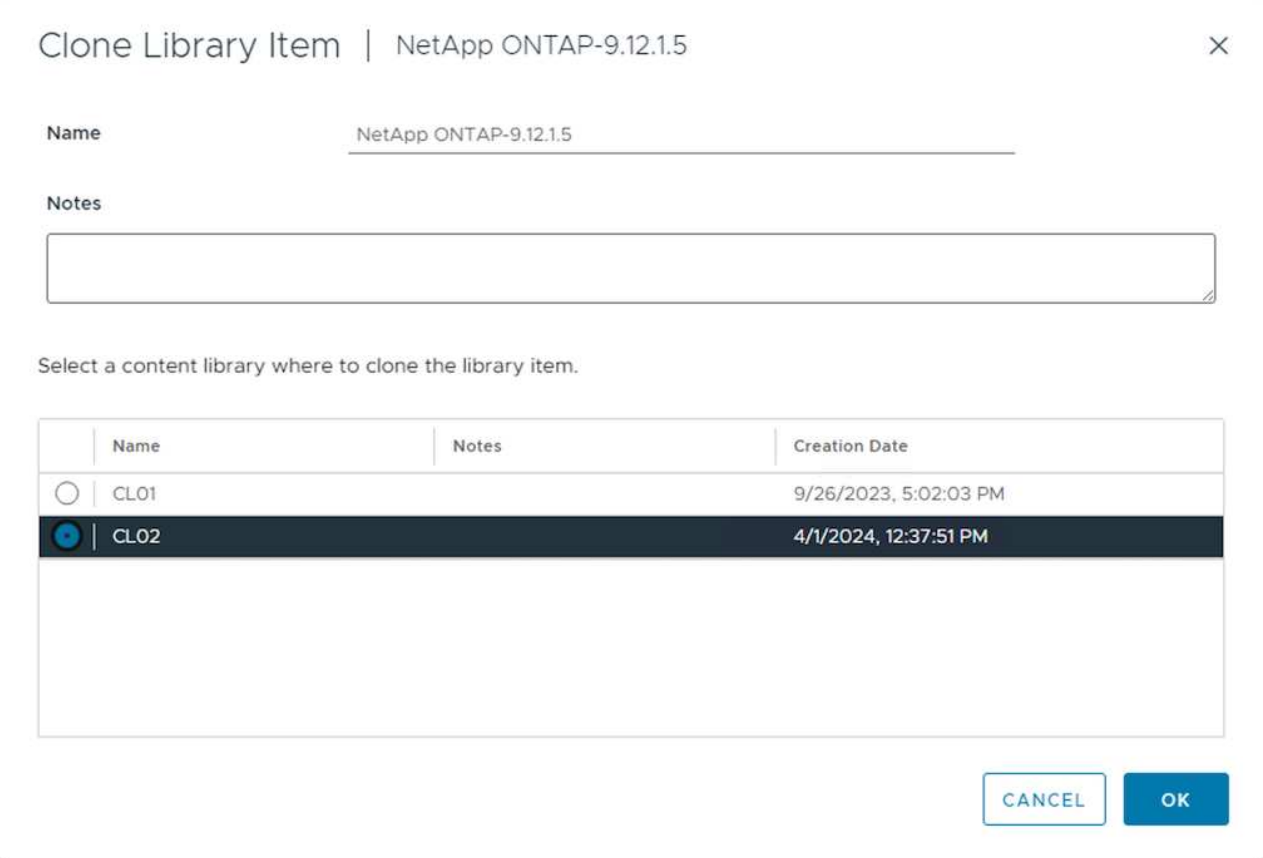
2. Select the content library in which the item you like to clone
3. Right click on the item and click on Clone Item ..



Name	Guest OS	Stored Locally	Security Compliant	Size	Last Modified Date	Last Sync Date	Content Library	UUID	Content Version	Description
NetApp ONTAP-9.12.1.5		Yes	Yes	16.97 MB	04/03/2024, 5:08:57 PM		CL01	urn:vapi:com.vmware.content.library.Item:9a40ee20-16f7-4e42-aec9-f6ee559b6e36:13119a50-8239-45f7-86ad-2ffc3f1461d8	2	

If using action menu, make sure correct target object is listed to perform action.

4. Select the target content library and click on OK.



Clone Library Item | NetApp ONTAP-9.12.1.5

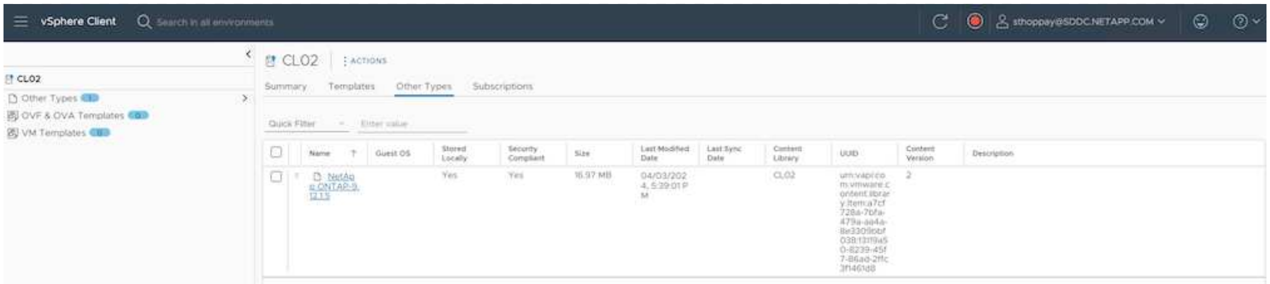
Name: NetApp ONTAP-9.12.1.5

Notes:

Select a content library where to clone the library item.

	Name	Notes	Creation Date
○	CL01		9/26/2023, 5:02:03 PM
●	CL02		4/1/2024, 12:37:51 PM

5. Validate the item is available on target content library.



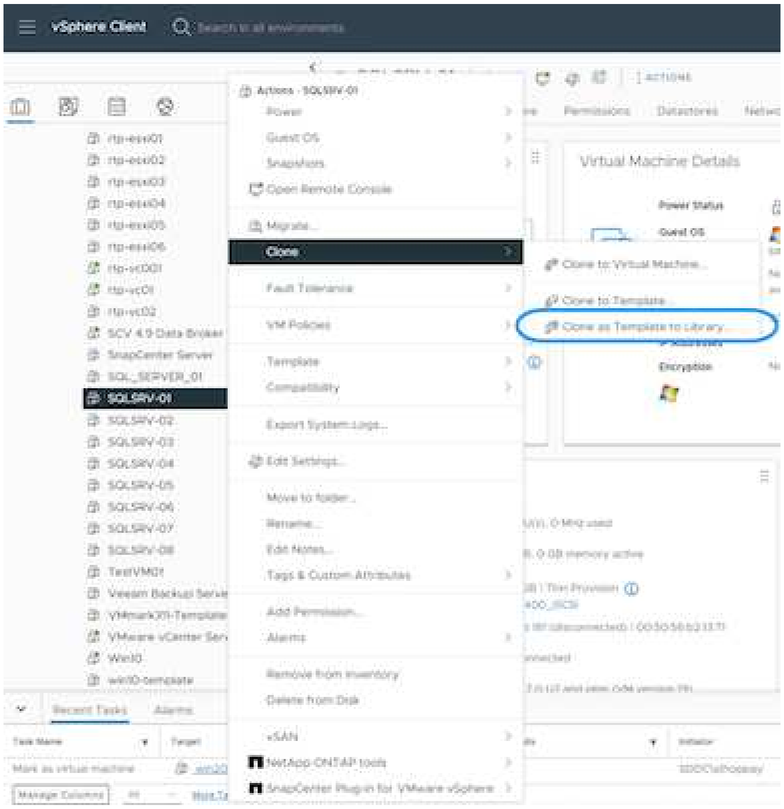
	Name	Guest OS	Stored Locally	Security Compliant	Size	Last Modified Date	Last Sync Date	Content Library	UUID	Content Version	Description
□	NetApp ONTAP-9.12.1.5		Yes	Yes	16.97 MB	04/03/2024, 5:39:01 PM		CL02	urn:vapi:com.vmware.content.library.item:a7cf728a-7bfa-479a-aa4a-8e3309bbf038:13119a50-8239-45f7-86ad-2ffc3f1461d8	2	

Here is the sample PowerCLI script to copy the content libary items from content library CL01 to CL02.

```
#Authenticate to vCenter Server(s)
$sourcevc = Connect-VIServer -server 'vcenter01.domain' -force
$targetvc = Connect-VIServer -server 'vcenter02.domain' -force

#Copy content library items from source vCenter content library CL01 to target vCenter content library CL02.
Get-ContentLibaryItem -ContentLibary (Get-ContentLibary 'CL01' -Server $sourcevc) | Where-Object { $_.ItemType -ne 'vm-template' } | Copy-ContentLibaryItem -ContentLibrary (Get-ContentLibary 'CL02' -Server $targetvc)
```

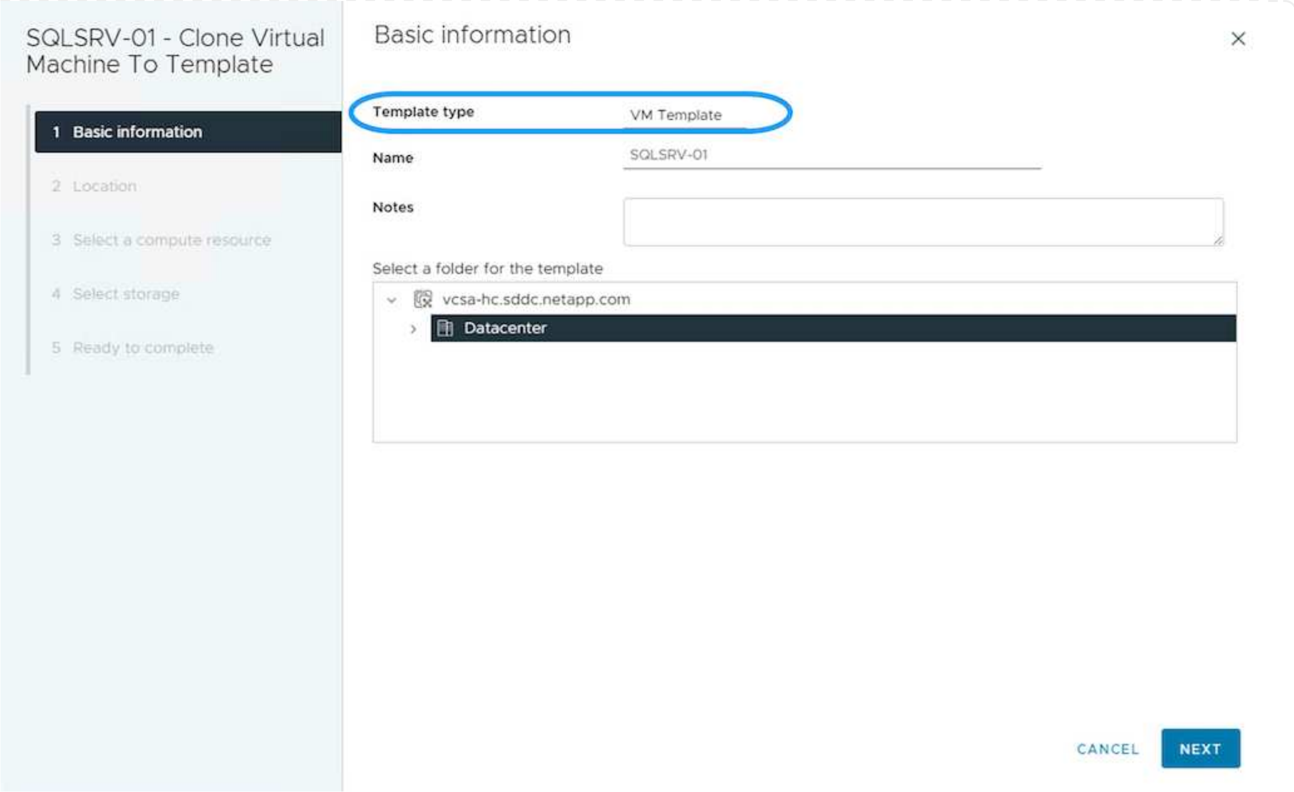
Adding VM as Templates in Content Library

1. In vSphere Web Client, select the VM and right click to choose Clone as Template in Library



When VM template is selected to clone in libary, it can only store it as OVF & OVA template and not as VM template.

2. Confirm Template type is selected as VM Template and follow answering the wizard to complete the operation.


SQLSRV-01 - Clone Virtual Machine To Template

1 Basic information

2 Location

3 Select a compute resource

4 Select storage

5 Ready to complete

Basic information

Template type: VM Template

Name: SQLSRV-01

Notes

Select a folder for the template

For additional details on VM templates on content library, check vSphere VM administration guide

Use Cases

Migration from third party storage systems (including vSAN) to ONTAP datastores.

- Based on where the ONTAP datastore is provisioned, pick the VM migration options from above.

Migration from previous version to latest version of vSphere.

- If in-place upgrade is not possible, can bring up new environment and use the migration options above.

In Cross vCenter migration option, import from target if export option is not available on source. For that procedure, check Import or Clone a Virtual Machine with Advanced Cross vCenter vMotion

Migration to VCF Workload Domain.

- Migrate VMs from each vSphere Cluster to target workload domain.

> ⓘ To allow network communication with existing VMs on other clusters on source vCenter, either extend NSX segment by adding the source vcenter vSphere hosts to transport zone or use L2 bridge on edge to allow L2 communication in VLAN. Check NSX documentation of Configure an Edge VM for Bridging

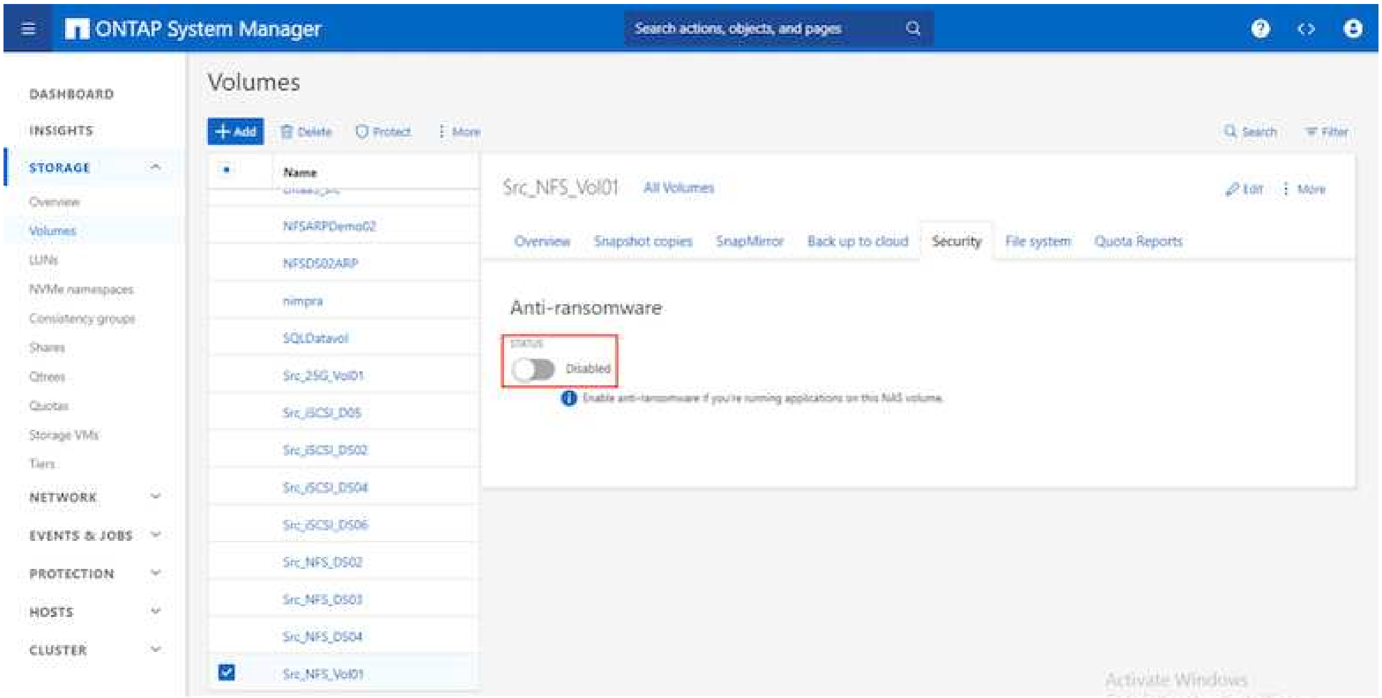
Additional Resources

- vSphere Virtual Machine Migration
- Migrating Virtual Machines with vSphere vMotion
- Tier-0 Gateway Configurations in NSX Federation
- HCX 4.8 User Guide
- VMware Live Recovery Documentation
- NetApp Disaster Recovery for VMware

Autonomous Ransomware Protection for NFS Storage

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

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



STATUS

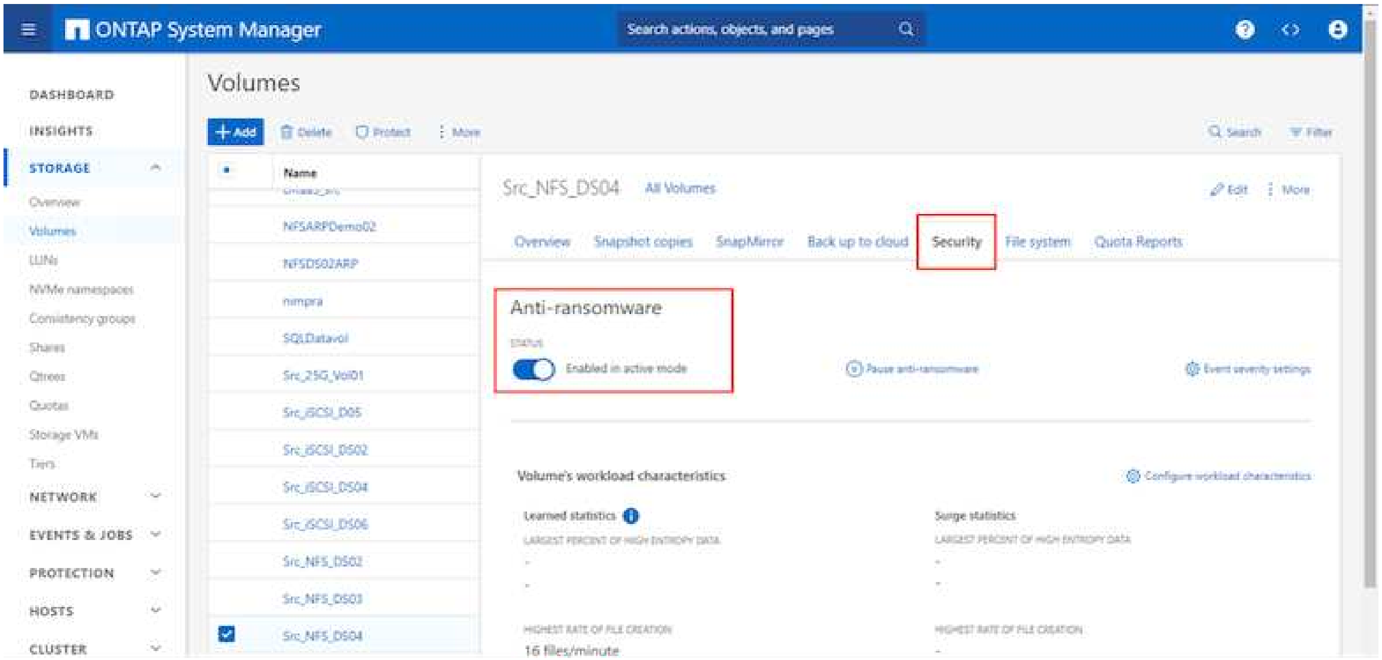
Disabled

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

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

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

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



Volumes

Name
NFSARPDemo02
NFSDS02ARP
nimpra
SQLDatavol
Src_25G_Vol01
Src_iSCSI_DS05
Src_iSCSI_DS02
Src_iSCSI_DS04
Src_iSCSI_DS06
Src_NFS_DS02
Src_NFS_DS03
☑ Src_NFS_DS04

Src_NFS_DS04 All Volumes

Anti-ransomware

STATUS

Enabled in active mode

Volume's workload characteristics

Learned statistics

LARGEST PERCENT OF HIGH ENTROPY DATA

-

-

HIGHEST RATE OF FILE CREATION

16 files/minute

Surge statistics

LARGEST PERCENT OF HIGH ENTROPY DATA

-

-

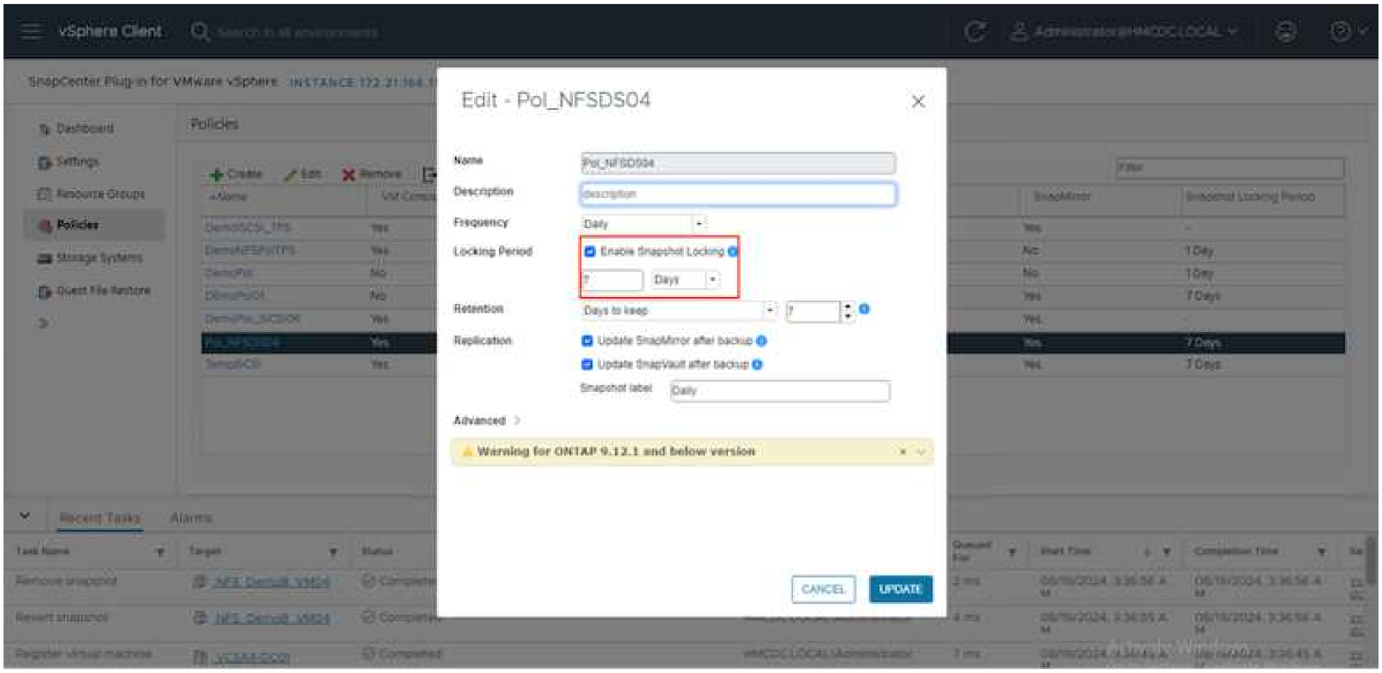
HIGHEST RATE OF FILE CREATION

-

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

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

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



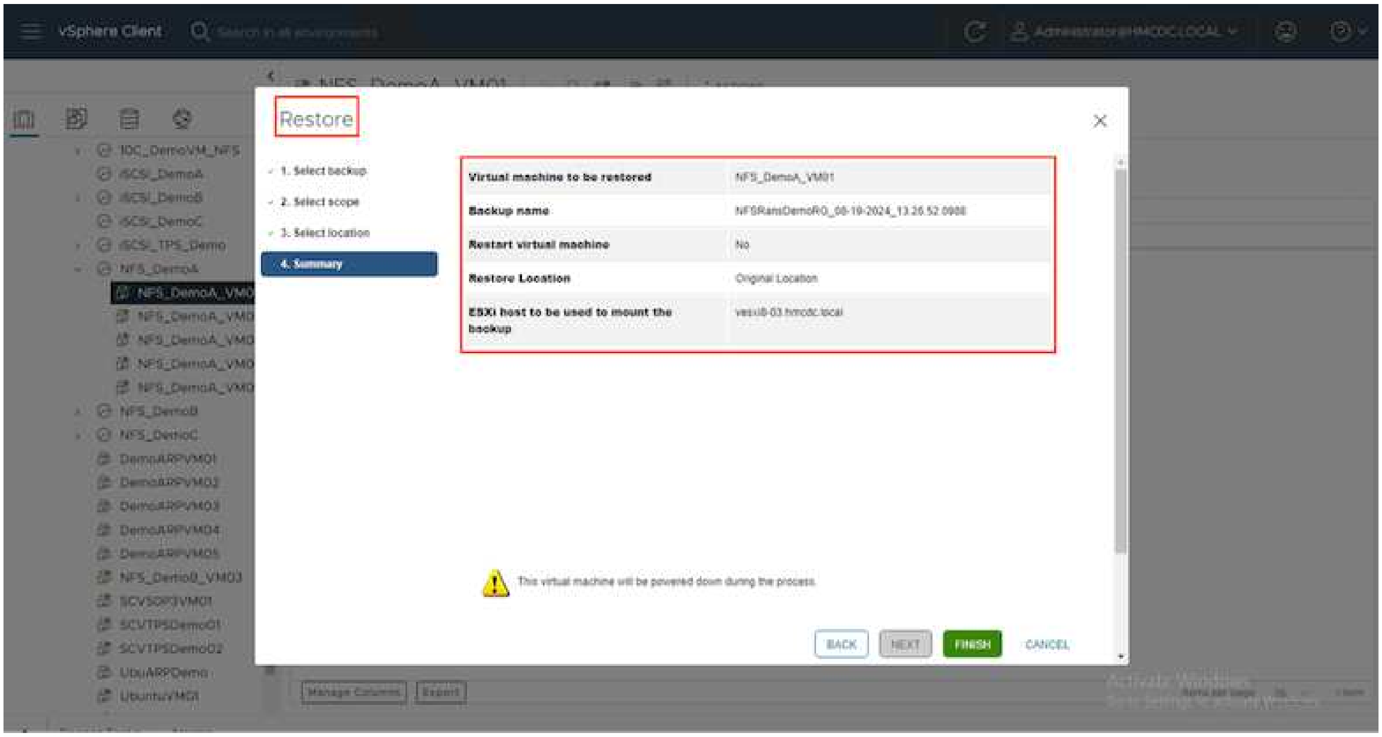
Edit - Pol_NFSDS04

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

Advanced >

Warning for ONTAP 9.12.1 and below version

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



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

This virtual machine will be powered down during the process.

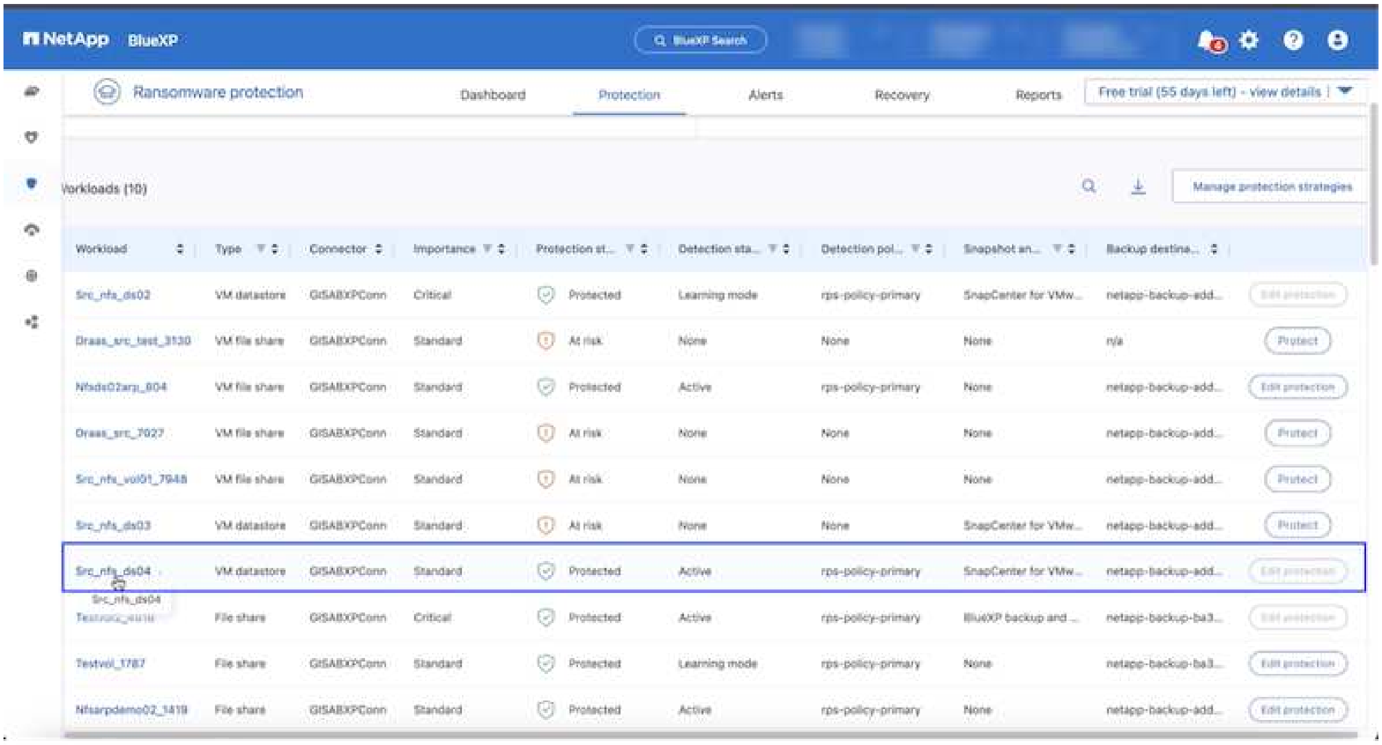
The above demonstrates how ONTAP storage adds an additional layer to the existing techniques, enhancing futureproofing of the environment.

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

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

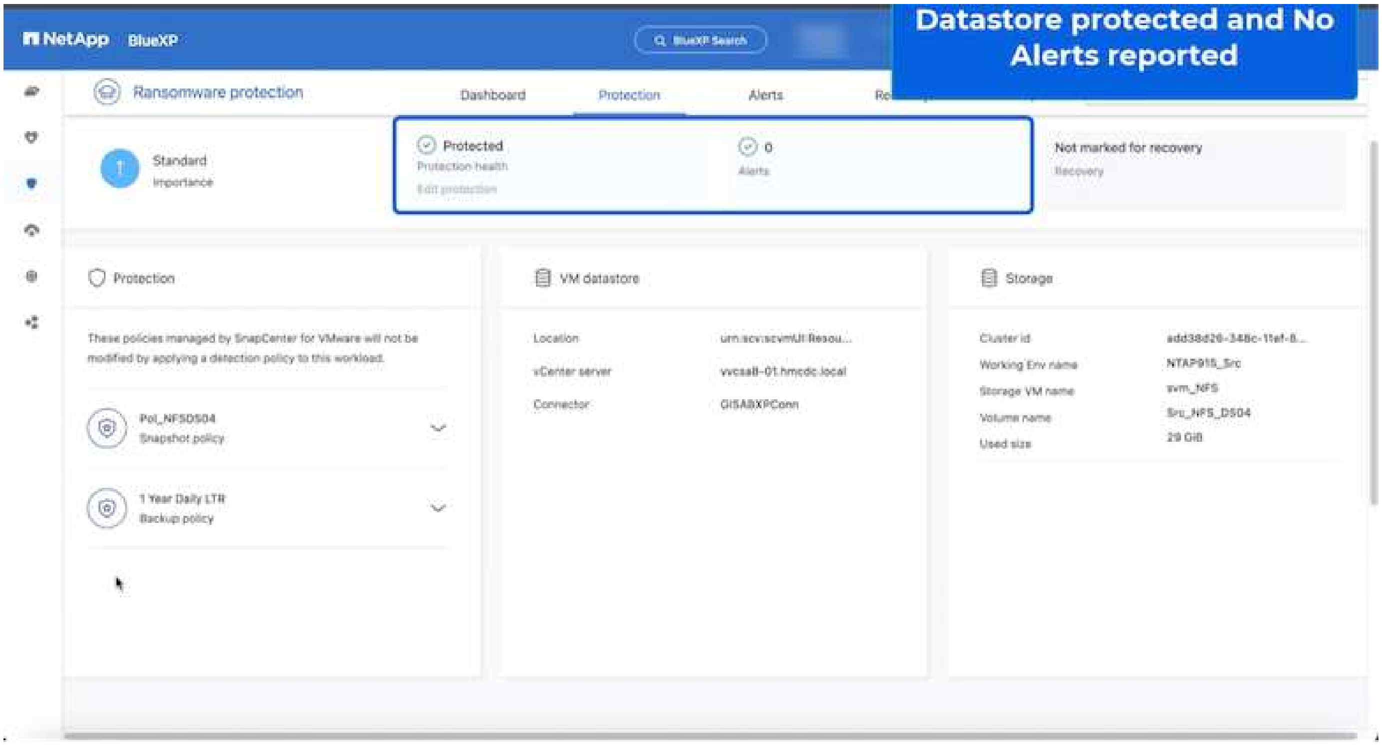
In this example, NFS datastore "Src_NFS_DS04" is protected using NetApp Ransomware Resilience.

ⓘ The steps outlined below are with BlueXP. The workflow is similar with the NetApp Console.



Workloads (10)

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



Datastore protected and No Alerts reported

Standard
Importance

Protected
Protection health
Edit protection

0
Alerts

Not marked for recovery
Recovery

Protection

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

Pol_NFSDS04
Snapshot policy

1 Year Daily LTR
Backup policy

VM datastore

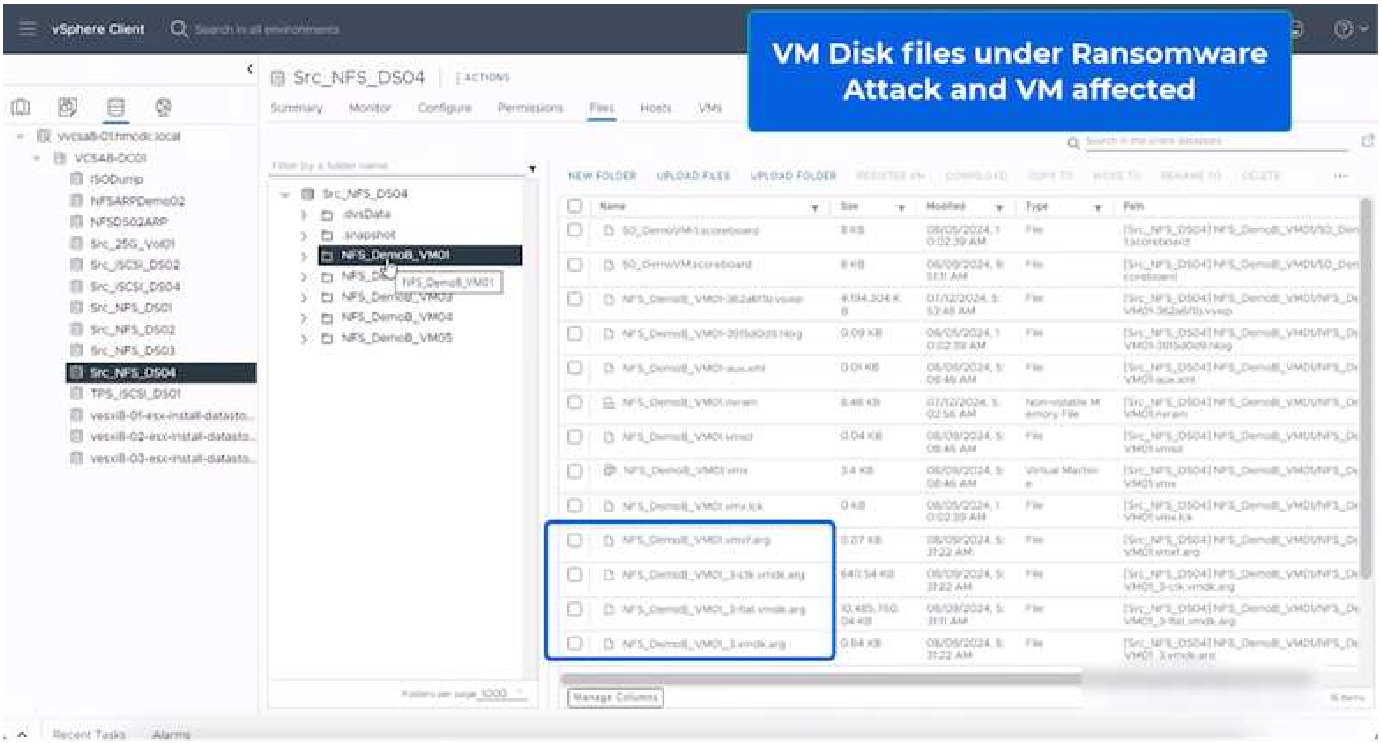
Location	urn:scv:scvmUI:Resou...
vCenter server	vvcsa8-01.hmcdc.local
Connector	GISABXPConn

Storage

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

For detailed information on to configure NetApp Ransomware Resilience, refer to Setup NetAp Ransomware Resilience and Configure NetAp Ransomware Resilience settings.

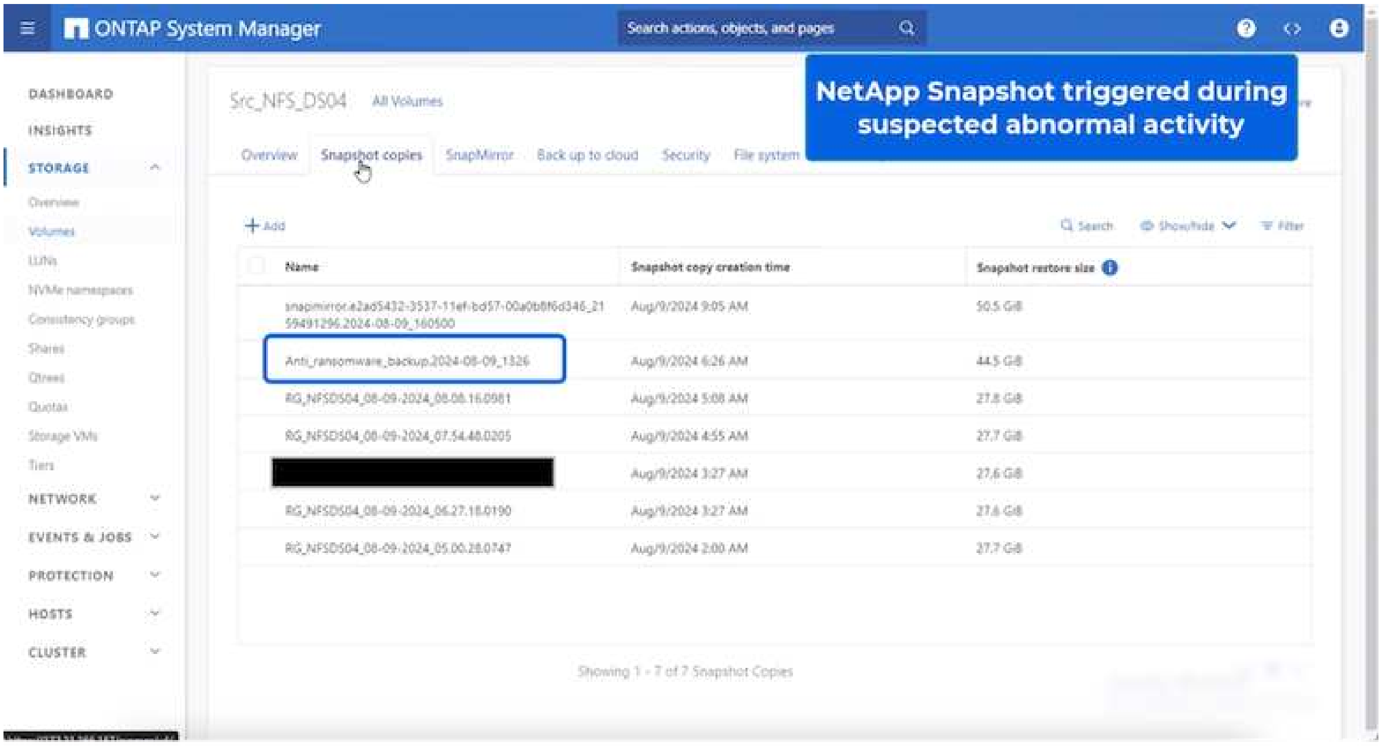
It’s time to walk through this with an example. In this walkthrough, the datastore "Src_NFS_DS04" is affected.



VM Disk files under Ransomware Attack and VM affected

Name	Size	Modified	Type	Path
SO_DemoVM-1.scoreboard	8 KB	08/05/2024, 10:02:39 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/SO_Dem 1.scoreboard
SO_DemoVM.scoreboard	8 KB	08/09/2024, 9:51:11 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/SO_Dem coreboard
NFS_DemoB_VM01-362a6f1b.vswp	4,194,304 KB	07/12/2024, 5:53:48 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01-362a6f1b.vswp
NFS_DemoB_VM01-3015d0d9.hlog	0.09 KB	08/05/2024, 10:02:39 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01-3015d0d9.hlog
NFS_DemoB_VM01-aux.xml	0.01 KB	08/09/2024, 5:08:46 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01-aux.xml
NFS_DemoB_VM01.nvram	8.48 KB	07/12/2024, 5:02:56 AM	Non-volatile Memory File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01.nvram
NFS_DemoB_VM01.vmsd	0.04 KB	08/09/2024, 5:08:45 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01.vmsd
NFS_DemoB_VM01.vmx	3.4 KB	08/09/2024, 5:08:46 AM	Virtual Machine	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01.vmx
NFS_DemoB_VM01.vmx.lck	0 KB	08/05/2024, 10:02:39 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01.vmx.lck
NFS_DemoB_VM01.vmxf.arg	0.07 KB	08/09/2024, 5:31:22 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01.vmxf.arg
NFS_DemoB_VM01_3-ctk.vmdk.arg	640.54 KB	08/09/2024, 5:31:22 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01_3-ctk.vmdk.arg
NFS_DemoB_VM01_3-flat.vmdk.arg	10,485,760.04 KB	08/09/2024, 5:31:11 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01_3-flat.vmdk.arg
NFS_DemoB_VM01_3.vmdk.arg	0.84 KB	08/09/2024, 5:31:22 AM	File	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_De VM01_3.vmdk.arg

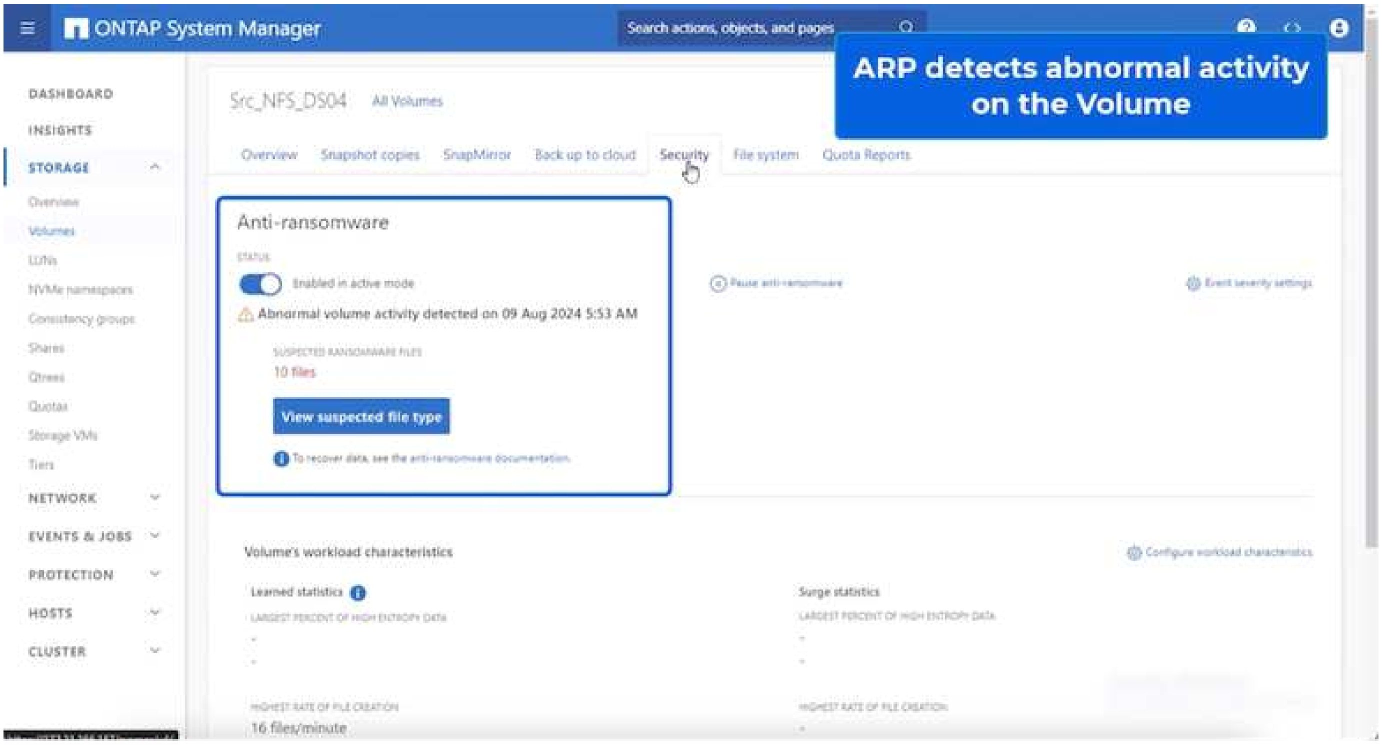
ARP immediately triggered a snapshot on the volume upon detection.



NetApp Snapshot triggered during suspected abnormal activity

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

Showing 1 - 7 of 7 Snapshot Copies



ARP detects abnormal activity on the Volume

ONTAP System Manager

Src_NFS_DS04 All Volumes

Overview | Snapshot copies | SnapMirror | Back up to cloud | Security | File system | Quota Reports

Anti-ransomware

STATUS

Enabled in active mode

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

SUSPECTED RANSOMWARE FILES
10 files

View suspected file type

To recover data, see the anti-ransomware documentation.

Pause anti-ransomware

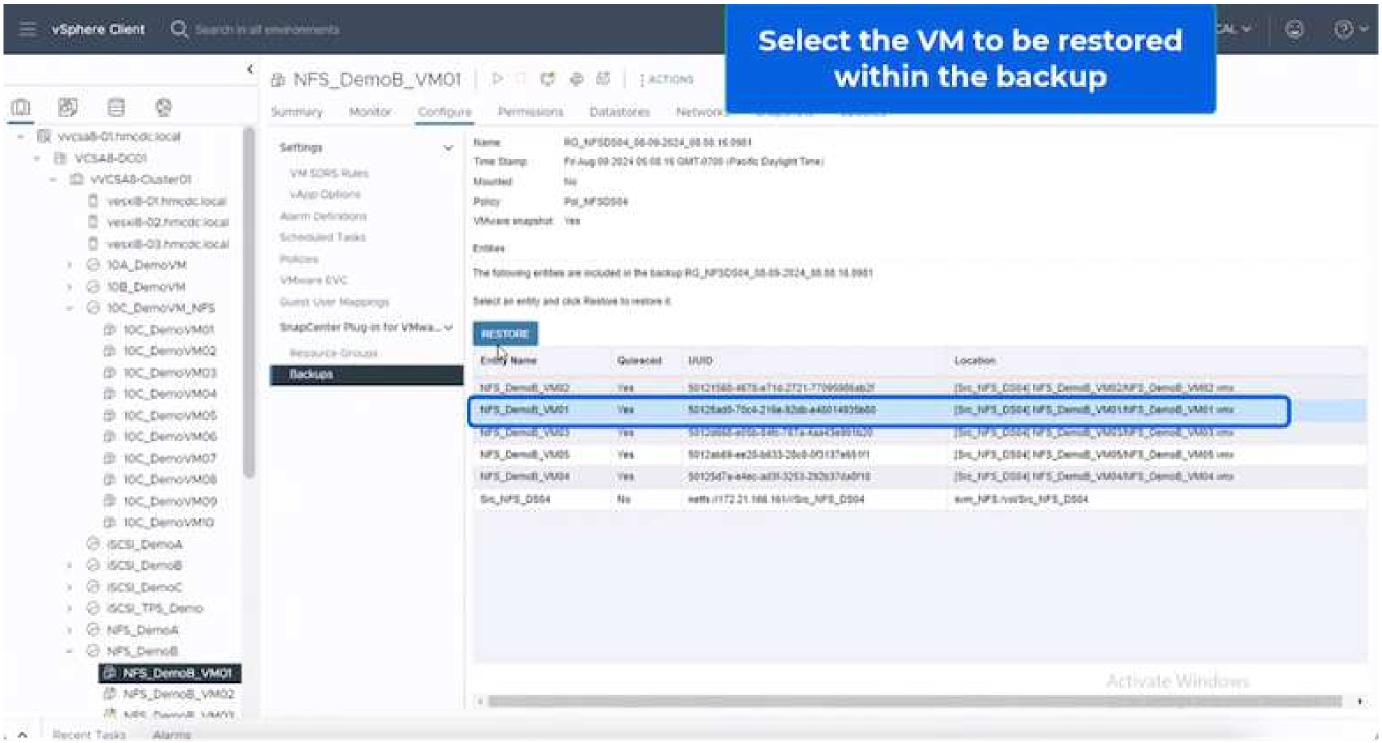
Event severity settings

Volume's workload characteristics

Configure workload characteristics

Learned statistics	Surge statistics
LARGEST PERCENT OF HIGH ENTROPY DATA	LARGEST PERCENT OF HIGH ENTROPY DATA
-	-
-	-
HIGHEST RATE OF FILE CREATION	HIGHEST RATE OF FILE CREATION
16 files/minute	-

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



Select the VM to be restored within the backup

NFS_DemoB_VM01

Name	RG_NFSDS04_08-09-2024_05.08.16.0981
Time Stamp	Fri Aug 09 2024 05:08:16 GMT-0700 (Pacific Daylight Time)
Mounted	No
Policy	Pol_NFSDS04
VMware snapshot	Yes

Entities

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

Select an entity and click Restore to restore it.

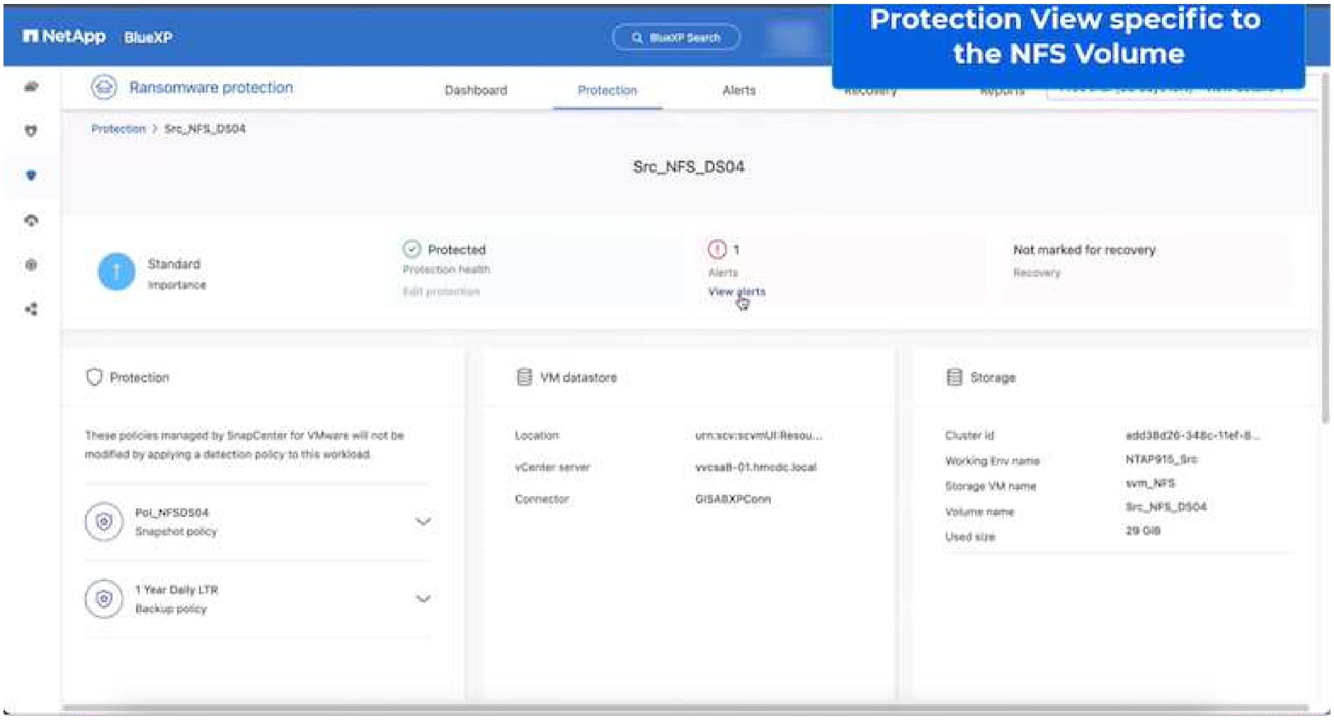
RESTORE

Entity Name	Quiesced	UUID	Location
NFS_DemoB_VM02	Yes	50121568-4678-a71d-2721-77095906ab2f	[Src_NFS_DS04] NFS_DemoB_VM02/NFS_DemoB_VM02.vmx
NFS_DemoB_VM01	Yes	50125ad0-70c4-216e-82db-a46014935a80	[Src_NFS_DS04] NFS_DemoB_VM01/NFS_DemoB_VM01.vmx
NFS_DemoB_VM03	Yes	5012a668-a058-84fc-787a-4aa43e901620	[Src_NFS_DS04] NFS_DemoB_VM03/NFS_DemoB_VM03.vmx
NFS_DemoB_VM05	Yes	5012ab69-ee20-b633-28c0-0f5137e65f1f	[Src_NFS_DS04] NFS_DemoB_VM05/NFS_DemoB_VM05.vmx
NFS_DemoB_VM04	Yes	50125d7a-a4ec-ad31-3253-292b37da0f18	[Src_NFS_DS04] NFS_DemoB_VM04/NFS_DemoB_VM04.vmx
Src_NFS_DS04	No	netfs://172.21.166.161//Src_NFS_DS04	svm_NFS:/vol/Src_NFS_DS04

This section looks at how NetApp Ransomware Resilience orchestrates recovery from a ransomware incident wherein the VM files are encrypted.

> ⓘ If the VM is managed by SnapCenter, NetApp Ransomware Resilience restores the VM back to its previous state using the VM-consistent process.

1. Access NetApp Ransomware Resilience and an alert appears on the NetApp Ransomware Resilience Dashboard.
2. Click on the alert to review the incidents on that specific volume for the generated alert



Protection View specific to the NFS Volume

Src_NFS_DS04

Standard
Importance

Protected
Protection health

1
Alerts

Not marked for recovery
Recovery

Protection

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

Pol_NFSDS04
Snapshot policy

1 Year Daily LTR
Backup policy

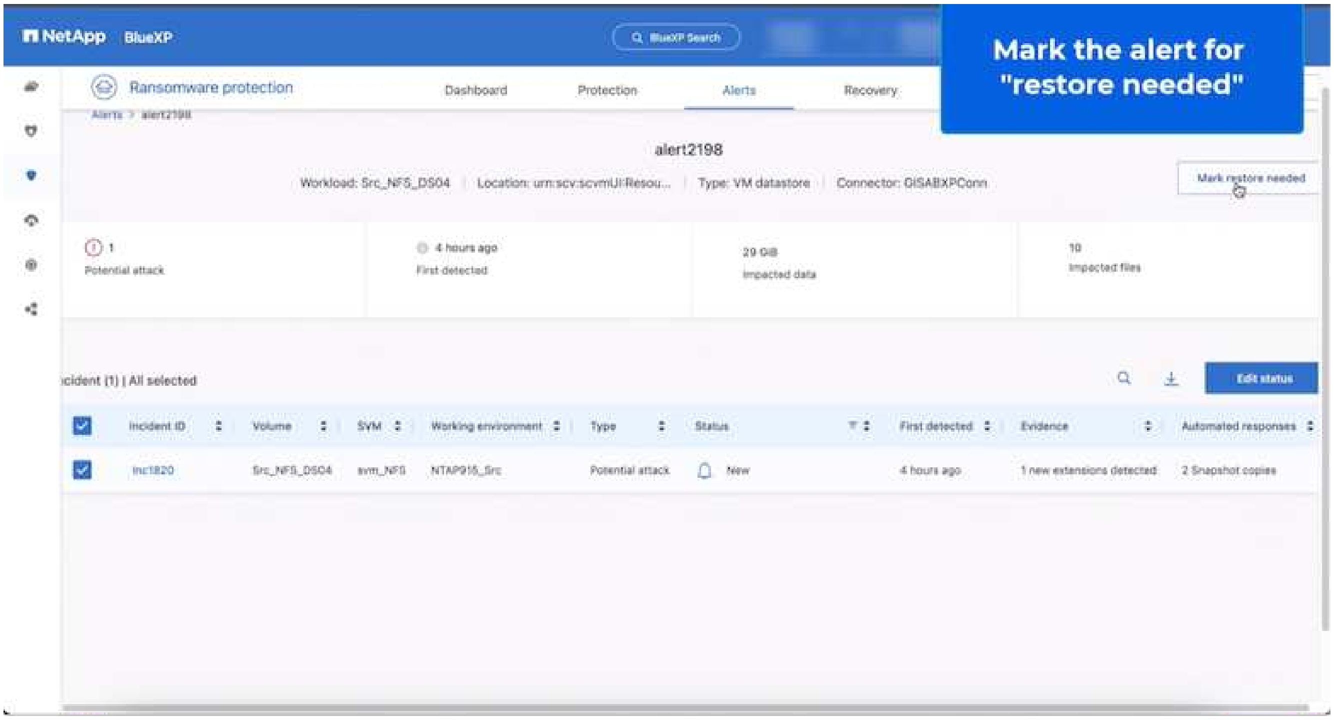
VM datastore

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

Storage

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

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



Mark the alert for "restore needed"

alert2198

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

1
Potential attack

4 hours ago
First detected

29 GiB
Impacted data

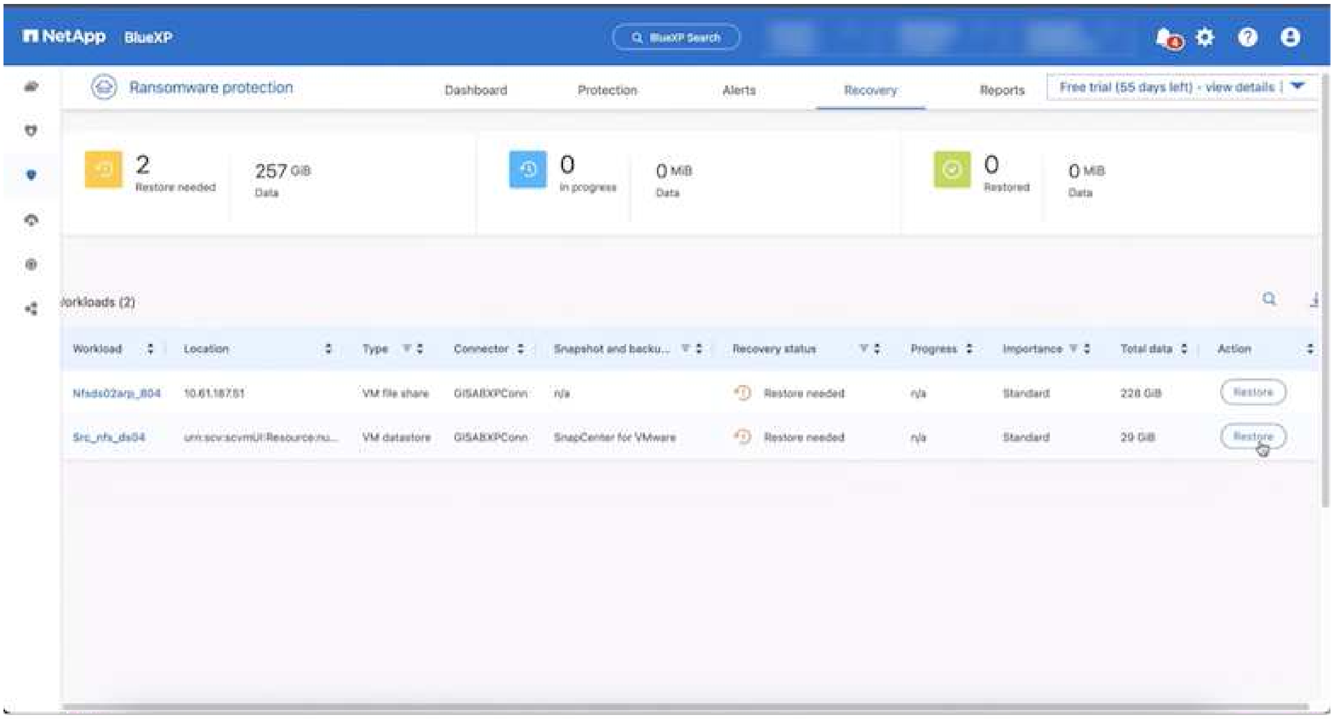
10
Impacted files

Incident (1) | All selected

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

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

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

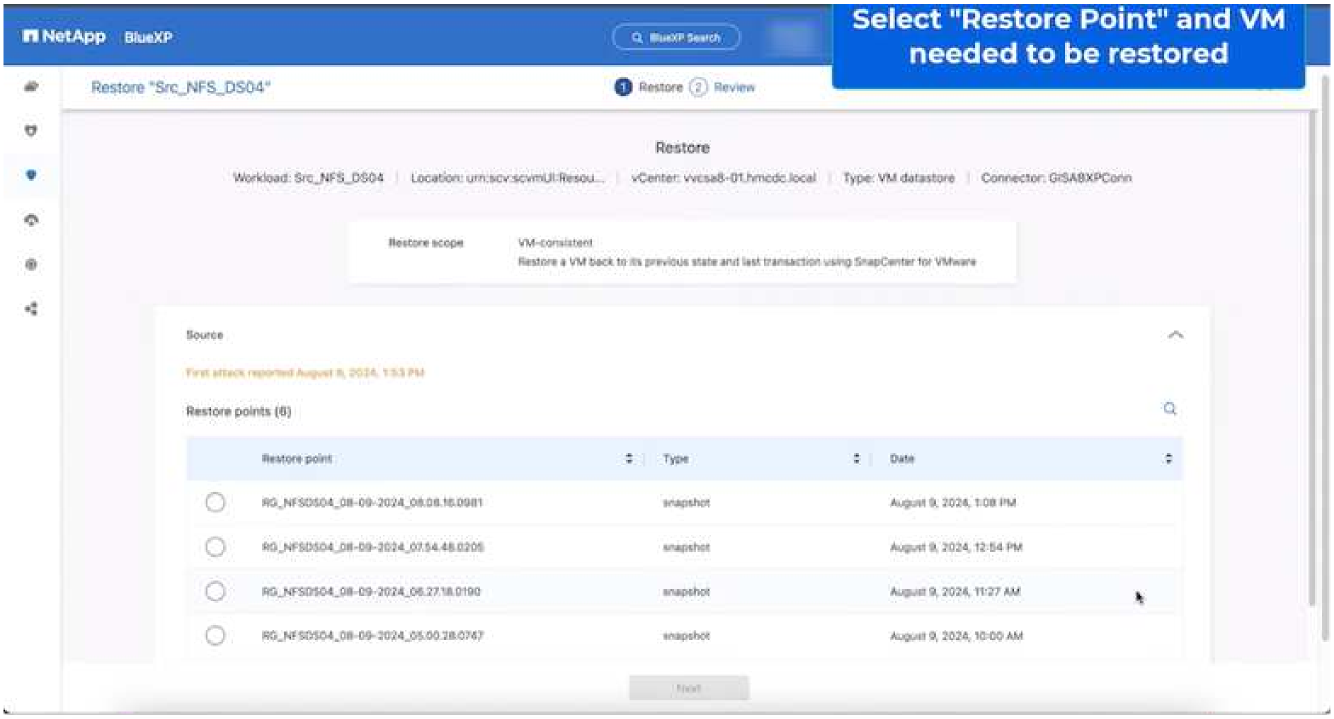


2 Restore needed | 257 GiB Data
0 In progress | 0 MiB Data
0 Restored | 0 MiB Data

Workloads (2)

Workload	Location	Type	Connector	Snapshot and backu...	Recovery status	Progress	Importance	Total data	Action
Nfsds02arp_804	10.61.187.51	VM file share	GISABXPConn	n/a	Restore needed	n/a	Standard	228 GiB	Restore
Src_nfs_ds04	urn:scv:scvmUI:Resource:nu...	VM datastore	GISABXPConn	SnapCenter for VMware	Restore needed	n/a	Standard	20 GiB	Restore

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



Restore

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

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

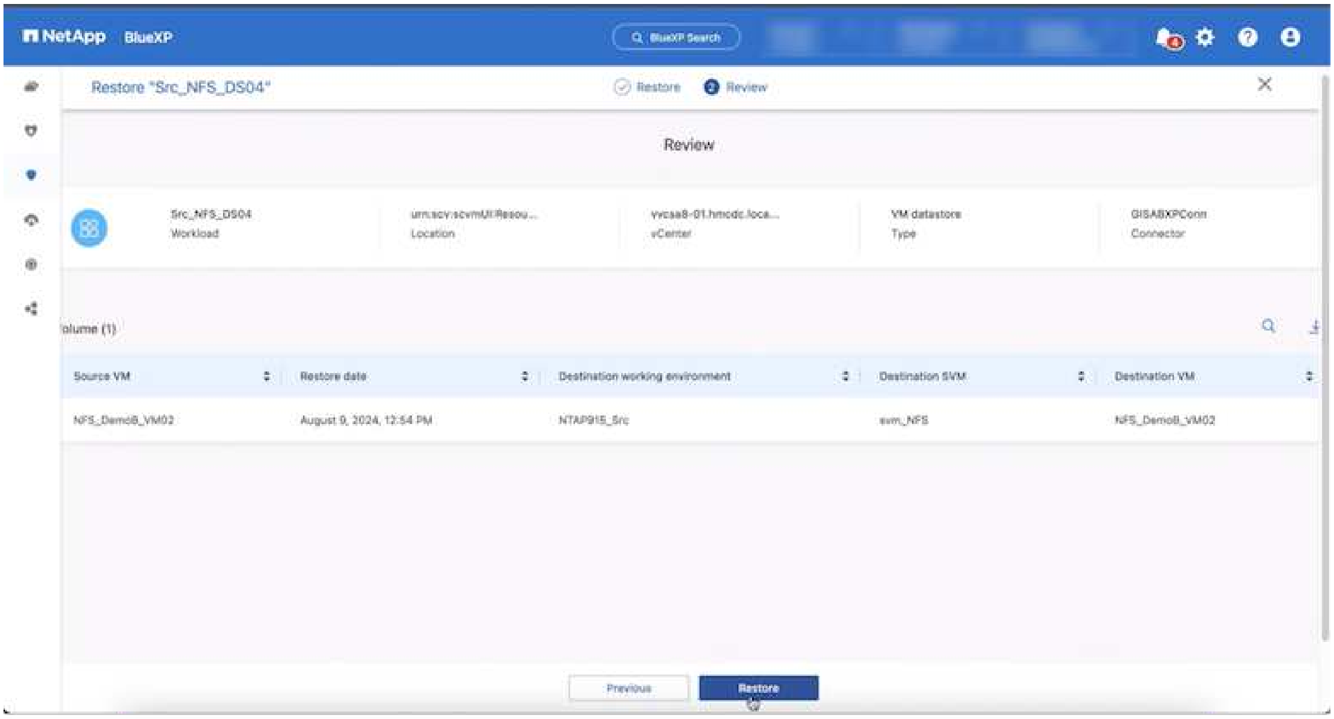
Source

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

Restore points (6)

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

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

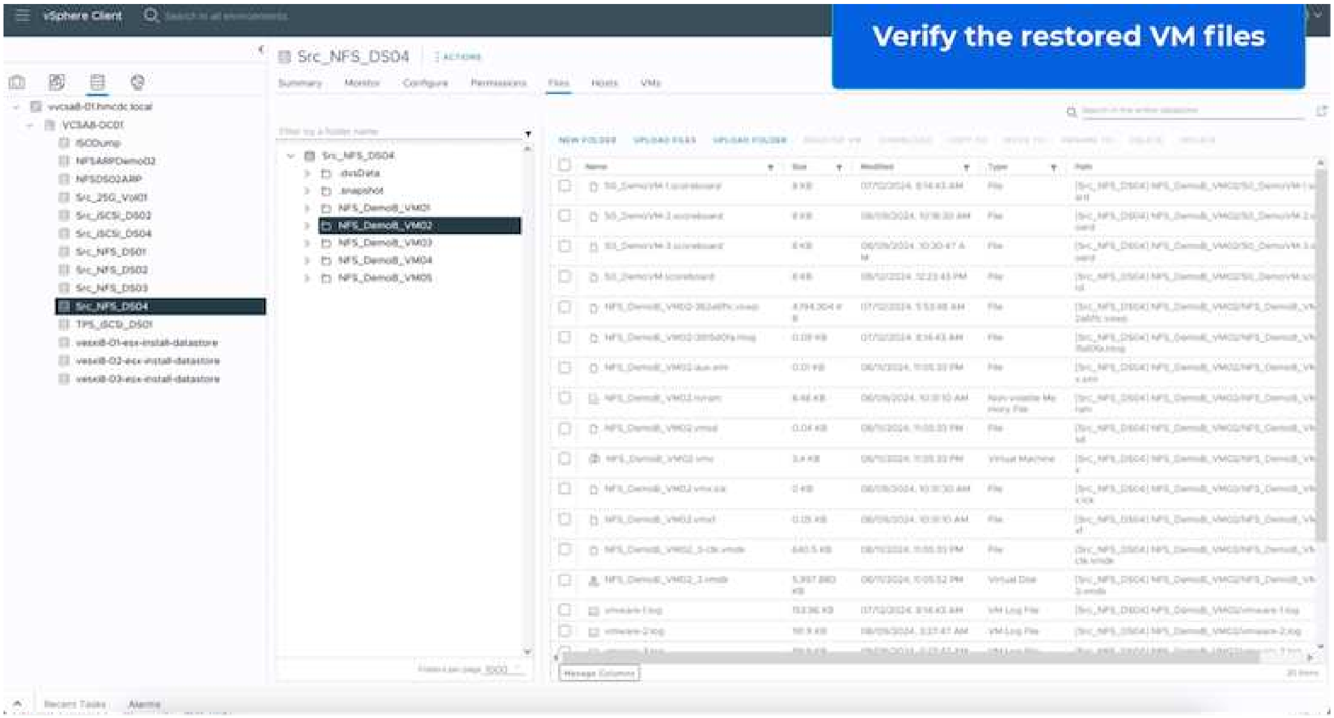


Src_NFS_DS04	urn:scv:scvmUI:Resou...	vvcsa8-01.hmcdc.loca...	VM datastore	GISABXPConn
Workload	Location	vCenter	Type	Connector

olume (1)

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

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



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

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

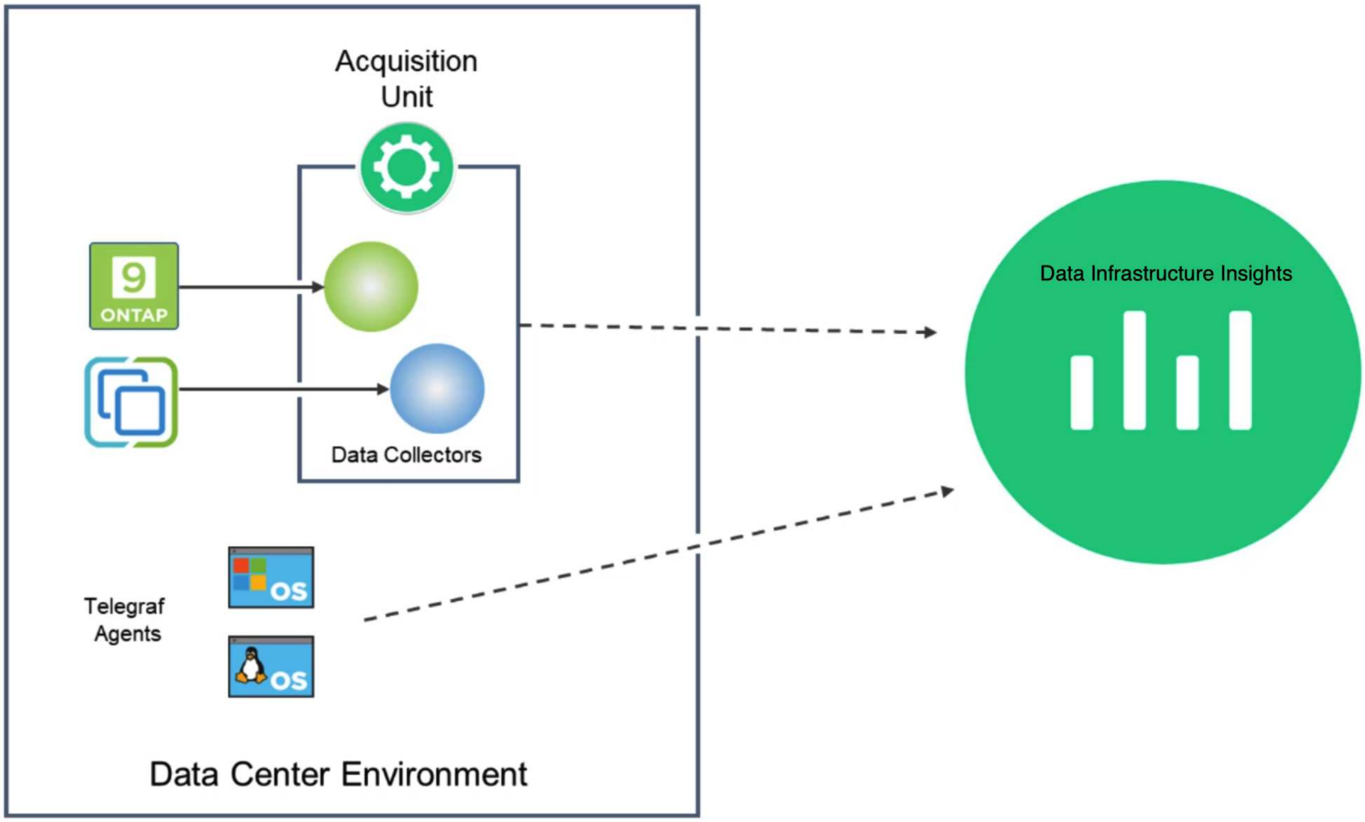
Monitor on-premises storage with Data Infrastructure Insights

NetApp Data Infrastructure Insights (formerly Cloud Insights) is a cloud-based platform designed to monitor and analyze the performance, health, and costs of IT infrastructures, both on-premises and in the cloud. Learn how to deploy data collectors, analyze performance metrics, and use dashboards to identify issues and optimize resources.

Monitoring On-Premises Storage with Data Infrastructure Insights

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

Data Infrastructure Insights architecture diagram:



Solution Deployment Overview

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

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

1. Configure Data Collector for a vSphere cluster.
2. Configure Data Collector for an ONTAP storage system.

3. Use Annotation Rules to tag assets.
4. Explore and correlate assets.
5. Use a Top VM Latency dashboard to isolate noisy neighbors.
6. Identify opportunities to rightsize VMs.
7. Use queries to isolate and sort metrics.

Prerequisites

This solution uses the following components:

1. NetApp All-Flash SAN Array A400 with ONTAP 9.13.
2. VMware vSphere 8.0 cluster.
3. NetApp Console account.
4. NetApp Data Infrastructure Insights Acquisition Unit software installed on a local VM with network connectivity to assets for data collection.

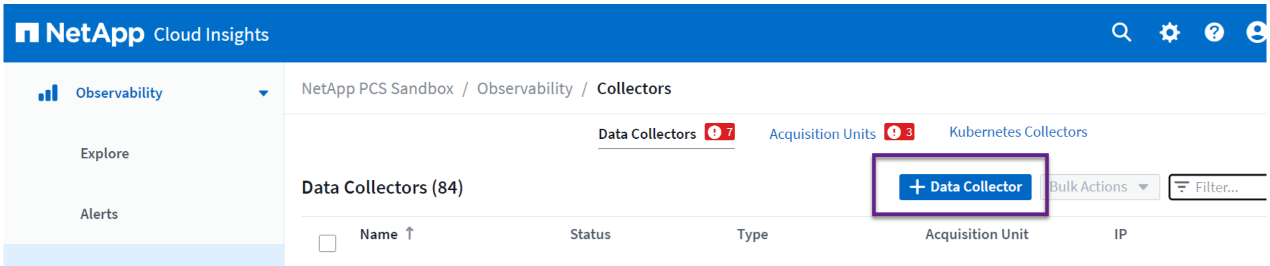
Solution Deployment

Configure Data Collectors

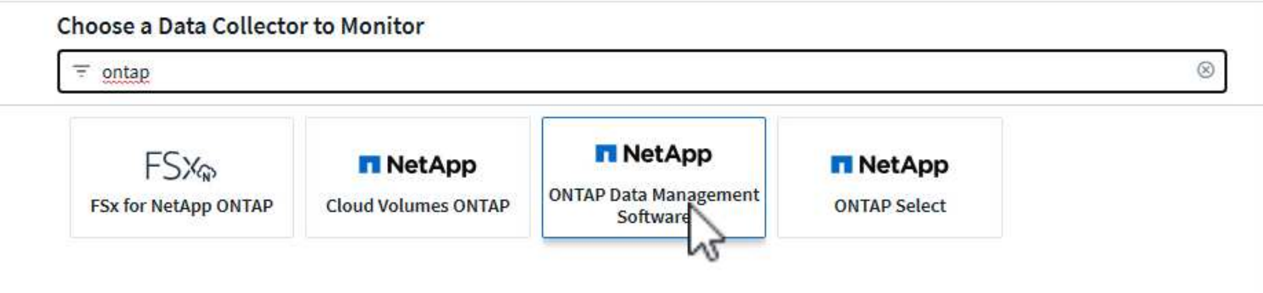
To configure Data Collectors for VMware vSphere and ONTAP storage systems complete the following steps:

Add a Data Collector for an ONTAP storage systems

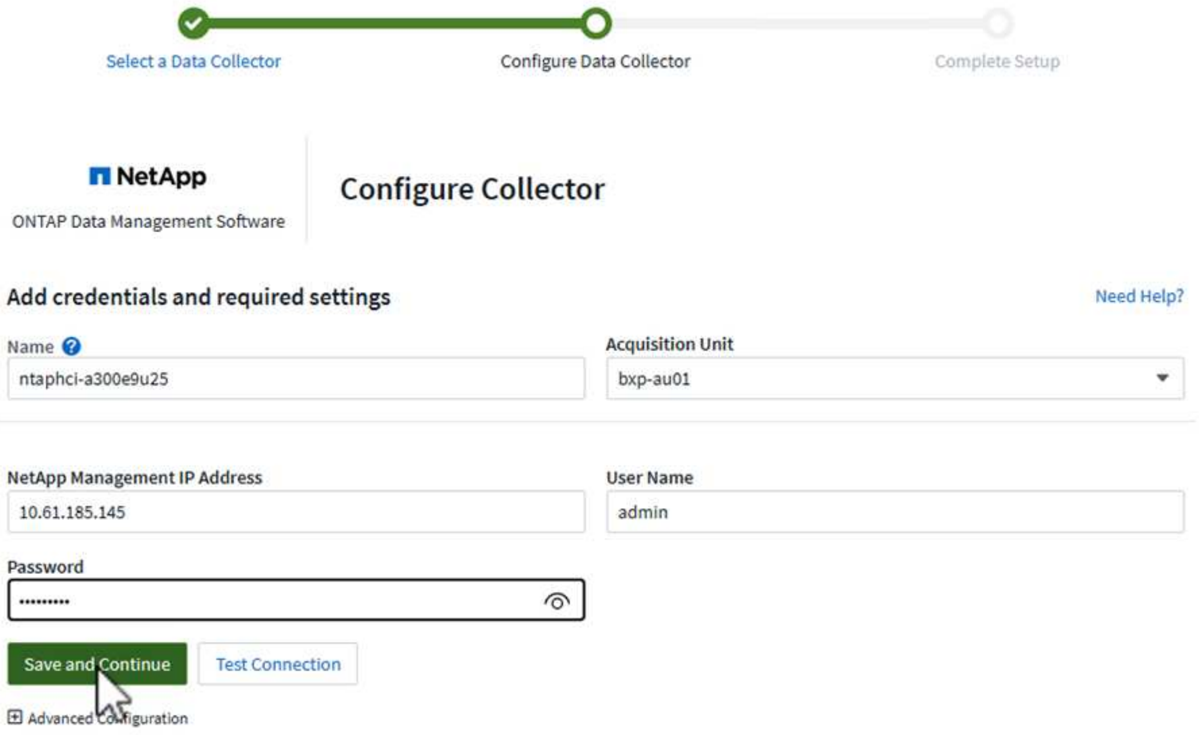
1. Once logged into Data Infrastructure Insights, navigate to **Observability > Collectors > Data Collectors** and press the button to install a new Data Collector.



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


Choose a Data Collector to Monitor
ontap
FSx for NetApp ONTAP
NetApp Cloud Volumes ONTAP
NetApp ONTAP Data Management Software
NetApp ONTAP Select

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



Name: ntaphci-a300e9u25

Acquisition Unit: bxp-au01

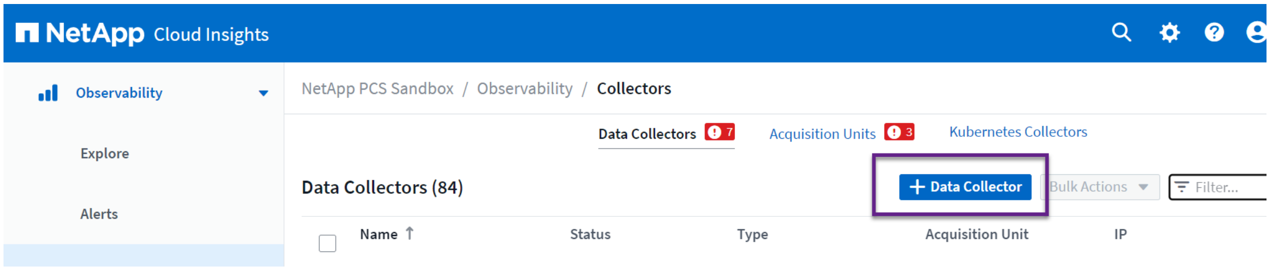
NetApp Management IP Address: 10.61.185.145

User Name: admin

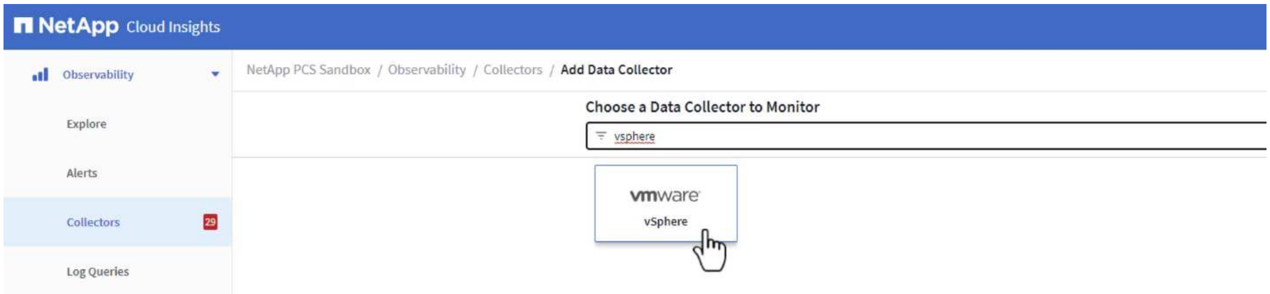
Password: ••••••••••

Add a Data Collector for a VMware vSphere cluster

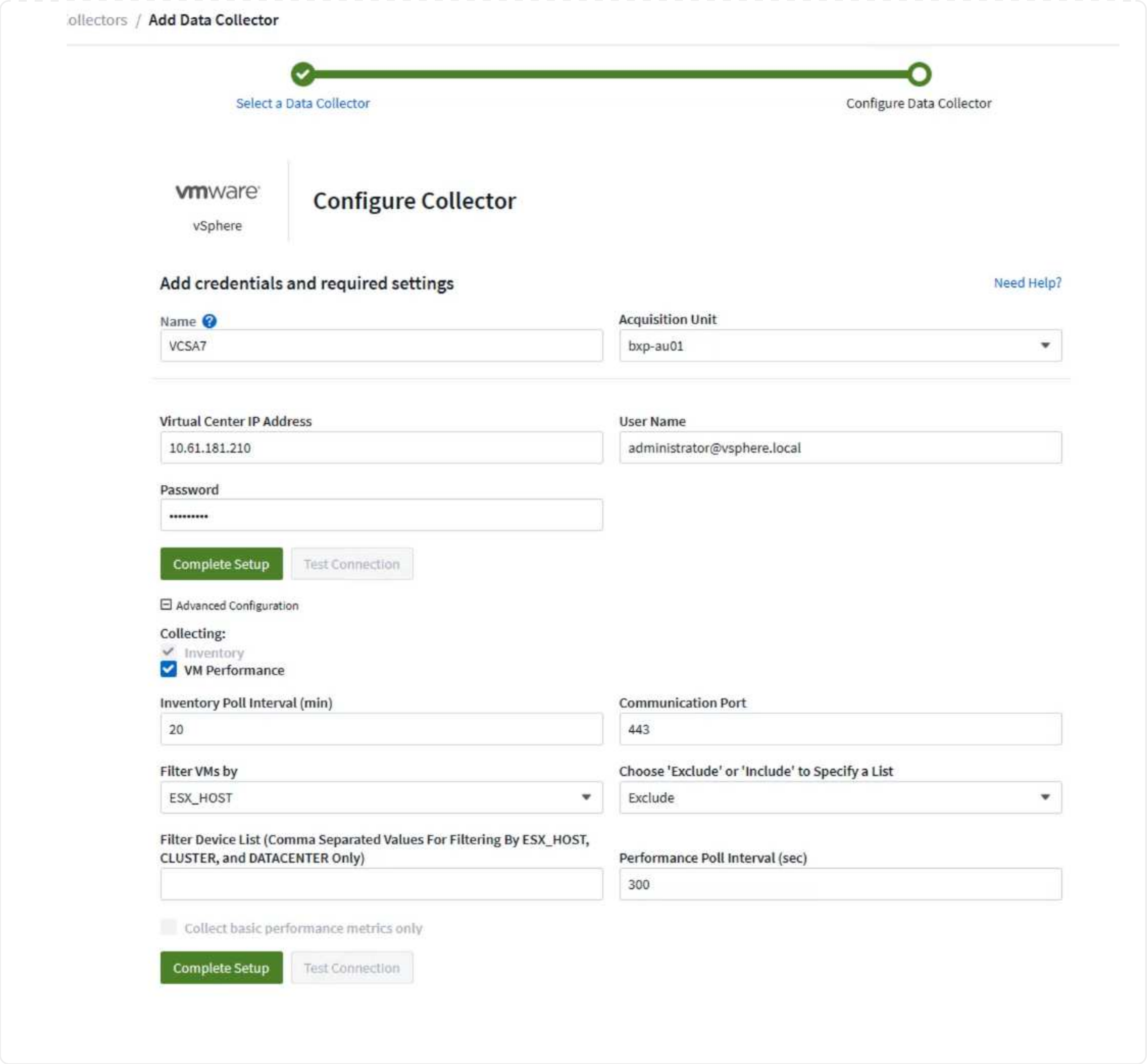
1. Once again, navigate to **Observability > Collectors > Data Collectors** and press the button to install a new Data Collector.



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


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

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



ollectors / Add Data Collector

Configure Collector

Add credentials and required settings

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

Collecting:
- ✓ Inventory
- ☑ VM Performance

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

□ Collect basic performance metrics only

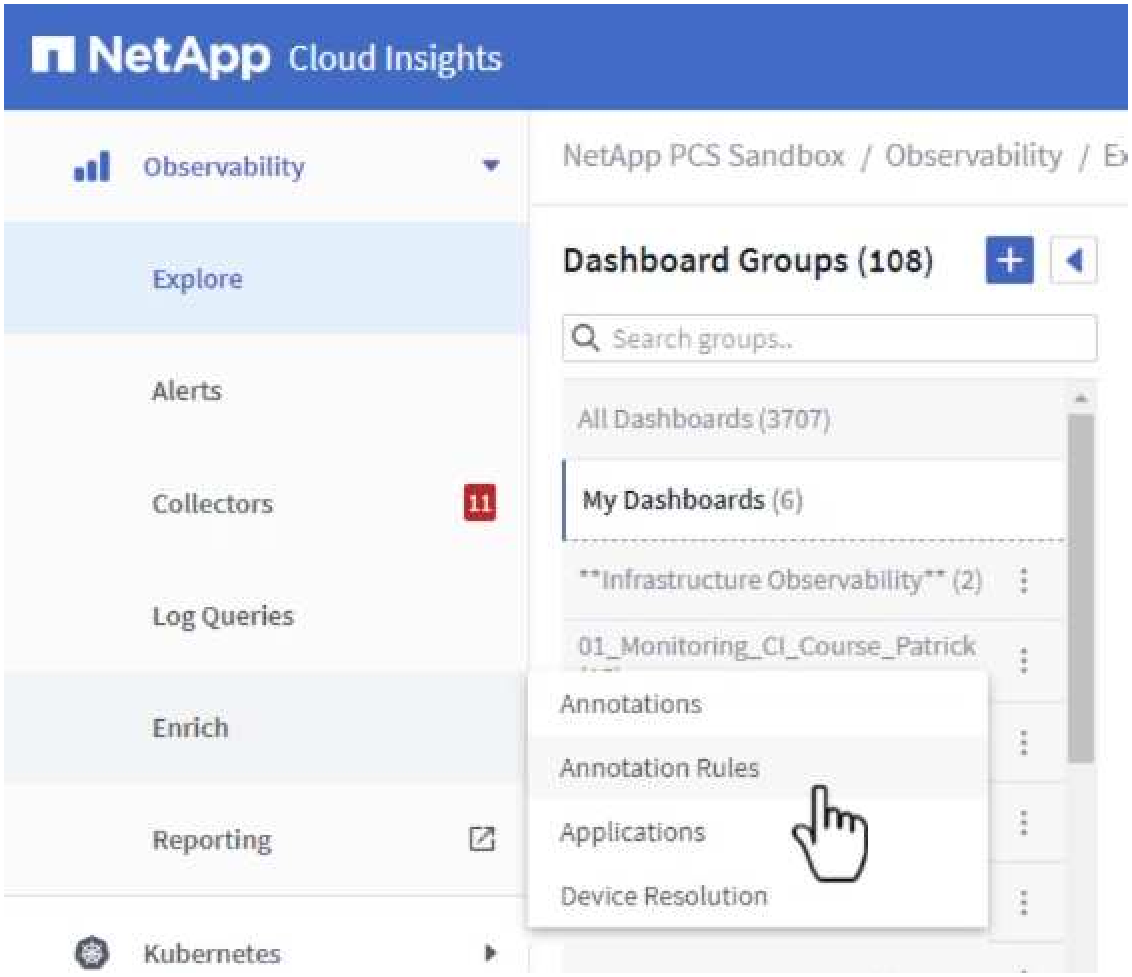
Add Annotations to assets

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

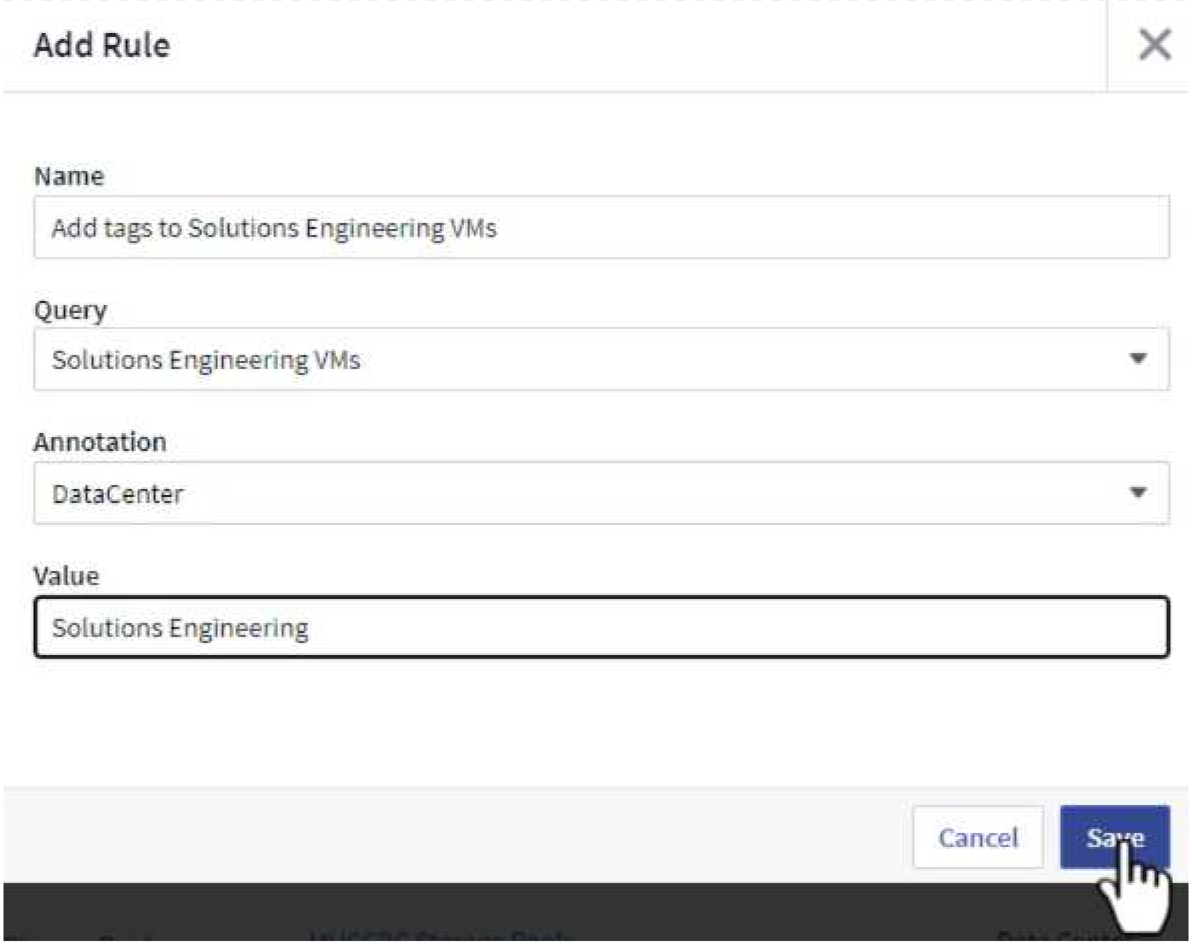
In this section, annotations will be added to virtual machine assets for filtering by **Data Center**.

Use Annotation Rules to tag assets

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



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



Add Rule

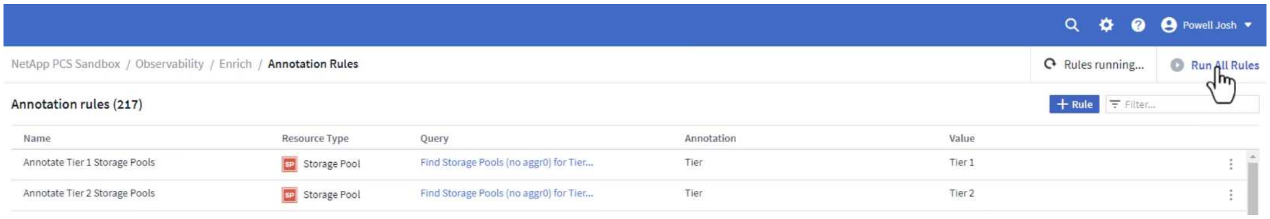
Name: Add tags to Solutions Engineering VMs

Query: Solutions Engineering VMs

Annotation: DataCenter

Value: Solutions Engineering

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



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

Annotation rules (217)

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

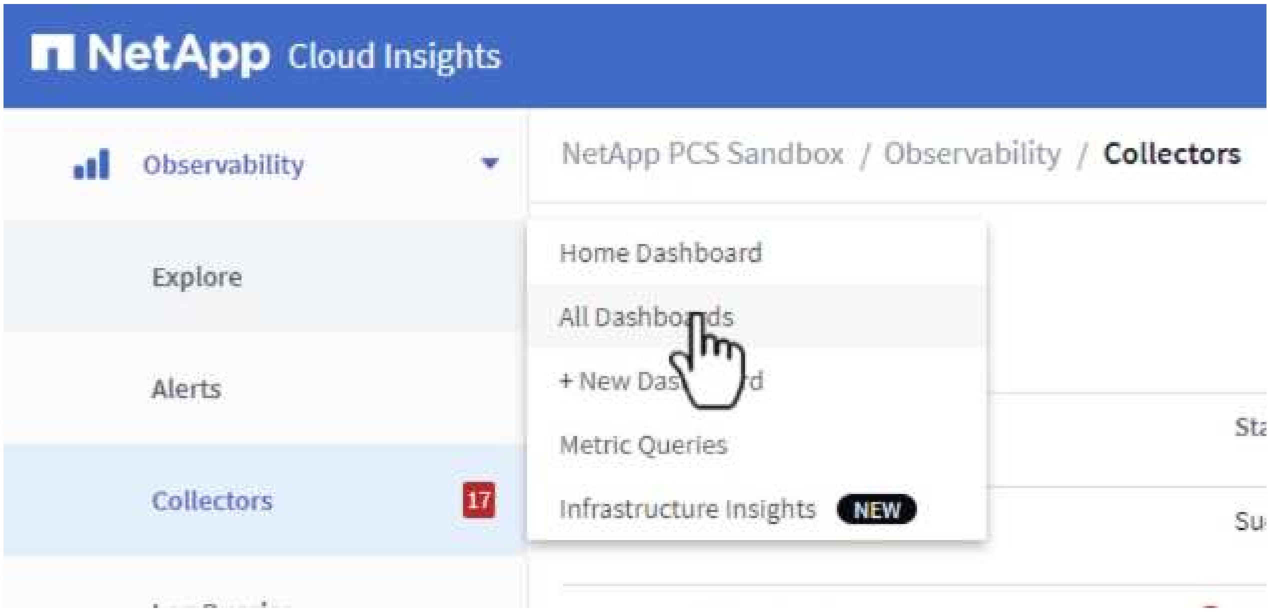
Explore and correlate assets

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

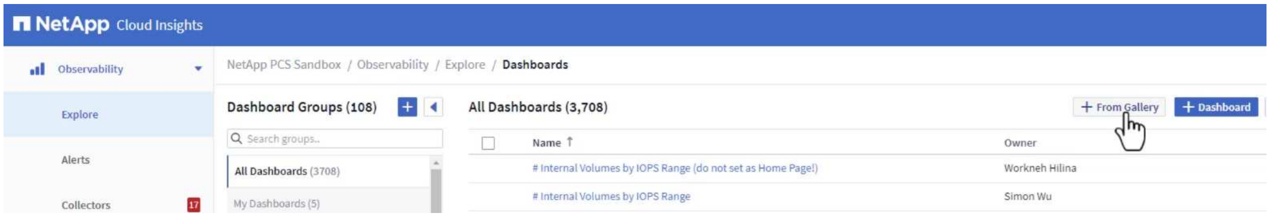
This sections illustrates how to use dashboards to correlate assets.

Correlating assets from a storage performance Dashboard

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

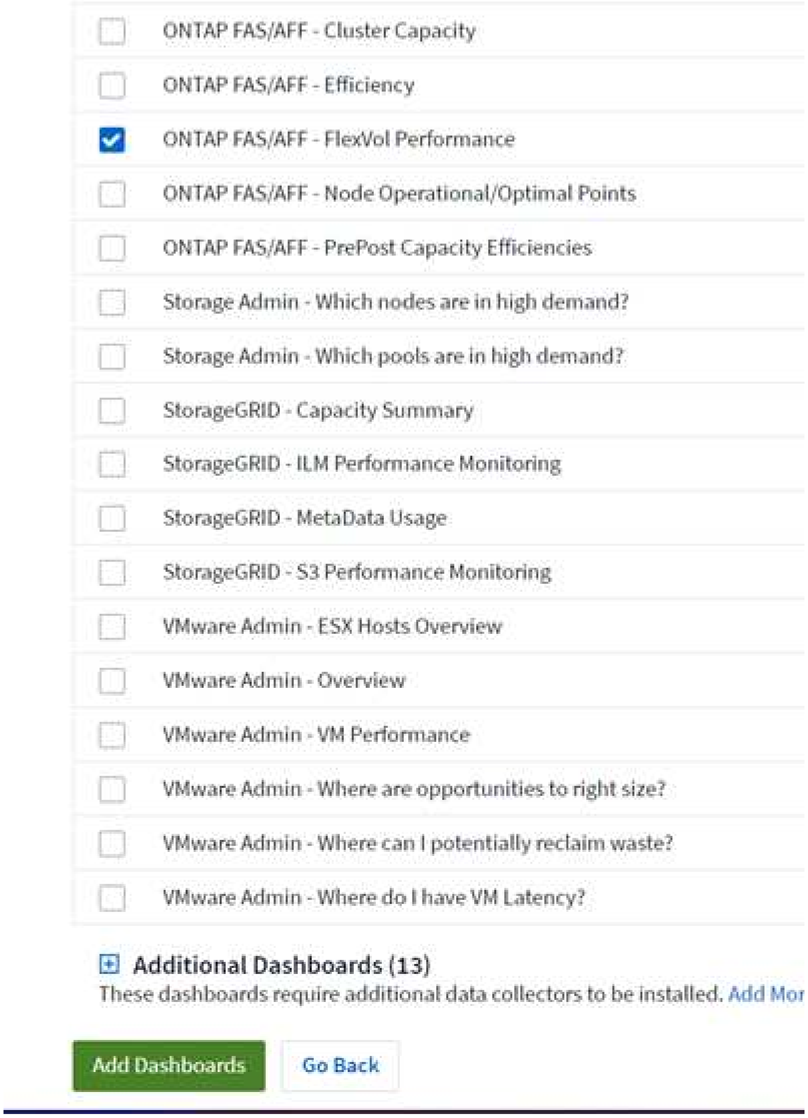


2. Click on the **+ From Gallery** button to view a list of ready-made dashboards that can be imported.



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

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



□ ONTAP FAS/AFF - Cluster Capacity

□ ONTAP FAS/AFF - Efficiency

☑ ONTAP FAS/AFF - FlexVol Performance

□ ONTAP FAS/AFF - Node Operational/Optimal Points

□ ONTAP FAS/AFF - PrePost Capacity Efficiencies

□ Storage Admin - Which nodes are in high demand?

□ Storage Admin - Which pools are in high demand?

□ StorageGRID - Capacity Summary

□ StorageGRID - ILM Performance Monitoring

□ StorageGRID - MetaData Usage

□ StorageGRID - S3 Performance Monitoring

□ VMware Admin - ESX Hosts Overview

□ VMware Admin - Overview

□ VMware Admin - VM Performance

□ VMware Admin - Where are opportunities to right size?

□ VMware Admin - Where can I potentially reclaim waste?

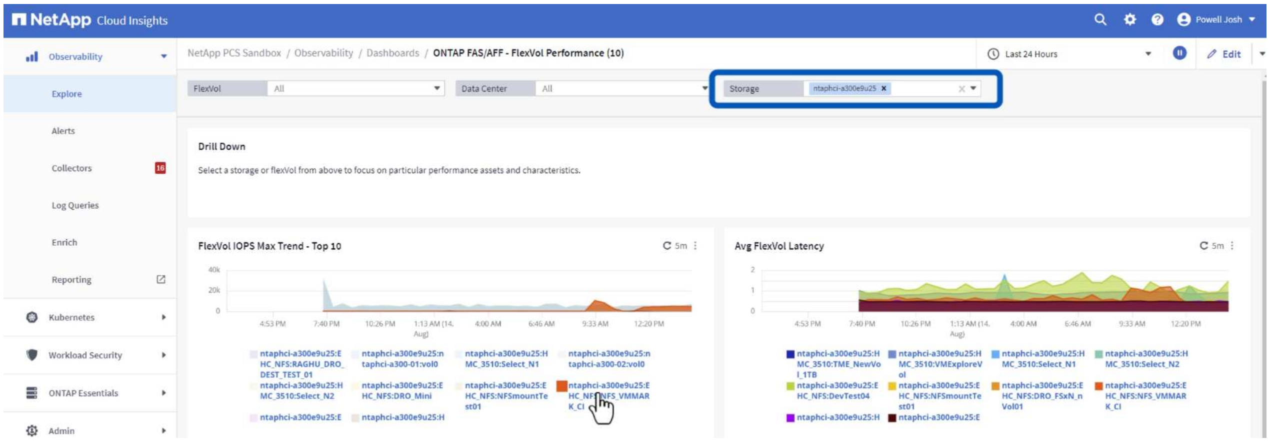
□ VMware Admin - Where do I have VM Latency?

⊞ Additional Dashboards (13)

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

Add Dashboards | Go Back

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



NetApp Cloud Insights
Powell Josh
Observability
Explore
Alerts
Collectors
16
Log Queries
Enrich
Reporting
Kubernetes
Workload Security
ONTAP Essentials
Admin
Last 24 Hours
Edit

NetApp PCS Sandbox / Observability / Dashboards / ONTAP FAS/AFF - FlexVol Performance (10)

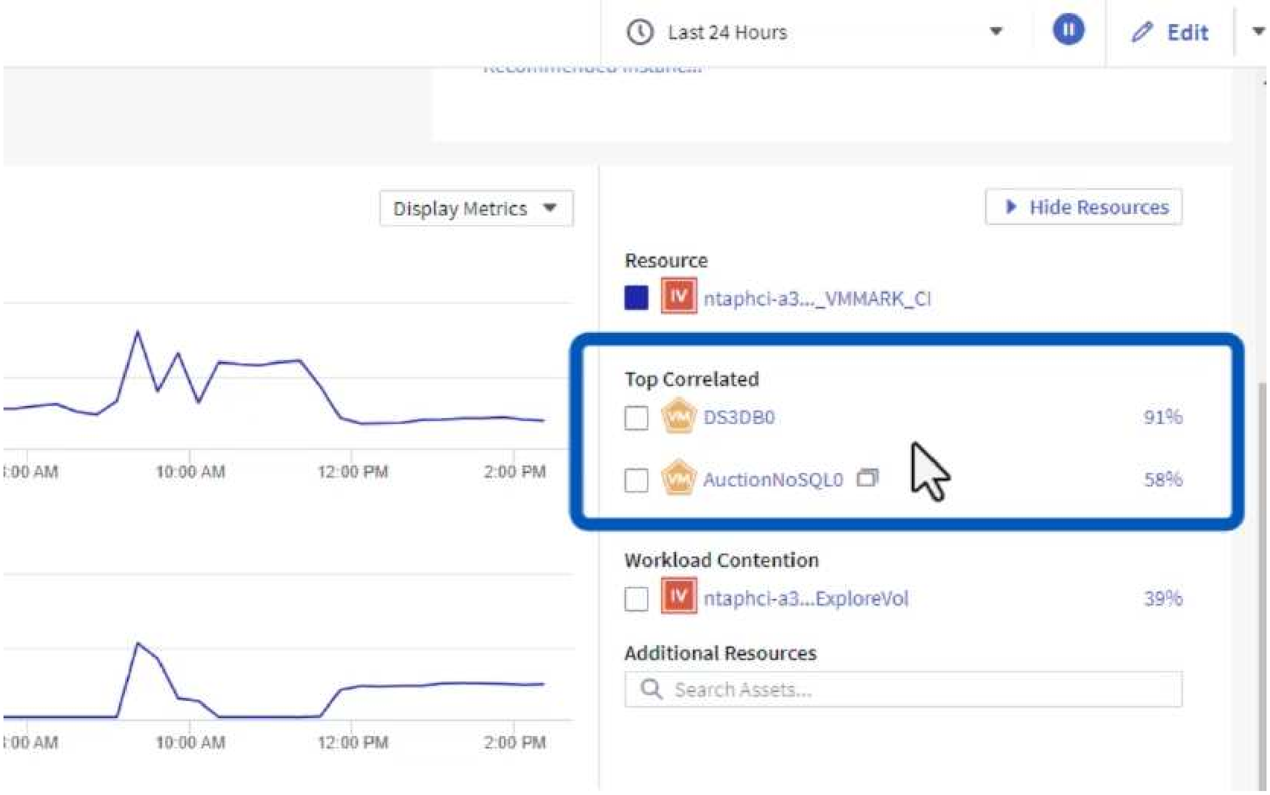
FlexVol: All | Data Center: All | Storage: ntaphci-a300e9u25

Drill Down

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

FlexVol IOPS Max Trend - Top 10
5m
40k
20k
0
4:53 PM
7:40 PM
10:26 PM
1:13 AM (14. Aug)
4:00 AM
6:46 AM
9:33 AM
12:20 PM
ntaphci-a300e9u25:EHC_NFS:RAGHU_DRO_DEST_TEST_01
ntaphci-a300e9u25:ntaphci-a300-01:vol0
ntaphci-a300e9u25:HMC_3510:Select_N1
ntaphci-a300e9u25:ntaphci-a300-02:vol0
ntaphci-a300e9u25:HMC_3510:Select_N2
ntaphci-a300e9u25:EHC_NFS:DRO_Mini
ntaphci-a300e9u25:EHC_NFS:NFSmountTest01
ntaphci-a300e9u25:EHC_NFS:NFS_VMMARK_CI
ntaphci-a300e9u25:E
ntaphci-a300e9u25:H
Avg FlexVol Latency
5m
2
1
0
4:53 PM
7:40 PM
10:26 PM
1:13 AM (14. Aug)
4:00 AM
6:46 AM
9:33 AM
12:20 PM
ntaphci-a300e9u25:HMC_3510:TME_NewVol_1TB
ntaphci-a300e9u25:HMC_3510:VMExploreVol
ntaphci-a300e9u25:HMC_3510:Select_N1
ntaphci-a300e9u25:HMC_3510:Select_N2
ntaphci-a300e9u25:EHC_NFS:DevTest04
ntaphci-a300e9u25:EHC_NFS:NFSmountTest01
ntaphci-a300e9u25:EHC_NFS:DRO_FSxN_nVol01
ntaphci-a300e9u25:EHC_NFS:NFS_VMMARK_CI
ntaphci-a300e9u25:H
ntaphci-a300e9u25:E

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



Resource

IV ntaphci-a3..._VMMARK_CI

Top Correlated

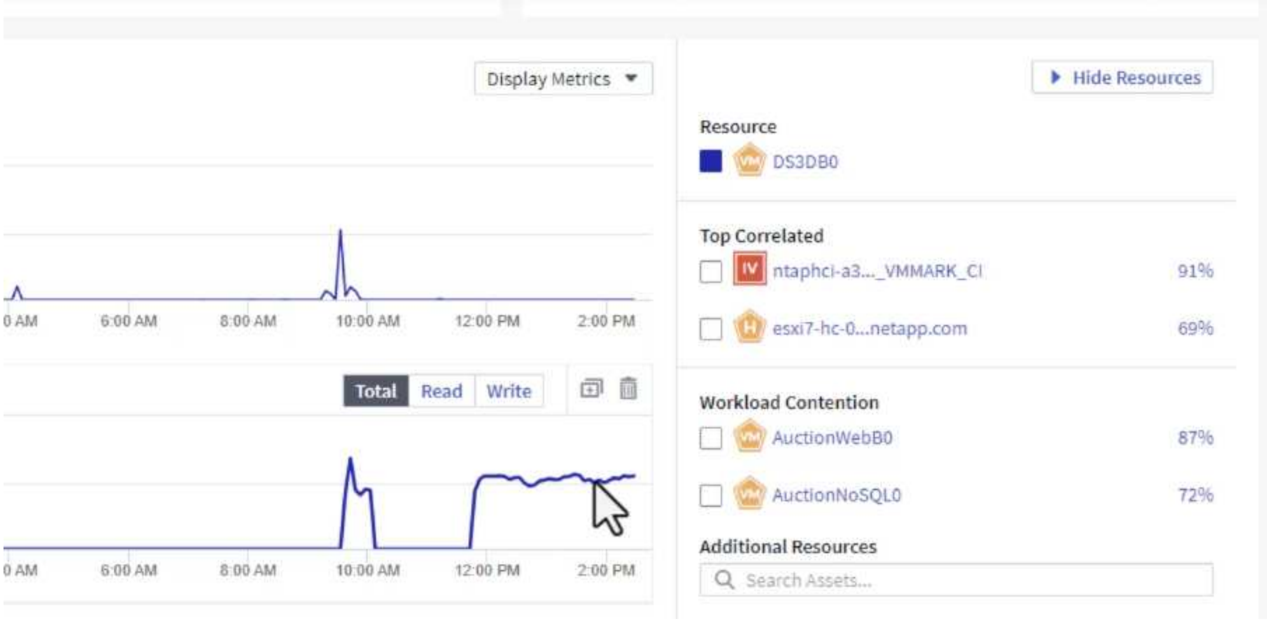
□	VM DS3DB0	91%
□	VM AuctionNoSQL0	58%

Workload Contention

□	IV ntaphci-a3...ExploreVol	39%

Additional Resources

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



Resource

VM DS3DB0

Top Correlated

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

Workload Contention

□	VM AuctionWebB0	87%
□	VM AuctionNoSQL0	72%

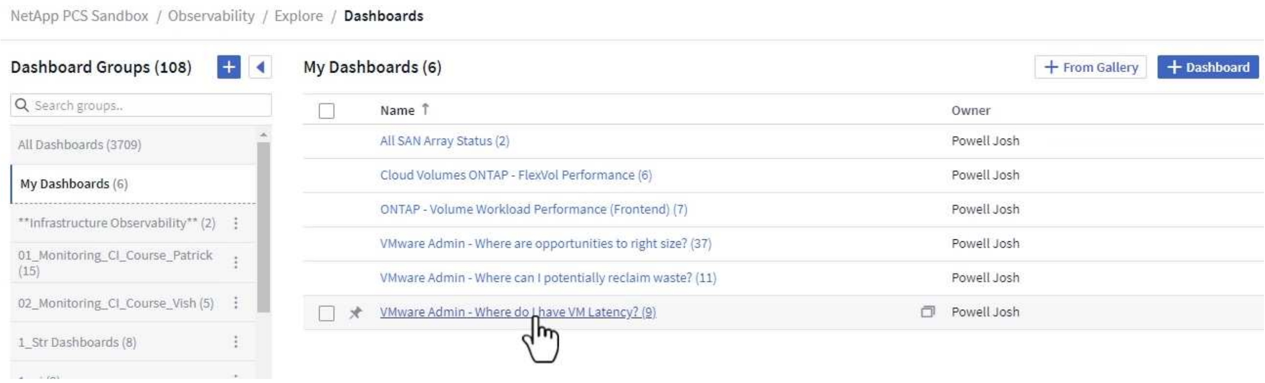
Additional Resources

Use Cloud Insights to identify noisy neighbors

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

Use a Top VM Latency dashboard to isolate noisy neighbors

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



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

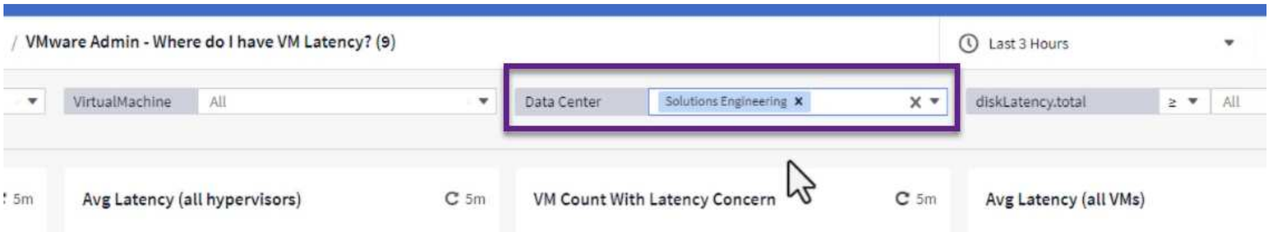
Dashboard Groups (108)

- All Dashboards (3709)
- My Dashboards (6)
- **Infrastructure Observability** (2)
- 01_Monitoring_CI_Course_Patrick (15)
- 02_Monitoring_CI_Course_Vish (5)
- 1_Str Dashboards (8)

My Dashboards (6)

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

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



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

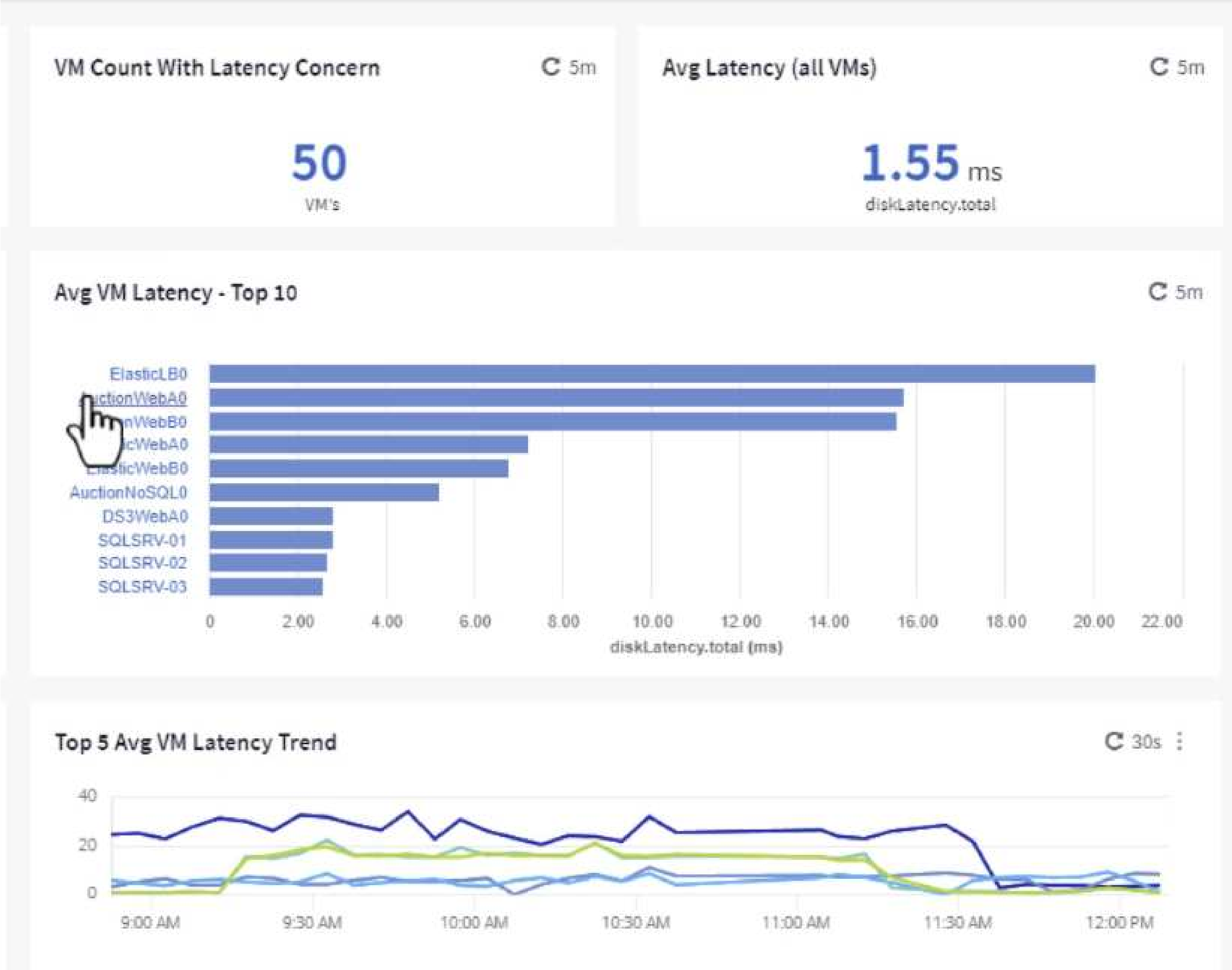
Last 3 Hours

VirtualMachine: All

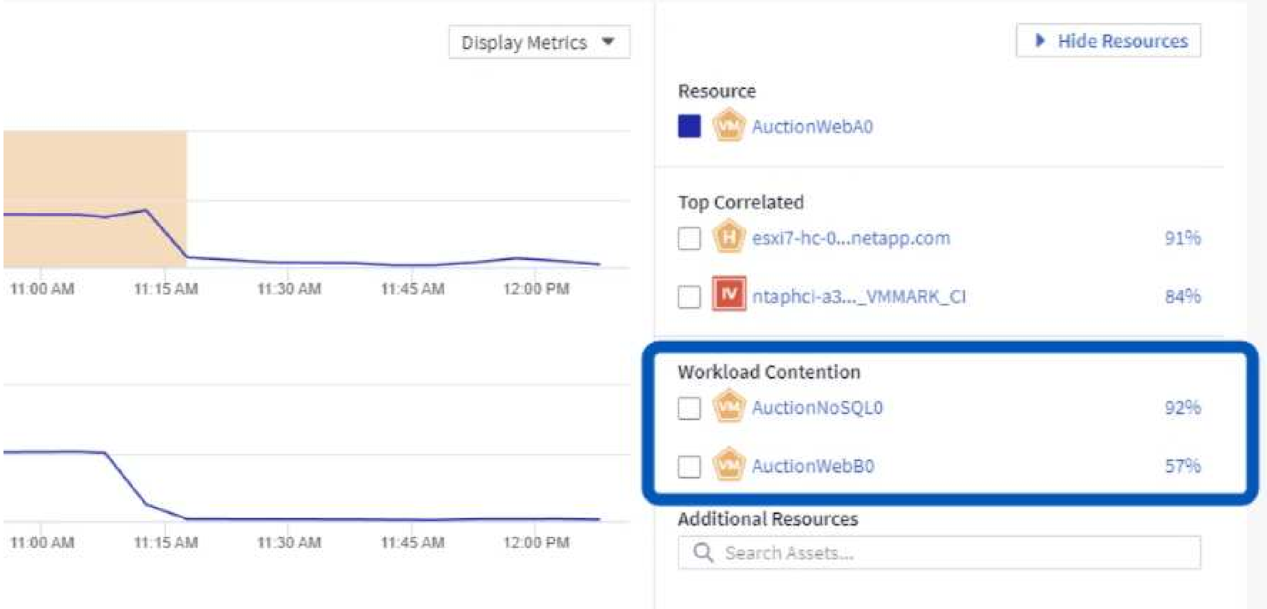
Data Center: Solutions Engineering

diskLatency.total ≥ All

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



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



Resource

■ AuctionWebA0

Top Correlated

□	esxi7-hc-0...netapp.com	91%
□	ntaphci-a3..._VMMARK_CI	84%

Workload Contention

□	AuctionNoSQL0	92%
□	AuctionWebB0	57%

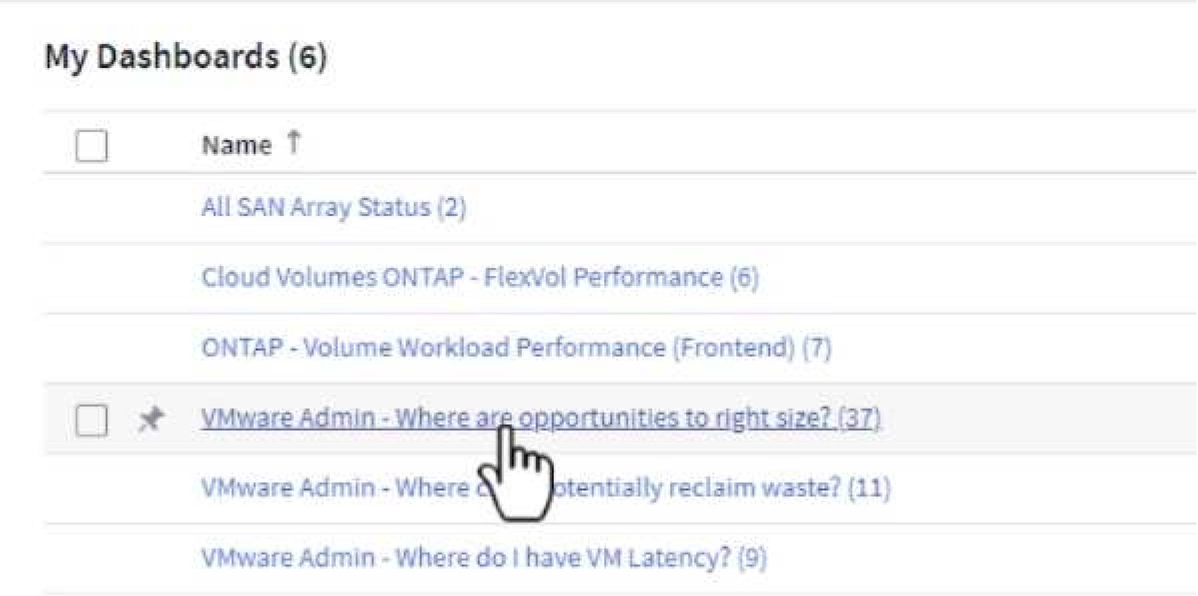
Additional Resources

View over and under utilized resources in Cloud Insights

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

Identify opportunities to right size VMs

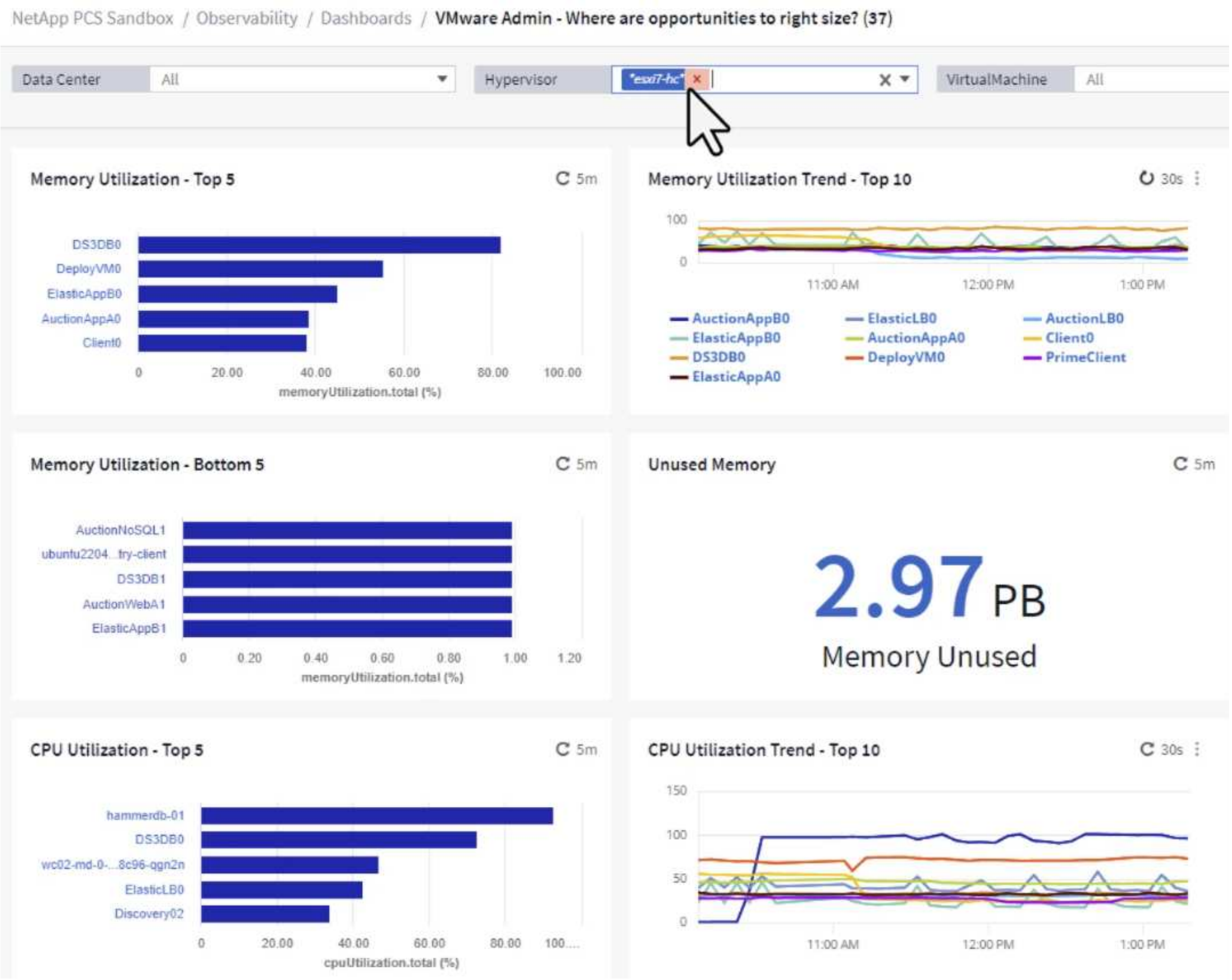
1. In this example access a dashboard available in the **Gallery** called **VMware Admin - Where are opportunities to right size?**



My Dashboards (6)

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

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



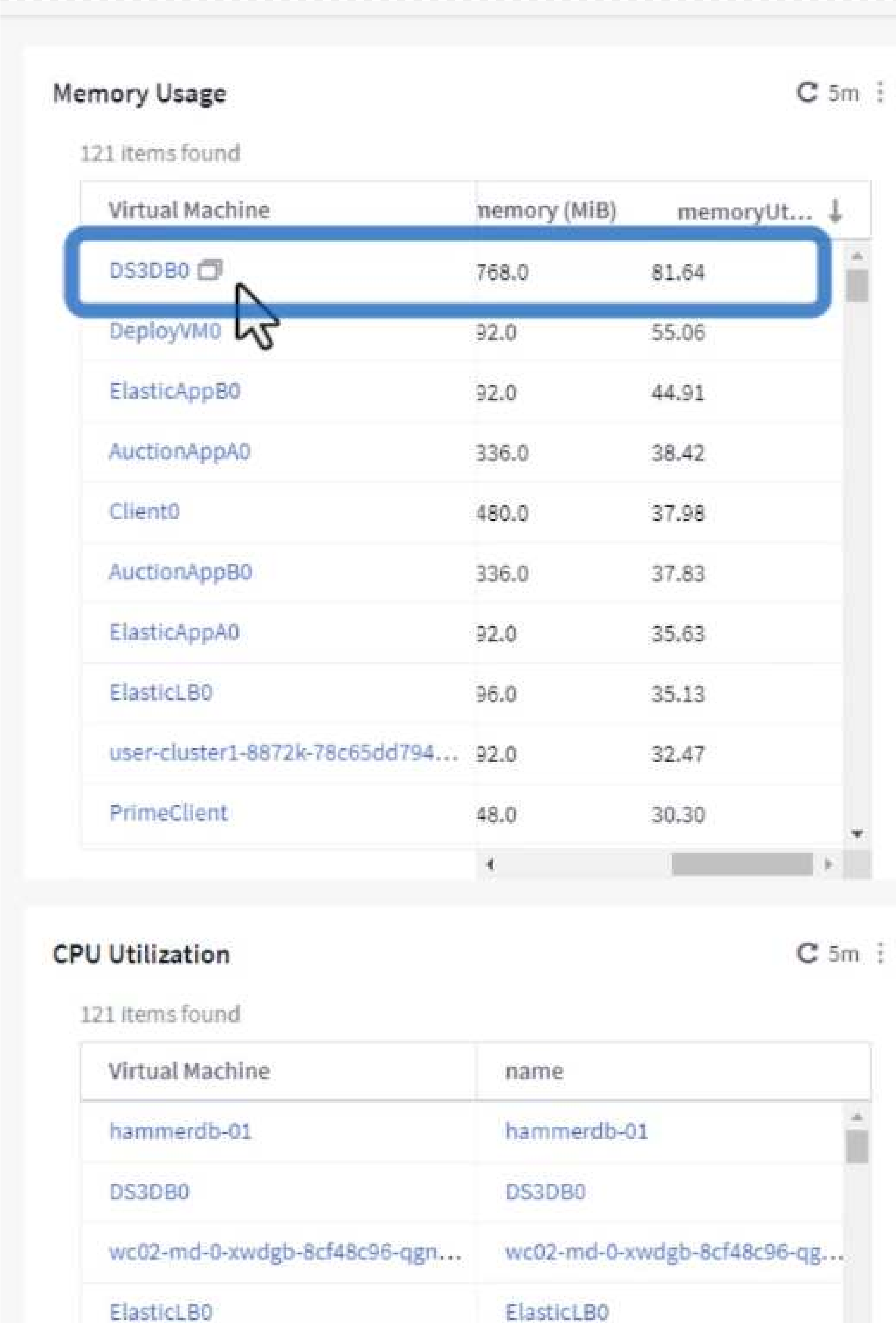
NetApp PCS Sandbox / Observability / Dashboards / VMware Admin - Where are opportunities to right size? (37)

Data Center: All

Hypervisor: *esxi7-hc*

VirtualMachine: All

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



Memory Usage

121 items found

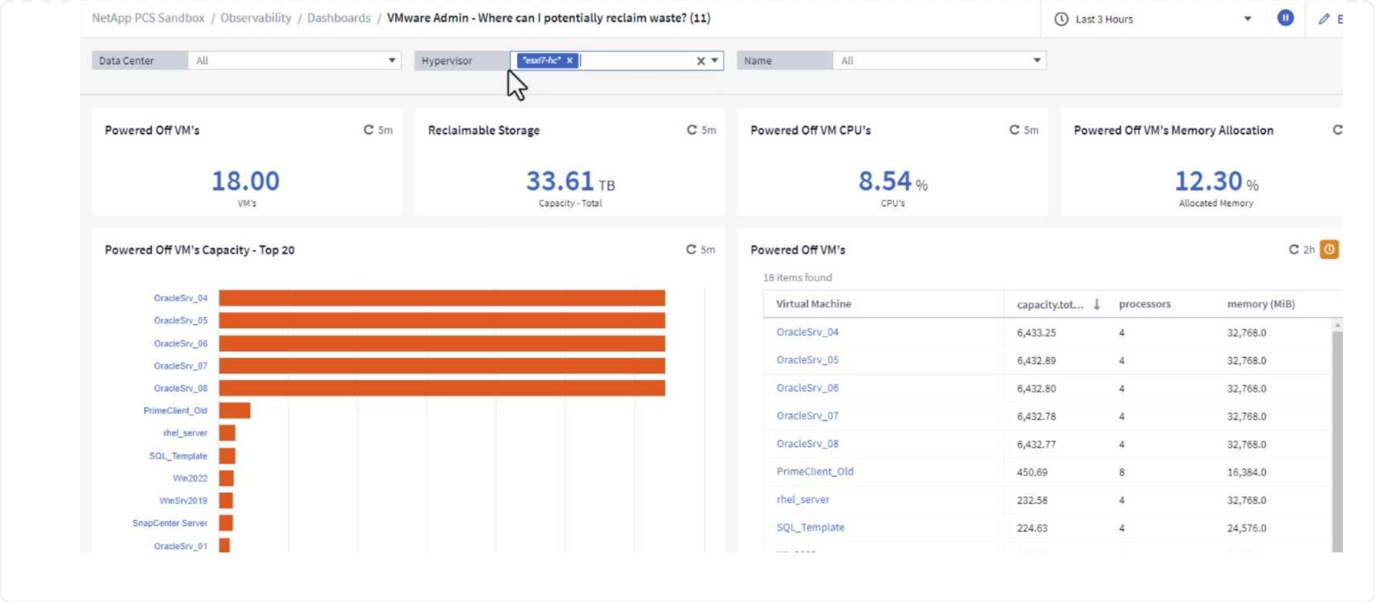
Virtual Machine	nemory (MiB)	memoryUt...
DS3DB0	768.0	81.64
DeployVM0	92.0	55.06
ElasticAppB0	92.0	44.91
AuctionAppA0	336.0	38.42
Client0	480.0	37.98
AuctionAppB0	336.0	37.83
ElasticAppA0	92.0	35.63
ElasticLB0	96.0	35.13
user-cluster1-8872k-78c65dd794...	92.0	32.47
PrimeClient	48.0	30.30

CPU Utilization

121 items found

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

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


NetApp PCS Sandbox / Observability / Dashboards / VMware Admin - Where can I potentially reclaim waste? (11)

Last 3 Hours

Data Center: All

Hypervisor: *esxi7-hc*

Name: All

Powered Off VM's: 18.00 VM's

Reclaimable Storage: 33.61 TB Capacity - Total

Powered Off VM CPU's: 8.54 % CPU's

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

Powered Off VM's

18 items found

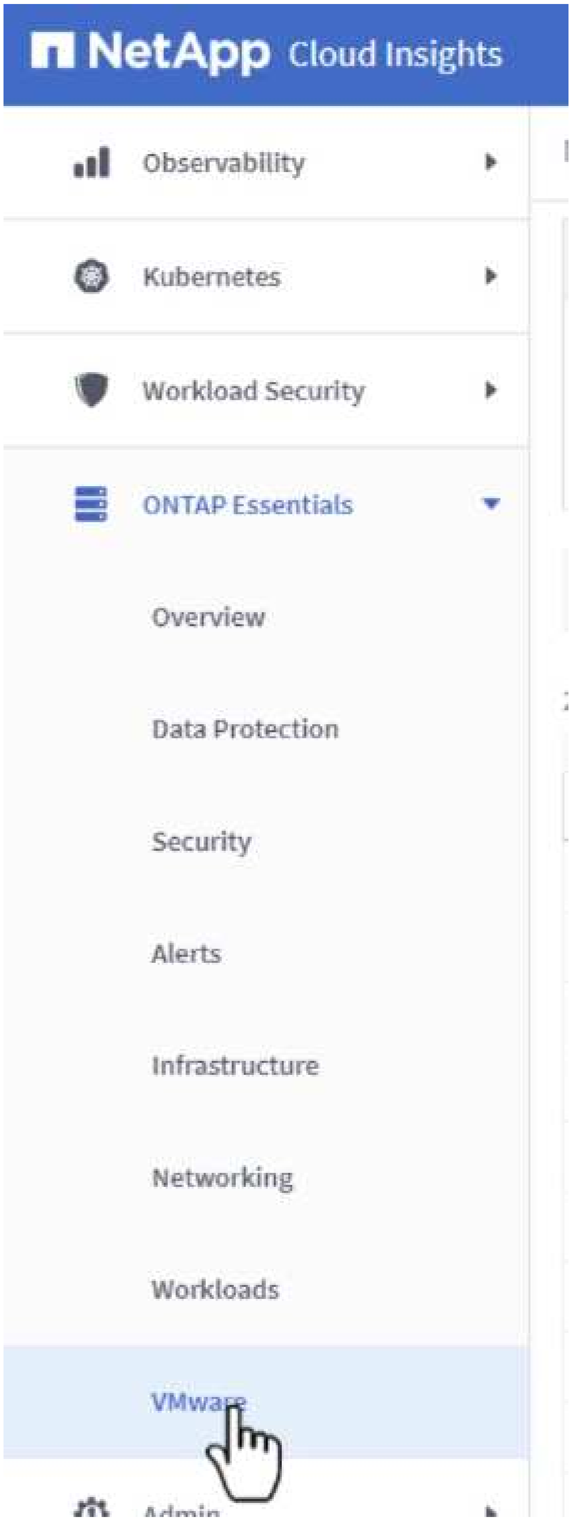
Virtual Machine	capacity.tot... ↓	processors	memory (MiB)
OracleSrv_04	6,433.25	4	32,768.0
OracleSrv_05	6,432.89	4	32,768.0
OracleSrv_06	6,432.80	4	32,768.0
OracleSrv_07	6,432.78	4	32,768.0
OracleSrv_08	6,432.77	4	32,768.0
PrimeClient_Old	450.69	8	16,384.0
rhel_server	232.58	4	32,768.0
SQL_Template	224.63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

Use queries to isolate and sort metrics

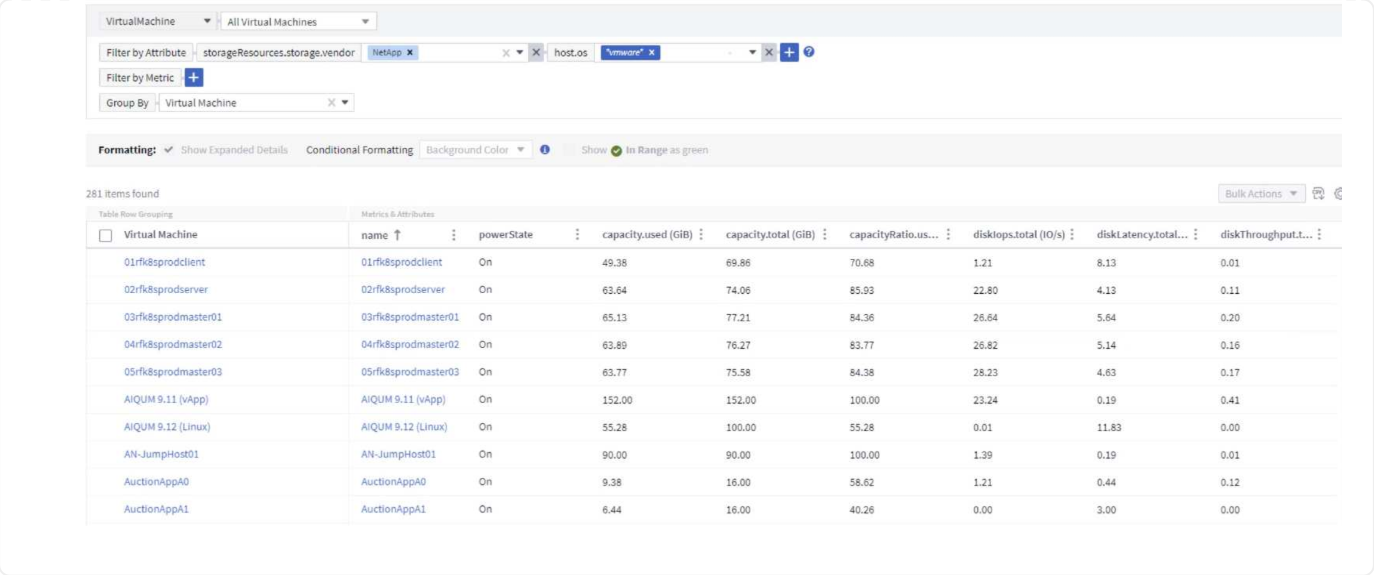
The amount of data captured by Cloud Insights is quite comprehensive. Metric queries provide a powerful way to sort and organize large amounts of data in useful ways.

View a detailed VMware query under ONTAP Essentials

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



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



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

Group By: Virtual Machine

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

281 items found

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

Conclusion

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

Additional Information

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

- NetApp Console landing page
- NetApp Data Infrastructure Insights landing page
- NetApp Data Infrastructure Insights documentation

Copyright information

Trademark information