



VMware Cloud Foundation on NetApp

NetApp virtualization solutions

NetApp
August 25, 2025

This PDF was generated from <https://docs.netapp.com/us-en/netapp-solutions-virtualization/vmware/vmw-vcf-overview.html> on August 25, 2025. Always check docs.netapp.com for the latest.

Table of Contents

VMware Cloud Foundation on NetApp	1
Simplify hybrid cloud experience with VMware Cloud Foundation and ONTAP	1
Introduction	1
Introduction to NetApp ONTAP	1
Introduction to VMware Cloud Foundation	1
VCF Domains	1
Storage with VCF	2
Why ONTAP for VCF	3
Additional information:	4
Summary	5
Documentation resources	5
Design options with VMware Cloud Foundation and ONTAP	6
Storage options	6
Blueprints	6
Set up private cloud environments with VMware Cloud Foundation and ONTAP	11
Deploy a new VCF 9 instance	11
Converge existing components into VCF 9	13
Upgrade an existing VCF environment to VCF 9	14
Implementing Disaster Recovery with NetApp SnapMirror and BlueXP DRaaS	14
Getting started	15
BlueXP disaster recovery configuration	17
Configuring Storage replication between source site array and destination site array	17
How to set it up for VMware Disaster Recovery	18
What can BlueXP disaster recovery do for you?	18
Test failover	23
Cleanup failover test Operation	25
Planned Migration and Fail over	25
Failback	27
Monitoring and Dashboard	28
Convert existing vSphere clusters to VCF	29
Learn about converting a vSphere environment with existing datastores to VCF	30
Convert vCenter server instance to VCF management domain (NFS datastore)	30
Convert vCenter server instance to VCF management domain (FC datastore)	44
Provision VCF with principal storage	58
Provision a VCF environment with ONTAP as the principal storage solution	58
Use an FC-based VMFS datastore on ONTAP as principal storage for VCF management domain	58
Use an NFS datastore on ONTAP as principal storage for VCF management domain	59
Use an FC-based VMFS datastore on ONTAP as principal storage for a VI workload domain	60
Use an NFS datastore on ONTAP as principal storage for a VI workload domain	62
Expand VCF with supplemental storage	83
Learn about expanding storage for a VCF environment using supplemental storage	83
Add an iSCSI datastore as supplemental storage for a management domain using ONTAP tools for VMware vSphere	83

Add an FC-based VMFS datastore as supplemental storage for a management domain using ONTAP tools for VMware vSphere	107
Add vVols as supplemental storage to VI workload domains using ONTAP tools for VMware vSphere ..	108
Add NFS and vVols as supplemental storage to VI workload domains using ONTAP tools for VMware vSphere	135
Add NVMe over TCP as supplemental storage to VI workload domains	159
Add an FC-based VMFS datastore as supplemental storage to VI workload domains	183
Protect VCF with SnapCenter	184
Learn about protecting VCF workload domains with SnapCenter plug-in for VMware vSphere	184
Protect a VCF workload domain with SnapCenter plug-in for VMware vSphere	184
Protect a VCF management and workload domains using SnapCenter plug-in for VMware vSphere ..	220
Protect VCF workload domains with NVMe over TCP storage and SnapCenter plug-in for VMware vSphere	233
Protect VMware datastores with BlueXP	240
Learn about protecting VMware datastores using BlueXP disaster recovery	240
Configure 3-2-1 data protection for VMware with SnapCenter plug-in for VMware vSphere and BlueXP backup and recovery	240
Set up disaster recovery for VMFS datastores using BlueXP disaster recovery	282
Set up disaster recovery for NFS datastores using BlueXP disaster recovery	301
Protect workloads with vSphere Metro Storage Cluster	322
Learn about integrating ONTAP high availability with VMware vSphere Metro Storage Cluster (vMSC)	322
Configure a stretch cluster for a VCF management domain using MetroCluster	323
Configure a stretch cluster for a VI workload domain using MetroCluster	334
Configure a stretch cluster for a VCF management domain using SnapMirror Active Sync	345
Configure a stretch cluster for a VI workload domain using SnapMirror Active Sync	347
Migrate VMs from VMware vSphere to ONTAP datastores	349
Network Requirements	349
VM Migration Scenarios	351
VM Template Migration Scenarios	374
Use Cases	381
Additional Resources	382
Autonomous Ransomware Protection for NFS Storage	382
Monitor on-premises storage with Data Infrastructure Insights	392
Monitoring On-Premises Storage with Data Infrastructure Insights	392
Solution Deployment Overview	392
Prerequisites	393
Solution Deployment	393
Conclusion	410
Additional Information	410

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

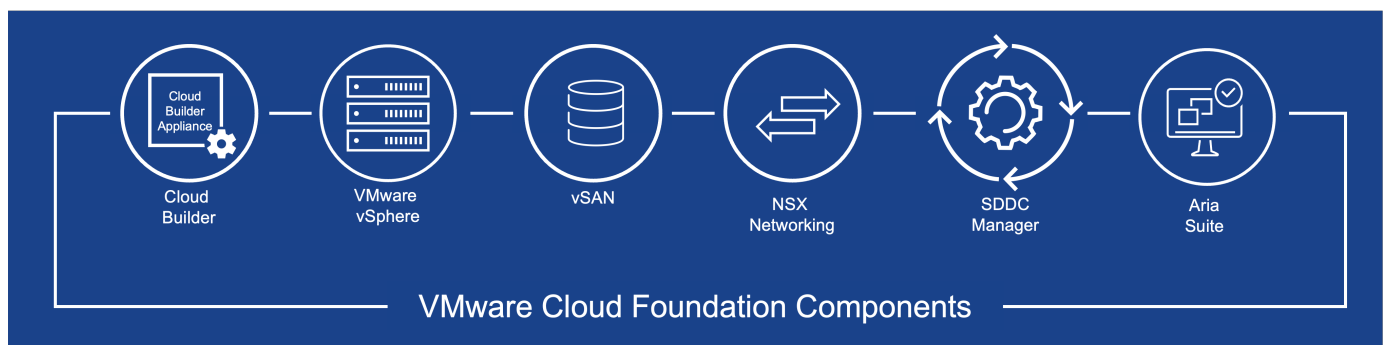
Using NetApp with VCF enhances data management and storage efficiency through NetApp's advanced features like deduplication, compression, and snapshots. This combination provides seamless integration, high performance, and scalability for virtualized environments. Additionally, it simplifies hybrid cloud 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.

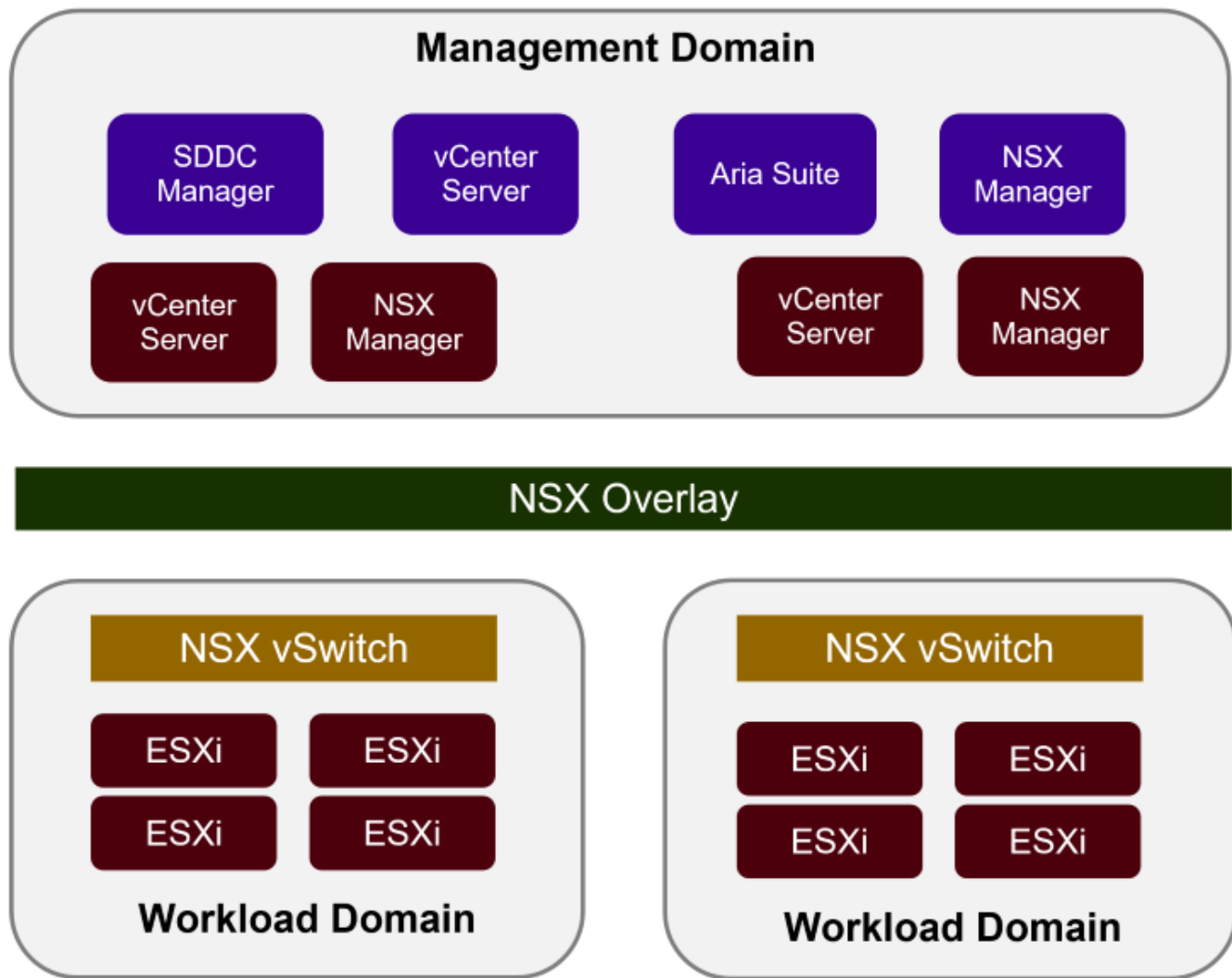
Introduction to VMware Cloud Foundation

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, Tanzu Kubernetes Grid, 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.

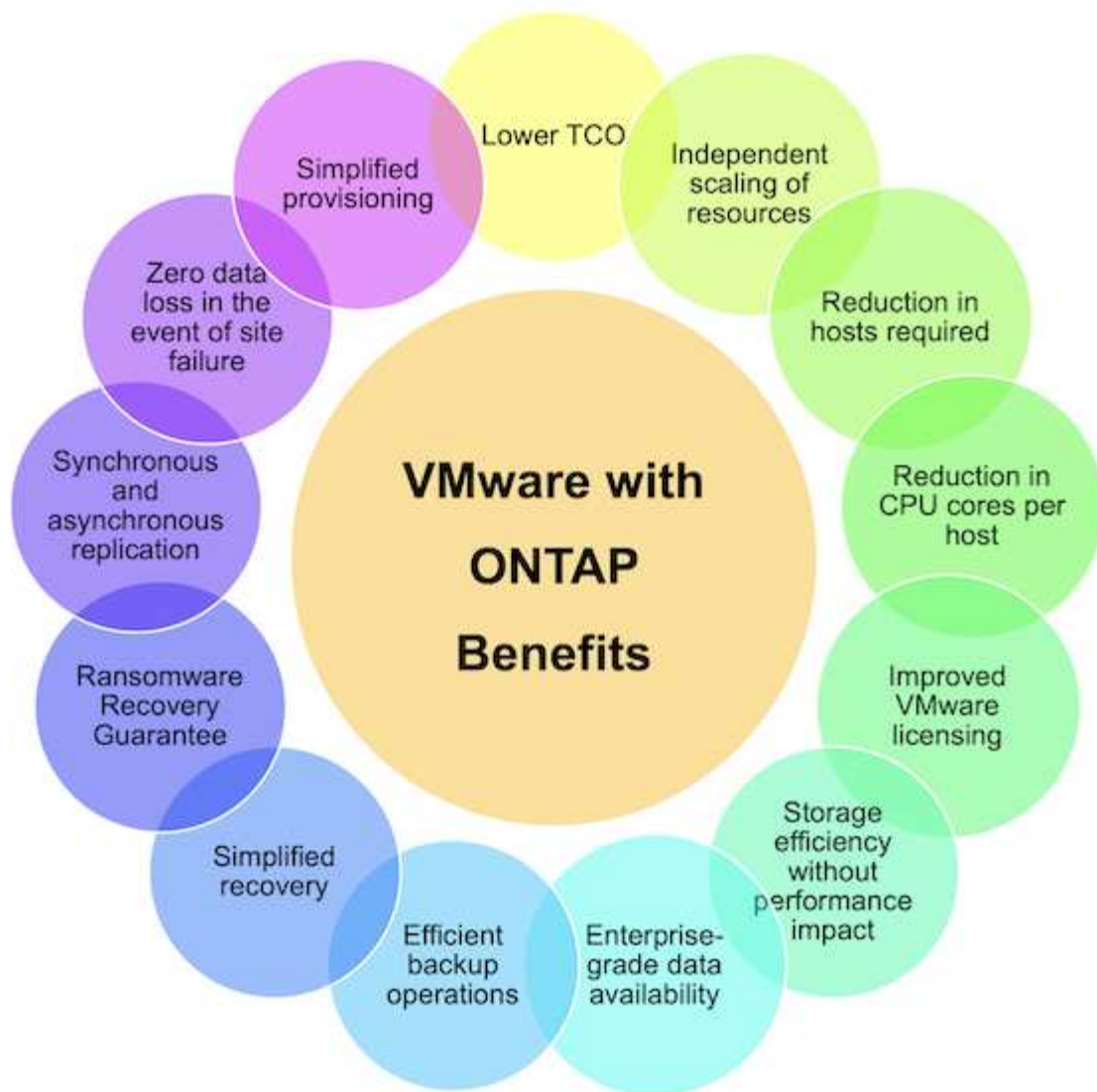
Support VCF Storage types

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.



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](#)
- [BlueXP Disaster Recovery](#)
- [Data Infrastructure 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

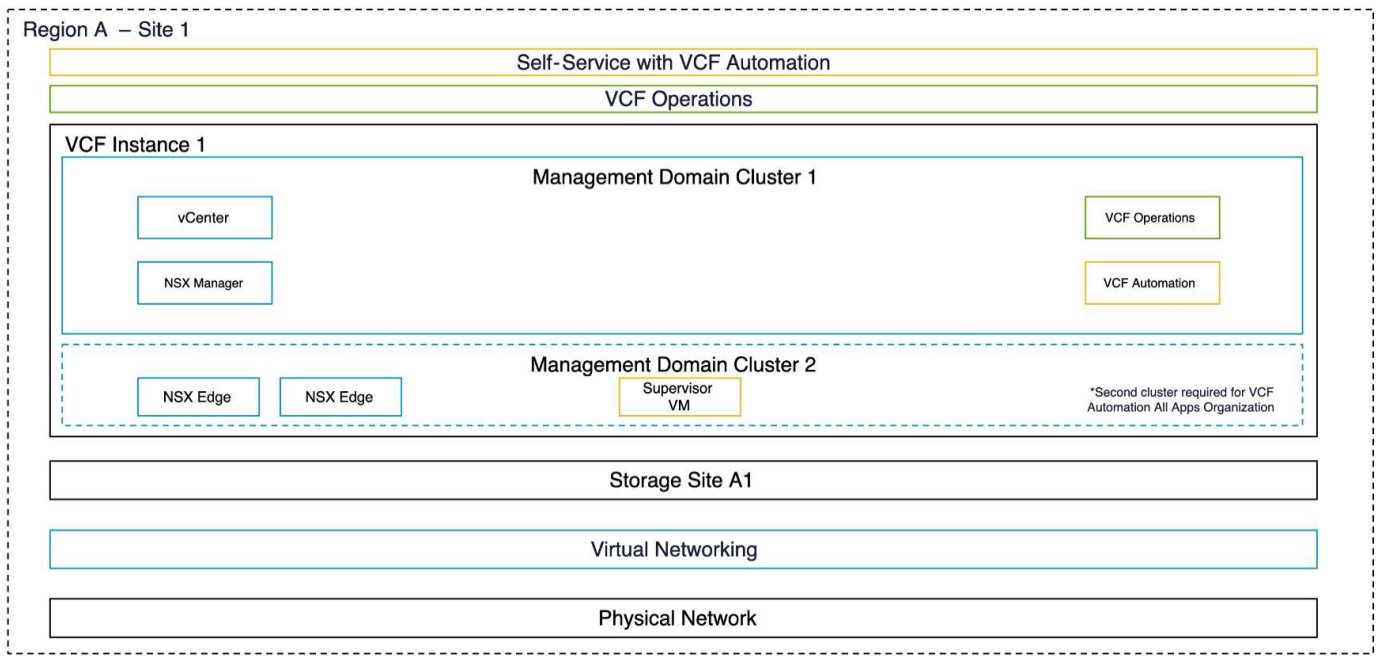
Product Family	VMFS on FC	VMFS on iSCSI	VMFS on NVMe-oF	NFSv3	NFSv4.1
ASA A-Series and C-Series	Yes	Yes	Yes	No	No
AFF A-Series and C-Series	Yes	Yes	Yes	Yes	Yes
FAS	Yes	Yes	Yes	Yes	Yes

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](#).

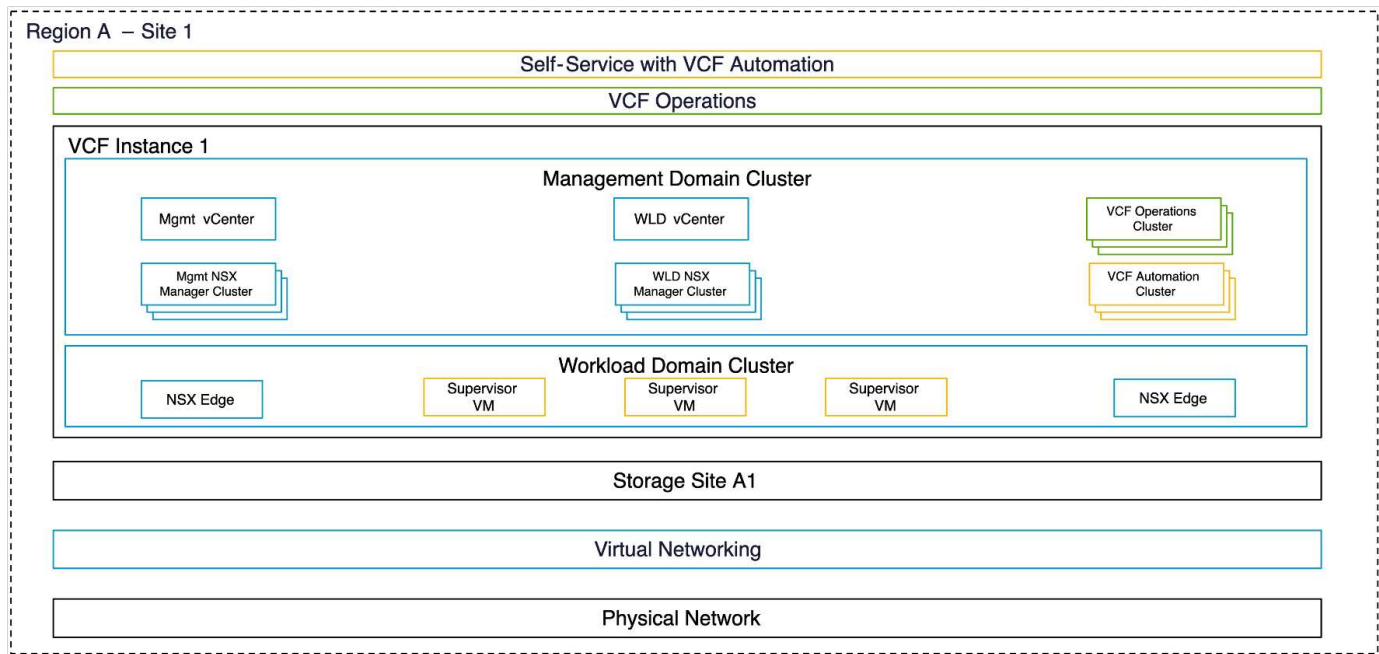
VCF fleet in a single site

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](#).

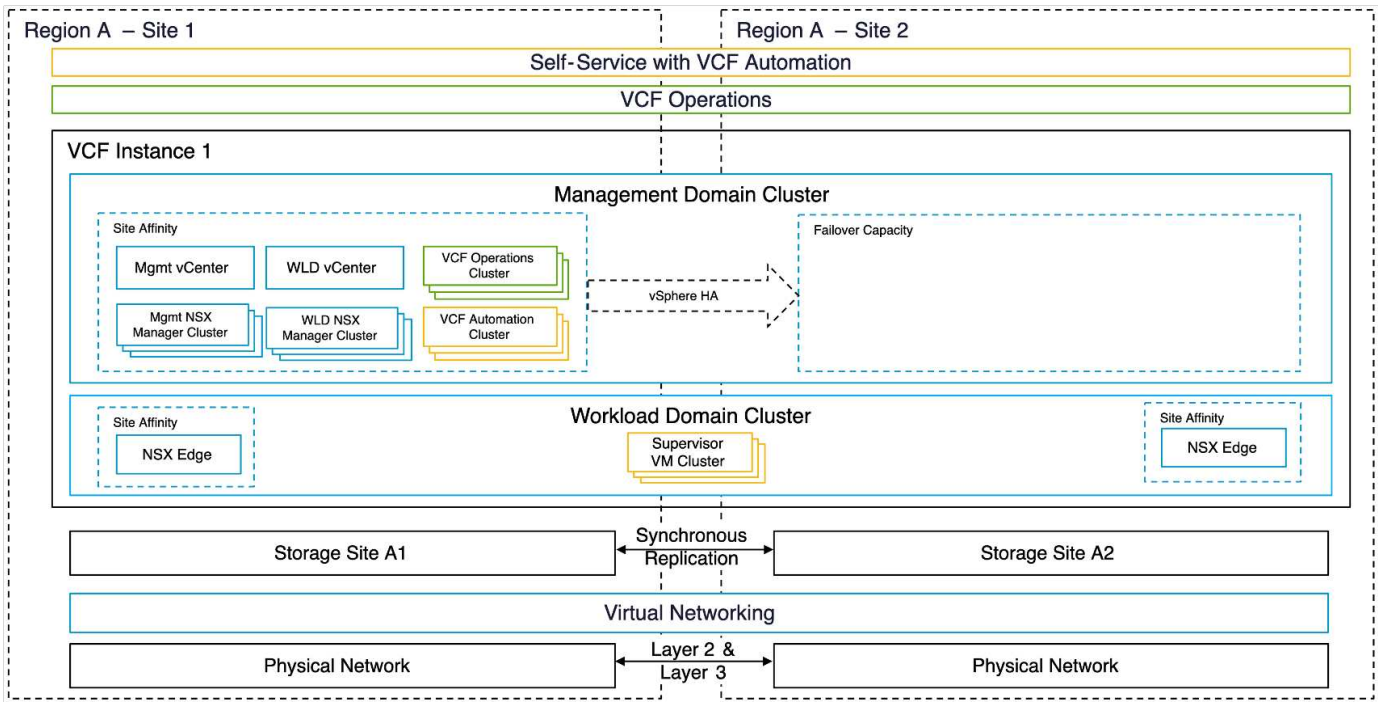
VCF fleet with multiple sites in a single region

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 BlueXP.

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 BlueXP Backup and Recovery for VMs via SnapMirror and SnapMirror to Cloud. You can perform restores from any of the three locations.

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

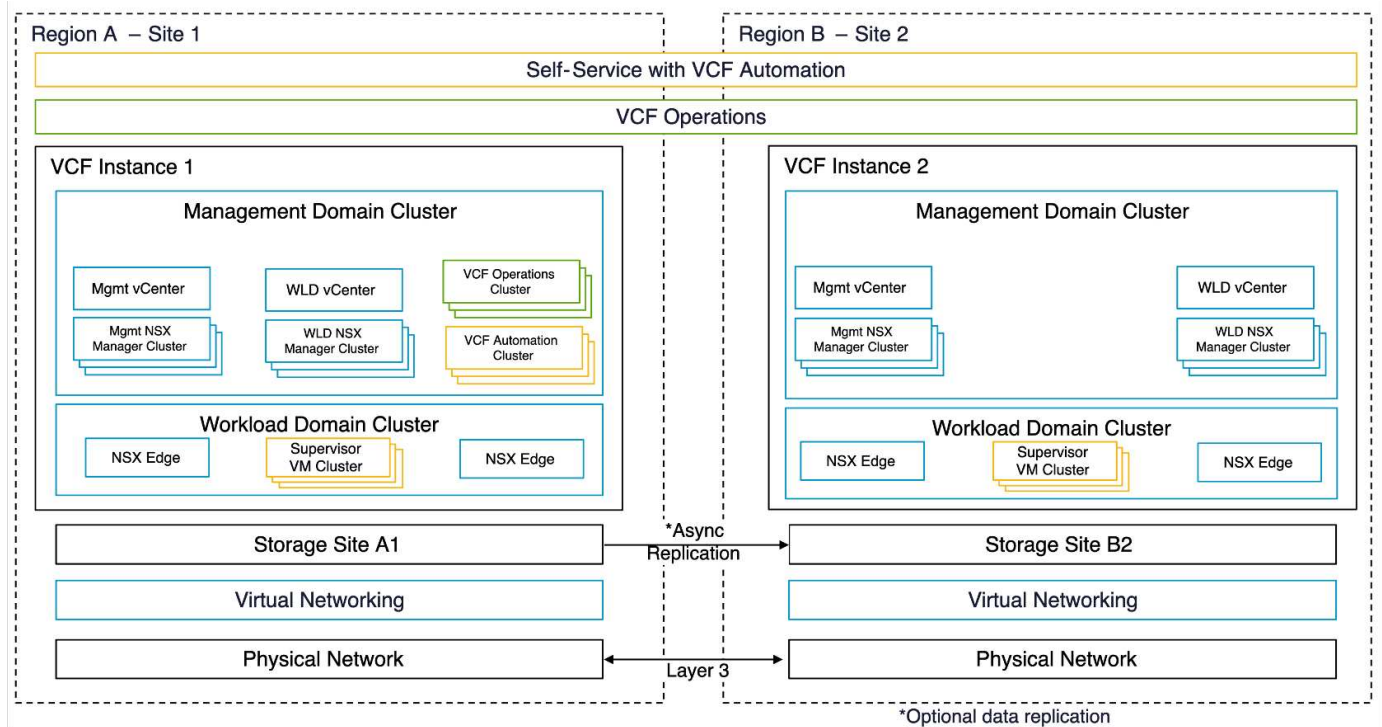
For more info, check the [Broadcom Technical Documentation on VCF Fleet with Multiple Sites in a Single Region](#).

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 BlueXP Disaster Recovery as a Service. 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



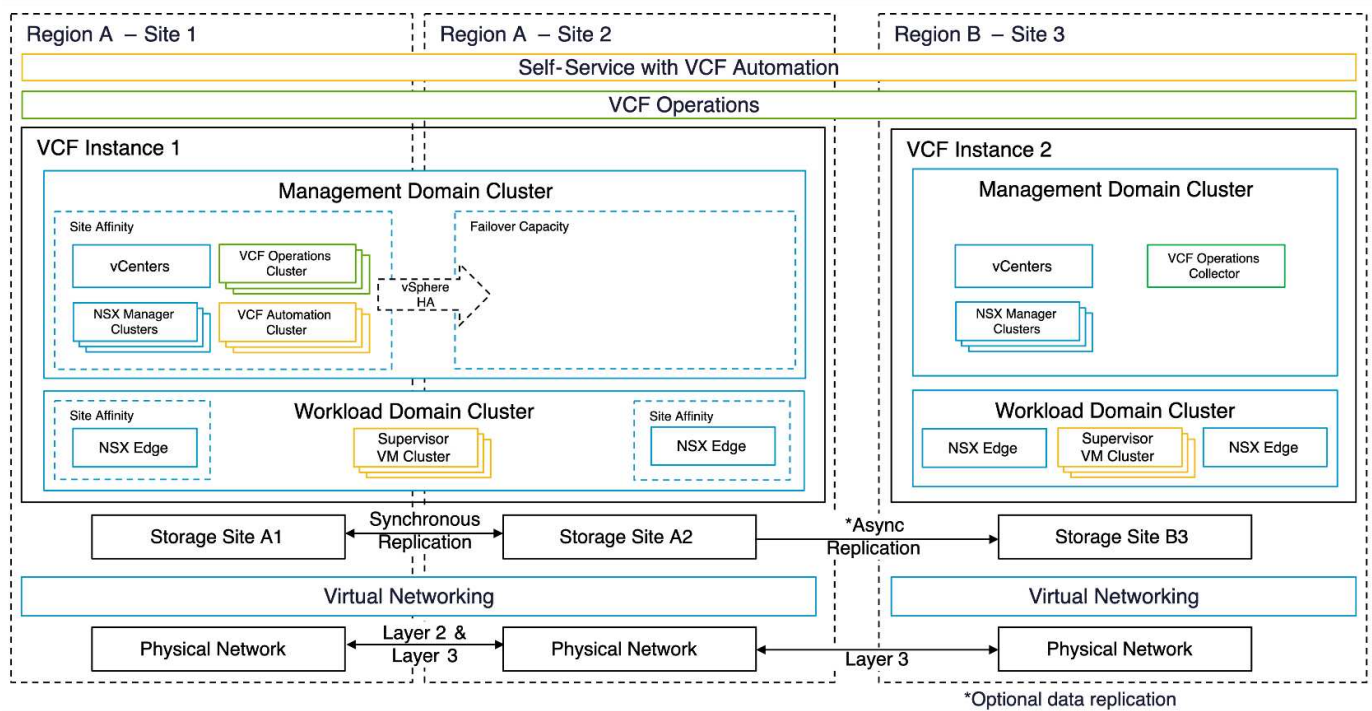
ONTAP tools provide a UI for datastore replication setup. BlueXP can also be used for replication between storage arrays. SnapCenter Plug-in for VMware vSphere utilizes existing SnapMirror relationships for SnapShots.

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 BlueXP 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 BlueXP Connector
 - [Review what you can do without a Connector.](#)
 - [Deploy the Connector.](#)
 - d. Use BlueXP for 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 BlueXP for 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 SnapMirror and BlueXP DRaaS

VCF disaster recovery solution for NFS datastore with NetApp SnapMirror and BlueXP DRaaS

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.

This section outlines the configuration of BlueXP Disaster Recovery as a Service (DRaaS) to establish DR for on-premises VMware virtual machines.

The setup includes:

- Creating a BlueXP account and deploying a BlueXP Connector.
- Adding ONTAP arrays to the BlueXP canvas 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.

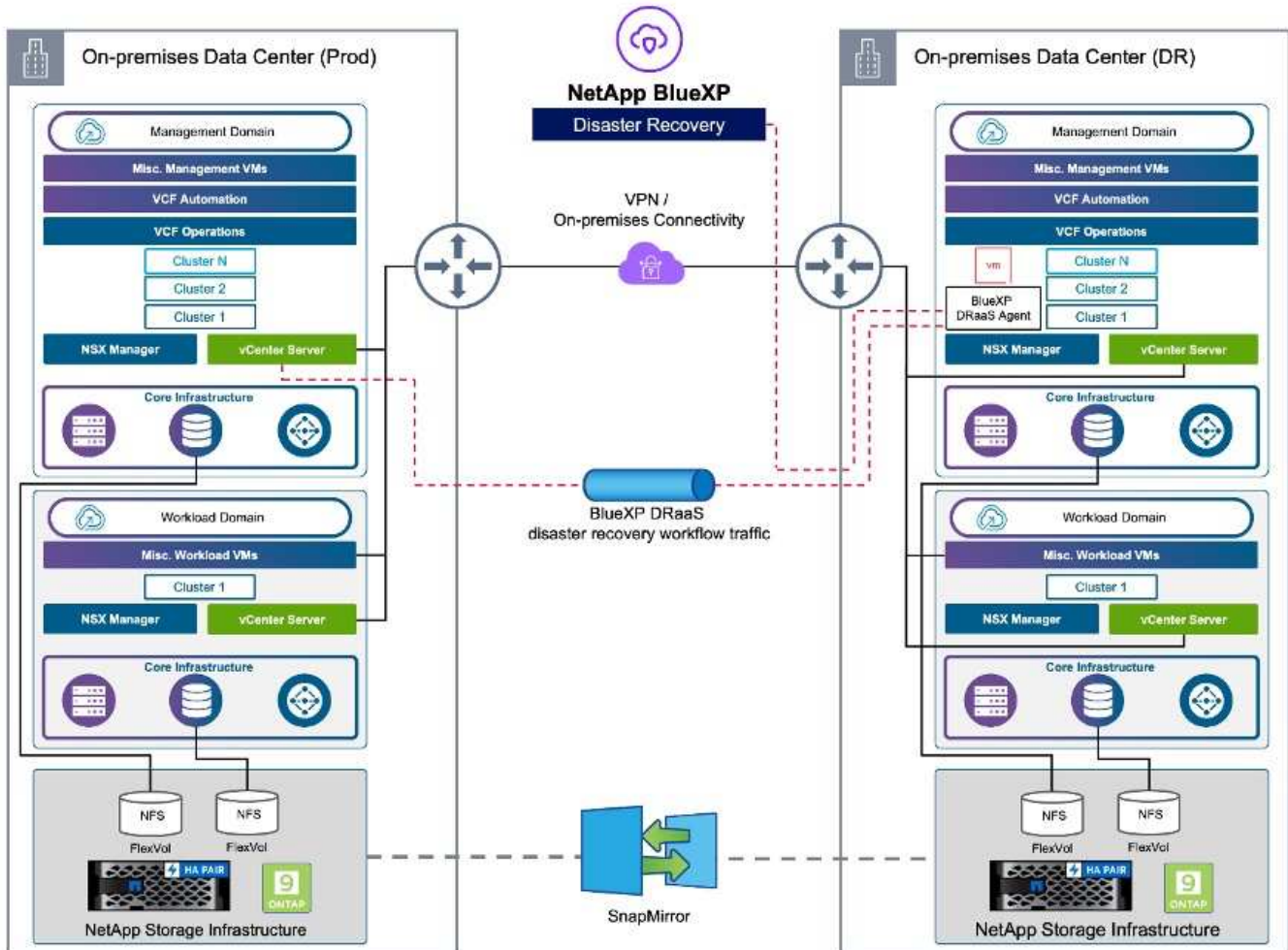
The BlueXP disaster recovery service, integrated within the NetApp BlueXP console, enables organizations to seamlessly discover their on-premises VMware vCenters and ONTAP storage systems. Once discovered, administrators can define resource groupings, create disaster recovery plans, associate them with the appropriate resources, and initiate or test failover and fallback 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.

BlueXP DRaaS 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, BlueXP 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.

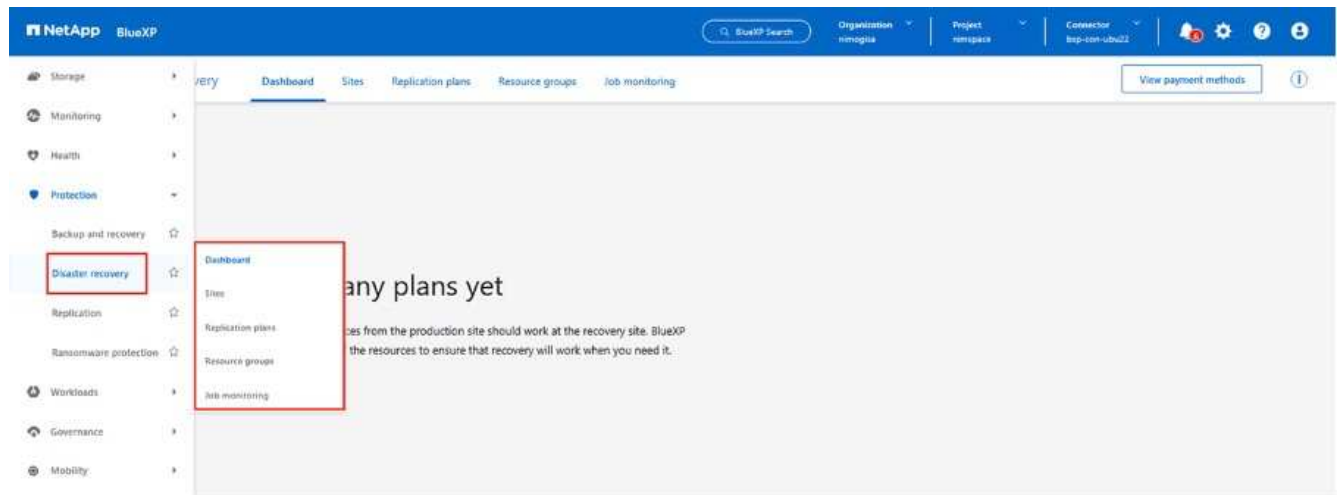
All these capabilities are delivered at a significantly lower cost compared to traditional disaster recovery solutions.



Getting started

To get started with BlueXP disaster recovery, use BlueXP console and then access the service.

1. Log in to BlueXP.
2. From the BlueXP left navigation, select Protection > Disaster recovery.
3. The BlueXP disaster recovery Dashboard appears.



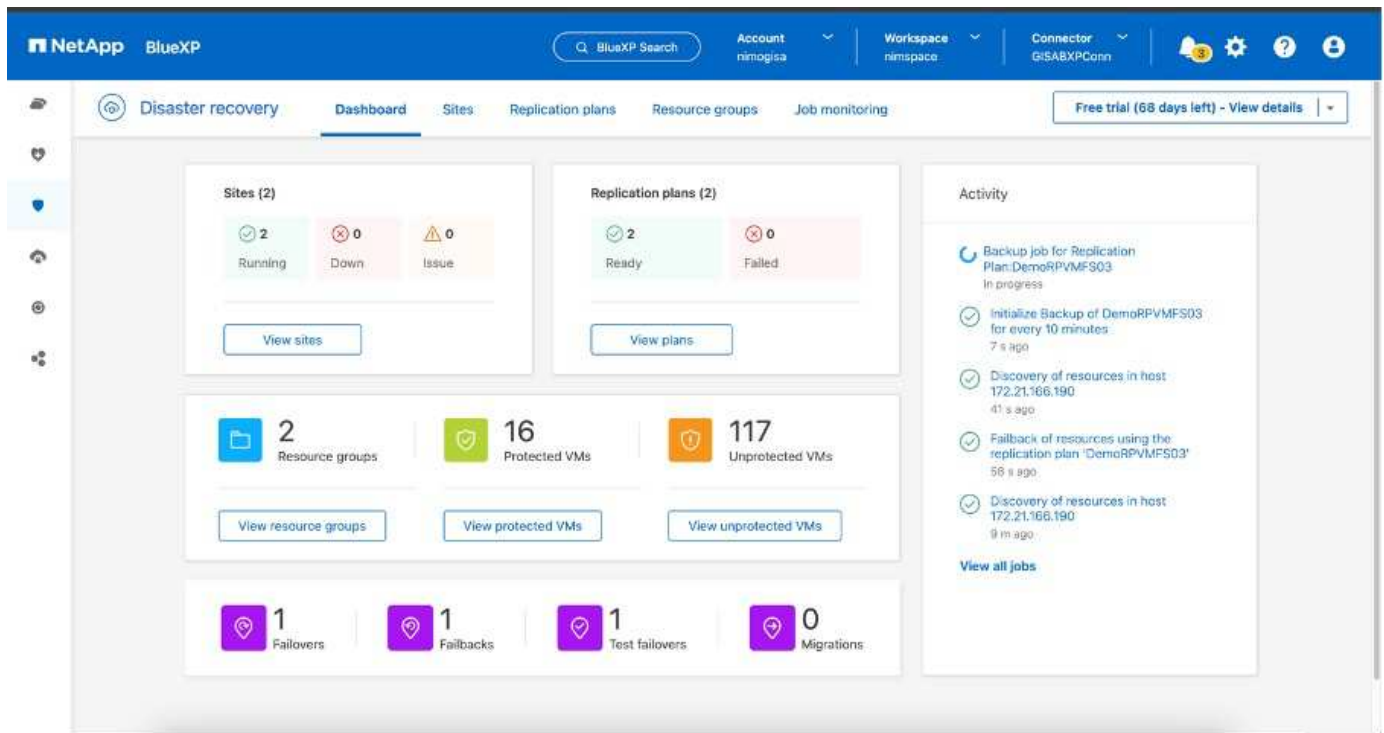
Before configuring disaster recovery plan, ensure the following [pre-requisites](#) are met:

- BlueXP Connector is set up in NetApp BlueXP.
- BlueXP connector 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 BlueXP.
- 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 BlueXP connector in the destination site or in a third site, so that the BlueXP connector 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.



BlueXP disaster recovery configuration

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

Open BlueXP console and select Protection > Disaster Recovery from left navigation. Select Discover vCenter servers or use top menu, Select Sites > Add > Add vCenter.

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. BlueXP DRaaS 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 BlueXP DRaaS 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, BlueXP DRaaS picks up the relationship and continues with the rest of the workflow operations.

How to set it up for VMware Disaster Recovery

The 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 BlueXP DRaaS which will automate the same provided the following two criteria's are met:

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

NetApp BlueXP

BlueXP Search Organization nmogisa Project namespace Connector tap-con-ubu22

Add replication plan vCenter servers Applications Resource mapping Review

Datastores

☐ Use platform managed backups and retention schedules

Start taking backups and running retention from 2025-08-14 12:00 AM

Take backups and run retention once every 03 Hour(s) 00 Minute(s)

Retention count for all datastores 30

Source datastore DRaaS_SrcB (DR_Src_NewDRaaS_SrcB)

Target datastore

Working environment NTAP-328-N2 SVM SVM_DR_Dstn Destination volume name DRaaS_SrcB_dest

Preferred NFS LIF Select preferred NFS LIF Export policy Select export policy

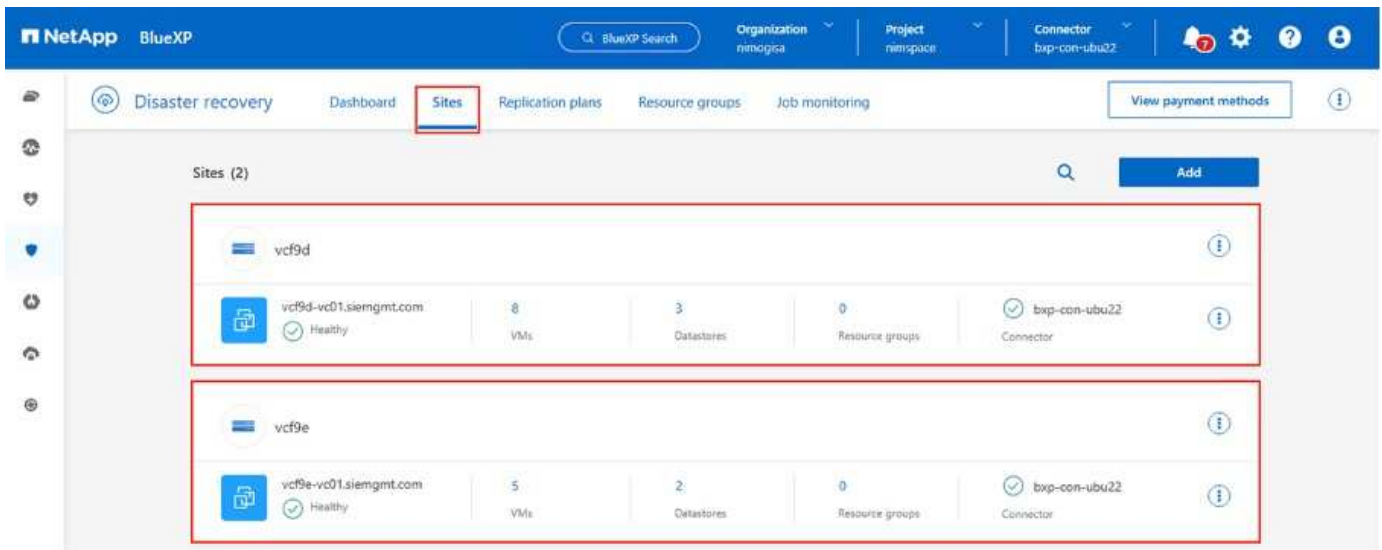
Previous Next

Activate Windows Go to Settings to activate Windows.

BlueXP 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 BlueXP disaster recovery do for you?

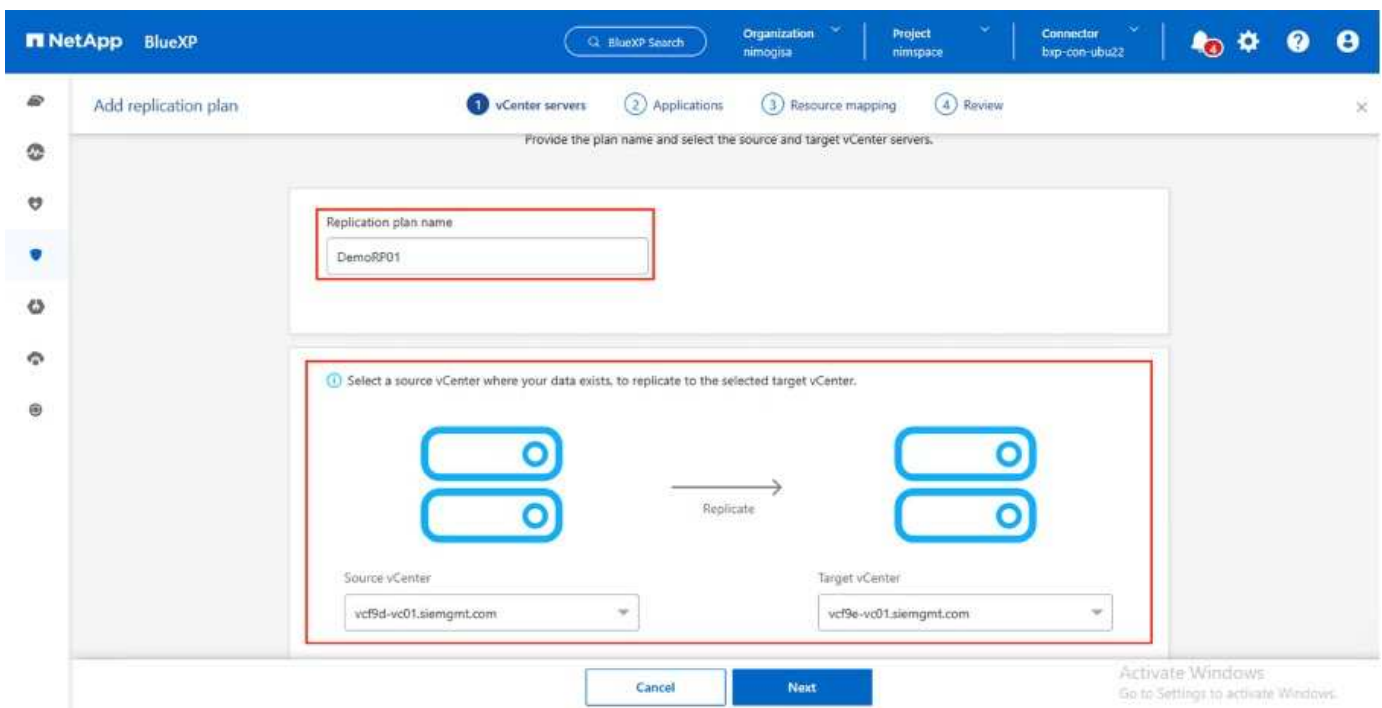
After the source and destination sites are added, BlueXP disaster recovery performs automatic deep discovery and displays the VMs along with associated metadata. BlueXP disaster recovery also automatically detects the networks and port groups used by the VMs and populates them.



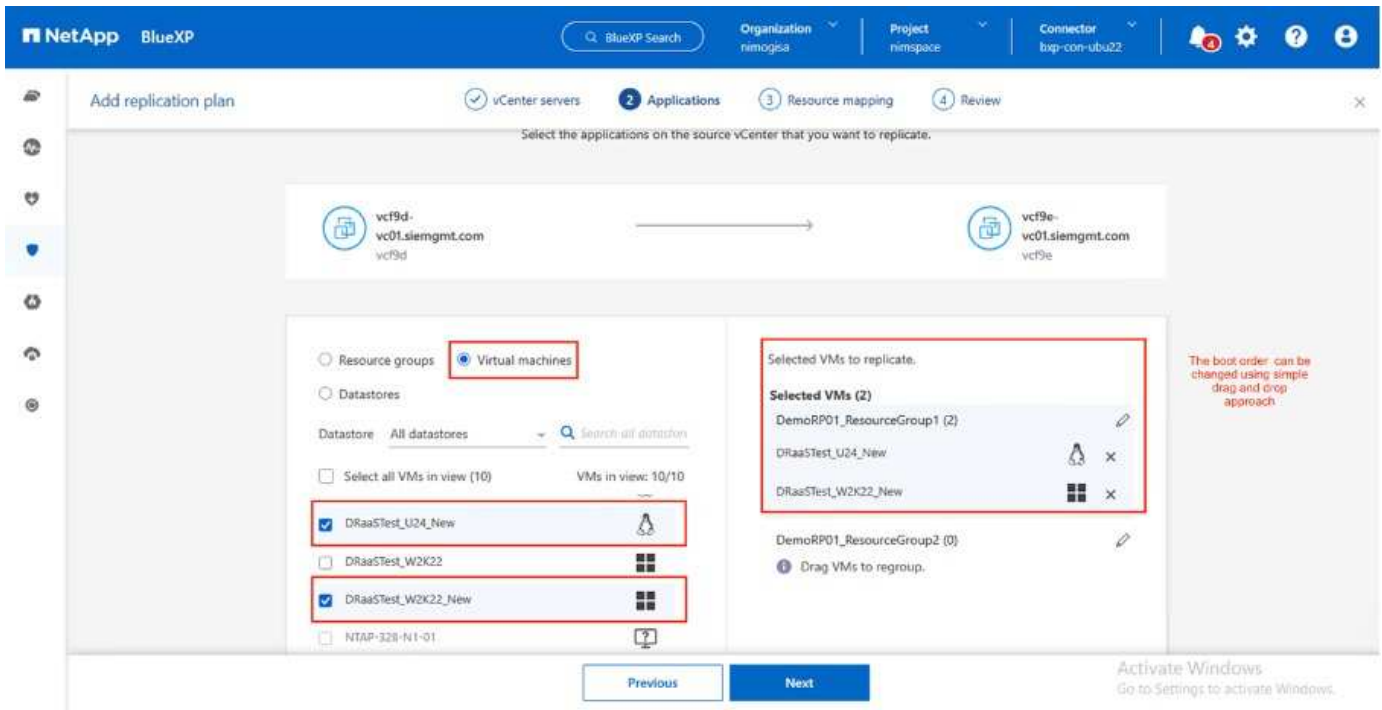
After the sites have been added, configure the replication plan by selecting the source and destination vCenter platforms from the drop down and pick the resource groups to be included in the plan, along with the grouping of how applications should be restored and powered on and mapping of clusters and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

In this step, the VMs can be grouped into resource groups. BlueXP 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. The resource group can also be created using Resource group tab.

First, select the source vCenter and then select the destination vCenter.



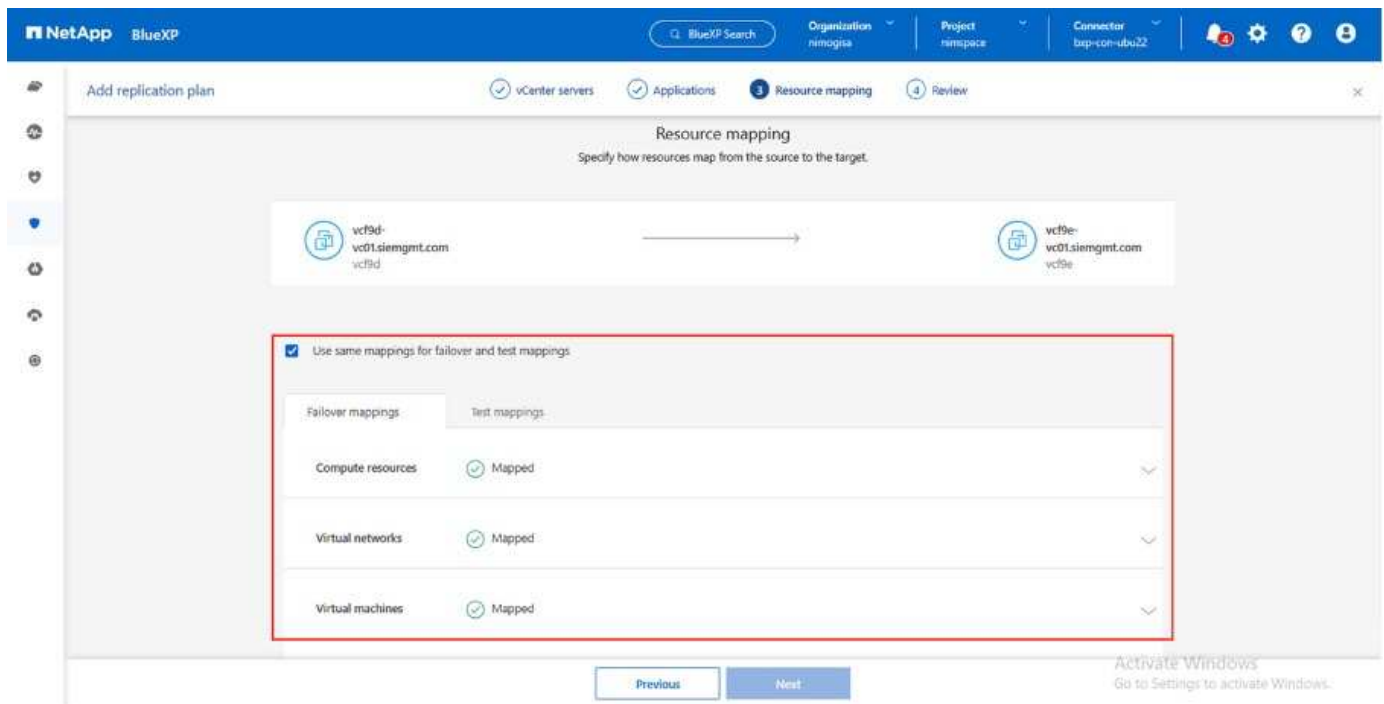
The next step is to select existing resource groups. If no resource groups created, then the wizard helps to group the required virtual machines (basically create functional resource groups) based on the recovery objectives. This also helps define the operation sequence of how application virtual machines should be restored.



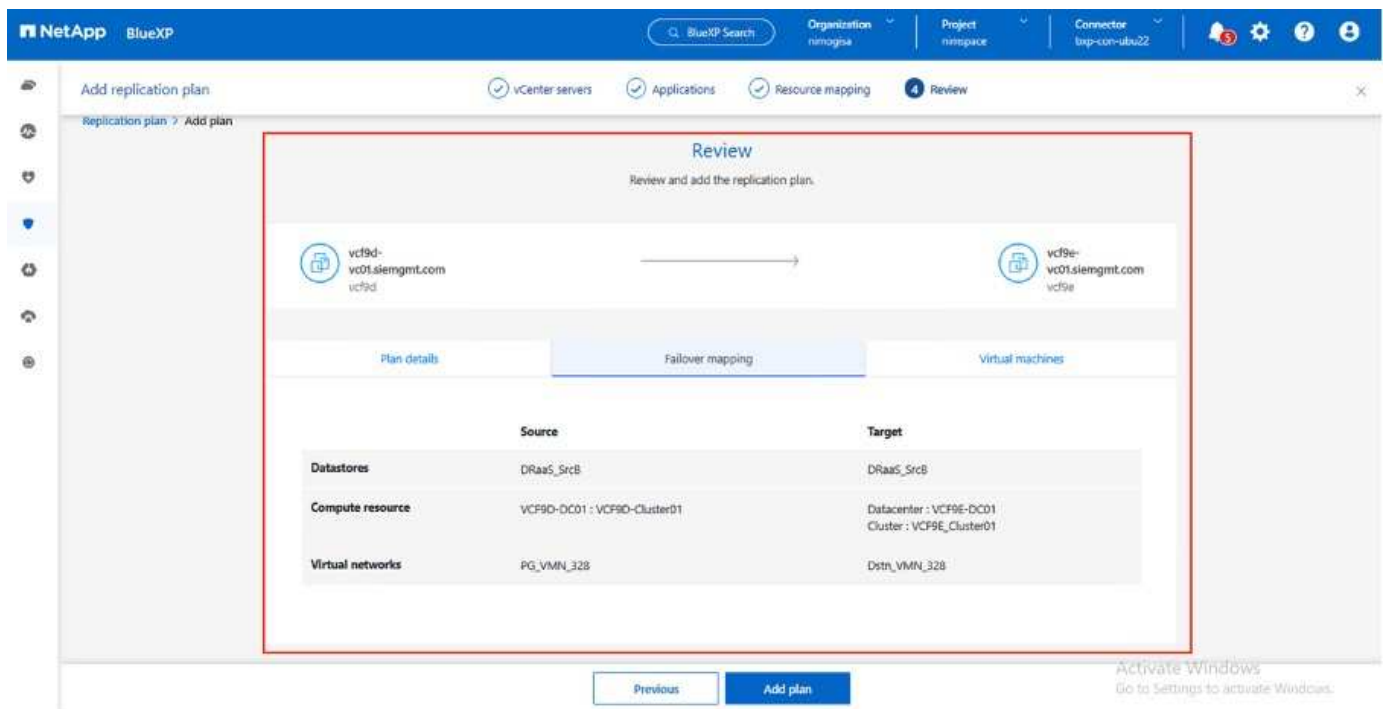
Resource group allows to set boot order using the drag and drop functionality. It can be used to easily modify the order in which the VMs would be powered on during the recovery process.

Once the resource groups are created via replication plan, the next step is to select the blueprint or a mapping to recover virtual machines and applications in the event of a disaster. In this step, specify how the resources from the source environment maps 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.

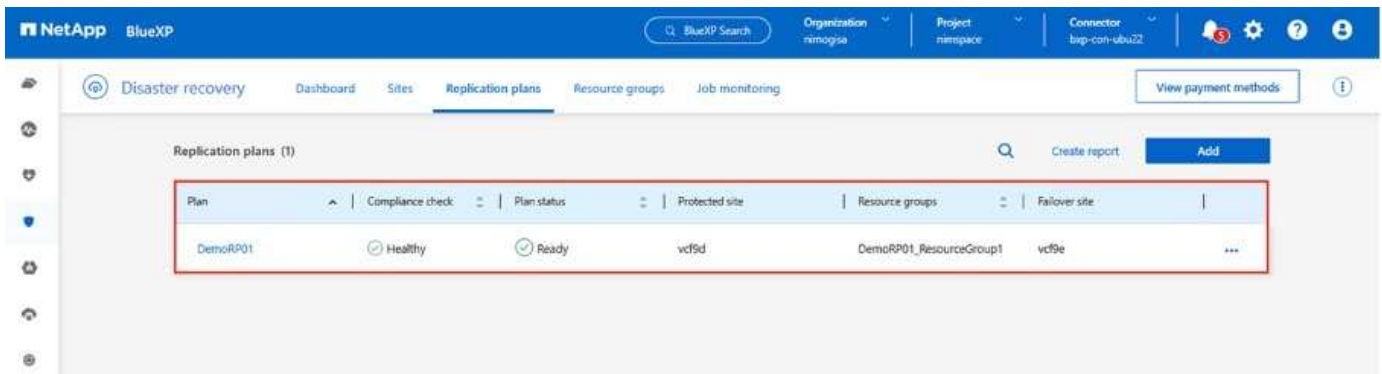
Note: By default, same mapping parameters are used for both test and failover operations. To set different mappings for test environment, select the Test mapping option after unchecking the checkbox “Use same mappings for failover and test mappings”. Once the resource mapping is complete, click Next.



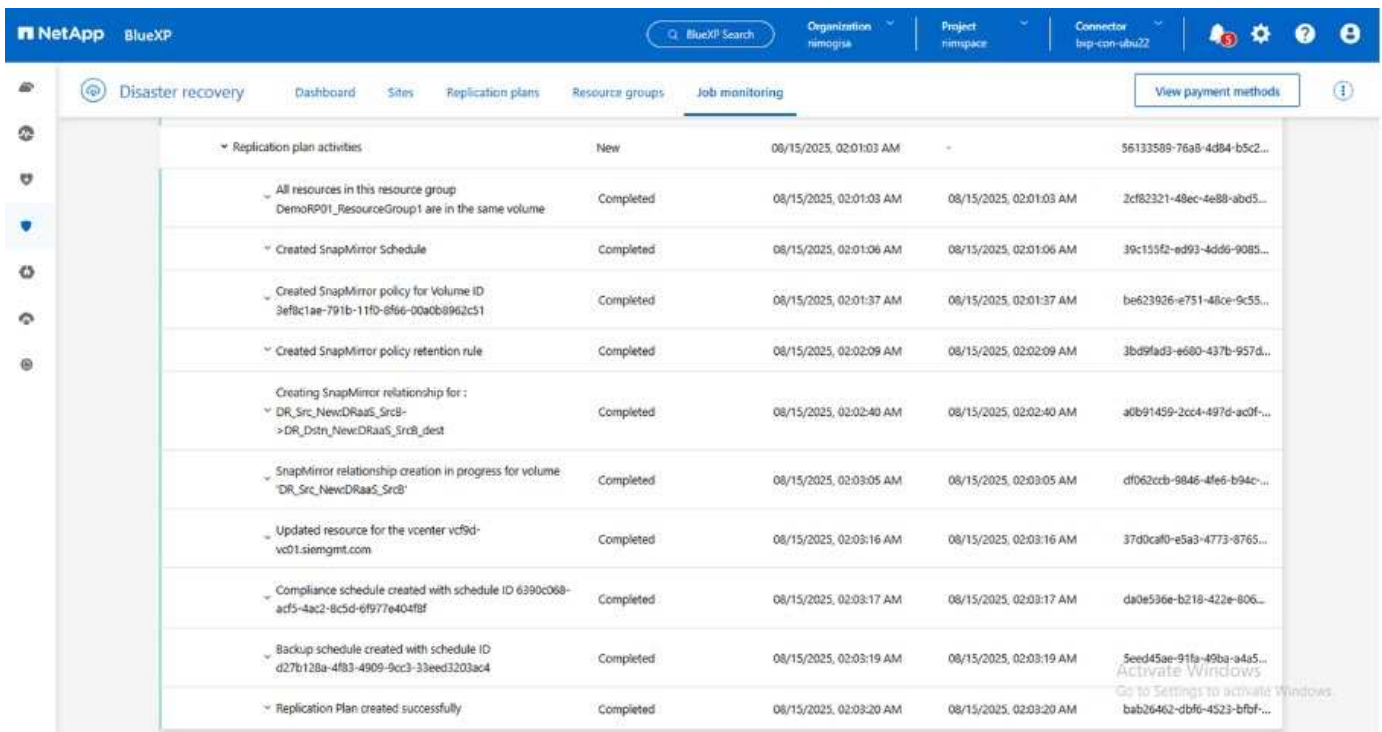
Once done, review the created mappings and then click on Add plan.



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), the BlueXP disaster recovery creates a Consistency Group Snapshot.

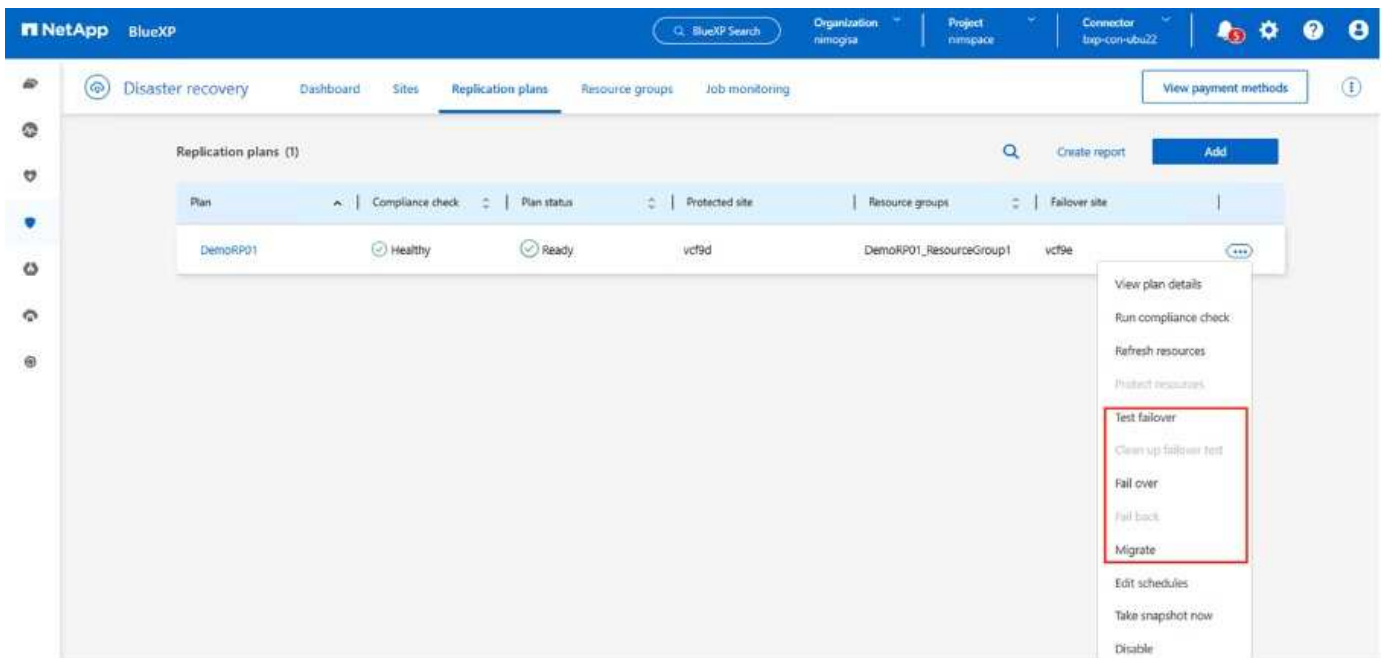


As soon as the plan is created, a series of validations are triggered and SnapMirror replication and schedules are configured as per the selection.



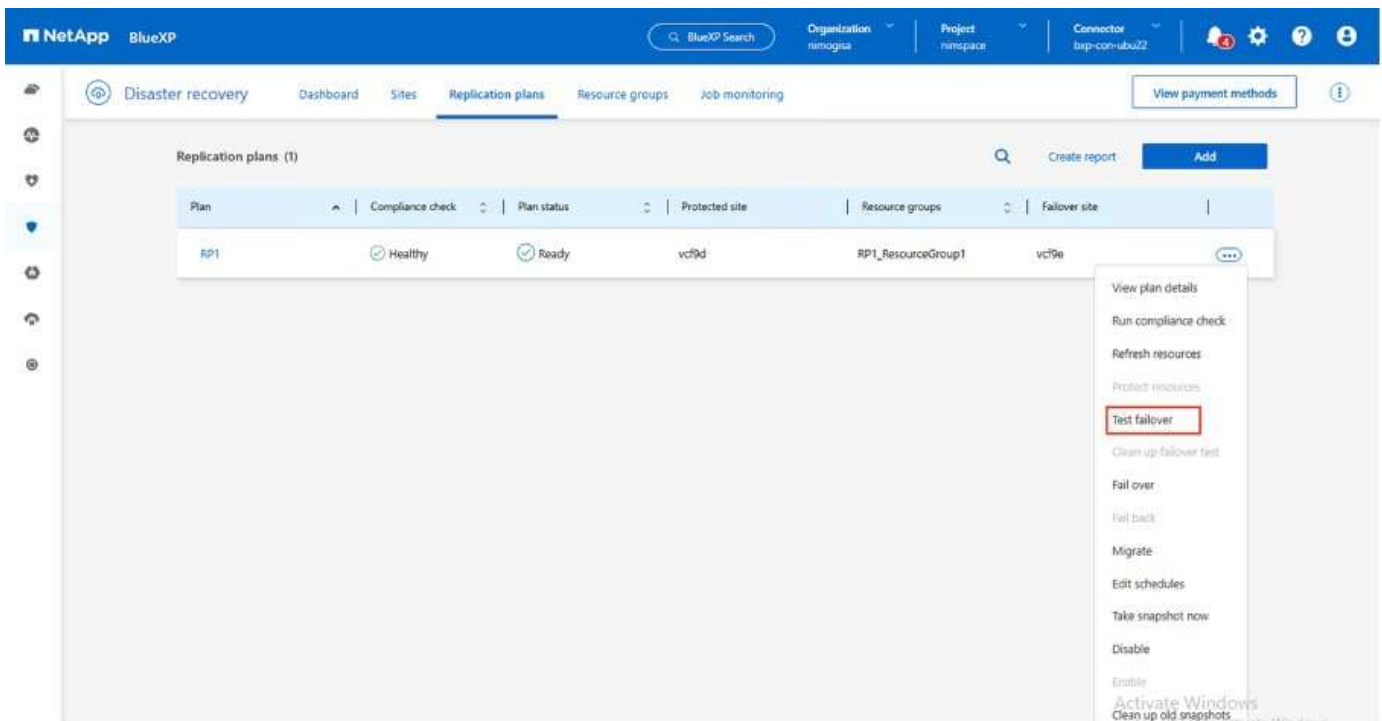
BlueXP DRaaS consists of the following workflows:

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

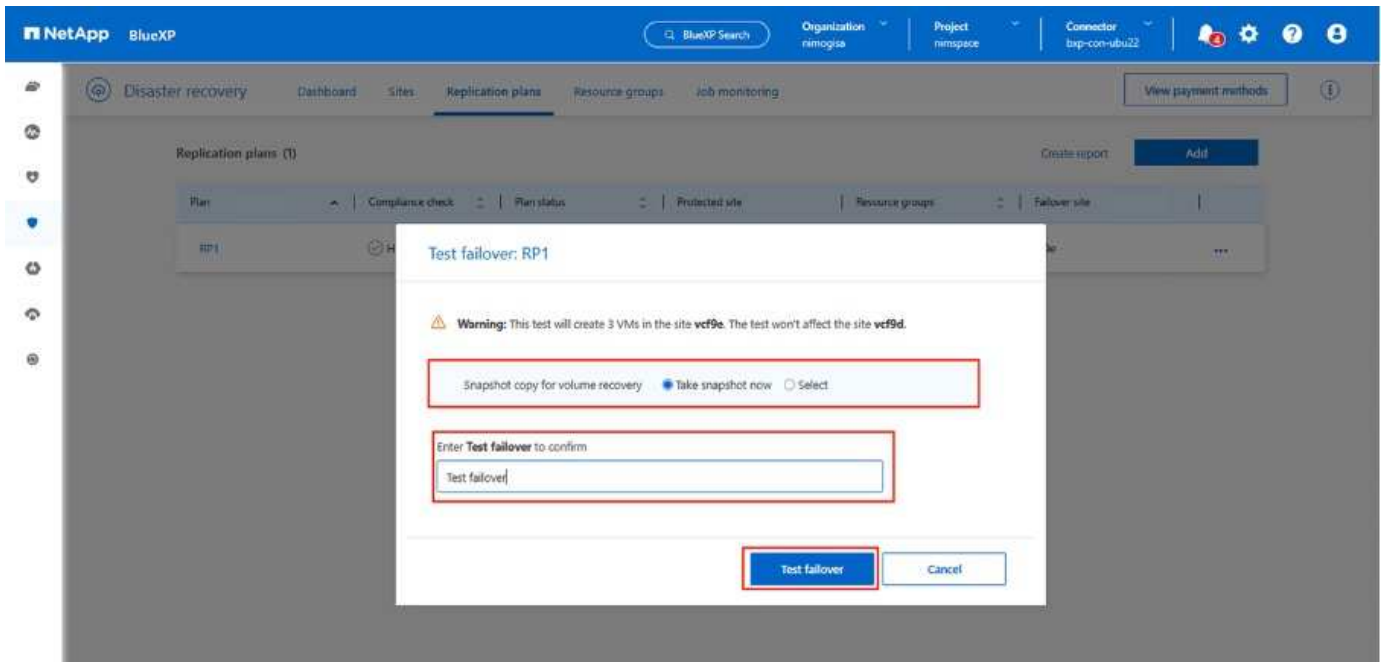


Test failover

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

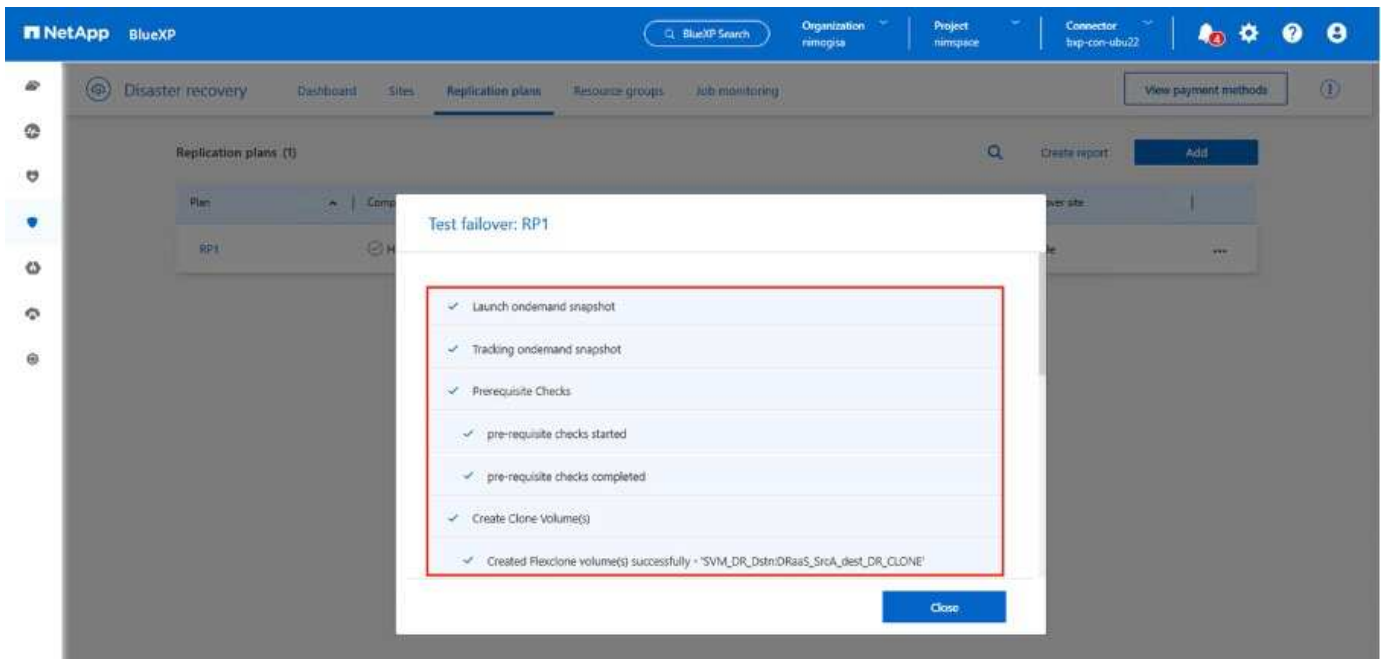


BlueXP DRaaS incorporates the ability to select the snapshot as an optional capability in the test failover operation. This capability allows the VMware administrator to verify that any changes that were recently made in the environment are replicated to the destination site and thus are present during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



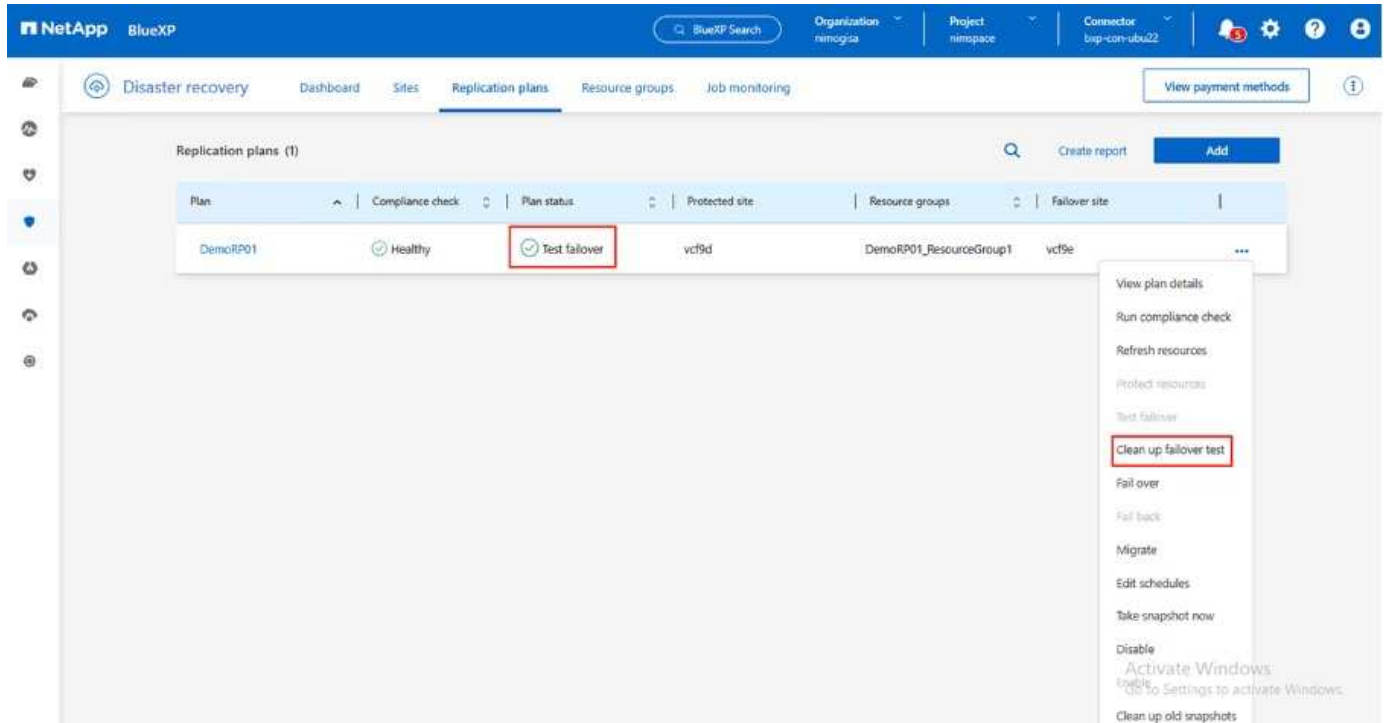
When the VMware administrator runs a test failover operation, BlueXP DRaaS automates the following tasks:

- 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.



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.

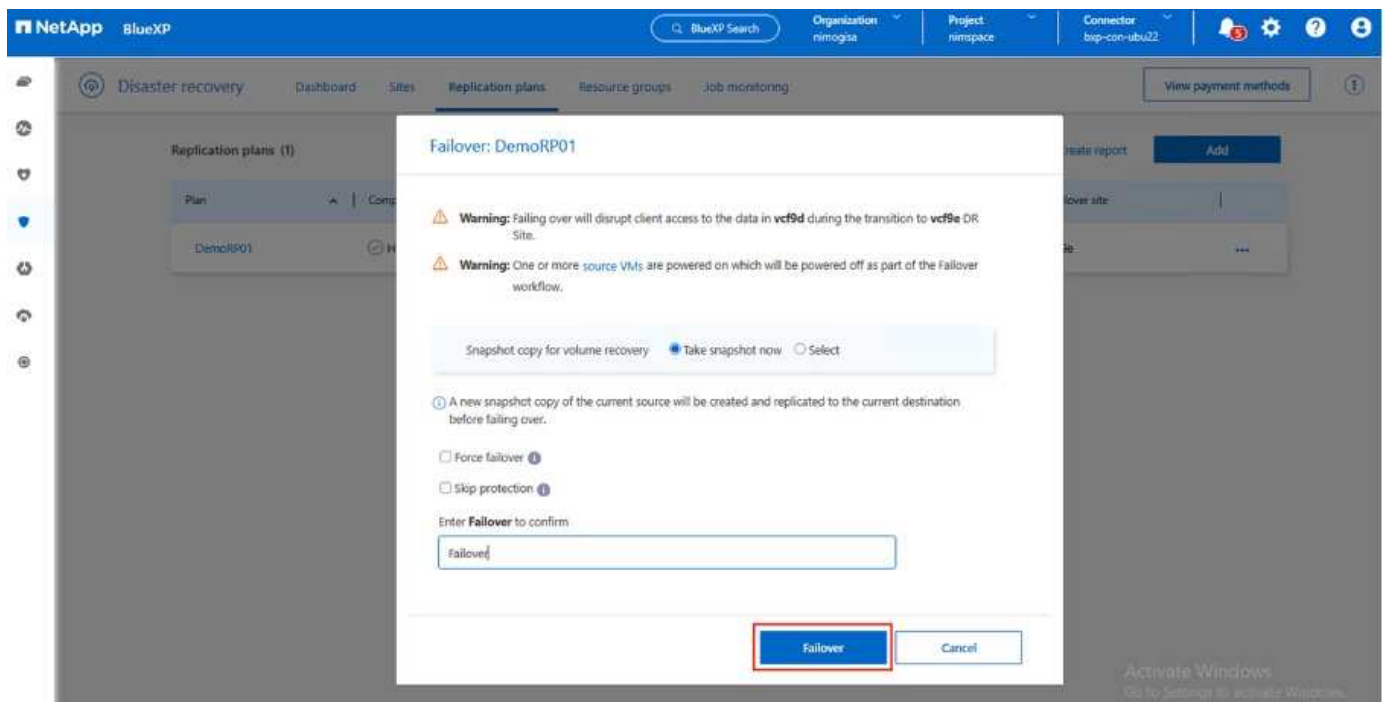
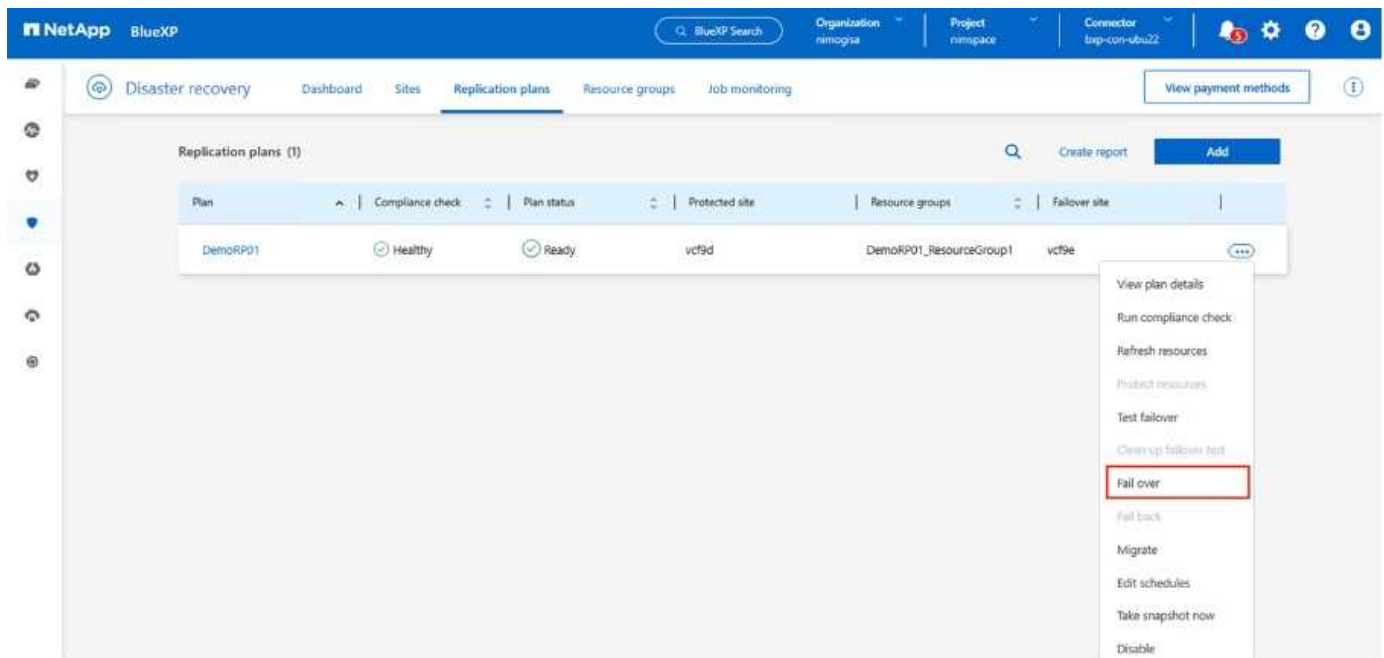


This action will reset the virtual machines (VMs) and the status of the replication plan to the ready state. When the VMware administrator performs a recovery operation, BlueXP DRaaS completes the following process:

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.

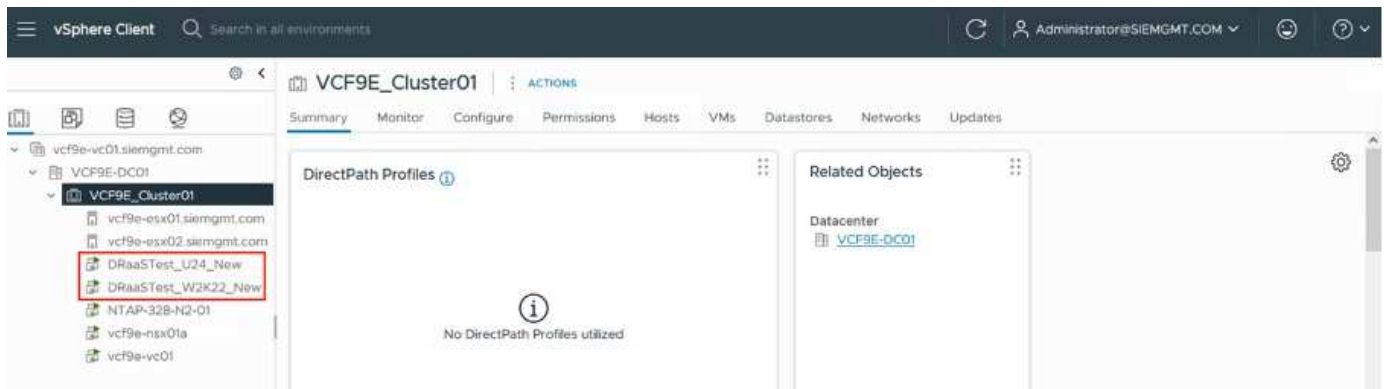
Planned Migration and Fail over

BlueXP DRaaS 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.



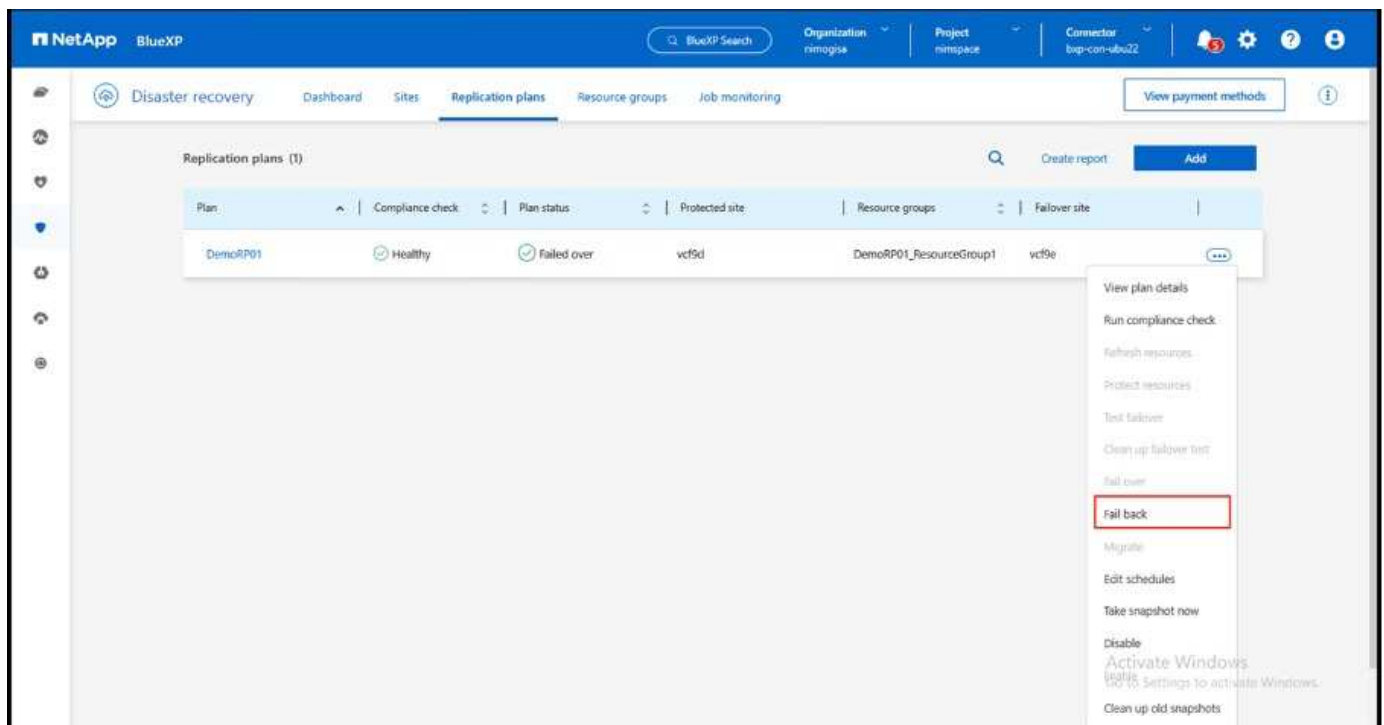
When the VMware administrator performs a failover operation, BlueXP DRaaS automates the following tasks:

- 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.



Failback

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



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



BlueXP DRaaS 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.

Recent Tasks

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time
Remove datastore	DRaaS_SrcB	Completed		SIEMGMT.COM\Administrator	7 ms	08/15/2025, 2:27:02 AM	08/15/2025, 2:27:03 AM
Remove datastore	DRaaS_SrcB	Completed		SIEMGMT.COM\Administrator	7 ms	08/15/2025, 2:27:01 AM	08/15/2025, 2:27:02 AM
Unregister virtual machine	DRaaSTest_U24_New	Completed		SIEMGMT.COM\Administrator	4 ms	08/15/2025, 2:27:00 AM	08/15/2025, 2:27:01 AM
Unregister virtual machine	DRaaSTest_W2K22_New	Completed		SIEMGMT.COM\Administrator	15 ms	08/15/2025, 2:27:00 AM	08/15/2025, 2:27:00 AM
Power Off virtual machine	DRaaSTest_U24_New	Completed		SIEMGMT.COM\Administrator	26 ms	08/15/2025, 2:23:55 AM	08/15/2025, 2:23:56 AM
Power Off virtual machine	DRaaSTest_W2K22_New	Completed		SIEMGMT.COM\Administrator	9 ms	08/15/2025, 2:23:55 AM	08/15/2025, 2:23:57 AM

- 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.

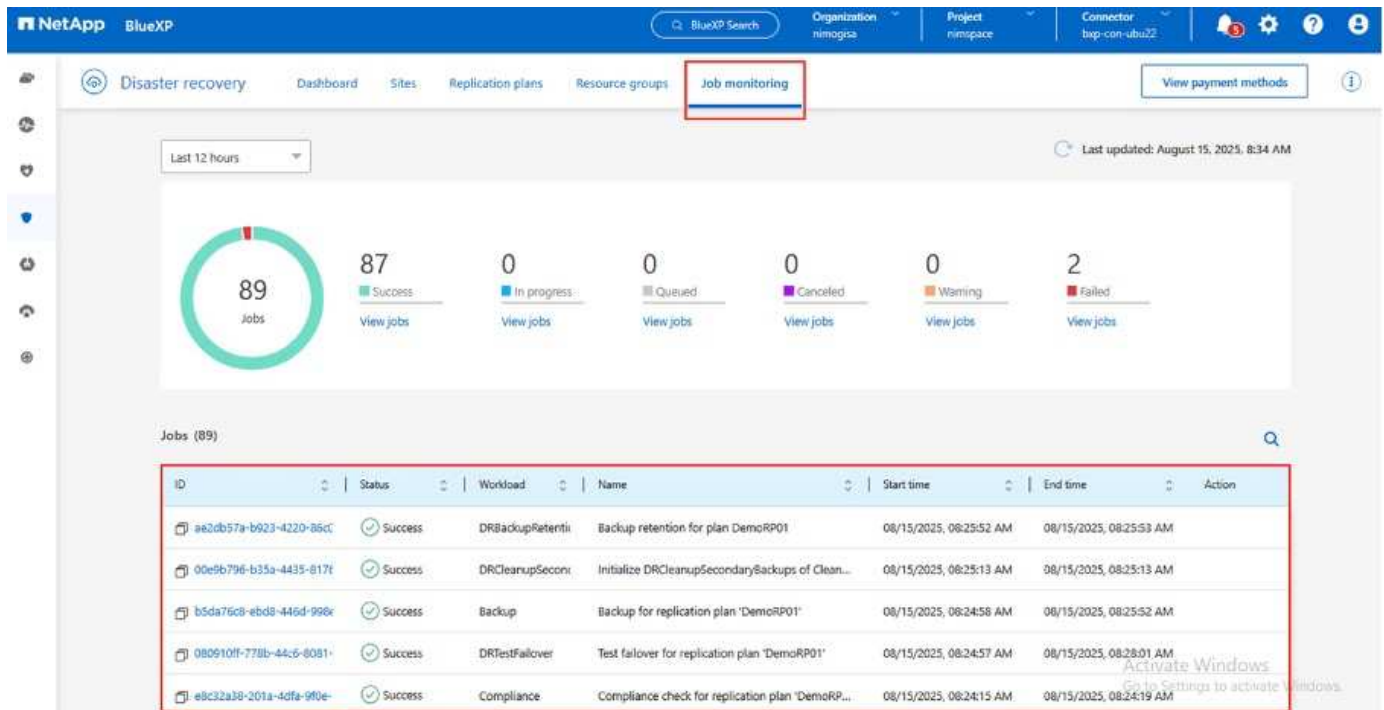
Recent Tasks

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time
Power On virtual machine	DRaaSTest_W2K22_New	Completed		SIEMGMT.COM\Administrator	6 ms	08/15/2025, 2:25:47 AM	08/15/2025, 2:25:48 AM
Power On virtual machine	DRaaSTest_U24_New	Completed		SIEMGMT.COM\Administrator	7 ms	08/15/2025, 2:25:47 AM	08/15/2025, 2:25:48 AM

For more details about accessing and configuring BlueXP DRaaS, see the [Learn about BlueXP Disaster Recovery for VMware](#).

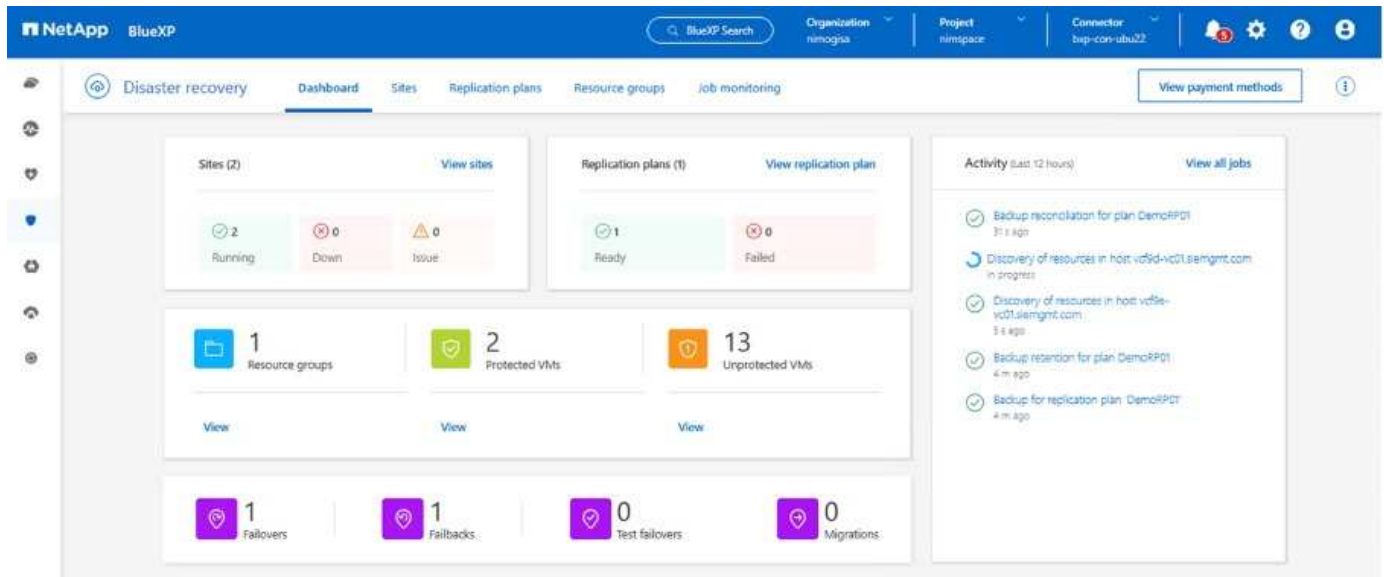
Monitoring and Dashboard

From BlueXP 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.



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

With the BlueXP 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.



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 VCF

Converting a vSphere environment with existing datastores running on ONTAP into a VMware Cloud Foundation (VCF) environment involves integrating the current infrastructure into a modern private cloud architecture.

This process leverages the flexibility of ONTAP storage for seamless data access and management. Once the VCF management domain is established, administrators can efficiently import additional vSphere environments into the VCF ecosystem. This integration enhances resource utilization, simplifies private cloud management, and ensures a smooth transition with minimal disruption to existing workloads.

Please refer to the following solutions for the technical details of converting a vCenter instance.

- [Convert Existing vCenter Instance to VCF Management Domain \(NFS\)](#)
- [Convert vCenter Instance \(FC datastore\) to VCF Management Domain](#)

Convert vCenter server instance to VCF management domain (NFS datastore)

Convert an existing vSphere 8 cluster with NetApp ONTAP NFS datastores into a VMware Cloud Foundation (VCF) management domain. This procedure includes provisioning NFS storage, deploying ONTAP tools for VMware, and using the VCF Import Tool to convert the cluster for streamlined management and optimized resource utilization within VCF.

Introduction

Converting a cluster, with an existing NFS datastore running on ONTAP, involves integrating existing infrastructure into a modern private cloud architecture. This process benefits from the flexibility of NFS 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 clusters, including those using NFS datastores, into the VCF ecosystem. This integration not only enhances resource utilization but also simplifies the management of private cloud infrastructure, ensuring a smooth transition with minimal disruption to existing workloads.

In this solution we will demonstrate how an NFS datastore in vSphere 8 becomes principal storage when the cluster is converted to a VCF management domain.

Scenario Overview

This scenario covers the following high level steps:

- Deploy ONTAP tools for VMware vSphere 10.
- Provision an NFS datastore using ONTAP tools.
- Use the VCF Import Tool to validate the vSphere cluster.
- Deploy the SDDC Manager in the vSphere cluster.
- Configure a JSON file to create NSX during the VCF conversion.
- Use the VCF Import Tool to convert the vSphere 8 cluster to VCF 5.2.

Prerequisites

This scenario requires the following components and configurations:

- NetApp AFF storage system with a storage virtual machine (SVM) configured to allow NFS traffic.
- Logical interface (LIF) has been created on the IP network that is to carry NFS traffic and is associated with the SVM.
- 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.

ONTAP tools for VMware vSphere 10 can be installed in either HA or non-HA configurations. For complete information on prerequisites for ONTAP tools refer to [Prerequisites for ONTAP tools for VMware vSphere deployment](#).

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](#).

For required software, go to the [Broadcom Support Portal](#).

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

The solution covers using ONTAP tools for VMware vSphere to provision NFS datastores and the process of converting an existing vSphere 8 cluster to a VCF management domain.

Complete the following steps:

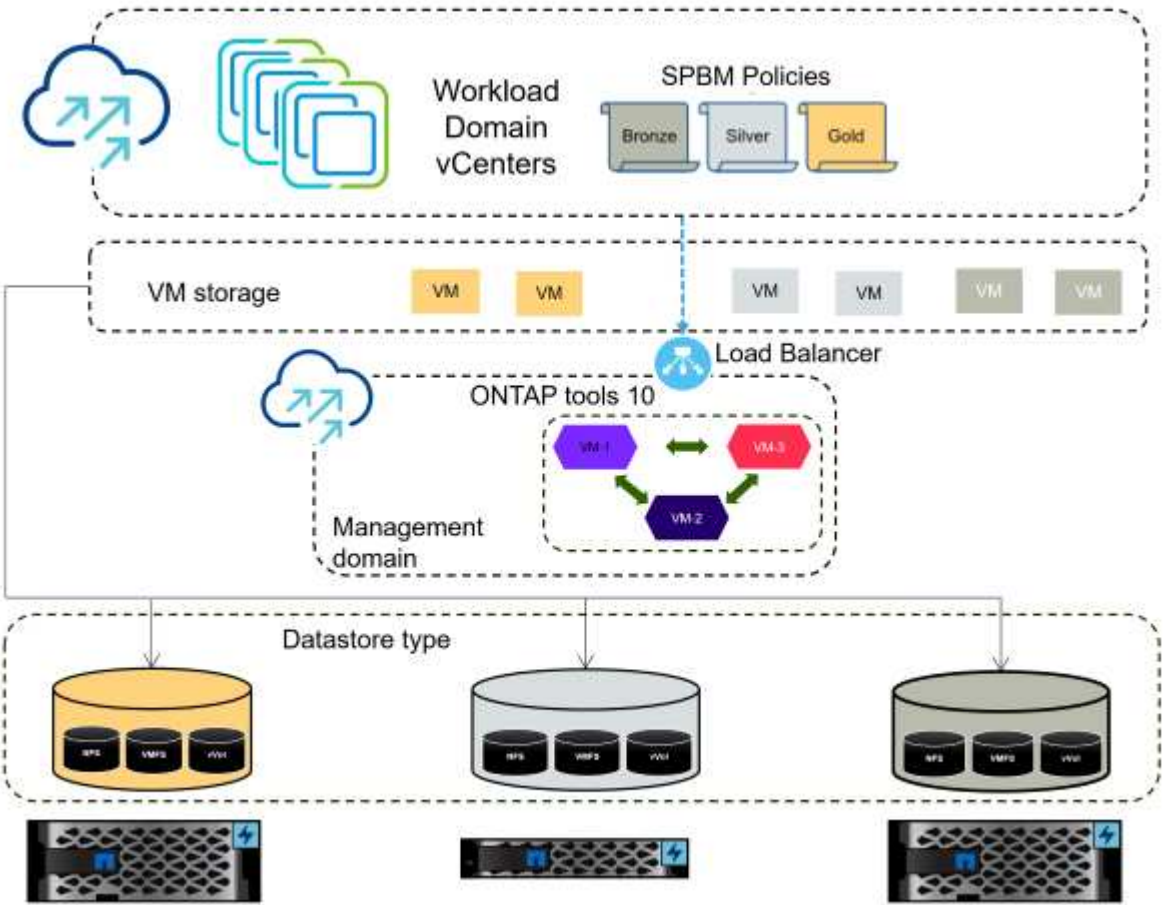
- Deploy ONTAP tools for VMware vSphere 10.
- Provision an NFS datastore using ONTAP tools.
- Copy the VCF Import Tool to the vCenter appliance.
- Run a precheck on the vCenter appliance using the VCF Import Tool.
- Deploy the SDDC manager VM on the vCenter cluster.
- Create a JSON file for an NSX cluster to be deployed during the conversion process.
- Upload the required software to the SDDC manager.
- Convert the vSphere cluster into the SDDC manager inventory.

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 ONTAP tools and provision an NFS datastore

The architecture of ONTAP tools 10 is designed to integrate 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 10 can be installed in either HA or non-HA configurations.

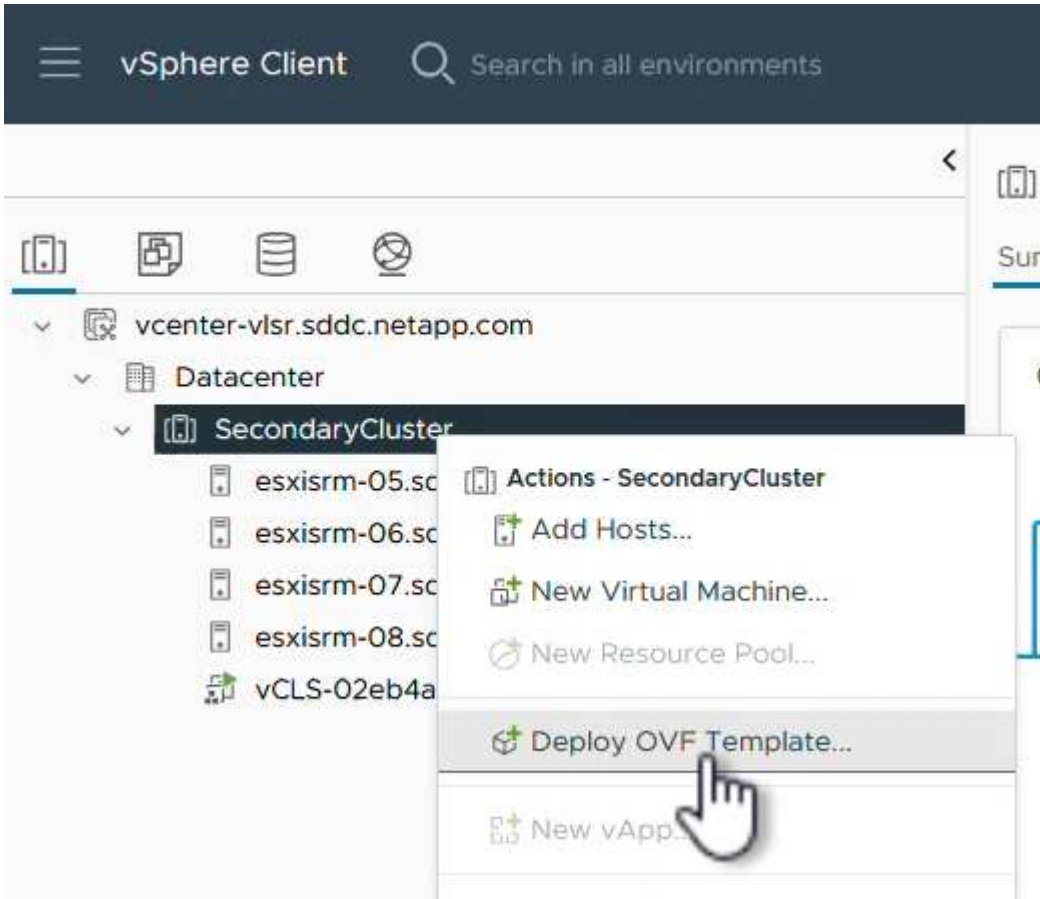


Deploy ONTAP tools for VMware vSphere 10

In this step ONTAP tools 10 is deployed with a non-HA configuration.

For additional deployment details on HA and non-HA configurations refer to [Deploy ONTAP tools for VMware vSphere](#).

1. Download the ONTAP tools 10 OVA template from the [NetApp support site](#).
2. In the vSphere client, right click on the cluster and click on **Deploy OVF Template**



3. In the **Deploy OVF Template** complete the steps to:
 - Select an OVF template.
 - Select a name and folder.
 - Select a compute resource.
 - Review Details.
 - Agree to the license agreement.
4. On the **Configuration** page of the template, select the deployment type including whether to deploy ONTAP tools in an HA configuration. Click on **Next** to continue.

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Configuration**
- Select storage
- Select networks
- Customize template
- Ready to complete

Configuration

Select a deployment configuration

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

8 Items

CANCEL
BACK
NEXT

- On the **Select storage** page choose the datastore on which to install the VM, and click on **Next**.
- Select the network that the ONTAP tools VM will communicate on. Click on **Next** to continue.
- On the "Customize template" window, fill out all required information.
 - Application username and password
 - Choose whether to enable ASUP (auto support) including a proxy URL.
 - Administrator username and password.
 - NTP servers.
 - Maintenance username and password (maint account used at the console).
 - Provide the required IP addresses for the deployment configuration.
 - Provide all networking information for the node configuration.

Node Configuration		10 settings
HostName(*)	Specify the hostname for the VM	otv10-primary
IP Address(*)	Specify the IP address for the appliance	172.21.120.56
IPv6 Address	Specify the IPv6 address on the deployed network only when you need dual stack.	
Prefix length	Specify the prefix length	
Netmask (Only for IPv4)(*)	Specify the subnet to use on the deployed network	255.255.255.0
Gateway(*)	Specify the gateway on the deployed network	172.21.120.1
Primary DNS(*)	Specify the primary DNS server's IP address	10.61.185.231
Secondary DNS(*)	Specify the secondary DNS server's IP address	10.61.186.231

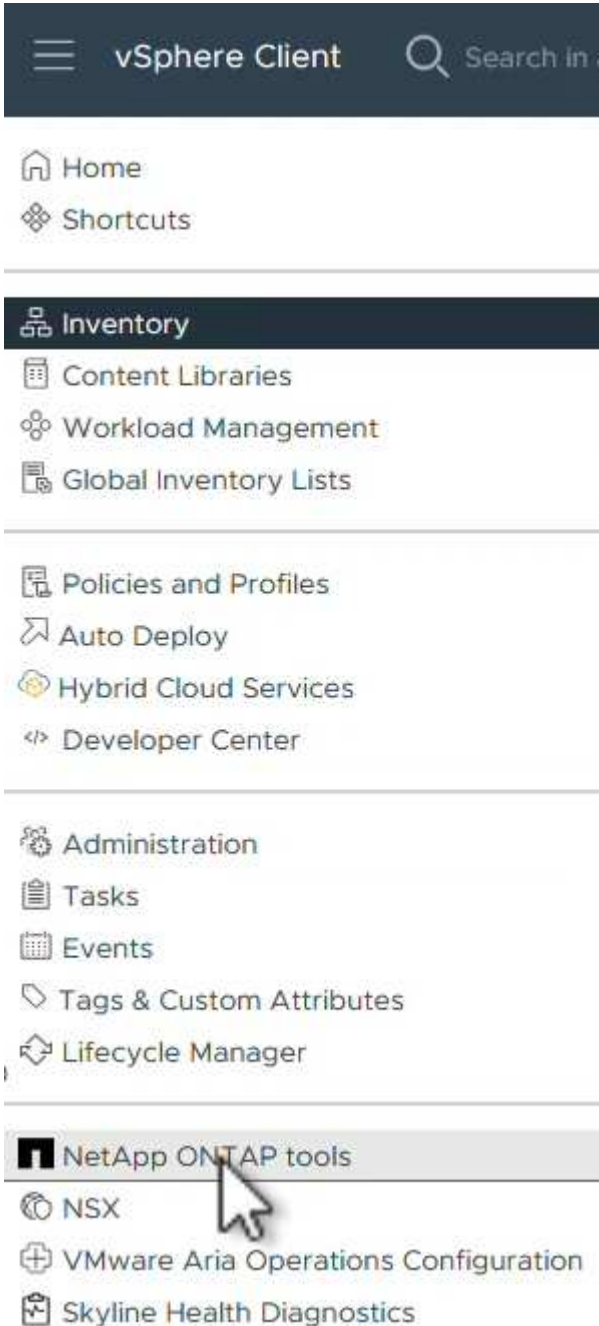
CANCELBACKNEXT

8. Finally, click on **Next** to continue and then on then on **Finish** to begin the deployment.

Configure ONTAP tools

Once the ONTAP tools VM is installed and powered up, there will be some basic configuration required such as adding vCenter servers and ONTAP storage systems to manage. Refer to the documentation at [ONTAP tools for VMware vSphere documentation](#) for detailed information.

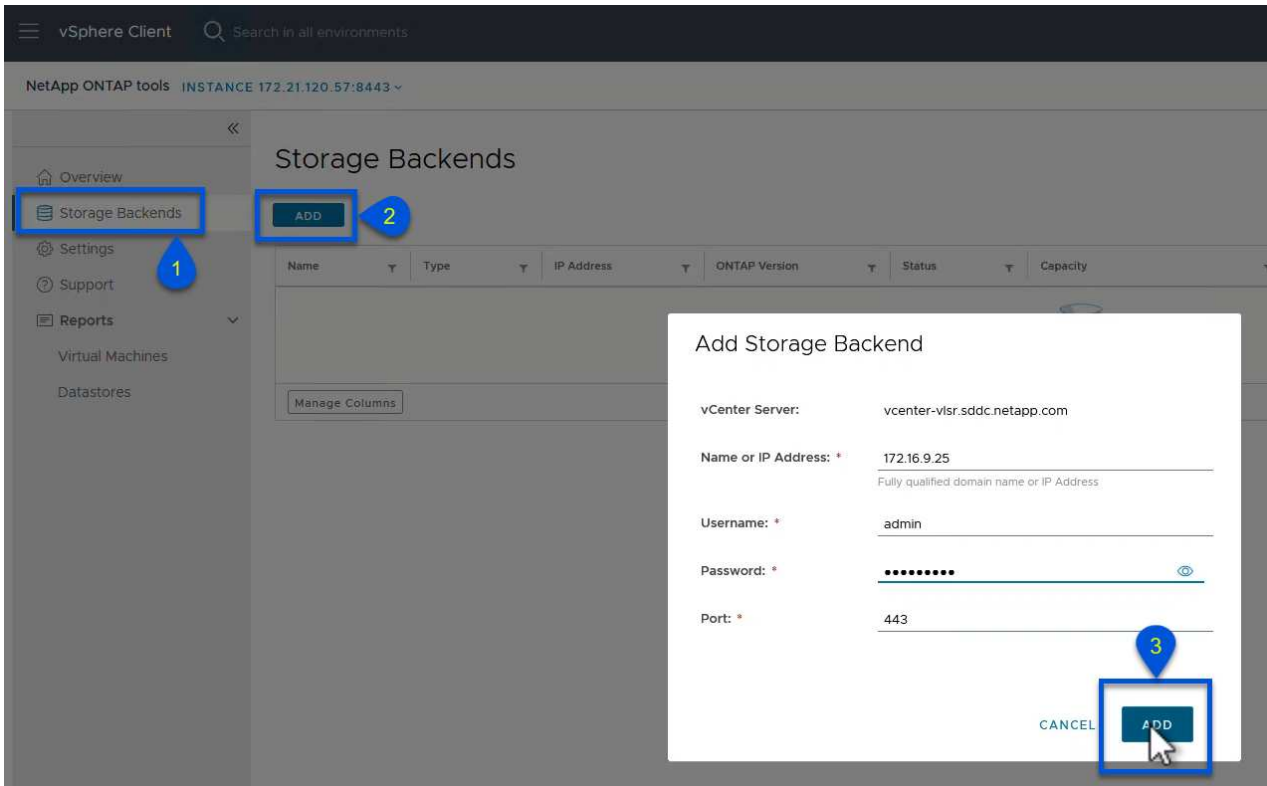
1. Refer to [Add vCenter instances](#) to configure the vCenter instances to be managed with ONTAP tools.
2. To add an ONTAP storage system, log into the vSphere client and navigate to the main menu on the left. Click on **NetApp ONTAP tools** to launch user interface.



3. Navigate to **Storage Backends** in the left hand menu and click on **Add** to access the **Add Storage**

Backend window.

4. Fill out the IP address and credentials for the ONTAP storage system to be managed. Click on **Add** to finish.

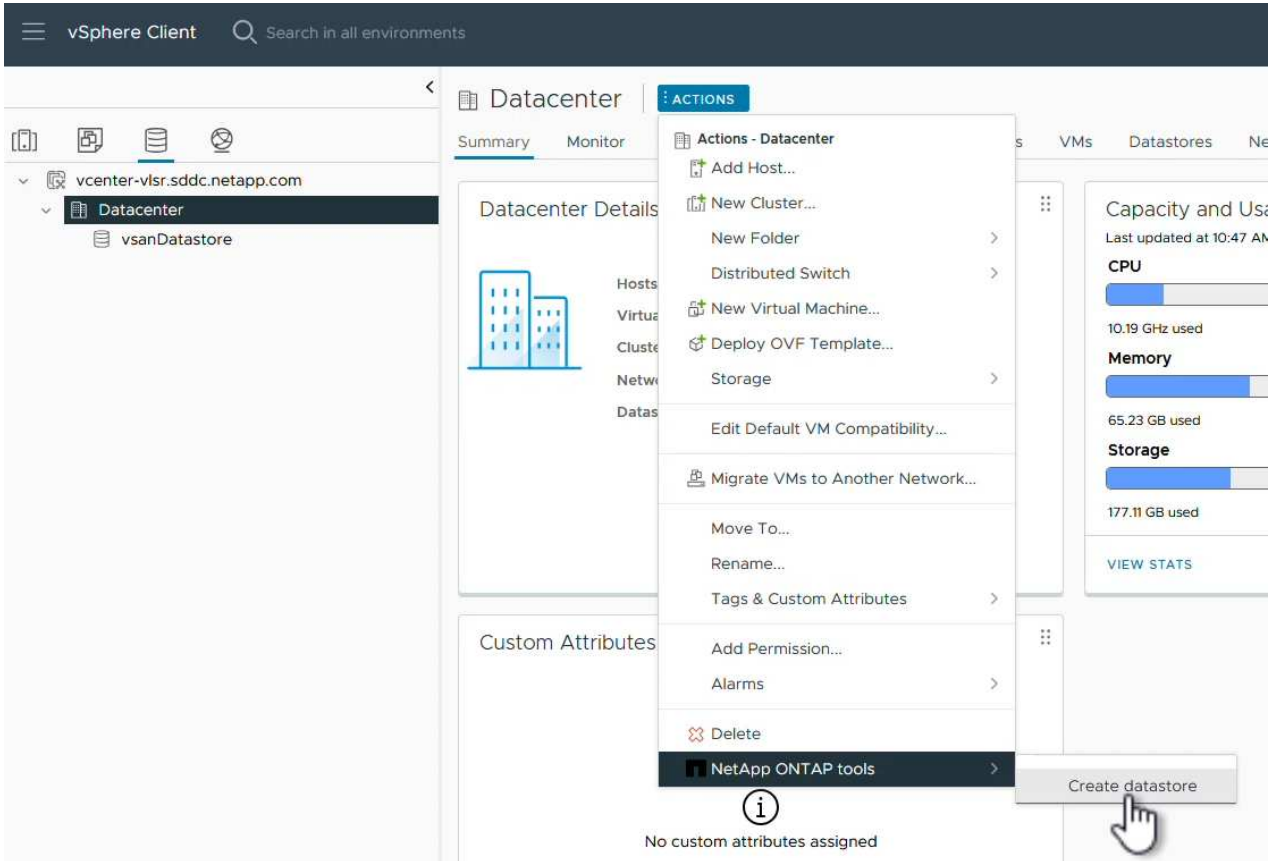


Here, the storage backend is added in the vSphere client UI using the cluster IP address. This allows full management over all SVMs in the storage system. Alternately, the storage backend can be added and associated with a vCenter instance using ONTAP tools Manager at <https://loadBalanceIP:8443/virtualization/ui/>. With this method only SVM credentials can be added at the vSphere client UI, providing more granular control over storage access.

Provision NFS datastore with ONTAP tools

ONTAP tools integrates functionality throughout the vSphere client UI. In this step an NFS datastore will be provisioned from the storage inventory page.

1. In the vSphere client, navigate to the storage inventory.
2. Navigate to **ACTIONS > NetApp ONTAP tools > Create datastore**.



3. In the **Create Datastore** wizard, select the type of datastore to create. Options are NFS or VMFS.
4. On the **Name and Protocol** page, fill in a name for the datastore, the size, and the NFS protocol to be used.

Create Datastore

1 Type

2 Name and Protocol

3 Storage

4 Storage Attributes

5 Summary

Name and Protocol

Datastore name:

NFS_DS1

Size:

2

TB

Minimum supported size is 1 GB.

Protocol:

NFS 3

Advanced Options

Datastore Cluster:

CANCEL

BACK

NEXT

- On the **Storage** page, select the ONTAP storage platform and the storage virtual machine (SVM). You can also select any available custom export policies here. Click on **Next** to continue.

Create Datastore

1 Type

2 Name and Protocol

3 Storage

4 Storage Attributes

5 Summary

Storage

Platform: *

Performance (A)

Storage VM: *

VCF_NFS

ntaphci-a300e9u25 (172.16.9.25)

Advanced Options

Custom Export Policy:

Search or specify policy name

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

CANCEL

BACK

NEXT

- On the **Storage Attributes** page select the storage aggregate to be used. Click on **Next** to continue.
- On the **Summary** page, review the information and click on **Finish** to begin the provisioning process. ONTAP tools will create a volume on the ONTAP storage system and mount it as an NFS datastore to all ESXi hosts in the cluster.

39

The screenshot shows the 'Create Datastore' wizard in a web interface. On the left, a sidebar lists five steps: 1 Type, 2 Name and Protocol, 3 Storage, 4 Storage Attributes, and 5 Summary. The 'Summary' step is selected and highlighted. The main area is titled 'Summary' and contains a message: 'A new datastore will be created with these settings.' Below this, the configuration is organized into three sections: 'Type', 'Name and Protocol', and 'Storage'. The 'Type' section shows 'Destination: Datacenter' and 'Datastore type: NFS'. The 'Name and Protocol' section shows 'Datastore name: NFS_DS1', 'Size: 2 TB', and 'Protocol: NFS 3'. The 'Storage' section shows 'Platform: Performance (A)' and 'Storage VM: VCF_NFS'. At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'FINISH'. A mouse cursor is pointing at the 'FINISH' button.

Type	
Destination:	Datacenter
Datastore type:	NFS

Name and Protocol	
Datastore name:	NFS_DS1
Size:	2 TB
Protocol:	NFS 3

Storage	
Platform:	Performance (A)
Storage VM:	VCF_NFS

Convert vSphere cluster to VCF 5.2

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 Tools 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 Precheck on the Target vCenter Before Conversion](#) to run the validation.
2. The following output shows that the vCenter appliance has passed the precheck.

```
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter 172.21.166.57 --sso-user administrator@vsphere.local
[2024-10-23 19:03:23,609] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.0-24307788
Enter vCenter SSO password:
[2024-10-23 19:03:28,825] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2024-10-23 19:03:28,938] [INFO] vc_precheck: Connected to vCenter 172.21.166.57 in 0.11 seconds
[2024-10-23 19:03:28,939] [INFO] vc_precheck: Running pre-checks for vCenter 172.21.166.57...
[2024-10-23 19:03:28,939] [INFO] vc_precheck: [1/10] VC BOM version check... PASS
[2024-10-23 19:03:28,975] [INFO] vc_precheck: [2/10] vSAN stretched cluster check... PASS
[2024-10-23 19:03:28,999] [INFO] vc_precheck: [3/10] Supported storage available check... PASS
[2024-10-23 19:03:29,020] [INFO] vc_precheck: [4/10] vCenter VM location check... PASS
[2024-10-23 19:03:29,233] [INFO] vc_precheck: [5/10] VxRail registration check... PASS
[2024-10-23 19:03:29,414] [INFO] vc_precheck: [6/10] NSX-T registration check... PASS
[2024-10-23 19:03:29,437] [INFO] vc_precheck: [7/10] Standalone host check... PASS
[2024-10-23 19:03:31,870] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check... PASS
[2024-10-23 19:03:32,962] [INFO] vc_precheck: [9/10] ELM ring topology check... PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: [10/10] WCP import check... PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: All pre-checks passed!
[2024-10-23 19:03:33,383] [INFO] vc_precheck: Pre-checks for vCenter 172.21.166.57 completed in 4.44 seconds
root@localhost [ /tmp/vcfimport/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.

Refer to [Deploy the SDDC Manager Appliance on the Target vCenter](#).

For more information see [Commission Hosts](#) in the VCF Administration Guide.

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 networking is utilized. For details on the limitations of NSX-VLAN networking, 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:

```
{
  "license_key": "xxxxx-xxxxx-xxxxx-xxxxx-xxxxx",
  "form_factor": "medium",
  "admin_password": "NetApp!23456789",
  "install_bundle_path": "/tmp/vcfimport/bundle-133764.zip",
  "cluster_ip": "172.21.166.72",
  "cluster_fqdn": "vcf-m02-nsx01.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "vcf-m02-nsx01a.sddc.netapp.com",
    "name": "vcf-m02-nsx01a",
    "ip_address": "172.21.166.73",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01b.sddc.netapp.com",
    "name": "vcf-m02-nsx01b",
    "ip_address": "172.21.166.74",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01c.sddc.netapp.com",
    "name": "vcf-m02-nsx01c",
    "ip_address": "172.21.166.75",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  }
]
```

Copy the JSON file to a directory on the SDDC Manager.

Upload software to SDDC Manager

Copy the VCF Import Tool and the NSX deployment bundle to /home/vcf/vcfimport directory on the SDDC Manager.

See [Upload the Required Software to the SDDC Manager Appliance](#) for detailed instructions.

Convert vSphere cluster to VCF management domain

The VCF Import Tool is used to conduct the conversion process.

Run the following command from the /home/vcf/vcf-import-package/vcf-brownfield-import-<version>/vcf-brownfield-toolset directory, to review a printout of VCF import tool functions:

```
python3 vcf_brownfield.py --help
```

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>' --domain-name '<wld-domain-name>' --nsx-deployment-spec -path '<nsx-deployment-json-spec-path>'
```

For complete instructions, refer to [Convert or Import the vSphere Environment into the SDDC Manager Inventory](#).

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.

Video demo for ONTAP tools for VMware vSphere 10

[NFS datastore with ONTAP tools for VMware vSphere 10](#)

Convert vCenter server instance to VCF management domain (FC datastore)

Convert a vSphere 8 cluster using ONTAP Fibre Channel datastores into a VMware Cloud Foundation management domain. This procedure includes provisioning FC storage, deploying ONTAP tools for VMware, and using the VCF import tool to migrate and manage the cluster within the VCF environment.

Introduction

Converting a vSphere environment, with an existing Fibre Channel (FC) datastore running on ONTAP, involves integrating existing infrastructure into a modern private cloud architecture. This process benefits from the robustness of FC 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 FC datastores, into the VCF ecosystem. This integration not only enhances resource utilization but also simplifies the management of private cloud infrastructure, ensuring a smooth transition with minimal disruption to existing workloads.

In this solution we will demonstrate how an FC datastore in vSphere 8 becomes principal storage when the cluster is converted to a VCF management domain.

Scenario Overview

This scenario covers the following high level steps:

- Deploy ONTAP tools for VMware vSphere 10.
- Provision a FC datastore using ONTAP tools.
- Use the VCF Import Tool to validate the vSphere cluster.
- Deploy the SDDC Manager in the vSphere cluster.
- Configure a JSON file to create NSX during the VCF conversion.
- Use the VCF Import Tool to convert the vSphere 8 cluster to VCF 5.2.1

Prerequisites

This scenario requires the following components and configurations:

- NetApp ASA R2/ASA/AFF storage system with a storage virtual machine (SVM) configured to allow Fibre Channel (FC) traffic.
- Logical interface (LIF) has been created to carry FC traffic and is associated with the SVM.
- FC zoning has been configured on the switches designated to carry FC traffic.
- A vSphere 8 cluster with 4 x ESXi hosts and a vCenter appliance colocated on the cluster.
- Distributed port group configured for vMotion on the VLANs or network segments established for this purpose.
- Download software required for the VCF conversion.

ONTAP tools for VMware vSphere 10 can be installed in either HA or non-HA configurations. For complete information on prerequisites for ONTAP tools refer to [Prerequisites for ONTAP tools for VMware vSphere deployment](#).

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.](#)

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 5.2 Documentation.](#)

Deployment Steps

The solution covers using ONTAP tools for VMware vSphere to provision FC datastores and the process of converting an existing vSphere 8 cluster to a VCF management domain.

Complete the following steps:

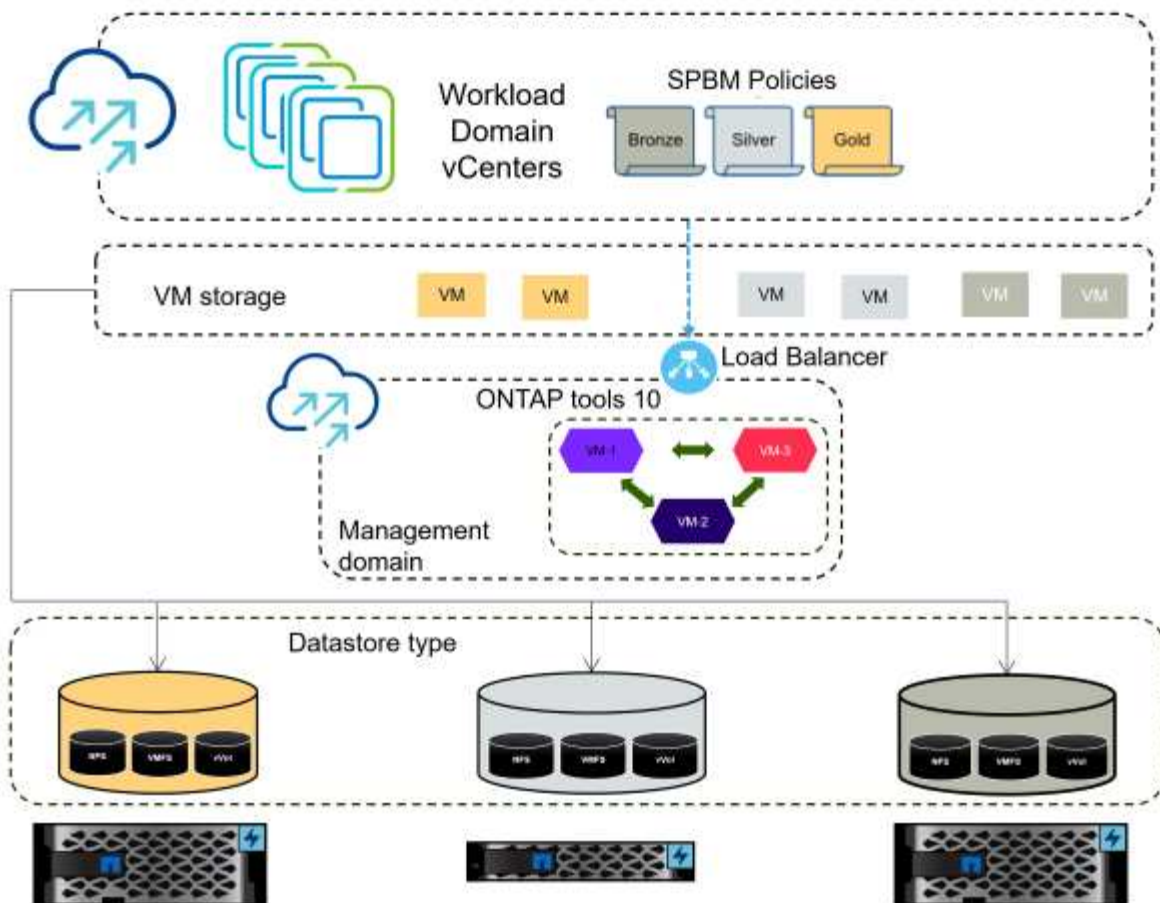
- Deploy ONTAP tools for VMware vSphere 10.
- Provision a FC datastore using ONTAP tools.
- Copy the VCF Import Tool to the vCenter appliance.
- Run a precheck on the vCenter appliance using the VCF Import Tool.
- Deploy the SDDC manager VM on the vCenter cluster.
- Create a JSON file for an NSX cluster to be deployed during the conversion process.
- Upload the required software to the SDDC manager.
- Convert the vSphere cluster into the SDDC manager inventory.

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 ONTAP tools and provision a FC datastore

The architecture of ONTAP tools 10 is designed to integrate 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 10 can be installed in either HA or non-HA configurations.

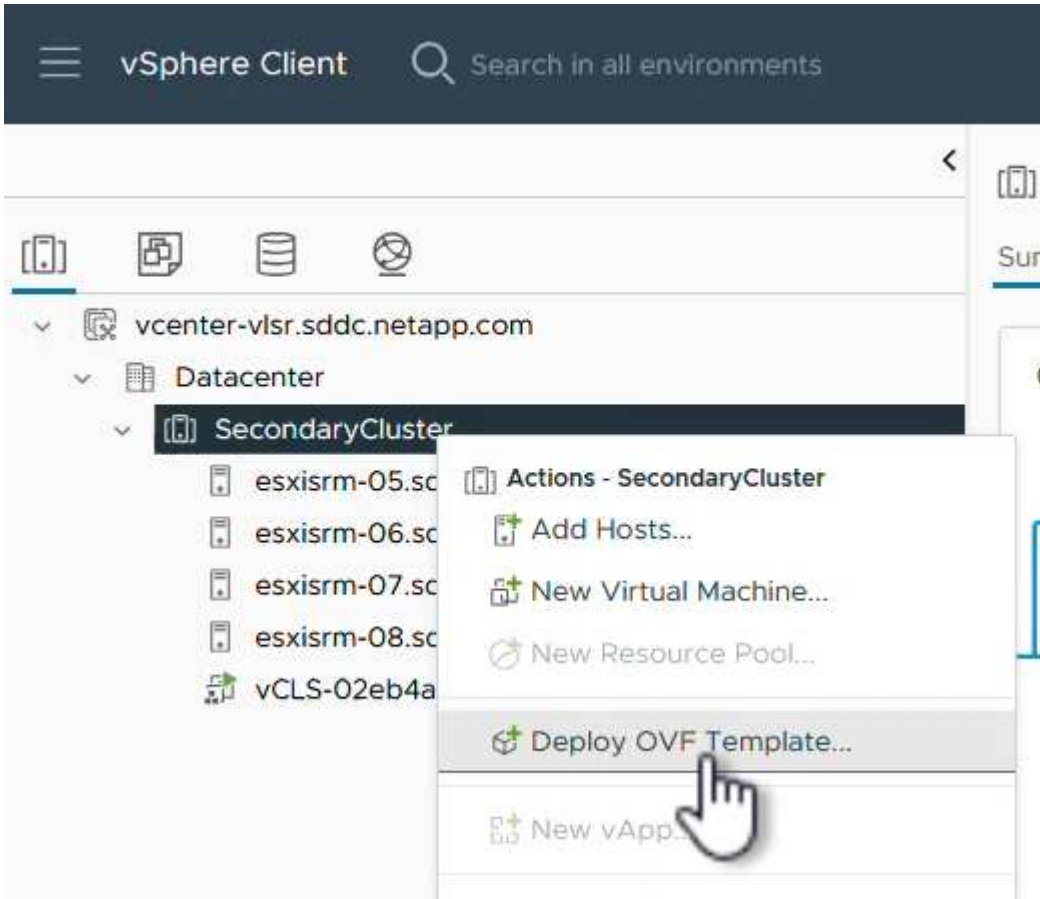


Deploy ONTAP tools for VMware vSphere 10

In this step ONTAP tools 10 is deployed with a non-HA configuration.

For additional deployment details on HA and non-HA configurations refer to [Deploy ONTAP tools for VMware vSphere](#).

1. Download the ONTAP tools 10 OVA template from the [NetApp support site](#).
2. In the vSphere client, right click on the cluster and click on **Deploy OVF Template**



3. In the **Deploy OVF Template** complete the steps to:
 - Select an OVF template.
 - Select a name and folder.
 - Select a compute resource.
 - Review Details.
 - Agree to the license agreement.
4. On the **Configuration** page of the template, select the deployment type including whether to deploy ONTAP tools in an HA configuration. Click on **Next** to continue.

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Configuration**
- Select storage
- Select networks
- Customize template
- Ready to complete

Configuration

Select a deployment configuration


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

8 Items

CANCEL

BACK

NEXT



- On the **Select storage** page choose the datastore on which to install the VM, and click on **Next**.
- Select the network that the ONTAP tools VM will communicate on. Click on **Next** to continue.
- On the "Customize template" window, fill out all required information.
 - Application username and password
 - Choose whether to enable ASUP (auto support) including a proxy URL.
 - Administrator username and password.
 - NTP servers.
 - Maintenance username and password (maint account used at the console).
 - Provide the required IP addresses for the deployment configuration.
 - Provide all networking information for the node configuration.

Node Configuration	10 settings
HostName(*)	Specify the hostname for the VM otv10-primary
IP Address(*)	Specify the IP address for the appliance 172.21.120.56
IPv6 Address	Specify the IPv6 address on the deployed network only when you need dual stack.
Prefix length	Specify the prefix length
Netmask (Only for IPv4)(*)	Specify the subnet to use on the deployed network 255.255.255.0
Gateway(*)	Specify the gateway on the deployed network 172.21.120.1
Primary DNS(*)	Specify the primary DNS server's IP address 10.61.185.231
Secondary DNS(*)	Specify the secondary DNS server's IP address 10.61.186.231

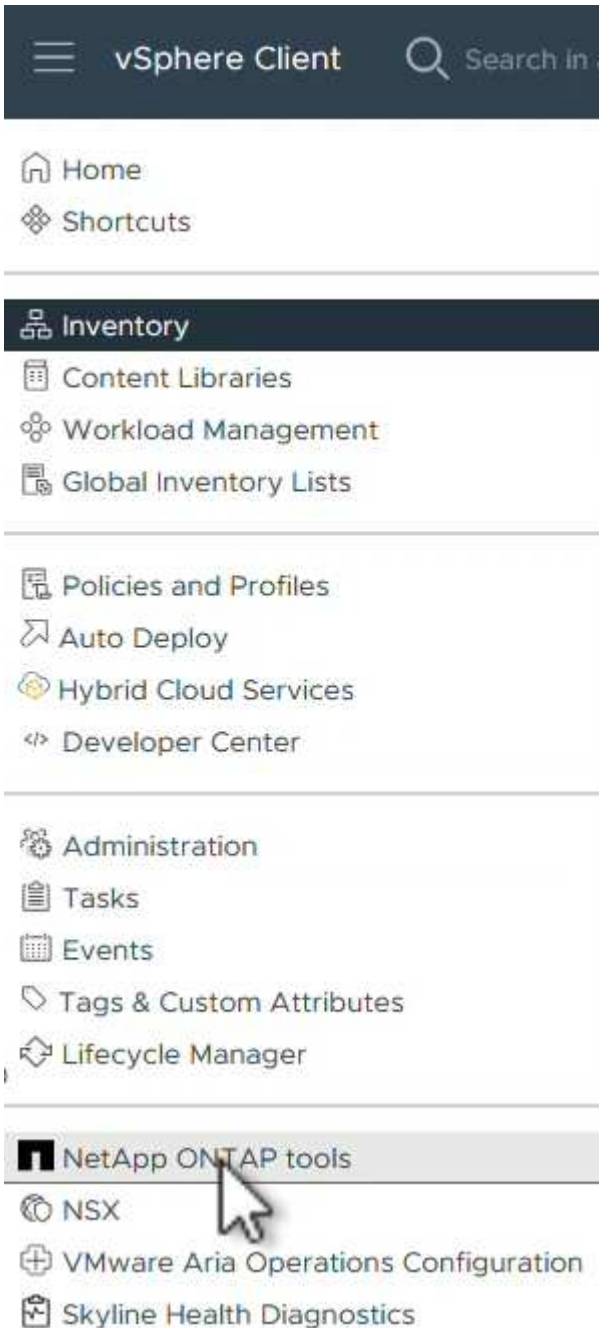
CANCELBACKNEXT

8. Finally, click on **Next** to continue and then on then on **Finish** to begin the deployment.

Configure ONTAP tools

Once the ONTAP tools VM is installed and powered up, there will be some basic configuration required such as adding vCenter servers and ONTAP storage systems to manage. Refer to the documentation at [ONTAP tools for VMware vSphere documentation](#) for detailed information.

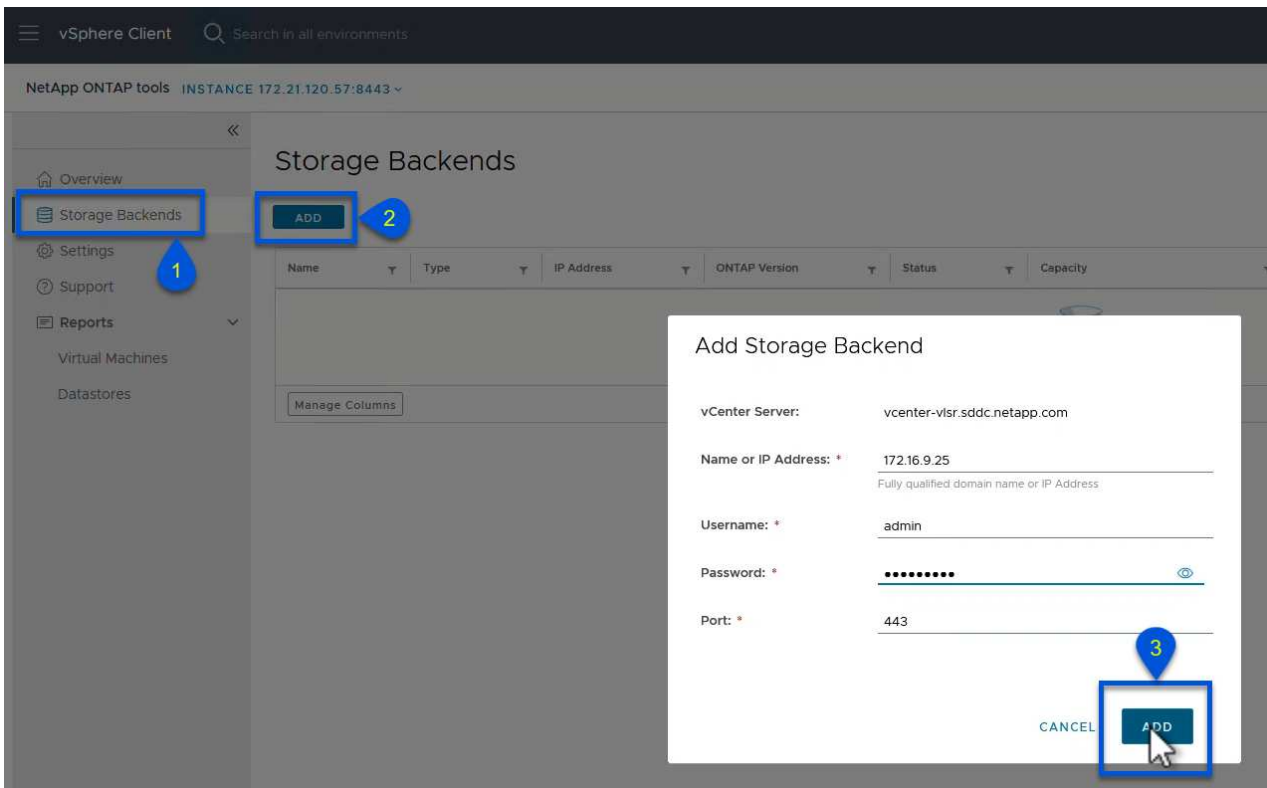
1. Refer to [Add vCenter instances](#) to configure the vCenter instances to be managed with ONTAP tools.
2. To add an ONTAP storage system, log into the vSphere client and navigate to the main menu on the left. Click on **NetApp ONTAP tools** to launch user interface.



3. Navigate to **Storage Backends** in the left hand menu and click on **Add** to access the **Add Storage**

Backend window.

4. Fill out the IP address and credentials for the ONTAP storage system to be managed. Click on **Add** to finish.



Here, the storage backend is added in the vSphere client UI using the cluster IP address. This allows full management over all SVMs in the storage system. Alternately, the storage backend can be added and associated with a vCenter instance using ONTAP tools Manager at <https://loadBalanceIP:8443/virtualization/ui/>. With this method only SVM credentials can be added at the vSphere client UI, providing more granular control over storage access.

Provision FC datastore with ONTAP tools

ONTAP tools integrates functionality throughout the vSphere client UI. In this step an FC datastore will be provisioned from the hosts inventory page.

1. In the vSphere client, navigate to the hosts (or storage) inventory.
2. Navigate to **ACTIONS > NetApp ONTAP tools > Create datastore**.

The screenshot shows the vSphere Client interface. The left sidebar displays the inventory tree with 'vcsa-vcf.sddc.netapp.com' expanded, showing a 'Datacenter' and a 'New Cluster'. The main pane shows the 'New Cluster' page with tabs for 'Summary' and 'Monitor'. The 'Summary' tab is active, displaying 'Capacity and Usage' (CPU, Memory, Storage) and 'Cluster Consumers' (Resource pools, vApps, Virtual machines). The 'ACTIONS' menu is open, showing options like 'Add Hosts...', 'New Virtual Machine...', 'New Resource Pool...', 'Deploy OVF Template...', 'New vApp...', 'Import VMs', 'Storage', 'Host Profiles', 'Edit Default VM Compatibility...', 'Assign vSAN Cluster License...', 'Settings', 'Move To...', 'Rename...', 'Tags & Custom Attributes', 'Add Permission...', 'Alarms', 'Remove from Inventory', 'Delete', 'vSAN', and 'NetApp ONTAP tools'. The 'NetApp ONTAP tools' option is highlighted, and its sub-menu is open, showing 'Create datastore', 'Mount datastore', 'Protect cluster', and 'Update hosts data'. A hand cursor is pointing at 'Create datastore'. The bottom pane shows a table of 'Recent Tasks'.

Task Name	Target	Status	Details	Initiated By	Queue For
ONTAP tools Discover hosts	vcsa-vcf.sddc.netapp.com	Completed	Discover hosts initiated with job id 137	VSAN	13 m
ONTAP tools Discover hosts	vcsa-vcf.sddc.netapp.com	Completed	Discover hosts initiated with job id 136	VSAN	13 m
ONTAP tools Discover hosts	vcsa-vcf.sddc.netapp.com	Completed	Discover hosts initiated with job id 135	VSPHERE.LOCAL\Administrator	8 m

3. In the **Create Datastore** wizard, select VMFS for the type of datastore to create.

Create datastore

- Type
- Name and protocol
- Storage
- Storage attributes
- Summary

Type

Destination:

New Cluster

Datastore type:

☐ NFS

☒ VMFS

☐ vVols

CANCEL

NEXT

4. On the **Name and Protocol** page, fill in a name for the datastore, the size, and the FC protocol to be used.

Create datastore

- Type
- Name and protocol
- Storage
- Storage attributes
- Summary

Name and protocol

Datastore name:

DS01FC

Size:

2 TB

Minimum supported size is 2 GB.

Protocol:

FC

Advanced options

CANCEL

BACK

NEXT

5. On the **Storage** page, select the ONTAP storage platform and the storage virtual machine (SVM). You can also select any available custom export policies here. Click on **Next** to continue.

Create datastore

1 Type

2 Name and protocol

3 Storage

4 Storage attributes

5 Summary

Storage

Choose a storage VM where the datastore will be created.

	Storage VM name	Tier	Platform type	QoS configured
<input type="radio"/>	HCG-NetApp-A400-E9U1 / proxmox	Performance	ASA	No
<input checked="" type="radio"/>	HCG-NetApp-A400-E9U1 / sddc_fc	Performance	ASA	No
<input type="radio"/>	HCG-NetApp-A400-E9U1 / vcf_az1	Performance	ASA	No
<input type="radio"/>	HCG-NetApp-C250-E9U7 / svm0_c250	Capacity	AFF	No

Manage Columns

4 Storage VMs

Advanced options

CANCEL

BACK

NEXT

- On the **Storage Attributes** page select the storage aggregate to be used. Click on **Next** to continue.
- On the **Summary** page, review the information and click on **Finish** to begin the provisioning process. ONTAP tools will create a volume on the ONTAP storage system and mount it as an FC datastore to all ESXi hosts in the cluster.

Create datastore

1 Type

2 Name and protocol

3 Storage

4 Storage attributes

5 Summary

Summary

A new datastore will be created with these settings.

Type

Destination:

New Cluster

Datastore type:

VMFS

Name and protocol

Datastore name:

DS01FC

Size:

2 TB

Protocol:

FC

Storage

Storage VM:

HCG-NetApp-A400-E9U1 / sddc_fc

Storage attributes

CANCEL

BACK

FINISH

Convert vSphere environment to VCF 5.2

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 Tools 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 Precheck on the Target vCenter Before Conversion](#) to run the validation.
2. The following output shows that the vCenter appliance has passed the precheck.

```
root@localhost: /tmp/vcfimport/vcf-brownfield-toolset # python3 vcf_brownfield.py precheck --vcenter 172.21.166.57 --sso-user administrator@vsphere.local
[2024-10-23 19:03:23,609] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.0-24307788
Enter vCenter SSO password:
[2024-10-23 19:03:28,825] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2024-10-23 19:03:28,938] [INFO] vc_precheck: Connected to vCenter 172.21.166.57 in 0.11 seconds
[2024-10-23 19:03:28,939] [INFO] vc_precheck: Running pre-checks for vCenter 172.21.166.57...
[2024-10-23 19:03:28,939] [INFO] vc_precheck: [1/10] VC BOM version check... PASS
[2024-10-23 19:03:28,975] [INFO] vc_precheck: [2/10] vSAN stretched cluster check... PASS
[2024-10-23 19:03:28,999] [INFO] vc_precheck: [3/10] Supported storage available check... PASS
[2024-10-23 19:03:29,020] [INFO] vc_precheck: [4/10] vCenter VM location check... PASS
[2024-10-23 19:03:29,233] [INFO] vc_precheck: [5/10] VxRail registration check... PASS
[2024-10-23 19:03:29,414] [INFO] vc_precheck: [6/10] NSX-T registration check... PASS
[2024-10-23 19:03:29,437] [INFO] vc_precheck: [7/10] Standalone host check... PASS
[2024-10-23 19:03:31,870] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check... PASS
[2024-10-23 19:03:32,962] [INFO] vc_precheck: [9/10] ELM ring topology check... PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: [10/10] WCP import check... PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: All pre-checks passed!
[2024-10-23 19:03:33,383] [INFO] vc_precheck: Pre-checks for vCenter 172.21.166.57 completed in 4.44 seconds
root@localhost: /tmp/vcfimport/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.

Refer to [Deploy the SDDC Manager Appliance on the Target vCenter](#).

For more information see [Commission Hosts](#) in the VCF Administration Guide.

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.

For complete information, refer to [Generate an NSX Deployment Specification for Converting or Importing Existing vSphere Environments](#).



When deploying an NSX Manager cluster in a convert or import operation, NSX-VLAN networking is utilized. For details on the limitations of NSX-VLAN networking, 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:

```
{
  "license_key": "xxxxx-xxxxx-xxxxx-xxxxx-xxxxx",
  "form_factor": "medium",
  "admin_password": "*****",
  "install_bundle_path": "/tmp/vcfimport/bundle-133764.zip",
  "cluster_ip": "172.21.166.72",
  "cluster_fqdn": "vcf-m02-nsx01.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "vcf-m02-nsx01a.sddc.netapp.com",
    "name": "vcf-m02-nsx01a",
    "ip_address": "172.21.166.73",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01b.sddc.netapp.com",
    "name": "vcf-m02-nsx01b",
    "ip_address": "172.21.166.74",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01c.sddc.netapp.com",
    "name": "vcf-m02-nsx01c",
    "ip_address": "172.21.166.75",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  }
]
```


Copy the JSON file to a directory on the SDDC Manager.

Upload software to SDDC Manager

Copy the VCF Import Tool and the NSX deployment bundle to /home/vcf/vcfimport directory on the SDDC Manager.

See [Upload the Required Software to the SDDC Manager Appliance](#) for detailed instructions.

Convert vSphere cluster to VCF management domain

The VCF Import Tool is used to conduct the conversion process.

Run the following command from the /home/vcf/vcf-import-package/vcf-brownfield-import-<version>/vcf-brownfield-toolset directory, to review a printout of VCF import tool functions:

```
python3 vcf_brownfield.py --help
```

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>' --domain-name '<wld-domain-name>' --nsx-deployment-spec -path '<nsx-deployment-json-spec-path>'
```

For complete instructions, refer to [Convert or Import the vSphere Environment into the SDDC Manager Inventory](#).

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.

Video demo for ONTAP tools for VMware vSphere 10

[NFS datastore with ONTAP tools for VMware vSphere 10](#)

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 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 (prior 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 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 traffic
- 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.

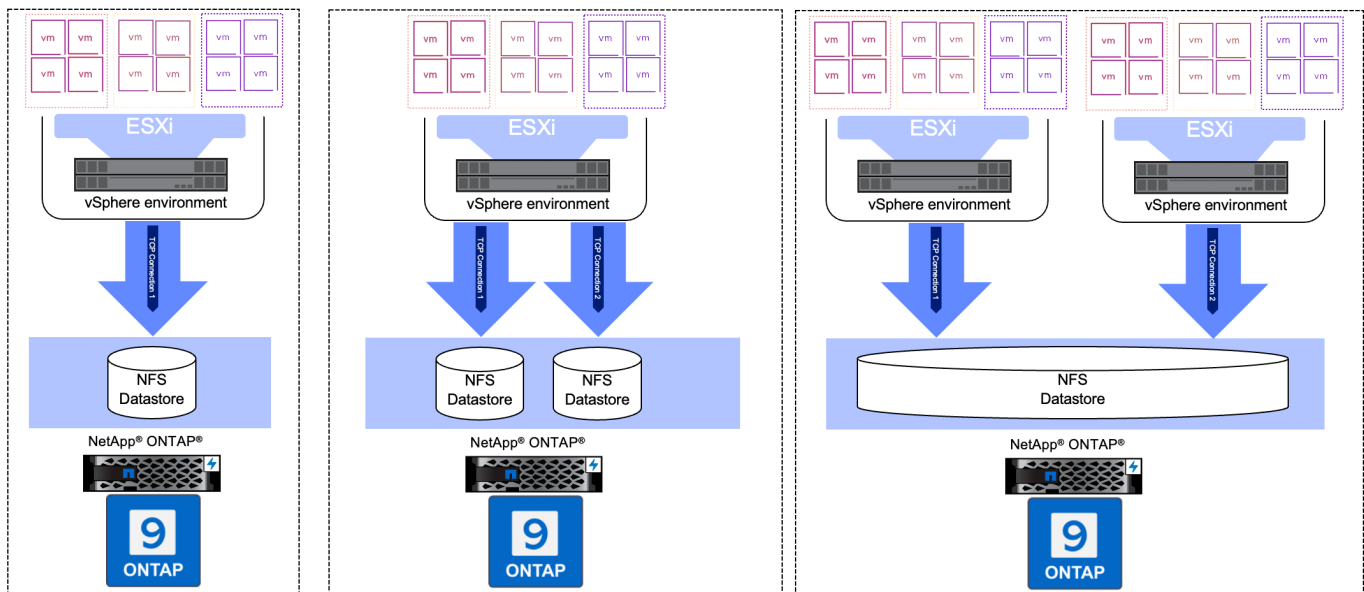


When deploying a VI Workload Domain, VCF validates connectivity to the NFS Server. This is done using the management adapter on the ESXi hosts before any additional vmkernel adapter is added with the NFS IP address. Therefore, it is necessary to ensure that either 1) the management network is routable 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.

The screenshot shows the ONTAP System Manager interface. On the left is a navigation menu with sections: DASHBOARD, INSIGHTS, STORAGE (expanded), and NETWORK. Under STORAGE, 'Storage VMs' is selected. The main panel is titled 'Storage VMs' and contains a table of SVMs. 'EHC_NFS' is selected and highlighted. To the right of the table, there are tabs for 'Overview', 'Settings', and 'SnapMirror (l)'. The 'Overview' tab is active, showing a 'NETWORK IP INTERFACES' section. Under this section, 'NFS' is listed with a numeric value '7' to its right. A dropdown menu is open for 'NFS', displaying a list of IP addresses. Two IP addresses are highlighted with blue boxes: '172.21.118.163' and '172.21.118.164'.

Name
EHC_ISCSI
<input checked="" type="checkbox"/> EHC_NFS
HMC_187
HMC_3510
HMC_ISCSI_3510
infra_svm_a300
JS_EHC_ISCSI
QTVtest
svm0
Temp_3510_N1
zoneb

Overview Settings SnapMirror (l)

NETWORK IP INTERFACES

NFS 7

172.21.253.117

172.21.253.118

172.21.253.116

172.21.253.112

172.21.253.113

172.21.118.163

172.21.118.164

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

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

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

```
vmkping <IP Address>
```

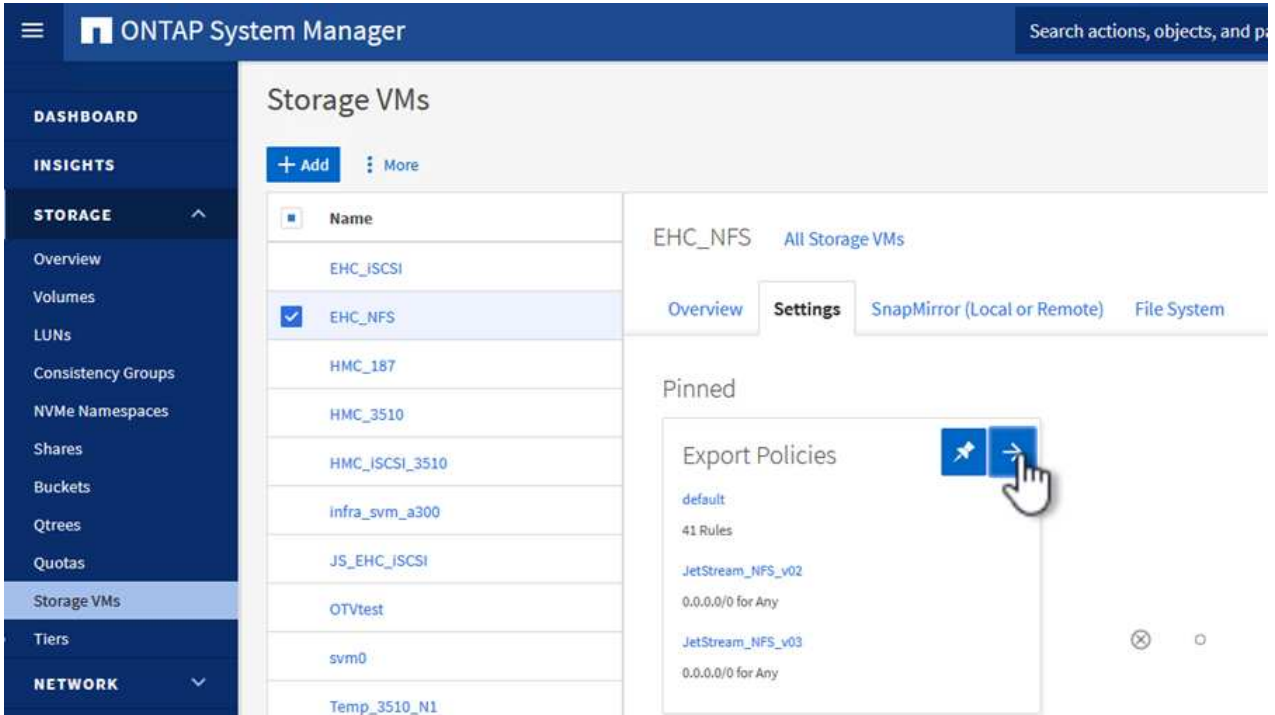



When deploying a VI Workload Domain, VCF validates connectivity to the NFS Server. This is done using the management adapter on the ESXi hosts before any additional vmkernel adapter is added with the NFS IP address. Therefore, it is necessary to ensure that either 1) the management network is routable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

Create Export Policy for sharing NFS volume

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

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



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

New export policy

NAME

WKLD_DM01

☒ Copy rules from existing policy

STORAGE VM

svm0

EXPORT POLICY

default

RULES

No data

+ Add



Add New Rules

Save

Cancel

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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All (As anonymous user) 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5p	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NTLM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel

Save



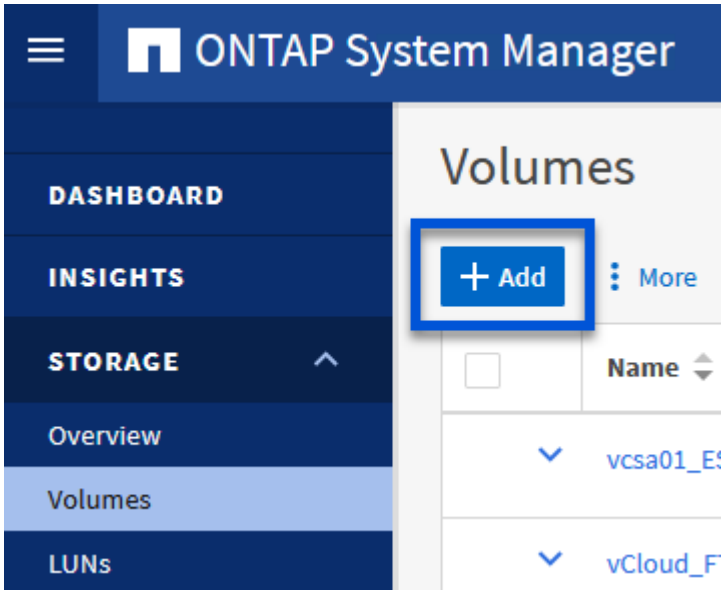
When deploying a VI Workload Domain, VCF validates connectivity to the NFS Server. This is done using the management adapter on the ESXi hosts before any additional vmkernel adapter is added with the NFS IP address. Therefore, it is necessary to ensure that the export policy includes the VCF management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

- Once all rules have been entered click on the **Save** button to save the new Export Policy.
- 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

More Options

Cancel


Save

- 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



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, 172.21.252.208

+



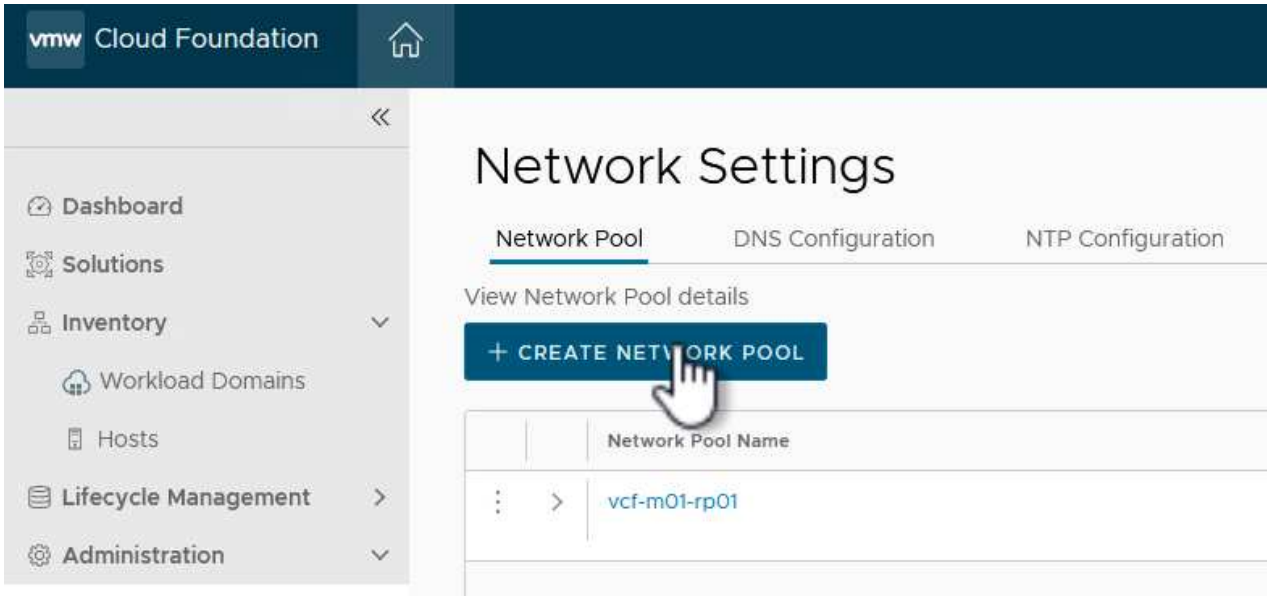
When deploying a VI Workload Domain, VCF validates connectivity to the NFS Server. This is done using the management adapter on the ESXi hosts before any additional vmkernel adapter is added with the NFS IP address. Therefore, it is necessary to ensure that either 1) the management network is routable 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

A Network 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.

vmw Cloud Foundation

Dashboard

Solutions

Inventory

Workload Domains

Hosts

Lifecycle Management

Administration

Network Settings

Storage Settings

Licensing

Single Sign On

Proxy Settings

Online Depot

Composable Infrastructure

VMware Aria Suite

Backup

VMware CEP

Security

Password Management

Certificate Authority

Developer Center

Network Settings

Network Pool

DNS Configuration

NTP Configuration

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

CANCEL

SAVE

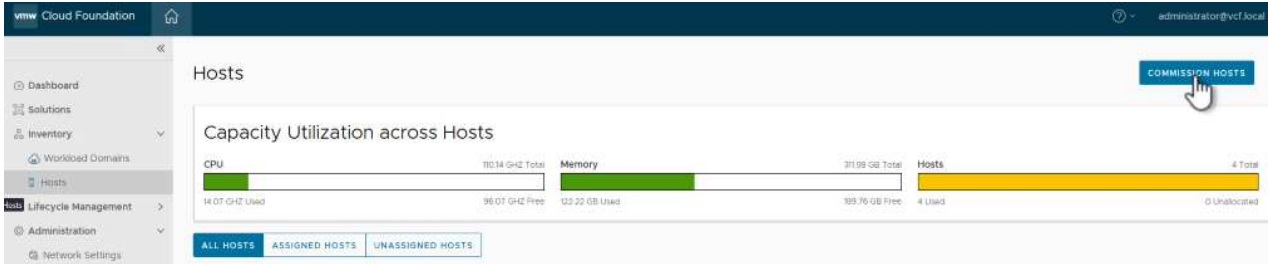
3. Click the **Save** button to complete creating the Network Pool.

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).

CANCEL

PROCEED

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

Storage Type ☐ vSAN ☒ NFS ☐ VMFS on FC ☐ vVol

Network Pool Name ⓘ

User Name

Password ⓘ

ADD

Hosts Added

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

REMOVE

☐ Confirm all Finger Prints ⓘ

VALIDATE ALL

<input checked="" type="checkbox"/>	FQDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status ⓘ
<input checked="" type="checkbox"/>	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01 ⓘ	172.21.166.135	<input checked="" type="checkbox"/> SHA256:CKbsinf EOG+Hz/ lpFUoFDI2tLuY FZ47WicVdp6v EQM	⊖ Not Validated

1 hosts

CANCEL

NEXT

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

Hosts Added

✓ Host Validated Successfully.

REMOVE



Confirm all Finger Prints



VALIDATE ALL

<input checked="" type="checkbox"/>	FQDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
<input checked="" type="checkbox"/>	vcf-wkld-esx04.sddc.netapp.com	NFS_NP01	172.21.166.138	✓ SHA256:9Kg+9 nQaE4SQkOMs QPON/ k5gZB9zyKN+6 CBPmXsvLBc	✓ Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx03.sddc.netapp.com	NFS_NP01	172.21.166.137	✓ SHA256:nPX4/ mei/ 2zmLJHfmPwbk 6zhapoUxV2IO wZDPFH+zo	✓ Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx02.sddc.netapp.com	NFS_NP01	172.21.166.136	✓ SHA256:AMhyR 60OpTQ1YYq0 DJhqVbj/M/ GvrQaqUy7Ce+ M4IWY	✓ Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01	172.21.166.135	✓ SHA256:CKbsinf EOG+!+z/ lpFUoFDI2tLuY FZ47WicVDp6v EQM	✓ Valid

CANCEL

NEXT

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



Commission Hosts

1 Host Addition and Validation

2 **Review**

Review

Skip failed hosts during commissioning ⓘ ☒ On

Validated Host(s)

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

CANCEL

BACK

COMMISSION

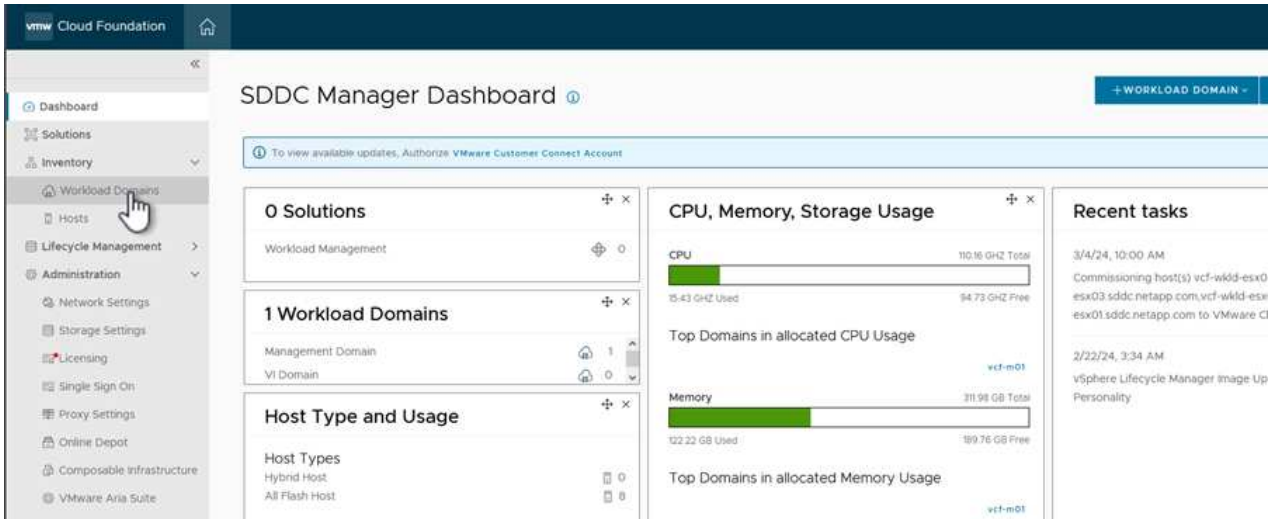


Deploy VI Workload Domain

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

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

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



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

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

+

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.

VI Configuration

- 1 General Info
- 2 Cluster
- 3 Compute
- 4 Networking
- 5 Host Selection
- 6 NFS Storage**

NFS Storage

NFS Share Details

Datastore Name ⓘ	VCF_WKLD_01
Folder ⓘ	/VCF_WKLD_01
NFS Server IP Address ⓘ	172.21.118.163

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

VI Configuration

- General Info
- Cluster
- Compute
- Networking
- Host Selection
- NFS Storage
- Switch Configuration
- License
- Review**

Review

General	
Virtual Infrastructure Name	vcf-wkld-01
Organization Name	it-inf
SSO Domain Option	Joining Management SSO Domain
Cluster	
Cluster Name	IT-INF-WKLD-01
Compute	
vCenter IP Address	172.21.166.143
vCenter DNS Name	vcf-wkld-vc01.sddc.netapp.com
vCenter Subnet Mask	255.255.255.0
vCenter Default Gateway	172.21.166.1
Networking	
NSX Manager Instance Option	Creating new NSX instance
NSX Manager Cluster IP	172.21.166.147
NSX Manager Cluster FQDN	vcf-w01-nxsci01.sddc.netapp.com
NSX Manager IP Addresses	172.21.166.144, 172.21.166.145, 172.21.166.146

CANCEL
BACK
FINISH

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 simplify 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, enhancing storage performance, efficiency, and scalability within the VCF environment.

Please refer to the following solutions for the technical details to expand the VCF environment.

- [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](#)

Add an iSCSI datastore as supplemental storage for a management domain using ONTAP tools for VMware vSphere

In this use case we outline the procedure to add an iSCSI datastore as supplemental storage for a VMware Cloud Foundation (VCF) management domain. This procedure summarizes setting up a Storage Virtual Machine (SVM) with logical interfaces (LIFs) for iSCSI, configuring iSCSI networking on ESXi hosts, deploying ONTAP Tools for VMware vSphere, and creating a VMFS datastore.

Benefits of iSCSI

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: Utilizes 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](#).

Scenario Overview

This scenario covers the following high level steps:

- Create a storage virtual machine (SVM) with logical interfaces (LIFs) for iSCSI traffic.

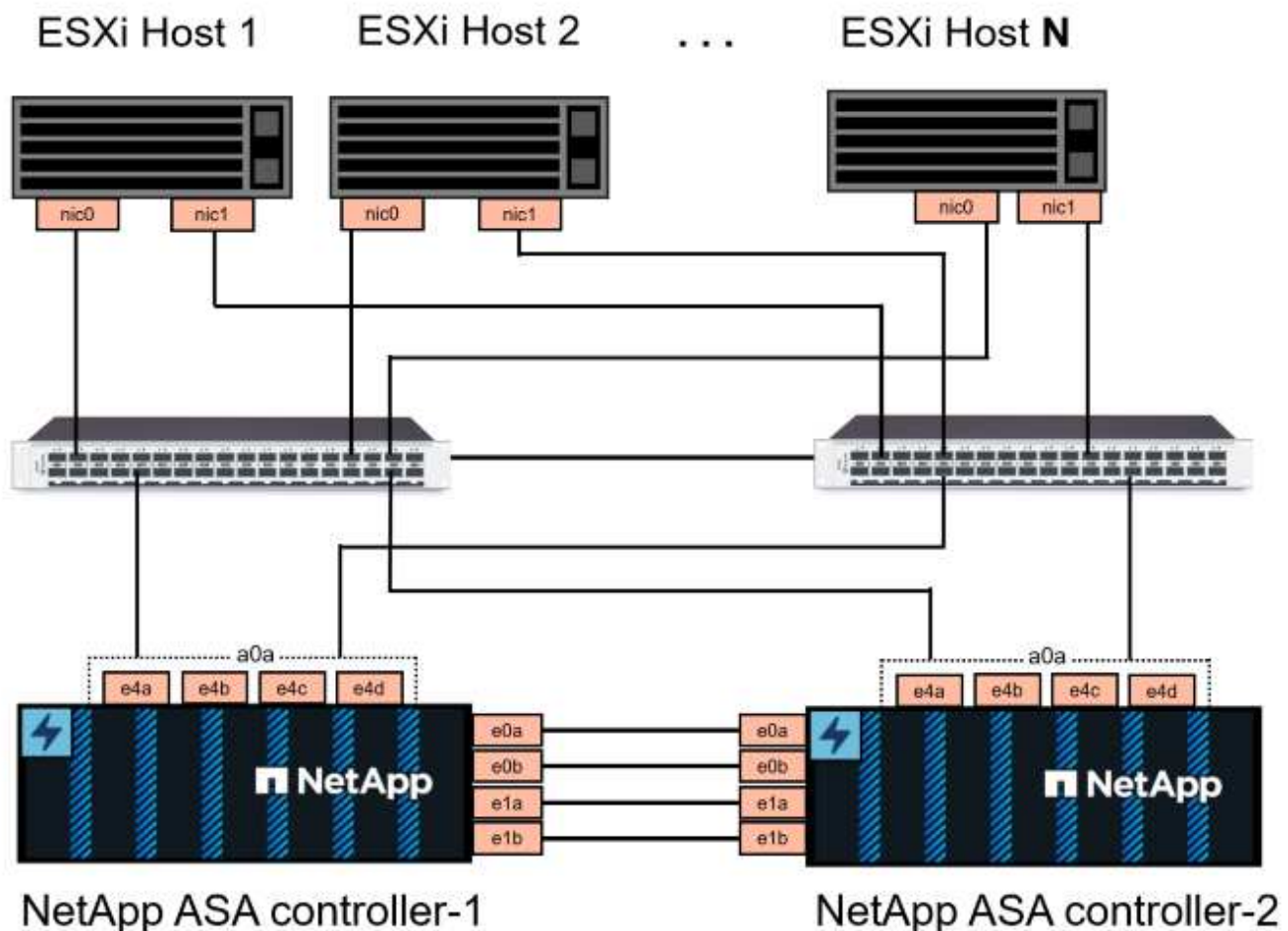
- Create distributed port groups for iSCSI networks on the VCF management domain.
- Create vmkernel adapters for iSCSI on the ESXi hosts for the VCF management domain.
- Deploy ONTAP Tools on the VCF management domain.
- Create a new VMFS datastore on the VCF management domain.

Prerequisites

This scenario requires the following components and configurations:

- An ONTAP 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.

NetApp recommends fully redundant network designs for iSCSI. The following diagram illustrates an example of a redundant configuration, providing fault tolerance for storage systems, switches, networks adapters and host systems. Refer to the NetApp [SAN configuration reference](#) for additional information.



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

This documentation demonstrates the process of creating a new SVM and specifying the IP address

information to create multiple LIFs for iSCSI traffic. To add new LIFs to an existing SVM refer to [Create a LIF \(network interface\)](#).

For additional information on using VMFS iSCSI datastores with VMware refer to [vSphere VMFS Datastore - iSCSI Storage backend with ONTAP](#).



In situations where multiple VMkernel adapters are configured on the same IP network, it is recommended to use software iSCSI port binding on the ESXi hosts to ensure that load balancing across the adapters occurs. Refer to KB article [Considerations for using software iSCSI port binding in ESX/ESXi \(2038869\)](#).

Deployment Steps

To deploy ONTAP Tools and use it to create a VMFS datastore on the VCF management domain, complete the following steps:

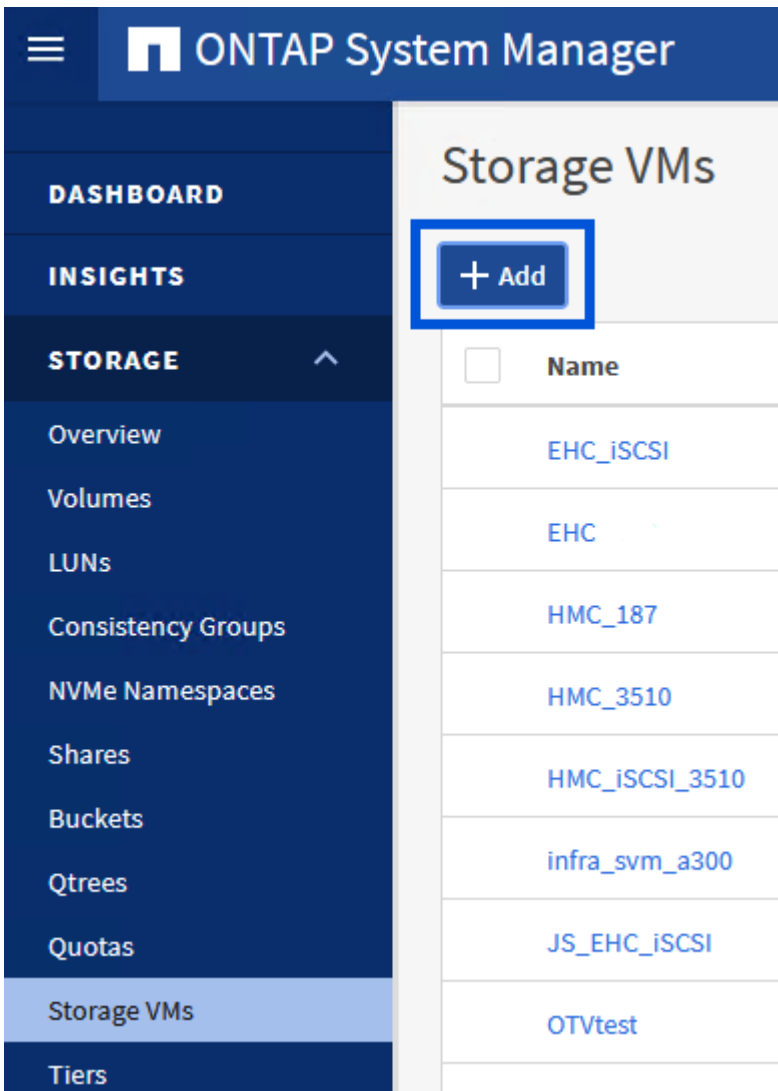
Create SVM and LIFs on ONTAP storage system

The following step is performed in ONTAP System Manager.

Create the storage VM and LIFs

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

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



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

Add Storage VM



STORAGE VM NAME

SVM_ISCSI

IPSPACE

Default



Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe



Enable iSCSI

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



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

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.179

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS_iSCSI



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

IP ADDRESS

172.21.119.179

PORT

a0a-3375



ntaphci-a300-02

IP ADDRESS

172.21.118.180

PORT

a0a-3374



IP ADDRESS

172.21.119.180

PORT

a0a-3375



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

Storage VM Administration

☐

Manage administrator account

Save

Cancel

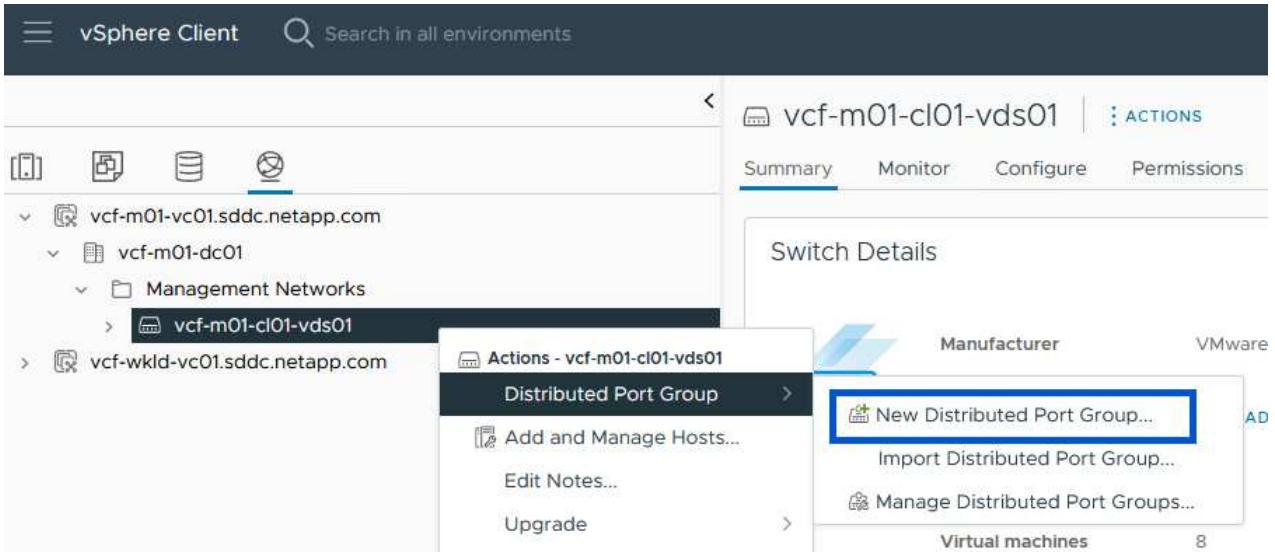
Set up networking for iSCSI on ESXi hosts

The following steps are performed on the VCF management domain cluster using the vSphere client.

Create Distributed Port Groups for iSCSI traffic

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

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



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

New Distributed Port Group

- 1 Name and location
- 2 **Configure settings**
- 3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding

Static binding

Port allocation

Elastic ⓘ

Number of ports

8

Network resource pool

(default)

VLAN

VLAN type

VLAN

VLAN ID

3374

Advanced

☐ Customize default policies configuration

CANCEL

BACK

NEXT

- On the **Ready to complete** page, review the changes and click on **Finish** to create the new distributed port group.
- 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**.
- Once both port groups have been created, navigate to the first port group and select the action to **Edit settings....**

vSphere Client

Search in all environments

vcf-m01-cl01-vds01-pg-iscsi-a

ACTIONS

Summary

Monitor

Configure

Permissions

Ports

Distributed Port Group Details

Port binding

Static binding

Port allocation

Elastic

VLAN ID

3374

Distributed switch

vcf-m01-cl01-vds01

Network protocol profile

--

Network resource pool

--

Hosts

4

vcf-m01-vc01.sddc.netapp.com

vcf-m01-dc01

Management Networks

vcf-m01-cl01-vds01

SDDC-DPortGroup-VM-Mgmt

vcf-m01-cl01-vds-DVUplinks-19

vcf-m01-cl01-vds01-pg-iscsi-a

vcf-m01-cl01-vds01

vcf-m01-cl01-vds01

vcf-m01-cl01-vds01

vcf-m01-cl01-vds01

vcf-wkld-vc01.sddc.netapp.com

Actions - vcf-m01-cl01-vds01-pg-iscsi-a

Edit Settings...

Export Configuration...

Restore Configuration...

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

Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-a ×

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual port ▼

Network failure detection

Link status only ▼

Notify switches

Yes ▼

Failback

Yes ▼

Failover order ⓘ

MOVE UP

MOVE DOWN

Active uplinks

uplink1

Standby uplinks

Unused uplinks

uplink2

CANCEL

OK

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

Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-b

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual port ▾

Network failure detection

Link status only ▾

Notify switches

Yes ▾

Failback

Yes ▾

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink2

Standby uplinks

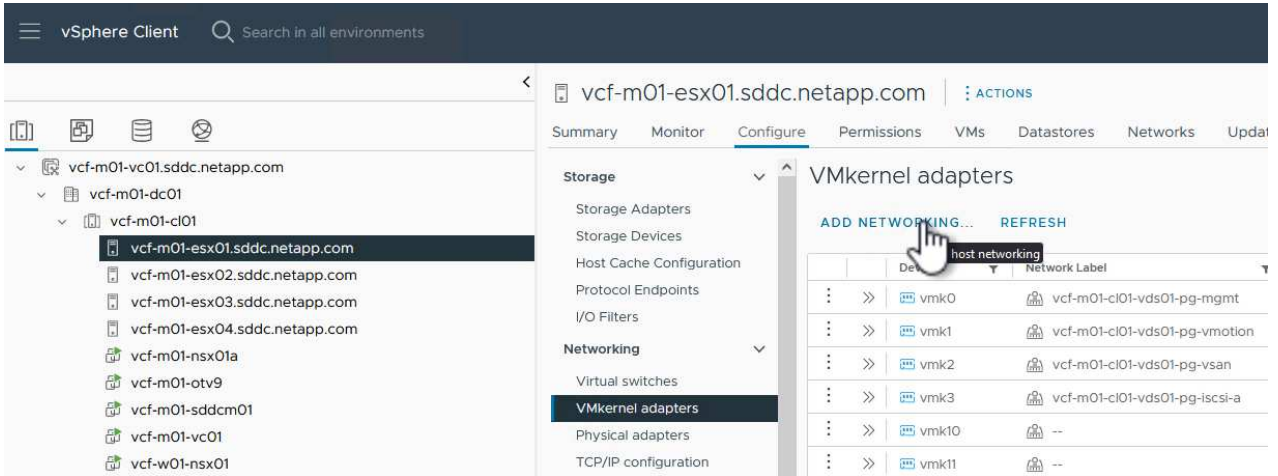
Unused uplinks

uplink1

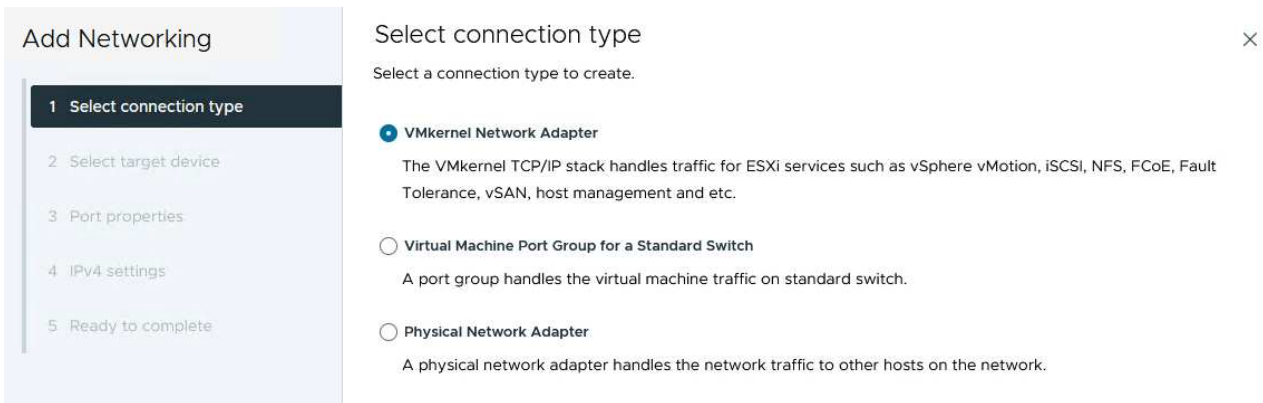
Create VMkernel adapters on each ESXi host

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

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



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



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

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

Select an existing network

Select an existing standard switch

New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	SDDC-DPortGroup-VM-Mgmt	--	vcf-m01-cl01-vds01
<input checked="" type="radio"/>	vcf-m01-cl01-vds01-pg-iscsi-a	--	vcf-m01-cl01-vds01
<input type="radio"/>	vcf-m01-cl01-vds01-pg-iscsi-b	--	vcf-m01-cl01-vds01
<input type="radio"/>	vcf-m01-cl01-vds01-pg-mgmt	--	vcf-m01-cl01-vds01
<input type="radio"/>	vcf-m01-cl01-vds01-pg-vmotion	--	vcf-m01-cl01-vds01
<input type="radio"/>	vcf-m01-cl01-vds01-pg-vsan	--	vcf-m01-cl01-vds01

Manage Columns

6 items

CANCEL

BACK

NEXT

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

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label

vcf-m01-cl01-vds01-pg-iscsi-a (vcf-m01-cl01-vds01)

MTU

Get MTU from switch

9000

TCP/IP stack

Default

Available services

Enabled services

☒ vMotion

☐ Provisioning

☐ Fault Tolerance logging

☐ Management

☐ vSphere Replication

☐ vSphere Replication NFC

☐ vSAN

☐ vSAN Witness

☐ vSphere Backup NFC

☐ NVMe over TCP

☐ NVMe over RDMA

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

94

Add Networking

- Select connection type
- Select target device
- Port properties
- IPv4 settings**
- Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

☐ Obtain IPv4 settings automatically
☒ Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway ☐ Override default gateway for this adapter

DNS server addresses

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

Add Networking

- Select connection type
- Select target device
- Port properties
- IPv4 settings
- Ready to complete**

Ready to complete

Review your selections before finishing the wizard

Select target device
 Distributed port group
 Distributed switch

Port properties
 New port group
 MTU
 vMotion
 Provisioning
 Fault Tolerance logging
 Management
 vSphere Replication
 vSphere Replication NFC
 vSAN
 vSAN Witness
 vSphere Backup NFC
 NVMe over TCP
 NVMe over RDMA

IPv4 settings
 IPv4 address
 Subnet mask

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

Deploy and use ONTAP Tools to configure storage

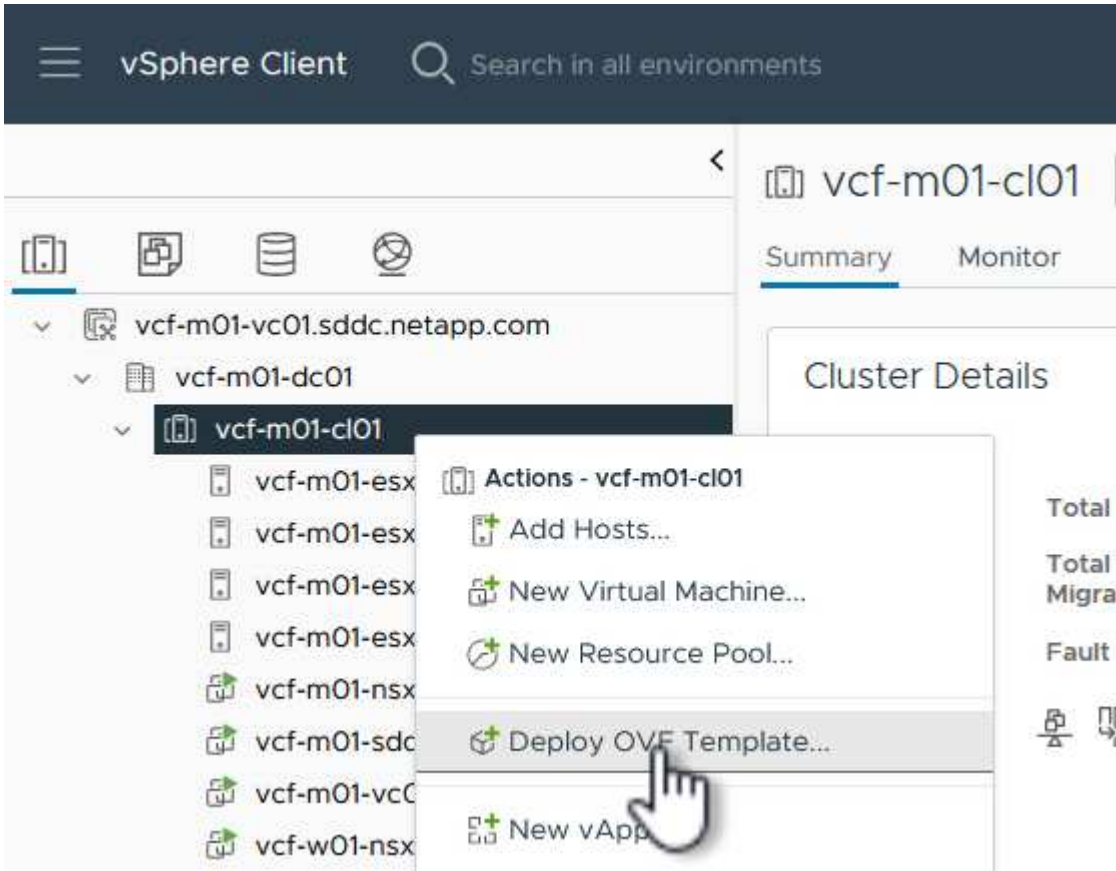
The following steps are performed on the VCF management domain cluster using the vSphere client and involve deploying OTV, creating a VMFS iSCSI datastore, and migrating management VM's to the new datastore.

Deploy ONTAP tools for VMware vSphere

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

Complete the following to Deploy ONTAP tools for VMware vSphere:

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



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

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

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

☐ URL

[http | https://remoteserver-address/filetoinstall.ovf | .ova](http://https://remoteserver-address/filetoinstall.ovf)

☒ Local file

UPLOAD FILES

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

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

Deploy OVF Template

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

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine [?](#)

Select virtual disk format

As defined in the VM storage policy

VM Storage Policy

Datastore Default

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	V
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
<input type="radio"/>	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.

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

vcf-m01-cl01-vds01-pg-vsan
SDDC-DPortGroup-VM-Mgmt
Browse ...

1 item

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

8. On the Customize template page fill out all required information:

- Password to be used for administrative access to OTV.
- NTP server IP address.
- OTV maintenance account password.
- OTV Derby DB password.
- Do not check the box to **Enable VMware Cloud Foundation (VCF)**. VCF mode is not required for deploying supplemental storage.
- FQDN or IP address of the vCenter appliance and provide credentials for vCenter.
- Provide the required network properties fields.

Click on **Next** to continue.

Deploy OVF Template

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

Customize template

Customize the deployment properties of this software solution.

2 properties have invalid values

System Configuration	4 settings
Application User Password (*)	Password to assign to the administrator account. For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.
	Password:
	Confirm Password:
NTP Servers	A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used. 172.21.166.1
Maintenance User Password (*)	Password to assign to maint user account.
	Password:
	Confirm Password:

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.

172.21.166.140

Port (*)

Specify the HTTPS port of an existing vCenter to register to.

443

Username (*)

Specify the username of an existing vCenter to register to.

administrator@vsphere.local

Password (*)

Specify the password of an existing vCenter to register to.

Password

.....

👁

Confirm Password

.....

👁

Network Properties

8 settings

Host Name

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

vcf-m01-otv9

IP Address

Specify the IP address for the appliance. (Leave blank if DHCP is

CANCEL

BACK

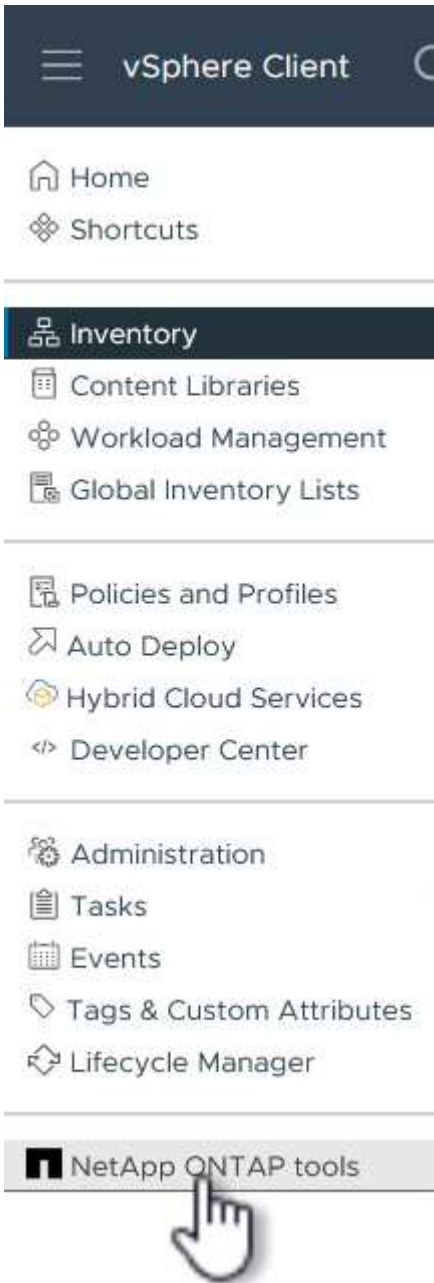
NEXT

9. Review all information on the Ready to complete page and the click Finish to begin deploying the OTV appliance.

Configure a VMFS iSCSI datastore on Management Domain using OTV

Complete the following to use OTV to configure a VMFS iSCSI datastore as supplemental storage on the management domain:

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



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

☰

vSphere Client

🔍 Search in all environments

🔄

👤 Ac

NetApp ONTAP tools INSTANCE 172.21.166.139:8443

Overview

Storage Systems

Storage capability profile

Storage Mapping

Settings

▼ Reports

Datastore Report

Virtual Machine Report

vVols Datastore Report

vVols Virtual Machine Report

Log Integrity Report

ONTAP tools for VMware vSphere

Getting StartedTraditional DashboardvVols Dashboard

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 System

Add storage systems to ONTAP tools for VMware vSphere.

ADD

🗄️+

Provision Datastore

Create traditional or vVols datastores.

PROVISION

🕒

View Dashboard

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

⚙️

Settings

Configure administrative settings such as credentials, alarm thresholds.

📄

What's new?

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

📄

Resources

- [ONTAP tools for VMware vSphere Documentation Resources](#)
- [RBAC User Creator for Data ONTAP](#)
- [ONTAP tools for VMware vSphere REST API Documentation](#)

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

Add Storage System



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

vCenter server	vcf-m01-vc01.sddc.netapp.com
Name or IP address:	172.16.9.25
Username:	admin
Password:	••••••••
Port:	443
Advanced options	>

CANCEL


SAVE & ADD MORE

ADD



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

Add Storage System

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

vCenter server

vcf-m01-vc01.sddc.netapp.com

Authorize Cluster Certificate

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

[Show certificate](#)

Do you want to trust this certificate?

NO

YES



CANCEL

SAVE & ADD MORE

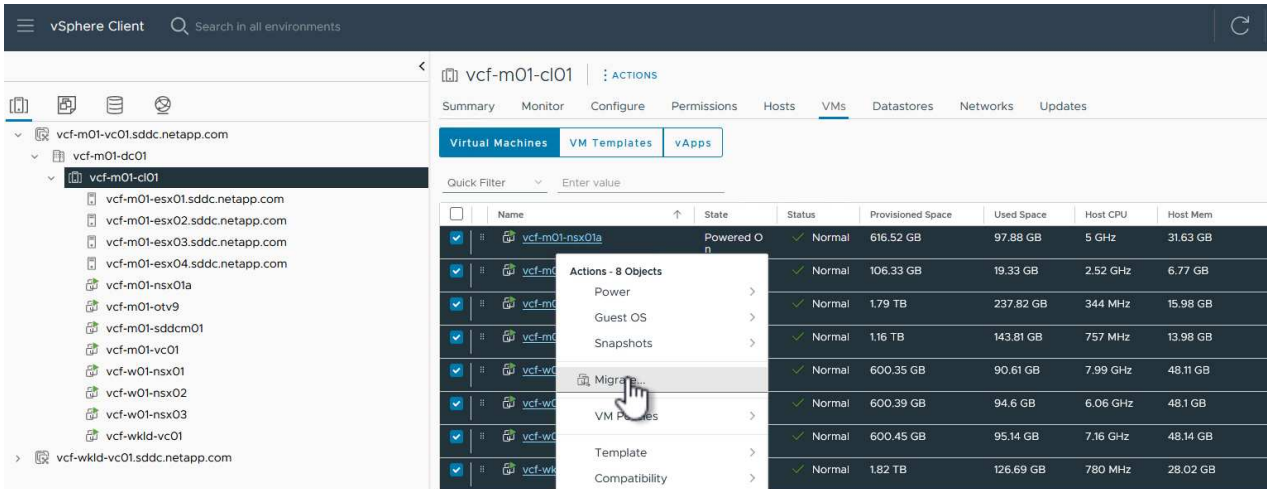
ADD

Migrate management VM's to iSCSI Datastore

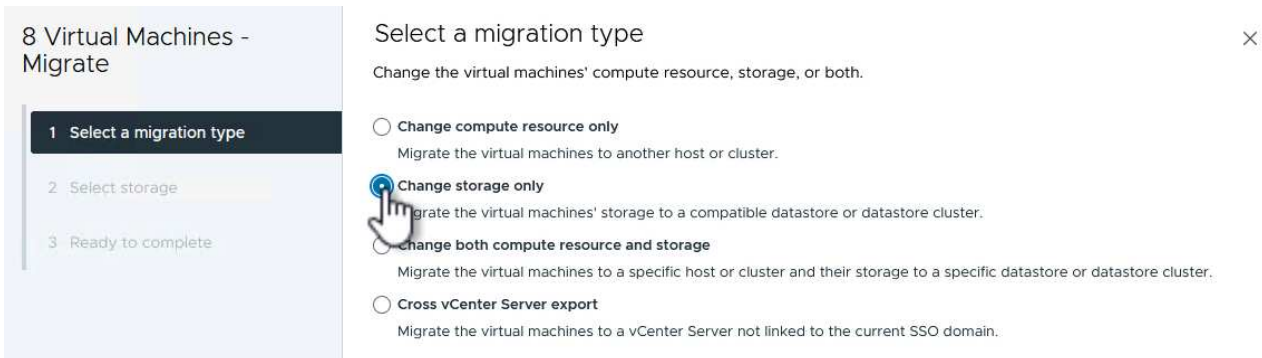
In cases where it is preferred to use ONTAP storage to protect the VCF management VM's vMotion can be used to migrate the VM's to the newly created iSCSI datastore.

Complete the following steps to migrate the VCF management VM's to the iSCSI datastore.

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



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



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

8 Virtual Machines - Migrate

1 Select a migration type

2 **Select storage**

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE

CONFIGURE PER DISK

Select virtual disk format

Same format as source

VM Storage Policy

Datastore Default

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	mgmt_01_iscsi	--	3 TB	1.46 GB	3 TB	
<input type="radio"/>	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.28 TB	52.38 GB	

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Review the selections and click on **Finish** to start the migration.

6. The relocation status can be viewed from the **Recent Tasks** pane.

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

Additional information

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

For information on configuring VCF refer to [VMware Cloud Foundation Documentation](#).

Video demo for this solution

[iSCSI Datastores as Supplemental Storage for VCF Management Domains](#)

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 the procedure to use ONTAP Tools for VMware to configure a VMFS datastore over Fiber Channel (FC) as supplemental storage for the VMware Cloud Foundation (VCF) management domain. This procedure summarizes deploying ONTAP Tools for VMware vSphere, registering vCenter servers, defining the storage backend, and provisioning the FC datastore.

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

VCF Supplemental datastore is provisioned as part of day-2 operations using vCenter. This scenario covers the following high level steps:

- Deployment of ONTAP tools on management domain
- Register VI workload vCenter servers to ONTAP tools
- Define Storage backend on ONTAP tools plugin for VMware vSphere
- Provision VMFS on FC transport

Prerequisites

This scenario requires the following components and configurations:

- 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.

NetApp recommends multipath for FC LUNs.

For complete information on configuring fibre channel on ONTAP storage systems, refer to [SAN storage management](#) in the ONTAP 9 documentation.

For more information on using VMFS with ONTAP storage systems, refer to the [Deployment Guide for VMFS](#).

Deployment Steps for management domain

To deploy ONTAP Tools and use it to create a VMFS datastore on the VCF management domain, complete the following steps:

- [Deploy ONTAP tools on management domain](#)
- [Define Storage backend using vSphere client interface](#)
- [Provision VMFS on FC](#)

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

[VMFS\(FC\) Datastore as Supplemental Storage for VCF Management Domain](#)

Add vVols as supplemental storage to VI workload domains using ONTAP tools for VMware vSphere

In this use case we outline the procedure to configure a vVols datastore with iSCSI for supplemental storage in a VMware Cloud Foundation (VCF) Virtual Infrastructure (VI) workload domain. This procedure summarizes setting up iSCSI networking, deploying ONTAP Tools for VMware vSphere, and provisioning the vVols datastore.

iSCSI is used as the storage protocol for the vVols datastore.

Benefits of iSCSI

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: Utilizes 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](#).

Scenario Overview

This scenario covers the following high level steps:

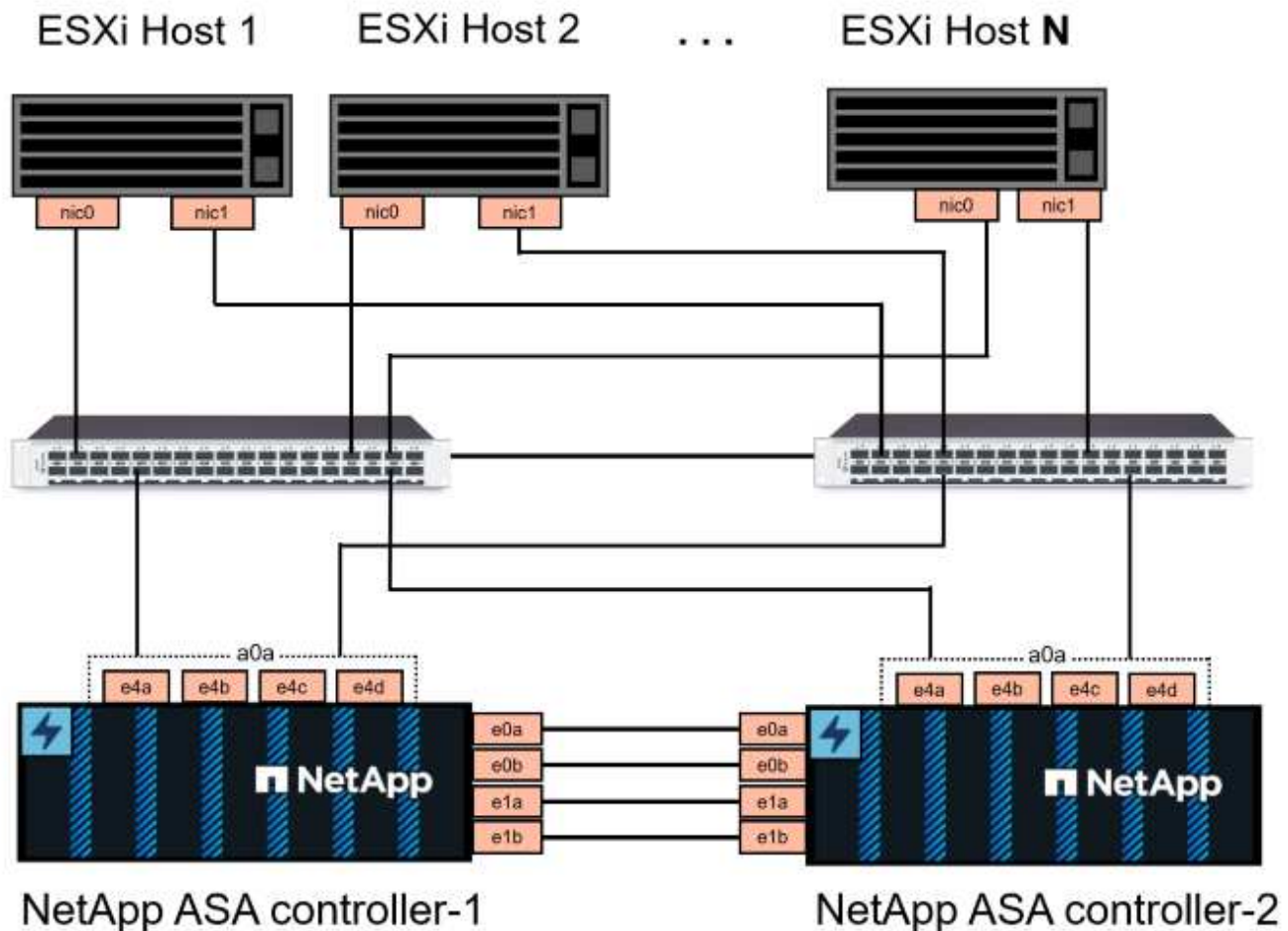
- Create a storage virtual machine (SVM) with logical interfaces (LIFs) for iSCSI traffic.
- Create distributed port groups for iSCSI networks on the VI workload domain.
- Create vmkernel adapters for iSCSI on the ESXi hosts for the VI workload domain.
- Deploy ONTAP Tools on the VI workload domain.
- Create a new vVols datastore on the VI workload domain.

Prerequisites

This scenario requires the following components and configurations:

- An ONTAP 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.

NetApp recommends fully redundant network designs for iSCSI. The following diagram illustrates an example of a redundant configuration, providing fault tolerance for storage systems, switches, networks adapters and host systems. Refer to the NetApp [SAN configuration reference](#) for additional information.



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

This documentation demonstrates the process of creating a new SVM and specifying the IP address information to create multiple LIFs for iSCSI traffic. To add new LIFs to an existing SVM refer to [Create a LIF \(network interface\)](#).



In situations where multiple VMkernel adapters are configured on the same IP network, it is recommended to use software iSCSI port binding on the ESXi hosts to ensure that load balancing across the adapters occurs. Refer to KB article [Considerations for using software iSCSI port binding in ESX/ESXi \(2038869\)](#).

For additional information on using VMFS iSCSI datastores with VMware refer to [vSphere VMFS Datastore - iSCSI Storage backend with ONTAP](#).

Deployment Steps

To deploy ONTAP Tools and use it to create a vVols datastore on the VCF management domain, complete the following steps:

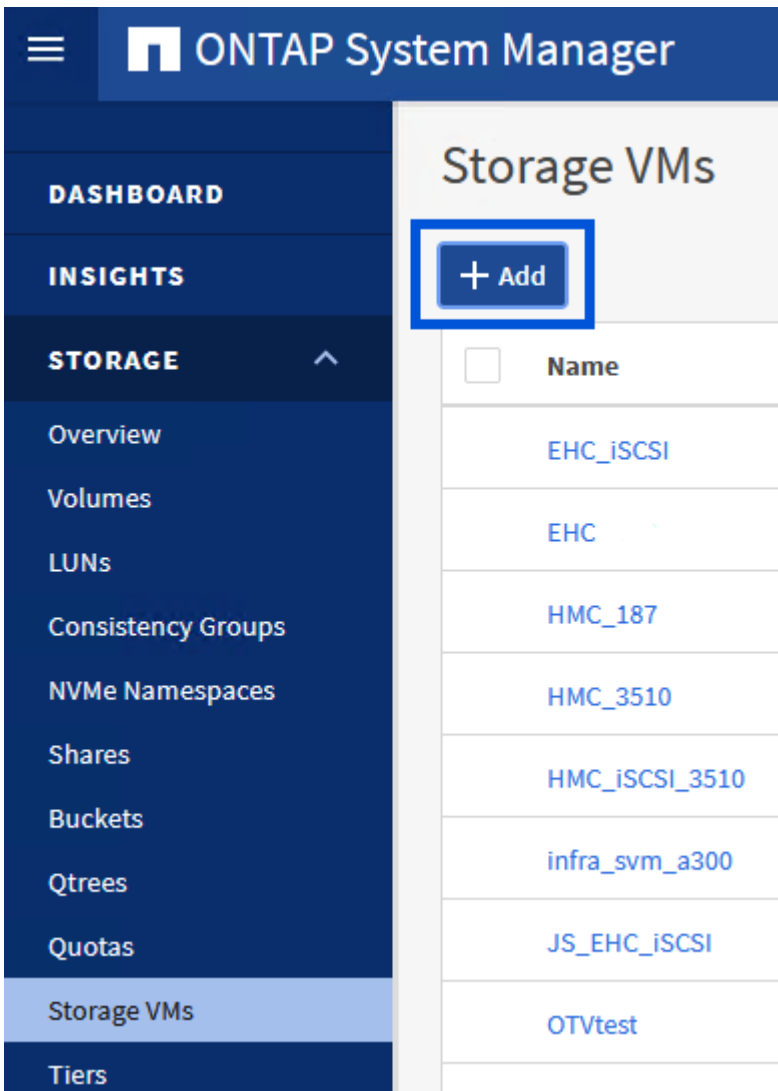
Create SVM and LIFs on ONTAP storage system

The following step is performed in ONTAP System Manager.

Create the storage VM and LIFs

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

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



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

Add Storage VM



STORAGE VM NAME

SVM_ISCSI

IPSPACE

Default



Access Protocol

SMB/CIFS, NFS, S3

✓ iSCSI

FC

NVMe

☒ Enable iSCSI

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



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

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.179

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS_iSCSI



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

IP ADDRESS

172.21.119.179

PORT

a0a-3375



ntaphci-a300-02

IP ADDRESS

172.21.118.180

PORT

a0a-3374



IP ADDRESS

172.21.119.180

PORT

a0a-3375



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

Storage VM Administration

☐

Manage administrator account

Save

Cancel

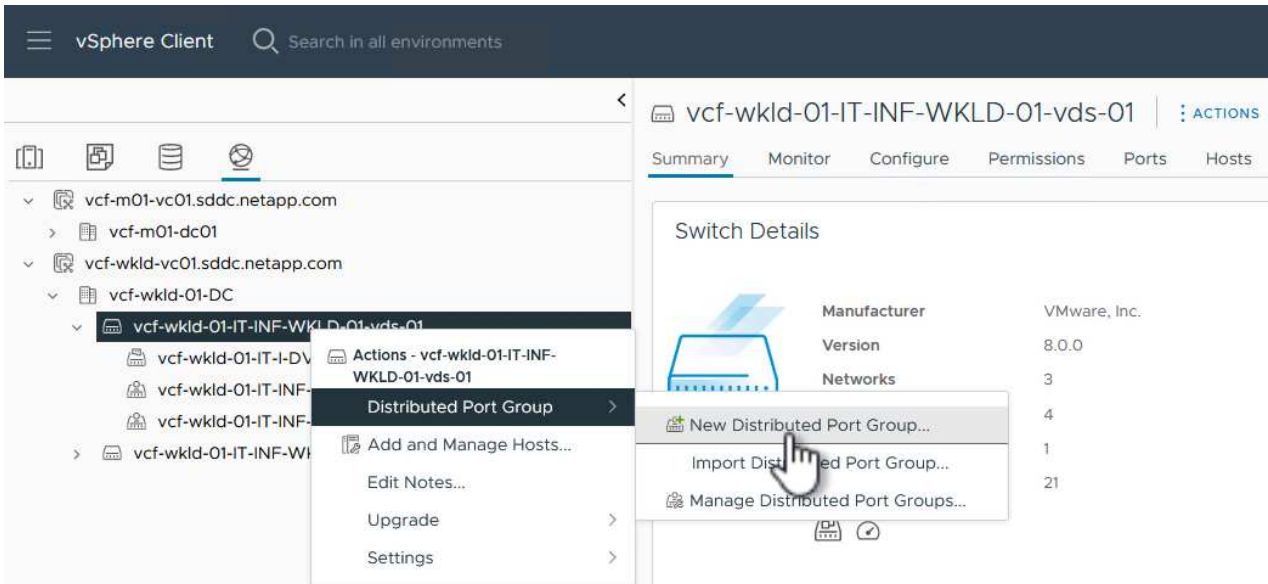
Set up networking for iSCSI on ESXi hosts

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

Create Distributed Port Groups for iSCSI traffic

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

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



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

New Distributed Port Group

- Name and location
- Configure settings**
- 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

CANCEL

BACK

NEXT

- On the **Ready to complete** page, review the changes and click on **Finish** to create the new distributed port group.
- 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**.
- Once both port groups have been created, navigate to the first port group and select the action to **Edit settings....**

vSphere Client

Search in all environments

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-iscsi-a

vcf-wkld-01-i

vcf-wkld-01-i

vcf-wkld-01-i

vcf-wkld-01-i

Actions - vcf-wkld-01-iscsi-a

Edit Settings...

Port Configuration...

vcf-wkld-01-iscsi-a

ACTIONS

Summary

Monitor

Configure

Permissions

Ports

Hosts

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

--

116

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

Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-a ×

General	Load balancing	Route based on originating virtual por ▼
Advanced	Network failure detection	Link status only ▼
VLAN	Notify switches	Yes ▼
Security	Failback	Yes ▼
Traffic shaping		
Teaming and failover		
Monitoring		
Miscellaneous		

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink1

Standby uplinks

Unused uplinks

uplink2

CANCEL OK

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

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

General	Load balancing	Route based on originating virtual por ▼
Advanced	Network failure detection	Link status only ▼
VLAN	Notify switches	Yes ▼
Security	Failback	Yes ▼
Traffic shaping		
Teaming and failover		
Monitoring		
Miscellaneous		

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink2

Standby uplinks

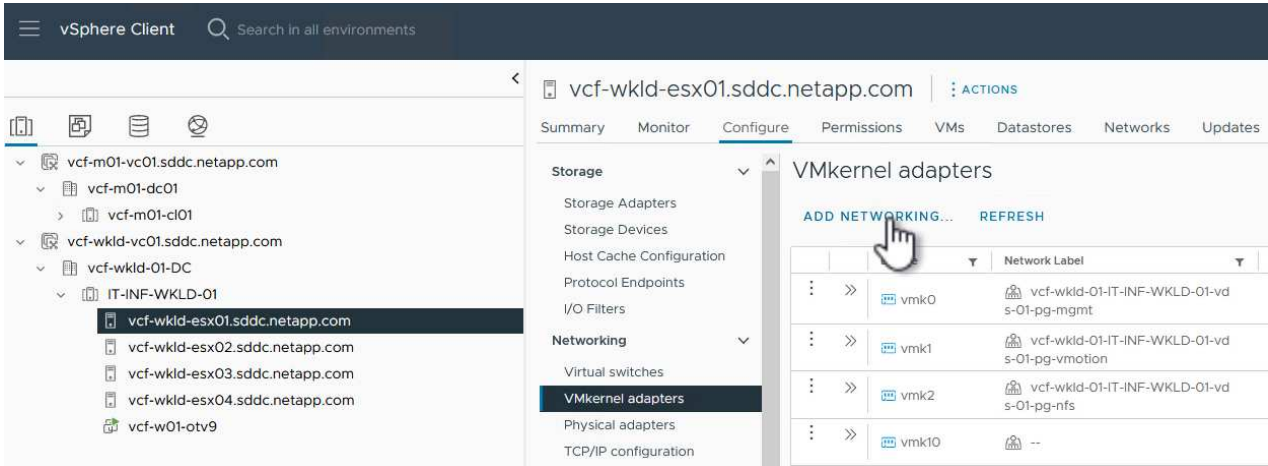
Unused uplinks

uplink1

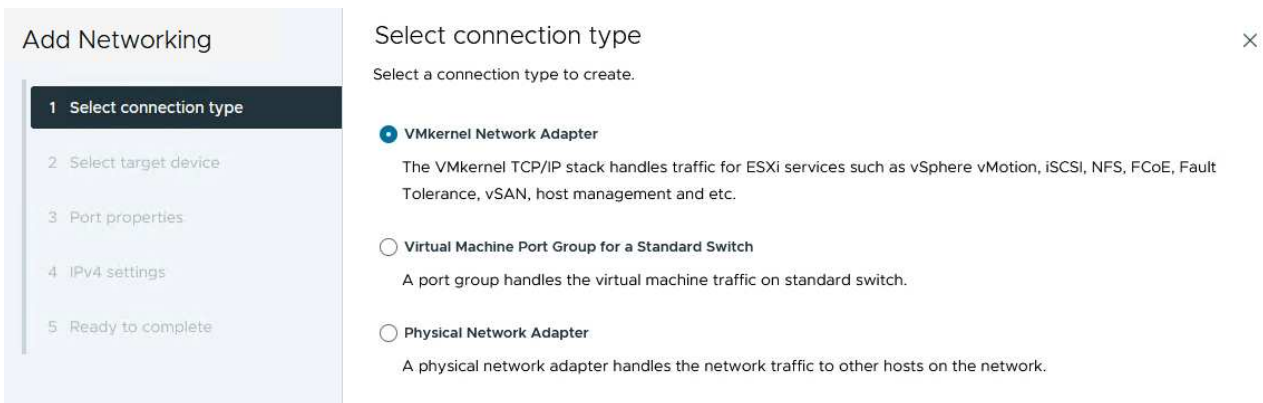
Create VMkernel adapters on each ESXi host

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

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



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



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

Add Networking

- Select connection type
- Select target device**
- Port properties
- IPv4 settings
- 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

	Name	NSX Port Group ID	Distributed Switch
<input checked="" type="radio"/>	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Manage Columns 5 items

CANCEL
BACK
NEXT

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

Add Networking

- Select connection type
- Select target device
- Port properties**
- IPv4 settings
- Ready to complete

Port properties

Specify VMkernel port settings.

Network label

MTU

TCP/IP stack

Available services

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

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

Add Networking

- Select connection type
- Select target device
- Port properties
- IPv4 settings**
- Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

☐ Obtain IPv4 settings automatically
☒ Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway ☐ Override default gateway for this adapter

DNS server addresses

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

Add Networking

- Select connection type
- Select target device
- Port properties
- IPv4 settings
- 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

[CANCEL](#)
[BACK](#)
[FINISH](#)

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

Deploy and use ONTAP Tools to configure storage

The following steps are performed on the VCF management domain cluster using the vSphere client and involve deploying ONTAP Tools, creating a vVols iSCSI datastore, and migrating management VM's to the new datastore.

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

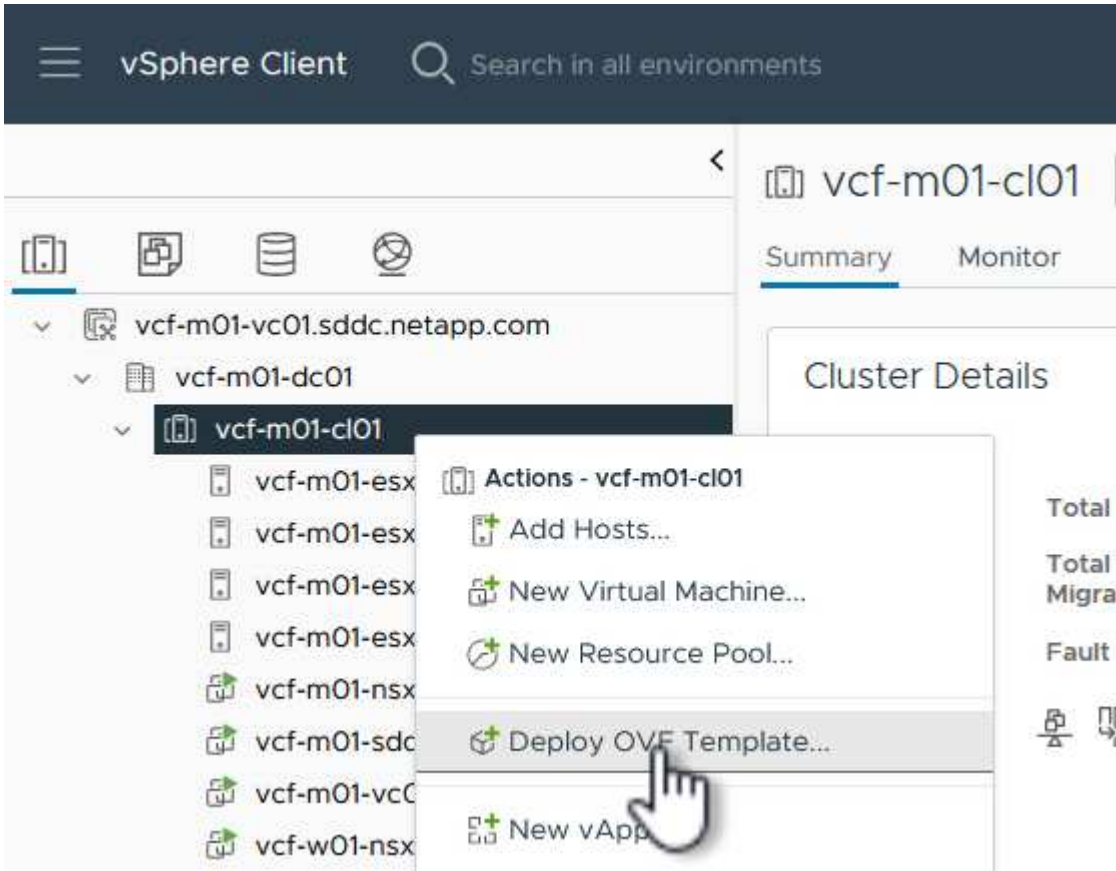
For additional information on deploying and using ONTAP Tools in a multiple vCenter environment refer to [Requirements for registering ONTAP tools in multiple vCenter Servers environment](#).

Deploy ONTAP tools for VMware vSphere

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

Complete the following to Deploy ONTAP tools for VMware vSphere:

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



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

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

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

☐ URL

[http | https://remoteserver-address/filetoinstall.ovf](http://https://remoteserver-address/filetoinstall.ovf) | .ova

☒ Local file

UPLOAD FILES

netapp-ontap-tools-for-vmware-vmware-9.13-9554.ova

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

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine [?](#)

Select virtual disk format

As defined in the VM storage policy

VM Storage Policy

Datastore Default

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	v
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v

Manage Columns

Items per page 10 5 items

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

Deploy OVF Template

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

Select networks

Select a destination network for each source network.

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

Manage Columns

vcf-m01-cl01-vds01-pg-vsan
SDDC-DPortGroup-VM-Mgmt
Browse ...

1 item

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

8. On the Customize template page fill out all required information:

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

Click on **Next** to continue.

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 <input type="password" value="....."/> Confirm Password <input type="password" value="....."/>
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. <input type="text" value="172.21.166.1"/>
Maintenance User Password (*)	Password to assign to maint user account. Password <input type="password" value="....."/> Confirm Password <input type="password" value="....."/>

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. <input type="checkbox"/>
vCenter Server Address (*)	Specify the IP address/hostname of an existing vCenter to register to. <input type="text" value="cf-wkld-vc01.sddc.netapp.com"/>
Port (*)	Specify the HTTPS port of an existing vCenter to register to. <input type="text" value="443"/>
Username (*)	Specify the username of an existing vCenter to register to. <input type="text" value="administrator@vsphere.local"/>
Password (*)	Specify the password of an existing vCenter to register to. Password <input type="password" value="....."/> Confirm Password <input type="password" value="....."/>

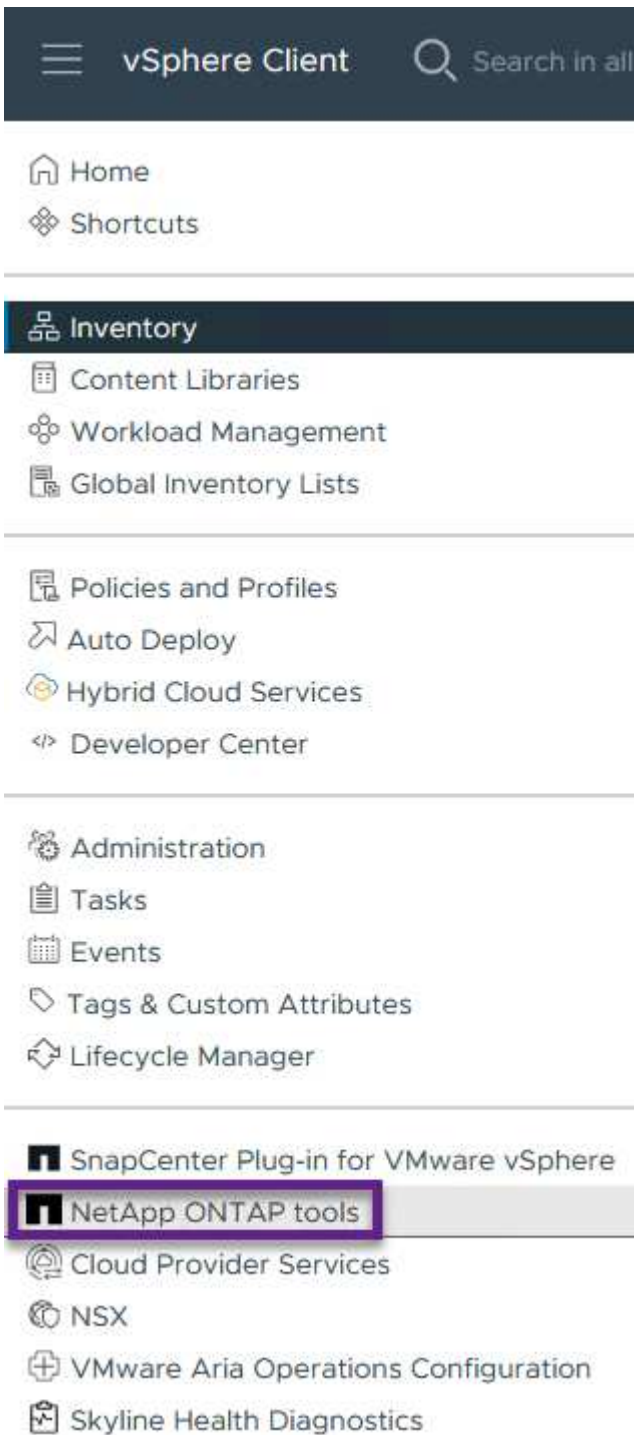
Network Properties	8 settings
Host Name	Specify the hostname for the appliance. (Leave blank if DHCP is desired) <input type="text" value="vcf-w01-otv9"/>
IP Address	Specify the IP address for the appliance. (Leave blank if DHCP is desired)

CANCEL BACK NEXT

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

Add a storage system to ONTAP Tools.

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



2. From the **INSTANCE** drop down menu in the ONTAP Tool interface, select the ONTAP Tools instance associated with the workload domain to be managed.

vSphere Client

Search in all environments

NetApp ONTAP tools

INSTANCE 172.21.166.139:8443

Overview

Storage Systems

Storage capability profile

Storage Mapping

Settings

Plugin Instance	Version	vCenter Server
172.21.166.139:8443	9.13.0.36905	vcf-m01-vc01.sddc.netapp.com
172.21.166.149:8443	9.13.0.36905	vcf-wkld-vc01.sddc.netapp.com

+

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

vSphere Client

Search in all environments

NetApp ONTAP tools

INSTANCE 172.21.166.149:8443

Overview

Storage Systems

Storage capability profile

Storage Systems

ADD

REDISCOVER ALL


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



vVol requires ONTAP cluster credentials rather than SVM credentials. For more information refer to [Add storage systems](#) In the ONTAP Tools documentation.

Add Storage System

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

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

Name or IP address: 172.16.9.25

Username: admin

Password: ●●●●●●●●

Port: 443

Advanced options 

ONTAP Cluster Certificate: ☒ Automatically fetch ☐ Manually upload

CANCEL

SAVE & ADD MORE

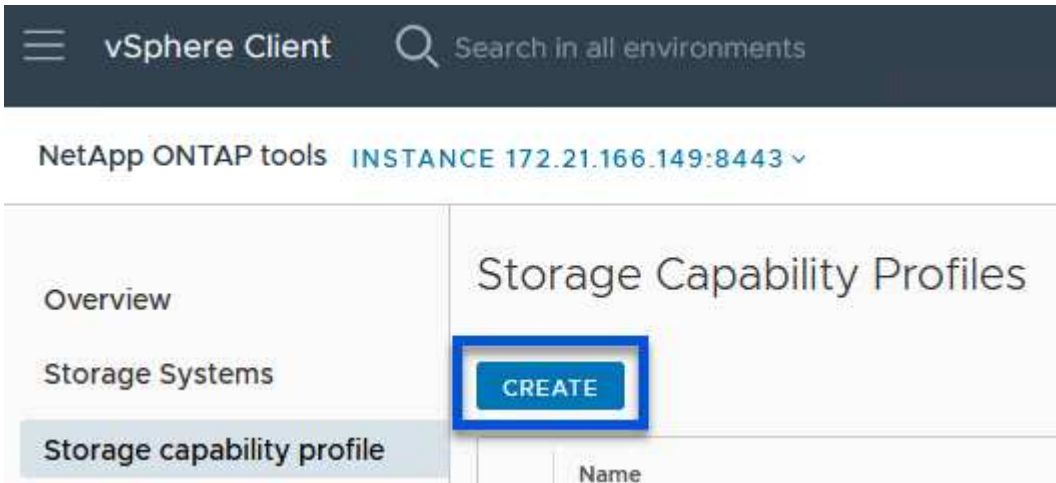
ADD

Create a storage capability profile in ONTAP Tools

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

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

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



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

The screenshot shows the 'Create Storage Capability Profile' wizard. On the left, there's a sidebar with the title 'Create Storage Capability Profile' and a list of steps: '1 General', '2 Platform', '3 Protocol', '4 Performance', '5 Storage attributes', and '6 Summary'. The '1 General' step is selected and highlighted. The main area is titled 'General' and contains the instruction 'Specify a name and description for the storage capability profile.' with a question mark icon. Below this, there are two fields: 'Name:' with the value 'Gold_ASA_ISCSI' entered, and 'Description:' with an empty text area. At the bottom right, there are two buttons: 'CANCEL' and 'NEXT'. The 'NEXT' button is highlighted in blue.

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

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Platform

Platform: Performance

Asymmetric:



CANCEL

BACK

NEXT

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

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Protocol

Protocol:

Any

Any

FCP

iSCSI

NVMe/FC

CANCEL

BACK

NEXT

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

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Performance

☐ None ⓘ

☒ QoS policy group ⓘ

Min IOPS:

Max IOPS:

6000

☐ Unlimited

CANCEL

BACK

NEXT

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

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Storage attributes

Deduplication:

Yes



Compression:

Yes



Space reserve:

Thin



Encryption:

No



Tiering policy (FabricPool):

None



CANCEL

BACK

NEXT

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

Create Storage Capability Profile

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

Summary

Name:	ASA_Gold_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

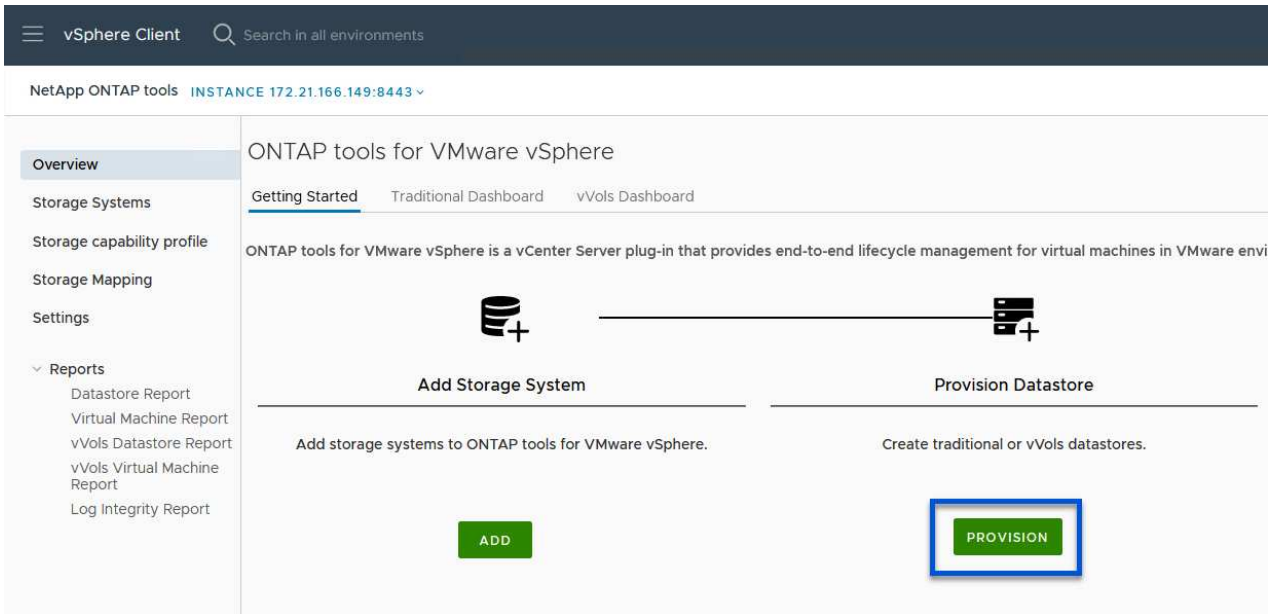
CANCEL BACK FINISH



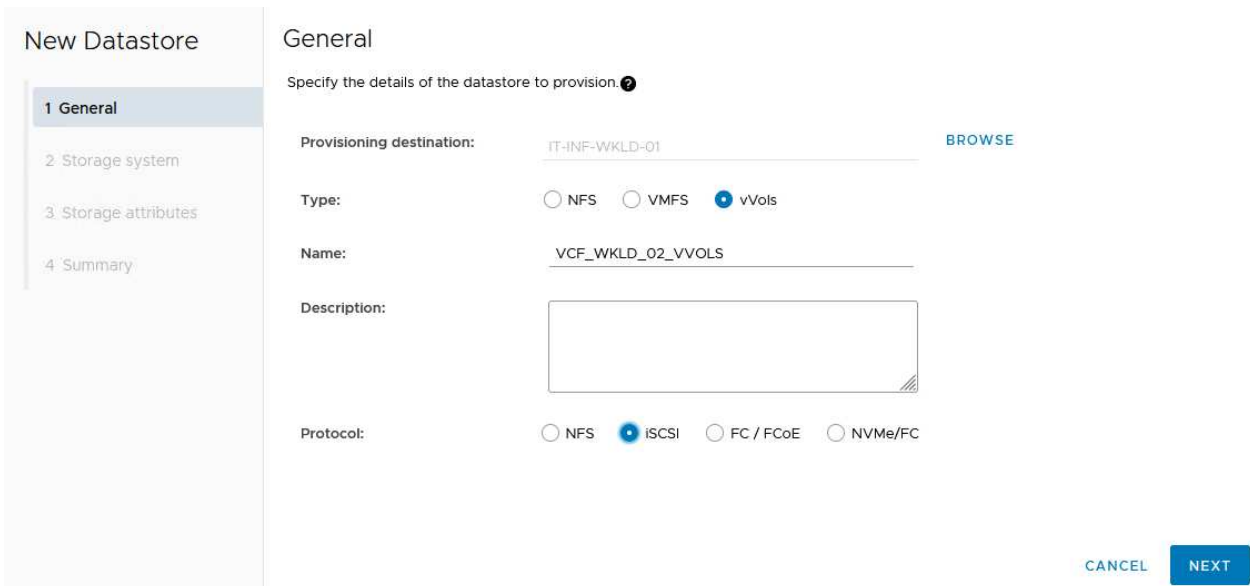
Create a vVols datastore in ONTAP Tools

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

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



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



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

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

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

Storage capability profiles:

AFF_Encrypted_Min50_ASA_A
FAS_Default
FAS_Max20
Custom profiles
ASA_Gold_iSCSI

Storage system:

ntaphci-a300e9u25 (172.16.9.25)

Storage VM:

VCF_iSCSI

CANCEL

BACK

NEXT

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

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: ☒ Create new volumes ☐ Select volumes

Create new volumes

Name	Size	Storage Capability Profile	Aggregate
 FlexVol volumes are not added.			

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
f_wkld_02_vvols	3000	ASA_Gold_iSCSI	EHCaggr02 - (27053.3 GE	Thin

ADD

CANCEL

BACK

NEXT

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

New Datastore

- General
- Storage system
- Storage attributes
- Summary

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.

CANCEL
BACK
FINISH

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](#).

Add NFS and vVols as supplemental storage to VI workload domains using ONTAP tools for VMware vSphere

In this use case we outline the procedure to use ONTAP Tools for VMware to add NFS and vVols datastores as supplemental storage for a VMware Cloud Foundation (VCF) Virtual Infrastructure (VI) workload domain. This procedure summarizes deploying ONTAP Tools for VMware vSphere, configuring a Storage Virtual Machine (SVM) with NFS logical interfaces, and provisioning both NFS and vVols datastores.

NFS is used as the storage protocol for the vVols datastore.

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](#).

Scenario Overview

This scenario covers the following high level steps:

- Create a storage virtual machine (SVM) with logical interfaces (LIFs) for NFS traffic.
- Create a distributed port group for the NFS network on the VI workload domain.
- Create a vmkernel adapter for NFS on the ESXi hosts for the VI workload domain.
- Deploy ONTAP Tools on the VI workload domain.
- Create a new NFS datastore on the VI workload domain.
- Create a new vVols datastore on the VI workload domain.

Prerequisites

This scenario requires the following components and configurations:

- An ONTAP AFF 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.

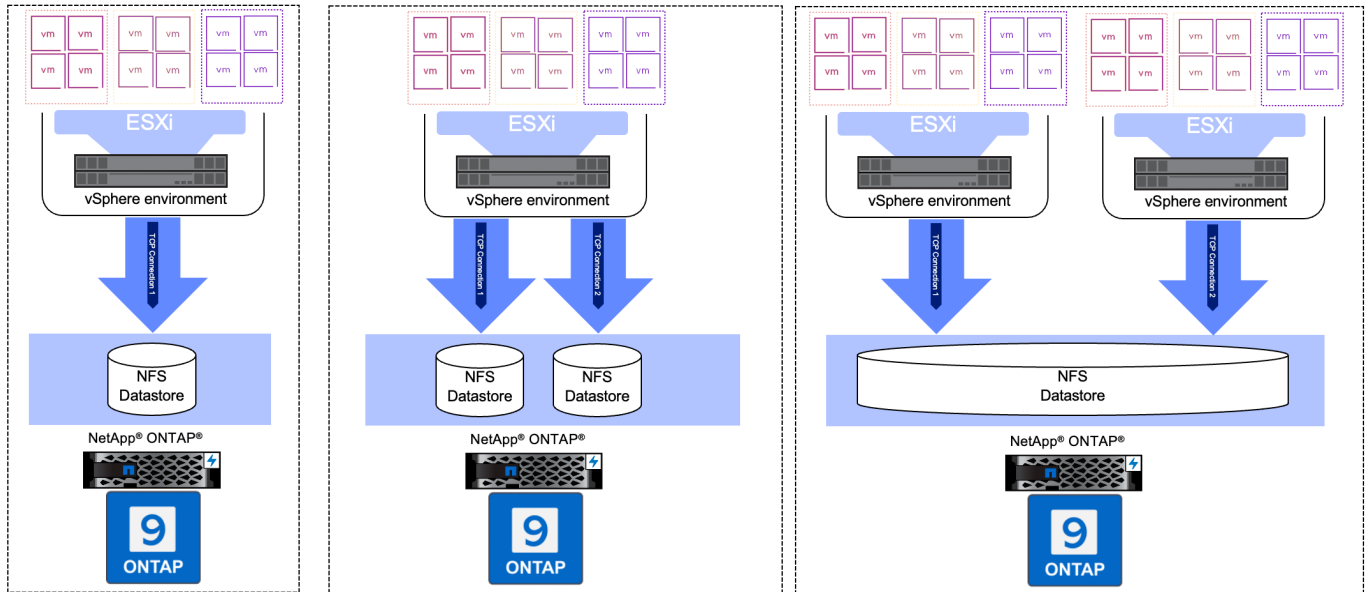
NetApp recommends a redundant network designs for NFS, providing fault tolerance for storage systems, switches, networks adapters and host systems. It is common to deploy NFS with a single subnet or multiple subnets depending on the architectural requirements.

Refer to [Best Practices For Running NFS with VMware vSphere](#) for detailed information specific to VMware vSphere.

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

This documentation demonstrates the process of creating a new SVM and specifying the IP address information to create multiple LIFs for NFS traffic. To add new LIFs to an existing SVM refer to [Create a LIF \(network interface\)](#).

For complete information on using NFS with vSphere clusters, refer to the [NFS v3 Reference Guide for vSphere 8](#).



Deployment Steps

To deploy ONTAP Tools and use it to create a vVols and NFS datastore on the VCF management domain, complete the following steps:

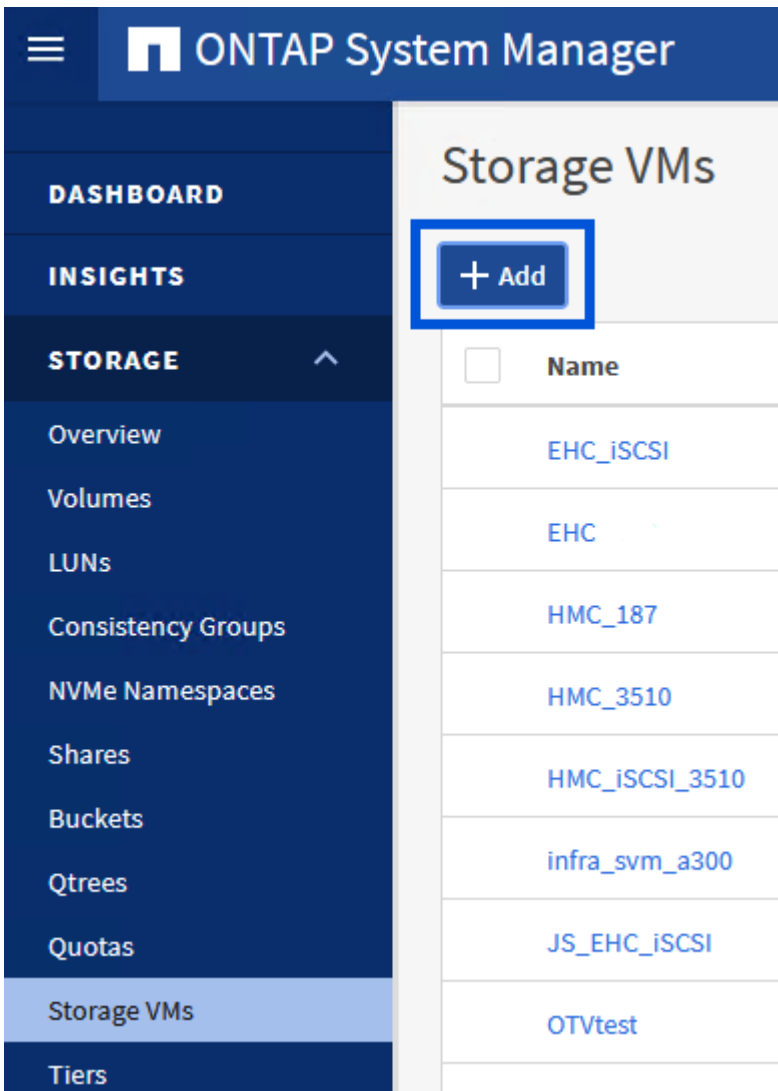
Create SVM and LIFs on ONTAP storage system

The following step is performed in ONTAP System Manager.

Create the storage VM and LIFs

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

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



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

Add Storage VM



STORAGE VM NAME

VCF_NFS

IPSPACE

Default

Access Protocol

☒ SMB/CIFS, NFS, S3

iSCSI


FC

NVMe

☐ Enable SMB/CIFS

☒ Enable NFS

☐ Allow NFS client access

 Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

☐ Enable S3

DEFAULT LANGUAGE [?](#)

c.utf_8



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

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

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET

Without a subnet

IP ADDRESS

172.21.118.119

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS_iSCSI

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

ntaphci-a300-02

SUBNET

Without a subnet

IP ADDRESS

172.21.118.120

PORT

a0a-3374

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

Storage VM Administration

☐ Manage administrator account

Save

Cancel

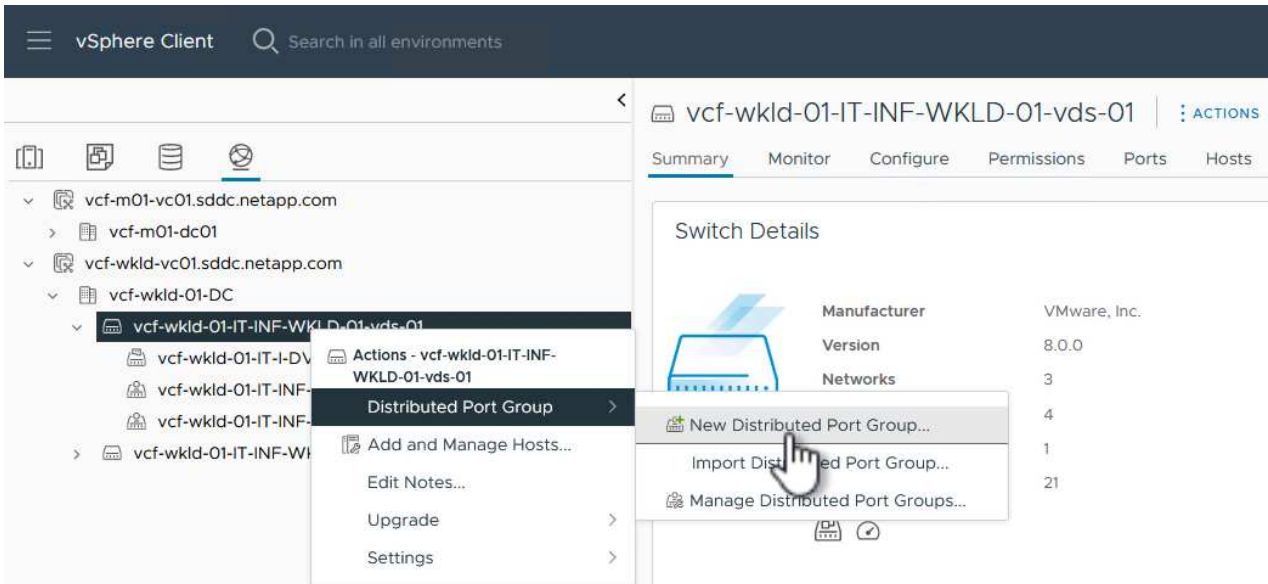
Set up networking for NFS on ESXi hosts

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

Create a Distributed Port Group for NFS traffic

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

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



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

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

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

CANCEL

BACK

NEXT

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

☰

vSphere Client

🔍 Search in all environments

🏠

vcf-wkld-01-nfs

⋮ ACTIONS

Summary

Monitor

Configure

Perf

📁

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-...

🏠

vcf-wkld-01-IT-INF-WKLD-01-vds-01-...

🏠

vcf-wkld-01-nfs

🏠

vcf-wkld-01-nvm

🏠

vcf-wkld-01-nvm

📁

vcf-wkld-01-IT-INF-

🌐

Distributed Port Group Details

🌐

Port binding

🌐

Port allocation

🌐

VLAN ID

🌐

Distributed switch

🌐

Network protocol profile

🌐

Network resource pool

🌐

Hosts

🌐

Virtual machines

⋮

Actions - vcf-wkld-01-nfs

🔧



Edit Settings...

📄

Export Configuration...

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

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

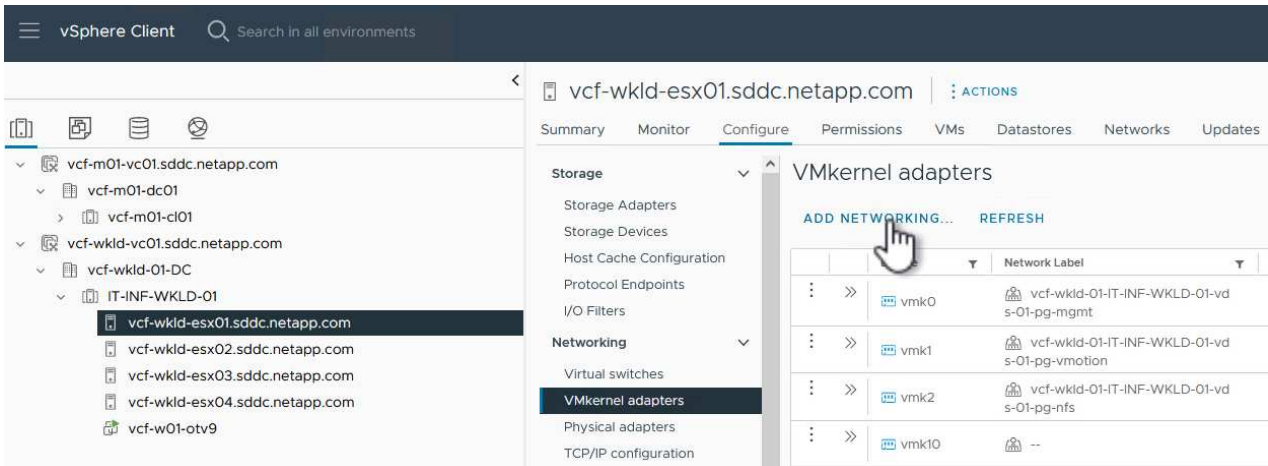
General	Load balancing	Route based on originating virtual port ▾
Advanced	Network failure detection	Link status only ▾
VLAN	Notify switches	Yes ▾
Security	Failback	Yes ▾
Traffic shaping		
Teaming and failover	Failover order ⓘ	
Monitoring	MOVE UP MOVE DOWN	
Miscellaneous	Active uplinks	
	 uplink2	
	 uplink1	
	Standby uplinks	
	Unused uplinks	

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

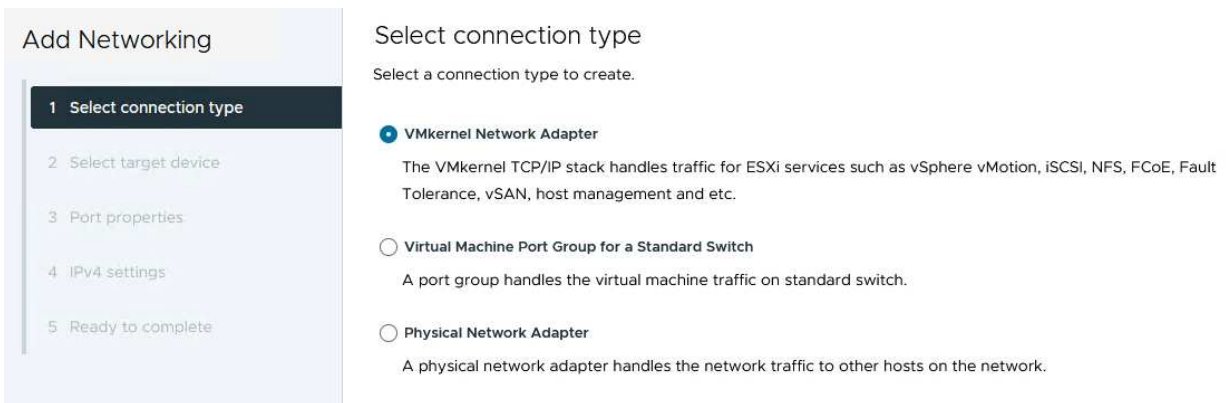
Create a VMkernel adapter on each ESXi host

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

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



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



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

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

- ☒ Select an existing network
- ☐ Select an existing standard switch
- ☐ New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input checked="" type="radio"/>	vcf-wkld-01-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Manage Columns 8 items

CANCEL

BACK

NEXT

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

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

- ☐ Obtain IPv4 settings automatically
- ☒ Use static IPv4 settings

IPv4 address 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

CANCEL

BACK

NEXT

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

VMkernel adapter.

Add Networking

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

Ready to complete

Review your selections before finishing the wizard

▼ Select target device

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

▼ Port properties

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

CANCEL

BACK

FINISH

Deploy and use ONTAP Tools to configure storage

The following steps are performed on the VCF management domain cluster using the vSphere client and involve deploying OTV, creating a vVols NFS datastore, and migrating management VM's to the new datastore.

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

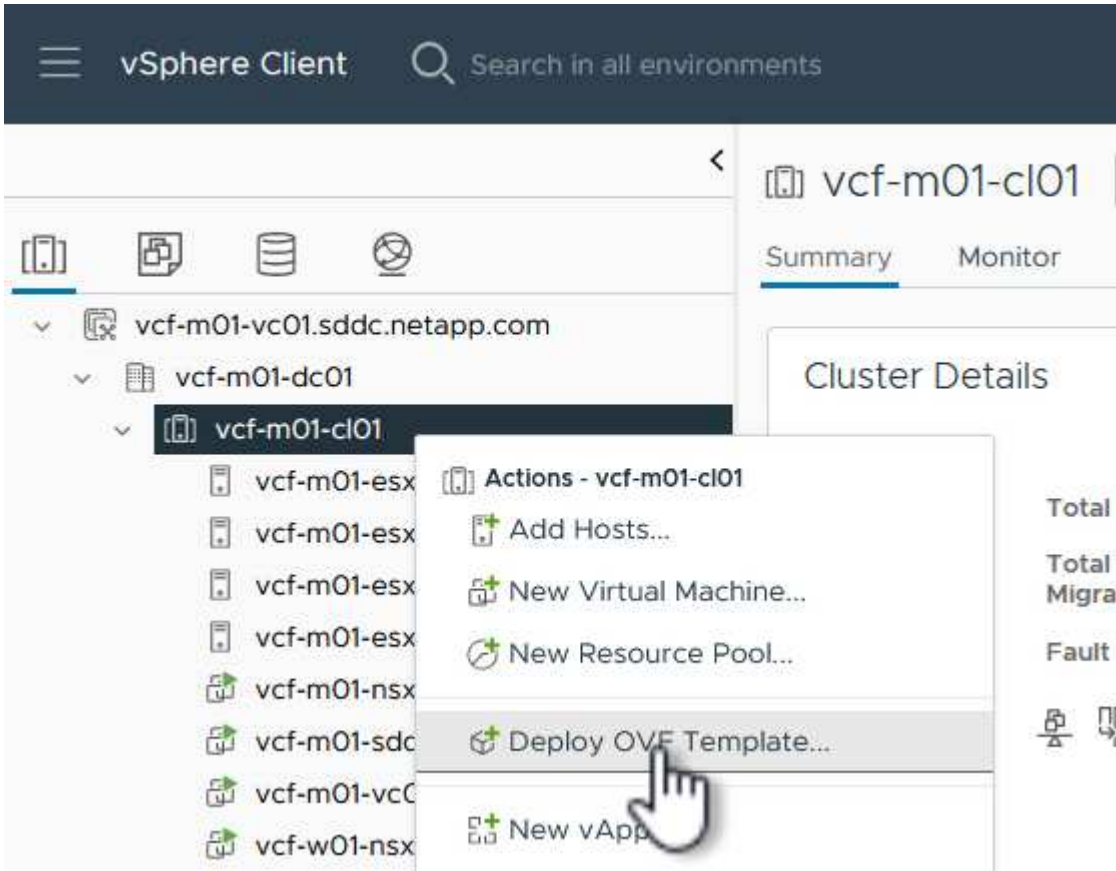
For additional information on deploying and using ONTAP Tools in a multiple vCenter environment refer to [Requirements for registering ONTAP tools in multiple vCenter Servers environment](#).

Deploy ONTAP tools for VMware vSphere

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

Complete the following to Deploy ONTAP tools for VMware vSphere:

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



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

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/filetoinstall.ovf | .ova](http://https://remoteserver-address/filetoinstall.ovf)

☒ Local file

UPLOAD FILES

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

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

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine [?](#)

Select virtual disk format

As defined in the VM storage policy

VM Storage Policy

Datastore Default

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	v
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v

Manage Columns

Items per page 10 5 items

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

Deploy OVF Template

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

Select networks

Select a destination network for each source network.

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

Manage Columns

vcf-m01-cl01-vds01-pg-vsan
SDDC-DPortGroup-VM-Mgmt
Browse ...

1 item

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

8. On the Customize template page fill out all required information:

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

Click on **Next** to continue.

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 <input type="password" value="....."/> Confirm Password <input type="password" value="....."/>
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. <input type="text" value="172.21.166.1"/>
Maintenance User Password (*)	Password to assign to maint user account. Password <input type="password" value="....."/> Confirm Password <input type="password" value="....."/>

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. <input type="checkbox"/>
vCenter Server Address (*)	Specify the IP address/hostname of an existing vCenter to register to. <input type="text" value="cf-wkld-vc01.sddc.netapp.com"/>
Port (*)	Specify the HTTPS port of an existing vCenter to register to. <input type="text" value="443"/>
Username (*)	Specify the username of an existing vCenter to register to. <input type="text" value="administrator@vsphere.local"/>
Password (*)	Specify the password of an existing vCenter to register to. Password <input type="password" value="....."/> Confirm Password <input type="password" value="....."/>

Network Properties 8 settings

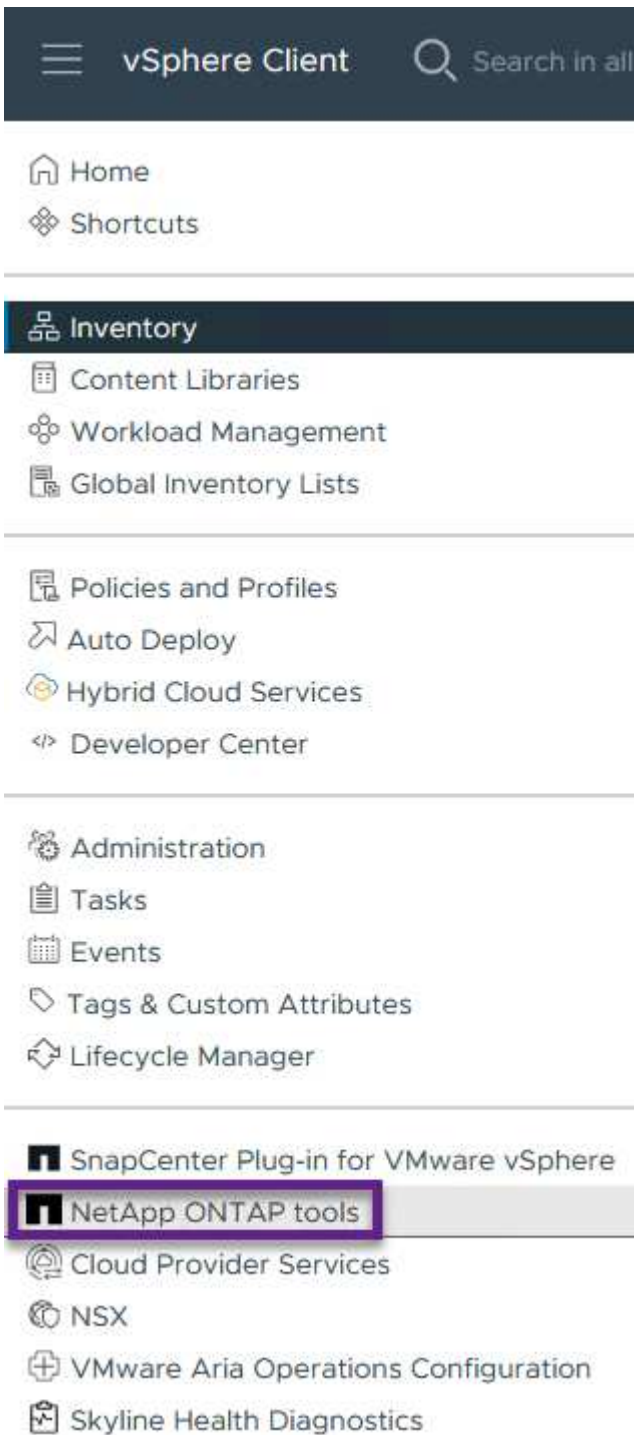
Host Name	Specify the hostname for the appliance. (Leave blank if DHCP is desired) <input type="text" value="vcf-w01-otv9"/>
IP Address	Specify the IP address for the appliance. (Leave blank if DHCP is desired) <input type="text"/>

CANCEL BACK NEXT

9. Review all information on the Ready to complete page and the click Finish to begin deploying the OTV appliance.

Add a storage system to ONTAP Tools.

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



2. From the **INSTANCE** drop down menu in the ONTAP Tool interface, select the OTV instance associated with the workload domain to be managed.

vSphere Client

Search in all environments

NetApp ONTAP tools

INSTANCE 172.21.166.139:8443

Overview

Storage Systems

Storage capability profile

Storage Mapping

Settings

Plugin Instance	Version	vCenter Server
172.21.166.139:8443	9.13.0.36905	vcf-m01-vc01.sddc.netapp.com
172.21.166.149:8443	9.13.0.36905	vcf-wkld-vc01.sddc.netapp.com

+

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

vSphere Client

Search in all environments

NetApp ONTAP tools

INSTANCE 172.21.166.149:8443

Overview

Storage Systems

Storage capability profile

Storage Systems

ADD

REDISCOVER ALL

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

Add Storage System

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

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

Name or IP address: 172.16.9.25

Username: admin

Password: ●●●●●●●●

Port: 443

Advanced options ^

ONTAP Cluster Certificate: ☒ Automatically fetch ☐ Manually upload

CANCEL

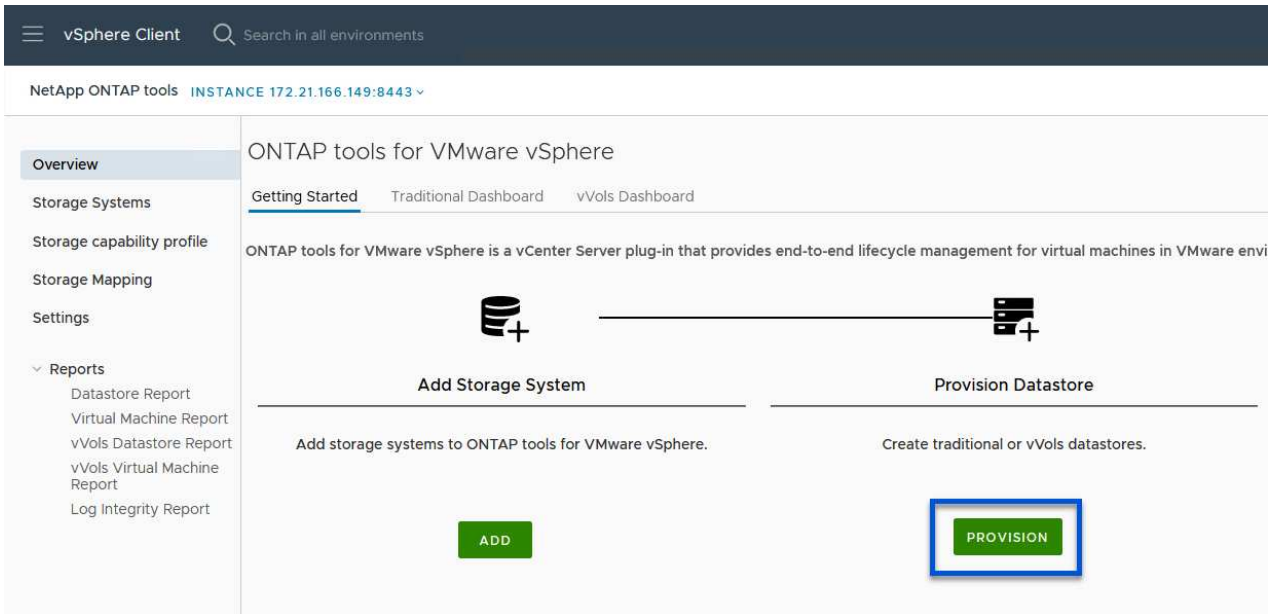
SAVE & ADD MORE

ADD

Create an NFS datastore in ONTAP Tools

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

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



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

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

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

General

Specify the details of the datastore to provision. ?

Provisioning destination:

vcf-wkld-01-DC

BROWSE

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

Advanced options

>

CANCEL

NEXT

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

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

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

Storage capability profile:

Platinum_AFF_A

Storage system:

ntaphci-a300e9u25 (172.16.9.25)

Storage VM:

VCF_NFS

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

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Aggregate:

EHCAGgr02 - (25350.17 GB Free)

Volumes:

Automatically creates a new volume.

Advanced options

>

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

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

CANCEL

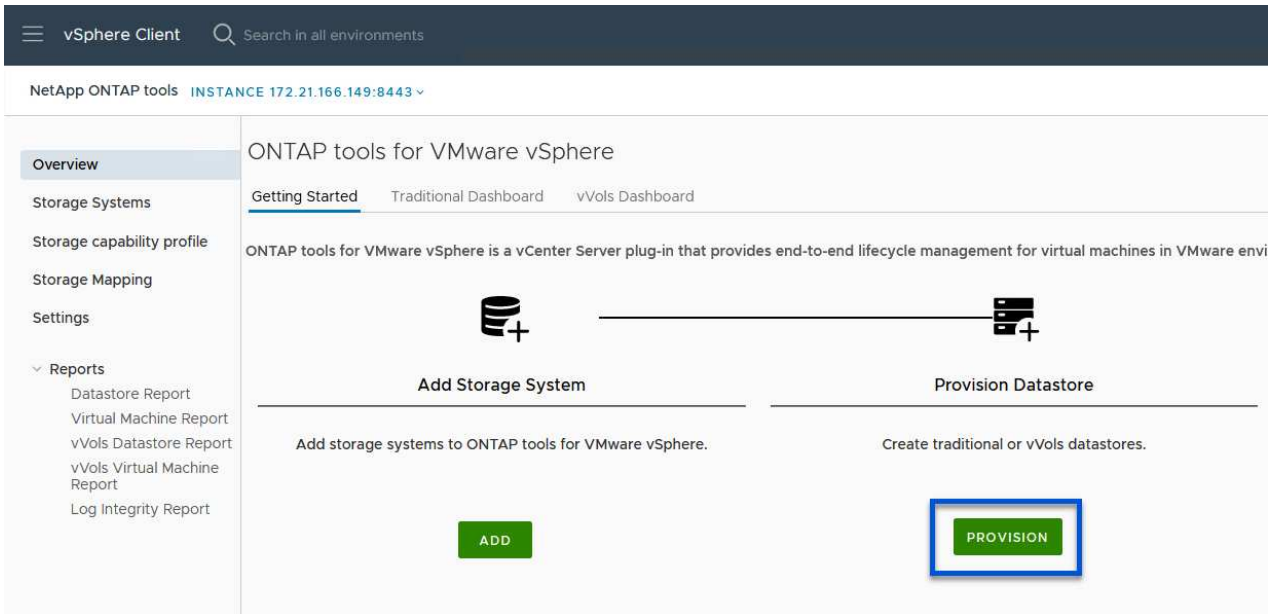
BACK

FINISH

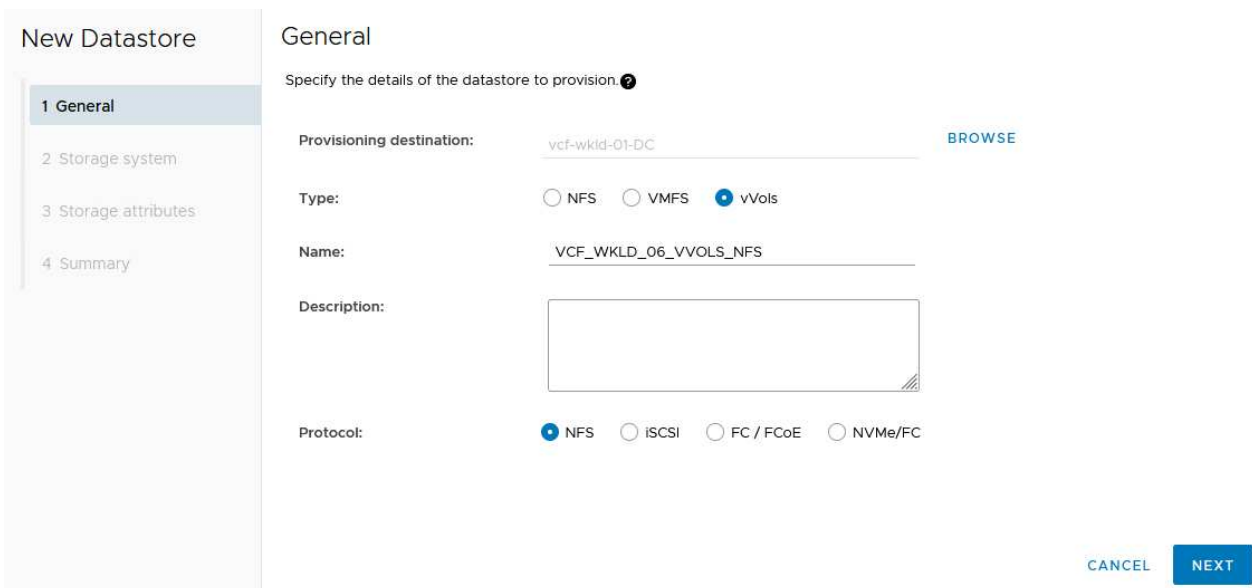
Create a vVols datastore in ONTAP Tools

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

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



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



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

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

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

Storage capability profile:	Platinum_AFF_A
Storage system:	ntaphci-a300e9u25 (172.16.9.25)
Storage VM:	VCF_NFS

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

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
vcf_wkld_06_vv	2000	Platinum_AFF_A	EHCaggr02 - (25404 GB I	Thin

ADD

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

ADD

Default storage capability profile: Platinum_AFF_A

CANCEL

BACK

NEXT

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

New Datastore

- General
- Storage system
- Storage attributes
- 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

CANCEL
BACK
FINISH

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](#).

Add NVMe over TCP as supplemental storage to VI workload domains

In this use case we outline the procedure to use ONTAP Tools for VMware to configure NVMe over TCP (NVMe/TCP) as supplemental storage for a VMware Cloud Foundation (VCF) Virtual Infrastructure (VI) workload domain. This procedure summarizes setting up an NVMe/TCP-enabled Storage Virtual Machine (SVM), creating NVMe namespaces, configuring ESXi host networking, and deploying a VMFS datastore.

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.

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?](#)

Scenario Overview

This scenario covers the following high level steps:

- Create a storage virtual machine (SVM) with logical interfaces (LIFs) for NVMe/TCP traffic.
- Create distributed port groups for iSCSI networks on the VI workload domain.

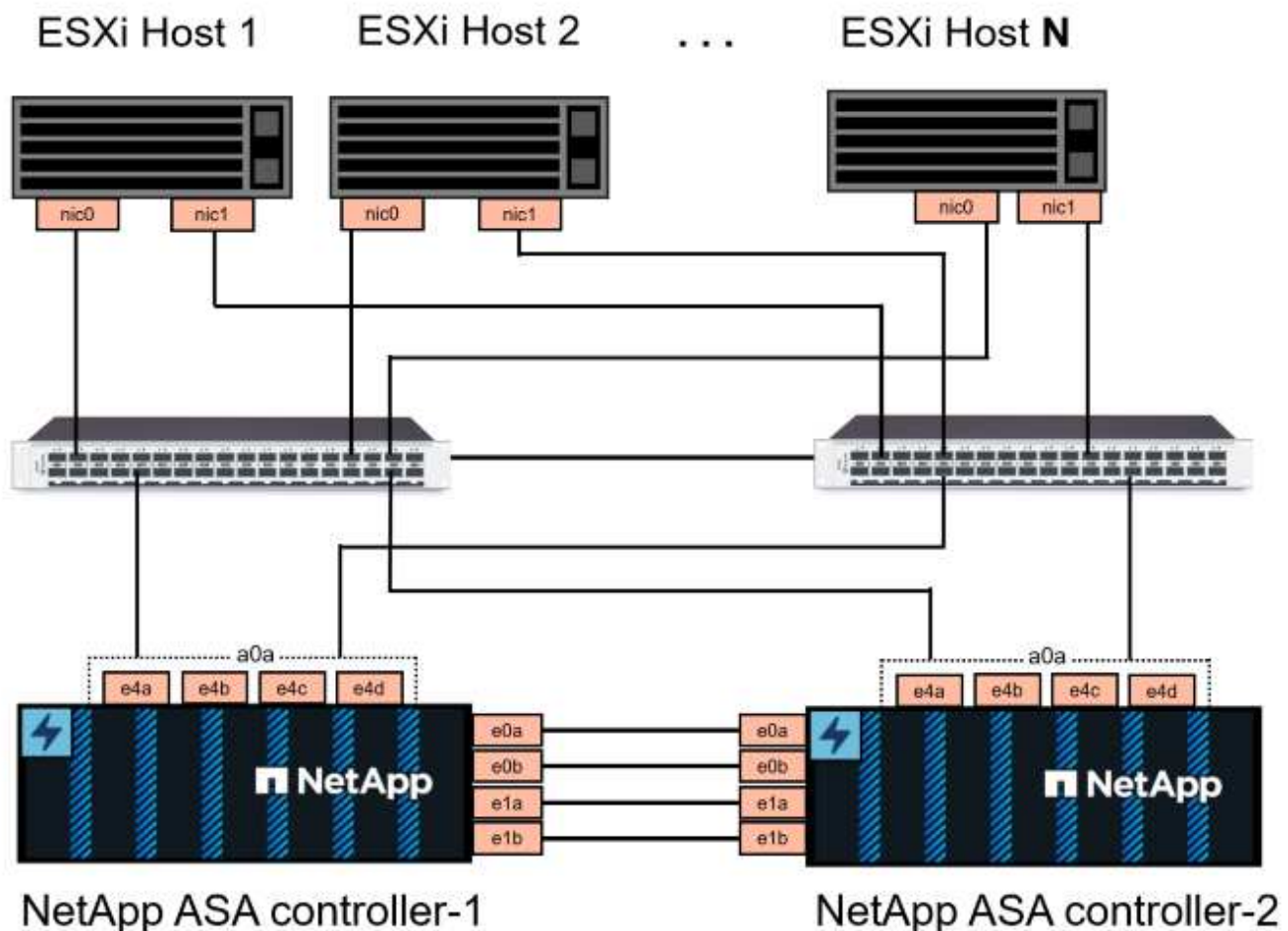
- Create vmkernel adapters for iSCSI on the ESXi hosts for the VI workload domain.
- Add NVMe/TCP adapters on ESXi hosts.
- Deploy NVMe/TCP datastore.

Prerequisites

This scenario requires the following components and configurations:

- An ONTAP 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.

NetApp recommends fully redundant network designs for NVMe/TCP. The following diagram illustrates an example of a redundant configuration, providing fault tolerance for storage systems, switches, networks adapters and host systems. Refer to the NetApp [SAN configuration reference](#) for additional information.



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

This documentation demonstrates the process of creating a new SVM and specifying the IP address information to create multiple LIFs for NVMe/TCP traffic. To add new LIFs to an existing SVM refer to [Create a](#)

[LIF \(network interface\)](#).

For additional information on NVMe design considerations for ONTAP storage systems, refer to [NVMe configuration, support and limitations](#).

Deployment Steps

To create a VMFS datastore on a VCF workload domain using NVMe/TCP, complete the following steps.

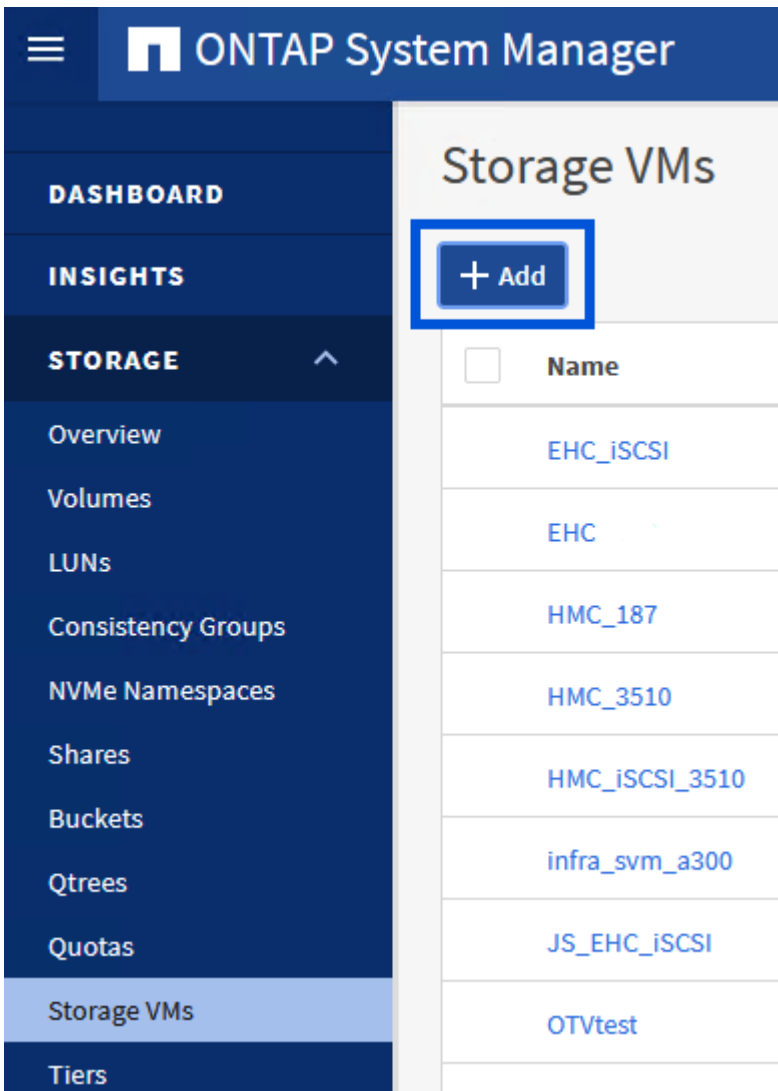
Create SVM, LIFs and NVMe Namespace on ONTAP storage system

The following step is performed in ONTAP System Manager.

Create the storage VM and LIFs

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

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



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

Add Storage VM



STORAGE VM NAME

VCF_NVMe

IPSPACE

Default



Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

✓ NVMe



Enable NVMe/FC



Enable NVMe/TCP

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



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

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.189

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

172.21.119.189

PORT

a0a-3375

ntaphci-a300-02

IP ADDRESS

172.21.118.190

PORT

a0a-3374

IP ADDRESS

172.21.119.190

PORT

a0a-3375

Storage VM Administration

☐ Manage administrator account

Save

Cancel

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

Storage VM Administration

☐ Manage administrator account

Save

Cancel

Create the NVMe Namespace

NVMe namespaces are analogous to LUNs for iSCSi or FC. The NVMe Namespace must be created before a VMFS datastore can be deployed from the vSphere Client. To create the NVMe namespace, the NVMe Qualified Name (NQN) must first be obtained from each ESXi host in the cluster. The NQN is used by ONTAP to provide access control for the namespace.

Complete the following steps to create an NVMe Namespace:

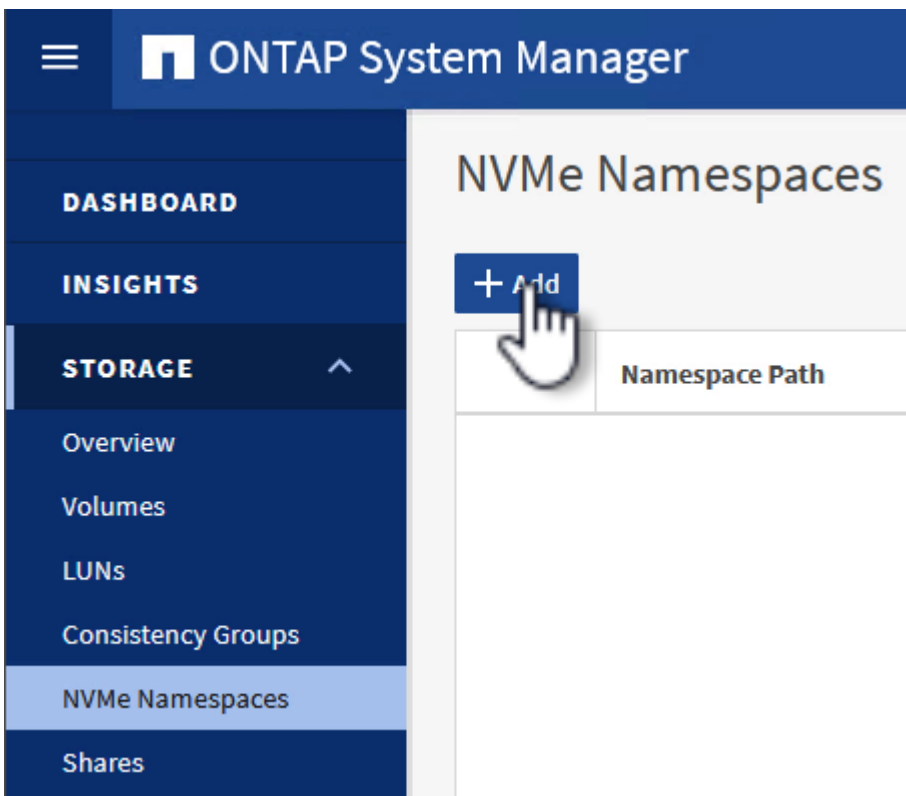
1. Open an SSH session with an ESXi host in the cluster to obtain its NQN. Use the following command from the CLI:

```
esxcli nvme info get
```

An output similar to the following should be displayed:

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

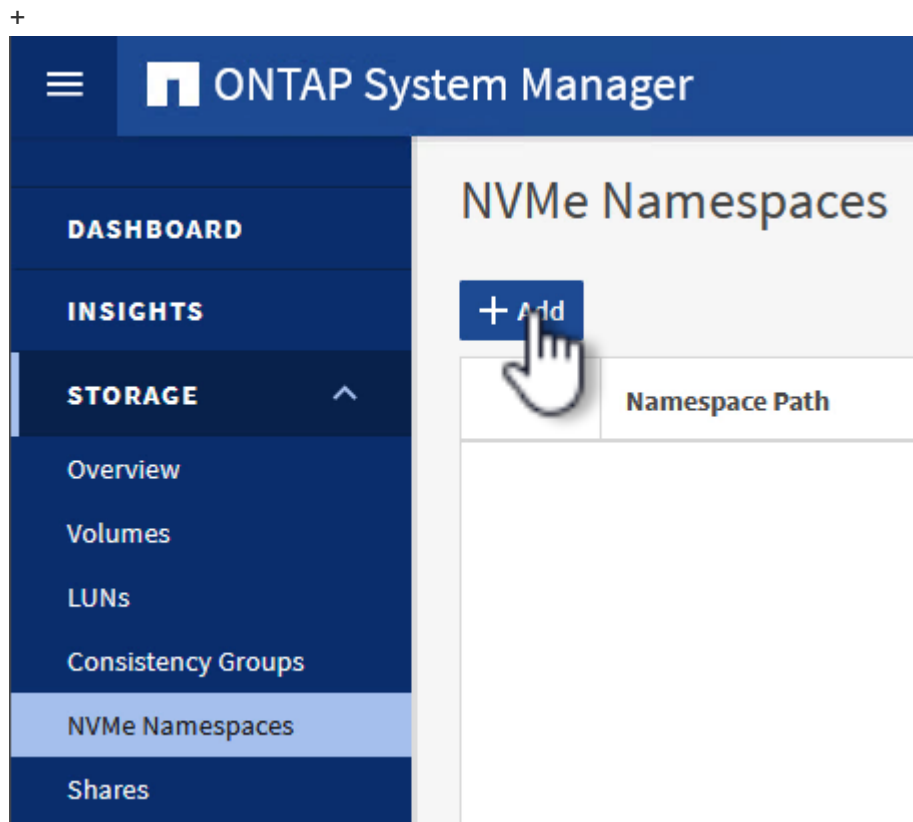
2. Record the NQN for each ESXi host in the cluster
3. From ONTAP System Manager navigate to **NVMe Namespaces** in the left-hand menu and click on **+ Add** to start.



4. On the **Add NVMe Namespace** page, fill in a name prefix, the number of namespaces to create, the size of the namespace, and the host operating system that will be accessing the namespace. In the

Host NQN section create a comma separated list of the NQN's previously collected from the ESXi hosts that will be accessing the namespaces.

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



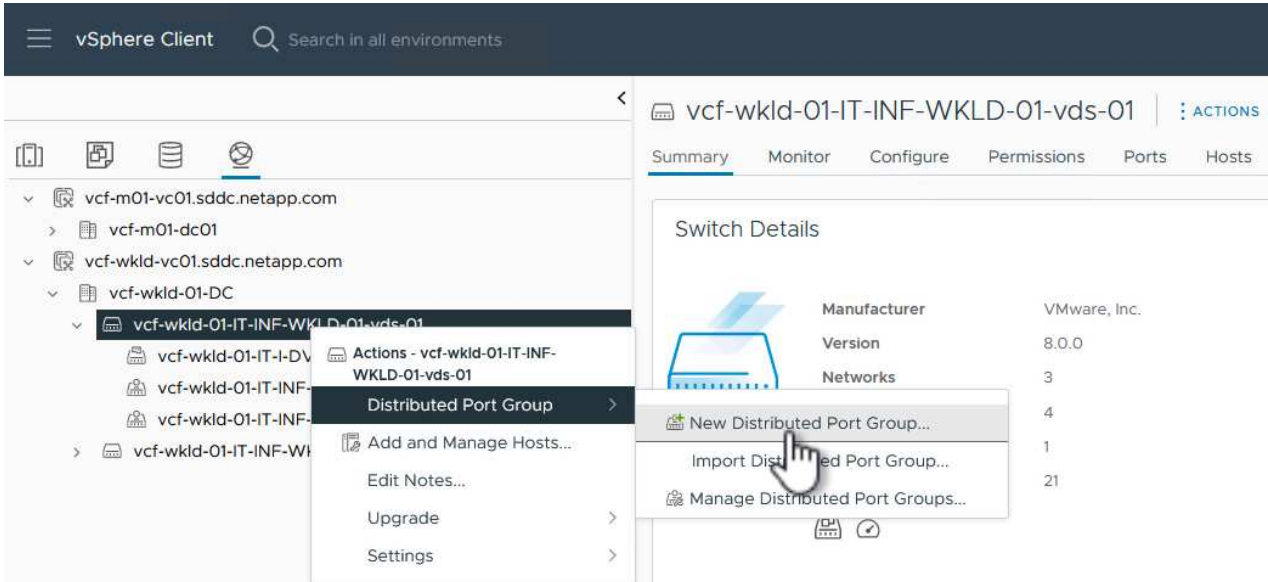
Set up networking and NVMe software adapters on ESXi hosts

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

Create Distributed Port Groups for NVMe/TCP traffic

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

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



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

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding

Static binding

Port allocation

Elastic

Number of ports

8

Network resource pool

(default)

VLAN

VLAN type

VLAN

VLAN ID

3374

Advanced

☐ Customize default policies configuration

CANCEL

BACK

NEXT

- On the **Ready to complete** page, review the changes and click on **Finish** to create the new distributed port group.
- 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**.
- Once both port groups have been created, navigate to the first port group and select the action to **Edit settings....**

vSphere Client

Search in all environments

vcf-wkld-01-nvme-a

ACTIONS

Summary

Monitor

Configure

Permissions

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-IT-INF-WKLD-01-vds-01-pg-vmotion

vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion

vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion

vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion

Actions - vcf-wkld-01-nvme-a

Edit Settings...

Export Configuration...

Restore Configuration...

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

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

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

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Network failure detection

Notify switches

Failback

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink1

Standby uplinks

Unused uplinks

uplink2

Route based on originating virtual port

Link status only

Yes

Yes

- Repeat this step for the second NVMe/TCP port group. However, this time move **uplink1** down to

170

Unused uplinks.

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

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Network failure detection

Notify switches

Fallback

Failover order ⓘ

MOVE UP

MOVE DOWN

Active uplinks

uplink2

Standby uplinks

Unused uplinks

uplink1

Route based on originating virtual por

Link status only

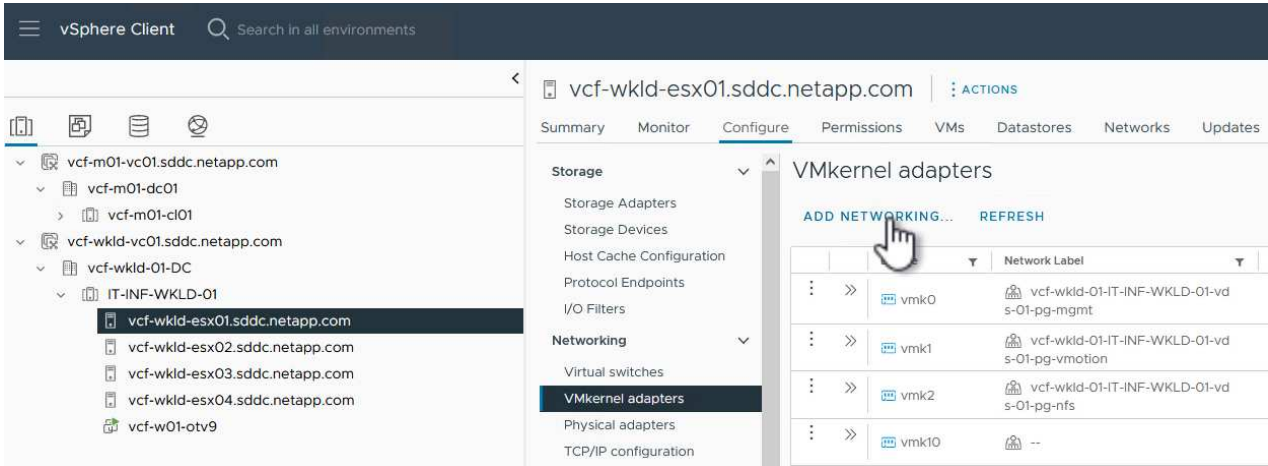
Yes

Yes

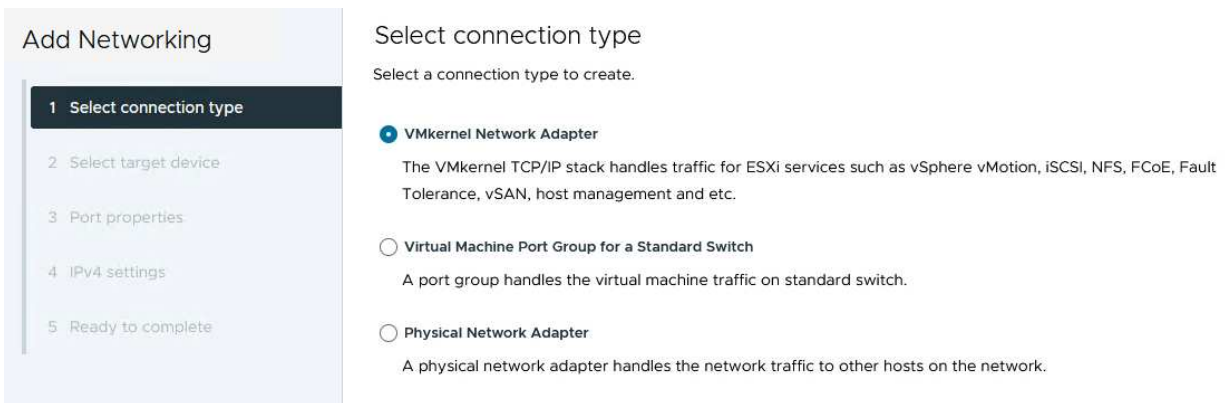
Create VMkernel adapters on each ESXi host

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

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



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



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

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device



Select a target device for the new connection.

- ☒ Select an existing network
- ☐ Select an existing standard switch
- ☐ New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input checked="" type="radio"/>	vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
Manage Columns 7 items			

CANCEL

BACK

NEXT



Packages

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

Add Networking

- Select connection type
- Select target device
- Port properties**
- IPv4 settings
- Ready to complete

Port properties

Specify VMkernel port settings.

Network label

MTU

TCP/IP stack

Available services

Enabled services

☒ vMotion
 ☐ vSphere Replication NFC
 ☐ NVMe over RDMA

☐ Provisioning
 ☐ vSAN
 ☐ vSAN Witness

☐ Fault Tolerance logging
 ☐ vSphere Backup NFC
 ☒ NVMe over TCP

☐ Management
 ☐ vSphere Replication

CANCEL BACK **NEXT**

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

Add Networking

- Select connection type
- Select target device
- Port properties
- IPv4 settings**
- Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

☐ Obtain IPv4 settings automatically
☒ Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway ☐ Override default gateway for this adapter

DNS server addresses

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

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

▼ Select target device

Distributed port groupvcf-wkld-01-nvme-a

Distributed switchvcf-wkld-01-IT-INF-WKLD-01-vds-01

▼ Port properties

New port groupvcf-wkld-01-nvme-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)

MTU9000

vMotionDisabled

ProvisioningDisabled

Fault Tolerance loggingDisabled

ManagementDisabled

vSphere ReplicationDisabled

vSphere Replication NFCDisabled

vSANDisabled

vSAN WitnessDisabled

vSphere Backup NFCDisabled

NVMe over TCPEnabled

NVMe over RDMADisabled

▼ IPv4 settings

IPv4 address172.21.118.191 (static)

Subnet mask255.255.255.0

CANCEL

BACK

FINISH

Packages

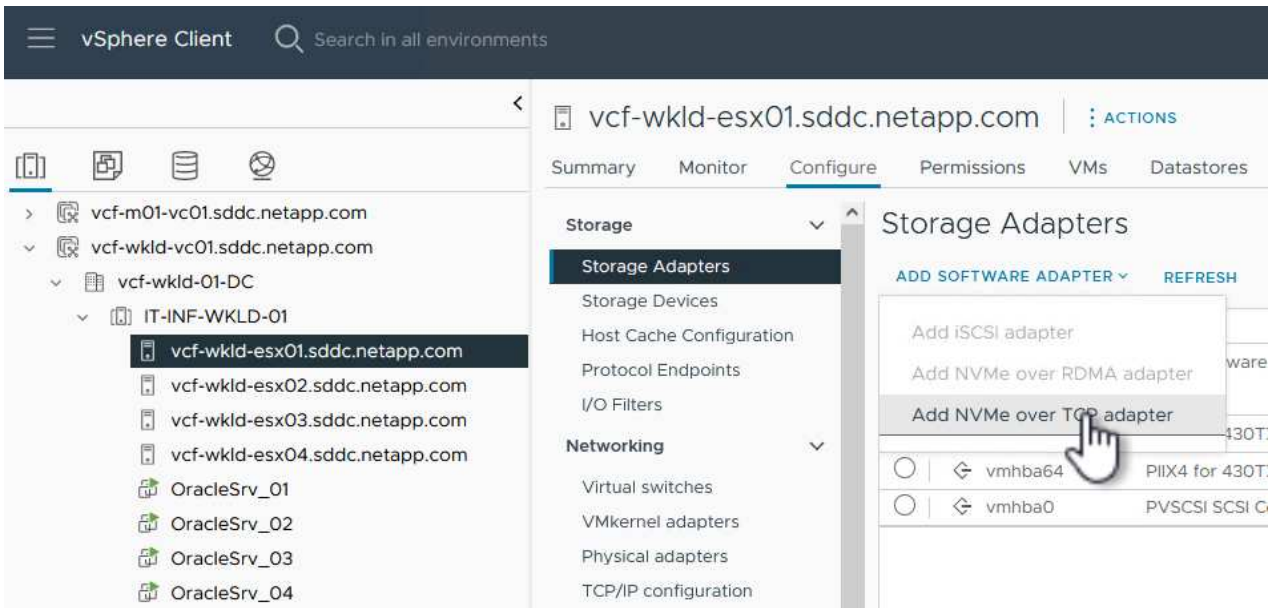
7. Repeat this process to create a VMkernel adapter for the second iSCSI network.

Add NVMe over TCP adapter

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

To install NVMe over TCP adapters and discover the NVMe controllers, complete the following steps:

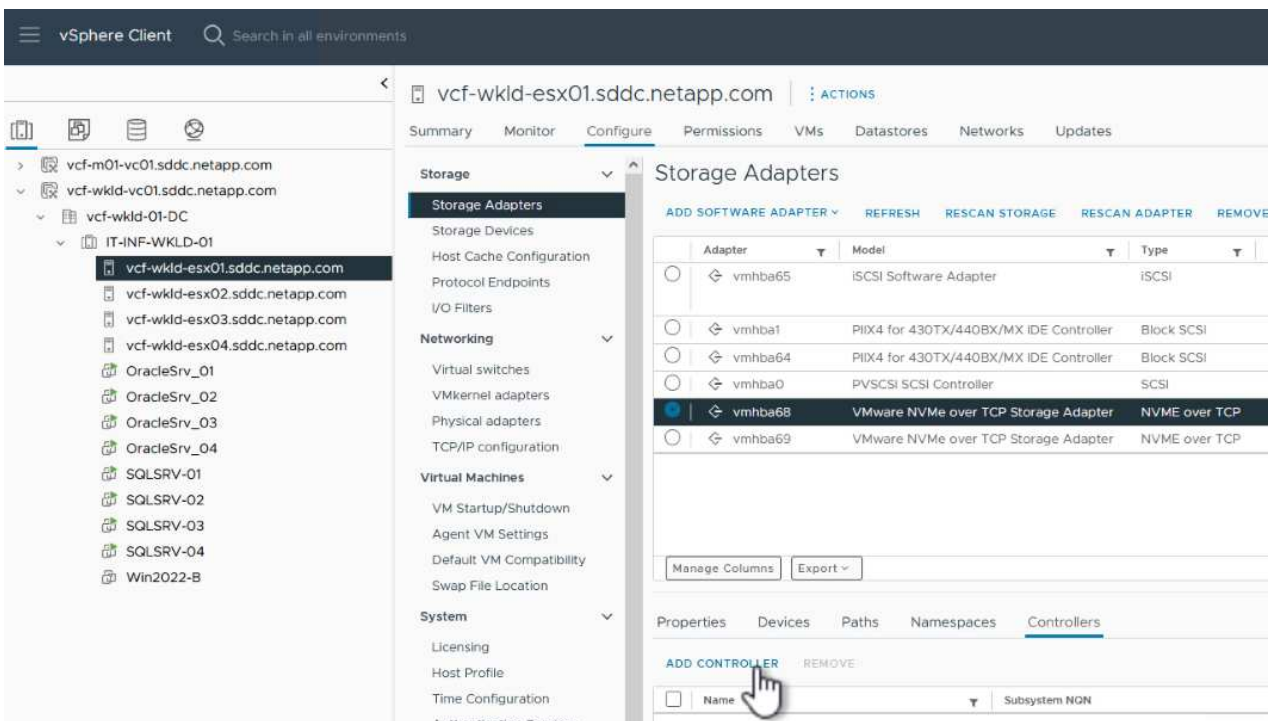
- 1. In the vSphere client navigate to one of the ESXi hosts in the workload domain cluster. From the **Configure** tab click on **Storage Adapters** in the menu and then, from the **Add Software Adapter** drop-down menu, select **Add NVMe over TCP adapter**.



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



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



5. In the **Add controller** window, select the **Automatically** tab and complete the following steps.
 - Fill in an IP addresses for one of the SVM logical interfaces on the same network as the physical adapter assigned to this NVMe over TCP adapter.
 - Click on the **Discover Controllers** button.
 - From the list of discovered controllers, click the check box for the two controllers with network addresses aligned with this NVMe over TCP adapter.
 - Click on the **OK** button to add the selected controllers.

Add controller | vmhba68



Automatically

Manually

Host NQN

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

COPY

IP

172.21.118.189

Enter IPv4 / IPv6 address

☐ Central discovery controller

Port Number

Range more from 0

Digest parameter

☐ Header digest

☐ Data digest

DISCOVER CONTROLLERS

Select which controller to connect

<input type="checkbox"/>	Id	Subsystem NQN	Transport Type	IP	Port Number
<input checked="" type="checkbox"/>	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF_WKLD_04_NVMe_VCF_WKLD_04_NVMe	nvm	172.21.118.189	4420
<input checked="" type="checkbox"/>	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF_WKLD_04_NVMe_VCF_WKLD_04_NVMe	nvm	172.21.118.190	4420

Manage Columns

4 items

3

4

OK

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

Storage Adapters

ADD SOFTWARE ADAPTER ▾ REFRESH RESCAN STORAGE RESCAN ADAPTER REMOVE

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

Manage Columns

Export ▾

6 items

Properties **Devices** Paths Namespaces Controllers

REFRESH ATTACH DETACH RENAME

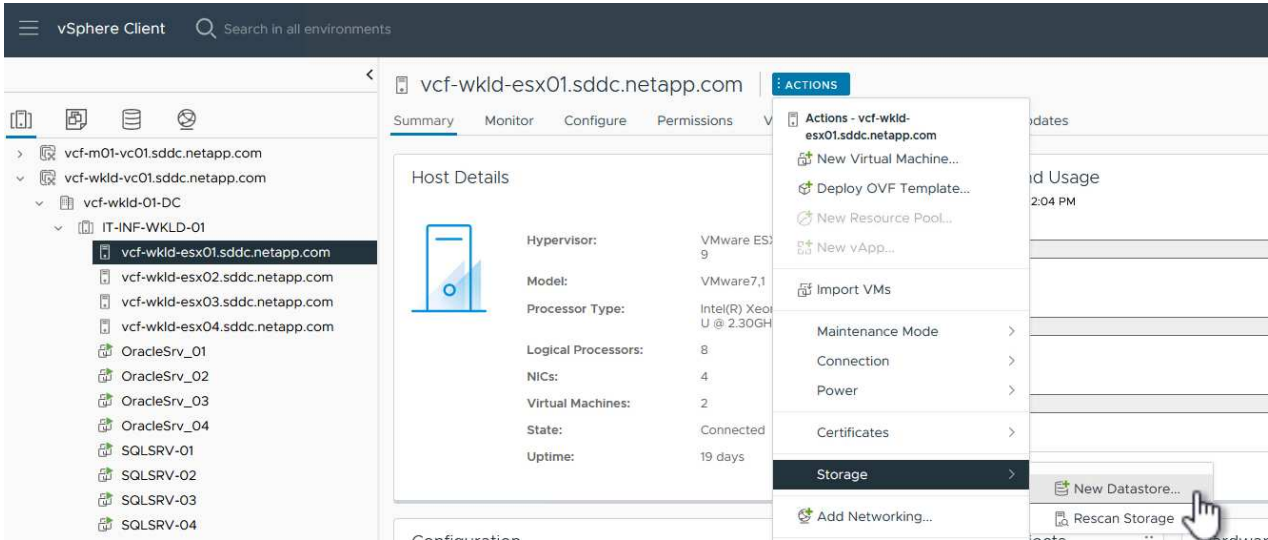
<input type="checkbox"/>	Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type	Transport
<input type="checkbox"/>	NVMe TCP Disk (uuid.929a6a90457647849146e09d6e55b076)	0	disk	3.00 TB	Not Consumed	Attached	Supported	Flash	TCPTN:RT

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

Deploy NVMe over TCP datastore

To create a VMFS datastore on the NVMe namespace, complete the following steps:

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



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

New Datastore

1 Type

2 Name and device selection

3 VMFS version

4 Partition configuration

5 Ready to complete

Name and device selection



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

Name VCF_WKLD_04_NVMe

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format	Cl V St
<input checked="" type="radio"/>	NVMe TCP Disk (uuid.929a6a90457647849146e09d6e55b076)	0	3.00 TB	Supported	Flash	512e	N
<input type="radio"/>	Local VMware Disk (naa.6000c29f83dcf1e42d230340deb66036)	0	4.00 GB	Not supported	Flash	512n	N
<input type="radio"/>	Local VMware Disk (naa.6000c291464644a835bc23d384813ac0)	0	75.00 GB	Not supported	Flash	512n	N

Manage Columns Export 3 items

CANCEL

BACK

NEXT

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

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

CANCEL

BACK

NEXT

- On the **Ready to complete** page, review the summary and click on **Finish** to create the datastore.
- Navigate to the new datastore in inventory and click on the **Hosts** tab. If configured correctly, all ESXi hosts in the cluster should be listed and have access to the new datastore.

vSphere Client

Search in all environments

Administrator@VCF.LOCAL

VCF_WKLD_04_NVMe

ACTIONS

Summary

Monitor

Configure

Permissions

Files

Hosts

VMs

Quick Filter

Enter value

<input type="checkbox"/>	Name	State	Status	Cluster	Consumed CPU %	Consumed Memory %	HA State	Uptime
<input type="checkbox"/>	vcf-wkld-esx01.sddc.netapp.co	Connected	✓ Normal	JT-INF-WKLD-Q	15%	13%	✓ Connected (Secondary)	19 days
<input type="checkbox"/>	vcf-wkld-esx02.sddc.netapp.co	Connected	✓ Normal	JT-INF-WKLD-Q	9%	15%	✓ Running (Primary)	19 days
<input type="checkbox"/>	vcf-wkld-esx03.sddc.netapp.co	Connected	✓ Normal	JT-INF-WKLD-Q	9%	21%	✓ Connected (Secondary)	19 days
<input type="checkbox"/>	vcf-wkld-esx04.sddc.netapp.co	Connected	✓ Normal	JT-INF-WKLD-Q	11%	4%	✓ Connected (Secondary)	19 days

Additional information

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

For information on configuring VCF refer to [VMware Cloud Foundation Documentation](#).

Add an FC-based VMFS datastore as supplemental storage to 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.

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

VCF Supplemental datastore is provisioned as part of day-2 operations using vCenter. This scenario covers the following high level steps:

- Deployment of ONTAP tools on management domain
- Register VI workload vCenter servers to ONTAP tools
- Define Storage backend on ONTAP tools plugin for VMware vSphere
- Provision VMFS on FC transport

Prerequisites

This scenario requires the following components and configurations:

- 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.

NetApp recommends multipath for FC LUNs.

For complete information on configuring fibre channel on ONTAP storage systems, refer to [SAN storage management](#) in the ONTAP 9 documentation.

For more information on using VMFS with ONTAP storage systems, refer to the [Deployment Guide for VMFS](#).

Deployment Steps for VI workload domain

To deploy ONTAP Tools and use it to create a VMFS datastore on the VCF VI workload domain, complete the following steps:

- [Register VI workload vCenter to enable the vCenter Plugin](#)
- [Define Storage backend using vSphere client interface](#)
- [Provision VMFS on FC](#)

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

[VMFS\(FC\) Datastore as Supplemental Storage for VCF Management Domain](#)

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](#)
- [3-2-1 Data Protection for VMware with SnapCenter Plug-in and BlueXP backup and recovery for VMs](#)

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

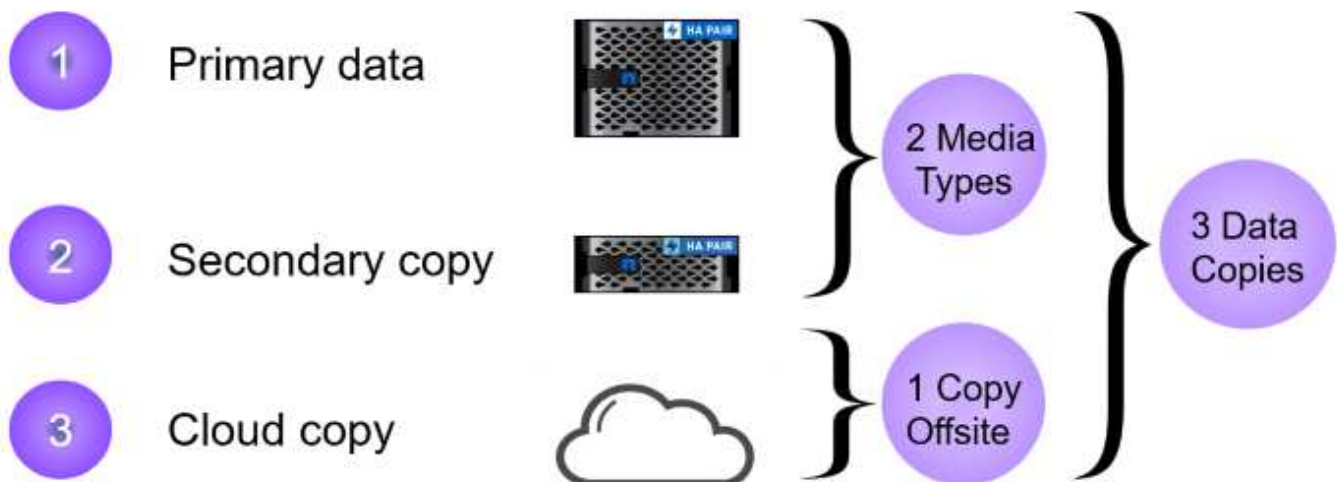
This scenario requires the following components and configurations:

- 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 BlueXP backup and recovery for VMs. For more information refer to the solution [3-2-1 Data Protection for VMware with SnapCenter Plug-in and BlueXP backup and recovery for VMs](#).



Deployment Steps

To deploy the SnapCenter Plug-in and use it to create backups, and restore VMs and datastores, complete the following steps:

Deploy and use SCV to protect data in a VI workload domain

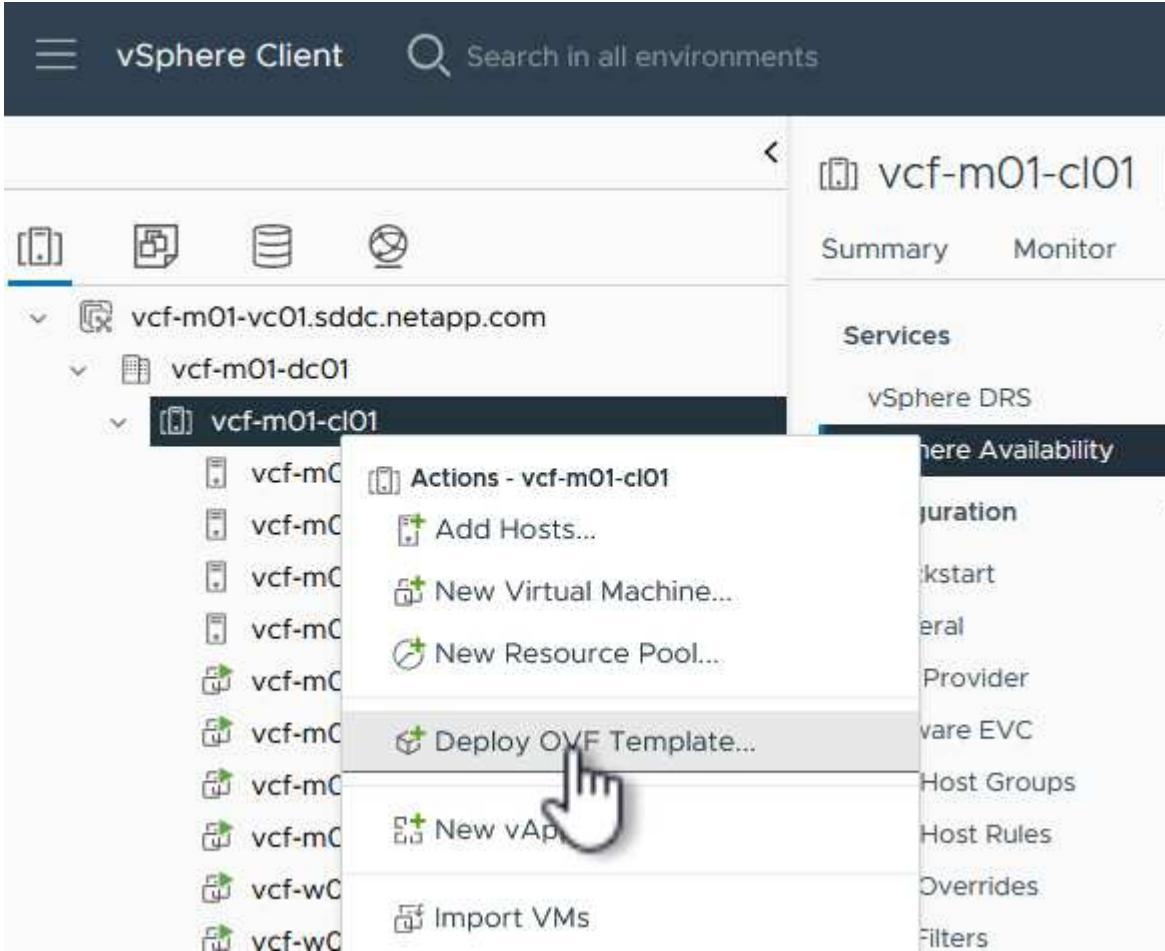
Complete the following steps to deploy, configure, and use SCV to protect data in a VI workload domain:

Deploy the SnapCenter Plug-in for VMware vSphere

The SnapCenter Plug-in is hosted on the VCF management domain but registered to the vCenter for the VI workload domain. One SCV instance is required for each vCenter instance and, keep in mind that, a Workload domain can include multiple clusters managed by a single vCenter instance.

Complete the following steps from the vCenter client to deploy SCV to the VI workload domain:

1. Download the OVA file for the SCV deployment from the download area of the NetApp support site [HERE](#).
2. From the management domain vCenter Client, select to **Deploy OVF Template....**



3. In the **Deploy OVF Template** wizard, click on the **Local file** radio button and then select to upload the previously downloaded OVF template. Click on **Next** to continue.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

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

☐ URL

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

☒ Local file

UPLOAD FILES

scv-5.0P2-240310_1514.ova

- 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.
- On the **Select a compute resource** page, select the management domain cluster or specific ESXi host within the cluster to install the VM to.
- Review information pertaining to the OVF template on the **Review details** page and agree to the licensing terms on the **Licensing agreements** page.
- 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	
<input checked="" type="radio"/>	mgmt_01_iscsi	--	3 TB	3.71 TB	2.5 TB	V
<input type="radio"/>	vcf-m01-cl01-ds-vsant01	--	999.97 GB	49.16 GB	957.54 GB	V
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V

Compatibility

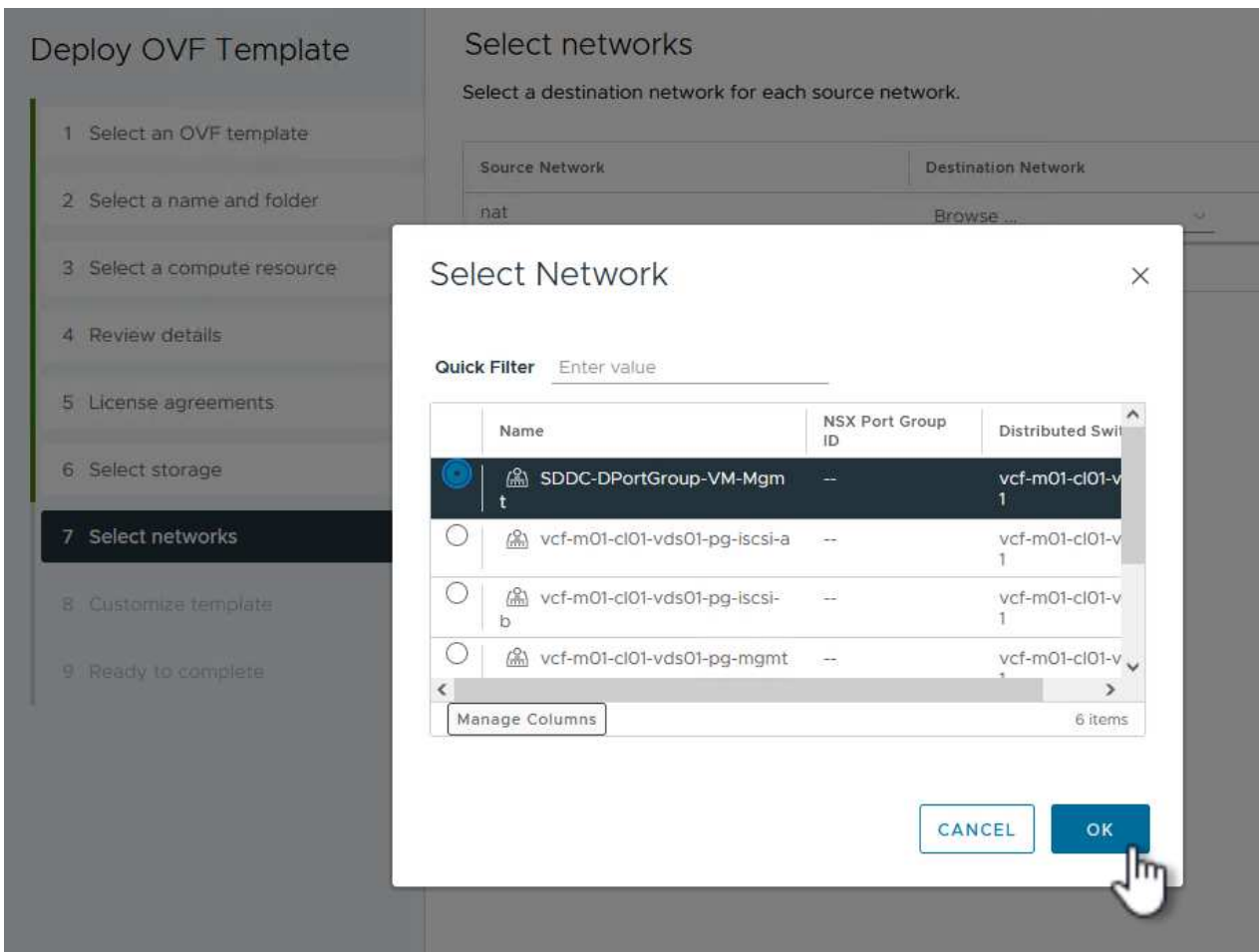
✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

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.



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.

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.

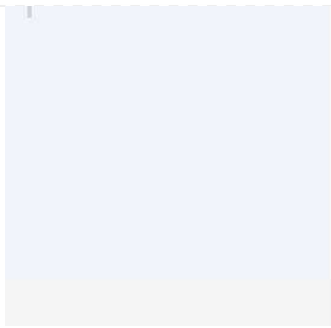
1. Register to existing vCenter		4 settings
1.1 vCenter Name(FQDN) or IP Address	cf-wkld-vc01.sddc.netapp.com	
1.2 vCenter username	administrator@vcf.local	
1.3 vCenter password	Password
	Confirm Password
1.4 vCenter port	443	
2. Create SCV Credentials		2 settings
2.1 Username	admin	
2.2 Password	Password
	Confirm Password
3. System Configuration		1 settings

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

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.

5.2 Time Zone setting

Sets the selected timezone setting for the VM

CANCEL

BACK

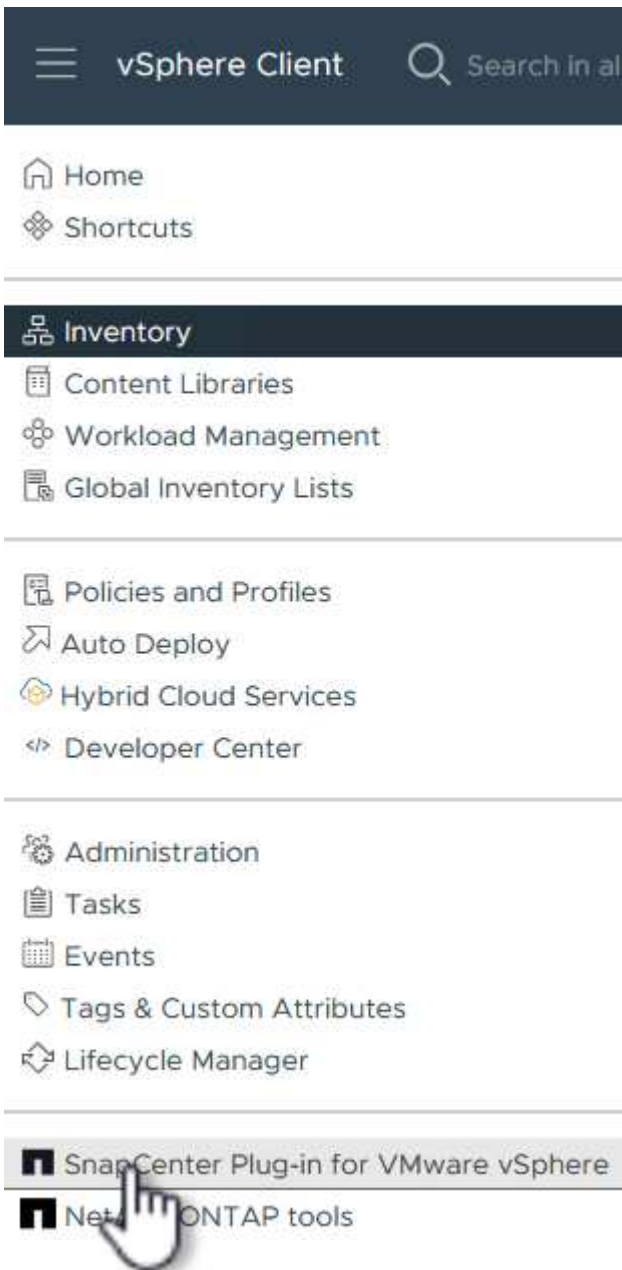
NEXT

10. Finally, on the **Ready to complete page**, review all settings and click on Finish to start the deployment.

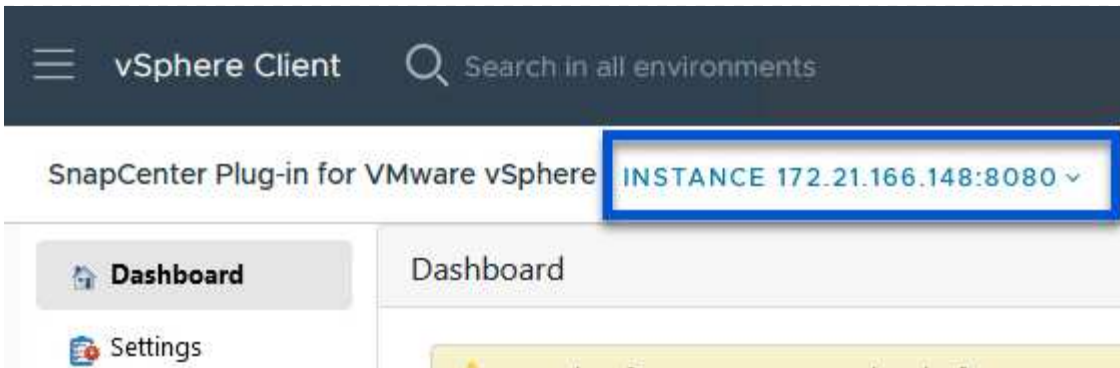
Add Storage Systems to SCV

Once the SnapCenter Plug-in is installed complete the following steps to add storage systems to SCV:

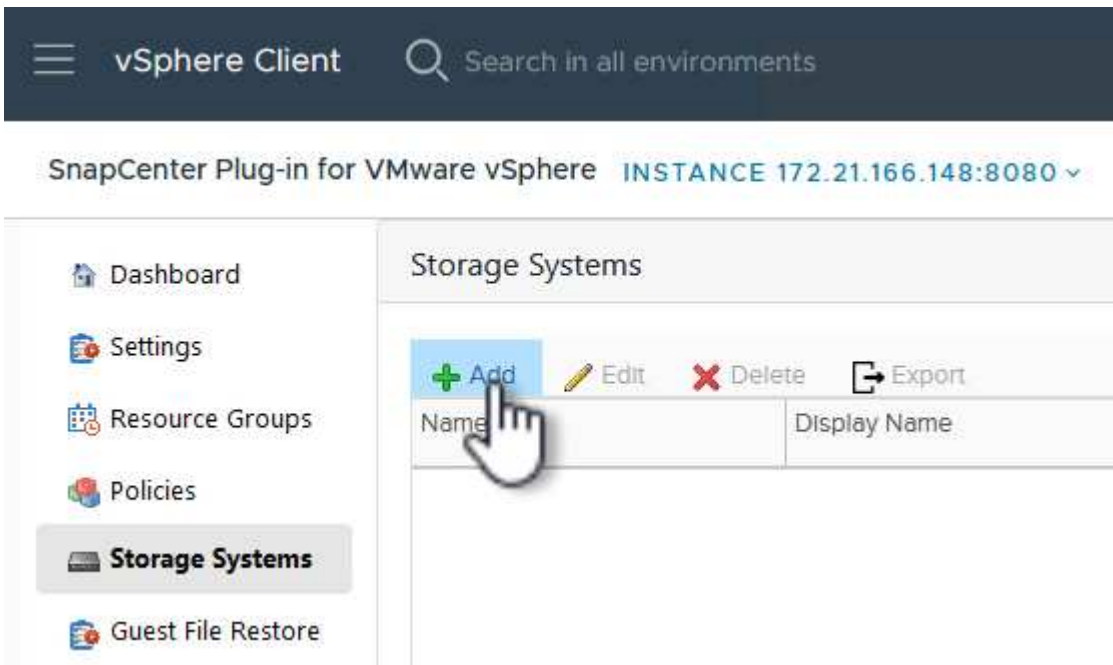
1. SCV can be accessed from the main menu in the vSphere Client.



2. At the top of the SCV UI interface, select the correct SCV instance that matches the vSphere cluster to be protected.



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	<input type="text" value="172.16.9.25"/>
Authentication Method	<input checked="" type="radio"/> Credentials <input type="radio"/> Certificate
Username	<input type="text" value="admin"/>
Password	<input type="password" value="••••••••"/>
Protocol	<input type="text" value="HTTPS"/>
Port	<input type="text" value="443"/>
Timeout	<input type="text" value="60"/> Seconds
<input type="checkbox"/> Preferred IP	<input type="text" value="Preferred IP"/>
Event Management System(EMS) & AutoSupport Setting	
<input type="checkbox"/> Log Snapcenter server events to syslog	
<input type="checkbox"/> Send AutoSupport Notification for failed operation to storage system	

CANCEL

ADD



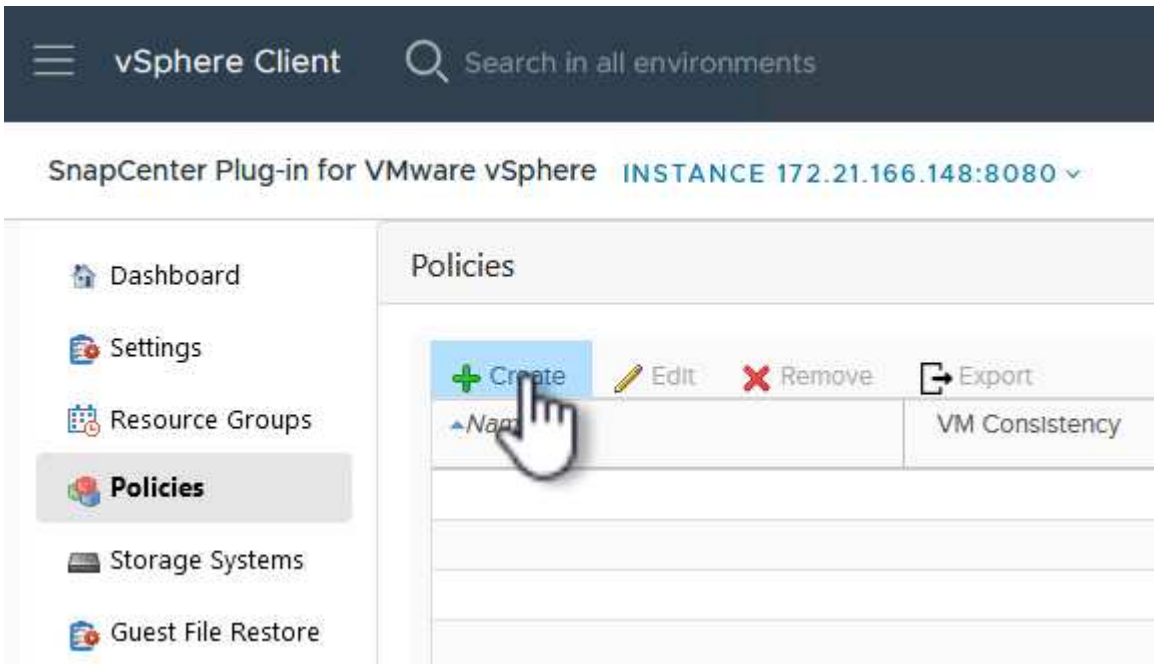
5. Repeat this procedure for any additional storage systems to be managed, including any systems to be used as secondary backup targets.

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	<input type="text" value="Daily_Snapmirror"/>
Description	<input type="text" value="description"/>
Frequency	<input type="text" value="Daily"/>
Locking Period	<input type="checkbox"/> Enable Snapshot Locking
Retention	<input type="text" value="Days to keep"/> <input type="text" value="15"/>
Replication	<input checked="" type="checkbox"/> Update SnapMirror after backup <input type="checkbox"/> Update SnapVault after backup
	Snapshot label <input type="text"/>
Advanced	<input type="checkbox"/> VM consistency <input type="checkbox"/> Include datastores with independent disks
	Scripts <div><input type="text" value="Enter script path"/></div>

CANCEL

ADD

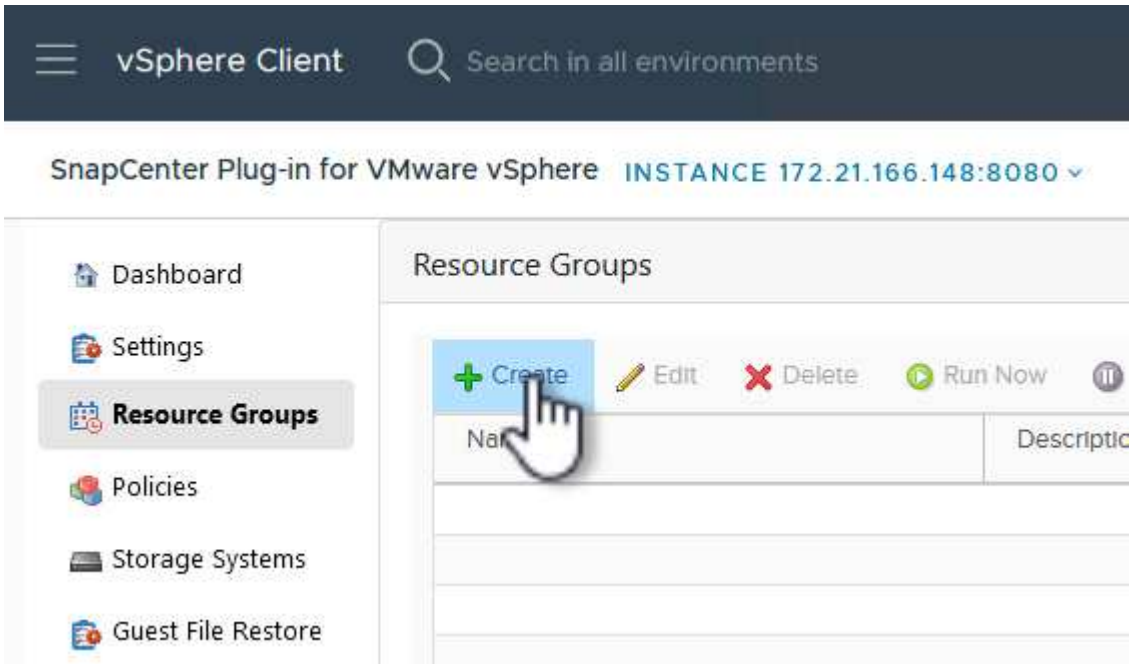


Create resource groups in SCV

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 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

✓ 1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Scope: Virtual Machines

Parent entity: VCF_WKLD_03_iSCSI

Enter available entity name

Available entities

OracleSrv_01
OracleSrv_02
OracleSrv_03
OracleSrv_04

Selected entities

SQLSRV-01
SQLSRV-02
SQLSRV-03
SQLSRV-04

BACK

NEXT

FINISH

CANCEL

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

✓ 1. General info & notification

✓ 2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

☐ 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.

BACK

NEXT

FINISH

CANCEL

5. On the **Policies** page select a previously created policy or multiple policies that will be used with this resource group. Click on **Next** to continue.

Create Resource Group

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

[+ Create](#)

[illegible]

BACK NEXT FINISH CANCEL

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

BACK

NEXT

FINISH

CANCEL

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	Frequency	Snapshot Locking Period
	Daily_Snapmir...	Daily	-

BACK NEXT **FINISH** CANCEL

8. With the resource group created click on the **Run Now** button to run the first backup.

vSphere Client Search in all environments

SnapCenter Plug-in for VMware vSphere INSTANCE 172.21.166.148:8080

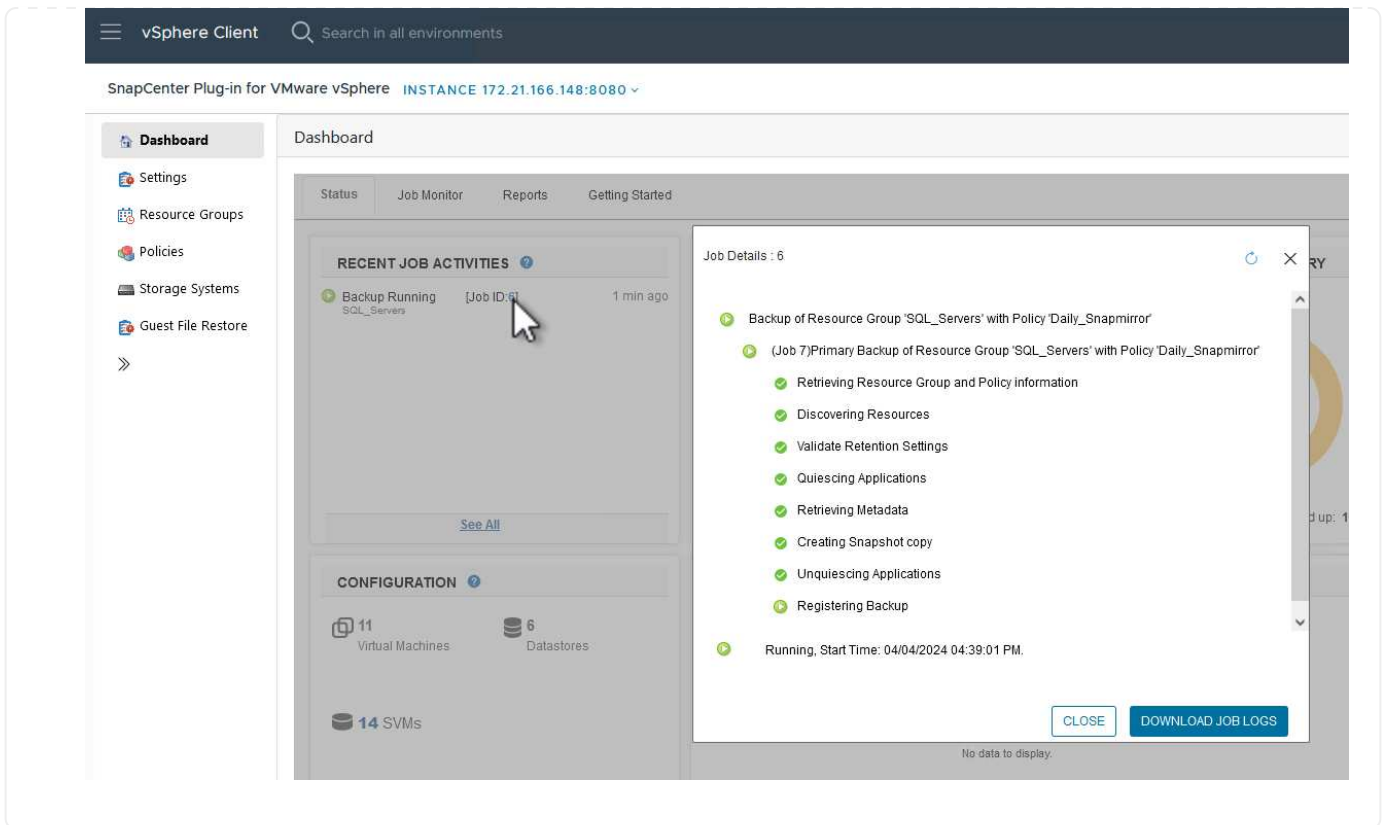
Dashboard Settings **Resource Groups** Policies Storage Systems Guest File Restore >>

Resource Groups

+ Create Edit Delete **Run Now** Suspend Resume Export

Name	Description	Policy
SQL_Servers		Daily_

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.



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.

OracleSrv_04

Summary Monitor Configure Permissions

Guest OS Virtual Mac

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

vcf-wkl

OracleS

OracleS

OracleS

OracleS

SQLSR

SQLSR

SQLSR

SQLSR

Win20

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

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

Create Resource Group

Add to Resource Group

Attach Virtual Disk(s)

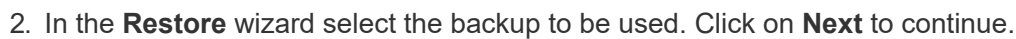
Detach Virtual Disk(s)

Restore

File Restore

Manage Columns

Run



- **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

Restore VM

Restore Location

Entire virtual machine

▼

☐

☐ 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

▼

BACK

NEXT

FINISH

CANCEL

VCF_WKLD_03_ISCSI

Click on **Next** to continue.

- 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.

BACK

NEXT

FINISH

CANCEL

6. The restore job progress can be monitored from the **Recent Tasks** pane in the vSphere Client and from the job monitor in SCV.

Dashboard

Settings

Resource Groups

Policies

Storage Systems

Guest File Restore

>>

Dashboard

Status Job Monitor Reports Getting Started

RECENT JOB ACTIVITIES

- Restore Running [Job ID:18]
VCF_WKLD_ISCI_Datastore_04-04-20... 1 min ago
- Backup Successful [Job ID:15]
VCF_WKLD_ISCI_Datastore 8 min ago
- Backup Successful [Job ID:12]
VCF_WKLD_ISCI_Datastore 13 min ago
- Backup Successful [Job ID:9]
SQL_Servers 13 min ago
- Backup Successful [Job ID:6]
SQL_Servers 19 min ago

[See All](#)

CONFIGURATION

11 Virtual Machines 6 Datastores

14 SVMs

2 Resource Groups 2 Backup Policies

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.

CLOSE

DOWNLOAD JOB LOGS

No data to display.

Recent Tasks Alarms

Task Name	Target	Status	Details	Initiator	Queued For	Start Time
NetApp Mount Datastore	vcf-wkld-esx04.sdd c.netapp.com	35%	Mount operation completed successfully.	VCF.LOCAL\Administrator	6 ms	04/04/2024, 4:58:27 PM
NetApp Restore	vcf-wkld-esx04.sdd c.netapp.com	2%	Restore operation started.	VCF.LOCAL\Administrator	10 ms	04/04/2024, 4:58:27 PM

Manage Columns

Running

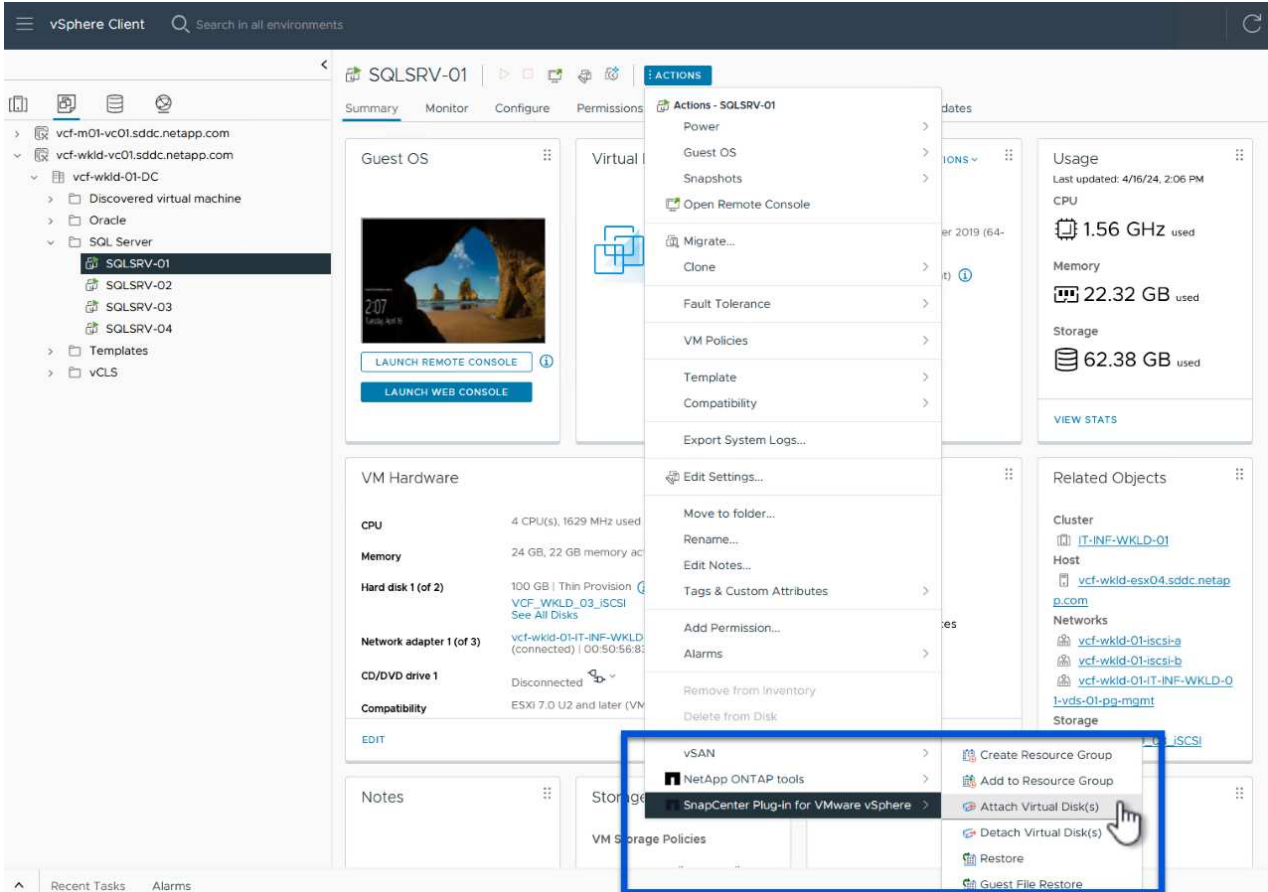
[More Tasks](#)

Restore VMDKs using SnapCenter Plug-in

ONTAP Tools allows full restore of VMDK's to their original location or the ability to attach a VMDK as a new disk to a host system. In this scenario a VMDK will be attached to a Windows host in order to access the file system.

To attach a VMDK from a backup, complete the following steps:

1. In the vSphere Client navigate to a VM and, from the **Actions** menu, select **SnapCenter Plug-in for VMware vSphere > Attach Virtual Disk(s)**.



2. In the **Attach Virtual Disk(s)** wizard, select the backup instance to be used and the particular VMDK to be attached.

Attach Virtual Disk(s)



[Click here to attach to alternate VM](#)

Backup

Search for Backups



(This list shows primary backups. **1** 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

<input type="checkbox"/> Virtual disk	Location
<input type="checkbox"/> [VCF_WKLD_03_ISCSI] SQLSRV-01/SQLSRV-01.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_ISCI_Datastore_04-17-2024_09.50.01.0218
<input checked="" type="checkbox"/> [VCF_WKLD_03_ISCSI] SQLSRV-01/SQLSRV-01_1.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_ISCI_Datastore_04-17-2024_09.50.01.0218

2

3

CANCEL

ATTACH



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](#)

Backup

Search for Backups



(This list shows primary backups.)

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

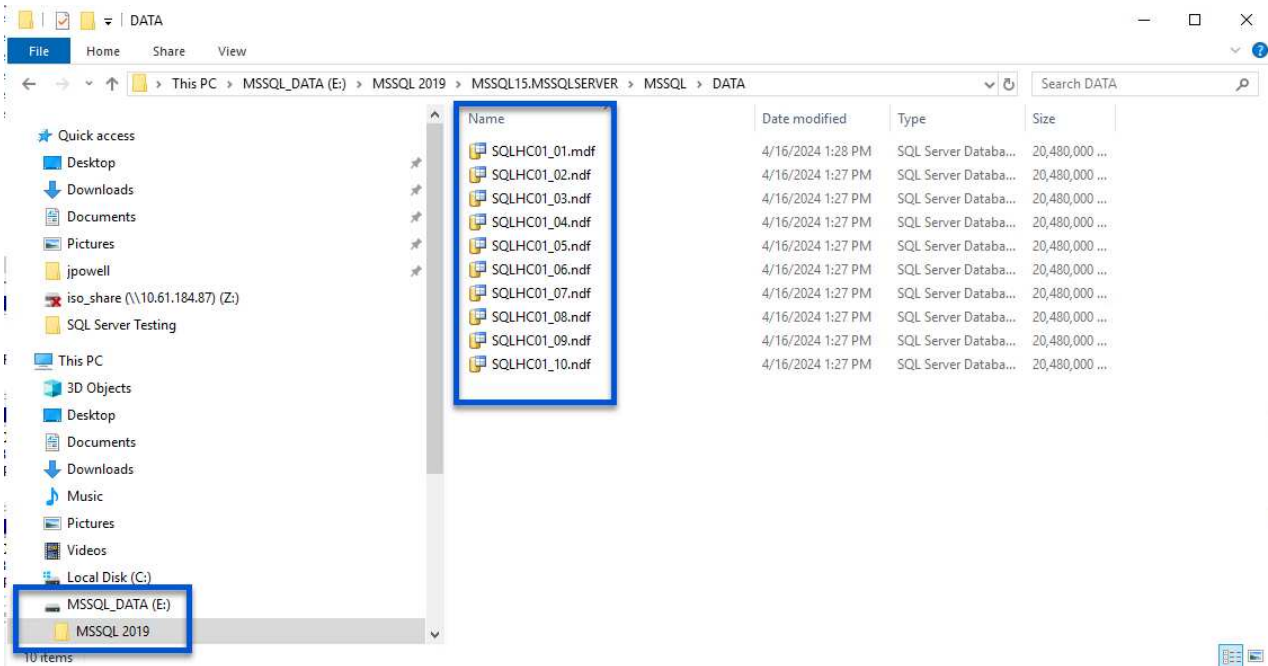
CLEAR

OK

CANCEL

ATTACH

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.



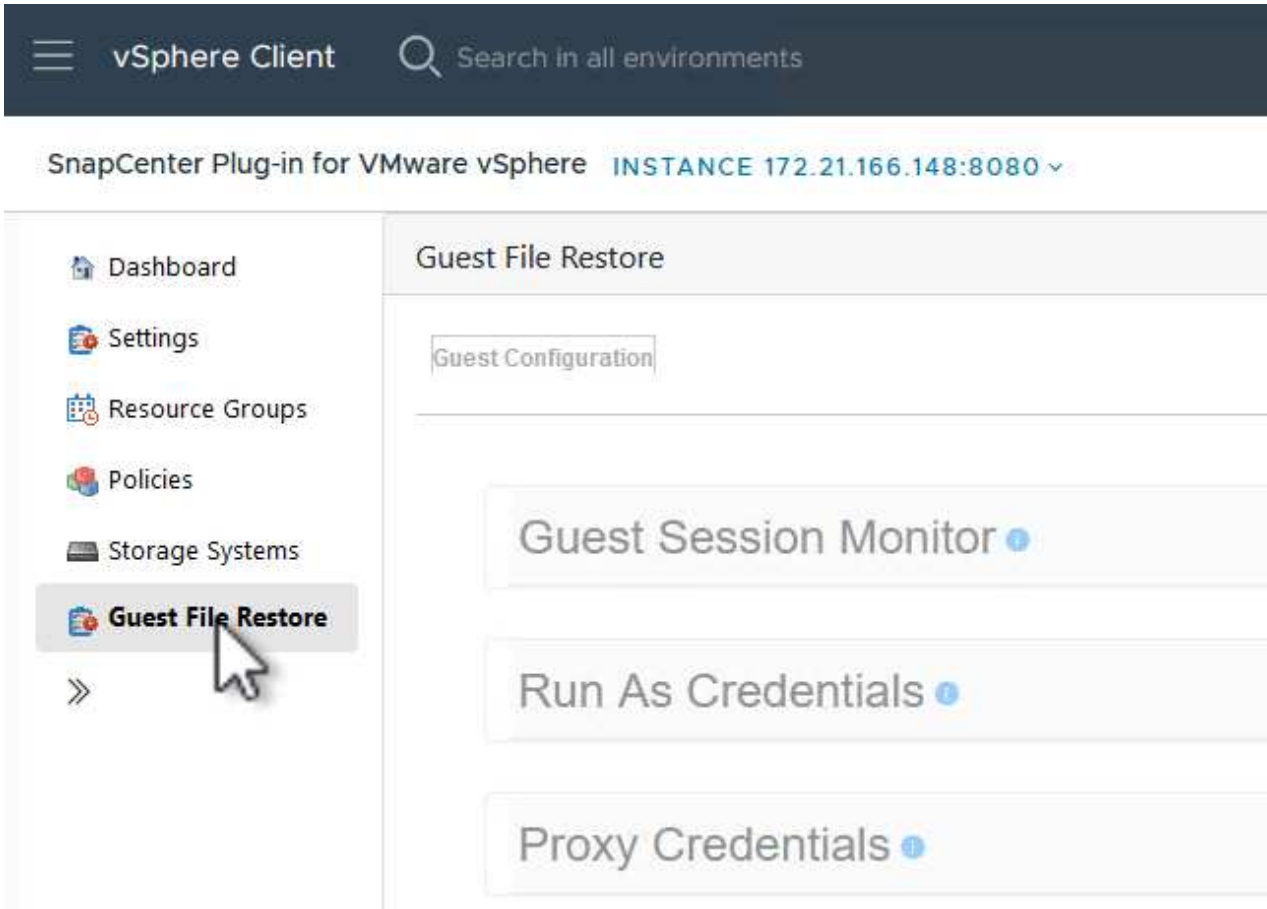
Guest File System Restore using SnapCenter Plug-in

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 

Username 

Password 

Authentication Mode

VM Name

Select VM



CANCEL

SAVE

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

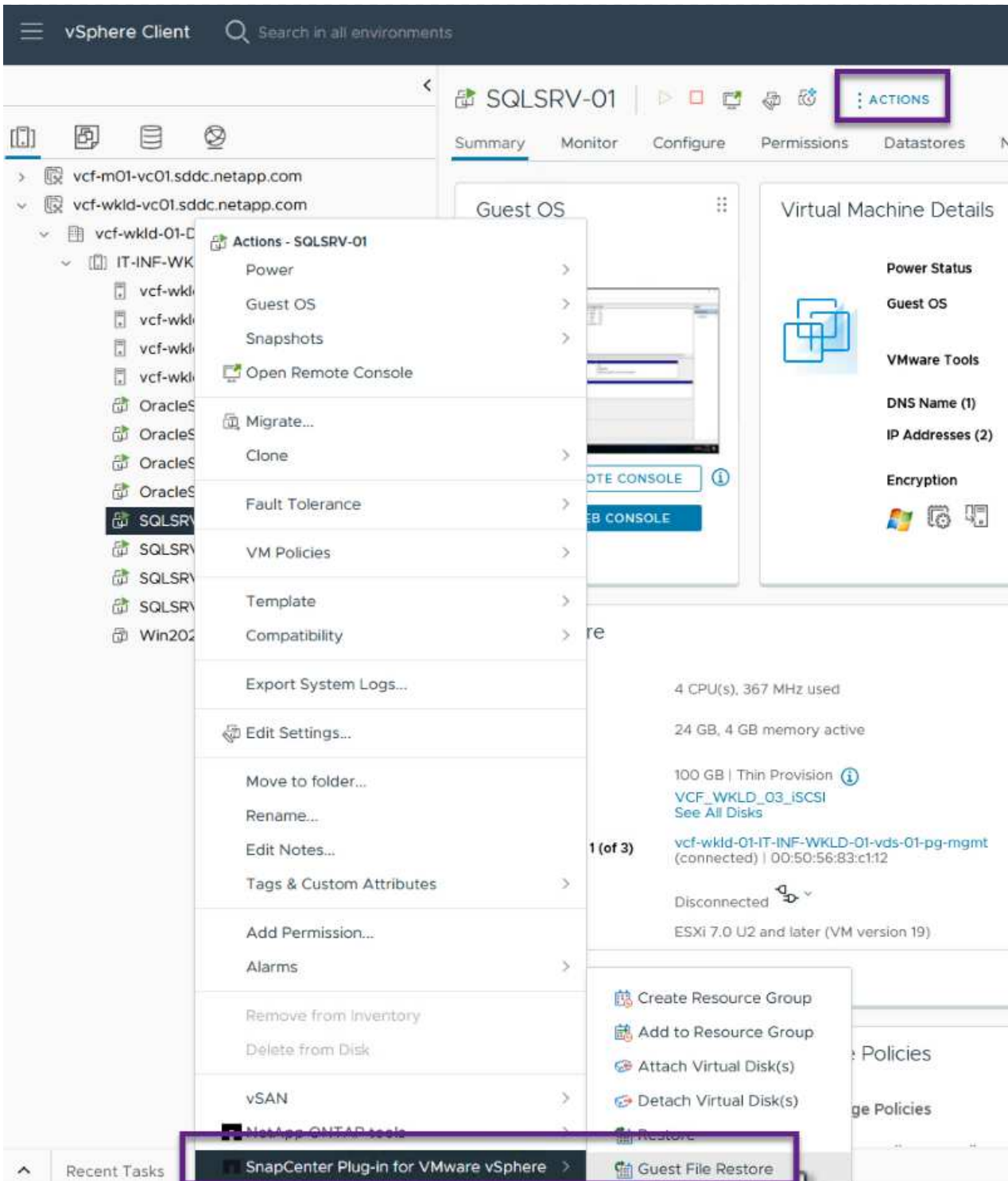
☐ Search by Virtual Machine name

CANCEL

SAVE



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.

×

3. Summary

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

CANCEL

Storage

YCE WORLD 02 15

- 217

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:

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

- Finally, review the **Summary** page and click on **Finish** to begin the Guest File System Restore session.
- 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.

The screenshot shows the vSphere Client interface with the SnapCenter Plug-in for VMware vSphere. The left sidebar contains navigation links: Dashboard, Settings, Resource Groups, Policies, Storage Systems, and Guest File Restore. The main content area is titled "Guest File Restore" and shows the "Guest Configuration" tab. Below this, the "Guest Session Monitor" table is displayed, showing a single session. The table has columns for Backup Name, Source VM, Disk Path, Guest Mount Path, Time To Expire, and Browse Files. A hand icon is shown clicking on the "Browse Files" column. Below the table, there are sections for "Run As Credentials" and "Proxy Credentials".

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]SCSI(c-202404161419...	E1	23h:58m	

- 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 

	Name	Size	
<input type="checkbox"/>	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!

CANCEL

RESTORE

Select Restore Location

Select address family for UNC path:

☒ IPv4

☐ IPv6

Restore to path

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

CANCEL 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.

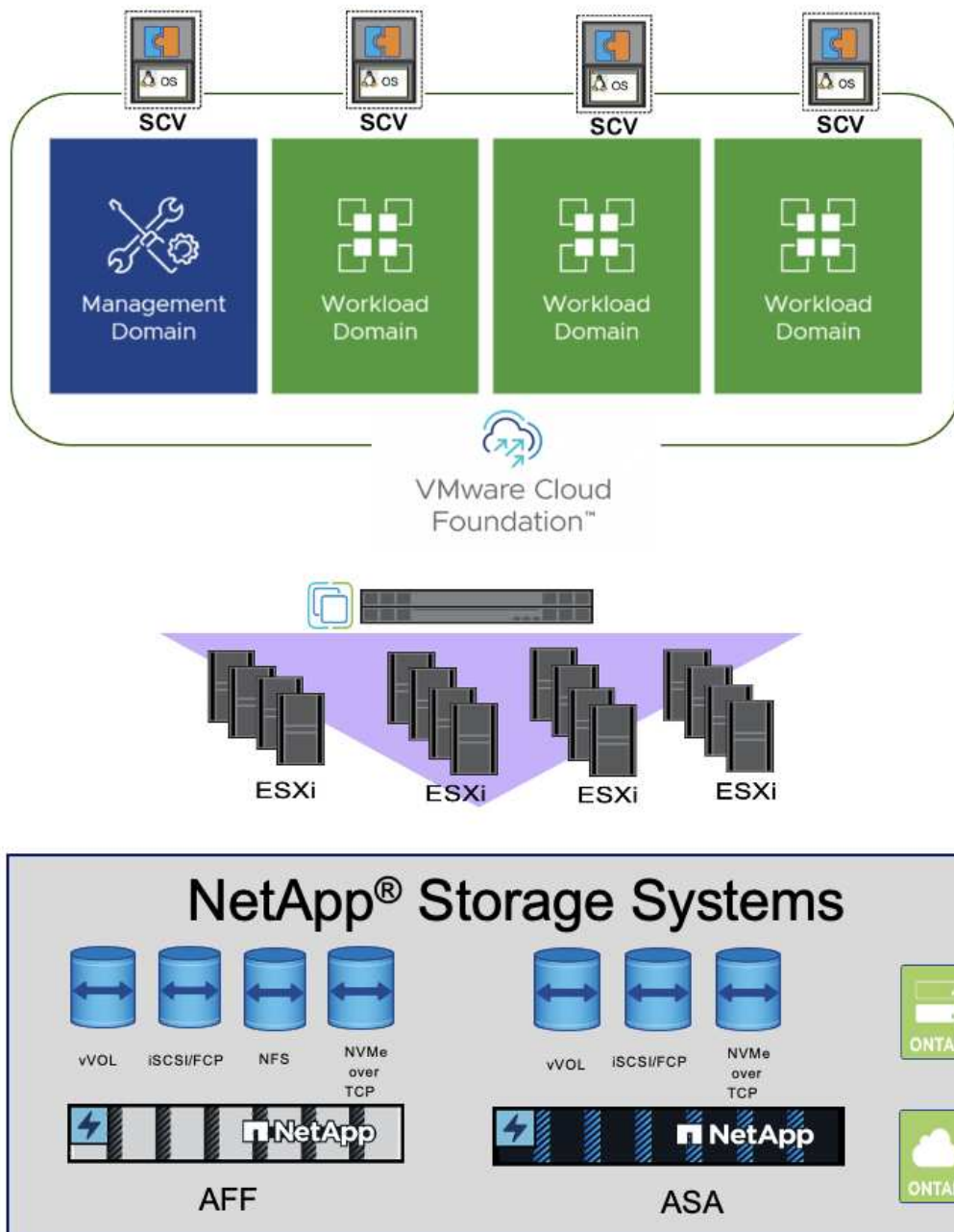
Audience

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](#).

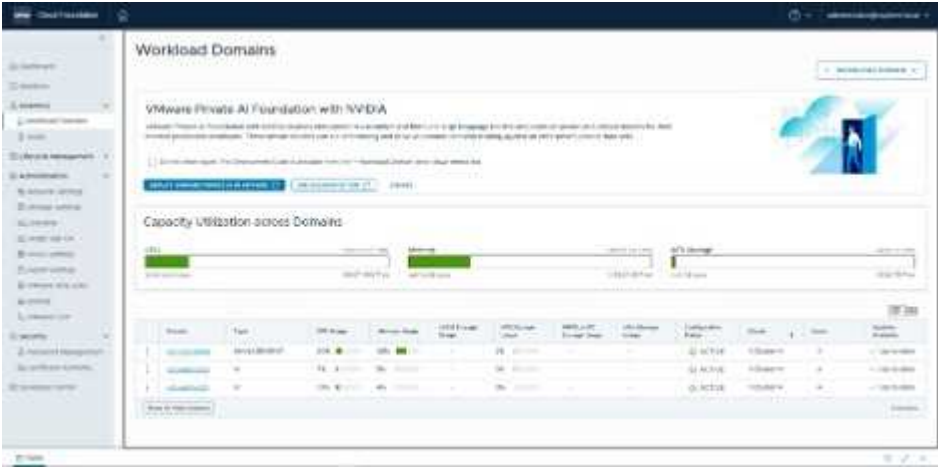


The 3-2-1 backup rule is a data protection strategy that involves making three copies of data, storing them on two different types of media, and keeping one copy off-site. BlueXP backup and recovery is a cloud based tool for data management that provides a single control plane for a wide range of backup and recovery operations across both on-premises and cloud environments. Part of the NetApp BlueXP backup and recovery suite is a feature that integrates with SCV (on-premises) to extend a copy of the data to object storage in the cloud. This establishes a third copy of the data offsite that is sourced from the primary or secondary storage backups. BlueXP backup and recovery makes it easy to set up storage policies that transfer copies of your data from either of these two on-prem locations. For more details, check [3-2-1 Data Protection for VMware with SnapCenter Plug-in and BlueXP backup and recovery for VMs](#).

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](#).



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	<input type="text"/>
2.2 Password	<input type="password"/>
3. Setup Network Properties	1 settings
3.1 Setup IPv4 Network Properties	4 settings
3.2 Setup IPv6 Network Properties	0 settings
5. Setup Date and Time	2 settings

CANCEL BACK NEXT

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.

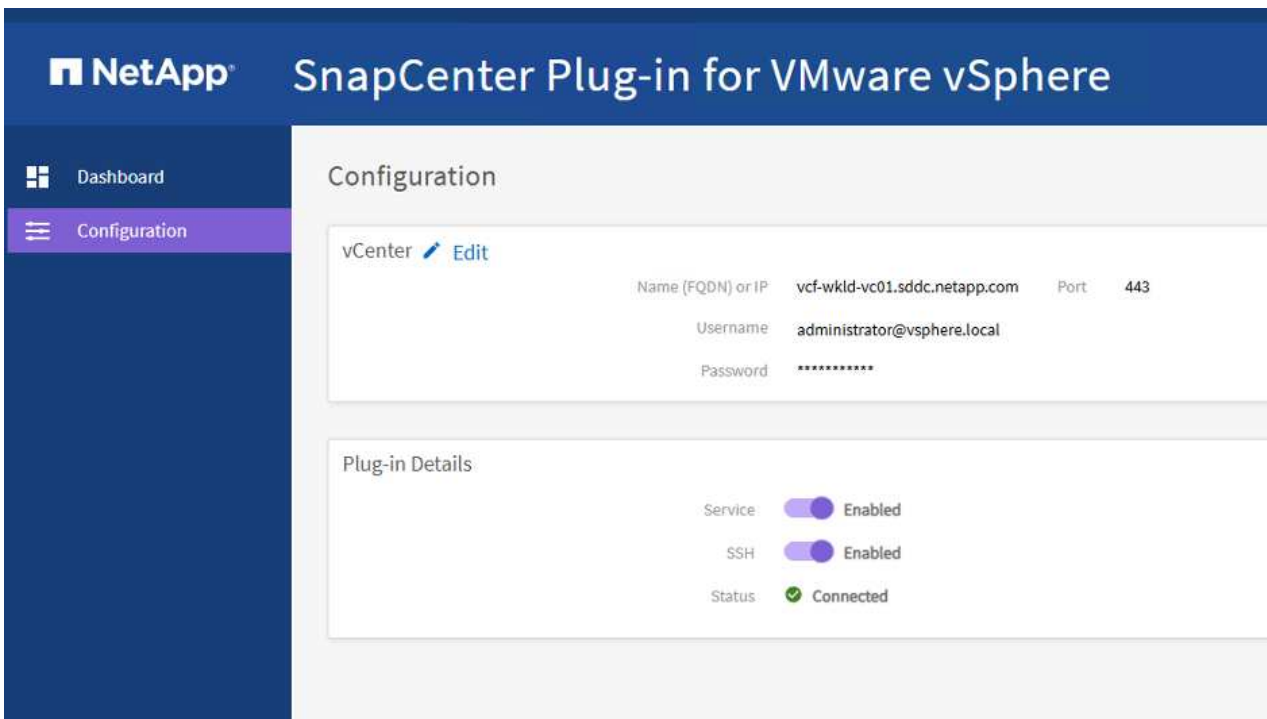

```
System Configuration Menu:
-----
1 ) Reboot virtual machine
2 ) Shut down virtual machine
3 ) Change 'maint' user password
4 ) Change time zone
5 ) Change NTP server
6 ) Enable SSH access
7 ) Increase jail disk size (/jail)
8 ) Upgrade
9 ) Install VMware Tools
10 ) Generate MFA Token
b ) Back
x ) 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.



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. 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

wkid01

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

Advanced

CANCEL

ADD

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



✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

✓ 4. Policies

✓ 5. Schedules

✓ 6. Summary

Name	wkld01RG								
Description									
Send email	Never								
Latest Snapshot name	None ⓘ								
Custom snapshot format	None ⓘ								
Entities	wkld01								
Spanning	True								
Policies	<table><thead><tr><th>Name</th><th>Frequency</th><th>Snapshot Locking Period</th></tr></thead><tbody><tr><td>wkld01</td><td>Daily</td><td>1 Day</td></tr></tbody></table>	Name	Frequency	Snapshot Locking Period	wkld01	Daily	1 Day		
Name	Frequency	Snapshot Locking Period							
wkld01	Daily	1 Day							

BACK

NEXT

FINISH

CANCEL

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.

Restore


✓ 1. Select backup

✓ 2. Select scope

✓ 3. Select location

4. Summary

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.

BACK

NEXT

FINISH

CANCEL

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

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
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

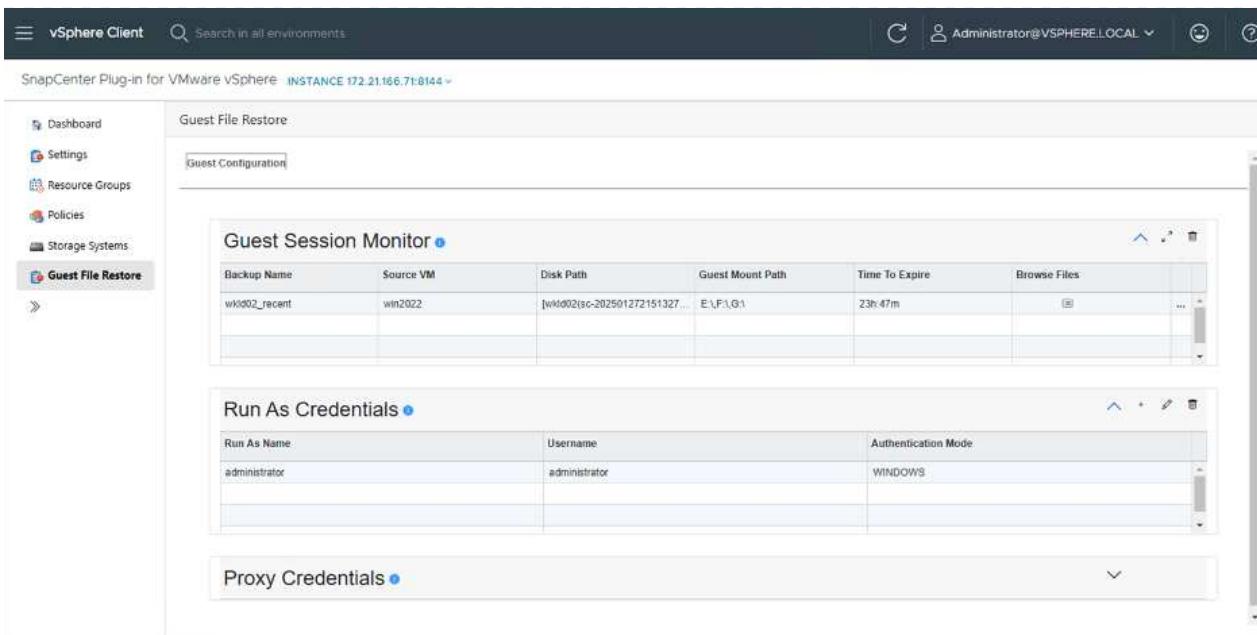
Backup type	Location
Primary	172.21.118.118:vcf_md_wkld02:wkld02_recent

CANCEL

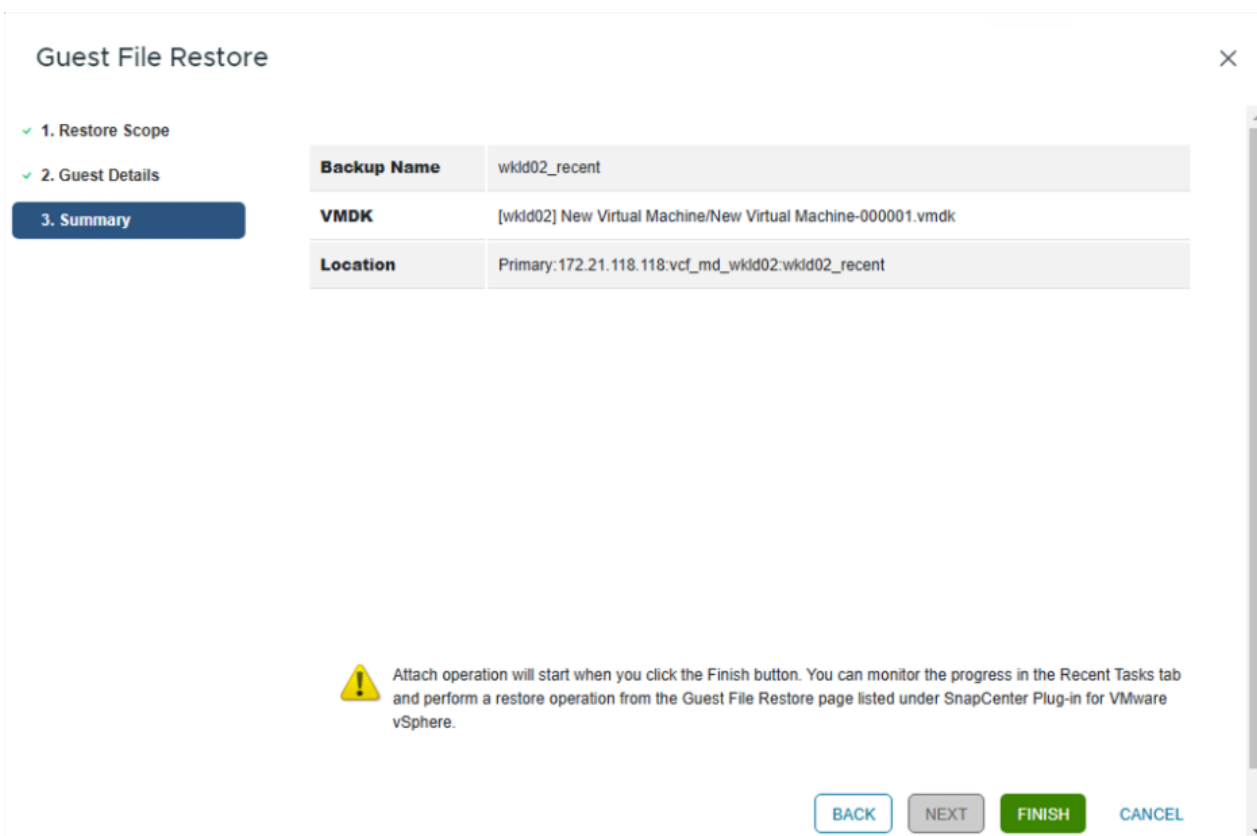
MOUNT

Files and Folders Restore Steps

1. When you attach a virtual 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".



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.



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

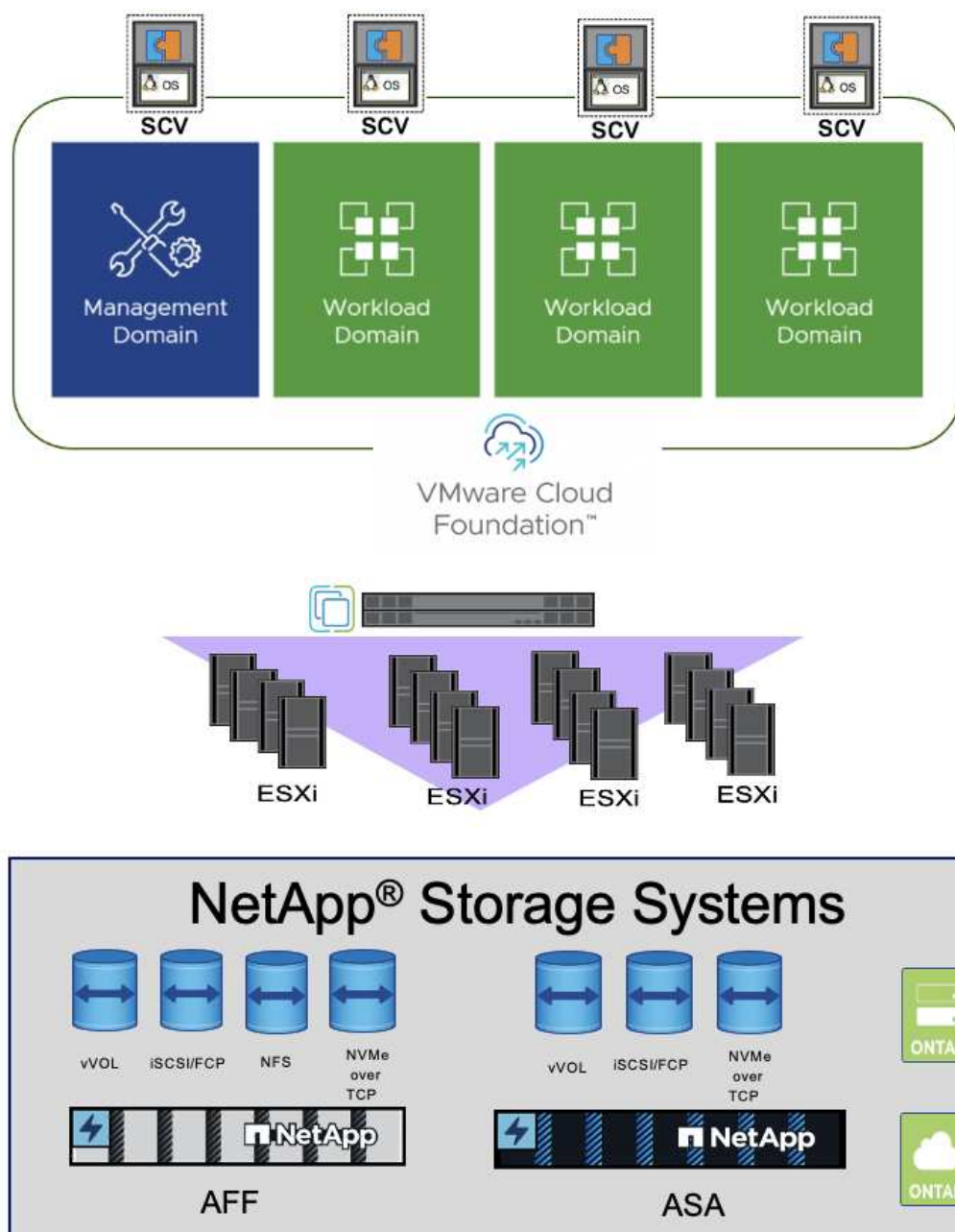
SCV is a powerful tool designed to facilitate fast, space-efficient, crash-consistent, and VM-consistent backup and restore operations for VMs, datastores, and files and folders in VMware environments. SCV is deployed as a Linux virtual appliance using an OVA file and leverages a remote plug-in architecture.

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. BlueXP 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. Part of the NetApp BlueXP backup and recovery suite is a feature that integrates with SCV (on-premises) to extend a copy of the data to object storage in the cloud. This establishes a third copy of the data offsite that is sourced from the primary or secondary storage backups.

BlueXP backup and recovery makes it easy to set up storage policies that transfer copies of your data from either of these two on-prem locations. For more details, check [3-2-1 Data Protection for VMware with SnapCenter Plug-in and BlueXP backup and recovery for VMs](#).

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.

Restore


✓ 1. Select backup

✓ 2. Select scope

✓ 3. Select location

4. Summary

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.

BACK

NEXT

FINISH

CANCEL

- 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

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_02-19-2025_...	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

CANCEL

MOUNT

- 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

<input type="checkbox"/> Virtual disk	Location
<input checked="" type="checkbox"/> [VCF_NVMe_DS] Win2022NVMe/Win2022NVMe.vmdk	Primary:VCF_NVMe:VCF_WKLD_DS:VCF-NVMe_02-17-2025_18.57.02.0697

CANCEL

ATTACH

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 attach a virtual 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".

The screenshot shows the vSphere Client interface with the SnapCenter Plug-in for VMware vSphere. The left sidebar contains navigation options: Dashboard, Settings, Resource Groups, Policies, Storage Systems, and Guest File Restore (selected). The main area displays the 'Guest File Restore' configuration for a specific instance (172.21.166.71:8144).

Guest Session Monitor

Backup Name	Source VM	Disk Path	Guest Mount Path	Time To Expire	Browse Files
wkld02_recent	win2022	[wkld02(sic-202501272151327...	E:\F\G\1	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 Summary to confirm.

Guest File Restore

✓ 1. Restore Scope

✓ 2. Guest Details

3. Summary

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.

BACK

NEXT

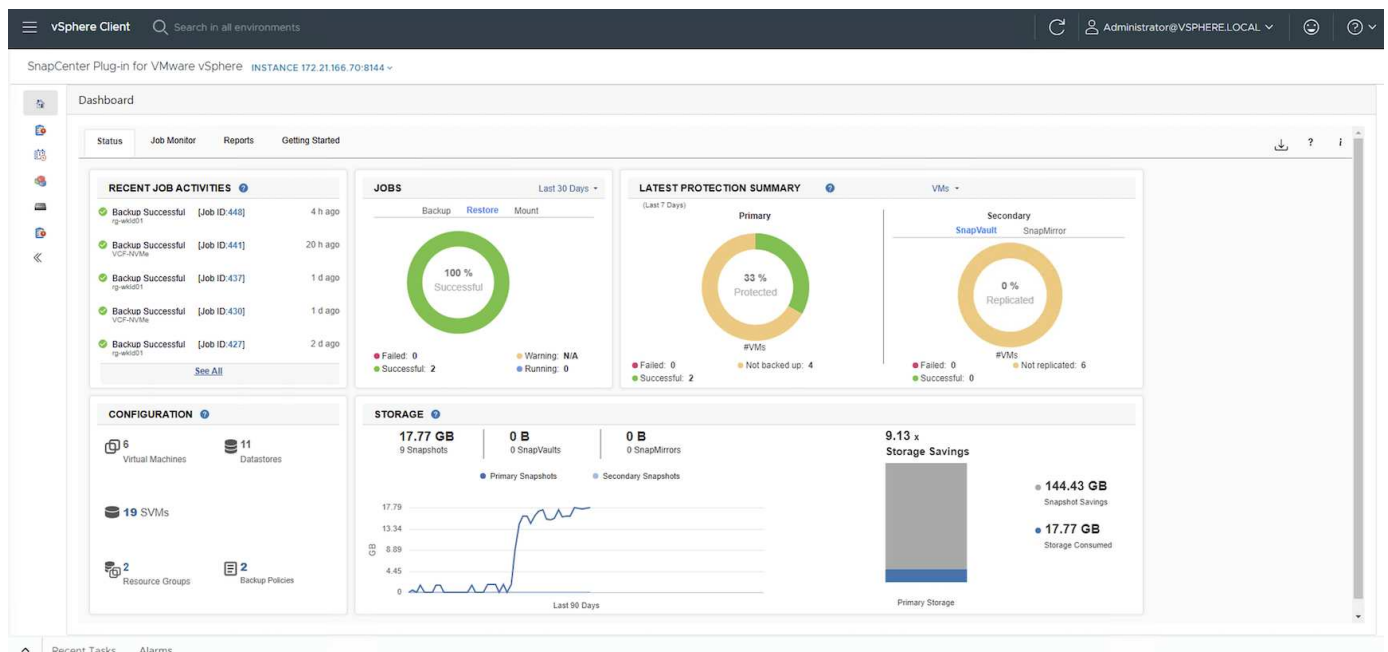
FINISH

CANCEL

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 VMware datastores with BlueXP

Learn about protecting VMware datastores using BlueXP disaster recovery

Learn about the NetApp solutions for disaster recovery using BlueXP disaster recovery for VMware. This provides for robust solutions for disaster recovery using block-level replication from a primary site to a disaster recovery site.

BlueXP DRaaS is an effective and economical method to safeguard workloads against site failures and data integrity issues, including ransomware attacks. Furthermore, NetApp BlueXP DRaaS enhances this strategy by providing a managed, cloud-based disaster recovery solution, ensuring swift recovery and minimal downtime during disasters.

Please refer to the following solutions for the technical details.

- [DR using BlueXP DRaaS for VMFS Datastores](#)
- [DR using BlueXP DRaaS for NFS Datastores](#)

Configure 3-2-1 data protection for VMware with SnapCenter plug-in for VMware vSphere and BlueXP backup and recovery

Configure a 3-2-1 data protection strategy for VMware environments using the SnapCenter plug-in for VMware vSphere and BlueXP backup and recovery. This procedure includes setting up backups of VMs and datastores on primary and secondary ONTAP clusters, configuring the plug-in and BlueXP, and managing data replication to cloud or offsite storage for reliable recovery.

The 3-2-1 backup strategy is an industry accepted data protection method, providing a comprehensive approach to safeguarding valuable data. This strategy is reliable and ensures that even if some unexpected disaster strikes, there will still be a copy of the data available.

Overview

The strategy is comprised of three fundamental rules:

1. Keep at least three copies of your data. This ensures that even if one copy is lost or corrupted, you still have at least two remaining copies to fall back on.
2. Store two backup copies on different storage media or devices. Diversifying storage media helps protect against device-specific or media-specific failures. If one device gets damaged or one type of media fails, the other backup copy remains unaffected.
3. Finally, ensure that at least one backup copy is offsite. Offsite storage serves as a fail-safe against localized disasters like fires or floods that could render onsite copies unusable.

This solution document covers a 3-2-1 backups solution using SnapCenter Plug-in for VMware vSphere (SCV) to create primary and secondary backups of our on-premises virtual machines and BlueXP backup and

recovery for virtual machines to backup a copy of our data to cloud storage or StorageGRID.





Use Cases

This solution addresses the following use cases:

- Backup and restore of on-premises virtual machines and datastores using SnapCenter Plug-in for VMware vSphere.
- Backup and restore of on-premises virtual machines and datastores, hosted on ONTAP clusters, and backed up to object storage using BlueXP backup and recovery for virtual machines.

NetApp ONTAP Data Storage

ONTAP is NetApp's industry leading storage solution that offers unified storage whether you access over SAN or NAS protocols. The 3-2-1 backup strategy ensures on-premises data is protected on more than one media type and NetApp offers platforms ranging from high-speed flash to lower-cost media.

FAS	AFF C-Series	AFF A-Series	ASA A-Series
			
Hybrid flash storage	Capacity all-flash storage	Performance all-flash storage	All-flash SAN storage
Unified (file, block, object)	Unified (file, block, object)	Unified (file, block, object)	Block optimized
Lowest price storage	Balanced price storage	Premium priced storage	Aggressively priced storage
Tier 2 @ 5-10ms latency Backup / Low-cost DR	Refresh of hybrid flash, Tier 1 @ 2-4ms latency Tier 2 workloads VMware datastores	Ideal for Tier 1 business-critical workloads with <1ms latency	Ideal for Tier 1 Block Six Nines Guaranteed

For more information on all of NetApp's hardware platform's check out [NetApp Data Storage](#).

SnapCenter Plug-in for VMware vSphere

The SnapCenter Plugin for VMware vSphere is a data protection offering which is tightly integrated with VMware vSphere and allows easy management of backup and restores for virtual machines. As part of that solution, SnapMirror provides a fast and reliable method to create a second immutable backup copy of virtual machine data on a secondary ONTAP storage cluster. With this architecture in place, virtual machine restore operations can easily be initiated from either the primary or secondary backup locations.

SCV is deployed as a linux virtual appliance using an OVA file. The plug-in now uses a remote plug-in architecture. The remote plug-in runs outside of the vCenter server and is hosted on the SCV virtual appliance.

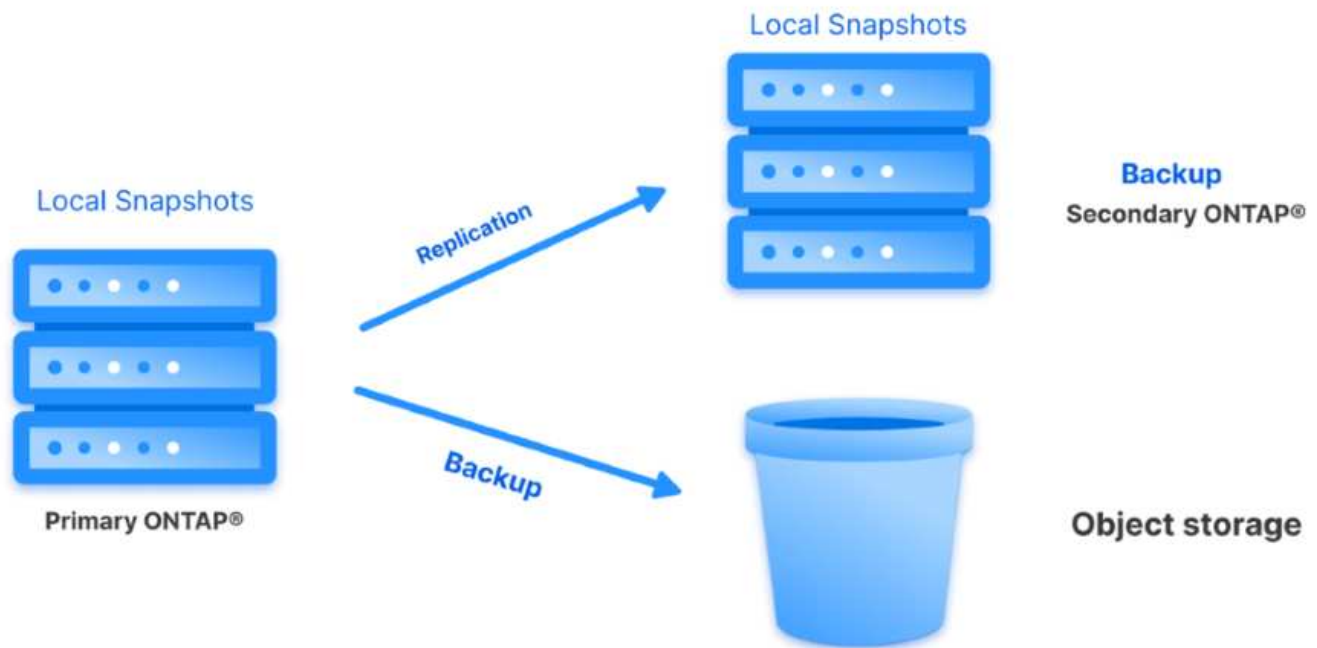
For detailed information on SCV refer to [SnapCenter Plug-in for VMware vSphere documentation](#).

BlueXP backup and recovery for virtual machines

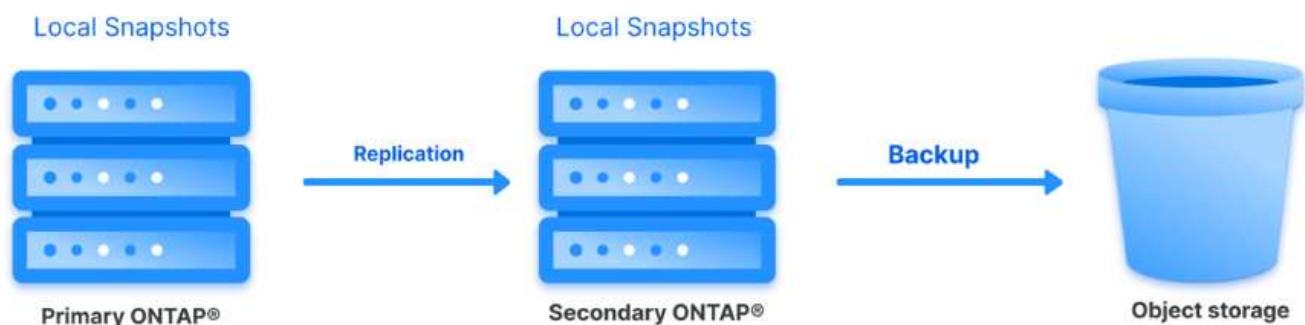
BlueXP backup and recovery is a cloud based tool for data management that provides a single control plane for a wide range of backup and recovery operations across both on-premises and cloud environments. Part of the NetApp BlueXP backup and recovery suite is a feature that integrates with the SnapCenter Plugin for VMware vSphere (on-premises) to extend a copy of the data to object storage in the cloud. This establishes a third copy of the data offsite that is sourced from the primary or secondary storage backups. BlueXP backup and recovery makes it easy to set up storage policies that transfer copies of your data from either of these two on-prem locations.

Choosing between the primary and secondary backups as the source in BlueXP Backup and Recovery will result in one of two topologies being implemented:

Fan-out Topology – When a backup is initiated by the SnapCenter Plug-in for VMware vSphere, a local snapshot is immediately taken. SCV then initiates a SnapMirror operation that replicates the most recent snapshot to the Secondary ONTAP cluster. In BlueXP Backup and Recovery, a policy specifies the primary ONTAP cluster as the source for a snapshot copy of the data to be transferred to object storage in your cloud provider of choice.



Cascading Topology – Creating the primary and secondary data copies using SCV is identical to the fan-out topology mentioned above. However, this time a policy is created in BlueXP Backup and Recovery specifying that the backup to object storage will originate from the secondary ONTAP cluster.



BlueXP backup and recovery can create backup copies of on-premises ONTAP snapshots to AWS Glacier, Azure Blob, and GCP Archive storage.



AWS Glacier and Deep Glacier



Azure Blob Archive



GCP Archive Storage

In addition, you can use NetApp StorageGRID as the object storage backup target. For more on StorageGRID refer to the [StorageGRID landing page](#).

Solution Deployment Overview

This list provides the high level steps necessary to configure this solution and execute backup and restore operations from SCV and BlueXP backup and recovery:

1. Configure SnapMirror relationship between the ONTAP clusters to be used for primary and secondary data copies.
2. Configure SnapCenter Plug-In for VMware vSphere.
 - a. Add Storage Systems
 - b. Create backup policies
 - c. Create resource groups
 - d. Run backup first backup jobs
3. Configure BlueXP backup and recovery for virtual machines
 - a. Add working environment
 - b. Discover SCV and vCenter appliances
 - c. Create backup policies
 - d. Activate backups
4. Restore virtual machines from primary and secondary storage using SCV.
5. Restore virtual machines from object storage using BlueXP backup and restore.

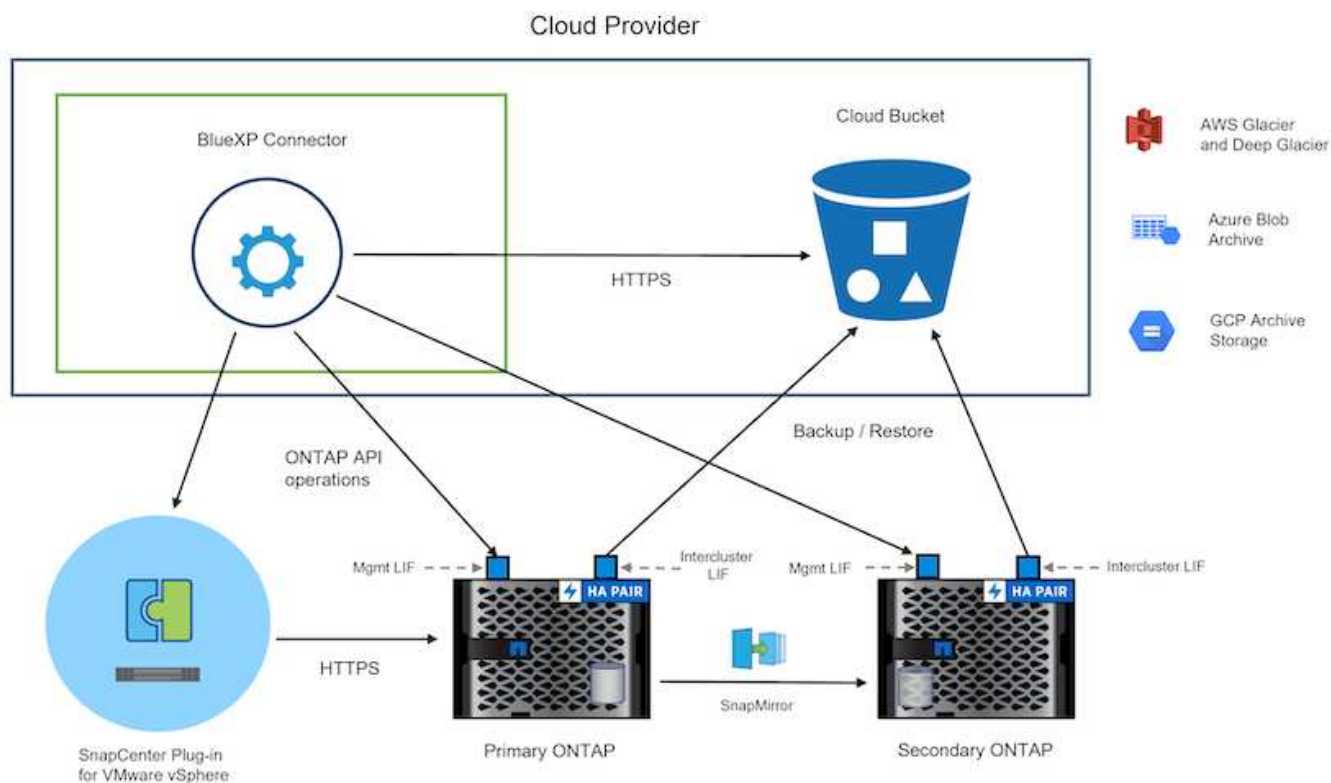
Prerequisites

The purpose of this solution is to demonstrate data protection of virtual machines running in VMware vSphere, VCF VI workload domains, or VCF management domains. Virtual machines in this solution are hosted on NFS datastores provided by NetApp ONTAP. This solution assumes the following components are configured and ready for use:

1. ONTAP storage cluster with NFS or VMFS datastores connected to VMware vSphere. Both NFS and VMFS datastores are supported. NFS datastores were utilized for this solution.
2. Secondary ONTAP storage cluster with SnapMirror relationships established for volumes used for NFS datastores.
3. BlueXP connector installed for cloud provider used for object storage backups.
4. Virtual machines to be backed are on NFS datastores residing on the primary ONTAP storage cluster.
5. Network connectivity between the BlueXP connector and on-premises ONTAP storage cluster management interfaces.
6. Network connectivity between the BlueXP connector and on-premises SCV appliance VM and between the BlueXP connector and vCenter.
7. Network connectivity between the on-premises ONTAP intercluster LIFs and the object storage service.
8. DNS configured for management SVM on primary and secondary ONTAP storage clusters. For more information refer to [Configure DNS for host-name resolution](#).

High Level Architecture

The testing / validation of this solution was performed in a lab that may or may not match the final deployment environment.



Solution Deployment

In this solution, we provide detailed instructions for deploying and validating a solution that utilizes SnapCenter Plug-in for VMware vSphere, along with BlueXP backup and recovery, to perform the backup and recovery of Windows and Linux virtual machines within a VMware vSphere cluster located in an on-premises data center. The virtual machines in this setup are stored on NFS datastores hosted by an ONTAP A300 storage cluster. Additionally, a separate ONTAP A300 storage cluster serves as a secondary destination for volumes replicated using SnapMirror. Furthermore, object storage hosted on Amazon Web Services and Azure Blob were employed as targets for a third copy of the data.

We will go over creating SnapMirror relationships for secondary copies of our backups managed by SCV and configuration of backup jobs in both SCV and BlueXP backup and recovery.

For detailed information on SnapCenter Plug-in for VMware vSphere refer to the [SnapCenter Plug-in for VMware vSphere documentation](#).

For detailed information on BlueXP backup and recovery refer to the [BlueXP backup and recovery documentation](#).

Establish SnapMirror relationships between ONTAP Clusters

SnapCenter Plug-in for VMware vSphere uses ONTAP SnapMirror technology to manage the transport of secondary SnapMirror and/or SnapVault copies to a secondary ONTAP Cluster.

SCV backup policies have the option of using SnapMirror or SnapVault relationships. The primary difference is that when using the SnapMirror option, the retention schedule configured for backups in the policy will be the same at the primary and secondary locations. SnapVault is designed for archiving and when using this option a separate retention schedule can be established with the SnapMirror relationship for the snapshot copies on the secondary ONTAP storage cluster.

Setting up SnapMirror relationships can be done in BlueXP where many of the steps are automated, or it can be done using System Manager and the ONTAP CLI. All of these methods are discussed below.

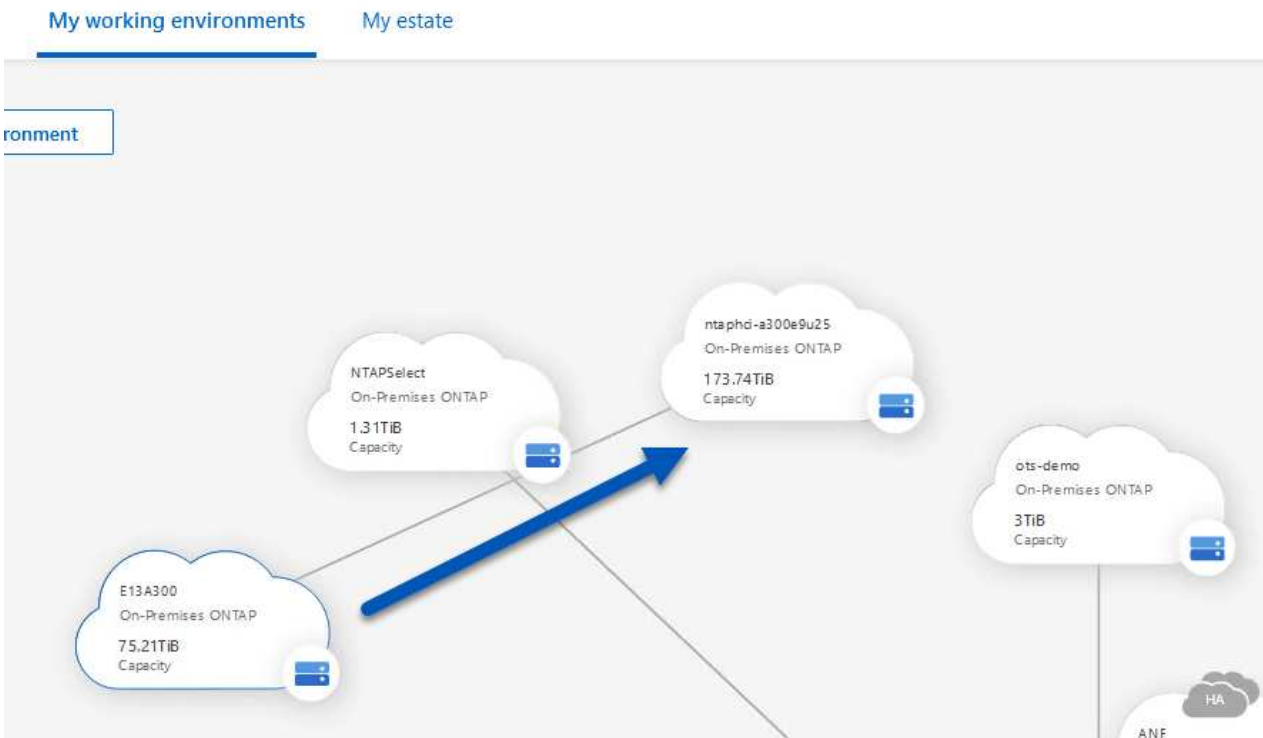
Establish SnapMirror relationships with BlueXP

The following steps must be completed from the BlueXP web console:

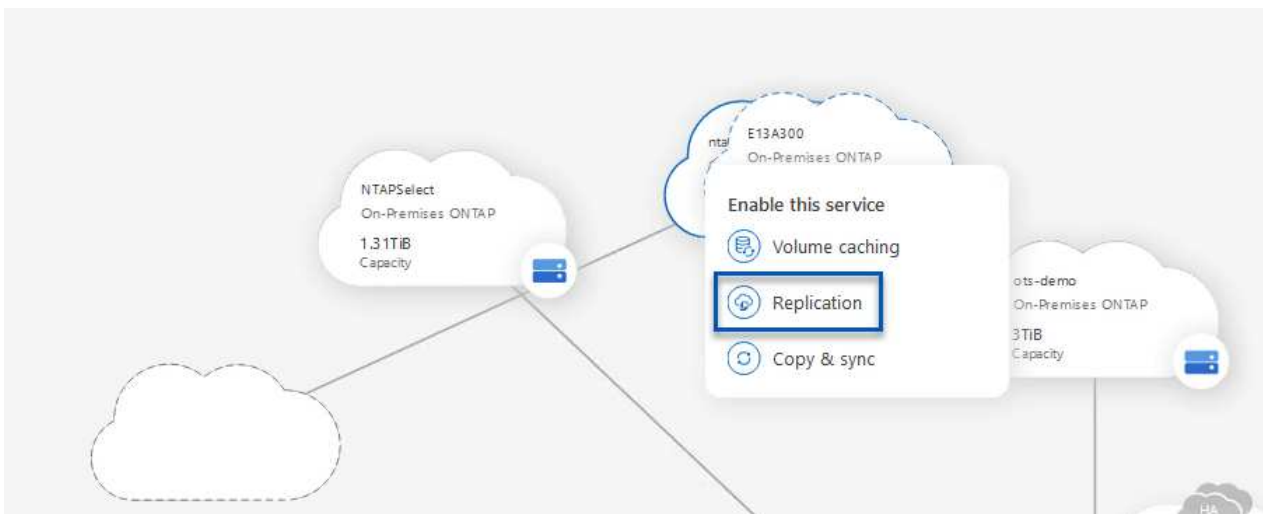
Replication setup for primary and secondary ONTAP storage systems

Begin by logging into the BlueXP web console and navigating to the Canvas.

1. Drag and drop the source (primary) ONTAP storage system onto the destination (secondary) ONTAP storage system.



2. From the menu that appears select **Replication**.



3. On the **Destination Peering Setup** page select the destination Intercluster LIFs to be used for the connection between storage systems.

Select the destination LIFs you would like to use for cluster peering setup.
Replication requires an initial connection between the two working environments which is called a cluster peer relationship.
For more information about LIF selections, see Cloud Manager documentation.





<input type="checkbox"/> CVO_InterCluster_B ntaphci-a300-02 : a0a-3510 172.21.254.212/24 up	<input type="checkbox"/> CVO_InterCluster_A ntaphci-a300-01 : a0a-3510 172.21.254.211/24 up	<input type="checkbox"/> zoneb-n1 ntaphci-a300-01 : a0a-3484 172.21.228.21/24 up	<input type="checkbox"/> zoneb-n2 ntaphci-a300-02 : a0a-3484 172.21.228.22/24 up	<input checked="" type="checkbox"/> intercluster_node_1 ntaphci-a300-01 : a0a-181 10.61.181.193/24 up	<input checked="" type="checkbox"/> intercluster_node_2 ntaphci-a300-01 : a0a-181 10.61.181.194/24 up
--	--	---	---	---	---

4. On the **Destination Volume Name** page, first select the source volume and then fill out the destination volume name and select the destination SVM and aggregate. Click on **Next** to continue.

Select the volume that you want to replicate

E13A300

288 Volumes

 CDM01 ONLINE INFO Storage VM Name: FS02 Tiering Policy: None Volume Type: RW CAPACITY 206 GB Allocated 53.72 MB Disk Used	 Data ONLINE INFO Storage VM Name: FS02 Tiering Policy: None Volume Type: RW CAPACITY 512 GB Allocated 0 GB Disk Used
 Demo ONLINE INFO Storage VM Name: zonea Tiering Policy: None Volume Type: RW CAPACITY 250 GB Allocated 1.79 GB Disk Used	 Demo02_01 ONLINE INFO Storage VM Name: Demo Tiering Policy: None Volume Type: RW CAPACITY 500 GB Allocated 34.75 MB Disk Used

Destination Volume Name

Destination Volume Name

Demo_copy

Destination Storage VM

EHC_NFS

Destination Aggregate

EHCaggr01

5. Choose the max transfer rate for replication to occur at.

Max Transfer Rate

You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your Internet performance.

- ☒ Limited to: MB/s
- ☐ Unlimited (recommended for DR only machines)

6. Choose the policy that will determine the retention schedule for secondary backups. This policy can be created beforehand (see the manual process below in the **Create a snapshot retention policy** step) or can be changed after the fact if desired.

[↑ Previous Step](#)

Default Policies

Additional Policies

CloudBackupService-1674046623282

Original Policy Name: CloudBackupService-1674046623282

Creates a SnapVault relationship which replicates Snapshot copies with the following labels to the destination volume:
hourly (12), daily (15), weekly (6)
(# of retained Snapshot copies in parenthesis)

CloudBackupService-1674047424679

Custom Policy - No Comment

[More info](#)

CloudBackupService-1674047718637

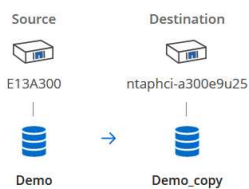
Custom Policy - No Comment

[More info](#)

7. Finally, review all information and click on the **Go** button to start the replication setup process.

[↑ Previous Step](#)

Review your selection and start the replication process



Source Volume Allocated Size:	250 GB
Source Volume Used Size:	1.79 GB
Source Thin Provisioning:	Yes
Destination Volume Allocated Size:	250 GB
Destination Thin Provisioning:	No

Destination Aggregate:	EHCaggr01
Destination Storage VM:	EHC_NFS
Max Transfer Rate:	100 MB/s
SnapMirror Policy:	Mirror
Replication Schedule:	One-time copy

Establish SnapMirror relationships with System Manager and ONTAP CLI

All required steps for establishing SnapMirror relationships can be accomplished with System Manager or the ONTAP CLI. The following section provides detailed information for both methods:

Record the source and destination Intercluster logical interfaces

For the source and destination ONTAP clusters, you can retrieve the inter-cluster LIF information from System Manager or from the CLI.

1. In ONTAP System Manager, navigate to the Network Overview page and retrieve the IP addresses of Type: Intercluster that are configured to communicate with the AWS VPC where FSx is installed.

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Portset	Protocols	Type	Thr
vream_repo	✓	Backup	Default	10.61.181.179	E13A300_1	a0a-181		SMB/CIFS, NFS, S3	Data	0
CM01	✓		Default	10.61.181.180	E13A300_1	a0a-181			Cluster/Node Mgmt	0
HC_N1	✓		Default	10.61.181.183	E13A300_1	a0a-181			Intercluster/Cluster/Node Mgmt	0
HC_N2	✓		Default	10.61.181.184	E13A300_2	a0a-181			Intercluster/Cluster/Node Mgmt	0
BF_ora_vvm_614	✓	ora_vvm	Default	10.61.181.185	E13A300_1	a0a-181		SMB/CIFS, NFS, FL...	Data	0

2. To retrieve the Intercluster IP addresses using the CLI run the following command:

```
ONTAP-Dest::> network interface show -role intercluster
```


Establish cluster peering between ONTAP clusters

To establish cluster peering between ONTAP clusters, a unique passphrase entered at the initiating ONTAP cluster must be confirmed in the other peer cluster.

1. Set up peering on the destination ONTAP cluster using the `cluster peer create` command. When prompted, enter a unique passphrase that is used later on the source cluster to finalize the creation process.

```
ONTAP-Dest::> cluster peer create -address-family ipv4 -peer-addr  
source_intercluster_1, source_intercluster_2  
Enter the passphrase:  
Confirm the passphrase:
```

2. At the source cluster, you can establish the cluster peer relationship using either ONTAP System Manager or the CLI. From ONTAP System Manager, navigate to Protection > Overview and select Peer Cluster.

The screenshot shows the ONTAP System Manager interface. The left sidebar contains a navigation menu with sections: DASHBOARD, STORAGE (with sub-items: Overview, Volumes, LUNs, Consistency Groups, NVMe Namespaces, Shares, Buckets, Qtrees, Quotas, Storage VMs, Tiers), NETWORK (with sub-items: Overview, Ethernet Ports, FC Ports), EVENTS & JOBS, PROTECTION (with sub-items: Overview, Relationships), and HOSTS. The 'Overview' item under the PROTECTION section is highlighted with a red box and a red callout bubble labeled '1'. The main content area is titled 'Overview' and contains three sections: 'Intercluster Settings' (with a sub-section 'Network Interfaces' listing four IP addresses, each with a green checkmark), 'Cluster Peers' (with a sub-section 'PEERED CLUSTER NAME' listing two entries, each with a green checkmark), and 'Mediator' (with a status 'Not configured.' and a 'Configure' button). The 'Cluster Peers' section has a red callout bubble labeled '3' pointing to the 'Peer Cluster' link, and a red callout bubble labeled '2' pointing to the three-dot menu icon next to it. Below the 'Peer Cluster' link are two more links: 'Generate Passphrase' and 'Manage Cluster Peers'. The 'Storage VM Peers' section at the bottom shows 'PEERED STORAGE VMS' with a green checkmark and the number '3'.

ONTAP System Manager

DASHBOARD

STORAGE

- Overview
- Volumes
- LUNs
- Consistency Groups
- NVMe Namespaces
- Shares
- Buckets
- Qtrees
- Quotas
- Storage VMs
- Tiers

NETWORK

- Overview
- Ethernet Ports
- FC Ports

EVENTS & JOBS

PROTECTION

- Overview
- Relationships

HOSTS

Overview

< Intercluster Settings

Network Interfaces

IP ADDRESS

- ✓ 10.61.181.184
- ✓ 172.21.146.217
- ✓ 10.61.181.183
- ✓ 172.21.146.216

Cluster Peers

PEERED CLUSTER NAME

- ✓ FsxId0ae40e08acc0dea67
- ✓ OTS02

[Peer Cluster](#)

[Generate Passphrase](#)

[Manage Cluster Peers](#)

Mediator ?

Not configured.

[Configure](#)

Storage VM Peers

PEERED STORAGE VMS

- ✓ 3

3. In the Peer Cluster dialog box, fill out the required information:
 - a. Enter the passphrase that was used to establish the peer cluster relationship on the destination ONTAP cluster.

- b. Select **Yes** to establish an encrypted relationship.
- c. Enter the intercluster LIF IP address(es) of the destination ONTAP cluster.
- d. Click **Initiate Cluster Peering** to finalize the process.

Peer Cluster ✕

Local

STORAGE VM PERMISSIONS

All storage VMs (incl... ✕)

Storage VMs created in the future also will be given permissions.

Remote

PASSPHRASE ?

.....

It cannot be determined from the passphrase whether this relationship was encrypted. Is the relationship encrypted?

Yes

No

To generate passphrase, [Launch Remote Cluster](#)

Intercluster Network Interfaces IP Addresses

172.30.15.42

172.30.14.28

Cancel

+ Add

4

Initiate Cluster Peering

Cancel

4. Verify the status of the cluster peer relationship from the destination ONTAP cluster with the following command:

```
ONTAP-Dest::> cluster peer show
```

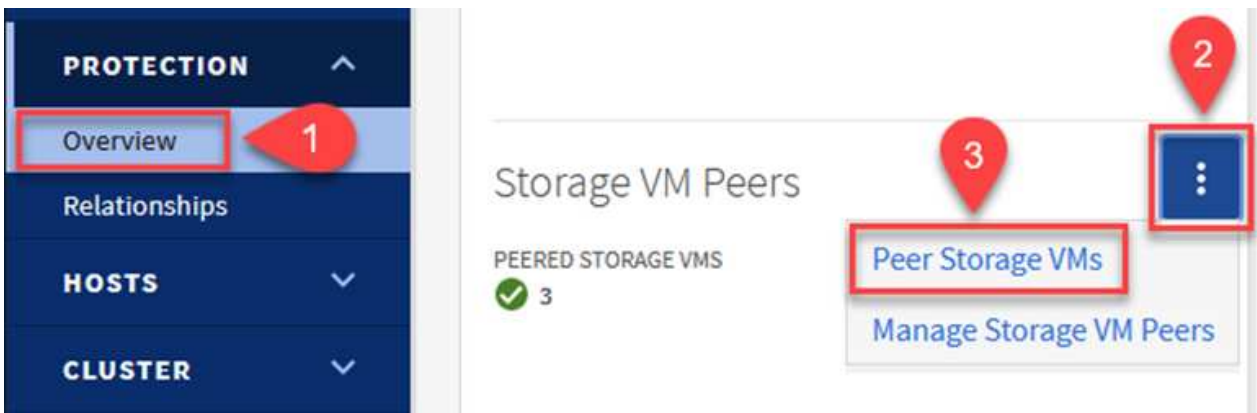

Establish SVM peering relationship

The next step is to set up an SVM relationship between the destination and source storage virtual machines that contain the volumes that will be in SnapMirror relationships.

1. From the destination ONTAP cluster, use the following command from the CLI to create the SVM peering relationship:

```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. From the source ONTAP cluster, accept the peering relationship with either ONTAP System Manager or the CLI.
3. From ONTAP System Manager, go to Protection > Overview and select Peer Storage VMs under Storage VM Peers.



4. In the Peer Storage VM's dialog box, fill out the required fields:
 - The source storage VM
 - The destination cluster
 - The destination storage VM



5. Click Peer Storage VMs to complete the SVM peering process.

Create a snapshot retention policy

SnapCenter manages retention schedules for backups that exist as snapshot copies on the primary storage system. This is established when creating a policy in SnapCenter. SnapCenter does not manage retention policies for backups that are retained on secondary storage systems. These policies are managed separately through a SnapMirror policy created on the secondary FSx cluster and associated with the destination volumes that are in a SnapMirror relationship with the source volume.

When creating a SnapCenter policy, you have the option to specify a secondary policy label that is added to the SnapMirror label of each snapshot generated when a SnapCenter backup is taken.



On the secondary storage, these labels are matched to policy rules associated with the destination volume for the purpose of enforcing retention of snapshots.

The following example shows a SnapMirror label that is present on all snapshots generated as part of a policy used for daily backups of our SQL Server database and log volumes.

Select secondary replication options ⓘ

☐ Update SnapMirror after creating a local Snapshot copy.

☒ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Custom Label ⓘ

sql-daily

Error retry count

3 ⓘ

For more information on creating SnapCenter policies for a SQL Server database, see the [SnapCenter documentation](#).

You must first create a SnapMirror policy with rules that dictate the number of snapshot copies to retain.

1. Create the SnapMirror Policy on the FSx cluster.

```
ONTAP-Dest::> snapmirror policy create -vserver DestSVM -policy  
PolicyName -type mirror-vault -restart always
```

2. Add rules to the policy with SnapMirror labels that match the secondary policy labels specified in the SnapCenter policies.

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy  
PolicyName -snapmirror-label SnapMirrorLabelName -keep  
#ofSnapshotsToRetain
```

The following script provides an example of a rule that could be added to a policy:


```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest  
-policy Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```



Create additional rules for each SnapMirror label and the number of snapshots to be retained (retention period).

Create destination volumes

To create a destination volume on ONTAP that will be the recipient of snapshot copies from our source volumes, run the following command on the destination ONTAP cluster:

```
ONTAP-Dest::> volume create -vserver DestSVM -volume DestVolName  
-aggregate DestAggrName -size VolSize -type DP
```

Create the SnapMirror relationships between source and destination volumes

To create a SnapMirror relationship between a source and destination volume, run the following command on the destination ONTAP cluster:

```
ONTAP-Dest::> snapmirror create -source-path  
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type  
XDP -policy PolicyName
```

Initialize the SnapMirror relationships

Initialize the SnapMirror relationship. This process initiates a new snapshot generated from the source volume and copies it to the destination volume.

To create a volume, run the following command on the destination ONTAP cluster:

```
ONTAP-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

Configure the SnapCenter Plug-in for VMware vSphere

Once installed, the SnapCenter Plug-in for VMware vSphere can be accessed from the vCenter Server Appliance Management interface. SCV will manage backups for the NFS datastores mounted to the ESXi hosts and that contain the Windows and Linux VMs.

Review the [Data protection workflow](#) section of the SCV documentation for more information on the steps involved in configuring backups.

To configure backups of your virtual machines and datastores the following steps will need to be completed

from the plug-in interface.

Discovery ONTAP storage systems

Discover the ONTAP storage clusters to be used for both primary and secondary backups.

1. In the SnapCenter Plug-in for VMware vSphere navigate to **Storage Systems** in the left-hand menu and click on the **Add** button.

SnapCenter Plug-in for VMware vSphere **INSTANCE 10.61.181.201:8080** ▾

[Dashboard](#)
[Settings](#)
[Resource Groups](#)
[Policies](#)
[Storage Systems](#)
[Guest File Restore](#)
[»](#)

Storage Systems

[+ Add](#) [Edit](#) [Delete](#) [Export](#)

Name	Display Name
10.61.181.180	E13A300
Anthos	Anthos
Backup	Backup
Demo	Demo
172.21.146.131	FS02
172.21.146.155	FS03

2. Fill out the credentials and platform type for the primary ONTAP storage system and click on **Add**.

Add Storage System

Storage System	<input type="text" value="10.61.185.145"/>
Platform	<input type="text" value="All Flash FAS"/>
Authentication Method	<input checked="" type="radio"/> Credentials <input type="radio"/> Certificate
Username	<input type="text" value="admin"/>
Password	<input type="password" value="••••••••"/>
Protocol	<input type="text" value="HTTPS"/>
Port	<input type="text" value="443"/>
Timeout	<input type="text" value="60"/> <input type="text" value="Seconds"/>
<input type="checkbox"/> Preferred IP	<input type="text" value="Preferred IP"/>
Event Management System(EMS) & AutoSupport Setting	
<input type="checkbox"/> Log Snapcenter server events to syslog	
<input type="checkbox"/> Send AutoSupport Notification for failed operation to storage system	

3. Repeat this procedure for the secondary ONTAP storage system.

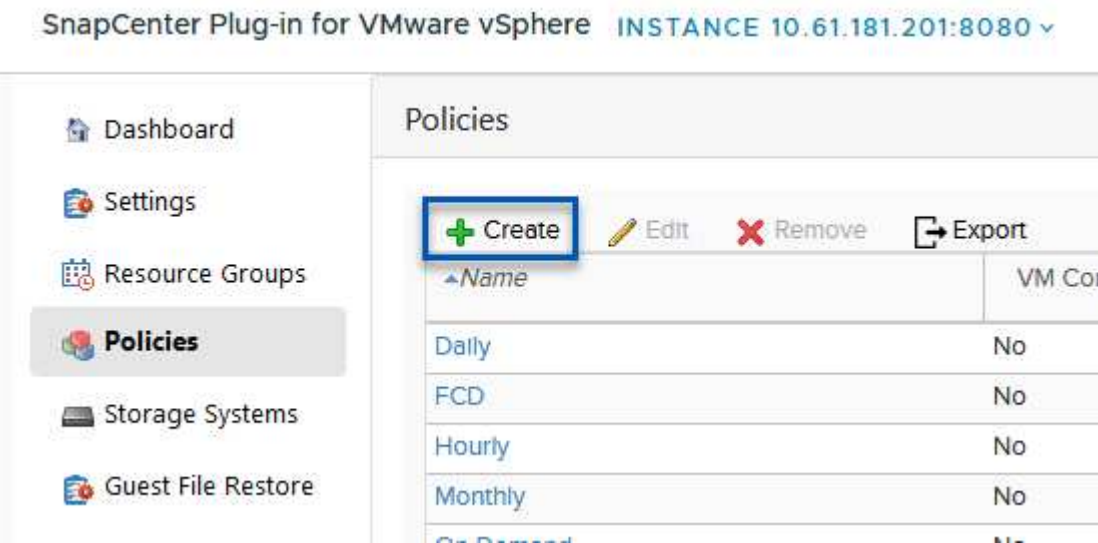
Create SCV backup policies

Policies specify the retention period, frequency and replication options for the backups managed by SCV.

Review the [Create backup policies for VMs and datastores](#) section of the documentation for more information.

To create backup policies complete the following steps:

- 1. In the SnapCenter Plug-in for VMware vSphere navigate to **Policies** in the left-hand menu and click on the **Create** button.



- 2. Specify a name for the policy, retention period, frequency and replication options, and snapshot label.

New Backup Policy

Name	<input type="text" value="Daily"/>
Description	<input type="text" value="description"/>
Retention	<div>Days to keep <input type="text" value="30"/></div>
Frequency	<input type="text" value="Daily"/>
Replication	<div><input type="checkbox"/> Update SnapMirror after backup </div> <div><input checked="" type="checkbox"/> Update SnapVault after backup </div> <div>Snapshot label <input type="text" value="Daily"/></div>
Advanced	<div><input checked="" type="checkbox"/> VM consistency </div> <div><input type="checkbox"/> Include datastores with independent disks</div> <div>Scripts </div> <div><input type="text" value="Enter script path"/></div>



When creating a policy in the SnapCenter Plug-in you will see options for SnapMirror and SnapVault. If you choose SnapMirror, the retention schedule specified in the policy will be the same for both the primary and secondary snapshots. If you choose SnapVault, the retention schedule for the secondary snapshot will be based on a separate schedule implemented with the SnapMirror relationship. This is useful when you wish longer retention periods for secondary backups.



Snapshot labels are useful in that they can be used to enact policies with a specific retention period for the SnapVault copies replicated to the secondary ONTAP cluster. When SCV is used with BlueXP Backup and Restore, the Snapshot label field must either be blank or match the label specified in the BlueXP backup policy.

3. Repeat the procedure for each policy required. For example, separate policies for daily, weekly, and monthly backups.

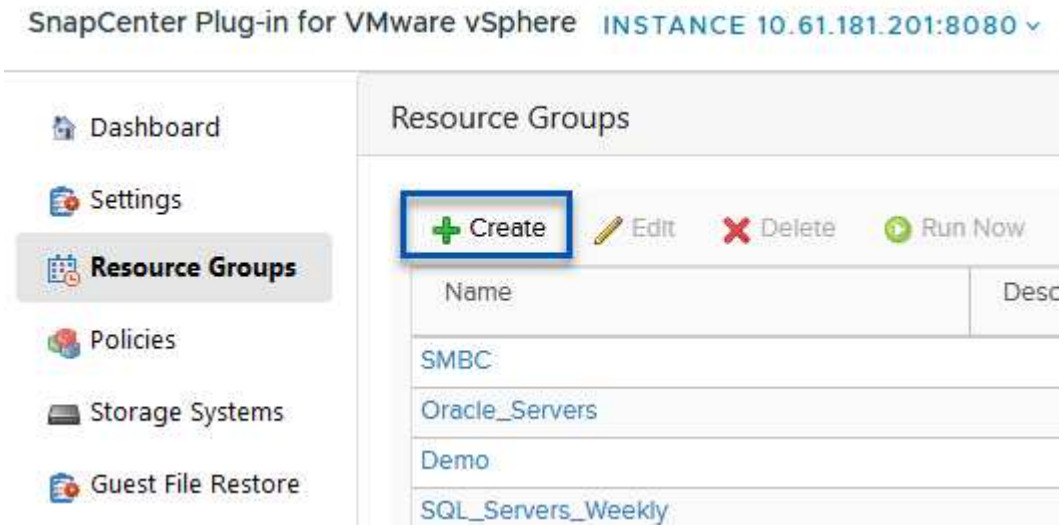
Create resource groups

Resource groups contain the datastores and virtual machines to be included in a backup job, along with the associated policy and backup schedule.

Review the [Create resource groups](#) section of the documentation for more information.

To create resource groups complete the following steps.

1. In the SnapCenter Plug-in for VMware vSphere navigate to **Resource Groups** in the left-hand menu and click on the **Create** button.



2. In the Create Resource Group wizard, enter a name and description for the group, as well as information required to receive notifications. Click on **Next**
3. On the next page select the datastores and virtual machines that wish to be included in the backup job and then click on **Next**.

Create Resource Group

✓ 1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Scope:

Datastores

Datacenter:

Datastores
Virtual Machines
Tags
Folders

Entity name

Available entities

Demo
DemoDS
destination
esxi7-hc-01 Local
esxi7-hc-02 Local
esxi7-hc-03 Local
esxi7-hc-04 Local

Selected entities

NFS_SCV
NFS_WKLD



You have the option to select specific VMs or entire datastores. Regardless of which you choose, the entire volume (and datastore) is backed up since the backup is the result of taking a snapshot of the underlying volume. In most cases, it is easiest to choose the entire datastore. However, if you wish to limit the list of available VMs when restoring, you can choose only a subset of VMs for backup.

4. Choose options for spanning datastores for VMs with VMDKs that reside on multiple datastores and then click on **Next**.

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

☒ 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.



BlueXP backup and recovery does not currently support backing up VMs with VMDKs that span multiple datastores.

5. On the next page select the policies that will be associated with the resource group and click on **Next**.

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

4. Policies

5. Schedules

6. Summary

+ Create

<input type="checkbox"/>	Name	VM Consistent	Include independent di...	Schedule
<input checked="" type="checkbox"/>	Daily	No	No	Daily
<input type="checkbox"/>	FCD	No	Yes	On Demand Only
<input type="checkbox"/>	Monthly	No	No	Monthly
<input type="checkbox"/>	On Demand	No	No	On Demand Only
<input type="checkbox"/>	Weekly	No	No	Weekly



When backing up SCV managed snapshots to object storage using BlueXP backup and recovery, each resource group can only be associated with a single policy.

6. Select a schedule that will determine at what times the backups will run. Click on **Next**.

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

✓ 4. Policies

✓ 5. Schedules

✓ 6. Summary

Daily



Type

Daily

Every

1

Day(s)

Starting

06/23/2023



At

07



00



PM



7. Finally, review the summary page and then on **Finish** to complete the resource group creation.

Run a backup job

In this final step, run a backup job and monitor its progress. At least one backup job must be successfully completed in SCV before resources can be discovered from BlueXP backup and recovery.

1. In the SnapCenter Plug-in for VMware vSphere navigate to **Resource Groups** in the left-hand menu.
2. To initiate a backup job, select the desired resource group and click the **Run Now** button.

SnapCenter Plug-in for VMware vSphere **INSTANCE 10.61.181.201:8080** ▾

Dashboard

Settings

Resource Groups

Policies

Storage Systems

Guest File Restore

»

Resource Groups

+ Create

✎ Edit

✖ Delete

▶ Run Now

⏸ Suspend

Name	Description
Win01	
SMBC	
Oracle_Servers	
Demo	
SQL_Servers_Daily	
SQL_Servers_Weekly	

3. To monitor the backup job, navigate to **Dashboard** on the left hand menu. Under **Recent Job Activities** click on the Job ID number to monitor the job progress.

Job Details : 2614

✓ Validate Retention Settings

✓ Quiescing Applications

✓ Retrieving Metadata

✓ Creating Snapshot copy

✓ Unquiescing Applications

✓ Registering Backup

✓ Backup Retention

✓ Clean Backup Cache

✓ Send EMS Messages

▶ (Job 2616)SnapVault Update

▶ Running, Start Time: 07/31/2023 07:24:40 PM.

CLOSE

DOWNLOAD JOB LOGS

Configure Backups to Object Storage in BlueXP backup and recovery

For BlueXP to manage the data infrastructure effectively, it requires the prior installation of a Connector. The Connector executes the actions involved in discovering resources and managing data operations.

For more information on the BlueXP Connector refer to [Learn about Connectors](#) in the BlueXP documentation.

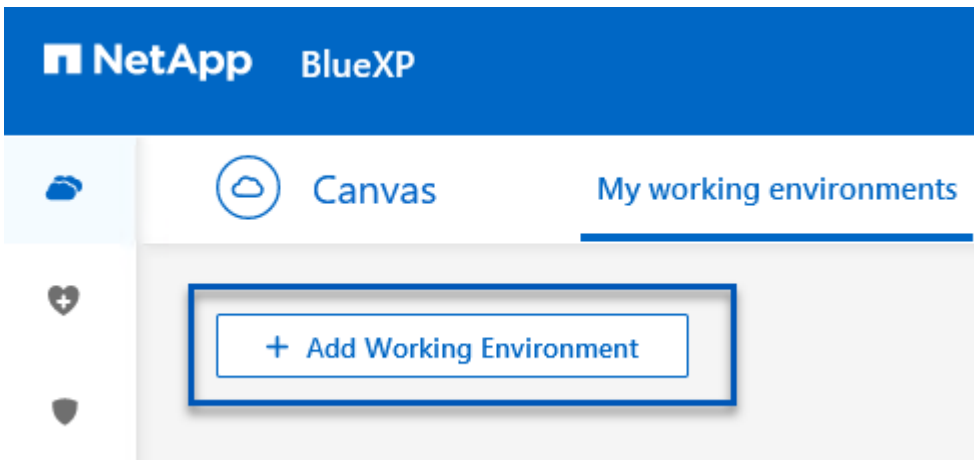
Once the connector is installed for the cloud provider being utilized, a graphic representation of the object storage will be viewable from the Canvas.

To configure BlueXP backup and recovery to backup data managed by SCV on-premises, complete the following steps:

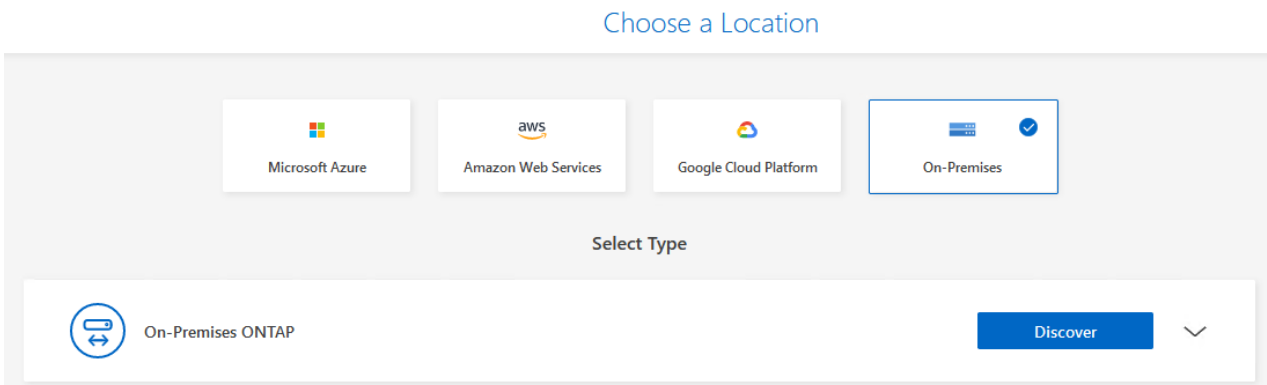
Add working environments to the Canvas

The first step is to add the on-premises ONTAP storage systems to BlueXP

1. From the Canvas select **Add Working Environment** to begin.



2. Select **On-Premises** from the choice of locations and then click on the **Discover** button.



3. Fill out the credentials for the ONTAP storage system and click the **Discover** button to add the working environment.

ONTAP Cluster IP

10.61.181.180

User Name

admin

Password

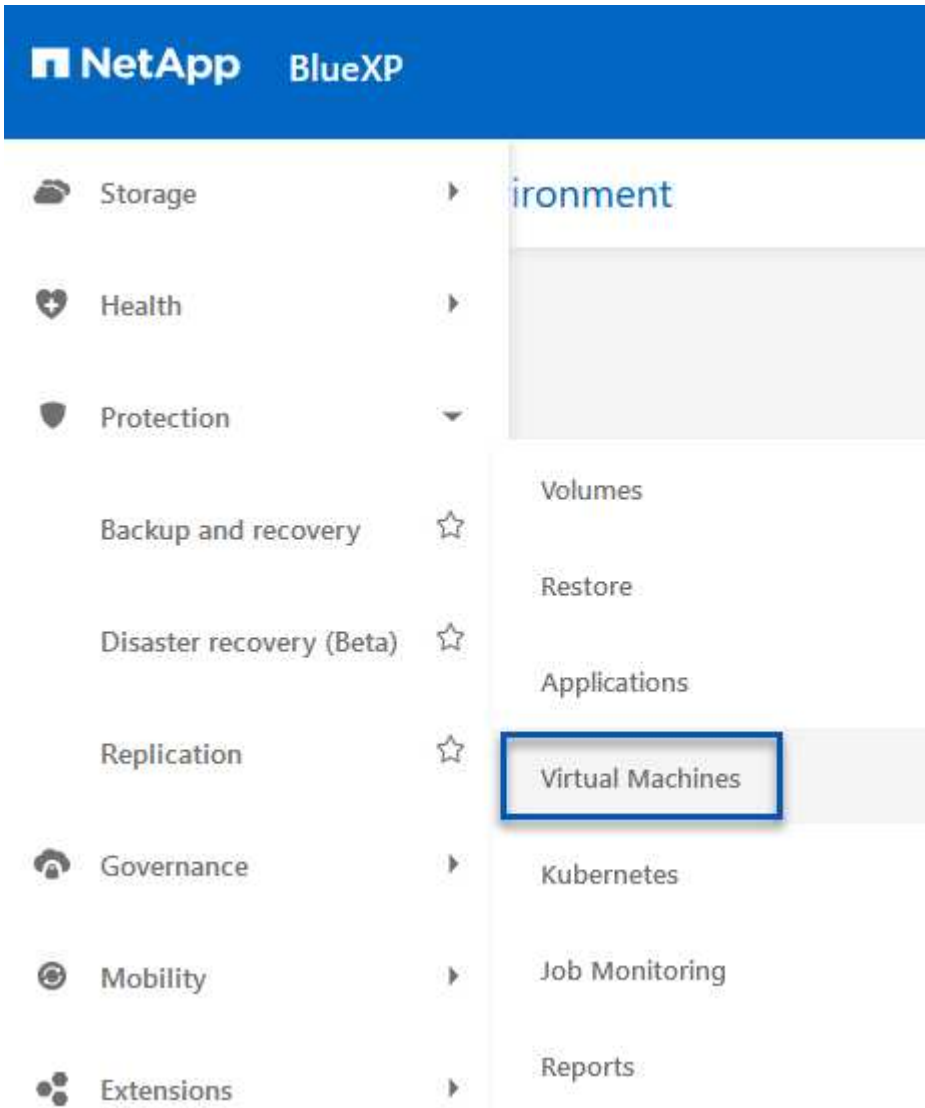
••••••••



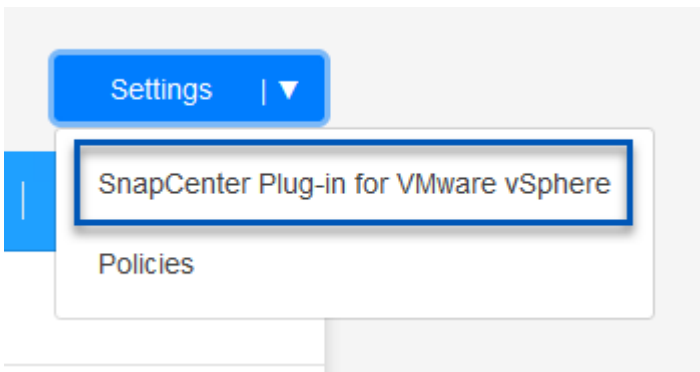
Discover on-premises SCV appliance and vCenter

To discover the on-premises datastore and virtual machine resources, add info for the SCV data broker and credentials for the vCenter management appliance.

1. From the BlueXP left-hand menu selection **Protection > Backup and recovery > Virtual Machines**



2. From the Virtual Machines main screen access the **Settings** drop down menu and select **SnapCenter Plug-in for VMware vSphere**.




- Click on the **Register** button and then enter the IP address and port number for the SnapCenter Plug-in appliance and the username and password for the vCenter management appliance. Click on the **Register** button to begin the discovery process.


Register SnapCenter Plug-in for VMware vSphere


SnapCenter Plug-in for VMware vSphere	Username
<input type="text" value="10.61.181.201"/>	<input type="text" value="administrator@vsphere.local"/>
Port	Password
<input type="text" value="8144"/>	<input type="password" value="••••••••"/>


- The progress of jobs can be monitored from the Job Monitoring tab.

Job Name: Discover Virtual Resources from SnapCenter Plugin for VMWare vSphere
Job Id: 559167ba-8876-45db-9131-b918a165d0a1


Other
Job Type


Jul 31 2023, 9:18:22 pm
Start Time


Jul 31 2023, 9:18:26 pm
End Time


Success
Job Status

Sub-Jobs(2) Collapse All ^

Job Name	Job ID	Start Time	End Time	Duration
Discover Virtual Resources from SnapCenter Plu...	559167ba-8876-45db-...	Jul 31 2023, 9:18:22 pm	Jul 31 2023, 9:18:26 pm	4 Seconds
Discovering Virtual Resources	99446761-f997-4c80-8...	Jul 31 2023, 9:18:22 pm	Jul 31 2023, 9:18:24 pm	2 Seconds
Registering Datastores	b7ab4195-1ee5-40ff-9a...	Jul 31 2023, 9:18:24 pm	Jul 31 2023, 9:18:26 pm	2 Seconds

- Once discovery is complete you will be able to view the datastores and virtual machines across all discovered SCV appliances.

 4
Working Environments

 6
Datastores

 14
Virtual Machines

Datastore Protection


 4
Protected







 2
Unprotected

6 Datastores

Filter By 

  VM View

Settings 

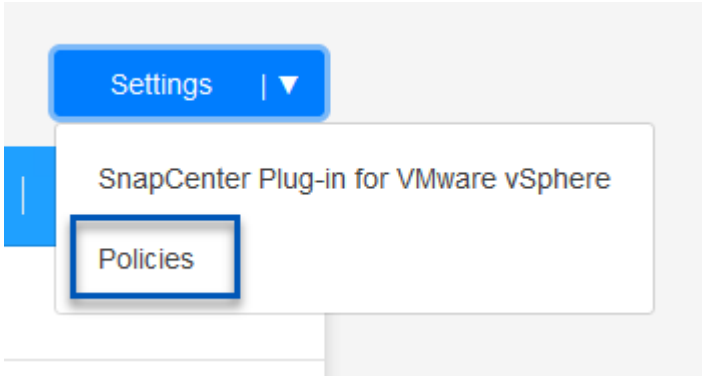
Datastore	Datastore Type	vCenter	Policy Name	Protection Status	
NFS_SCV	NFS	vcsa7-hc.sddc.netapp.com		 Unprotected	...
OTS_DS01	NFS	172.21.254.160	1 Year Daily LTR	 Protected	...
SCV_WKLD	NFS	vcsa7-hc.sddc.netapp.com	1 Year Daily LTR	 Protected	...
NFS_SQL	NFS	vcsa7-hc.sddc.netapp.com	1 Year Daily LTR	 Protected	...
NFS_SQL2	NFS	vcsa7-hc.sddc.netapp.com	1 Year Daily LTR	 Protected	...
SCV_DEMO	NFS	vcsa7-hc.sddc.netapp.com		 Unprotected	...

Create BlueXP backup policies

In BlueXP backup and recovery for virtual machines, create policies to specify the retention period, backup source and the archival policy.

For more information on creating policies refer to [Create a policy to back up datastores](#).

1. From the BlueXP backup and recovery for virtual machines main page, access the **Settings** drop down menu and select **Policies**.



2. Click on **Create Policy** to access the **Create Policy for Hybrid Backup** window.
 - a. Add a name for the policy
 - b. Select the desired retention period
 - c. Select if backups will be sourced from the primary or secondary on-premises ONTAP storage system
 - d. Optionally, specify after what period of time backups will be tiered to archival storage for additional cost savings.

Create Policy for Hybrid Backup

Policy Details

Policy Name
12 week - daily backups

Retention ⓘ

☒ Daily ^

Backups to retain
84

SnapMirror Label
Daily

☐ Weekly Setup Retention Weekly ▼

☐ Monthly Setup Retention Monthly ▼

Backup Source

☒ Primary

☐ Secondary

Archival Policy ⓘ

Backups reside in standard storage for frequently accessed data. Optionally, you can tier backups to archival storage for further cost optimization.

☐ Tier Backups to Archival

Archival After (Days)

Cancel Create



The SnapMirror Label entered here is used to identify which backups to apply the policy too. The label name must match the label name in the corresponding on-premises SCV policy.

3. Click on **Create** to complete the policy creation.

Backup datastores to Amazon Web Services

The final step is to activate data protection for the individual datastores and virtual machines. The following steps outline how to activate backups to AWS.

For more information refer to [Back up datastores to Amazon Web Services](#).

1. From the BlueXP backup and recovery for virtual machines main page, access the settings drop down for the datastore to be backed up and select **Activate Backup**.

6 Datastores

Filter By + VM View Settings

Datastore	Datastore Type	vCenter	Policy Name	Protection Status
NFS_SCV	NFS	vcsa7-hc.sddc.netapp.com		Unprotected
OTS_DS01	NFS	172.21.254.160	1 Year Daily LTR	Protected
SCV_WKLD	NFS	vcsa7-hc.sddc.netapp.com	1 Year Daily LTR	Protected

2. Assign the policy to be used for the data protection operation and click on **Next**.

Assign Policy

1 Assign Policy 2 Add Working Environments 3 Select Provider 4 Configure Provider 5 Review

21 Policies

	Policy Name	SnapMirror Label	Retention Count	Backup Source	Archival Policy
<input type="radio"/>	5 Year Daily LTR	daily	daily : 1830	Primary	Not Active
<input checked="" type="radio"/>	5 Year Daily LTR	daily	daily : 1830	Primary	Not Active
<input type="radio"/>	7 Year Weekly LTR	weekly	weekly : 370	Primary	Not Active

3. At the **Add Working Environments** page the datastore and working environment with a check mark should appear if the working environment has been previously discovered. If the working environment has not been previously discovered you can add it here. Click on **Next** to continue.

Add Working Environments


Provide ONTAP cluster (working environment) details that you want Cloud Manager to discover. Working environment details will appear for all volumes that reside on the same cluster. You will need to enter multiple working environments when volumes reside on different clusters.


SVM	Volume	Working Environment	
EHC_NFS	NFS_SCV	OnPremWorkingEnvironment-6MzE27u1	Edit


4. At the **Select Provider** page click on AWS and then click on the **Next** button to continue.


Progress bar: ✓ Assign Policy ✓ Add Working Environments **3 Select Provider** 4 Configure Provider 5 Review

Select Provider


Amazon Web Services


Microsoft Azure


Google Cloud Platform


StorageGRID

5. Fill out the provider specific credential information for AWS including the AWS access key and secret key, region, and archival tier to be used. Also, select the ONTAP IP space for the on-premises ONTAP storage system. Click on **Next**.

Progress bar: ✓ Assign Policy ✓ Add Working Environments ✓ Select Provider **4 Configure Provider** 5 Review

Configure Provider

Cloud Manager needs the following details to connect with the cloud provider.

Provider Information	Location and Connectivity
<p>AWS Account</p> <div></div>	<p>Region</p> <div>US East (N. Virginia)</div>
<p>AWS Access Key</p> <div>Enter AWS Access Key</div> <p>Required</p>	<p>IP space for Environment</p> <p>OnPremWorkingEnvironment-6MzE27u1</p> <div>Default</div>
<p>AWS Secret Key</p> <div>Enter AWS Secret Key</div> <p>Required</p>	<p>Archival Tier</p> <div>Glacier</div>

6. Finally, review the backup job details and click on the **Activate Backup** button to initiate data protection of the datastore.

Review

Policy	5 Year Daily LTR
SVM	EHC_NFS
Volumes	NFS_SCV
Working Environment	OnPremWorkingEnvironment-6MzE27u1
Backup Source	Primary
Cloud Service Provider	AWS
AWS Account	[REDACTED]
AWS Access Key	[REDACTED]
Region	US East (N. Virginia)
IP space	Default
Tier Backups to Archival	No

Previous

Activate Backup



At this point data transfer may not immediately begin. BlueXP backup and recovery scans for any outstanding snapshots every hour and then transfers them to object storage.

Restoring Virtual Machines in the case of data loss

Ensuring the safeguarding of your data is only one aspect of comprehensive data protection. Equally crucial is the ability to promptly restore data from any location in the event of data loss or a ransomware attack. This capability is vital for maintaining seamless business operations and meeting recovery point objectives.

NetApp offers a highly adaptable 3-2-1 strategy, providing customized control over retention schedules at the

primary, secondary, and object storage locations. This strategy provides the flexibility to tailor data protection approaches to specific needs.

This section provides an overview of the data restoration process from both the SnapCenter Plug-in for VMware vSphere and BlueXP backup and recovery for virtual machines.

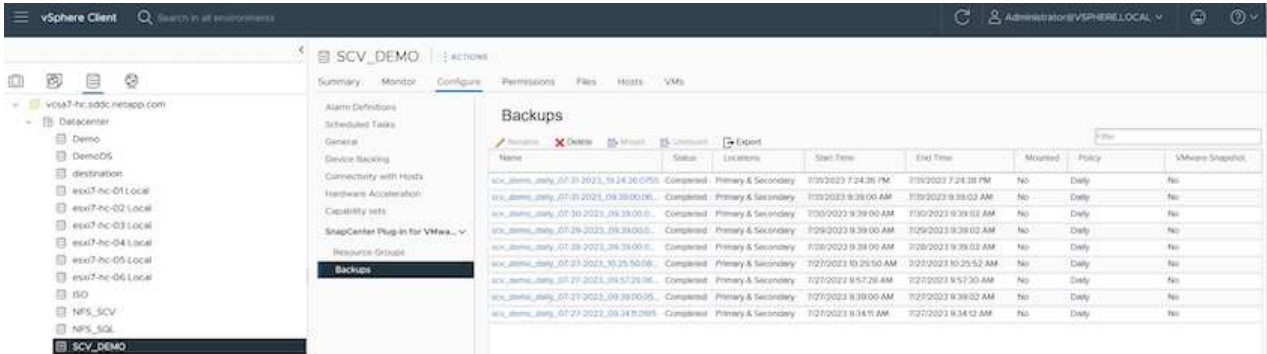
Restoring Virtual Machines from SnapCenter Plug-in for VMware vSphere

For this solution virtual machines were restored to original and alternate locations. Not all aspects of SCV's data restoration capabilities will be covered in this solution. For in depth information on all that SCV has to offer refer to the [Restore VMs from backups](#) in the product documentation.

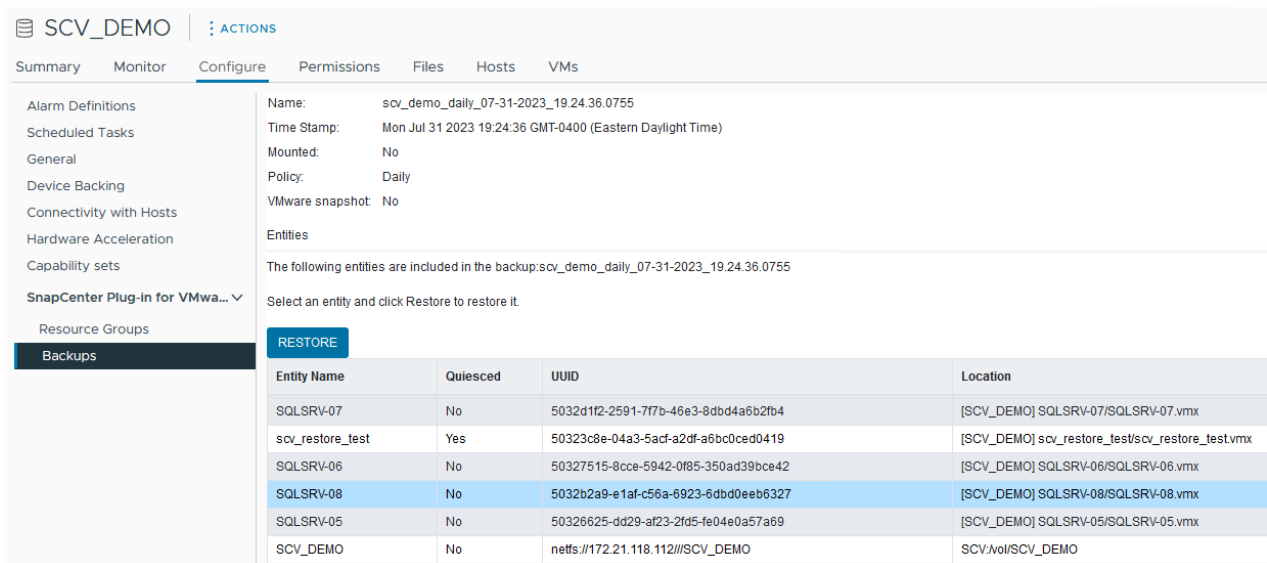
Restore virtual machines from SCV

Complete the following steps to restore a virtual machine restore from primary or secondary storage.

1. From the vCenter client navigate to **Inventory > Storage** and click on the datastore that contains the virtual machines you wish to restore.
2. From the **Configure** tab click on **Backups** to access the list of available backups.



3. Click on a backup to access the list of VMs and then select a VM to restore. Click on **Restore**.



4. From the Restore wizard select to restore the entire virtual machine or a specific VMDK. Select to install to the original location or alternate location, provide VM name after restore, and destination datastore. Click **Next**.

Restore

1. Select scope

2. Select location

3. Summary

Restore scope

Restore Location

Destination vCenter Server

Destination ESXi host

Network

VM name after restore

Select Datastore:

Entire virtual machine

☐

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.)

10.61.181.210

esxi7-hc-04.sddc.netapp.com

Management 181

SQL_SRV_08_restored

NFS_SCV

BACK

NEXT

FINISH

CANCEL

5. Choose to backup from the primary or secondary storage location.

Restore

1. Select scope

2. Select location

3. Summary

Destination datastore	Locations
SCV_DEMO	(Primary) SCV:SCV_DEMO
	(Primary) SCV:SCV_DEMO
	(Secondary) EHC_NFS:SCV_DEMO_dest

6. Finally, review a summary of the backup job and click on Finish to begin the restore process.

Restoring Virtual Machines from BlueXP backup and recovery for virtual machines

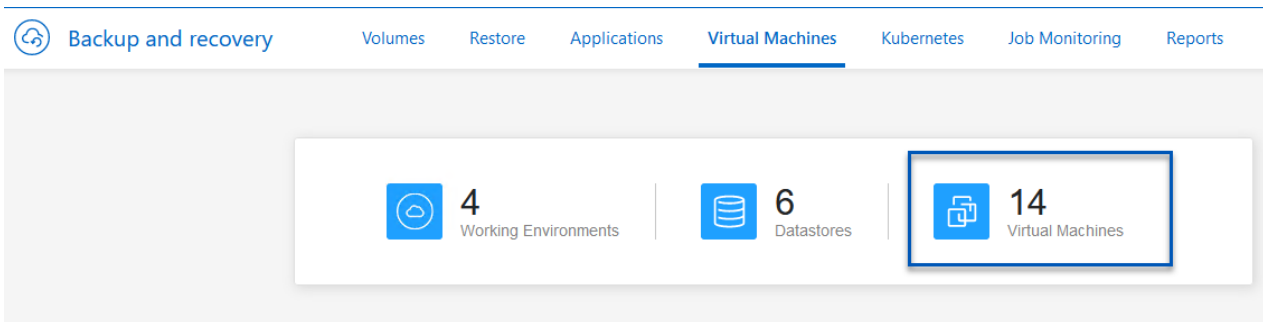
BlueXP backup and recovery for virtual machines allows restores of virtual machines to their original location. Restore functions are accessed through the BlueXP web console.

For more information refer to [Restore virtual machines data from the cloud](#).

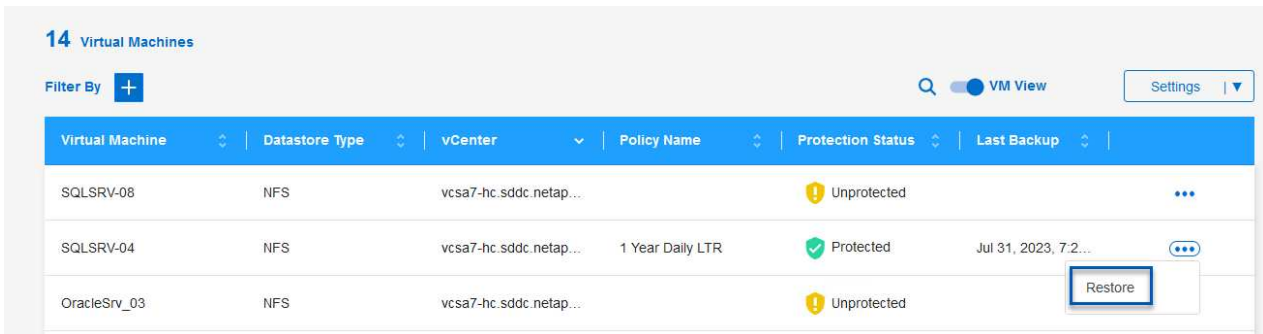
Restore virtual machines from BlueXP backup and recovery

To restore a virtual machine from BlueXP backup and recovery, complete the following steps.

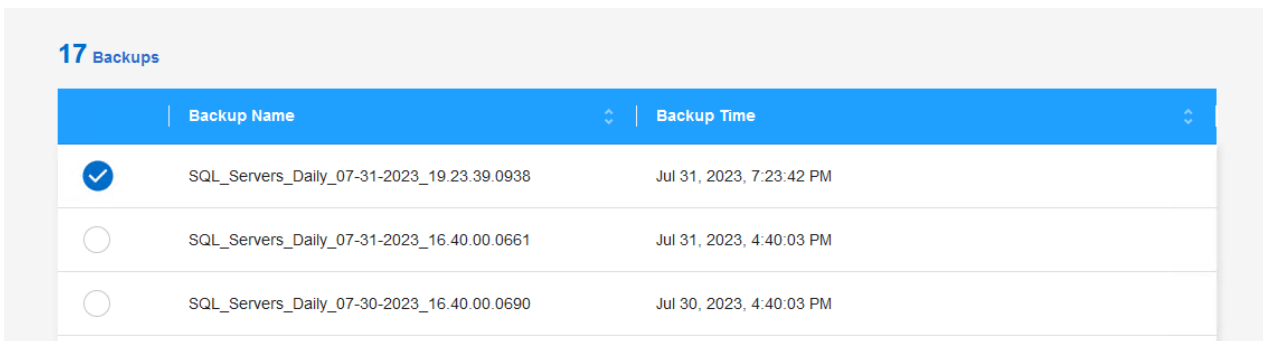
1. Navigate to **Protection > Backup and recovery > Virtual Machines** and click on Virtual Machines to view the list of virtual machines available to be restored.



2. Access the settings drop down menu for the VM to be restored and select



3. Select the backup to restore from and click on **Next**.



4. Review a summary of the backup job and click on **Restore** to start the restore process.
5. Monitor the progress of the restore job from the **Job Monitoring** tab.

[Volumes](#)
[Restore](#)
[Applications](#)
[Virtual Machines](#)
[Kubernetes](#)
[Job Monitoring](#)
[Reports](#)

restore 17 files from Cloud

Job Name: Restore 17 files from Cloud
 Job Id: ec567065-dcf4-4174-b7ef-b27e6620fdbf

Restore Files
Job Type

NFS_SQL
Restore Content

17 Files
Content Files

NFS_SQL
Restore to

In Progress
Job Status

Restore Content

	ots-demo Working Environment Name	NAS_VOLS SVM Name	NFS_SQL Volume Name	SQL_Servers_Daily_07-31-2023_... Backup Name	Jul 31 2023, 7:24:03 pm Backup Time
--	--------------------------------------	----------------------	------------------------	---	--

Restore from

	AWS Provider	us-east-1 Region	982589175402 Account ID	netapp-backup-d56250b0-24ad... Bucket/Container Name
--	-----------------	---------------------	----------------------------	---

Expand All

Conclusion

The 3-2-1 backup strategy, when implemented with SnapCenter Plug-in for VMware vSphere and BlueXP backup and recovery for virtual machines, offers a robust, reliable, and cost-effective solution for data protection. This strategy not only ensures data redundancy and accessibility but also provides the flexibility of restoring data from any location and from both on-premises ONTAP storage systems and cloud based object storage.

The use case presented in this documentation focuses on proven data protection technologies that highlight the integration between NetApp, VMware, and the leading cloud providers. The SnapCenter Plug-in for VMware vSphere provides seamless integration with VMware vSphere, allowing for efficient and centralized management of data protection operations. This integration streamlines the backup and recovery processes for virtual machines, enabling easy scheduling, monitoring, and flexible restore operations within the VMware ecosystem. BlueXP backup and recovery for virtual machines provides the one (1) in 3-2-1 by providing secure, air-gapped backups of virtual machine data to cloud based object storage. The intuitive interface and logical workflow provide a secure platform for long-term archival of critical data.

Additional Information

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

- [SnapCenter Plug-in for VMware vSphere documentation](#)
- [BlueXP documentation](#)

Set up disaster recovery for VMFS datastores using BlueXP disaster recovery

In this use case we outline the procedure to set up disaster recovery using BlueXP disaster recovery for on-premises VMware VMs using VMware Virtual Machine File System (VMFS) datastores. This procedure includes setting up the BlueXP account and

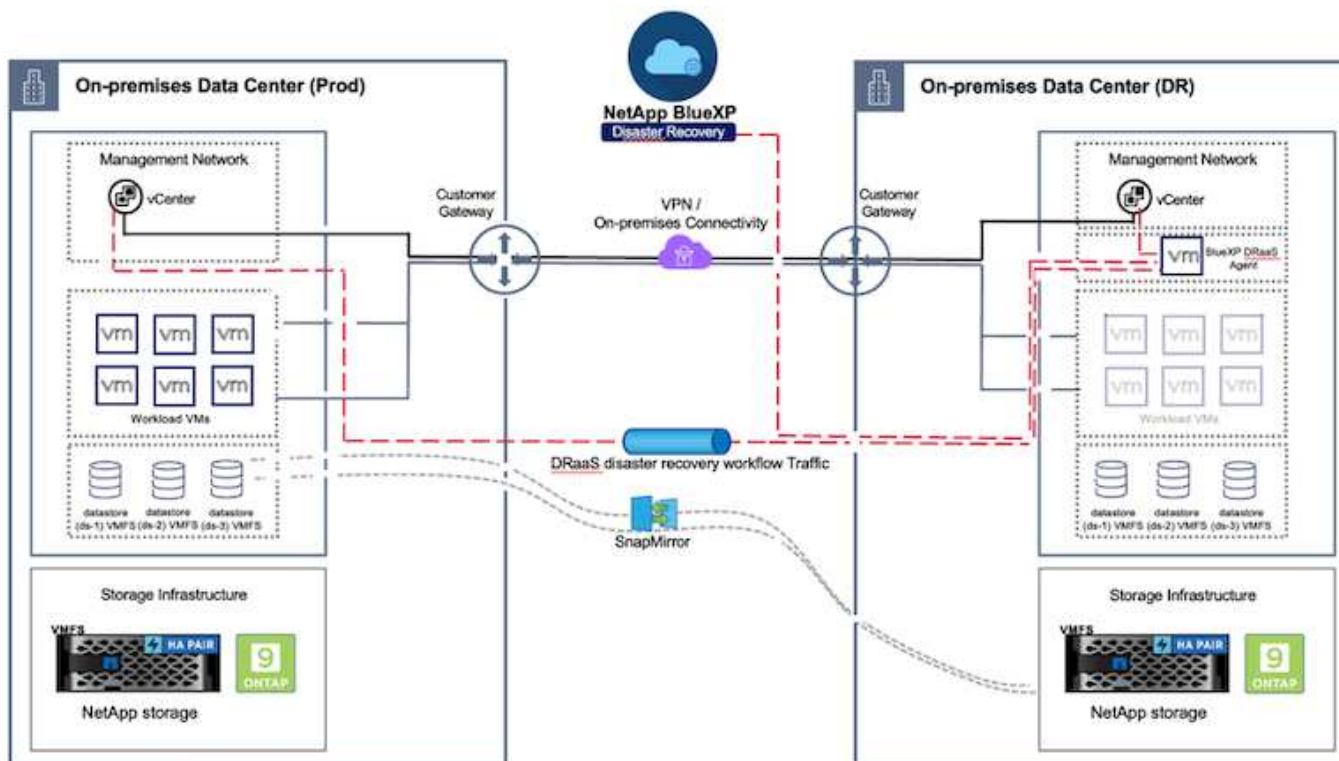
connector, establishing SnapMirror replication between ONTAP systems, integrating with VMware vCenter, and automating failover and failback operations.

Disaster recovery using block-level replication from production site to disaster recovery site is a resilient and cost-effective way of protecting the workloads against site outages and data corruption events, like ransomware attacks. With NetApp SnapMirror replication, VMware workloads running on-premises ONTAP systems using VMFS datastore can be replicated to another ONTAP storage system in a designated recovery datacenter where VMware resides

Introduction

This section of the document describes the configuration of BlueXP DRaaS to set up disaster recovery for on-premises VMware VMs to another designated site. As part of this setup, the BlueXP account, BlueXP connector, the ONTAP arrays added within BlueXP workspace which is needed to enable communication from VMware vCenter to the ONTAP storage. In addition, this document details how to configure replication between sites and how to setup and test a recovery plan. The last section has instructions for performing a full site failover and how to failback when the primary site is recovered and brought online.

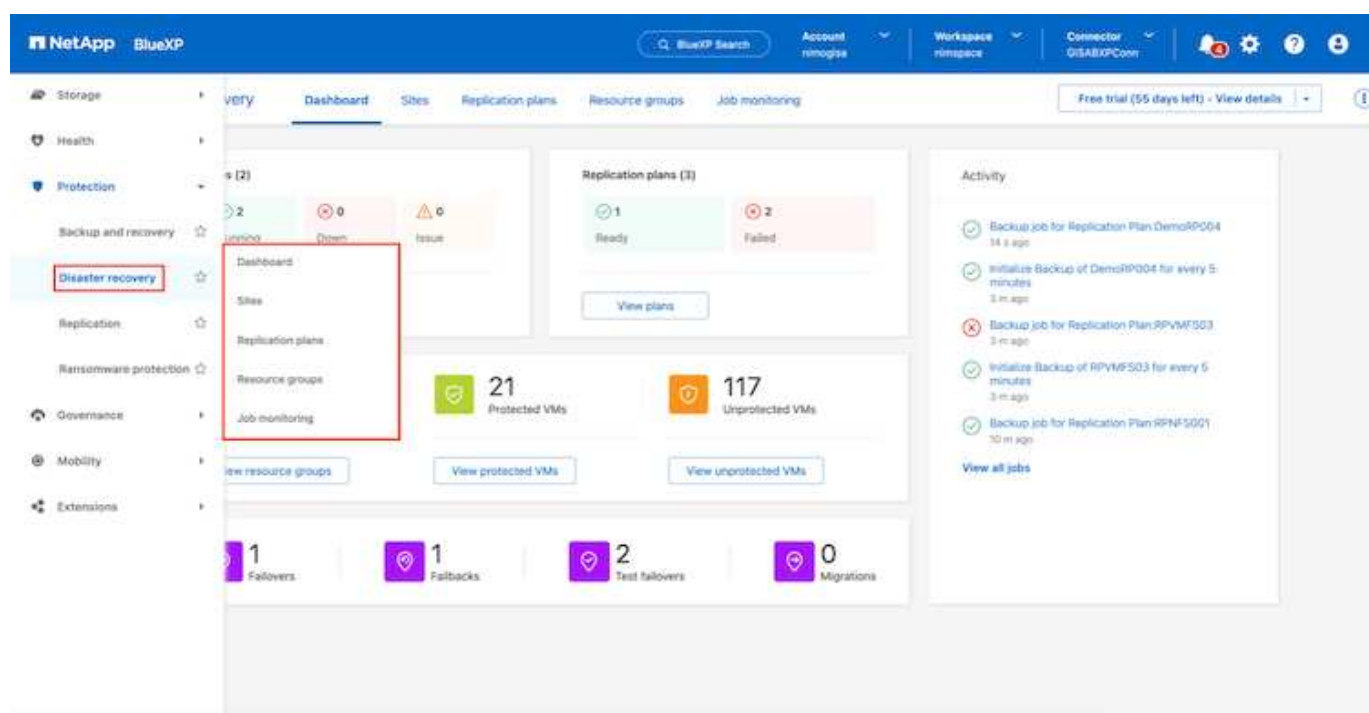
Using the BlueXP disaster recovery service, which is integrated into the NetApp BlueXP console, customers can discover their on-premises VMware vCenters along with ONTAP storage, create resource groupings, create a disaster recovery plan, associate it with resource groups, and test or execute failover and failback. SnapMirror provides storage-level block replication to keep the two sites up to date with incremental changes, resulting in a RPO of up to 5 minutes. It is also possible to simulate DR procedures as a regular drill without impacting the production and replicated datastores or incurring additional storage costs. BlueXP disaster recovery takes advantage of ONTAP's FlexClone technology to create a space-efficient copy of the VMFS datastore from the last replicated Snapshot on the DR site. Once the DR test is complete, customers can simply delete the test environment, again without any impact to actual replicated production resources. When there is a need (planned or unplanned) for actual failover, with a few clicks, the BlueXP disaster recovery service will orchestrate all the steps needed to automatically bring up the protected virtual machines on designated disaster recovery site. The service will also reverse the SnapMirror relationship to the primary site and replicate any changes from secondary to primary for a failback operation, when needed. All of these can be achieved with a fraction of cost compared to other well-known alternatives.



Getting started

To get started with BlueXP disaster recovery, use BlueXP console and then access the service.

1. Log in to BlueXP.
2. From the BlueXP left navigation, select Protection > Disaster recovery.
3. The BlueXP disaster recovery Dashboard appears.



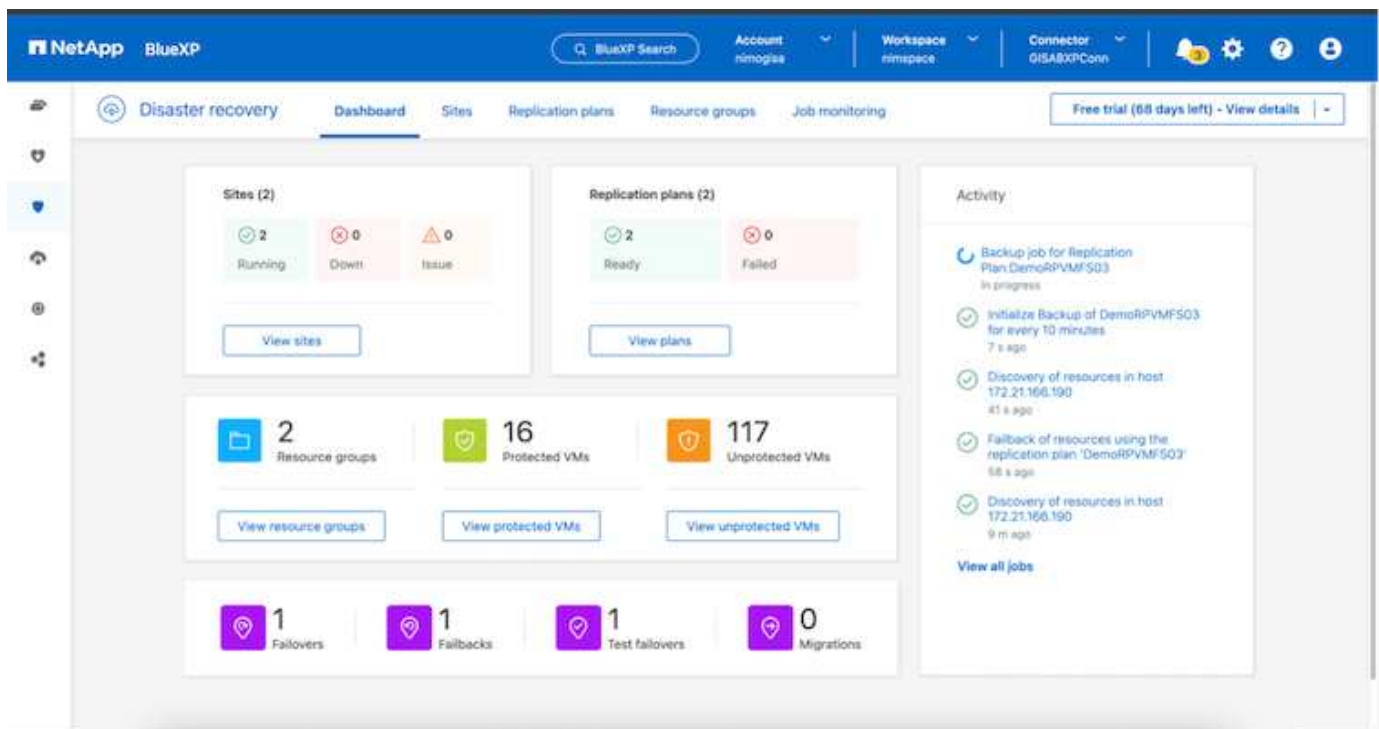
Before configuring disaster recovery plan, ensure the following pre-requisites are met:

- BlueXP Connector is set up in NetApp BlueXP. The connector should be deployed in AWS VPC.
- BlueXP connector instance have connectivity to the source and destination vCenter and storage systems.
- On-premises NetApp storage systems hosting VMFS datastores for VMware are added in BlueXP.
- DNS resolution should be in place when using DNS names. Otherwise, use IP addresses for the vCenter.
- SnapMirror replication is configured for the designated VMFS based datastore volumes.

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



NetApp recommends deploying the BlueXP connector in the disaster recovery site or in a third site, so that the BlueXP connector can communicate through the network with source and destination resources during real outages or natural disasters.



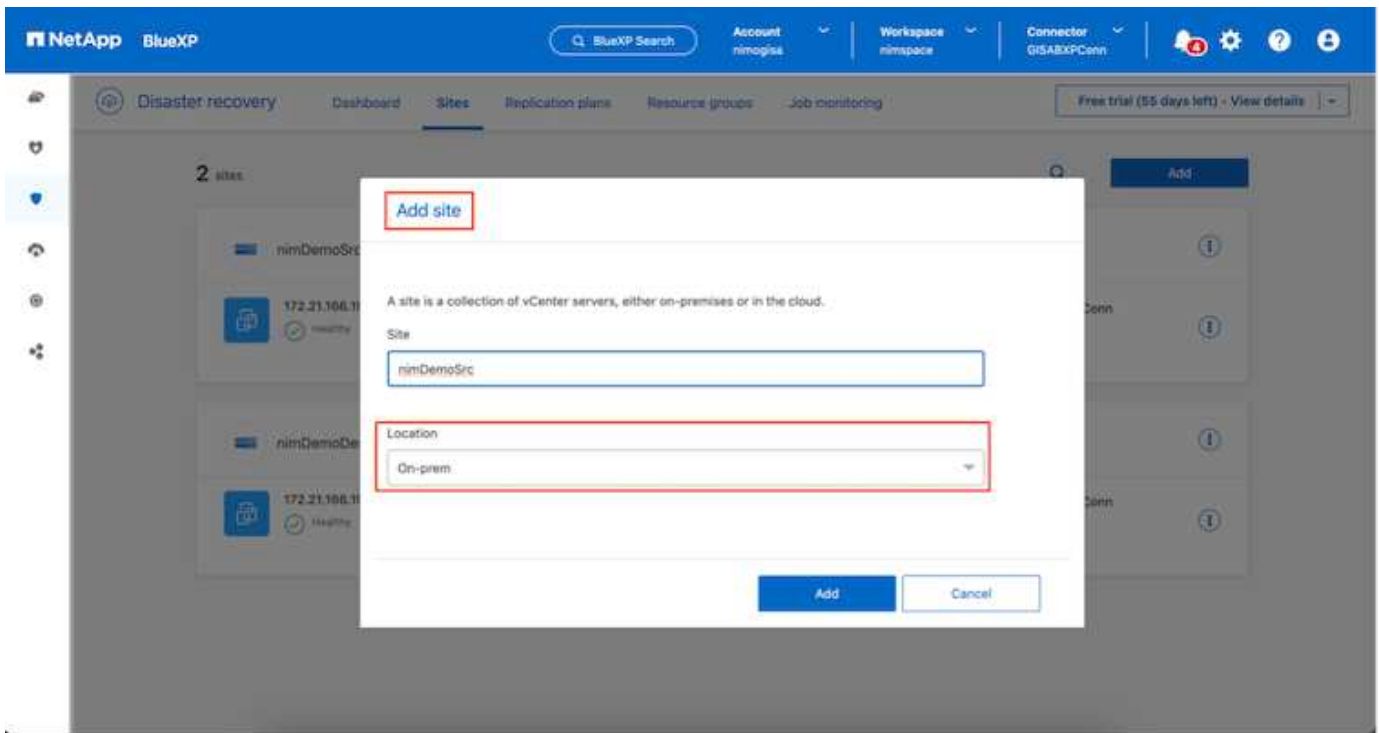
Support for on-premises to on-premises VMFS datastores is in technology preview while writing this document. The capability is supported with both FC and iSCSI protocol based VMFS datastores.

BlueXP disaster recovery configuration

The first step in preparing for disaster recovery is to discover and add the on-premises vCenter and storage resources to BlueXP disaster recovery.

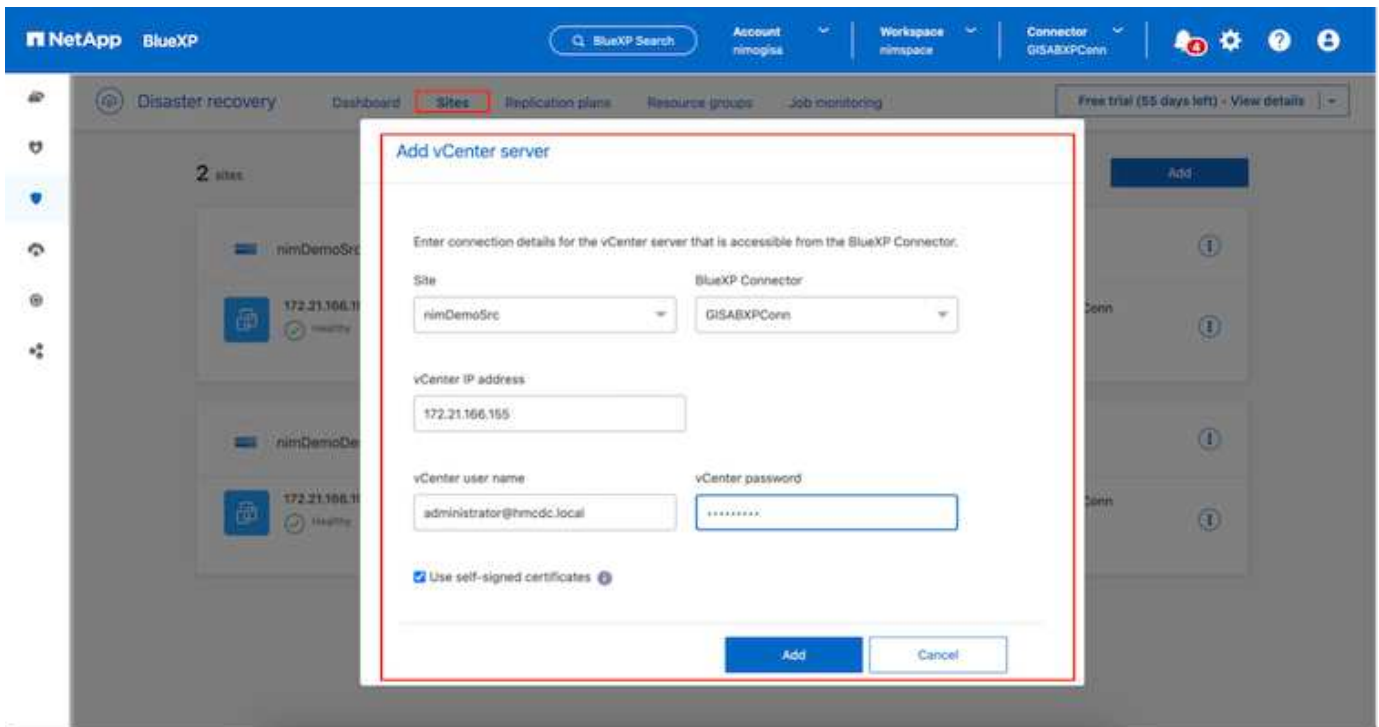


Ensure the ONTAP storage systems are added to the working environment within the canvas. Open BlueXP console and select **Protection > Disaster Recovery** from left navigation. Select **Discover vCenter servers** or use top menu, Select **Sites > Add > Add vCenter**.

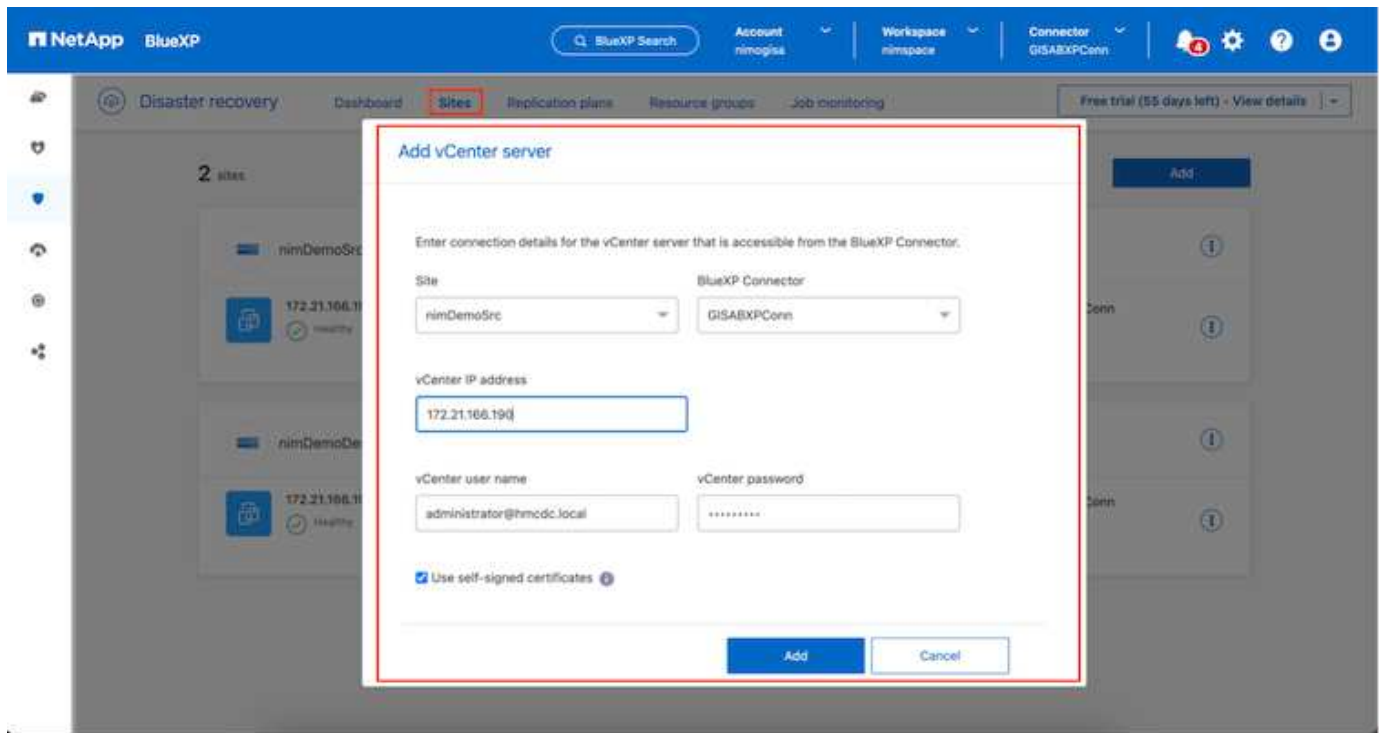


Add the following platforms:

- **Source.** On-premises vCenter.



- **Destination.** VMC SDDC vCenter.



Once the vCenters are added, automated discovery is triggered.

Configuring Storage replication between source and destination site

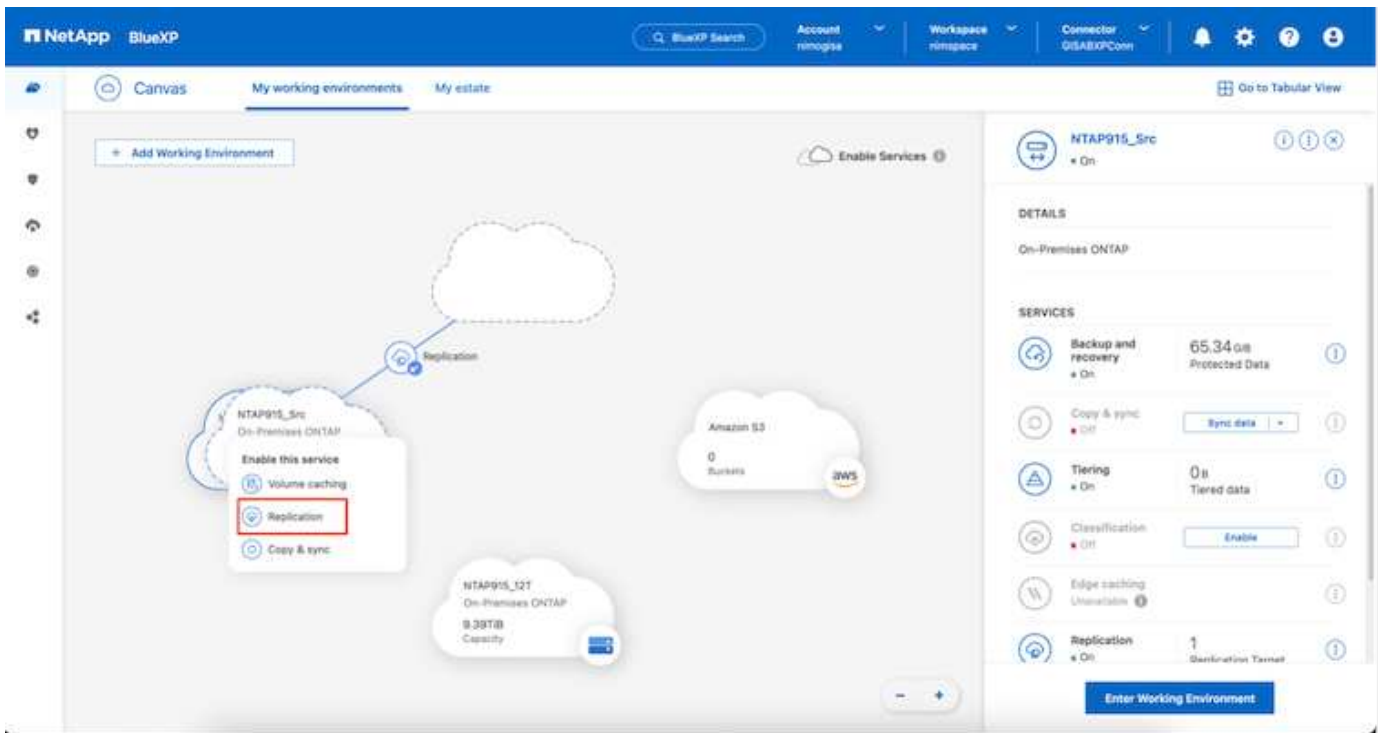
SnapMirror makes use of ONTAP snapshots to manage the transfer of data from one location to another. Initially, a full copy based on a snapshot of the source volume is copied over to the destination to perform a baseline synchronization. As data changes occur at the source, a new snapshot is created and compared to the baseline snapshot. The blocks found to have changed are then replicated to the destination, with the newer snapshot becoming the current baseline, or newest common snapshot. This enables the process to be repeated and incremental updates to be sent to the destination.

When a SnapMirror relationship has been established, the destination volume is in an online read-only state, and so is still accessible. SnapMirror works with physical blocks of storage, rather than at a file or other logical level. This means that the destination volume is an identical replica of the source, including snapshots, volume settings, etc. If ONTAP space efficiency features, such as data compression and data deduplication, are being used by the source volume, the replicated volume will retain these optimizations.

Breaking the SnapMirror relationship makes the destination volume writable and would typically be used to perform a failover when SnapMirror is being used to synchronize data to a DR environment. SnapMirror is sophisticated enough to allow the data changed at the failover site to be efficiently resynchronized back to the primary system, should it later come back online, and then allow for the original SnapMirror relationship to be re-established.

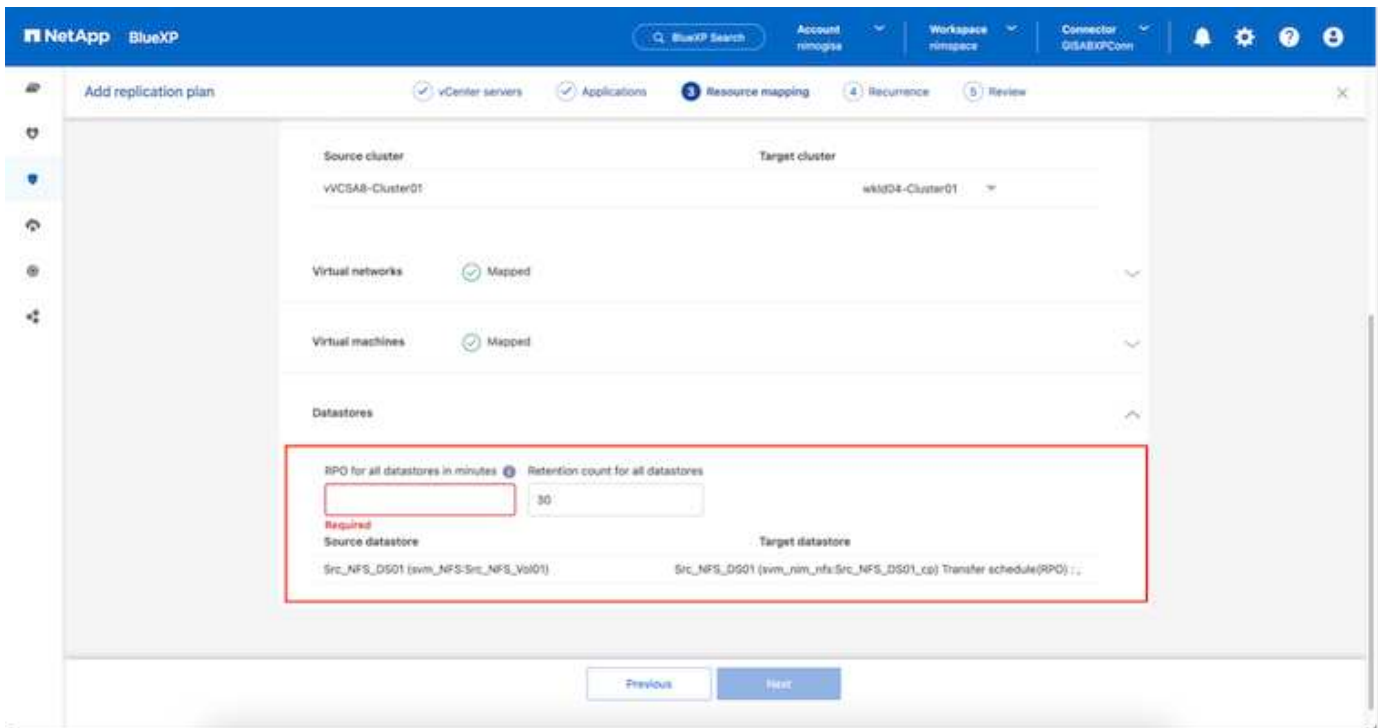
How to set it up for VMware Disaster Recovery

The 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 BlueXP 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.



BlueXP DRaaS can also automate the same provided the following two criteria's are met:

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



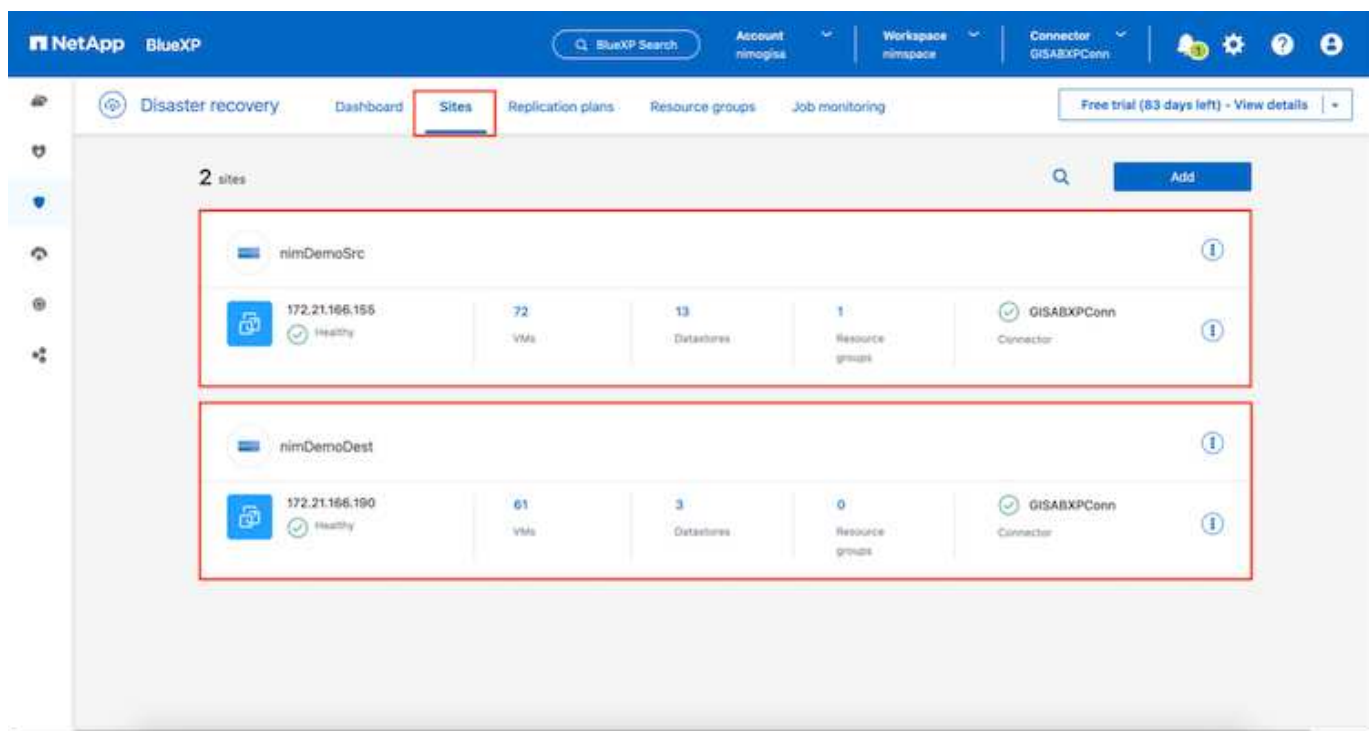
If SnapMirror relationship is already configured for the volume via CLI, BlueXP DRaaS picks up the relationship and continues with the rest of the workflow operations.



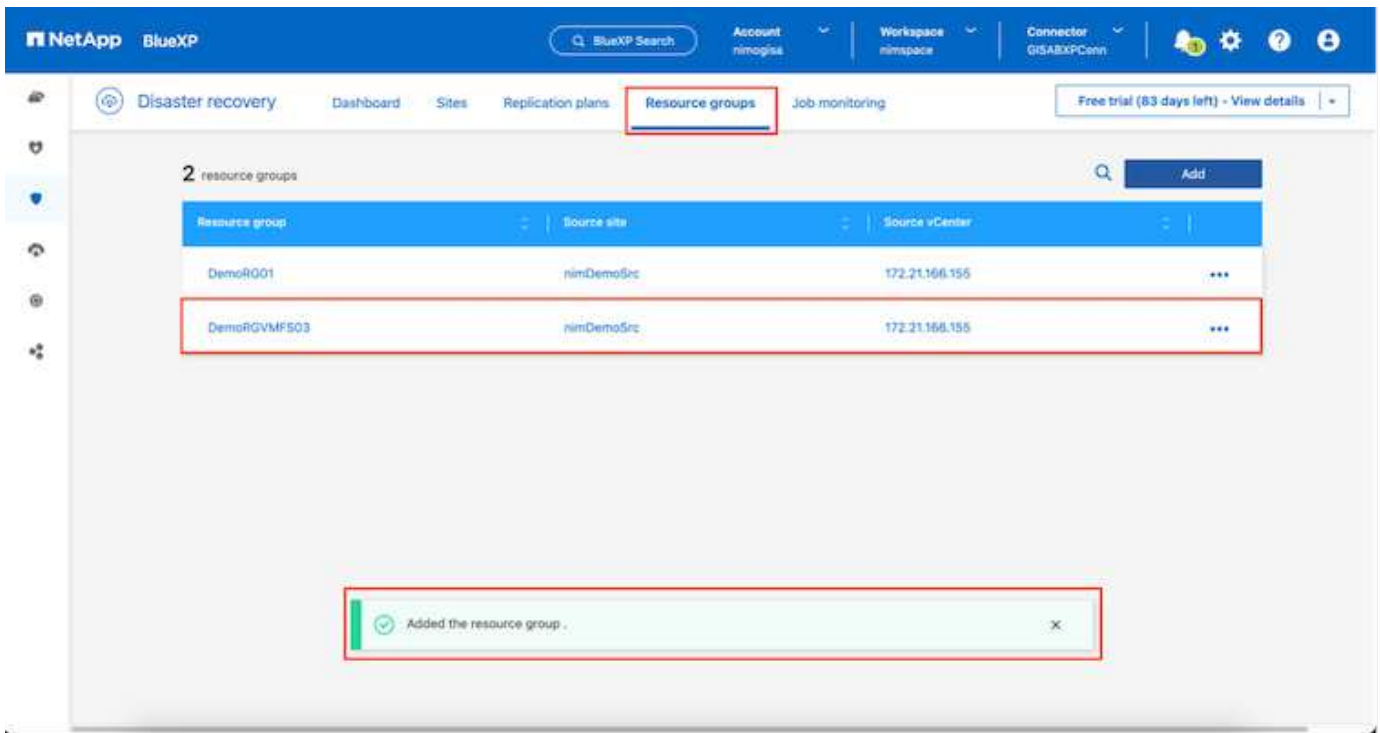
Apart from the above approaches, SnapMirror replication can also be created via ONTAP CLI or System Manager. Irrespective of the approach used to synchronize the data using SnapMirror, BlueXP DRaaS orchestrates the workflow for seamless and efficient disaster recovery operations.

What can BlueXP disaster recovery do for you?

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

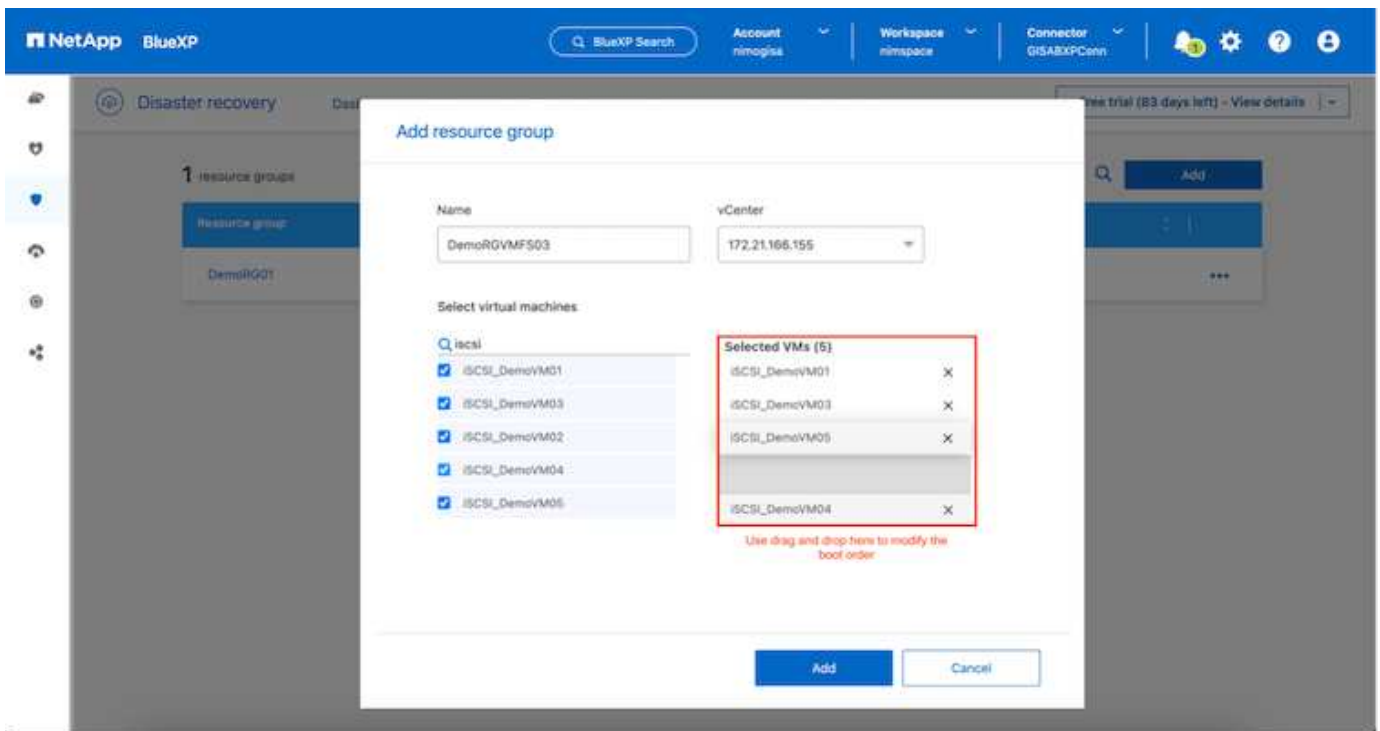


After the sites have been added, VMs can be grouped into resource groups. BlueXP disaster recovery resource groups allow you to group a set of dependent VMs into logical groups that contain their boot orders and boot delays that can be executed upon recovery. To start creating resource groups, navigate to **Resource Groups** and click **Create New Resource Group**.

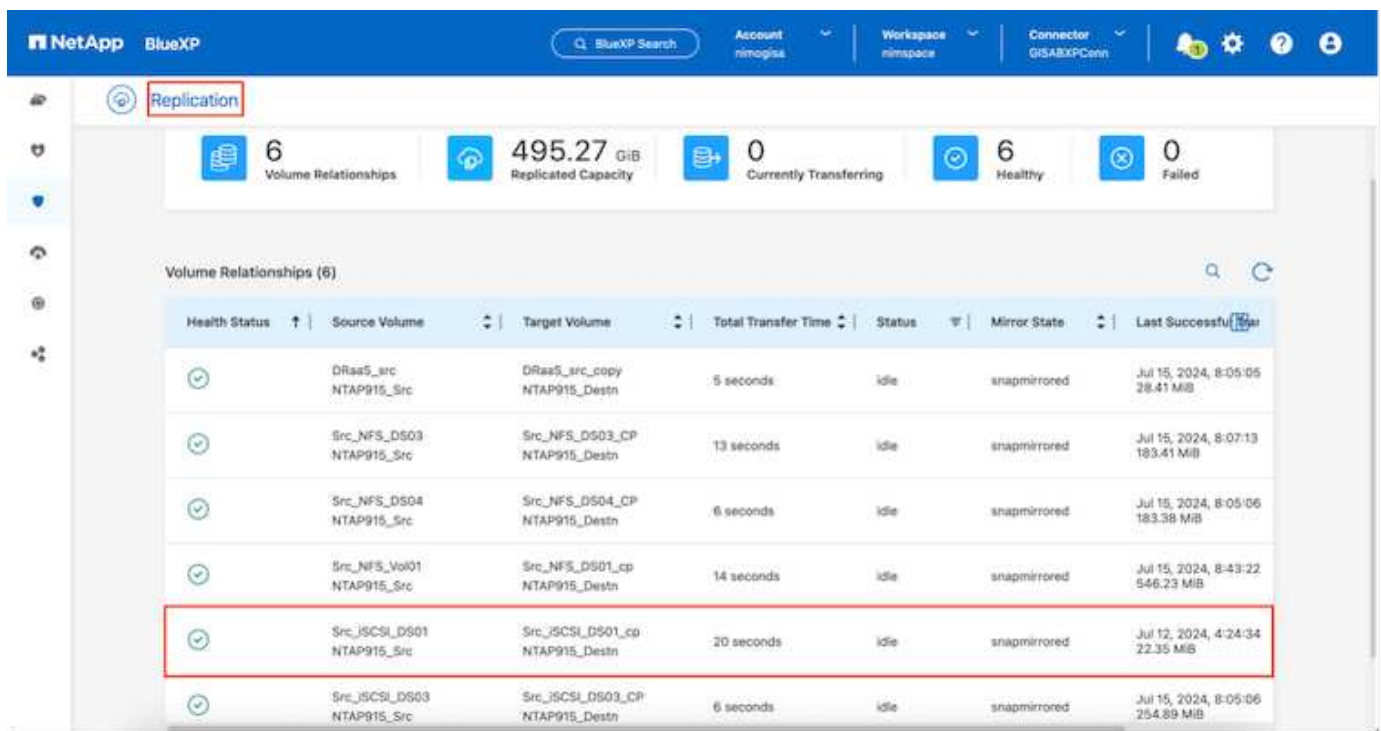
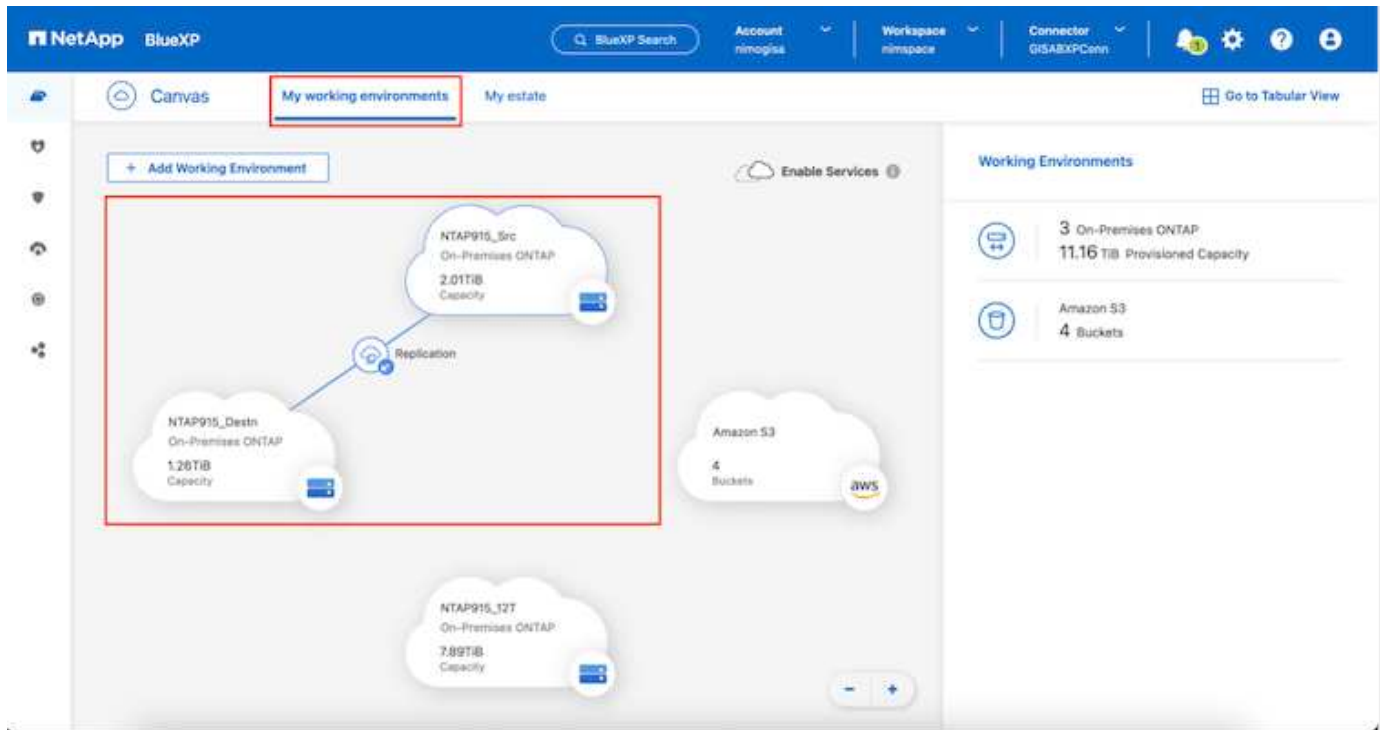


The resource group can also be created while creating a replication plan.

The boot order of the VMs can be defined or modified during the creation of resource groups by using simple drag and drop mechanism.

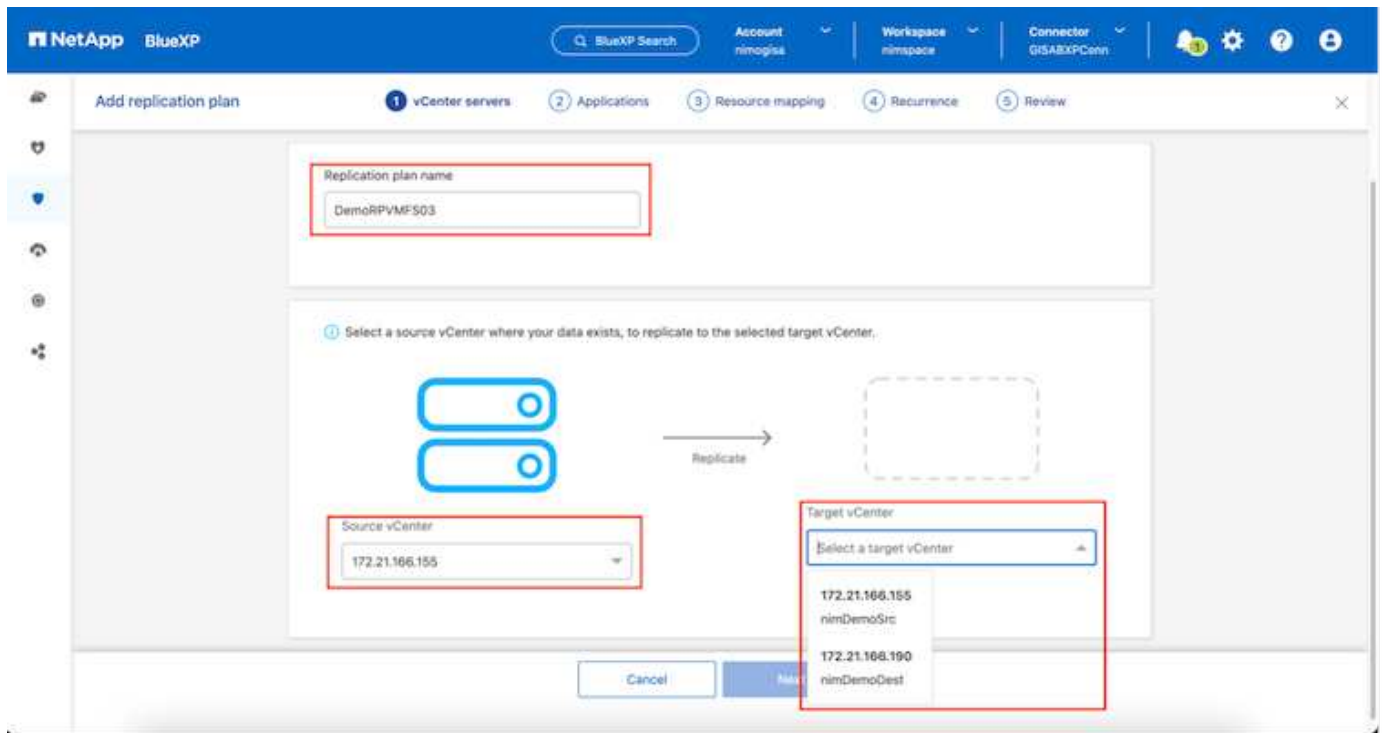


Once the resource groups are created, the next step is to create the execution blueprint or a plan to recover virtual machines and applications in the event of a disaster. As mentioned in the prerequisites, SnapMirror replication can be configured beforehand or DRaaS can configure it using the RPO and retention count specified during creation of the replication plan.

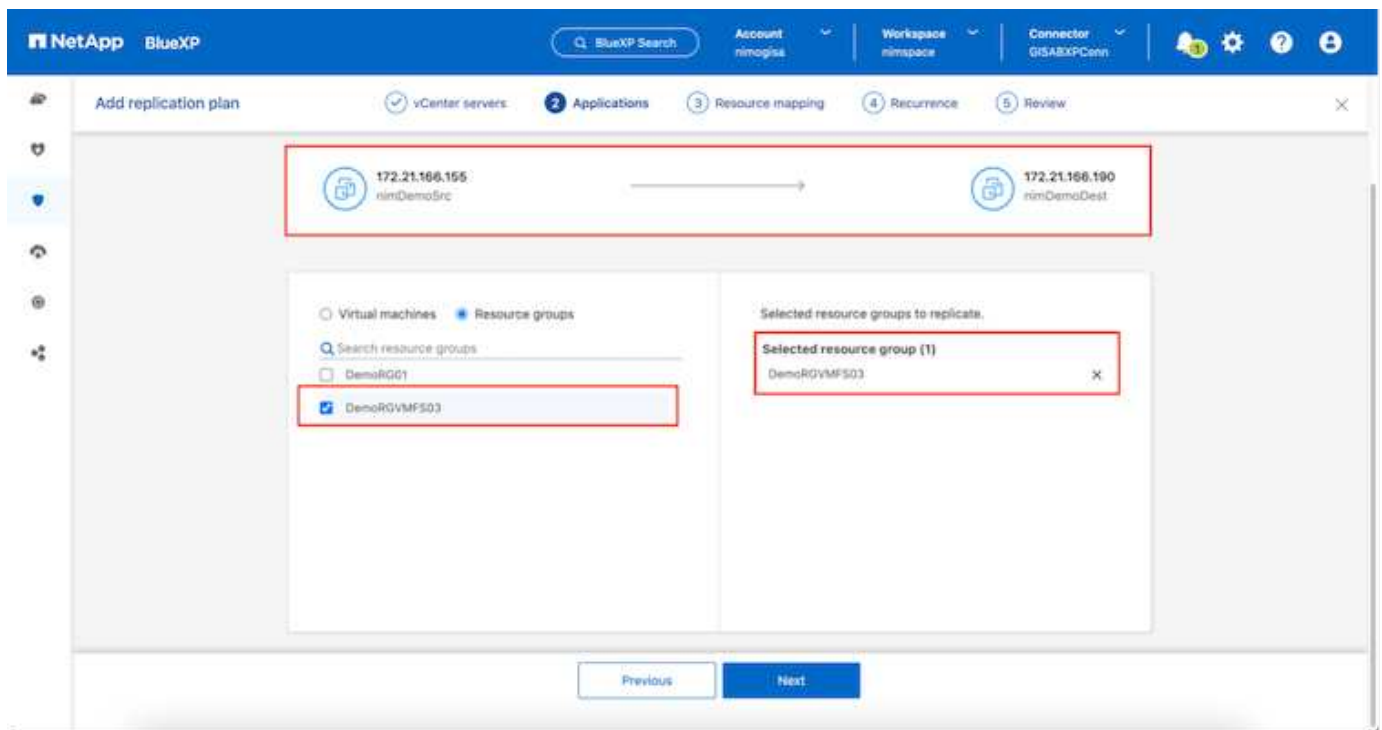


Configure the replication plan by selecting the source and destination vCenter platforms from the drop down and pick the resource groups to be included in the plan, along with the grouping of how applications should be restored and powered on and mapping of clusters and networks. To define the recovery plan, navigate to the **Replication Plan** tab and click **Add Plan**.

First, select the source vCenter and then select the destination vCenter.



The next step is to select existing resource groups. If no resource groups 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.

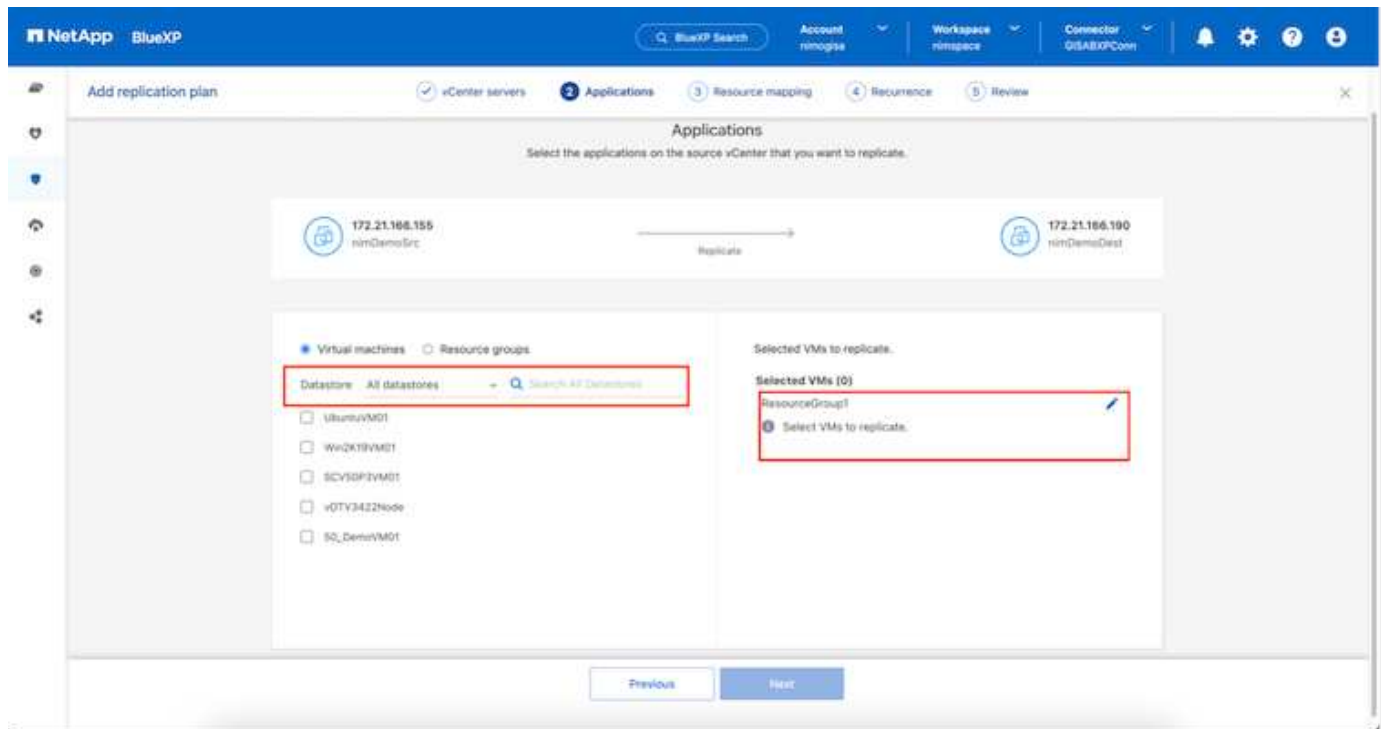


Resource group allows to set boot order using the drag and drop functionality. It can be used to easily modify the order in which the VMs would be powered on during the recovery process.



Each virtual machine within a resource group is started in sequence based on the order. Two resource groups are started in parallel.

The below screenshot shows the option to filter virtual machines or specific datastores based on organizational requirements if resource groups are not created beforehand.



Once the resource groups are selected, create the failover mappings. In this step, specify how the resources from the source environment maps 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](#).

Virtual machines

IP address type: Static Target IP: Same as source

☐ Use the same credentials for all VMs

☐ Use the same script for all VMs

Source VM	CPUs	RAM	Boot delay(mins between 0 and 10)	Create application consistent replicas	Scripts
DemoR001					
S0_DemoVM	2	4 GiB	0	<input type="checkbox"/>	None
S0_DemoVM01	2	4 GiB	0	<input type="checkbox"/>	None
S0_DemoVM02	2	4 GiB	0	<input type="checkbox"/>	None

Previous Next



By default, same mapping parameters are used for both test and failover operations. To apply different mappings for test environment, select the Test mapping option after unchecking the checkbox as shown below:

Resource mapping

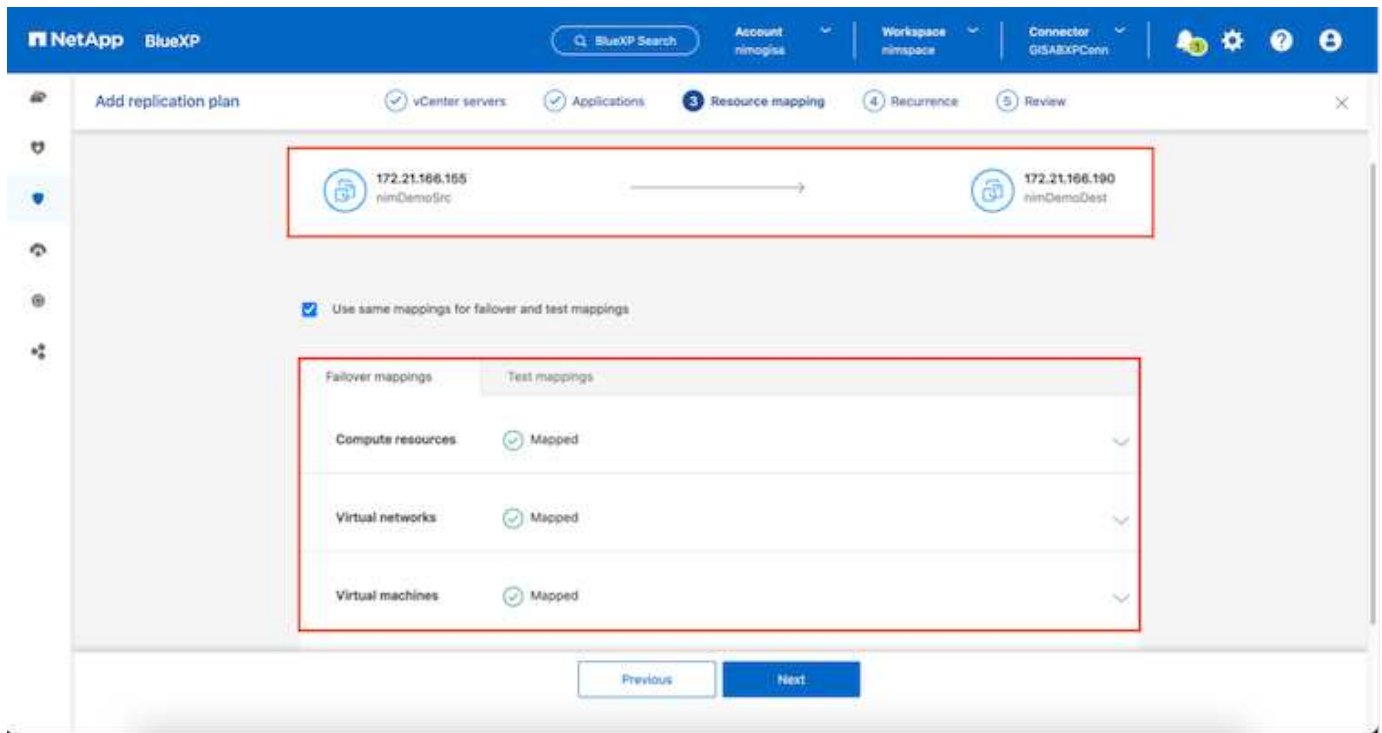
Specify how resources map from the source to the target.

172.21.166.155 nimDemoSrc → 172.21.166.190 nimDemoDest

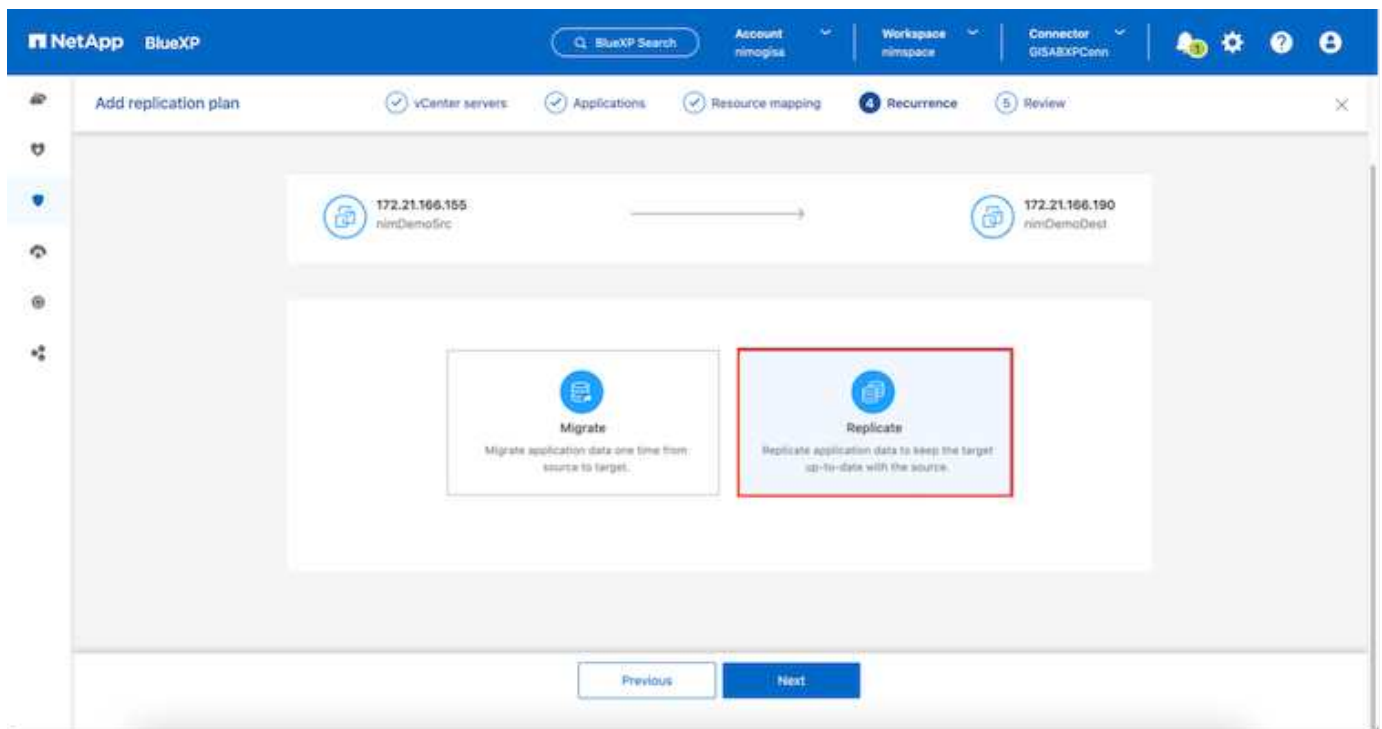
☒ Use same mappings for failover and test mappings

Failover mappings Test mappings

Once the resource mapping is complete, click Next.



Select the recurrence type. In simple words, select Migrate (one time migration using failover) or recurring continuous replication option. In this walkthrough, Replicate option is selected.



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

NetApp BlueXP

BlueXP Search Account nimoglas Workspace nimspace Connector GISABXPConn

Add replication plan vCenter servers Applications Resource mapping Recurrence **Review**

172.21.166.155 nimDemoSrc Replicate 172.21.166.190 nimDemoDest

Plan details Failover mapping Virtual machines

Plan name DemoRPMVF503

Recurrence Replicate

Previous Add plan

NetApp BlueXP

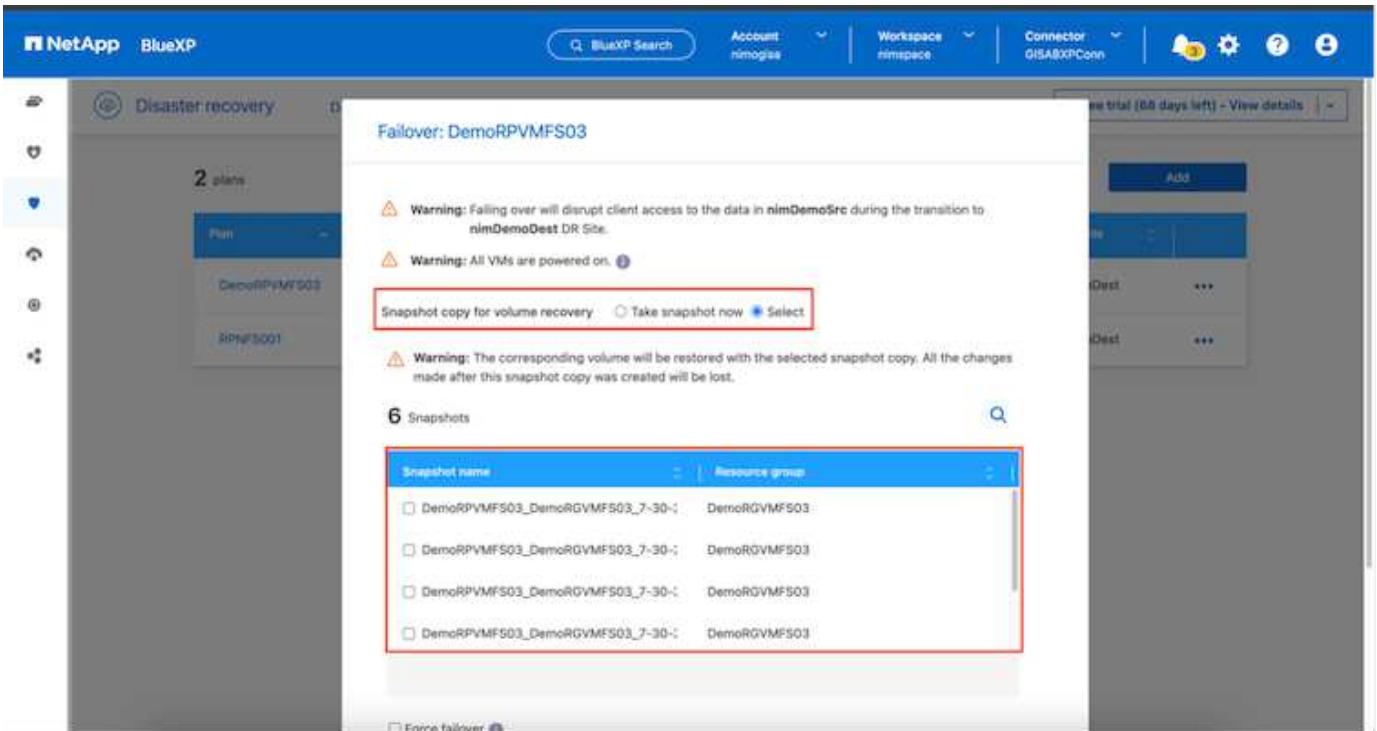
BlueXP Search Account nimoglas Workspace nimspace Connector GISABXPConn

Disaster recovery Dashboard Sites **Replication plans** Resource groups Job monitoring Free trial (63 days left) - View details

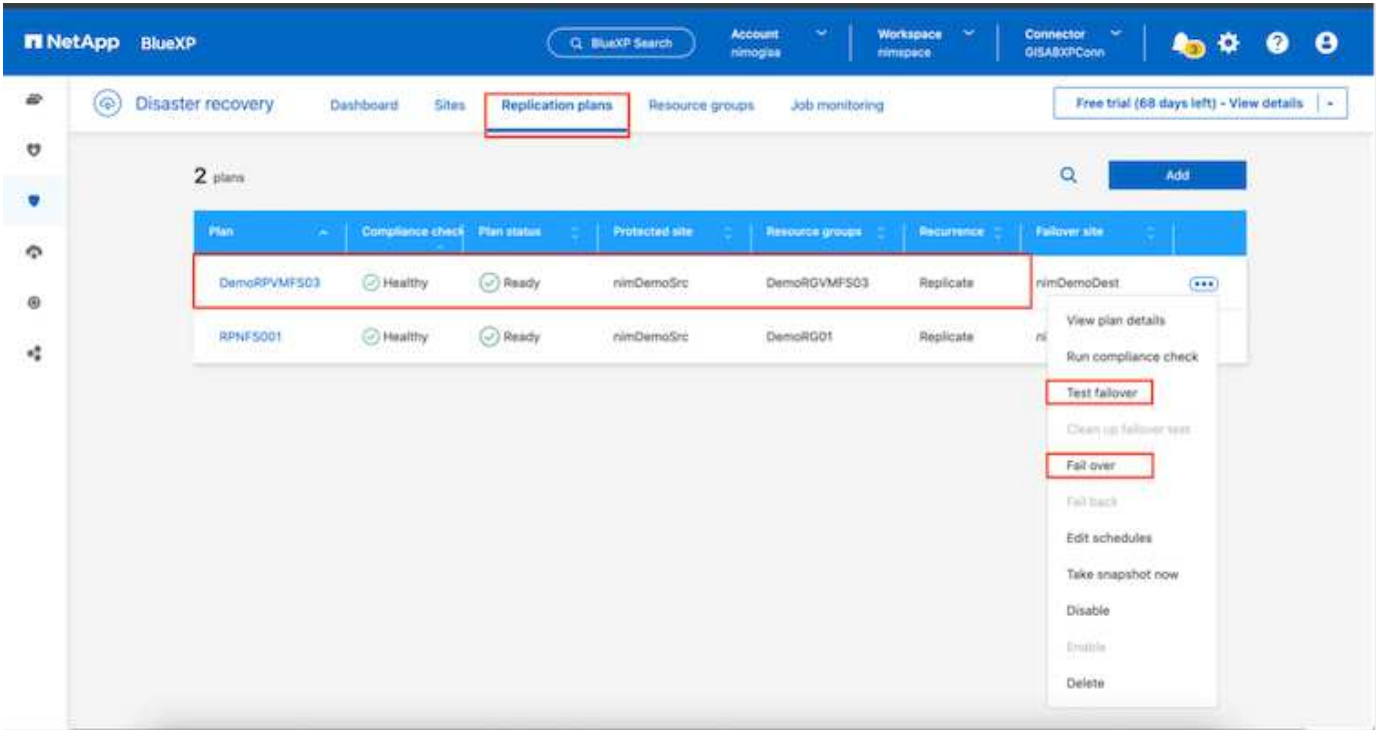
2 plans

Plan	Compliance check	Plan status	Protected site	Resource groups	Recurrence	Failover site
DemoRPMVF503	Healthy	Ready	nimDemoSrc	DemoRPMVF503	Replicate	nimDemoDest
RPMFS001	Healthy	Ready	nimDemoSrc	DemoRG01	Replicate	nimDemoDest

Once the replication plan is created, failover can be performed depending on the requirements by selecting the failover option, test-failover option, or the migrate option. BlueXP disaster recovery ensures that the replication process is being executed according to the plan every 30 minutes. During the failover and test-failover options, you can use the most recent SnapMirror Snapshot copy, or you can select a specific Snapshot copy from a point-in-time Snapshot copy (per the retention policy of SnapMirror). The point-in-time option can be very helpful if there is a corruption event like ransomware, where the most recent replicas are already compromised or encrypted. BlueXP disaster recovery shows all available recovery points.



To trigger failover or test failover with the configuration specified in the replication plan, click on **Failover** or **Test failover**.



What happens during a failover or test failover operation?

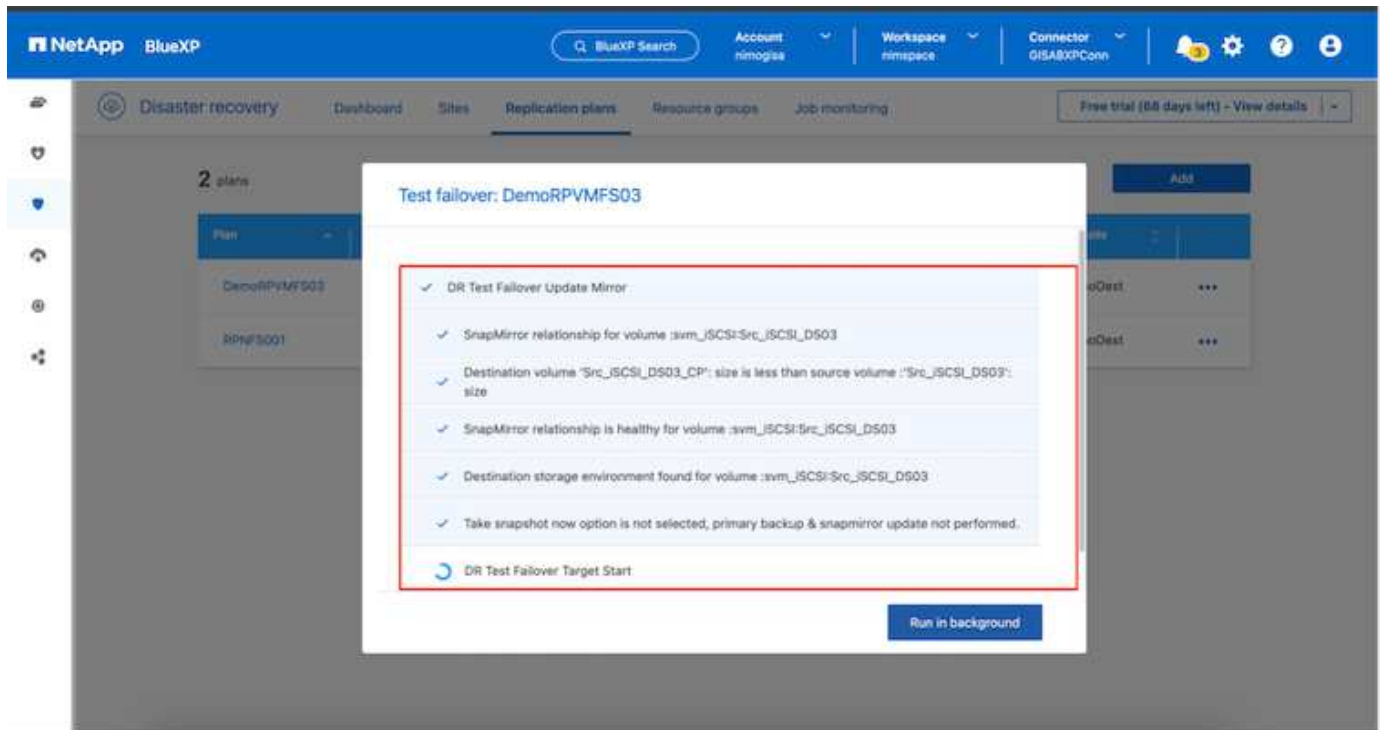
During a test failover operation, BlueXP disaster recovery creates a FlexClone volume on the destination ONTAP storage system using the latest Snapshot copy or a selected snapshot of the destination volume.



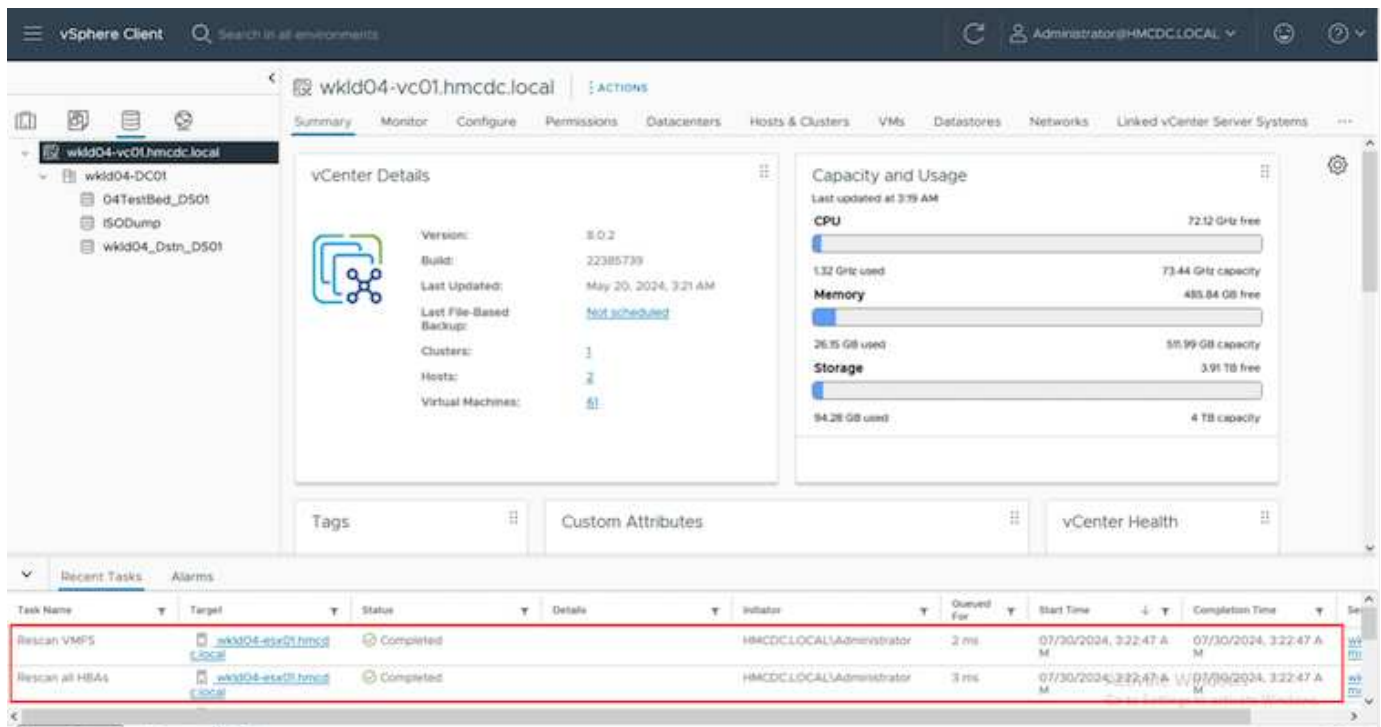
A test failover operation creates a cloned volume on the destination ONTAP storage system.

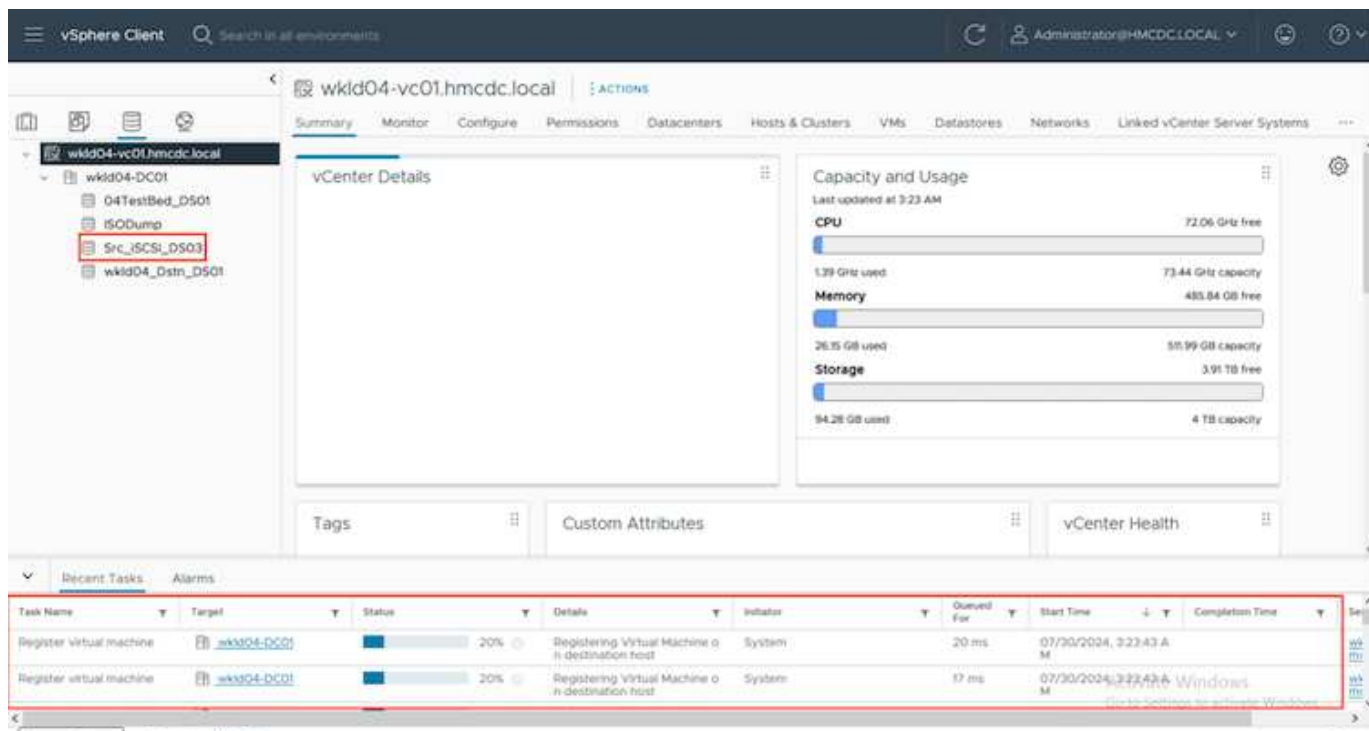


Running a test recovery operation does not affect the SnapMirror replication.



During the process, BlueXP disaster recovery does not map the original target volume. Instead, it makes a new FlexClone volume from the selected Snapshot and a temporary datastore backing the FlexClone volume is mapped to the ESXi hosts.

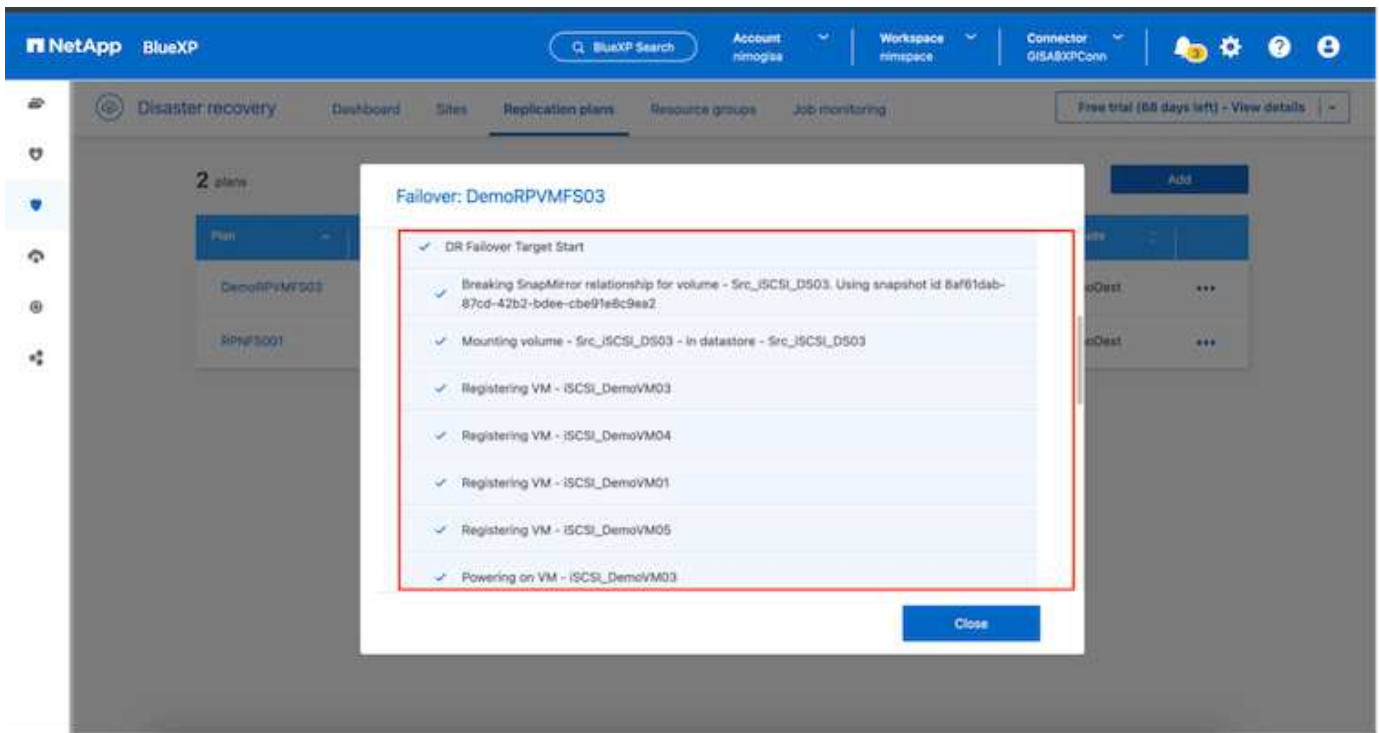




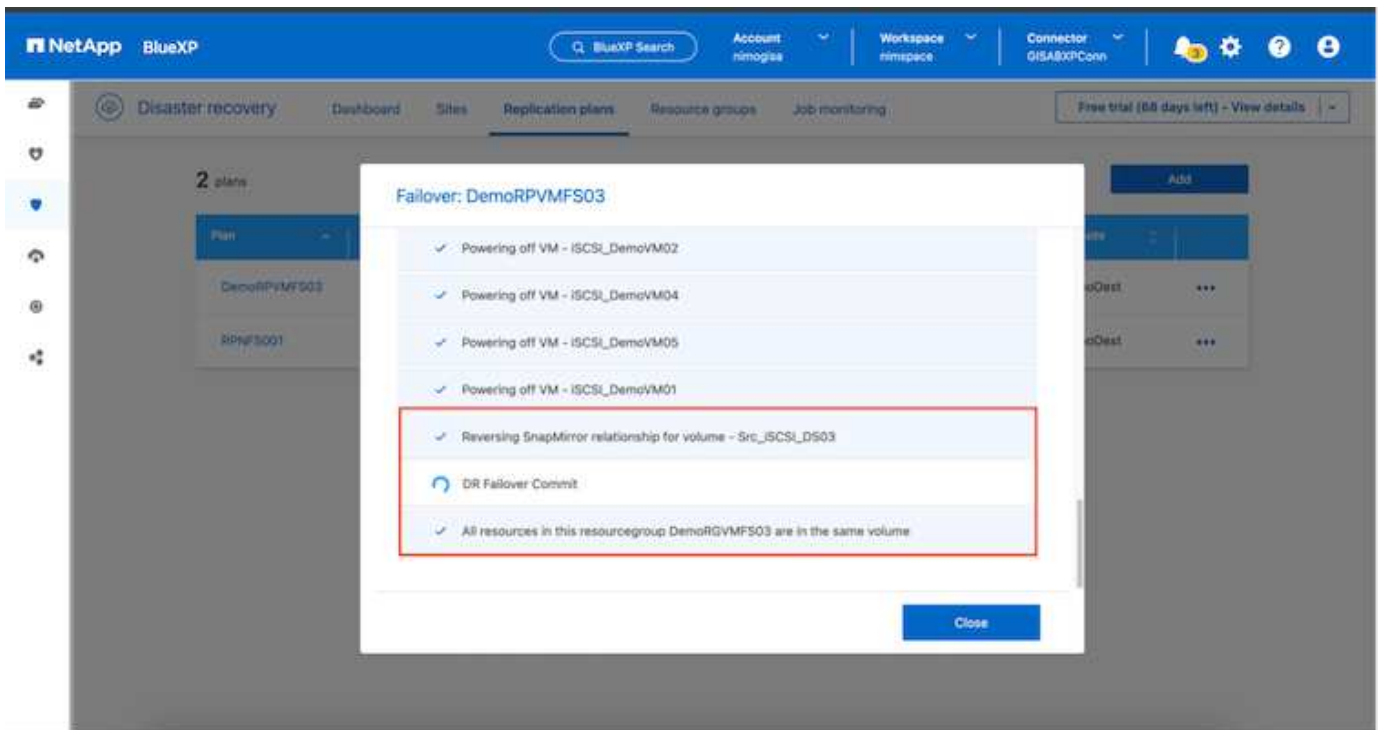
When the test failover operation completes, the cleanup operation can be triggered using **"Clean Up failover test"**. During this operation, BlueXP disaster recovery destroys the FlexClone volume that was used in the operation.

In the event of real disaster event occurs, BlueXP disaster recovery performs the following steps:

1. Breaks the SnapMirror relationship between the sites.
2. Mounts the VMFS datastore volume after resignature for immediate use.
3. Register the VMs
4. Power on VMs

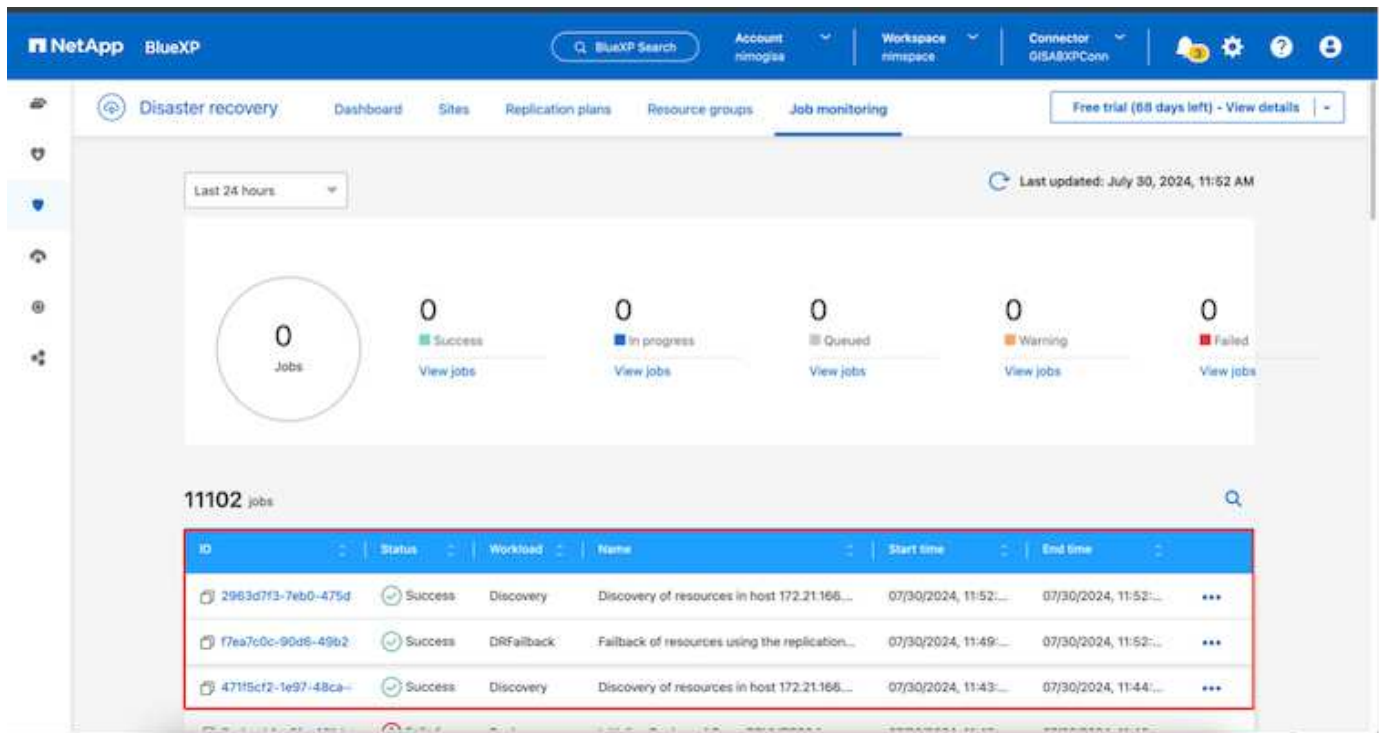


Once the primary site is up and running, BlueXP disaster recovery enables reverse resync for SnapMirror and enables failback, which again can be performed with the click of a button.



And if migrate option is chosen, it is considered as a planned failover event. In this case, an additional step is triggered which is to shut down the virtual machines at the source site. The rest of the steps remains the same as failover event.

From BlueXP 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.



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.

To learn more about this process, feel free to follow the detailed walkthrough video or use the [solution simulator](#).

Set up disaster recovery for NFS datastores using BlueXP disaster recovery

In this use case we outline the procedure to set up disaster recovery using BlueXP disaster recovery for on-premises VMware VMs using NFS datastores. This procedure includes setting up the BlueXP account and connector, adding ONTAP arrays to enable communication between VMware vCenter and ONTAP storage, configuring replication between sites, and creating and testing recovery plans.

Implementing disaster recovery through block-level replication from the production site to the disaster recovery site is a resilient and cost-effective method for safeguarding workloads against site outages and data corruption events, such as ransomware attacks. Using NetApp SnapMirror replication, VMware workloads running on on-premises ONTAP systems with NFS datastore can be replicated to another ONTAP storage system located in a designated recovery datacenter where VMware is also deployed.

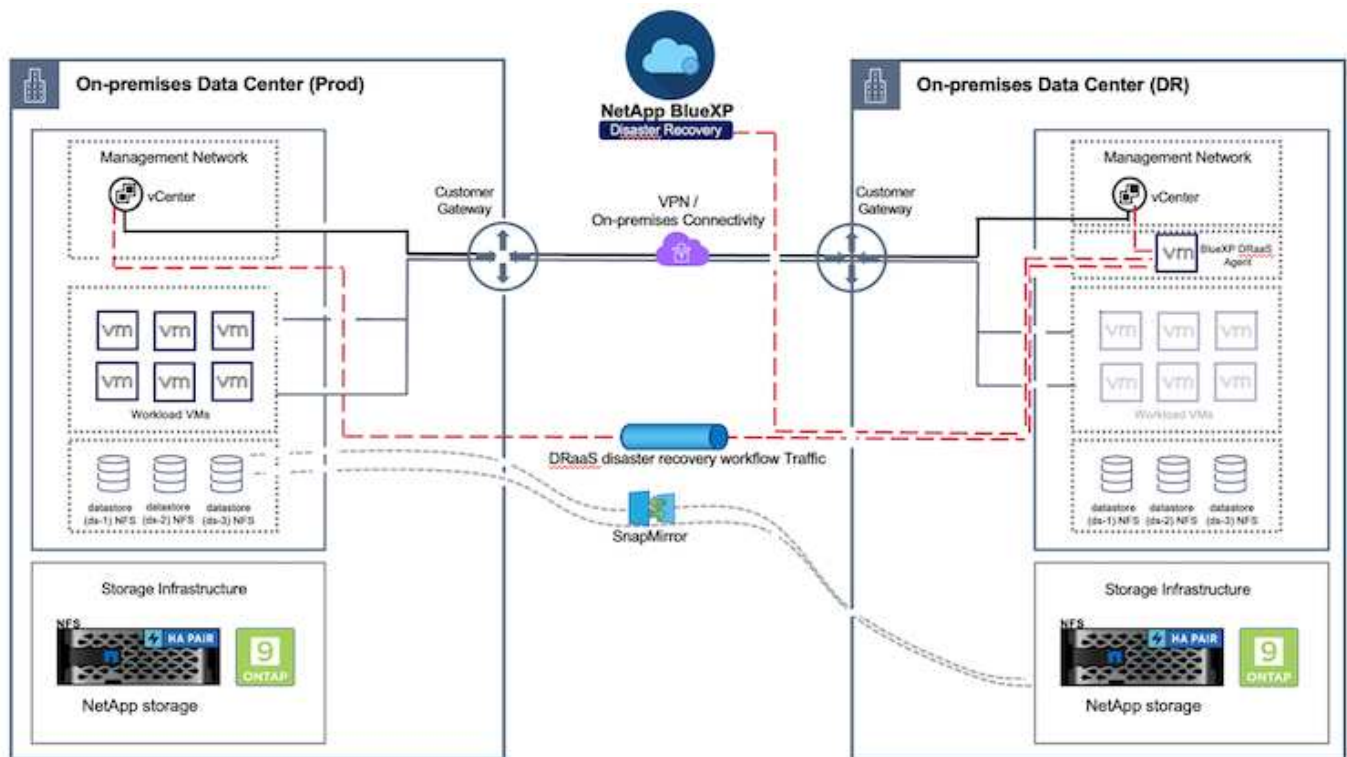
Introduction

This section of the document describes the configuration of BlueXP DRaaS to set up disaster recovery for on-premises VMware VMs to another designated site. As part of this setup, the BlueXP account, BlueXP connector, the ONTAP arrays added within BlueXP workspace which is needed to enable communication from VMware vCenter to the ONTAP storage. In addition, this document details how to configure replication between sites and how to setup and test a recovery plan. The last section has instructions for performing a full site failover and how to failback when the primary site is recovered and brought online.

Utilizing the BlueXP disaster recovery service, integrated into the NetApp BlueXP console, companies can

easily discover their on-premises VMware vCenters and ONTAP storage. Organizations can then create resource groupings, create a disaster recovery plan, associate it with resource groups, and test or execute failover and failback. SnapMirror provides storage-level block replication to keep the two sites up to date with incremental changes, resulting in a Recovery Point Objective (RPO) of up to 5 minutes. Additionally, it is possible to simulate disaster recovery procedures without affecting production or incurring additional storage costs.

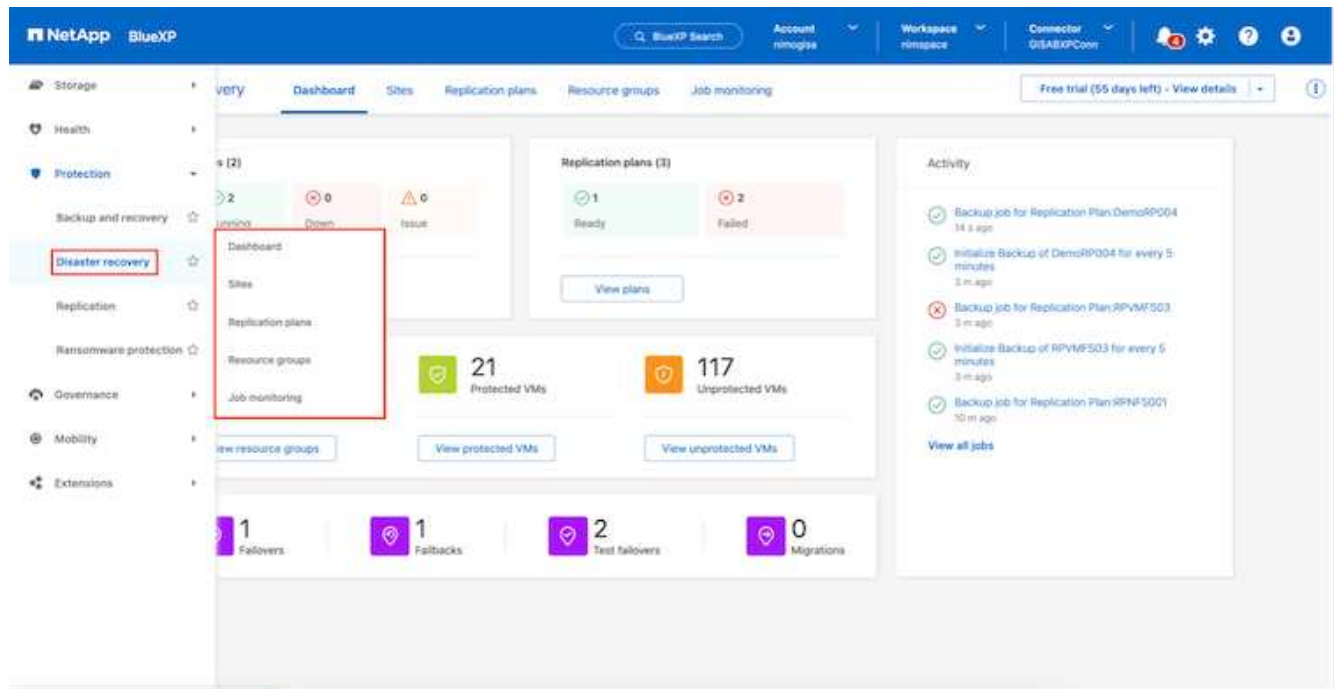
BlueXP disaster recovery leverages ONTAP's FlexClone technology to create a space-efficient copy of the NFS datastore from the last replicated Snapshot on the disaster recovery site. After completing the disaster recovery test, customers can easily delete the test environment without impacting actual replicated production resources. In case of an actual failover, the BlueXP disaster recovery service orchestrates all the necessary steps to automatically bring up the protected virtual machines on the designated disaster recovery site with just a few clicks. The service will also reverse the SnapMirror relationship to the primary site and replicate any changes from the secondary to the primary for a failback operation, when needed. All these capabilities come at a fraction of the cost compared to other well-known alternatives.



Getting started

To get started with BlueXP disaster recovery, use BlueXP console and then access the service.

1. Log in to BlueXP.
2. From the BlueXP left navigation, select Protection > Disaster recovery.
3. The BlueXP disaster recovery Dashboard appears.



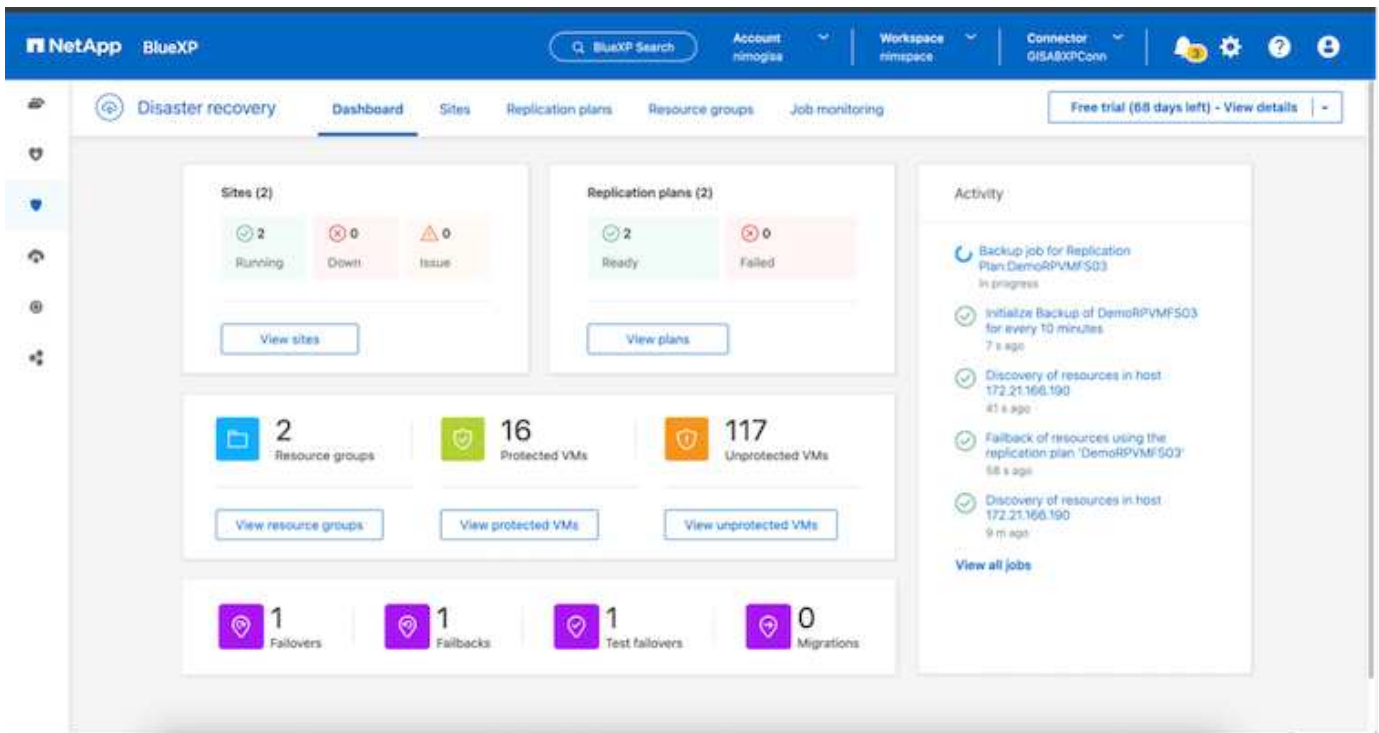
Before configuring disaster recovery plan, ensure the following pre-requisites are met:

- BlueXP Connector is set up in NetApp BlueXP.
- BlueXP connector instance have connectivity to the source and destination vCenter and storage systems.
- NetApp Data ONTAP cluster to provide storage NFS datastores.
- On-premises NetApp storage systems hosting NFS datastores for VMware are added in BlueXP.
- 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 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.



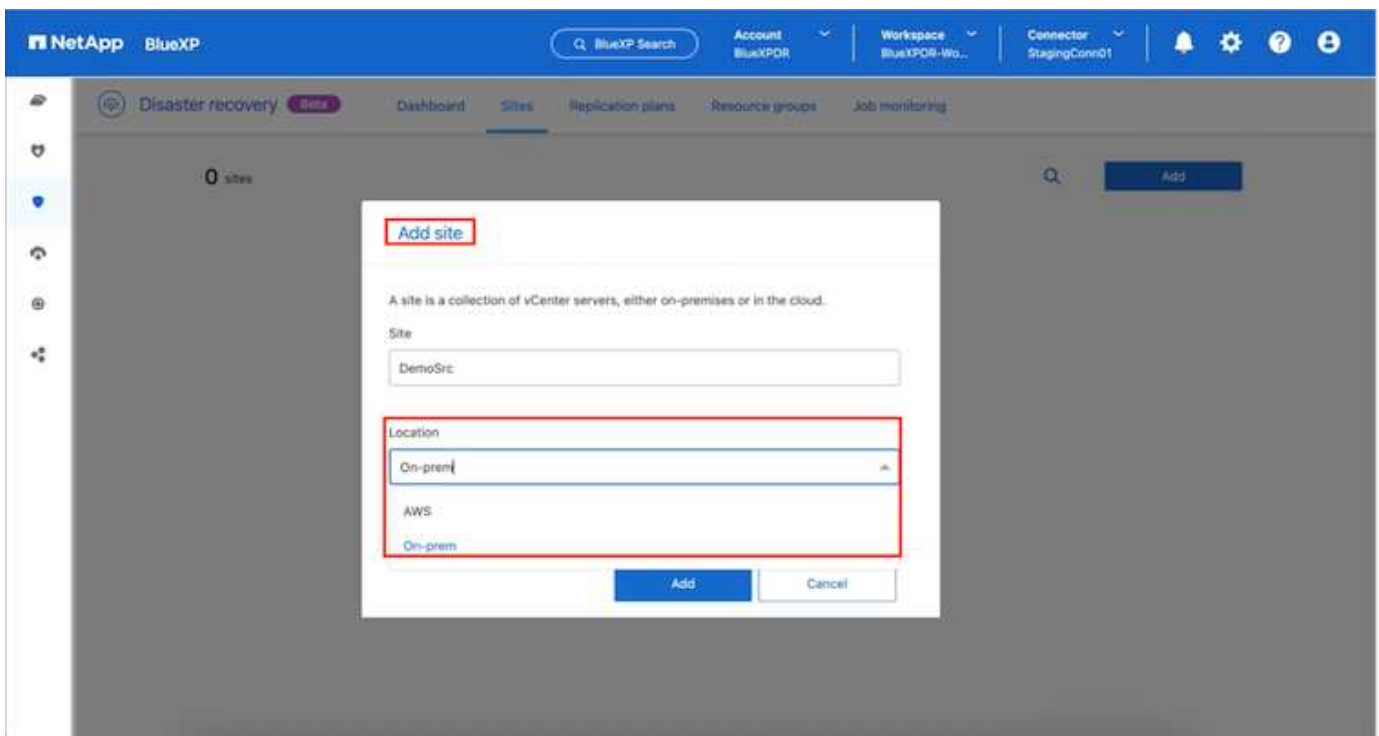
NetApp recommends deploying the BlueXP connector in the destination site or in a third site, so that the BlueXP connector can communicate through the network with source and destination resources.



BlueXP disaster recovery configuration

The first step in preparing for disaster recovery is to discover and add the on-premises vCenter and storage resources to BlueXP disaster recovery.

Open BlueXP console and select **Protection > Disaster Recovery** from left navigation. Select **Discover vCenter servers** or use top menu, Select **Sites > Add > Add vCenter**.



Add the following platforms:

- **Source.** On-premises vCenter.

Add vCenter server

Enter connection details for the vCenter server that is accessible from the BlueXP Connector.

Site: BlueXP Connector:

vCenter IP address:

vCenter user name: vCenter password:

☒ Use self-signed certificates

- **Destination.** VMC SDDC vCenter.

Add vCenter server

Enter connection details for the vCenter server that is accessible from the BlueXP Connector.

Site: BlueXP Connector:

vCenter IP address:

vCenter user name: vCenter password:

☒ Use self-signed certificates

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. BlueXP DRaaS also creates the SnapMirror relationship provided cluster and SVM peering is configured beforehand.

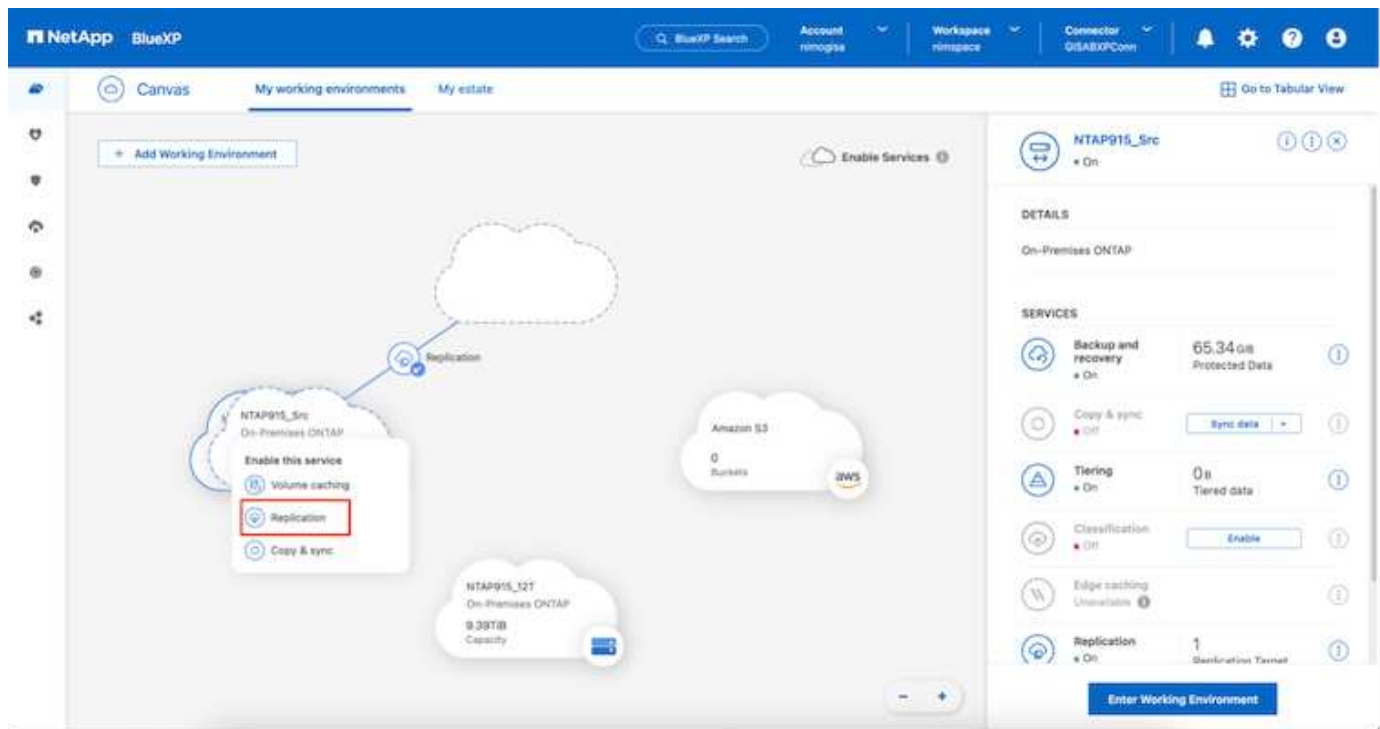
For cases in which the primary storage is not completely lost, SnapMirror provides an efficient means of resynchronizing the primary and DR sites. SnapMirror can resynchronize the two sites, transferring only changed or new data back to the primary site from the DR site by simply reversing the SnapMirror relationships. This means replication plans in BlueXP DRaaS 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, BlueXP DRaaS picks up the relationship and continues with the rest of the workflow operations.

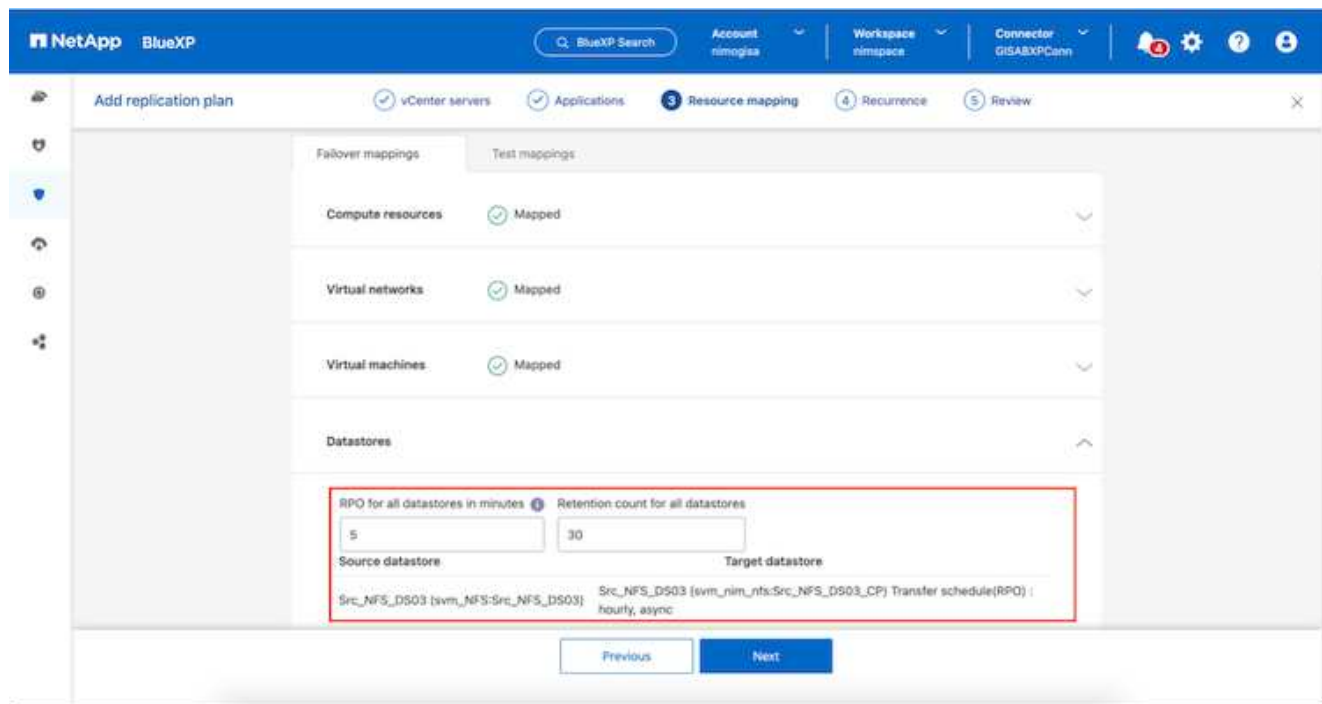
How to set it up for VMware Disaster Recovery

The 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 BlueXP 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.



BlueXP DRaaS can also automate the same provided the following two criteria's are met:

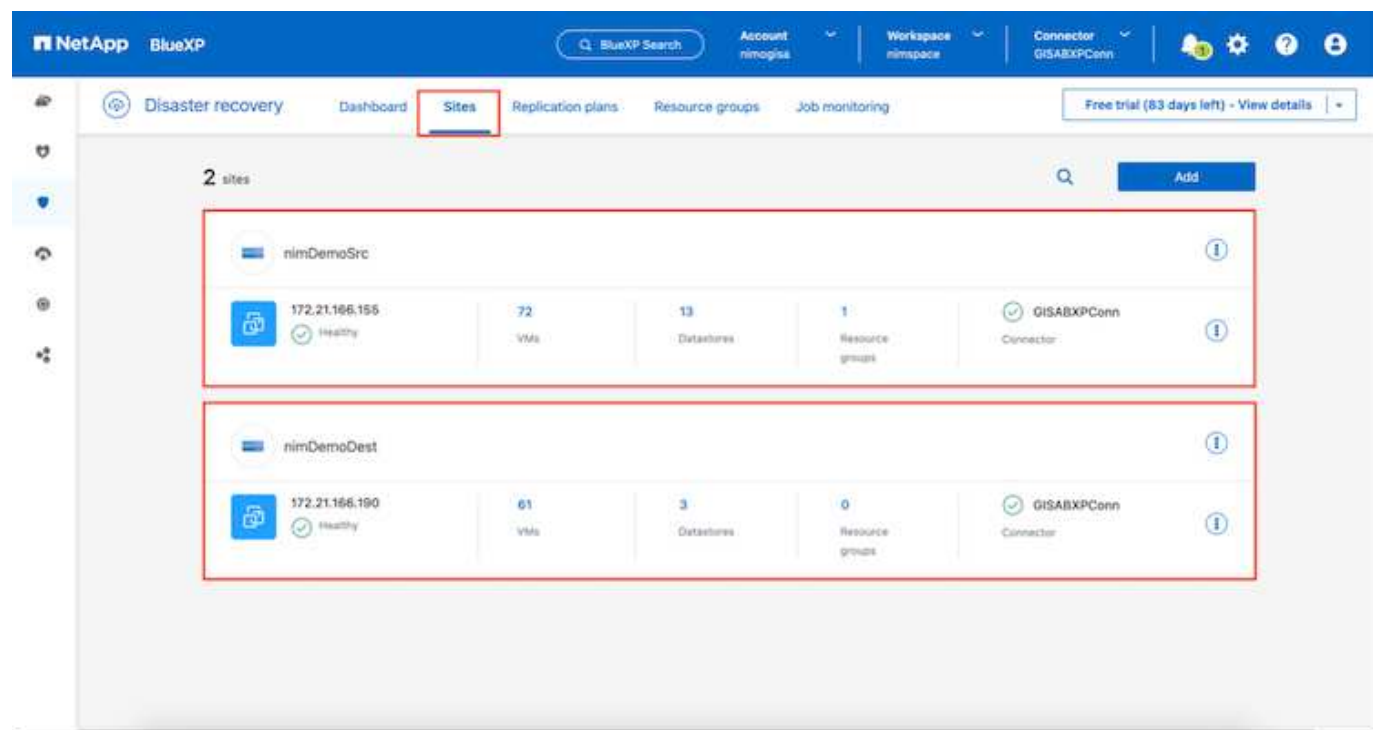
- Source and destination clusters have a peer relationship.
- Source SVM and destination SVM have a peer relationship.



If SnapMirror relationship is already configured for the volume via CLI, BlueXP DRaaS picks up the relationship and continues with the rest of the workflow operations.

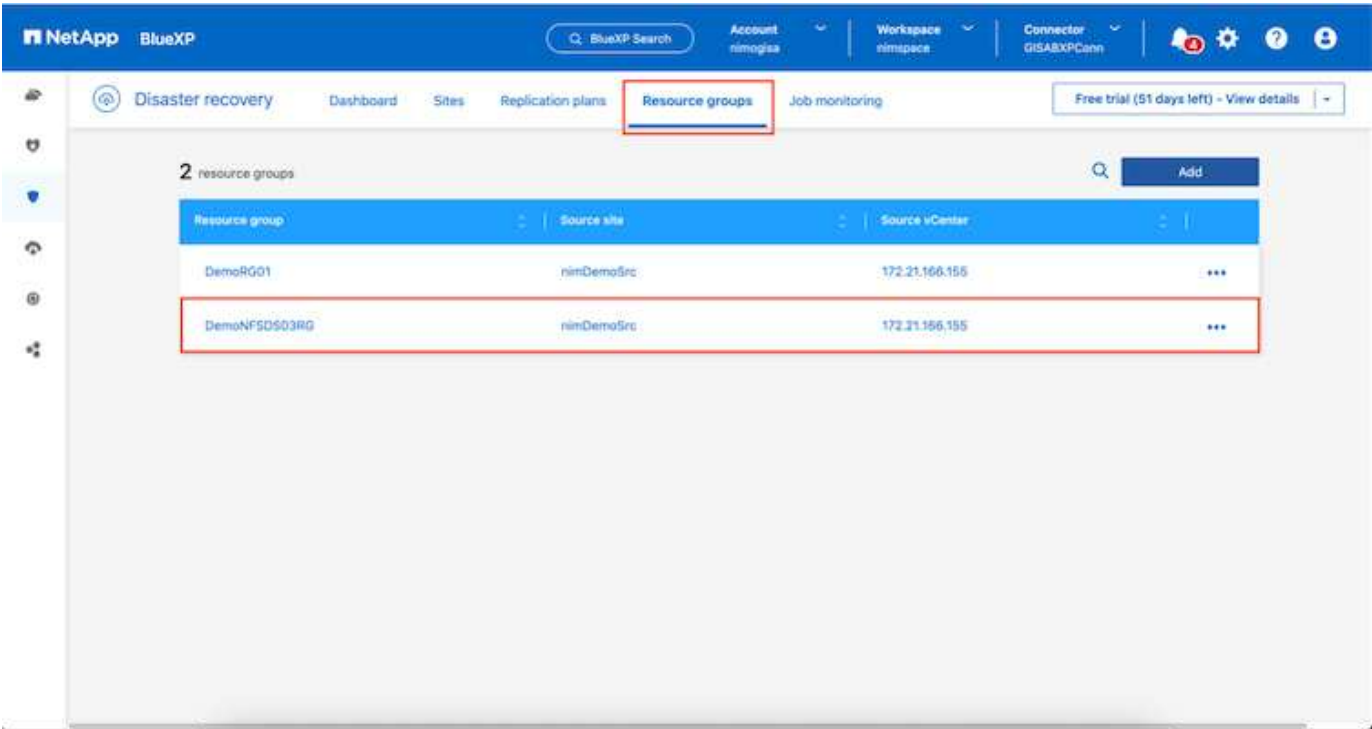
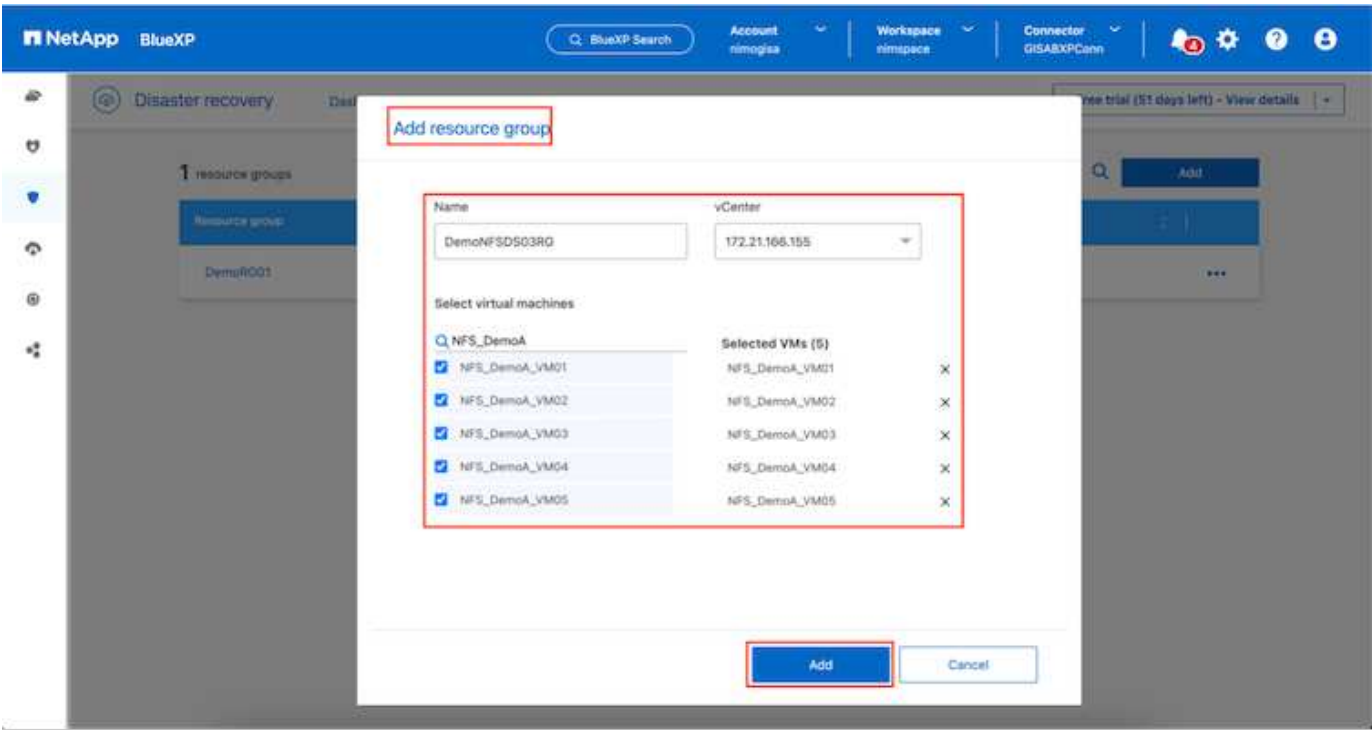
What can BlueXP disaster recovery do for you?

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



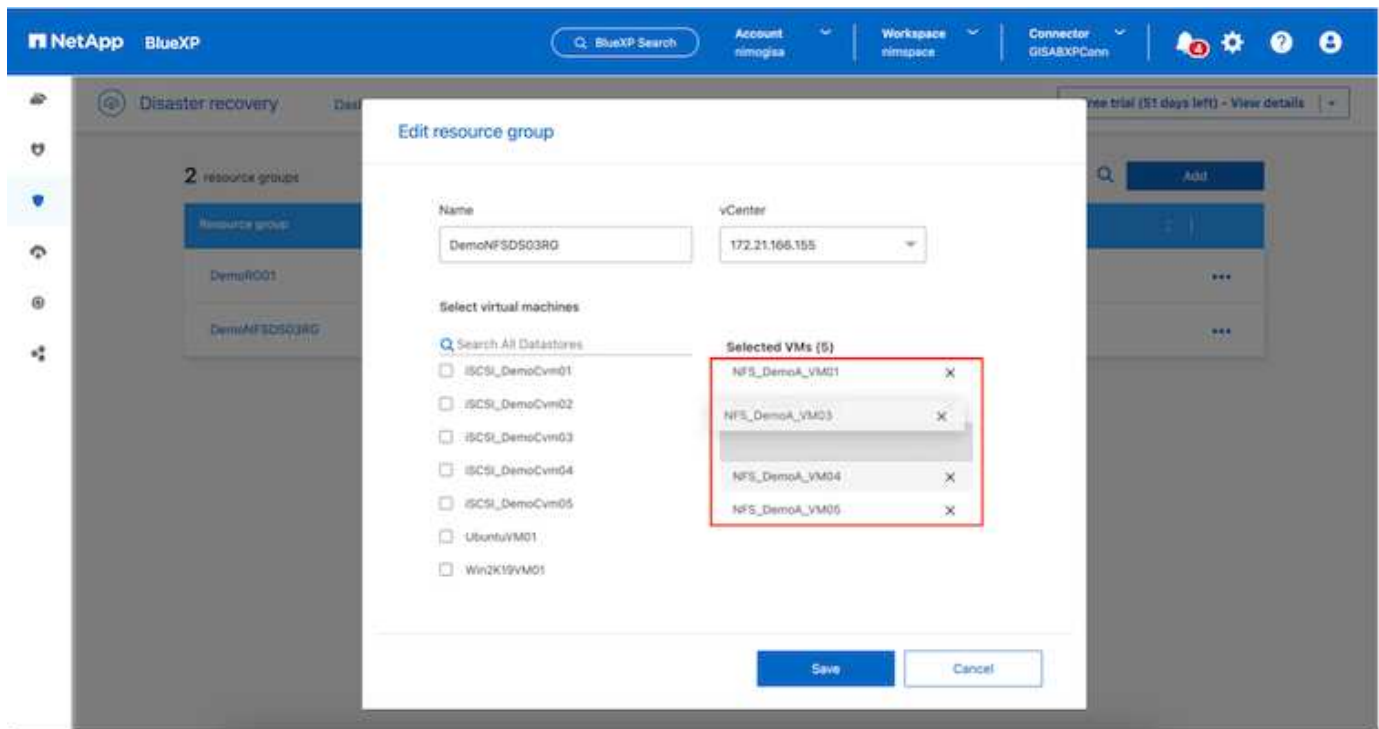
After the sites have been added, VMs can be grouped into resource groups. BlueXP disaster recovery

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. To start creating resource groups, navigate to **Resource Groups** and click **Create New Resource Group**.

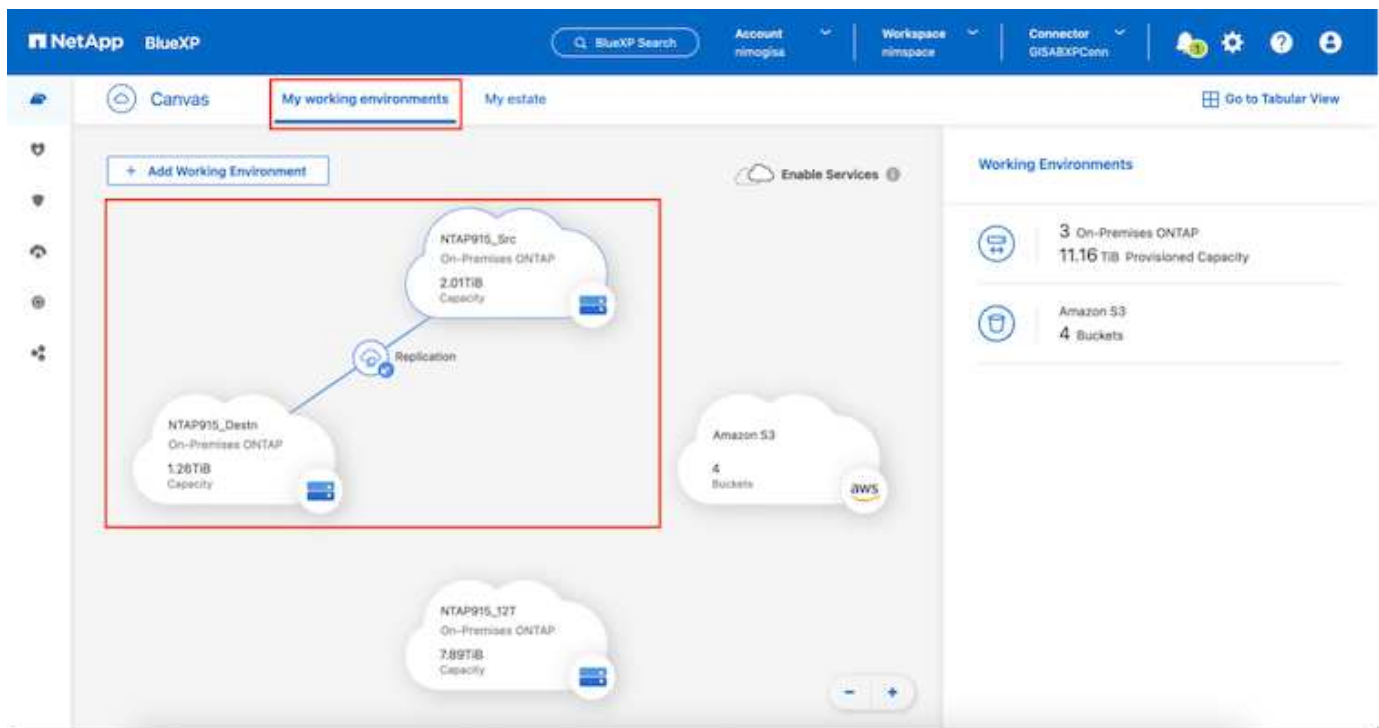


The resource group can also be created while creating a replication plan.

The boot order of the VMs can be defined or modified during the creation of resource groups by using simple drag and drop mechanism.



Once the resource groups are created, the next step is to create the execution blueprint or a plan to recover virtual machines and applications in the event of a disaster. 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.



Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
	NTAP915_Src	NTAP915_Destn				2023 Sep
✓	Demo_TPS_DS01 NTAP915_Src	Demo_TPS_DS01_Copy NTAP915_Destn	13 seconds	idle	snapmirrored	Aug 5, 2024, 6:15 386.63 MiB
✓	Src_250_Vol01 NTAP915_Src	Src_250_Vol01_Copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12:1 79.23 MiB
✓	Src_NFS_DS03 NTAP915_Src	Src_NFS_DS03_CP NTAP915_Destn	12 seconds	idle	snapmirrored	Aug 16, 2024, 12:1 24.64 MiB
✓	Src_NFS_DS04 NTAP915_Src	Src_NFS_DS04_CP NTAP915_Destn	3 seconds	idle	snapmirrored	Aug 16, 2024, 12:1 47.38 MiB
✓	Src_JSCSI_DS04 NTAP915_Src	Src_JSCSI_DS04_copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12:1 108.87 MiB
✓	nimpra NTAP915_Src	nimpra_dest NTAP915_Destn	2 seconds	idle	snapmirrored	Aug 16, 2024, 12:1 3.48 KiB

Configure the replication plan by selecting the source and destination vCenter platforms from the drop down 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 Plan** tab and click **Add Plan**.

First, select the source vCenter and then select the destination vCenter.

1 vCenter servers 2 Applications 3 Resource mapping 4 Recurrence 5 Review

Replication plan name
DemoNFSDS03RP

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

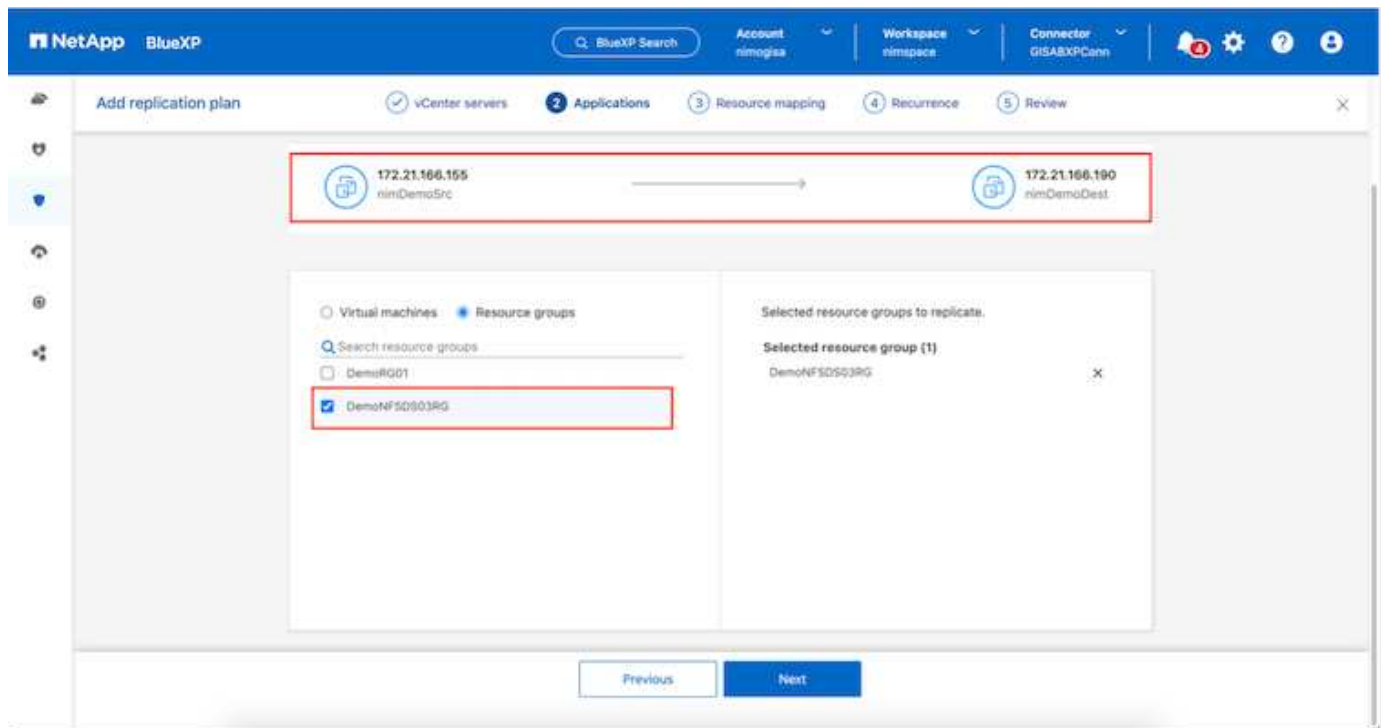
Source vCenter: 172.21.166.155

Target vCenter: 172.21.166.190

Cancel Next

The next step is to select existing resource groups. If no resource groups 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.

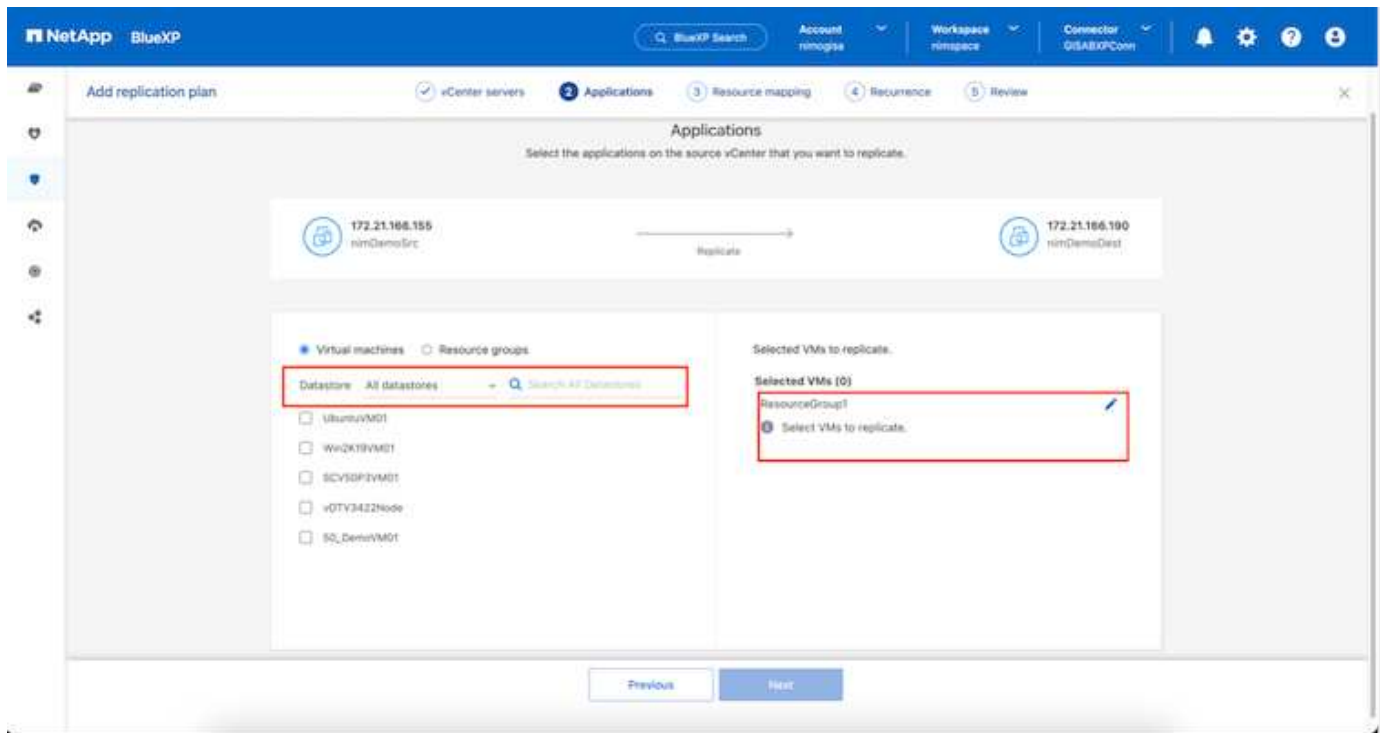


Resource group allows to set boot order using the drag and drop functionality. It can be used to easily modify the order in which the VMs would be powered on during the recovery process.

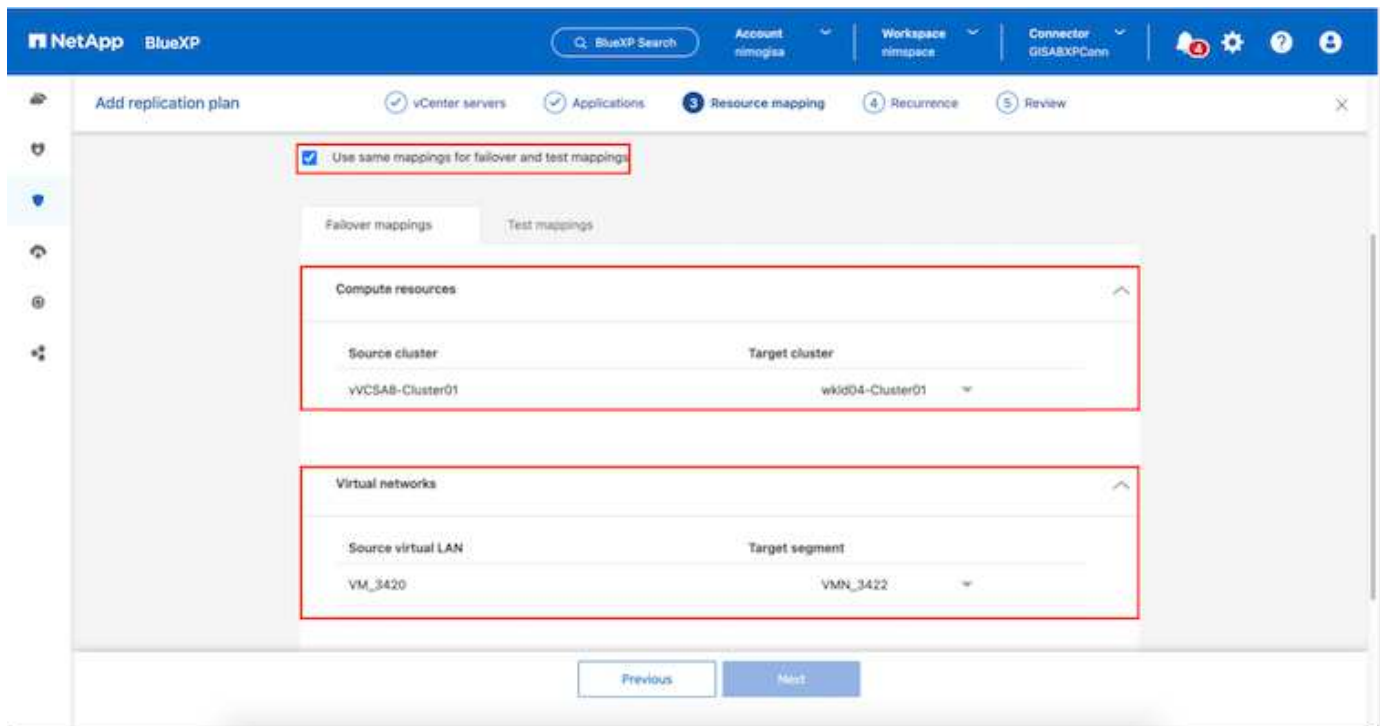


Each virtual machine within a resource group is started in sequence based on the order. Two resource groups are started in parallel.

The below screenshot shows the option to filter virtual machines or specific datastores based on organizational requirements if resource groups are not created beforehand.



Once the resource groups are selected, create the failover mappings. In this step, specify how the resources from the source environment maps 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](#).



By default, 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 as shown below:

NetApp BlueXP

BlueXP Search Account nimogisa Workspace nimspace Connector GISABXPCann

Add replication plan vCenter servers Applications **3 Resource mapping** 4 Recurrence 5 Review

Virtual machines

IP address type: Static Target IP: Same as source

☐ Use the same credentials for Same as source

☐ Use the same script for all VMs Different from source

Source VM	CPU(s)	RAM	Boot delay(mins between 0 and 10)	Create application consistent replicas
DemoNFSDS03RQ				
NFS_DemoA_VM01	2	4 GB	0	<input type="checkbox"/>
NFS_DemoA_VM02	2	4 GB	0	<input type="checkbox"/>

Previous Next

Once the resource mapping is complete, click Next.

NetApp BlueXP

BlueXP Search Account nimogisa Workspace nimspace Connector GISABXPCann

Add replication plan vCenter servers Applications **3 Resource mapping** 4 Recurrence 5 Review

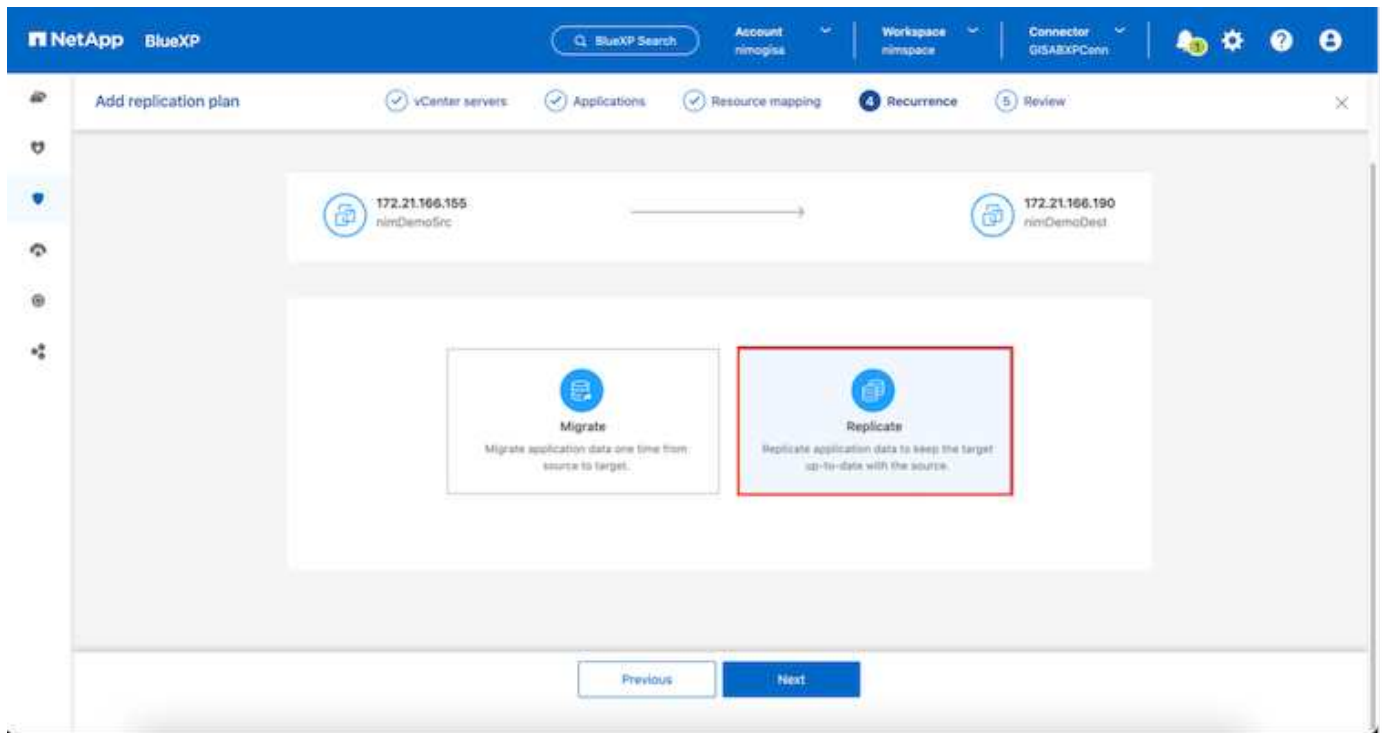
172.21.166.165 nimDemoSrc → 172.21.166.190 nimDemoDest

☒ Use same mappings for failover and test mappings

Fallover mappings	Test mappings
Compute resources	Mapped
Virtual networks	Mapped
Virtual machines	Mapped

Previous Next

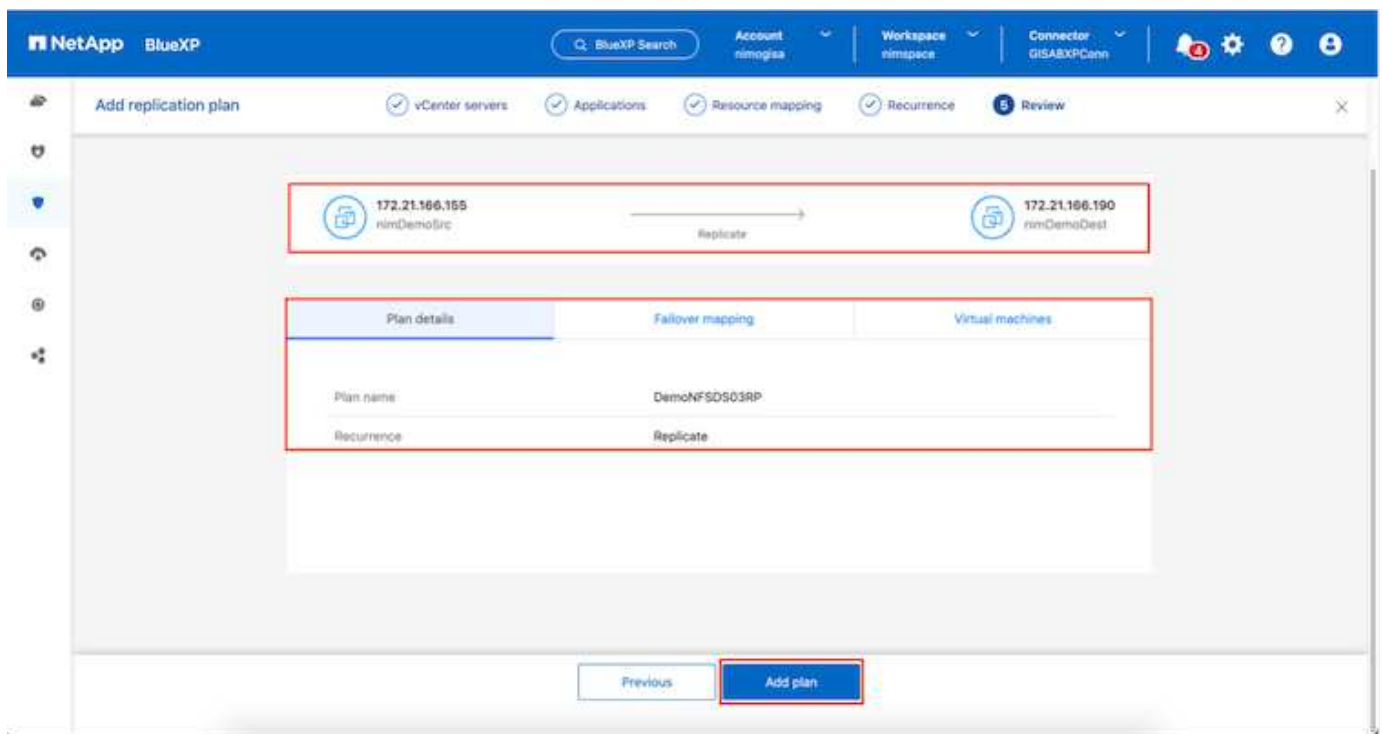
Select the recurrence type. In simple words, select Migrate (one time migration using failover) or recurring continuous replication option. In this walkthrough, Replicate option is selected.

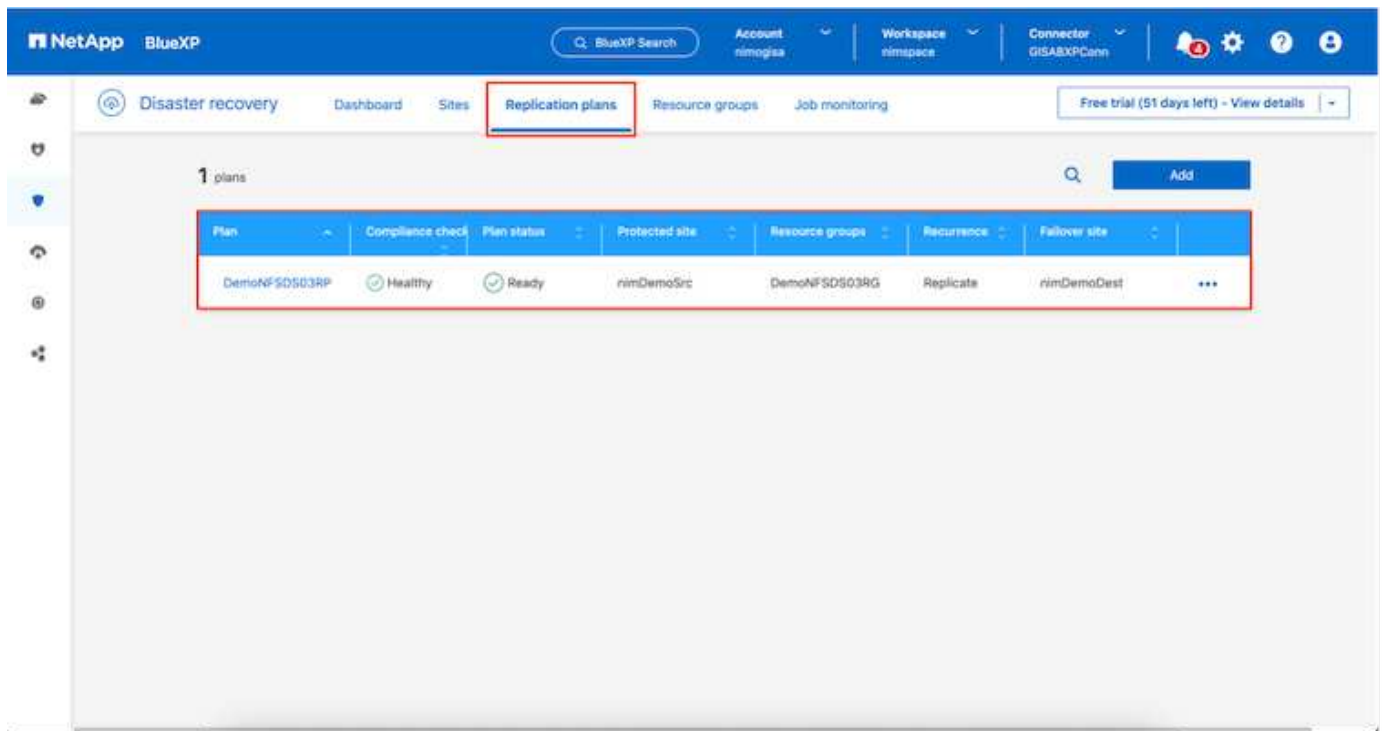


Once done, review the created mappings and then click on **Add plan**.



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), the BlueXP disaster recovery creates a Consistency Group Snapshot.



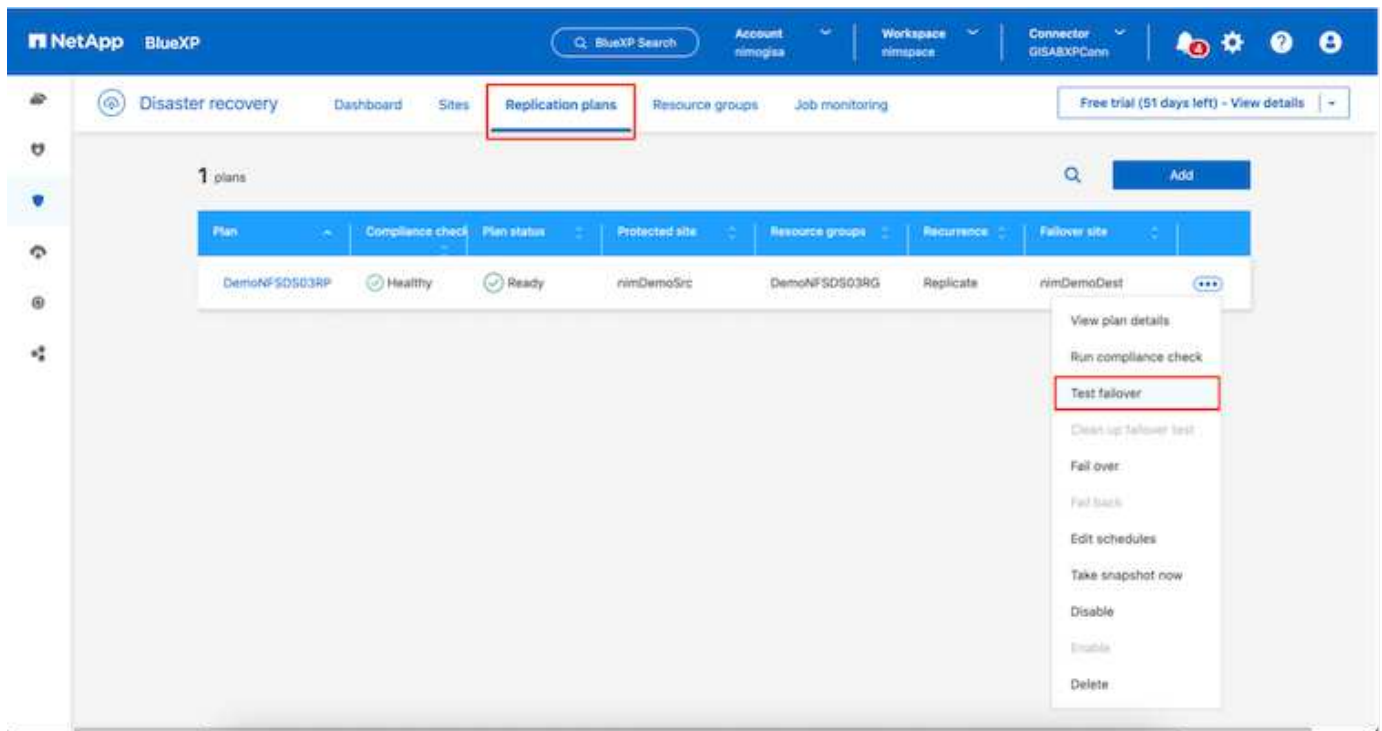


BlueXP DRaaS consists of the following workflows:

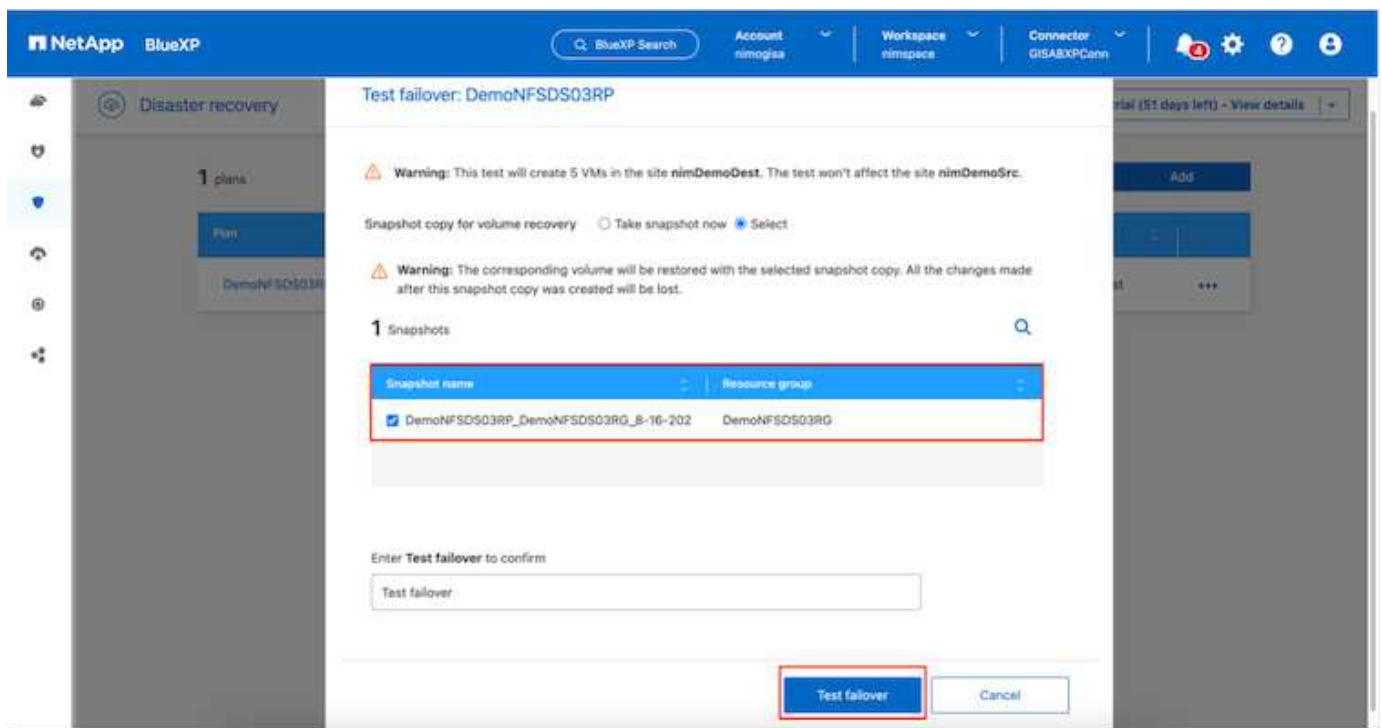
- Test failover (including periodic automated simulations)
- Cleanup failover test
- Failover
- Failback

Test failover

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



BlueXP DRaaS 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



When the VMware administrator runs a test failover operation, BlueXP DRaaS 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 NFS 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.

The screenshot shows the vSphere Client interface for the 'Src_NFS_DS03' NFS datastore. The left sidebar shows a tree view with the following items: wkl04-vc01.hmc.local, wkl04-DC01, 04TestBed_DS01, ISO001, **Src_NFS_DS03** (highlighted with a red box), temodel, and wkl04-Distr_DS01. The central 'Details' pane shows the following information:

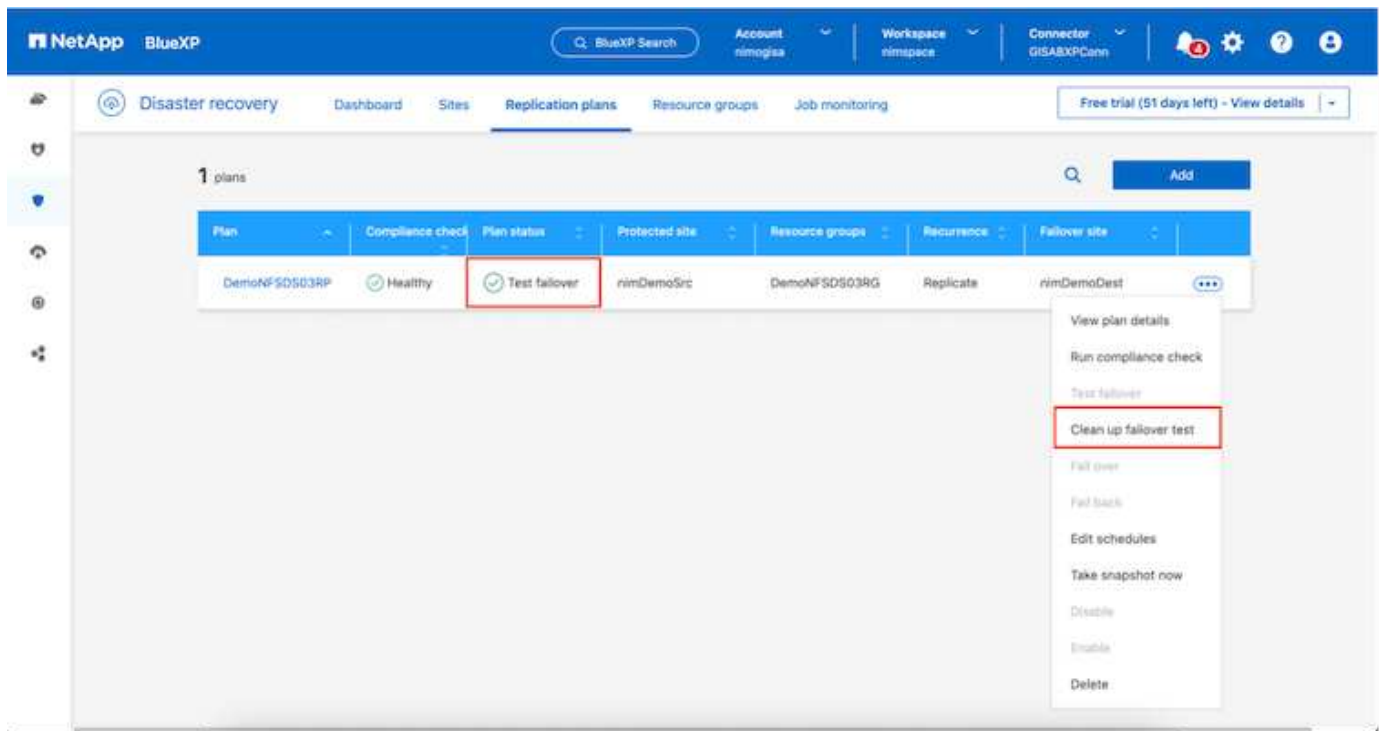
Property	Value
Type	NFS 3
Hosts	2
Virtual machines	5
VM templates	
Server	172.21.166.166
Folder	/Src_NFS_DS03_TEST
Location	gs://vmfs/volumes/b0c5bc2d-1a687494/

The 'Capacity and Usage' section shows a storage bar with 71.22 GB free, 26.78 GB used, and 100 GB capacity. Below this, the 'Recent Tasks' table is displayed:

Task Name	Target	Status	Details	Initiator	Outward For	Start Time	Completion Time	Se
Reconfigure virtual machine	NFS Remount VM02	Completed		HMCDCLOCAL/Administrator	3 ms	06/16/2024, 6:53:59 A	06/16/2024, 6:53:59 A	10
Register virtual machine	src04-DC01	Completed		System	6 ms	06/16/2024, 6:53:58 A	06/16/2024, 6:53:59 A	10
Register virtual machine	src04-DC01	Completed		System	2 ms	06/16/2024, 6:53:58 A	06/16/2024, 6:53:59 A	10
Register virtual machine	src04-DC01	Completed	Registering Virtual Machine 0 in destination host.	System	2 ms	06/16/2024/6:53:58 A	06/16/2024, 6:54:00 A	10

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.



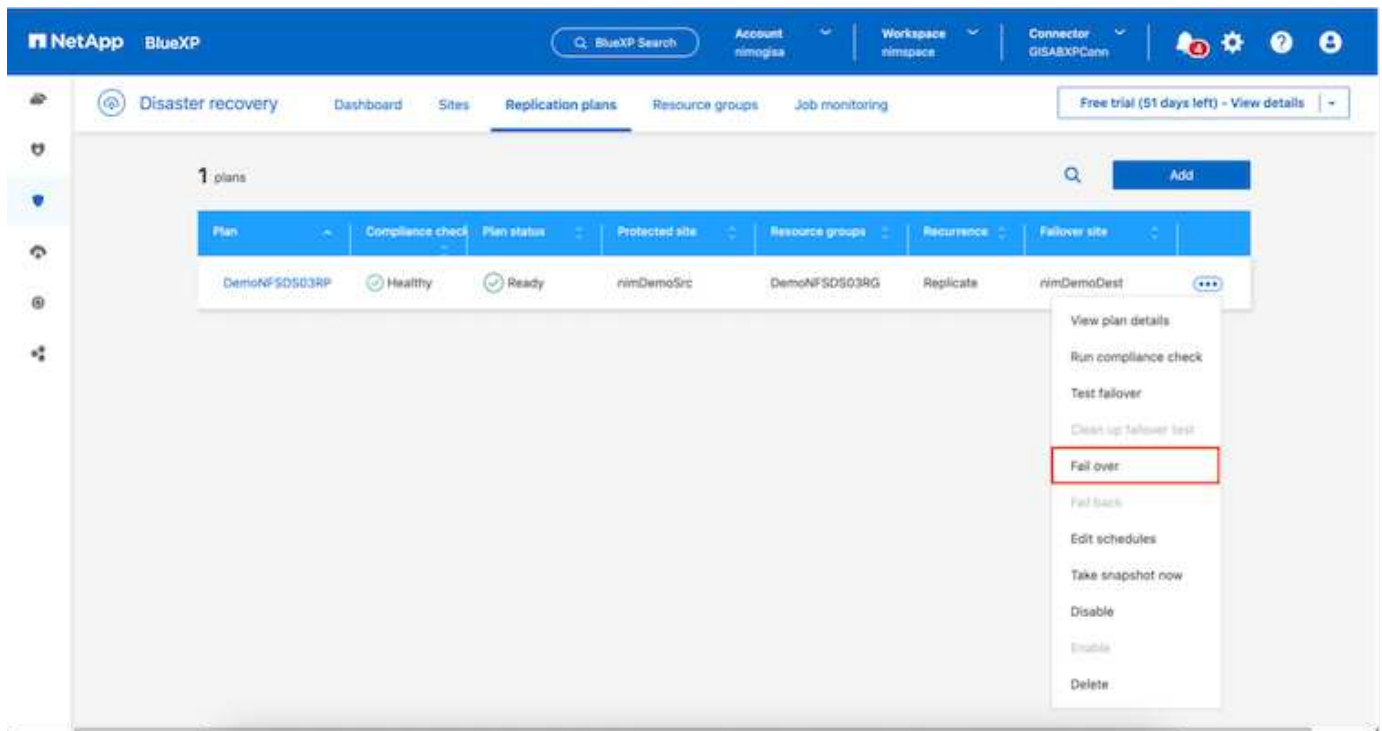
This action will reset the virtual machines (VMs) and the status of the replication plan to the ready state.

When the VMware administrator performs a recovery operation, BlueXP DRaaS 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.

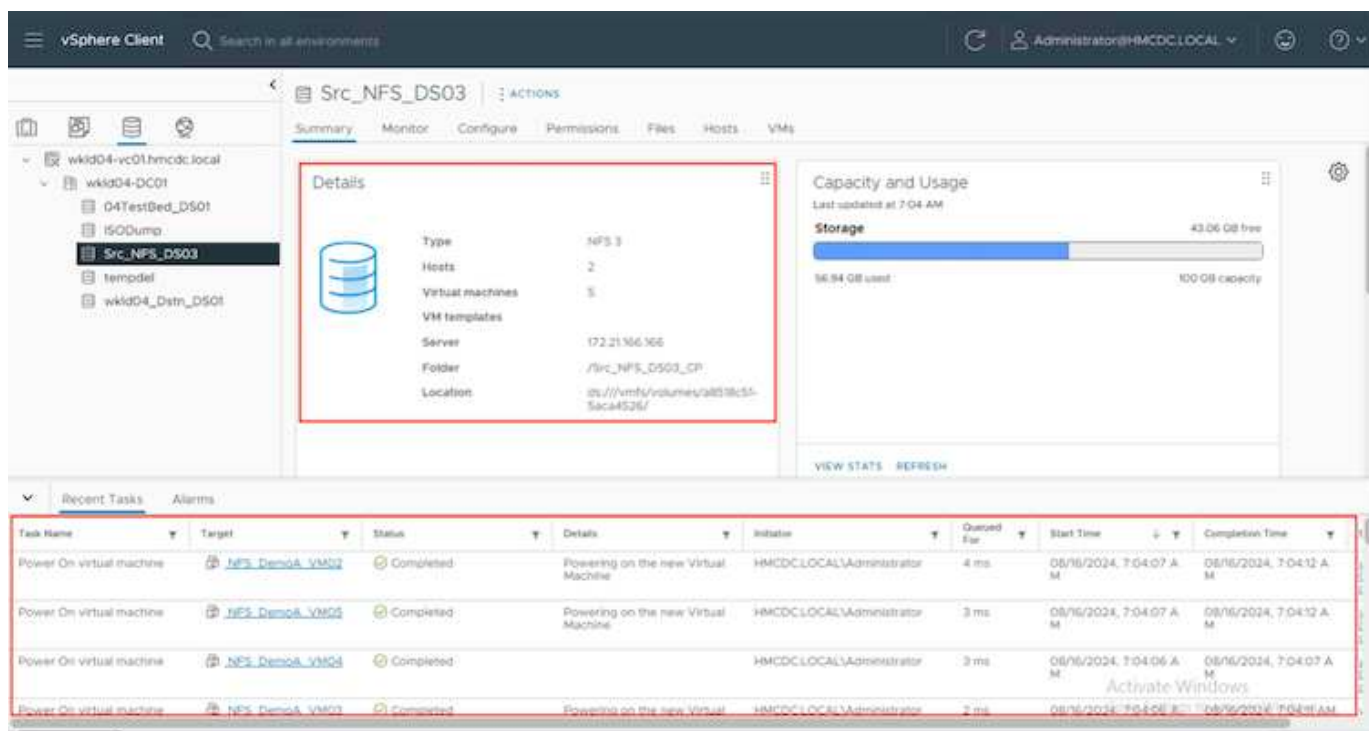
Planned Migration and Fail over

BlueXP DRaaS 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 an 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.



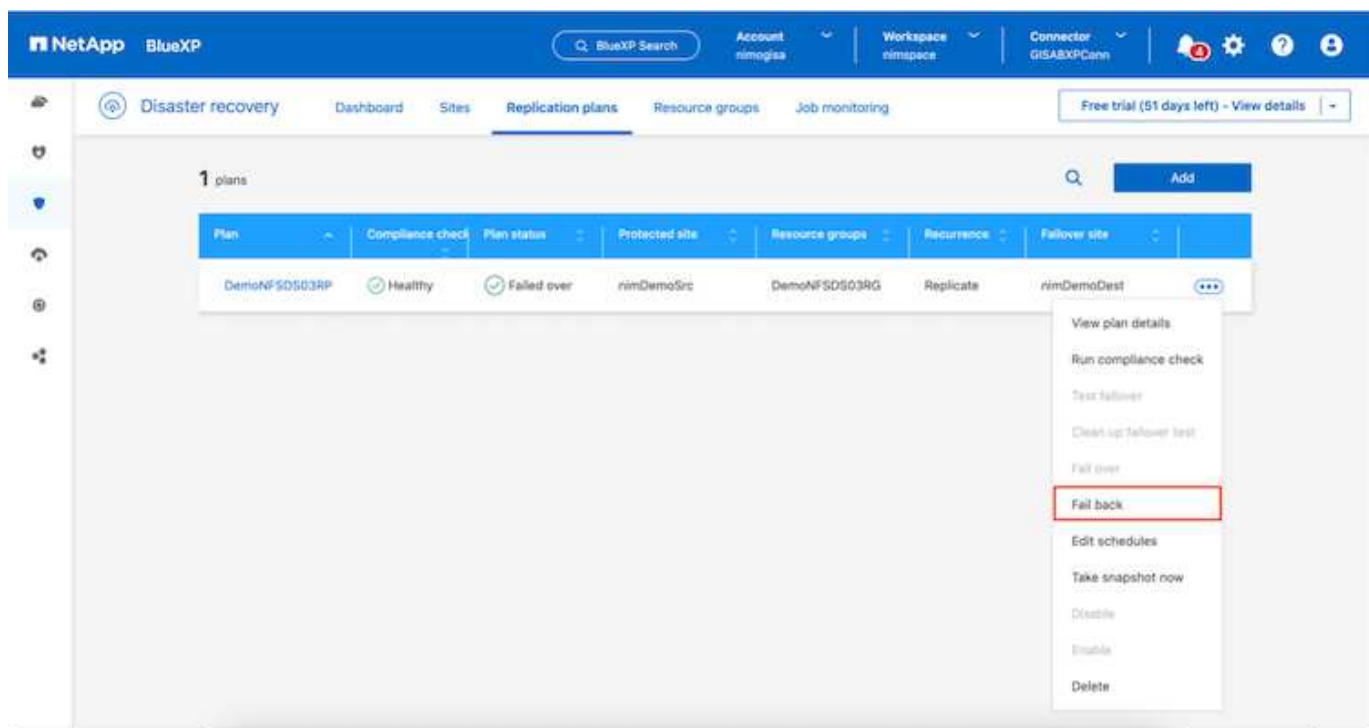
When the VMware administrator performs a failover operation, BlueXP DRaaS automates the following tasks:

- Break and fail over the NetApp SnapMirror relationships.
- Connect the replicated NFS 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.



Failback

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



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

NOTE: BlueXP DRaaS 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

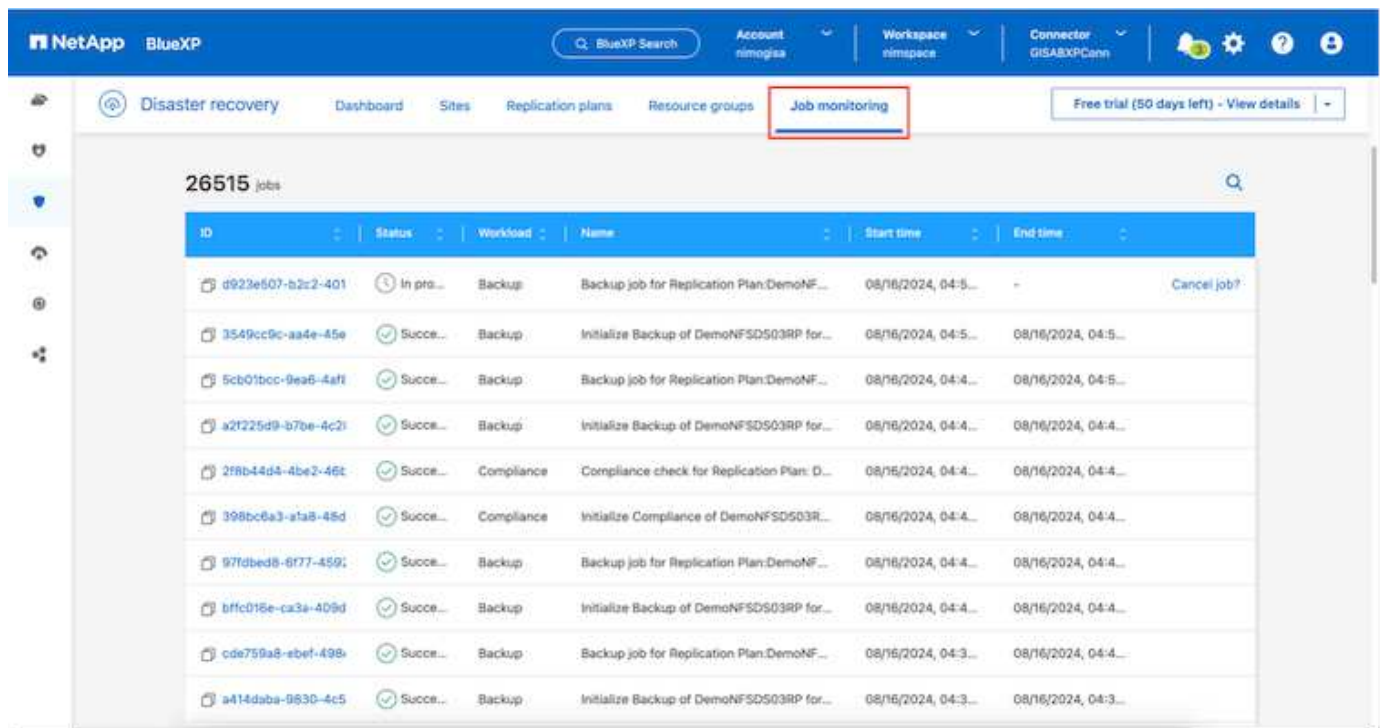
target and involves the following steps:

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

For more details about accessing and configuring BlueXP DRaaS, see the [Learn about BlueXP Disaster Recovery for VMware](#).

Monitoring and Dashboard

From BlueXP 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.

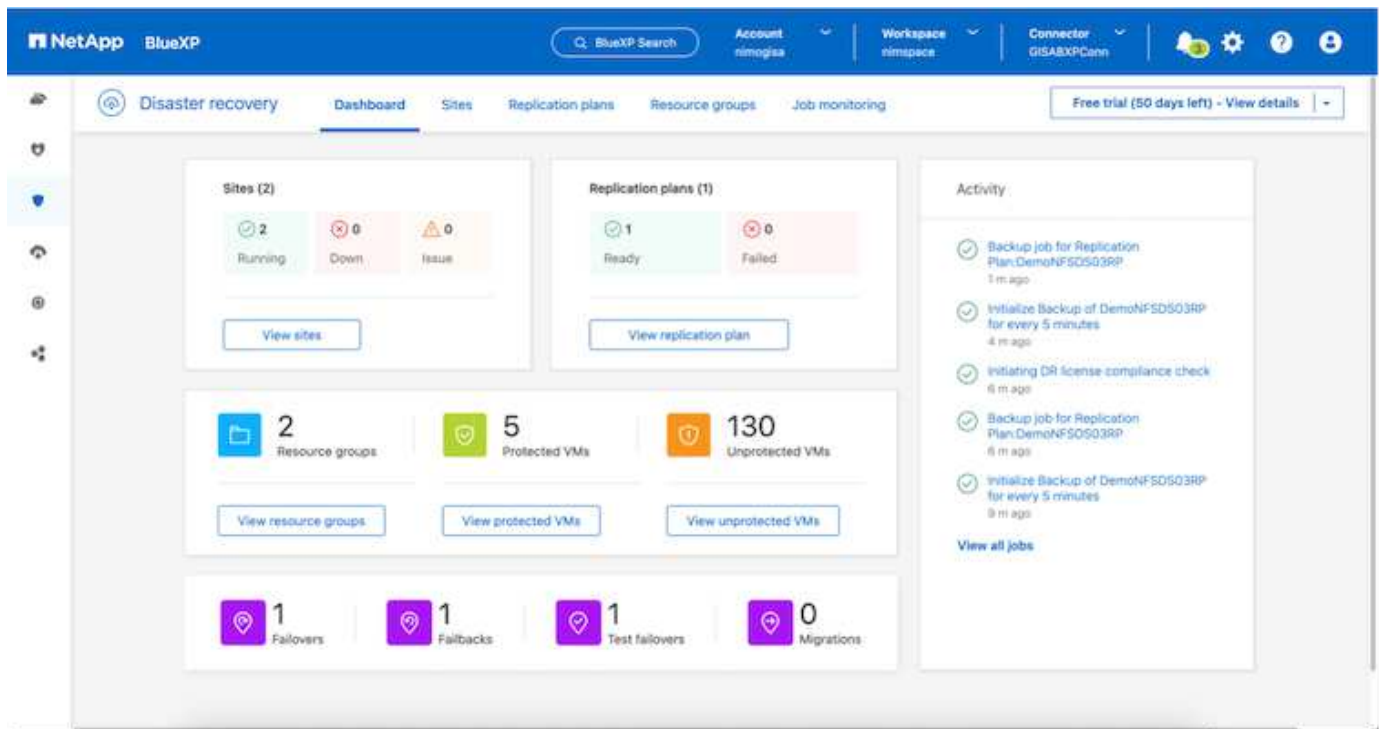


ID	Status	Workload	Name	Start time	End time	
d923e507-b2c2-401	In pro...	Backup	Backup job for Replication Plan:DemoNF...	08/16/2024, 04:5...	-	Cancel job?
3549cc9c-aa4e-45e	Succe...	Backup	Initialize Backup of DemoNFSDS03RP for...	08/16/2024, 04:5...	08/16/2024, 04:5...	
5cb01bcc-9ea6-4af1	Succe...	Backup	Backup job for Replication Plan:DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:5...	
a2f225d9-b7be-4c2f	Succe...	Backup	Initialize Backup of DemoNFSDS03RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...	
2f8b44d4-4be2-46f	Succe...	Compliance	Compliance check for Replication Plan: D...	08/16/2024, 04:4...	08/16/2024, 04:4...	
398bc6a3-ata8-48d	Succe...	Compliance	Initialize Compliance of DemoNFSDS03R...	08/16/2024, 04:4...	08/16/2024, 04:4...	
97fdbed8-6f77-459f	Succe...	Backup	Backup job for Replication Plan:DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:4...	
bffcd18e-ca3a-409d	Succe...	Backup	Initialize Backup of DemoNFSDS03RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...	
cde759a8-ebef-498	Succe...	Backup	Backup job for Replication Plan:DemoNF...	08/16/2024, 04:3...	08/16/2024, 04:4...	
a414daba-0630-4c5	Succe...	Backup	Initialize Backup of DemoNFSDS03RP for...	08/16/2024, 04:3...	08/16/2024, 04:3...	



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

With the BlueXP 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.



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.

To learn more about this process, feel free to follow the detailed walkthrough video or use the [solution simulator](#).

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.

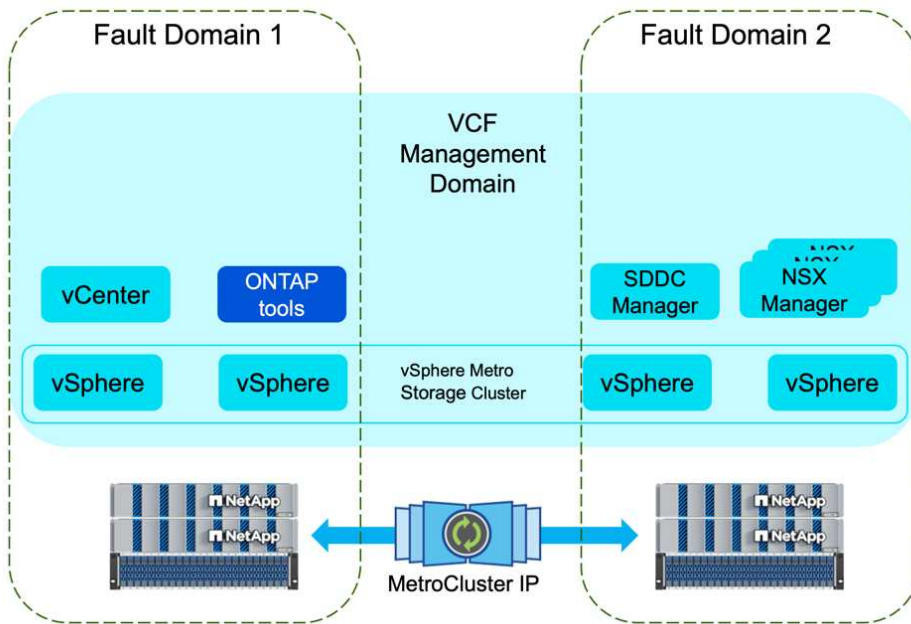
This combination ensures continuous data availability, seamless failover, and disaster recovery across geographically dispersed sites, enhancing resilience and operational continuity for critical workloads. SnapMirror active sync, enables business services to continue operating even through a complete 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.

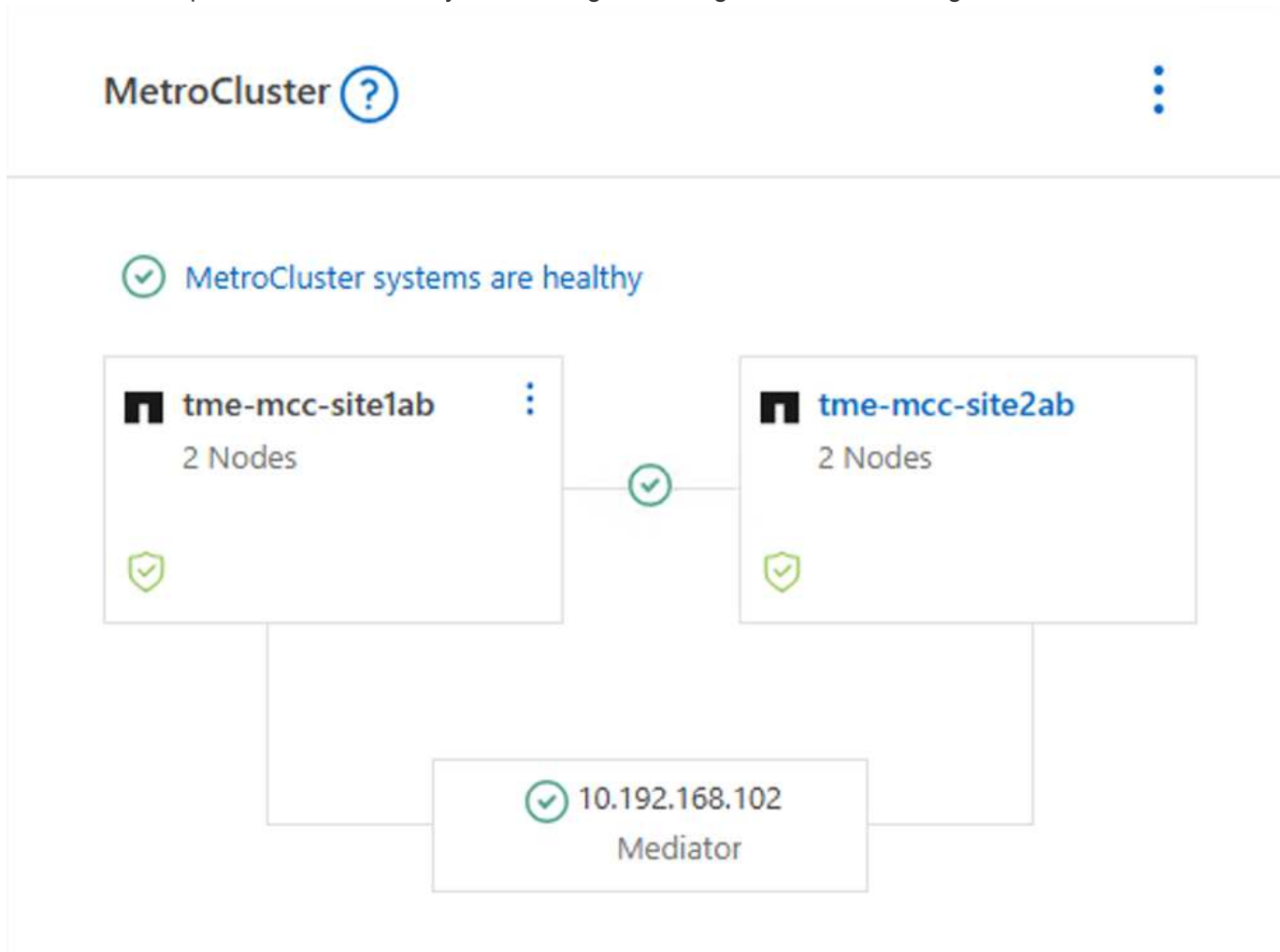
Prerequisites

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.

Network interfaces

Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node	↑
<input type="text"/>		<input type="text"/> ch-svm	<input type="text"/>	<input type="text"/>	<input type="text"/>	
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	

Network interfaces

Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node	↑
<input type="text"/>		<input type="text"/> ch-svm	<input type="text"/>	<input type="text"/>	<input type="text"/>	
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

Storage VMs

+ Add

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

Storage VMs

+ Add

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 Vmknfc 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 Vmknix 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.

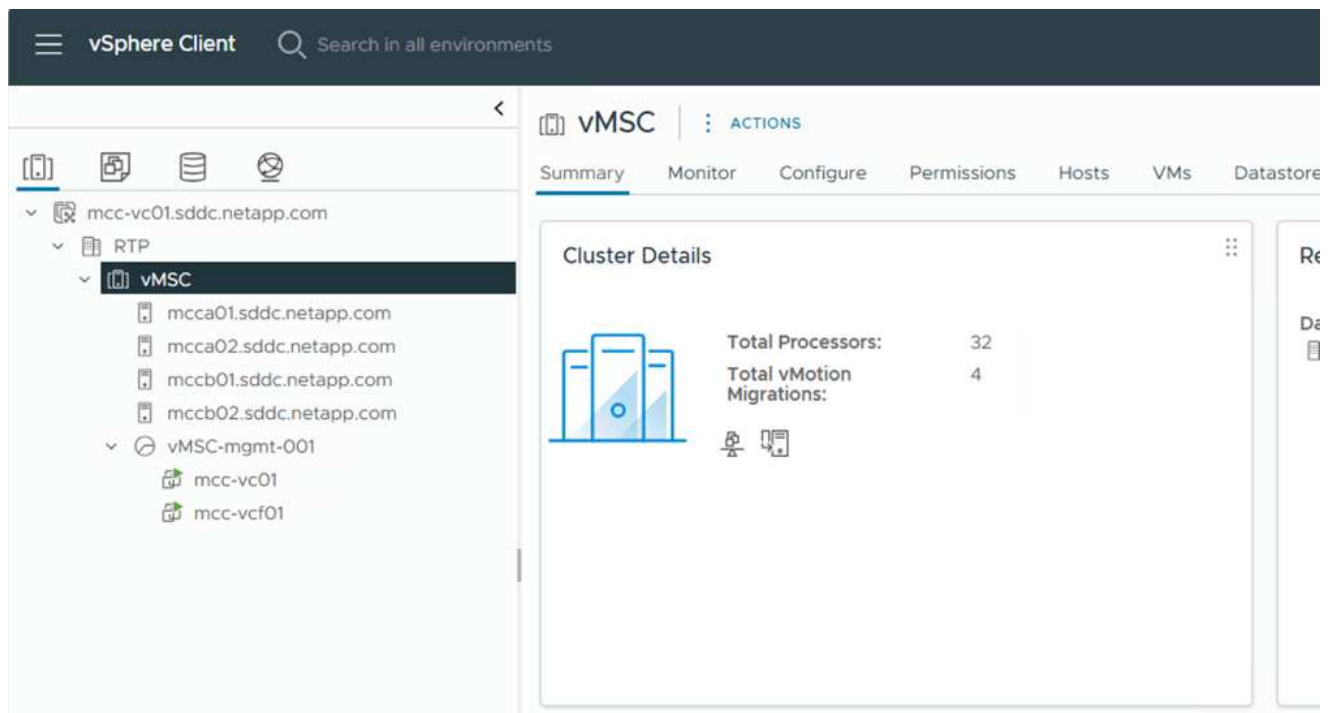
1. Follow the steps at [Run a Pre-check on the Target vCenter Before Conversion](#) to run the validation.
2. The following output shows that the vCenter appliance has passed the pre-check.

```
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] vReal 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] EIP ping 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.



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.

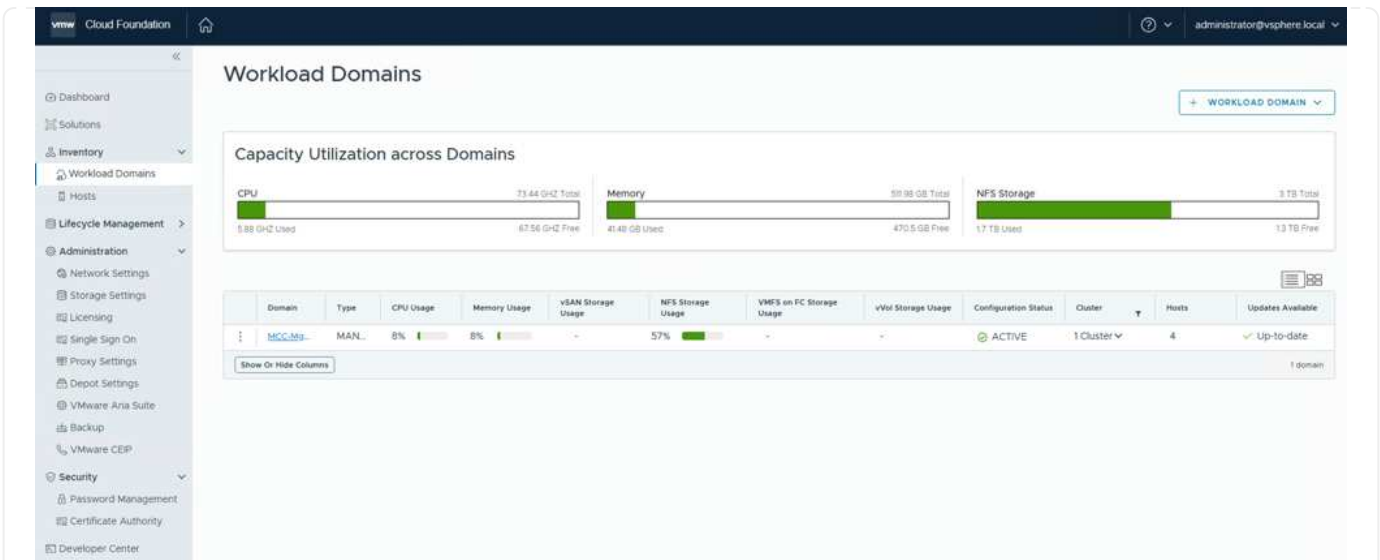
```
[2025-03-24 19:29:00,394] [INFO] vcenter_connection: Connecting to mcc-vc01.sddc.netapp.com as administrator@vsphere.local
[2025-03-24 19:29:00,583] [INFO] discover_domain: =====
[2025-03-24 19:29:00,583] [INFO] discover_domain: Starting inventory payload generation for vCenter: mcc-vc01.sddc.netapp.com, 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](#).

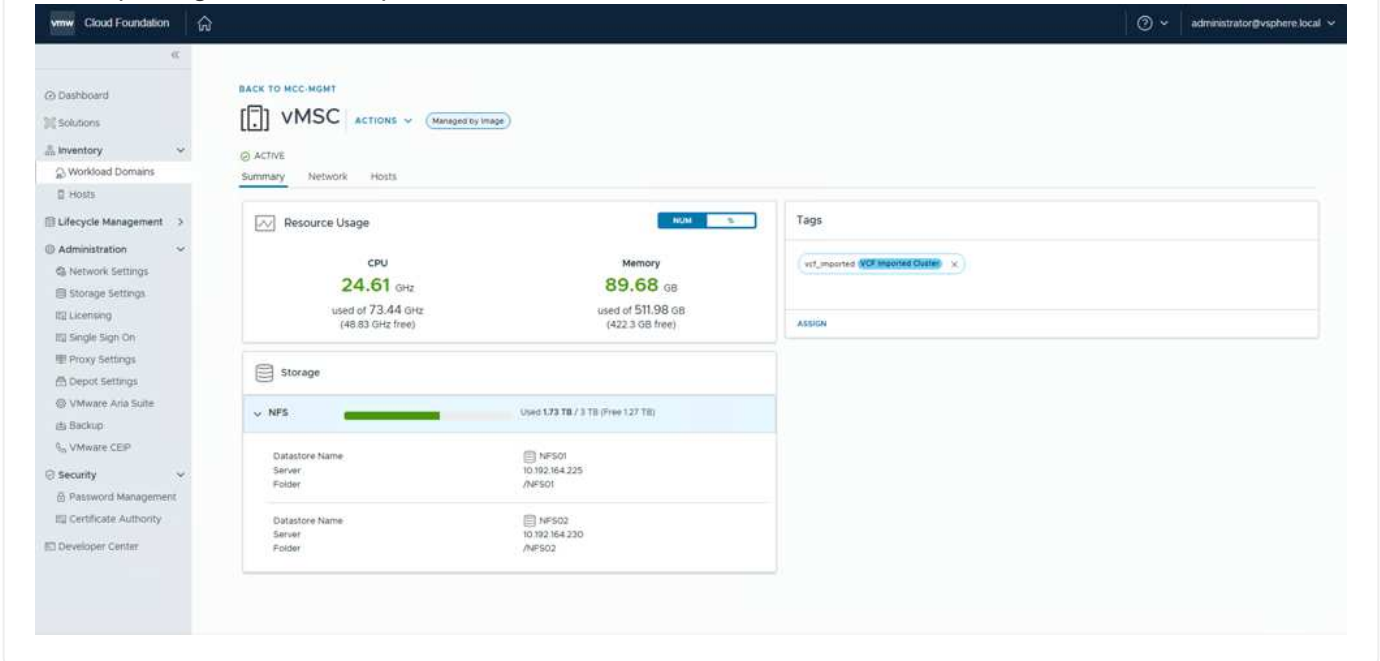
NSX VMs will be deployed to vCenter.

The screenshot shows the vSphere Client interface. On the left, the navigation pane displays the hierarchy: **mcc-vc01.sddc.netapp.com** > **RTP** > **vMSC**. Under **vMSC**, several hosts are listed, including **mcca01.sddc.netapp.com**, **mcca02.sddc.netapp.com**, **mccb01.sddc.netapp.com**, **mccb02.sddc.netapp.com**, and **vMSC-mgmt-001**. The main pane shows the **vMSC** cluster details. The **Summary** tab is selected, displaying a bar chart and the following statistics: **Total Processors: 32** and **Total vMotion Migrations: 5**. Other tabs like **Monitor**, **Configure**, **Permissions**, **Hosts**, **VMs**, and **Datastores** are visible at the top of the main pane.

SDDC Manager shows the Management domain created with the name that was provided and NFS as Datastore.



On Inspecting the cluster, it provides the information of NFS Datastore.



Add licensing to VCF

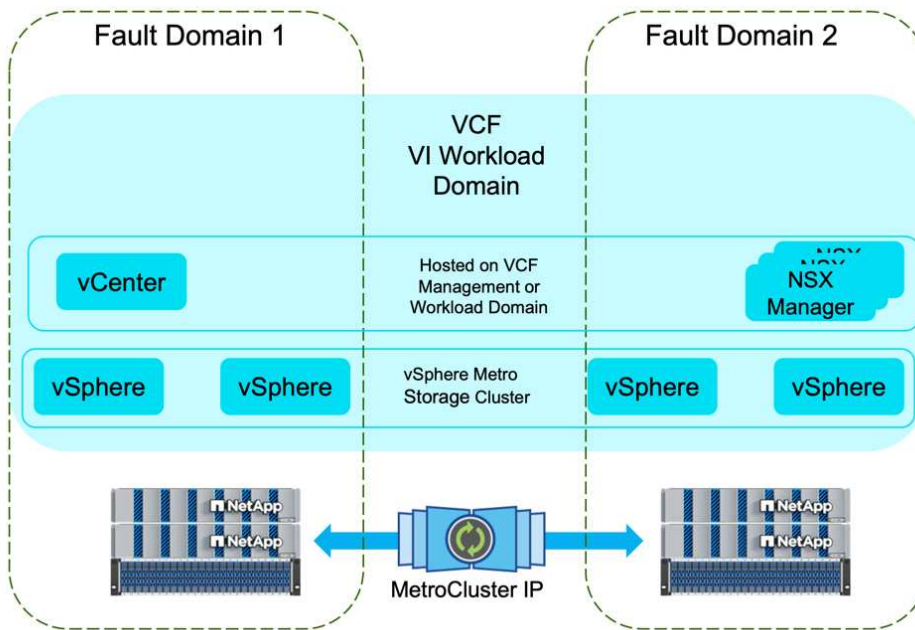
After completing the conversion, licensing must be added to the environment.

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 Stretched 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:

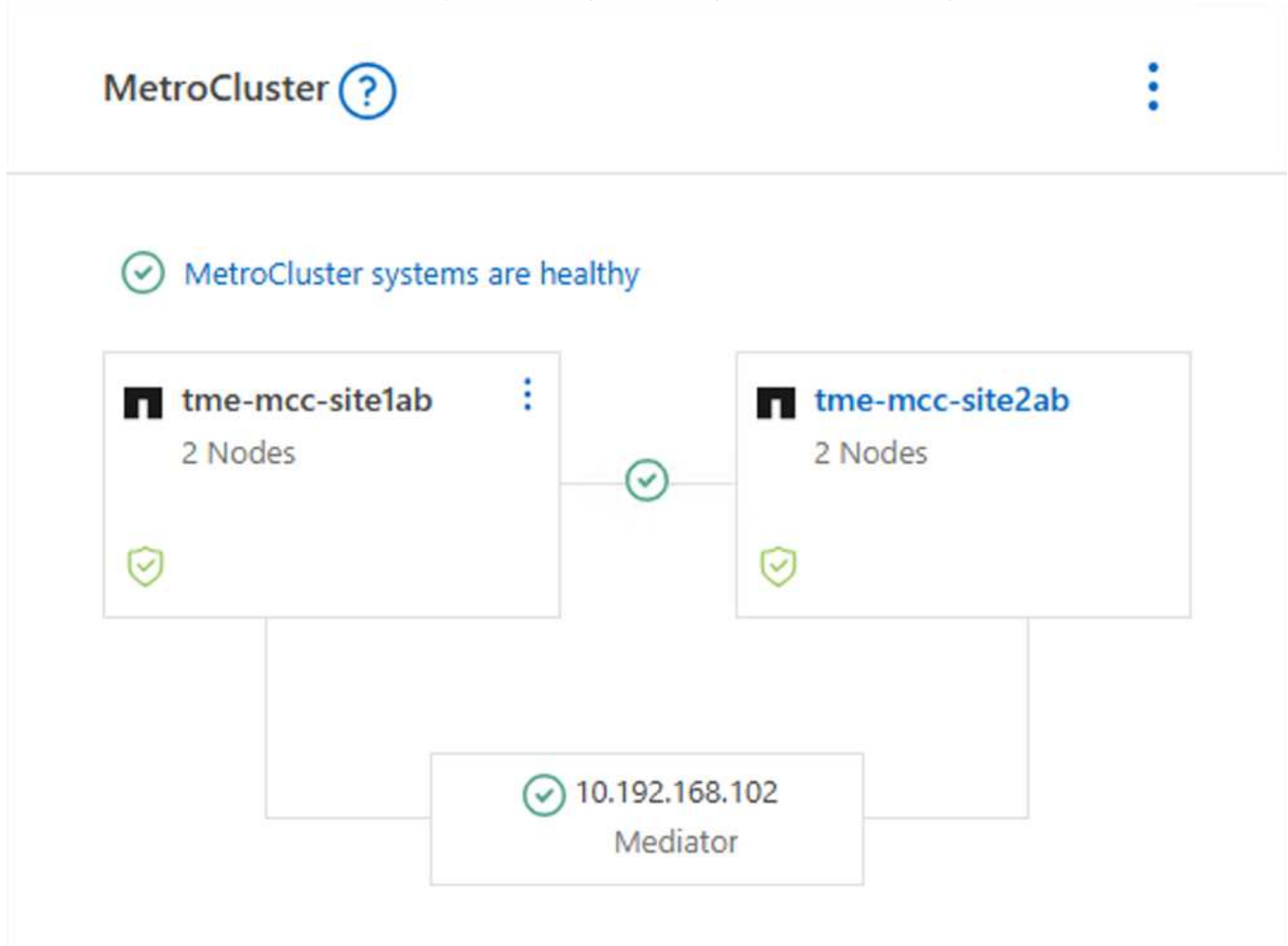
- Deploy vSphere hosts and vCenter server.
- Provision NFS datastore to vSphere hosts.
- Use the VCF Import Tool to validate the vSphere cluster.
- Configure a JSON file for create an NSX during the VCF conversion.
- Use the VCF Import Tool to import the vSphere 8 environment as VCF VI Workload domain 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.



and here is the SVM Network interfaces from both fault domains.

Network interfaces

Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node	↑
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	

Network interfaces

Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node	↑
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

Storage VMs

+ Add

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

Storage VMs

+ Add

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

☐ Add as a cache for a remote volume (FlexCache)
Simplifies file distribution, reduces WAN latency, and lowers WAN bandwidth costs.

Storage and optimization

Capacity

Performance service level

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

Optimization options

☐ Distribute volume data across the cluster (FlexGroup) [?](#)

Access permissions

☒ Export via NFS

GRANT ACCESS TO HOST

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/vaa1-nasd start
ESX VAAI-NAS Daemon started.
```

and vStorage is enabled on the SVM that hosts the volume.


```
tme-mcc-site1ab::~*> vservers nfs modify -vservers 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	Vmknick	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.

The screenshot shows the vSphere Client interface. On the left, the inventory tree shows a vCenter named 'mcc-vc02.sddc.netapp.com' with a single host 'siteb-vs02.sddc.netapp.com' selected. The right pane shows the 'Host Details' for this host, including the Hypervisor (VMware ESXi, 8.0.3, 24280767), Model, Processor Type (Intel(R) Xeon(R) Gold 5120 C PU @ 2.20GHz), Logical Processors (12), NICs (2), Virtual Machines (1), State (Connected), and 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@mc-vcf01: ~$ cd vcf-brownfield-import-5.2.1.2-24404579/vcf-brownfield-toolset/
vcf@mc-vcf01: ~$ ./vcf-brownfield-import-5.2.1.2-24404579/vcf-brownfield-toolset $ python3 vcf_brownfield.py check
[2025-03-23 17:40:44.979] [INFO] vcf_brownfield: brownfield import main version: 5.2.1.2-24404579
[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@mc-vcf01: ~$ ./vcf-brownfield-import-5.2.1.2-24404579/vcf-brownfield-toolset $ python3 vcf_brownfield.py check --vcenter mcc-vc02.sddc.netapp.com --sso-user administrator@vsphere.local --sso-password '*****' --local-admin-password '*****' --accept-trust
[2025-03-23 17:41:46.491] [INFO] vcf_brownfield: brownfield import main version: 5.2.1.2-24404579
[2025-03-23 17:41:46.492] [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:B7:7D:15:85:68:38:A1:F0:27:20:58:6D:85:FA:D5:D2:AE:3C:46
[2025-03-23 17:41:48.419] [WARN] 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: 9c4a9d66a8cc841d51adace988b7f85ca9b7f 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: 9c4a9d66a8cc841d51adace988b7f85ca9b7f with thumbprint: DA:6F:94:90:D9:E3:E6:66:E7:CD:60:49:1C:9B:3E:03:EA:AB:57:ED:0B:1C:03:5C:3A:B5:4C:4C:60:40:F4:FF
[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:B7:7D:15:85:68:38:A1:F0:27:28:56:6D:85:FA:D5:D2: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 17:41:52.074] [INFO] request_helper: Response status from certificates import: 200
[2025-03-23 17:41:53.180] [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.

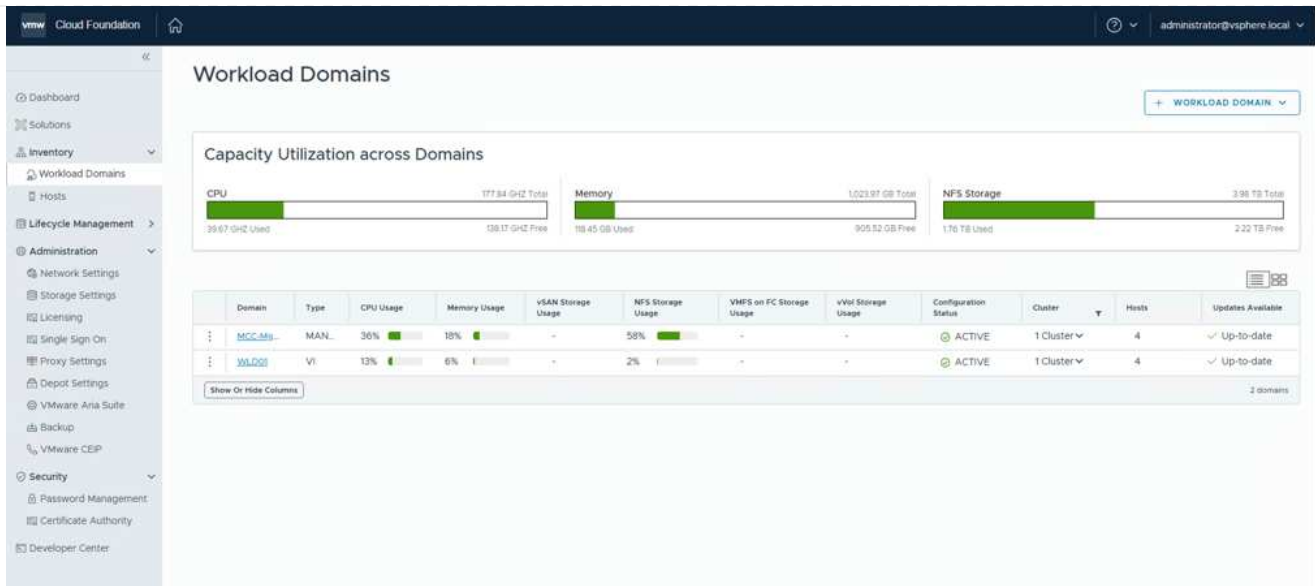
For complete instructions, refer to [VCF Convert Procedure](#).

NSX VMs will be deployed to vCenter.

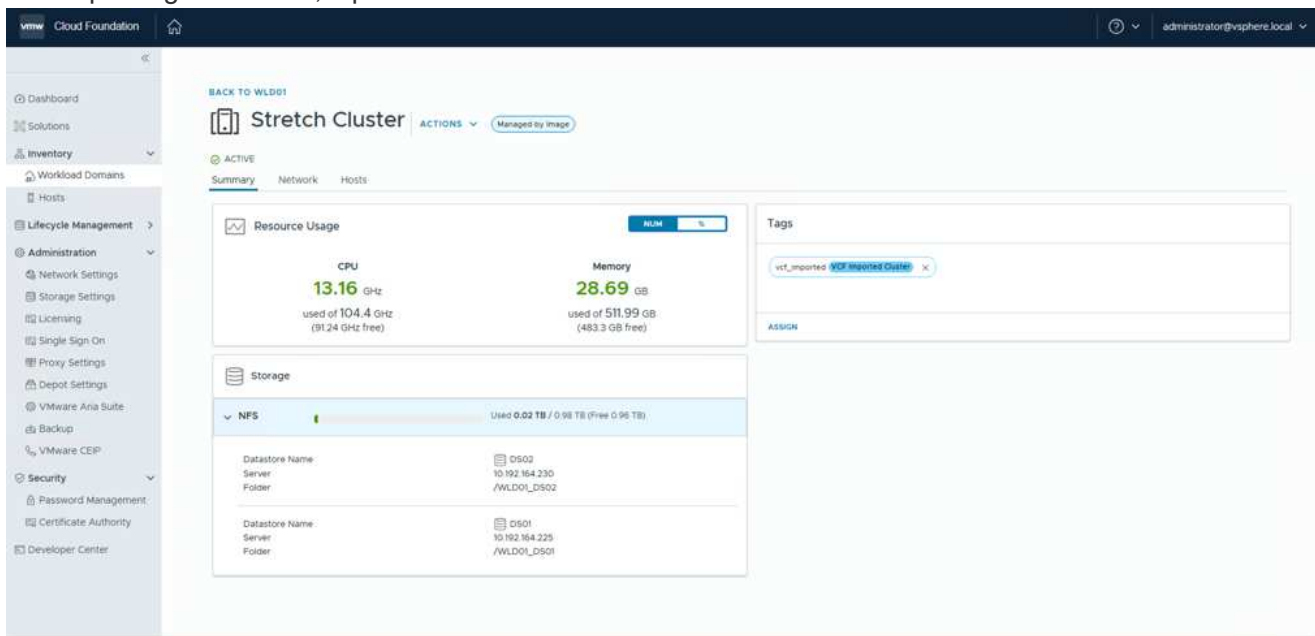
The screenshot displays the vSphere Client interface. At the top, there is a dark header with the 'vSphere Client' logo and a search bar. Below this, the main content area is divided into a left sidebar and a right pane. The left sidebar shows a tree view of the environment, with 'siteb-vs02.sddc.netapp.com' selected under the 'RTP' folder. The right pane shows the 'Host Details' for the selected host, including information about the Hypervisor, Model, Processor Type, Logical Processors, NICs, Virtual Machines, State, and Uptime.

Host Details	
Hypervisor:	VMware ESXi, 8.0.3, 242807 67
Model:	
Processor Type:	Intel(R) Xeon(R) Gold 5120 C PU @ 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.



On Inspecting the cluster, it provides the information of NFS Datastores.



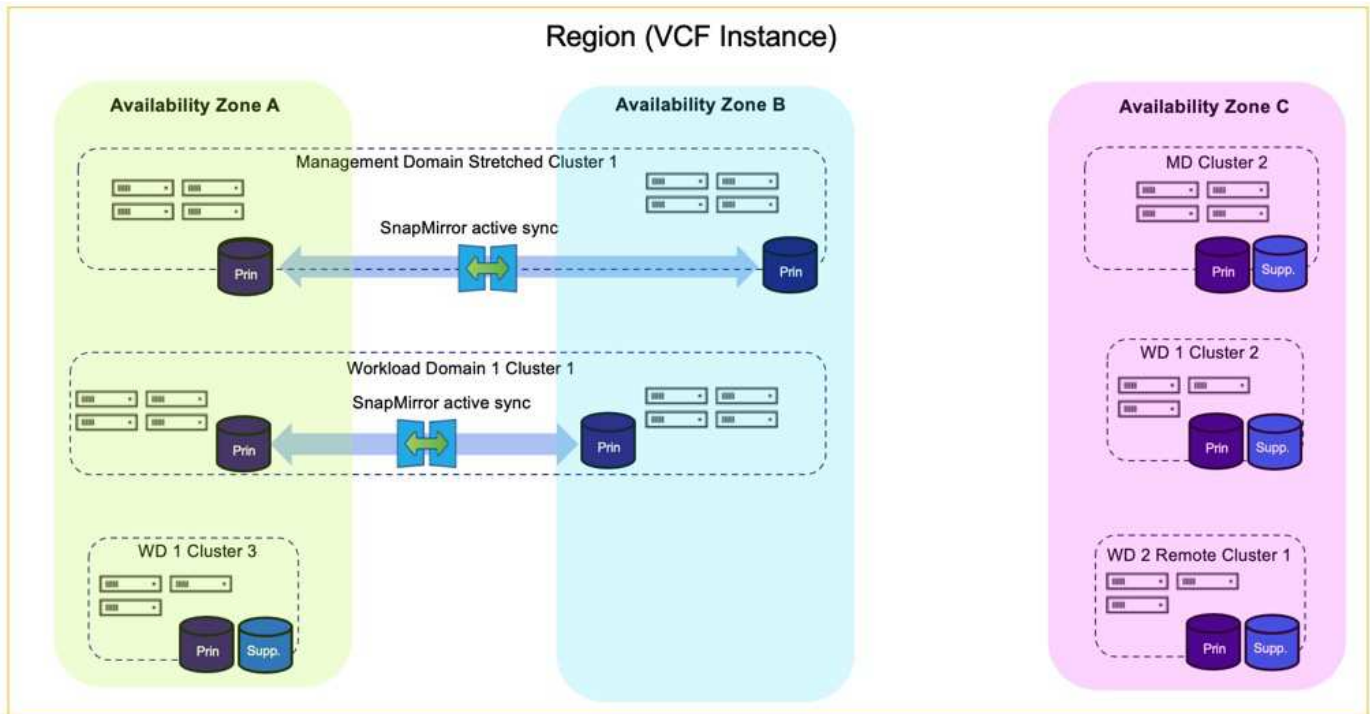
Add licensing to VCF

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.

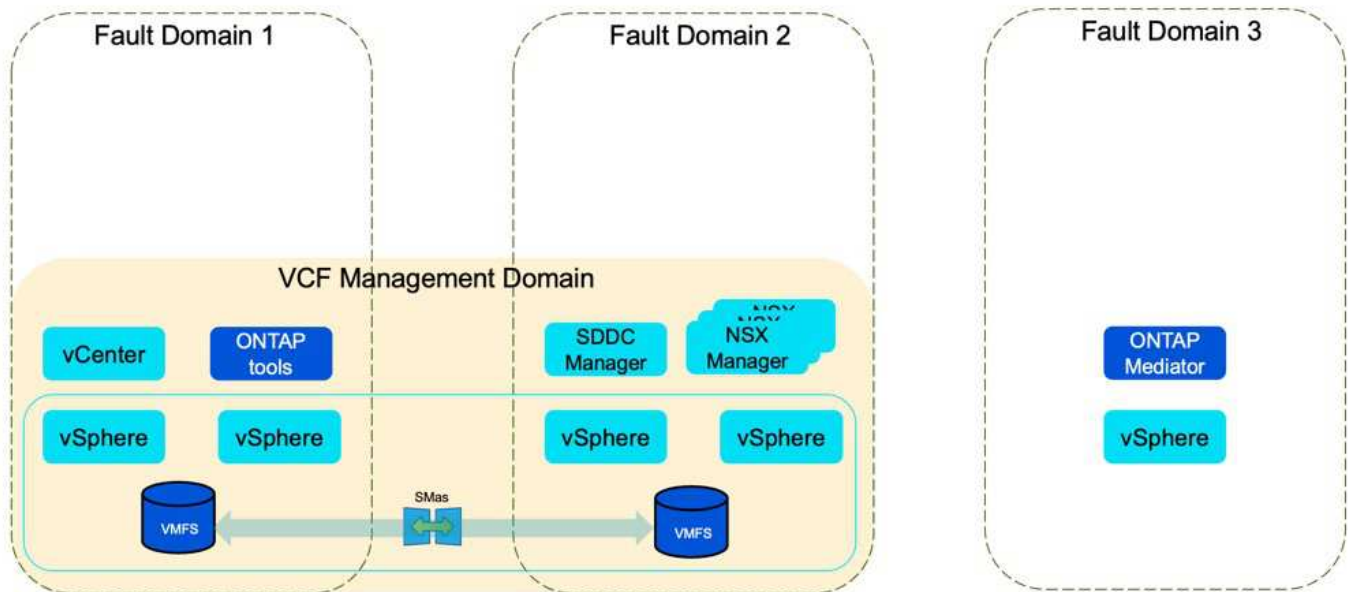


Scenario Overview

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.

VMFS with FC



Principal storage on Management Domain

With VCF 5.2 onwards management 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 shrunk, 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.

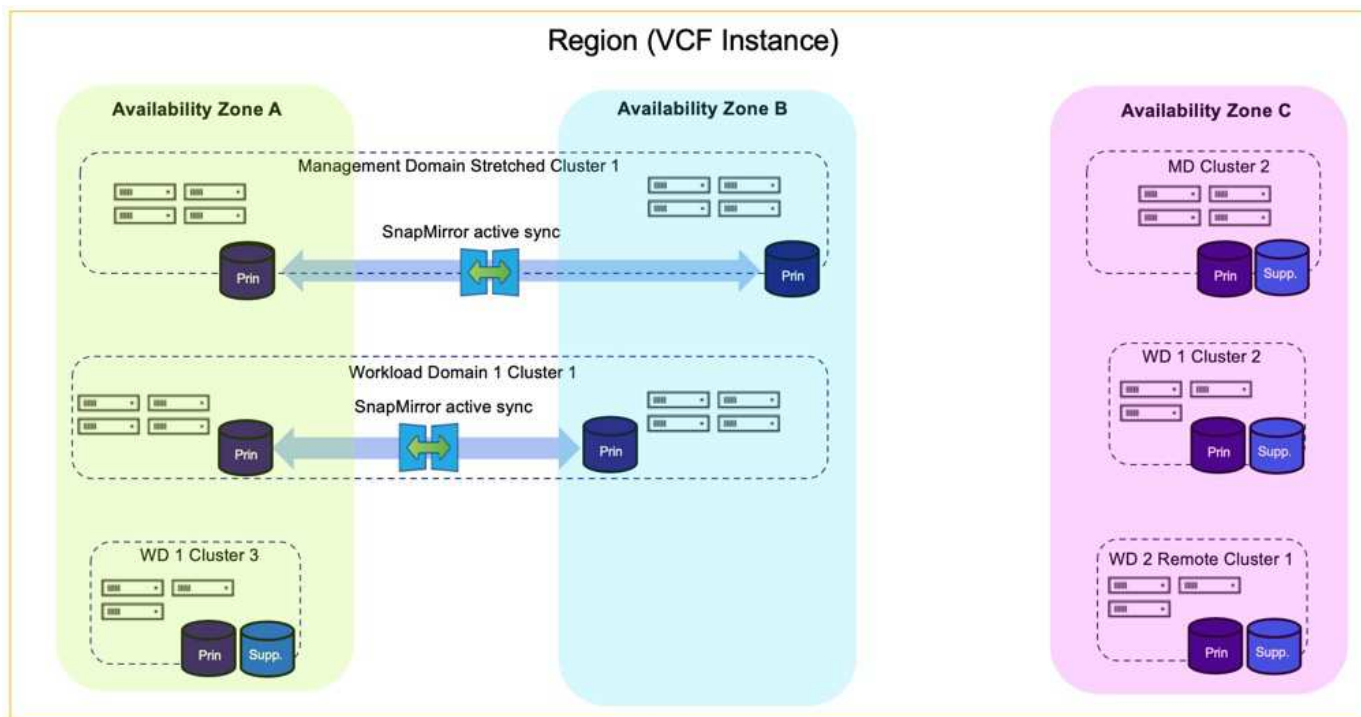
For information on configuring VCF refer to [VMware Cloud Foundation 5.2 Documentation](#).

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.



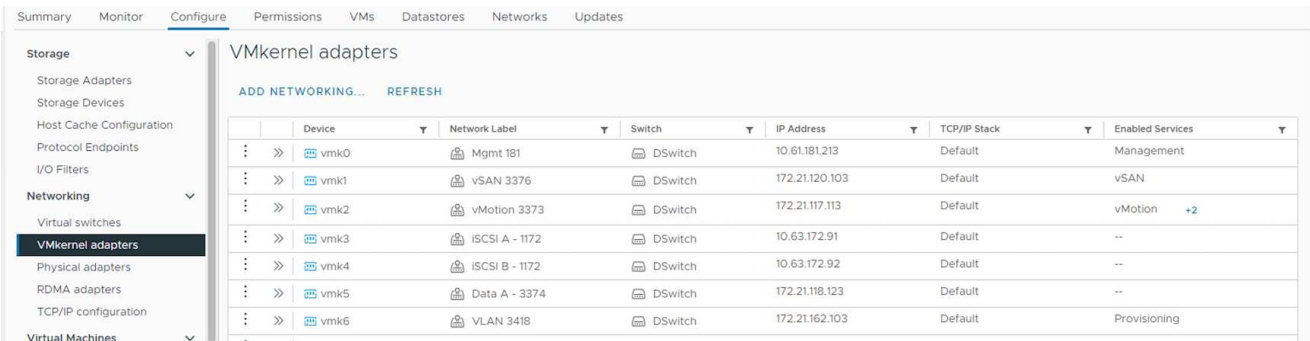
Some VMs which are deployed with external management tool like Aria Automation, Tanzu (or other Kubernetes flavors) are usually depends on VM storage policy. If migrating between the datastores within same VM storage policy, it should be of less impact for the applications. Check with Application owners to properly migrate those VMs to new datastore. vSphere 8 introduced [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.

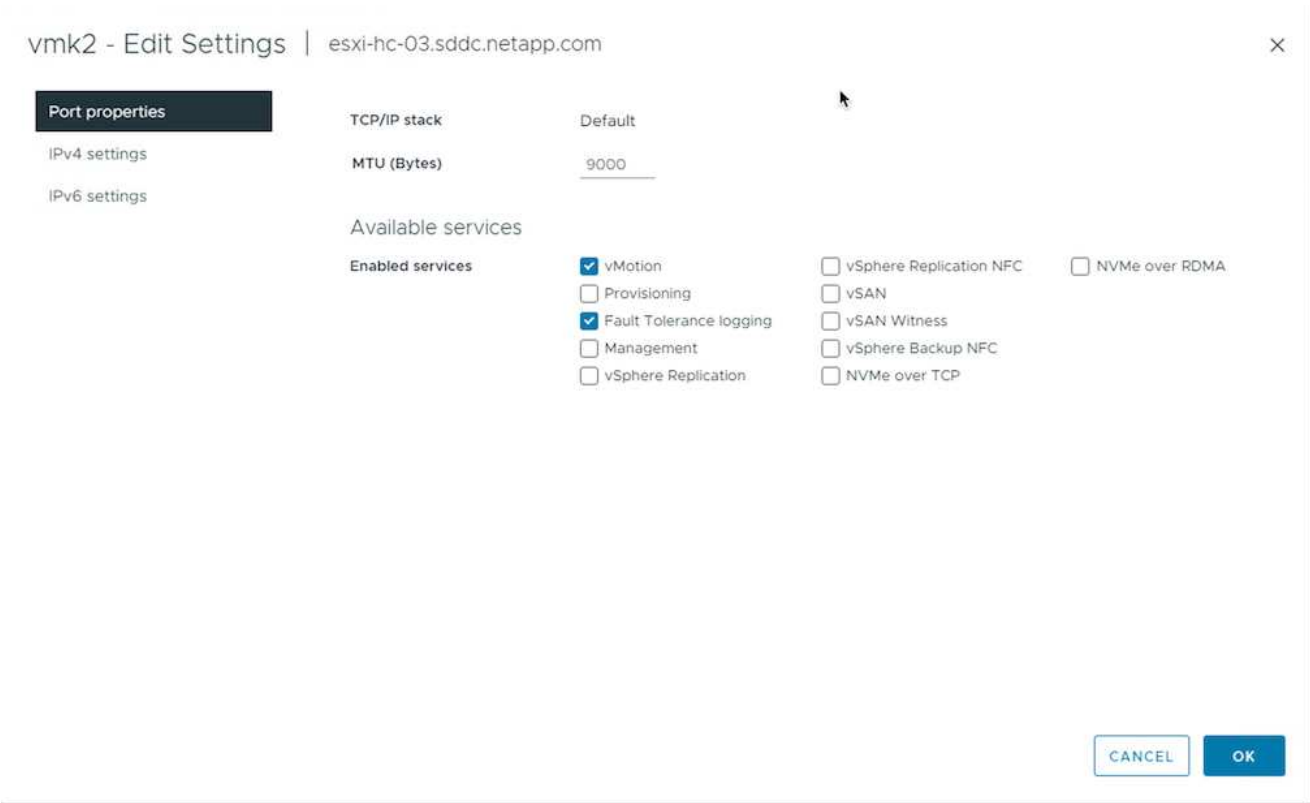
Migration of VMs across the vSphere hosts are also handled by the VMKernel interface of the vSphere host. For hot migration (powered on VMs), VMKernel interface with vMotion enabled service is used and for cold migration (powered off VMs), VMKernel interface with Provisioning service enabled is consumed 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.



The screenshot shows the 'Configure' tab in the vSphere Client. On the left, the 'Networking' section is expanded, and 'VMkernel adapters' is selected. The main area displays a table of VMkernel adapters. The table has columns for Device, Network Label, Switch, IP Address, TCP/IP Stack, and Enabled Services. There are 7 rows of adapters, each with a 'vmk' prefix in the device name. The 'Enabled Services' column shows 'Management' for vmk0, 'vSAN' for vmk1, 'vMotion' for vmk2, and 'Provisioning' for vmk6. vmk3, vmk4, and vmk5 have no services enabled.

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
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.



The screenshot shows the 'vmk2 - Edit Settings' dialog box. The 'Port properties' tab is selected. The 'TCP/IP stack' is set to 'Default' and the 'MTU (Bytes)' is 9000. Under 'Available services', there are two columns of checkboxes. The first column has 'vMotion' checked, 'Provisioning' unchecked, 'Fault Tolerance logging' checked, 'Management' unchecked, and 'vSphere Replication' unchecked. The second column has 'vSphere Replication NFC' unchecked, 'vSAN' unchecked, 'vSAN Witness' unchecked, 'vSphere Backup NFC' unchecked, and 'NVMe over TCP' unchecked. The third column has 'NVMe over RDMA' unchecked. At the bottom right, there are 'CANCEL' and 'OK' buttons.

vmk2 - Edit Settings | esxi-hc-03.sddc.netapp.com

Port properties

IPv4 settings

IPv6 settings

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

CANCEL

OK

 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.

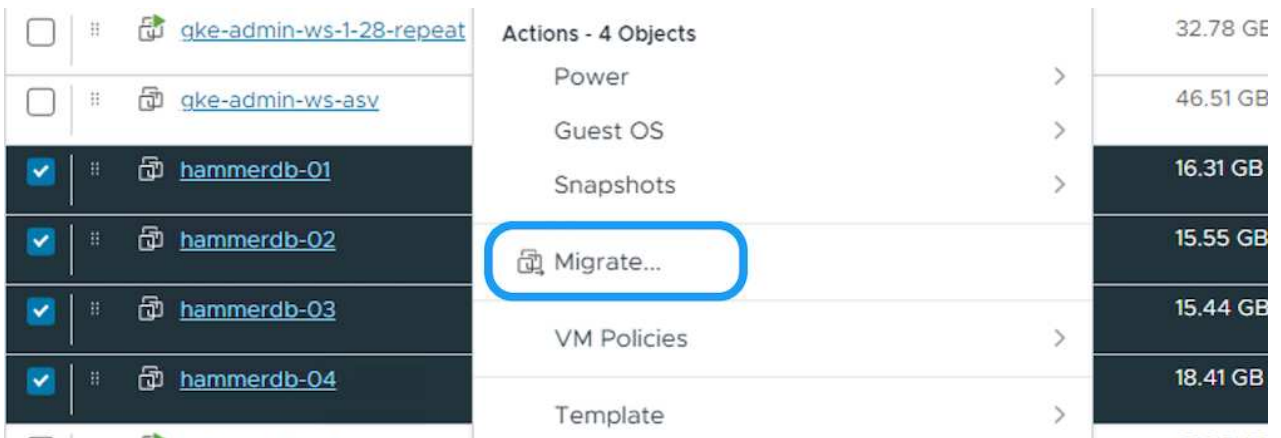
Migration of VMs from specific vSphere Datastore

Follow the procedure below to migrate VMs to new Datastore using UI.

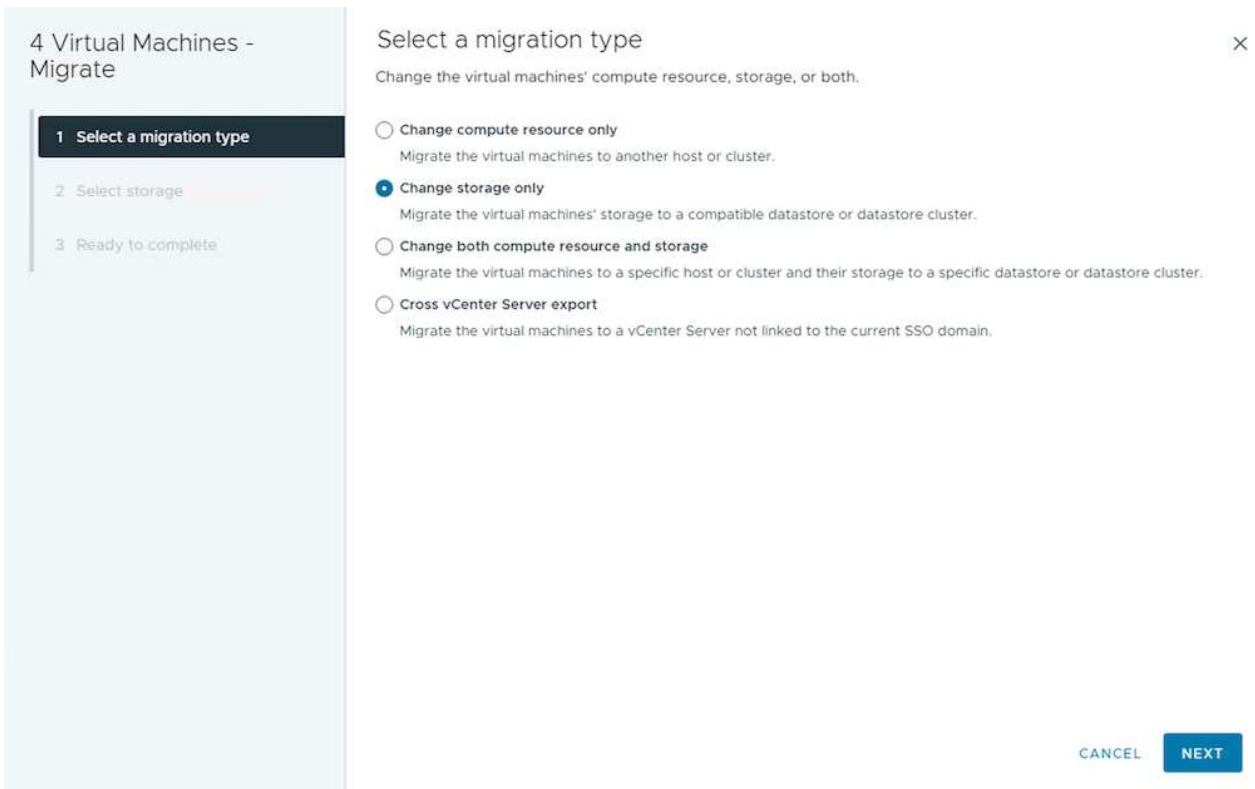
1. With vSphere Web Client, select the Datastore from the storage inventory and click on VMs tab.



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



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	
ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB	
DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB	
destination	Incompatible	250 GB	31.8 MB	249.97 GB	
DRaaSTest	Incompatible	1 TB	201.13 GB	880.86 GB	
E13A400_JCSI	Incompatible	2 TB	858.66 GB	1.85 TB	

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 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

```

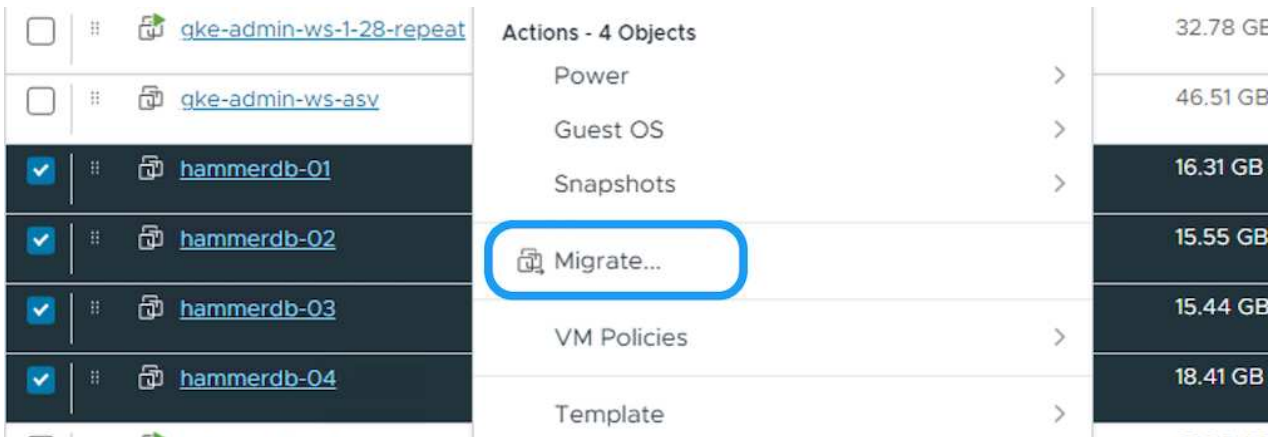

Migration of VMs in same vSphere cluster

Follow the procedure below to migrate VMs to new Datastore using UI.

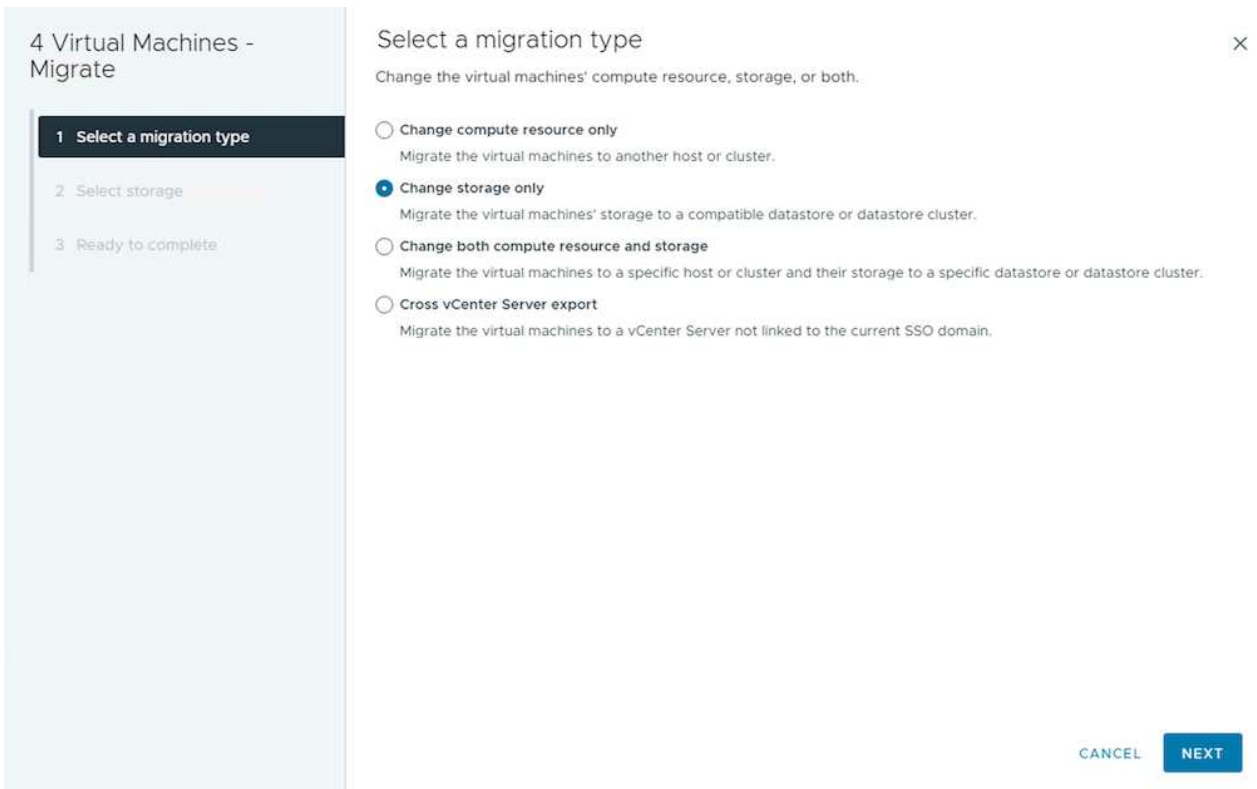
1. With vSphere Web Client, select the Cluster from the Host and Cluster inventory and click on VMs tab.



2. Select the VMs that need to be migrated and right-click to select the Migrate option.



3. Choose option to change storage only, Click Next



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	
<input checked="" type="radio"/>	ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB	
<input type="radio"/>	DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB	
<input type="radio"/>	destination	Incompatible	250 GB	31.8 MB	249.97 GB	
<input type="radio"/>	DRaaSTest	Incompatible	1 TB	201.13 GB	880.86 GB	
<input type="radio"/>	E13A400_JCSI	Incompatible	2 TB	858.66 GB	1.85 TB	

Manage Columns

Items per page

5

1 - 5 of 14 items

<

>

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



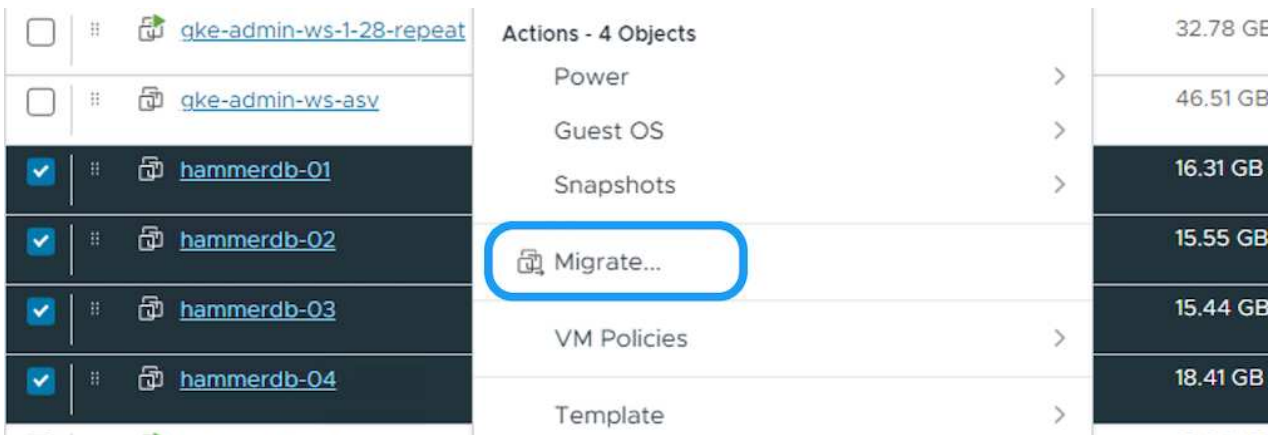
Refer [CPU Compatibility](#) and [vSphere Enhanced vMotion Compatibility](#) when source and target hosts are of different CPU family or model.

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.

CANCEL

NEXT

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.

CANCEL

BACK

NEXT

5. Select the desired VM Storage Policy and pick the datastore that is compatible. Click Next.

4 Virtual Machines - Migrate

- Select a migration type
- Select a compute resource
- Select storage**
- Select folder
- Select networks
- Select vMotion priority
- 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	
<input checked="" type="radio"/>	VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB	
<input type="radio"/>	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB	
<input type="radio"/>	VCF_WKLD_03_ISCSI	Incompatible	3 TB	858.61 GB	2.85 TB	
<input type="radio"/>	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	
<input type="radio"/>	vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	
<input type="radio"/>	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

- Select a migration type
- Select a compute resource
- Select storage
- Select folder**
- Select networks
- Select vMotion priority
- 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

- Select a migration type
- Select a compute resource
- Select storage
- Select folder
- Select networks**
- Select vMotion priority
- Ready to complete

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

ADVANCED >>

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

8. Review and click on Finish.

4 Virtual Machines - Migrate

- Select a migration type
- Select storage
- 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 vc.sa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to another cluster and Datastore specified by Policy
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy)


#When Portgroup is specific to each cluster, replace the above command
with
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy) -PortGroup
(Get-VirtualPortGroup 'VLAN 101')

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration

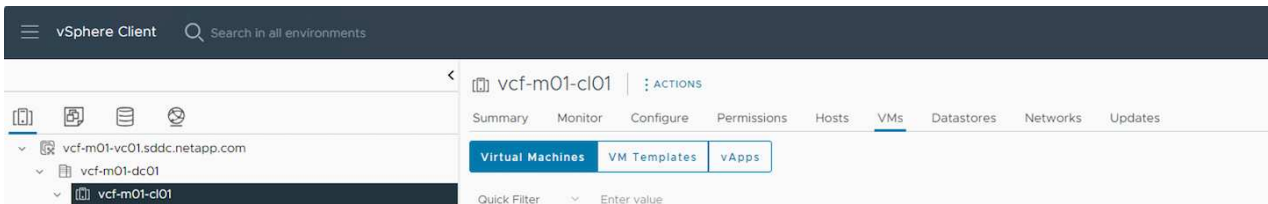
```


Migration of VMs across vCenter servers in same SSO domain

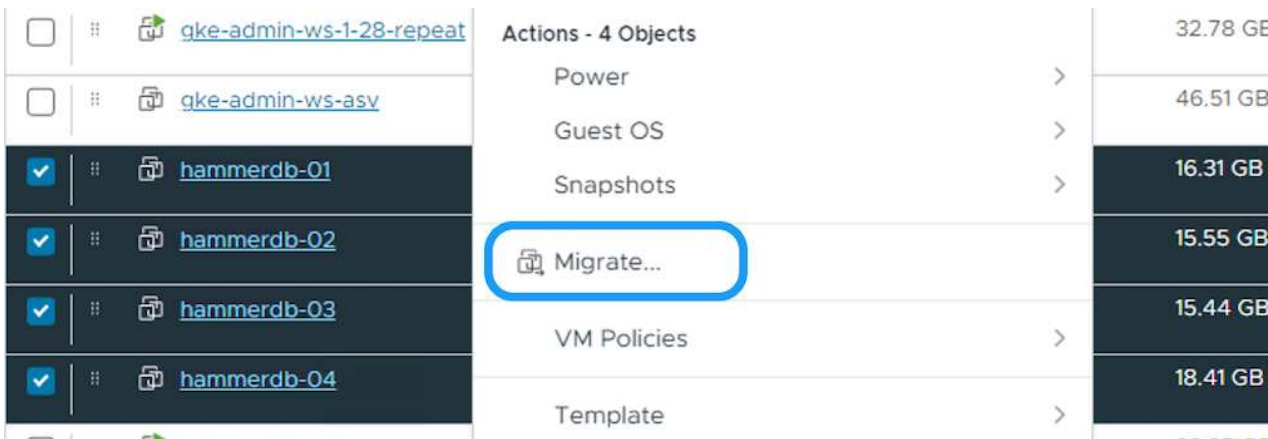
Follow the procedure below to migrate VMs to new vCenter server which is listed on same vSphere Client UI.

 For additional requirements like source and target vCenter versions,etc., check [vSphere documentation on requirements for vMotion between vCenter server instances](#)

- 1. With vSphere Web Client, select the Cluster from the Host and Cluster inventory and click on VMs tab.



- 2. Select the VMs that needs to be migrated and right click to select Migrate option.



- 3. Choose option to change compute resource and storage, Click Next

4 Virtual Machines - Migrate

1 Select a migration type

- 2 Select a compute resource
- 3 Select storage
- 4 Select networks
- 5 Select vMotion priority
- 6 Ready to complete

Select a migration type

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

- ☐ **Change compute resource only**
Migrate the virtual machines to another host or cluster.
- ☐ **Change storage only**
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- ☒ **Change both compute resource and storage**
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- ☐ **Cross vCenter Server export**
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Select the target cluster in target vCenter server.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

- 3 Select storage
- 4 Select networks
- 5 Select vMotion priority
- 6 Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

- ▼ vcf-m01-vc01.sddc.netapp.com
 - > vcf-m01-dc01
- ▼ vcf-wkld-vc01.sddc.netapp.com
 - ▼ vcf-wkld-01-DC
 - > IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Select the desired VM Storage Policy and pick the datastore that is compatible. Click Next.

4 Virtual Machines - Migrate

- Select a migration type
- Select a compute resource
- Select storage**
- Select folder
- Select networks
- Select vMotion priority
- 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	
<input checked="" type="radio"/>	VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB	
<input type="radio"/>	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB	
<input type="radio"/>	VCF_WKLD_03_ISCSI	Incompatible	3 TB	858.61 GB	2.85 TB	
<input type="radio"/>	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	
<input type="radio"/>	vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	
<input type="radio"/>	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

- Select a migration type
- Select a compute resource
- Select storage
- Select folder**
- Select networks
- Select vMotion priority
- 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

- Select a migration type
- Select a compute resource
- Select storage
- Select folder
- Select networks
- Select vMotion priority
- Ready to complete

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

ADVANCED >>

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

8. Review the migration options and click Finish.

4 Virtual Machines - Migrate

- Select a migration type
- Select storage
- 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 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

```

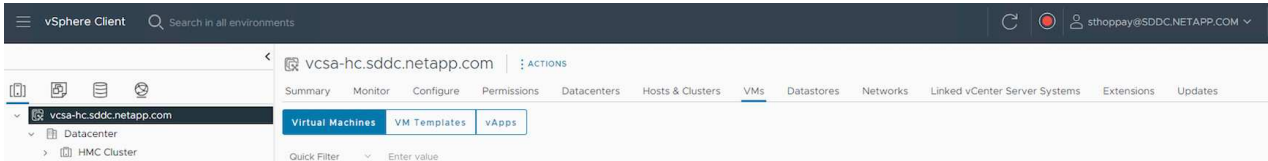

Migration of VMs across vCenter servers in different SSO domain



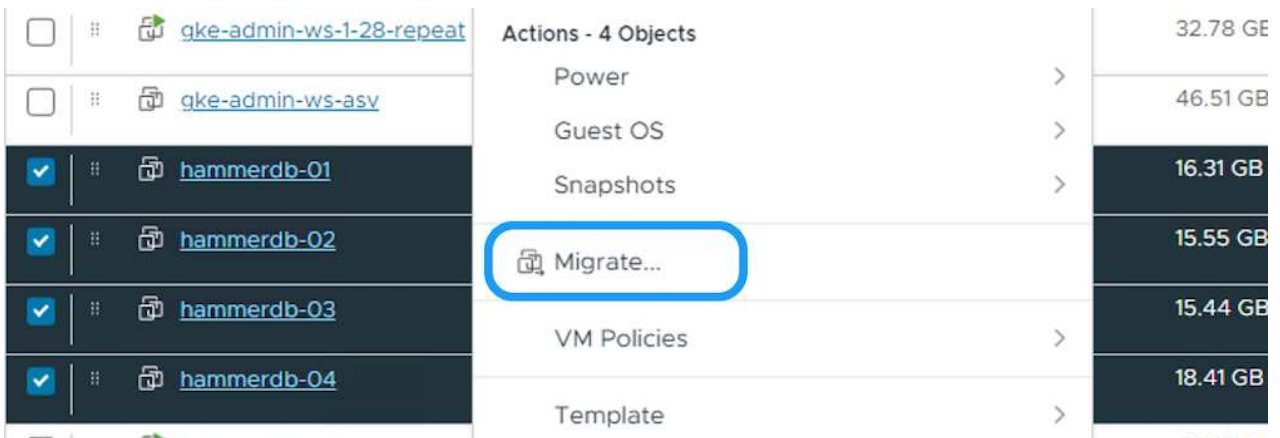
This scenario assumes the communication exists between the vCenter servers. Otherwise check the across datacenter location scenario listed below. For prerequisites, check [vSphere documentation on Advanced Cross vCenter vMotion](#)

Follow the procedure below to migrate VMs to different vCenter server using UI.

1. With vSphere Web Client, select the source vCenter server and click on VMs tab.



2. Select the VMs that need 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

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select a migration type

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

- ☐ **Change compute resource only**
Migrate the virtual machines to another host or cluster.
- ☐ **Change storage only**
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- ☐ **Change both compute resource and storage**
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- ☒ **Cross vCenter Server export**
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.
 - ☐ Keep VMs on the source vCenter Server (performs a VM clone operation).

CANCEL

NEXT



VM can also be imported from the target vCenter server. For that procedure, check [Import or Clone a Virtual Machine with Advanced Cross vCenter vMotion](#)

4. Provide vCenter credential details and click Login.

Migrate | SQLSRV-05

1 Select a migration type

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select networks
- 6 Ready to complete

Select a target vCenter Server

Export Virtual Machines to the selected target vCenter Server.

[SAVED VCENTER SERVERS](#) [NEW VCENTER SERVER](#)

vCenter Server address
vCenter Server FQDN or IP address

Username
example@domain.local

Password

Save vCenter Server address ☒

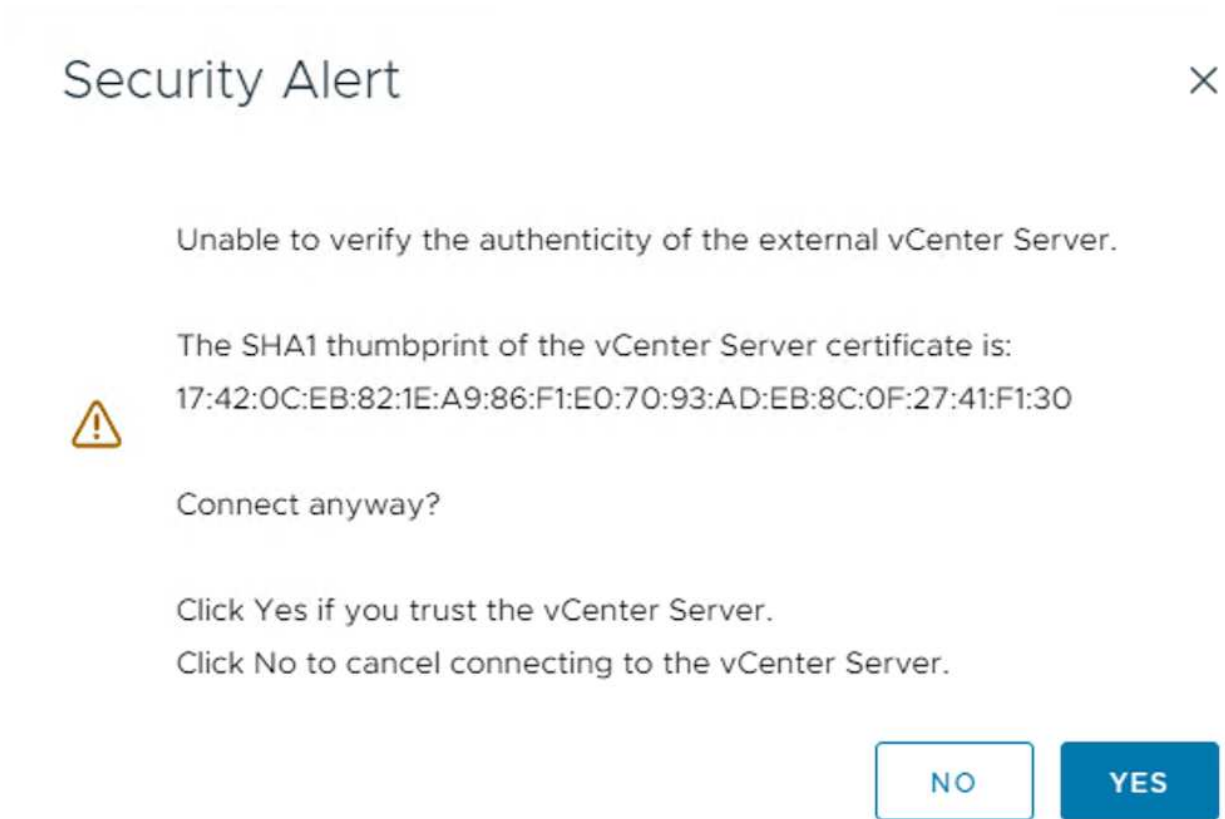
LOGIN

CANCEL

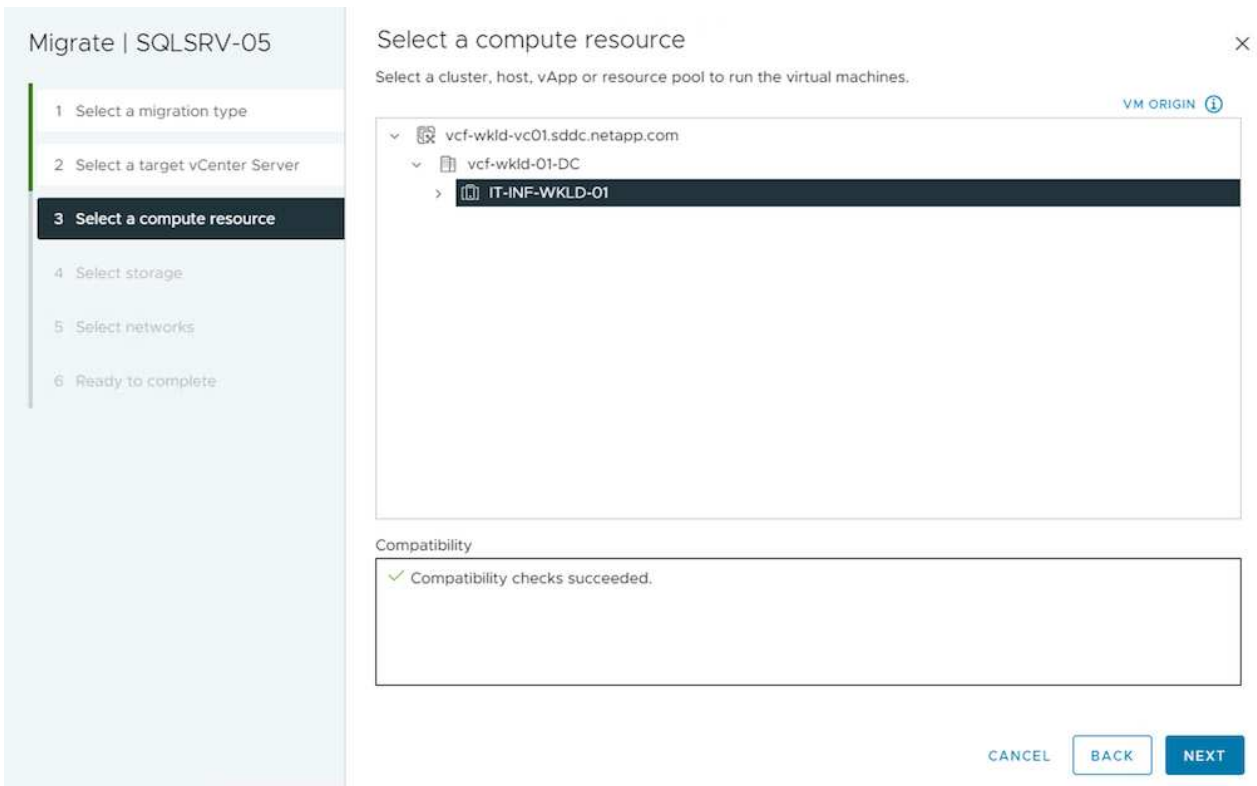
BACK

NEXT

5. Confirm and Accept the SSL certificate thumbprint of vCenter server



6. Expand target vCenter and select the target compute cluster.



7. Select the target datastore based on the VM Storage Policy.

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 storage

Select the destination storage for the virtual machine migration.

VM ORIGIN ⓘ

BATCH CONFIGURE

CONFIGURE PER DISK

Select virtual disk format

Thin Provision

VM Storage Policy

NFS

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
<input checked="" type="radio"/>	VCF_WKLD_01	Compatible	5 TB	5.93 GB	5 TB	N
<input type="radio"/>	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	24 MB	2.93 TB	v
<input type="radio"/>	VCF_WKLD_03_JSCSI	Incompatible	3 TB	1.35 TB	2.59 TB	v
<input type="radio"/>	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	v
<input type="radio"/>	vcf-wkld-esx02-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.

CANCEL

BACK

NEXT

8. Select the target VM folder.

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 folder

Select the destination virtual machine folder for the virtual machine migration.

VM ORIGIN ⓘ

Select location for the virtual machine migration.

vcf-wkld-01-DC

Discovered virtual machine

Oracle

SQL Server

vCLS

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

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.

CANCEL

BACK

NEXT

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

CANCEL

BACK

FINISH

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.
- Continuous Data Protection (CDP) products use [vSphere API for IO \(VAIO\)](#) to intercept the data and send a copy to remote location for near zero RPO solution.
- Backup and Recovery products can also be utilized. But often results in longer RTO.
- [BlueXP Disaster Recovery as a Service \(DRaaS\)](#) utilizes storage array based replication and automates certain tasks to recover the VMs at target site.

Migration of VMs in hybrid cloud environment

- [Configure Hybrid Linked Mode](#) and follow the procedure of [Migration of VMs across vCenter servers in same SSO domain](#)
- HCX provides various [migration types](#) including Replication Assisted vMotion across the datacenters to move VM while it is powered on.
 - [TR 4942: Migrate Workloads to FSx ONTAP datastore using VMware HCX](#)
 - [TR-4940: Migrate workloads to Azure NetApp Files datastore using VMware HCX - Quickstart guide](#)
 - [Migrate workloads to Google Cloud NetApp Volumes datastore on Google Cloud VMware Engine using VMware HCX - Quickstart guide](#)
- [BlueXP Disaster Recovery as a Service \(DRaaS\)](#) utilizes storage array based replication and automates certain tasks to recover the VMs at target site.
- With supported Continuous 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.

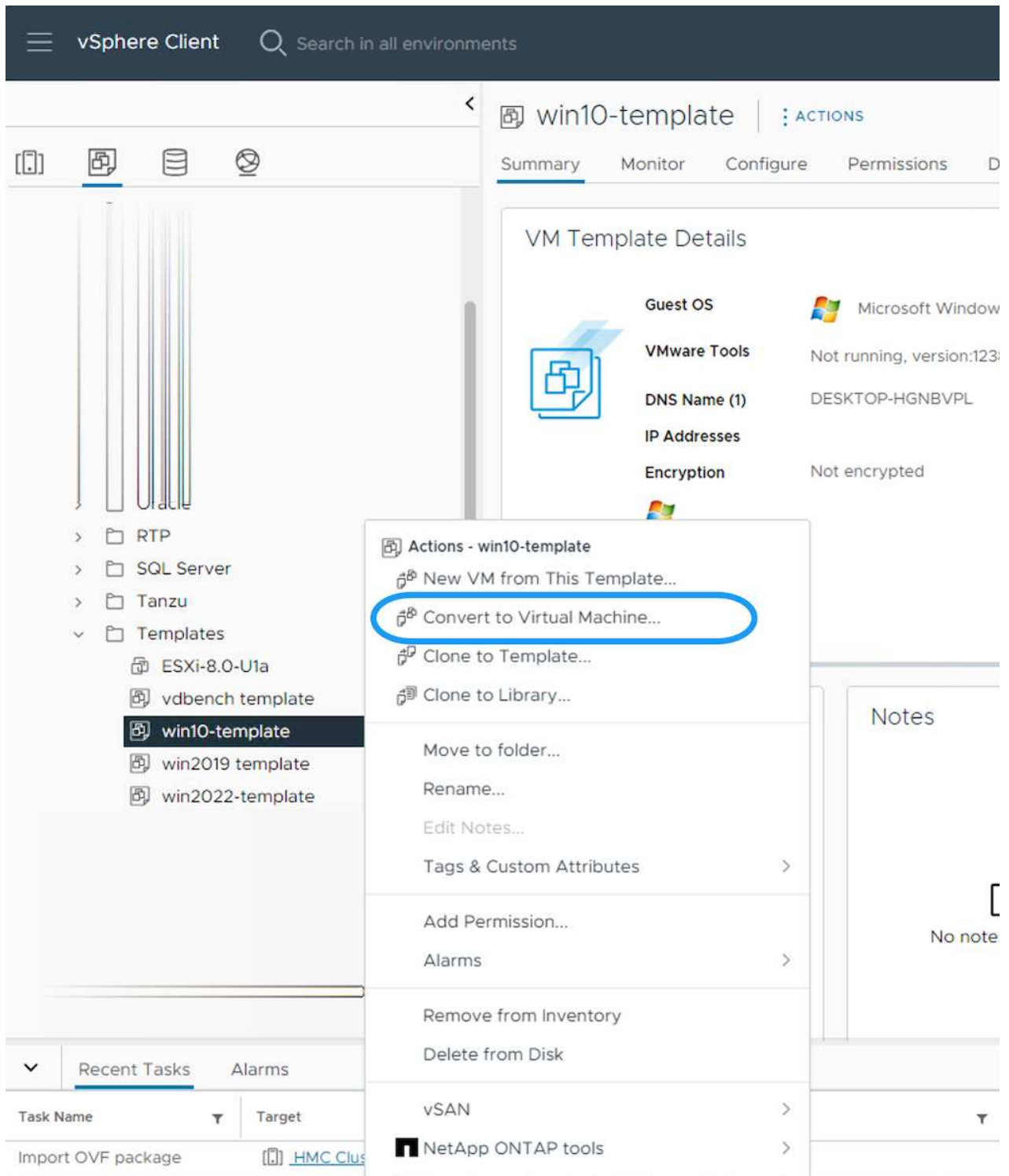
VM Template Migration Scenarios

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.



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



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

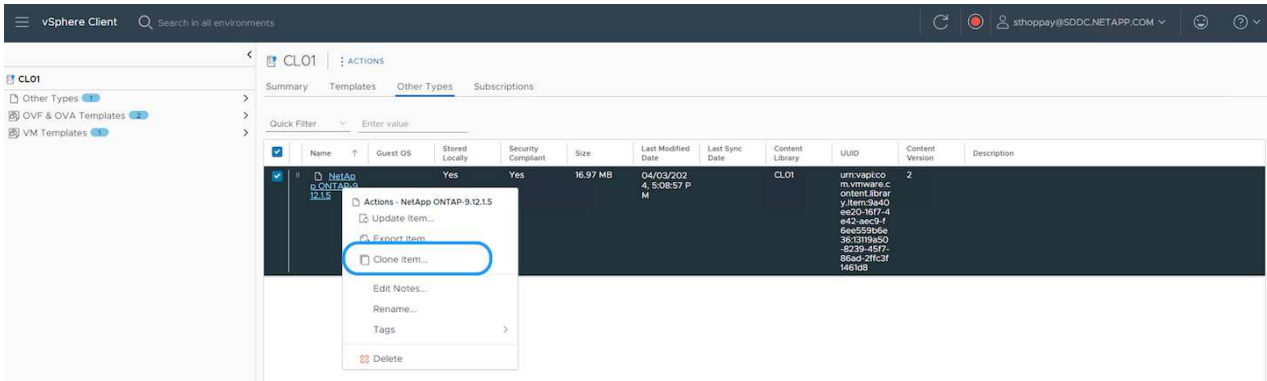


VMware Aria Operations Configuration



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 ..



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

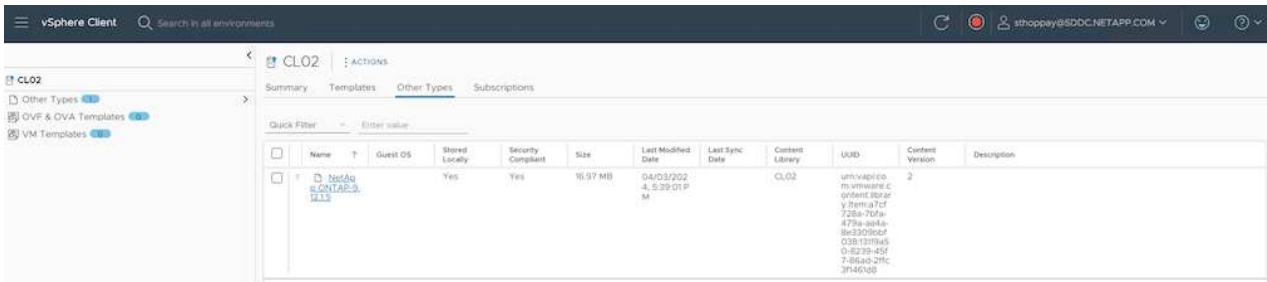
Select a content library where to clone the library item.

	Name	Notes	Creation Date
<input type="radio"/>	CL01		9/26/2023, 5:02:03 PM
<input checked="" type="radio"/>	CL02		4/1/2024, 12:37:51 PM

CANCEL

OK

5. Validate the item is available on target content library.



The screenshot shows the vSphere Client interface. On the left, there's a navigation pane with 'CL02' selected. The main pane shows the 'Other Types' tab for content library 'CL02'. A table lists the content library items.

Name	Guest OS	Stored Locally	Security Compliant	Size	Last Modified Date	Last Sync Date	Content Library	UUID	Content Version	Description
vmware-vmware-cs-NetApp-5.013		Yes	Yes	16.97 MB	04/03/2024 5:39:01 PM		CL02	urn:vmware:content-library-item:a7cf728a-702a-479a-a0fa-8e330562f03b:1b19a50-6239-45f7-86aa-29fc3f1465b8	2	

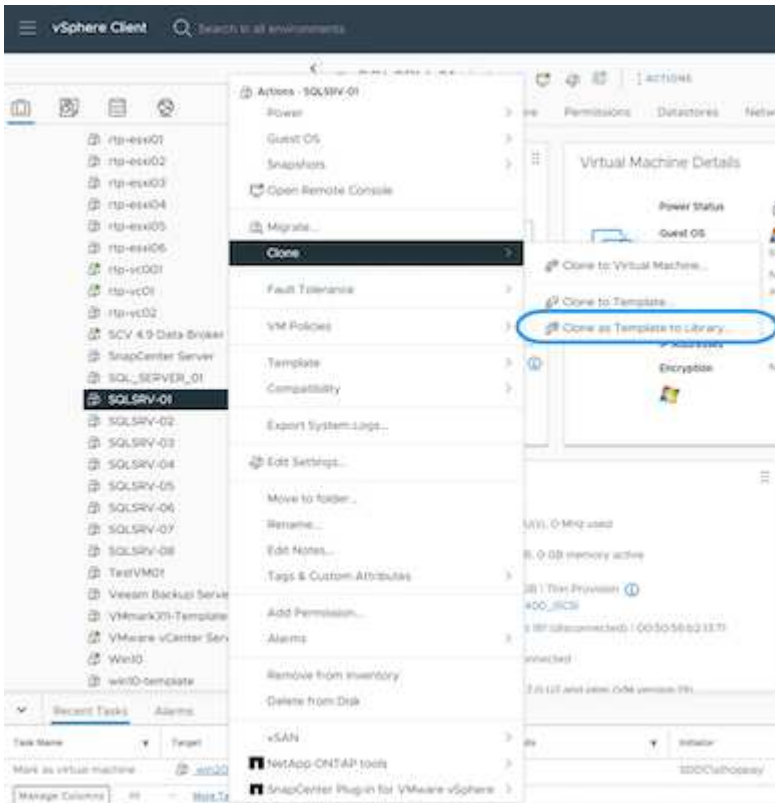
Here is the sample PowerCLI script to copy the content library items from content library CL01 to CL02.

```
#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-ContentLibraryItem -ContentLibrary (Get-ContentLibrary 'CL01' -Server
$sourcevc) | Where-Object { $_.ItemType -ne 'vm-template' } | Copy-
ContentLibraryItem -ContentLibrary (Get-ContentLibrary '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 library, 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

vcasa-hc.sddc.netapp.com

Datacenter

CANCEL

NEXT

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](#)

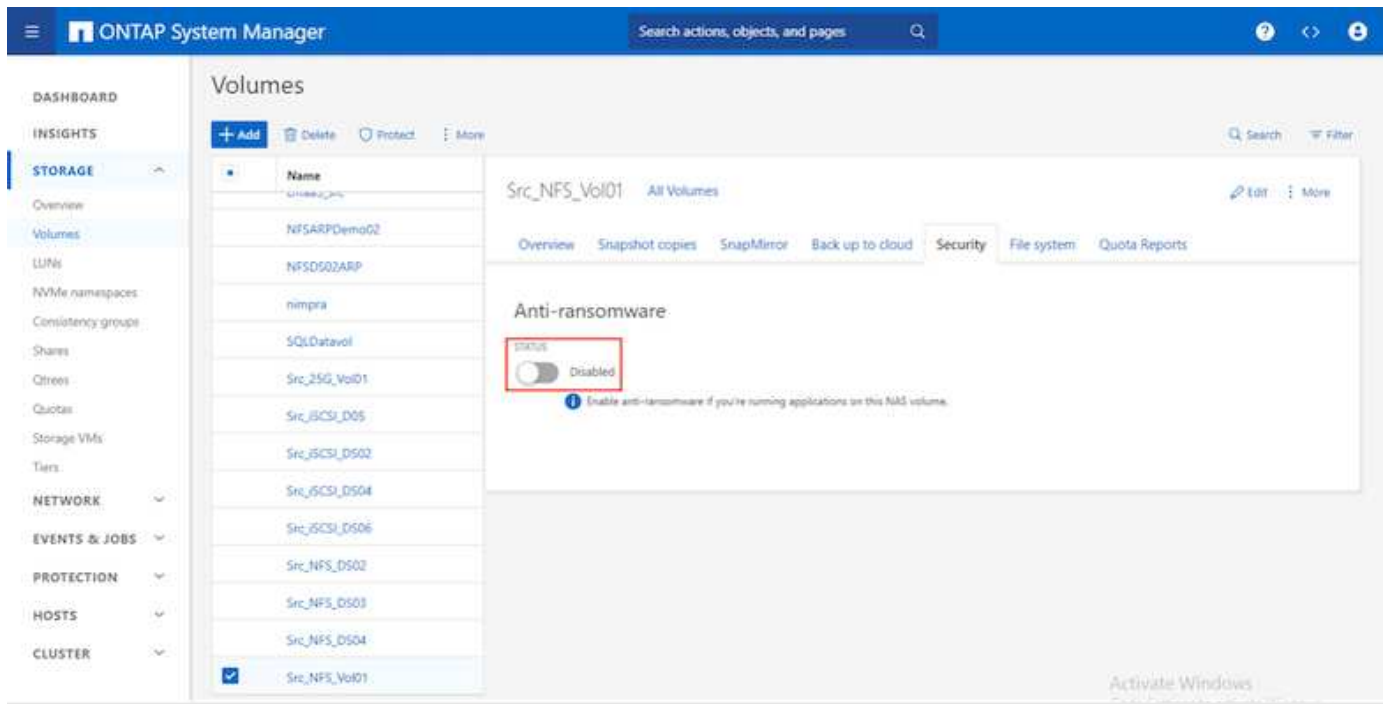
Additional Resources

- [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](#)
- [BlueXP 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.

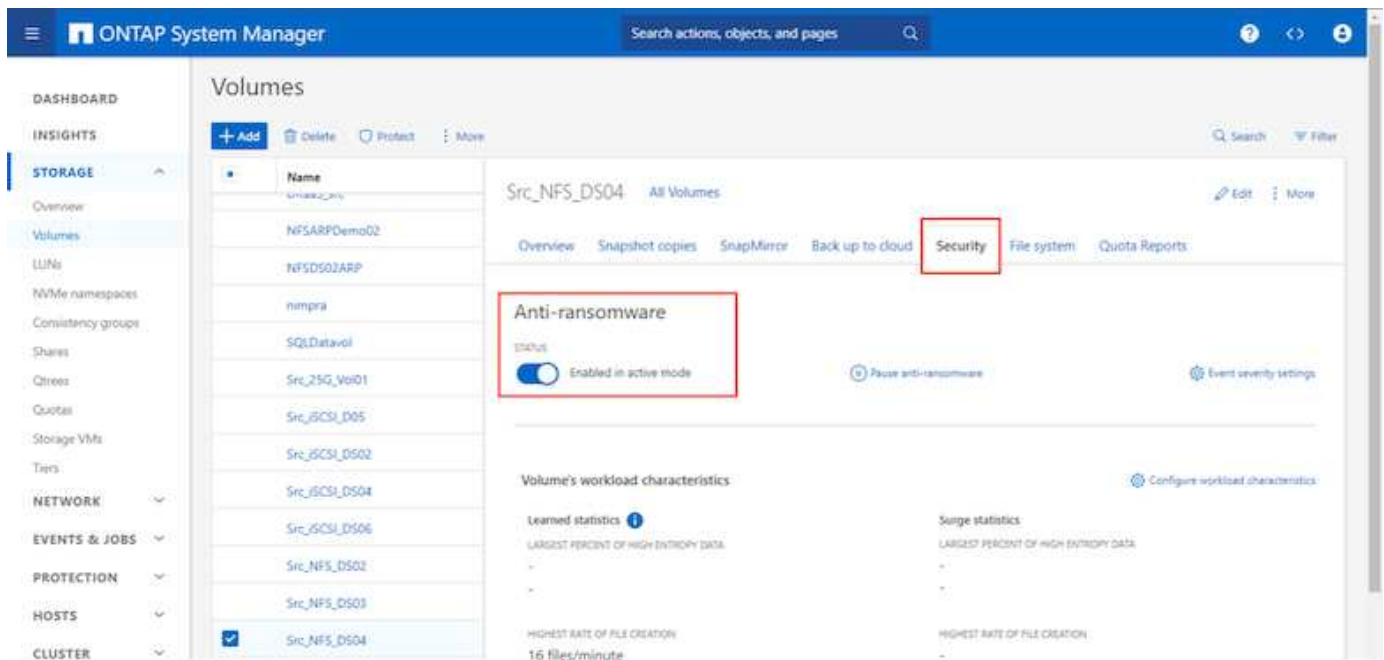


With the new NetApp ARP/AI, which is currently in tech preview, there is no need for a learning mode. Instead, it can go straight to active mode with its AI-powered ransomware detection capability.



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

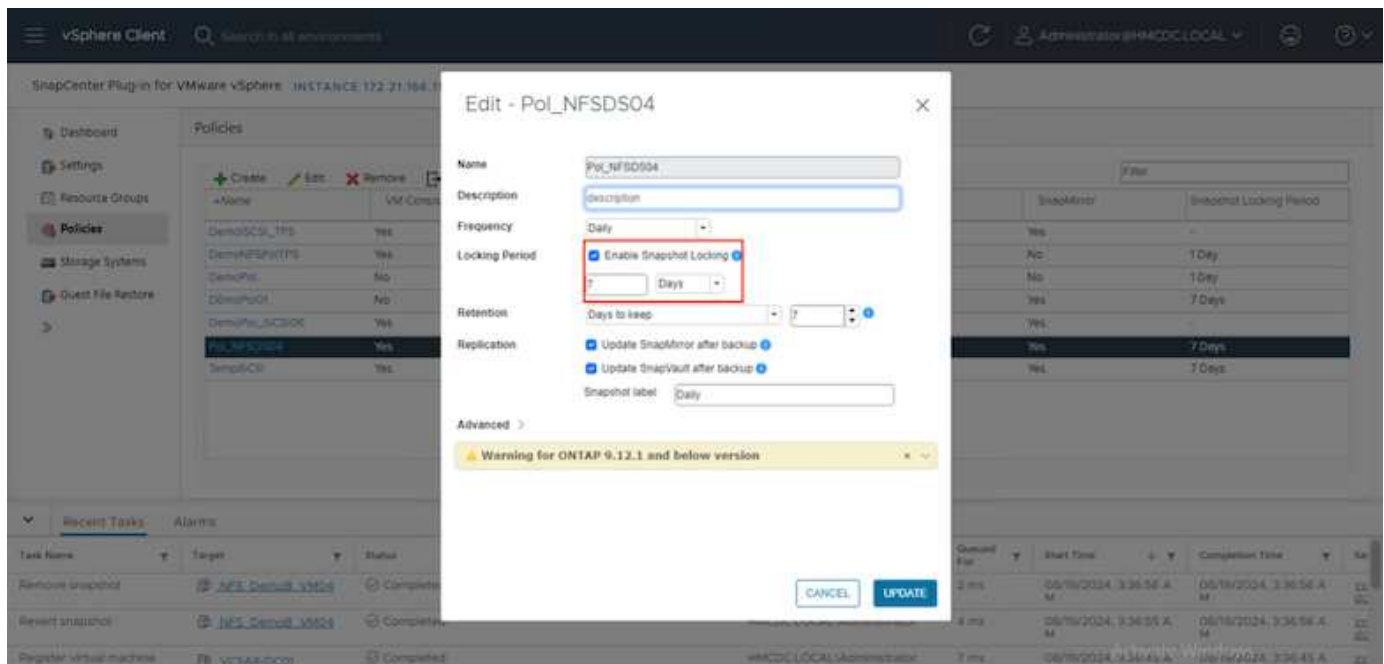
Once in active mode, it starts looking for the abnormal volume activity that might potentially be ransomware. If abnormal activity is detected, an automatic Snapshot copy is immediately taken, which provides a restoration point as close as possible to the file infection. ARP can detect changes in VM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



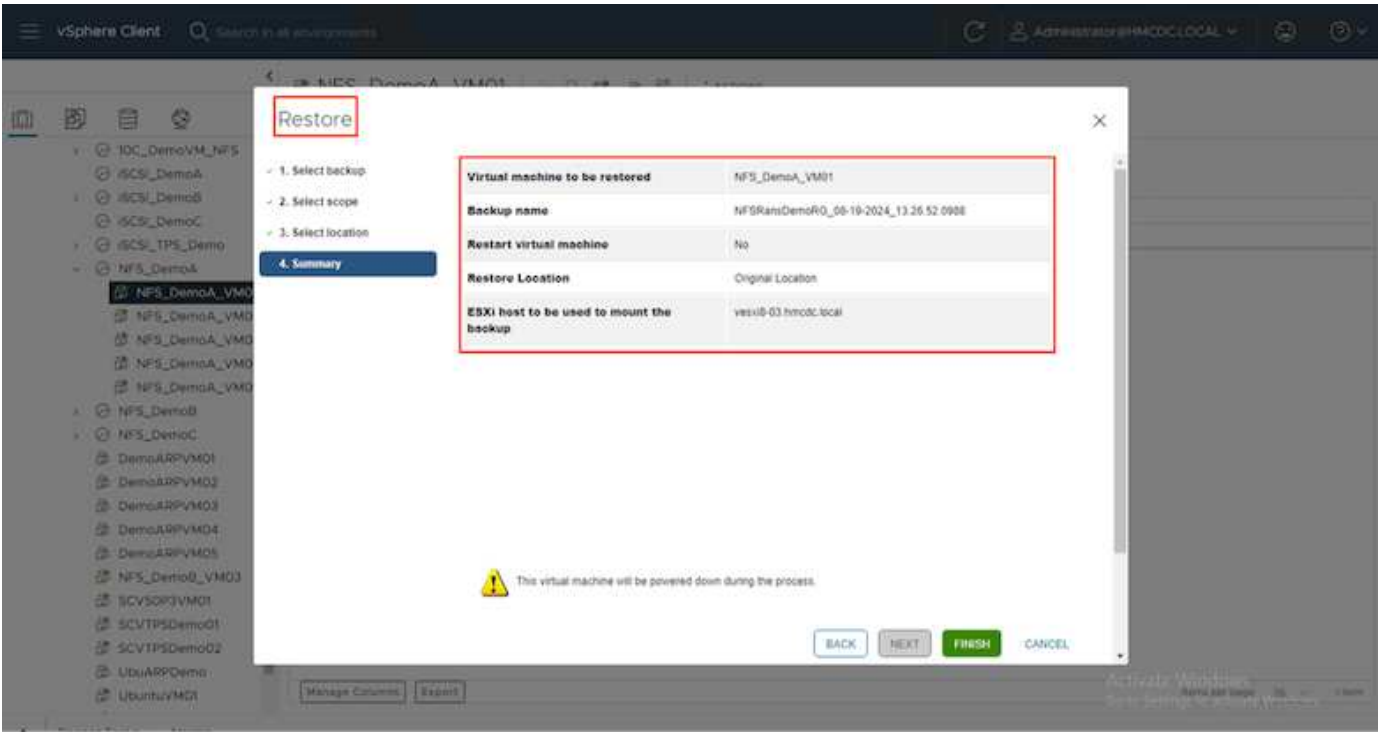
If a ransomware attack targets the virtual machine (VM) and alter files within the VM without making changes outside the VM, the Advanced Ransomware Protection (ARP) will still detect the threat if the default entropy of the VM is low, for example, for file types like .txt, .docx, or .mp4 files. Even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

For detailed information, refer to "ARP and Virtual machines" section in [ARP usecases and considerations](#).

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



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



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

For additional information, view guidance for [NetApp solutions for ransomware](#).

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

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

NetApp BlueXP

BlueXP Search

Ransomware protection

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

Workloads (10)

Workload	Type	Connector	Importance	Protection st...	Detection sta...	Detection pol...	Snapshot an...	Backup destina...	
Src_nfs_ds02	VM datastore	GISABXPConn	Critical	Protected	Learning mode	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	Edit protection
Draas_src_test_3130	VM file share	GISABXPConn	Standard	At risk	None	None	None	n/a	Protect
Nfsds02src_804	VM file share	GISABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	Edit protection
Draas_src_7027	VM file share	GISABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	Protect
Src_nfs_vsi01_7948	VM file share	GISABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	Protect
Src_nfs_ds03	VM datastore	GISABXPConn	Standard	At risk	None	None	SnapCenter for VMw...	netapp-backup-add...	Protect
Src_nfs_ds04	VM datastore	GISABXPConn	Standard	Protected	Active	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	Edit protection
Src_nfs_ds04	File share	GISABXPConn	Critical	Protected	Active	rps-policy-primary	BlueXP backup and ...	netapp-backup-ba3...	Edit protection
Testvol_1787	File share	GISABXPConn	Standard	Protected	Learning mode	rps-policy-primary	None	netapp-backup-ba3...	Edit protection
Nfsarpdemo02_3419	File share	GISABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	Edit protection

NetApp BlueXP

BlueXP Search

Ransomware protection

Dashboard Protection Alerts Recovery Reports

Standard Importance

Protected Protection health Alerts

Not marked for recovery Recovery

Protection

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

Pol_NFS04 Snapshot policy

1 Year Daily LTR Backup policy

VM datastore

Location urn:scv:scvmUI:Resou...

vCenter server vvcas8-01.hmclic.local

Connector GISABXPConn

Storage

Cluster id add38d26-348c-11ef-8...

Working Env name NTAP915_Src

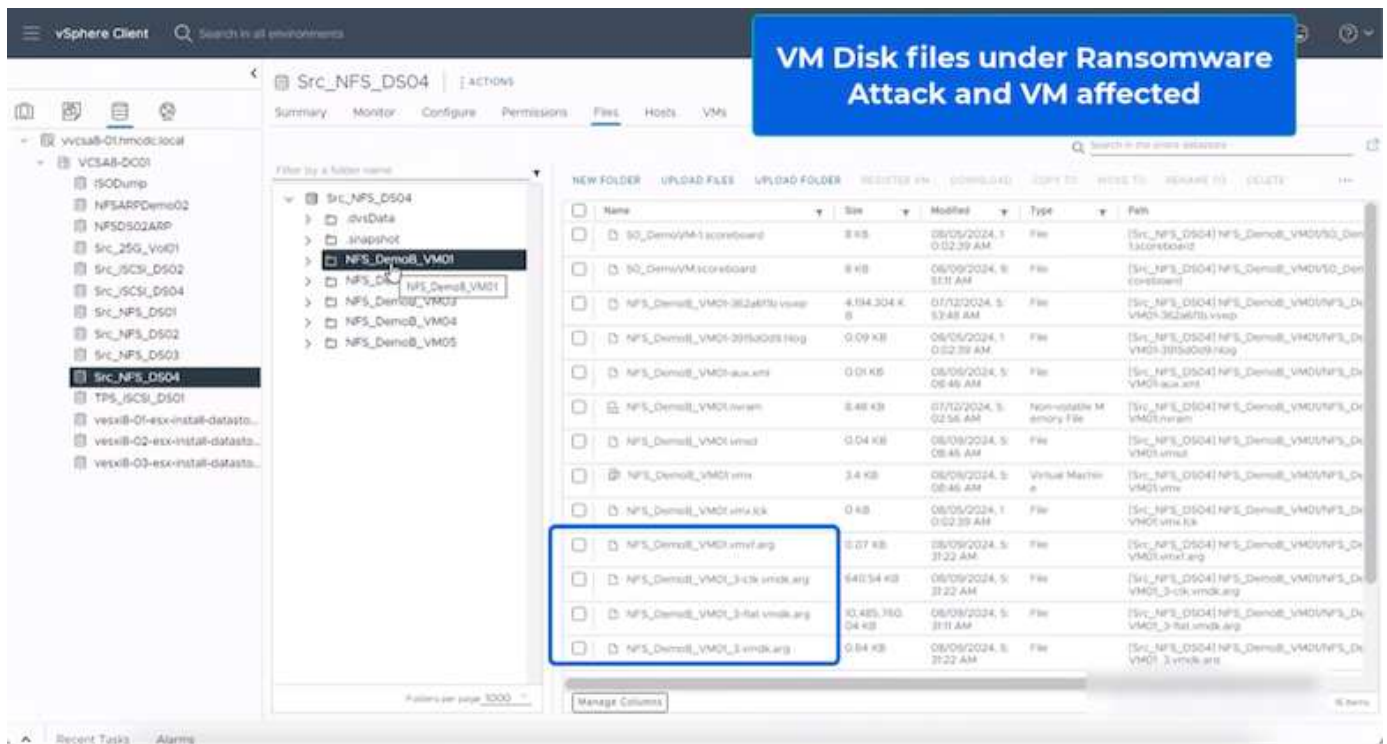
Storage VM name svm_NFS

Volume name Src_NFS_DS04

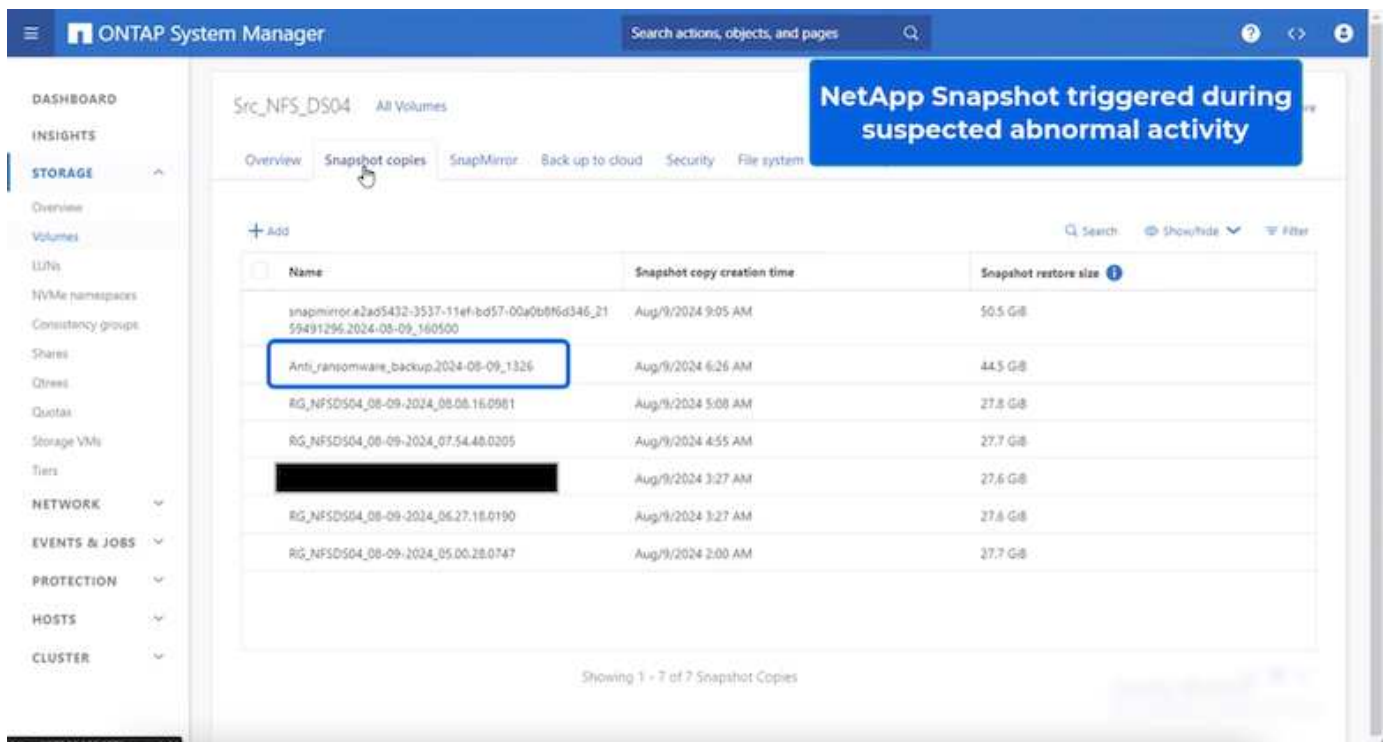
Used size 29 GiB

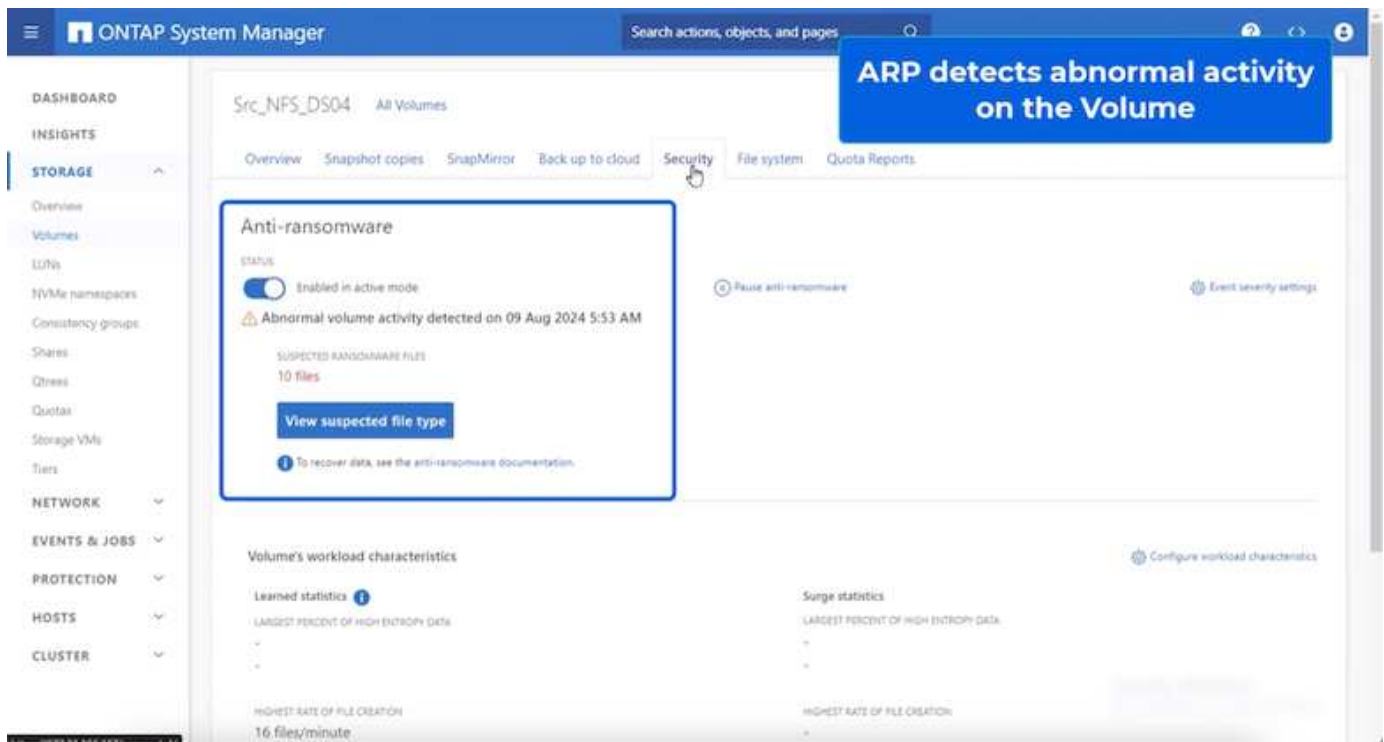
For detailed information on to configure BlueXP ransomware protection, refer to [Setup BlueXP ransomware protection](#) and [Configure BlueXP ransomware protection settings](#).

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

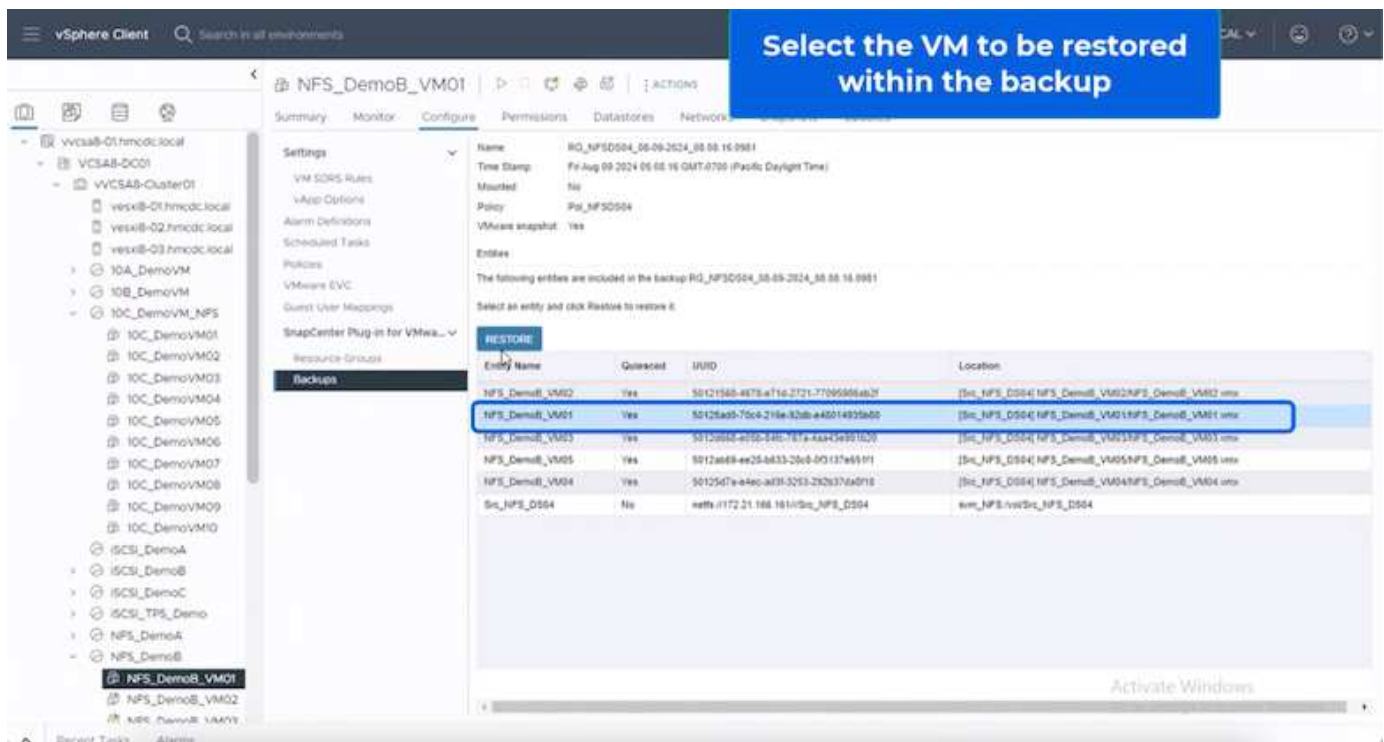


ARP immediately triggered a snapshot on the volume upon detection.





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

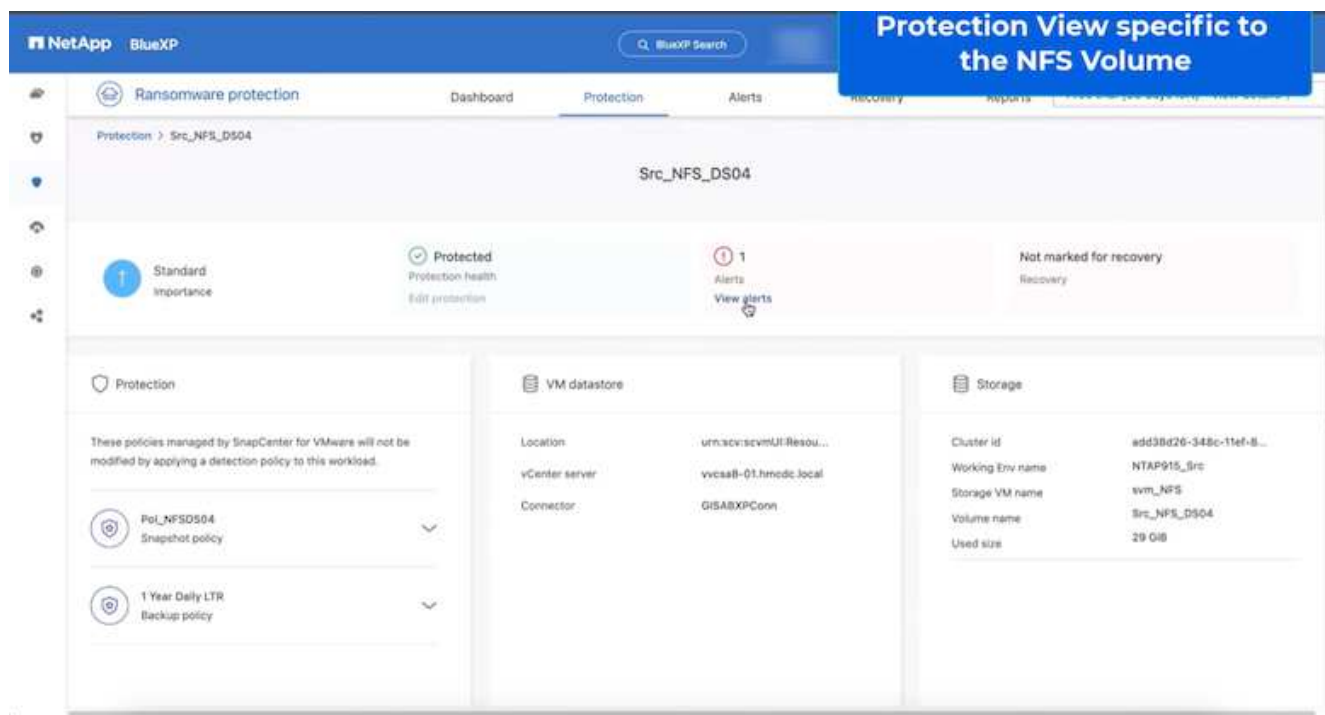


This section looks at how BlueXP ransomware protection orchestrates recovery from a ransomware incident wherein the VM files are encrypted.

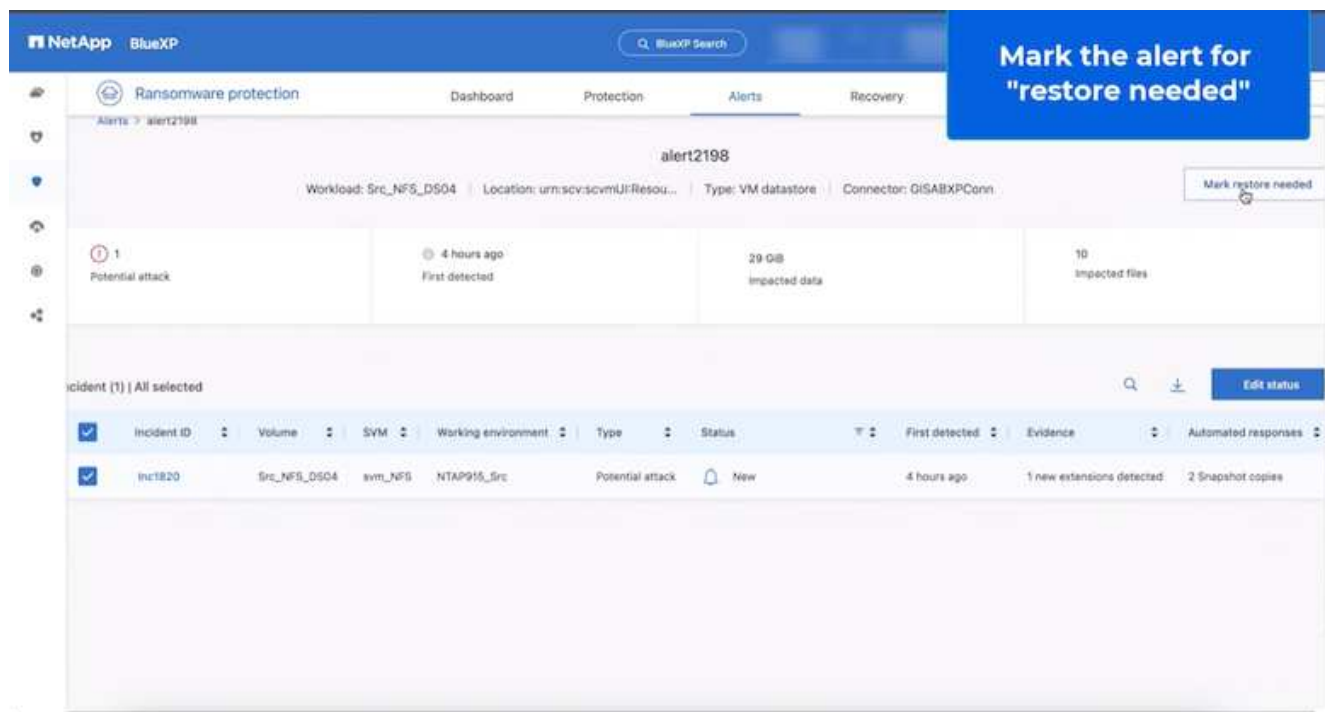


If the VM is managed by SnapCenter, BlueXP ransomware protection restores the VM back to its previous state using the VM-consistent process.

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

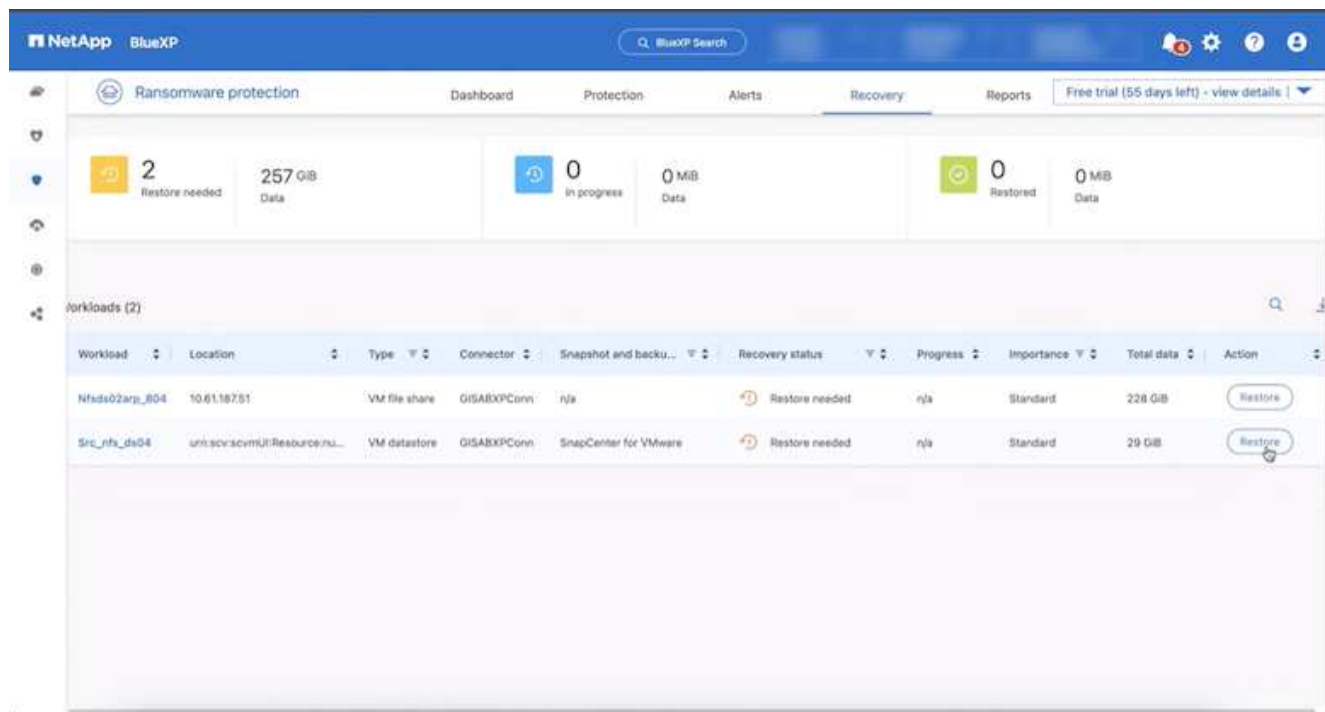


3. Mark the ransomware incident as ready for recovery (after incidents are neutralized) by selecting "Mark restore needed"

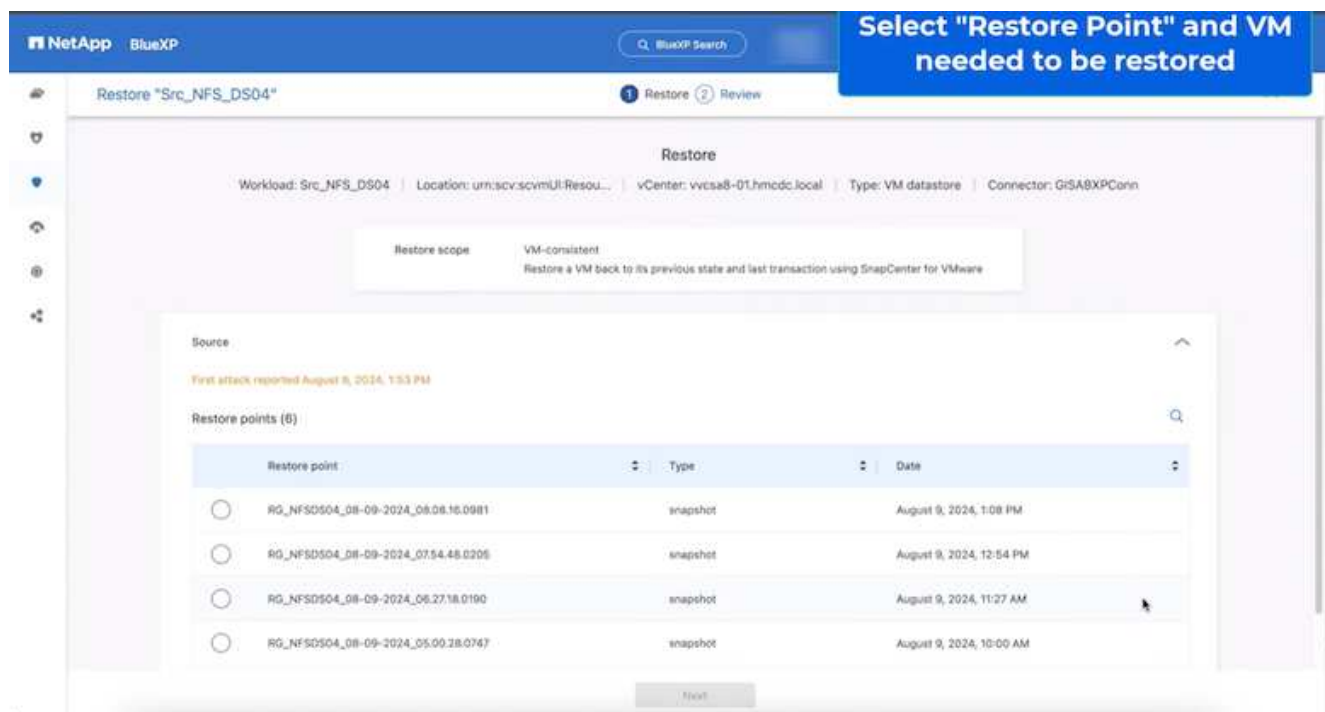


The alert can be dismissed if the incident turns out to be false positive.

- 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.



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



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

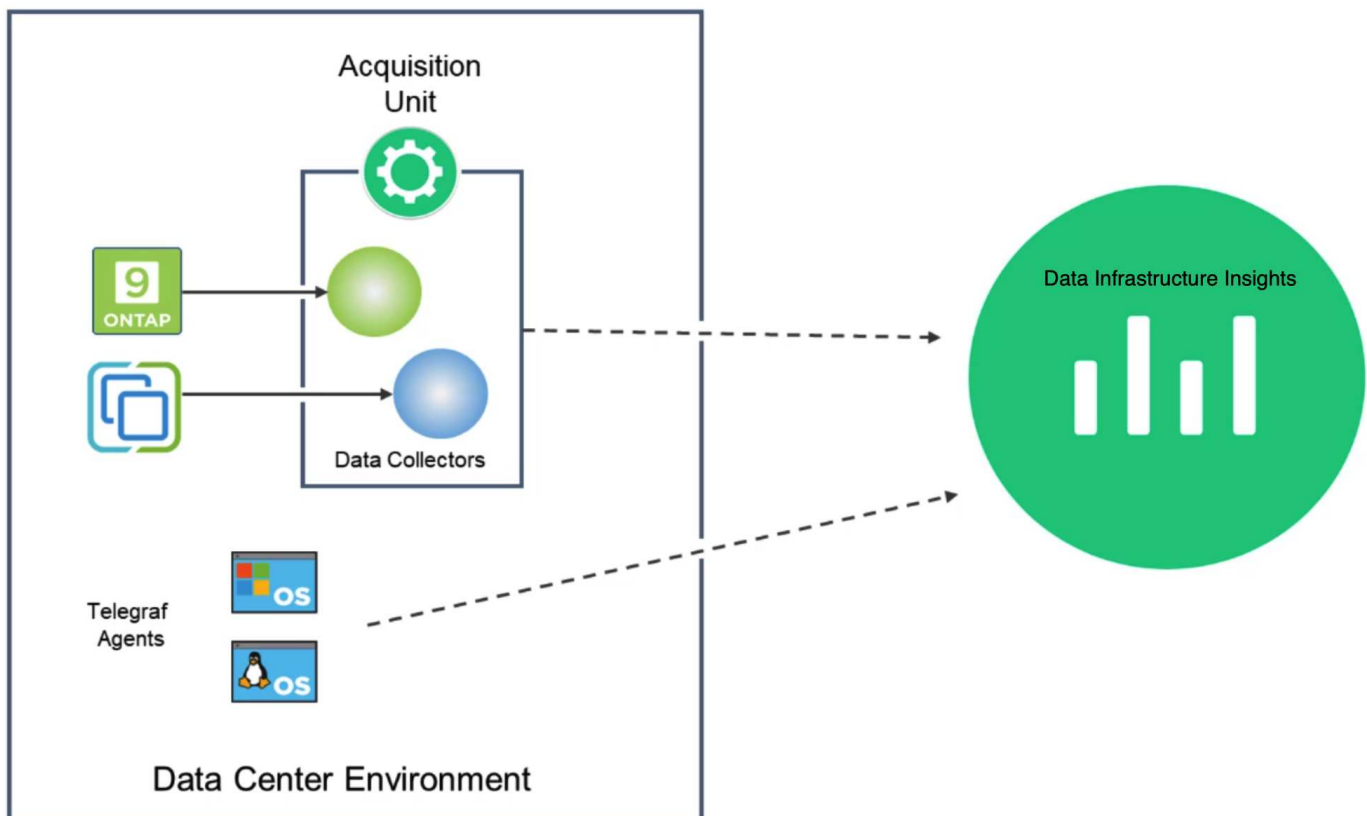
Monitor on-premises storage with Data Infrastructure Insights

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 BlueXP account.
4. NetApp Data Infrastructure Insights Acquisition Unit software installed on a local VM with network connectivity to assets for data collection.

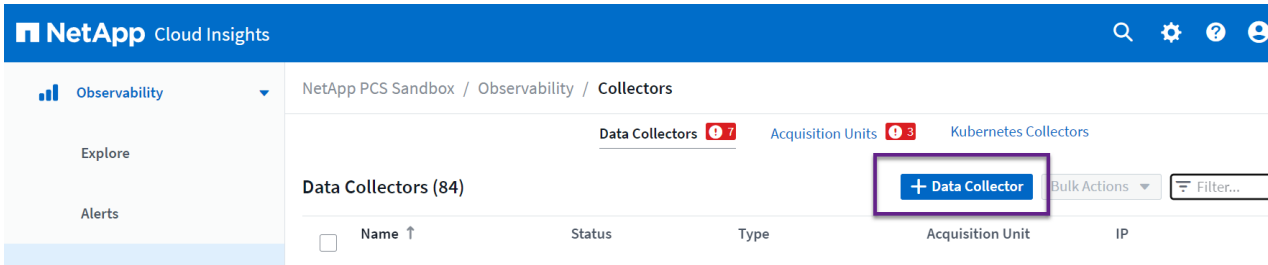
Solution Deployment

Configure Data Collectors

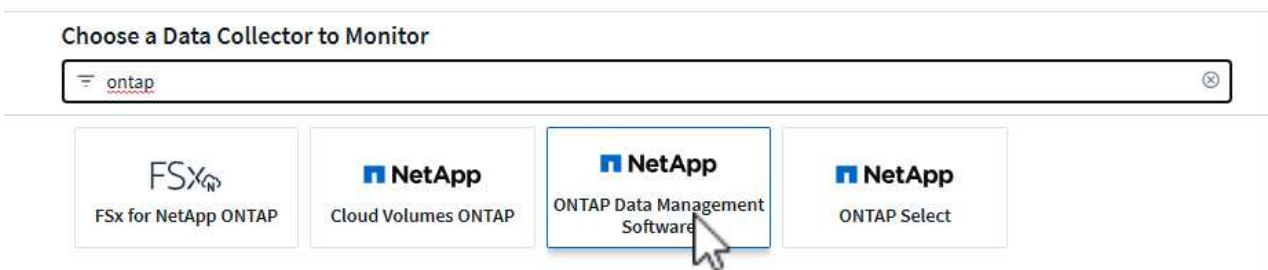
To configure Data Collectors for VMware vSphere and ONTAP storage systems complete the following steps:

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**.



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.

Select a Data Collector Configure Data Collector Complete Setup

NetApp ONTAP Data Management Software

Configure Collector

Add credentials and required settings Need Help?

Name ntaphci-a300e9u25 Acquisition Unit bxp-au01

NetApp Management IP Address 10.61.185.145 User Name admin

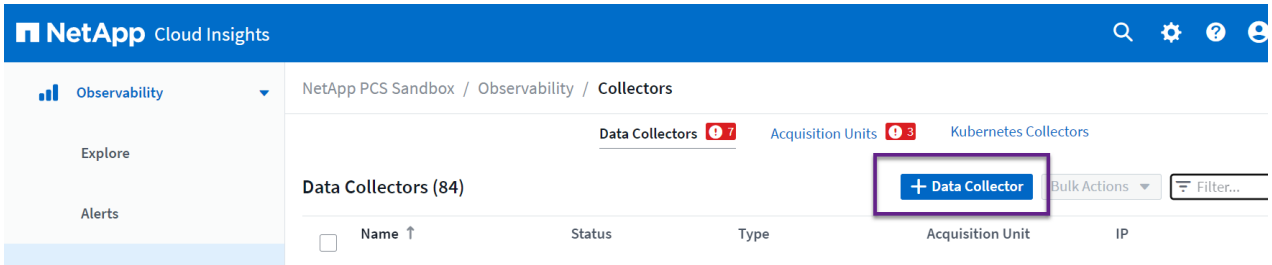
Password

Save and Continue Test Connection

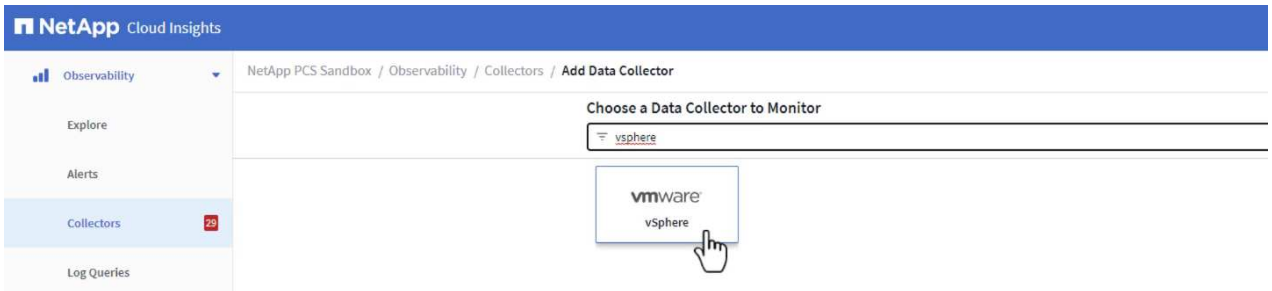
Advanced Configuration

Add a Data Collector for a VMware vSphere cluster

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



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



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



Configure Collector

Add credentials and required settings

[Need Help?](#)

Name  <input type="text" value="VCSA7"/>	Acquisition Unit <input type="text" value="bxp-au01"/>
--	---

Virtual Center IP Address <input type="text" value="10.61.181.210"/>	User Name <input type="text" value="administrator@vsphere.local"/>
Password <input type="password" value="*****"/>	

☐ Advanced Configuration

Collecting:

- ☒ Inventory
- ☒ VM Performance

Inventory Poll Interval (min) <input type="text" value="20"/>	Communication Port <input type="text" value="443"/>
--	--

Filter VMs by <input type="text" value="ESX_HOST"/>	Choose 'Exclude' or 'Include' to Specify a List <input type="text" value="Exclude"/>
--	---

Filter Device List (Comma Separated Values For Filtering By ESX_HOST, CLUSTER, and DATACENTER Only) <input type="text"/>	Performance Poll Interval (sec) <input type="text" value="300"/>
---	---

☐ Collect basic performance metrics only

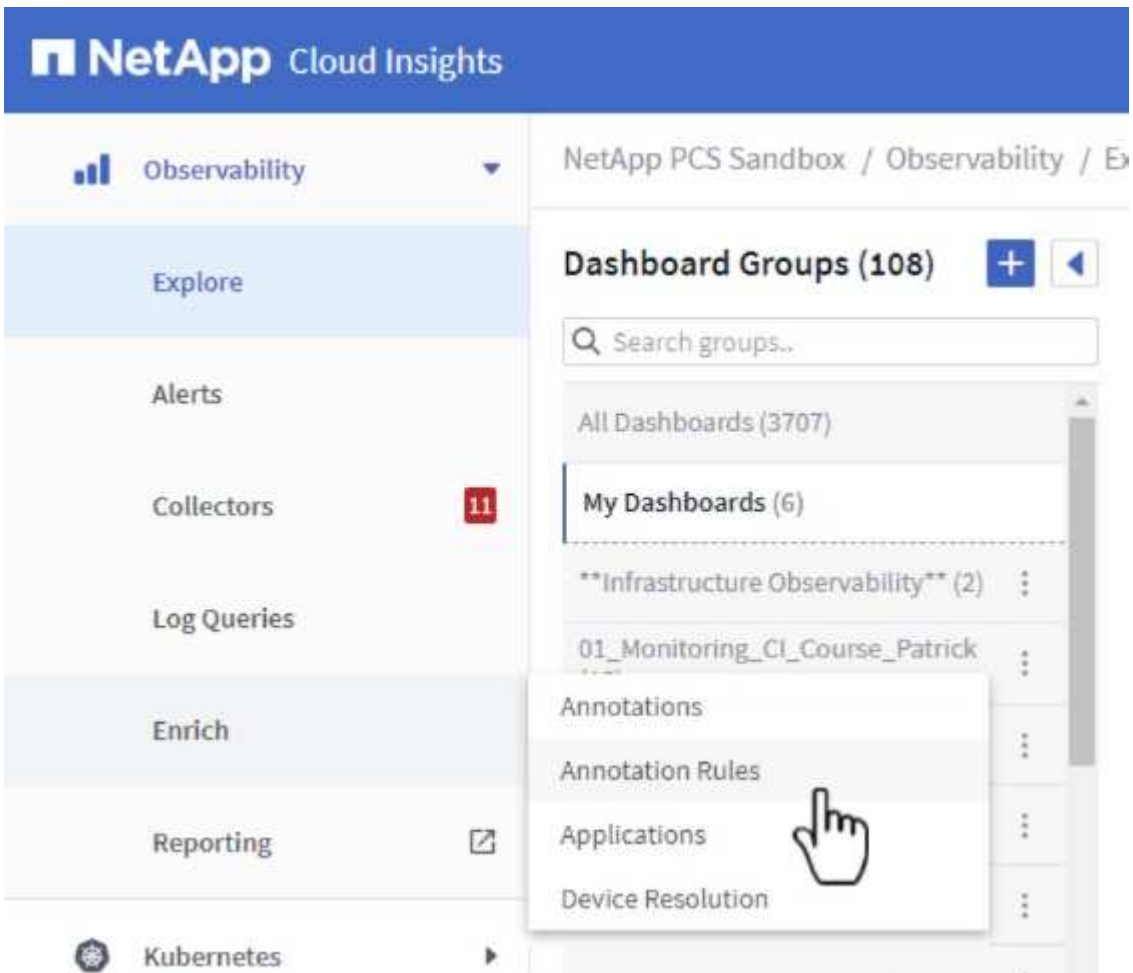
Add Annotations to assets

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.

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.

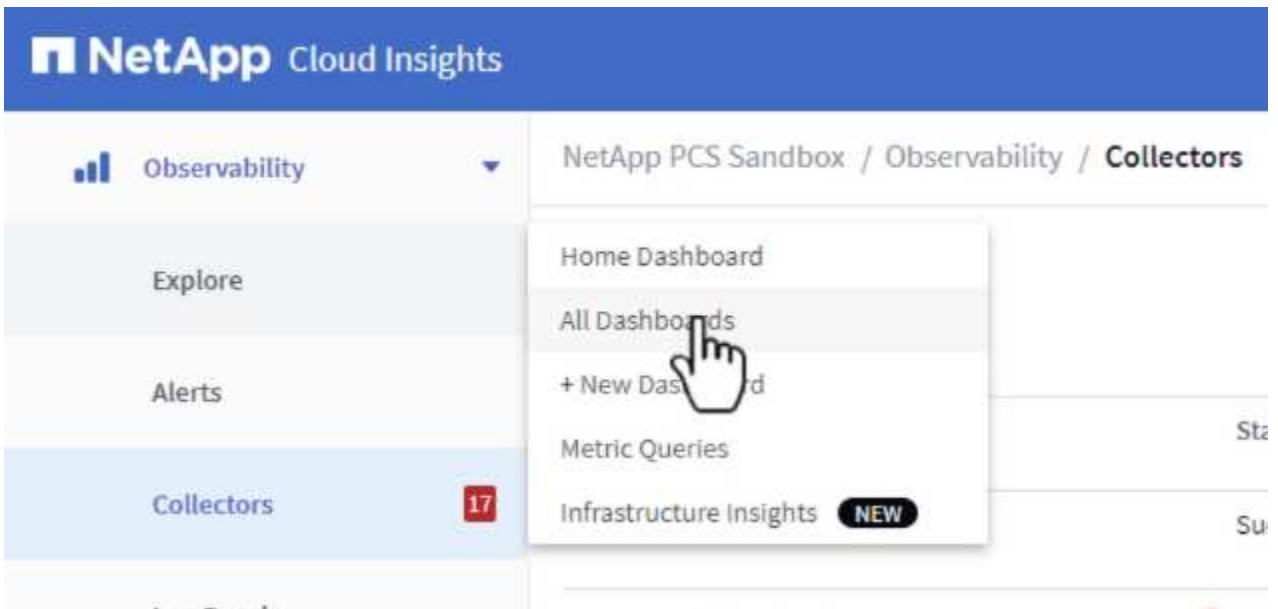
Explore and correlate assets

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

This sections illustrates how to use dashboards to correlate assets.

Correlating assets from a storage performance Dashboard

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



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



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

☐ ONTAP FAS/AFF - Cluster Capacity

☐ ONTAP FAS/AFF - Efficiency

☒ ONTAP FAS/AFF - FlexVol Performance

☐ ONTAP FAS/AFF - Node Operational/Optimal Points

☐ ONTAP FAS/AFF - PrePost Capacity Efficiencies

☐ Storage Admin - Which nodes are in high demand?

☐ Storage Admin - Which pools are in high demand?

☐ StorageGRID - Capacity Summary

☐ StorageGRID - ILM Performance Monitoring

☐ StorageGRID - MetaData Usage

☐ StorageGRID - S3 Performance Monitoring

☐ VMware Admin - ESX Hosts Overview

☐ VMware Admin - Overview

☐ VMware Admin - VM Performance

☐ VMware Admin - Where are opportunities to right size?

☐ VMware Admin - Where can I potentially reclaim waste?

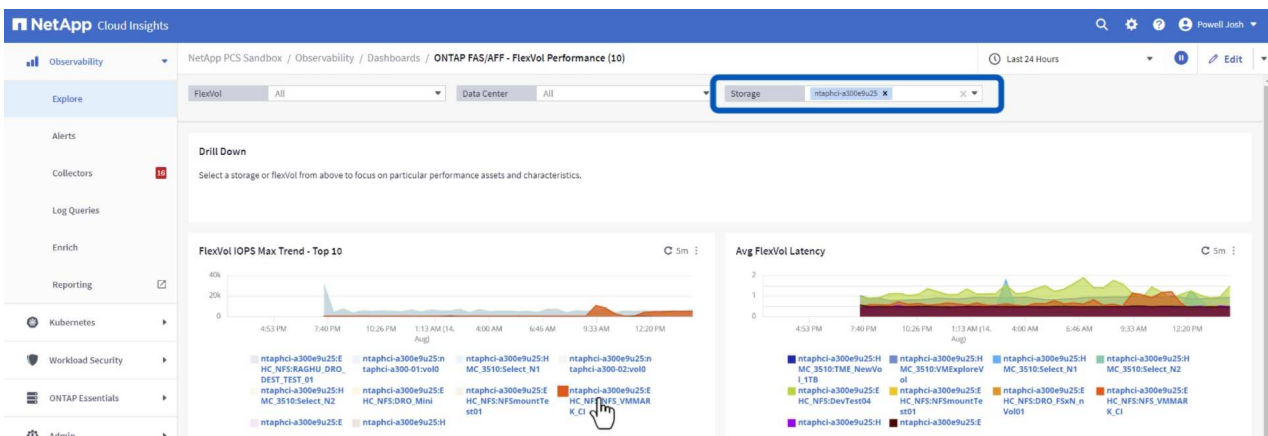
☐ VMware Admin - Where do I have VM Latency?

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

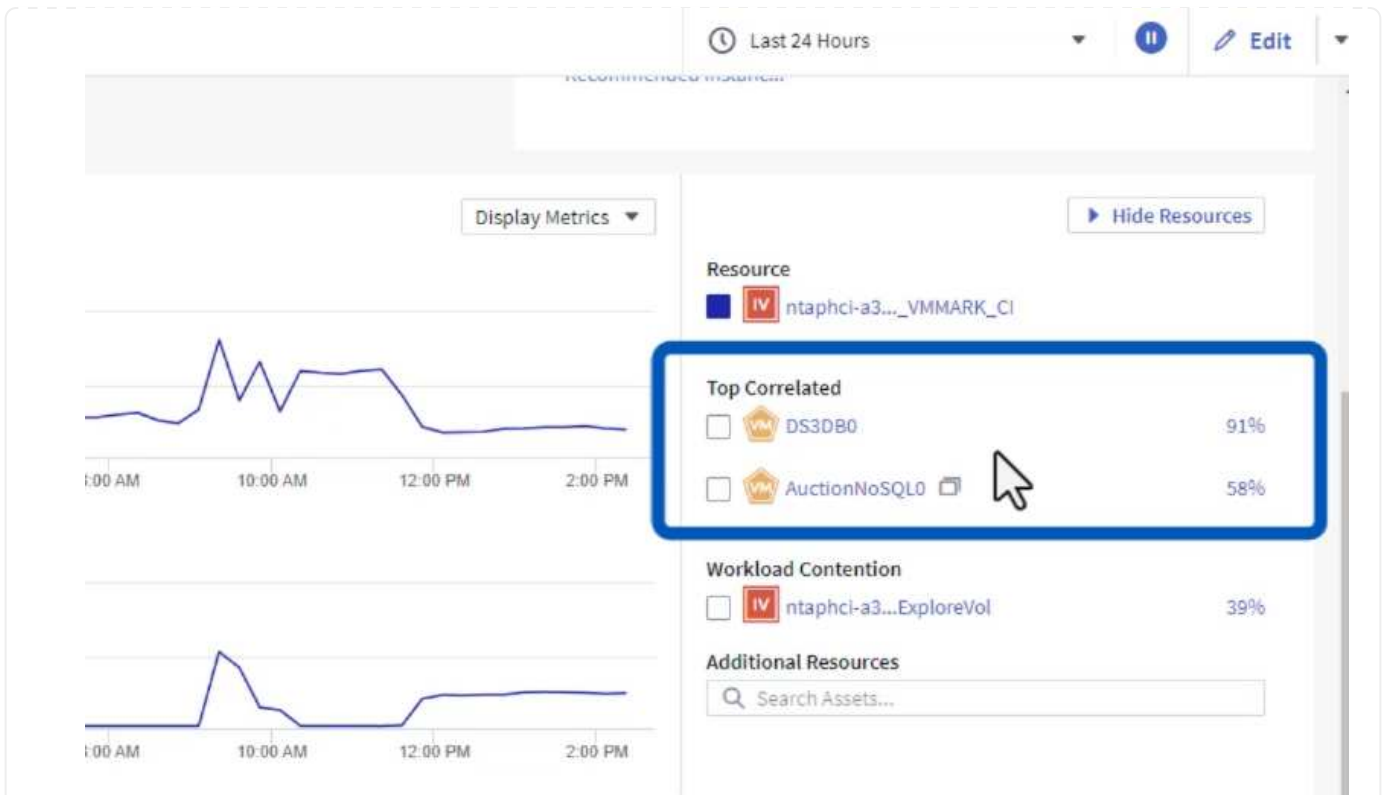
Add Dashboards

Go Back

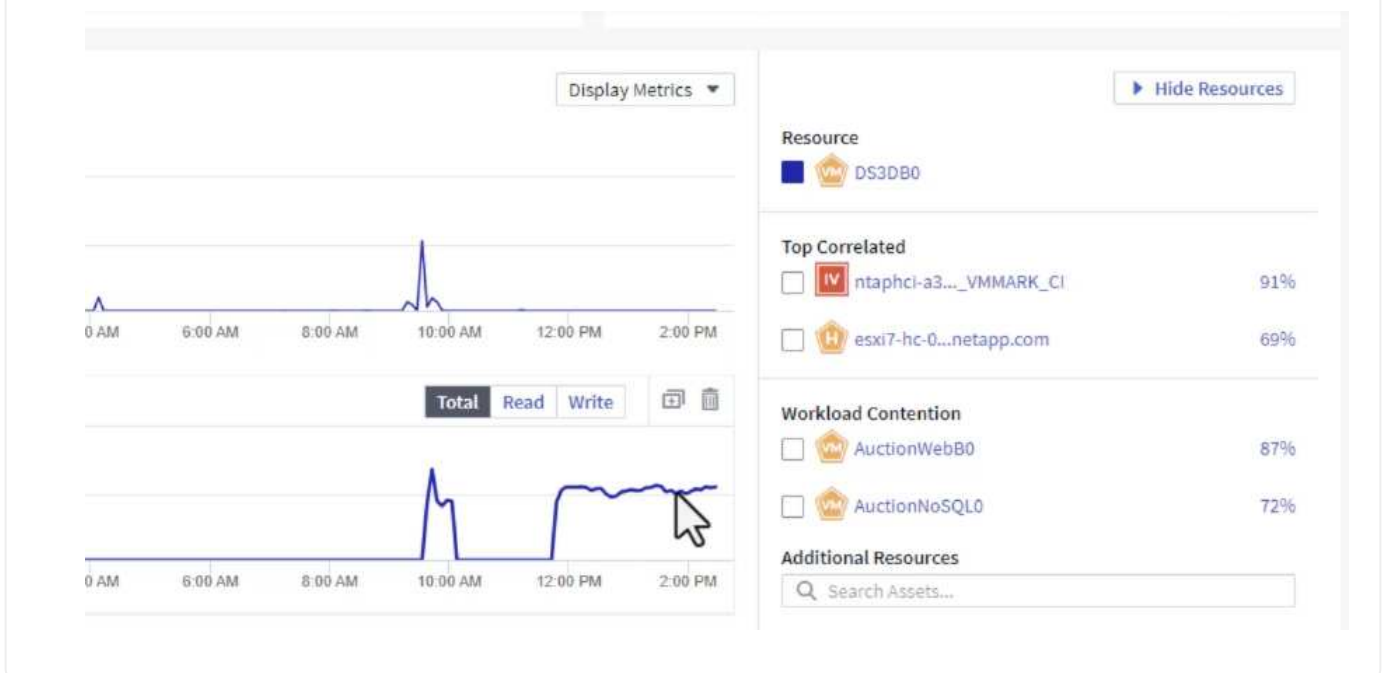
- Once imported, open the dashboard. From here you can see various widgets with detailed performance data. Add a filter to view a single storage system and select a storage volume to drill into it's details.



- 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.



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



Use Cloud Insights to identify noisy neighbors

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

Use a Top VM Latency dashboard to isolate noisy neighbors

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

NetApp PCS Sandbox / Observability / Explore / Dashboards

Dashboard Groups (108)

Search groups..

All Dashboards (3709)

My Dashboards (6)

Infrastructure Observability (2)

01_Monitoring_CI_Course_Patrick (15)

02_Monitoring_CI_Course_Vish (5)

1_Str Dashboards (8)

My Dashboards (6)

+ From Gallery

+ Dashboard

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

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

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

Last 3 Hours

VirtualMachine All

Data Center Solutions Engineering X

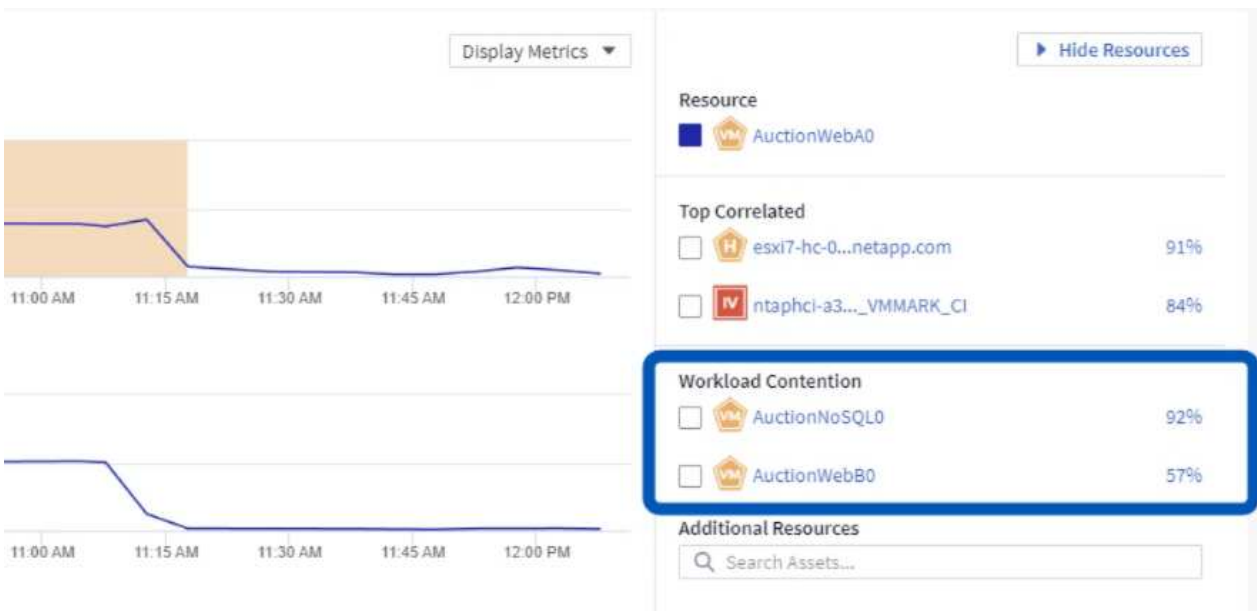
diskLatency.total ≥ All

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

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



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



View over and under utilized resources in Cloud Insights

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

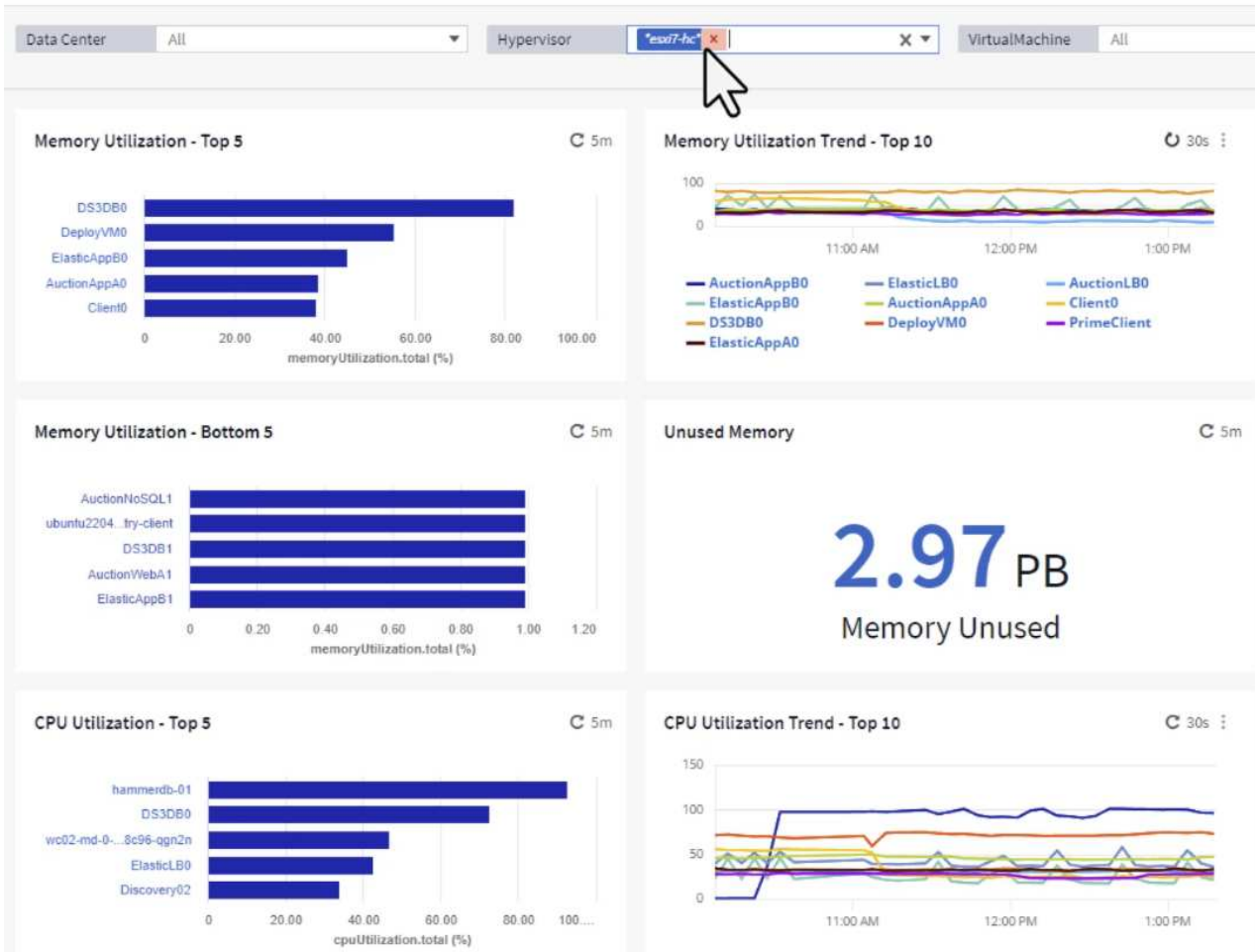
Identify opportunities to right size VMs

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

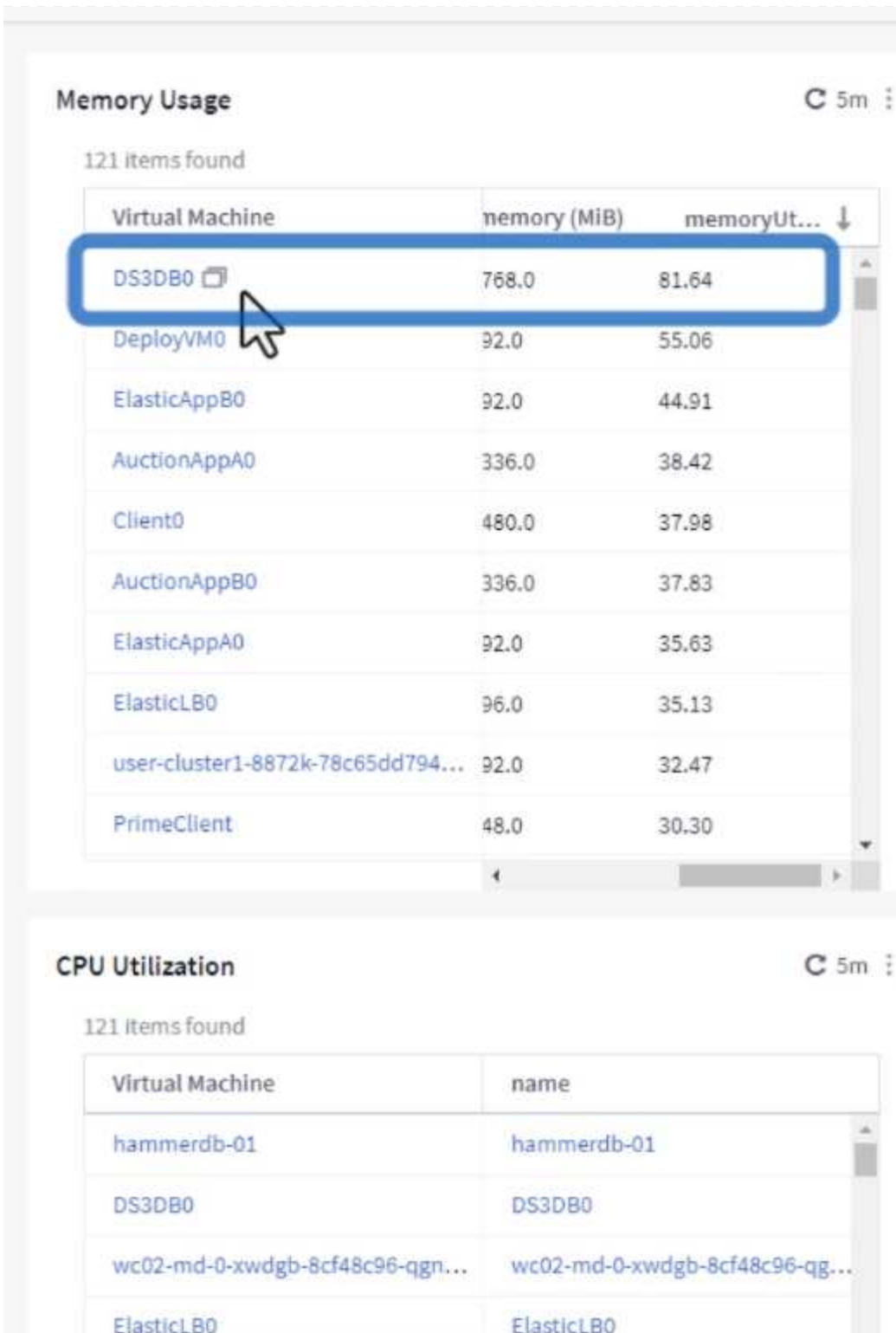
My Dashboards (6)

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

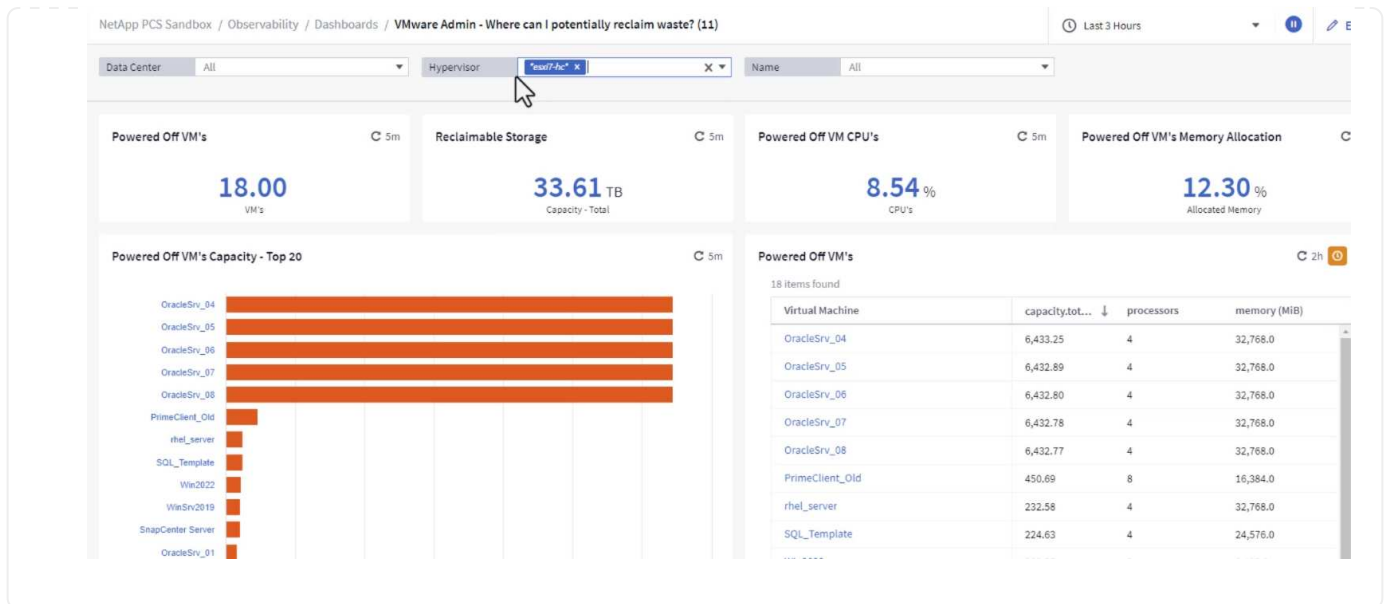
2. First filter by all of the ESXi hosts in the cluster. You can then see ranking of the top and bottom VMs by memory and CPU utilization.



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



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

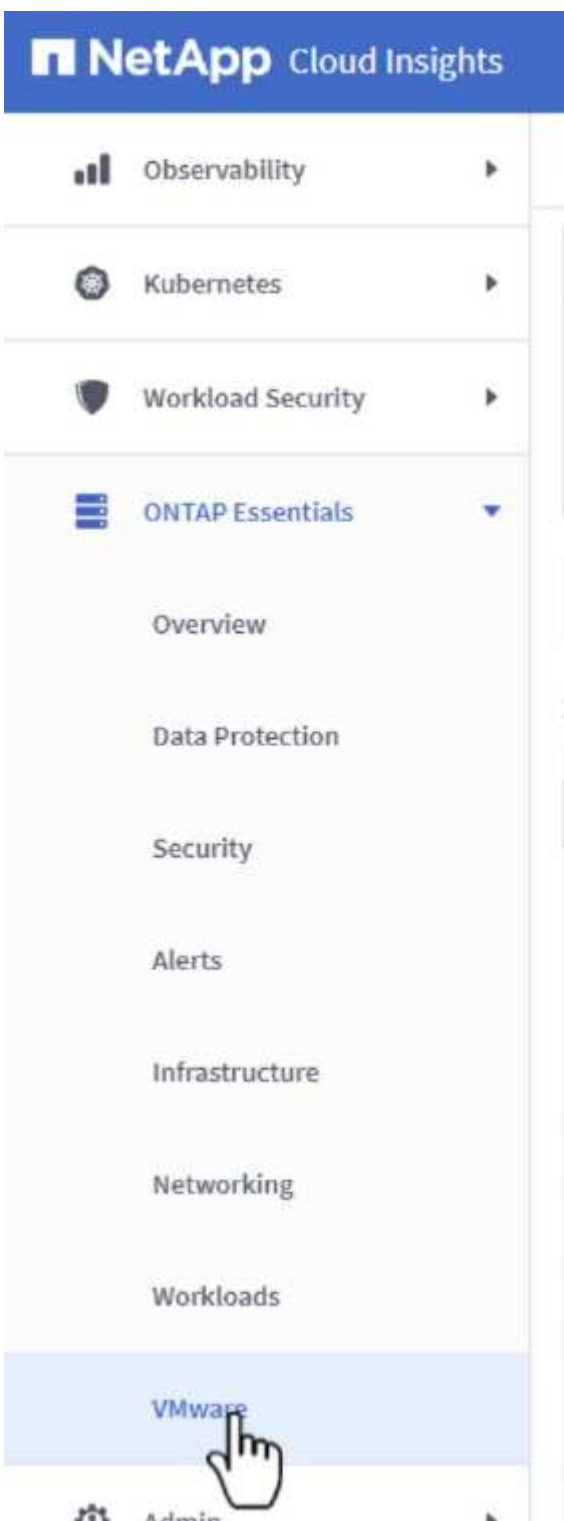


Use queries to isolate and sort metrics

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

View a detailed VMware query under ONTAP Essentials

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



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

VirtualMachine | All Virtual Machines

Filter by Attribute: storageResources.storage.vendor: NetApp | host.os: "vmware"

Filter by Metric: +

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

Conclusion

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

Additional Information

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

- [NetApp BlueXP and Data Infrastructure Insights landing page](#)
- [NetApp Data Infrastructure Insights documentation](#)

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

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

Trademark information

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