



Disaster Recovery with VMC on AWS (guest connected)

NetApp Solutions

NetApp
December 19, 2022

This PDF was generated from <https://docs.netapp.com/us-en/netapp-solutions/ehc/aws/aws-guest-dr-solution-overview.html> on December 19, 2022. Always check docs.netapp.com for the latest.

Table of Contents

- TR-4931: Disaster Recovery with VMware Cloud on Amazon Web Services and Guest Connect 1
 - TR-4931: Disaster Recovery with VMware Cloud on Amazon Web Services and Guest Connect 1
 - Technology 2
 - AWS guest-connected storage disaster recovery 5
 - Disaster recovery 21
 - Conclusion 80

TR-4931: Disaster Recovery with VMware Cloud on Amazon Web Services and Guest Connect

Chris Reno, Josh Powell, and Suresh Thoppay

A proven disaster recovery (DR) environment and plan is critical for organizations to ensure that business-critical applications can be rapidly restored in the event of a major outage. This solution focuses on demonstrating DR use cases with a focus on VMware and NetApp technologies, both on-premises and with VMware Cloud on AWS.

NetApp has a long history of integration with VMware as evidenced by the tens of thousands of customers that have chosen NetApp as their storage partner for their virtualized environment. This integration continues with guest-connected options in the cloud and recent integrations with NFS datastores as well. This solution focuses on the use case commonly referred to as guest-connected storage.

In guest-connected storage, the guest VMDK is deployed on a VMware-provisioned datastore, and application data is housed on iSCSI or NFS and mapped directly to the VM. Oracle and MS SQL applications are used to demonstrate a DR scenario, as shown in the following figure.



Next: [Technology](#).

TR-4931: Disaster Recovery with VMware Cloud on Amazon Web Services and Guest Connect

Chris Reno, Josh Powell, and Suresh Thoppay

A proven disaster recovery (DR) environment and plan is critical for organizations to ensure that business-critical applications can be rapidly restored in the event of a major outage. This solution focuses on demonstrating DR use cases with a focus on VMware and NetApp technologies, both on-premises and with VMware Cloud on AWS.

NetApp has a long history of integration with VMware as evidenced by the tens of thousands of customers that have chosen NetApp as their storage partner for their virtualized environment. This integration continues with guest-connected options in the cloud and recent integrations with NFS datastores as well. This solution focuses on the use case commonly referred to as guest-connected storage.

In guest-connected storage, the guest VMDK is deployed on a VMware-provisioned datastore, and application

data is housed on iSCSI or NFS and mapped directly to the VM. Oracle and MS SQL applications are used to demonstrate a DR scenario, as shown in the following figure.



[Next: Technology.](#)

Technology

[Previous: Solution overview.](#)

This solution includes innovative technologies from NetApp, VMware, Amazon Web Services (AWS), and Veeam.

VMware

VMware Cloud Foundation

The VMware Cloud Foundation platform integrates multiple products offerings that enable administrators to provision logical infrastructures across a heterogeneous environment. These infrastructures (known as domains) provide consistent operations across private and public clouds. Accompanying the Cloud Foundation software is a bill of materials that identifies prevalidated and qualified components to reduce risk for customers and ease deployment.

The components of the Cloud Foundation BoM include the following:

- Cloud Builder
- SDDC Manager
- VMware vCenter Server Appliance
- VMware ESXi
- VMware NSX
- vRealize Automation
- vRealize Suite Lifecycle Manager
- vRealize Log Insight

For more information on the VMware Cloud Foundation, see the [VMware Cloud Foundation documentation](#).

VMware vSphere

VMware vSphere is a virtualization platform that transforms physical resources into pools of compute, network, and storage that can be used to satisfy customers' workload and application requirements. The main components of VMware vSphere include the following:

- **ESXi.** This VMware hypervisor enables the abstraction of compute processors, memory, network, and other resources and makes them available to virtual machines and container workloads.
- **vCenter.** VMware vCenter creates a central management experience for interacting with compute resources, networking, and storage as part of your virtual infrastructure.

Customers realize the full potential of their vSphere environment by using NetApp ONTAP with deep product integration, robust support, and powerful features and storage efficiencies to create a robust hybrid multi-cloud.

For more information about VMware vSphere, follow [this link](#).

For more information about NetApp solutions with VMware, follow [this link](#).

VMware NSX

Commonly referred to as a network hypervisor, VMware NSX employs a software-defined model to connect virtualized workloads. VMware NSX is ubiquitous on premises and in VMware Cloud on AWS where it powers network virtualization and security for customer applications and workloads.

For more information on VMware NSX, follow [this link](#).

NetApp

NetApp ONTAP

NetApp ONTAP software has been a leading storage solution for VMware vSphere environments for almost two decades and continues to add innovative capabilities to simplify management while reducing costs. Using ONTAP together with vSphere is a great combination that lets you reduce host hardware and VMware software expenses. You can also protect your data at lower cost with consistent high performance while taking advantage of native storage efficiencies.

For more information on NetApp ONTAP, follow [this link](#).

NetApp ONTAP tools for VMware

ONTAP tools for VMware combine multiple plugins into a single virtual appliance that provides end-to-end lifecycle management for virtual machines in VMware environments that use NetApp storage systems. ONTAP tools for VMware includes the following:

- **Virtual Storage Console (VSC).** Performs comprehensive administrative tasks for VMs and datastores using NetApp storage.
- **VASA Provider for ONTAP.** Enables Storage Policy- Based Management (SPBM) with VMware virtual volumes (vVols) and NetApp storage.
- **Storage Replication Adapter (SRA).** Recovers vCenter datastores and virtual machines in the event of a failure when coupled with VMware Site Recovery Manager (SRM).

ONTAP tools for VMware allows users to manage not only external storage but also integrate with vVols as well as VMware Site Recovery Manager. This makes it much easier to deploy and operate NetApp storage

from within your vCenter environment.

For more information on NetApp ONTAP tools for VMware, follow [this link](#).

NetApp SnapCenter

NetApp SnapCenter software is an easy-to-use enterprise platform to securely coordinate and manage data protection across applications, databases, and file systems. SnapCenter simplifies backup, restore, and clone lifecycle management by offloading these tasks to application owners without sacrificing the ability to oversee and regulate activity on the storage systems. By leveraging storage-based data management, SnapCenter increases performance and availability as well as reducing testing and development times.

The SnapCenter Plug-in for VMware vSphere supports crash-consistent and VM-consistent backup and restore operations for virtual machines (VMs), datastores, and virtual machine disks (VMDKs). It also supports SnapCenter application-specific plug-ins to protect application-consistent backup and restore operations for virtualized databases and file systems.

For more information on NetApp SnapCenter, follow [this link](#).

Third-party data protection

Veeam Backup & Replication

Veeam Backup & Replication is a backup, recovery, and data management solution for cloud, virtual, and physical workloads. Veeam Backup & Replication has specialized integrations with NetApp Snapshot technology that further protect vSphere environments.

For more information on Veeam Backup & Replication, follow [this link](#).

Public cloud

AWS identity and access management

AWS environments contain a wide variety of products including compute, storage, database, network, analytics, and much more to help solve business challenges. Enterprises must be able to define who is authorized to access these products, services, and resources. It is equally important to determine under which conditions users are allowed to manipulate, change, or add configurations.

AWS Identity and Access Management (IAM) provides a secure control plane for managing access to AWS services and products. Properly configured users, access keys, and permissions allow for the deployment of VMware Cloud on AWS and Amazon FSx.

For more information on IAM, follow [this link](#).

VMware Cloud on AWS

VMware Cloud on AWS brings VMware's enterprise-class SDDC software to the AWS Cloud with optimized access to native AWS services. Powered by the VMware Cloud Foundation, VMware Cloud on AWS integrates VMware's compute, storage, and network virtualization products (VMware vSphere, VMware vSAN, and VMware NSX) along with VMware vCenter Server management optimized to run on dedicated, elastic, bare-metal AWS infrastructure.

For more information on VMware Cloud on AWS, follow [this link](#).

Amazon FSx for NetApp ONTAP

Amazon FSx for NetApp ONTAP is a fully featured and fully managed ONTAP system available as a native AWS service. Built on NetApp ONTAP, it offers familiar features while offering the simplicity of a fully managed cloud service.

Amazon FSx for ONTAP offers multiprotocol support to a variety of compute types including VMware in the public cloud or on premises. Available for guest-connected use cases today and NFS datastores in tech preview, Amazon FSx for ONTAP allows enterprises to take advantage of familiar features from their on-premises environments and in the cloud.

For more information on Amazon FSx for NetApp ONTAP, follow [this link](#).

Next: [Overview - AWS guest-connected storage disaster recovery](#).

AWS guest-connected storage disaster recovery

Overview - AWS guest-connected storage disaster recovery

Previous: [Technology](#).

This section provides instructions to help users verify, configure, and validate their on-premises and cloud environments for use with NetApp and VMware. Specifically, this solution is focused on the VMware guest-connected use case with ONTAP AFF on-premises and VMware Cloud and AWS FSx ONTAP for the cloud. This solution is demonstrated with two applications: Oracle and MS SQL in a disaster recovery scenario.

Next: [Requirements](#).

Requirements

Previous: [Overview - AWS guest-connected storage disaster recovery](#).

This section details the requirements to access and configure on-premises resources, VMware Cloud, and Amazon FSx ONTAP.

Skills and knowledge

The following skills and information are required to access Cloud Volumes Service for AWS:

- Access to and knowledge of your VMware and ONTAP on-premises environment.
- Access to and knowledge of VMware Cloud and AWS.
- Access to and knowledge of AWS and Amazon FSx ONTAP.
- Knowledge of your SDDC and AWS resources.
- Knowledge of the network connectivity between your on-premises and cloud resources.
- Working knowledge of disaster recovery scenarios.
- Working knowledge of applications deployed on VMware.

Administrative

Whether interacting with resources on-premises or in the cloud, users and administrators must have the ability and entitlements to provision those resources where they need them when they need according to their

entitlements. The interaction of your roles and permissions for your on-premises systems, including ONTAP and VMware, and your cloud resources, including VMware Cloud and AWS, is paramount for a successful hybrid cloud deployment.

The following administrative tasks must be in place to construct a DR solution with VMware and ONTAP on-premises and VMware Cloud on AWS and FSx ONTAP.

- Roles and accounts enabling provisioning of the following:
 - ONTAP storage resources
 - VMware VMs, datastores, and so on
 - AWS VPC and security groups
- Provisioning of on-premises VMware environment and ONTAP
- VMware Cloud environment
- An Amazon FSx for ONTAP file system
- Connectivity between your on-premises environment and AWS
- Connectivity for your AWS VPC

On-premises

The VMware virtual environment includes licensing of ESXi hosts, VMware vCenter Server, NSX networking, and other components, as can be seen in the following figure. All are licensed differently, and it is important to understand how the underlying components consume the available licensed capacity.



ESXi hosts

Compute hosts in a VMware environment are deployed with ESXi. When licensed with vSphere at various capacity tiers, virtual machines can take advantage of the physical CPUs on each host and applicable entitled features.

VMware vCenter

Managing ESXi hosts and storage is one of the many capabilities made available to the VMware administrator with vCenter Server. As of VMware vCenter 7.0, there are three editions of VMware vCenter available, depending on the license:

- vCenter Server Essentials
- vCenter Server Foundation
- vCenter Server Standard

VMware NSX

VMware NSX provides administrators with the flexibility required to enable advanced features. Features are enabled depending upon the version of NSX-T Edition that is licensed:

- Professional
- Advanced
- Enterprise Plus
- Remote Office/Branch Office

NetApp ONTAP

Licensing with NetApp ONTAP refers to how administrators gain access to various capabilities and features within NetApp storage. A license is a record of one or more software entitlements. Installing license keys, also known as license codes, enables you to use certain features or services on your storage system. For instance, ONTAP supports all major industry-standard client protocols (NFS, SMB, FC, FCoE, iSCSI, and NVMe/FC) through licensing.

Data ONTAP feature licenses are issued as packages, each of which contains multiple features or a single feature. A package requires a license key, and installing the key enables you to access all features in the package.

License types are as follows:

- **Node-locked license.** Installing a node-locked license entitles a node to the licensed functionality. For the cluster to use the licensed functionality, at least one node must be licensed for the functionality.
- **Master/site license.** A master or site license is not tied to a specific system serial number. When you install a site license, all the nodes in the cluster are entitled to the licensed functionality.
- **Demo/temporary license.** A demo or temporary license expires after a certain time. This license enables you to try certain software functionality without purchasing an entitlement.
- **Capacity license (ONTAP Select and FabricPool only).** An ONTAP Select instance is licensed according to the amount of data that the user wants to manage. Starting with ONTAP 9.4, FabricPool requires a capacity license to be used with a third-party storage tier (for example, AWS).

NetApp SnapCenter

SnapCenter requires several licenses to enable data protection operations. The type of SnapCenter licenses you install depends on your storage environment and the features that you want to use. The SnapCenter Standard license protects applications, databases, files systems, and virtual machines. Before you add a storage system to SnapCenter, you must install one or more SnapCenter licenses.

To enable the protection of applications, databases, file systems, and virtual machines, you must have either a Standard controller-based license installed on your FAS or AFF storage system or a Standard capacity-based license installed on your ONTAP Select and Cloud Volumes ONTAP platforms.

See the following SnapCenter Backup prerequisites for this solution:

- A volume and SMB share created on the on-premises ONTAP system to locate the backed- up database and configuration files.
- A SnapMirror relationship between the on-premises ONTAP system and FSx or CVO in the AWS account. Used for transporting the snapshot containing the backed up SnapCenter database and configuration files.
- Windows Server installed in the cloud account, either on an EC2 instance or on a VM in the VMware Cloud SDDC.
- SnapCenter installed on the Windows EC2 instance or VM in VMware Cloud.

MS SQL

As part of this solution validation, we use MS SQL to demonstrate disaster recovery.

For more information regarding best practices with MS SQL and NetApp ONTAP, follow [this link](#).

Oracle

As part of this solution validation, we use ORACLE to demonstrate disaster recovery. For more information regarding best practices with ORACLE and NetApp ONTAP, follow [this link](#).

Veeam

As part of this solution validation, we use Veeam to demonstrate disaster recovery. For more information regarding best practices with Veeam and NetApp ONTAP, follow [this link](#).

Cloud

AWS

You must be able to perform the following tasks:

- Deploy and configure domain services.
- Deploy FSx ONTAP per application requirements in a given VPC.
- Configure VMware Cloud on the AWS Compute gateway to allow for traffic from FSx ONTAP.
- Configure an AWS security group to allow communication between the VMware Cloud on AWS subnets to the AWS VPC subnets where FSx ONTAP service is deployed.

VMware Cloud

You must be able to perform the following tasks:

- Configure the VMware Cloud on AWS SDDC.

Cloud Manager account verification

You must be able to deploy resources with NetApp Cloud Manager. To verify that you can, complete the following tasks:

- [Sign up for Cloud Central](#) if you haven't already.
- [Log into Cloud Manager](#).
- [Set up Workspaces and Users](#).
- [Create a connector](#).

Amazon FSx for NetApp ONTAP

You must be able to perform the following task after you have an AWS account:

- Create an IAM administrative user capable of provisioning Amazon FSx for the NetApp ONTAP file system.

Configuration prerequisites

Given the varying topologies that customers have, this section focuses on the ports necessary to enable communication from on-premises to cloud resources.

Required ports and firewall considerations

The following tables describe the ports that must be enabled throughout your infrastructure.

For a more comprehensive list of required ports for Veeam Backup & Replication software, follow [this link](#).

For a more comprehensive list of port requirements for SnapCenter, follow [this link](#).

The following table lists the Veeam port requirements for Microsoft Windows Server.

From	To	Protocol	Port	Notes
Backup server	Microsoft Windows server	TCP	445	Port required for deploying Veeam Backup & Replication components.
Backup proxy		TCP	6160	Default port used by the Veeam Installer Service.
Backup repository		TCP	2500 to 3500	Default range of ports used as data transmission channels and for collecting log files.
Mount server		TCP	6162	Default port used by the Veeam Data Mover.



For every TCP connection that a job uses, one port from this range is assigned.

The following table lists the Veeam port requirements for Linux Server.

From	To	Protocol	Port	Notes
Backup server	Linux server	TCP	22	Port used as a control channel from the console to the target Linux host.

From	To	Protocol	Port	Notes
		TCP	6162	Default port used by the Veeam Data Mover.
		TCP	2500 to 3500	Default range of ports used as data transmission channels and for collecting log files.



For every TCP connection that a job uses, one port from this range is assigned.

The following table lists the Veeam Backup Server port requirements.

From	To	Protocol	Port	Notes
Backup server	vCenter Server	HTTPS, TCP	443	Default port used for connections to vCenter Server. Port used as a control channel from the console to the target Linux host.
	Microsoft SQL Server hosting the Veeam Backup & Replication configuration database	TCP	1443	Port used for communication with Microsoft SQL Server on which the Veeam Backup & Replication configuration database is deployed (if you use a Microsoft SQL Server default instance).
	DNS Server with name resolution of all backup servers	TCP	3389	Port used for communication with the DNS Server



If you use vCloud Director, make sure to open port 443 on underlying vCenter Servers.

The following table lists Veeam Backup Proxy port requirements.

From	To	Protocol	Port	Notes
Backup server	Backup proxy	TCP	6210	Default port used by the Veeam Backup VSS Integration Service for taking a VSS snapshot during the SMB file share backup.
Backup proxy	vCenter Server	TCP	1443	Default VMware web service port that can be customized in vCenter settings.

The following table lists SnapCenter port requirements.

Port Type	Protocol	Port	Notes
SnapCenter management port	HTTPS	8146	This port is used for communication between the SnapCenter client (the SnapCenter user) and the SnapCenter Server. Also used for communication from the plug-in hosts to the SnapCenter Server.
SnapCenter SMCore communication port	HTTPS	8043	This port is used for communication between the SnapCenter Server and the hosts where the SnapCenter plug-ins are installed.
Windows plug-in hosts, installation	TCP	135, 445	These ports are used for communication between the SnapCenter Server and the host where the plug-in is being installed. The ports can be closed after installation. In addition, Windows Instrumentation Services searches ports 49152 through 65535, which must be open.

Port Type	Protocol	Port	Notes
Linux plug-in hosts, installation	SSH	22	These ports are used for communication between the SnapCenter Server and the host where the plug-in is being installed. The ports are used by SnapCenter to copy plug-in package binaries to Linux plug-in hosts.
SnapCenter Plug-ins Package for Windows / Linux	HTTPS	8145	This port is used for communication between SMCORE and hosts where the SnapCenter plug-ins are installed.
VMware vSphere vCenter Server port	HTTPS	443	This port is used for communication between the SnapCenter Plug-in for VMware vSphere and vCenter server.
SnapCenter Plug-in for VMware vSphere port	HTTPS	8144	This port is used for communication from the vCenter vSphere web client and from the SnapCenter Server.

[Next: Networking.](#)

Networking

[Previous: Requirements.](#)

This solution requires successful communication from the on-premises ONTAP cluster to AWS FSx for NetApp ONTAP interconnect cluster network addresses to perform NetApp SyncMirror operations. Also, a Veeam backup server must have access to an AWS S3 bucket. Instead of using Internet transport, an existing VPN or Direct Connect link can be used as a private link to an S3 bucket.

On premises

ONTAP supports all major storage protocols used for virtualization, including iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), or Non-Volatile Memory Express over Fibre Channel (NVMe/FC) for SAN environments. ONTAP also supports NFS (v3 and v4.1) and SMB or S3 for guest connections. You are free to pick what works best for your environment, and you can combine protocols as needed on a single system. For example, you can augment general use of NFS datastores with a few iSCSI LUNs or guest shares.

This solution leverages NFS datastores for on-premises datastores for guest VMDKs and both iSCSI and NFS for guest application data.

Client networks

VMkernel network ports and software-defined networking provide connectivity to ESXi hosts allowing them to communicate with elements outside the VMware environment. Connectivity depends on the type of VMkernel

interfaces used.

For this solution, the following VMkernel interfaces were configured:

- Management
- vMotion
- NFS
- iSCSI

Storage networks provisioned

A LIF (logical interface) represents a network access point to a node in the cluster. This allows communication with the storage virtual machines that house the data accessed by clients. You can configure LIFs on ports over which the cluster sends and receives communications over the network.

For this solution, LIFs are configured for the following storage protocols:

- NFS
- iSCSI

Cloud connectivity options

Customers have a lot of options when connecting their on-premises environment to cloud resources, including deploying VPN or Direct Connect topologies.

Virtual Private Network (VPN)

VPNs (Virtual Private Networks) are often used to create a secure IPSec tunnel with internet-based or private MPLS networks. A VPN is easy to set up, but it lacks reliability (if internet-based) and speed. The end point can be terminated at the AWS VPC or at the VMware Cloud SDDC. For this disaster recovery solution, we created connectivity to AWS FSx for NetApp ONTAP from the on-premises network. So, it can be terminated at the AWS VPC (Virtual Private Gateway or Transit Gateway) where FSx for NetApp ONTAP is connected.

VPN setup can be route-based or policy-based. With a route-based setup, the endpoints exchange the routes automatically and setup learns the route to the newly created subnets. With a policy-based setup, you must define the local and remote subnets, and, when new subnets are added and allowed to communicate in the IPSec tunnel, you must update the routes.



If the IPSec VPN tunnel is not created on the default gateway, remote network routes must be defined in route tables via the local VPN tunnel end point.

The following figure depicts typical VPN connection options.



Direct Connect

Direct Connect provides a dedicated link to the AWS network. Dedicated connections create links to AWS using a 1Gbps, 10Gbps, or 100Gbps Ethernet port. AWS Direct Connect partners provide hosted connections using pre-established network links between themselves and AWS and are available from 50Mbps up to 10Gbps. By default, the traffic is unencrypted. However, options are available to secure traffic with MACsec or IPsec. MACsec provides layer-2 encryption while IPsec provides layer-3 encryption. MACsec provides better security by concealing which devices are communicating.

Customers must have their router equipment in an AWS Direct Connect location. To set this up, you can work with AWS Partner Network (APN). A physical connection is made between that router and the AWS router. To enable access to FSx for NetApp ONTAP on VPC, you must have either a private virtual interface or a transit virtual interface from Direct Connect to a VPC. With a private virtual interface, the Direct Connect to VPC connection scalability is limited.

The following figure depicts the Direct Connect interface options.



Transit gateway

The transit gateway is a region-level construct that allows increased scalability of a Direct Connect-to-VPC connection within a region. If a cross-region connection is required, the transit gateways must be peered. For more information, check the [AWS Direct Connect documentation](#).

Cloud network considerations

In the cloud, the underlying network infrastructure is managed by the cloud service provider, whereas customers must manage the VPC networks, subnets, route tables, and so on in AWS. They must also manage NSX network segments at the compute edge. SDDC groups routes for the external VPC and Transit Connect.

When FSx for NetApp ONTAP with Multi-AZ availability is deployed on a VPC connected to VMware Cloud, iSCSI traffic receives necessary route table updates to enable communication. By default, there is no route available from VMware Cloud to the FSx ONTAP NFS/SMB subnet on the connected VPC for Multi-AZ deployment. To define that route, we used the VMware Cloud SDDC group, which is a VMware-managed transit gateway, to allow communication between the VMware Cloud SDDCs in the same region as well as to external VPCs and other transit gateways.



There are data transfer costs associated with using a transit gateway. For cost details specific to a region, see [this link](#).

VMware Cloud SDDC can be deployed in a single availability zone, which is like having a single datacenter. A stretch cluster option is also available, which is like a NetApp MetroCluster solution that can provide higher availability and reduced downtime in case of availability-zone failure.

To minimize data-transfer cost, keep the VMware Cloud SDDC and AWS Instances or services in the same availability zone. It is better to match with an availability zone ID rather than with a name because AWS provides the AZ order list specific to the account to spread the load across availability zones. For example, one account (US-East-1a) might point to AZ ID 1 whereas another account (US-East-1c) might point to AZ ID 1. The availability zone ID can be retrieved in several ways. In the following example, we retrieved the AZ ID from the VPC subnet.

VPC > Subnets > subnet-04f5fe7073ff514fb

subnet-04f5fe7073ff514fb / priv-subnet-01 Actions ▾

Details

Subnet ID

Available IPv4 addresses

97

Network border group

us-east-1

Default subnet

No

Customer-owned IPv4 pool

-

IPv6-only

No

DNS64

Disabled

Subnet ARN

IPv6 CIDR

-

VPC

Auto-assign public IPv4 address

No

Outpost ID

-

Hostname type

IP name

Owner

State

Available

Availability Zone

us-east-1a

Route table

rtb-08c08b5db175cded2

Auto-assign IPv6 address

No

IPv4 CIDR reservations

-

Resource name DNS A record

Disabled

IPv4 CIDR

172.30.15.0/25

Availability Zone ID

use1-az6

Network ACL

acl-0b7f41adaade25077

Auto-assign customer-owned IPv4 address

No

IPv6 CIDR reservations

-

Resource name DNS AAAA record

Disabled

In the VMware Cloud SDDC, networking is managed with NSX, and the edge gateway (Tier-0 router) that handles the north-south traffic uplink port is connected to the AWS VPC. The compute gateway and the management gateways (Tier-1 routers) handle east-west traffic. If the uplink ports of the edge becomes heavily used, you can create traffic groups to associate with specific host IPs or subnets. Creation of a traffic group creates additional edge nodes to separate the traffic. Check the [VMware documentation](#) on the minimum number of vSphere hosts required to use a multi-edge setup.

Client networks

When you provision the VMware Cloud SDDC, VMKernel ports are already configured and are ready for consumption. VMware manages those ports and there is no need to make any updates.

The following figure depicts sample Host VMKernel info.

VMkernel adapters

ADD NETWORKING... REFRESH

	Device	Network Label	Switch	IP Address	TCP/IP Stack	Enabled Services
⋮ >>	vmk0	o-vmk0-ls	vmc-hostswitch	172.30.160.68	Default	Management
⋮ >>	vmk1	VSAN	vmc-hostswitch	172.30.160.4	Default	vSAN
⋮ >>	vmk2	VMOTION	vmc-hostswitch	172.30.160.36	vMotion	vMotion
⋮ >>	vmk3	vmcd-backplane-ls	vmc-hostswitch	169.252.32.4	api	--
⋮ >>	vmk4	vmk4-ls	vmc-hostswitch	172.30.160.196	api	--
⋮ >>	vmk10	--	vmc-hostswitch	172.30.160.100	nsx-overlay	--
⋮ >>	vmk50	--	vmc-hostswitch	169.254.1.1	nsx-hyperbus	--

Storage networks provisioned (iSCSI, NFS)

For VM guest storage networks, we typically create port groups. With NSX, we create segments that are consumed on vCenter as port groups. Because storage networks are in a routable subnet, you can access the LUNs or mount the NFS exports using the default NIC even without creating separate network segments. To separate storage traffic, you can create additional segments, define rules, and control the MTU size on those segments. To provide fault tolerance, it is better to have at least two segments dedicated for the storage network. As we mentioned previously, if uplink bandwidth becomes an issue, you can create traffic groups and assign IP prefixes and gateways to perform source-based routing.

We recommend matching the segments in the DR SDDC with the source environment to prevent guessing of

mapping network segments during failover.

Security groups

Many security options provide secure communication on the AWS VPC and the VMware Cloud SDDC network. Within the VMware Cloud SDDC network, you can use NSX trace flow to identify the path, including the rules used. Then, you can use a network analyzer on the VPC network to identify the path, including the route tables, security groups, and network access control lists, that is consumed during the flow.

[Next: Storage.](#)

Storage

[Previous: Networking.](#)

NetApp AFF A-Series systems deliver a high-performance storage infrastructure with flexible data management options that are cloud enabled to meet a wide variety of enterprise scenarios. In this solution, we used an ONTAP AFF A300 as our primary on-premises storage system.

NetApp ONTAP together with ONTAP Tools for VMware and SnapCenter were used in the solution to provide comprehensive management and application backup capabilities that are tightly integrated with VMware vSphere.

On-premises

We used ONTAP storage for the VMware datastores that hosted the virtual machines and their VMDK files. VMware supports multiple storage protocols for connected datastores, and, in this solution, we used NFS volumes for datastores on the ESXi hosts. However, ONTAP storage systems support all protocols supported by VMware.

The following figure depicts VMware storage options.



ONTAP volumes were used for both iSCSI and NFS guest-connected storage for our application VMs. We used the following storage protocols for application data:

- NFS volumes for guest connected Oracle database files.
- iSCSI LUNs for guest connected Microsoft SQL Server databases and transaction logs.

Operating system	Database type	Storage protocol	Volume description
Windows Server 2019	SQL Server 2019	iSCSI	Database files
		iSCSI	Log files
Oracle Linux 8.5	Oracle 19c	NFS	Oracle binary
		NFS	Oracle data
		NFS	Oracle recovery files

We also used ONTAP storage for the primary Veeam backup repository as well as for a backup target for the SnapCenter database backups.

- SMB share for the Veeam backup repository.
- SMB share as a target for the SnapCenter database backups.

Cloud storage

This solution includes VMware Cloud on AWS for hosting virtual machines that are restored as a part of the failover process. As of this writing, VMware supports vSAN storage for the datastores that host the VMs and VMDKs.

FSx for ONTAP is used as the secondary storage for application data that is mirrored using SnapCenter and SyncMirror. As a part of the failover process, the FSx for ONTAP cluster is converted to primary storage, and the database applications can resume normal function running on the FSx storage cluster.

Amazon FSx for NetApp ONTAP setup

To deploy AWS FSx for NetApp ONTAP using Cloud Manager, follow the instructions at [this link](#).

After FSx ONTAP is deployed, drag and drop the on-premises ONTAP instances into FSx ONTAP to start replication setup of volumes.

The following figure depicts our FSx ONTAP environment.



Network interfaces created

FSx for NetApp ONTAP has network interfaces preconfigured and ready to use for iSCSI, NFS, SMB, and inter-cluster networks.

VM datastore storage

The VMware Cloud SDDC comes with two VSAN datastores named `vsandatastore` and `workloaddatastore`. We used `vsandatastore` to host management VMs with access restricted to `cloudadmin` credential. For workloads, we used `workloaddatastore`.

Next: [Compute](#).

Compute

[Previous: Storage.](#)

VMware vSphere provides virtualized infrastructure in the datacenter and across all the major cloud providers. This ecosystem is ideal for disaster recovery scenarios for which virtualized compute stays consistent regardless of location. This solution uses VMware virtualized compute resources at both the datacenter location and in the VMware Cloud on AWS.

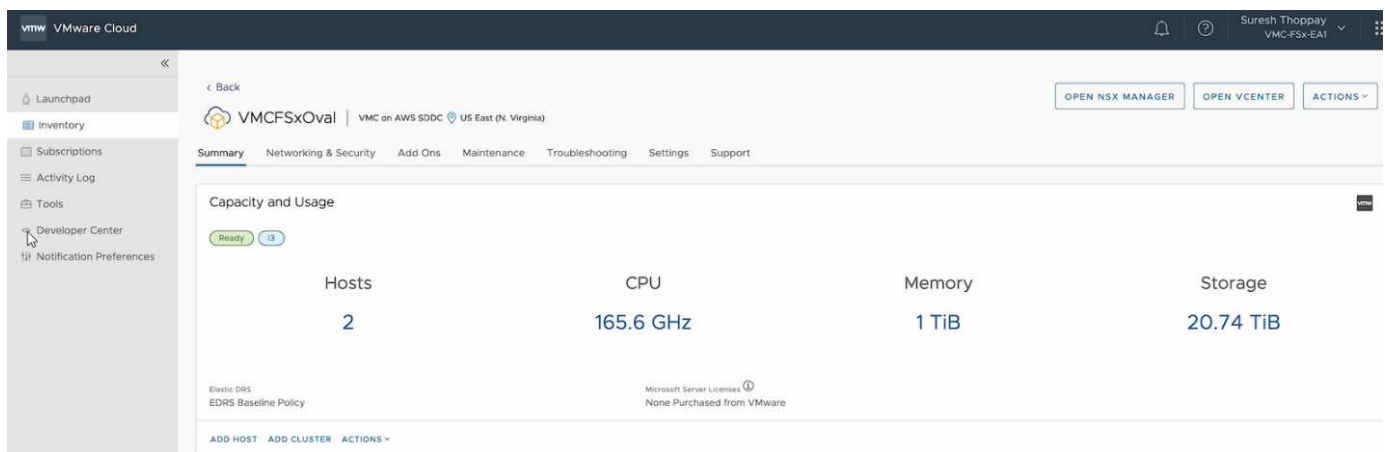
On-premises

This solution uses HPE Proliant DL360 Gen 10 Servers running VMware vSphere v7.0U3. We deployed six compute instances to provide adequate resources for our SQL server and Oracle servers.

We deployed 10 Windows Server 2019 VMs running SQL Server 2019 with varying database sizes and 10 Oracle Linux 8.5 VMs running Oracle 19c, again, with varying database sizes.

Cloud

We deployed an SDDC in VMware Cloud on AWS with two hosts to provide adequate resources to run the virtual machines restored from our primary site.



[Next: Cloud Backup Tools.](#)

Cloud Backup Tools

[Previous: Compute.](#)

To conduct a failover of our application VMs and database volumes to VMware Cloud Volume services running in AWS, it was necessary to install and configure a running instance of both SnapCenter Server and Veeam Backup and Replication Server. After failover is complete, these tools must also be configured to resume normal backup operations until a failback to the on-premises datacenter is planned and executed.

Deployment of backup tools

SnapCenter server and Veeam Backup & Replication server can be installed in the VMware Cloud SDDC or they can be installed on EC2 instances residing in a VPC with network connectivity to the VMware Cloud environment.

SnapCenter Server

SnapCenter software is available from the NetApp support site and can be installed on Microsoft Windows systems that reside either in a Domain or Workgroup. A detailed planning guide and installation instructions can be found at the [NetApp documentation center](#).

The SnapCenter software can be found at [this link](#).

Veeam Backup & Replication server

You can install the Veeam Backup & Replication server on a Windows server in VMware Cloud on AWS or on an EC2 instance. For detailed implementation guidance, see the [Veeam Help Center Technical Documentation](#).

Backup tools and configuration

After they are installed, SnapCenter and Veeam Backup & Replication must be configured to perform the necessary tasks to restore data to VMware Cloud on AWS.

SnapCenter configuration

To restore application data that has been mirrored to FSx ONTAP, you must first perform a full restore of the on-premises SnapCenter database. After this process is complete, communication with the VMs is reestablished and application backups can now resume using FSx ONTAP as primary storage.

For a list of steps to be completed on the SnapCenter Server residing in AWS, see the section [Deploy Secondary Windows SnapCenter Server](#).

Veeam Backup & Replication configuration

To restore virtual machines that have been backed up to Amazon S3 storage, the Veeam Server must be installed on a Windows server and configured to communicate with VMware Cloud, FSx ONTAP, and the S3 bucket that contains the original backup repository. It must also have a new backup repository configured on FSx ONTAP to conduct new backups of the VMs once they are restored.

For a complete list of steps required to complete failover of the application VMs, see the section [Deploy Secondary Veeam Backup & Replication Server](#).

Next: [Overview - Disaster recovery](#).

Disaster recovery

Overview - Disaster recovery

[Previous: Cloud Backup Tools](#).

In this solution, SnapCenter provides application-consistent snapshots for SQL Server and Oracle application data. This configuration, together with SnapMirror technology, provides high-speed data replication between our on-premises AFF and FSx ONTAP cluster. Additionally, Veeam Backup & Replication provides backup and restore capabilities for our virtual machines.

In this section, we cover the configuration of SnapCenter, SnapMirror, and Veeam for both backup and restore.

The following sections cover configuration and the steps needed to complete a failover at the secondary site:

- Configure SnapMirror and retention schedules (secondary storage).
- Deploy and configure Windows SnapCenter server on-premises.
- Deploy and configure Veeam Backup & Replication server on-premises.
- Deploy and configure cloud backup tools, SnapCenter, and Veeam.
- SnapCenter database backup for disaster recovery.
- SnapCenter database restore at a secondary site.
- Restore application virtual machines using Veeam Backup & Replication.
- Restore SQL Server application data.
- Restore Oracle application data.

[Next: Configure SnapMirror relationships and retention schedules.](#)

Configure SnapMirror relationships and retention schedules

[Previous: Overview - Disaster recovery.](#)

SnapCenter can update SnapMirror relationships within the primary storage system (primary > mirror) and to secondary storage systems (primary > vault) for the purpose of long-term archiving and retention. To do so, you must establish and initialize a data replication relationship between a destination volume and a source volume using SnapMirror.

The source and destination ONTAP systems must be in networks that are peered using Amazon VPC peering, a transit gateway, AWS Direct Connect, or an AWS VPN.

The following steps are required for setting up SnapMirror relationships between an on-premises ONTAP system and FSx ONTAP:

- Record the source and destination intercluster logical interfaces.
- Establish cluster peering between ONTAP and FSx.
- Establish an SVM peering relationship.
- Create a snapshot retention policy.
- Create the destination volume in FSx.
- Create the SnapMirror relationships between source and destination volumes.
- Initialize SnapMirror relationships.

Refer to the [FSx for ONTAP – ONTAP User Guide](#) for more information on creating SnapMirror relationships with FSx.

Record the source and destination Intercluster logical interfaces

For the source ONTAP system residing on-premises, 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
veeam_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_3	a0a-181			Intercluster, Cluster/Node Mgmt	0
lif_ora_vvm_014	✓	ora_vvm	Default	10.61.181.185	E13A300_1	a0a-181		SMB/CIFS, NFS, FL...	Data	0

- To retrieve the Intercluster IP addresses for FSx, log into the CLI and run the following command:

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

```

FsxId0ae40e08acc0dea67::> network interface show -role intercluster
Vserver      Logical      Status      Network      Current      Current      Is
Interface    Admin/Oper   Address/Mask Node          Port         Home
-----
FsxId0ae40e08acc0dea67
inter_1      up/up       172.30.15.42/25  FsxId0ae40e08acc0dea67-01
                                     e0e         true
inter_2      up/up       172.30.14.28/26  FsxId0ae40e08acc0dea67-02
                                     e0e         true
2 entries were displayed.

```

Establish cluster peering between ONTAP and FSx

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

- Set up peering on the destination FSx 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.

```

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

```

- 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.

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 v

PROTECTION ^

- Overview 1
- Relationships

HOSTS v

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 2

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 FSx cluster.
 - b. Select **Yes** to establish an encrypted relationship.
 - c. Enter the intercluster LIF IP address(es) of the destination FSx cluster.

d. Click Initiate Cluster Peering to finalize the process.

The screenshot shows the 'Peer Cluster' configuration window. On the left, under 'Local', there is a 'STORAGE VM PERMISSIONS' section with a dropdown menu set to 'All storage VMs (incl... X)' and a note: 'Storage VMs created in the future also will be given permissions.' On the right, under 'Remote', there are three main steps indicated by red callouts: 1. A 'PASSPHRASE' field with a question mark icon and a red box around it. Below it, a red warning message states: 'It cannot be determined from the passphrase whether this relationship was encrypted. Is the relationship encrypted?'. 2. Two buttons, 'Yes' and 'No', with the 'Yes' button highlighted by a red box. 3. A section titled 'Intercluster Network Interfaces IP Addresses' containing two IP addresses: '172.30.15.42' and '172.30.14.28' (the latter is highlighted with a blue box). Below the list is a '+ Add' button and a 'Cancel' button. At the bottom left, a red callout 4 points to the 'Initiate Cluster Peering' button, which is highlighted with a red box. A 'Cancel' button is also present at the bottom right.

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

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

```
FSxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name      Cluster Serial Number Availability  Authentication
-----
E13A300                1-80-000011    Available   ok
```

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 source FSx cluster, use the following command from the CLI to create the SVM peer relationship:

```
FSx-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.

```
FSx-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.

```
FSx-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:

```
FSx-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 FSx that will be the recipient of snapshot copies from our source volumes, run the following command on FSx ONTAP:

```
FSx-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 FSx ONTAP:

```
FSx-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 FSx ONTAP:

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

[Next: Deploy and configure Windows SnapCenter Server on premises.](#)

Deploy and configure Windows SnapCenter Server on premises

[Previous: Configure SnapMirror relationships and retention schedules.](#)

Deploy Windows SnapCenter Server on premises

This solution uses NetApp SnapCenter to take application-consistent backups of SQL Server and Oracle databases. In conjunction with Veeam Backup & Replication for backing up virtual machine VMDKs, this provides a comprehensive disaster recovery solution for on-premises and cloud-based datacenters.

SnapCenter software is available from the NetApp support site and can be installed on Microsoft Windows

systems that reside either in a domain or workgroup. A detailed planning guide and installation instructions can be found at the [NetApp Documentation Center](#).

The SnapCenter software can be obtained at [this link](#).

After it is installed, you can access the SnapCenter console from a web browser using https://Virtual_Cluster_IP_or_FQDN:8146.

After you log into the console, you must configure SnapCenter for backup SQL Server and Oracle databases. To do so, complete the following high-level steps:

1. Add storage controllers that contain volumes hosting application data.
2. Add host systems to be backed up with SnapCenter.
3. Configure policies that specify backup parameters and schedules.
4. Configure resource groups that contain resources to be backed up and policies used for the backups.

Add storage controllers to SnapCenter

To add storage controllers to SnapCenter, complete the following steps:

1. From the left menu, select Storage Systems and then click New to begin the process of adding your storage controllers to SnapCenter.



The screenshot shows the NetApp SnapCenter web interface. The left sidebar contains a navigation menu with options: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems (highlighted), Settings, and Alerts. The main content area is titled 'ONTAP Storage'. It includes a 'Type' dropdown set to 'ONTAP SVMs', a 'Search by Name' input field, and a 'New' button (a blue square with a white plus sign) highlighted by a red box. Below this is a table titled 'ONTAP Storage Connections' with columns: Name, IP, Cluster Name, User Name, Platform, and Controller License. The table lists several storage systems, including 'Backup', 'FS02', 'ora_svm', 'ora_svm_dest', 'sql_svm', 'sql_svm_dest', and 'svm_HCApps'.

	Name	IP	Cluster Name	User Name	Platform	Controller License
<input type="checkbox"/>	Backup	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	FS02	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	ora_svm	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	ora_svm_dest		172.30.15.42		AFF	Not applicable
<input type="checkbox"/>	sql_svm	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	sql_svm_dest		172.30.15.42		AFF	Not applicable
<input type="checkbox"/>	svm_HCApps		172.30.15.42		AFF	Not applicable

2. In the Add Storage System dialog box, add the management IP address for the local on-premises ONTAP cluster and the username and password. Then click Submit to begin discovery of the storage system.

Add Storage System

Add Storage System

Storage System

10.61.181.180

Username

admin

Password

●●●●●●●●

Event Management System (EMS) & AutoSupport Settings

☒ Send AutoSupport notification to storage system

☒ Log SnapCenter Server events to syslog

 **More Options** : Platform, Protocol, Preferred IP etc..

Submit

Cancel

Reset

3. Repeat this process to add the FSx ONTAP system to SnapCenter. In this case, select More Options at the bottom of the Add Storage System window and click the check box for Secondary to designate the FSx system as the secondary storage system updated with SnapMirror copies or our primary backup snapshots.

More Options

Platform

FAS

Protocol

HTTPS

Port

443

Timeout

60

seconds

☐ Preferred IP

Save

Cancel

☒ Secondary

For more information related to adding storage systems to SnapCenter, see the documentation at [this link](#).

Add hosts to SnapCenter

The next step is adding host application servers to SnapCenter. The process is similar for both SQL Server and Oracle.

1. From the left menu, select Hosts and then click Add to begin the process of adding storage controllers to SnapCenter.
2. In the Add Hosts window, add the Host Type, Hostname, and the host system Credentials. Select the plug-in type. For SQL Server, select the Microsoft Windows and Microsoft SQL Server plug-in.

NetApp SnapCenter®

Managed Hosts

Search by Name

	Name
<input type="checkbox"/>	oraclesrv_01.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_02.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_03.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_04.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_05.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_06.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_07.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_08.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_09.sddc.netapp.com
<input type="checkbox"/>	oraclesrv_10.sddc.netapp.com

Add Host

Host Type: Windows

Host Name: sqlsrv-01.sddc.netapp.com

Credentials: sddc-jpowell

Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Windows

- ☒ Microsoft Windows
- ☒ Microsoft SQL Server
- ☐ Microsoft Exchange Server
- ☐ SAP HANA

[More Options](#) : Port, gMSA, Install Path, Custom Plug-Ins...

Submit **Cancel**

- For Oracle, fill out the required fields in the Add Host dialog box and select the check box for the Oracle Database plug-in. Then click Submit to begin the discovery process and to add the host to SnapCenter.

Add Host

Host Type: Linux

Host Name: oraclesrv_11.sddc.netapp.com

Credentials: root

+ **i**

Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux

- ☒ Oracle Database
- ☐ SAP HANA

[More Options](#) : Port, Install Path, Custom Plug-Ins...

Submit **Cancel**

Create SnapCenter policies

Policies establish the specific rules to be followed for a backup job. They include, but are not limited to, the backup schedule, replication type, and how SnapCenter handles backing up and truncating transaction logs.

You can access policies in the Settings section of the SnapCenter web client.



The screenshot shows the NetApp SnapCenter web client interface. The top navigation bar includes 'Global Settings', 'Policies', 'Users and Access', 'Roles', 'Credential', and 'Software'. The 'Policies' tab is selected, and the dropdown menu shows 'Microsoft SQL Server'. A search bar labeled 'Search by Name' is present. A red box highlights the 'New' button, which is represented by a plus sign icon. Below the search bar, there is a table with the following data:

Name	Backup Type	Schedule Type	Replication
SQL-Daily	Full and Log backup	Daily	SnapVault
SQL-Hourly	Full and Log backup	Hourly	SnapVault
SQL-Hourly-Logs	Log backup	Hourly	SnapVault
SQL-OnDemand	Full and Log backup	On demand	SnapVault
SQL-Weekly	Full and Log backup	Weekly	SnapVault

For complete information on creating policies for SQL Server backups, see the [SnapCenter documentation](#).

For complete information on creating policies for Oracle backups, see the [SnapCenter documentation](#).

Notes:

- As you progress through the policy creation wizard, take special note of the Replication section. In this section you stipulate the types of secondary SnapMirror copies that you want taken during the backups process.
- The “Update SnapMirror after creating a local Snapshot copy” setting refers to updating a SnapMirror relationship when that relationship exists between two storage virtual machines residing on the same cluster.
- The “Update SnapVault after creating a local SnapShot copy” setting is used to update a SnapMirror relationship that exists between two separate cluster and between an on-premises ONTAP system and Cloud Volumes ONTAP or FSxN.

The following image shows the preceding options and how they look in the backup policy wizard.

New SQL Server Backup Policy

1 Name
2 Backup Type
3 Retention
4 Replication
5 Script

Select secondary replication options i

☐ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label Choose i

Error retry count 3 i

Create SnapCenter Resource Groups

Resource Groups allow you to select the database resources you want to include in your backups and the policies followed for those resources.

1. Go to the Resources section in the left-hand menu.
2. At the top of the window, select the resource type to work with (In this case Microsoft SQL Server) and then click New Resource Group.

The screenshot shows the NetApp SnapCenter interface. The left-hand menu has 'Resources' selected. The top navigation bar shows 'Microsoft SQL Server' selected. The main area displays a table of resource groups.

Name	Resource Count	Tags	Policies	Last Backup	Overall Status
SQLSRV-01	1		SQL-Daily SQL-Hourly SQL-OnDemand SQL-Weekly	05/11/2022 ...	Completed
SQLSRV-02	1		SQL-Daily SQL-Hourly SQL-OnDemand SQL-Weekly	03/28/2022 ...	Failed
SQLSRV-03	1		SQL-Daily SQL-Hourly	05/11/2022 ...	Completed

The SnapCenter documentation covers step-by-step details for creating Resource Groups for both SQL Server and Oracle databases.

For backing up SQL resources, follow [this link](#).

For Backing up Oracle resources, follow [this link](#).

[Next: Deploy and configure Veeam Backup Server.](#)

Deploy and configure Veeam Backup Server

[Previous: Deploy and configure Windows SnapCenter Server on premises.](#)

Veeam Backup & Replication software is used in the solution to back up our application virtual machines and archive a copy of the backups to an Amazon S3 bucket using a Veeam scale-out backup repository (SOBR). Veeam is deployed on a Windows server in this solution. For specific guidance on deploying Veeam, see the [Veeam help Center Technical documentation](#).

Configure Veeam scale-out backup repository

After you deploy and license the software, you can create a scale-out backup repository (SOBR) as target storage for backup jobs. You should also include an S3 bucket as a backup of VM data offsite for disaster recovery.

See the following prerequisites before getting started.

1. Create an SMB file share on your on-premises ONTAP system as the target storage for backups.
2. Create an Amazon S3 bucket to include in the SOBR. This is a repository for the offsite backups.

Add ONTAP Storage to Veeam

First, add the ONTAP storage cluster and associated SMB/NFS filesystem as storage infrastructure in Veeam.

1. Open the Veeam console and log in. Navigate to Storage Infrastructure and then select Add Storage.



2. In the Add Storage wizard, select NetApp as the storage vendor and then select Data ONTAP.
3. Enter the management IP address and check the NAS Filer box. Click Next.

**Name**

Register NetApp Data ONTAP storage by specifying DNS name or IP address.

Name	Management server DNS name or IP address: <input type="text" value="10.61.181.180"/>
Credentials	Description: <input type="text" value="Created by SDDC\jpowell at 5/17/2022 10:34 AM."/>
NAS Filer	Role: <input type="checkbox"/> Block or file storage for VMware vSphere <input type="checkbox"/> Block storage for Microsoft Windows servers <input checked="" type="checkbox"/> NAS filer
Apply	
Summary	

4. Add your credentials to access the ONTAP cluster.

**Credentials**

Specify account with storage administrator privileges.

Name	
Credentials	<div>Credentials: <div> HCIEUC\Admin (HCIEUC\Admin, last edited: 98 days ago) ▼</div><div>Add...</div><div>Manage accounts</div></div>
NAS Filer	<div>Protocol: <div>HTTPS ▼</div></div>
Apply	<div>Port: <div>443 ▲▼</div></div>
Summary	

< Previous

Next >

Finish

Cancel

5. On the NAS Filer page choose the desired protocols to scan and select Next.

**NAS Filer**

Specify how this storage can be accessed by file backup jobs.

Name	Protocol to use:	
Credentials	<input checked="" type="checkbox"/> SMB <input type="checkbox"/> NFS <input checked="" type="checkbox"/> Create required export rules automatically	
NAS Filer	Volumes to scan: <input type="text" value="All volumes"/> <input type="button" value="Choose..."/>	
Apply	Backup proxies to use: <input type="text" value="Automatic selection"/> <input type="button" value="Choose..."/>	
Summary		

6. Complete the Apply and Summary pages of the wizard and click Finish to begin the storage discovery process. After the scan completes, the ONTAP cluster is added along with the NAS filers as available resources.



7. Create a backup repository using the newly discovered NAS shares. From Backup Infrastructure, select Backup Repositories and click the Add Repository menu item.



8. Follow all steps in the New Backup Repository Wizard to create the repository. For detailed information on creating Veeam Backup Repositories, see the [Veeam documentation](#).

**Share**

Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.

Name	Shared folder:
Share	<input type="text" value="\\172.21.162.181\VBRRRepo"/> <input type="button" value="Browse..."/>
	Use \\server\folder format
Repository	<input checked="" type="checkbox"/> This share requires access credentials:
Mount Server	<input type="text" value="sddc\administrator (sddc\administrator, last edited: 85 days ago)"/> <input type="button" value="Add..."/>
Review	Manage accounts
Apply	Gateway server:
Summary	<input checked="" type="radio"/> Automatic selection
	<input type="radio"/> The following server:
	<input type="text" value="veeam.sddc.netapp.com (Backup server)"/>
	Use this option to improve performance and reliability of backup to a NAS located in a remote site.
<input type="button" value=" < Previous"/> <input type="button" value=" Next > "/> <input type="button" value=" Finish"/> <input type="button" value=" Cancel"/>	

Add the Amazon S3 bucket as a backup repository

The next step is to add the Amazon S3 storage as a backup repository.

1. Navigate to Backup Infrastructure > Backup Repositories. Click Add Repository.



2. In the Add Backup Repository wizard, select Object Storage and then Amazon S3. This starts the New Object Storage Repository wizard.

Add Backup Repository

Select the type of backup repository you want to add.



Direct attached storage

Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.



Network attached storage

Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.



Deduplicating storage appliance

Dell EMC Data Domain, ExaGrid, HPE StoreOnce or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.



Object storage

On-prem object storage system or a cloud object storage provider. Object storage can only be used as a Capacity Tier of scale-out backup repositories, backing up directly to object storage is not currently supported.

3. Provide a name for your object storage repository and click Next.
4. In the next section, provide your credentials. You need an AWS Access Key and Secret Key.

New Object Storage Repository



Account

Specify AWS account to use for connecting to Amazon S3 storage bucket.



Name

Account

Bucket

Summary

Credentials:

 AKIA4H43ZT557HXQT2W (last edited: 107 days ago) 

Add...

[Manage cloud accounts](#)

AWS region:

Global 

☐ Use the following gateway server:

veeam.sddc.netapp.com (Backup server) 

Select a gateway server to proxy access to Amazon S3. If no gateway server is specified, all scale-out backup repository extents must have direct Internet access.

< Previous

Next >

Finish

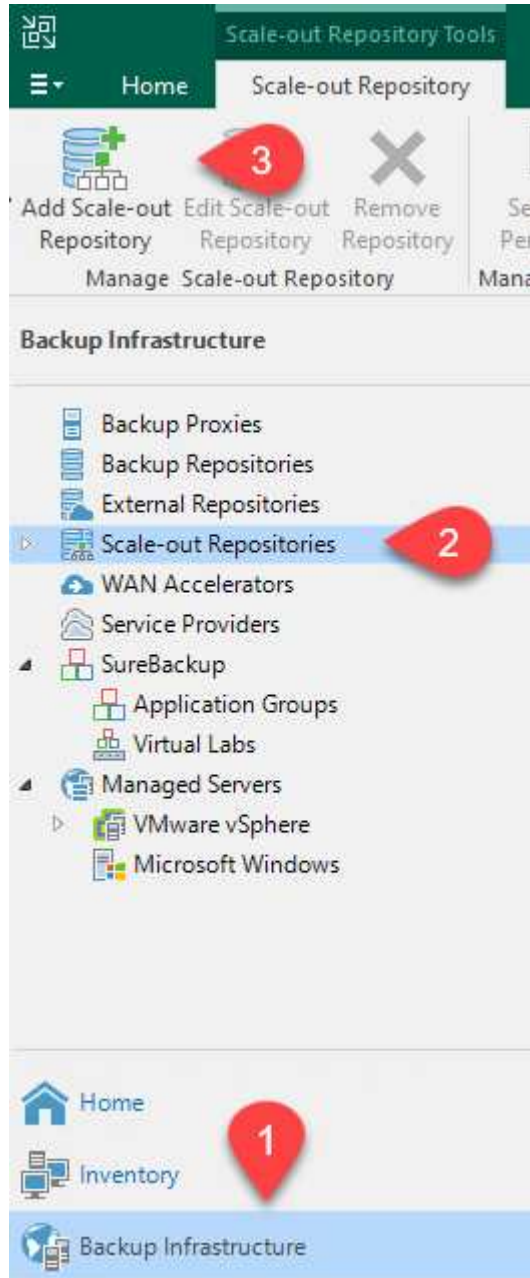
Cancel

5. After the Amazon configuration loads, choose your datacenter, bucket, and folder and click Apply. Finally, click Finish to close out the wizard.

Create scale-out backup repository

Now that we have added our storage repositories to Veeam, we can create the SOBR to automatically tier backup copies to our offsite Amazon S3 object storage for disaster recovery.

1. From Backup Infrastructure, select Scale-out Repositories and then click the Add Scale-out Repository menu item.



2. In the New Scale-out Backup Repository provide a name for the SOBR and click Next.
3. For the Performance Tier, choose the backup repository that contains the SMB share residing on your local ONTAP cluster.

**Performance Tier**

Select backup repositories to use as the landing zone and for the short-term retention.

Name	Extents:	
Performance Tier	Name	Add...
Placement Policy	VBRRepo2	Remove

- For the Placement Policy, choose either Data Locality or Performance based your requirements. Select next.
- For Capacity Tier we extend the SOBR with Amazon S3 object storage. For the purposes of disaster recovery, select Copy Backups to Object Storage as Soon as They are Created to ensure timely delivery of our secondary backups.

**Capacity Tier**

Specify object storage to copy backups to for redundancy and DR purposes. Older backups can be moved to object storage completely to reduce long-term retention costs while preserving the ability to restore directly from offloaded backups.

Name	<input checked="" type="checkbox"/> Extend scale-out backup repository capacity with object storage:
Performance Tier	Amazon S3 Repo Add...
Placement Policy	Define time windows when uploading to capacity tier is allowed Window...
Capacity Tier	<input checked="" type="checkbox"/> Copy backups to object storage as soon as they are created Create additional copy of your backups for added redundancy by having all backups copied to the capacity tier as soon as they are created on the performance tier.
Archive Tier	<input checked="" type="checkbox"/> Move backups to object storage as they age out of the operational restore window Reduce your long-term retention costs by moving older backups to object storage completely while preserving the ability to restore directly from offloaded backups.
Summary	Move backup files older than 14 days (your operational restore window) Override...
	<input type="checkbox"/> Encrypt data uploaded to object storage Password: Add... Manage passwords
<input type="button" value="Previous"/> <input checked="" type="button" value="Next >"/> <input type="button" value="Finish"/> <input type="button" value="Cancel"/>	

- Finally, select Apply and Finish to finalize creation of the SOBR.

Create the scale-out backup repository jobs

The final step to configuring Veeam is to create backup jobs using the newly created SOBR as the backup destination. Creating backup jobs is a normal part of any storage administrator's repertoire and we do not cover the detailed steps here. For more complete information on creating backup jobs in Veeam, see the [Veeam Help Center Technical Documentation](#).

[Next: Cloud backup tools and configuration.](#)

Cloud backup tools and configuration

[Previous: Deploy and configure Veeam Backup Server.](#)

To conduct a failover of application VMs and database volumes to VMware Cloud Volume services running in AWS, you must install and configure a running instance of both SnapCenter Server and Veeam Backup and Replication Server. After the failover is complete, you must also configure these tools to resume normal backup operations until a failback to the on-premises datacenter is planned and executed.

Deploy secondary Windows SnapCenter Server

SnapCenter Server is deployed in the VMware Cloud SDDC or installed on an EC2 instance residing in a VPC with network connectivity to the VMware Cloud environment.

SnapCenter software is available from the NetApp support site and can be installed on Microsoft Windows systems that reside either in a domain or workgroup. A detailed planning guide and installation instructions can be found at the [NetApp documentation center](#).

You can find the SnapCenter software at [this link](#).

Configure secondary Windows SnapCenter Server

To perform a restore of application data mirrored to FSx ONTAP, you must first perform a full restore of the on-premises SnapCenter database. After this process is complete, communication with the VMs is reestablished and application backups can now resume using FSx ONTAP as the primary storage.

To achieve this, you must complete the following items on the SnapCenter Server:

1. Configure the computer name to be identical to the original on-premises SnapCenter Server.
2. Configure networking to communicate with VMware Cloud and the FSx ONTAP instance.
3. Complete the procedure to restore the SnapCenter database.
4. Confirm that SnapCenter is in Disaster Recovery mode to make sure that FSx is now the primary storage for backups.
5. Confirm that communication is reestablished with the restored virtual machines.

For more information on completing these steps, see to section ["SnapCenter database Restore Process"](#).

Deploy secondary Veeam Backup & Replication server

You can install the Veeam Backup & Replication server on a Windows server in the VMware Cloud on AWS or on an EC2 instance. For detailed implementation guidance, see the [Veeam Help Center Technical Documentation](#).

Configure secondary Veeam Backup & Replication server

To perform a restore of virtual machines that have been backed up to Amazon S3 storage, you must install the Veeam Server on a Windows server and configure it to communicate with VMware Cloud, FSx ONTAP, and the S3 bucket that contains the original backup repository. It must also have a new backup repository configured on FSx ONTAP to conduct new backups of the VMs after they are restored.

To perform this process, the following items must be completed:

1. Configure networking to communicate with VMware Cloud, FSx ONTAP, and the S3 bucket containing the original backup repository.
2. Configure an SMB share on FSx ONTAP to be a new backup repository.
3. Mount the original S3 bucket that was used as part of the scale-out backup repository on premises.
4. After restoring the VM, establish new backup jobs to protect SQL and Oracle VMs.

For more information on restoring VMs using Veeam, see the section ["Restore Application VMs with Veeam Full Restore"](#).

[Next: SnapCenter database backup for disaster recovery.](#)

SnapCenter database backup for disaster recovery

[Previous: Cloud backup tools and configuration.](#)

SnapCenter allows for the backup and recovery of its underlying MySQL database and configuration data for the purpose of recovering the SnapCenter server in the case of a disaster. For our solution, we recovered the SnapCenter database and configuration on an AWS EC2 instance residing in our VPC. For more information on this step, see [this link](#).

SnapCenter backup prerequisites

The following prerequisites are required for SnapCenter backup:

- A volume and SMB share created on the on-premises ONTAP system to locate the backed-up database and configuration files.
- A SnapMirror relationship between the on-premises ONTAP system and FSx or CVO in the AWS account. This relationship is used for transporting the snapshot containing the backed-up SnapCenter database and configuration files.
- Windows Server installed in the cloud account, either on an EC2 instance or on a VM in the VMware Cloud SDDC.
- SnapCenter installed on the Windows EC2 instance or VM in VMware Cloud.

SnapCenter backup and restore process summary

- Create a volume on the on-premises ONTAP system for hosting the backup db and config files.
- Set up a SnapMirror relationship between on-premises and FSx/CVO.
- Mount the SMB share.
- Retrieve the Swagger authorization token for performing API tasks.
- Start the db restore process.
- Use the xcopy utility to copy the db and config file local directory to the SMB share.
- On FSx, create a clone of the ONTAP volume (copied via SnapMirror from on-premises).
- Mount the SMB share from FSx to EC2/VMware Cloud.
- Copy the restore directory from the SMB share to a local directory.
- Run the SQL Server restore process from Swagger.

Back up the SnapCenter database and configuration

SnapCenter provides a web client interface for executing REST API commands. For information on accessing the REST APIs through Swagger, see the SnapCenter documentation at [this link](#).

Log into Swagger and obtain authorization token

After you have navigated to the Swagger page, you must retrieve an authorization token to initiate the database restore process.

1. Access the SnapCenter Swagger API web page at *https://<SnapCenter Server IP>:8146/swagger/*.



SnapCenter API

[Base URL: /api]

<https://snapcenter.sddc.netapp.com:8146/Content/swagger/SnapCenter.yaml>

Manage your SnapCenter Server using the SnapCenter API.

To access the swagger documentation of "SnapCenter Plug-in for VMware vSphere" API's, please use https://{SCV_hostname}:{SCV_host_port}/api/swagger-ui.html

2. Expand the Auth section and click Try it Out.

Auth

POST **/4.6/auth/login** Service login

The login endpoint exposes the method required to log in to the SnapCenter service. The login method returns a token that is used to authenticate subsequent requests.

Parameters Try it out

3. In the UserOperationContext area, fill in the SnapCenter credentials and role and click Execute.

Name	Description
TokenNeverExpires	Token never expires
boolean (query)	<div>false</div>
UserOperationContext * required	User credentials
object (body)	<div> Edit Value Model </div> <div> <pre>{ "UserOperationContext": { "User": { "Name": "localhost\\scadmin", "Passphrase": "NetApp321", "Rolename": "SnapCenterAdmin" } } }</pre> </div> <div> <div>Cancel</div> </div> <div> Parameter content type <div>application/json</div> </div>

Execute

- In the Response body below, you can see the token. Copy the token text for authentication when executing the backup process.

200

Response body

```
{
  "PluginName": null,
  "HostId": 0,
  "RoleId": null,
  "JobIds": null
},
{
  "User": {
    "Token": "KLYxOg==tsV6EOdtDAmAlpe8q5SG6wcoGaSjwME6jrNy5CsY63HRQ5LkoZLIESRNaHpGJJ0UUDQynENdgtVGDZnvx+I/ZJZIn5M1NZrj6CLfGTApG1GacagT08bqb5bMTx07EcdRAidzAXUDb3GyLOKtW0GdwKzSeUwKj3uVupnk1E3lSkK6PRBv9RS8j0qHQvo4v4RL0hhThwFhV9/23nPeJVP/p1E4vrV/zeZVTUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkQ==",
    "Name": "SCAdmin",
    "TokenHashed": null,
    "Type": "",
    "TokenTime": "2022-03-22T14:21:57.3665661-07:00",
    "Id": "1",
    "FullName": "SCAdmin",
    "Host": null,
    "Author": null,
    "UserName": "",
    "Domain": "",
    "Passphrase": ""
  }
}
```

Download

Perform a SnapCenter database backup

Next go to the Disaster Recovery area on the Swagger page to begin the SnapCenter backup process.

1. Expand the Disaster Recovery area by clicking it.

Disaster Recovery

GET

/4.6/disasterrecovery/server/backup

Fetch all the existing SnapCenter Server DR Backups.

POST

/4.6/disasterrecovery/server/backup

Starts the SnapCenter Server DR backup.

DELETE

/4.6/disasterrecovery/server/backup

Deletes the existing Snapcenter DR backup.

POST

/4.6/disasterrecovery/server/restore

Starts SnapCenter Server Restore.

POST

/4.6/disasterrecovery/storage

Enable or disable the storage disaster recovery.

2. Expand the `/4.6/disasterrecovery/server/backup` section and click Try it Out.

POST

/4.6/disasterrecovery/server/backup

Starts the SnapCenter Server DR backup.

Starts and creates a new SnapCenter Server DR backup.

Parameters

Try it out

3. In the `SmDRBackupRequest` section, add the correct local target path and select Execute to start the backup of the SnapCenter database and configuration.



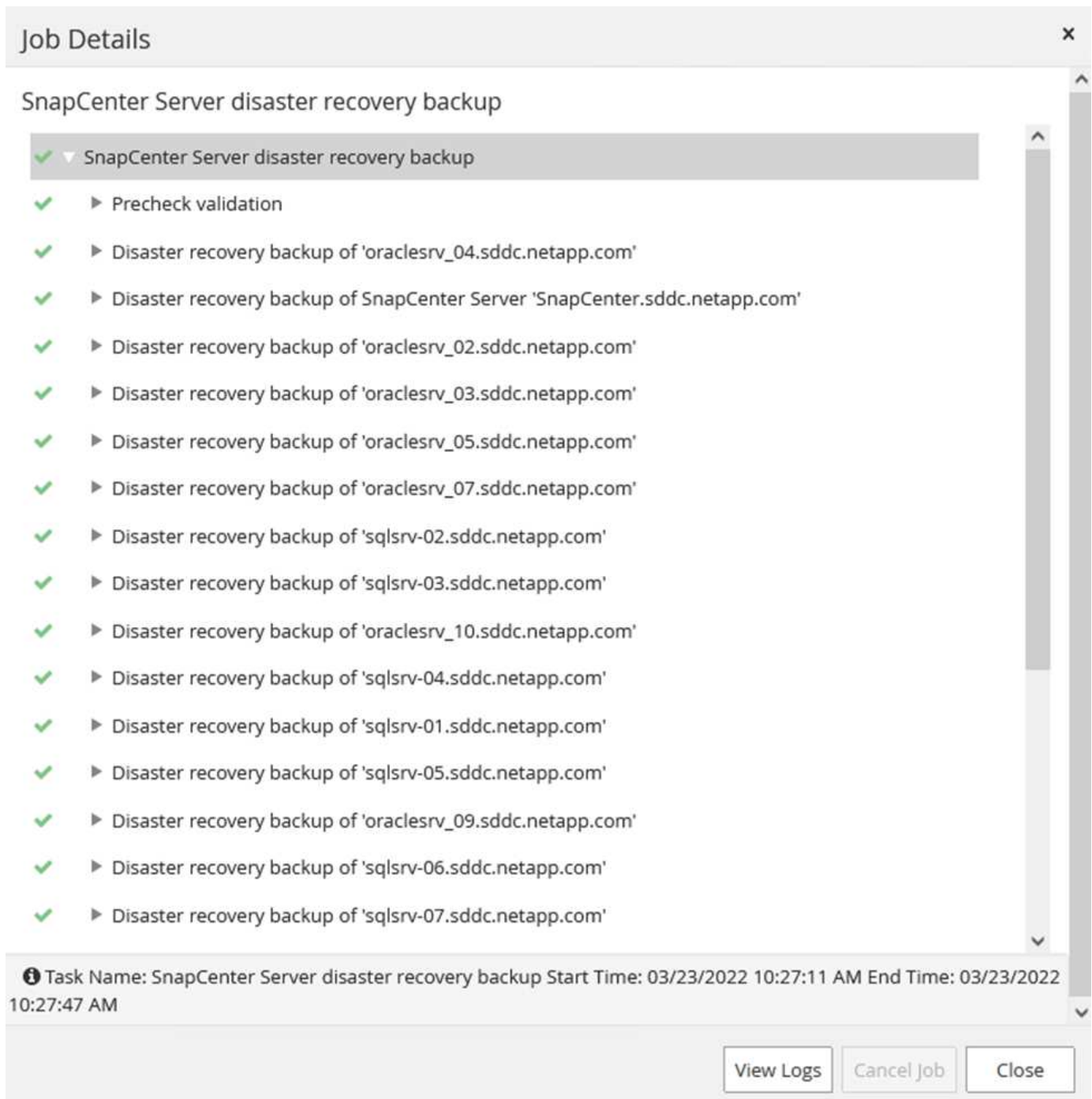
The backup process does not allow backing up directly to an NFS or CIFS file share.

Name	Description
Token * required string (header)	User authorization token <div>TUHFHUM069XRe5cuW9nwyj4b0l5Y5FN3XDkjQ==</div>
SmDRBackupRequest * required object (body)	Parameters to take Backup <div>Edit Value Model</div> <div><pre>{ "TargetPath": "C:\\\\SnapCenter_Backups\\\\" }</pre></div> <div>Cancel</div> <div>Parameter content type application/json</div>

Execute

Monitor the backup job from SnapCenter

Log into SnapCenter to review log files when starting the database restore process. Under the Monitor section, you can view the details of the SnapCenter server disaster recovery backup.



Use XCOPY utility to copy the database backup file to the SMB share

Next you must move the backup from the local drive on the SnapCenter server to the CIFS share that is used to SnapMirror copy the data to the secondary location located on the FSx instance in AWS. Use xcopy with specific options that retain the permissions of the files.

Open a command prompt as Administrator. From the command prompt, enter the following commands:

```
xcopy <Source_Path> \\<Destination_Server_IP>\<Folder_Path> /O /X /E /H /K
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O /X /E /H /K
```

[Next: Failover.](#)

Failover

[Previous: SnapCenter database backup for disaster recovery.](#)

Disaster occurs at primary site

For a disaster that occurs at the primary on-premises datacenter, our scenario includes failover to a secondary site residing on Amazon Web Services infrastructure using VMware Cloud on AWS. We assume that the virtual machines and our on-premises ONTAP cluster are no longer accessible. In addition, both the SnapCenter and Veeam virtual machines are no longer accessible and must be rebuilt at our secondary site.

This section address failover of our infrastructure to the cloud, and we cover the following topics:

- SnapCenter database restore. After a new SnapCenter server has been established, restore the MySQL database and configuration files and toggle the database into disaster recovery mode in order to allow the secondary FSx storage to become the primary storage device.
- Restore the application virtual machines using Veeam Backup & Replication. Connect the S3 storage that contains the VM backups, import the backups, and restore them to VMware Cloud on AWS.
- Restore the SQL Server application data using SnapCenter.
- Restore the Oracle application data using SnapCenter.

SnapCenter database restore process

SnapCenter supports disaster recovery scenarios by allowing the backup and restore of its MySQL database and configuration files. This allows an administrator to maintain regular backups of the SnapCenter database at the on-premises datacenter and later restore that database to a secondary SnapCenter database.

To access the SnapCenter backup files on the remote SnapCenter server, complete the following steps:

1. Break the SnapMirror relationship from the FSx cluster, which makes the volume read/write.
2. Create a CIFS server (if necessary) and create a CIFS share pointing to the junction path of the cloned volume.
3. Use xcopy to copy the backup files to a local directory on the secondary SnapCenter system.
4. Install SnapCenter v4.6.
5. Ensure that SnapCenter server has the same FQDN as the original server. This is required for the db restore to be successful.

To start the restore process, complete the following steps:

1. Navigate to the Swagger API web page for the secondary SnapCenter server and follow the previous instructions to obtain an authorization token.

2. Navigate to the Disaster Recovery section of the Swagger page, select /4.6/disasterrecovery/server/restore, and click Try it Out.

POST /4.6/disasterrecovery/server/restore Starts SnapCenter Server Restore.

Starts SnapCenter Server Restore.

Parameters

Try it out

3. Paste in your authorization token and, in the SmDRResterRequest section, paste in the name of the backup and the local directory on the secondary SnapCenter server.

Name	Description
Token * required string (header)	User authorization token <div>KlYxOg==rMXzS7EPIGRzTXjfton6Q+JoNGpueQt</div>
SmDRRestoreRequest * required object (body)	Parameters to take for Restore <div>Edit Value Model { "BackupName": "SnapCenter.sddc.netapp.com_03-23-2022_12.38.00.6713", "BackupPath": "C:\\SnapCenter\\" }</div>

4. Select the Execute button to start the restore process.
5. From SnapCenter, navigate to the Monitor section to view the progress of the restore job.

<

Dashboard

Resources

Monitor

Reports

Hosts

Storage Systems

Settings

Alerts

Jobs

Schedules

Events

Logs

search by name

✓

Jobs - Filter

ID	Status	Name
20482	✓	SnapCenter Server Disaster Recovery
20481	✓	SnapCenter Server disaster recovery backup
20480	✗	SnapCenter Server disaster recovery backup
20475	✓	Backup of Resource Group 'SQLSRV-09' with policy 'SQL-Hourly'
20474	✓	Backup of Resource Group 'SQLSRV-05' with policy 'SQL-Hourly'
20473	⌚	Backup of Resource Group 'OracleSrv_06' with policy 'Oracle-Hourly'
20472	✗	SnapCenter Server disaster recovery backup

Job Details

SnapCenter Server Disaster Recovery

- ✓ ▼ SnapCenter Server Disaster Recovery
- ✓ ▼ Prepare for restore job
- ✓ ▼ Precheck validation
- ✓ ▼ Saving original server state
- ✓ ▼ Schedule restore
- ✓ ▼ Repository restore
- ✓ ▼ Config restore
- ✓ ▼ Reset MySQL password

6. To enable SQL Server restores from secondary storage, you must toggle the SnapCenter database into Disaster Recovery mode. This is performed as a separate operation and initiated on the Swagger API web page.
 - a. Navigate to the Disaster Recovery section and click `/4.6/disasterrecovery/storage`.
 - b. Paste in the user authorization token.
 - c. In the `SmSetDisasterRecoverySettingsRequest` section, change `EnableDisasterRecover` to `true`.
 - d. Click Execute to enable disaster recovery mode for SQL Server.

Name	Description
Token * required string (header)	User authorization token <div>KIYxOg==rMXzS7EPIGRzTXjfton6Q+JoNGpueQt</div>
SmSetDisasterRecoverySettingsRequest * required object (body)	Parameters to enable or disable the DR mode <div> Edit Value Model <pre>{ "EnableDisasterRecovery": true }</pre> </div>



See comments regarding additional procedures.

[Next: Restore application VMs with Veeam full restore.](#)

Restore application VMs with Veeam full restore

[Previous: Failover.](#)

Create a backup repository and import backups from S3

From the secondary Veeam server, import the backups from S3 storage and restore the SQL Server and Oracle VMs to your VMware Cloud cluster.

To import the backups from the S3 object that was part of the on-premises scale-out backup repository, complete the following steps:

1. Go to Backup Repositories and click Add Repository in the top menu to launch the Add Backup Repository wizard. On the first page of the wizard, select Object Storage as the backup repository type.

Add Backup Repository

Select the type of backup repository you want to add.



Direct attached storage

Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.



Network attached storage

Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.



Deduplicating storage appliance

Dell EMC Data Domain, ExaGrid, HPE StoreOnce or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.



Object storage

On-prem object storage system or a cloud object storage provider. Object storage can only be used as a Capacity Tier of scale-out backup repositories, backing up directly to object storage is not currently supported.

2. Select Amazon S3 as the Object Storage type.



Object Storage

Select the type of object storage you want to use as a backup repository.



S3 Compatible

Adds an on-premises object storage system or a cloud object storage provider.



Amazon S3

Adds Amazon cloud object storage. Amazon S3, Amazon S3 Glacier (including Deep Archive) and Amazon Snowball Edge are supported.



Google Cloud Storage

Adds Google Cloud storage. Both Standard and Nearline storage classes are supported.



IBM Cloud Object Storage

Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.



Microsoft Azure Storage

Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage, Microsoft Azure Archive Storage and Microsoft Azure Data Box are supported.

- From the list of Amazon Cloud Storage Services, select Amazon S3.



- Select your pre-entered credentials from the drop-down list or add a new credential for accessing the cloud storage resource. Click Next to continue.



- On the Bucket page, enter the data center, bucket, folder, and any desired options. Click Apply.

New Object Storage Repository

Bucket
Specify Amazon S3 bucket to use.

Name

Account

Bucket

Summary

Data center:
US East (N. Virginia)

Bucket:
ehcveeamrepo Browse...

Folder:
RTP Browse...

☐ Limit object storage consumption to: 10 TB
This is a soft limit to help control your object storage spend. If the specified limit is exceeded, already running backup offload tasks will be allowed to complete, but no new tasks will be started.

☐ Make recent backups immutable for: 30 days
Protects backups from modification or deletion by ransomware, hackers or malicious insiders using native object storage capabilities.

☐ Use infrequent access storage class (may result in higher costs)
With lower price per GB but higher retrieval and early deletion fees, this storage class is best suited for long-term storage of GFS full backups. Avoid using it for short-term storage of recent backups.

☐ Store backups in a single availability zone (even lower price per GB, reduced resilience)

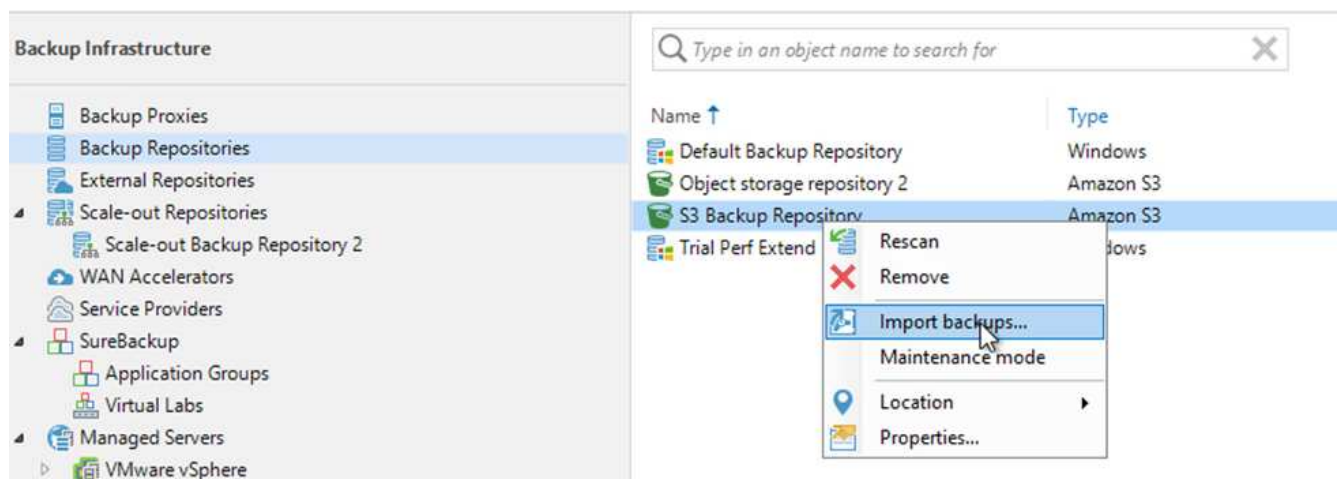
< Previous Apply Finish Cancel

6. Finally, select Finish to complete the process and add the repository.

Import backups from S3 object storage

To import the backups from the S3 repository that was added in the previous section, complete the following steps.

1. From the S3 backup repository, select Import Backups to launch the Import Backups wizard.



2. After the database records for the import have been created, select Next and then Finish at the summary screen to start the import process.

3. After the import is complete, you can restore VMs into the VMware Cloud cluster.



Restore application VMs with Veeam full restore to VMware Cloud

To restore SQL and Oracle virtual machines to the VMware Cloud on AWS workload domain/cluster, complete the following steps.

1. From the Veeam Home page, select the object storage containing the imported backups, select the VMs to restore, and then right click and select Restore Entire VM.



2. On the first page of the Full VM Restore wizard, modify the VMs to backup if desired and select Next.



3. On the Restore Mode page, select Restore to a New Location, or with Different Settings.



Full VM Restore

Restore Mode
Specify whether selected VMs should be restored back to the original location, or to a new location or with different settings.

Virtual Machines

- Restore Mode
- Host
- Resource Pool
- Datastore
- Folder
- Network
- Secure Restore
- Summary

☐ **Restore to the original location**
Quickly initiate the restore of selected VM to its original location, with the original name and settings. This option minimizes the chance of user input error.

☒ **Restore to a new location, or with different settings**
Customize the restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the defaults.

☐ **Staged restore**
Run the selected VM directly from backup files in the isolated DataLab to make changes to the guest OS or applications prior to placing the VM into production environment.

[Pick proxy to use](#)

☐ **Quick rollback (restore changed blocks only)**
Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.

< Previous **Next >** Finish Cancel

4. On the host page, select the Target ESXi host or cluster to restore the VM to.



5. On the Datastores page, select the target datastore location for both the configuration files and hard disk.



Datastore

By default, original datastore and disk type are selected for each VM file. You can change them by selecting desired VM file, and clicking Datastore or Disk Type. Use multi-select (Ctrl-click and Shift-click) to select multiple VMs at once.

Virtual Machines

Restore Mode

Host

Resource Pool

Datastore

Folder

Network

Secure Restore

Summary

File	Size	Datastore	Disk type
SQLSRV-04			
Configuration files		WorkloadDatastore (VM...)	
Hard disk 1 (SQLSR...	100 GB	WorkloadDatastore (VM...)	Same as source

Datastore...

[< Previous](#)

Next >

Cancer

6. On the Network page, map the original networks on the VM to the networks in the new target location.



7. Select whether to scan the restored VM for malware, review the summary page, and click Finish to start the restore.

Next: [Restore SQL Server application data.](#)

Restore SQL Server application data

Previous: [Restore application VMs with Veeam full restore.](#)

The following process provides instructions on how to recover a SQL Server in VMware Cloud Services in AWS in the event of a disaster that renders the on-premises site inoperable.

The following prerequisites are assumed to be complete in order to continue with the recovery steps:

1. The Windows Server VM has been restored to the VMware Cloud SDDC using Veeam Full Restore.
2. A secondary SnapCenter server has been established and SnapCenter database restore and configuration has been completed using the steps outlined in the section "[SnapCenter backup and restore process summary.](#)"

A summary of the SQL Server application data recovery process is as follows:

1. Configure the VM in preparation for the restore process.
2. Set up FSx for iSCSI access.
3. Set up the Windows VM for iSCSI access.
4. Attach the SQL Server database and bring it online.
5. Confirm communication between SnapCenter and the SnapCenter SQL Server Plug-in.

VM: Post restore configuration for SQL Server VM

After the restore of the VM is complete, you must configure networking and other items in preparation for rediscovering the host VM within SnapCenter.

1. Assign new IP addresses for Management and iSCSI or NFS.
2. Join the host to the Windows domain.
3. Add the hostnames to DNS or to the hosts file on the SnapCenter server.



If the SnapCenter plug-in was deployed using domain credentials different than the current domain, you must change the Log On account for the Plug-in for Windows Service on the SQL Server VM. After changing the Log On account, restart the SnapCenter SMCORE, Plug-in for Windows, and Plug-in for SQL Server services.



To automatically rediscover the restored VMs in SnapCenter, the FQDN must be identical to the VM that was originally added to the SnapCenter on premises.

Configure FSx storage for SQL Server restore

To accomplish the disaster recovery restore process for a SQL Server VM, you must break the existing SnapMirror relationship from the FSx cluster and grant access to the volume. To do so, complete the following steps.

1. To break the existing SnapMirror relationship for the SQL Server database and log volumes, run the following command from the FSx CLI:

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. Grant access to the LUN by creating an initiator group containing the iSCSI IQN of the SQL Server Windows VM:

```
FSx-Dest::> igroup create -vserver DestSVM -igroup groupName -protocol iSCSI -ostype windows -initiator IQN
```

3. Finally, map the LUNs to the initiator group that you just created:

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath groupName
```

4. To find the path name, run the `lun show` command.

Set up the Windows VM for iSCSI access and discover the file systems

1. From the SQL Server VM, set up your iSCSI network adapter to communicate on the VMware Port Group that has been established with connectivity to the iSCSI target interfaces on your FSx instance.
2. Open the iSCSI Initiator Properties utility and clear out the old connectivity settings on the Discovery, Favorite Targets, and Targets tabs.
3. Locate the IP address(es) for accessing the iSCSI logical interface on the FSx instance/cluster. This can be found in the AWS console under Amazon FSx > ONTAP > Storage Virtual Machines.

Endpoints

Management DNS name	svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com	Management IP address	198.19.254.53
NFS DNS name	svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com	NFS IP address	198.19.254.53
iSCSI DNS name	iscsi.svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com	iSCSI IP addresses	172.30.15.101, 172.30.14.49

4. From the Discovery tab, click Discover Portal and enter the IP addresses for your FSx iSCSI targets.



Discover Target Portal ✕

Enter the IP address or DNS name and port number of the portal you want to add.

To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: Port: (Default is 3260.)

5. On the Target tab, click Connect, select Enable Multi-Path if appropriate for your configuration and then click OK to connect to the target.



6. Open the Computer Management utility and bring the disks online. Verify that they retain the same drive letters that they previously held.



Attach the SQL Server databases

1. From the SQL Server VM, open Microsoft SQL Server Management Studio and select Attach to start the process of connecting to the database.



2. Click Add and navigate to the folder containing the SQL Server primary database file, select it, and click OK.



3. If the transaction logs are on a separate drive, choose the folder that contains the transaction log.
4. When finished, click OK to attach the database.



Confirm SnapCenter communication with SQL Server Plug-in

With the SnapCenter database restored to its previous state, it automatically rediscovers the SQL Server hosts. For this to work correctly, keep in mind the following prerequisites:

- SnapCenter must be placed in Disaster Recover mode. This can be accomplished through the Swagger API or in Global Settings under Disaster Recovery.
- The FQDN of the SQL Server must be identical to the instance that was running in the on-premises datacenter.
- The original SnapMirror relationship must be broken.
- The LUNs containing the database must be mounted to the SQL Server instance and the database attached.

To confirm that SnapCenter is in Disaster Recovery mode, navigate to Settings from within the SnapCenter web client. Go to the Global Settings tab and then click Disaster Recovery. Make sure that the Enable Disaster Recovery checkbox is enabled.



Next: [Restore Oracle application data.](#)

Restore Oracle application data

Previous: [Restore SQL Server application data.](#)

The following process provides instructions on how to recover Oracle application data in VMware Cloud Services in AWS in the event of a disaster that renders the on-premises site inoperable.

Complete the following prerequisites to continue with the recovery steps:

1. The Oracle Linux server VM has been restored to the VMware Cloud SDDC using Veeam Full Restore.
2. A secondary SnapCenter server has been established and the SnapCenter database and configuration files have been restored using the steps outlined in this section ["SnapCenter backup and restore process summary."](#)

A summary of the Oracle application data recovery process is as follows:

1. Configure the VM in preparation for the restore process.
2. Set up FSx for iSCSI access.
3. Set up the Linux VM for NFS access.
4. Attach the SQL Server database and bring it online.
5. Confirm communication between SnapCenter and the SnapCenter SQL Server Plug-in.

A summary of the Oracle Server failover process is as follows:

1. Restore the Oracle VM to the VMware Cloud using Veeam.
2. Clean up the VM in preparation for the restore process:
 - a. Change the IP addresses as required.
 - b. Add the system to DNS with an FQDN identical to the original.
3. Set up FSx for NFS access.
4. Mount the NFS volumes on the Oracle Linux Server.

Configure FSx for Oracle restore – Break the SnapMirror relationship

To make the secondary storage volumes hosted on the FSxN instance accessible to the Oracle servers, you must first break the existing SnapMirror relationship.

1. After logging into the FSx CLI, run the following command to view the volumes filtered by the correct name.

```
FSx-Dest::> volume show -volume VolumeName*
```

```

FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver    Volume          Aggregate      State    Type    Size    Available  Used%
-----
ora_svm_dest
  oraclesrv_03_u01_dest
    aggr1      online    DP      100GB    93.12GB    6%
ora_svm_dest
  oraclesrv_03_u02_dest
    aggr1      online    DP      200GB    34.98GB    82%
ora_svm_dest
  oraclesrv_03_u03_dest
    aggr1      online    DP      150GB    33.37GB    77%
3 entries were displayed.

FsxId0ae40e08acc0dea67::> █

```

2. Run the following command to break the existing SnapMirror relationships.

```

FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName

```

```

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".

```

3. Update the junction-path in the Amazon FSx web client:

FSx > Volumes > fsvol-01167370e9b7aefa0

oraclesrv_03_u01_dest (fsvol-01167370e9b7aefa0)

Attach

Actions ▲

Update volume

Create backup

Delete volume

Summary

Volume ID	fsvol-01167370e9b7aefa0	Creation time	2022-03-08T14:52:09-05:00	SVM ID	svm-02b2ad25c6b2e5bc2
Volume name	oraclesrv_03_u01_dest	Lifecycle state	Created	Junction path	-
UUID	3d7338ce-9f19-11ec-b007-4956fb75f45c	Volume type	ONTAP	Tiering policy name	SNAPSHOT_ONLY
File system ID	fs-0ae40e08acc0dea67	Size	100.00 GB	Tiering policy cooling period (days)	2
Resource ARN	arn:aws:fsx:us-east-1:541696183547:volume/fs-0ae40e08acc0dea67/fsvol-01167370e9b7aefa0			Storage efficiency enabled	Disabled

4. Add the junction path name and click Update. Specify this junction path when mounting the NFS volume from the Oracle server.

Update volume



Junction path

/oraclesrv_03_u01_dest

The location within your file system where your volume will be mounted.

Volume size

102400

Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

☐ Enabled (recommended)

☒ Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

Snapshot Only

Cancel

Update

Mount NFS volumes on Oracle Server

In Cloud Manager, you can obtain the mount command with the correct NFS LIF IP address for mounting the NFS volumes that contain the Oracle database files and logs.

1. In Cloud Manager, access the list of volumes for your FSx cluster.



50 volumes

Volume Name ↕	State ↕	Storage VM ↕	Disk Type
oraclesrv_02_u02_dest	● Online	ora_svm_dest	SSD
oraclesrv_02_u03_dest	● Online	ora_svm_dest	SSD
oraclesrv_03_u01_dest	● Online	ora_svm_dest	SSD

2. From the action menu, select Mount Command to view and copy the mount command to be used on our Oracle Linux server.



Mount Volume NFS

oraclesrv_03_u01_dest

Go to your linux machine and enter this mount command

Mount Command

```
mount 198.19.254.180:/oraclesrv_03_u01_dest <dest_d...
```



3. Mount the NFS file system to the Oracle Linux Server. The directories for mounting the NFS share already exist on the Oracle Linux host.
4. From the Oracle Linux server, use the mount command to mount the NFS volumes.

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

Repeat this step for each volume associated with the Oracle databases.



To make the NFS mount persistent upon rebooting, edit the `/etc/fstab` file to include the mount commands.

5. Reboot the Oracle server. The Oracle databases should start up normally and be available for use.

[Next: Failback.](#)

Failback

[Previous: Restore Oracle application data.](#)

Upon successful completion of the failover process outlined in this solution, SnapCenter and Veeam resume their backup functions running in AWS, and FSx for ONTAP is now designated as primary storage with no existing SnapMirror relationships with the original on-premises datacenter. After normal function has resumed on premises, you can use a process identical to the one outlined in this documentation to mirror data back to the on-premises ONTAP storage system.

As is also outlined in this documentation, you can configure SnapCenter to mirror the application data volumes from FSx for ONTAP to an ONTAP storage system residing on premises. Similarly, you can configure Veeam to replicate backup copies to Amazon S3 using a scale-out backup repository so that those backups are accessible to a Veeam backup server residing at the on-premises datacenter.

Failback is outside the scope of this documentation, but failback differs little from the detailed process outlined here.

[Next: Conclusion.](#)

Conclusion

[Previous: Failback.](#)

The use case presented in this documentation focuses on proven disaster recovery technologies that highlight the integration between NetApp and VMware. NetApp ONTAP storage systems provide proven data-mirroring technologies that allow organizations to design disaster recovery solutions that span on-premises and ONTAP technologies residing with the leading cloud providers.

FSx for ONTAP on AWS is one such solution that allows for seamless integration with SnapCenter and SyncMirror for replicating application data to the cloud. Veeam Backup & Replication is another well-known technology that integrates well with NetApp ONTAP storage systems and can provide failover to vSphere-native storage.

This solution presented a disaster recovery solution using guest connect storage from an ONTAP system hosting SQL Server and Oracle application data. SnapCenter with SnapMirror provides an easy-to-manage solution for protecting application volumes on ONTAP systems and replicating them to FSx or CVO residing in the cloud. SnapCenter is a DR-enabled solution for failing over all application data to VMware Cloud on AWS.

Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- Links to solution documentation

[NetApp Hybrid Multicloud with VMware Solutions](#)

[NetApp Solutions](#)

Copyright information

Copyright © 2022 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.