



# **NetApp Hybrid Multicloud with Red Hat OpenShift**

NetApp Solutions

NetApp  
May 18, 2023

# Table of Contents

- NetApp Hybrid Multicloud with Red Hat OpenShift Container workloads ..... 1
  - NetApp Hybrid Multicloud solutions for Red Hat OpenShift Container workloads ..... 1
  - NetApp Hybrid Multicloud solutions for Red Hat OpenShift Container workloads ..... 11
  - NetApp Hybrid Multicloud solutions for Red Hat OpenShift Container workloads ..... 22
  - NetApp Hybrid Multicloud solutions for Red Hat OpenShift Container workloads ..... 31

# NetApp Hybrid Multicloud with Red Hat OpenShift Container workloads

## NetApp Hybrid Multicloud solutions for Red Hat OpenShift Container workloads

### Overview

NetApp is seeing a significant increase in customers modernizing their legacy enterprise applications and building new applications using containers and orchestration platforms built around Kubernetes. Red Hat OpenShift Container Platform is one example that we see adopted by many of our customers.

As more and more customers begin adopting containers within their enterprises, NetApp is perfectly positioned to help serve the persistent storage needs of their stateful applications and classic data management needs such as data protection, data security, and data migration. However, these needs are met using different strategies, tools, and methods.

**NetApp ONTAP** based storage options listed below, deliver security, data protection, reliability, and flexibility for containers and Kubernetes deployments.

- Self-managed storage in on-premises:
  - NetApp Fabric Attached Storage (FAS), NetApp All Flash FAS Arrays (AFF), NetApp All SAN Array (ASA) and ONTAP Select
- Provider-managed storage in on-premises:
  - NetApp Keystone provides Storage as a Service (STaaS)
- Self-managed storage in the cloud:
  - NetApp Cloud Volumes ONTAP(CVO) provide self managed storage in the hyperscalers
- Provider-managed storage in the cloud:
  - Cloud Volumes Service for Google Cloud (CVS), Azure NetApp Files (ANF), Amazon FSx for NetApp ONTAP offer fully managed storage in the hyperscalers

## ONTAP feature highlights



<b>Storage Administration</b> <ul style="list-style-type: none"> <li>Multi-tenancy</li> <li>FlexVol &amp; FlexGroup</li> <li>LUN</li> <li>Quotas</li> <li>ONTAP CLI &amp; API</li> <li>System Manager &amp; BlueXP</li> </ul>	<b>Performance &amp; Scalability</b> <ul style="list-style-type: none"> <li>FlexCache</li> <li>FlexClone</li> <li>nconnect, session trunking, multipathing</li> <li>Scale-out clusters</li> </ul>
<b>Availability &amp; Resilience</b> <ul style="list-style-type: none"> <li>Multi-AZ HA deployment (MetroCluster)</li> <li>SnapShot &amp; SnapRestore</li> <li>SnapMirror</li> <li>SnapMirror Business Continuity (MetroCluster)</li> <li>SnapMirror Cloud</li> </ul>	<b>Access Protocols</b> <ul style="list-style-type: none"> <li>NFS –v3, v4, v4.1, v4.2</li> <li>SMB – v2, v3</li> <li>iSCSI</li> <li>Multi-protocol access</li> </ul>
<b>Storage Efficiency</b> <ul style="list-style-type: none"> <li>Deduplication &amp; Compression</li> <li>Compaction</li> <li>Thin provisioning</li> <li>Data Tiering (Fabric Pool)</li> </ul>	<b>Security &amp; Compliance</b> <ul style="list-style-type: none"> <li>Fpolicy &amp; Vscan</li> <li>Active Directory integration</li> <li>LDAP &amp; Kerberos</li> <li>Certificate based authentication</li> </ul>

**NetApp BlueXP** enables you to manage all of your storage and data assets from a single control plane/interface.

You can use BlueXP to create and administer cloud storage (for example, Cloud Volumes ONTAP and Azure NetApp Files), to move, protect, and analyze data, and to control many on-prem and edge storage devices.

**NetApp Astra Trident** is a CSI Compliant Storage Orchestrator that enable quick and easy consumption of persistent storage backed by a variety of the above-mentioned NetApp storage options. It is an open-source software maintained and supported by NetApp.

## Astra Trident CSI feature highlights



<b>CSI specific</b> <ul style="list-style-type: none"> <li>CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies</li> <li>CSI topology</li> <li>Volume expansion</li> </ul>	<b>Security</b> <ul style="list-style-type: none"> <li>Dynamic-export policy management</li> <li>iSCSI initiator-groups dynamic management</li> <li>iSCSI bidirectional CHAP</li> </ul>
<b>Control</b> <ul style="list-style-type: none"> <li>Storage and performance consumption</li> <li>Monitoring</li> <li>Volume Import</li> <li>Cross Namespace Volume Access</li> </ul>	<b>Installation methods</b> <ul style="list-style-type: none"> <li>Binary</li> <li>Helm chart</li> <li>Operator</li> <li>GitOps</li> </ul>
<b>Choose your access mode</b> <ul style="list-style-type: none"> <li>RWO (ReadWriteOnce, i.e 1↔1)</li> <li>RWX (ReadWriteMany, i.e 1↔n)</li> <li>ROX (ReadOnlyMany)</li> <li>RWOP (ReadWriteOnce POD)</li> </ul>	<b>Choose your protocol</b> <ul style="list-style-type: none"> <li>NFS</li> <li>SMB</li> <li>iSCSI</li> </ul>

Business critical container workloads need more than just persistent volumes. Their data management requirements require protection and migration of the application kubernetes objects as well.



Application data includes kubernetes objects in addition to the user data: Some examples are as follows:

- kubernetes objects such as pods specs, PVCs, deployments, services
- custom config objects such as config maps and secrets
- persistent data such as Snapshot copies, backups, clones
- custom resources such as CRs and CRDs

**NetApp Astra Control**, available as both fully-managed and self-managed software, provides orchestration for robust application data management. Refer to the [Astra documentation](#) for additional details on the Astra family of products.

This reference documentation provides validation of migration and protection of container-based applications, deployed on RedHat OpenShift container platform, using NetApp Astra Control Center. In addition, the solution provides high-level details for the deployment and the use of Red Hat Advanced Cluster Management (ACM) for managing the container platforms. The document also highlights the details for the integration of NetApp storage with Red Hat OpenShift container platforms using Astra Trident CSI provisioner. Astra Control Center is deployed on the hub cluster and is used to manage the container applications and their persistent storage lifecycle. Finally, it provides a solution for replication and failover and fail-back for container workloads on managed Red Hat OpenShift clusters in AWS (ROSA) using Amazon FSx for NetApp ONTAP (FSxN) as persistent storage.

## Value propositions of NetApp Hybrid Multicloud solutions for Red Hat OpenShift Container workloads

Most customers do not just start out building Kubernetes based environments without any existing infrastructure. Perhaps they are a traditional IT shop running most of their enterprise applications on virtual machines (in large VMware environments for example). Then they start building small container-based environments to satisfy the needs of their modern application development teams. These initiatives usually start small and begin to become more pervasive as the teams learn these new technologies and skills, and begin to recognize the many benefits of adopting them.

The good news for customers is that NetApp can serve the needs of both environments. This set of solutions for hybrid multicloud with Red Hat OpenShift will empower NetApp customers to adopt modern cloud technologies and services without having to overhaul their entire infrastructure and organization. Whether customer applications and data are hosted on-premises, in cloud, run on virtual machines, or on containers, NetApp can provide consistent data management, protection, security, and portability. With these new solutions, the same value NetApp has delivered in on-premises data center environments for decades will be available across the enterprise entire data horizon, without requiring significant investment to retool, acquire new skills, or build new teams. NetApp is positioned well to help customers solve these business challenges regardless of what phase of their cloud journey they are in.

NetApp Hybrid Multi-Cloud with Red Hat Openshift:

- Gives customers validated designs and practices which demonstrate the best ways for customers to manage, protect, secure, and migrate their data and applications when using Red Hat OpenShift with

NetApp based storage solutions.

- Present best practices for customers running Red Hat OpenShift with NetApp storage in VMware environments, bare metal infrastructure, or a combination of both.
- Demonstrate strategies and options for both on-prem and cloud environments, as well as hybrid environments where both are used.

## **Supported Solutions of NetApp Hybrid Multicloud for Red Hat OpenShift Container workloads**

The solution tests and validates Migration & Centralized Data Protection with OpenShift container platform (OCP), OpenShift Advanced Cluster Manager (ACM), NetApp ONTAP, NetApp BlueXP and NetApp Astra Control Center (ACC).

For this solution, the following scenarios are tested and validated by NetApp. The solution is separated into multiple scenarios based on the following characteristics:

- on-premises
- cloud
  - self-managed OpenShift clusters and self-managed NetApp storage
  - provider-managed OpenShift clusters and provider-managed NetApp storage

**We will be building out additional solutions and use cases in the future.**

### **Scenario 1: Data protection and migration within the on-premises environment using ACC**

#### **On-premises: self-managed OpenShift clusters and self-managed NetApp storage**

- Using ACC, create Snapshot copies, backups and restores for data protection.
- Using ACC, perform a SnapMirror replication of container applications.

#### **Scenario 1**



## Scenario 2: Data protection and migration from the on-premises environment to AWS environment using ACC:

**On-premises: Self-managed OpenShift cluster and self-managed storage**

**AWS Cloud: Self-managed OpenShift cluster and self-managed storage**

- Using ACC, perform backups and restores for data protection.
- Using ACC, perform a SnapMirror replication of container applications.

### Scenario 2



### Scenario 3: Data protection and migration from the on-premises environment to AWS environment:

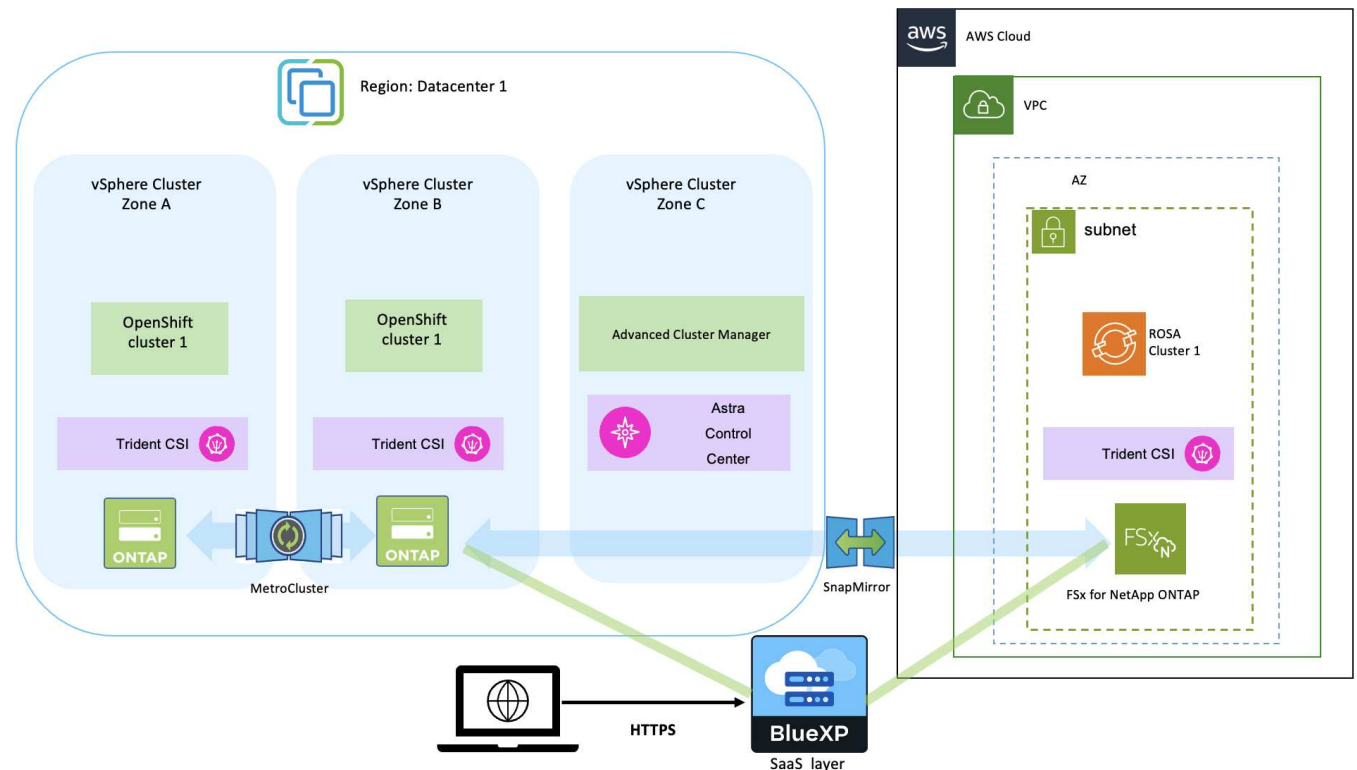
**On-premises: Self-managed OpenShift cluster and self-managed storage**

**AWS Cloud: Provider-managed OpenShift cluster (ROSA) and provider-managed storage (FSxN)**

- Using BlueXP, perform replication of persistent volumes (FSxN).
- Using OpenShift GitOps, recreate application metadata.

### Scenario 3





For considerations when using ONTAP in a MetroCluster configuration, refer [here](#).

## Versions of various components used in the solution validation

The solution tests and validates Migration & Centralized Data Protection with OpenShift container platform, OpenShift Advanced Cluster Manager, NetApp ONTAP, and NetApp Astra Control Center.

Various scenarios of the solution were validated using the versions as shown in the table below:

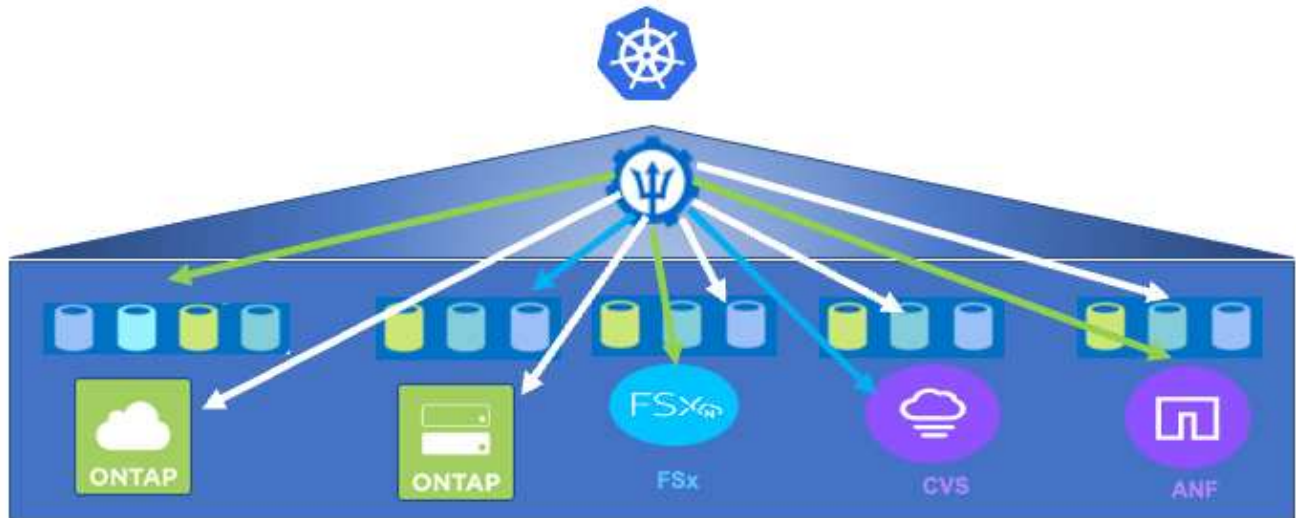
Component	Version
<b>VMware</b>	vSphere Client version 8.0.0.10200 VMware ESXi, 8.0.0, 20842819
<b>Hub Cluster</b>	OpenShift 4.11.34
<b>Source and Destination Clusters</b>	OpenShift 4.12.9 on-premises and in AWS
<b>NetApp Astra Trident</b>	Trident Server and Client 23.04.0
<b>NetApp Astra Control Center</b>	ACC 22.11.0-82
<b>NetApp ONTAP</b>	ONTAP 9.12.1
<b>AWS FSx for NetApp ONTAP</b>	Single AZ

## Supported NetApp Storage integrations with Red Hat Open Shift Containers

Whether the Red Hat Open Shift containers are running on VMware or in the

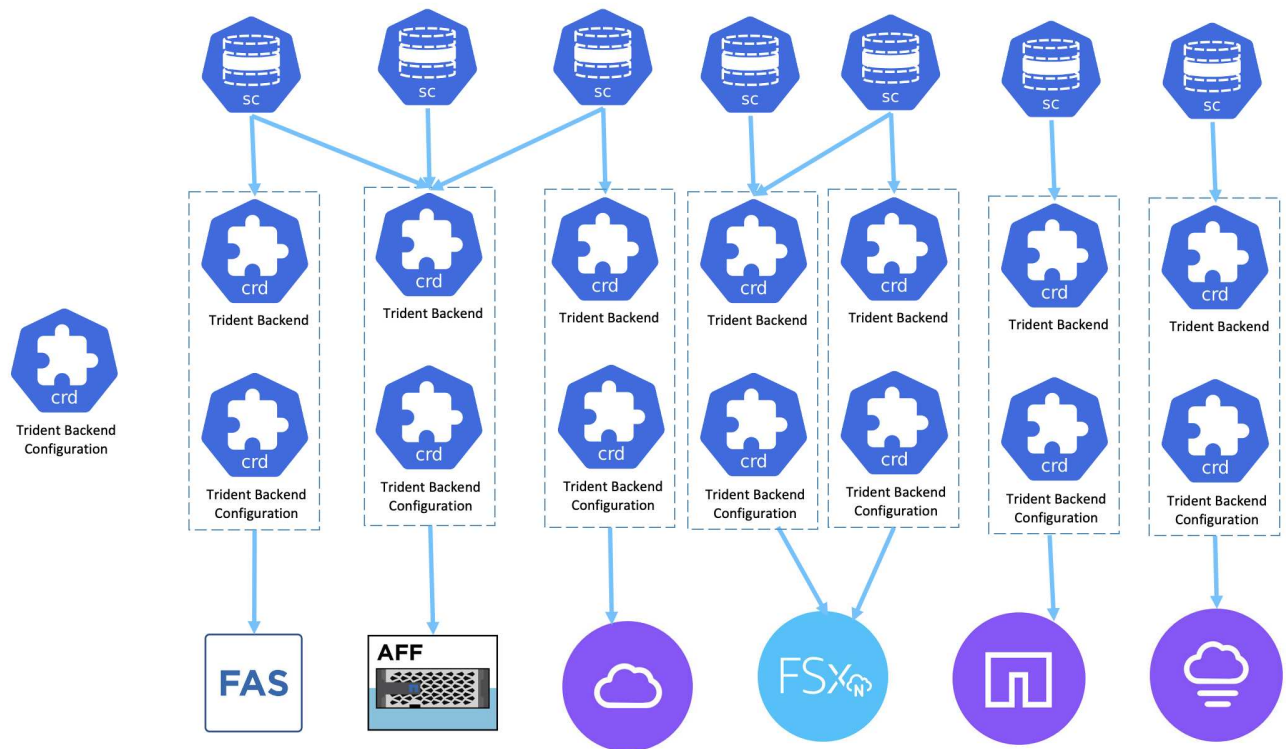
hyperscalers, NetApp Astra Trident can be used as the CSI provisioner for the various types of backend NetApp storage that it supports.

The following diagram depicts the various backend NetApp storage that can be integrated with OpenShift clusters using NetApp Astra Trident.



ONTAP Storage Virtual Machine (SVM) provides secure multi-tenancy. A Single OpenShift cluster can connect to single SVM or multiple SVMs or even to multiple ONTAP clusters. Storage class filters the backend storage based on parameters or by labels. Storage administrators define the parameters to connect to storage system using trident backend configuration. On successful connection establishment, it creates the trident backend and populates the information which the storage class can filter.

The relationship between the storageclass and backend is shown below.



Application owner requests persistent volume using storage class. The storage class filters the backend storage.

The relationship between the pod and backend storage is shown below.



## Container Storage Interface (CSI) Options

On vSphere environments, customers can pick VMware CSI driver and/or Astra Trident CSI to integrate with ONTAP. With VMware CSI, the persistent volumes are consumed as local SCSI disks, whereas with Trident, it is consumed with network.

As VMware CSI does not support RWX access modes with ONTAP, applications need to use Trident CSI if RWX mode is required. With FC based deployments, VMware CSI is preferred and SnapMirror Business Continuity (SMBC) provides zone level high availability.

## VMware CSI supports

- Core Block based datastores (FC, FCoE, iSCSI, NVMeoF)
- Core File based datastores (NFS v3, v4)
- vVol datastores (block and file)

## Trident has following drivers to support ONTAP

- ontap-san (dedicated volume)
- ontap-san-economy (shared volume)
- ontap-nas (dedicated volume)
- ontap-nas-economy (shared volume)
- ontap-nas-flexgroup (dedicated large scale volume)

For both VMware CSI and Astra Trident CSI, ONTAP supports nconnect, session trunking, kerberos, etc. for NFS and multipathing, chap authentication, etc. for block protocols.

In AWS, FSx for NetApp ONTAP (FSxN) can be deployed in single Availability Zone (AZ) or in Multi AZ. For production workloads that requires high availability, multi-AZ provides zonal level fault tolerance and has better NVMe read cache compared to single AZ. For more info, check [AWS performance guidelines](#).

To save cost on disaster recovery site, single AZ FSx ONTAP can be utilized.



For number of SVMs that are supported by FSx ONTAP, refer [managing FSx ONTAP storage virtual machine](#)

## NetApp Hybrid Multicloud solutions for Red Hat OpenShift Container workloads

## Overview

NetApp is seeing a significant increase in customers modernizing their legacy enterprise applications and building new applications using containers and orchestration platforms built around Kubernetes. Red Hat OpenShift Container Platform is one example that we see adopted by many of our customers.

As more and more customers begin adopting containers within their enterprises, NetApp is perfectly positioned to help serve the persistent storage needs of their stateful applications and classic data management needs such as data protection, data security, and data migration. However, these needs are met using different strategies, tools, and methods.

**NetApp ONTAP** based storage options listed below, deliver security, data protection, reliability, and flexibility for containers and Kubernetes deployments.

- Self-managed storage in on-premises:
  - NetApp Fabric Attached Storage (FAS), NetApp All Flash FAS Arrays (AFF), NetApp All SAN Array (ASA) and ONTAP Select
- Provider-managed storage in on-premises:
  - NetApp Keystone provides Storage as a Service (STaaS)
- Self-managed storage in the cloud:
  - NetApp Cloud Volumes ONTAP(CVO) provide self managed storage in the hyperscalers
- Provider-managed storage in the cloud:
  - Cloud Volumes Service for Google Cloud (CVS), Azure NetApp Files (ANF), Amazon FSx for NetApp ONTAP offer fully managed storage in the hyperscalers

## ONTAP feature highlights



<b>Storage Administration</b> <ul style="list-style-type: none"><li>• Multi-tenancy</li><li>• FlexVol &amp; FlexGroup</li><li>• LUN</li><li>• Quotas</li><li>• ONTAP CLI &amp; API</li><li>• System Manager &amp; BlueXP</li></ul>	<b>Performance &amp; Scalability</b> <ul style="list-style-type: none"><li>• FlexCache</li><li>• FlexClone</li><li>• nconnect, session trunking, multipathing</li><li>• Scale-out clusters</li></ul>
<b>Availability &amp; Resilience</b> <ul style="list-style-type: none"><li>• Multi-AZ HA deployment (MetroCluster)</li><li>• SnapShot &amp; SnapRestore</li><li>• SnapMirror</li><li>• SnapMirror Business Continuity</li><li>• SnapMirror Cloud</li></ul>	<b>Access Protocols</b> <ul style="list-style-type: none"><li>• NFS –v3, v4, v4.1, v4.2</li><li>• SMB – v2, v3</li><li>• iSCSI</li><li>• Multi-protocol access</li></ul>
<b>Storage Efficiency</b> <ul style="list-style-type: none"><li>• Deduplication &amp; Compression</li><li>• Compaction</li><li>• Thin provisioning</li><li>• Data Tiering (Fabric Pool)</li></ul>	<b>Security &amp; Compliance</b> <ul style="list-style-type: none"><li>• Fpolicy &amp; Vscan</li><li>• Active Directory integration</li><li>• LDAP &amp; Kerberos</li><li>• Certificate based authentication</li></ul>

**NetApp BlueXP** enables you to manage all of your storage and data assets from a single control plane/interface.

You can use BlueXP to create and administer cloud storage (for example, Cloud Volumes ONTAP and Azure

NetApp Files), to move, protect, and analyze data, and to control many on-prem and edge storage devices.

**NetApp Astra Trident** is a CSI Compliant Storage Orchestrator that enable quick and easy consumption of persistent storage backed by a variety of the above-mentioned NetApp storage options. It is an open-source software maintained and supported by NetApp.

## Astra Trident CSI feature highlights



<b>CSI specific</b> <ul style="list-style-type: none"><li>• CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies</li><li>• CSI topology</li><li>• Volume expansion</li></ul>	<b>Security</b> <ul style="list-style-type: none"><li>• Dynamic-export policy management</li><li>• iSCSI initiator-groups dynamic management</li><li>• iSCSI bidirectional CHAP</li></ul>
<b>Control</b> <ul style="list-style-type: none"><li>• Storage and performance consumption</li><li>• Monitoring</li><li>• Volume Import</li><li>• Cross Namespace Volume Access</li></ul>	<b>Installation methods</b> <ul style="list-style-type: none"><li>• Binary</li><li>• Helm chart</li><li>• Operator</li><li>• GitOps</li></ul>
<b>Choose your access mode</b> <ul style="list-style-type: none"><li>• RWO (ReadWriteOnce, i.e 1↔1)</li><li>• RWX (ReadWriteMany, i.e 1↔n)</li><li>• ROX (ReadOnlyMany)</li><li>• RWOP (ReadWriteOnce POD)</li></ul>	<b>Choose your protocol</b> <ul style="list-style-type: none"><li>• NFS</li><li>• SMB</li><li>• iSCSI</li></ul>

Business critical container workloads need more than just persistent volumes. Their data management requirements require protection and migration of the application kubernetes objects as well.



Application data includes kubernetes objects in addition to the user data: Some examples are as follows:

- kubernetes objects such as pods specs, PVCs, deployments, services
- custom config objects such as config maps and secrets
- persistent data such as Snapshot copies, backups, clones
- custom resources such as CRs and CRDs

**NetApp Astra Control**, available as both fully-managed and self-managed software, provides orchestration for robust application data management. Refer to the [Astra documentation](#) for additional details on the Astra family of products.

This reference documentation provides validation of migration and protection of container-based applications, deployed on RedHat OpenShift container platform, using NetApp Astra Control Center. In addition, the solution provides high-level details for the deployment and the use of Red Hat Advanced Cluster Management (ACM) for managing the container platforms. The document also highlights the details for the integration of NetApp storage with Red Hat OpenShift container platforms using Astra Trident CSI provisioner. Astra Control Center is deployed on the hub cluster and is used to manage the container applications and their persistent storage lifecycle. Finally, it provides a solution for replication and failover and fail-back for container workloads on managed Red Hat OpenShift clusters in AWS (ROSA) using Amazon FSx for NetApp ONTAP (FSxN) as persistent storage.



## NetApp Solution with Red Hat OpenShift Container platform workloads on VMware

If customers have a need to run their modern containerized applications on infrastructure in their private data centers, they can do so. They should plan and deploy the Red Hat OpenShift container platform (OCP) for a successful production-ready environment for deploying their container workloads. Their OCP clusters can be deployed on VMware or bare metal.

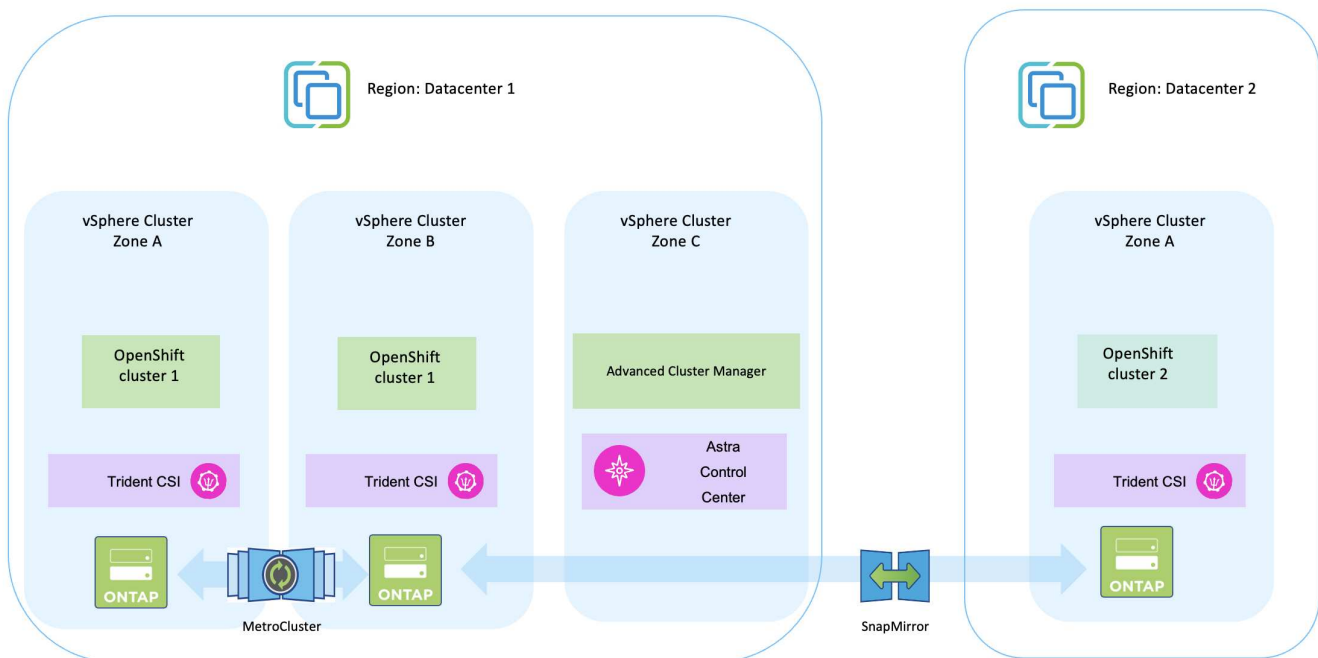
NetApp ONTAP storage delivers data protection, reliability, and flexibility for container deployments. Astra Trident serves as the dynamic storage provisioner to consume persistent ONTAP storage for customers' stateful applications. Astra Control Center can be used to orchestrate the many data management requirements of stateful applications such as data protection, migration, and business continuity.

With VMware vSphere, NetApp ONTAP tools provides a vCenter Plugin which can be utilized to provision datastores. Apply tags and use it with OpenShift for storing the node configuration and data. NVMe based storage provides lower latency and high performance.

This solution provides details for data protection and migration of container workloads using Astra Control Center. For this solution, the container workloads are deployed on Red Hat OpenShift clusters on vSphere within the on-premises environment.

NOTE: We will provide a solution for container workloads on OpenShift clusters on bare metal in the future.

### Data protection and migration solution for OpenShift Container workloads using Astra Control Center



## Deploy and configure the Red Hat OpenShift Container platform on VMware

This section describes a high-level workflow of how to set up and manage OpenShift clusters and manage stateful applications on them. It shows the use of NetApp ONTAP storage arrays with the help of Astra Trident to provide persistent volumes. Details are

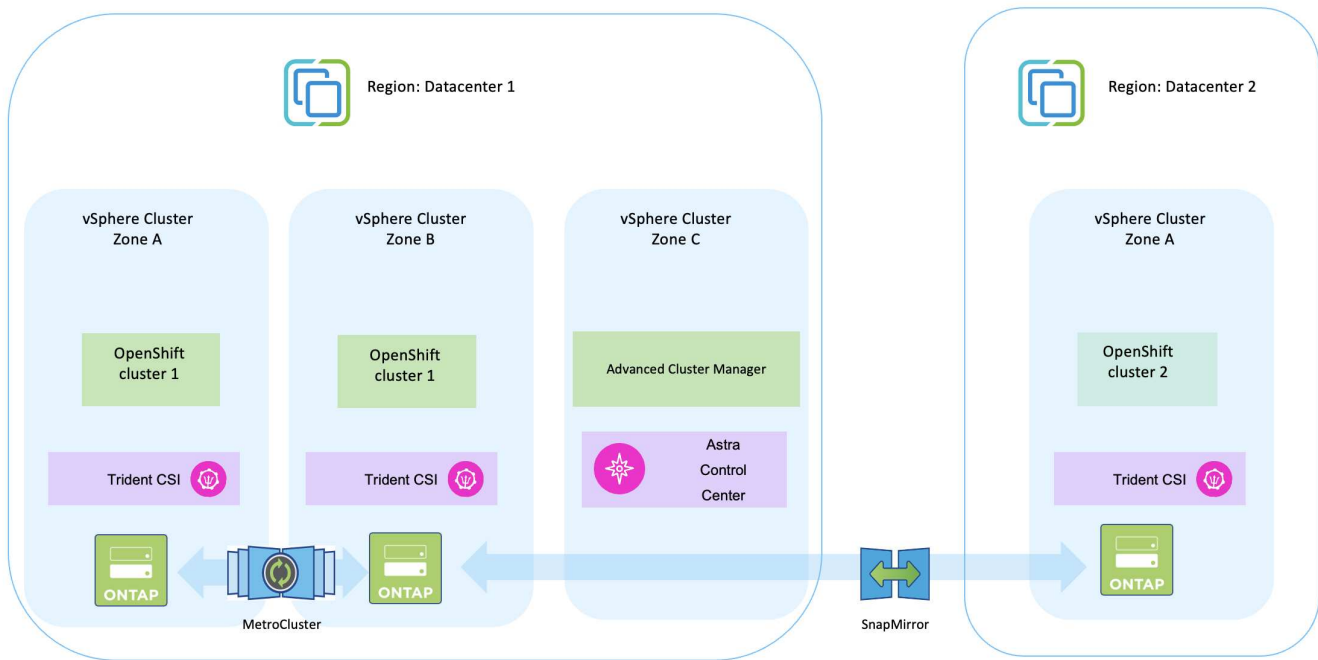


provided about the use of Astra Control Center to perform data protection and migration activities for the stateful applications.



There are several ways of deploying Red Hat OpenShift Container platform clusters. This high-level description of the setup provides documentation links for the specific method that was used. You can refer to the other methods in the relevant links provided in the [resources section](#).

Here is a diagram that depicts the clusters deployed on VMware in a data center.



The setup process can be broken down into the following steps:

#### Deploy and configure a CentOS VM

- It is deployed in the VMware vSphere environment.
- This VM is used for deploying some components such as NetApp Astra Trident and NetApp Astra Control Center for the solution.
- A root user is configured on this VM during installation.

## Deploy and configure an OpenShift Container Platform cluster on VMware vSphere (Hub Cluster)

Refer to the instructions for the [Assisted deployment](#) method to deploy an OCP cluster.



Remember the following:

- Create ssh public and private key to provide to the installer. These keys will be used to login to the master and worker nodes if needed.
- Download the installer program from the assisted installer. This program is used to boot the VMs that you create in the VMware vSphere environment for the master and worker nodes.
- VMs should have the minimum CPU, memory, and hard disk requirement. (Refer to the vm create commands on [this](#) page for the master and the worker nodes which provide this information)
- The diskUUID should be enabled on all VMs.
- Create a minimum of 3 nodes for master and 3 nodes for worker.
- Once they are discovered by the installer, turn on the VMware vSphere integration toggle button.

### Install Advanced Cluster Management on the Hub cluster

This is installed using the Advanced Cluster Management Operator on the Hub Cluster.  
Refer to the instructions [here](#).

### Install an internal Red Hat Quay registry on the Hub Cluster.

- An internal registry is required to push the Astra image. A Quay internal registry is installed using the Operator in the Hub cluster.
- Refer to the instructions [here](#)

### Install two additional OCP clusters (Source and Destination)

- The additional clusters can be deployed using the ACM on the Hub Cluster.
- Refer to the instructions [here](#).

### Configure NetApp ONTAP storage

- Install an ONTAP cluster with connectivity to the OCP VMs in VMWare environment.
- Create an SVM.
- Configure NAS data lif to access the storage in SVM.

## Install NetApp Trident on the OCP clusters

- Install NetApp Trident on all three clusters: Hub, source, and destination clusters
- Refer to the instructions [here](#).
- Create a storage backend for ontap-nas .
- Create a storage class for ontap-nas.
- Refer to instructions [here](#).

## Install NetApp Astra Control Center

- NetApp Astra Control Center is installed using the Astra Operator on the Hub Cluster.
- Refer to the instructions [here](#).

Points to remember:

- \* Download NetApp Astra Control Center image from the support site.
- \* Push the image to an internal registry.
- \* Refer to instructions [here](#).

## Deploy an Application on Source Cluster

Use OpenShift GitOps to deploy an application. (eg. Postgres, Ghost)

## Add the Source and Destination clusters into Astra Control Center.

After you add a cluster to Astra Control management, you can install apps on the cluster (outside of Astra Control) and then go to the Applications page in Astra Control to define the apps and their resources. Refer to [Start managing apps section of Astra Control Center](#).

The next step is to use the Astra Control Center for Data protection and Data migration from the source to the destination cluster.

## Data protection using Astra

This page shows the data protection options for Red Hat OpenShift Container based applications running on VMware vSphere using Astra Control Center (ACC).

As users take their journey of modernizing their applications with Red Hat OpenShift, a data protection strategy should be in place to protect them from accidental deletion or any other human errors. Often a protection strategy is also required for regulatory or compliance purposes to protect their data from a disaster.

The requirements of data protection varies from reverting back to a point in time copy to automatically failing over to a different fault domain without any human intervention. Many customers pick ONTAP as their preferred storage platform for their Kubernetes applications because of its rich features like multitenancy, multi-protocol, high performance and capacity offerings, replication and caching for multi-site locations, security and flexibility.

Data protection in ONTAP can be achieved using ad-hoc or policy controlled

### - Snapshot

## - backup and restore

Both Snapshot copies and backups protect the following types of data:

- **The application metadata that represents the state of the application**
- **Any persistent data volumes associated with the application**
- **Any resource artifacts belonging to the application**

## Snapshot with ACC

A point in time copy of data can be captured using Snapshot with ACC. Protection policy defines the number of Snapshot copies to keep. Minimum schedule option available is hourly. Manual, on-demand Snapshot copies can be taken at any time and at shorter intervals than scheduled Snapshot copies. Snapshot copies are stored on the same provisioned volume as the app.

## Configuring Snapshot with ACC

Name	State	Hook state	On-Schedule / On-Demand	Created	Actions
replication-schedule-wodfw-50aug	Healthy	Healthy	On-Schedule	2023/04/26 19:50 UTC	
ghost-snapshot-20230426155028	Healthy	Healthy	On-Schedule	2023/04/26 15:50 UTC	
ghost-snapshot-20230426145026	Healthy	Healthy	On-Schedule	2023/04/26 14:50 UTC	
ghost-snapshot-20230416182551	Healthy	Healthy	On-Demand	2023/04/16 18:25 UTC	

## Backup and Restore with ACC

A backup is based on a Snapshot. ACC can take Snapshot copies using CSI and perform backup using the point in time Snapshot copy. The backup is stored in an external object store (any s3 compatible including ONTAP S3 at a different location). Protection policy can be configured for scheduled backups and the number of backup versions to keep. The minimum RPO is one hour.

## Restoring an application from a backup using ACC

ACC restores application from the S3 bucket where the backups are store.

Name	State	Hook state	On-Schedule / On-Demand	Bucket	Created	Actions
hourly-bat5u-bpc7m	Healthy	Healthy	On-Schedule	astra	2023/04/26 15:50 UTC	<div>Restore application Delete backup</div>

## Application specific execution hooks

In addition, execution hooks can be configured to run in conjunction with a data protection operation of a managed app. Even though storage array level data protection features are available, often additional steps are needed to make backups and restores, application consistent. The app-specific additional steps could be:

- before or after a Snapshot copy is created.
- before or after a backup is created.
- after restoring from a Snapshot copy or backup.

Astra Control can execute these app-specific steps coded as custom scripts called execution hooks.

[NetApp Verda GitHub project](#) provides execution hooks for popular cloud-native applications to make protecting applications straightforward, robust, and easy to orchestrate. Feel free to contribute to that project if you have enough information for an application that is not in the repository.

### Sample execution hook for pre-Snapshot of a redis application.

Edit execution hook

HOOK DETAILS ?

Operation

Pre-snapshot

Hook arguments (optional)

1 pre

Enter hook arguments

Hook name

redis-pre-snapshot

CONTAINER IMAGES ?

☐ Apply to all container images

Use a regular expression to target container images for the hook.

Container image names to match

redis

SCRIPT ?

+ Add

Search

Name ↓

☐ mariadb\_mysql.sh

☐ postgresql.sh

☒ redis\_hook.sh

EXECUTION HOOKS

Execution hooks allow Astra Control to execute your own custom scripts before or after a snapshot.

Read more in [Manage application execution hooks](#)

Cancel

Save ✓

## Replication with ACC

For regional protection or for a low RPO and RTO solution, an application can be replicated to another Kubernetes instance running at a different site, preferably in another region. ACC utilizes ONTAP async SnapMirror with RPO as low as 5 minutes. Replication is done by replicating to ONTAP and then a fail over

creates the Kubernetes resources in the destination cluster.



Note that replication is different from the backup and restore where the backup goes to S3 and restore is performed from S3. Refer [xref:./rhhc/on-premises/ here](#) to get additional details about the differences between the two types of data protection.

Refer [here](#) for SnapMirror setup instructions.

## SnapMirror with ACC

The screenshot shows the Astra Control Center interface for configuring SnapMirror. The left sidebar contains navigation links: Dashboard, Applications, Clusters, Cloud instances, Backends, Buckets, Account, Activity, and Support. The main content area is titled 'ghost' and shows the application status as 'Healthy'. Below this, there are tabs for Data protection, Storage, Resources, Execution hooks, Activity, and Tasks. The 'Data protection' tab is active, showing a replication relationship between a source cluster 'ghost-cluster5' and a destination cluster 'ghost-cluster7'. The replication is scheduled every 5 minutes and the last sync was on 2023/04/26 at 19:16 UTC. A diagram shows the data flow from the source to the destination.



san-economy and nas-economy storage drivers do not support replication feature. Refer [here](#) for additional details.

## Demo video:

[Demonstration video of disaster recovery with Astra Control Center](#)

## Business Continuity with MetroCluster

Most of our hardware platform for ONTAP has high availability features to protect from device failures avoiding the need to perform disaster recovery. But to protect from fire or any other disaster and to continue the business with zero RPO and low RTO, often a MetroCluster solution is used.

Customers who currently have an ONTAP system can extend to MetroCluster by adding supported ONTAP systems within the distance limitations for providing zone level disaster recovery.

Astra Trident, the CSI (Container Storage Interface) supports NetApp ONTAP including MetroCluster configuration as well as other options like Cloud Volumes ONTAP, Azure NetApp Files, AWS FSx for NetApp ONTAP, etc. Astra Trident provides five storage driver options for ONTAP and all are supported for MetroCluster configuration. Refer [here](#) for additional details about ONTAP storage drivers supported by Astra Trident.

The MetroCluster solution requires layer 2 network extension or capability to access the same network address from both fault domains. Once MetroCluster configuration is in place, the solution is transparent to application owners as all the volumes in the MetroCluster svm are protected and get the benefits of SyncMirror (zero RPO).



For Trident Backend Configuration (TBC), do not specify the dataLIF and SVM when using MetroCluster configuration. Specify SVM management IP for managementLIF and use vsadmin role credentials.

Details on Astra Control Center Data Protection features are available [here](#)

## Data migration using Astra Control Center

This page shows the data migration options for container workloads on Red Hat OpenShift clusters with Astra Control Center (ACC).

Kubernetes Applications are often required to be moved from one environment to another. To migrate an application along with its persistent data, NetApp ACC can be utilized.

### Data Migration between different Kubernetes environment

ACC supports various Kubernetes flavors including Google Anthos, Red Hat OpenShift, Tanzu Kubernetes Grid, Rancher Kubernetes Engine, Upstream Kubernetes, etc. For additional details, refer [here](#).

To migrate application from one cluster to another, you can use one of the following features of ACC:

- replication
- backup and restore
- clone

Refer to the [data protection section](#) for the **replication and backup and restore** options.  
Refer [here](#) for additional details about **cloning**.



Astra Replication feature is only supported with Trident Container Storage Interface (CSI). However, replication is not supported by nas-economy & san-economy drivers.

## Performing data replication using ACC

The screenshot displays the Astra management console interface. On the left is a sidebar with navigation links: Dashboard, Applications, Clusters, Cloud instances, Backends, Buckets, Account, Activity, and Support. The main content area is titled 'ghost' and shows the 'APPLICATION STATUS' as 'Healthy'. Below this, it indicates the 'Definition' is 'ghost-zonea' and the 'Cluster' is 'ocp-cluster5'. The 'APPLICATION PROTECTION' section shows three status indicators: 'Fully protected', 'Protection policy configured', and 'Replication policy configured'. A 'Data protection' tab is active, showing a 'Configure' button. On the right, an 'Actions' dropdown menu is open, listing options: Snapshot, Back up, Clone, Restore, Fail over, Reverse replication, and Unmanage. Below the main configuration area, a diagram illustrates the replication relationship between a 'Source' cluster (ghost, Healthy, ocp-cluster5, ghost-zonea, Active site) and a 'Destination' cluster (ghost, Healthy, ocp-cluster7, blog-zoneb). On the far right, a 'Replication relationship' panel shows the 'STATUS' as 'Healthy' and 'Established', the 'SCHEDULE' as 'Replicate snapshot every 5 minutes to ocp-cluster7', and the 'LAST SYNC' as '2023/04/26 19:16 UTC' with a 'Sync duration: 30 seconds'.

# NetApp Hybrid Multicloud solutions for Red Hat OpenShift Container workloads

## Overview

NetApp is seeing a significant increase in customers modernizing their legacy enterprise applications and building new applications using containers and orchestration platforms built around Kubernetes. Red Hat OpenShift Container Platform is one example that we see adopted by many of our customers.

As more and more customers begin adopting containers within their enterprises, NetApp is perfectly positioned to help serve the persistent storage needs of their stateful applications and classic data management needs such as data protection, data security, and data migration. However, these needs are met using different strategies, tools, and methods.

**NetApp ONTAP** based storage options listed below, deliver security, data protection, reliability, and flexibility for containers and Kubernetes deployments.



- Self-managed storage in on-premises:
  - NetApp Fabric Attached Storage (FAS), NetApp All Flash FAS Arrays (AFF), NetApp All SAN Array (ASA) and ONTAP Select
- Provider-managed storage in on-premises:
  - NetApp Keystone provides Storage as a Service (STaaS)
- Self-managed storage in the cloud:
  - NetApp Cloud Volumes ONTAP(CVO) provide self managed storage in the hyperscalers
- Provider-managed storage in the cloud:
  - Cloud Volumes Service for Google Cloud (CVS), Azure NetApp Files (ANF), Amazon FSx for NetApp ONTAP offer fully managed storage in the hyperscalers

## ONTAP feature highlights



<b>Storage Administration</b> <ul style="list-style-type: none"> <li>• Multi-tenancy</li> <li>• FlexVol &amp; FlexGroup</li> <li>• LUN</li> <li>• Quotas</li> <li>• ONTAP CLI &amp; API</li> <li>• System Manager &amp; BlueXP</li> </ul>	<b>Performance &amp; Scalability</b> <ul style="list-style-type: none"> <li>• FlexCache</li> <li>• FlexClone</li> <li>• nconnect, session trunking, multipathing</li> <li>• Scale-out clusters</li> </ul>
<b>Availability &amp; Resilience</b> <ul style="list-style-type: none"> <li>• Multi-AZ HA deployment (MetroCluster)</li> <li>• SnapShot &amp; SnapRestore</li> <li>• SnapMirror</li> <li>• SnapMirror Business Continuity</li> <li>• SnapMirror Cloud</li> </ul>	<b>Access Protocols</b> <ul style="list-style-type: none"> <li>• NFS –v3, v4, v4.1, v4.2</li> <li>• SMB – v2, v3</li> <li>• iSCSI</li> <li>• Multi-protocol access</li> </ul>
<b>Storage Efficiency</b> <ul style="list-style-type: none"> <li>• Deduplication &amp; Compression</li> <li>• Compaction</li> <li>• Thin provisioning</li> <li>• Data Tiering (Fabric Pool)</li> </ul>	<b>Security &amp; Compliance</b> <ul style="list-style-type: none"> <li>• Fpolicy &amp; Vscan</li> <li>• Active Directory integration</li> <li>• LDAP &amp; Kerberos</li> <li>• Certificate based authentication</li> </ul>

**NetApp BlueXP** enables you to manage all of your storage and data assets from a single control plane/interface.

You can use BlueXP to create and administer cloud storage (for example, Cloud Volumes ONTAP and Azure NetApp Files), to move, protect, and analyze data, and to control many on-prem and edge storage devices.

**NetApp Astra Trident** is a CSI Compliant Storage Orchestrator that enable quick and easy consumption of persistent storage backed by a variety of the above-mentioned NetApp storage options. It is an open-source software maintained and supported by NetApp.

## Astra Trident CSI feature highlights



<b>CSI specific</b> <ul style="list-style-type: none"><li>• CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies</li><li>• CSI topology</li><li>• Volume expansion</li></ul>	<b>Security</b> <ul style="list-style-type: none"><li>• Dynamic-export policy management</li><li>• iSCSI initiator-groups dynamic management</li><li>• iSCSI bidirectional CHAP</li></ul>
<b>Control</b> <ul style="list-style-type: none"><li>• Storage and performance consumption</li><li>• Monitoring</li><li>• Volume Import</li><li>• Cross Namespace Volume Access</li></ul>	<b>Installation methods</b> <ul style="list-style-type: none"><li>• Binary</li><li>• Helm chart</li><li>• Operator</li><li>• GitOps</li></ul>
<b>Choose your access mode</b> <ul style="list-style-type: none"><li>• RWO (ReadWriteOnce, i.e 1↔1)</li><li>• RWX (ReadWriteMany, i.e 1↔n)</li><li>• ROX (ReadOnlyMany)</li><li>• RWOP (ReadWriteOnce POD)</li></ul>	<b>Choose your protocol</b> <ul style="list-style-type: none"><li>• NFS</li><li>• SMB</li><li>• iSCSI</li></ul>

Business critical container workloads need more than just persistent volumes. Their data management requirements require protection and migration of the application kubernetes objects as well.



Application data includes kubernetes objects in addition to the user data: Some examples are as follows:

- kubernetes objects such as pods specs, PVCs, deployments, services
- custom config objects such as config maps and secrets
- persistent data such as Snapshot copies, backups, clones
- custom resources such as CRs and CRDs

**NetApp Astra Control**, available as both fully-managed and self-managed software, provides orchestration for robust application data management. Refer to the [Astra documentation](#) for additional details on the Astra family of products.

This reference documentation provides validation of migration and protection of container-based applications, deployed on RedHat OpenShift container platform, using NetApp Astra Control Center. In addition, the solution provides high-level details for the deployment and the use of Red Hat Advanced Cluster Management (ACM) for managing the container platforms. The document also highlights the details for the integration of NetApp storage with Red Hat OpenShift container platforms using Astra Trident CSI provisioner. Astra Control Center is deployed on the hub cluster and is used to manage the container applications and their persistent storage lifecycle. Finally, it provides a solution for replication and failover and fail-back for container workloads on managed Red Hat OpenShift clusters in AWS (ROSA) using Amazon FSx for NetApp ONTAP (FSxN) as persistent storage.

## NetApp Solution with Red Hat OpenShift Container platform workloads in Hybrid Cloud

Customers may be at a point in their modernization journey when they are ready to move some select workloads or all workloads from their data centers to the cloud. They may choose to use self-managed OpenShift containers and self-managed NetApp storage in the cloud for various reasons. They should plan and deploy the Red Hat OpenShift

container platform (OCP) in the cloud for a successful production-ready environment for migrating their container workloads from their data centers. Their OCP clusters can be deployed on VMware or Bare Metal in their data centers and on AWS, Azure or Google Cloud in the cloud environment.

NetApp Cloud Volumes ONTAP storage delivers data protection, reliability, and flexibility for container deployments in AWS, Azure and in Google Cloud. Astra Trident serves as the dynamic storage provisioner to consume the persistent Cloud Volumes ONTAP storage for customers' stateful applications. Astra Control Center can be used to orchestrate the many data management requirements of stateful applications such as data protection, migration, and business continuity.

### Data protection and migration solution for OpenShift Container workloads in a hybrid cloud using Astra Control Center



### Deploy and configure the Red Hat OpenShift Container platform on AWS

This section describes a high-level workflow of how to set up and manage OpenShift Clusters in AWS and deploy stateful applications on them. It shows the use of NetApp Cloud Volumes ONTAP storage with the help of Astra Trident to provide persistent volumes. Details are provided about the use of Astra Control Center to perform data protection and migration activities for the stateful applications.



There are several ways of deploying Red Hat OpenShift Container platform clusters on AWS. This high-level description of the setup provides documentation links for the specific method that was used. You can refer to the other methods in the relevant links provided in the [resources section](#).

Here is a diagram that depicts the clusters deployed on AWS and connected to the data center using a VPN.



The setup process can be broken down into the following steps:

#### Install an OCP cluster on AWS from the Advanced Cluster Management.

- Create a VPC with a site-to-site VPN connection (using pfSense) to connect to the on-premises network.
- On-premises network has internet connectivity.
- Create 3 private subnets in 3 different AZs.
- Create a Route 53 private hosted zone and a DNS resolver for the VPC.

Create OpenShift Cluster on AWS from the Advanced Cluster Management (ACM) Wizard. Refer to instructions [here](#).



You can also create the cluster in AWS from the OpenShift Hybrid Cloud console. Refer [here](#) for instructions.



When creating the cluster using the ACM, you have the ability to customize the installation by editing the yaml file after filling in the details in the form view. After the cluster is created, you can ssh login to the nodes of the cluster for troubleshooting or additional manual configuration. Use the ssh key you provided during installation and the username core to login.

## Deploy Cloud Volumes ONTAP in AWS using BlueXP.

- Install the connector in on-premises VMware environment. Refer to instructions [here](#).
- Deploy a CVO instance in AWS using the connector. Refer to instructions [here](#).



The connector can also be installed in the cloud environment. Refer [here](#) for additional information.

## Install Astra Trident in the OCP Cluster

- Deploy Trident Operator using Helm.  
Refer to instructions [here](#)
- Create a backend and a storage class. Refer to instructions [here](#).

## Add the OCP cluster on AWS to the Astra Control Center.

Add the OCP cluster in AWS to Astra Control Center.

## Using CSI Topology feature of Trident for multi-zone architectures

Cloud providers, today, enable Kubernetes/OpenShift cluster administrators to spawn nodes of the clusters that are zone based. Nodes can be located in different availability zones within a region, or across various regions. To facilitate the provisioning of volumes for workloads in a multi-zone architecture, Astra Trident uses CSI Topology. Using the CSI Topology feature, access to volumes can be limited to a subset of nodes, based on regions and availability zones. Refer [here](#) for additional details.



Kubernetes supports two volume binding modes:

- When **VolumeBindingMode is set to Immediate** (default), Astra Trident creates the volume without any topology awareness. Persistent Volumes are created without having any dependency on the requesting pod's scheduling requirements.
- When **VolumeBindingMode set to WaitForFirstConsumer**, the creation and binding of a Persistent Volume for a PVC is delayed until a pod that uses the PVC is scheduled and created. This way, volumes are created to meet the scheduling constraints that are enforced by topology requirements.

Astra Trident storage backends can be designed to selectively provision volumes based on availability zones (Topology-aware backend). For StorageClasses that make use of such a backend, a volume would only be created if requested by an application that is scheduled in a supported region/zone. (Topology-aware StorageClass)

Refer [here](#) for additional details.

## Data protection using Astra Control Center

This page shows the data protection options for Red Hat OpenShift Container based applications running on VMware vSphere using Astra Control Center (ACC).

As users take their journey of modernizing their applications with Red Hat OpenShift, a data protection strategy should be in place to protect them from accidental deletion or any other human errors. Often a protection strategy is also required for regulatory or compliance purposes to protect their data from a disaster.

The requirements of data protection varies from reverting back to a point in time copy to automatically failing over to a different fault domain without any human intervention. Many customers pick ONTAP as their preferred storage platform for their Kubernetes applications because of its rich features like multitenancy, multi-protocol, high performance and capacity offerings, replication and caching for multi-site locations, security and flexibility.

Customers may have a cloud environment setup as their data center extension, so that they can leverage the benefits of the cloud as well as be well positioned to move their workloads at a future time. For such customers, backing up of their OpenShift applications and their data to the cloud environment becomes an inevitable choice. They can then restore the applications and the associated data either to an OpenShift cluster in the cloud or in their data center.

## Backup and Restore with ACC

Application owners can review and update the applications discovered by ACC. ACC can take Snapshot copies using CSI and perform backup using the point in time Snapshot copy. Backup destination can be an object store in the cloud environment. Protection policy can be configured for scheduled backups and the number of backup versions to keep. The minimum RPO is one hour.

### Restoring an application from a backup using ACC



## Application specific execution hooks

Even though storage array level data protection features are available, often additional steps are needed to make backups and restores application consistent. The app-specific additional steps could be:

- before or after a Snapshot copy is created.
- before or after a backup is created.
- after restoring from a Snapshot copy or backup.

Astra Control can execute these app-specific steps coded as custom scripts called execution hooks.

NetApp's [open source project Verda](#) provides execution hooks for popular cloud-native applications to make protecting applications straightforward, robust, and easy to orchestrate. Feel free to contribute to that project if you have enough information for an application that is not in the repository.

### Sample execution hook for pre-Snapshot of a redis application.

**Edit execution hook**
×

HOOK DETAILS ?

Operation

Pre-snapshot

▼

Hook arguments (optional)

1 pre ×

?

Enter hook arguments

Hook name

redis-pre-snapshot

CONTAINER IMAGES ?

☐
Apply to all container images

Use a regular expression to target container images for the hook.

Container image names to match

redis

SCRIPT ?

+ Add

Search

Name ↓

☐ mariadb\_mysql.sh

☐ postgresql.sh

☒ redis\_hook.sh

EXECUTION HOOKS

Execution hooks allow Astra Control to execute your own custom scripts before or after a snapshot.

Read more in

[Manage application execution hooks](#)

Cancel

Save ✓

## Replication with ACC

For regional protection or for a low RPO and RTO solution, an application can be replicated to another Kubernetes instance running at a different site, preferably in another region. ACC utilizes ONTAP async SnapMirror with RPO as low as 5 minutes.

Refer [here](#) for SnapMirror setup instructions.

## SnapMirror with ACC

29



san-economy and nas-economy storage drivers do not support replication feature. Refer [here](#) for additional details.

#### Demo video:

[Demonstration video of disaster recovery with Astra Control Center](#)

Details on Astra Control Center Data Protection features are available [here](#)

## Data migration using Astra Control Center

This page shows the data migration options for container workloads on Red Hat OpenShift clusters with Astra Control Center (ACC). Specifically, customers can use ACC to

- move some selected workloads or all workloads from their on-premises data centers to the cloud
- clone their apps to the cloud either for testing purposes or move from the data center to the cloud

### Data Migration

To migrate application from one environment to another, you can use one of the following features of ACC:

- **replication**
- **backup and restore**
- **clone**

Refer to the [data protection section](#) for the **replication and backup and restore** options. Refer [here](#) for additional details about **cloning**.





Astra Replication feature is only supported with Trident Container Storage Interface (CSI). However, replication is not supported by nas-economy & san-economy drivers.

## Performing data replication using ACC

The screenshot displays the Astra console interface for configuring data replication. On the left is a navigation sidebar with options: Dashboard, Applications, Clusters, Cloud instances, Backends, Buckets, Account, Activity, and Support. The main panel shows the 'ghost' application configuration. At the top, there are two status boxes: 'APPLICATION STATUS' (Healthy) and 'APPLICATION PROTECTION' (Fully protected). Below these, tabs for 'Data protection', 'Storage', 'Resources', 'Execution hooks', 'Activity', and 'Tasks' are visible. The 'Data protection' tab is active, showing a 'Configure' button. A diagram illustrates the replication relationship between a 'Source' (ghost application, ocp-cluster5, ghost-zonea) and a 'Destination' (ghost application, ocp-cluster7, blog-zoneb). On the right, a 'Replication relationship' panel shows the status as 'Healthy' and 'Established', with a schedule to replicate snapshots every 5 minutes to ocp-cluster7. The last sync occurred on 2023/04/26 at 19:16 UTC with a duration of 30 seconds. An 'Actions' menu on the far right includes options like Snapshot, Back up, Clone, Restore, Fail over, Reverse replication, and Unmanage.

# NetApp Hybrid Multicloud solutions for Red Hat OpenShift Container workloads

## Overview

NetApp is seeing a significant increase in customers modernizing their legacy enterprise applications and building new applications using containers and orchestration platforms built around Kubernetes. Red Hat OpenShift Container Platform is one example that we see adopted by many of our customers.

As more and more customers begin adopting containers within their enterprises, NetApp is perfectly positioned to help serve the persistent storage needs of their stateful applications and classic data management needs such as data protection, data security, and data migration. However, these needs are met using different strategies, tools, and methods.

**NetApp ONTAP** based storage options listed below, deliver security, data protection, reliability, and flexibility for containers and Kubernetes deployments.

- Self-managed storage in on-premises:
  - NetApp Fabric Attached Storage (FAS), NetApp All Flash FAS Arrays (AFF), NetApp All SAN Array (ASA) and ONTAP Select
- Provider-managed storage in on-premises:
  - NetApp Keystone provides Storage as a Service (STaaS)
- Self-managed storage in the cloud:

- NetApp Cloud Volumes ONTAP(CVO) provide self managed storage in the hyperscalers
- Provider-managed storage in the cloud:
  - Cloud Volumes Service for Google Cloud (CVS), Azure NetApp Files (ANF), Amazon FSx for NetApp ONTAP offer fully managed storage in the hyperscalers

## ONTAP feature highlights



<b>Storage Administration</b> <ul style="list-style-type: none"> <li>• Multi-tenancy</li> <li>• FlexVol &amp; FlexGroup</li> <li>• LUN</li> <li>• Quotas</li> <li>• ONTAP CLI &amp; API</li> <li>• System Manager &amp; BlueXP</li> </ul>	<b>Performance &amp; Scalability</b> <ul style="list-style-type: none"> <li>• FlexCache</li> <li>• FlexClone</li> <li>• nconnect, session trunking, multipathing</li> <li>• Scale-out clusters</li> </ul>
<b>Availability &amp; Resilience</b> <ul style="list-style-type: none"> <li>• Multi-AZ HA deployment (MetroCluster)</li> <li>• SnapShot &amp; SnapRestore</li> <li>• SnapMirror</li> <li>• SnapMirror Business Continuity</li> <li>• SnapMirror Cloud</li> </ul>	<b>Access Protocols</b> <ul style="list-style-type: none"> <li>• NFS –v3, v4, v4.1, v4.2</li> <li>• SMB – v2, v3</li> <li>• iSCSI</li> <li>• Multi-protocol access</li> </ul>
<b>Storage Efficiency</b> <ul style="list-style-type: none"> <li>• Deduplication &amp; Compression</li> <li>• Compaction</li> <li>• Thin provisioning</li> <li>• Data Tiering (Fabric Pool)</li> </ul>	<b>Security &amp; Compliance</b> <ul style="list-style-type: none"> <li>• Fpolicy &amp; Vscan</li> <li>• Active Directory integration</li> <li>• LDAP &amp; Kerberos</li> <li>• Certificate based authentication</li> </ul>

**NetApp BlueXP** enables you to manage all of your storage and data assets from a single control plane/interface.

You can use BlueXP to create and administer cloud storage (for example, Cloud Volumes ONTAP and Azure NetApp Files), to move, protect, and analyze data, and to control many on-prem and edge storage devices.

**NetApp Astra Trident** is a CSI Compliant Storage Orchestrator that enable quick and easy consumption of persistent storage backed by a variety of the above-mentioned NetApp storage options. It is an open-source software maintained and supported by NetApp.

## Astra Trident CSI feature highlights



<b>CSI specific</b> <ul style="list-style-type: none"><li>• CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies</li><li>• CSI topology</li><li>• Volume expansion</li></ul>	<b>Security</b> <ul style="list-style-type: none"><li>• Dynamic-export policy management</li><li>• iSCSI initiator-groups dynamic management</li><li>• iSCSI bidirectional CHAP</li></ul>
<b>Control</b> <ul style="list-style-type: none"><li>• Storage and performance consumption</li><li>• Monitoring</li><li>• Volume Import</li><li>• Cross Namespace Volume Access</li></ul>	<b>Installation methods</b> <ul style="list-style-type: none"><li>• Binary</li><li>• Helm chart</li><li>• Operator</li><li>• GitOps</li></ul>
<b>Choose your access mode</b> <ul style="list-style-type: none"><li>• RWO (ReadWriteOnce, i.e 1↔1)</li><li>• RWX (ReadWriteMany, i.e 1↔n)</li><li>• ROX (ReadOnlyMany)</li><li>• RWOP (ReadWriteOnce POD)</li></ul>	<b>Choose your protocol</b> <ul style="list-style-type: none"><li>• NFS</li><li>• SMB</li><li>• iSCSI</li></ul>

Business critical container workloads need more than just persistent volumes. Their data management requirements require protection and migration of the application kubernetes objects as well.



Application data includes kubernetes objects in addition to the user data: Some examples are as follows:

- kubernetes objects such as pods specs, PVCs, deployments, services
- custom config objects such as config maps and secrets
- persistent data such as Snapshot copies, backups, clones
- custom resources such as CRs and CRDs

**NetApp Astra Control**, available as both fully-managed and self-managed software, provides orchestration for robust application data management. Refer to the [Astra documentation](#) for additional details on the Astra family of products.

This reference documentation provides validation of migration and protection of container-based applications, deployed on RedHat OpenShift container platform, using NetApp Astra Control Center. In addition, the solution provides high-level details for the deployment and the use of Red Hat Advanced Cluster Management (ACM) for managing the container platforms. The document also highlights the details for the integration of NetApp storage with Red Hat OpenShift container platforms using Astra Trident CSI provisioner. Astra Control Center is deployed on the hub cluster and is used to manage the container applications and their persistent storage lifecycle. Finally, it provides a solution for replication and failover and fail-back for container workloads on managed Red Hat OpenShift clusters in AWS (ROSA) using Amazon FSx for NetApp ONTAP (FSxN) as persistent storage.

### NetApp Solution with Managed Red Hat OpenShift Container platform workloads on AWS

Customers may be "born in the cloud" or may be at a point in their modernization journey when they are ready to move some select workloads or all workloads from their data centers to the cloud. They may choose to use provider-managed OpenShift containers and provider-managed NetApp storage in the cloud for running their workloads. They should plan and deploy the Managed Red Hat OpenShift container clusters (ROSA) in

the cloud for a successful production-ready environment for their container workloads. When they are in AWS cloud, they could also deploy FSx for NetApp ONTAP for the storage needs.

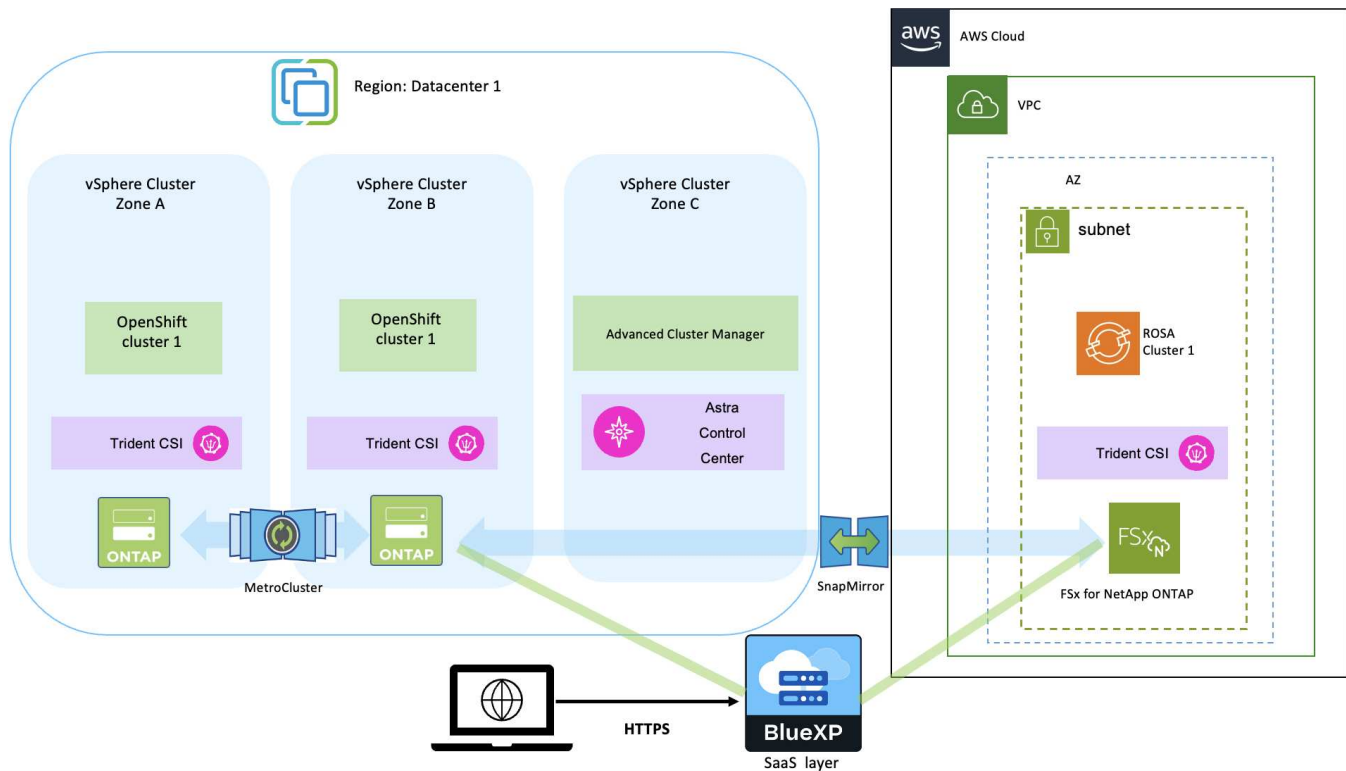
FSx for NetApp ONTAP delivers data protection, reliability, and flexibility for container deployments in AWS. Astra Trident serves as the dynamic storage provisioner to consume the persistent FSxN storage for customers' stateful applications.

As ROSA can be deployed in HA mode with control plane nodes spread across multiple availability zones, FSx ONTAP can also be provisioned with Multi-AZ option which provides high availability and protect against AZ failures.



There are no data transfer charges when accessing an Amazon FSx file system from the file system's preferred Availability Zone (AZ). For more info on pricing, refer [here](#).

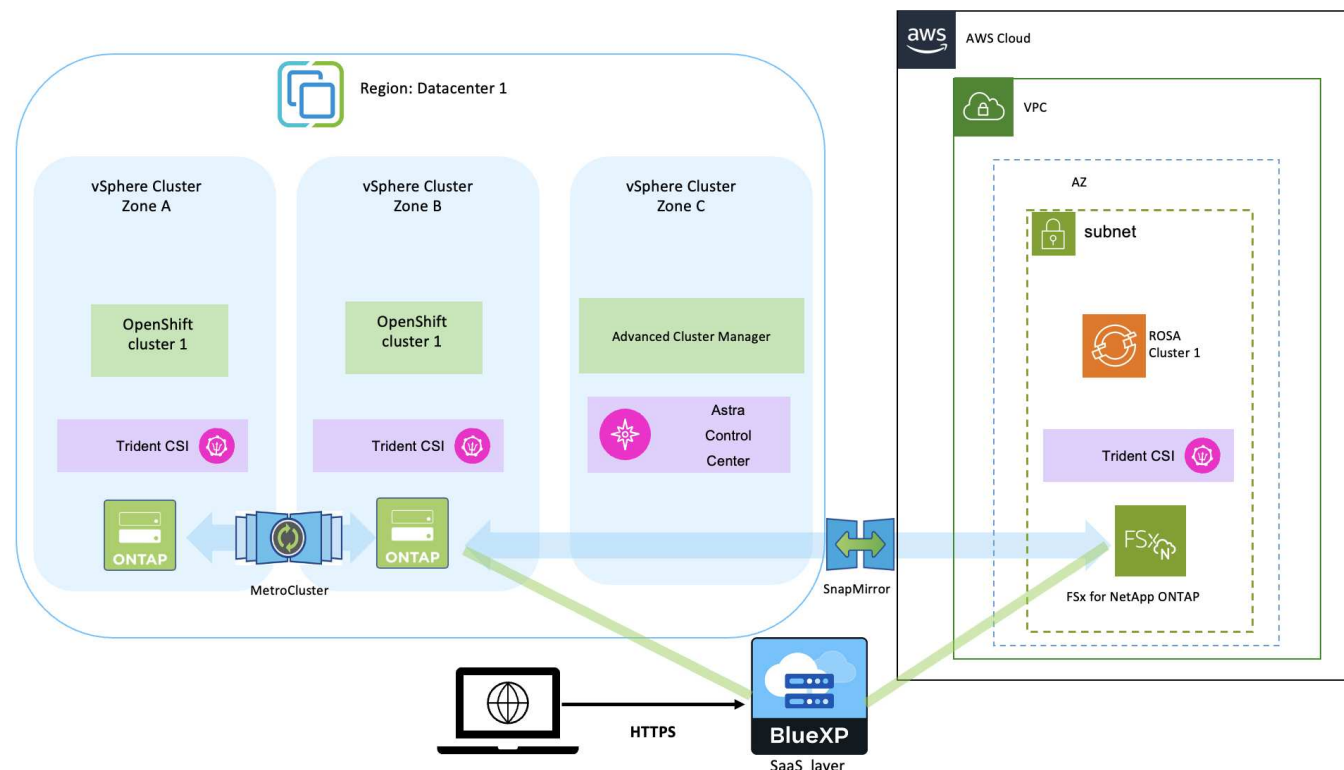
### Data protection and migration solution for OpenShift Container workloads



### Deploy and configure the Managed Red Hat OpenShift Container platform on AWS

This section describes a high-level workflow of setting up the Managed Red Hat OpenShift clusters on AWS(ROSA). It shows the use of Managed FSx for NetApp ONTAP (FSxN) as the storage backend by Astra Trident to provide persistent volumes. Details are provided about the deployment of FSxN on AWS using BlueXP. Also, details are provided about the use of BlueXP and OpenShift GitOps (Argo CD) to perform data protection and migration activities for the stateful applications on ROSA clusters.

Here is a diagram that depicts the ROSA clusters deployed on AWS and using FSxN as the backend storage.



This solution was verified by using two ROSA clusters in two VPCs in AWS. Each ROSA cluster was integrated with FSxN using Astra Trident. There are several ways of deploying ROSA clusters and FSxN in AWS. This high-level description of the setup provides documentation links for the specific method that was used. You can refer to the other methods in the relevant links provided in the [resources section](#).

The setup process can be broken down into the following steps:

### Install ROSA clusters

- Create two VPCs and set up VPC peering connectivity between the VPCs.
- Refer [here](#) for instructions to install ROSA clusters.

### Install FSxN

- Install FSxN on the VPCs from BlueXP.  
Refer [here](#) for BlueXP account creation and to get started.  
Refer [here](#) for installing FSxN.  
Refer [here](#) for creating a connector in AWS to manage the FSxN.
- Deploy FSxN using AWS.  
Refer [here](#) for deployment using AWS console.

## Install Trident on ROSA clusters (using Helm chart)

- Use Helm chart to install Trident on ROSA clusters.  
url for the Helm chart: <https://netapp.github.io/trident-helm-chart>
- Demonstration video: Integration of FSxN with Astra Trident for ROSA clusters

► <https://docs.netapp.com/us-en/netapp-solutions/media/rhbc-install-trident-using-helm.mp4> (video)



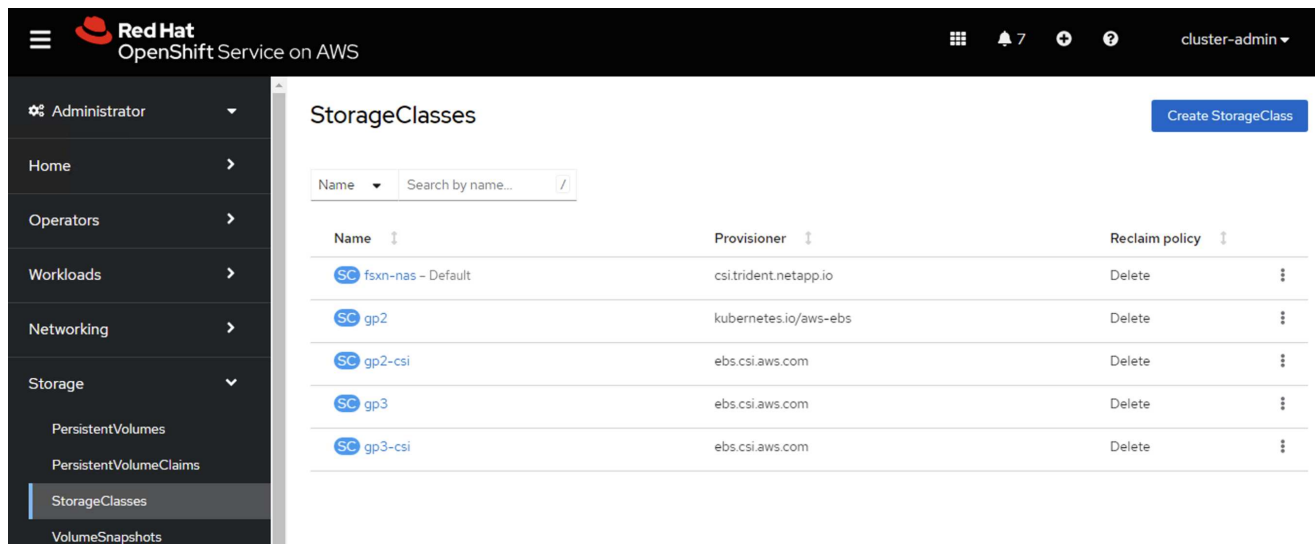
OpenShift GitOps can be utilized to deploy Astra Trident CSI to all managed clusters as they get registered to ArgoCD using ApplicationSet.

```
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: trident-operator
spec:
  generators:
  - clusters: {}
    # selector:
    #   matchLabels:
    #     tridentversion: '23.04.0'
  template:
    metadata:
      name: '{{nameNormalized}}-trident'
    spec:
      destination:
        namespace: trident
        server: '{{server}}'
      source:
        repoURL: 'https://netapp.github.io/trident-helm-chart'
        targetRevision: 23.04.0
        chart: trident-operator
      project: default
      syncPolicy:
        syncOptions:
          - CreateNamespace=true
```



## Create backend and storage classes using Trident (for FSxN)

- Refer [here](#) for details about creating backend and storage class.
- Make the storage class created for FsxN with Trident CSI as default from OpenShift Console. See screenshot below:



## Deploy an application using OpenShift GitOps (Argo CD)

- Install OpenShift GitOps operator on the cluster. Refer to instructions [here](#).
- SetUp a new Argo CD instance for the cluster. Refer to instructions [here](#).

Open the console of Argo CD and deploy an app.

As an example, you can deploy a Jenkins App using Argo CD with a Helm Chart.

When creating the application, the following details were provided:

Project: default

cluster: <https://kubernetes.default.svc>

Namespace: Jenkins

The url for the Helm Chart: <https://charts.bitnami.com/bitnami>

Helm Parameters:

global.storageClass: fsxn-nas

## Data protection

This page shows the data protection options for Managed Red Hat OpenShift on AWS (ROSA) using Astra Control Service.

### FSx NetApp ONTAP for Red Hat OpenShift Service on AWS (ROSA)

The following video shows the backup of a ROSA application running in one region and restoring to another region.

► <https://docs.netapp.com/us-en/netapp-solutions/media/rhhc-Rosa-DR-demo-audio.mp4> (video)

## Data migration

This page shows the data migration options for container workloads on Managed Red Hat OpenShift clusters using FSx for NetApp ONTAP for persistent storage.

### Data Migration

Red Hat OpenShift service on AWS as well as FSx for NetApp ONTAP (FSxN) are part of their service portfolio by AWS. FSxN is available on Single AZ or Multi-AZ options.

Multi-Az option provides data protection from availability zone failure.

FSxN can be integrated with Astra Trident to provide persistent storage for applications on ROSA clusters.

#### Integration of FSxN with Trident using Helm chart

► <https://docs.netapp.com/us-en/netapp-solutions/media/rhhc-install-trident-using-helm.mp4> (video)

The migration of container applications involves:

- Persistent volumes: this can be accomplished using BlueXP.  
Another option is to use Astra Control Center to handle container application migrations from on-premises to the cloud environment. Automation can be used for the same purpose.
- Application metadata: this can be accomplished using OpenShift GitOps (Argo CD).

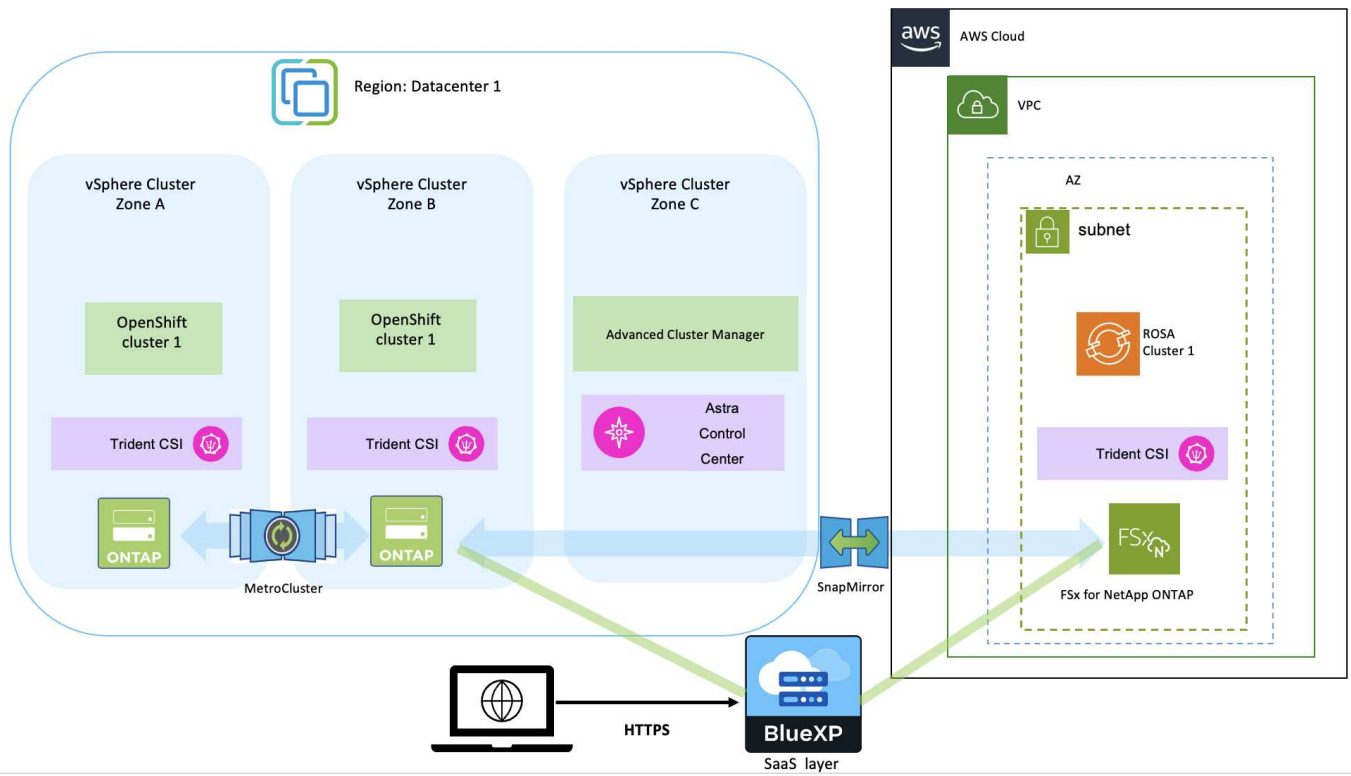
#### Failover and Fail-back of applications on ROSA cluster using FSxN for persistent storage

The following video is a demonstration of application failover and fail-back scenarios using BlueXP and Argo CD.

► <https://docs.netapp.com/us-en/netapp-solutions/media/rhhc-failover-failback.mp4> (video)

#### Data protection and migration solution for OpenShift Container workloads





## Copyright information

Copyright © 2023 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.