

NetApp Hybrid Multicloud with Red Hat OpenShift

NetApp Solutions

NetApp July 31, 2024

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions/rhhc/rhhc-value-prop.html on July 31, 2024. Always check docs.netapp.com for the latest.

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	. 13
NetApp Hybrid Multicloud solutions for Red Hat OpenShift Container workloads	. 24
NetApp Hybrid Multicloud solutions for Red Hat OpenShift Container workloads	. 40
Data protection for Container Apps in OpenShift Container Platform using OpenShift API for Data	
Protection (OADP)	. 63

NetApp Hybrid Multicloud with Red Hat OpenShift Container workloads

NetApp Hybrid Multicloud solutions for Red Hat OpenShift Container workloads

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.

Overview

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

Performance & Scalability
FlexCache Inconnect, session trunking, multipathing FlexClone Scale-out clusters
Access Protocols
NFS –v3, v4, v4.1, v4.2 iSCSI SMB – v2, v3 Multi-protocol access
Security & Compliance
Fpolicy & Vscan LDAP & Kerberos

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.



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

(i)

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



Scenario 4: Data protection and migration from the on-premises environment to GCP environment using ACC

On-premises: Self-managed OpenShift cluster and self-managed storage Google 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.



For considerations when using ONTAP in a MetroCluster configuration, refer here.

Scenario 5: Data protection and migration from the on-premises environment to Azure environment using ACC

On-premises: Self-managed OpenShift cluster and self-managed storage Azure 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.



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.

Scenarios 1, 2 and 3 of the solution were validated using the versions as shown in the table below:

Component	Version	
VMware	vSphere Client version 8.0.0.10200 VMware ESXi, 8.0.0, 20842819	
Hub Cluster	OpenShift 4.11.34	

Source and Destination Clusters	OpenShift 4.12.9 on-premises and in AWS	
NetApp Astra Trident	Trident Server and Client 23.04.0	
NetApp Astra Control Center	ACC 22.11.0-82	
NetApp ONTAP	ONTAP 9.12.1	
AWS FSx for NetApp ONTAP	Single AZ	

Scenario 4 of the solution was validated using the versions as shown in the table below:

Component	Version	
VMware	vSphere Client version 8.0.2.00000 VMware ESXi, 8.0.2, 22380479	
Hub Cluster	OpenShift 4.13.13	
Source and Destination Clusters	OpenShift 4.13.12 on-premises and in Google Cloud	
NetApp Astra Trident	Trident Server and Client 23.07.0	
NetApp Astra Control Center	ACC 23.07.0-25	
NetApp ONTAP	ONTAP 9.12.1	
Cloud Volumes ONTAP	Single AZ, Single node,9.14.0	

Scenario 5 of the solution was validated using the versions as shown in the table below:

Component	Version
\/ \	vSphere Client version 8.0.2.00000
vmware	VMware ESXi, 8.0.2, 22380479
Source and Destination	OpenShift 4.13.25
Clusters	on-premises and in Azure
NetApp Astra Trident	Trident Server and Client and Astra Control Provisioner 23.10.0
NetApp Astra Control Center	ACC 23.10
	ONTAP 9 12 1
NetApp ON TAP	ONTAL 3.12.1
Cloud Volumes ONTAP	Single AZ, Single node,9.14.0

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. image::rhhc_storage_options_fsxn_options.png["Replication between Multi-AZ and Single-AZ"]

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

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.

Overview

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

9

Storage Administration	Performance & Scalability
 Multi-tenancy ONTAP CLI & API FlexVol & FlexGroup System Manager & BlueXP LUN Quotas 	FlexCache flexCache roonnect, session trunking, multipathing FlexClone Scale-out clusters
Availability & Resilience	Access Protocols
 Multi-AZ HA deployment (MetroCluster) SnapShot & SnapRestore SnapMirror Cloud SnapMirror 	NFS –v3, v4, v4.1, v4.2 iSCSI SMB – v2, v3 Multi-protocol access
Storage Efficiency	Security & Compliance
Deduplication & Compression	Fpolicy & Vscan LDAP & Kerberos
Compaction Data Tiering (Fabric Pool)	Active Directory integration Certificate based authentication

ONTAP feature highlights

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



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 highlevel 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.

	Region: Datacenter 1		Region: Datacenter 2
vSphere Cluster Zone A	vSphere Cluster Zone B	vSphere Cluster Zone C	vSphere Cluster Zone A
OpenShift cluster 1	OpenShift cluster 1	Advanced Cluster Manager	OpenShift cluster 2
Trident CSI	Trident CSI	Astra Control Center	Trident CSI
			SnapMirror

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.

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)

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 diaster.

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

d Ams						
D faithead	a) gbost -				c.	Adapta - W
a) topicalism () therein	-de-Annumation starus		e sharest	9 Administration Protocology	 System print printeret 	- 02
C) Over Interes	- Protection	0				
13 Burley	Cataponenter Streep. Annuality Statistics	han Arris San				
2 mm	Arrest			W and	0 B tota	an 2 Australian
1					141	fammer (
inerit (10 April	tow	Terral state	(in tribulate) (2+2ehand	Could F.	An Original
	- uptates which write ling	121 marting	i contra	(I) the Schemater	methodologic tacht off	1
	gint market intractions	(distance	10 million		100 p (mg (d) 10 (d) (d))	10
	S good country 22 million	2	12	0	2012/06/10 1414 171	10
	given sequine the method life	(2) -same	0.000	O the Canada	1011000 (0.1011) (172	1

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.

🗳 Ame								
10 matrices	- molg 🗊						e	6
i and a state of the state of t	-1,- 2003. 	atom Garos nativ		B Mumor	9 errus altice resolution O monitor polici configurat	C factories print or	0) mini	
Conditioners	1000000 10 percent		O restant					
C Loine	Carlo protochom - Horago - Hain	antar (ministra kasha) A	corp : tan					
5 mm	Alter * Testare *				T and .	O Departm	D today 2 Automa	6
	2 mil	Also (-	(Sei Saltanian / On (second	Rodal	10000 K.S.	Action of the Action	-
	in an in the test of test	P rates	6 tr	(i) the Latence	974	and water that one) Anima gydrafae Anima Saring	

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.

K DETAILS 3				EXECUTION HOOKS
ration -snapshot	Hook arguments (optional) T (pre X) Enter hook arguments		?	Execution hooks allow Astra Control to execute your own custom scripts before or after snapshot.
nk name Is-pre-snapshot				Read more in Manage application execution hooks
TAINER IMAGES ?				
Apply to all container images				
e a regular expression to target container images for the book.				
rtainer Image names to match Iis				
PT 7				
⊢ Add		∓ Search		
Name 4				
mariadb_mysql.sh				
o postgresql.sh				
redis_hook.sh				

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/ here to get additional details about the differences between the two types of data protection.

Refer here for SnapMirror setup instructions.

SnapMirror with ACC

	⊚ ghost ∧			c	Adam
Applications Clusters Cloud Instances	-tp- APPLICATION STATUS	 Fully protected Outer 	APPLICATION PROTECTION	 Anglication policy configured 	Stapbet Rack op Cone Nastore
tackends	🖌 ghoù zonia	O speciated			fall over Reverse replicat
Buckett	Data perturbition Storage Resources Essecution hooks Activity	Tanks			transie
Angunt Antony Support	source ghost	Destination ghott		Replication relationship STATUS Disatify statuster SCHEDUS Replicate sequence every 5 mean Concretent/2 LAST STRC 2022/04/26 Vield URC Sprin disations 20 search	hei to
	C tourty to applications white the	image of the second secon			

san-economy and nas-economy storage drivers do not support replication feature. Refer here for additional details.

Demo video:

(i

Demonstration video of disaster recovery with Astra Control Center

Data protection 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 diaster 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

(<mark>Q</mark>)

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

2 Dattoart	i ghost 🔿			c	Adam •
ið Applications Si Clusters	-\$- APPERATION STATUS	 Fully protected 	S APPLICATION PROTECTION	 Regisation policy configured 	Stagebet Rack op Clone
	Defentan ghai zuizz	Chaine O sep-shares			Fall-over
] luckm	Data pretection Storage Researces Esecution hooks Activity	fails			benauge
B. Annuat	Configure +			🖸 Stapholo 😫 Back	ge 2 Agoun
3 Automy 3 Support	Source phose @ insultry @ insultry @ insultry @ insultry Millior site	Contrustors ghott O insetty O tex-insetty M they insets		Replication relationship STATUS D thattise Status Replicate supplier every 5 med C concluste? LAST SYNC Speri duration 30 seconds	NH 10

NetApp Hybrid Multicloud solutions for Red Hat OpenShift Container workloads

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.

Overview

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

Storage Administration	Performance & Scalability		
Multi-tenancy ONTAP CLI & API System Manager & BlueXP LUN Ountas	FlexCache Inconnect, session trunking, multipathing Scale-out clusters		
Availability & Resilience	Access Protocols		
 Multi-AZ HA deployment (MetroCluster) SnapShot & SnapRestore SnapMirror Cloud SnapMirror 	NFS -v3, v4, v4.1, v4.2 iSCSI SMB - v2, v3 Multi-protocol access		
Storage Efficiency	Security & Compliance		
 Deduplication & Compression Compaction Data Tiering (Fabric Pool) 	Fpolicy & Vscan LDAP & Kerberos Active Directory integration Certificate based authentication		

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.

9

Astra Trident CSI feature highlights



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

On-premises and AWS image::rhhc-self-managed-aws.png[]

On-premises and Google Cloud image::rhhc-self-managed-gcp.png[]

On-premises and Azure Cloud image::rhhc-self-managed-azure.png[]

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.

- 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.

Deploy and configure the Red Hat OpenShift Container platform on GCP

This section describes a high-level workflow of how to set up and manage OpenShift Clusters in GCP 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.

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



There are several ways of deploying Red Hat OpenShift Container platform clusters in GCP. 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:

(i)

- Ensure that you have met all the prerequisites stated here.
- For the VPN connectivity between on-premises and GCP, a pfsense VM was created and configured. For instructions, see here.
 - The remote gateway address in pfsense can be configured only after you have created a VPN gateway in Google Cloud Platform.
 - The remote network IP addresses for the Phase 2 can be configured only after the OpenShift cluster installation program runs and creates the infrastructure components for the cluster.
 - The VPN in Google Cloud can only be configured after the infrastructure components for the cluster are created by the installation program.
- Now install the OpenShift cluster on GCP.
 - Obtain the installation program and the pull secret and deploy the cluster following the steps provided in the documentation here.
 - The installation creates a VPC network in Google Cloud Platform. It also creates a private zone in Cloud DNS and adds A records.
 - Use the CIDR block address of the VPC network to configure the pfsense and establish the VPN connection. Ensure firewalls are setup correctly.
 - Add A records in the DNS of the on-premises environment using the IP address in the A records of the Google Cloud DNS.
 - The installation of the cluster completes and will provide a kubeconfig file and username and password to login to the console of the cluster.

Deploy Cloud Volumes ONTAP in GCP using BlueXP.

- Install a connector in Google Cloud. Refer to instructions here.
- Deploy a CVO instance in Google Cloud using the connector. Refer to instructions here. https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html

Install Astra Trident in the OCP Cluster in GCP

- There are many methods to deploy Astra Trident as shown here.
- For this project, Astra Trident was installed by deploying Astra Trident Operator manually using the instructions here.
- Create backend and a storage classes. Refer to instructions here.

Add the OCP cluster on GCP to the Astra Control Center.

- Create a separate KubeConfig file with a cluster role that contains the minimum permissions necessary for a cluster to be managed by Astra Control. The instructions can be found here.
- Add the cluster to Astra Control Center following the instructions here

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.

Demonstration Video

OpenShift Cluster installation on Google Cloud Platform

Importing OpenShift clusters into Astra Control Center

Deploy and configure the Red Hat OpenShift Container platform on Azure

This section describes a high-level workflow of how to set up and manage OpenShift Clusters in Azure and deploy stateful applications on them. It shows the use of NetApp Cloud Volumes ONTAP storage with the help of Astra Trident/Astra Control Provisioner 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.

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

	Kegron: Datacenter 1		Virtual Network
vSphere Cluster Zone A	vSphere Cluster Zone B	vSphere Cluster Zone C	Master nodes subnet OpenShift cluster Master nodes
OpenShift cluster 1	OpenShift cluster 1	OpenShift cluster Advanced Cluster Manager	Worker nodes subnet
Trident CSI	Trident CSI	Astra Control Center	Trident CSI
		SnapMirro	Cloud Volumes ONTAP

There are several ways of deploying Red Hat OpenShift Container platform clusters in Azure. 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:

(i)

- Ensure that you have met all the prerequisites stated here.
- Create a VPN, subnets and network security groups and a private DNS zone. Create VPN gateway and site-to-site VPN Connection.
- For the VPN connectivity between on-premises and Azure, a pfsense VM was created and configured. For instructions, see here.
- Obtain the installation program and the pull secret and deploy the cluster following the steps provided in the documentation here.
- The installation of the cluster completes and will provide a kubeconfig file and username and password to login to the console of the cluster.

A sample install-config.yaml file is given below.

```
apiVersion: v1
baseDomain: sddc.netapp.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD LRS"
      type: Standard D2s v3
      ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium LRS
      type: Standard D8s v3
      ultraSSDCapability: Disabled
  replicas: 3
```
```
metadata:
  creationTimestamp: null
  name: azure-cluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
        diskSizeGB: 1024
        diskType: "StandardSSD LRS"
      ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp vnet ncus
publish: Internal
pullSecret:
```

Deploy Cloud Volumes ONTAP in Azure using BlueXP.

- Install a connector in in Azure. Refer to instructions here.
- Deploy a CVO instance in Azure using the connector. Refer to instructions link:https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-azure.html [here.]

Install Astra Control Provisioner in the OCP Cluster in Azure

- For this project, Astra Control Provisioner (ACP) was installed on all the clusters (on-prem cluster, onprem cluster where Astra Control Center is deployed and the cluster in Azure). Learn more about the Astra Control Provisioner here.
- Create backend and a storage classes. Refer to instructions here.

Add the OCP cluster on Azure to the Astra Control Center.

- Create a separate KubeConfig file with a cluster role that contains the minimum permissions necessary for a cluster to be managed by Astra Control. The instructions can be found here.
- Add the cluster to Astra Control Center following the instructions here

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.

Demonstration Video

Using Astra Control for Failover and Failback of applications

Data protection using Astra Control Center

This page shows the data protection options for Red Hat OpenShift Container based applications running on VMware vSphere or in the cloud 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 diaster.

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.

DK DETAILS ?			EXECUTION HOOKS
peration ~	Hook arguments (optional) 1 pre × Enter hook arguments	1	Execution hooks allow Astra Control to execute your own custom scripts before or after snapshot.
ook name dis-pre-snapshot			Read more in Manage application executio hooks
NTAINER IMAGES ?			
Apply to all container images			
se a regular expression to target container images for the book.			
ontainer image names to match : idis			
IPT 7			
+ Add	(₹ Search	
Name 4			
mariadb_mysql.sh			
o postgresqLsh			
• redis_hook.sh			

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

38

Datioart	🔞 ghost 🔿	2	C Adon
) Applications) Clusters) Could Instances	-4- APPLICATION STATUS	APPLICATION PROTECTION O fully protected O fully protected O fully protected O fully protected	taupher Rick op Cone Redox Fallowr
Backends Bucketts	Data protection Storage Resources Execution hooks Activity Configure +	fasis	Anverse inglicat Utercarcoje 2 Bactope – 2 Reptor
Angeut Antony Support	Source ghost @ isauty @ isauty if generate if generate if generate if generate	Centranteer Centranteer Sharts Statute Statute Statute	nship 5 mmulez ta

 (\mathbf{i})

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

Data protection with Astra Control Center

Details on Astra Control Center Data Protection features are available here

Disaster recovery (Failover and Failback using replication) with ACC

Using Astra Control for Failover and Failback of applications

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

2 Defiloart	⊚ ghost ∧				с	Attons
) Appleations 3 Outers 3 Octoberations	-%- APPERATION STATUS	٥	Fully protected	APPLICATION PROTECTION	Stephaton policy configured	Srapsher Rack op Clone Nexton
- Rathenda	(Selforstann ■ ghuid aunses	O sep-shate()				Fall-over Revenie replication
Buckett	Data protection Storage Resources Execution books Activity	Tanks				tonage
	Configure 1				🖸 Stephers 📓 Said	ige 2 Autor
i Auguport	Source Source		Destination ghost @ iseethy C segulated IS ling seeth		Replication relationship STATUS D Halffy [Intelliner Scheldung Conscience] LAST SYNC Zent Galge Webs URC Spine diatation: 20 senarth	Area Tao

NetApp Hybrid Multicloud solutions for Red Hat OpenShift Container workloads

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.

Overview

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

Storage Administration	Performance & Scalability				
Multi-tenancy ONTAP CLI & API FlexVol & FlexGroup System Manager & BlueXP LUN Quotas	FlexCache Inconnect, session trunking, multipathing FlexClone Scale-out clusters				
Availability & Resilience	Access Protocols				
Multi-AZ HA deployment (MetroCluster) SnapShot & SnapRestore SnapMirror Cloud SnapMirror	NFS -v3, v4, v4.1, v4.2 iSCSI SMB - v2, v3 Multi-protocol access				
Storage Efficiency	Security & Compliance				
 Deduplication & Compression Compaction Data Tiering (Fabric Pool) 	 Fpolicy & Vscan LDAP & Kerberos Active Directory integration Certificate based authentication 				

ONTAP feature highlights

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



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

(i)

- 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.

• Use Helm chart to install Trident on ROSA clusters. url for the Helm chart: https://netapp.github.io/trident-helm-chart

Integration of FSxN with Astra Trident for ROSA clusters



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





- 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:

Create Storage		StorageClasses		C Administrator
		Name Search by name. /	>	Home
Reclaim policy 1	Provisioner	Name	•	Operators
Delete	csitrident.netappio	👀 foxn-nas - Default	>	Workloads
Delete	kubernetes io/aws-ebs	() gp2	>	Networking
Delete	ebs.csi.aws.com	50 gp2+csi		.
Delete	ebs.csi.aws.com	60 gp3	Č	Storage
Delete	ebs.csi.aws.com	(p)3-csi	ns	PersistentVolumes PersistentVolumeClain
At this is the			ns	PersistentVolumeClain StorageClasses
				StorageClasses VolumeSnapshots

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) clusters using Astra Control Service. Astra Control Service (ACS) provides an easy-to-use graphical user-interface with which you can add clusters, define applications running on them, and perform application aware data management activities. ACS functions can also be accessed using an API that allows for automation of workflows.

Powering Astra Control (ACS or ACC) is NetApp Astra Trident. Astra Trident integrates several types of Kubernetes clusters such as Red Hat OpenShift, EKS, AKS, SUSE Rancher, Anthos etc., with various flavors of NetApp ONTAP storage such as FAS/AFF, ONTAP Select, CVO, Google Cloud Volumes Service, Azure

NetApp Files and Amazon FSx for NetApp ONTAP.

This section provides details for the following data protection options using ACS:

- A video showing Backup and Restore of a ROSA application running in one region and restoring to another region.
- A video showing Snapshot and Restore of a ROSA application.
- Step-by-step details of installing a ROSA cluster, Amazon FSx for NetApp ONTAP, using NetApp Astra Trident to integrate with storage backend, installing a postgresql application on ROSA cluster, using ACS to create a snapshot of the application and restoring the application from it.
- A blog showing step-by-step details of creating and restoring from a snapshot for a mysql application on a ROSA cluster with FSx for ONTAP using ACS.

Backup/Restore from Backup

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

FSx NetApp ONTAP for Red Hat OpenShift Service on AWS

Snapshot/Restore from snapshot

The following video shows taking a snapshot of a ROSA application and restoring from the snapshot after.

Snapshot/Restore for Applications on Red Hat OpenShift Service on AWS (ROSA)clusters with Amazon FSx for NetApp ONTAP storage

Blog

• Using Astra Control Service for data management of apps on ROSA clusters with Amazon FSx storage

Step-by-Step Details to create snapshot and restore from it

Prerequisite setup

- AWS account
- Red Hat OpenShift account
- · IAM user with appropriate permissions to create and access ROSA cluster
- AWS CLI
- ROSA CLI
- OpenShift CLI(oc)
- · VPC with subnets and appropriate gateways and routes
- ROSA Cluster installed into the VPC
- Amazon FSx for NetApp ONTAP created in the same VPC
- Access to the ROSA cluster from OpenShift Hybrid Cloud Console

Next Steps

1. Create an admin user and login to the cluster.

- 2. Create a kubeconfig file for the cluster.
- 3. Install Astra Trident on the cluster.
- 4. Create a backend, storage class and snapshot class configuration using the Trident CSI provisioner.
- 5. Deploy a postgresql application on the cluster.
- 6. Create a database and add a record.
- 7. Add the cluster into ACS.
- 8. Define the application in ACS.
- 9. Create a snapshot using ACS.
- 10. Delete the database in the postgresql application.
- 11. Restore from a snapshot using ACS.
- 12. Verify your app has been restored form the snapshot.

1. Create an admin user and login to the cluster

Access the ROSA cluster by creating an admin user with the following command : (You need to create an admin user only if you did not create one at the time of installation)

rosa create admin --cluster=<cluster-name>

The command will provide an output that will look like the following. Login to the cluster using the oc login command provided in the output.

W: It is recommended to add an identity provider to login to this cluster. See 'rosa create idp --help' for more information. I: Admin account has been added to cluster 'my-rosa-cluster'. It may take up to a minute for the account to become active. I: To login, run the following command: oc login https://api.my-rosa-cluster.abcd.p1.openshiftapps.com:6443 \ --username cluster-admin \ --password FWGYL-2mkJI-00000-00000



You can also login to the cluster using a token. If you already created an admin-user at the time of cluster creation, you can login to the cluster from the Red Hat OpenShift Hybrid Cloud console with the admin-user credentials. Then by clicking on the top right corner where it displays the name of the logged in user, you can obtain the oc login command (token login) for the command line.

2. Create a kubeconfig file for the cluster

Follow the procedures here to create a kubeconfig file for the ROSA cluster. This kubeconfig file will be used later when you add the cluster into ACS.

3. Install Astra Trident on the cluster

Install Astra Trident (latest version) on the ROSA cluster. To do this, you can follow any one of the procedures

given here. To install Trident using helm from the console of the cluster, first create a project called Trident.

E SpenSi	t hift Service on AWS				=	\$ 2	Ð	0	cluster-ac	imin -
Projects									Create	Project
▼ Filter ▼ Nam	e 👻 trident									
Name trident X C	lear all filters									
Name 1	Display name	Status	1	Requester	I		Created	1.1		
PR trident	trident	Active		rosaadmin			🛛 Feb 1	2, 2024, 9	9:54 PM	I

Then from the Developer view, create a Helm chart repository. For the URL field use

'https://netapp.github.io/trident-helm-chart'. Then create a helm release for Trident operator.

Project trident 👻
Create Helm Chart Repository Add helm chart repository.
Configure via: Form view O YAML view
Scope type Namespaced scoped (ProjectHelmChartRepository) Add Helm Chart Repository in the selected namespace. Cluster scoped (HelmChartRepository)
Add Helm Chart Repository at the cluster level and in all namespaces. Name trident
A unique name for the Helm Chart repository. Display name
Astra Trident
A display name for the Helm Chart repository. Description
NetApp Astra Trident
A description for the Helm Chart repository. Disable usage of the repo in the developer catalog. URL *
https://netapp.github.io/trident-helm-chart

Project: trident 🔻		
Developer Catalog > Helm Cha	rts	
Helm Charts		
Browse for charts that help man catalog. Alternatively, develope	nage complex installations and upgrades. Clu rs can try to configure their own custom Heln	ster administrators can custo n Chart repository.
All items	All items	
CI/CD	0	
Languages	Q Filter by keyword	A-Z •
Other		
Chart Repositories	Helm Chart	ts
Astra Trident (1)	TRIDANT	
 OpenShift Helm Charts (87) 	Trident Operator	
	A Helm chart for deploying	
Source	NetApp's Trident CSI storage	
Community (33)	provisioner using the Trident	
Partner (42)		
Red Hat (12)		

Verify all trident pods are running by going back to the Administrator view on the console and selecting pods in the trident project.

Red Hat OpenShift Service	on AWS					
Administrator 👻	Project: trident 🔻					
Home >	Pods					
Operators >	▼ Filter ▼ Name	Search by name	1			
Workloads 🗸	Name 1	Status 1	Ready 1	Restarts 1	Owner 1	Mem
Pods	P trident-controller- 69cff44ddf-4dqnj	C Running	6/6	0	RS trident-controller- 69cff44ddf	
Deployments DeploymentConfigs	P trident-node-linux- 4b6fm	C Running	2/2	0	DS trident-node-linux	α.
StatefulSets	P trident-node-linux- 4sckw	C Running	2/2	0	OS trident-node-linux	-
ConfigMaps	P trident-node-linux- 7I42w	C Running	2/2	0	DS trident-node-linux	-
CronJobs	P trident-node-linux- dbhp4	C Running	2/2	0	OS trident-node-linux	-
Jobs DaemonSets	P trident-node-linux- gj5km	C Running	2/2	0	DS trident-node-linux	~
ReplicaSets	P trident-node-linux- r79c8	C Running	2/2	0	DS trident-node-linux	-
HorizontalPodAutoscalers	P trident-node-linux- tzwdp	C Running	2/2	0	OS trident-node-linux	~
PodDisruptionBudgets	P trident-node-linux- vdvxt	C Running	2/2	0	DS trident-node-linux	-
Networking >	P trident-operator- 7f7fd45c68-6crcb	C Running	1/1	0	RS trident-operator- 7f7fd45c68	-

4. Create a backend, storage class and snapshot class configuration using the Trident CSI provisioner

Use the yaml files shown below to create a trident backend object, storage class object and the Volumesnapshot object. Be sure to provide the credentials to your Amazon FSx for NetApp ONTAP file system you created, the management LIF and the vserver name of your file system in the configuration yaml for the backend. To get those details, go to the AWS console for Amazon FSx and select the file system, navigate to the Administration tab. Also, click on update to set the password for the fsxadmin user.



You can use the command line to create the objects or create them with the yaml files from the hybrid cloud console.

Esx > File systems > fs-049f9a23aac951429								
fsx-for-rosa (fs-049f9a23aac951429)								
▼ Summary								
File system ID fs-049f9a23aac951429 Lifecycle state Available File system type ONTAP Deployment type Single-AZ	SSD storage capacity Update 1	Availability Zones us-west-2b 🗇 Creation time 2024-02-12T20:15:23-05:00						
Network & security Monitoring & performance Administration Stora	ge virtual machines Volumes Backups Updates Tags							
ONTAP administration								
Management endpoint - DNS name management.fs-049f9a23aac951429.fsx.us-west-2.amazonaws.com 🗗 Inter-cluster endpoint - DNS name intercluster.fs-049f9a23aac951429.fsx.us-west-2.amazonaws.com 🗗	Management endpoint - IP address 10.49.9.135 🗗 Inter-cluster endpoint - IP address 10.49.9.49 🗗 10.49.9.251 🗗	ONTAP administrator username fsxadmin 🗗 ONTAP administrator password Update						

Trident Backend Configuration

```
apiVersion: v1
kind: Secret
metadata:
 name: backend-tbc-ontap-nas-secret
type: Opaque
stringData:
 username: fsxadmin
 password: <password>
___
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
 name: ontap-nas
spec:
 version: 1
  storageDriverName: ontap-nas
  managementLIF: <management lif>
  backendName: ontap-nas
  svm: fsx
  credentials:
    name: backend-tbc-ontap-nas-secret
```

Storage Class

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
   name: ontap-nas
provisioner: csi.trident.netapp.io
parameters:
   backendType: "ontap-nas"
   media: "ssd"
   provisioningType: "thin"
   snapshots: "true"
allowVolumeExpansion: true
```

snapshot class

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
    name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

Verify that the backend, storage class and the trident-snapshotclass objects are created by issuing the commands shown below.

[ec2-user@ip	-10-49-11-13	2 storage]\$ kul	pectl get	tbc -n	trident				
NAME	BACKEND NAME	BACKEND UUI)			PHASE	STAT	JS	
ontap-nas	ontap-nas	8a5e4583-2da	ic-46bb-b	01e-fa70	3816f121	Bound	Succ	ess	
[ec2-user@ip	-10-49-11-13	2 storage]\$ kut	ectl get	sc					
NAME	PROVISIO	NER	RECLAIM	POLICY	VOLUMEBI	NDINGMODE		ALLOWVOLUMEEXPANSION	AGE
gp2	kubernet	es.io/aws-ebs	Delete		WaitForF	irstConsu	ımer	true	3h23m
gp2-csi	ebs.csi.	aws.com	Delete		WaitForF	irstConsu	mer	true	3h19m
gp3 (default	:) ebs.csi.	aws.com	Delete		WaitForF	irstConsu	mer	true	3h23m
gp3-csi	ebs.csi.	aws.com	Delete		WaitForF	irstConsu	mer	true	3h19m
ontap-nas	csi.trid	lent.netapp.io	Delete		Immediat	e		true	141m
[ec2-user@ip	-10-49-11-13	2 storage]\$ kut	ectl get	Volumes	mapshotcl	ass			
NAME		DRIVER		DELETIC	ONPOLICY	AGE			
csi-aws-vsc		ebs.csi.aws.com	n	Delete		3h19m			
trident-snap	oshotclass	csi.trident.net	tapp.io	Delete		6m56s			
[ec2-user@ip	0-10-49-11-13	2 storage]\$							

At this time, an important modification you need to make is to set ontap-nas as the default storage class instead of gp3 so that the postgresql app you deploy later can use the default storage class. In the Openshift console of your cluster, under Storage select StorageClasses. Edit the annotation of the current default class to be false and add the annotation storageclass.kubernetes.io/is-default-class set to true for the ontap-nas storage class.

■ ^{Sed} Hat OpenShift Servi				0	cluster-admin -
StorageClasses	Edit annotations Key storageclass.kubernetes.io/is	Value false	•	Cre	eate StorageClass
Name 1	Add more	ſ	Cancel Save	Reclaim policy	/ 1 1
SC gp2-csi SC gp3 - Default	ebsicsilav	vs.com		Delete Delete	:
SS gp3-csi	ebs.csi.av	vs.com		Delete	i
SC ontap-nas	csitriden	t.netapp.io		Delete	1

StorageClasses		Create StorageClass
Name Search by name		
Name 1	Provisioner 1	Reclaim policy 1
SC gp2	kubernetes.io/aws-ebs	Delete
SC gp2-csi	ebs.csi.aws.com	Delete #
SC gp3	ebs.csi.aws.com	Delete
SS gp3-csi	ebs.csi.aws.com	Delete
ⓒ ontap-nas – Default	csitrident.netapp.io	Delete

5. Deploy a postgresql application on the cluster

You can deploy the application from the command line as follows:

helm install postgresql bitnami/postgresql -n postgresql --create-namespace

[ec2-user@ip-10-	49-11-132 astra]\$ helm install postgresql bitnami/postgresql -n postgresqlcreate-namespace
NAME: postgresql	(un Fab 13 14/46-16 2024
NAMESPACE: posta	ue res la tradit dece
STATUS: deployed	
REVISION: 1	
TEST SUITE: None	
NOTES:	
CHART MARE: post	gresq1
APP VERSION: 16	44.049 2.0
** Please be nat	ient while the chart is being deployed **
Statement and the second	
PostgreSQL can b	e accessed via port \$432 on the following DMS names from within your cluster:
postgresql.p	ostgresql.svc.cluster.local - Read/Write connection
To get the passw	word for "postgres" run:
export POSTG	RES_PASSWORD=\$(kubect1 get secretnamespace postgresq1 postgresq1 -o jsonpath="{.data.postgres-password}" base64 -d)
To connect to yo	our database run the following command:
kubectl run	postgresql-clientrmtty -irestart='Never'namespace postgresqlimage docker.io/bitnami/postgresql:16.2.0-debian-11-r1env="PG
command	psqlhost postgresql -U postgres -d postgres -p 5432
> NOTE: If y the error "psql:	ou access the container using bash, make sure that you execute "/opt/bitnami/scripts/postgresql/entrypoint.sh /bin/bash" in order to avoid local user with ID 1001} does not exist"
To connect to yo	our database from outside the cluster execute the following commands:
kubectl port PGPASSWORD="	-forwardnamespace postgresql svc/postgresql 5432:5432 & \$POSTGRES_PASSWORD" psqlhost 127.0.0.1 -U postgres -d postgres -p 5432
WARNING: The con case, old PVC w [ec2-usen@ip-10-	ofigured password will be ignored on new installation in case when previous PostgreSQL release was deleted through the helm command. In that ill have an old password, and setting it through helm won't take effect. Deleting persistent volumes (PVs) will solve the issue. 49-11-132 astra]5 _
	If you do not see the application pods running, then there might be an error caused due to
	in you do not do ano application pous running, then there might be an error baused due to
	security context constraints.

image::rhhc-scc-error.png[]

(i)

Fix the error by editing the runAsUser and fsGroup fields in statefuleset.apps/postgresql object with the uid that is in the output of the oc get project command as shown below. image::rhhc-scc-fix.png[]

postgresql app should be running and using persistent volumes backed by Amazon FSx for NetApp ONTAP storage.

postgresql-0 1/1 Running 0 2m46s	[ec2-user@ip-1	L0-49-11	-132 astra]\$ oc get po	ods -n postgresql
	NAME	READY	STATUS	RESTARTS	AGE
[ecz-user@ip-i0-49-ii-i5z astra]	postgresql-0 [ec2-user@ip-1	1/1 10-49-11-	Running -132 astra	0]\$	2m46s

[ec2-user@ip-10-49-	11-132 st	corage]\$ kubectl get pvc -n postgresql				
NAME	STATUS	VOLUME	CAPACITY	ACCESS MODES	STORAGECLASS	AGE
data-postgresql-0	Bound	pvc-dd09524a-de75-4825-9424-03a9b91195ca	8Gi	RWO	ontap-nas	4m2s
[ec2-user@ip-10-49-	11-132 st	corage]\$				

6. Create a database and add a record



7. Add the cluster into ACS

Log in to ACS. Select cluster and click on Add. Select other and upload or paste the kubeconfig file.

Add cluster		STEP 1/3: DETAILS	
ROVIDER			
Microsoft Azure	Google Cloud Platform	aws Amazon Web Services	le Other
JBECONFIG			
(i) Please ensure that the k	ubeconfig used for this cluster has	a long-lived token associated with it.	
Provide Astra Control access to a dedicated admin-role kubeco	your Kubernetes clusters by entering a nfig.	kubeconfig credential. Follow these instr	uctions 🖸 on how to create
Upload file Paste or type			
XJuZXR1cv5pbv9zZXJ2aWN1Y	Witb3VudC9zZXJ2aWN1LWFtY291bnOu	bmFtZSI6ImFzdHJhY29udHJvbC1zZXJ2a	WN1LWF1Y291bn01LCJrdWJ
1cm51dGVzLmlvL3NlcnZpY2V TciLCJzdWI10iJzeXN02W06c	hY2NvdW50L3N1cnZpY2UtYWNjb3VudC 2VydmljZWFjY291bnQ62GVmYXVsdDph	51aWQ101I4NzFhOTI4MC0wMTEyLTRmYzA c3RyYWNvbnRyb2wtc2Vydm1jZS1hY2Nvd	tOWFkNS0zZDI5NzA2N2NiN W50In0.M7-IRxcaKOe7S-
LkW-SZDYOShQ5UolaSbJ- OSId5r0Fbyfc03rSf40VC72m	MAR-YENRODOU/VSTEF30G7-V19X1T-M	X98x1XJ00720062xhv10f0+LCFD23 uS9	UNITEST RITIMAAD CRICMORAD
3XWHF22cTXXpdKqtzWfmBLxY	huN1CzBMY7S55MVnB2WD_e1kptN02a1	vaWmIZjrUQL0_q8Uj2Exe9vVH1KPkfb0C	xU4TvHncbathvL6m21N7Om

Click **Next** and select ontap-nas as the default storage class for ACS. Click **Next**, review the details and **Add** the cluster.

Add cluster STEP 2/3: STORAGE								
STORAGE								
✓ Assign a	new default storage class							
The following	storage classes are available on	the cluster.						
Set default	Storage class	Storage provisioner	Reclaim policy	Binding mode	Eligibility			
	gp2	kubernetesio/aws-ebs	Delete	waitForFirstConsumer				
0	gp2-csi	ebs.csi.aws.com	Delete	WaitForFirstConsumer	⊘ Eligible			
0	gp3	ebs.csi.aws.com	Delete	WaitForFirstConsumer	⊘ Eligible			
0	gp3-csi	ebs.csi.aws.com	Delete	WaitForFirstConsumer	⊘ Eligible			
•	ontap-nas Default	csi.trident.netapp.io	Delete	Immediate	⊘ Eligible			
		← Back Ne	xt →					

8. Define the application in ACS

Define the postgresql application in ACS. From the landing page, select **Applications**, **Define** and fill in the appropriate details. Click **Next** a couple of times, Review the details and click **Define**. The application gets added to ACS.

Add cluster STEP 2/3: STORAGE									
STORAGE									
✓ Assign a	new default storage class								
The following	storage classes are available o	n the cluster.							
Set default	Storage class	Storage provisioner	Reclaim policy	Binding mode	Eligibility				
<u>v</u>	gp∠	kopemetesto/aws-eps	Delete	waitForFirstConsumer					
	gp2-csi	ebs.csi.aws.com	Delete	WaitForFirstConsumer	Seligible				
	gp3	ebs.csi.aws.com	Delete	WaitForFirstConsumer	 Eligible 				
	gp3-csi	ebs.csi.aws.com	Delete	WaitForFirstConsumer	⊘ Eligible				
	ontap-nas Default	csi.trident.netapp.io	Delete	Immediate	⊘ Eligible				
		← Back	Next →						

9. Create a snapshot using ACS

There are many ways to create a snapshot in ACS. You can select the application and create a snapshot from the page that shows the details of the application. You can click on Create snapshot to create an on-demand snapshot or configure a protection policy.

Create an on-demand snapshot by simply clicking on **Create snapshot**, providing a name, reviewing the details, and clicking on **Snapshot**. The snapshot state changes to Healthy after the operation is completed.

	Dashboard	Data protection	Storage	Resources	Execution hooks	Activity	Tasks	Snapshots
١	Applications	Actions *	Configur	e protection policy		- Search		
٨	Clusters						0-0 of 0 entries	
	Cloud instances	Name	State	On-Schedu	e / On-Demand		Created ↑	Actions
٥	Buckets							
8	Account							
≣	Activity							
	Support			After you have o	don't have any snap	pshots will be listed b	ere	
(<)	III NetApp				Create snapshot			
		- hosedicadi						10119
密	Dashboard							
١	Applications	-M- APPLICA	ATION STATUS		 Partially protecte 	PPLICATION PR	OTECTION	(i)
٨	Clusters				•			
	Cloud instances	Definition postgresql			Cluster S api-i	rosa-cluster1-nn5w	<u>v-p1</u>	
۵	Buckets	Data protection	Storage	Resources	Execution hooks	Activity	Tasks	
8	Account	Actions 💌	Sconfigur	e protection policy		= Search		
	Activity						1-1 of 1 entries	$\langle \rangle$
5	Support	Name		State	on-Schedu	le / On-Demand	Created ↑	Actions
	NetApp	postgresql-sna	apshot-2024021	3154610 📀 H	lealthy 🔘 On-Den	nand	2024/02/13 15:4	8 UTC 🔅

10. Delete the database in the postgresql application

Log back into postgresql, list the available databases, delete the one you created previously and list again to ensure that the database has been deleted.

postgres=# \1 List of databases | Owner | Encoding | Locale Provider | Collate | ICU Locale | ICU Rules | Access priv Name Ctype postgres UTF8 libc en US.UTF-8 | en US.UTF-8 erp postgres postgres UTF8 libc en US.UTF-8 | en US.UTF-8 1 template0 | postgres | UTF8 libc en_US.UTF-8 | en_US.UTF-8 | =c/postgres postgres=CTc UTF8 en_US.UTF-8 | en_US.UTF-8 template1 | postgres libc -c/postgres | postgres=CTc/ (4 rows) postgres=# DROP DATABASE erp; DROP DATABASE postgres=# \1 List of databases | Encoding | Locale Provider | | ICU Locale | ICU Rules | Access priv Name Owner Collate Ctype postgres | UTF8 libc en_US.UTF-8 | en_US.UTF-8 postgres en US.UTF-8 | en_US.UTF-8 | UTF8 libc template0 | postgres | =c/postgres postgres=CTc template1 | postgres UTF8 libc en_US.UTF-8 | en_US.UTF-8 =c/postgres I postgres=CTc (3 rows)

11. Restore from a snapshot using ACS

To restore the application from a snapshot, go to ACS UI landing page, select the application and select Restore. You need to pick a snapshot or a backup from which to restore. (Typically, you would have multiple created based on a policy that you have configured). Make appropriate choices in the next couple of screens and then click on **Restore**. The application status moves from Restoring to Available after it has been restored from the snapshot.

따 Dashboard	© postgresql ^		C	Actions V
 Applications Clusters 	APPLICATION STATUS	(i) Partially prote	APPLICATION PROTECTION	Snapshot Back up Clone
Cloud instances	Definition postgresql	Cluster	i-rosa-cluster1-nn5w-p1-op	Unmanage
요 Account Activity	Data protection Storage Resources Actions Configure protection p	Execution hooks Ac	ctivity Tasks	
u	Name	State On-Scheo	dule / On-Demand Created †	Actions
 III NetApp 	postgresql-snapshot-20240213164912	⊘ Healthy © On-De	emand 2024/02/13	16:50 UTC 🔋

RESTORE TYPE			
Restore the application to new namespaces on any available	ble cluster or to original na	mespaces on the original cluster.	
Restore to new namespaces		Restore to original namespaces	
RESTORE SOURCE			
Select a snapshot or backup to restore the application to	a previous state.		
	Time range 🗸	Filter	Snapshots 🔒 Backups
Application snapshot	Snapshot state	On-Schedule / On-Demand	Created ↑
postgresql-snapshot-20240213164912	⊘ Healthy	On-Demand	2024/02/13 16:50 UTC
	Ca	ncel Next →	

Ƙ Dashboard	🍥 postgresql \land			C Actions	~
 Applications Clusters Cloud instances 	- →- APPLICATION STATUS	(i) <u>P</u>	S APPLICATION PROT artially protected A No	ECTION scheduled protection policy	(1)
Buckets	Definition postgresql		Cluster api-rosa-cluster1-nn5w-p1-o	p	
& Account	Data protection Storage Resource	s Execution ho	ooks Activity Tasks		
E Activity	Actions Configure protection	policy	- Search		
Support				1–1 of 1 entries	
	Name	State	On-Schedule / On-Demand	Created 1	Actions
In NetApp	postgresql-snapshot-20240213164912	⊘ Healthy	On-Demand	2024/02/13 16:50 UTC	

12. Verify your app has been restored from the snapshot

Login to the postgresql client and you should now see the table and the record in the table that you previously had. That's it. Just by clicking a button, your application has been restored to a previous state. That is how easy we make it for our customers with Astra Control.

[ec2-user@i 2.0-debian- Warning: wo legeEscalat: pod or cont. text.seccom If you don' postgres=#	0-10-49-11- 11-r1env uld violate ion=false), ainer "post pProfile.ty t see a com	132 ~]\$ kube ="PGPASSWORD PodSecurity unrestricte grosql-clier pe to "Runti mand prompt,	ectl run postgresg) -\$POSTGRES_PASSMOR / "restricted:v1.2/ d capabilities (co nt" must set securi imeDefault" or "Loc , try pressing ento	<pre>l-clientrm RD"command I": allowPrivi Intainer "postg ityContext.rund :alhost") er.</pre>	tty -1rest psqlhost iegeEscalation gresql-client" isNonRoot=true)	cart='Never' postgresql -l != false (cor must set sec), seccompProt	-namespace p I postgres -d itainer "post rityContext. Sile (pod or	ostgresqlimage docker.io/bitnami/postgresql:16. postgres -p 5432 gresql-client" must set securityContext.allowPrivi capabilities.drop=["ALL"]), runAsNonRoot != true (container "postgresql-client" must set securityCon
Mame	Ourser	Encoding	Locale Provider	List of dat	tabases Ctune	T(I) Locale	TOT Rules	Arcass privilanas
erp postgres template8 (4 rows) postgres=# You are now erp=# \dt U Schema 1 public p (1 row)	postgres postgres postgres postgres connected list of rela kame Ty ersons ta	UTF8 UTF8 UTF8 UTF8 UTF8 to database tions pe Owner ble postgr	libc libc libc libc rerp" as user "pos "es	en_US.UTF-8 en_US.UTF-8 en_US.UTF-8 en_US.UTF-8	en_US.UTF-8 en_US.UTF-8 en_US.UTF-8 en_US.UTF-8			<pre>-c/postgres + postgres=CTc/postgres -c/postgres + postgres=CTc/postgres</pre>
erp=# SELEC id first	i * from PE name last	name						
1 John (1 row)	Dae							Activate Windows

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

ROSA Cluster Integration with Amazon FSx for ONTAP

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.

Failover and Fail-back of applications on ROSA cluster



Data protection for Container Apps in OpenShift Container Platform using OpenShift API for Data Protection (OADP)

Author: Banu Sundhar, NetApp

This section of the reference document provides details for creating backups of Container Apps using the OpenShift API for Data Protection (OADP) with Velero on NetApp ONTAP S3 or NetApp StorageGRID S3. The backups of namespace scoped resources including Persistent Volumes(PVs) of the app are created using CSI Astra Trident Snapshots.

The persistent storage for container apps can be backed by ONTAP storage integrated to the OpenShift Cluster using Astra Trident CSI. In this section we use OpenShift API for Data Protection (OADP) to perform backup of apps including its data volumes to

- ONTAP Object Storage
- StorageGrid

We then restore from the backup when needed. Please note that the app can be restored only to the cluster from where the backup was created.

OADP enables backup, restore, and disaster recovery of applications on an OpenShift cluster. Data that can be protected with OADP include Kubernetes resource objects, persistent volumes, and internal images.



Red Hat OpenShift has leveraged the solutions developed by the OpenSource communities for data protection. Velero is an open-source tool to safely backup and restore, perform disaster recovery, and migrate Kubernetes cluster resources and persistent volumes. To use Velero easily, OpenShift has developed the OADP operator and the Velero plugin to integrate with the CSI storage drivers. The core of the OADP APIs that are exposed are based on the Velero APIs. After installing the OADP operator and configuring it, the backup/restore operations that can be performed are based on the operations exposed by the Velero API.



OADP 1.3 is available from the operator hub of OpenShift cluster 4.12 and later. It has a built-in Data Mover that can move CSI volume snapshots to a remote object store. This provides portability and durability by

moving snapshots to an object storage location during backup. The snapshots are then available for restoration after disasters.

The following are the versions of the various components used for the examples in this section

- OpenShift Cluster 4.14
- OADP Operator 1.13 provided by Red Hat
- Velero CLI 1.13 for Linux
- Astra Trident 24.02
- ONTAP 9.12
- postgresql installed using helm.

Astra Trident CSI OpenShift API for Data Protection (OADP) Velero

Data protection for Container Apps in OpenShift Container Platform using OpenShift API for Data Protection (OADP)

Author: Banu Sundhar, NetApp

This section of the reference document provides details for creating backups of Container Apps using the OpenShift API for Data Protection (OADP) with Velero on NetApp ONTAP S3 or NetApp StorageGRID S3. The backups of namespace scoped resources including Persistent Volumes(PVs) of the app are created using CSI Astra Trident Snapshots.

The persistent storage for container apps can be backed by ONTAP storage integrated to the OpenShift Cluster using Astra Trident CSI. In this section we use OpenShift API for Data Protection (OADP) to perform backup of apps including its data volumes to

- ONTAP Object Storage
- StorageGrid

We then restore from the backup when needed. Please note that the app can be restored only to the cluster from where the backup was created.

OADP enables backup, restore, and disaster recovery of applications on an OpenShift cluster. Data that can be protected with OADP include Kubernetes resource objects, persistent volumes, and internal images.



Red Hat OpenShift has leveraged the solutions developed by the OpenSource communities for data protection. Velero is an open-source tool to safely backup and restore, perform disaster recovery, and migrate Kubernetes cluster resources and persistent volumes. To use Velero easily, OpenShift has developed the OADP operator and the Velero plugin to integrate with the CSI storage drivers. The core of the OADP APIs that are exposed are based on the Velero APIs. After installing the OADP operator and configuring it, the backup/restore operations that can be performed are based on the operations exposed by the Velero API.



OADP 1.3 is available from the operator hub of OpenShift cluster 4.12 and later. It has a built-in Data Mover that can move CSI volume snapshots to a remote object store. This provides portability and durability by

moving snapshots to an object storage location during backup. The snapshots are then available for restoration after disasters.

The following are the versions of the various components used for the examples in this section

- OpenShift Cluster 4.14
- OADP Operator 1.13 provided by Red Hat
- Velero CLI 1.13 for Linux
- Astra Trident 24.02
- ONTAP 9.12
- postgresql installed using helm.

Astra Trident CSI OpenShift API for Data Protection (OADP) Velero

Installation of OpenShift API for Data Protection (OADP) Operator

This section outlines the installation of OpenShift API for Data Protection (OADP) Operator.

Prerequisites

- A Red Hat OpenShift cluster (later than version 4.12) installed on bare-metal infrastructure with RHCOS worker nodes
- · A NetApp ONTAP cluster integrated with the cluster using Astra Trident
- · A Trident backend configured with an SVM on ONTAP cluster
- A StorageClass configured on the OpenShift cluster with Astra Trident as the provisioner
- · Trident Snapshot class created on the cluster
- · Cluster-admin access to Red Hat OpenShift cluster
- Admin access to NetApp ONTAP cluster
- · An application eg. postgresql deployed on the cluster
- An admin workstation with tridentctl and oc tools installed and added to \$PATH

Steps to install OADP Operator

1. Go to the Operator Hub of the cluster and select Red Hat OADP operator. In the Install page, use all the default selections and click install. On the next page, again use all the defaults and click Install. The OADP operator will be installed in the namespace openshift-adp.

Home >	OperatorHub			
Operators 🗸	Discover Operators from the Kub optional add-ons and shared serv	ernetes community and Red Hat partners, curated b vices to your developers. After installation, the Opera	y Red Hat. You can purchase commercial so ator capabilities will appear in the Developer	ftware through Red Hat Ma Catalog providing a self-se
Installed Operators	All Items Al/Machine Learning	All Items		
Workloads >	Application Runtime	Q OADP X		
Virtualization >	Cloud Provider	Red Hat	Community	
Networking >	Developer Tools	OADP Operator	OADP Operator provided by Red Hat OADP (OpenShift API for Data	
Storage	Drivers and plugins	provided by Red Hat OADP (OpenShift API for Data		
Builds >	Integration & Delivery Logging & Tracing	Protection) operator sets up and installs Data Protection	Protection) operator sets up and installs Velero on the OpenShift	
Observe >	Modernization & Migration			



Project: A	Il Projects 🔻			
Installed Operator	ed Operators Operators are represented by C and ClusterServiceVersion usin	ClusterServiceVersions within this Name ng the Operator SDK 🗗.	space. For more information, see the Under	standing Operators documentation 🗹
Name •	Search by name	Namespace	Managed Namespaces 🗍	Status
	OpenShift Virtualization 4.14.4 provided by Red Hat	NS openshift-cnv	NS openshift-cnv	Succeeded Up to date
4	OADP Operator 1.3.0 provided by Red Hat	NS openshift-adp	NS openshift-adp	Succeeded Up to date
4	Package Server 0.0.1-snapshot provided by	NS openshift-operator-lifecycle- manager	NS openshift-operator-lifecycle- manager	Succeeded

Prerequisites for Velero configuration with Ontap S3 details

After the installation of the operator succeeds, configure the instance of Velero.

Velero can be configured to use S3 compatible Object Storage. Configure ONTAP S3 using the procedures shown in the Object Storage Management section of ONTAP documentation. You will need the following information from your ONTAP S3 configuration to integrate with Velero.

- A Logical Interface (LIF) that can be used to access S3
- · User credentials to access S3 that includes the access key and the secret access key
- A bucket name in S3 for backups with access permissions for the user
- For secure access to the Object storage, TLS certificate should be installed on the Object Storage server.

Prerequisites for Velero configuration with StorageGrid S3 details

Velero can be configured to use S3 compatible Object Storage. You can configure StorageGrid S3 using the procedures shown in the StorageGrid documentation. You will need the following information from your StorageGrid S3 configuration to integrate with Velero.

- The endpoint that can be used to access S3
- · User credentials to access S3 that includes the access key and the secret access key
- · A bucket name in S3 for backups with access permissions for the user
- For secure access to the Object storage, TLS certificate should be installed on the Object Storage server.

Steps to configure Velero

• First, create a secret for an ONTAP S3 user credential or StorageGrid Tenant user credentials. This will be used to configure Velero later. You can create a secret from the CLI or from the web console. To create a secret from the web console, select Secrets, then click on Key/Value Secret. Provide the values for the credential name, key and the value as shown. Be sure to use the Access Key Id and Secret Access Key of your S3 user. Name the secret appropriately. In the sample below, a secret with ONTAP S3 user credentials named ontap-s3-credentials is created.

Installed Operators	Project: openshift-adp 🔻		
Workloads 🗸 🗸	Secrets	Create 👻	
Pods		Key/value secret	
Deployments	▼ Filter ▼ Name ▼ Search by name 7 Size	Image pull secret	
DeploymentConfigs	Name I Type I S	Created 1 Source secret	
StatefulSets	Suilder-dockercfg-7g8ww kubernetes.io/dockercfg 1	Apr 11, 2024, 10:52 AN Webhook secret	
Secrets	S builder-token-rm4s kubernetes.io/service-account-token 4	Apr 11, 2024, 10:52 AN	

Edit key/value sec	ret	
Key/value secrets let you inject variables.	sensitive data into your application as files or environment	
Secret name *		
ontap-s3-credentials		
Unique name of the new secret		
Key *		
cloud		
Value		
	Browse	
Drag and drop file with your val	ue here or browse to upload it.	
[default] aws_access_key_id= aws_secret_access_key=	· · · · · · · · · · · · · · · · · · ·	
Add keyAralije		
· Add Key value		

To create a secret named sg-s3-credentials from the CLI you can use the following command.
oc create secret generic sg-s3-credentials --namespace openshift-adp --from-file cloud=cloud-credentials.txt Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3 user in the following format: [default] aws_access_key_id=< Access Key ID of S3 user> aws_secret_access_key=<Secret Access key of S3 user>

• Next, to configure Velero, select Installed Operators from the menu item under Operators, click on OADP operator, and then select the **DataProtectionApplication** tab.

Home	>	Installed Operators								
Operators	•	Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the Understanding Operators documentation 12. Or create an Operator and ClusterServiceVersion								
OperatorHub		Operator SDK 🗹	perator SDK 💋							
Installed Operators		Name Search by name	7							
Workloads	>	Name 1	Managed Namespaces 1	Status	Last updated	Provided APIs				
Virtualization	>	OADP Operator 1.3.0 provided by Red Hat	NS openshift-adp	Succeeded Up to date	Apr 11, 2024, 10:53 AM	BackupRepository : Backup				
Networking	>					BackupStorageLocation DeleteBackupRequest View 11 more				

Click on Create DataProtectionApplication. In the form view, provide a name for the DataProtection Application or use the default name.

Project: openshift-adp	•				
Installed Operators > Operator OADP Operator 1.3.0 provided by R	ator details ed Hat				Actions 💌
ServerStatusRequest	VolumeSnapshotLocation	DataDownload	DataUpload	CloudStorage	DataProtectionApplication
DataProtection	Applications				Create DataProtectionApplication

Now go to the YAML view and replace the spec information as shown in the yaml file examples below.

Sample yaml file for configuring Velero with ONTAP S3 as the backupLocation

```
spec:
 backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false' ->use this for https
communication with ONTAP S3
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true' ->This allows use of IP in s3URL
          s3Url: 'https://10.61.181.161' ->Ensure TLS certificate for S3
is configured
        credential:
          key: cloud
          name: ontap-s3-credentials -> previously created secret
        default: true
        objectStorage:
          bucket: velero -> Your bucket name previously created in S3 for
backups
          prefix: container-demo-backup ->The folder that will be created
in the bucket
          caCert: <base64 encoded CA Certificate installed on ONTAP
Cluster with the SVM Scope where the bucker exists>
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
      #default Data Mover uses Kopia to move snapshots to Object Storage
    velero:
      defaultPlugins:
        - csi ->This plugin to use CSI snapshots
        - openshift
        - aws
        - kubevirt -> This plugin to use Velero with OIpenShift
Virtualization
```

Sample yaml file for configuring Velero with StorageGrid S3 as the backupLocation

```
spec:
 backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1 ->region of your StorageGrid system
          s3ForcePathStyle: 'True'
          s3Url: 'https://172.21.254.25:10443' ->the IP used to access S3
        credential:
          key: cloud
          name: sg-s3-credentials ->secret created earlier
        default: true
        objectStorage:
          bucket: velero
          prefix: demobackup
        provider: aws
 configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

The spec section in the yaml file should be configured appropriately for the following parameters similar to the example above

backupLocations

ONTAP S3 or StorageGrid S3 (with its credentials and other information as shown in the yaml) is configured as the default BackupLocation for velero.

snapshotLocations

If you use Container Storage Interface (CSI) snapshots, you do not need to specify a snapshot location because you will create a VolumeSnapshotClass CR to register the CSI driver. In our example, you use Astra Trident CSI and you have previously created VolumeSnapShotClass CR using the Trident CSI driver.

Enable CSI plugin

Add csi to the defaultPlugins for Velero to back up persistent volumes with CSI snapshots. The Velero CSI plugins, to backup CSI backed PVCs, will choose the VolumeSnapshotClass in the cluster that has **velero.io/csi-volumesnapshot-class** label set on it. For this

- You must have the trident VolumeSnapshotClass created.
- · Edit the label of the trident-snapshotclass and set it to

velero.io/csi-volumesnapshot-class=true as shown below.



Ensure that the snapshots can persist even if the VolumeSnapshot objects are deleted. This can be done by setting the **deletionPolicy** to Retain. If not, deleting a namespace will completely lose all PVCs ever backed up in it.

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
   name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```

VolumeSnapshotClasses > VolumeSnapshotClass details						
vsc trident-snapshotclass						
Details YAML Events						
VolumeSnapshotClass details						
Name						
trident-snapshotclass						
Labels	Edit 🖋					
velero.io/csi-volumesnapshot-class=true						
Annotations						
1 annotation 🖋						
Driver						
csi.trident.netapp.io						
Deletion policy						
Retain						

Ensure that the DataProtectionApplication is created and is in condition:Reconciled.

Proje <mark>ct:</mark> oj	penshift-adp 🝷							
Installed Op	erators > Operator details OPDP Operator 3.2 provided by Red Hat							Actions 🔸
Schedule	ServerStatusRequ	est VolumeSnapshotl	Location	DataDownload	DataUpload	CloudStorage	DataProtection	Application
DataPr Name -	Search by name	ations				I	Create DataProtecti	onApplication
Name	1	Kind I	Status	1	Labels I	Last up	odated I	
DPA v b	elero-container- ackup-ontap	DataProtectionApplication	Conditio	n: Reconciled	No labels	🕲 Jul	15, 2024, 2:31 PM	I

The OADP operator will create a corresponding BackupStorageLocation. This will be used when creating a backup.

Project: openshift-adp 🔹					
Installed Operators > Operator d OADP Operator 1.3.2 provided by Red Ha	etails It				Actions 👻
kupRepository Backup	BackupStorageLocation	DeleteBackupRequest	DownloadRequest F	PodVolumeBackup	PodVolumeRestore
Name Search by name Name	Kind 1	Status	Labels 1	Create 1	BackupStorageLocation
ESI velero-container- backup-ontap-1	BackupStorageLocation	Phase: Available	app.kubernetes.io/component app.kubernet=velero-contai app.kubernetes.io/m=oadp- app.kubernetes=oadp-oper	etebal 🚯 Jul 15, 2024, 2:3	≋PM ₿
			openshiftio/oadp=True openshiftio/oadp-registry=Tr	rue	

Creating on-demand backup for Apps in OpenShift Container Platform

This section outlines how to create on-demand backup for VMs in OpenShift Virtualization.

Steps to create a backup of an App

To create an on-demand backup of an app (app metadata and persistent volumes of the app), click on the **Backup** tab to create a Backup Custom Resource (CR). A sample yaml is provided to create the Backup CR. Using this yaml, the app and its persistent storage in the specified namespace will be backed up. Additional parameters can be set as shown in the documentation.

A snapshot of the persistent volumes and the app resources in the namespace specified will be created by the CSI. This snapshot will be stored in the backup location specified in the yaml. The backup will remain in the system for 30 days as specified in the ttl.

```
spec:
    csiSnapshotTimeout: 10m0s
    defaultVolumesToFsBackup: false
    includedNamespaces:
        - postgresql ->namespace of the app
    itemOperationTimeout: 4h0m0s
    snapshotMoveData: false
    storageLocation: velero-container-backup-ontap-1 -->this is the
backupStorageLocation previously created when Velero is configured.
    ttl: 720h0m0s
```

Once the backup completes, its Phase will show as completed.

Installed C	OADP 1.3.2 pro	 Operato operato 	rator details or Red Hat							Actions 👻
Details	YA	ML	Subscription	Events	All instances	BackupReposito	bry Backup	BackupStorageLocation	Delete	BackupReques
Backu	ups									Create Backup
Name	• s	earch by	name	1						
Name	1		Kind	1	Status	I	Labels 1	Last updated	1	
B ba	ackup-p	ostgresql	-ontaps3 Backu	P	Phase	Completed	velero.io/sto =ve	elero-container) 🕲 Jul 16, 202	4, 10:01 AM	I

You can inspect the backup in the Object storage with the help of an S3 browser application. The path of the backup shows up in the configured bucket with the prefix name (velero/container-demo-backup). You can see the contents of the backup includes the volume snapshots, logs, and other metadata of the application.



In StorageGrid, you can also use the S3 console that is available from the Tenant Manager to view the backup objects.

lame	Size	Туре	Last Modified	Storage Class
backup-postgresql-ontaps3.tar.gz	384.66 KB	GZ File	7/16/2024 10:01:20 AM	STANDARD
velero-backup.json	3.30 KB	JSON File	7/16/2024 10:01:20 AM	STANDARD
backup-postgresql-ontaps3-csi-volumesnap	731 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
backup-postgresql-ontaps3-csi-volumesnap	760 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
backup-postgresql-ontaps3-resource-list.jso	823 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
backup-postgresql-ontaps3-itemoperations.j	378 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
backup-postgresql-ontaps3-volumesnapshot	29 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
backup-postgresql-ontaps3-podvolumeback	29 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
backup-postgresql-ontaps3-results.gz	49 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
backup-postgresql-ontaps3-csi-volumesnap	429 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
hackup-postaresal-ontans3-logs az	12 01 KB	G7 File	7/16/2024 10:01:19 AM	STANDARD

Creating scheduled backups for Apps

To create backups on a schedule, you need to create a Schedule CR.

The schedule is simply a Cron expression allowing you to specify the time at which you want to create the backup. A sample yaml to create a Schedule CR is shown below.

```
apiVersion: velero.io/v1
kind: Schedule
metadata:
    name: schedule1
    namespace: openshift-adp
spec:
    schedule: 0 7 * * *
    template:
        includedNamespaces:
            - postgresql
        storageLocation: velero-container-backup-ontap-1
```

The Cron expression 0 7 * * * means a backup will be created at 7:00 every day. The namespaces to be included in the backup and the storage location for the backup are also specified. So instead of a Backup CR, Schedule CR is used to create a backup at the specified time and frequency.

Once the schedule is created, it will be Enabled.

Project: openshift-adp	•				
Installed Operators > Operator OADP Operator 1.3.2 provided by Rev	or details d Hat				Actions 👻
PodVolumeRestore Re	store Schedule	ServerStatusRequest	VolumeSnapshotLocation	DataDownload DataUpload	CloudStorage
4					•
Schedules				a	eate Schedule
Name 👻 Search by na	me				
Name 1	Kind I	Status 1	Labels 1	Last updated	
S schedule1	Schedule	Phase: 🔮 En	abled No labels	🕲 Jul 16, 2024, 10:32 AM	1

Backups will be created according to this schedule, and can be viewed from the Backup tab.

indicer openisin	t-adp •					
Installed Operators OADP O 132 provi	 Operator details perator ded by Red Hat 					Actions 👻
All instances	BackupRepositor	Backup	BackupStorageLocation	DeleteBackupRequest	DownloadRequest	PodVolumeBackup
Backups						Create Backup
Backups	rch by name Kind	2	Status	Labels I	Last updated	Create Backup
Backups Name Set Name I Backup-post	rch by name Kind tgresql-ontaps3 Backup	2	Status I Phase: @ Completed	Labels I velero.io/sto =velero-contai	Last updated I iner 3 Jul 16, 2024, 10:01	Create Backup

Migrate an App from one cluster to another

Velero's backup and restore capabilities make it a valuable tool for migrating your data between clusters. This section describes how to migrate apps(s) from one cluster to another by creating a backup of the app in Object storage from one cluster and then restoring the app from the same object storage to another cluster.

Prerequisites on Cluster 1

- Astra Trident must be installed on the cluster.
- A trident backend and Storage class must be created.
- OADP operator must be installed on the cluster.
- The DataProtectionApplication should be configured.

Use the following spec to configure the DataProtectionApplication object.

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false'
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'
          s3Url: 'https://10.61.181.161'
        credential:
          key: cloud
          name: ontap-s3-credentials
        default: true
        objectStorage:
          bucket: velero
          caCert: <base-64 encoded tls certificate>
          prefix: container-backup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

• Create an application on the cluster and take a backup of this application. As an example, install a postgres application.

[root@localhos	t ~]# oc	get nodes	5							
NAME	STATUS	ROLES		AGE	VERSION					
ocp6-master1	Ready	control-	plane, maste	r 3d13h	v1.27.15+614	7456				
ocp6-master2	Ready	worker		3d12h	v1.27.15+6142	7456				
ocp6-master3	Ready	control-	plane,maste	r 3d13h	v1.27.15+6147	7456				
ocp6-worker1	Ready	worker		3d12h	v1.27.15+6147	7456				
ocp6-worker2	Ready	worker		3d12h	v1.27.15+6147	7456				
ocp6-worker3	Ready	control-	plane, maste	r 3d12h	v1.27.15+6147	7456				
[root@localhos	t ~]# he	lm install	postgresql	bitnami/p	ostgresql -n po	ostgresqlcre	ate namespac	2^C		
[root@localhos	t ~]# oc	get pods	-n postgres	q1						2
NAME	READY	STATUS	RESTARTS	AGE						
postgresql-0	1/1	Running	0	4h53m						9
[root@localhos	t ~]# oc	get pvc -	n postgresq	1						1
NAME	ST	ATUS VOL	UME			CAPACITY	ACCESS MODE	5 STORAGECLASS	AGE	
data-postgresq	1-0 Bo	und pvc	-f7a3c772-0	e61-49cb-a	3d0-7c7b2ec87d	:6 8Gi	RWO	ontap-nas	4h53m	i i
[root@localhos	t ~]# oc	get pv -n	postgresq1							
NAME				CAPACITY	ACCESS MODES	RECLAIM POLIC	Y STATUS	CLAIM		STORAGECLASS
REASON AGE										
pvc-2e9e982f-5 4h55m	4a4-4e7b	-8eae-a589	e0d9d819	1G1	RWO	Delete	Bound	trident/basic		ontap-nas
pvc-f7a3c772-0 4h53m	e61-49cb	-a3d0-7c7b	2ec87dc6	8Gi	RWO	Delete	Bound	postgresq19dätätj Go to Sett	ostgresq100 tings to activate	ontap-nas Windows.
[root@localhos	t ~]# _									

• Use the following spec for the backup CR:

```
spec:
    csiSnapshotTimeout: 10m0s
    defaultVolumesToFsBackup: false
    includedNamespaces:
        - postgresql
    itemOperationTimeout: 4h0m0s
    snapshotMoveData: true
    storageLocation: velero-sample-1
    ttl: 720h0m0s
```

Project: ope	nshift-adp	•				
Installed Opera OAI 1.4.0	tors > Operato DP Operator provided by Red	or details d Hat				Actions 👻
Repository	Backup	BackupStorageLocation	n DeleteBackupReques	t DownloadRequest	PodVolumeBackup	PodVolumeRes
Backups	5					Create Backup
Name 👻	Search by nar	ne /				
Name 1			Kind 1		Status 1	
(B) backup			Backup		Activate Wind Go to Settings to a	OWS pleted crivate Windows.

You can click on the **All instances** tab to see the different objects being created and moving through different phases to finally come to the backup **completed** phase.

A backup of the resources in the namespace postgresql will be stored in the Object Storage location (ONTAP S3) specified in the backupLocation in the OADP spec.

Prerequisites on Cluster 2

- Astra Trident must be installed on cluster 2.
- The postgresql app must NOT be already installed in the postgresql namespace.
- OADP operator must be installed on cluster 2, and the BackupStorage Location must be pointing to the same object storage location where the backup was stored from the first cluster.
- The Backup CR must be visible from the second cluster.

NAME	READY	STATUS	RESTARTS	AGE
trident-controller-6799cfb77f-8rzvk	6/6	Running	6	2d7h
trident-node-linux-7wvjz	2/2	Running	2	2d7h
trident-node-linux-8vvm2	2/2	Running	0	2d7h
trident-node-linux-bgs6f	2/2	Running	2	2d7h
trident-node-linux-njwb8	2/2	Running	0	2d7h
trident-node-linux-scqjl	2/2	Running	0	2d7h
trident-node-linux-swr69	2/2	Running	2	2d7h
trident-operator-b88b86fc8-7fk68 [root@localbost ~]#	1/1	Running	1	2d7h





1.4.0 provided	ator by Red Hat							Actions 🝷
Details YAML	Subscription	Events	All instances	BackupRepository	Backup	BackupStorageLocation	DeleteBackupRequest	DownloadRequest
3ackups								Create Backup
Name 🔻 Search	by name	1						
Name 1		Kind I		Status 1		Labels 1	Last updated 1	
					a.	(

Restore the app on this cluster from the backup. Use the following yaml to create the Restore CR.

```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
   name: restore
   namespace: openshift-adp
spec:
   backupName: backup
   restorePVs: true
```

When the restore is completed, you will see that the postgresql app is running on this cluster and is associated with the pvc and a corresponding pv. The state of the app is the same as when the backup was taken.

Project: ope	nshift-adp 🔻						
Installed Opera	ators > Operator details DP Operator 0 provided by Red Hat					Action	ns 🔻
eLocation •	DeleteBackupRequest	DownloadRequest	PodVolumeBackup	PodVolumeRestore	Restore	Schedule	Server
Restore	S					Create R	estore
Name 🔻	Search by name						
Name 1		Kind	1 I.		Status 1		
(R) restore		Rest	tore	1	Activate Win Phase: @ C Go to Settings to	dows ompleted activate Wind	ows.

Project: ope	nshift-adp 🔻						
OA 1.4.0	DP Operator details DP Operator provided by Red Hat					Action	is 🔻
Location	DeleteBackupRequest	DownloadRequest	PodVolumeBackup	PodVolumeRestore	Restore	Schedule	Serve
Restore	s					Create R	estore
Name 👻	Search by name	Z					
Name 1		Kind	I		Status 1		
R restore		Resto	re	F	Activate Wind Phase: O Co	dows	

Restore an App from a backup

This section describes how to restore apps(s) from a backup.

Prerequisites

To restore from a backup, let us assume that the namespace where the app existed got accidentally deleted.



To restore from the backup that we just created, we need to create a Restore Custom Resource (CR). We need to provide it a name, provide the name of the backup that we want to restore from and set the restorePVs to true. Additional parameters can be set as shown in the documentation. Click on Create button.

Proj	ect: openshift-adp 🔹						
Insta	OADP Operator 1.3.0 provided by Red Ha	etails					Actions 💌
est	DownloadRequest	PodVolumeBackup	PodVolumeRestore	Restore	Schedule	ServerStatusRequest	VolumeSnap •
Re	stores					C	reate Restore

```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
   name: restore
   namespace: openshift-adp
spec:
   backupName: backup-postgresql-ontaps3
   restorePVs: true
```

When the phase shows completed, you can see that the app has been restored to the state when the snapshot was taken. The app is restored to the same namespace.

Proj	ect: openshift-adp 🔹						
Instal	Iled Operators > Operator def OADP Operator 1.3.0 provided by Red Hat	tails					Actions 👻
est	DownloadRequest	PodVolumeBackup	PodVolumeRestore	Restore	Schedule	ServerStatusRequest	: VolumeSr
Re	stores						Create Restore
Nar	me 👻 Search by name	1					
١	Name 1	Kind 1	:	Status 💲	Labe	ls 🕽	
•	R restore1	Restore	I	Phase: 🕏 Comp	oleted No lai	bels	

[root@localhos	t ~]#				
[root@localhos	t ~]# oc	get pods	-n postgre	sql	
No resources fo	ound in p	postgresql	namespace		
[root@localhos	t ~]# oc	get pods	-n postgre	sql	
NAME	READY	STATUS		RESTARTS	AGE
postgresql-0	0/1	Container	Creating	0	16s
[root@localhos	t ~]# oc	get pods	-n postgre	sql	
NAME	READY	STATUS	RESTARTS	AGE	
postgresql-0	0/1	Running	0	22s	
[root@localhos	t ~]# oc	get pods	-n postgre	sql	
NAME	READY	STATUS	RESTARTS	AGE	
postgresql-0	0/1	Running	0	29s	
[root@localhos	t ~]# oc	get pods	-n postgre	sql	
NAME	READY	STATUS	RESTARTS	AGE	
postgresql-0	1/1	Running	0	37s	
[root@localhos	t~]#				

To restore the App to a different namespace, you can provide a namespaceMapping in the yaml definition of the Restore CR.

The following sample yaml file creates a Restore CR to restore an App and its persistent storage from the postgresql namespace, to the new namespace postgresql-restored.

```
apiVersion: velero.io/v1
kind: Restore
metadata:
   name: restore-to-different-ns
   namespace: openshift-adp
spec:
   backupName: backup-postgresql-ontaps3
   restorePVs: true
   includedNamespaces:
        postgresql
   namespaceMapping:
        postgresql: postgresql-restored
```

When the phase shows completed, you can see that the app has been restored to the state when the snapshot was taken. The App is restored to a different namespace as specified in the yaml.

[root@localhos	t ~]# oc	get pods	-n postgres	ql
No resources f	ound in p	postgresql	namespace.	
[root@localhos	t ~]# oc	get pods	-n postgres	ql-restored
NAME	READY	STATUS	RESTARTS	AGE
postgresql-0	0/1	Running	0	19s
[root@localhos	t ~]# oc	get pods	-n postgres	ql-restored
NAME	READY	STATUS	RESTARTS	AGE
postgresql-0	0/1	Running	0	22s
[root@localhos	t ~]# oc	get pods	-n postgres	ql-restored
NAME	READY	STATUS	RESTARTS	AGE
postgresql-0	1/1	Running	0	36s
[root@localhos	t ~]#			

Velero provides a generic ability to modify the resources during restore by specifying json patches. The json patches are applied to the resources before they are restored. The json patches are specified in a configmap and the configmap is referenced in the restore command. This feature enables you to restore using different storage class.

In the example below, the app, during deployment uses ontap-nas as the storage class for its persistent volumes. A backup of the app named backup-postgresql-ontaps3 is created.

Construction of the second of		
Details YAML Events VolumeSnapshots		
PersistentVolumeClaim details		
\frown		
8 GIB		
Name data-postgresql-0		Status © Bound
Namespace		Requested capacity 8 GB
	Edit #	Capacity
(appluberretesio/componentspirmary) (appluberretesio/instance-postgress) (appluberretesio/instance-postgress) (welenio/instance-postgress) (welenio/instance-postgress) (welenio/instance-postgress)		Used
(velerolig/volume-ortgothol+vame-velero-data-pointgreagl=0-74ph)		13 MB
Annotetions		Access modes ReadWriteOnce
Samotations		Volume mode
Label selector No selector		Filetystem
Created at		StorgeClasses
O Jul 15, 2024, 259 PM		PersistentVolumes
Owner Na owner		
Moject openantr-acp 💌		
Installed Operators > Operator details OADP Operator		
S 132 provided by Red Het		

Details YAML Subscription	Events All instances	BackupRepository	Backup	BackupStorageLocation	DeleteBackupRequest	DownloadRequest	PodVolumeBackup	PodVolumeRestore	Restore
Backups									0
Name • Search by name	1								
Name 1	Kind 1		s	tatus	Labels 1		Lest updated	1	
A REAL PROPERTY OF A READ REAL PROPERTY OF A REAL P					6				

Simulate a loss of the app by uninstalling the app.

To restore the VM using a different storage class, for example, ontap-nas-eco storage class, you need to do the following two steps:

Step 1

Create a config map (console) in the openshift-adp namespace as follows: Fill in the details as shown in the screenshot: Select namespace : openshift-adp Name: change-ontap-sc (can be any name) Key: change-ontap-sc-config.yaml: Value:

```
version: v1
resourceModifierRules:
- conditions:
    groupResource: persistentvolumeclaims
    resourceNameRegex: "data-postgresql*"
    namespaces:
    - postgresql
    patches:
    - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"
```

ECIT CONTIGNAD Config maps hold key-value pairs that can be used in pods to read application configuration. Configure via: Form view VAML view Name * change-ontap-sc A unique name for the ConfigMap within the project Immutable Immutable (Immutable Immutable (Immutable Immutable, if set to true, ensures that data stored in the ConfigMap cannot be updated Data Data Data contains the configuration data that is in UTF-8 range Key * change-ontap-sc.yaml Value Drag and drop file with your value here or browse to upload it. version: v1 resourceNodifierRules: - conditions: groupResource: persistent/volumeclains resourceNoteFireRise: - opersignesa] patches: - opersion: replace patter:		
Configure via: Form view YaML view Name * change-ontap-sc A unique name for the ConfigMap within the project Immutable Immutable, if set to true, ensures that data stored in the ConfigMap cannot be updated Data Data Data Data Configure via: Configuration data that is in UTF-8 range Remove key/value Key * change-ontap-scyaml Value Drag and drop file with your value here or browse to upload it. version: v1 resource/idaffierRules:	Lait ConfigMap	
Configure via: Form view YAML view Name * Change-ontap-sc A unique name for the ConfigMap within the project Immutable Immutable Is to true, ensures that data stored in the ConfigMap cannot be updated Data Data contains the configuration data that is in UTF-8 range Remove key/value Key * Change-ontap-scyaml Value Value Drag and drop file with your value here or browse to upload it. Version: v1 resourcevoidflerRules: - conditions: grougResource: persistentvolumeclaims resourcevoidflerRules: - operation: replace patches: - operation: replace patches: - operation: replace	Config maps hold key-value pairs that can be used in pods to read application configuration.	
Name * change-ontap-sc A unique name for the ConfigMap within the project Immutable Immutable, if set to true, ensures that data stored in the ConfigMap cannot be updated Data Data Data Data Data Data Change-ontap-scyamI Change-ontap-scyamI Colored Data Drag and drop file with your value here or browse to upload it. Version: v1 ressource(valueeColored) Remove to upload it. Version: v1 remove to upload it. Version: v1 remove to upload Remo	Configure via: 💿 Form view 🔿 YAML view	
change-ontap-sc A unique name for the ConfigMap within the project I mmutable Immutable Immutable Data Data Data Data contains the configuration data that is in UTF-8 range Change-ontap-sc yaml Value Value Drag and drop file with your value here or browse to upload it. Version: v1 resourceModifierRules: - conditions: groupResource: persistentvolumeclaims resourceModifierRules: - opstgressi patses: - operation: replace patt: "/spec/storageClassName" value: "ortap-nas-eco"	lame *	
A unique name for the ConfigMap within the project Immutable Immutable Bata Data Data Data Certains the configuration data that is in UTF-8 range Centage-ontage-scyaml Value Value Drag and drop file with your value here or browse to upload it. Version: v1 resourceModifierRules: - conditions: groupResource: persistentvolumeclaims resourceMateRegex: "data-postgresgle"	change-ontap-sc	
Immutable Immutable, if set to true, ensures that data stored in the ConfigMap cannot be updated Data Data contains the configuration data that is in UTF-8 range Remove key/value Key * change-ontap-scyaml Value Value Drag and drop file with your value here or browse to upload it. version: v1 resourceWodifierRules: - conditions: groupResource: persistentvolumeclains resourceHameRegex: "data-postgresgl*" namespaces: - opsration: replace patt: "/spec/storageclassName" value: "ontap-nas-eco"	unique name for the ConfigMap within the project	
Immutable, if set to true, ensures that data stored in the ConfigMap cannot be updated Data Data contains the configuration data that is in UTF-8 range Remove key/value Key * change-ontap-sc.yaml Value Trag and drop file with your value here or browse to upload it. version: v1 resource/codifierRules: - conditions: groupResource: persistentvolumeclaims resource/codifierRules: - conditions: groupResource: persistentvolumeclaims resource/codifierRules: - postgress1 patches: - operation: replace pat: "/spec/storageClassName" value: "ontap-nas-eco"] Immutable	
Data contains the configuration data that is in UTF-8 range Remove key/value Key change-ontap-scyaml Value Drag and drop file with your value here or browse to upload it. version: v1 resourceWodifierRules: - conditions: groupResource: persistentvolumeclaims resourcellaneRegex: "data-postgresol*" namespaces: - postgresol patches: - operation: replace path: "/spec/storrageClassName" value: "ontap-nas-eco"	mmutable, if set to true, ensures that data stored in the ConfigMap cannot be updated	
Data contains the configuration data that is in UTF-8 range Remove key/value Key * Change-ontap-scyaml Value Drag and drop file with your value here or browse to upload it. Version: v1 resourceWodifierRules: - conditions: groupResource: persistentvolumeclaims resourceNodifierRules: - conditions: groupResource: relate-postgresal*" namespaces: - postgresal patches: - operation: replace path: "/spec/storageclassName" value: "ontap-nas-eco"	Data	
<pre> Remove key/value Key * change-ontap-scyaml Value Drag and drop file with your value here or browse to upload it. version: v1 resourceWodifierRules: - conditions: groupResource: persistentvolumeclaims resourceNameRegex: "dta-postgresgl*" namespaces: - postgresgl patches: - operation: replace path: "/spec/storageclassName" value: "ortap-nas-eco" </pre>	ata contains the configuration data that is in UTF-8 range	
Key change-ontap-scyaml Value Drag and drop file with your value here or browse to upload it. version: v1 resourceWodifierRules: - conditions: groupResource: persistentvolumeclaims resourceNameRegex: "data-postgresgl*" namespaces: - postgresgl patches: - operation: replace path: "/spec/storageClassName" value: "ontap-nas-eco"		Remove key/value
change-ontap-scyaml Value Browse Drag and drop file with your value here or browse to upload it. version: v1 resourceModifierRules: - conditions: groupResource: persistentvolumeclaims resourceNameRegex: "data-postgresgl*" namespaces: - postgresgl patches: - operation: replace path: "/spec/storageClassName" value: "ontap-nas-eco"	(ey *	
Value Browse Drag and drop file with your value here or browse to upload it. version: v1 resourceWodifierRules: - conditions: groupResource: persistentvolumeclaims resourceNameRegex: "data-postgresgl*" namespaces: - postgresgl patches: - operation: replace path: "/spec/storageClassName" value: "ontap-nas-eco"	change-ontap-sc.yaml	
Value Browse Drag and drop file with your value here or browse to upload it. version: v1 resourceModifierRules: - conditions: groupResource: persistentvolumeclaims resourceNameRegex: "data-postgresgl*" namespaces: - postgresgl patches: - operation: replace path: "/spec/storageClassName" value: "ontap-nas-eco"		
Browse Drag and drop file with your value here or browse to upload it. version: v1 resourceModifierRules: - conditions: groupResource: persistentvolumeclaims resourceNameRegex: "data-postgresgl*" namespaces: - postgresgl patches: - operation: replace patt: "/spec/storageClassName" value: "ontap-nas-eco"	/alue	
Drag and drop file with your value here or browse to upload it. version: v1 resourceWodifierRules: - conditions: groupResource: persistentvolumeclaims resourceNameRegex: "data-postgresgl*" namespaces: - postgresgl patches: - operation: replace path: "/spec/storageClassName" value: "ontap-nas-eco"		Browse
<pre>version: v1 resourceModifierRules: - conditions: groupResource: persistentvolumeclaims resourceNameRegex: "data-postgresgl*" namespaces: - postgresgl patches: - operation: replace path: "/spec/storageClassName" value: "ontap-nas-eco"</pre>	Drag and drop file with your value here or browse to upload it.	
<pre>resourceModifierRules: - conditions: groupResource: persistentvolumeclaims resourceNameRegex: "data-postgresgl*" namespaces: - postgresgl patches: - operation: replace path: "/spec/storageClassName" value: "ontap-nas-eco"</pre>	version: v1	
<pre>- conditions: groupResource: persistentvolumeclaims resourceNameRegex: "data-postgresgl*" namespaces: - postgresgl patches: - operation: replace path: "/spec/storageClassName" value: "ontap-nas-eco"</pre>	resourceModifierRules:	
<pre>groupkesource: persistentVolumeclaims resourceNameRegex: "data-postgresgl*" namespaces: postgresgl patches: operation: replace path: "/spec/storageClassName" value: "ontap-nas-eco"</pre>	- conditions:	
<pre>resourcentainteregex: data-postgresur namespaces: - postgresgl patches: - operation: replace patt: "/spec/storageClassName" value: "ontap-nas-eco"</pre>	groupkesource: persistentvolumeclaims	
<pre>- postgresgl patches: - operation: replace path: "/spec/storageClassName" value: "ontap-nas-eco"</pre>	namespaces:	
<pre>patches: - operation: replace path: "/spec/storageClassName" value: "ontap-nas-eco"</pre>	- postgresal	
- operation: replace path: "/spec/storageClassName" value: "ontap-nas-eco"	patches:	
path: "/spec/storageClassName" value: "ontap-nas-eco"	- operation: replace	
value: "ontap-nas-eco"	<pre>path: "/spec/storageClassName"</pre>	
Contraction of the second s	value: "ontap-nas-eco"	

The resulting config map object should look like this (CLI):

[root@localhos	st ~]# kubectl describe cm/change-ontap-sc -n openshift-adp
Name:	change-ontap-sc
Namespace:	openshift-adp
Labels:	<none></none>
Annotations:	<none></none>
Data	
====	
change-ontap-s	sc.yaml:
version: v1	
resourceModifi	ierRules:
- conditions:	
groupResc	ource: persistentvolumeclaims
resource	NameRegex: "data-postgresql*"
namespace	25:
- postgre	esql
patches:	
- operation:	: replace
path: "/sp	pec/storageClassName"
value: "or	ntap-nas-eco"
BinaryData	
====	
Events: <none< td=""><td>2></td></none<>	2>
[root@localhos	st ~]#

This config map will apply the resource modifier rule when the restore is created. A patch will be applied to replace the storage class name to ontap-nas-eco for all persistent volume claims starting with rhel.

Step 2

To restore the VM use the following command from the Velero CLI:

```
#velero restore create restore1 --from-backup backup1 --resource
-modifier-configmap change-storage-class-config -n openshift-adp
```

The app is restored in the same namespace with the persistent volume claims created using the storage class ontap-nas-eco.

[root@localhost	t~]# o	c get po	ds -n postgre	sql					
NAME	READY	STATUS	RESTARTS	AGE					
postgresql-0	1/1	Runnin	g 0	11m					
[root@localhost	t ~]# o	c get pv	c -n postgres	1l					
NAME	S	TATUS	VOLUME			CAPACITY	ACCESS MODES	STORAGECLASS	AGE
data-postgresq]	L-0 B	ound	pvc-33526ea4-	37c2-4180-a9f6-fb47a	aea3b4e2	8Gi	RWO	ontap-nas-eco	11m
[root@localhost	t ~]# 📕								

Deleting backups and restores in using Velero

This section outlines how to delete backups and restores of Apps in OpenShift container platform using Velero.

List all backups

You can list all Backup CRs by using the OC CLI tool or the Velero CLI tool. Download the Velero CLI as given in the instructions in the Velero documentation.

[root@localhost ~]# oc get	backups -n c	penshift	-adp					
NAME	AGE							
backup-postgresql-ontaps3	23h							
backup2	26s							
schedule1-20240717070005	6h42m							
[root@localhost ~]# velero	get backups	-n opensk	hift-adp					
NAME	STATUS	ERRORS	WARNINGS	CREATED		EXPIRES	STORAGE LOCATION	SELECTOR
backup-postgresql-ontaps3	Completed	0	0	2024-07-16 10:01:08 -04	400 EDT	29d	velero-container-backup-ontap-1	<none></none>
backup2	Completed	0	0	2024-07-17 09:42:32 -04	100 EDT	29d	velero-container-backup-ontap-1	<none></none>
schedule1-20240717070005	Completed	0	0	2024-07-17 03:00:05 -04	400 EDT	29d	velero-container-backup-ontap-1	<none></none>
[root@localhost ~]#								

Deleting a backup

You can delete a Backup CR without deleting the Object Storage data by using the OC CLI tool. The backup will be removed from the CLI/Console output. However, since the corresponding backup is not removed from the object storage, it will re-appear in the CLI/console output.

[root@localhost ~]# oc del@	ete backup backup2 -n openshift-adp
backup.velero.io "backup2"	deleted
[root@localhost ~]# oc get	backups -n openshift-adp
NAME	AGE
backup-postgresql-ontaps3	23h
schedule1-20240717070005	6h49m
<pre>[root@localhost ~]# oc get</pre>	backups -n openshift-adp
NAME	AGE
backup-postgresql-ontaps3	23h
backup2	24s
schedule1-20240717070005	6h50m
[root@localhost ~]# 🛓	

If you want to delete the Backup CR AND the associated object storage data, you can do so by using the Velero CLI tool.

[root@localhost ~]# velero	get backups	-n opensh	ift-adp				
NAME	STATUS	ERRORS	WARNINGS	CREATED	EXPIRES	STORAGE LOCATION	SELECTO
backup-postgresql-ontaps3	Completed	0	0	2024-07-16 10:01:08 -0400 EDT	29d	velero-container-backup-ontap-1	<none></none>
backup2	Completed	0	0	2024-07-17 09:42:32 -0400 EDT	29d	velero-container-backup-ontap-1	<none></none>
schedule1-20240717070005	Completed	0	0	2024-07-17 03:00:05 -0400 EDT	29d	velero-container-backup-ontap-1	<none></none>
[root@localhost ~]# velero	delete backu	p backup2	-n openshi	ft-adp			
Are you sure you want to co	ontinue (Y/N)	? Y					
Request to delete backup "b	backup2" subm	itted suc	cessfully.				
The backup will be fully de	eleted after	all assoc	iated data	(disk snapshots, backup files, r	estores) a	re removed.	
[root@localhost ~]# velero	get backups	-n opensh	ift-adp				
NAME	STATUS	ERRORS	WARNINGS	CREATED	EXPIRES	STORAGE LOCATION	SELECTO
backup-postgresql-ontaps3	Completed	0	0	2024-07-16 10:01:08 -0400 EDT	29d	velero-container-backup-ontap-1	<none></none>
schedule1-20240717070005	Completed	0	0	2024-07-17 03:00:05 -0400 EDT	29d	velero-container-backup-ontap-1	<none></none>
[root@localhost ~]#							

Deleting the Restore

You can delete the Restore CR Object by using either the OC CLI or the Velero CLI

[root@loca	lhost ~]# velero get restore	e -n openshif	t-adp								
NAME	BACKUP	STATUS	STARTED	COMPLETED	ERRORS	WARNINGS	CREATED		SELECTOR		
restore	backup-postgresql-ontaps3	Completed	2024-07-16 14:59:22 -0400 EDT	2024-07-16 14:59:45 -0400 EDT		10	2024-07-16 14:59:22	-0400 EDT	<none></none>		
restore1	backup-postgresql-ontaps3	Completed	2024-07-16 16:36:37 -0400 EDT	2024-07-16 16:36:59 -0400 EDT			2024-07-16 16:36:37	-0400 EDT	<none></none>		
[root@localhost ~]# velero restore delete restore1 -n openshift-adp											
Are you sure you want to continue (Y/N)? Y											
Request to delete restore "restore1" submitted successfully.											
The restore will be fully deleted after all associated data (restore files in object storage) are removed.											
[root@localhost ~]# velero get restore -n openshift-adp											
NAME	BACKUP	STATUS	STARTED	COMPLETED	ERRORS	WARNINGS	CREATED		SELECTOR		
restore	backup-postgresql-ontaps3	Completed	2024-07-16 14:59:22 -0400 EDT	2024-07-16 14:59:45 -0400 EDT	0	10	2024-07-16 14:59:22	-0400 EDT	<none></none>		
[root@loca	lhost ~]#										
root@localhost ~]# oc delete restore restore -n openshift-adp											
restore.ve	lero.io "restore" deleted										
[root@localhost ~]# oc get restore -n openshift-adp											
No resources found in openshift-adp namespace.											
[root@localhost ~]# velero get restore -n openshift-adp											
[root@loca	root@localhost ~]#										

Copyright information

Copyright © 2024 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.