Data Protection of Container Apps Using Third Party Tools

NetApp Solutions

NetApp
July 24, 2024
# Table of Contents

Data protection for Container Apps in OpenShift Container Platform using OpenShift API for Data Protection (OADP) ................................................................. 1

Data protection for Container Apps in OpenShift Container Platform using OpenShift API for Data Protection (OADP) ................................................................. 2

Installation of OpenShift API for Data Protection (OADP) Operator ................................................................. 4

Creating on-demand backup for Apps in OpenShift Container Platform ................................................................. 14

Restore an App from a backup .......................................................................................................................... 17

Deleting backups and restores in using Velero ............................................................................................... 25
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.

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.

**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.
OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.

Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.

OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.

- Installing OADP for application backup and restore
- Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM
- Frequently Asked Questions

Installed Operators

Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the Understanding Operators documentation for Operator and ClusterServiceVersion using the Operator SDK.
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.
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.
Click on Create DataProtectionApplication. In the form view, provide a name for the DataProtection Application or use the default name.

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**
Sample yaml file for configuring Velero with StorageGrid S3 as the backupLocation
spec:
  backupLocations:
    
  - velero:
    
      config:
        
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'True'

      credential:
        
          key: cloud
          name: sg-s3-credentials
          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
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.

```yaml
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```
Ensure that the DataProtectionApplication is created and is in condition: Reconciled.

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

```yaml
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.

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.

---

### 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
class: 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.

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

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.

```yaml
apiVersion: velero.io/v1
kind: Restore
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.
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pods -n postgresql
NAME        READY STATUS              RESTARTS AGE
postgresql-0 0/1  ContainerCreating 0      16s
[root@localhost ~]# oc get pods -n postgresql
NAME        READY STATUS              RESTARTS AGE
postgresql-0 0/1  Running             0      22s
[root@localhost ~]# oc get pods -n postgresql
NAME        READY STATUS              RESTARTS AGE
postgresql-0 0/1  Running             0      29s
[root@localhost ~]# oc get pods -n postgresql
NAME        READY STATUS              RESTARTS AGE
postgresql-0 1/1  Running             0      37s
[root@localhost ~]#
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`.

```yaml
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@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pods -n postgresql-restored
NAME       READY   STATUS   RESTARTS AGE
postgresql-0 0/1     Running 0 19s
[root@localhost ~]# oc get pods -n postgresql-restored
NAME       READY   STATUS   RESTARTS AGE
postgresql-0 0/1     Running 0 22s
[root@localhost ~]# oc get pods -n postgresql-restored
NAME       READY   STATUS   RESTARTS AGE
postgresql-0 1/1     Running 0 36s
[root@localhost ~]#
```
Restore to a different storage class

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.

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)
version: v1
resourceModifierRules:
- conditions:
  groupResource: persistentvolumeclaims
  resourceNameRegex: "data-postgresql*"
  namespaces:
  - postgresql
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"
The resulting config map object should look like this (CLI):

```
version: v1
resourceModifierRules:
  - conditions:
      resourceNameRegex: "data-postgresql"
      namespaces: ["postgresql"],
      patches: [{
        operation: "replace",
        path: ["/spec/storageClassName"],
        value: "ontap-nas-eco"
      }]
```
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.
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.

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.

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

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