



# **NetApp Astra Control Center Overview**

NetApp Solutions

NetApp  
September 05, 2023

This PDF was generated from [https://docs.netapp.com/us-en/netapp-solutions/containers/tanzu\\_with\\_netapp/vtwn\\_astra\\_register.html](https://docs.netapp.com/us-en/netapp-solutions/containers/tanzu_with_netapp/vtwn_astra_register.html) on September 05, 2023. Always check docs.netapp.com for the latest.

# Table of Contents

- NetApp Astra Control overview ..... 1
  - Astra Control Center automation ..... 2
  - Astra Control Center installation prerequisites ..... 2
  - Install Astra Control Center ..... 2
  - Register your VMware Tanzu Kubernetes Clusters with the Astra Control Center ..... 8
  - Choose the applications to protect ..... 11
  - Protect your applications ..... 13

# NetApp Astra Control overview

NetApp Astra Control Center offers a rich set of storage and application-aware data management services for stateful Kubernetes workloads deployed in an on-premises environment and powered by NetApp data protection technology.



NetApp Astra Control Center can be installed on a VMware Tanzu cluster that has the Astra Trident storage orchestrator deployed and configured with storage classes and storage backends to NetApp ONTAP storage systems.

For more information on Astra Trident, see [this document here](#).

In a cloud-connected environment, Astra Control Center uses Cloud Insights to provide advanced monitoring and telemetry. In the absence of a Cloud Insights connection, limited monitoring and telemetry (seven days worth of metrics) is available and exported to Kubernetes native monitoring tools (Prometheus and Grafana) through open metrics endpoints.

Astra Control Center is fully integrated into the NetApp AutoSupport and Active IQ ecosystem to provide support for users, provide assistance with troubleshooting, and display usage statistics.

In addition to the paid version of Astra Control Center, a 90-day evaluation license is also available. The evaluation version is supported through email and the community Slack channel. Customers have access to these resources, other knowledge-base articles, and documentation available from the in-product support dashboard.

To understand more about the Astra portfolio, visit the [Astra website](#).

# Astra Control Center automation

Astra Control Center has a fully functional REST API for programmatic access. Users can use any programming language or utility to interact with Astra Control REST API endpoints. To learn more about this API, see the documentation [here](#).

If you are looking for a ready-made software development toolkit for interacting with Astra Control REST APIs, NetApp provides a toolkit with the Astra Control Python SDK that you can download [here](#).

If programming is not appropriate for your situation and you would like to use a configuration management tool, you can clone and run the Ansible playbooks that NetApp publishes [here](#).

## Astra Control Center installation prerequisites

Astra Control Center installation requires the following prerequisites:

- One or more Tanzu Kubernetes clusters, managed either by a management cluster or TKGS or TKGI. TKG workload clusters 1.4+ and TKGI user clusters 1.12.2+ are supported.
- Astra Trident must already be installed and configured on each of the Tanzu Kubernetes clusters.
- One or more NetApp ONTAP storage systems running ONTAP 9.5 or greater.



It's a best practice for each Tanzu Kubernetes install at a site to have a dedicated SVM for persistent storage. Multi-site deployments require additional storage systems.

- A Trident storage backend must be configured on each Tanzu Kubernetes cluster with an SVM backed by an ONTAP cluster.
- A default StorageClass configured on each Tanzu Kubernetes cluster with Astra Trident as the storage provisioner.
- A load balancer must be installed and configured on each Tanzu Kubernetes cluster for load balancing and exposing Astra Control Center if you are using ingressType `AccTraefik`.
- An ingress controller must be installed and configured on each Tanzu Kubernetes cluster for exposing Astra Control Center if you are using ingressType `Generic`.
- A private image registry must be configured to host the NetApp Astra Control Center images.
- You must have Cluster Admin access to the Tanzu Kubernetes cluster where Astra Control Center is being installed.
- You must have Admin access to NetApp ONTAP clusters.
- A RHEL or Ubuntu admin workstation.

## Install Astra Control Center

This solution describes an automated procedure for installing Astra Control Center using Ansible playbooks. If you are looking for a manual procedure to install Astra Control Center, follow the detailed installation and operations guide [here](#).

1. To use the Ansible playbooks that deploy Astra Control Center, you must have an Ubuntu/RHEL machine with Ansible installed. Follow the procedures [here](#) for Ubuntu and RHEL.
2. Clone the GitHub repository that hosts the Ansible content.

```
git clone https://github.com/NetApp-
Automation/na_astra_control_suite.git
```

3. Log into the NetApp Support Site and download the latest version of NetApp Astra Control Center. To do so requires a license attached to your NetApp account. After you download the tarball, transfer it to the workstation.



To get started with a trial license for Astra Control, visit the [Astra registration site](#).

4. Create or obtain the kubeconfig file with admin access to the user or workload Tanzu Kubernetes cluster on which Astra Control Center is to be installed.
5. Change the directory to `na_astra_control_suite`.

```
cd na_astra_control_suite
```

6. Edit the `vars/vars.yml` file and fill the variables with the required information.

```
#Define whether or not to push the Astra Control Center images to your
private registry [Allowed values: yes, no]
push_images: yes

#The directory hosting the Astra Control Center installer
installer_directory: /home/admin/

#Specify the ingress type. Allowed values - "AccTraefik" or "Generic"
#"AccTraefik" if you want the installer to create a LoadBalancer type
service to access ACC, requires MetalLB or similar.
#"Generic" if you want to create or configure ingress controller
yourself, installer just creates a ClusterIP service for traefik.
ingress_type: "AccTraefik"

#Name of the Astra Control Center installer (Do not include the
extension, just the name)
astra_tar_ball_name: astra-control-center-22.04.0

#The complete path to the kubeconfig file of the kubernetes/openshift
cluster Astra Control Center needs to be installed to.
hosting_k8s_cluster_kubeconfig_path: /home/admin/cluster-kubeconfig.yml

#Namespace in which Astra Control Center is to be installed
astra_namespace: netapp-astra-cc

#Astra Control Center Resources Scaler. Leave it blank if you want to
accept the Default setting.
```

```

astra_resources_scaler: Default

#Storageclass to be used for Astra Control Center PVCs, it must be
created before running the playbook [Leave it blank if you want the PVCs
to use default storageclass]
astra_trident_storageclass: basic

#Reclaim Policy for Astra Control Center Persistent Volumes [Allowed
values: Retain, Delete]
storageclass_reclaim_policy: Retain

#Private Registry Details
astra_registry_name: "docker.io"

#Whether the private registry requires credentials [Allowed values: yes,
no]
require_reg_creds: yes

#If require_reg_creds is yes, then define the container image registry
credentials
#Usually, the registry namespace and usernames are same for individual
users
astra_registry_namespace: "registry-user"
astra_registry_username: "registry-user"
astra_registry_password: "password"

#Kuberenets/OpenShift secret name for Astra Control Center
#This name will be assigned to the K8s secret created by the playbook
astra_registry_secret_name: "astra-registry-credentials"

#Astra Control Center FQDN
acc_fqdn_address: astra-control-center.cie.netapp.com

#Name of the Astra Control Center instance
acc_account_name: ACC Account Name

#Administrator details for Astra Control Center
admin_email_address: admin@example.com
admin_first_name: Admin
admin_last_name: Admin

```

7. Run the playbook to deploy Astra Control Center. The playbook requires root privileges for certain configurations.

Run the following command to run the playbook if the user running the playbook is root or has passwordless sudo configured.

```
ansible-playbook install_acc_playbook.yml
```

If the user has password-based sudo access configured, then run the following command to run the playbook and then enter the sudo password.

```
ansible-playbook install_acc_playbook.yml -K
```

## Post Install Steps

1. It might take several minutes for the installation to complete. Verify that all the pods and services in the `netapp-astra-cc` namespace are up and running.

```
[netapp-user@rhel7 ~]$ kubectl get all -n netapp-astra-cc
```

2. Check the `acc-operator-controller-manager` logs to ensure that the installation is completed.

```
[netapp-user@rhel7 ~]$ kubectl logs deploy/acc-operator-controller-  
manager -n netapp-acc-operator -c manager -f
```



The following message indicates the successful installation of Astra Control Center.

```
{"level":"info","ts":1624054318.029971,"logger":"controllers.AstraContro  
lCenter","msg":"Successfully Reconciled AstraControlCenter in  
[seconds]s","AstraControlCenter":"netapp-astra-  
cc/astra","ae.Version":"[22.04.0]"}
```

3. The username for logging into Astra Control Center is the email address of the administrator provided in the CRD file and the password is a string `ACC-` appended to the Astra Control Center UUID. Run the following command:

```
[netapp-user@rhel7 ~]$ oc get astracontrolcenters -n netapp-astra-cc  
NAME      UUID  
astra     345c55a5-bf2e-21f0-84b8-b6f2bce5e95f
```



In this example, the password is `ACC-345c55a5-bf2e-21f0-84b8-b6f2bce5e95f`.

4. Get the traefik service load balancer IP if the `ingressType` is `AccTraefik`.

```
[netapp-user@rhel7 ~]$ oc get svc -n netapp-astra-cc | egrep  
'EXTERNAL|traefik'
```

NAME	EXTERNAL-IP	PORT(S)	TYPE	CLUSTER-IP
traefik	10.61.186.181	80:30343/TCP, 443:30060/TCP	LoadBalancer	172.30.99.142
AGE				
16m				

5. Add an entry in the DNS server pointing the FQDN provided in the Astra Control Center CRD file to the EXTERNAL-IP of the traefik service.



New Host

Name (uses parent domain name if blank):  
astra-control-center

Fully qualified domain name (FQDN):  
astra-control-center.cie.netapp.com.

IP address:  
10.61.186.181

☒ Create associated pointer (PTR) record

☐ Allow any authenticated user to update DNS records with the same owner name

Add Host Cancel

6. Log into the Astra Control Center GUI by browsing its FQDN.





7. When you log into Astra Control Center GUI for the first time using the admin email address provided in CRD, you need to change the password.



8. If you wish to add a user to Astra Control Center, navigate to Account > Users, click Add, enter the details of the user, and click Add.

**Add user**

**USER DETAILS**

First name: Nikhil

Last name: Kulkarni

Email address: tme\_nik@netapp.com

**PASSWORD**

Temporary password: \*\*\*\*\*

Confirm temporary password: \*\*\*\*\*

Passwords must contain:

- At least 8 characters
- No more than 64 characters
- At least one lowercase letter
- At least one uppercase letter
- At least one number
- At least one special character

**USER ROLE**

Role: Owner

Cancel Add

**ADD NEW USER**

Add new user

Add a new user to your Astra Control Center account. New users will be prompted to update their password the first time they log in to Astra Control Center. They will also inherit access to account-wide credentials according to their role. Read more in [users](#).

9. Astra Control Center requires a license for all of its functionalities to work. To add a license, navigate to Account > License, click Add License, and upload the license file.

**Account**

Users Credentials Notifications **License** Connections

**ASTRA CONTROL CENTER LICENSE**

To get started with Astra Control Center, select Add license to manually upload the file.

**ADD LICENSE**

Select and add a license file.

License file: EvalNLF-AstraControlCenter-480Cores(vCPU)-100000002-ACC60f19...

Cancel Add

Add license



If you encounter issues with the install or configuration of NetApp Astra Control Center, the knowledge base of known issues is available [here](#).

Next: [Register your Tanzu Kubernetes clusters.](#)

## Register your VMware Tanzu Kubernetes Clusters with the Astra Control Center

To enable the Astra Control Center to manage your workloads, you must first register your Tanzu Kubernetes clusters.

## Register VMware Tanzu Kubernetes clusters

1. The first step is to add the Tanzu Kubernetes clusters to the Astra Control Center and manage them. Go to Clusters and click Add a Cluster, upload the kubeconfig file for the Tanzu Kubernetes cluster, and click Select Storage.

 **Add Kubernetes cluster**

STEP 1/3: CREDENTIALS

×

CREDENTIALS

Provide Astra Control access to your Kubernetes and OpenShift clusters by entering a kubeconfig credential.

Follow [instructions](#) on how to create a dedicated admin-role kubeconfig.

[Upload file](#) [Paste from clipboard](#)

Kubeconfig YAML file  
tkgi-kubeconfig.txt

↑ ×

Credential name  
tkgi-acc

 **ADDING CLUSTERS**

Adding a cluster allows Astra Control to install its storage services, and enable data management operations on your containerized applications.

For more details on required versions or cloud specific setup refer to the documentation.

Read more in [Adding clusters](#).

Cancel

Next →

2. Astra Control Center detects the eligible storage classes. Now select the way that storageclass provisions volumes using Trident backed by an SVM on NetApp ONTAP and click Review. In the next pane, verify the details and click Add Cluster.
3. When the cluster is added, it moves to the Discovering status while Astra Control Center inspects it and installs the necessary agents. The cluster status changes to `Healthy` after it is successfully registered.

 **Clusters**

Actions ▾

+ Add Kubernetes cluster

⌵

 Search

1-1 of 1 entries < >

<input type="checkbox"/>	Name ↓	State	Type	Version	Actions
<input type="checkbox"/>	<a href="#">tkgi-acc</a>	✓ Healthy	 Kubernetes	v1.22.6+vmware.1	<div>⋮</div>



All Tanzu Kubernetes clusters to be managed by Astra Control Center should have access to the image registry that was used for its installation as the agents installed on the managed clusters pull the images from that registry.

4. Import ONTAP clusters as storage resources to be managed as backends by Astra Control Center. When Tanzu Kubernetes clusters are added to Astra and a storageclass is configured, it automatically discovers and inspects the ONTAP cluster backing the storageclass but does not import it into the Astra Control Center to be managed.

**Backends**

+ Add

Search

1

1-1 of 1 entries

Name ↓	State	Capacity	Throughput	Type	Cluster	Cloud	Actions
172.21.224.201(trident)	Discovered	Not available yet	Not available yet	ONTAP	Not applicable	Not applicable	

- To import the ONTAP clusters, navigate to Backends, click the dropdown, and select Manage next to the ONTAP cluster to be managed. Enter the ONTAP cluster credentials, click Review Information, and then click Import Storage Backend.

**Manage ONTAP storage backend**

STEP 1/2: CREDENTIALS

×

CREDENTIALS

Enter cluster administrator credentials for the ONTAP storage backend you want to manage.

Cluster management IP address

172.21.224.201

User name

admin

Password

.....

**MANAGING STORAGE BACKENDS**

Storage backends provide storage to your Kubernetes applications.

Managing storage clusters in Astra Control as a storage backend will allow you to get linkages between PVs and the storage backend. You will also see capacity and health details of the storage backend, including performance metrics if Astra Control is connected to Cloud Insights.

Read more in [Storage type](#) .



ONTAP

Cancel

Next →

- After the backends are added, the status changes to Available. These backends now have the information about the persistent volumes in the Tanzu Kubernetes cluster and the corresponding volumes on the ONTAP system.

## Backends

<div><div><div><div></div></div><div>+ Add</div></div><div><div></div><div>Search</div></div><div><div>★</div><div>Q</div></div></div>							
							1–1 of 1 entries
Name ↓	State	Capacity	Throughput	Type	Cluster	Cloud	Actions
<a href="#">K8s-Ontap</a>	 Available	Not available yet	Not available yet	ONTAP 9.9.1	Not applicable	Not applicable	

- For backup and restore across Tanzu Kubernetes clusters using Astra Control Center, you must provision an object storage bucket that supports the S3 protocol. Currently supported options are ONTAP S3, StorageGRID, AWS S3, and Microsoft Azure Blob storage. For the purpose of this installation, we are going to configure an AWS S3 bucket. Go to Buckets, click Add bucket, and select Generic S3. Enter the details about the S3 bucket and credentials to access it, click the checkbox Make this Bucket the Default Bucket for the Cloud, and then click Add.

Add bucket

×

Enter the access details of your existing object store bucket to allow Astra Control to store your application backups.

Type

 Generic S3

Existing bucket name

na-tanzu-astra/na-astra-tkgi

Description (optional)

S3 server name or IP address

s3.us-east-1.amazonaws.com

☒ Make this bucket the default bucket for this cloud

?

SELECT CREDENTIALS

Astra Control requires S3 access credentials with the roles necessary to facilitate Kubernetes application data management.

Add

[Use existing](#)

Select credential

AWS Creds

BUCKETS

Astra Control stores backups in your existing object store buckets. The first bucket added for a selected cloud will be designated as the default bucket for backup and clone operations.

Read more in [Storage buckets](#).

Cancel

Add ✓

Next: [Choose the Applications To Protect](#).

## Choose the applications to protect

After you have registered your Tanzu Kubernetes clusters, you can discover the applications that are deployed and manage them via the Astra Control Center.

## Manage applications

1. After the Tanzu Kubernetes clusters and ONTAP backends are registered with the Astra Control Center, the control center automatically starts discovering the applications in all the namespaces that are using the storageclass configured with the specified ONTAP backend.

The screenshot shows the 'Applications' page in the Astra Control Center. The left sidebar contains navigation links: Dashboard, Applications (selected), Clusters, Backends, Buckets, Account, Activity, and Support. The main content area is titled 'Applications' and features a table of discovered applications. The table has columns for Name, State, Cluster, Group, Discovered, and Actions. The applications listed are magento-5295b, magento, pks-system, netapp-acc-operator, and netapp-astra-cc, all in a 'Healthy' state. A dropdown menu is visible next to the 'magento' application, showing 'Manage' and 'Ignore' options.

Name	State	Cluster	Group	Discovered	Actions
magento-5295b	Healthy	tkgi-acc	magento-5295b	2022/05/11 09:52 UTC	⋮
magento	Healthy	tkgi-acc	magento	2022/05/09 18:20 UTC	⋮
pks-system	Healthy	tkgi-acc	pks-system	2022/05/04 06:40 UTC	⋮
netapp-acc-operator	Healthy	tkgi-acc	netapp-acc-operator	2022/05/04 06:40 UTC	⋮
netapp-astra-cc	Healthy	tkgi-acc	netapp-astra-cc	2022/05/04 06:40 UTC	⋮

2. Navigate to Apps > Discovered and click the dropdown menu next to the application you would like to manage using Astra. Then click Manage.

This screenshot is similar to the previous one, showing the 'Applications' page. The dropdown menu for the 'magento' application is open, highlighting the 'Manage' option. The 'Ignore' option is also visible. The table of applications remains the same.

Name	State	Cluster	Group	Discovered	Actions
magento-5295b	Healthy	tkgi-acc	magento-5295b	2022/05/11 09:52 UTC	⋮
magento	Healthy	tkgi-acc	magento	2022/05/09 18:20 UTC	⋮
pks-system	Healthy	tkgi-acc	pks-system	2022/05/04 06:40 UTC	⋮
netapp-acc-operator	Healthy	tkgi-acc	netapp-acc-operator	2022/05/04 06:40 UTC	⋮
netapp-astra-cc	Healthy	tkgi-acc	netapp-astra-cc	2022/05/04 06:40 UTC	⋮

3. The application enters the Available state and can be viewed under the Managed tab in the Apps section.

Applications

Actions ▾

+ Define

All clusters ▾

☰

Search

★ Managed

🔍

Discovered 

60

🚫

Ignored

🔄

1-1 of 1 entries

<

>

<input type="checkbox"/>	Name	State	Protection	Cluster	Group	Discovered ↓	Actions
<input type="checkbox"/>	<a href="#">magento</a>	<div>✓</div> Healthy	<div>⚠</div> Unprotected	<div>⚙️</div> <a href="#">tkgi-acc</a>	<div>■</div> magento	2022/05/09 18:20 UTC	<div>⋮</div>

Next: [Protect Your applications.](#)

# Protect your applications

After application workloads are managed by Astra Control Center, you can configure the protection settings for those workloads.

## Create an application snapshot

A snapshot of an application creates an ONTAP Snapshot copy and a copy of the application metadata that can be used to restore or clone the application to a specific point in time based on that Snapshot copy.

1. To take a snapshot of the application, navigate to the Apps > Managed tab and click the application you would like to make a Snapshot copy of. Click the dropdown menu next to the application name and click Snapshot.

 **magento**

APPLICATION STATUS

✓ Healthy

APPLICATION PROTECTION STATUS

⚠ Unprotected

Images

docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61  
docker.io/bitnami/magento:2.4.1-debian-10-r14  
docker.io/bitnami/mariadb:10.3.24-debian-10-r49

Protection schedule

Disabled

Group

■ magento

Cluster

 [tkgi-acc](#)

Actions ▾

Snapshot

Backup

Clone

Restore

Unmanage

2. Enter the snapshot details, click Next, and then click Snapshot. It takes about a minute to create the snapshot, and the status becomes Available after the snapshot is successfully created.

**Snapshot namespace application**

STEP 1/2: DETAILS

✕

SNAPSHOT DETAILS

Name

magento-snapshot-20220516212403

**CREATING APPLICATION SNAPSHOTS**

Astra Control can take a quick snapshot of your application configuration and persistent storage. Enter a snapshot name to get started.

Read more in [Protect apps](#)

Namespace application  
magento

Namespace  
magento

Cluster  
tkgi-acc

Cancel

Next →

## Create an application backup

A backup of an application captures the active state of the application and the configuration of it's resources, converts them into files, and stores them in a remote object storage bucket.

- For the backup and restore of managed applications in the Astra Control Center, you must configure superuser settings for the backing ONTAP systems as a prerequisite. To do so, enter the following commands.

```
ONTAP::> export-policy rule modify -vserver ocp-trident -policyname
default -ruleindex 1 -superuser sys
ONTAP::> export-policy rule modify -policyname default -ruleindex 1
-anon 65534 -vserver ocp-trident
```

- To create a backup of the managed application in the Astra Control Center, navigate to the Apps > Managed tab and click the application that you want to take a backup of. Click the dropdown menu next to the application name and click Backup.

**magento**

↻

Actions

Snapshot

Backup

Clone

Restore

Unmanage

**APPLICATION STATUS**

**APPLICATION PROTECTION STATUS**

Healthy

Unprotected

Images  
docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61  
docker.io/bitnami/magento:2.4.1-debian-10-r14  
docker.io/bitnami/mariadb:10.3.24-debian-10-r49

Protection schedule  
Disabled

Group  
magento

Cluster  
tkgi-acc

- Enter the backup details, select the object storage bucket to hold the backup files, click Next, and, after reviewing the details, click Backup. Depending on the size of the application and data, the backup can take several minutes, and the status of the backup becomes Available after the backup is completed



 **Back up namespace application**

STEP 1/2: DETAILS

✕

BACKUP DETAILS

Name

magento-backup-20220516212622

☐ Back up from an existing snapshot 

?

BACKUP DESTINATION

Bucket

na-tanzu-astro/na-astro-tkgi

Available

Default

 **CREATING APPLICATION BACKUPS**

Astra Control can take a backup of your application configuration and persistent storage. Persistent storage backups are transferred to your object store. Enter a backup name to get started.

Read more in [Application backups](#) .

 Namespace application  
magento


 Namespace  
magento

 Cluster  
tkgi-acc




Cancel

Next →

At the push of a button, you can restore an application to the originating namespace in the same cluster or to a remote cluster for application protection and disaster recovery purposes.

- 
🔄

Actions ▼

Application Status	Application Protection Status	Cluster
 APPLICATION STATUS <span style="color: green; font-weight: bold;">✔ Healthy</span>	 APPLICATION PROTECTION STATUS <span style="color: orange; font-weight: bold;">⚠ Unprotected</span>	<div style="display: flex; justify-content: space-between; align-items: center;"> <div>Images</div> <div>Protection schedule</div> <div>Group</div> </div> <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div>docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61</div> <div>Disabled</div> <div> magento</div> </div> <div style="display: flex; justify-content: space-between; align-items: flex-start; margin-top: 10px;"> <div>docker.io/bitnami/magento:2.4.1-debian-10-r14</div> <div></div> <div></div> </div> <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div>docker.io/bitnami/mariadb:10.3.24-debian-10-r49</div> <div></div> <div></div> </div>

- Snapshot
  - Backup
  - Clone
  - Restore
  - Unmanage

Restore namespace application

STEP 1/2: DETAILS

X

RESTORE DETAILS

Destination cluster

tkgi-acc

Destination namespace

magento

RESTORE SOURCE

Filter

Snapshots

Backups

Application backup	State	On-Schedule/On-Demand	Created ↑
<input type="radio"/> <div>magento-backup-20220516212730</div>	<div>Healthy</div>	<div>On-Demand</div>	<div>2022/05/16 21:27 UTC</div>

Cancel

Next →

RESTORING APPLICATIONS

Astra Control can restore your application configuration and persistent storage. Select a source snapshot or backup for the restored application.

- Namespace application magento
- Namespace magento
- Cluster tkgi-acc

- On the review pane, enter `restore` and click Restore after you have reviewed the details.

Restore namespace application

STEP 2/2: SUMMARY

X

REVIEW RESTORE INFORMATION

⚠

All existing resources associated with this namespace application will be deleted and replaced with the source backup "magento-backup-20220516212730" taken on 2022/05/16 21:27 UTC. Persistent volumes will be deleted and recreated. External resources with dependencies on this namespace application might be impacted.

We recommend taking a snapshot or a backup of your namespace application before proceeding.

BACKUP

magento-backup-20220516212730

ORIGINAL GROUP

magento

ORIGINAL CLUSTER

tkgi-acc

RESOURCE LABELS

Config Maps

app.kubernetes.io/name: elasticsearch +9

Deployments

RESTORE

magento

DESTINATION GROUP

magento

DESTINATION CLUSTER

tkgi-acc

RESOURCE LABELS

Config Maps

app.kubernetes.io/name: elasticsearch +9

Deployments

Are you sure you want to restore the namespace application "magento"?

Type `restore` below to confirm.

Confirm to restore

restore

← Back

Restore ✓

- The new application goes to the Restoring state while Astra Control Center restores the application on the selected cluster. After all the resources of the application are installed and detected by Astra, the application goes to the Available state.

16

Applications

Actions ▾

+ Define

All clusters ▾

⌵

Search

★ Managed

🔍

Discovered

60

🚫

Ignored

🔄

1-1 of 1 entries

<

>

<input type="checkbox"/>	Name	State	Protection	Cluster	Group	Discovered ↓	Actions
<input type="checkbox"/>	<a href="#">magento</a>	<div>✔ Healthy</div>	<div>⚠ Unprotected</div>	<div>⚙ <a href="#">tkgi-acc</a></div>	<div>📁 magento</div>	2022/05/09 18:20 UTC	<div>⋮</div>

## Cloning an application

You can clone an application to the originating cluster or to a remote cluster for dev/test or application protection and disaster recovery purposes. Cloning an application within the same cluster on the same storage backend uses NetApp FlexClone technology, which clones the PVCs instantly and saves storage space.

1. To clone an application, navigate to the Apps > Managed tab and click the app in question. Click the dropdown menu next to the application name and click Clone.

**magento**

**APPLICATION STATUS**

**Healthy**

**APPLICATION PROTECTION STATUS**

**Unprotected**

Images

docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61  
 docker.io/bitnami/magento:2.4.1-debian-10-r14  
 docker.io/bitnami/mariadb:10.3.24-debian-10-r49

Protection schedule

Disabled

Group

magento

Cluster

tkgi-acc

Actions ▾

Snapshot

Backup

Clone

Restore

Unmanage

2. Enter the details of the new namespace, select the cluster you want to clone it to, and choose if you want to clone it from an existing snapshot, from a backup, or from the current state of the application. Click Next and then click Clone on the review pane after you have reviewed the details.

**Clone namespace application**

STEP 1/2: DETAILS

✕

CLONE DETAILS

Clone namespace  
magento-bef7f

Destination cluster  
tkgi-acc

☐ Clone from an existing snapshot or backup

CLONING APPLICATIONS

Astra Control can create a clone of your application configuration and persistent storage. Persistent storage backups are transferred from your object store, so choosing a clone from an existing backup will complete the fastest. Enter a clone name to get started.

Not all applications may support cloning.

Read more in [Clone applications](#).

- Namespace application magento
- Namespace magento
- Cluster tkgi-acc

Cancel

Next →

- The new application goes to the Discovering state while Astra Control Center creates the application on the selected cluster. After all the resources of the application are installed and detected by Astra, the application goes to the Available state.

**Applications**

Actions ▾
+ Define

All clusters ▾

Search

★ Managed

🔍 Discovered 60

🚫 Ignored

1-2 of 2 entries

<input type="checkbox"/>	Name	State	Protection	Cluster	Group	Discovered ↓	Actions
<input type="checkbox"/>	<a href="#">magento-bef7f</a>	✓ Healthy	⚠️ Unprotected	tkgi-acc	magento-bef7f	2022/05/16 21:31 UTC	⋮
<input type="checkbox"/>	<a href="#">magento</a>	✓ Healthy	ℹ️ Partially protected	tkgi-acc	magento	2022/05/09 18:20 UTC	⋮

Next: Videos and demos: VMware Tanzu with NetApp.

## Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.