Get started

Project Astra

NetApp
November 17, 2020

This PDF was generated from https://docs.netapp.com/us-en/project-astra/get-started/get-started/intro.html on November 17, 2020. Always check docs.netapp.com for the latest.

Table of Contents

Get started

Intro to Astra

Astra is a Kubernetes application data lifecycle management service that simplifies operations for stateful applications. Easily back up Kubernetes apps, migrate data to a different cluster, and instantly create working application clones.

Features

The Astra beta program offers critical capabilities for Kubernetes application data lifecycle management:

- Create a protection policy for each of your apps
- Migrate applications and data from one Kubernetes cluster to another
- Easily clone an application from production to staging
- Create on-demand snapshots and backups
- Identify the health of your apps

Supported Kubernetes clusters

Astra can manage data for Google Kubernetes Engine (GKE) clusters.

On-prem Kubernetes clusters and clusters running in other cloud providers aren't supported at this time.

Learn more about cluster requirements.

How Astra works

Astra is a NetApp-managed cloud service that is always on and updated with the latest capabilities. It utilizes several components to enable application data lifecycle management. The following image shows the relationship between each component:

[diagram overview]

At a high level, Astra works like this:

- You set up your cloud provider.
- You add your first Kubernetes cluster to Astra. Astra then does the following:
  - Uses the cloud provider credentials that you provided to discover the cluster and the applications running on the cluster.

- Creates an object store in your cloud provider account, which is where backup copies are sent.
- Creates a new admin role on the cluster.
- Uses the role to install NetApp's Trident, to create storage classes, and to eventually create namespaces and support cloning of applications.

  Astra uses Trident to provision persistent volumes backed by NetApp Cloud Volumes Service for Google Cloud.

  Astra creates three storage classes that use Cloud Volumes Service for Google Cloud: netapp-cvs-extreme, netapp-cvs-premium (default), and netapp-cvs-standard.

- At this point, cluster configuration is complete. You can now choose which apps to manage and start creating snapshots, backups, and clones.

Note that Astra continually watches your clusters for state changes, so it's aware of any new apps that you add along the way.

Join the Astra Beta release

There's still time to sign up for the Astra Beta program. Click this link and fill out the form to request participation. A NetApp representative will contact you soon after.

Release notes

Known issues

Known issues identify problems that might prevent you from using this release of the product successfully.

Clone performance impacted by large persistent volumes

Clones of very large and consumed persistent volumes might be intermittently slow, dependent on cluster access to the object store. If the clone is hung and no data has been copied for more than 30 minutes, Astra terminates the clone action.

Clone fails after deleting a backup

If you delete a backup that's used for an active clone operation, the clone fails and the newly cloned app gets stuck in a provisioning state. Contact NetApp support to clear the stuck app from the application listing.

Known limitations

Known limitations identify platforms, devices, or functions that are not supported by this release of the product, or that do not interoperate correctly with it. Review these limitations carefully.

One GCP project and one service account are supported

The Astra Beta program supports one Google Cloud Platform project and one service account. You should not add more than one service account to Astra and you shouldn't rotate service account credentials.

If you want to change the GCP project that you're using with Astra, then we will need to set up a new account for you.

We intend to address this limitation in a future release.

Persistent volume limit

You can have up to 100 volumes per Google Cloud region. If you reach this limit, creation of new clones or volumes will fail. Contact support to increase the volume limit.

Unhealthy pods affect app management

If a managed app has pods in an unhealthy state, Astra can't create new backups and clones.

Trident isn't uninstalled from a cluster

When you unmanage a cluster from Astra, Trident isn't automatically uninstalled from the cluster. To uninstall Trident, you'll need to follow these steps in the Trident documentation.

Existing connections to a Postgres pod causes failures

When you perform operations on Postgres pods, you shouldn't connect directly within the pod to use the psql command. Astra requires psql access to freeze and thaw the databases. If there is a pre-existing connection, the snapshot, backup, or clone will fail.

Get started with Astra

Quick start for Astra

This page provides a high-level overview of the steps that you need to complete to get started with Project Astra. The links within each step take you to a page that provides more details.

[Number 1] Review Kubernetes cluster requirements

- Astra supports Kubernetes clusters that are managed by Google Kubernetes Engine (GKE).

- Clusters must be running a healthy state, with at least one online worker node, in a supported Google Cloud region, and using CVS-Performance (not CVS Beta).
- A cluster must be running Kubernetes version 1.17 or later.
- The image type for each worker node must be Ubuntu.

Learn more about the Kubernetes cluster requirements.

[Number 2] Set up Google Cloud

a. Set up a Google Cloud account and project.
b. Create a service account that has the required permissions:
    - Kubernetes Engine Admin
    - NetApp Cloud Volumes Admin
    - Storage Admin
    - Service Usage Viewer
    - Compute Network Viewer
c. Create a service account key.
d. Enable the required APIs.
e. Enable networking for Cloud Volumes Service for Google Cloud.

Learn more about Google Cloud requirements.

[Number 3] Sign up to NetApp Cloud Central

Sign up to NetApp Cloud Central so you can access Astra and NetApp's other cloud services. Learn more about signing up.

[Number 4] Accept your Beta invitation

After you've been accepted into the Astra Beta program, you'll receive an invitation to join an Astra account. Accept this invitation to join the account and log in to the Astra interface. Learn more about accepting your invitation.

[Number 5] Add your first cluster

After you log in, click **Add a Kubernetes Cluster** to start managing your first cluster with Astra. Learn more about adding your first cluster.

Requirements

Get started by verifying support for your Kubernetes clusters, apps, and web browser.

Supported Kubernetes clusters

- The Astra beta program supports Kubernetes clusters that are managed by Google Kubernetes Engine (GKE).

  On-prem Kubernetes clusters and clusters running in other cloud providers are not supported at this time.

- Clusters must be running in a healthy state, in one of the supported regions:
  - us-central1
  - us-east4
  - us-west2
  - europe-west3
  - europe-west2
  - australia-southeast1
  - Other regions will be added in the future.
- A cluster must be running Kubernetes version 1.17 or later.
- The cluster must have at least one online worker node.
- The image type for each worker node must be Ubuntu.
- The cluster must be using CVS-Performance (not CVS Beta).
- If the cluster is private, it must have the master authorized network set to allow the Astra IP addresses:
  - 18.232.241.74
  - 52.72.239.237
  - 3.210.60.146

Supported apps

Astra supports all applications running on your Kubernetes clusters.

NetApp has validated some apps to ensure the safety and consistency of the snapshots and backups.

Learn the difference between a Validated and a Standard app.

No matter which type of app that you use with Astra, you should always test the backup and restore workflow yourself to ensure that you can meet your disaster recovery requirements.

Supported web browsers

Astra supports recent versions of Firefox, Safari, and Chrome with a minimum resolution of 1280 x 720.

Set up Google Cloud

A few steps are required to prepare your Google Cloud project before you can manage Google Kubernetes Engine clusters with the Astra beta program.

Quick start for Google Cloud set up

Get started quickly by following these steps or scroll down to the remaining sections for full details.

[Number 1] Set up a Google Cloud account and project

You need a Google Cloud account and a project.

[Number 2] Create a service account that has the required permissions

Create a Google Cloud service account that has the following permissions:

- Kubernetes Engine Admin
- NetApp Cloud Volumes Admin
- Storage Admin
- Service Usage Viewer
- Compute Network Viewer

Read step-by-step instructions.

[Number 3] Create a service account key

Create a key for the service account and save the key file in a secure location. Follow step-by-step instructions.

[Number 4] Enable APIs in your Google Cloud project

Enable the following Google Cloud APIs:

- Google Kubernetes Engine
- Cloud Storage
- Cloud Storage JSON API
- Service Usage
- Cloud Resource Manager API
- NetApp Cloud Volumes Service
- Service Consumer Management API
- Service Networking API

- Service Management API
- Service Consumer Management API

Follow step-by-step instructions.

[Number 5] Enable private services access

Set up private services access for Cloud Volumes Service for Google Cloud. Follow step-by-step instructions.

The following image depicts each of these steps that you'll need to complete.

[A conceptual diagram that shows a Google Cloud project]

Create a service account

Astra uses a Google Cloud service account to facilitate Kubernetes application data management on your behalf.

Steps

1. Go to Google Cloud and create a service account by using the console, gcloud command, or another preferred method.
2. Grant the service account the following roles:
    - **Kubernetes Engine Admin** - Used to list clusters and create admin access to manage apps.
    - **NetApp Cloud Volumes Admin** - Used to manage persistent storage for apps.
    - **Storage Admin** - Used to manage buckets and objects for backups of apps.
    - **Service Usage Viewer** - Used to check if the required Cloud Volumes Service for Google Cloud APIs are enabled.
    - **Compute Network Viewer** - Used to check if the Kubernetes VPC is allowed to reach Cloud Volumes Service for Google Cloud.

If you'd like to use gcloud, you can follow steps from within the Astra user interface. Click **Account** > **Credentials** > **Add Credentials**, and then click **Instructions**.

If you'd like to use the Google Cloud console, the following video shows how to create the service account from the console.

▶ https://docs.netapp.com/us-en/project-astra/get-started/media/video-create-gcp-service-account.mp4

(video)

Create a service account key

Instead of providing a user name and password to Astra, you'll provide a service account key when you add your first cluster. Astra uses the service account key to establish the identity of the service account that you just set up.

The service account key is plaintext stored in the JavaScript Object Notation (JSON) format. It contains information about the GCP resources that you have permission to access.

You can only view or download the JSON file when you create the key. However, you can create a new key at any time.

Steps

1. Go to Google Cloud and create a service account key by using the console, gcloud command, or another preferred method.
2. When prompted, save the service account key file in a secure location.

The following video shows how to create the service account key from the Google Cloud console.

▶ https://docs.netapp.com/us-en/project-astra/get-started/media/video-create-gcp-service-account-

key.mp4 *(video)*

Enable APIs in your project

Your project needs permissions to access specific Google Cloud APIs. APIs are used to interact with Google Cloud resources, such as Google Kubernetes Engine (GKE) clusters and NetApp Cloud Volumes Service storage.

Step

1. Use the Google Cloud console or gcloud CLI to enable the following APIs:
    - Google Kubernetes Engine
    - Cloud Storage
    - Cloud Storage JSON API
    - Service Usage
    - Cloud Resource Manager API
    - NetApp Cloud Volumes Service
    - Service Consumer Management API
    - Service Networking API
    - Service Management API

      The last two APIs are required for Cloud Volumes Service for Google Cloud.

The following video shows how to enable the APIs from the Google Cloud console.

▶ https://docs.netapp.com/us-en/project-astra/get-started/media/video-enable-gcp-apis.mp4 *(video)*

If you'd rather use the gcloud CLI, you can use these commands after setting your project:

```
gcloud services enable container.googleapis.com
gcloud services enable storage-component.googleapis.com
gcloud services enable storage-api.googleapis.com
gcloud services enable serviceusage.googleapis.com
gcloud services enable cloudresourcemanager.googleapis.com
gcloud services enable cloudvolumesgcp-api.netapp.com
gcloud services enable serviceconsumermanagement.googleapis.com
gcloud services enable servicenetworking.googleapis.com
gcloud services enable servicemanagement.googleapis.com
```

Enable private services access

Astra uses Cloud Volumes Service for Google Cloud as the backend storage for your persistent volumes. Other than the APIs that you enabled in the previous step, the only other requirement is to enable

private services access to Cloud Volumes Service.

Step

1. Set up private services access from your project to create a high-throughput and low-latency data-path connection, as described in the Cloud Volumes Service for Google Cloud documentation.

Sign up to Cloud Central

The Astra beta program is integrated within NetApp Cloud Central's authentication service. Sign up to Cloud Central so you can access Astra and NetApp's other cloud services.

Steps

1. Open your web browser and go to NetApp Cloud Central.
2. In the top right, click **Sign up**.
3. Fill out the form and click **Sign up**.

   

   You'll need to provide the email address that you enter in this form to the person who adds you to Astra.

   [A screenshot of the Cloud Central sign up page where you need to enter your email address, password, name, company, and your phone number, which is optional.]

4. Wait for an email from NetApp Cloud Central.
5. Click the link in the email to verify your email address.

Result

You now have an active Cloud Central user login.

Accept your Beta invitation

After you've been accepted into the Astra Beta program, you'll receive an invitation to join a Astra account. Accept this invitation to gain access to the Astra interface.

Steps

1. Open the email invitation to join a Astra account.

   [A screenshot of an email that invites you to join a Astra account. It includes a Join Now button that you can click to accept the invitation.]

2. Confirm that the email address in the invitation matches the email address that you used to sign up to Cloud Central.

If they don't match, then contact the person who added you to the account and let them know the email address that's associated with your Cloud Central account.

3. Click **Join Now**.

   A prompt should load in your web browser.

   [A screenshot that shows the Accept Invitation dialog box that appears in a web browser after you click the Join Now button from the email invitation.]

4. Click **Accept Invitation**.

   If you are the first person to join the Astra organization, you will be prompted to provide your address and serial number. **Be sure to use a valid physical address.** Please note the account name must be between 5 and 19 characters long. If you are being added to an existing account, you should now see the Astra interface.

   [A screenshot that shoes the Astra Dashboard.]

Add your first cluster to Astra

After you log in to the Astra beta program, your first step is to add a Kubernetes cluster.

Steps

1. On the Dashboard, click **Add a Kubernetes Cluster**.

   Follow the prompts to add the cluster.

2. **Provider**: Provide the service account key file either by uploading the file or by pasting the contents from your clipboard.

   [screenshot compute select credentials]

   Astra uses the service account to discover the clusters running in Google Kubernetes Engine.

3. **Compute**: Select the cluster that you'd like to add and click **Configure storage**.

   Pay careful attention to the Eligible tab. If a warning appears, hover over the warning to determine if there's an issue with the cluster. For example, it might identify the cluster doesn't have a worker node.

4. **Storage**: Select the default storage class that you'd like to use with this cluster and click **Review information**.

   Each storage class utilizes Cloud Volumes Service for Google Cloud.

5. **Review & Approve**: Review the configuration details and click **Add compute**.

   [screenshot compute approve]

The following video shows how to add a cluster.

▶ https://docs.netapp.com/us-en/project-astra/get-started/media/video-manage-cluster.mp4 *(video)*

Result

Astra creates an object store for application backups, creates an admin account on the cluster, and sets the default storage class that you specified. This process takes up to 5 minutes.

What's next?

Now that you've logged in and added your first cluster to the Astra beta program, you're ready to start using Astra's application data management features.

- Start managing apps
- Protect apps
- Clone apps
- Invite and manage users
- Manage cloud provider credentials
- Manage notifications

Astra videos

Many of the pages on this doc site include videos that show you how to complete a task for Astra. If you're just interested in videos, we've made it easy for you by collecting all of the videos on this single page (kind of like a playlist).

Videos for setting up Google Cloud

The following videos show how to complete set up requirements in Google Cloud before you can discover Kubernetes clusters running in GCP.

Create a service account

Astra uses a Google Cloud service account to facilitate Kubernetes application data management on your behalf. The following video shows how to create the service account from the Google Cloud console.

▶ https://docs.netapp.com/us-en/project-astra/get-started/media/video-create-gcp-service-account.mp4

(video)

Create a service account key

Astra uses a service account key to establish the identity of the service account that you just set up. The following video shows how to create the service account key from the Google Cloud console.

▶ https://docs.netapp.com/us-en/project-astra/get-started/media/video-create-gcp-service-account-

key.mp4 *(video)*

Enable APIs

Your project needs permissions to access specific Google Cloud APIs. The following video shows how to enable the APIs from the Google Cloud console.

▶ https://docs.netapp.com/us-en/project-astra/get-started/media/video-enable-gcp-apis.mp4 *(video)*

Click here to view the full list of required APIs.

Videos for using Astra

The following videos show how to complete a few common tasks using Astra.

Add your first cluster to Astra

After you log in to Astra, your first step is to add a Kubernetes cluster.

▶ https://docs.netapp.com/us-en/project-astra/get-started/media/video-manage-cluster.mp4 *(video)*

Start managing an app

After you add a Kubernetes cluster to Astra, go to the Apps page to start managing the apps that run on the cluster.

▶ https://docs.netapp.com/us-en/project-astra/get-started/media/video-manage-app.mp4 *(video)*

Astra frequently asked questions for Beta

Overview

Welcome to the Astra Beta program!

Astra aims to simplify your application data lifecycle management operations for Kubernetes native applications. In the Beta, Astra support is limited to Kubernetes clusters running on Google Kubernetes Engine (GKE) on Google Compute Platform (GCP). Other cloud providers will be added in later phases of the project.

The following sections provide answers to some additional questions that you might come across as you use Astra. For any additional clarifications, please reach out to projectastra.feedback@netapp.com

Access to Astra

How can I access Astra?

Visit Astra at https://astra.netapp.io.

How can I get an invitation to the Beta?

Beta preview access is limited to a select few parties. Please register at https://cloud.netapp.com/project-astra-register.

I received an invitation to participate in the Beta. Where do I register my company?

Astra access is granted to your organization email address. This is the same email address that is registered with NetApp Cloud Central.

If you don't have a NetApp Cloud Central account yet, sign up using the **same** email in the invitation. You can create a NetApp Cloud Central account here: https://cloud.netapp.com.

I've added my colleagues to Astra, but they haven't received an email yet. What should I do?

Ask them to check their spam folder, or search their inbox for "invitation". You can also remove the user and attempt to re-add them. If neither of these work, please contact NetApp technical support with your organization name and the email addresses of people who haven't received the email invitation.

Registering Kubernetes Clusters

Can I add a private cluster to Astra?

Yes, you can add private clusters in Astra beta. To create a Google Kubernetes Engine (GKE) private cluster, follow the instructions in this knowledgebase article.

Private clusters must have the master authorized network set to allow the Astra IP addresses:

- 18.232.241.74
- 52.72.239.237
- 3.210.60.146

Can I use a custom network?

Yes, custom Virtual Private Cloud (VPC) networks are supported and Astra Beta will identify the right network peering and automate the required configuration.

Where can I find my service account credentials on GCP?

After you log in to the Google Cloud Console, your service account details will be in the **IAM and Admin** section. For more details, refer to how to set up Google Cloud for Astra.

How can I disable the service credentials I've registered with Astra?

When the Beta workflow testing is complete and you want to completely remove all credentials and objects from Astra, please contact NetApp Technical support and request to remove the Account. You

can also invalidate any credentials stored with Astra by deleting the service account from the Google Cloud Console.

I've set permissions on the service account credentials in my GCP account, but it still doesn't work. What should I do?

Contact NetApp Technical Support with a description of your problem and any error messages that you received.

I've changed my GCP service account roles. How do I update them in Astra?

Service account details are used when adding a GKE Kubernetes cluster to Astra. If the required roles and permissions are retained in the service account, you will not need to update anything in Astra.

If you rename or delete the service account, this will impact the application and cluster management features of Astra. You should contact projectastra.support@netapp.com to get help.

How many GCP service accounts can I register?

Different service accounts can be used when adding GKE clusters to Astra as long as they have the required roles and permissions. At a minimum, for each project, you need to provide one service account with the required roles and permissions.

How many Kubernetes clusters can I register?

You will need to register a minimum of two GKE Kubernetes clusters in order to exercise the Astra features. The maximum number of clusters for the Beta program is 100.

Do I need to install CSI drivers on my GKE cluster before adding it to Astra?

No. When your GKE cluster is added to Astra, the service will automatically install NetApp's Trident Container Storage Interface (CSI) driver on the Kubernetes cluster. This CSI driver is used to provision persistent volumes backed by NetApp Cloud Volumes Service for Google Cloud.

I have a GKE cluster that's running a different Kubernetes version than supported by Astra. Can I add that cluster to Astra?

The cluster discovery phase will not add a GKE cluster with an unsupported Kubernetes version. Astra provides information about supported Kubernetes version when it discovers a cluster running an unsupported Kubernetes version.

Can Astra validate the required GCP service account permissions?

Yes, Astra verifies that the required permissions are enabled before registering a GKE cluster, and will attempt to provide information about missing permissions.

How do I verify my GKE Kubernetes cluster is running supported Kubernetes version for Astra?

There are two ways you can verify the GKE Kubernetes cluster version:

1. Verify it from Google cloud console. Go to **Kubernetes Engine** > **Cluster** and select the relevant cluster. Check the Release Channel and Master Version.
2. Astra checks the GKE cluster version when the cluster is added. If Astra identifies an unsupported Kubernetes version, it provides more information in the Add compute user interface.

How do I know the worker nodes in the GKE Kubernetes cluster are running a supported image type?

The cluster discovery phase will not add a GKE cluster if the worker nodes are running an unsupported image type. If this happens, Astra will provide details on the supported image version (Ubuntu) in the Add compute user interface. Alternatively, you can verify the worker node image version from the Google Cloud Console.

How do I create a GKE cluster with a supported worker node image type?

When you create a GKE cluster or node pool, you can choose the operating system image that runs on each node. You can also upgrade an existing cluster to use a different node image type.

I would like to add different GKE clusters from different GCP projects. Is this supported in Astra?

No, this is not a supported configuration. Beta will only support a single GCP project.

How do I verify my GKE cluster was added successfully to Astra?

When you add the cluster, the user interface will show the status update and any error messages. When the cluster is added successfully, the status of the GKE cluster in the **Compute** section will be *Available*.

Alternatively, you can also verify if the Trident operator and CSI drivers deployed successfully under the namespace *trident* by running the kubectl commands:

```
kubectl get pods -n trident
```

or

```
kubectl get pods -|grep trident
```

I need to add worker nodes to my GKE cluster after adding to Astra. What should I do?

New worker nodes can be added to existing pools, or new pools can be created as long as they are the Ubuntu image type. These will be automatically discovered by Astra. If the new nodes are not visible in Astra, check if the new worker nodes are running the supported image type. You can also verify the health of the new worker nodes by using the `kubectl get nodes` command.

Can I unmanage my Kubernetes cluster from Astra?

Yes, you can remove one or more Kubernetes cluster from Astra at the same time. All managed applications from the unamanged cluster will be removed and Astra snapshots or backups taken of

applications on that cluster will be unavailable to restore.

Always remove a cluster from Astra before you delete it through GCP. Deleting a cluster from GCP while it's still being managed by Astra can cause problems for your Astra account.

What happens to my applications and data after removing the GKE cluster from Astra?

Removing a GKE cluster from Astra will not make any changes to the cluster's configuration (applications and persistent storage). Any Astra snapshots or backups taken of applications on that cluster will be unavailable to restore. Volume snapshot data stored within Cloud Volumes Service will not be removed. Persistent Storage backups created by Astra will remain within the Google Cloud object store, but they are unavailable for restore.

Always remove a cluster from Astra before you delete it through GCP. Deleting a cluster from GCP while it's still being managed by Astra can cause problems for your Astra account.

Will NetApp Trident be uninstalled when I remove a GKE cluster from Astra?

Trident will not be uninstalled from a cluster when you remove it from Astra.

Managing Applications

How many apps per namespace?

There is no limitation about number applications under a namespace. Astra will discover all application in the name space by application name.

I have deployed my applications using Helm and kubectl. My newly-deployed application is not showing up on the Discovered Apps list. What can I check to identify the problem?

When an application is successfully deployed, Astra will automatically discover the application and add it to the Discovered Apps list. When applications are not listed in **Discovered Apps**, check the status and health of the Kubernetes pod by running `kubectl get pod -A |grep [pod name]`. If the pods are healthy and running, check to see if the application is listed under **Ignored Apps**.

I've deployed my applications using Helm and kubectl. I don't see any of my application's PVCs bound to GCP CVS. What's wrong?

The NetApp Trident operator sets the default storage class to `netapp-cvs-premium` after it's successfully added to Astra. When an application's PVCs are not bound to Cloud Volumes Services for Google Cloud, there are a few steps that you can take:

- Run `kubectl get sc` and check to see if the default storage class is set to *netapp-cvs*.
- Check the yaml file or Helm chart that was used to deploy the application and see if a different

storage class is defined.

- Check to make sure that the worker node image type is Ubuntu and the NFS mount succeeded.

I have an existing cluster that has applications using GCP persistent disks. Can I register those applications with Astra?

Applications using GCP PVCs will be discovered and registered by Astra. And it's allowed to perform Astra data management operations. But snapshots and backups taken with Astra for those applications will not be application consistent.

How many applications can I simultaneously manage with Astra?

Multiple applications from different GKE cluster can be managed at the same time.

I moved my application to the Ignored list by mistake. Can I manage the applications that are on the Ignore list?

Yes, applications on the Ignored list can be registered successfully. Data management operations will function as usual after you start managing the application.

Can I register applications that are not MySQL, Jenkins, or PostgreSQL?

Yes, we can use data management services offered by Astra on any persistent volumes managed by Cloud Volumes Service for Google Cloud. However, application-level consistent snapshots, backup, migration, etc. will not be orchestrated through Astra.

Can Astra deploy an application?

Astra doesn't deploy an application. Applications must be deployed outside of Astra by using kubectl or Helm charts.

What storage classes can I use in my PVCs to support Astra data management operations?

As part of adding the GKE cluster to Astra, NetApp Trident will create three different storage classes for Cloud Volume Services in GCP. Astra data management operations are only supported on storage class *netapp-cvs-extreme*, *netapp-cvs-premium*, and *netapp-cvs-standard*. And you can choose either of these storage class as default when adding a Kubernetes cluster to Astra.

What happens to applications after I stop managing them from Astra?

Applications, data, and any existing backups or snapshots remain available. Data management operations will not be available for unmanaged applications or any backups or snapshots that belong to it. When the application is managed by Astra again, the existing snapshots and backups will be available for data management operations.

Data Management Operations

My application uses several PVs. Will Astra take snapshots and backups of all these PVCs?

Astra aims to simplify application data lifecycle management. Using Astra eliminates the need for individual volume-level data management operations. A snapshot operation on an application by Astra includes snapshot of all the PVs that are bound to the application's PVCs.

Can I create snapshot schedules and assign retention schedules?

Yes, you can use the Configure Protection Policy option to set a retention policy for each individual application.

What is the difference between snapshots and backups?

Snapshot refers to local snapshots, where data is stored as part of the provisioned volumes. Given that they are stored on the same provisioned volume, they are usually faster. Local snapshots are used to restore the application to an earlier point in time.

Backups are stored on object storage. They could be slower compared to the local snapshots. However, they can be accessed across regions in the cloud. Backups are used for migrating applications across regions in the cloud. Also, a user can choose to have longer retention period for backups.

Can I manage snapshots taken by Astra directly through the Cloud Volumes Service snapshot management interface or object storage?

Snapshots and backups taken through Astra can only be managed through Astra. Astra provides interfaces to create, view, and delete the snapshots and backups. If data objects associated with these snapshots are managed outside of the Astra interface, it can result in intermittent behavior.

Copyright Information

Copyright © 2020 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.