Concepts

Astra Control Center

NetApp
June 15, 2022

Table of Contents

Concepts

Learn about Astra Control

Astra Control is a Kubernetes application data lifecycle management solution that simplifies operations for stateful applications. Easily protect, back up, and migrate Kubernetes workloads, and instantly create working application clones.

Features

Astra Control offers critical capabilities for Kubernetes application data lifecycle management:

- Automatically manage persistent storage
- Create application-aware, on-demand snapshots and backups
- Automate policy-driven snapshot and backup operations
- Migrate applications and data from one Kubernetes cluster to another
- Easily clone an application from production to staging
- Visualize application health and protection status
- Use a user interface or an API to implement your backup and migration workflows

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

Deployment models

Astra Control is available in two deployment models:

- **Astra Control Service**: A NetApp-managed service that provides application-aware data management of Kubernetes clusters in Google Kubernetes Engine (GKE) and Azure Kubernetes Service (AKS).
- **Astra Control Center**: Self-managed software that provides application-aware data management of Kubernetes clusters running in your on-premises environment.

	Astra Control Service	Astra Control Center
How is it offered?	As a fully managed cloud service from NetApp	As software that you download, install, and manage
Where is it hosted?	On a public cloud of NetApp's choice	On your provided Kubernetes cluster
How is it updated?	Managed by NetApp	You manage any updates
What are the app data management capabilities?	Same capabilities on both platforms with exceptions to storage backend or to external services	Same capabilities on both platforms with exceptions to storage backend or to external services

	Astra Control Service	Astra Control Center
What is the storage backend support?	NetApp cloud service offerings	• NetApp ONTAP AFF and FAS systems • Astra Data Store as storage backend • Cloud Volumes ONTAP storage backend

Supported apps

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

- Learn the difference between a validated app and a standard app in Astra Control Service.
- Learn the difference between a validated app and a standard app in Astra Control Center.

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

How Astra Control Service works

Astra Control Service 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.

At a high level, Astra Control Service works like this:

- You get started with Astra Control Service by setting up your cloud provider and by registering for an Astra account.
  - For GKE clusters, Astra Control Service uses NetApp Cloud Volumes Service for Google Cloud or Google Persistent Disks as the storage backend for your persistent volumes.
  - For AKS clusters, Astra Control Service uses Azure NetApp Files or Azure Disk Storage as the storage backend for your persistent volumes.
- You add your first Kubernetes compute to Astra Control Service. Astra Control Service then does the following:
  - Creates an object store in your cloud provider account, which is where backup copies are stored.

    In Azure, Astra Control Service also creates a resource group, a storage account, and keys for the Blob container.

  - Creates a new admin role and Kubernetes service account on the cluster.
  - Uses that new admin role to install Astra Trident on the cluster and to create one or more storage classes.
  - If you use Azure NetApp Files or NetApp Cloud Volumes Service for Google Cloud as your storage backend, Astra Control Service uses Astra Trident to provision persistent volumes for your apps.
- At this point, you can add apps to your cluster. Persistent volumes will be provisioned on the new default storage class.
- You then use Astra Control Service to manage these apps, and start creating snapshots, backups, and clones.

  Astra Control Service continually watches your compute for state changes, so it's aware of any new apps

that you add along the way.

Astra Control's Free Plan enables you to manage up to 10 apps in your account. If you want to manage more than 10 apps, then you'll need to set up billing by upgrading from the Free Plan to the Premium Plan.

How Astra Control Center works

Astra Control Center runs locally in your own private cloud.

Astra Control Center supports OpenShift Kubernetes clusters with:

- Trident storage backends with ONTAP 9.5 and above
- Astra Data Store storage backends

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 (7-days of metrics) monitoring and telemetry is available in Astra Control Center and also exported to Kubernetes native monitoring tools (such as Prometheus and Grafana) through open metrics end points.

Astra Control Center is fully integrated into the AutoSupport and Active IQ ecosystem to provide users and NetApp Support with troubleshooting and usage information.

You can try Astra Control Center out using a 90-day evaluation license. The evaluation version is supported through email and community (Slack channel) options. Additionally, you have access to Knowledgebase articles and documentation from the in-product support dashboard.

To install and use Astra Control Center, you'll need to meet certain requirements.

At a high level, Astra Control Center works like this:

- You install Astra Control Center in your local environment. Learn more about how to install Astra Control Center.
- You complete some setup tasks such as these:
  - Set up licensing.
  - Add your first cluster.
  - Add storage backend that is discovered when you added the cluster.
  - Add an object store bucket that will store your app backups.

Learn more about how to set up Astra Control Center.

Astra Control Center does this:

- Discovers details about the managed Kubernetes clusters.
- Discovers your Astra Trident or Astra Data Store configuration on the clusters that you choose to manage and lets you monitor the storage backends.
- Discovers apps on those clusters and enables you to manage and protect the apps.

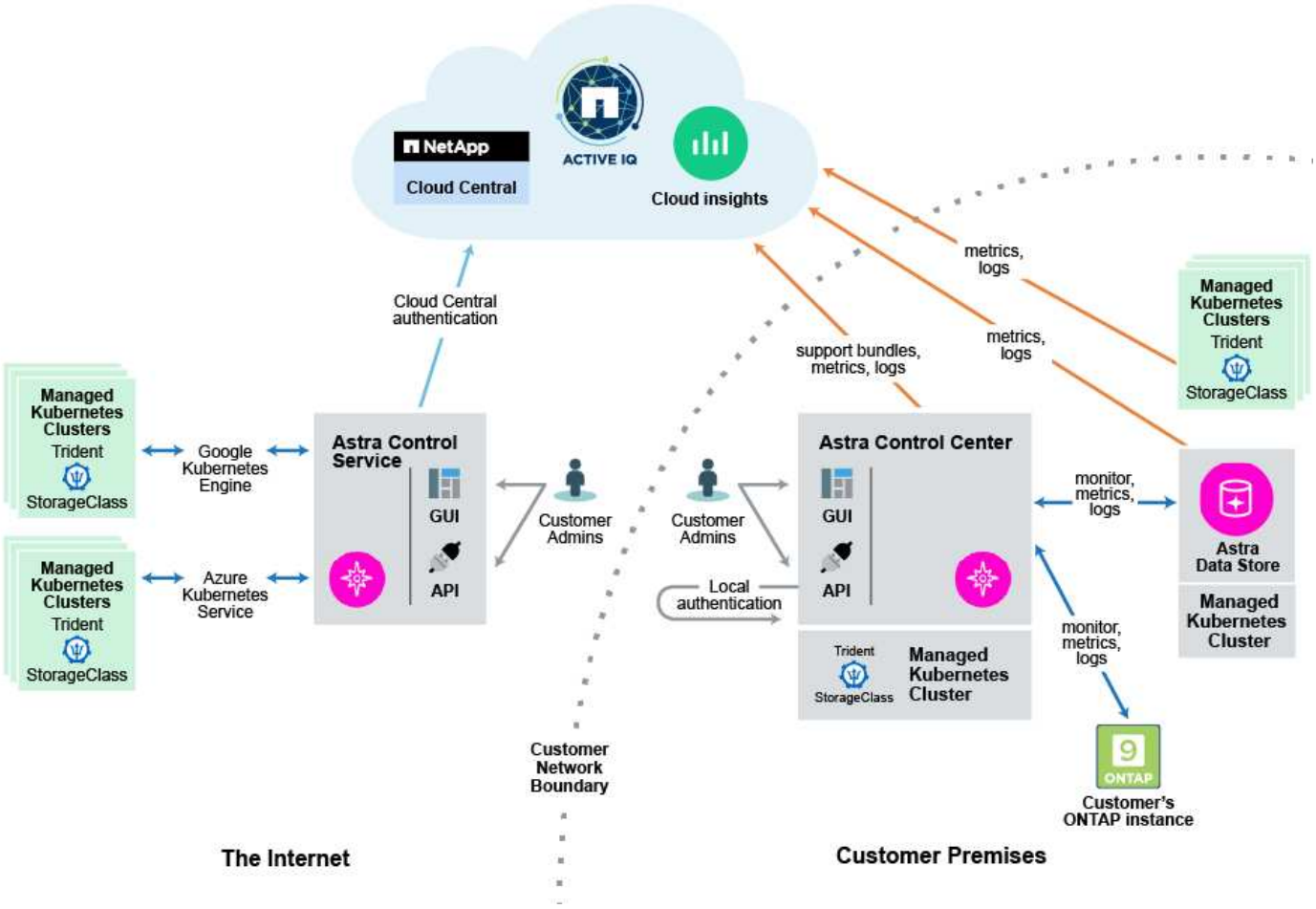
You can add apps to your cluster. Or, if you have some apps already in the cluster being managed, you can use Astra Control Center to discover and manage them. Then, use Astra Control Center to create snapshots, backups, and clones.

For more information

- Astra Control Service documentation
- Astra Control Center documentation
- Astra Data Store documentation
- Astra Trident documentation
- Use the Astra Control API
- Cloud Insights documentation
- ONTAP documentation

Architecture and components

Here is an overview of the various components of the Astra Control environment.



Astra Control components

- **Kubernetes clusters**: Kubernetes is a portable, extensible, open-source platform for managing containerized workloads and services, that facilitates both declarative configuration and automation. Astra provides management services for applications hosted in a Kubernetes cluster.
- **Astra Trident**: As a fully supported open source storage provisioner and orchestrator maintained by NetApp, Trident enables you to create storage volumes for containerized applications managed by Docker

and Kubernetes. When deployed with Astra Control Center, Trident includes a configured ONTAP storage backend, and also supports Astra Data Store as a storage backend.

- **Storage backend**:
  - Astra Control Service uses NetApp Cloud Volumes Service for Google Cloud as the storage backend for GKE clusters and Azure NetApp Files as the storage backend for AKS clusters.
  - Astra Control Service also supports Azure Managed Disks and Google Persistent Disk as backend storage options.
  - Astra Control Center uses the following storage backends:
    - Astra Data Store storage backend
    - ONTAP AFF and FAS storage backend. As a storage software and hardware platform, ONTAP provides core storage services, support for multiple storage access protocols, and storage management functionality, such as snapshots and mirroring.
    - Cloud Volumes ONTAP storage backend
- **Cloud Insights**: A NetApp cloud infrastructure monitoring tool, Cloud Insights enables you to monitor performance and utilization for your Kubernetes clusters managed by Astra Control Center. Cloud Insights correlates storage usage to workloads. When you enable the Cloud Insights connection in Astra Control Center, telemetry information shows in Astra Control Center UI pages.

Astra Control interfaces

You can complete tasks using different interfaces:

- **Web user interface (UI)**: Both Astra Control Service and Astra Control Center use the same web-based UI where you can manage, migrate and protect apps. Use the UI also to manage user accounts and configuration settings.
- **API**: Both Astra Control Service and Astra Control Center use the same Astra Control API. Using the API, you can perform the same tasks that you would using the UI.

Astra Control Center also enables you to manage, migrate, and protect Kubernetes clusters running within VM environments.

For more information

- Astra Control Service documentation
- Astra Control Center documentation
- Astra Trident documentation
- Use the Astra Control API
- Cloud Insights documentation
- ONTAP documentation

Data protection

Learn about the available types of data protection in Astra Control Center, and how best to use them to protect your apps.

Snapshots, backups, and protection policies

A *snapshot* is a point-in-time copy of an app that's stored on the same provisioned volume as the app. They are usually fast. You can use local snapshots to restore the application to an earlier point in time. Snapshots are useful for fast clones; snapshots include all of the Kubernetes objects for the app, including configuration files.

A *backup* is stored in the external object store, and can be slower to take compared to local snapshots. You can restore an app backup to the same cluster, or you can migrate an app by restoring its backup to a different cluster. You can also choose a longer retention period for backups. Because they are stored in the external object store, backups generally offer you better protection than snapshots in cases of server failure or data loss.

A *protection policy* is a way to protect an app by automatically creating snapshots, backups, or both according to a schedule that you define for that app. A protection policy also enables you to choose how many snapshots and backups to retain in the schedule. Automating your backups and snapshots with a protection policy is the best way to ensure each app is protected according to the needs of your organization.

You can't be fully protected until you have a recent backup. This is important because backups are stored in an object store away from the persistent volumes. If a failure or accident wipes out the cluster and its associated persistent storage, then you need a backup to recover. A snapshot would not enable you to recover.

Clones

A *clone* is an exact duplicate of an app, its configuration, and its persistent storage. You can manually create a clone on either the same Kubernetes cluster or on another cluster. Cloning an app can be useful if you need to move applications and storage from one Kubernetes cluster to another.

Licensing

Astra Control Center requires a license to be installed for the full App Data Management functionality to be enabled. When you deploy Astra Control Center without a license, a banner is displayed in the web UI, warning that system functionality is limited.

The following operations require a valid license:

- Managing new applications
- Creating snapshots or backups
- Configuring a protection policy to schedule snapshots or backups
- Restoring from a snapshot or backup
- Cloning from a snapshot or current state

You can add a cluster, add a bucket, and manage an Astra Data Store storage backend without a license. However, you need a valid Astra Control Center license to manage apps using Astra Data Store as a storage backend.

How license consumption is calculated

When you add a new cluster to Astra Control Center, it doesn't count toward consumed licenses until at least one application running on the cluster is managed by Astra Control Center. You can also add an Astra Data Store storage backend to Astra Control Center without affecting license consumption. This enables you to manage an Astra Data Store backend from an unlicensed Astra Control Center system.

When you start managing an app on a cluster, the cluster's CPU units are included in the Astra Control Center license consumption calculation.

Find more information

- Update an existing license

Validated vs standard apps

There are two types of applications you can bring to Astra Control: validated and standard. Learn the difference between these two categories and the potential impacts on your projects and strategy.

It's tempting to think of these two categories as "supported" and "unsupported." But as you will see, there is no such thing as an "unsupported" app in Astra Control. You can add any app to Astra Control, although validated apps have more infrastructure built around their Astra Control workflows compared to standard apps.

Validated apps

Validated apps for Astra Control include the following:

- MySQL 8.0.25
- MariaDB 10.5.9
- PostgreSQL 11.12
- Jenkins 2.277.4 LTS and 2.289.1 LTS

The list of validated apps represents applications that Astra Control recognizes. The Astra Control team has analyzed and confirmed these apps to be fully tested to restore. Astra Control executes custom workflows to help ensure application-level consistency of snapshots and backups.

If an app is validated, the Astra Control team has identified and implemented steps that can be taken to quiesce the app before taking a snapshot in order to obtain an application-consistent snapshot. For example, when Astra Control takes a backup of a PostgreSQL database, it first quiesces the database. After the backup is complete, Astra Control restores the database to normal operation.

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

Standard apps

Other apps, including custom programs, are considered standard apps. You can add and manage standard apps through Astra Control. You can also create basic, crash-consistent snapshots and backups of a standard app. However, these have not been fully tested to restore the app to its original state.

Astra Control itself is not a standard app; it is a "system app." Astra Control itself isn't shown by default for management. You should not try to manage Astra Control itself.

Storage classes and persistent volume size

Astra Control Center supports ONTAP or Astra Data Store as the storage backend.

Overview

Astra Control Center supports the following:

- **Trident storage classes backed by Astra Data Store storage**: If you installed one or more Astra Data Store clusters manually, Astra Control Center offers the ability to import these and retrieve their topology (nodes, disks) as well as various statuses.

  Astra Control Center displays the underlying Kubernetes cluster from the Astra Data Store configuration, the cloud that the Kubernetes cluster belongs to, any persistent volumes provisioned by Astra Data Store, the name of the corresponding internal volume, the application using the persistent volume, and the cluster containing the app.

- **Trident storage classes backed by ONTAP storage**: If you are using an ONTAP backend, Astra Control Center offers the ability to import the ONTAP backend to report various monitoring information.

Trident storage classes should be preconfigured outside of Astra Control Center.

Storage classes

When you add a cluster to Astra Control Center, you're prompted to select one previously configured storage class on that cluster as the default storage class. This storage class will be used when no storage class is specified in a persistent volume claim (PVC). The default storage class can be changed at any time within Astra Control Center and any storage class can be used at any time by specifying the name of the storage class within the PVC or Helm chart. Ensure that you have only a single default storage class defined for your Kubernetes cluster.

When you use Astra Control Center integrated with an Astra Data Store storage backend, after the installation, no storage classes are defined. You will need to create the Trident default storage class and apply it to the storage backend. See Astra Data Store getting started to create a default Astra Data Store storage class.

For more information

- Astra Trident documentation

User roles and namespaces

Learn about user roles and namespaces in Astra Control, and how you can use them to control access to resources in your organization.

User roles

You can use roles to control the access users have to resources or capabilities of Astra Control. The following are the user roles in Astra Control:

- A **Viewer** can view resources.
- A **Member** has Viewer role permissions and can manage apps and clusters, unmanage apps, and delete snapshots and backups.
- An **Admin** has Member role permissions and can add and remove any other users except the Owner.
- An **Owner** has Admin role permissions and can add and remove any user accounts.

You can add constraints to a Member or Viewer user to restrict the user to one or more Namespaces.

Namespaces

A namespace is a scope you can assign to specific resources within a cluster that is managed by Astra Control. Astra Control discovers a cluster's namespaces when you add the cluster to Astra Control. Once discovered, the namespaces are available to assign as constraints to users. Only members that have access to that namespace are able to use that resource. You can use namespaces to control access to resources using a paradigm that makes sense for your organization; for example, by physical regions or divisions within a company. When you add constraints to a user, you can configure that user to have access to all namespaces or only a specific set of namespaces. You can also assign namespace constraints using namespace labels.

Find more information

Manage roles