



Concepts

Astra Control Service

NetApp
December 16, 2021

Table of Contents

- Concepts 1
 - Architecture and components 1
 - Storage classes and PV size for AKS clusters 2
 - Service type, storage classes, and PV size for GKE clusters 3
 - Validated vs standard apps 5
 - Define a custom app 6

Concepts

Architecture and components

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

[Astra Control architecture diagram and components]

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.
- **Storage backend:**
 - Astra Control Service uses [NetApp Cloud Volumes Service for Google Cloud](#) as the backend storage for GKE clusters and [Azure NetApp Files](#) as the backend storage for AKS clusters.
 - 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 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](#)

Storage classes and PV size for AKS clusters

Astra Control Service supports Azure NetApp Files or Azure managed disks as the storage backend for Azure Kubernetes Service (AKS) clusters.

Azure NetApp Files

Astra Control Service supports Azure NetApp Files as the storage backend for Azure Kubernetes Service (AKS) clusters. You should understand how choosing a storage class and persistent volume size can help you meet your performance objectives.

Service levels and storage classes

Azure NetApp Files supports three service levels: Ultra storage, Premium storage, and Standard storage. Each of these service levels are designed for different performance needs:

Ultra storage

Provides up to 128 MiB/s of throughput per 1 TiB.

Premium storage

Provides up to 64 MiB/s of throughput per 1 TiB.

Standard storage

Provides up to 16 Mib/s of throughput per 1 TiB.

These service levels are an attribute of a capacity pool. You need to set up a capacity pool for each service level that you want to use with your Kubernetes clusters. [Learn how to set up capacity pools.](#)

Astra Control Service uses these service levels as storage classes for your persistent volumes. When you add Kubernetes clusters to Astra Control Service, you're prompted to choose either Ultra, Premium, or Standard as the default storage class. The names of the storage classes are *netapp-anf-perf-ultra*, *netapp-anf-perf-premium*, and *netapp-anf-perf-standard*.

[Learn more about these service levels in the Azure NetApp Files docs.](#)

Persistent volume size and performance

As described above, the throughput for each service level is per 1 TiB of provisioned capacity. That means larger volumes provide better performance. So you should take both capacity and performance needs into consideration when provisioning volumes.

Minimum volume size

Astra Control Service provisions persistent volumes using a minimum volume size of 100 GiB, even if the PVC asks for a smaller volume size. For example, if the PVC in a Helm chart asks for 6 GiB, Astra Control Service automatically provisions a 100 GiB volume.

Azure managed disks

Astra Control Service supports Azure managed disks as a storage backend option. This service provides block-level storage that is managed by Azure.

[Learn more about Azure managed disks.](#)

Service type, storage classes, and PV size for GKE clusters

Astra Control Service supports Cloud Volumes Service for Google Cloud or Google Persistent Disk as the storage backend options for persistent volumes.

Cloud Volumes Service for Google Cloud

Astra Control Service can use Cloud Volumes Service for Google Cloud as the storage backend for persistent volumes. You should understand how choosing a service type, storage class, and persistent volume size can help you meet your performance objectives.

Overview

Cloud Volumes Service for Google Cloud provides two service types: *CVS* and *CVS-Performance*. These service types are supported in specific Google Cloud regions. [Go to NetApp Cloud Central's Global Regions Maps](#) to identify the service type that's supported in the Google Cloud region where your clusters reside.

If your Kubernetes clusters must reside in a specific region, then you'll be using the service type supported in that region.

But if you have the flexibility to choose between Google Cloud regions, then we recommend the following based on your performance requirements:

- For K8s applications that have medium-to-high performance storage needs, choose a Google Cloud region that supports CVS-Performance and use the Premium or Extreme storage class. Such workloads include AI/ML pipelines, CI/CD pipelines, media processing, and databases including relational, noSQL, time series, etc.
- For K8s applications that have low-to-medium storage performance needs (web apps, general purpose file storage, etc.), choose a Google Cloud region that supports either CVS or CVS-Performance, with the Standard storage class.

The following table provides a quick comparison of the information described on this page.

Service type	Use case	Supported regions	Storage classes	Min volume size
CVS-Performance	Apps with medium-to-high storage performance needs	View supported Google Cloud regions	<ul style="list-style-type: none">• netapp-cvs-standard• netapp-cvs-premium• netapp-cvs-extreme	100 GiB

Service type	Use case	Supported regions	Storage classes	Min volume size
CVS	Apps with low-to-medium storage performance needs	View supported Google Cloud regions	netapp-cvs-standard	300 GiB

CVS-Performance service type

Learn more about the CVS-Performance service type before you choose a storage class and create persistent volumes.

Storage classes

Three service levels are supported with the CVS-Performance service type: Standard, Premium, and Extreme. When you add a cluster to Astra Control Service, you're prompted to choose either Standard, Premium, or Extreme as the default storage class for persistent volumes. Each of these service levels are designed for different capacity and bandwidth needs.

The names of the storage classes are *netapp-cvs-standard*, *netapp-cvs-premium*, and *netapp-cvs-extreme*.

[Learn more about these service levels in the Cloud Volumes Service for Google Cloud docs.](#)

Persistent volume size and performance

[As the Google Cloud docs explain](#), the allowed bandwidth for each service level is per GiB of provisioned capacity. That means larger volumes will provide better performance.

Be sure to read through the Google Cloud page linked to above. It includes cost comparisons and examples that can help you better understand how to couple a service level with volume size to meet your performance objectives.

Minimum volume size

Astra Control Service provisions persistent volumes using a minimum volume size of 100 GiB with the CVS-Performance service type, even if the PVC requests a smaller volume size. For example, if the PVC in a Helm chart asks for 6 GiB, Astra Control Service automatically provisions a 100 GiB volume.

CVS service type

Learn more about the CVS service type before you choose a storage class and create persistent volumes.

Storage class

One service level is supported with the CVS service type: Standard. When you manage clusters in regions where the CVS service type is supported, Astra Control Service uses the Standard service level as the default storage class for persistent volumes. The storage class is named *netapp-cvs-standard*.

[Learn more about the Standard service level in the Cloud Volumes Service for Google Cloud docs.](#)

Persistent volume size and performance

The allowed bandwidth for the CVS service type is per GiB of provisioned capacity. That means larger volumes will provide better performance.

Minimum volume size

Astra Control Service provisions persistent volumes using a minimum volume size of 300 GiB with the CVS service type, even if the PVC asks for a smaller volume size. For example, if 20 GiB is requested, Astra Control Service automatically provisions a 300 GiB volume.

Due to a limitation, if a PVC requests a volume between 700-999 GiB, Astra Control Service automatically provisions a volume size of 1000 GiB.

Google Persistent Disk

Astra Control Service supports Google Persistent Disk as a storage backend option. This service provides block-level storage that is managed by Google.

[Learn more about Google Persistent Disk.](#)

[Learn more about different performance levels of Google Persistent Disks.](#)

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.

Define a custom app

Creating a custom app lets you group elements of your Kubernetes cluster into a single app.

A custom app gives you more granular control over what to include in an Astra Control operation, including:

- Clone
- Snapshot
- Backup
- Protection policy

In most cases you will want to use Astra Control's features on your entire app. However, you can also create a custom app to use these features by the labels you assign to Kubernetes objects in a namespace.

To create a custom app, go to the Apps page and select **+ Define custom app**.

As you make your selections, the Custom App window will show you which resources will be included or excluded from your custom app. This helps you make sure you are choosing the correct criteria for defining your custom app.

The screenshot shows a 'Custom Application' window with two columns: 'SELECTED RESOURCES' and 'UNSELECTED RESOURCES'. Each column has a 'Filter by name' input field and a table of resources.

SELECTED RESOURCES	
Resources (1) ↑	Created
Pod (1)	
nginx-pod0 deployment: canary +1	2020/10/09 14:01 UTC

UNSELECTED RESOURCES	
Resources (2) ↑	Created
Pod (2)	
nginx-pod1 deployment: stable +1	2020/10/09 14:01 UTC
nginx-pod2	2020/10/09 14:01 UTC

In the above example, one resource (the pod `nginx-pod0` labeled `deployment: canary`) will be included in the custom app. Two pods (`nginx-pod1` and `nginx-pod2` both labeled `deployment: stable`) will be excluded.



Custom apps can only be created within a specified namespace on a single cluster. Astra Control does not support the ability for a custom app to span multiple namespaces or clusters.

A label is a key/value pair you can assign to Kubernetes objects for identification. Labels make it easier to sort, organize, and find your Kubernetes objects. To learn more about Kubernetes labels, [see the official Kubernetes documentation](#).



Overlapping policies for the same resource under different names can cause data conflicts. If you create a custom app for a resource, be sure it's not being cloned or backed up under any other policies.

Example: Separate Protection Policy for canary release

In this example, the DevOps team is managing a canary release deployment. Their cluster has three pods running NginX. Two of the pods are dedicated to the stable release. The third pod is for the canary release.

The team's Kubernetes admin adds the label `deployment=stable` to the stable release pods. The admin also adds the label `deployment=canary` to the canary release pod.

```
:~$ kubectl get pods --namespace=nginx-app --show-labels
```

NAME	READY	STATUS	RESTARTS	AGE	LABELS
nginx-pod0	1/1	Running	0	50s	deployment=canary,run=nginx-pod0
nginx-pod1	1/1	Running	0	45s	deployment=stable,run=nginx-pod1
nginx-pod2	1/1	Running	0	41s	deployment=stable,run=nginx-pod2

```
:~$
```

The team's stable release includes a requirement for hourly snapshots and daily backups. The canary release is more ephemeral, so they want to create a less aggressive, short-term protection policy for anything labeled `deployment=canary`.

In order to avoid possible data conflicts, the admin creates two custom apps: one for the canary release, and one for the stable release. This keeps the backups, snapshots, and clone operations separate for the two groups of Kubernetes objects.

After the admin adds the cluster to Astra Control, the next step is to define a custom app. To do this, the admin selects the **+ Define custom app** button on the Apps page.

In the pop-up window which appears, the admin sets `devops-canary-deployment` as the app name. The admin then chooses the cluster in the **Cluster** drop-down, then the app's namespace from the **Namespace** drop-down.

At this point, the admin can either type `deployment=canary` in the **Labels** field, or select that label from the resources listed below.

After defining the custom app for the canary deployment, the admin repeats the process for the stable deployment.

After creating the two custom apps, the admin can treat these resources as any other Astra Control application. The admin can clone them, create backups and snapshots, and create a custom protection policy for each group of resources based on the Kubernetes labels.

Copyright Information

Copyright © 2021 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.