# Known issues

## Astra Control Center

NetApp
August 16, 2022

# Table of Contents

# Known issues

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

The following known issues affect the current release:

**Apps**



**Clusters**



**Other issues**



## Restore of an app results in PV size larger than original PV

If you resize a persistent volume after creating a backup and then restore from that backup, the persistent volume size will match the new size of the PV instead of using the size of the backup.

## App clones fail using a specific version of PostgreSQL

App clones within the same cluster consistently fail with the Bitnami PostgreSQL 11.5.0 chart. To clone successfully, use an earlier or later version of the chart.

## App clones fail when using Service Account level OCP Security Context Constraints (SCC)

An application clone might fail if the original security context constraints are configured at the service account level within the namespace on the OpenShift Container Platform cluster. When the application clone fails, it appears in the Managed Applications area in Astra Control Center with status `Removed`. See the knowledgebase article for more information.

## App backups and snapshots fail if the volumesnapshotclass is added after a cluster is managed

Backups and snapshots fail with a `UI 500 error` in this scenario. As a workaround, refresh the app list.

# App clones fail after an application is deployed with a set storage class

After an application is deployed with a storage class explicitly set (for example, `helm install …-set global.storageClass=netapp-cvs-perf-extreme`), subsequent attempts to clone the application require that the target cluster have the originally specified storage class.
Cloning an application with an explicitly set storage class to a cluster that does not have the same storage class will fail. There are no recovery steps in this scenario.

# Managing a cluster with Astra Control Center fails when default kubeconfig file contains more than one context

You cannot use a kubeconfig with more than one cluster and context in it. See the knowledgebase article for more information.

# App data management operations fail with Internal Service Error (500) when Astra Trident is offline

If Astra Trident on an app cluster goes offline (and is brought back online) and 500 internal service errors are encountered when attempting app data management, restart all of the Kubernetes nodes in the app cluster to restore functionality.

# Snapshots might fail with snapshot controller version 4.2.0

When you use Kubernetes snapshot-controller (also known as external-snapshotter) version 4.2.0 with Kubernetes 1.20 or 1.21, snapshots can eventually begin to fail. To prevent this, use a different supported version of external-snapshotter, such as version 4.2.1, with Kubernetes versions 1.20 or 1.21.

1. Run a POST call to add an updated kubeconfig file to the `/credentials` endpoint and retrieve the assigned `id` from the response body.
2. Run a PUT call from the `/clusters` endpoint using the appropriate cluster ID and set the `credentialID` to the `id` value from the previous step.

After you complete these steps, the credential associated with the cluster is updated and the cluster should reconnect and update its state to `available`.

# Find more information

- Known issues with Astra Data Store preview and this Astra Control Center release
- Known limitations

# Known issues with Astra Data Store and this Astra Control Center release

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

See these additional Astra Data Store known issues that might affect the management of Astra Data Store with

the current release of the Astra Control Center.

## Astra Data Store volume details do not appear in Storage Backends page of the Astra Control Center UI

Details such as capacity and throughput do not appear in the UI. When this issue occurs, unmanage the storage backend and add it back again.

## Unmanaging a cluster with Astra Data Store requires first removing a managed system app

If you added a cluster that contains Astra Data Store to an Astra Control Center cluster, the astrads-system app is managed by default as a hidden application. To unmanage the cluster, you must first unmanage the astrads-system app. You cannot unmanage this type of app using the Astra Control Center UI. Instead, use an Astra Control API request to manually remove the app:

**Details**

**Steps**

1. Get the ID for the managed cluster using this API:

```
/accounts/{account_id}/topology/v1/managedClusters
```

Response:

```
{
"items": [
{
"type": "application/astra-managedCluster",
"version": "1.1",
"id": "123ab987-0bc0-00d0-a00a-1234567abd8d",
"name": "astrads-cluster-1234567",
...
```

2. Get the managed astrads-system app ID:

```
/accounts/{account_id}/topology/v2/managedClusters/{managedCluster_id}/apps
```

Response:

```
{
  "items": [
    [
      "1b011d11-bb88-40c7-a1a1-ab1234c123d3",
      "astrads-system",
      "ready"
    ]
  ],
  "metadata": {}
}
```

3. Delete the astrads-system app using the app ID you acquired in the previous step (`1b011d11-bb88-40c7-a1a1-ab1234c123d3`).

```
/accounts/{account_id}/k8s/v2/apps/{astrads-system_app_id}
```

## Find more information

- Known issues
- Known limitations