Release notes

Astra Control Center

NetApp
February 12, 2024

Table of Contents

Release notes

We’re pleased to announce the latest release of Astra Control Center.

- What’s in this release of Astra Control Center
- Known issues
- Known limitations

Follow us on Twitter @NetAppDoc. Send feedback about documentation by becoming a GitHub contributor or sending an email to doccomments@netapp.com.

What’s new in this release of Astra Control Center

We’re pleased to announce the latest release of Astra Control Center.

22 November 2022 (22.11.0)

New features and support

- Support for applications that span across multiple namespaces
- Support for including cluster resources in an application definition
- Enhanced LDAP authentication with role-based access control (RBAC) integration
- Added support for Kubernetes 1.25 and Pod Security Admission (PSA)
- Enhanced progress reporting for your backup, restore, and clone operations

Known issues and limitations

- Known issues for this release
- Known limitations for this release

8 September 2022 (22.08.1)

This patch release (22.08.1) for Astra Control Center (22.08.0) fixes minor bugs in app replication using NetApp SnapMirror.

10 August 2022 (22.08.0)

Details

New features and support

- App replication using NetApp SnapMirror technology
- Improved app management workflow
- Enhanced provide-your-own execution hooks functionality

> The NetApp provided default pre- and post-snapshot execution hooks for specific applications have been removed in this release. If you upgrade to this release and do not provide your own execution hooks for snapshots, Astra Control will take crash-consistent snapshots only. Visit the NetApp Verda GitHub repository for sample execution hook scripts that you can modify to fit your environment.

- Support for VMware Tanzu Kubernetes Grid Integrated Edition (TKGI)
- Support for Google Anthos
- LDAP configuration (via Astra Control API)

Known issues and limitations

- Known issues for this release
- Known limitations for this release

26 April 2022 (22.04.0)

Details

New features and support

- Namespace role-based access control (RBAC)
- Support for Cloud Volumes ONTAP
- Generic ingress enablement for Astra Control Center
- Bucket removal from Astra Control
- Support for VMware Tanzu Portfolio

Known issues and limitations

- Known issues for this release
- Known limitations for this release

14 December 2021 (21.12)

Details

New features and support

- Application restore
- Execution hooks
- Support for applications deployed with namespace-scoped operators
- Additional support for upstream Kubernetes and Rancher
- Astra Control Center upgrades
- Red Hat OperatorHub option for installation

Resolved issues

- Resolved issues for this release

Known issues and limitations

- Known issues for this release
- Known limitations for this release

5 August 2021 (21.08)

Details

Initial release of Astra Control Center.

- What it is
- Understand architecture and components
- What it takes to get started
- Install and setup
- Manage and protect apps
- Manage buckets and storage backends
- Manage accounts
- Automate with API

Find more information

- Known issues for this release
- Known limitations for this release
- Earlier versions of Astra Control Center documentation

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

- Restore of an app results in PV size larger than original PV
- App clones fail using a specific version of PostgreSQL
- App clones fail when using Service Account level OCP Security Context Constraints (SCC)
- App clones fail after an application is deployed with a set storage class
- App backups and snapshots fail if the volumesnapshotclass is added after a cluster is managed

Clusters

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

Other issues

- Managed clusters do not appear in NetApp Cloud Insights when connecting through a proxy
- App data management operations fail with Internal Service Error (500) when Astra Trident is offline

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.

Managed clusters do not appear in NetApp Cloud Insights when connecting through a proxy

When Astra Control Center connects to NetApp Cloud Insights through a proxy, managed clusters might not appear in Cloud Insights. As a workaround, run the following commands on each managed cluster:

```
kubectl get cm telegraf-conf -o yaml -n netapp-monitoring | sed
'/\[\[outputs.http\]\]/c\    [[outputs.http]]\n    use_system_proxy =
true' | kubectl replace -f -
```

```
kubectl get cm telegraf-conf-rs -o yaml -n netapp-monitoring | sed
'/\[\[outputs.http\]\]/c\    [[outputs.http]]\n    use_system_proxy =
true' | kubectl replace -f -
```

```
kubectl get pods -n netapp-monitoring --no-headers=true | grep 'telegraf-
ds\|telegraf-rs' | awk '{print $1}' | xargs kubectl delete -n netapp-
monitoring pod
```

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.

Find more information

- Known limitations

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.

Cluster management limitations

- The same cluster cannot be managed by two Astra Control Center instances
- Astra Control Center cannot manage two identically named clusters

Role-based Access Control (RBAC) limitations

- A user with namespace RBAC constraints can add and unmanage a cluster
- A member with namespace constraints cannot access the cloned or restored apps until admin adds the namespace to the constraint

App management limitations

- Multiple applications in a single namespace cannot be restored collectively to a different namespace
- Astra Control does not automatically assign default buckets for cloud instances
- Clones of apps installed using pass-by-reference operators can fail
- In-place restore operations of apps that use a certificate manager are not supported
- OLM-enabled and cluster-scoped operator deployed apps not supported
- Apps deployed with Helm 2 are not supported

General limitations

- S3 buckets in Astra Control Center do not report available capacity
- Astra Control Center does not validate the details you enter for your proxy server
- Existing connections to a Postgres pod causes failures
- Backups and snapshots might not be retained during removal of an Astra Control Center instance
- LDAP user and group limitations

The same cluster cannot be managed by two Astra Control Center instances

If you want to manage a cluster on another Astra Control Center instance, you should first unmanage the cluster from the instance on which it is managed before you manage it on another instance. After you remove the cluster from management, verify that the cluster is unmanaged by executing this command:

```
oc get pods n -netapp-monitoring
```

There should be no pods running in that namespace or the namespace should not exist. If either of those are true, the cluster is unmanaged.

Astra Control Center cannot manage two identically named clusters

If you try to add a cluster with the same name of a cluster that already exists, the operation will fail. This issue most often occurs in a standard Kubernetes environment if you have not changed the cluster name default in Kubernetes configuration files.

As a workaround, do the following:

1. Edit your `kubeadm-config` ConfigMap:

   ```
   kubectl edit configmaps -n kube-system kubeadm-config
   ```

2. Change the `clusterName` field value from `kubernetes` (the Kubernetes default name) to a unique custom name.

3. Edit kubeconfig (`.kube/config`).
4. Update cluster name from `kubernetes` to a unique custom name (`xyz-cluster` is used in the examples below). Make the update in both `clusters` and `contexts` sections as shown in this example:

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data:
ExAmPLERb2tCcjZ5K3E2Njk4eQotLExAMpLEORCBDRVJUSUZJQ0FURS0txxxxXX==
    server: https://x.x.x.x:6443
  name: xyz-cluster
contexts:
- context:
    cluster: xyz-cluster
    namespace: default
    user: kubernetes-admin
  name: kubernetes-admin@kubernetes
current-context: kubernetes-admin@kubernetes
```

A user with namespace RBAC constraints can add and unmanage a cluster

A user with namespace RBAC constraints should not be allowed to add or unmanage clusters. Due to a current limitation, Astra does not prevent such users from unmanaging clusters.

A member with namespace constraints cannot access the cloned or restored apps until admin adds the namespace to the constraint

Any `member` user with RBAC constraints by namespace name/ID can clone or restore an app to a new namespace on the same cluster or to any other cluster in their organization's account. However, the same user cannot access the cloned or restored app in the new namespace. After a new namespace is created by a clone or restore operation, the account admin/owner can edit the `member` user account and update role constraints for the affected user to grant access to the new namespace.

Multiple applications in a single namespace cannot be restored collectively to a different namespace

If you manage multiple applications in a single namespace (by creating multiple app definitions in Astra Control), you cannot restore all of the applications to a different single namespace. You need to restore each application to its own separate namespace.

Astra Control does not automatically assign default buckets for cloud instances

Astra Control does not automatically assign a default bucket for any cloud instance. You need to manually set a default bucket for a cloud instance. If a default bucket is not set, you won't be able to perform app clone operations between two clusters.

Clones of apps installed using pass-by-reference operators can fail

Astra Control supports apps installed with namespace-scoped operators. These operators are generally designed with a "pass-by-value" rather than "pass-by-reference" architecture. The following are some operator apps that follow these patterns:

- Apache K8ssandra

> For K8ssandra, in-place restore operations are supported. A restore operation to a new namespace or cluster requires that the original instance of the application to be taken down. This is to ensure that the peer group information carried over does not lead to cross-instance communication. Cloning of the app is not supported.

- Jenkins CI
- Percona XtraDB Cluster

Astra Control might not be able to clone an operator that is designed with a “pass-by-reference” architecture (for example, the CockroachDB operator). During these types of cloning operations, the cloned operator attempts to reference Kubernetes secrets from the source operator despite having its own new secret as part of the cloning process. The clone operation might fail because Astra Control is unaware of the Kubernetes secrets in the source operator.

> During clone operations, apps that need an IngressClass resource or webhooks to function properly must not have those resources already defined on the destination cluster.

In-place restore operations of apps that use a certificate manager are not supported

This release of Astra Control Center does not support in-place restore of apps with certificate managers. Restore operations to a different namespace and clone operations are supported.

OLM-enabled and cluster-scoped operator deployed apps not supported

Astra Control Center does not support application management activities with cluster-scoped operators.

Apps deployed with Helm 2 are not supported

If you use Helm to deploy apps, Astra Control Center requires Helm version 3. Managing and cloning apps deployed with Helm 3 (or upgraded from Helm 2 to Helm 3) is fully supported. For more information, see Astra Control Center requirements.

S3 buckets in Astra Control Center do not report available capacity

Before backing up or cloning apps managed by Astra Control Center, check bucket information in the ONTAP or StorageGRID management system.

Astra Control Center does not validate the details you enter for your proxy server

Ensure that you enter the correct values when establishing a connection.

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 Control requires psql access to freeze and thaw the databases. If there is a pre-existing connection, the snapshot, backup, or clone will fail.

Backups and snapshots might not be retained during removal of an Astra Control Center instance

If you have an evaluation license, be sure you store your account ID to avoid data loss in the event of Astra Control Center failure if you are not sending ASUPs.

LDAP user and group limitations

Astra Control Center supports up to 5,000 remote groups and 10,000 remote users.

Find more information

- Known issues

Copyright information

Trademark information