



Release notes

Astra Control Center

NetApp
March 12, 2024

Table of Contents

- Release notes 1
 - What's new in this release of Astra Control Center 1
 - Known issues 5
 - Known limitations 7

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](#)

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.

7 November 2023 (23.10.0)

New features and support

- **Backup and restore capabilities for applications with `ontap-nas-economy` driver-backed storage backends:** Enable backup and restore operations for `ontap-nas-economy` with some [simple steps](#).
- **Immutable Backups:** Astra Control now supports [unalterable, read-only backups](#) as an additional security layer against malware and other threats.
- **Introducing Astra Control Provisioner**

With the 23.10 release, Astra Control introduces a new software component called Astra Control Provisioner that will be available to all licensed Astra Control users. Astra Control Provisioner provides access to a superset of advanced management and storage provisioning features beyond those that Astra Trident provides. These features are available to all Astra Control customers at no additional cost.

- **Get started with Astra Control Provisioner**
You can [enable Astra Control Provisioner](#) if you have installed and configured your environment to use Astra Trident 23.10.
- **Astra Control Provisioner functionality**

The following features are available with the Astra Control Provisioner 23.10 release:

- **Enhanced storage backend security with Kerberos 5 encryption:** You can improve storage security by [enabling encryption](#) for the traffic between your managed cluster and the storage backend. Astra Control Provisioner supports Kerberos 5 encryption over NFSv4.1 connections from Red Hat OpenShift clusters to Azure NetApp Files and on-premise ONTAP volumes
- **Recover data using a snapshot:** Astra Control Provisioner provides rapid, in-place volume restoration from a snapshot using the `TridentActionSnapshotRestore` (TASR) CR.
- **SnapMirror enhancements:** Use the app replication feature in environments where Astra Control does not have direct connectivity to an ONTAP cluster or access to ONTAP credentials. This feature allows you to use replication without having to manage a storage backend or its credentials in Astra Control.
- **Backup and restore capabilities for applications with `ontap-nas-economy` driver-backed storage backends:** As described [above](#).

- **Support for managing applications that use NVMe/TCP storage**

Astra Control can now manage applications backed by persistent volumes that are connected using NVMe/TCP.

- **Execution hooks turned off by default:** Beginning with this release, execution hooks functionality can be [enabled](#) or disabled for additional security (it is disabled by default). If you have not yet created execution hooks for use with Astra Control, you need to [enable the execution hooks feature](#) to begin creating hooks. If you created execution hooks prior to this release, the execution hooks functionality stays enabled and you can use hooks as you would normally.

Known issues and limitations

- [Known issues for this release](#)
- [Known limitations for this release](#)

31 July 2023 (23.07.0)

Details

New features and support

- [Support for using NetApp MetroCluster in a stretch configuration as a storage backend](#)
- [Support for using Longhorn as a storage backend](#)
- [Applications can now be replicated between ONTAP backends from the same Kubernetes cluster](#)
- [Astra Control Center now supports 'userPrincipalName' as an alternative login attribute for remote \(LDAP\) users](#)
- [New execution hook type 'post-failover' can be run after replication failover with Astra Control Center](#)
- [Clone workflows now support live clones only \(the current state of managed application\). To clone from a snapshot or backup, use the \[restore workflow\]\(#\).](#)

Known issues and limitations

- [Known issues for this release](#)
- [Known limitations for this release](#)

18 May 2023 (23.04.2)

Details

This patch release (23.04.2) for Astra Control Center (23.04.0) provides support for [Kubernetes CSI external snapshotter v6.1.0](#) and fixes the following:

- [A bug with in-place application restore when using execution hooks](#)
- [Connection issues with the bucket service](#)

25 April 2023 (23.04.0)

Details

New features and support

- [90-day evaluation license enabled by default for new Astra Control Center installations](#)
- [Enhanced execution hooks functionality with additional filtering options](#)
- [Execution hooks can now be run after replication failover with Astra Control Center](#)
- [Support for migrating volumes from the 'ontap-nas-economy storage' class to the 'ontap-nas' storage class](#)
- [Support for including or excluding application resources during restore operations](#)
- [Support for managing data-only applications](#)

Known issues and limitations

- [Known issues for this release](#)
- [Known limitations for this release](#)

22 November 2022 (22.11.0)

Details

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)

Details

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:

- [App backups and snapshots fail if the volumesnapshotclass is added after a cluster is managed](#)
- [Managing a cluster with Astra Control Center fails when kubeconfig file contains more than one context](#)
- [A monitoring pod can crash in Istio environments](#)
- [App data management operations fail with Internal Service Error \(500\) when Astra Trident is offline](#)
- [In-place restore operations to ontap-nas-economy storage classes fail](#)
- [Restoring from a backup when using Kerberos in-flight encryption can fail](#)
- [Backup data remains in bucket after deletion for buckets with expired retention policy](#)

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.

Managing a cluster with Astra Control Center fails when 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.

A monitoring pod can crash in Istio environments

If you pair Astra Control Center with Cloud Insights in an Istio environment, the `telegraf-rs` pod can crash. As a workaround, perform the following steps:

1. Find the crashed pod:

```
kubectl -n netapp-monitoring get pod | grep Error
```

You should see output similar to the following:

```
NAME READY STATUS RESTARTS AGE
telegraf-rs-fhhrh 1/2 Error 2 (26s ago) 32s
```

2. Restart the crashed pod, replacing `<pod_name_from_output>` with the name of the affected pod:

```
kubectl -n netapp-monitoring delete pod <pod_name_from_output>
```

You should see output similar to the following:

```
pod "telegraf-rs-fhhrh" deleted
```


3. Verify that the pod has restarted, and is not in an Error state:

```
kubectl -n netapp-monitoring get pod
```

You should see output similar to the following:

```
NAME READY STATUS RESTARTS AGE
telegraf-rs-rrnsb 2/2 Running 0 11s
```

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.

In-place restore operations to ontap-nas-economy storage classes fail

If you perform an in-place restore of an application (restore the app to its original namespace), and the app's storage class uses the `ontap-nas-economy` driver, the restore operation can fail if the snapshot directory is not hidden. Before restoring in-place, follow the instructions in [Enable backup and restore for ontap-nas-economy operations](#) to hide the snapshot directory.

Restoring from a backup when using Kerberos in-flight encryption can fail

When you restore an application from a backup to a storage backend that is using Kerberos in-flight encryption, the restore operation can fail. This issue does not affect restoring from a snapshot or replicating the application data using NetApp SnapMirror.



When using Kerberos in-flight encryption with NFSv4 volumes, ensure that the NFSv4 volumes are using the correct settings. Refer to the NetApp NFSv4 Domain Configuration section (page 13) of the [NetApp NFSv4 Enhancements and Best Practices Guide](#).

Backup data remains in bucket after deletion for buckets with expired retention policy

If you delete an app's immutable backup after the bucket's retention policy has expired, the backup is deleted from Astra Control but not from the bucket. This issue will be fixed in an upcoming release.

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 support apps that use multiple storage classes per 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
- Snapshots might fail for Kubernetes 1.25 or later clusters with certain snapshot controller versions
- Backups and snapshots might not be retained during removal of an Astra Control Center instance

General limitations

- LDAP user and group 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
- The Activity page displays up to 100000 events
- SnapMirror does not support applications using NVMe over TCP for storage backends

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 clone or restore operation creates a new namespace, 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 support apps that use multiple storage classes per namespace

Astra Control supports apps that use a single storage class per namespace. When you add an app to a namespace, be sure the app has the same storage class as other apps in the 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, refer to [Astra Control Center requirements](#).

Snapshots might fail for Kubernetes 1.25 or later clusters with certain snapshot controller versions

Snapshots for Kubernetes clusters running version 1.25 or later can fail if version v1beta1 of the snapshot controller APIs are installed on the cluster.

As a workaround, do the following when upgrading existing Kubernetes 1.25 or later installations:

1. Remove any existing Snapshot CRDs and any existing snapshot controller.
2. [Uninstall Astra Trident](#).
3. [Install the snapshot CRDs and the snapshot controller](#).
4. [Install the latest Astra Trident version](#).
5. [Create a VolumeSnapshotClass](#).

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.

Astra Control does not support an LDAP entity (user or group) that has a DN containing an RDN with a trailing '\ ' or trailing space.

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.

The Activity page displays up to 100000 events

The Astra Control Activity page can display up to 100,000 events. To view all logged events, retrieve the events using the [Astra Control API](#).

SnapMirror does not support applications using NVMe over TCP for storage backends

Astra Control Center does not support NetApp SnapMirror replication for storage backends that are using the NVMe over TCP protocol.

Find more information

- [Known issues](#)

Copyright information

Copyright © 2024 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.