



Release notes

Astra Control Center

NetApp
August 26, 2021

This PDF was generated from <https://docs.netapp.com/us-en/astra-control-center/release-notes/whats-new.html> on August 26, 2021. Always check docs.netapp.com for the latest.

Table of Contents

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

Release notes

We're pleased to announce the initial 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 in this release of Astra Control Center

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

5 August 2021 (21.08)

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](#)

Known issues with this release

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

App with user-defined label goes into "removed" state

If you define an app with a non-existent k8s label, Astra Control Center will create, manage, and then immediately remove the app. To avoid this, add the k8s label to pods and resources after the app is managed by Astra Control Center.

Unable to stop running app backup

There is no way to stop a running backup. If you need to delete the backup, wait until it has completed and then use the instructions in [Delete backups](#). To delete a failed backup, use the [Astra API](#).

Astra Control Center UI slow to show changes to app resources such as persistent volume changes

After a data protection operation (clone, backup, restore) and subsequent persistent volume resize, there is up to a twenty-minute delay before the new volume size is shown in the UI. This delay in the UI can also occur when any app resources are added or modified. In this case, a data protection operation is successful within minutes and you can use the management software for the storage backend to confirm the change in volume size.

Clone performance impacted by large persistent volumes

Clones of very large and consumed persistent volumes might be intermittently slow, dependent on cluster access to the object store. If the clone is hung and no data has been copied for more than 30 minutes, Astra Control terminates the clone action.

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.

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.

Reusing buckets between instances of Astra Control Center causes failures

If you try to reuse a bucket used by another or previous installation of Astra Control Center, backup and restore will fail. You must use a different bucket or completely clean out the previously used bucket. You can't share buckets between instances of Astra Control Center.

Selecting a bucket provider type with credentials for another type causes data protection failures

When you add a bucket, select the correct bucket provider type with credentials that are correct for that provider. For example, the UI accepts NetApp ONTAP S3 as the type with StorageGRID credentials; however, this will cause all future app backups and restores using this bucket to 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.

Clone operation can't use other buckets besides the default

During an app backup or app restore, you can optionally specify a bucket ID. An app clone operation, however, always uses the default bucket that has been defined. There is no option to change buckets for a clone. If you want control over which bucket is used, you can either [change the bucket default](#) or do a [backup](#) followed by a [restore](#) separately.

Can't determine ASUP tar bundle status in scaled environment

During ASUP collection, the status of the bundle in the UI is reported as either `collecting` or `done`. Collection can take up to an hour for large environments. During ASUP download the network file transfer speed for the bundle might be insufficient, and the download might time out after 15 minutes without any indication in the UI. Download issues depend on the size of the ASUP, the scaled cluster size, and if collection time goes beyond the seven day limit.

Uninstall of Astra Control Center fails to clean up the monitoring-operator pod on the managed cluster

If you did not unmanage your clusters before you uninstalled Astra Control Center, you can manually delete the pods in the `netapp-monitoring` namespace and the namespace with the following commands:

Steps

1. Delete `acc-monitoring` agent:

```
oc delete agents acc-monitoring -n netapp-monitoring
```

Result:

```
agent.monitoring.netapp.com "acc-monitoring" deleted
```

2. Delete the namespace:

```
oc delete ns netapp-monitoring
```

Result:

```
namespace "netapp-monitoring" deleted
```

3. Confirm resources removed:

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

Result:

```
No resources found in netapp-monitoring namespace.
```

4. Confirm monitoring agent removed:

```
oc get crd|grep agent
```

Sample result:

```
agents.monitoring.netapp.com
```

```
2021-07-21T06:08:13Z
```

5. Delete custom resource definition (CRD) information:

```
oc delete crds agents.monitoring.netapp.com
```

Result:

```
customresourcedefinition.apiextensions.k8s.io  
"agents.monitoring.netapp.com" deleted
```

Uninstall of Astra Control Center fails to clean up Traefik CRDs

You can manually delete the Traefik CRDs:

Steps

1. Confirm which CRDs were not deleted by the uninstall process:

```
kubectl get crds |grep -E 'traefik'
```

Response

```
ingressroutes.traefik.containo.us      2021-06-23T23:29:11Z  
ingressroutetcps.traefik.containo.us   2021-06-23T23:29:11Z  
ingressrouteudps.traefik.containo.us   2021-06-23T23:29:12Z  
middlewares.traefik.containo.us        2021-06-23T23:29:12Z  
serverstransports.traefik.containo.us  2021-06-23T23:29:13Z  
tlsoptions.traefik.containo.us         2021-06-23T23:29:13Z  
tlsstores.traefik.containo.us          2021-06-23T23:29:14Z  
traefikservices.traefik.containo.us    2021-06-23T23:29:15Z
```

2. Delete the CRDs:

```
kubectl delete crd agents.monitoring.netapp.com
ingressroutes.traefik.containo.us ingressroutetcps.traefik.containo.us
ingressrouteudps.traefik.containo.us middlewares.traefik.containo.us
serverstransports.traefik.containo.us tlsoptions.traefik.containo.us
tlsstores.traefik.containo.us traefikservices.traefik.containo.us
```

Find more information

- [Known limitations for this release](#)

Known limitations with this release

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.

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.

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

Astra Control Center does not support apps that are deployed with Operator Lifecycle Manager (OLM)-enabled operators or cluster-scoped operators.

Cloning apps can only be done with same K8s distribution

If you clone an app between clusters, the source and destination clusters must be the same distribution of Kubernetes. For example, if you clone an app from an OpenShift 4.7 cluster, use a destination cluster that is also OpenShift 4.7.

OpenShift 4.8 is not supported

OpenShift 4.8 is not supported for the July release of Astra Control Center. For more information, see [Astra Control Center requirements](#).

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) are fully supported. For more information, see [Astra Control Center requirements](#).

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.

Data protection for Astra Control Center as app not yet available

This release does not support the ability to manage Astra as an app using snapshot, backup, or restore options.

Unhealthy pods affect app management

If a managed app has pods in an unhealthy state, Astra Control can't create new backups and clones.

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.

Trident isn't uninstalled from a cluster

When you unmanage a cluster from Astra Control Center, Trident isn't automatically uninstalled from the cluster. To uninstall Trident, you'll need to [follow these steps in the Trident documentation](#).

Find more information

- [Known issues for this release](#)

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.