



Known issues

Astra Control Center

NetApp
May 11, 2022

Table of Contents

- Known issues 1
 - Restore of an app results in PV size larger than original PV 1
 - App clones fail using a specific version of PostgreSQL 1
 - App clones fail when using Service Account level OCP Security Context Constraints (SCC) 1
 - App clones fail after an application is deployed with a set storage class. 1
 - Managing a cluster with Astra Control Center fails when default kubeconfig file contains more than one context 2
 - App data management operations fail with Internal Service Error (500) when Astra Trident is offline 2
 - Snapshots might fail with snapshot controller version 4.2.0 2
 - Find more information 2
 - Known issues with Astra Data Store preview and this Astra Control Center release. 2

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](#)

Clusters

- [Managing a cluster with Astra Control Center fails when default kubeconfig file contains more than one context](#)

Other issues

- [App data management operations fail with Internal Service Error \(500\) when Astra Trident is offline](#)
- [Snapshots might fail with snapshot controller version 4.2.0](#)

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 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 preview and this Astra Control Center release

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

The following known issues affect the management of Astra Data Store with this current release of the Astra Control Center:

Astra Data Store preview cannot be used as a storage class for Astra Control Center due to MongoDB pod liveness probe failure

When you attempt to use Astra Data Store preview as the storage class provisioner during an Astra Control Center deployment, the MongoDB pod liveness probe fails, resulting in a deployment that will not complete.

To correct this issue, make the following changes in addition to the standard YAML changes when completing the [Astra Control Center installation process](#):

1. Edit the [Astra Control Center operator deployment YAML \(astra_control_center_operator_deploy.yaml\)](#) to change the Helm install timeout:

```
- name: ACCOP_HELM_INSTALLTIMEOUT
  value: 20m
```

2. Edit the [Astra Control Center custom resource \(CR\) file \(astra_control_center_min.yaml\)](#) and include the highlighted additional values under spec:

```
apiVersion: astra.netapp.io/v1
kind: AstraControlCenter
metadata:
  name: astra
spec:
  accountName: "Example"
  astraVersion: "ASTRA_VERSION"
  astraAddress: "astra.example.com"
  autoSupport:
    enrolled: true
  email: "[admin@example.com]"
  firstName: "SRE"
  lastName: "Admin"
  imageRegistry:
    name: "[your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
  additionalValues:
    polaris-mongodb:
      mongodb:
        livenessProbe:
          initialDelaySeconds: 400
    metrics:
      livenessProbe:
        initialDelaySeconds: 400
```

Find more information

- [Known issues](#)
- [Known limitations](#)
- [Astra Data Store documentation](#)

Copyright Information

Copyright © 2022 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.