# Versionshinweise

## Astra Control Center

NetApp
June 06, 2024

# Inhalt

# Versionshinweise

Wir freuen uns, die erste Version des Astra Control Center ankündigen zu können.

- "In dieser Version des Astra Control Center"
- "Bekannte Probleme"
- "Bekannte Einschränkungen"

Bleiben Sie mit Twitter am Ball. @NetAppDoc. Senden Sie Feedback zu Dokumentation, indem Sie ein "GitHub-Autor" Oder senden Sie eine E-Mail an doccomments@netapp.com.

# Was ist in dieser Version von Astra Control Center

Wir freuen uns, die Veröffentlichung des Astra Control Center ankündigen zu können.

### August 5 2021 (21.08)

Erste Version des Astra Control Center.

- "Was ist das"
- "Verstehen von Architektur und Komponenten"
- "Was Sie benötigen, um zu beginnen"
- "Installieren" Und "Einrichtung"
- "Managen" Und "Sichern" Anwendungen
- "Buckets verwalten" Und "Storage-Back-Ends"
- "Konten verwalten"
- "Automatisierung mit API"

### Weitere Informationen

- "Bekannte Probleme in diesem Release"
- "Bekannte Einschränkungen für diese Version"

# Bekannte Probleme in dieser Version

Bekannte Probleme identifizieren Probleme, die Sie daran hindern könnten, diese Produktversion erfolgreich zu verwenden.

Die folgenden bekannten Probleme wirken sich auf die aktuelle Version aus:

- die von Astra Control Center CRD während der Installation erstellt wurde
- App mit benutzerdefiniertem Label geht in den Status „entfernt“
- App-Backup kann nicht beendet werden
- die PVCs mit Dezimaleinheiten im Astra Control Center verwenden
- z. B. Änderungen am persistenten Volume

- Trident erstellt während der Wiederherstellung der App aus einem Backup ein größeres PV als das ursprüngliche PV
- Performance-Beeinträchtigung des Klons durch große persistente Volumes
- Applikationsklone können nicht mit einer bestimmten Version von PostgreSQL verwendet werden
- Anwendungsklone sind bei der Verwendung von OCP-Sicherheitskontextsensitonen (SCC) auf Servicekontoebene fehlgeschlagen.
- S3 Buckets im Astra Control Center berichten nicht über die verfügbare Kapazität
- Die Wiederverwendung von Buckets zwischen den Instanzen des Astra Control Centers verursacht Fehler
- führt dies zu Fehlern bei der Datensicherung
- Backups und Snapshots werden während der Entfernung einer Astra Control Center-Instanz nicht aufbewahrt
- Zusätzliche Backups werden im Rahmen des geplanten Backups aufbewahrt
- "Der Klonvorgang kann außer dem Standard keine anderen Buckets verwenden"
- wenn die standardmäßige kubeconfig-Datei mehr als einen Kontext enthält
- "In skalierten Umgebungen kann der ASUP tar-Bundle-Status nicht ermittelt werden"
- Bei der Deinstallation des Astra Control Center wird der Monitor-Operator POD im Managed Cluster nicht bereinigt
- Bei der Deinstallation von Astra Control Center werden die Traefik CRDs nicht bereinigt
- ASUP-Sammlung ist in einem Erzeugen oder Hochladen enthalten

## Falsche Clusterrollenbinding, die von Astra Control Center CRD während der Installation erstellt wurde

Wenden Sie den folgenden Patch auf alle Kubernetes-Cluster an, in denen die ACC-Operator-Version 21.08.65 bereitgestellt wurde. Sie sollte auch angewendet werden, wenn der ACC-Operator erneut eingesetzt wird.

So lösen Sie dieses Problem:

1. Austausch `ACC_NAMESPACE` Im Skript unten mit dem Namespace, den Sie verwendet haben "Implementieren Sie Astra Control Center".

```
cat <<EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: acc-operator-manager-rolebinding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: acc-operator-manager-role
subjects:
- kind: ServiceAccount
  name: default
  namespace: netapp-acc-operator
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:serviceaccounts:ACC_NAMESPACE
EOF
```

2. Führen Sie das Skript aus.

Der Patch entfernt die folgenden beiden Themen aus `ClusterRoleBinding: "acc-operator-manager-rolebinding"`

```
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:serviceaccounts
- apiGroup: ""
  kind: Group
  name: system:serviceaccounts
```

## App mit benutzerdefiniertem Label geht in den Status „entfernt“

Wenn Sie eine App mit einem nicht vorhandenen k8s-Label definieren, erstellt, verwaltet und entfernt die App sofort. Um dies zu vermeiden, fügen Sie das k8s-Etikett zu Pods und Ressourcen hinzu, nachdem die App vom Astra Control Center verwaltet wurde.

## App-Backup kann nicht beendet werden

Es gibt keine Möglichkeit, ein ausgelaufes Backup zu stoppen. Wenn Sie das Backup löschen müssen, warten Sie, bis es abgeschlossen ist, und befolgen Sie die Anweisungen unter "Backups löschen". Verwenden Sie zum Löschen eines fehlgeschlagenen Backups den "Astra API".

## Backup oder Klon schlägt bei Anwendungen fehl, die PVCs mit Dezimaleinheiten im Astra Control Center verwenden

Volumes, die mit Dezimaleinheiten erstellt wurden, scheitern mit dem Astra Control Center Backup- oder

Klonprozess. Siehe "knowledgebase-Artikel" Finden Sie weitere Informationen.

## Die UI des Astra Control Center zeigt nur langsam Änderungen an Applikationsressourcen, z. B. Änderungen am persistenten Volume

Nach einer Datensicherungsoperation (Klonen, Backup, Restore) und einer anschließenden Anpassung des persistenten Volumes beträgt die Verzögerung bis zu zwanzig Minuten, bevor die neue Volume-Größe in der UI angezeigt wird. Diese Verzögerung in der Benutzeroberfläche kann auch auftreten, wenn App-Ressourcen hinzugefügt oder geändert werden. In diesem Fall ist eine Datensicherung innerhalb weniger Minuten erfolgreich und Sie können mit der Management Software für das Storage-Backend die Änderung der Volume-Größe bestätigen.

## Trident erstellt während der Wiederherstellung der App aus einem Backup ein größeres PV als das ursprüngliche PV

Wenn Sie ein persistentes Volume nach der Erstellung eines Backups skalieren und dann aus diesem Backup wiederherstellen, entspricht die persistente Volume-Größe der neuen PV-Größe und nicht die Backup-Größe.

## Performance-Beeinträchtigung des Klons durch große persistente Volumes

Klone von sehr großen und verbrauchten persistenten Volumes können zeitweise langsam sein und sind vom Cluster-Zugriff auf den Objektspeicher abhängig. Wenn der Klon aufgehängt wurde und seit mehr als 30 Minuten keine Daten kopiert wurden, beendet Astra Control die Klonaktion.

## Applikationsklone können nicht mit einer bestimmten Version von PostgreSQL verwendet werden

App-Klone innerhalb desselben Clusters schlagen konsequent mit dem Bitnami PostgreSQL 11.5.0 Diagramm fehl. Um erfolgreich zu klonen, verwenden Sie eine frühere oder höhere Version des Diagramms.

## Anwendungsklone sind bei der Verwendung von OCP-Sicherheitskontextsensitonen (SCC) auf Servicekontoebene fehlgeschlagen.

Ein Applikationsklon kann fehlschlagen, wenn die ursprünglichen Einschränkungen des Sicherheitskontexts auf der Service-Account-Ebene innerhalb des Namespace auf dem OCP-Cluster konfiguriert sind. Wenn der Anwendungsklon ausfällt, wird er im Bereich Managed Applications im Astra Control Center mit dem Status angezeigt `Removed`. Siehe "knowledgebase-Artikel" Finden Sie weitere Informationen.

## S3 Buckets im Astra Control Center berichten nicht über die verfügbare Kapazität

Bevor Sie Backups oder Klonanwendungen durchführen, die von Astra Control Center gemanagt werden, sollten Sie die Bucket-Informationen im ONTAP oder StorageGRID Managementsystem prüfen.

## Die Wiederverwendung von Buckets zwischen den Instanzen des Astra Control Centers verursacht Fehler

Wenn Sie versuchen, einen Eimer, der von einer anderen oder einer früheren Installation von Astra Control Center verwendet wird, zu verwenden, wird Backup und Restore fehlschlagen. Sie müssen einen anderen Eimer verwenden oder den zuvor verwendeten Eimer vollständig reinigen. Sie können die Buckets nicht zwischen Instanzen des Astra Control Center teilen.

## Wenn Sie einen Bucket-Provider-Typ mit Zugangsdaten für einen anderen Typ auswählen, führt dies zu Fehlern bei der Datensicherung

Wenn Sie einen Bucket hinzufügen, wählen Sie den richtigen Bucket-Provider-Typ mit den Zugangsdaten aus, die für diesen Provider korrekt sind. Die UI akzeptiert beispielsweise NetApp ONTAP S3 als Typ mit StorageGRID Zugangsdaten. Dies führt jedoch dazu, dass alle künftigen Applikations-Backups und -Wiederherstellungen mit diesem Bucket fehlschlagen.

## Backups und Snapshots werden während der Entfernung einer Astra Control Center-Instanz nicht aufbewahrt

Wenn Sie über eine Evaluierungslizenz verfügen, sollten Sie Ihre Konto-ID speichern, um Datenverlust im Falle eines Ausfalls des Astra Control Center zu vermeiden, wenn Sie ASUPs nicht senden.

## Zusätzliche Backups werden im Rahmen des geplanten Backups aufbewahrt

Manchmal werden ein oder mehrere Backups im Astra Control Center über die im Backup-Zeitplan festgelegte Anzahl hinaus aufbewahrt. Diese zusätzlichen Backups sollten im Rahmen eines geplanten Backups gelöscht werden, aber nicht gelöscht werden und in einem stecken bleiben `pending` Bundesland. Um das Problem zu lösen, "Löschen erzwingen" Die zusätzlichen Backups.

## Der Klonvorgang kann außer dem Standard keine anderen Buckets verwenden

Während eines Applikations-Backups oder Applikations-Restores können Sie optional eine Bucket-ID angeben. Ein Applikationsklonvorgang verwendet jedoch immer den definierten Standard-Bucket. Es besteht keine Möglichkeit, die Buckets für einen Klon zu ändern. Wenn Sie die Kontrolle darüber haben möchten, welcher Bucket verwendet wird, können Sie entweder "Ändern Sie den Bucket-Standard" Oder machen Sie ein "Backup" Gefolgt von A "Wiederherstellen" Separat.

## Das Verwalten eines Clusters mit Astra Control Center schlägt fehl, wenn die standardmäßige kubeconfig-Datei mehr als einen Kontext enthält

Sie können ein kubeconfig nicht mit mehr als einem Cluster und Kontext darin verwenden. Siehe "knowledgebase-Artikel" Finden Sie weitere Informationen.

## In skalierten Umgebungen kann der ASUP tar-Bundle-Status nicht ermittelt werden

Während der ASUP Sammlung wird der Status des Bundles in der UI als entweder gemeldet `collecting` Oder `done`. Die Sammlung kann in großen Umgebungen bis zu einer Stunde dauern. Während des ASUP Downloads reicht die Netzwerk-Dateiübertragungsgeschwindigkeit für das Bundle möglicherweise nicht aus, und der Download kann nach 15 Minuten ohne Angabe im UI außerhalb der Zeit erfolgen. Download-Probleme hängen von der Größe des ASUP, der skalierten Cluster-Größe und ab, ob die Erfassungszeit das siebentägige Limit übersteigt.

## Bei der Deinstallation des Astra Control Center wird der Monitor-Operator POD im Managed Cluster nicht bereinigt

Wenn Sie das Management Ihrer Cluster nicht rückgängig gemacht haben, bevor Sie Astra Control Center deinstalliert haben, können Sie die Pods im netapp-Monitoring Namespace und den Namespace manuell mit den folgenden Befehlen löschen:

**Schritte**

1. Löschen `acc-monitoring` Agent:

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

Ergebnis:

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

2. Löschen Sie den Namespace:

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

Ergebnis:

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

3. Bestätigen der entfernten Ressourcen:

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

Ergebnis:

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

4. Bestätigen Sie, dass der Monitoring Agent entfernt wurde:

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

Beispielergebnis:

```
agents.monitoring.netapp.com                    2021-07-21T06:08:13Z
```

5. Informationen zur benutzerdefinierten Ressourcendefinition löschen:

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

Ergebnis:

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

## Bei der Deinstallation von Astra Control Center werden die Traefik CRDs nicht bereinigt

Sie können die Traefik-CRDs manuell löschen:

**Schritte**

1. Bestätigen Sie, welche CRDs beim Deinstallationsprozess nicht gelöscht wurden:

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

Antwort

```
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. Löschen Sie die CRDs:

```
kubectl delete crd 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
```

## ASUP-Sammlung ist in einem Erzeugen oder Hochladen enthalten

Wenn ein ASUP POD abgebrochen oder neu gestartet wird, kann eine ASUP Sammlung in einem Erzeugungs- oder Upload-Status stecken. Führen Sie Folgendes durch "Astra Control REST-API" Aufruf zum erneuten Starten der manuellen Erfassung:

| HTTP-Methode | Pfad |
|---|---|
| POST | /Accounts/{AccountID}/Core/v1/asups |

Diese API-Problemumgehung funktioniert nur, wenn sie mehr als 10 Minuten nach Start von ASUP durchgeführt hat.

### Weitere Informationen

- "Bekannte Einschränkungen für diese Version"

# Bekannte Einschränkungen in dieser Version

Bekannte Einschränkungen identifizieren Plattformen, Geräte oder Funktionen, die von dieser Version des Produkts nicht unterstützt werden oder nicht korrekt mit dem Produkt zusammenarbeiten. Lesen Sie diese Einschränkungen sorgfältig durch.

## Derselbe Cluster kann nicht von zwei Astra Control Center Instanzen gemanagt werden

Wenn Sie ein Cluster auf einer anderen Astra Control Center-Instanz verwalten möchten, sollten Sie zuerst "Heben Sie das Management des Clusters ab" Von der Instanz, auf der sie verwaltet wird, bevor Sie sie auf einer anderen Instanz verwalten. Nachdem Sie das Cluster aus dem Management entfernt haben, überprüfen Sie, ob das Cluster mit dem folgenden Befehl nicht gemanagt wird:

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

Es sollten keine Pods in diesem Namespace laufen oder der Namespace nicht existieren sollte. Wenn einer dieser beiden Optionen true ist, wird das Cluster nicht gemanagt.

## Das Cluster befindet sich in `removed` Status, obwohl Cluster und Netzwerk ordnungsgemäß funktionieren

Wenn ein Cluster vorhanden ist `removed` Der Zustand der Cluster- und Netzwerk-Konnektivität erscheint jedoch ordnungsgemäß (externe Versuche, mit Kubernetes-APIs erfolgreich auf das Cluster zuzugreifen, sind dennoch erfolgreich), ist das Kubeconsg, das Sie Astra Control zur Verfügung gestellt haben, möglicherweise nicht mehr gültig. Dies kann an einer Zertifikatrotation oder einem Ablaufdatum im Cluster liegen. Um dieses Problem zu beheben, aktualisieren Sie die Anmeldeinformationen, die mit dem Cluster in Astra Control verbunden sind, mithilfe des "Astra Control API":

1. Führen Sie einen POST-Anruf aus, um dem eine aktualisierte kubeconfy-Datei hinzuzufügen `/credentials` endpunkt und Abrufen der zugewiesenen Daten `id` Aus dem Antwortkörper.
2. Führen Sie einen PUT-Anruf aus dem aus `/clusters` endpunkt mithilfe der entsprechenden Cluster-ID und Festlegen des `credentialID` Bis zum `id` Wert aus dem vorherigen Schritt.

Nachdem Sie diese Schritte ausgeführt haben, werden die mit dem Cluster verknüpften Anmeldeinformationen aktualisiert, und das Cluster sollte die Verbindung wiederherstellen und seinen Status auf aktualisieren `available`.

## Vom Betreiber bereitgestellte Apps mit OLM-Enabled und Cluster-Scoped werden nicht unterstützt

Astra Control Center unterstützt keine Apps, die mit OLM-fähigen Operatoren (Operator Lifecycle Manager)

oder Operatoren mit Cluster-Umfang bereitgestellt werden.

## Das Klonen von Apps kann nur mit derselben K8s-Distribution erfolgen

Wenn Sie eine Applikation zwischen Clustern klonen, müssen die Quell- und Ziel-Cluster dieselbe Verteilung von Kubernetes aufweisen. Wenn Sie beispielsweise eine App aus einem OpenShift 4.7-Cluster klonen, verwenden Sie ein Ziel-Cluster, das auch OpenShift 4.7 ist.

## OpenShift 4.8 wird nicht unterstützt

OpenShift 4.8 wird für die Juli-Version von Astra Control Center nicht unterstützt. Weitere Informationen finden Sie unter "Anforderungen des Astra Control Centers".

## Mit Helm 2 implementierte Apps werden nicht unterstützt

Wenn Sie Helm zur Implementierung von Apps verwenden, erfordert Astra Control Center Helm Version 3. Das Management und Klonen von mit Helm 3 bereitgestellten Apps (oder ein Upgrade von Helm 2 auf Helm 3) werden vollständig unterstützt. Weitere Informationen finden Sie unter "Anforderungen des Astra Control Centers".

## Astra Control Center überprüft nicht die von Ihnen eingegebenen Details für Ihren Proxy-Server

Stellen Sie sicher, dass Sie "Geben Sie die richtigen Werte ein" Beim Herstellen einer Verbindung.

## Datensicherung für Astra Control Center als App ist noch nicht verfügbar

Diese Version unterstützt nicht die Möglichkeit, Astra als Applikation mithilfe von Snapshot-, Backup- oder Restore-Optionen zu managen.

## Ungesunde Pods wirken sich auf das App-Management aus

Wenn eine gemanagte App Pods in einem ungesunden Zustand aufweist, kann Astra Control keine neuen Backups und Klone erstellen.

## Bestehende Verbindungen zu einem Postgres-Pod führen zu Fehlern

Wenn Sie Vorgänge auf Postgres-Pods durchführen, sollten Sie nicht direkt innerhalb des Pods verbinden, um den psql-Befehl zu verwenden. Astra Control erfordert psql-Zugriff, um die Datenbanken einzufrieren und zu tauen. Wenn eine bereits vorhandene Verbindung besteht, schlägt der Snapshot, die Sicherung oder der Klon fehl.

## Trident wird nicht von einem Cluster deinstalliert

Wenn Sie ein Cluster aus Astra Control Center deinstallieren, wird Trident nicht automatisch aus dem Cluster deinstalliert. Um Trident zu deinstallieren, müssen Sie es benötigen "Befolgen Sie die folgenden Schritte in der Trident-Dokumentation".

## Weitere Informationen

- "Bekannte Probleme in diesem Release"