



## **Versionshinweise**

### **Astra Control Center**

NetApp  
August 11, 2025

This PDF was generated from <https://docs.netapp.com/de-de/astra-control-center/release-notes/whats-new.html> on August 11, 2025. Always check docs.netapp.com for the latest.

# Inhalt

Versionshinweise	1
Neuerungen in dieser Version des Astra Control Center	1
15. März 2024 (24.02.0)	1
7. November 2023 (23.10.0)	1
31. Juli 2023 (23.07.0)	3
18. Mai 2023 (23.04.2)	3
25. April 2023 (23.04.0)	3
22. November 2022 (22.11.0)	4
8. September 2022 (22.08.1)	4
August 10 2022 (22.08.0)	4
26. April 2022 (22.04.0)	4
Bis 14. Dezember 2021 (21.12)	5
August 5 2021 (21.08)	5
Weitere Informationen	5
Bekannte Probleme	6
App-Backups und Snapshots schlagen fehl, wenn die Volume-Snapshot-Klasse nach dem Management eines Clusters hinzugefügt wird	6
Das Verwalten eines Clusters mit Astra Control Center schlägt fehl, wenn die Datei kubeconfig mehr als einen Kontext enthält	6
Das Management der App-Daten schlägt mit Fehler des internen Service (500) fehl, wenn Astra Trident offline ist	6
Die Wiederherstellung aus einem Backup bei Verwendung der Kerberos-Verschlüsselung während der Übertragung kann fehlschlagen	6
Backup-Daten bleiben nach dem Löschen von Buckets mit abgelaufener Aufbewahrungsrichtlinie im Bucket erhalten	7
Weitere Informationen	7
Bekannte Einschränkungen	7
Derselbe Cluster kann nicht von zwei Astra Control Center Instanzen gemanagt werden	8
Astra Control Center kann nicht zwei identisch benannte Cluster managen	8
Benutzer mit rollenbasierten Bedingungen für die Namespace-Zugriffssteuerung können ein Cluster hinzufügen und aus dem Management wieder aufheben	9
Ein Mitglied mit Namespace-Einschränkungen kann nicht auf die geklonten oder wiederhergestellten Apps zugreifen, bis der Administrator den Namespace zu der Bedingung hinzufügt	9
Restriktive Rolleneinschränkungen können für Ressourcen auf Clustern ohne Konnektor ignoriert werden	9
Mehrere Applikationen in einem einzelnen Namespace können nicht zusammen in einem anderen Namespace wiederhergestellt werden	10
Astra Control unterstützt nicht Apps, die mehrere Storage-Klassen pro Namespace verwenden	10
Astra Control weist nicht automatisch Standard-Buckets für Cloud-Instanzen zu	10
Klone von über Benutzer mit Pass-by-Reference installierten Applikationen können fehlschlagen	10
In-Place-Wiederherstellungsvorgänge von Anwendungen, die einen Zertifikatmanager verwenden, werden nicht unterstützt	11
Vom Betreiber bereitgestellte Apps mit OLM-Enabled und Cluster-Scoped werden nicht unterstützt	11

Mit Helm 2 implementierte Apps werden nicht unterstützt .....	11
Snapshots fehlschlagen bei Clustern mit Kubernetes 1.25 oder höher bei bestimmten Snapshot-Controller-Versionen möglicherweise .....	11
Backups und Snapshots werden während der Entfernung einer Astra Control Center-Instanz nicht aufbewahrt .....	11
Vorgänge zur Wiederherstellung nach ontap-nas-Economy-Storage-Klassen schlagen fehl .....	11
Einschränkungen für LDAP-Benutzer und -Gruppen .....	12
S3 Buckets im Astra Control Center berichten nicht über die verfügbare Kapazität .....	12
Astra Control Center überprüft nicht die von Ihnen eingegebenen Details für Ihren Proxy-Server .....	12
Bestehende Verbindungen zu einem Postgres-Pod führen zu Fehlern .....	12
Auf der Seite „Aktivität“ werden bis zu 100000 Ereignisse angezeigt .....	12
SnapMirror unterstützt keine Applikationen, die NVMe over TCP für Storage-Back-Ends verwenden ...	12
Weitere Informationen .....	12

# Versionshinweise

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

- ["In dieser Version des Astra Control Center"](#)
- ["Bekannte Probleme"](#)
- ["Bekannte Einschränkungen"](#)

Senden Sie Feedback zu Dokumentation, indem Sie ein ["GitHub-Autor"](#) Oder senden Sie eine E-Mail an [doccomments@netapp.com](mailto:doccomments@netapp.com).

## Neuerungen in dieser Version des Astra Control Center

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

### 15. März 2024 (24.02.0)

#### Neue Funktionen und Support

- **Versetzen Sie Astra Control Center ohne private Registrierung:** Sie müssen Astra Control Center-Images nicht mehr in eine private Registrierung verschieben oder als Teil Ihrer Astra Control-Umgebung verwenden.
- \* Kleine Fehlerbehebungen \*

#### Bekannte Probleme und Einschränkungen

- ["Bekannte Probleme in diesem Release"](#)
- ["Bekannte Einschränkungen für diese Version"](#)

#### (Tech Preview) erklärende Kubernetes-Workflows

Diese Version von Astra Control Center enthält deklarative Kubernetes-Funktionen, mit denen Sie das Datenmanagement von einer nativen benutzerdefinierten Kubernetes-Ressource (Custom Resource, CR) aus durchführen können.

Nachdem Sie den installiert haben ["Astra Connector"](#) Auf dem Cluster, das Sie verwalten möchten, können Sie die folgenden CR-basierten Clustervorgänge in der Benutzeroberfläche oder von einem CR-System aus durchführen:

- ["Definieren Sie eine Anwendung mithilfe einer benutzerdefinierten Ressource"](#)
- ["Definieren Sie den Bucket"](#)
- ["Schützen Sie ein gesamtes Cluster"](#)
- ["Sichern Sie Ihre Anwendung"](#)
- ["Erstellen Sie einen Snapshot"](#)
- ["Erstellen Sie Zeitpläne für Snapshots oder Backups"](#)
- ["Stellen Sie eine Anwendung aus einem Snapshot oder einem Backup wieder her"](#)

### 7. November 2023 (23.10.0)

#### Neue Funktionen und Support

- **Backup- und Restore-Funktionen für Applikationen mit ontap-nas-Economy Treiber-Backends:**  
Aktivieren Sie Backup- und Restore-Vorgänge für ontap-nas-economy Mit einigen ["Einfache Schritte"](#).
- **Unveränderliche Backups:** Astra Control unterstützt jetzt ["Unveränderbare, schreibgeschützte Backups"](#)  
Als zusätzliche Sicherheitsschicht gegen Malware und andere Bedrohungen.
- **Neu: Astra Control Provisioner**

In der Version 23.10 hat Astra Control eine neue Software-Komponente namens Astra Control Provisioner eingeführt, die für alle lizenzierten Astra Control Benutzer verfügbar sein wird. Mit Astra Control Provisioner erhalten Sie Zugriff auf umfassende Funktionen für erweitertes Management und Storage-Bereitstellung, die über den Funktionsumfang von Astra Trident hinausgehen. Diese Funktionen sind für alle Astra Control Kunden ohne zusätzliche Kosten verfügbar.

- **Erste Schritte mit Astra Control Provisioner**

Das können Sie ["Astra Control Provisioner aktivieren"](#) Falls Sie Ihre Umgebung installiert und konfiguriert haben, um Astra Trident 23.10 zu verwenden.

- **Astra Control Provisioner-Funktionalität**

Die Version 23.10 von Astra Control Provisioner bietet folgende Funktionen:

- **Verbesserte Sicherheit des Speicher-Backends mit Kerberos 5-Verschlüsselung:** Sie können die Speichersicherheit durch verbessern ["Aktivieren der Verschlüsselung"](#) Für den Datenverkehr zwischen dem gemanagten Cluster und dem Storage-Backend. Astra Control Provisioner unterstützt Kerberos-5-Verschlüsselung über NFSv4.1-Verbindungen von Red hat OpenShift-Clustern zu Azure NetApp Files und lokalen ONTAP Volumes
  - **Wiederherstellen von Daten mit einem Snapshot:** Astra Control Provisioner bietet schnelle, in-Place-Wiederherstellung von Volumes aus einem Snapshot mithilfe des TridentActionSnapshotRestore (TASR) CR.
  - **SnapMirror Verbesserungen:** Verwenden Sie die App-Replizierungsfunktion in Umgebungen, in denen Astra Control keine direkte Verbindung zu einem ONTAP-Cluster hat oder auf ONTAP-Anmeldedaten zugreifen kann. Mit dieser Funktion können Sie Replizierung verwenden, ohne ein Storage-Back-End oder dessen Anmeldedaten in Astra Control verwalten zu müssen.
  - **Sicherungs- und Wiederherstellungsfunktionen für Anwendungen mit ontap-nas-economy Treiber-Backends:** Wie beschrieben [Oben](#).
- **Unterstützung für die Verwaltung von Anwendungen, die NVMe/TCP-Speicher verwenden**  
Astra Control kann jetzt Applikationen managen, die von persistenten Volumes unterstützt werden, die über NVMe/TCP verbunden sind.
  - **Ausführungs-Hooks standardmäßig ausgeschaltet:** Ab diesem Release können Ausführungshaken-Funktionen sein ["Aktiviert"](#) Oder deaktiviert für zusätzliche Sicherheit (standardmäßig deaktiviert). Wenn Sie noch keine Ausführungshaken für die Verwendung mit Astra Control erstellt haben, müssen Sie dies tun ["Aktivieren Sie die Funktion „Ausführungshaken“"](#) Um mit dem Erstellen von Hooks zu beginnen. Wenn Sie vor diesem Release Testsuitehaoks erstellt haben, bleibt die Funktionalität „Ausführungshaken“ aktiviert und Sie können Hooks wie gewohnt verwenden.

## Bekannte Probleme und Einschränkungen

- ["Bekannte Probleme in diesem Release"](#)
- ["Bekannte Einschränkungen für diese Version"](#)

## 31. Juli 2023 (23.07.0)

### Neue Funktionen und Support

- "Unterstützung für den Einsatz von NetApp MetroCluster in einer Stretch-Konfiguration als Storage Backend"
- "Unterstützung von Longhorn als Storage-Backend"
- "Applikationen können jetzt zwischen ONTAP-Back-Ends aus demselben Kubernetes-Cluster repliziert werden"
- "Astra Control Center unterstützt jetzt „userPrincipalName“ als alternatives Login-Attribut für Remote-Benutzer (LDAP)"
- "Der neue Ausführungs-Hook-Typ 'Post-Failover' kann nach dem Replikations-Failover mit Astra Control Center ausgeführt werden"
- Klon-Workflows unterstützen jetzt nur Live-Klone (der aktuelle Status der gemanagten Applikation). Um aus einem Snapshot oder Backup zu klonen, verwenden Sie den ["Wiederherstellen des Workflows"](#).

### Bekannte Probleme und Einschränkungen

- ["Bekannte Probleme in diesem Release"](#)
- ["Bekannte Einschränkungen für diese Version"](#)

## 18. Mai 2023 (23.04.2)

Dieses Patch-Release (23.04.2) für Astra Control Center (23.04.0) bietet Unterstützung für ["Externer Kubernetes CSI-Snapshot v6.1.0"](#) Und behebt Folgendes:

- Ein Fehler bei der Wiederherstellung von Anwendungen vor Ort, wenn Ausführungshaken verwendet werden
- Verbindungsprobleme mit dem Bucket-Service

## 25. April 2023 (23.04.0)

### Neue Funktionen und Support

- "Bei neuen Astra Control Center-Installationen ist eine 90-Tage-Evaluierungslizenz standardmäßig aktiviert"
- "Verbesserte Funktionalität der Testsuitehasen mit zusätzlichen Filteroptionen"
- "Ausführungs-Hooks können jetzt nach dem Replizierungs-Failover mit Astra Control Center ausgeführt werden"
- "Unterstützung bei der Migration von Volumes aus der Klasse „ontap-nas-Economy“ in die Storage-Klasse „ontap-nas“"
- "Unterstützung für das ein- oder Ausschließen von Anwendungsressourcen während der Wiederherstellung"
- "Unterstützung für das Management von rein datenbasierten Applikationen"

### Bekannte Probleme und Einschränkungen

- ["Bekannte Probleme in diesem Release"](#)
- ["Bekannte Einschränkungen für diese Version"](#)

## 22. November 2022 (22.11.0)

### Neue Funktionen und Support

- "Unterstützung von Applikationen, die mehrere Namespaces umfassen"
- "Unterstützung, um Cluster-Ressourcen in eine Applikationsdefinition zu enthalten"
- "Erweiterte LDAP-Authentifizierung mit rollenbasierter Integration der Zugriffssteuerung (Role Based Access Control, RBAC)"
- "Zusätzliche Unterstützung für Kubernetes 1.25 und Pod Security Admission (PSA)"
- "Verbesserte Fortschrittsberichte für Backup-, Restore- und Klonvorgänge"

### Bekannte Probleme und Einschränkungen

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

## 8. September 2022 (22.08.1)

Dieses Patch-Release (22.08.1) für Astra Control Center (22.08.0) behebt kleinere Bugs bei der App-Replikation mit NetApp SnapMirror.

## August 10 2022 (22.08.0)

### Neue Funktionen und Support

- "Applikationsreplizierung mit NetApp SnapMirror Technologie"
- "Verbesserter Applikations-Management-Workflow"
- "Verbesserte Funktionalität für Ihre eigenen Testsuiten"



Von NetApp wurden in dieser Version standardmäßige Pre- und Post-Snapshot-Testbügel für spezifische Applikationen entfernt. Wenn Sie ein Upgrade auf diese Version durchführen und keine eigenen Testsuiten für Snapshots bereitstellen, führt Astra Control nur absturzkonsistente Snapshots durch. Besuchen Sie das "[NetApp Verda](#)" GitHub-Repository für Hook-Beispielskripts, die Sie an Ihre Umgebung anpassen können.

- "Unterstützung von VMware Tanzu Kubernetes Grid Integrated Edition (TKGI)"
- "Unterstützung für Google Anthos"
- "LDAP-Konfiguration (über Astra Control API)"

### Bekannte Probleme und Einschränkungen

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

## 26. April 2022 (22.04.0)

### Neue Funktionen und Support

- "Rollenbasierte Zugriffssteuerung (Namespace)"
- "Unterstützung von Cloud Volumes ONTAP"
- "Generisches Ingress-Enablement für Astra Control Center"

- ["Eimer Entfernung aus Astra Control"](#)
- ["Unterstützung für VMware Tanzu Portfolio"](#)

#### **Bekannte Probleme und Einschränkungen**

- ["Bekannte Probleme in diesem Release"](#)
- ["Bekannte Einschränkungen für diese Version"](#)

### **Bis 14. Dezember 2021 (21.12)**

#### **Neue Funktionen und Support**

- ["Applikationswiederherstellung"](#)
- ["Ausführungshaken"](#)
- ["Unterstützung für Applikationen, die mit Betreibern im Namespace-Umfang implementiert wurden"](#)
- ["Zusätzliche Unterstützung für Upstream Kubernetes und Rancher"](#)
- ["Astra Control Center-Upgrades"](#)
- ["Red hat OperatorHub-Option zur Installation"](#)

#### **Behobene Probleme**

- ["Probleme in diesem Release wurden behoben"](#)

#### **Bekannte Probleme und Einschränkungen**

- ["Bekannte Probleme in diesem Release"](#)
- ["Bekannte Einschränkungen für diese Version"](#)

### **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"](#)
- ["Frühere Versionen der Astra Control Center-Dokumentation"](#)



# Bekannte Probleme

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:

- wenn die Volume-Snapshot-Klasse nach dem Management eines Clusters hinzugefügt wird
- wenn die Datei kubeconfig mehr als einen Kontext enthält
- wenn Astra Trident offline ist
- Die Wiederherstellung aus einem Backup bei Verwendung der Kerberos-Verschlüsselung während der Übertragung kann fehlschlagen
- Backup-Daten bleiben nach dem Löschen von Buckets mit abgelaufener Aufbewahrungsrichtlinie im Bucket erhalten

## App-Backups und Snapshots schlagen fehl, wenn die Volume-Snapshot-Klasse nach dem Management eines Clusters hinzugefügt wird

Backups und Snapshots schlagen fehl UI 500 error In diesem Szenario. Aktualisieren Sie die App-Liste als Workaround.

## Das Verwalten eines Clusters mit Astra Control Center schlägt fehl, wenn die Datei kubeconfig 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.

## Das Management der App-Daten schlägt mit Fehler des internen Service (500) fehl, wenn Astra Trident offline ist

Wenn Astra Trident auf einem App-Cluster offline geschaltet wird (und wieder online geschaltet wird) und 500 interne Servicefehler auftreten, wenn versucht wird, das App-Datenmanagement zu managen, starten Sie alle Kubernetes-Nodes im App-Cluster neu, um die Funktionalität wiederherzustellen.

## Die Wiederherstellung aus einem Backup bei Verwendung der Kerberos-Verschlüsselung während der Übertragung kann fehlschlagen

Wenn Sie eine Anwendung von einem Backup auf einem Speicher-Back-End wiederherstellen, das Kerberos in-Flight-Verschlüsselung verwendet, kann der Wiederherstellungsvorgang fehlschlagen. Dieses Problem hat keine Auswirkung auf die Wiederherstellung von einem Snapshot oder die Replizierung der Applikationsdaten mit NetApp SnapMirror.



Wenn Sie Kerberos-Verschlüsselung während der Übertragung mit NFSv4-Volumes verwenden, stellen Sie sicher, dass die NFSv4-Volumes die richtigen Einstellungen verwenden. Weitere Informationen finden Sie im Abschnitt NetApp NFSv4-Domänenkonfiguration (Seite 13) des ["NetApp Leitfaden zu NFSv4-Verbesserungen und Best Practices"](#).

## Backup-Daten bleiben nach dem Löschen von Buckets mit abgelaufener Aufbewahrungsrichtlinie im Bucket erhalten

Wenn Sie das unveränderliche Backup einer App löschen, nachdem die Aufbewahrungsrichtlinie für den Bucket abgelaufen ist, wird das Backup aus Astra Control gelöscht, nicht jedoch aus dem Bucket. Dieses Problem wird in einer kommenden Version behoben.

### Weitere Informationen

- ["Bekannte Einschränkungen"](#)

## Bekannte Einschränkungen

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.

### Einschränkungen beim Cluster-Management

- [Derselbe Cluster kann nicht von zwei Astra Control Center Instanzen gemanagt werden](#)
- [Astra Control Center kann nicht zwei identisch benannte Cluster managen](#)

### Einschränkungen bei der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC)

- [Benutzer mit rollenbasierten Bedingungen für die Namespace-Zugriffssteuerung können ein Cluster hinzufügen und aus dem Management wieder aufheben](#)
- [bis der Administrator den Namespace zu der Bedingung hinzufügt](#)
- [Restriktive Rolleneinschränkungen können für Ressourcen auf Clustern ohne Konnektor ignoriert werden](#)

### Einschränkungen beim Applikationsmanagement

- [Mehrere Applikationen in einem einzelnen Namespace können nicht zusammen in einem anderen Namespace wiederhergestellt werden](#)
- [die mehrere Storage-Klassen pro Namespace verwenden](#)
- [Astra Control weist nicht automatisch Standard-Buckets für Cloud-Instanzen zu](#)
- [Klone von über Benutzer mit Pass-by-Reference installierten Applikationen können fehlschlagen](#)
- [die einen Zertifikatmanager verwenden, werden nicht unterstützt](#)
- [Vom Betreiber bereitgestellte Apps mit OLM-Enabled und Cluster-Scoped werden nicht unterstützt](#)
- [Mit Helm 2 implementierte Apps werden nicht unterstützt](#)
- [Snapshots fehlschlagen bei Clustern mit Kubernetes 1.25 oder höher bei bestimmten Snapshot-Controller-Versionen möglicherweise](#)
- [Backups und Snapshots werden während der Entfernung einer Astra Control Center-Instanz nicht aufbewahrt](#)
- [Vorgänge zur Wiederherstellung nach ontap-nas-Economy-Storage-Klassen schlagen fehl](#)

### Allgemeine Einschränkungen

- [Einschränkungen für LDAP-Benutzer und -Gruppen](#)
- [S3 Buckets im Astra Control Center berichten nicht über die verfügbare Kapazität](#)

- [Astra Control Center überprüft nicht die von Ihnen eingegebenen Details für Ihren Proxy-Server](#)
- [Bestehende Verbindungen zu einem Postgres-Pod führen zu Fehlern](#)
- [Auf der Seite „Aktivität“ werden bis zu 100000 Ereignisse angezeigt](#)
- [die NVMe over TCP für Storage-Back-Ends verwenden](#)

## 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.

## Astra Control Center kann nicht zwei identisch benannte Cluster managen

Wenn Sie versuchen, einen Cluster mit demselben Namen wie ein bereits vorhandener Cluster hinzuzufügen, schlägt der Vorgang fehl. Dieses Problem tritt meist in einer Standard-Kubernetes-Umgebung auf, wenn in den Kubernetes-Konfigurationsdateien der Standardwert für den Cluster-Namen nicht geändert wurde.

Führen Sie als Workaround folgende Schritte aus:

1. Bearbeiten Sie das `kubeadm-config` Konfigmap:

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

2. Ändern Sie das `clusterName` Feldwert von `kubernetes` (Der Kubernetes-Standardname) wird einem eindeutigen benutzerdefinierten Namen verwendet.
3. Kubeconfig bearbeiten (`.kube/config`).
4. Aktualisieren des Cluster-Namens von `kubernetes` Zu einem eindeutigen benutzerdefinierten Namen (`xyz-cluster` Wird in den folgenden Beispielen verwendet). Machen Sie das Update in beiden `clusters` Und `contexts` Abschnitte wie in diesem Beispiel dargestellt:

```

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

```

## Benutzer mit rollenbasierten Bedingungen für die Namespace-Zugriffssteuerung können ein Cluster hinzufügen und aus dem Management wieder aufheben

Benutzer mit rollenbasierten Namespace-Einschränkungen dürfen Cluster nicht hinzufügen oder aus dem Management rückgängig machen. Aufgrund der derzeitigen Beschränkungen verhindert Astra nicht, dass solche Benutzer Cluster nicht mehr verwalten.

## Ein Mitglied mit Namespace-Einschränkungen kann nicht auf die geklonten oder wiederhergestellten Apps zugreifen, bis der Administrator den Namespace zu der Bedingung hinzufügt

Alle member Benutzer mit rollenbasierter Zugriffssteuerung nach Namespace-Name/ID können eine Applikation in einem neuen Namespace im selben Cluster oder einem anderen Cluster im Konto des Unternehmens klonen oder wiederherstellen. Derselbe Benutzer kann jedoch nicht auf die geklonte oder wiederhergestellte Anwendung im neuen Namespace zugreifen. Nachdem durch einen Klon- oder Wiederherstellungsvorgang ein neuer Namespace erstellt wurde, kann der Kontoadministrator/Kontoinhaber den bearbeiten member Benutzerkonto und Aktualisierung von Rollenbeschränkungen für den betroffenen Benutzer, um den Zugriff auf den neuen Namespace zu gewähren.

## Restriktive Rolleneinschränkungen können für Ressourcen auf Clustern ohne Konnektor ignoriert werden

- **Wenn die Ressourcen, auf die zugegriffen wird, zu Clustern gehören, auf denen der neueste Astra Connector installiert ist:** Wenn einem Benutzer über eine LDAP-Gruppenmitgliedschaft mehrere Rollen zugewiesen werden, werden die Einschränkungen der Rollen kombiniert. Wenn beispielsweise ein Benutzer mit einer lokalen Viewer-Rolle drei Gruppen Beitritt, die an die Mitgliedrolle gebunden sind, hat der Benutzer jetzt Zugriff auf die Viewer-Rolle auf die ursprünglichen Ressourcen sowie auf die Mitgliederrolle, die durch die Gruppenmitgliedschaft gewonnen wird.
- **Wenn die Ressourcen, auf die zugegriffen wird, zu Clustern gehören, auf denen kein Astra Connector installiert ist:** Wenn einem Benutzer mehrere Rollen über eine LDAP-Gruppenmitgliedschaft zugewiesen werden, sind die Einschränkungen der freizügigsten Rolle die einzigen, die wirksam werden.

## Mehrere Applikationen in einem einzelnen Namespace können nicht zusammen in einem anderen Namespace wiederhergestellt werden

Wenn Sie mehrere Applikationen in einem einzigen Namespace managen (durch das Erstellen mehrerer App-Definitionen in Astra Control), können Sie nicht alle Applikationen auf einem anderen Single Namespace wiederherstellen. Jede Applikation muss ihrem eigenen separaten Namespace wiederhergestellt werden.

## Astra Control unterstützt nicht Apps, die mehrere Storage-Klassen pro Namespace verwenden

Astra Control unterstützt Applikationen, die eine einzelne Storage-Klasse pro Namespace verwenden. Wenn Sie eine App zu einem Namespace hinzufügen, stellen Sie sicher, dass die App dieselbe Storage-Klasse wie andere Apps im Namespace hat.

## Astra Control weist nicht automatisch Standard-Buckets für Cloud-Instanzen zu

Astra Control weist keinem Cloud-Instanz automatisch einen Standard-Bucket zu. Sie müssen manuell einen Standard-Bucket für eine Cloud-Instanz festlegen. Wenn kein Standard-Bucket festgelegt ist, können Sie keine App-Klonvorgänge zwischen zwei Clustern durchführen.

## Klone von über Benutzer mit Pass-by-Reference installierten Applikationen können fehlschlagen

Astra Control unterstützt Applikationen, die mit Betreibern im Namespace-Umfang installiert sind. Diese Betreiber sind in der Regel mit einer "Pass-by-Value"-Architektur statt "Pass-by-reference"-Architektur ausgelegt. Im Folgenden sind einige Bedieneranwendungen aufgeführt, die folgende Muster befolgen:

- ["Apache K8ssandra"](#)



Für K8ssandra werden in-Place-Wiederherstellungsvorgänge unterstützt. Für einen Restore-Vorgang in einem neuen Namespace oder Cluster muss die ursprüngliche Instanz der Applikation ausgefallen sein. Dadurch soll sichergestellt werden, dass die überführten Peer-Group-Informationen nicht zu einer instanzübergreifenden Kommunikation führen. Das Klonen der App wird nicht unterstützt.

- ["Jenkins CI"](#)
- ["Percona XtraDB Cluster"](#)

Astra Control kann einen Operator, der mit einer „Pass-by-reference“-Architektur entworfen wurde, möglicherweise nicht klonen (z.B. der CockroachDB-Operator). Während dieser Art von Klonvorgängen versucht der geklonte Operator, Kubernetes Secrets vom Quelloperator zu beziehen, obwohl er im Zuge des Klonens ein eigenes neues Geheimnis hat. Der Klonvorgang kann fehlschlagen, da Astra Control die Kubernetes-Geheimnisse im Quelloperator nicht kennt.



Während Klonvorgängen müssen Applikationen, die eine Ressource oder Webhooks der ProgresClass benötigen, nicht über die Ressourcen verfügen, die bereits auf dem Ziel-Cluster definiert sind.

## **In-Place-Wiederherstellungsvorgänge von Anwendungen, die einen Zertifikatmanager verwenden, werden nicht unterstützt**

Diese Version von Astra Control Center unterstützt keine in-Place-Wiederherstellung von Anwendungen mit Zertifikatmanagern. Restore-Vorgänge in einem anderen Namespace und Klonvorgänge werden unterstützt.

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

Astra Control Center unterstützt keine Aktivitäten des Applikationsmanagements mit Operatoren mit Cluster-Umfang.

## **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 Anwendungen (oder ein Upgrade von Helm 2 auf Helm 3) wird vollständig unterstützt. Weitere Informationen finden Sie unter ["Anforderungen des Astra Control Centers"](#).

## **Snapshots fehlschlagen bei Clustern mit Kubernetes 1.25 oder höher bei bestimmten Snapshot-Controller-Versionen möglicherweise**

Snapshots für Kubernetes-Cluster, die Version 1.25 oder höher ausführen, können fehlschlagen, wenn Version v1beta1 der Snapshot-Controller-APIs auf dem Cluster installiert sind.

Führen Sie als Workaround beim Upgrade vorhandener Installationen von Kubernetes 1.25 oder höher die folgenden Schritte aus:

1. Entfernen Sie alle vorhandenen Snapshot CRDs und alle vorhandenen Snapshot Controller.
2. ["Deinstallieren Sie Astra Trident"](#).
3. ["Installieren Sie die Snapshot-CRDs und den Snapshot-Controller"](#).
4. ["Installieren Sie die neueste Version von Astra Trident"](#).
5. ["Erstellen Sie eine VolumeSnapshotClass"](#).

## **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.

## **Vorgänge zur Wiederherstellung nach ontap-nas-Economy-Storage-Klassen schlagen fehl**

Wenn Sie eine in-Place-Wiederherstellung einer Anwendung durchführen (die App in ihren ursprünglichen Namespace wiederherstellen) und die Storage-Klasse der App den verwendet `ontap-nas-economy` Treiber, der Wiederherstellungsvorgang kann fehlschlagen, wenn das Snapshot-Verzeichnis nicht ausgeblendet ist. Befolgen Sie vor der Wiederherstellung vor Ort die Anweisungen unter ["Backup und Restore für den wirtschaftlichen Betrieb von ontap-nas"](#) Um das Snapshot-Verzeichnis auszublenden.

## Einschränkungen für LDAP-Benutzer und -Gruppen

Astra Control Center unterstützt bis zu 5,000 Remote-Gruppen und 10,000 Remote-Benutzer.

Astra Control unterstützt keine LDAP-Entität (Benutzer oder Gruppe) mit einem DN, der einen RDN mit einem nachgestellten '\' oder nachgestellten Leerzeichen enthält.

## 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.

## 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.

## 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.

## Auf der Seite „Aktivität“ werden bis zu 100000 Ereignisse angezeigt

Auf der Seite Astra Control Activity können bis zu 100,000 Ereignisse angezeigt werden. Um alle protokollierten Ereignisse anzuzeigen, rufen Sie die Ereignisse mithilfe des ab ["Astra Control API"](#).

## SnapMirror unterstützt keine Applikationen, die NVMe over TCP für Storage-Back-Ends verwenden

Astra Control Center unterstützt keine NetApp SnapMirror Replizierung für Storage-Back-Ends, die das NVMe-over-TCP-Protokoll verwenden.

## Weitere Informationen

- ["Bekannte Probleme"](#)

## Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.