Versionshinweise

Astra Control Center

NetApp
November 21, 2023

Inhalt

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"

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 neu in dieser Version des Astra Control Center

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

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)

Details

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)

Details

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)

Details

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)

Details

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)

Details

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)

Details

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:

Anwendungen

- die größer ist als das ursprüngliche PV
- Applikationsklone können nicht mit einer bestimmten Version von PostgreSQL verwendet werden
- Anwendungsklone sind bei der Verwendung von OCP-Sicherheitskontextsensitonen (SCC) auf Servicekontoebene fehlgeschlagen.
- nachdem eine Applikation mit einer festgelegten Storage-Klasse implementiert wurde
- wenn die Volume-Snapshot-Klasse nach dem Management eines Clusters hinzugefügt wird

Cluster

- wenn die standardmäßige kubeconfig-Datei mehr als einen Kontext enthält
- Einige Pods können nach dem Upgrade auf Astra Control Center 23.04 nicht gestartet werden
- Einige Pods zeigen nach der Phase des Upgrades von 23.04 auf 23.04.2 einen Fehlerstatus
- Ein Monitoring-Pod kann in Istio Umgebungen zum Absturz kommen

Andere Probleme

- wenn die Verbindung über einen Proxy hergestellt wird
- wenn Astra Trident offline ist

Die Wiederherstellung einer App führt zu einer PV-Größe, die größer ist als das ursprüngliche PV

Wenn Sie ein persistentes Volume nach der Erstellung eines Backups skalieren und dann aus diesem Backup wiederherstellen, wird die Größe des persistenten Volumes an die neue PV-Größe angepasst, anstatt die Backup-Größe zu verwenden.

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-Kontoebene im Namespace im Cluster der OpenShift Container Platform 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.

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.

Applikationsklone scheitern, nachdem eine Applikation mit einer festgelegten Storage-Klasse implementiert wurde

Nachdem eine Applikation mit einer Storage-Klasse bereitgestellt wurde (z. B. `helm install …-set global.storageClass=netapp-cvs-perf-extreme`). Nachfolgende Klonversuche der Applikation erfordern, dass das Ziel-Cluster die ursprünglich angegebene Storage-Klasse hat.
Das Klonen einer Applikation mit einer explizit festgelegten Storage-Klasse auf ein Cluster ohne dieselbe Storage-Klasse schlägt fehl. Es gibt keine Wiederherstellungsschritte in diesem Szenario.

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.

Einige Pods können nach dem Upgrade auf Astra Control Center 23.04 nicht gestartet werden

Nach dem Upgrade auf Astra Control Center 23.04 können einige Pods möglicherweise nicht gestartet werden. Um dies zu umgehen, starten Sie die betroffenen Pods mithilfe der folgenden Schritte manuell neu:

1. Ermitteln Sie die betroffenen Pods, und ersetzen Sie <namespace> durch den aktuellen Namespace:

```
kubectl get pods -n <namespace> | grep au-pod
```

Die betroffenen Pods haben ähnliche Ergebnisse wie die folgenden:

```
pcloud-astra-control-center-au-pod-0 0/1 CreateContainerConfigError 0
13s
```

2. Starten Sie jeden betroffenen Pod neu, indem Sie <namespace> durch den aktuellen Namespace ersetzen:

```
kubectl delete pod pcloud-astra-control-center-au-pod-0 -n <namespace>
```

Einige Pods zeigen nach der Phase des Upgrades von 23.04 auf 23.04.2 einen Fehlerstatus

Nach einem Upgrade auf Astra Control Center 23.04.2 wird bei einigen Pods möglicherweise ein Fehler angezeigt
Protokolle in Bezug auf `task-service-task-purge`:

```
kubectl get all -n netapp-acc -o wide|grep purge

pod/task-service-task-purge-28282828-ab1cd     0/1     Error       0
48m     10.111.0.111   openshift-clstr-ol-07-zwlj8-worker-jhp2b   <none>
<none>
```

Dieser Fehlerstatus bedeutet, dass ein Bereinigungsschritt nicht ordnungsgemäß ausgeführt wurde. Das Upgrade auf 23.04.2 ist erfolgreich. Führen Sie den folgenden Befehl aus, um die Aufgabe zu bereinigen und den Fehlerstatus zu entfernen:

```
kubectl delete job task-service-task-purge-[system-generated task ID] -n
<netapp-acc or custom namespace>
```

Ein Monitoring-Pod kann in Istio Umgebungen zum Absturz kommen

Wenn Sie Astra Control Center mit Cloud Insights in einer Istio Umgebung koppeln, bietet die `telegraf-rs` Pod kann abstürzen. Führen Sie als Workaround die folgenden Schritte aus:

1. Suchen Sie den abgestürzten POD:

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

Sie sollten eine Ausgabe wie die folgende sehen:

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

2. Starten Sie den abgestürzten Pod neu, und ersetzen Sie ihn `<pod_name_from_output>` Mit dem Namen des betroffenen Pods:

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

Sie sollten eine Ausgabe wie die folgende sehen:

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

3. Überprüfen Sie, ob der Pod neu gestartet wurde und sich nicht im Fehlerzustand befindet:

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

Sie sollten eine Ausgabe wie die folgende sehen:

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

Verwaltete Cluster werden nicht in NetApp Cloud Insights angezeigt, wenn die Verbindung über einen Proxy hergestellt wird

Wenn Astra Control Center eine Verbindung zu NetApp Cloud Insights über einen Proxy herstellt, werden gemanagte Cluster möglicherweise nicht im Cloud Insights angezeigt. Führen Sie als Workaround die folgenden Befehle auf jedem verwalteten Cluster aus:

```
kubectl get cm telegraf-conf -o yaml -n netapp-monitoring | sed
'/\[\[outputs.http\]\]/c\    [[outputs.http]]\n    use_system_proxy =
true' | kubectl replace -f -
```

```
kubectl get cm telegraf-conf-rs -o yaml -n netapp-monitoring | sed
'/\[\[outputs.http\]\]/c\    [[outputs.http]]\n    use_system_proxy =
true' | kubectl replace -f -
```

```
kubectl get pods -n netapp-monitoring --no-headers=true | grep 'telegraf-ds\|telegraf-rs' | awk '{print $1}' | xargs kubectl delete -n netapp-monitoring pod
```

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.

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

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

Allgemeine Einschränkungen

- 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

- Backups und Snapshots werden während der Entfernung einer Astra Control Center-Instanz nicht aufbewahrt
- Einschränkungen für LDAP-Benutzer und -Gruppen
- Auf der Seite „Aktivität“ werden bis zu 100000 Ereignisse angezeigt
- Snapshots fehlschlagen bei Clustern mit Kubernetes 1.25 oder höher bei bestimmten Snapshot-Controller-Versionen möglicherweise

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 ein neuer Namespace durch einen Klon- oder Wiederherstellungsvorgang erstellt wurde, kann der Account-Administrator/-Eigentümer den bearbeiten `member` Benutzerkonto und Aktualisierung von Rollenbeschränkungen für den betroffenen Benutzer, um den Zugriff auf den neuen Namespace zu gewähren.

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".

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.

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.

Einschränkungen für LDAP-Benutzer und -Gruppen

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

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 REST-API".

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".

Weitere Informationen

- "Bekannte Probleme"