Versionshinweise

Astra Control Center

NetApp
June 06, 2024

Inhalt

Versionshinweise

Wir freuen uns, die Version 21.12 des Astra Control Center ankündigen zu können.

- "In dieser Version des Astra Control Center"
- "Behobene Probleme"
- "Bekannte Probleme"
- "Bekannte Probleme mit der Vorschau des Astra Data Stores und dieser Version des Astra Control Center"
- "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 21.12 des Astra Control Center ankündigen zu können.

Bis 14. Dezember 2021 (21.12)

Aktualisierte Version des Astra Control Center.

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 Data Store: Backend-Management und -Monitoring in der Vorschau"
- "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 Probleme mit der Vorschau des Astra Data Stores und dieser Version des Astra Control Center"
- "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"
- "Astra Data Store-Dokumentation"
- "Frühere Versionen der Astra Control Center-Dokumentation"

Behobene Probleme

Diese Probleme wurden in dieser Version des Produkts behoben.

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.

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.

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.

Falsche Cluster Role Binding, die von Astra Control Center zur individuellen Ressourcendefinition während der Installation erstellt wurde

In diesem Release ist der Patch zur Korrektur der Cluster-Rollenbindung während der Installation nicht mehr erforderlich.

ASUP-Sammlung ist in einem Erzeugen oder Hochladen enthalten

Wenn ein ASUP Pod angehalten oder neu gestartet wird, hängt möglicherweise eine ASUP Sammlung in einem Generierung- oder Upload-Status ab.

Vom Betreiber bereitgestellte Applikationen und Namespaces

Ein Operator und die von ihm verwendete App müssen denselben Namespace verwenden. Astra Control unterstützt nur eine vom Betreiber bereitgestellte Applikation pro Namespace.

Weitere Informationen

- "Bekannte Probleme"
- "Bekannte Einschränkungen"
- "Bekannte Probleme mit der Vorschau des Astra Data Stores und dieser Version des Astra Control Center"

Bekannte Probleme mit der Vorschau des Astra Data Stores und dieser Version des Astra Control Center

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

Die folgenden bekannten Probleme betreffen die Verwaltung des Astra Data Stores mit dieser aktuellen Version des Astra Control Centers:

Astra Data Store-Vorschau kann aufgrund eines Ausfalls der POD-Liess-Sonde nicht als Storage-Klasse für Astra Control Center verwendet werden

Wenn Sie versuchen, Astra Data Store Preview als Storage-Bereitstellung während einer Astra Control Center Implementierung zu verwenden, schlägt die MongoDB POD-Liveness-Sonde fehl. Das Ergebnis ist eine Implementierung, die nicht abgeschlossen wird.

Um dieses Problem zu beheben, nehmen Sie zusätzlich zu den Standard-YAML-Änderungen folgende Änderungen vor, wenn Sie das abschließen "Astra Control Center-Installationsprozess":

1. Bearbeiten Sie das "Astra Control Center Operator Deployment YAML (astra_Control_Center_Operator_Deploy.yaml)" So ändern Sie die Zeitüberschreitung für die Installation des Helm:

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

2. Bearbeiten Sie das "Astra Control Center – Datei für benutzerdefinierte Ressourcen (CR) (astra_Control_Center_min.yaml)" Und fügen Sie die hervorgehobenen zusätzlichen Werte unter hinzu `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
```

Astra Control Center zeigt das vorab-Storage-Backend für Astra Data Store in `Unknown` Bundesland

Astra Control Center zeigt das vorab-Storage-Backend für den Astra Data Store in einem `Unknown` Status auf der Seite Back Ends in der UI. In diesem Fall ist das Storage Backend tatsächlich verfügbar und kann kommuniziert werden. Eine Komponente im Speicher-Backend ist wahrscheinlich in einem ungesunden Zustand und muss wieder in einen gesunden Zustand versetzt werden, damit das Speicher-Backend als angezeigt wird `available`.

Weitere Informationen

- "Behobene Probleme"
- "Bekannte Probleme"
- "Bekannte Einschränkungen"
- "Astra Data Store-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:

- App mit benutzerdefiniertem Label geht in den Status „entfernt“
- App-Backup kann nicht beendet werden
- 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.
- 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
- "Der Klonvorgang kann außer dem Standard keine anderen Buckets verwenden"
- wenn die standardmäßige kubeconfig-Datei mehr als einen Kontext enthält
- das Management von Trident-App-Daten zu starten
- dass Skripte nach dem Snapshot nicht ausgeführt werden
- "In skalierten Umgebungen kann der ASUP tar-Bundle-Status nicht ermittelt werden"
- Snapshots beginnen schließlich beim Einsatz von External-Snapshotter Version 4.2.0 fehlschlagen
- Gleichzeitige Applikations-Wiederherstellungsvorgänge können im selben Namespace fehlschlagen
- wenn die Quellversion eine Container-Image-Registrierung verwendet, die keine Authentifizierung erfordert. Die Zielversion verwendet eine Container-Image-Registrierung, die eine Authentifizierung erfordert
- 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

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 Control API".

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, wird die Größe des persistenten Volumes an die neue PV-Größe angepasst, anstatt die Backup-Größe zu verwenden.

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.

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.

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

Wenn Sie versuchen, einen Bucket zu verwenden, der von einer anderen oder einer früheren Installation von Astra Control Center verwendet wird, werden Backup- und Restore-Vorgänge 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 aus und geben Sie die richtigen Anmeldedaten für diesen Provider ein. Beispielsweise akzeptiert die UI NetApp ONTAP S3 als Typ und akzeptiert StorageGRID-Anmeldedaten. Dies führt jedoch dazu, dass alle künftigen Applikations-Backups und -Wiederherstellungen, die diesen Bucket verwenden, 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.

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.

500 interner Servicefehler beim Versuch, das Management von Trident-App-Daten zu starten

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

Hook-Skripte für benutzerdefinierte Anwendungsausführungen haben Zeit und verursachen, dass Skripte nach dem Snapshot nicht ausgeführt werden

Wenn ein Execution Hook länger als 25 Minuten dauert, schlägt der Hook fehl und erstellt einen Ereignisprotokolleintrag mit einem Rückgabecode von „N/A“. Jeder betroffene Snapshot hat eine Zeitüberschreitung und wird als fehlgeschlagen markiert, wobei ein resultierende Eintrag im Ereignisprotokoll das Timeout angibt.

Da Testsuitehingel die Funktionalität der Anwendung, für die sie ausgeführt werden, oft reduzieren oder vollständig deaktivieren, sollten Sie immer versuchen, die Zeit zu minimieren, die Ihre benutzerdefinierten Testausführungshaken für die Ausführung benötigt.

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 Übertragungsgeschwindigkeit der Netzwerkdatei 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.

Snapshots beginnen schließlich beim Einsatz von External-Snapshotter Version 4.2.0 fehlschlagen

Wenn Sie Kubernetes Snapshot-Controller (auch bekannt als externer Snapshot) Version 4.2.0 mit Kubernetes 1.20 oder 1.21 verwenden, können Snapshots irgendwann fehlschlagen. Um dies zu verhindern, verwenden

Sie ein anderes "Unterstützte Version" Von externen Snapshots, wie Version 4.2.1, mit Kubernetes Versionen 1.20 oder 1.21.

Gleichzeitige Applikations-Wiederherstellungsvorgänge können im selben Namespace fehlschlagen

Wenn Sie versuchen, eine oder mehrere einzeln gemanagte Apps innerhalb eines Namespace gleichzeitig wiederherzustellen, können die Wiederherstellungsvorgänge nach einem langen Zeitraum fehlschlagen. Stellen Sie jede Anwendung einzeln als Workaround wieder her.

Das Upgrade schlägt fehl, wenn die Quellversion eine Container-Image-Registrierung verwendet, die keine Authentifizierung erfordert. Die Zielversion verwendet eine Container-Image-Registrierung, die eine Authentifizierung erfordert

Wenn Sie ein Astra Control Center-System aktualisieren, das eine Registrierung verwendet, die keine Authentifizierung auf eine neuere Version erfordert, die eine Registrierung verwendet, die eine Authentifizierung erfordert, schlägt das Upgrade fehl. Führen Sie als Workaround die folgenden Schritte aus:

1. Melden Sie sich bei einem Host an, der Netzwerkzugriff auf den Astra Control Center-Cluster hat.
2. Stellen Sie sicher, dass der Host über die folgende Konfiguration verfügt:
   - `kubectl` Version 1.19 oder höher ist installiert
   - Die Umgebungsvariable KUBECONFIG wird auf die Datei kubeconfigfile für den Astra Control Center-Cluster gesetzt
3. Führen Sie das folgende Skript aus:

```
namespace="<netapp-acc>"
statefulsets=("polaris-vault" "polaris-mongodb" "influxdb2" "nats"
"loki")
for ss in ${statefulsets[@]}; do
    existing=$(kubectl get -n ${namespace} statefulsets.apps ${ss} -o
jsonpath='{.spec.template.spec.imagePullSecrets}')
    if [ "${existing}" = "[{}]" ] || [ "${existing}" = "[{},{},{}]" ];
then
        kubectl patch -n ${namespace} statefulsets.apps ${ss} --type
merge --patch '{"spec": {"template": {"spec": {"imagePullSecrets":
[]}}}}'
    else
        echo "${ss} not patched"
    fi
done
```

Sie sollten eine Ausgabe wie die folgende sehen:

```
statefulset.apps/polaris-vault patched
statefulset.apps/polaris-mongodb patched
statefulset.apps/influxdb2 patched
statefulset.apps/nats patched
statefulset.apps/loki patched
```

4. Fahren Sie mit dem Upgrade fort "Upgrade-Anweisungen für das Astra Control Center".

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. CRDs sind globale Ressourcen, und das Löschen kann sich auf andere Anwendungen auf dem Cluster auswirken.

Schritte

1. Führen Sie die auf dem Cluster installierten Traefik-CRDs auf:

```
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
middlewaretcps.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
middlewaretcps.traefik.containo.us
```

Weitere Informationen

- "Behobene Probleme"
- "Bekannte Probleme bei der Prüfung des Astra Data Store und dieser Version des Astra Control Center"
- "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.

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 Cluster mit gleichen Namen in derselben Cloud managen

Wenn Sie versuchen, einen Cluster mit demselben Namen wie einen Cluster hinzuzufügen, der bereits in Ihrer Cloud vorhanden ist, 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 die Konfigurationskarte für kubeadm-config:

```
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
```

Klone von über Pass-by-Reference-Operatoren 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"
- "Jenkins CI"
- "Percona XtraDB Cluster"

Astra Control ist möglicherweise nicht in der Lage, einen Operator zu klonen, der mit einer „Pass-by-reference“-Architektur entworfen wurde (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.

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.

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.

MetalLB 0.11.0 wird nicht unterstützt

Die metalLB 0.11.0 ist kein unterstützter Load Balancer für Astra Control Center. Weitere Informationen zu unterstützten Load Balancer 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 Anwendungen (oder ein Upgrade von Helm 2 auf Helm 3) wird 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

- "Behobene Probleme"
- "Bekannte Probleme"
- "Bekannte Probleme mit der Vorschau des Astra Data Stores und dieser Version des Astra Control Center"