Dokumentation zu Astra Control Center 23.10

Astra Control Center

NetApp
August 11, 2025

Inhalt

Dokumentation zu Astra Control Center 23.10

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.

Neuerungen in dieser Version des Astra Control Center

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

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)

Details

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)

Details

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)

Details

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:

- wenn die Volume-Snapshot-Klasse nach dem Management eines Clusters hinzugefügt wird
- wenn die Datei kubeconfig mehr als einen Kontext enthält
- Ein Monitoring-Pod kann in Istio Umgebungen zum Absturz kommen
- wenn Astra Trident offline ist
- Vorgänge zur Wiederherstellung nach ontap-nas-Economy-Storage-Klassen schlagen fehl
- 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.

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
```

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.

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.

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

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

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.

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.

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"

Los geht’s

Weitere Informationen zu Astra Control

Astra Control ist eine Kubernetes-Lösung für das Lifecycle-Management von Applikationsdaten, die den Betrieb zustandsorientierte Applikationen vereinfacht. Einfacher Schutz, Backup, Replizierung und Migration von Kubernetes-Workloads und sofortige Erstellung von Applikationsklonen

Funktionen

Astra Control bietet entscheidende Funktionen für das Lifecycle Management von Kubernetes-Applikationsdaten:

- Automatisches Management von persistentem Storage
- Erstellen Sie applikationsorientierte Snapshots und Backups nach Bedarf
- Automatisierung von richtlinienbasierten Snapshot- und Backup-Vorgängen
- Migrieren Sie Applikationen und Daten von einem Kubernetes-Cluster zu einem anderen
- Replizieren von Applikationen auf ein Remote-System mit NetApp SnapMirror Technologie (Astra Control Center)
- Klonen von Applikationen von Staging hin zur Produktion
- Darstellung des Anwendungszustands und des Schutzstatus
- Verwenden Sie eine Web-Oberfläche oder eine API zur Implementierung Ihrer Backup- und Migration-Workflows

Implementierungsmodelle

Astra Control ist in zwei Implementierungsmodellen erhältlich:

- **Astra Control Service**: Ein von NetApp gemanagter Service, der applikationskonsistentes Datenmanagement von Kubernetes Clustern in Umgebungen mehrerer Cloud-Provider sowie selbst gemanagte Kubernetes Cluster bietet.
- **Astra Control Center**: Gemanagte Software für applikationsgerechtes Datenmanagement von Kubernetes-Clustern, die in Ihrer On-Premises-Umgebung ausgeführt werden. Astra Control Center kann auch in Umgebungen mit mehreren Cloud-Providern und einem NetApp Cloud Volumes ONTAP Storage-Back-End installiert werden.

	Astra Control Service	Astra Control Center
Wie wird das angeboten?	Vollständig gemanagter Cloud-Service von NetApp	Als Software, die Sie herunterladen, installieren und verwalten können
Wo wird sie gehostet?	In einer Public Cloud von NetApp ihrer Wahl	In Ihrem eigenen Kubernetes-Cluster
Wie wird sie aktualisiert?	Gemanagt von NetApp	Sie verwalten jegliche Updates

	Astra Control Service	Astra Control Center
Welche Storage-Back-Ends werden unterstützt?	• Amazon Web Services: ◦ Amazon EBS ◦ Amazon FSX für NetApp ONTAP ◦ "Cloud Volumes ONTAP" • Google Cloud: ◦ Google Persistent Disk ◦ NetApp Cloud Volumes Service ◦ "Cloud Volumes ONTAP" • Microsoft Azure: ◦ Über Azure Gemanagte Festplatten ◦ Azure NetApp Dateien ◦ "Cloud Volumes ONTAP" • Self-Managed Cluster: ◦ Amazon EBS ◦ Über Azure Gemanagte Festplatten ◦ Google Persistent Disk ◦ "Cloud Volumes ONTAP" ◦ NetApp MetroCluster ◦ "Longhorn" • Lokale Cluster: ◦ NetApp MetroCluster ◦ NetApp ONTAP AFF und FAS Systeme ◦ NetApp ONTAP Select ◦ "Cloud Volumes ONTAP" ◦ "Longhorn"	• NetApp ONTAP AFF und FAS Systeme • NetApp ONTAP Select • "Cloud Volumes ONTAP"

Funktionsweise des Astra Control Service

Astra Control Service ist ein von NetApp gemanagter Cloud-Service, der ständig verfügbar und mit den neuesten Funktionen aktualisiert ist. Verschiedene Komponenten unterstützen das Lifecycle-Management von Applikationsdaten.

Astra Control Service funktioniert auf hohem Niveau wie folgt:

- Starten Sie mit Astra Control Service, indem Sie Ihren Cloud-Provider einrichten und einen Astra Account anfordern.

    - Für GKE-Cluster verwendet der Astra Control Service "NetApp Cloud Volumes Service für Google Cloud" Oder Google Persistent Disks als Storage-Backend für Ihre persistenten Volumes.
    - Für AKS-Cluster nutzt der Astra Control Service "Azure NetApp Dateien" Oder von Azure gemanagte Festplatten als Storage-Backend für Ihre persistenten Volumes.
    - Für Amazon EKS-Cluster verwendet Astra Control Service "Amazon Elastic Block Store" Oder "Amazon FSX für NetApp ONTAP" Das Storage-Backend für Ihre persistenten Volumes
- Sie fügen Ihre ersten Kubernetes-Computing-Ressourcen in den Astra Control Service ein. Astra Control Service übernimmt dann Folgendes:
    - Erstellung eines Objektspeicher in Ihrem Cloud-Provider-Konto, an dem Backup-Kopien gespeichert werden

      In Azure erstellt Astra Control Service außerdem eine Ressourcengruppe, ein Storage-Konto und Schlüssel für den Blob-Container.

    - Erstellt eine neue Administratorrolle und ein Kubernetes-Servicekonto auf dem Cluster.
    - Verwendet diese neue Administratorrolle für die Installation "Astra Trident" Auf dem Cluster und um eine oder mehrere Storage-Klassen zu erstellen.
    - Wenn Sie ein Cloud-Service-Storage-Angebot von NetApp als Storage-Back-End verwenden, verwendet der Astra Control Service Astra Trident zur Bereitstellung persistenter Volumes für Ihre Applikationen. Wenn Sie von Amazon EBS oder Azure gemanagte Festplatten als Storage-Backend verwenden, müssen Sie einen Provider-spezifischen CSI-Treiber installieren. Installationsanweisungen finden Sie in "Einrichten von Amazon Web Services" Und "Richten Sie Microsoft Azure mit von Azure gemanagten Festplatten ein".
- An dieser Stelle können Sie Ihrem Cluster Apps hinzufügen. Persistente Volumes werden auf der neuen Standard-Storage-Klasse bereitgestellt.
- Anschließend verwalten Sie diese Applikationen mithilfe des Astra Control Service und erstellen Snapshots, Backups und Klone.

Mit dem kostenlosen Plan von Astra Control können Sie bis zu 10 Namespaces in Ihrem Konto verwalten. Wenn Sie mehr als 10 verwalten möchten, müssen Sie die Abrechnung durch ein Upgrade vom kostenlosen Plan auf den Premium-Plan einrichten.

So funktioniert Astra Control Center

Astra Control Center wird lokal in Ihrer eigenen Private Cloud ausgeführt.

Astra Control Center unterstützt Kubernetes-Cluster mit Astra Trident-basierter Storage-Klasse mit einem Storage-Back-End von ONTAP 9.5 und höher.

In einer Cloud-vernetzten Umgebung nutzt Astra Control Center erweiterte Monitoring- und Telemetriedaten mithilfe von Cloud Insights. Liegt keine Cloud Insights-Verbindung vor, ist das Monitoring und die Telemetrie nur begrenzt (7 Tage Metriken) im Astra Control Center verfügbar und wird auch über offene Messpunkte in native Kubernetes-Monitoring-Tools (wie Prometheus und Grafana) exportiert.

Astra Control Center ist vollständig in das Ecosystem von AutoSupport und Active IQ Digital Advisor (auch als digitaler Berater bekannt) integriert, um Benutzern und NetApp-Support Fehlerbehebungs- und Verwendungsinformationen zu bieten.

Sie können Astra Control Center mit einer eingebetteten 90-Tage-Evaluierungslizenz ausprobieren. Bei der Evaluierung von Astra Control Center können Sie Support über E-Mail- und Community-Optionen erhalten. Zudem haben Sie über das Dashboard für den Produktsupport Zugriff auf Knowledgebase-Artikel und

-Dokumentation.

Um Astra Control Center zu installieren und zu verwenden, müssen Sie sicher sein "Anforderungen".

Astra Control Center funktioniert auf hohem Niveau wie folgt:

- Sie installieren Astra Control Center in Ihrer lokalen Umgebung. Erfahren Sie mehr darüber, wie Sie "Installieren Sie Astra Control Center".
- Sie führen einige Setup-Aufgaben wie die folgenden aus:
  - Lizenzierung einrichten.
  - Fügen Sie den ersten Cluster hinzu.
  - Fügen Sie ein Storage-Back-End hinzu, das beim Hinzufügen des Clusters erkannt wird.
  - Fügen Sie einen Objektspeicher-Bucket hinzu, der Ihre Applikations-Backups speichert.

Erfahren Sie mehr darüber, wie Sie "Einrichten des Astra Control Center".

Sie können Applikationen zu Ihrem Cluster hinzufügen. Wenn auch einige Applikationen bereits im Cluster gemanagt werden, können Sie sie mit dem Astra Control Center managen. Nutzen Sie dann das Astra Control Center, um Snapshots, Backups, Klone und Replizierungsbeziehungen zu erstellen.

Finden Sie weitere Informationen

- "Dokumentation des Astra Control Service"
- "Astra Control Center-Dokumentation"
- "Astra Trident-Dokumentation"
- "Astra Control API-Dokumentation"
- "Cloud Insights-Dokumentation"
- "ONTAP-Dokumentation"

Anforderungen des Astra Control Centers

Prüfen Sie zunächst die Bereitschaft Ihrer Betriebsumgebung, Anwendungscluster, Applikationen, Lizenzen und Ihres Webbrowsers. Stellen Sie sicher, dass Ihre Umgebung für den Einsatz und Betrieb von Astra Control Center diese Anforderungen erfüllt.

Unterstützte Host-Cluster-Kubernetes-Umgebungen

Astra Control Center wurde mit den folgenden Kubernetes-Host-Umgebungen validiert:

> Stellen Sie sicher, dass die Kubernetes-Umgebung, für die Sie Astra Control Center hosten, die grundlegenden Ressourcenanforderungen erfüllt, die in der offiziellen Dokumentation der Umgebung aufgeführt sind.

Kubernetes-Distribution auf Host-Cluster	Unterstützte Versionen
Azure Kubernetes Service für Azure Stack HCI	Azure Stack HCI 21H2 und 22H2 mit AKS 1.24.x und 1.25.x

Kubernetes-Distribution auf Host-Cluster	Unterstützte Versionen
Google Anthos	1.15 bis 1.16 (siehe Anforderungen für Google Anthos Ingress)
Kubernetes (Vorgelagert)	1.26 bis 1.28
Rancher Kubernetes Engine (RKE)	RKE 1.3 mit Rancher Manager 2.6 RKE 1.4 mit Rancher Manager 2.7 RKE 2 (v1.24.x) mit Rancher 2.6 RKE 2 (v1.26.x) mit Rancher 2.7
Red hat OpenShift Container Platform	4.11 bis 4.14
VMware Tanzu Kubernetes Grid Integrated Edition	1.16.x (siehe Ressourcenanforderungen des Host-Clusters)

Ressourcenanforderungen des Host-Clusters

Astra Control Center erfordert zusätzlich zu den Ressourcenanforderungen der Umgebung die folgenden Ressourcen:

> Bei diesen Anforderungen wird davon ausgegangen, dass Astra Control Center die einzige Applikation ist, die in der Betriebsumgebung ausgeführt wird. Wenn in der Umgebung zusätzliche Applikationen ausgeführt werden, passen Sie diese Mindestanforderungen entsprechend an.

- **CPU-Erweiterungen**: Die CPUs in allen Knoten der Hosting-Umgebung müssen AVX-Erweiterungen aktiviert haben.
- **Worker Nodes**: Insgesamt mindestens 3 Worker Nodes, mit 4 CPU Cores und je 12 GB RAM
- **Anforderungen für den VMware Tanzu Kubernetes Grid Cluster**: Beachten Sie bei der Hosting von Astra Control Center auf einem VMware Tanzu Kubernetes Grid (TKG)- oder Tanzu Kubernetes Grid Integrated Edition (TKGi)-Cluster die folgenden Überlegungen.
  - Das standardmäßige VMware TKG- und TKGi-Konfigurationstoken läuft zehn Stunden nach der Bereitstellung ab. Wenn Sie Tanzu Portfolio-Produkte verwenden, müssen Sie eine Tanzu Kubernetes Cluster-Konfigurationsdatei mit einem nicht auslaufenden Token generieren, um Verbindungsprobleme zwischen Astra Control Center und verwalteten Anwendungsclustern zu vermeiden. Anweisungen finden Sie unter "Die Produktdokumentation zu VMware NSX-T Data Center."
  - Verwenden Sie die `kubectl get nsxlbmonitors -A` Befehl, um zu sehen, ob bereits ein Service-Monitor für die Annahme von Ingress-Traffic konfiguriert ist. Wenn vorhanden, sollten Sie MetalLB nicht installieren, da der vorhandene Servicemonitor eine neue Load Balancer-Konfiguration außer Kraft setzt.
  - Deaktivieren Sie die Durchsetzung der Standardspeicherklasse TKG oder TKGi auf allen Anwendungsclustern, die von Astra Control verwaltet werden sollen. Sie können dies tun, indem Sie die bearbeiten `TanzuKubernetesCluster` Ressource auf dem Namespace-Cluster.
  - Achten Sie bei der Implementierung des Astra Control Center in einer TKG- oder TKGi-Umgebung auf die speziellen Anforderungen von Astra Trident. Weitere Informationen finden Sie im "Astra Trident-Dokumentation".

Service-Mesh-Anforderungen

Eine unterstützte Vanilla-Version des Istio Service Mesh wird dringend empfohlen, auf dem Astra Control Center Host Cluster installiert zu werden. Siehe "Unterstützte Versionen" Für unterstützte Versionen von Istio. Markenversionen von Istio Service-Mesh, wie OpenShift Service Mesh, werden nicht mit Astra Control Center validiert.

Um Astra Control Center mit dem auf dem Host-Cluster installierten Istio-Service-Mesh zu integrieren, müssen Sie die Integration im Astra Control Center vornehmen "Installation" Prozess und nicht unabhängig von diesem Prozess.

Wenn Sie Astra Control Service installieren, ohne ein Service-Mesh auf dem Host-Cluster zu konfigurieren, hat dies möglicherweise schwerwiegende Auswirkungen auf die Sicherheit.

Anforderungen von Astra Trident

Stellen Sie sicher, dass Sie die folgenden Anforderungen für Astra Trident erfüllen, die Ihren Anforderungen Ihrer Umgebung entsprechen:

- **Mindestversion für Astra Control Center**: Astra Trident 23.01 oder neuer installiert und konfiguriert
- **ONTAP-Konfiguration mit Astra Trident**:
  - **Storage class**: Konfigurieren Sie mindestens eine Astra Trident Storage-Klasse auf dem Cluster. Wenn eine Standard-Storage-Klasse konfiguriert ist, stellen Sie sicher, dass es die einzige Storage-Klasse mit der Standardbezeichnung ist.
  - **Speichertreiber und Workerknoten**: Stellen Sie sicher, dass Sie die Workerknoten in Ihrem Cluster mit den entsprechenden Speichertreibern konfigurieren, damit die Pods mit dem Backend-Speicher interagieren können. Astra Control Center unterstützt die folgenden ONTAP-Treiber von Astra Trident:
    - `ontap-nas`
    - `ontap-san`
    - `ontap-san-economy` (App-Replizierung ist bei diesem Storage-Klassen-Typ nicht verfügbar)
    - `ontap-nas-economy` (Snapshots und Replizierungsrichtlinien sind bei diesem Typ der Storage-Klasse nicht verfügbar.)

Astra Control Provisioner

Um die erweiterten Storage-Funktionen von Astra Control Provisioner zu verwenden, müssen Sie Astra Trident 23.10 oder höher installieren und aktivieren "Funktionen für die Astra Control Provisioner".

Storage-Back-Ends

Stellen Sie sicher, dass Sie ein unterstütztes Backend mit ausreichender Kapazität haben.

- **Erforderliche Back-End-Speicherkapazität**: Mindestens 500 GB verfügbar
- **Unterstützte Backends**: Astra Control Center unterstützt folgende Speicher-Backends:
  - NetApp ONTAP 9.9.1 oder neuer AFF, FAS und ASA Systeme
  - NetApp ONTAP Select 9.9.1 oder höher
  - NetApp Cloud Volumes ONTAP 9.9.1 oder höher

- Longhorn 1.5.0 oder neuer
  - Erfordert die manuelle Erstellung eines VolumeSnapshotClass-Objekts. Siehe "Longhorn-Dokumentation" Weitere Anweisungen.
- NetApp MetroCluster
  - Verwaltete Kubernetes-Cluster müssen in einer Stretch-Konfiguration vorliegen.
- Storage-Back-Ends bei unterstützten Cloud-Providern verfügbar

ONTAP-Lizenzen

Um Astra Control Center zu nutzen, müssen Sie je nach den Anforderungen die folgenden ONTAP-Lizenzen besitzen:

- FlexClone
- SnapMirror: Optional Nur für die Replizierung auf Remote-Systeme mit SnapMirror Technologie erforderlich. Siehe "Informationen zu SnapMirror Lizenzen".
- S3-Lizenz: Optional Nur für ONTAP S3 Buckets erforderlich

Informationen darüber, ob auf Ihrem ONTAP System die erforderlichen Lizenzen vorhanden sind, finden Sie unter "Managen Sie ONTAP Lizenzen".

NetApp MetroCluster

Wenn Sie NetApp MetroCluster als Storage-Backend verwenden, müssen Sie Folgendes tun:

- Geben Sie eine SVM-Management-LIF als Back-End-Option im von Ihnen verwendeten Astra Trident-Treiber an
- Stellen Sie sicher, dass Sie über die entsprechende ONTAP-Lizenz verfügen

Weitere MetroCluster Informationen zu den einzelnen Treibern finden Sie in der Dokumentation zu Astra Trident:

- "San"
- "NAS"

Bildregistrierung

Sie müssen über eine vorhandene private Docker Image-Registrierung verfügen, auf die Sie Astra Control Center Build-Images übertragen können. Sie müssen die URL der Bildregistrierung angeben, in der Sie die Bilder hochladen.

Astra Control Center-Lizenz

Für Astra Control Center ist eine Astra Control Center Lizenz erforderlich. Bei der Installation von Astra Control Center ist bereits eine eingebettete 90-Tage-Evaluierungslizenz für 4,800 CPU-Einheiten aktiviert. Wenn Sie mehr Kapazität oder andere Evaluierungsbedingungen benötigen, oder ein Upgrade auf eine komplette Lizenz wünschen, können Sie eine andere Evaluierungslizenz oder volle Lizenz von NetApp erhalten. Sie benötigen eine Lizenz zum Schutz Ihrer Applikationen und Daten.

Astra Control Center können Sie ausprobieren, indem Sie sich für eine kostenlose Testversion anmelden. Registrieren Sie sich "Hier".

Informationen zum Einrichten der Lizenz finden Sie unter "Verwenden Sie eine 90-Tage-Evaluierungslizenz".

Weitere Informationen zur Funktionsweise von Lizenzen finden Sie unter "Lizenzierung".

Netzwerkanforderungen

Konfigurieren Sie Ihre Betriebsumgebung so, dass Astra Control Center ordnungsgemäß kommunizieren kann. Die folgenden Netzwerkkonfigurationen sind erforderlich:

- **FQDN-Adresse**: Sie müssen eine FQDN-Adresse für Astra Control Center haben.
- **Zugang zum Internet**: Sie sollten festlegen, ob Sie Zugang zum Internet von außen haben. Wenn nicht, sind einige Funktionen möglicherweise begrenzt, beispielsweise das Empfangen von Monitoring- und Kennzahlendaten von NetApp Cloud Insights oder das Senden von Support-Paketen an die "NetApp Support Website".
- **Port Access**: Die Betriebsumgebung, die das Astra Control Center hostet, kommuniziert über die folgenden TCP-Ports. Sie sollten sicherstellen, dass diese Ports über beliebige Firewalls zugelassen sind, und Firewalls so konfigurieren, dass jeder HTTPS-ausgehenden Datenverkehr aus dem Astra-Netzwerk zugelassen wird. Einige Ports erfordern Verbindungen zwischen der Umgebung, in der Astra Control Center gehostet wird, und jedem verwalteten Cluster (sofern zutreffend).

> Sie können Astra Control Center in einem Dual-Stack-Kubernetes-Cluster implementieren. Astra Control Center kann Applikationen und Storage-Back-Ends managen, die für den Dual-Stack-Betrieb konfiguriert wurden. Weitere Informationen zu Dual-Stack-Cluster-Anforderungen finden Sie im "Kubernetes-Dokumentation".

Quelle	Ziel	Port	Protokoll	Zweck
Client-PC	Astra Control Center	443	HTTPS	UI-/API-Zugriff – Stellen Sie sicher, dass dieser Port in beide Richtungen zwischen Astra Control Center und dem System offen ist, mit dem auf Astra Control Center zugegriffen wird
Kennzahlenverbraucher	Astra Control Center Worker-Node	9090	HTTPS	Kennzahlen Datenkommunikation - sicherstellen, dass jeder verwaltete Cluster auf diesen Port auf dem Cluster zugreifen kann, das Astra Control Center hostet (Kommunikation in zwei Bereichen erforderlich)

Quelle	Ziel	Port	Protokoll	Zweck
Astra Control Center	Gehosteter Cloud Insights Service (https://www.netapp.com/cloud-services/cloud-insights/)	443	HTTPS	Cloud Insights Kommunikation
Astra Control Center	Amazon S3 Storage-Bucket-Provider	443	HTTPS	Amazon S3 Storage-Kommunikation
Astra Control Center	NetApp AutoSupport (https://support.netapp.com)	443	HTTPS	Kommunikation zwischen NetApp AutoSupport
Astra Control Center	Gemanagter Kubernetes-Cluster	443/6443 **HINWEIS**: Der Port, den der verwaltete Cluster verwendet, kann je nach Cluster variieren. Informationen finden Sie in der Dokumentation des Anbieters der Cluster-Software.	HTTPS	Kommunikation mit dem verwalteten Cluster – Stellen Sie sicher, dass dieser Port auf beiden Wegen zwischen dem Cluster, der Astra Control Center hostet, und jedem verwalteten Cluster offen ist

Ingress für lokale Kubernetes Cluster

Sie können die Art der Netzwerk Ingress Astra Control Center verwendet wählen. Astra Control Center nutzt standardmäßig das Astra Control Center Gateway (Service/Trafik) als Cluster-weite Ressource. Astra Control Center unterstützt auch den Einsatz eines Service Load Balancer, sofern diese in Ihrer Umgebung zugelassen sind. Wenn Sie lieber einen Service-Load-Balancer verwenden und noch nicht eine konfiguriert haben, können Sie den MetalLB-Load-Balancer verwenden, um dem Dienst automatisch eine externe IP-Adresse zuzuweisen. In der Konfiguration des internen DNS-Servers sollten Sie den ausgewählten DNS-Namen für Astra Control Center auf die Load-Balanced IP-Adresse verweisen.

> ⓘ Der Load Balancer sollte eine IP-Adresse verwenden, die sich im gleichen Subnetz wie die IP-Adressen des Astra Control Center Worker-Knotens befindet.

Weitere Informationen finden Sie unter "Eindringen für den Lastenausgleich einrichten".

Anforderungen für Google Anthos Ingress

Beachten Sie beim Hosten von Astra Control Center auf einem Google Anthos Cluster, dass Google Anthos standardmäßig den MetalLB Load Balancer und den Istio Ingress Service enthält, sodass Sie während der Installation einfach die generischen Ingress-Funktionen von Astra Control Center verwenden können. Siehe "Konfigurieren Sie Astra Control Center" Entsprechende Details.

Unterstützte Webbrowser

Astra Control Center unterstützt aktuelle Versionen von Firefox, Safari und Chrome mit einer Mindestauflösung von 1280 x 720.

Zusätzliche Anforderungen an Applikations-Cluster

Beachten Sie diese Anforderungen, wenn Sie die folgenden Funktionen des Astra Control Center nutzen möchten:

- **Anforderungen an den Anwendungscluster**: "Anforderungen für das Cluster-Management"
  - **Verwaltete Anwendungsanforderungen**: "Anforderungen für das Applikationsmanagement"
  - **Zusätzliche Anforderungen für die Anwendungsreplikation**: "Replikationsvoraussetzungen"

Wie es weiter geht

Sehen Sie sich die an "Schnellstart" Überblick.

Schnellstart für Astra Control Center

Hier finden Sie eine Übersicht über die Schritte, die für den Einstieg in das Astra Control Center erforderlich sind. Die Links in den einzelnen Schritten führen zu einer Seite, die weitere Details enthält.

Kubernetes-Cluster-Anforderungen prüfen

Stellen Sie sicher, dass Ihre Umgebung die folgenden Anforderungen erfüllt:

- Kubernetes Cluster*
- "Stellen Sie sicher, dass Ihr Host-Cluster die Anforderungen der Betriebsumgebung erfüllt"
- "Konfigurieren Sie Ingress für den Lastausgleich von lokalen Kubernetes-Clustern"

Storage-Integration

- "Stellen Sie sicher, dass Ihre Umgebung eine von Astra Trident unterstützte Version enthält"
- "Aktivieren Sie Astra Control Provisioner für erweiterte Management- und Storage-Bereitstellungsfunktionen"
- "Bereiten Sie die Worker-Knoten vor"
- "Konfigurieren Sie das Astra Trident Storage-Back-End"
- "Konfigurieren Sie Astra Trident Storage-Kurse"
- "Installieren Sie den Astra Trident Volume Snapshot Controller"
- "Erstellen Sie eine Volume Snapshot-Klasse"

ONTAP-Anmeldedaten

- "Konfigurieren Sie die ONTAP-Anmeldedaten"

Laden Sie Astra Control Center herunter und installieren Sie es

Führen Sie die folgenden Installationsaufgaben aus:

- "Laden Sie Astra Control Center von der Download-Seite der NetApp Support-Website herunter"

- Beziehen Sie die NetApp Lizenzdatei:
  - Wenn Sie Astra Control Center evaluieren, ist bereits eine eingebettete Evaluierungslizenz enthalten
  - "Wenn Sie Astra Control Center bereits gekauft haben, generieren Sie Ihre Lizenzdatei"
- "Installieren Sie Astra Control Center"
- "Führen Sie weitere optionale Konfigurationsschritte durch"

Führen Sie einige erste Setup-Aufgaben aus

Führen Sie einige grundlegende Aufgaben aus, um zu beginnen:

- "Fügen Sie eine Lizenz hinzu"
- "Vorbereitung der Umgebung auf das Cluster Management"
- "Fügen Sie einen Cluster hinzu"
- "Fügen Sie ein Storage-Back-End hinzu"
- "Fügen Sie einen Bucket hinzu"

Nutzen Sie Das Astra Control Center

Nachdem Sie das Astra Control Center eingerichtet haben, verwenden Sie die Astra Control UI oder die "Astra Control API" So beginnen Sie mit der Verwaltung und dem Schutz von Apps:

- "Applikationsmanagement": Ressourcen definieren, die verwaltet werden sollen.
- "Schützen von Applikationen": Schutzrichtlinien konfigurieren und Anwendungen replizieren, klonen und migrieren.
- "Konten verwalten": Benutzer, Rollen, LDAP, Anmeldeinformationen und mehr.
- "Optional Verbindung mit Cloud Insights herstellen": Anzeige von Kennzahlen zur Gesundheit Ihres Systems.

Finden Sie weitere Informationen

- "Verwenden Sie die Astra Control API"
- "Upgrade Astra Control Center"
- "Holen Sie sich Hilfe mit Astra Control"

Übersicht über die Installation

Wählen Sie einen der folgenden Astra Control Center-Installationsverfahren aus:

- "Installieren Sie das Astra Control Center mithilfe des Standardprozesses"
- "(Wenn Sie Red hat OpenShift verwenden) installieren Sie Astra Control Center mit OpenShift OperatorHub"
- "Installieren Sie Astra Control Center mit einem Cloud Volumes ONTAP Storage-Backend"

Je nach Umgebung kann nach der Installation des Astra Control Center eine zusätzliche Konfiguration erforderlich sein:

- "Konfigurieren Sie nach der Installation das Astra Control Center"

Installieren Sie das Astra Control Center mithilfe des Standardprozesses

Laden Sie zum Installieren des Astra Control Center das Installationspaket von der NetApp Support Site herunter und führen Sie die folgenden Schritte aus. Mit diesem Verfahren können Sie Astra Control Center in Internet-angeschlossenen oder luftgekapderten Umgebungen installieren.

Für andere Installationsverfahren erweitern

- **Installation mit Red hat OpenShift OperatorHub**: Verwenden Sie diese "Alternativverfahren" So installieren Sie Astra Control Center unter Verwendung von OperatorHub auf OpenShift.
- **In der öffentlichen Cloud mit Cloud Volumes ONTAP-Backend installieren**: Verwenden "Derartige Verfahren" Zur Installation von Astra Control Center in Amazon Web Services (AWS), Google Cloud Platform (GCP) oder Microsoft Azure mit einem Cloud Volumes ONTAP Storage-Back-End

Eine Demonstration des Installationsvorgangs für Astra Control Center finden Sie unter "Dieses Video".

Bevor Sie beginnen

- **Umweltvoraussetzungen erfüllen**: "Bevor Sie mit der Installation beginnen, bereiten Sie Ihre Umgebung auf die Implementierung des Astra Control Center vor".

  Astra Control Center kann in einer dritten Fehlerdomäne oder an einem sekundären Standort implementiert werden. Dies wird für Applikationsreplizierung und nahtlose Disaster Recovery empfohlen.

- **Gesunde Dienste sicherstellen**: Überprüfen Sie, ob alle API-Dienste in einem gesunden Zustand sind und verfügbar sind:

  ```
  kubectl get apiservices
  ```

- **Stellen Sie einen routingfähigen FQDN sicher**: Der Astra FQDN, den Sie verwenden möchten, kann zum Cluster weitergeleitet werden. Das bedeutet, dass Sie entweder einen DNS-Eintrag in Ihrem internen DNS-Server haben oder eine bereits registrierte Core URL-Route verwenden.
- **Configure cert Manager**: Wenn ein cert Manager bereits im Cluster existiert, müssen Sie einige durchführen "Erforderliche Schritte" Damit Astra Control Center nicht versucht, seinen eigenen Cert Manager zu installieren. Standardmäßig installiert Astra Control Center während der Installation einen eigenen Cert-Manager.
- **Zugriff auf die NetApp Astra Control Image Registry**:
  Sie haben die Möglichkeit, Installations-Images und Funktionserweiterungen für Astra Control, wie z. B. Astra Control Provisioner, aus der NetApp-Image-Registrierung zu beziehen.

Für Schritte erweitern

a. Notieren Sie Ihre Astra Control Account-ID, die Sie zur Anmeldung in der Registrierung benötigen.

   Ihre Konto-ID wird in der Web-UI des Astra Control Service angezeigt. Wählen Sie das Symbol oben rechts auf der Seite aus, wählen Sie **API Access** aus und notieren Sie sich Ihre Konto-ID.

b. Wählen Sie auf derselben Seite **API-Token generieren** aus und kopieren Sie die API-Token-Zeichenfolge in die Zwischenablage und speichern Sie sie in Ihrem Editor.

c. Melden Sie sich in der Astra Control Registry an:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

- **Betrachten Sie ein Service-Mesh**: Es wird dringend empfohlen, die Kommunikationskanäle des Astra Control-Host-Clusters mit einem zu sichern "Unterstütztes Service-Mesh".

Istio Service Mesh-Details

Für die Nutzung von Istio Service Mesh müssen Sie Folgendes tun:

- Fügen Sie ein hinzu `istio-injection:enabled` Etikett In den Astra Namespace vor der Implementierung von Astra Control Center.
- Verwenden Sie die `Generic` Einstellung für Eindringen Und bieten eine alternative Ingress für Externe Lastverteilung.
- Für Red hat OpenShift-Cluster müssen Sie definieren `NetworkAttachmentDefinition` In allen zugehörigen Astra Control Center-Namespaces (`netapp-acc-operator`, `netapp-acc`, `netapp-monitoring` Für Anwendungscluster oder alle benutzerdefinierten Namespaces, die ersetzt wurden).

```
cat <<EOF | oc -n netapp-acc-operator create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-acc create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-monitoring create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF
```

- **Nur ONTAP-SAN-Treiber**: Wenn Sie einen ONTAP-SAN-Treiber verwenden, stellen Sie sicher, dass Multipath auf allen Kubernetes-Clustern aktiviert ist.

Schritte

Gehen Sie wie folgt vor, um Astra Control Center zu installieren:

- Laden Sie das Astra Control Center herunter und extrahieren Sie es
- Installieren Sie das NetApp Astra kubectl Plug-in
- Fügen Sie die Bilder Ihrer lokalen Registrierung hinzu
- Einrichten von Namespace und Geheimdienstraum für Registrys mit auth Anforderungen

- Installieren Sie den Operator Astra Control Center
- Konfigurieren Sie Astra Control Center
- Komplette Astra Control Center und Bedienerinstallation
- Überprüfen Sie den Systemstatus
- Eindringen für den Lastenausgleich einrichten
- Melden Sie sich in der UI des Astra Control Center an

> Löschen Sie den Operator Astra Control Center nicht (z. B. `kubectl delete -f astra_control_center_operator_deploy.yaml`) Zu jeder Zeit während der Astra Control Center Installation oder Betrieb, um das Löschen von Pods zu vermeiden.

Laden Sie das Astra Control Center herunter und extrahieren Sie es

Sie können das Bundle von Astra Control Center von der NetApp Support-Website herunterladen oder das Bundle mithilfe von Docker aus der Image-Registrierung des Astra Control Service abrufen.

NetApp Support Website

1. Laden Sie das Bundle mit Astra Control Center herunter (`astra-control-center-[version].tar.gz`) Vom "Download-Seite für Astra Control Center".
2. (Empfohlen, aber optional) Laden Sie das Zertifikaten- und Unterschriftenpaket für Astra Control Center herunter (`astra-control-center-certs-[version].tar.gz`) Um die Signatur des Bündels zu überprüfen.

   Erweitern Sie, um Details anzuzeigen

   ```
   tar -vxzf astra-control-center-certs-[version].tar.gz
   ```

   ```
   openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub
   -signature certs/astra-control-center-[version].tar.gz.sig
   astra-control-center-[version].tar.gz
   ```

   Die Ausgabe wird angezeigt `Verified OK` Nach erfolgreicher Überprüfung.

3. Extrahieren Sie die Bilder aus dem Astra Control Center Bundle:

   ```
   tar -vxzf astra-control-center-[version].tar.gz
   ```

Astra Control-Image-Registrierung

1. Melden Sie sich beim Astra Control Service an.
2. Wählen Sie im Dashboard **Deploy a self-Managed Instance of Astra Control** aus.
3. Folgen Sie den Anweisungen, um sich bei der Astra Control-Image-Registrierung anzumelden, das Astra Control Center-Installationsabbild zu ziehen und das Image zu extrahieren.

Installieren Sie das NetApp Astra kubectl Plug-in

Sie können das NetApp Astra kubectl Befehlszeilenschnittstelle-Plug-in verwenden, um Images in ein lokales Docker Repository zu verschieben.

Bevor Sie beginnen

NetApp bietet Plug-ins-Binärdateien für verschiedene CPU-Architekturen und Betriebssysteme. Sie müssen wissen, welche CPU und welches Betriebssystem Sie haben, bevor Sie diese Aufgabe ausführen.

Wenn Sie das Plugin bereits von einer früheren Installation installiert haben, "Stellen Sie sicher, dass Sie über die neueste Version verfügen" Bevor Sie diese Schritte ausführen.

Schritte

1. Listen Sie die verfügbaren NetApp Astra kubectl Plugin-Binärdateien auf:

Die kubectl Plugin-Bibliothek ist Teil des tar-Bündels und wird in den Ordner extrahiert `kubectl-astra`.

```
ls kubectl-astra/
```

2. Verschieben Sie die für Ihr Betriebssystem und die CPU-Architektur benötigte Datei in den aktuellen Pfad und benennen Sie sie in um `kubectl-astra`:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Fügen Sie die Bilder Ihrer lokalen Registrierung hinzu

1. Führen Sie die entsprechende Schrittfolge für Ihre Container-Engine durch:

Docker

1. Wechseln Sie in das Stammverzeichnis des Tarballs. Sie sollten den sehen `acc.manifest.bundle.yaml` Datei und diese Verzeichnisse:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Übertragen Sie die Paketbilder im Astra Control Center-Bildverzeichnis in Ihre lokale Registrierung. Führen Sie die folgenden Ersetzungen durch, bevor Sie den ausführen `push-images` Befehl:
   - Ersetzen Sie <BUNDLE_FILE> durch den Namen der Astra Control Bundle-Datei (`acc.manifest.bundle.yaml`).
   - <MY_FULL_REGISTRY_PATH> durch die URL des Docker Repositorys ersetzen, beispielsweise "<a href="https://<docker-registry>"" class="bare">https://<docker-registry>".
   - Ersetzen Sie <MY_REGISTRY_USER> durch den Benutzernamen.
   - Ersetzen Sie <MY_REGISTRY_TOKEN> durch ein autorisiertes Token für die Registrierung.

   ```
   kubectl astra packages push-images -m <BUNDLE_FILE> -r
   <MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
   <MY_REGISTRY_TOKEN>
   ```

Podman

1. Wechseln Sie in das Stammverzeichnis des Tarballs. Sie sollten diese Datei und das Verzeichnis sehen:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Melden Sie sich bei Ihrer Registrierung an:

   ```
   podman login <YOUR_REGISTRY>
   ```

3. Vorbereiten und Ausführen eines der folgenden Skripts, das für die von Ihnen verwendete Podman-Version angepasst ist. Ersetzen Sie <MY_FULL_REGISTRY_PATH> durch die URL Ihres Repositorys, die alle Unterverzeichnisse enthält.

   ```
   <strong>Podman 4</strong>
   ```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

Der Bildpfad, den das Skript erstellt, sollte abhängig von Ihrer Registrierungskonfiguration wie folgt aussehen:

```
https://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/23.10.0-68/image:version
```

Einrichten von Namespace und Geheimdienstraum für Registrys mit auth Anforderungen

1. Exportieren Sie den kubeconfig für den Host-Cluster Astra Control Center:

```
export KUBECONFIG=[file path]
```

Bevor Sie die Installation abschließen, vergewissern Sie sich, dass Ihr kubeconfig auf den Cluster zeigt, in dem Sie Astra Control Center installieren möchten.

2. Wenn Sie eine Registrierung verwenden, für die eine Authentifizierung erforderlich ist, müssen Sie Folgendes tun:

Für Schritte erweitern

a. Erstellen Sie die `netapp-acc-operator` Namespace:

```
kubectl create ns netapp-acc-operator
```

b. Erstellen Sie ein Geheimnis für das `netapp-acc-operator` Namespace. Fügen Sie Docker-Informationen hinzu und führen Sie den folgenden Befehl aus:

Platzhalter `your_registry_path` Sollte die Position der Bilder, die Sie früher hochgeladen haben, entsprechen (z. B. `[Registry_URL]/netapp/astra/astracc/23.10.0-68`).

```
kubectl create secret docker-registry astra-registry-cred -n
netapp-acc-operator --docker-server=[your_registry_path] --docker
-username=[username] --docker-password=[token]
```

Wenn Sie den Namespace löschen, nachdem das Geheimnis generiert wurde, erstellen Sie den Namespace neu und generieren Sie dann das Geheimnis für den Namespace neu.

c. Erstellen Sie die `netapp-acc` (Oder Name des benutzerdefinierten Namespace).

```
kubectl create ns [netapp-acc or custom namespace]
```

d. Erstellen Sie ein Geheimnis für das `netapp-acc` (Oder Name des benutzerdefinierten Namespace). Fügen Sie Docker-Informationen hinzu und führen Sie den folgenden Befehl aus:

```
kubectl create secret docker-registry astra-registry-cred -n
[netapp-acc or custom namespace] --docker
-server=[your_registry_path] --docker-username=[username]
--docker-password=[token]
```

Installieren Sie den Operator Astra Control Center

1. Telefonbuch ändern:

```
cd manifests
```

2. Bearbeiten Sie die YAML-Implementierung des Astra Control Center-Bedieners (`astra_control_center_operator_deploy.yaml`) Zu Ihrem lokalen Register und Geheimnis zu verweisen.

```
vim astra_control_center_operator_deploy.yaml
```

Ein YAML-Beispiel mit Anmerkungen folgt diesen Schritten.

a. Wenn Sie eine Registrierung verwenden, für die eine Authentifizierung erforderlich ist, ersetzen Sie die Standardzeile von `imagePullSecrets: []` Mit folgenden Optionen:

```
imagePullSecrets: [{name: astra-registry-cred}]
```

b. Ändern `ASTRA_IMAGE_REGISTRY` Für das `kube-rbac-proxy` Bild zum Registrierungspfad, in dem Sie die Bilder in ein geschoben haben Vorheriger Schritt.

c. Ändern `ASTRA_IMAGE_REGISTRY` Für das `acc-operator-controller-manager` Bild zum Registrierungspfad, in dem Sie die Bilder in ein geschoben haben Vorheriger Schritt.

Erweitern für Beispiel astra_control_Center_Operator_deploy.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: ASTRA_IMAGE_REGISTRY/kube-rbac-proxy:v4.8.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_INSTALLTIMEOUT
          value: 5m
        image: ASTRA_IMAGE_REGISTRY/acc-operator:23.10.72
        imagePullPolicy: IfNotPresent
        livenessProbe:
          httpGet:
            path: /healthz
```

```
            port: 8081
          initialDelaySeconds: 15
          periodSeconds: 20
        name: manager
        readinessProbe:
          httpGet:
            path: /readyz
            port: 8081
          initialDelaySeconds: 5
          periodSeconds: 10
        resources:
          limits:
            cpu: 300m
            memory: 750Mi
          requests:
            cpu: 100m
            memory: 75Mi
        securityContext:
          allowPrivilegeEscalation: false
      imagePullSecrets: []
      securityContext:
        runAsUser: 65532
      terminationGracePeriodSeconds: 10
```

3. Installieren Sie den Astra Control Center-Operator:

```
kubectl apply -f astra_control_center_operator_deploy.yaml
```

Erweitern für Probenantwort:

```
namespace/netapp-acc-operator created
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.as
tra.netapp.io created
role.rbac.authorization.k8s.io/acc-operator-leader-election-role
created
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role
created
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
created
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role
created
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding created
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding created
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding created
configmap/acc-operator-manager-config created
service/acc-operator-controller-manager-metrics-service created
deployment.apps/acc-operator-controller-manager created
```

4. Überprüfen Sie, ob Pods ausgeführt werden:

```
kubectl get pods -n netapp-acc-operator
```

Konfigurieren Sie Astra Control Center

1. Bearbeiten Sie die Datei Astra Control Center Custom Resource (CR) (`astra_control_center.yaml`) Zur Berücksichtigung, Unterstützung, Registrierung und anderen notwendigen Konfigurationen:

```
vim astra_control_center.yaml
```

Ein YAML-Beispiel mit Anmerkungen folgt diesen Schritten.

2. Ändern oder bestätigen Sie die folgenden Einstellungen:

<code>accountName</code>

Einstellung	Anleitung	Typ	Beispiel
`accountName`	Ändern Sie das `accountName` Zeichenfolge an den Namen, den Sie dem Astra Control Center-Konto zuordnen möchten. Es kann nur ein AccountName geben.	Zeichenfolge	`Example`

<code>astraVersion</code>

Einstellung	Anleitung	Typ	Beispiel
`astraVersion`	Die zu implementierende Version des Astra Control Center: Für diese Einstellung ist keine Aktion erforderlich, da der Wert bereits ausgefüllt wird.	Zeichenfolge	`23.10.0-68`

<code>astraAddress</code>

Einstellung	Anleitung	Typ	Beispiel
`astraAddress`	Ändern Sie das `astraAddress` Zeichenfolge an den FQDN (empfohlen) oder die IP-Adresse, die Sie in Ihrem Browser verwenden möchten, um auf Astra Control Center zuzugreifen. Diese Adresse legt fest, wie Astra Control Center in Ihrem Rechenzentrum zu finden ist und ist die gleiche FQDN- oder IP-Adresse, die Sie von Ihrem Load Balancer bereitgestellt haben, wenn Sie fertig sind "Anforderungen des Astra Control Centers". HINWEIS: Nicht verwenden `http://` Oder `https://` In der Adresse. Kopieren Sie diesen FQDN zur Verwendung in einem Später Schritt.	Zeichenfolge	`astra.example.com`

<code>autoSupport</code>

Ihre Auswahl in diesem Abschnitt bestimmt, ob Sie an der proaktiven Support-Anwendung Digital Advisor von NetApp teilnehmen und an welchem Ort Daten gesendet werden. Eine Internetverbindung ist erforderlich (Port 442), und alle Supportdaten werden anonymisiert.

Einstellung	Nutzung	Anleitung	Typ	Beispiel
`autoSupport.enrolled`	Entweder `enrolled` Oder `url` Felder müssen ausgewählt werden	Ändern `enrolled` Für AutoSupport bis `false` Für Websites ohne Internetverbindung oder Aufbewahrung `true` Für verbundene Standorte. Eine Einstellung von `true` Ermöglicht das Senden anonymer Daten an NetApp zu Supportzwecken. Die Standardwahl ist `false` Und zeigt an, dass keine Support-Daten an NetApp gesendet werden.	Boolesch	`false` (Dieser Wert ist der Standardwert)
`autoSupport.url`	Entweder `enrolled` Oder `url` Felder müssen ausgewählt werden	Diese URL legt fest, wo die anonymen Daten gesendet werden.	Zeichenfolge	`https://support.netapp.com/asupprod/post/1.0/postAsup`

<code>email</code>

Einstellung	Anleitung	Typ	Beispiel
`email`	Ändern Sie das `email` Zeichenfolge zur standardmäßigen ursprünglichen Administratoradresse. Kopieren Sie diese E-Mail-Adresse zur Verwendung in A Später Schritt. Diese E-Mail-Adresse wird als Benutzername für das erste Konto verwendet, um sich bei der UI anzumelden und wird über Ereignisse in Astra Control informiert.	Zeichenfolge	`admin@example.com`

<code>firstName</code>

Einstellung	Anleitung	Typ	Beispiel
`firstName`	Der erste Name des mit dem Astra-Konto verknüpften Standardadministrators. Der hier verwendete Name wird nach der ersten Anmeldung in einer Überschrift in der UI angezeigt.	Zeichenfolge	`SRE`

<code>LastName</code>

Einstellung	Anleitung	Typ	Beispiel
`lastName`	Der Nachname des mit dem Astra-Konto verknüpften Standard-Initialadministrators. Der hier verwendete Name wird nach der ersten Anmeldung in einer Überschrift in der UI angezeigt.	Zeichenfolge	`Admin`

<code>imageRegistry</code>

Ihre Auswahl in diesem Abschnitt definiert die Container-Image-Registry, die die Astra-Anwendungsabbilder, den Astra Control Center Operator und das Astra Control Center Helm Repository hostet.

Einstellung	Nutzung	Anleitung	Typ	Beispiel
`imageRegistry.name`	Erforderlich	Der Name der Bildregistrierung, in der Sie die Bilder in geschoben haben Vorheriger Schritt. Verwenden Sie es nicht `http://` Oder `https://` Im Registrierungsnamen.	Zeichenfolge	`example.registry.com/astra`
`imageRegistry.secret`	Erforderlich, wenn der von Ihnen eingegebene String eingegeben wird `imageRegistry.name' requires a secret.` `IMPORTANT: If you are using a registry that does not require authorization, you must delete this` `secret` Zeile in `imageRegistry` Oder die Installation schlägt fehl.	Der Name des Kubernetes Secret, das zur Authentifizierung mit der Bildregistrierung verwendet wird.	Zeichenfolge	`astra-registry-cred`

<code>storageClass</code>

Einstellung	Anleitung	Typ	Beispiel
`storageClass`	Ändern Sie das `storageClass` Wert von `ontap-gold` Je nach Installationsanforderungen zu einer anderen Ressource für Astra Trident Storage Class wechseln. Führen Sie den Befehl aus `kubectl get sc` So ermitteln Sie Ihre vorhandenen konfigurierten Speicherklassen. In die Manifest-Datei muss eine der Astra Trident-basierten Storage-Klassen eingegeben werden (`astra-control-center-<version>.manifest`) Und wird für Astra PVS verwendet. Wenn er nicht festgelegt ist, wird die Standard-Speicherklasse verwendet. HINWEIS: Wenn eine Standard-Storage-Klasse konfiguriert ist, stellen Sie sicher, dass diese die einzige Storage-Klasse mit der Standardbeschriftung ist.	Zeichenfolge	`ontap-gold`

<code>volumeReclaimPolicy</code>

Einstellung	Anleitung	Typ	Optionen
`volumeReclaimPolicy`	Damit wird die Rückgewinnungsrichtlinie für die PVS von Astra festgelegt. Festlegen dieser Richtlinie auf `Retain` Behält persistente Volumes nach dem Löschen von Astra bei. Festlegen dieser Richtlinie auf `Delete` Löscht persistente Volumes nach dem Löschen von astra. Wenn dieser Wert nicht festgelegt ist, werden die PVS beibehalten.	Zeichenfolge	• `Retain` (Dies ist der Standardwert) • `Delete`

<code>ingressType</code>

Einstellung	Anleitung	Typ	Optionen
`ingressType`	Verwenden Sie einen der folgenden Eingangstypen: `Generic`* (`ingressType: "Generic"`) (Standard) Verwenden Sie diese Option, wenn Sie einen anderen Ingress-Controller verwenden oder Ihren eigenen Ingress-Controller verwenden möchten. Nach der Implementierung des Astra Control Center müssen Sie den konfigurieren "Eingangs-Controller" Um Astra Control Center mit einer URL zu zeigen. WICHTIG: Wenn Sie ein Service-Mesh mit Astra Control Center verwenden möchten, müssen Sie auswählen `Generic` Als Eindringen Typ und richten Sie Ihre eigenen "Eingangs-Controller". **`AccTraefik`** (`ingressType: "AccTraefik"`) Verwenden Sie diese Option, wenn Sie keinen Ingress-Controller konfigurieren möchten. Dies implementiert das Astra Control Center `traefik` Gateway als Service des Typs Kubernetes Load Balancer: Astra Control Center nutzt einen Service vom Typ „loadbalancer“ (`svc/traefik` Im	Zeichenfolge	• `Generic` (Dies ist der Standardwert) • `AccTraefik`

<code>scaleSize</code>

Einstellung	Anleitung	Typ	Optionen
`scaleSize`	Astra verwendet standardmäßig High Availability (HA). `scaleSize` Von `Medium`, Die die meisten Dienste in HA bereitstellt und mehrere Replikate für Redundanz bereitstellt. Mit `scaleSize` Als `Small`, Astra wird die Anzahl der Replikate für alle Dienste reduzieren, außer für wesentliche Dienste, um den Verbrauch zu reduzieren. TIPP: `Medium` Implementierungen bestehen aus etwa 100 Pods (einschließlich transienter Workloads). 100 Pods basieren auf drei Master Nodes und einer Konfiguration mit drei Worker Nodes). Beachten Sie die Einschränkungen bei der Netzwerkgrenze pro Pod, die in Ihrer Umgebung möglicherweise ein Problem darstellen, insbesondere bei der Betrachtung von Disaster-Recovery-Szenarien.	Zeichenfolge	• `Small` • `Medium` (Dies ist der Standardwert)

<code>astraResourcesScaler</code>

Einstellung	Anleitung	Typ	Optionen
`astraResourcesScaler`	Skalierungsoptionen für die Ressourcengrenzen von AstraControlCenter. Astra Control Center implementiert standardmäßig mit Ressourcenanfragen, die für die meisten Komponenten in Astra bereitgestellt werden. Mit dieser Konfiguration verbessert sich die Leistung des Astra Control Center Software-Stacks auch bei erhöhter Applikationslast und -Skalierung. In Szenarien mit kleineren Entwicklungs- oder Testclustern jedoch das CR-Feld `astraResourcesScalar` Kann auf festgelegt werden `Off`. Dadurch werden Ressourcenanforderungen deaktiviert und die Bereitstellung auf kleineren Clustern ist möglich.	Zeichenfolge	• `Default` (Dies ist der Standardwert) • `Off`

<code>additionalValues</code>

Fügen Sie dem Astra Control Center CR die folgenden zusätzlichen Werte hinzu, um ein bekanntes Problem bei der Installation zu vermeiden:

```
additionalValues:
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
```

- Für die Kommunikation zwischen Astral Control Center und Cloud Insights ist die Überprüfung des TLS-Zertifikats standardmäßig deaktiviert. Sie können die TLS-Zertifizierungsüberprüfung für die Kommunikation zwischen Cloud Insights und dem Astra Control Center Host-Cluster und dem verwalteten Cluster aktivieren, indem Sie den folgenden Abschnitt in hinzufügen `additionalValues`.

```
 additionalValues:
   netapp-monitoring-operator:
     config:
       ciSkipTlsVerify: false
   cloud-insights-service:
     config:
       ciSkipTlsVerify: false
   telemetry-service:
     config:
       ciSkipTlsVerify: false
```

<code>crds</code>

Ihre Auswahl in diesem Abschnitt legt fest, wie Astra Control Center mit CRDs umgehen soll.

Einstellung	Anleitung	Typ	Beispiel
`crds.externalCertManager`	Wenn Sie einen externen Zertifikaten-Manager verwenden, ändern Sie `externalCertManager` Bis `true`. Der Standardwert `false` Führt dazu, dass Astra Control Center während der Installation seine eigenen CRT-Manager-CRDs installiert. CRDs sind Cluster-weite Objekte, die sich auf andere Teile des Clusters auswirken können. Mit diesem Flag können Sie dem Astra Control Center signalisieren, dass diese CRDs vom Clusteradministrator außerhalb des Astra Control Center installiert und verwaltet werden.	Boolesch	`False` (Dieser Wert ist der Standardwert)
`crds.externalTraefik`	Astra Control Center installiert standardmäßig die erforderlichen Trafik-CRDs. CRDs sind Cluster-weite Objekte, die sich auf andere Teile des Clusters auswirken können. Mit diesem Flag können Sie dem Astra Control Center signalisieren, dass diese CRDs vom Clusteradministrator außerhalb des Astra Control Center installiert und verwaltet werden.	Boolesch	`False` (Dieser Wert ist der Standardwert)

Stellen Sie sicher, dass Sie die richtige Storage-Klasse und den richtigen Ingress-Typ für Ihre Konfiguration ausgewählt haben, bevor Sie die Installation abschließen.

Erweitern für Beispiel astra_Control_Center.yaml

```
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"
  volumeReclaimPolicy: "Retain"
  ingressType: "Generic"
  scaleSize: "Medium"
  astraResourcesScaler: "Default"
  additionalValues:
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
  crds:
    externalTraefik: false
    externalCertManager: false
```

Komplette Astra Control Center und Bedienerinstallation

1. Wenn Sie dies in einem vorherigen Schritt nicht bereits getan haben, erstellen Sie das `netapp-acc` (Oder benutzerdefinierter) Namespace:

   ```
   kubectl create ns [netapp-acc or custom namespace]
   ```

2. Wenn Sie ein Service-Mesh mit Astra Control Center verwenden, fügen Sie dem die folgende Beschriftung

hinzu `netapp-acc` Oder benutzerdefinierter Namespace:

> Ihre Art des Eingangs (`ingressType`) Muss auf gesetzt werden `Generic` Im Astra Control Center CR, bevor Sie mit diesem Befehl fortfahren.

```
kubectl label ns [netapp-acc or custom namespace] istio-
injection:enabled
```

3. (Empfohlen) "Aktivieren Sie strenge MTLs" Für Istio Service Mesh:

```
kubectl apply -n istio-system -f - <<EOF
apiVersion: security.istio.io/v1beta1
kind: PeerAuthentication
metadata:
  name: default
spec:
  mtls:
    mode: STRICT
EOF
```

4. Installieren Sie das Astra Control Center im `netapp-acc` (Oder Ihr individueller) Namespace:

```
kubectl apply -f astra_control_center.yaml -n [netapp-acc or custom
namespace]
```

> Der Fahrer des Astra Control Center überprüft automatisch die Umgebungsanforderungen. Fehlt "Anforderungen" Kann dazu führen, dass Ihre Installation fehlschlägt oder Astra Control Center nicht ordnungsgemäß funktioniert. Siehe Nächster Abschnitt So prüfen Sie, ob Warnmeldungen zur automatischen Systemprüfung vorliegen.

Überprüfen Sie den Systemstatus

Sie können den Systemstatus mithilfe von kubectl-Befehlen überprüfen. Wenn Sie OpenShift verwenden möchten, können Sie vergleichbare oc-Befehle für Verifizierungsschritte verwenden.

Schritte

1. Vergewissern Sie sich, dass beim Installationsprozess keine Warnmeldungen zu den Validierungsprüfungen ausgegeben wurden:

```
kubectl get acc [astra or custom Astra Control Center CR name] -n
[netapp-acc or custom namespace] -o yaml
```

Zusätzliche Warnmeldungen werden auch in den Bedienerprotokollen des Astra Control Centers gemeldet.

2. Beheben Sie alle Probleme mit Ihrer Umgebung, die durch automatisierte Anforderungsprüfungen gemeldet wurden.

Sie können Probleme beheben, indem Sie sicherstellen, dass Ihre Umgebung den erfüllt "Anforderungen" Für Astra Control Center.

3. Vergewissern Sie sich, dass alle Systemkomponenten erfolgreich installiert wurden.

```
kubectl get pods -n [netapp-acc or custom namespace]
```

Jeder Pod sollte einen Status von haben `Running`. Es kann mehrere Minuten dauern, bis die System-Pods implementiert sind.

Erweitern, um die Probenantwort zu erhalten

```
NAME                                          READY   STATUS
RESTARTS     AGE
acc-helm-repo-6cc7696d8f-pmhm8                1/1     Running     0
9h
activity-597fb656dc-5rd4l                     1/1     Running     0
9h
activity-597fb656dc-mqmcw                     1/1     Running     0
9h
api-token-authentication-62f84                1/1     Running     0
9h
api-token-authentication-68nlf                1/1     Running     0
9h
api-token-authentication-ztgrm                1/1     Running     0
9h
asup-669d4ddbc4-fnmwp                         1/1     Running     1
(9h ago)   9h
authentication-78789d7549-lk686               1/1     Running     0
9h
bucketservice-65c7d95496-24x7l                1/1     Running     3
(9h ago)   9h
cert-manager-c9f9fbf9f-k8zq2                  1/1     Running     0
9h
cert-manager-c9f9fbf9f-qjlzm                  1/1     Running     0
9h
cert-manager-cainjector-dbbbd8447-b5qll       1/1     Running     0
9h
cert-manager-cainjector-dbbbd8447-p5whs       1/1     Running     0
9h
cert-manager-webhook-6f97bb7d84-4722b         1/1     Running     0
9h
cert-manager-webhook-6f97bb7d84-86kv5         1/1     Running     0
9h
certificates-59d9f6f4bd-2j899                 1/1     Running     0
9h
certificates-59d9f6f4bd-9d9k6                 1/1     Running     0
9h
certificates-expiry-check-28011180--1-8lkxz   0/1     Completed   0
9h
cloud-extension-5c9c9958f8-jdhrp              1/1     Running     0
9h
cloud-insights-service-5cdd5f7f-pp8r5         1/1     Running     0
9h
composite-compute-66585789f4-hxn5w            1/1     Running     0
9h
```

```
composite-volume-68649f68fd-tb7p4             1/1     Running     0
9h
credentials-dfc844c57-jsx92                   1/1     Running     0
9h
credentials-dfc844c57-xw26s                   1/1     Running     0
9h
entitlement-7b47769b87-4jb6c                  1/1     Running     0
9h
features-854d8444cc-c24b7                     1/1     Running     0
9h
features-854d8444cc-dv6sm                     1/1     Running     0
9h
fluent-bit-ds-9tlv4                           1/1     Running     0
9h
fluent-bit-ds-bpkcb                           1/1     Running     0
9h
fluent-bit-ds-cxmwx                           1/1     Running     0
9h
fluent-bit-ds-jgnhc                           1/1     Running     0
9h
fluent-bit-ds-vtr6k                           1/1     Running     0
9h
fluent-bit-ds-vxqd5                           1/1     Running     0
9h
graphql-server-7d4b9d44d5-zdbf5               1/1     Running     0
9h
identity-6655c48769-4pwk8                     1/1     Running     0
9h
influxdb2-0                                   1/1     Running     0
9h
keycloak-operator-55479d6fc6-slvmt            1/1     Running     0
9h
krakend-f487cb465-78679                       1/1     Running     0
9h
krakend-f487cb465-rjsxx                       1/1     Running     0
9h
license-64cbc7cd9c-qxsr8                      1/1     Running     0
9h
login-ui-5db89b5589-ndb96                     1/1     Running     0
9h
loki-0                                        1/1     Running     0
9h
metrics-facade-8446f64c94-x8h7b               1/1     Running     0
9h
monitoring-operator-6b44586965-pvcl4          2/2     Running     0
9h
```

```
nats-0                                          1/1     Running     0
9h
nats-1                                          1/1     Running     0
9h
nats-2                                          1/1     Running     0
9h
nautilus-85754d87d7-756qb                       1/1     Running     0
9h
nautilus-85754d87d7-q8j7d                       1/1     Running     0
9h
openapi-5f9cc76544-7fnjm                        1/1     Running     0
9h
openapi-5f9cc76544-vzr7b                        1/1     Running     0
9h
packages-5db49f8b5-lrzhd                        1/1     Running     0
9h
polaris-consul-consul-server-0                  1/1     Running     0
9h
polaris-consul-consul-server-1                  1/1     Running     0
9h
polaris-consul-consul-server-2                  1/1     Running     0
9h
polaris-keycloak-0                              1/1     Running     2
(9h ago)   9h
polaris-keycloak-1                              1/1     Running     0
9h
polaris-keycloak-2                              1/1     Running     0
9h
polaris-keycloak-db-0                           1/1     Running     0
9h
polaris-keycloak-db-1                           1/1     Running     0
9h
polaris-keycloak-db-2                           1/1     Running     0
9h
polaris-mongodb-0                               1/1     Running     0
9h
polaris-mongodb-1                               1/1     Running     0
9h
polaris-mongodb-2                               1/1     Running     0
9h
polaris-ui-66fb99479-qp9gq                      1/1     Running     0
9h
polaris-vault-0                                 1/1     Running     0
9h
polaris-vault-1                                 1/1     Running     0
9h
```

```
polaris-vault-2                                1/1     Running     0
9h
public-metrics-76fbf9594d-zmxzw                1/1     Running     0
9h
storage-backend-metrics-7d7fbc9cb9-lmd25       1/1     Running     0
9h
storage-provider-5bdd456c4b-2fftc              1/1     Running     0
9h
task-service-87575df85-dnn2q                   1/1     Running     3
(9h ago)   9h
task-service-task-purge-28011720--1-q6w4r      0/1     Completed   0
28m
task-service-task-purge-28011735--1-vk6pd      1/1     Running     0
13m
telegraf-ds-2r2kw                              1/1     Running     0
9h
telegraf-ds-6s9d5                              1/1     Running     0
9h
telegraf-ds-96jl7                              1/1     Running     0
9h
telegraf-ds-hbp84                              1/1     Running     0
9h
telegraf-ds-plwzv                              1/1     Running     0
9h
telegraf-ds-sr22c                              1/1     Running     0
9h
telegraf-rs-4sbg8                              1/1     Running     0
9h
telemetry-service-fb9559f7b-mk9l7              1/1     Running     3
(9h ago)   9h
tenancy-559bbc6b48-5msgg                       1/1     Running     0
9h
traefik-d997b8877-7xpf4                        1/1     Running     0
9h
traefik-d997b8877-9xv96                        1/1     Running     0
9h
trident-svc-585c97548c-d25z5                   1/1     Running     0
9h
vault-controller-88484b454-2d6sr               1/1     Running     0
9h
vault-controller-88484b454-fc5cz               1/1     Running     0
9h
vault-controller-88484b454-jktld               1/1     Running     0
9h
```

4. (Optional) Sehen Sie sich den an `acc-operator` Protokolle zur Überwachung des Fortschritts:

```
kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-
operator -c manager -f
```

> `accHost` Die Cluster-Registrierung ist einer der letzten Vorgänge, und bei Ausfall wird die Implementierung nicht fehlschlagen. Sollten in den Protokollen ein Fehler bei der Cluster-Registrierung angegeben sein, können Sie die Registrierung erneut über das versuchen "Fügen Sie in der UI einen Cluster-Workflow hinzu" Oder API.

5. Wenn alle Pods ausgeführt werden, überprüfen Sie, ob die Installation erfolgreich war (`READY` Ist `True`) Und holen Sie sich das erste Setup-Passwort, das Sie verwenden, wenn Sie sich bei Astra Control Center:

```
kubectl get AstraControlCenter -n [netapp-acc or custom namespace]
```

Antwort:

```
NAME    UUID                                   VERSION     ADDRESS
READY
astra   9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f  23.10.0-68
10.111.111.111  True
```

> Den UUID-Wert kopieren. Das Passwort lautet `ACC-` Anschließend der UUID-Wert (`ACC-[UUID]` Oder in diesem Beispiel `ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f`).

Eindringen für den Lastenausgleich einrichten

Sie können einen Kubernetes Ingress-Controller einrichten, der den externen Zugriff auf Services managt. Diese Verfahren enthalten Setup-Beispiele für einen Ingress-Controller, wenn Sie die Standardeinstellung von verwenden `ingressType: "Generic"` In der Astra Control Center Custom Resource (`astra_control_center.yaml`). Sie müssen diesen Vorgang nicht verwenden, wenn Sie angegeben haben `ingressType: "AccTraefik"` In der Astra Control Center Custom Resource (`astra_control_center.yaml`).

Nachdem Astra Control Center bereitgestellt wurde, müssen Sie den Ingress-Controller so konfigurieren, dass Astra Control Center mit einer URL verfügbar ist.

Die Einstellungsschritte unterscheiden sich je nach Typ des Ingress-Controllers. Astra Control Center unterstützt viele Ingress-Controller-Typen. Diese Einrichtungsverfahren bieten Beispielschritte für einige gängige Typen von Ingress-Controllern.

Bevor Sie beginnen

- Erforderlich "Eingangs-Controller" Sollte bereits eingesetzt werden.
- Der "Eingangsklasse" Entsprechend der Eingangs-Steuerung sollte bereits erstellt werden.

Schritte für Istio Ingress

1. Konfigurieren Sie Istio Ingress.

   Bei diesem Verfahren wird davon ausgegangen, dass Istio mithilfe des Konfigurationsprofils „Standard“ bereitgestellt wird.

2. Sammeln oder erstellen Sie die gewünschte Zertifikatdatei und die private Schlüsseldatei für das Ingress Gateway.

   Sie können ein CA-signiertes oder selbstsigniertes Zertifikat verwenden. Der allgemeine Name muss die Astra-Adresse (FQDN) sein.

   Beispielbefehl:

   ```
   openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout tls.key
   -out tls.crt
   ```

3. Erstellen Sie ein Geheimnis `tls secret name` Vom Typ `kubernetes.io/tls` Für einen privaten TLS-Schlüssel und ein Zertifikat im `istio-system namespace` Wie in TLS Secrets beschrieben.

   Beispielbefehl:

   ```
   kubectl create secret tls [tls secret name] --key="tls.key"
   --cert="tls.crt" -n istio-system
   ```

   Der Name des Geheimnisses sollte mit dem übereinstimmen `spec.tls.secretName` Verfügbar in `istio-ingress.yaml` Datei:

4. Bereitstellung einer Ingress-Ressource im `netapp-acc` (Oder Custom-Name) Namespace unter Verwendung des v1-Ressourcentyps für ein Schema (`istio-Ingress.yaml` Wird in diesem Beispiel verwendet):

```
apiVersion: networking.k8s.io/v1
kind: IngressClass
metadata:
  name: istio
spec:
  controller: istio.io/ingress-controller
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: istio
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: traefik
            port:
              number: 80
```

5. Übernehmen Sie die Änderungen:

```
kubectl apply -f istio-Ingress.yaml
```

6. Überprüfen Sie den Status des Eingangs:

```
kubectl get ingress -n [netapp-acc or custom namespace]
```

Antwort:

```
NAME    CLASS HOSTS             ADDRESS         PORTS   AGE
ingress istio astra.example.com 172.16.103.248  80, 443 1h
```

7. Astra Control Center-Installation abschließen.

Schritte für Nginx Ingress Controller

1. Erstellen Sie ein Geheimnis des Typs `kubernetes.io/tls` Für einen privaten TLS-Schlüssel und ein Zertifikat in `netapp-acc` (Oder Custom-Name) Namespace wie in beschrieben "TLS-Geheimnisse".
2. Bereitstellung einer Ingress-Ressource in `netapp-acc` (Oder Custom-Name) Namespace unter Verwendung des v1-Ressourcentyps für ein Schema (`nginx-Ingress.yaml` Wird in diesem Beispiel verwendet):

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: netapp-acc-ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: [class name for nginx controller]
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: <ACC address>
    http:
      paths:
        - path:
          backend:
            service:
              name: traefik
              port:
                number: 80
          pathType: ImplementationSpecific
```

3. Übernehmen Sie die Änderungen:

```
kubectl apply -f nginx-Ingress.yaml
```

NetApp empfiehlt die Installation des nginx Controllers als Bereitstellung statt als a `daemonSet`.

Schritte für OpenShift-Eingangs-Controller

1. Beschaffen Sie Ihr Zertifikat, und holen Sie sich die Schlüssel-, Zertifikat- und CA-Dateien für die OpenShift-Route bereit.
2. Erstellen Sie die OpenShift-Route:

```
oc create route edge --service=traefik --port=web -n [netapp-acc or
custom namespace] --insecure-policy=Redirect --hostname=<ACC
address> --cert=cert.pem --key=key.pem
```

Melden Sie sich in der UI des Astra Control Center an

Nach der Installation von Astra Control Center ändern Sie das Passwort für den Standardadministrator und melden sich im Astra Control Center UI Dashboard an.

Schritte

1. Geben Sie in einem Browser den FQDN ein (einschließlich `https://` Präfix), die Sie in verwendet haben `astraAddress` Im `astra_control_center.yaml` CR, wenn Sie haben das Astra Control Center installiert.
2. Akzeptieren Sie die selbstsignierten Zertifikate, wenn Sie dazu aufgefordert werden.

   Sie können nach der Anmeldung ein benutzerdefiniertes Zertifikat erstellen.

3. Geben Sie auf der Anmeldeseite des Astra Control Center den Wert ein, den Sie für verwendet haben `email` In `astra_control_center.yaml` CR, wenn Sie haben das Astra Control Center installiert, Gefolgt von dem anfänglichen Setup-Passwort (`ACC-[UUID]`).

   Wenn Sie dreimal ein falsches Passwort eingeben, wird das Administratorkonto 15 Minuten lang gesperrt.

4. Wählen Sie **Login**.
5. Ändern Sie das Passwort, wenn Sie dazu aufgefordert werden.

   Wenn dies Ihre erste Anmeldung ist und Sie das Passwort vergessen haben und noch keine anderen administrativen Benutzerkonten erstellt wurden, kontaktieren Sie "NetApp Support" Für Unterstützung bei der Kennwortwiederherstellung.

6. (Optional) Entfernen Sie das vorhandene selbst signierte TLS-Zertifikat und ersetzen Sie es durch ein "Benutzerdefiniertes TLS-Zertifikat, signiert von einer Zertifizierungsstelle (CA)".

Beheben Sie die Fehlerbehebung für die Installation

Wenn einer der Dienstleistungen in ist `Error` Status, können Sie die Protokolle überprüfen. Suchen Sie nach API-Antwortcodes im Bereich von 400 bis 500. Diese geben den Ort an, an dem ein Fehler aufgetreten ist.

Optionen

- Um die Bedienerprotokolle des Astra Control Center zu überprüfen, geben Sie Folgendes ein:

```
kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-
operator -c manager -f
```

- So überprüfen Sie die Ausgabe des Astra Control Center CR:

```
kubectl get acc -n [netapp-acc or custom namespace] -o yaml
```

Wie es weiter geht

- (Optional) Verarbeiten Sie abhängig von Ihrer Umgebung nach der Installation vollständig "Konfigurationsschritte".
- Führen Sie die Implementierung durch "Setup-Aufgaben".

Konfigurieren Sie einen externen Zertifikaten-Manager

Wenn bereits ein Cert Manager in Ihrem Kubernetes Cluster vorhanden ist, müssen Sie einige erforderliche Schritte durchführen, damit Astra Control Center keinen eigenen Cert Manager installiert.

Schritte

1. Vergewissern Sie sich, dass ein Zertifikaten-Manager installiert ist:

```
kubectl get pods -A | grep 'cert-manager'
```

Beispielantwort:

```
cert-manager   essential-cert-manager-84446f49d5-sf2zd              1/1
Running    0      6d5h
cert-manager   essential-cert-manager-cainjector-66dc99cc56-9ldmt   1/1
Running    0      6d5h
cert-manager   essential-cert-manager-webhook-56b76db9cc-fjqrq      1/1
Running    0      6d5h
```

2. Erstellen Sie ein Zertifikat-/Schlüsselpaar für das `astraAddress` FQDN:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout tls.key -out
tls.crt
```

Beispielantwort:

```
Generating a 2048 bit RSA private key
...................+++
.......................................+++
writing new private key to 'tls.key'
```

3. Erstellen eines Geheimnisses mit zuvor generierten Dateien:

```
kubectl create secret tls selfsigned-tls --key tls.key --cert tls.crt -n
<cert-manager-namespace>
```

Beispielantwort:

```
secret/selfsigned-tls created
```

4. Erstellen Sie ein `ClusterIssuer` Datei, die **genau** die folgenden ist, aber den Namespace-Speicherort enthält, wo Ihr `cert-manager` Pods sind installiert:

```
apiVersion: cert-manager.io/v1
kind: ClusterIssuer
metadata:
  name: astra-ca-clusterissuer
  namespace: <cert-manager-namespace>
spec:
  ca:
    secretName: selfsigned-tls
```

```
kubectl apply -f ClusterIssuer.yaml
```

Beispielantwort:

```
clusterissuer.cert-manager.io/astra-ca-clusterissuer created
```

5. Überprüfen Sie das `ClusterIssuer` Ist richtig aufgekommen. `Ready` Muss sein `True` Bevor Sie fortfahren können:

```
kubectl get ClusterIssuer
```

Beispielantwort:

```
NAME                        READY   AGE
astra-ca-clusterissuer      True    9s
```

6. Füllen Sie die aus "Astra Control Center-Installationsprozess". Es gibt ein "Erforderlicher Konfigurationsschritt für den Astra Control Center-Cluster YAML" In dem Sie den CRD-Wert ändern, um anzuzeigen, dass der Zertifikaten-Manager extern installiert ist. Sie müssen diesen Schritt während der Installation abschließen, damit das Astra Control Center den externen Zertifikaten-Manager erkennt.

Installieren Sie Astra Control Center mit OpenShift OperatorHub

Wenn Sie Red hat OpenShift verwenden, können Sie Astra Control Center mithilfe des von Red hat zertifizierten Betreibers installieren. Gehen Sie folgendermaßen vor, um Astra Control Center von der zu installieren "Red Hat Ecosystem Catalog" Oder die Red hat OpenShift-Container-Plattform verwenden.

Nach Abschluss dieses Verfahrens müssen Sie zum Installationsvorgang zurückkehren, um den abzuschließen "Verbleibende Schritte" Um die erfolgreiche Installation zu überprüfen, und melden Sie sich an.

Bevor Sie beginnen

- **Umweltvoraussetzungen erfüllen**: "Bevor Sie mit der Installation beginnen, bereiten Sie Ihre Umgebung auf die Implementierung des Astra Control Center vor".
- **Gewährleistung einer gesunden Clusteroperatoren und API-Dienste**:
  - Stellen Sie in Ihrem OpenShift-Cluster sicher, dass sich alle Clusterbetreiber in einem ordnungsgemäßen Zustand befinden:

    ```
    oc get clusteroperators
    ```

  - Stellen Sie in Ihrem OpenShift-Cluster sicher, dass sich alle API-Services in einem ordnungsgemäßen Zustand befinden:

    ```
    oc get apiservices
    ```

- **Stellen Sie einen routingfähigen FQDN sicher**: Der Astra FQDN, den Sie verwenden möchten, kann zum Cluster weitergeleitet werden. Das bedeutet, dass Sie entweder einen DNS-Eintrag in Ihrem internen DNS-Server haben oder eine bereits registrierte Core URL-Route verwenden.
- **OpenShift-Berechtigungen** erhalten: Sie benötigen alle erforderlichen Berechtigungen und Zugriff auf die Red hat OpenShift Container Platform, um die beschriebenen Installationsschritte auszuführen.
- **Configure a cert Manager**: Wenn ein cert Manager bereits im Cluster vorhanden ist, müssen Sie einige durchführen "Erforderliche Schritte" Damit Astra Control Center nicht seinen eigenen Cert-Manager installiert. Standardmäßig installiert Astra Control Center während der Installation einen eigenen Cert-Manager.
- **Betrachten Sie ein Service-Mesh**: Es wird dringend empfohlen, die Kommunikationskanäle des Astra Control-Host-Clusters mit einem zu sichern "Unterstütztes Service-Mesh".

Istio Service Mesh-Details

Für die Nutzung von Istio Service Mesh müssen Sie Folgendes tun:

- Fügen Sie ein hinzu `istio-injection:enabled` Kennzeichnen Sie den Astra-Namespace, bevor Sie Astra Control Center implementieren.
- Verwenden Sie die `Generic` Einstellung für Eindringen Und bieten eine alternative Ingress für "Externe Lastverteilung".
- Für Red hat OpenShift-Cluster müssen Sie definieren `NetworkAttachmentDefinition` In allen zugehörigen Astra Control Center-Namespaces (`netapp-acc-operator`, `netapp-acc`, `netapp-monitoring` Für Anwendungscluster oder alle benutzerdefinierten Namespaces, die ersetzt wurden).

```
cat <<EOF | oc -n netapp-acc-operator create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-acc create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF

cat <<EOF | oc -n netapp-monitoring create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF
```

- **Kubernetes Ingress-Controller**: Wenn Sie über einen Kubernetes Ingress-Controller verfügen, der externen Zugriff auf Services wie etwa den Lastausgleich in einem Cluster managt, müssen Sie ihn zur Verwendung mit Astra Control Center einrichten:

a. Erstellen Sie den Operator-Namespace:

```
oc create namespace netapp-acc-operator
```

b. "Einrichtung abschließen" Für Ihren Ingress-Controller-Typ.

- **Nur ONTAP-SAN-Treiber**: Wenn Sie einen ONTAP-SAN-Treiber verwenden, stellen Sie sicher, dass Multipath auf allen Kubernetes-Clustern aktiviert ist.

Schritte

- Laden Sie das Astra Control Center herunter und extrahieren Sie es
- Installieren Sie das NetApp Astra kubectl Plug-in
- Fügen Sie die Bilder Ihrer lokalen Registrierung hinzu
- Suchen Sie die Installationsseite des Bedieners
- Installieren Sie den Operator
- Installieren Sie Astra Control Center

Laden Sie das Astra Control Center herunter und extrahieren Sie es

Sie können das Bundle von Astra Control Center von der NetApp Support-Website herunterladen oder das Bundle mithilfe von Docker aus der Image-Registrierung des Astra Control Service abrufen.

NetApp Support Website

1. Laden Sie das Bundle mit Astra Control Center herunter (`astra-control-center-[version].tar.gz`) Vom "Download-Seite für Astra Control Center".
2. (Empfohlen, aber optional) Laden Sie das Zertifikaten- und Unterschriftenpaket für Astra Control Center herunter (`astra-control-center-certs-[version].tar.gz`) Um die Signatur des Bündels zu überprüfen.

   Erweitern Sie, um Details anzuzeigen

   ```
   tar -vxzf astra-control-center-certs-[version].tar.gz
   ```

   ```
   openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub
   -signature certs/astra-control-center-[version].tar.gz.sig
   astra-control-center-[version].tar.gz
   ```

   Die Ausgabe wird angezeigt `Verified OK` Nach erfolgreicher Überprüfung.

3. Extrahieren Sie die Bilder aus dem Astra Control Center Bundle:

   ```
   tar -vxzf astra-control-center-[version].tar.gz
   ```

Astra Control-Image-Registrierung

1. Melden Sie sich beim Astra Control Service an.
2. Wählen Sie im Dashboard **Deploy a self-Managed Instance of Astra Control** aus.
3. Folgen Sie den Anweisungen, um sich bei der Astra Control-Image-Registrierung anzumelden, das Astra Control Center-Installationsabbild zu ziehen und das Image zu extrahieren.

Installieren Sie das NetApp Astra kubectl Plug-in

Sie können das NetApp Astra kubectl Befehlszeilenschnittstelle-Plug-in verwenden, um Images in ein lokales Docker Repository zu verschieben.

Bevor Sie beginnen

NetApp bietet Plug-ins-Binärdateien für verschiedene CPU-Architekturen und Betriebssysteme. Sie müssen wissen, welche CPU und welches Betriebssystem Sie haben, bevor Sie diese Aufgabe ausführen.

Schritte

1. Geben Sie die verfügbaren Plug-ins-Binärdateien von NetApp Astra kubectl an und notieren Sie sich den Namen der für Ihr Betriebssystem und die CPU-Architektur erforderlichen Datei:

   Die kubectl Plugin-Bibliothek ist Teil des tar-Bündels und wird in den Ordner extrahiert `kubectl-astra`.

```
ls kubectl-astra/
```

2. Verschieben Sie die richtige Binärdatei in den aktuellen Pfad, und benennen Sie sie in um `kubectl-astra`:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Fügen Sie die Bilder Ihrer lokalen Registrierung hinzu

1. Führen Sie die entsprechende Schrittfolge für Ihre Container-Engine durch:

Docker

1. Wechseln Sie in das Stammverzeichnis des Tarballs. Sie sollten den sehen `acc.manifest.bundle.yaml` Datei und diese Verzeichnisse:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Übertragen Sie die Paketbilder im Astra Control Center-Bildverzeichnis in Ihre lokale Registrierung. Führen Sie die folgenden Ersetzungen durch, bevor Sie den ausführen `push-images` Befehl:
   - Ersetzen Sie <BUNDLE_FILE> durch den Namen der Astra Control Bundle-Datei (`acc.manifest.bundle.yaml`).
   - <MY_FULL_REGISTRY_PATH> durch die URL des Docker Repositorys ersetzen, beispielsweise "<a href="https://<docker-registry>"" class="bare">https://<docker-registry>".
   - Ersetzen Sie <MY_REGISTRY_USER> durch den Benutzernamen.
   - Ersetzen Sie <MY_REGISTRY_TOKEN> durch ein autorisiertes Token für die Registrierung.

     ```
     kubectl astra packages push-images -m <BUNDLE_FILE> -r
     <MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
     <MY_REGISTRY_TOKEN>
     ```

Podman

1. Wechseln Sie in das Stammverzeichnis des Tarballs. Sie sollten diese Datei und das Verzeichnis sehen:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Melden Sie sich bei Ihrer Registrierung an:

   ```
   podman login <YOUR_REGISTRY>
   ```

3. Vorbereiten und Ausführen eines der folgenden Skripts, das für die von Ihnen verwendete Podman-Version angepasst ist. Ersetzen Sie <MY_FULL_REGISTRY_PATH> durch die URL Ihres Repositorys, die alle Unterverzeichnisse enthält.

   ```
   <strong>Podman 4</strong>
   ```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

Der Bildpfad, den das Skript erstellt, sollte abhängig von Ihrer Registrierungskonfiguration wie folgt aussehen:

```
https://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/23.10.0-68/image:version
```

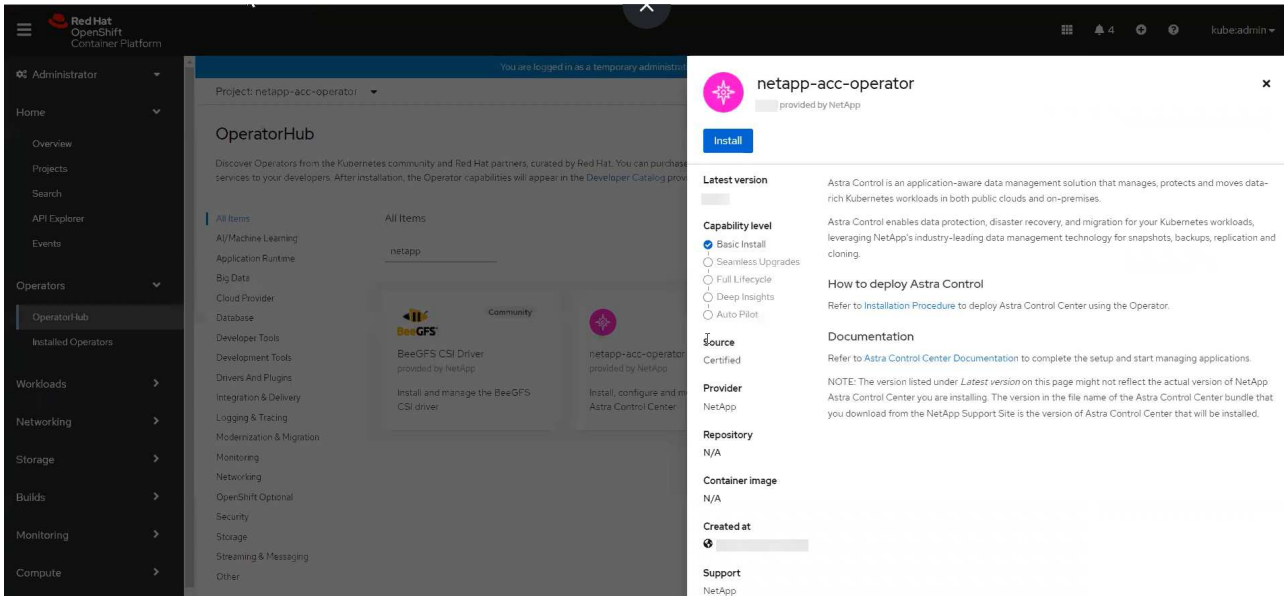
Suchen Sie die Installationsseite des Bedieners

1. Führen Sie eines der folgenden Verfahren aus, um auf die Installationsseite des Bedieners zuzugreifen:

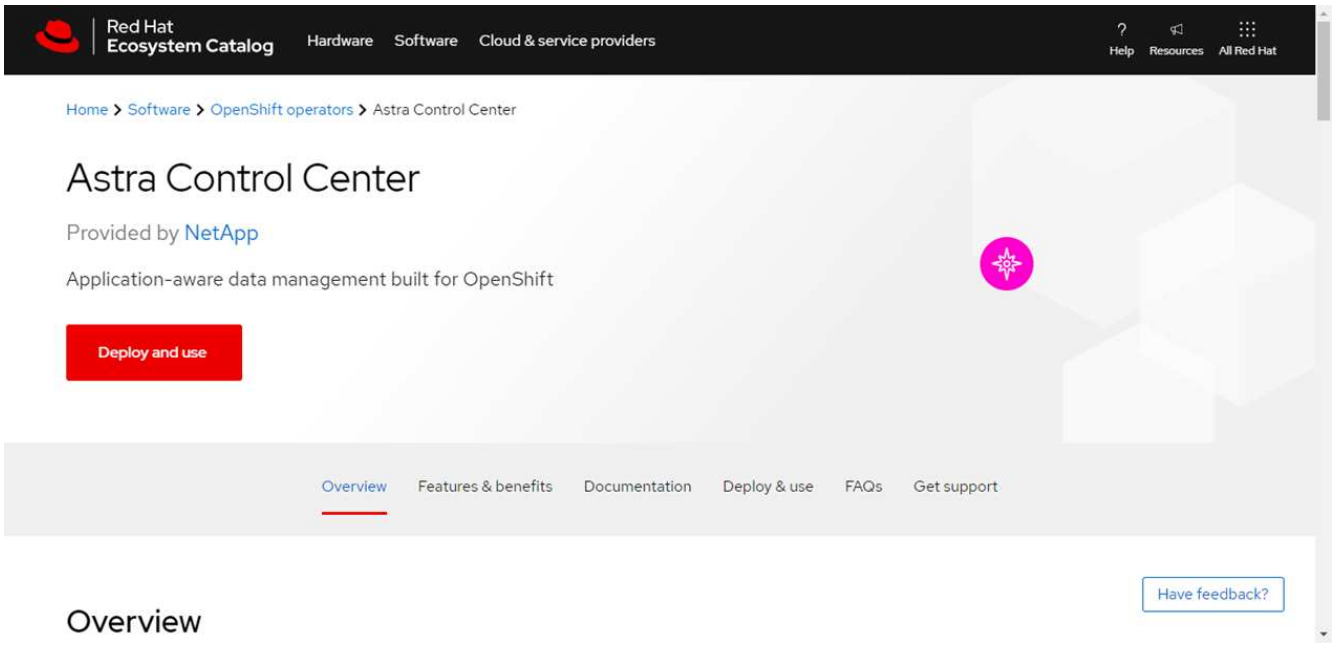
- Über die Red hat OpenShift-Webkonsole:
  i. Melden Sie sich in der OpenShift Container Platform UI an.
  ii. Wählen Sie im Seitenmenü die Option **Operatoren > OperatorHub** aus.

> Mit diesem Operator können Sie nur auf die aktuelle Version von Astra Control Center aktualisieren.

  iii. Suchen Sie nach und wählen Sie den Operator des NetApp Astra Control Center aus.



- Aus Dem Red Hat Ecosystem Catalog:
  i. Wählen Sie das NetApp Astra Control Center aus "Operator".
  ii. Wählen Sie **Bereitstellen und Verwenden**.



Installieren Sie den Operator

1. Füllen Sie die Seite **Install Operator** aus, und installieren Sie den Operator:

   Der Operator ist in allen Cluster-Namespaces verfügbar.

   a. Wählen Sie den Operator-Namespace oder aus `netapp-acc-operator` Der Namespace wird automatisch im Rahmen der Bedienerinstallation erstellt.

   b. Wählen Sie eine manuelle oder automatische Genehmigungsstrategie aus.

      Eine manuelle Genehmigung wird empfohlen. Sie sollten nur eine einzelne Operatorinstanz pro Cluster ausführen.

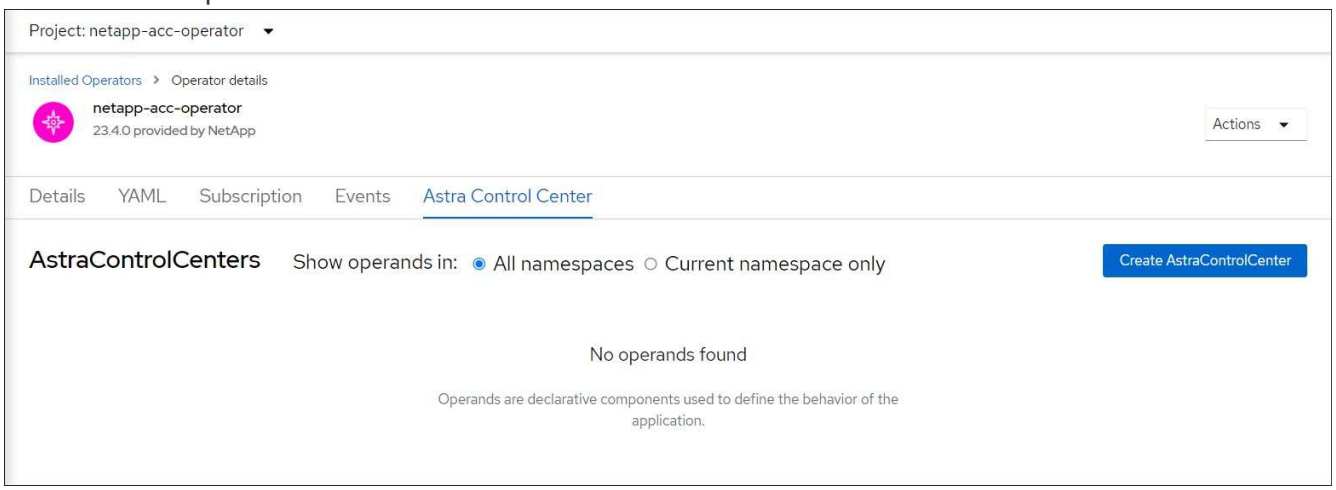
   c. Wählen Sie **Installieren**.

      Wenn Sie eine manuelle Genehmigungsstrategie ausgewählt haben, werden Sie aufgefordert, den manuellen Installationsplan für diesen Operator zu genehmigen.

2. Gehen Sie von der Konsole aus zum OperatorHub-Menü und bestätigen Sie, dass der Operator erfolgreich installiert wurde.

Installieren Sie Astra Control Center

1. Wählen Sie in der Konsole auf der Registerkarte **Astra Control Center** des Astra Control Center-Bedieners die Option **AstraControlCenter erstellen** aus.



2. Füllen Sie die aus `Create AstraControlCenter` Formularfeld:

   a. Behalten Sie den Namen des Astra Control Center bei oder passen Sie diesen an.

   b. Fügen Sie Etiketten für das Astra Control Center hinzu.

   c. Aktivieren oder deaktivieren Sie Auto Support. Es wird empfohlen, die Auto Support-Funktion beizubehalten.

   d. Geben Sie den FQDN des Astra Control Centers oder die IP-Adresse ein. Kommen Sie nicht herein `http://` Oder `https://` Im Adressfeld.

   e. Geben Sie die Astra Control Center-Version ein, z. B. 23.10.0-68.

   f. Geben Sie einen Kontonamen, eine E-Mail-Adresse und einen Administratornamen ein.

g. Wählen Sie eine Richtlinie zur Rückgewinnung von Volumes aus `Retain`, `Recycle`, Oder `Delete`. Der Standardwert ist `Retain`.

h. Wählen Sie die ScaleSize der Installation aus.

> Astra verwendet standardmäßig High Availability (HA). `scaleSize` Von `Medium`, Die die meisten Dienste in HA bereitstellt und mehrere Replikate für Redundanz bereitstellt. Mit `scaleSize` Als `Small`, Astra wird die Anzahl der Replikate für alle Dienste reduzieren, außer für wesentliche Dienste, um den Verbrauch zu reduzieren.

i. Wählen Sie den Typ der Eindringen aus:

- **`Generic`** (`ingressType: "Generic"`) (Standard)

  Verwenden Sie diese Option, wenn Sie einen anderen Ingress-Controller verwenden oder Ihren eigenen Ingress-Controller verwenden möchten. Nach der Implementierung des Astra Control Center müssen Sie den konfigurieren "Eingangs-Controller" Um Astra Control Center mit einer URL zu zeigen.

- **`AccTraefik`** (`ingressType: "AccTraefik"`)

  Verwenden Sie diese Option, wenn Sie keinen Ingress-Controller konfigurieren möchten. Dies implementiert das Astra Control Center `traefik` Gateway als Service vom Typ Kubernetes „Load Balancer“.

Astra Control Center nutzt einen Service vom Typ „loadbalancer“ (`svc/traefik` Im Astra Control Center Namespace) und erfordert, dass ihm eine zugängliche externe IP-Adresse zugewiesen wird. Wenn in Ihrer Umgebung Load Balancer zugelassen sind und Sie noch keine konfiguriert haben, können Sie MetalLB oder einen anderen externen Service Load Balancer verwenden, um dem Dienst eine externe IP-Adresse zuzuweisen. In der Konfiguration des internen DNS-Servers sollten Sie den ausgewählten DNS-Namen für Astra Control Center auf die Load-Balanced IP-Adresse verweisen.

> Weitere Informationen zum Servicetyp „loadbalancer“ und „ingress“ finden Sie unter "Anforderungen".

a. Geben Sie in **Image Registry** Ihren lokalen Container Image Registry-Pfad ein. Kommen Sie nicht herein `http://` Oder `https://` Im Adressfeld.

b. Wenn Sie eine Bildregistrierung verwenden, die eine Authentifizierung erfordert, geben Sie das Bildgeheimnis ein.

> Wenn Sie eine Registrierung verwenden, für die eine Authentifizierung erforderlich ist, Erstellen Sie ein Geheimnis auf dem Cluster.

c. Geben Sie den Vornamen des Administrators ein.

d. Konfiguration der Ressourcenskalierung

e. Stellen Sie die Standard-Storage-Klasse bereit.

> Wenn eine Standard-Storage-Klasse konfiguriert ist, stellen Sie sicher, dass diese die einzige Storage-Klasse mit der Standardbeschriftung ist.

f. Definieren Sie die Einstellungen für die Verarbeitung von CRD.

3. Wählen Sie die YAML-Ansicht aus, um die ausgewählten Einstellungen zu überprüfen.
4. Wählen Sie `Create`.

Erstellen Sie einen Registrierungsschlüssel

Wenn Sie eine Registrierung verwenden, die eine Authentifizierung erfordert, erstellen Sie einen Schlüssel im OpenShift-Cluster und geben Sie den geheimen Namen in das ein `Create AstraControlCenter` Formularfeld.

1. Erstellen Sie einen Namespace für den Astra Control Center-Betreiber:

```
oc create ns [netapp-acc-operator or custom namespace]
```

2. Erstellen eines Geheimnisses in diesem Namespace:

```
oc create secret docker-registry astra-registry-cred n [netapp-acc-
operator or custom namespace] --docker-server=[your_registry_path]
--docker username=[username] --docker-password=[token]
```

> Astra Control unterstützt nur die Geheimnisse der Docker-Registrierung.

3. Füllen Sie die übrigen Felder in aus Das Feld AstraControlCenter-Formular erstellen.

Wie es weiter geht

Füllen Sie die aus "Verbleibende Schritte" Um zu überprüfen, ob Astra Control Center erfolgreich installiert wurde, richten Sie einen Ingress-Controller ein (optional), und melden Sie sich an der UI an. Zusätzlich müssen Sie durchführen "Setup-Aufgaben" Nach Abschluss der Installation.

Installieren Sie Astra Control Center mit einem Cloud Volumes ONTAP Storage-Backend

Mit Astra Control Center können Sie Ihre Applikationen in einer Hybrid-Cloud-Umgebung mit automatisierten Kubernetes-Clustern und Cloud Volumes ONTAP Instanzen managen. Astra Control Center kann auch in lokalen Kubernetes-Clustern oder in einem der selbst gemanagten Kubernetes-Cluster in der Cloud-Umgebung implementiert werden.

Mit einer dieser Implementierungen können Sie Applikationsdatenmanagement-Vorgänge mithilfe von Cloud Volumes ONTAP als Storage-Backend durchführen. Außerdem können Sie einen S3-Bucket als Backup-Ziel konfigurieren.

Zur Installation von Astra Control Center in Amazon Web Services (AWS), Google Cloud Platform (GCP) und Microsoft Azure mit einem Cloud Volumes ONTAP Storage-Backend führen Sie je nach Cloud-Umgebung die folgenden Schritte aus.

- Implementieren Sie Astra Control Center in Amazon Web Services

- Implementieren Sie Astra Control Center in der Google Cloud Platform
- Implementieren Sie Astra Control Center in Microsoft Azure

Applikationen lassen sich in Distributionen mit selbst gemanagten Kubernetes-Clustern managen, wie z. B. mit OpenShift Container Platform (OCP). Nur selbst gemanagte OCP Cluster sind für die Implementierung des Astra Control Center validiert.

Implementieren Sie Astra Control Center in Amazon Web Services

Astra Control Center lässt sich in einem selbst gemanagten Kubernetes-Cluster implementieren, der in einer Public Cloud von Amazon Web Services (AWS) gehostet wird.

Was Sie für AWS benötigen

Vor der Implementierung von Astra Control Center in AWS sind folgende Fragen zu beachten:

- Astra Control Center-Lizenz: Siehe "Lizenzierungsanforderungen für Astra Control Center".
- "Sie erfüllen die Anforderungen des Astra Control Centers".
- NetApp Cloud Central Konto
- Bei Verwendung von OCP, Berechtigungen für die Red hat OpenShift Container Platform (OCP) (auf Namespace-Ebene zum Erstellen von Pods)
- AWS Zugangsdaten, Zugriffs-ID und geheimer Schlüssel mit Berechtigungen, mit denen Sie Buckets und Konnektoren erstellen können
- Zugriff und Anmeldung auf und bei dem AWS Konto Elastic Container Registry (ECR
- Für den Zugriff auf die Astra Control UI sind die Einträge für die gehostete AWS Zone und Amazon Route 53 erforderlich

Anforderungen der Betriebsumgebung für AWS

Astra Control Center erfordert die folgende Betriebsumgebung für AWS:

- Red hat OpenShift Container Platform 4.11 bis 4.13

> Stellen Sie sicher, dass die Betriebsumgebung, die Sie als Host für das Astra Control Center auswählen, den grundlegenden Ressourcenanforderungen in der offiziellen Dokumentation der Umgebung entspricht.

Astra Control Center erfordert zusätzlich zu den Ressourcenanforderungen der Umgebung die folgenden Ressourcen:

Komponente	Anforderungen
Back-End NetApp Cloud Volumes ONTAP Storage-Kapazität	Mindestens 300 GB verfügbar
Worker-Nodes (AWS EC2 Anforderung)	Insgesamt mindestens 3 Worker-Nodes mit 4 vCPU-Kernen und jeweils 12 GB RAM

Komponente	Anforderungen
Load Balancer	Der Servicetyp „loadbalancer“ ist für den Ingress Traffic verfügbar, der an Services im Cluster der Betriebsumgebung gesendet werden kann
FQDN	Eine Methode zum Zeigen des FQDN von Astra Control Center auf die Load Balanced IP-Adresse
Astra Trident (installiert im Rahmen der Kubernetes Cluster Discovery in NetApp BlueXP, ehemals Cloud Manager)	Astra Trident 23.01 oder höher installiert und konfiguriert und NetApp ONTAP Version 9.9.1 oder neuer als Storage-Backend
Bildregistrierung	NetApp stellt eine Registrierung bereit, mit der Sie Astra Control Center Build-Images abrufen können: http://netappdownloads.jfrog.io/docker-astra-control-prod Wenden Sie sich an den NetApp-Support, um Anweisungen zur Verwendung dieser Image-Registrierung während der Installation von Astra Control Center zu erhalten. Wenn Sie nicht auf die NetApp-Image-Registrierung zugreifen können, benötigen Sie eine bestehende private Registrierung, wie z. B. die AWS Elastic Container Registry (ECR), auf die Sie die Build-Images von Astra Control Center übertragen können. Sie müssen die URL der Bildregistrierung angeben, in der Sie die Bilder hochladen. Der gehostete Astra Control Center-Cluster und der verwaltete Cluster müssen Zugriff auf dieselbe Image-Registry haben, um Anwendungen mit dem Restic-basierten Image sichern und wiederherstellen zu können.
Konfiguration von Astra Trident/ONTAP	Astra Control Center erfordert, dass eine Storage-Klasse erstellt und als Standard-Storage-Klasse eingestellt wird. Astra Control Center unterstützt die folgenden Kubernetes-Storage-Klassen von ONTAP, die beim Importieren des Kubernetes Clusters in NetApp BlueXP (ehemals Cloud Manager) erstellt werden. Die folgenden Aufgaben werden von Astra Trident bereitgestellt: • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

Bei diesen Anforderungen wird davon ausgegangen, dass Astra Control Center die einzige Applikation ist, die in der Betriebsumgebung ausgeführt wird. Wenn in der Umgebung zusätzliche Applikationen ausgeführt werden, passen Sie diese Mindestanforderungen entsprechend an.

Das AWS-Registry-Token läuft innerhalb von 12 Stunden ab. Danach müssen Sie das Secret der Docker-Image-Registrierung verlängern.

Überblick über die Implementierung für AWS

Hier finden Sie eine Übersicht über die Vorgehensweise zur Installation des Astra Control Center für AWS mit Cloud Volumes ONTAP als Storage-Backend.

Jeder dieser Schritte wird unten im Detail erklärt.

1. dass Sie über ausreichende IAM-Berechtigungen verfügen.
2. Installation eines RedHat OpenShift-Clusters in AWS.
3. Konfigurieren von AWS.
4. Konfiguration von NetApp BlueXP für AWS.
5. Installieren Sie Astra Control Center für AWS.

Stellen Sie sicher, dass Sie über ausreichende IAM-Berechtigungen verfügen

Stellen Sie sicher, dass Sie über ausreichende IAM-Rollen und -Berechtigungen verfügen, mit denen Sie ein RedHat OpenShift Cluster und einen NetApp BlueXP (ehemals Cloud Manager) Connector installieren können.

Siehe "Erste AWS Zugangsdaten".

Installation eines RedHat OpenShift-Clusters in AWS

Installation eines RedHat OpenShift-Container-Plattform-Clusters auf AWS

Installationsanweisungen finden Sie unter "Installation eines Clusters auf AWS in OpenShift Container Platform".

Konfigurieren von AWS

Konfigurieren Sie als nächstes AWS, um ein virtuelles Netzwerk zu erstellen, EC2 Computing-Instanzen einzurichten und einen AWS S3-Bucket zu erstellen. Wenn Sie nicht auf den zugreifen können NetApp Astra Control Center Image-RegistrierungSie müssen auch eine Elastic Container Registry (ECR) erstellen, um die Astra Control Center-Images zu hosten und die Bilder in diese Registry zu verschieben.

Folgen Sie der AWS Dokumentation, um die folgenden Schritte auszuführen. Siehe "AWS Installationsdokumentation".

1. Virtuelles AWS Netzwerk erstellen.
2. EC2 Computing-Instanzen prüfen. Dabei können es sich um einen Bare Metal Server oder VMs in AWS handelt.
3. Wenn der Instanztyp nicht bereits den Mindestanforderungen für Ressourcen von Astra für Master- und Worker-Nodes entspricht, ändern Sie den Instanztyp in AWS, um die Astra-Anforderungen zu erfüllen. Siehe "Anforderungen des Astra Control Centers".

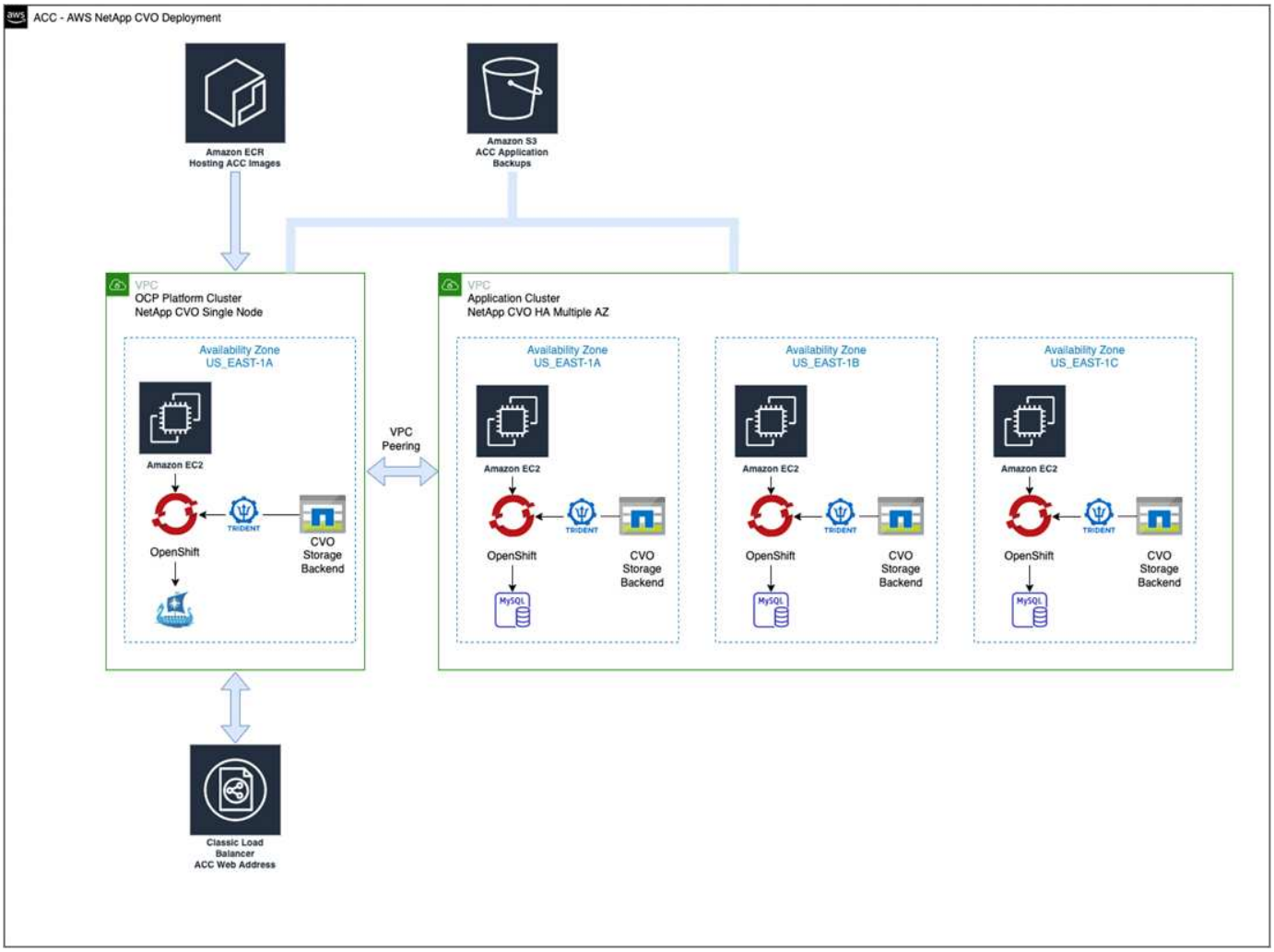
4. Erstellen Sie mindestens einen AWS S3-Bucket zum Speichern Ihrer Backups.
5. (Optional) Wenn Sie nicht auf den zugreifen können NetApp-Image-Registrierung, Gehen Sie wie folgt vor:
   a. Eine AWS Elastic Container Registry (ECR) erstellen, um alle Astra Control Center Images zu hosten.

> Wenn Sie den ECR nicht erstellen, kann Astra Control Center mit einem AWS Backend nicht auf die Monitoring-Daten von einem Cluster mit Cloud Volumes ONTAP zugreifen. Das Problem wird verursacht, wenn der Cluster, den Sie mit Astra Control Center ermitteln und verwalten möchten, keinen AWS ECR-Zugriff hat.

   b. Übertragen Sie die Astra Control Center Images in Ihre definierte Registrierung.

> Das AWS Elastic Container Registry (ECR) Token läuft nach 12 Stunden ab und verursacht das Fehlschlagen clusterübergreifender Klonvorgänge. Dieses Problem tritt auf, wenn ein Storage-Back-End von für AWS konfigurierten Cloud Volumes ONTAP gemanagt wird. Um dieses Problem zu beheben, müssen Sie sich erneut mit der ECR authentifizieren und ein neues Geheimnis generieren, damit Klonvorgänge erfolgreich fortgesetzt werden können.

Beispiel für eine AWS Implementierung:



Konfiguration von NetApp BlueXP für AWS

Erstellen Sie mit NetApp BlueXP (früher Cloud Manager) einen Workspace, fügen Sie eine Connector zu AWS hinzu, erstellen Sie eine Arbeitsumgebung und importieren Sie das Cluster.

Befolgen Sie die BlueXP-Dokumentation, um die folgenden Schritte auszuführen. Siehe folgendes:

- "Erste Schritte mit Cloud Volumes ONTAP in AWS".
- "Erstellen Sie einen Connector in AWS mit BlueXP"

Schritte

1. Fügen Sie Ihre Anmeldeinformationen zu BlueXP hinzu.
2. Erstellen Sie einen Arbeitsbereich.
3. Fügen Sie einen Connector für AWS hinzu. Entscheiden Sie sich für AWS als Provider.
4. Schaffen Sie eine Arbeitsumgebung für Ihre Cloud-Umgebung.
   a. Ort: „Amazon Web Services (AWS)“
   b. Typ: „Cloud Volumes ONTAP HA“
5. Importieren Sie den OpenShift-Cluster. Der Cluster wird mit der gerade erstellten Arbeitsumgebung verbunden.
   a. Zeigen Sie die NetApp Cluster-Details an, indem Sie **K8s** > **Cluster list** > **Cluster-Details** wählen.
   b. Beachten Sie in der oberen rechten Ecke die Astra Trident-Version.
   c. Beachten Sie die Cloud Volumes ONTAP Cluster-Storage-Klassen, für die NetApp als provisionierung angezeigt wird.

      Dies importiert Ihr Red hat OpenShift-Cluster und weist ihm eine Standardspeicherklasse zu. Sie wählen die Speicherklasse aus.
      Astra Trident wird automatisch im Rahmen des Imports und der Erkennung installiert.
6. Beachten Sie alle persistenten Volumes und Volumes in dieser Cloud Volumes ONTAP-Implementierung.

> Cloud Volumes ONTAP kann als Single Node oder in High Availability betrieben werden. Wenn HA aktiviert ist, notieren Sie den HA-Status und den Implementierungsstatus der Nodes, die in AWS ausgeführt werden.

Installieren Sie Astra Control Center für AWS

Dem Standard folgen "Installationsanweisungen für Astra Control Center".

> AWS verwendet den Bucket-Typ generischer S3.

Implementieren Sie Astra Control Center in der Google Cloud Platform

Astra Control Center lässt sich in einem selbst gemanagten Kubernetes-Cluster implementieren, der auf einer Google Cloud Platform (GCP) Public Cloud gehostet wird.

Was wird für GCP benötigt

Vor der Implementierung von Astra Control Center in GCP sind folgende Elemente erforderlich:

- Astra Control Center-Lizenz: Siehe "Lizenzierungsanforderungen für Astra Control Center".
- "Sie erfüllen die Anforderungen des Astra Control Centers".
- NetApp Cloud Central Konto
- Bei Verwendung von OCP, Red hat OpenShift Container Platform (OCP) 4.11 bis 4.13
- Bei Verwendung von OCP, Berechtigungen für die Red hat OpenShift Container Platform (OCP) (auf Namespace-Ebene zum Erstellen von Pods)
- GCP-Servicekonto mit Berechtigungen, mit denen Sie Buckets und Konnektoren erstellen können

Anforderungen an die Betriebsumgebung für GCP

Stellen Sie sicher, dass die Betriebsumgebung, die Sie als Host für das Astra Control Center auswählen, den grundlegenden Ressourcenanforderungen in der offiziellen Dokumentation der Umgebung entspricht.

Astra Control Center erfordert zusätzlich zu den Ressourcenanforderungen der Umgebung die folgenden Ressourcen:

Komponente	Anforderungen
Back-End NetApp Cloud Volumes ONTAP Storage-Kapazität	Mindestens 300 GB verfügbar
Worker-Nodes (GCP-Compute-Anforderung)	Insgesamt mindestens 3 Worker-Nodes mit 4 vCPU-Kernen und jeweils 12 GB RAM
Load Balancer	Der Servicetyp „loadbalancer“ ist für den Ingress Traffic verfügbar, der an Services im Cluster der Betriebsumgebung gesendet werden kann
FQDN (GCP-DNS-ZONE)	Eine Methode zum Zeigen des FQDN von Astra Control Center auf die Load Balanced IP-Adresse
Astra Trident (installiert im Rahmen der Kubernetes Cluster Discovery in NetApp BlueXP, ehemals Cloud Manager)	Astra Trident 23.01 oder höher installiert und konfiguriert und NetApp ONTAP Version 9.9.1 oder höher als Storage-Backend

Komponente	Anforderungen
Bildregistrierung	NetApp stellt eine Registrierung bereit, mit der Sie Astra Control Center Build-Images abrufen können: `http://netappdownloads.jfrog.io/docker-astra-control-prod` Wenden Sie sich an den NetApp-Support, um Anweisungen zur Verwendung dieser Image-Registrierung während der Installation von Astra Control Center zu erhalten. Wenn Sie nicht auf die NetApp-Image-Registrierung zugreifen können, benötigen Sie eine bestehende private Registrierung, wie z. B. die Google-Container-Registrierung, auf die Sie die Build-Images des Astra Control Centers übertragen können. Sie müssen die URL der Bildregistrierung angeben, in der Sie die Bilder hochladen. Sie müssen anonymen Zugriff aktivieren, um Restic Images für Backups zu erstellen.
Konfiguration von Astra Trident/ONTAP	Astra Control Center erfordert, dass eine Storage-Klasse erstellt und als Standard-Storage-Klasse eingestellt wird. Astra Control Center unterstützt die folgenden ONTAP Kubernetes Storage-Klassen, die beim Import des Kubernetes Clusters in NetApp BlueXP erstellt werden. Die folgenden Aufgaben werden von Astra Trident bereitgestellt: • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

Bei diesen Anforderungen wird davon ausgegangen, dass Astra Control Center die einzige Applikation ist, die in der Betriebsumgebung ausgeführt wird. Wenn in der Umgebung zusätzliche Applikationen ausgeführt werden, passen Sie diese Mindestanforderungen entsprechend an.

Übersicht über die Implementierung für GCP

Hier ist eine Übersicht über die Vorgehensweise bei der Installation des Astra Control Center auf einem selbst verwalteten OCP-Cluster in GCP mit Cloud Volumes ONTAP als Storage-Backend.

Jeder dieser Schritte wird unten im Detail erklärt.

1. Installieren Sie einen RedHat OpenShift-Cluster auf GCP.
2. Erstellung eines GCP-Projekts und einer virtuellen Private Cloud.
3. dass Sie über ausreichende IAM-Berechtigungen verfügen.

4. GCP konfigurieren.
5. NetApp BlueXP für GCP konfigurieren.
6. Astra Control Center für GCP installieren.

Installieren Sie einen RedHat OpenShift-Cluster auf GCP

Der erste Schritt ist die Installation eines RedHat OpenShift-Clusters auf GCP.

Anweisungen zur Installation finden Sie im folgenden Abschnitt:

- "Installation eines OpenShift-Clusters in GCP"
- "Erstellen eines GCP-Service-Kontos"

Erstellung eines GCP-Projekts und einer virtuellen Private Cloud

Erstellung von mindestens einem GCP-Projekt und einer Virtual Private Cloud (VPC).

> OpenShift kann möglicherweise eigene Ressourcengruppen erstellen. Darüber hinaus sollte auch eine GCP VPC definiert werden. Siehe OpenShift-Dokumentation.

Sie können eine Plattformcluster-Ressourcengruppe und eine Zielapplikation OpenShift-Cluster-Ressourcengruppe erstellen.

Stellen Sie sicher, dass Sie über ausreichende IAM-Berechtigungen verfügen

Stellen Sie sicher, dass Sie über ausreichende IAM-Rollen und -Berechtigungen verfügen, mit denen Sie ein RedHat OpenShift Cluster und einen NetApp BlueXP (ehemals Cloud Manager) Connector installieren können.

Siehe "Erste GCP-Zugangsdaten und -Berechtigungen".

GCP konfigurieren

Konfigurieren Sie anschließend GCP für die Erstellung einer VPC, die Einrichtung von Computing-Instanzen und die Erstellung eines Google Cloud Object Storage. Wenn Sie nicht auf den zugreifen können NetApp Astra Control Center Image-Registrierung, Sie müssen auch eine Google Container Registry erstellen, um die Astra Control Center-Bilder zu hosten, und die Bilder auf diese Registrierung zu schieben.

Befolgen Sie die GCP-Dokumentation, um die folgenden Schritte auszuführen. Siehe Installieren des OpenShift-Clusters in GCP.

1. Erstellen eines GCP-Projekts und der VPC in der GCP, die Sie für den OCP-Cluster mit dem CVO-Back-End verwenden möchten
2. Prüfen Sie die Computing-Instanzen. Dabei kann es sich um einen Bare Metal Server oder VMs in GCP handelt.
3. Wenn der Instanztyp nicht bereits den Astra-Mindestanforderungen für die Ressourcen für Master- und Worker-Nodes entspricht, ändern Sie den Instanztyp in GCP, um die Astra-Anforderungen zu erfüllen. Siehe "Anforderungen des Astra Control Centers".
4. Erstellen Sie mindestens einen GCP Cloud Storage Bucket, um Ihre Backups zu speichern.
5. Erstellen eines Geheimnisses, das für den Bucket-Zugriff erforderlich ist
6. (Optional) Wenn Sie nicht auf den zugreifen können NetApp-Image-Registrierung, Gehen Sie wie folgt vor:

a. Erstellen Sie eine Google Container Registry, um die Astra Control Center-Images zu hosten.
b. Richten Sie Google Container Registry-Zugriff für Docker Push/Pull für alle Astra Control Center-Bilder ein.

   Beispiel: Astra Control Center-Bilder können in diese Registrierung verschoben werden, indem das folgende Skript eingegeben wird:

   ```
   gcloud auth activate-service-account <service account email address>
   --key-file=<GCP Service Account JSON file>
   ```

   Dieses Skript erfordert eine Astra Control Center Manifest-Datei und Ihren Google Image Registry-Speicherort. Beispiel:

```
manifestfile=acc.manifest.bundle.yaml
GCP_CR_REGISTRY=<target GCP image registry>
ASTRA_REGISTRY=<source Astra Control Center image registry>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image
    docker push $GCP_CR_REGISTRY/$image
done < acc.manifest.bundle.yaml
```

7. Richten Sie DNS-Zonen ein.

NetApp BlueXP für GCP konfigurieren

Erstellen Sie mithilfe von NetApp BlueXP (früher Cloud Manager) einen Workspace, fügen Sie eine Connector zur GCP hinzu, erstellen Sie eine Arbeitsumgebung und importieren Sie das Cluster.

Befolgen Sie die BlueXP-Dokumentation, um die folgenden Schritte auszuführen. Siehe "Erste Schritte mit Cloud Volumes ONTAP in GCP".

Bevor Sie beginnen

- Zugriff auf das GCP-Servicekonto mit den erforderlichen IAM-Berechtigungen und -Rollen

Schritte

1. Fügen Sie Ihre Anmeldeinformationen zu BlueXP hinzu. Siehe "GCP-Konten hinzufügen".
2. Fügen Sie einen Connector für GCP hinzu.
   a. Entscheiden Sie sich für „GCP“ als Provider.
   b. GCP-Zugangsdaten eingeben. Siehe "Erstellen eines Connectors in GCP von BlueXP".
   c. Stellen Sie sicher, dass der Anschluss läuft, und wechseln Sie zu diesem Anschluss.
3. Schaffen Sie eine Arbeitsumgebung für Ihre Cloud-Umgebung.

a. Ort: „GCP“
b. Typ: „Cloud Volumes ONTAP HA“

4. Importieren Sie den OpenShift-Cluster. Der Cluster wird mit der gerade erstellten Arbeitsumgebung verbunden.
   a. Zeigen Sie die NetApp Cluster-Details an, indem Sie **K8s** > **Cluster list** > **Cluster-Details** wählen.
   b. Beachten Sie oben rechts die Trident-Version.
   c. Beachten Sie die Cloud Volumes ONTAP Cluster-Storage-Klassen mit „NetApp“ als provisionierung.

      Dies importiert Ihr Red hat OpenShift-Cluster und weist ihm eine Standardspeicherklasse zu. Sie wählen die Speicherklasse aus.
      Astra Trident wird automatisch im Rahmen des Imports und der Erkennung installiert.

5. Beachten Sie alle persistenten Volumes und Volumes in dieser Cloud Volumes ONTAP-Implementierung.

Cloud Volumes ONTAP kann als Single Node oder in High Availability (HA) betrieben werden. Wenn HA aktiviert ist, notieren Sie den HA-Status und den Node-Implementierungsstatus, der in GCP ausgeführt wird.

Astra Control Center für GCP installieren

Dem Standard folgen "Installationsanweisungen für Astra Control Center".

GCP verwendet den allgemeinen S3-Bucket-Typ.

1. Generieren Sie das Docker Secret, um Bilder für die Astra Control Center-Installation zu übertragen:

```
kubectl create secret docker-registry <secret name> --docker
-server=<Registry location> --docker-username=_json_key --docker
-password="$(cat <GCP Service Account JSON file>)" --namespace=pcloud
```

Implementieren Sie Astra Control Center in Microsoft Azure

Astra Control Center lässt sich in einem selbst gemanagten Kubernetes-Cluster implementieren, der in einer Microsoft Azure Public Cloud gehostet wird.

Was Sie für Azure benötigen

Vor der Implementierung von Astra Control Center in Azure sind folgende Fragen erforderlich:

- Astra Control Center-Lizenz: Siehe "Lizenzierungsanforderungen für Astra Control Center".
- "Sie erfüllen die Anforderungen des Astra Control Centers".
- NetApp Cloud Central Konto
- Bei Verwendung von OCP, Red hat OpenShift Container Platform (OCP) 4.11 bis 4.13
- Bei Verwendung von OCP, Berechtigungen für die Red hat OpenShift Container Platform (OCP) (auf Namespace-Ebene zum Erstellen von Pods)
- Azure Zugangsdaten mit Berechtigungen, mit denen Sie Buckets und Konnektoren erstellen können

Anforderungen an die Betriebsumgebung für Azure

Stellen Sie sicher, dass die Betriebsumgebung, die Sie als Host für das Astra Control Center auswählen, den grundlegenden Ressourcenanforderungen in der offiziellen Dokumentation der Umgebung entspricht.

Astra Control Center erfordert zusätzlich zu den Ressourcenanforderungen der Umgebung die folgenden Ressourcen:

Siehe "Anforderungen an die Betriebsumgebung des Astra Control Centers".

Komponente	Anforderungen
Back-End NetApp Cloud Volumes ONTAP Storage-Kapazität	Mindestens 300 GB verfügbar
Worker-Nodes (Azure-Computing-Anforderung)	Insgesamt mindestens 3 Worker-Nodes mit 4 vCPU-Kernen und jeweils 12 GB RAM
Load Balancer	Der Servicetyp „loadbalancer“ ist für den Ingress Traffic verfügbar, der an Services im Cluster der Betriebsumgebung gesendet werden kann
FQDN (Azure-DNS-Zone)	Eine Methode zum Zeigen des FQDN von Astra Control Center auf die Load Balanced IP-Adresse
Astra Trident (installiert im Rahmen der Kubernetes Cluster Discovery in NetApp BlueXP)	Astra Trident 23.01 oder höher installiert und konfiguriert und NetApp ONTAP Version 9.9.1 oder höher wird als Storage-Backend verwendet
Bildregistrierung	NetApp stellt eine Registrierung bereit, mit der Sie Astra Control Center Build-Images abrufen können: `http://netappdownloads.jfrog.io/docker-astra-control-prod` Wenden Sie sich an den NetApp-Support, um Anweisungen zur Verwendung dieser Image-Registrierung während der Installation von Astra Control Center zu erhalten. Wenn Sie nicht auf die NetApp-Image-Registrierung zugreifen können, benötigen Sie eine bestehende private Registrierung, wie z. B. die Azure-Container-Registrierung (ACR), auf die Sie die Build-Images des Astra Control Centers übertragen können. Sie müssen die URL der Bildregistrierung angeben, in der Sie die Bilder hochladen. Sie müssen anonymen Zugriff aktivieren, um Restic Images für Backups zu erstellen.

Komponente	Anforderungen
Konfiguration von Astra Trident/ONTAP	Astra Control Center erfordert, dass eine Storage-Klasse erstellt und als Standard-Storage-Klasse eingestellt wird. Astra Control Center unterstützt die folgenden ONTAP Kubernetes Storage-Klassen, die beim Import des Kubernetes Clusters in NetApp BlueXP erstellt werden. Die folgenden Aufgaben werden von Astra Trident bereitgestellt: • `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io` • `vsaworkingenvironment-<>-single-san csi.trident.netapp.io`

Bei diesen Anforderungen wird davon ausgegangen, dass Astra Control Center die einzige Applikation ist, die in der Betriebsumgebung ausgeführt wird. Wenn in der Umgebung zusätzliche Applikationen ausgeführt werden, passen Sie diese Mindestanforderungen entsprechend an.

Überblick über die Implementierung für Azure

Hier finden Sie eine Übersicht über die Vorgehensweise zur Installation von Astra Control Center für Azure.

Jeder dieser Schritte wird unten im Detail erklärt.

1. Installieren Sie einen RedHat OpenShift-Cluster auf Azure.
2. Erstellen von Azure Ressourcengruppen.
3. dass Sie über ausreichende IAM-Berechtigungen verfügen.
4. Konfigurieren Sie Azure.
5. Konfiguration von NetApp BlueXP (ehemals Cloud Manager) für Azure.
6. Installation und Konfiguration von Astra Control Center für Azure.

Installieren Sie einen RedHat OpenShift-Cluster auf Azure

Der erste Schritt ist die Installation eines RedHat OpenShift-Clusters unter Azure.

Anweisungen zur Installation finden Sie im folgenden Abschnitt:

- "OpenShift-Cluster wird auf Azure installiert".
- "Installieren eines Azure-Kontos".

Erstellen von Azure Ressourcengruppen

Erstellen Sie mindestens eine Azure-Ressourcengruppe.

OpenShift kann möglicherweise eigene Ressourcengruppen erstellen. Zusätzlich sollten Sie auch Azure-Ressourcengruppen definieren. Siehe OpenShift-Dokumentation.

Sie können eine Plattformcluster-Ressourcengruppe und eine Zielapplikation OpenShift-Cluster-Ressourcengruppe erstellen.

Stellen Sie sicher, dass Sie über ausreichende IAM-Berechtigungen verfügen

Stellen Sie sicher, dass Sie über ausreichende IAM-Rollen und -Berechtigungen verfügen, mit denen Sie ein RedHat OpenShift-Cluster und einen NetApp BlueXP Connector installieren können.

Siehe "Azure Zugangsdaten und Berechtigungen".

Konfigurieren Sie Azure

Konfigurieren Sie als nächstes Azure, um ein virtuelles Netzwerk zu erstellen, Compute-Instanzen einzurichten und einen Azure Blob-Container zu erstellen. Wenn Sie nicht auf den zugreifen können NetApp Astra Control Center Image-RegistrierungSie müssen auch eine Azure Container Registry (ACR) erstellen, um die Astra Control Center-Images zu hosten und die Bilder in diese Registrierung zu verschieben.

Folgen Sie der Azure-Dokumentation, um die folgenden Schritte durchzuführen. Siehe "OpenShift-Cluster wird auf Azure installiert".

1. Virtuelles Azure Netzwerk erstellen.
2. Prüfen Sie die Computing-Instanzen. Dabei können es sich um einen Bare Metal Server oder VMs in Azure handelt.
3. Wenn der Instanztyp nicht bereits den Mindestanforderungen für Ressourcen von Astra für Master- und Worker-Nodes entspricht, ändern Sie den Instanztyp in Azure, um die Astra-Anforderungen zu erfüllen. Siehe "Anforderungen des Astra Control Centers".
4. Erstellen Sie mindestens einen Azure Blob Container, um Ihre Backups zu speichern.
5. Erstellen Sie ein Speicherkonto. Sie benötigen ein Storage-Konto, um einen Container zu erstellen, der im Astra Control Center als Bucket verwendet wird.
6. Erstellen eines Geheimnisses, das für den Bucket-Zugriff erforderlich ist
7. (Optional) Wenn Sie nicht auf den zugreifen können NetApp-Image-Registrierung, Gehen Sie wie folgt vor:
    a. Azure Container Registry (ACR) erstellen, um die Astra Control Center Images zu hosten.
    b. ACR-Zugriff für Docker Push/Pull für alle Astra Control Center Images einrichten
    c. Übertragen Sie die Astra Control Center-Images mithilfe des folgenden Skripts in diese Registrierung:

```
az acr login -n <AZ ACR URL/Location>
This script requires the Astra Control Center manifest file and your
Azure ACR location.
```

        - Beispiel*:

```
manifestfile=acc.manifest.bundle.yaml
AZ_ACR_REGISTRY=<target Azure ACR image registry>
ASTRA_REGISTRY=<source Astra Control Center image registry>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image
    docker push $AZ_ACR_REGISTRY/$image
done < acc.manifest.bundle.yaml
```

8. Richten Sie DNS-Zonen ein.

Konfiguration von NetApp BlueXP (ehemals Cloud Manager) für Azure

Erstellen Sie mit BlueXP (früher Cloud Manager) einen Workspace, fügen Sie einen Connector zu Azure hinzu, erstellen Sie eine Arbeitsumgebung und importieren Sie das Cluster.

Befolgen Sie die BlueXP-Dokumentation, um die folgenden Schritte auszuführen. Siehe "Erste Schritte mit BlueXP in Azure".

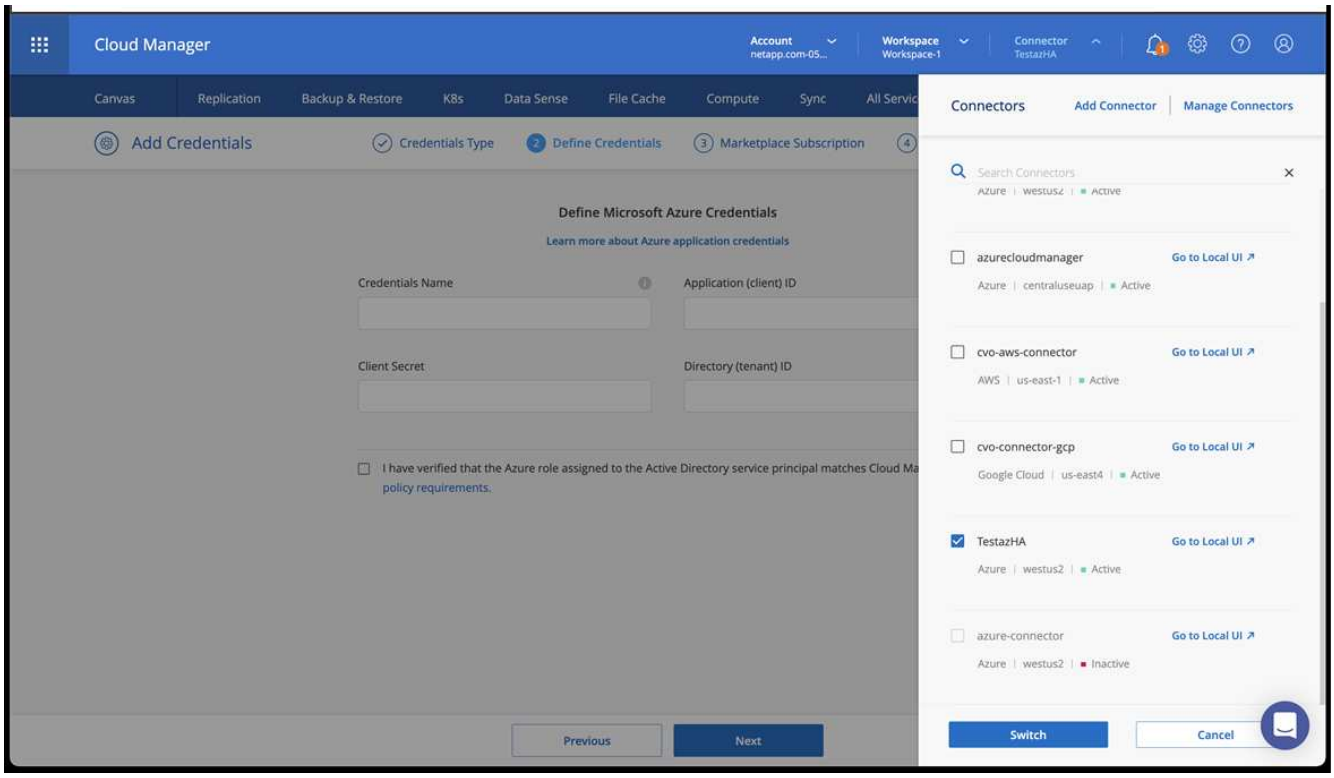
Bevor Sie beginnen

Zugriff auf das Azure Konto mit den erforderlichen IAM-Berechtigungen und -Rollen

Schritte

1. Fügen Sie Ihre Anmeldeinformationen zu BlueXP hinzu.
2. Fügen Sie einen Connector für Azure hinzu. Siehe "BlueXP-Richtlinien".
   a. Wählen Sie als Provider * Azure* aus.
   b. Geben Sie die Azure-Zugangsdaten ein, einschließlich der Anwendungs-ID, des Client-Geheimdienstes und der Verzeichniskennung (Mandanten).

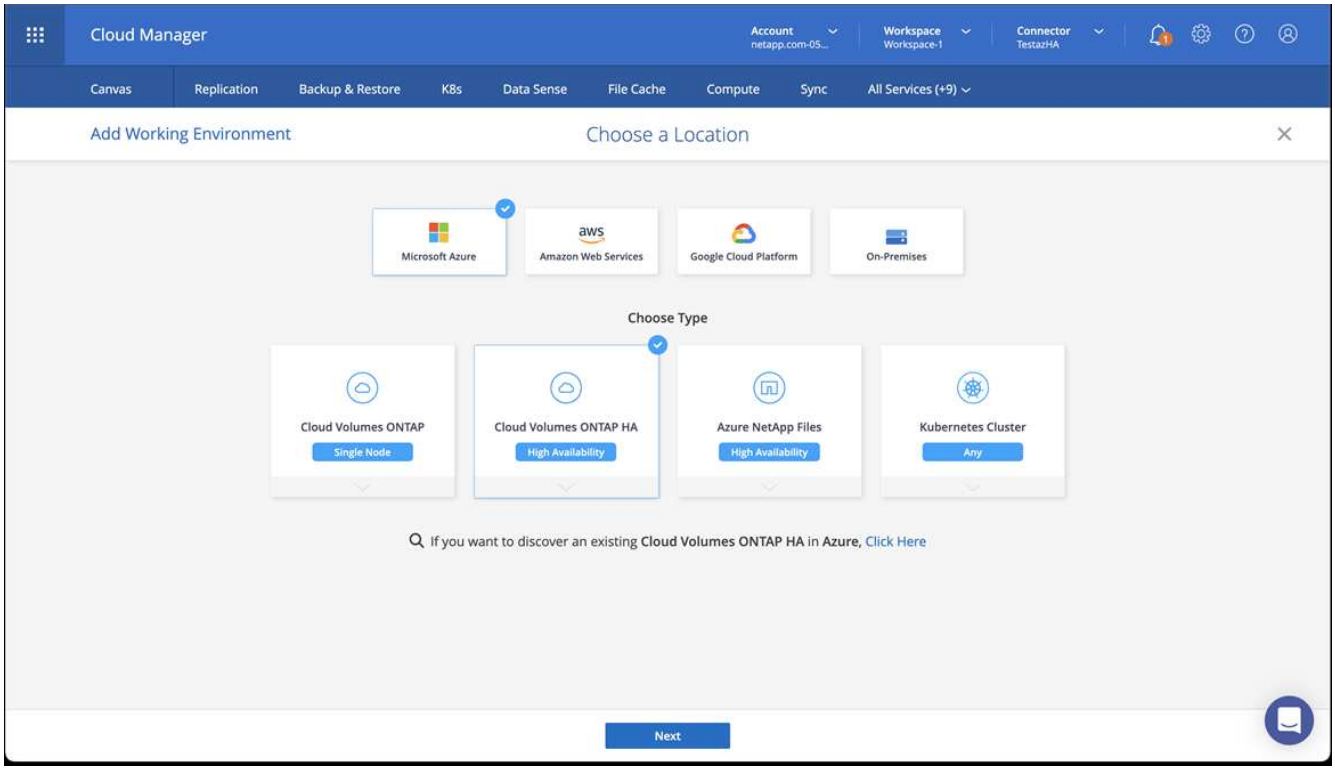
      Siehe "Erstellen eines Konnektors in Azure aus BlueXPr".
3. Stellen Sie sicher, dass der Anschluss läuft, und wechseln Sie zu diesem Anschluss.



4. Schaffen Sie eine Arbeitsumgebung für Ihre Cloud-Umgebung.

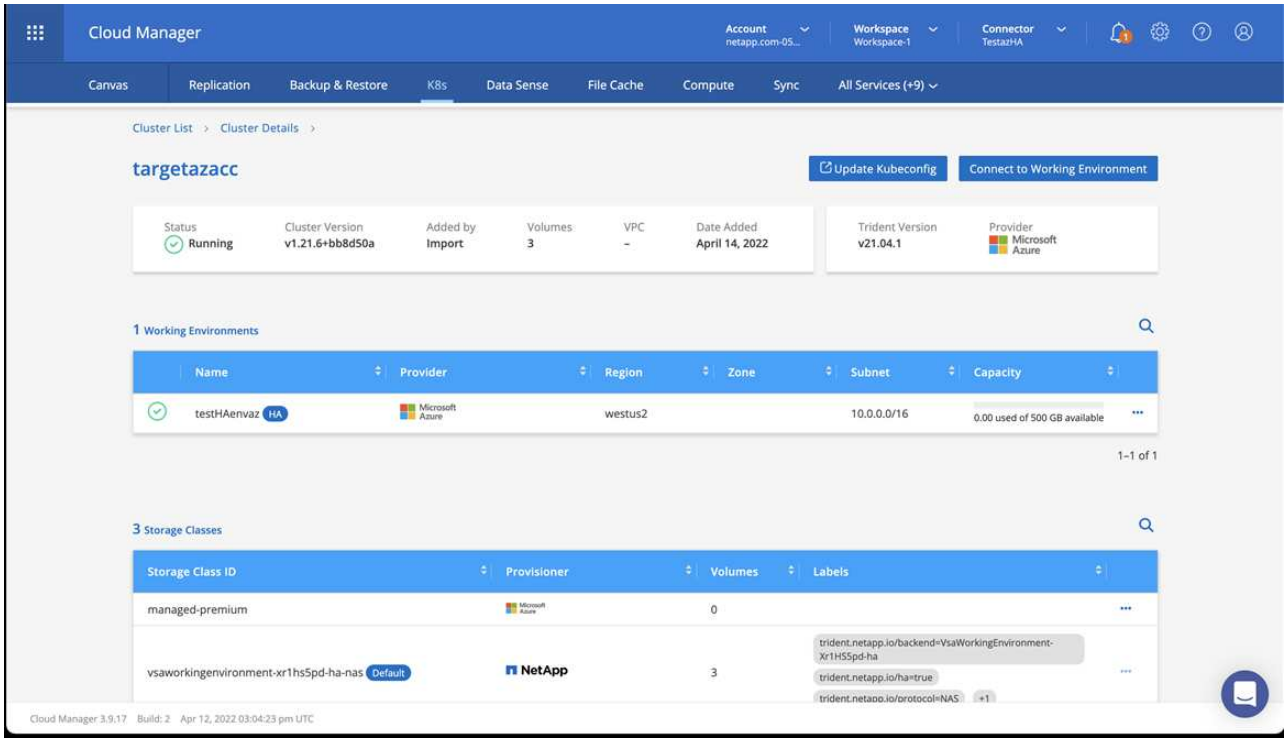
   a. Ort: „Microsoft Azure“.

   b. Typ: „Cloud Volumes ONTAP HA“.



5. Importieren Sie den OpenShift-Cluster. Der Cluster wird mit der gerade erstellten Arbeitsumgebung verbunden.

a. Zeigen Sie die NetApp Cluster-Details an, indem Sie **K8s** > **Cluster list** > **Cluster-Details** wählen.



b. Beachten Sie in der oberen rechten Ecke die Astra Trident-Version.

c. Beachten Sie die Cloud Volumes ONTAP Cluster-Storage-Klassen, für die NetApp als provisionierung angezeigt wird.

Damit wird Ihr Red hat OpenShift-Cluster importiert und eine Standardspeicherklasse zugewiesen. Sie wählen die Speicherklasse aus.
Astra Trident wird automatisch im Rahmen des Imports und der Erkennung installiert.

6. Beachten Sie alle persistenten Volumes und Volumes in dieser Cloud Volumes ONTAP-Implementierung.
7. Cloud Volumes ONTAP kann als Single Node oder in High Availability betrieben werden. Wenn HA aktiviert ist, notieren Sie den HA-Status und den Node-Implementierungsstatus, der in Azure ausgeführt wird.

Installation und Konfiguration von Astra Control Center für Azure

Installieren Sie Astra Control Center standardmäßig "Installationsanweisungen".

Fügen Sie über Astra Control Center einen Azure-Bucket hinzu. Siehe "Astra Control Center einrichten und Buckets hinzufügen".

Konfigurieren Sie nach der Installation das Astra Control Center

Je nach Umgebung kann es nach der Installation des Astra Control Center zusätzliche Konfigurationsmöglichkeiten geben.

Ressourceneinschränkungen entfernen

In einigen Umgebungen werden die Objekte ResourceQuotas und LimitRanges verwendet, um zu verhindern, dass die Ressourcen in einem Namespace alle verfügbaren CPUs und Speicher im Cluster verbrauchen. Das Astra Control Center stellt keine Höchstgrenzen ein, sodass diese Ressourcen nicht eingehalten werden.

Wenn Ihre Umgebung auf diese Weise konfiguriert ist, müssen Sie diese Ressourcen aus den Namespaces entfernen, in denen Sie Astra Control Center installieren möchten.

Sie können folgende Schritte verwenden, um diese Kontingente und Grenzen abzurufen und zu entfernen. In diesen Beispielen wird die Befehlsausgabe direkt nach dem Befehl angezeigt.

Schritte

1. Erhalten Sie die Ressourcen-Kontingente im `netapp-acc` (Oder benutzerdefinierter Name) Namespace:

```
kubectl get quota -n [netapp-acc or custom namespace]
```

Antwort:

```
NAME          AGE   REQUEST                                                 LIMIT
pods-high     16s   requests.cpu: 0/20, requests.memory: 0/100Gi
limits.cpu: 0/200, limits.memory: 0/1000Gi
pods-low      15s   requests.cpu: 0/1, requests.memory: 0/1Gi
limits.cpu: 0/2, limits.memory: 0/2Gi
pods-medium   16s   requests.cpu: 0/10, requests.memory: 0/20Gi
limits.cpu: 0/20, limits.memory: 0/200Gi
```

2. Alle Ressourcen-Kontingente nach Namen löschen:

```
kubectl delete resourcequota pods-high -n [netapp-acc or custom
namespace]
```

```
kubectl delete resourcequota pods-low -n [netapp-acc or custom
namespace]
```

```
kubectl delete resourcequota pods-medium -n [netapp-acc or custom
namespace]
```

3. Erhalten Sie die Grenzwerte im `netapp-acc` (Oder benutzerdefinierter Name) Namespace:

```
kubectl get limits -n [netapp-acc or custom namespace]
```

Antwort:

```
NAME              CREATED AT
cpu-limit-range   2022-06-27T19:01:23Z
```

4. Grenzwerte nach Namen löschen:

```
kubectl delete limitrange cpu-limit-range -n [netapp-acc or custom
namespace]
```

Fügen Sie ein benutzerdefiniertes TLS-Zertifikat hinzu

Astra Control Center verwendet standardmäßig ein selbstsigniertes TLS-Zertifikat für Ingress-Controller-Datenverkehr (nur in bestimmten Konfigurationen) und die Web-UI-Authentifizierung mit Webbrowsern. Sie können das vorhandene selbst signierte TLS-Zertifikat entfernen und durch ein TLS-Zertifikat ersetzen, das von einer Zertifizierungsstelle (CA) signiert ist.

> Das selbstsignierte Standardzertifikat wird für zwei Verbindungstypen verwendet:
>
> - HTTPS-Verbindungen zur Web-UI des Astra Control Center
> - Ingress-Controller-Verkehr (nur wenn der `ingressType: "AccTraefik"` Das Hotel wurde in der eingerichtet `astra_control_center.yaml` Datei während Astra Control Center Installation)
>
> Durch Ersetzen des Standard-TLS-Zertifikats wird das Zertifikat ersetzt, das für die Authentifizierung für diese Verbindungen verwendet wird.

Bevor Sie beginnen

- Kubernetes-Cluster mit installiertem Astra Control Center
- Administratorzugriff auf eine Command Shell auf dem zu ausgeführten Cluster `kubectl` Befehle
- Private Schlüssel- und Zertifikatdateien aus der CA

Entfernen Sie das selbstsignierte Zertifikat

Entfernen Sie das vorhandene selbstsignierte TLS-Zertifikat.

1. Melden Sie sich mit SSH beim Kubernetes Cluster an, der als administrativer Benutzer Astra Control Center hostet.
2. Suchen Sie das mit dem aktuellen Zertifikat verknüpfte TLS-Geheimnis mit dem folgenden Befehl, Ersetzen `<ACC-deployment-namespace>` Mit dem Astra Control Center Deployment Namespace:

```
kubectl get certificate -n <ACC-deployment-namespace>
```

3. Löschen Sie den derzeit installierten Schlüssel und das Zertifikat mit den folgenden Befehlen:

```
kubectl delete cert cert-manager-certificates -n <ACC-deployment-
namespace>
```

```
kubectl delete secret secure-testing-cert -n <ACC-deployment-namespace>
```

Fügen Sie mithilfe der Befehlszeile ein neues Zertifikat hinzu

Fügen Sie ein neues TLS-Zertifikat hinzu, das von einer CA signiert wird.

1. Verwenden Sie den folgenden Befehl, um das neue TLS-Geheimnis mit dem privaten Schlüssel und den Zertifikatdateien aus der CA zu erstellen und die Argumente in Klammern <> durch die entsprechenden Informationen zu ersetzen:

```
kubectl create secret tls <secret-name> --key <private-key-filename>
--cert <certificate-filename> -n <ACC-deployment-namespace>
```

2. Verwenden Sie den folgenden Befehl und das folgende Beispiel, um die Cluster-Datei CRD (Custom Resource Definition) zu bearbeiten und die zu ändern `spec.selfSigned` Mehrwert für `spec.ca.secretName` So verweisen Sie auf das zuvor erstellte TLS-Geheimnis:

```
kubectl edit clusterissuers.cert-manager.io/cert-manager-certificates -n
<ACC-deployment-namespace>
```

   CRD:

```
#spec:
#  selfSigned: {}

spec:
  ca:
    secretName: <secret-name>
```

3. Überprüfen Sie mit den folgenden Befehlen und der Beispiel-Ausgabe, ob die Änderungen korrekt sind und das Cluster bereit ist, Zertifikate zu validieren, und ersetzen Sie sie `<ACC-deployment-namespace>` Mit dem Astra Control Center Deployment Namespace:

```
kubectl describe clusterissuers.cert-manager.io/cert-manager-
certificates -n <ACC-deployment-namespace>
```

   Antwort:

```
Status:
  Conditions:
    Last Transition Time:  2021-07-01T23:50:27Z
    Message:               Signing CA verified
    Reason:                KeyPairVerified
    Status:                True
    Type:                  Ready
Events:                    <none>
```

4. Erstellen Sie die `certificate.yaml` Datei anhand des folgenden Beispiels, Ersetzen der Platzhalterwerte in Klammern <> durch entsprechende Informationen:

```
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  <strong>name: <certificate-name></strong>
  namespace: <ACC-deployment-namespace>
spec:
  <strong>secretName: <certificate-secret-name></strong>
  duration: 2160h # 90d
  renewBefore: 360h # 15d
  dnsNames:
  <strong>- <astra.dnsname.example.com></strong> #Replace with the
correct Astra Control Center DNS address
  issuerRef:
    kind: ClusterIssuer
    name: cert-manager-certificates
```

5. Erstellen Sie das Zertifikat mit dem folgenden Befehl:

```
kubectl apply -f certificate.yaml
```

6. Überprüfen Sie mithilfe der folgenden Befehl- und Beispielausgabe, ob das Zertifikat korrekt erstellt wurde und mit den während der Erstellung angegebenen Argumenten (z. B. Name, Dauer, Verlängerungsfrist und DNS-Namen).

```
kubectl describe certificate -n <ACC-deployment-namespace>
```

Antwort:

```
Spec:
  Dns Names:
    astra.example.com
  Duration:  125h0m0s
  Issuer Ref:
    Kind:        ClusterIssuer
    Name:        cert-manager-certificates
  Renew Before:  61h0m0s
  Secret Name:   <certificate-secret-name>
Status:
  Conditions:
    Last Transition Time:  2021-07-02T00:45:41Z
    Message:               Certificate is up to date and has not expired
    Reason:                Ready
    Status:                True
    Type:                  Ready
  Not After:               2021-07-07T05:45:41Z
  Not Before:              2021-07-02T00:45:41Z
  Renewal Time:            2021-07-04T16:45:41Z
  Revision:                1
Events:                    <none>
```

7. Bearbeiten Sie das TLS speichert CRD, um mit dem folgenden Befehl und Beispiel auf Ihren neuen geheimen Zertifikatnamen zu verweisen. Ersetzen Sie die Platzhalterwerte in Klammern <> durch die entsprechenden Informationen

```
kubectl edit tlsstores.traefik.io -n <ACC-deployment-namespace>
```

CRD:

```
...
spec:
  defaultCertificate:
    secretName: <certificate-secret-name>
```

8. Bearbeiten Sie die Option Ingress CRD TLS, um mit dem folgenden Befehl und Beispiel auf Ihr neues Zertifikatgeheimnis zu verweisen und die Platzhalterwerte in Klammern <> durch entsprechende Informationen zu ersetzen:

```
kubectl edit ingressroutes.traefik.io -n <ACC-deployment-namespace>
```

CRD:

```
...
 tls:
    secretName: <certificate-secret-name>
```

9. Navigieren Sie mithilfe eines Webbrowsers zur IP-Adresse der Implementierung von Astra Control Center.
10. Vergewissern Sie sich, dass die Zertifikatdetails mit den Details des installierten Zertifikats übereinstimmen.
11. Exportieren Sie das Zertifikat und importieren Sie das Ergebnis in den Zertifikatmanager in Ihrem Webbrowser.

Einrichten des Astra Control Center

Nachdem Sie Astra Control Center installiert haben, sich bei der UI einloggen und Ihr Passwort ändern, sollten Sie eine Lizenz einrichten, Cluster hinzufügen, die Authentifizierung aktivieren, den Storage managen und Buckets hinzufügen.

Aufgaben

- Fügen Sie eine Lizenz für Astra Control Center hinzu
- Bereiten Sie Ihre Umgebung mit Astra Control auf das Cluster-Management vor
- Cluster hinzufügen
- Aktivieren Sie die Authentifizierung auf dem ONTAP Storage Back-End
- Fügen Sie ein Storage-Back-End hinzu
- Fügen Sie einen Bucket hinzu

Fügen Sie eine Lizenz für Astra Control Center hinzu

Wenn Sie Astra Control Center installieren, ist bereits eine eingebettete Evaluierungslizenz installiert. Wenn Sie Astra Control Center evaluieren, können Sie diesen Schritt überspringen.

Über die Astra Control UI oder können Sie eine neue Lizenz hinzufügen "Astra Control API".

Astra Control Center Lizenzen messen die CPU-Ressourcen mithilfe von Kubernetes-CPU-Einheiten und berücksichtigen die CPU-Ressourcen, die den Worker-Nodes aller gemanagten Kubernetes-Cluster zugewiesen sind. Lizenzen basieren auf der vCPU-Nutzung. Weitere Informationen zur Berechnung von Lizenzen finden Sie unter "Lizenzierung".

Wenn Ihre Installation die Anzahl der lizenzierten CPU-Einheiten überschreitet, verhindert Astra Control Center die Verwaltung neuer Anwendungen. Bei Überschreitung der Kapazität wird eine Meldung angezeigt.

Informationen zum Aktualisieren einer vorhandenen Testversion oder einer vollständigen Lizenz finden Sie unter "Aktualisieren einer vorhandenen Lizenz".

Bevor Sie beginnen

- Zugriff auf eine neu installierte Astra Control Center-Instanz.

- Berechtigungen für Administratorrollen.
- A "NetApp Lizenzdatei" (NLF).

Schritte

1. Melden Sie sich in der UI des Astra Control Center an.
2. Wählen Sie **Konto** > **Lizenz**.
3. Wählen Sie **Lizenz Hinzufügen**.
4. Rufen Sie die Lizenzdatei (NLF) auf, die Sie heruntergeladen haben.
5. Wählen Sie **Lizenz Hinzufügen**.

Auf der Seite **Konto** > **Lizenz** werden Lizenzinformationen, Ablaufdatum, Lizenzseriennummer, Konto-ID und verwendete CPU-Einheiten angezeigt.

Wenn Sie über eine Evaluierungslizenz verfügen und keine Daten an AutoSupport senden, sollten Sie Ihre Konto-ID speichern, um Datenverlust im Falle eines Astra Control Center-Ausfalls zu vermeiden.

Bereiten Sie Ihre Umgebung mit Astra Control auf das Cluster-Management vor

Sie sollten sicherstellen, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie ein Cluster hinzufügen. Außerdem sollten Sie Eignungsprüfungen durchführen, um sicherzustellen, dass Ihr Cluster zum Astra Control Center hinzugefügt werden kann und Rollen für das Cluster-Management schafft.

Bevor Sie beginnen

- **Umweltvoraussetzungen erfüllen**: Ihre Umgebung erfüllt die "Anforderungen an die Betriebsumgebung" Für Astra Trident und Astra Control Center.
- **Configure Worker Nodes**: Stellen Sie sicher, dass Sie die Worker Nodes in Ihrem Cluster mit den entsprechenden Speichertreibern konfigurieren, damit die Pods mit dem Backend-Speicher interagieren können.
- **Kubeconfig zugänglich machen**: Sie haben Zugang zum "Standardcluster kubeconfig" Das "Sie haben während der Installation konfiguriert".
- **Hinweise zur Zertifizierungsstelle**: Wenn Sie den Cluster mit einer kubeconfig-Datei hinzufügen, die auf eine private Zertifizierungsstelle verweist, fügen Sie die folgende Zeile zum hinzu `cluster` Abschnitt der Datei kubeconfig. So kann Astra Control das Cluster hinzufügen:

```
insecure-skip-tls-verify: true
```

- **PSA-Einschränkungen aktivieren**: Wenn in Ihrem Cluster die Durchsetzung von Pod-Sicherheitszulassung aktiviert ist, was standardmäßig für Cluster ab Kubernetes 1.25 gilt, müssen Sie die PSA-Einschränkungen für diese Namespaces aktivieren:
  - `netapp-acc-operator` Namespace:

```
kubectl label --overwrite ns netapp-acc-operator pod-
security.kubernetes.io/enforce=privileged
```

- `netapp monitoring` Namespace:

```
kubectl label --overwrite ns netapp-monitoring pod-
security.kubernetes.io/enforce=privileged
```

- **Anforderungen für Astra Trident**:
  - **Installieren Sie eine unterstützte Version**: Eine Version von Astra Trident "Unterstützt durch Astra Control Center" Installiert:

> Das können Sie "Implementieren Sie Astra Trident" Mit dem Astra Trident Operator (manuell oder mit dem Helm Chart) oder `tridentctl`. Vor der Installation oder dem Upgrade von Astra Trident sollten Sie sich die "Unterstützte Frontends, Back-Ends und Host-Konfigurationen".

  - **Konfiguration eines Astra Trident Storage-Backends**: Es muss mindestens ein Astra Trident Storage-Backend sein "Konfiguriert" Auf dem Cluster.
  - **Konfiguration einer Astra Trident Storage-Klassen**: Es muss mindestens eine Astra Trident Storage-Klasse sein "Konfiguriert" Auf dem Cluster. Wenn eine Standard-Storage-Klasse konfiguriert ist, stellen Sie sicher, dass diese die einzige Storage-Klasse mit der Standardbeschriftung ist.
  - **Konfigurieren Sie einen Astra Trident Volume Snapshot Controller und installieren Sie eine Volume Snapshot Klasse**: Der Volume Snapshot Controller muss sein "Installiert" Damit Snapshots in Astra Control erstellt werden können. Mindestens ein Astra Trident `VolumeSnapshotClass` Gewesen "Einrichtung" Durch einen Administrator.
- **Astra Control Provisioner**: Um die erweiterten Management- und Storage-Bereitstellungsfunktionen von Astra Control verwenden zu können, die nur Benutzern von Astra Control zur Verfügung stehen, müssen Sie Astra Trident 23.10 oder höher installieren und aktivieren "Funktionen für die Astra Control Provisioner".
- **ONTAP-Anmeldeinformationen**: Sie benötigen ONTAP-Anmeldeinformationen und eine Superuser- und Benutzer-ID auf dem Backing-ONTAP-System, um Apps mit Astra Control Center zu sichern und wiederherzustellen.

  Führen Sie die folgenden Befehle in der ONTAP-Befehlszeile aus:

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

- **Rancher only**: Ändern Sie beim Verwalten von Anwendungsclustern in einer Rancher-Umgebung den Standardkontext des Anwendungsclusters in der von Rancher bereitgestellten kubeconfig-Datei, um einen Steuerebenen-Kontext anstelle des Rancher API-Serverkontexts zu verwenden. So wird die Last auf dem Rancher API Server reduziert und die Performance verbessert.

Führen Sie Eignungsprüfungen durch

Führen Sie die folgenden Eignungsprüfungen durch, um sicherzustellen, dass Ihr Cluster zum Astra Control Center hinzugefügt werden kann.

Schritte

1. Testen Sie die Version von Astra Trident.

```
kubectl get tridentversions -n trident
```

Wenn Astra Trident vorhanden ist, wird eine Ausgabe wie die folgende angezeigt:

```
NAME      VERSION
trident   23.XX.X
```

Wenn Astra Trident nicht existiert, wird eine Ausgabe wie die folgende angezeigt:

```
error: the server doesn't have a resource type "tridentversions"
```

> Wenn Astra Trident nicht installiert ist oder die installierte Version nicht die neueste ist, müssen Sie die neueste Version von Astra Trident installieren, bevor Sie fortfahren. Siehe "Astra Trident-Dokumentation" Weitere Anweisungen.

2. Stellen Sie sicher, dass die Pods ausgeführt werden:

```
kubectl get pods -n trident
```

3. Ermitteln, ob die Storage-Klassen die unterstützten Astra Trident Treiber verwenden. Der bereitstellungsname sollte lauten `csi.trident.netapp.io`. Das folgende Beispiel zeigt:

```
kubectl get sc
```

Beispielantwort:

```
NAME                  PROVISIONER            RECLAIMPOLICY
VOLUMEBINDINGMODE  ALLOWVOLUMEEXPANSION  AGE
ontap-gold (default)  csi.trident.netapp.io  Delete         Immediate
true                  5d23h
```

Erstellen Sie eine Clusterrolle kubeconfig

Sie können optional eine Administratorrolle mit eingeschränkten Berechtigungen oder erweiterten Berechtigungen für Astra Control Center erstellen. Dies ist kein erforderliches Verfahren für das Astra Control Center-Setup, da Sie bereits einen kubeconfig als Teil des konfiguriert haben "Installationsprozess".

Dieses Verfahren hilft Ihnen, ein separates kubeconfig zu erstellen, wenn eines der folgenden Szenarien auf Ihre Umgebung zutrifft:

- Sie möchten die Astra Control-Berechtigungen auf die Cluster beschränken, die sie verwaltet
- Sie verwenden mehrere Kontexte und können nicht den Standard Astra Control kubeconfig verwenden, der während der Installation konfiguriert wurde, oder eine eingeschränkte Rolle mit einem einzelnen Kontext funktioniert nicht in Ihrer Umgebung

Bevor Sie beginnen

Stellen Sie sicher, dass Sie für den Cluster, den Sie verwalten möchten, vor dem Ausführen der Schritte des Verfahrens Folgendes haben:

- Kubectl v1.23 oder höher installiert
- Kubectl Zugriff auf den Cluster, den Sie mit Astra Control Center hinzufügen und verwalten möchten

> Bei diesem Verfahren benötigen Sie keinen kubectl-Zugriff auf den Cluster, auf dem Astra Control Center ausgeführt wird.

- Ein aktiver kubeconfig für den Cluster, den Sie mit Clusteradministratorrechten für den aktiven Kontext verwalten möchten

Schritte

1. Service-Konto erstellen:

   a. Erstellen Sie eine Dienstkontendatei mit dem Namen `astracontrol-service-account.yaml`.

      Passen Sie Namen und Namespace nach Bedarf an. Wenn hier Änderungen vorgenommen werden, sollten Sie die gleichen Änderungen in den folgenden Schritten anwenden.

```
<strong>astracontrol-service-account.yaml</strong>
```

+

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: astracontrol-service-account
  namespace: default
```

   a. Wenden Sie das Servicekonto an:

```
kubectl apply -f astracontrol-service-account.yaml
```

2. Erstellen Sie eine der folgenden Clusterrollen mit ausreichenden Berechtigungen für ein Cluster, das von Astra Control gemanagt werden kann:

   - **Begrenzte Clusterrolle**: Diese Rolle enthält die Mindestberechtigungen, die für die Verwaltung eines Clusters durch Astra Control erforderlich sind:

Für Schritte erweitern

i. Erstellen Sie ein `ClusterRole` Datei mit dem Namen, z. B. `astra-admin-account.yaml`.

Passen Sie Namen und Namespace nach Bedarf an. Wenn hier Änderungen vorgenommen werden, sollten Sie die gleichen Änderungen in den folgenden Schritten anwenden.

```
<strong>astra-admin-account.yaml</strong>
```

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:

# Get, List, Create, and Update all resources
# Necessary to backup and restore all resources in an app
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - get
  - list
  - create
  - patch

# Delete Resources
# Necessary for in-place restore and AppMirror failover
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - crd.projectcalico.org
  - extensions
  - networking.k8s.io
  - policy
  - rbac.authorization.k8s.io
  - snapshot.storage.k8s.io
  - trident.netapp.io
  resources:
  - configmaps
  - cronjobs
  - daemonsets
```

```
  - deployments
  - horizontalpodautoscalers
  - ingresses
  - jobs
  - namespaces
  - networkpolicies
  - persistentvolumeclaims
  - poddisruptionbudgets
  - pods
  - podtemplates
  - podsecuritypolicies
  - replicasets
  - replicationcontrollers
  - replicationcontrollers/scale
  - rolebindings
  - roles
  - secrets
  - serviceaccounts
  - services
  - statefulsets
  - tridentmirrorrelationships
  - tridentsnapshotinfos
  - volumesnapshots
  - volumesnapshotcontents
  verbs:
  - delete

# Watch resources
# Necessary to monitor progress
- apiGroups:
  - ""
  resources:
  - pods
  - replicationcontrollers
  - replicationcontrollers/scale
  verbs:
  - watch

# Update resources
- apiGroups:
  - ""
  - build.openshift.io
  - image.openshift.io
  resources:
  - builds/details
  - replicationcontrollers
```

```
  - replicationcontrollers/scale
  - imagestreams/layers
  - imagestreamtags
  - imagetags
  verbs:
  - update

# Use PodSecurityPolicies
- apiGroups:
  - extensions
  - policy
  resources:
  - podsecuritypolicies
  verbs:
  - use
```

ii. (Nur für OpenShift-Cluster) Anhängen Sie am Ende des an `astra-admin-account.yaml` Datei oder nach dem `# Use PodSecurityPolicies` Abschnitt:

```
# OpenShift security
- apiGroups:
  - security.openshift.io
  resources:
  - securitycontextconstraints
  verbs:
  - use
```

iii. Wenden Sie die Cluster-Rolle an:

```
kubectl apply -f astra-admin-account.yaml
```

- **Erweiterte Clusterrolle**: Diese Rolle enthält erweiterte Berechtigungen für einen Cluster, der von Astra Control verwaltet werden soll. Sie können diese Rolle verwenden, wenn Sie mehrere Kontexte verwenden und nicht den während der Installation konfigurierten Astra Control kubeconfig verwenden können oder eine eingeschränkte Rolle mit einem einzelnen Kontext in Ihrer Umgebung nicht funktioniert:

> Im Folgenden `ClusterRole` Schritte sind ein allgemeines Kubernetes-Beispiel. Anweisungen zu Ihrer spezifischen Umgebung finden Sie in der Dokumentation zur Kubernetes-Distribution.

Für Schritte erweitern

i. Erstellen Sie ein `ClusterRole` Datei mit dem Namen, z. B. `astra-admin-account.yaml`.

Passen Sie Namen und Namespace nach Bedarf an. Wenn hier Änderungen vorgenommen werden, sollten Sie die gleichen Änderungen in den folgenden Schritten anwenden.

```
<strong>astra-admin-account.yaml</strong>
```

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - '*'
- nonResourceURLs:
  - '*'
  verbs:
  - '*'
```

ii. Wenden Sie die Cluster-Rolle an:

```
kubectl apply -f astra-admin-account.yaml
```

3. Erstellen Sie die Cluster-Rolle, die für die Cluster-Rolle an das Service-Konto gebunden ist:

a. Erstellen Sie ein `ClusterRoleBinding` Datei aufgerufen `astracontrol-clusterrolebinding.yaml`.

Passen Sie bei Bedarf alle beim Erstellen des Dienstkontos geänderten Namen und Namespaces an.

```
<strong>astracontrol-clusterrolebinding.yaml</strong>
```

+

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astracontrol-admin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: astra-admin-account
subjects:
- kind: ServiceAccount
  name: astracontrol-service-account
  namespace: default
```

a. Wenden Sie die Bindung der Cluster-Rolle an:

```
kubectl apply -f astracontrol-clusterrolebinding.yaml
```

4. Erstellen und Anwenden des Token-Geheimnisses:

a. Erstellen Sie eine Geheimdatei mit dem Namen Token `secret-astracontrol-service-account.yaml`.

```
<strong>secret-astracontrol-service-account.yaml</strong>
```

```
apiVersion: v1
kind: Secret
metadata:
  name: secret-astracontrol-service-account
  namespace: default
  annotations:
    kubernetes.io/service-account.name: "astracontrol-service-
account"
type: kubernetes.io/service-account-token
```

b. Wenden Sie den Token-Schlüssel an:

```
kubectl apply -f secret-astracontrol-service-account.yaml
```

5. Fügen Sie dem Dienstkonto den Token-Schlüssel hinzu, indem Sie den Namen dem hinzufügen `secrets` Array (die letzte Zeile im folgenden Beispiel):

```
kubectl edit sa astracontrol-service-account
```

```
apiVersion: v1
imagePullSecrets:
- name: astracontrol-service-account-dockercfg-48xhx
kind: ServiceAccount
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |

{"apiVersion":"v1","kind":"ServiceAccount","metadata":{"annotations":{},
"name":"astracontrol-service-account","namespace":"default"}}
  creationTimestamp: "2023-06-14T15:25:45Z"
  name: astracontrol-service-account
  namespace: default
  resourceVersion: "2767069"
  uid: 2ce068c4-810e-4a96-ada3-49cbf9ec3f89
secrets:
- name: astracontrol-service-account-dockercfg-48xhx
<strong>- name: secret-astracontrol-service-account</strong>
```

6. Listen Sie die Geheimnisse des Dienstkontos auf, ersetzen Sie `<context>` Mit dem richtigen Kontext für Ihre Installation:

```
kubectl get serviceaccount astracontrol-service-account --context
<context> --namespace default -o json
```

Das Ende der Ausgabe sollte wie folgt aussehen:

```
"secrets": [
{ "name": "astracontrol-service-account-dockercfg-48xhx"},
{ "name": "secret-astracontrol-service-account"}
]
```

Die Indizes für jedes Element im `secrets` Array beginnt mit 0. Im obigen Beispiel der Index für `astracontrol-service-account-dockercfg-48xhx` Wäre 0 und der Index für `secret-astracontrol-service-account` Sind es 1. Notieren Sie sich in Ihrer Ausgabe die Indexnummer für den Geheimschlüssel des Dienstkontos. Diese Indexnummer benötigen Sie im nächsten Schritt.

7. Erzeugen Sie den kubeconfig wie folgt:

   a. Erstellen Sie ein `create-kubeconfig.sh` Datei: Austausch `TOKEN_INDEX` Am Anfang des folgenden Skripts mit dem korrekten Wert.

```
<strong>create-kubeconfig.sh</strong>
```

```
# Update these to match your environment.
# Replace TOKEN_INDEX with the correct value
# from the output in the previous step. If you
# didn't change anything else above, don't change
# anything else here.

SERVICE_ACCOUNT_NAME=astracontrol-service-account
NAMESPACE=default
NEW_CONTEXT=astracontrol
KUBECONFIG_FILE='kubeconfig-sa'

CONTEXT=$(kubectl config current-context)

SECRET_NAME=$(kubectl get serviceaccount ${SERVICE_ACCOUNT_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.secrets[TOKEN_INDEX].name}')
TOKEN_DATA=$(kubectl get secret ${SECRET_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.data.token}')

TOKEN=$(echo ${TOKEN_DATA} | base64 -d)

# Create dedicated kubeconfig
# Create a full copy
kubectl config view --raw > ${KUBECONFIG_FILE}.full.tmp

# Switch working context to correct context
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp config use-context
${CONTEXT}

# Minify
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp \
  config view --flatten --minify > ${KUBECONFIG_FILE}.tmp

# Rename context
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  rename-context ${CONTEXT} ${NEW_CONTEXT}

# Create token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
```

```
  set-credentials ${CONTEXT}-${NAMESPACE}-token-user \
  --token ${TOKEN}

# Set context to use token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token
-user

# Set context to correct namespace
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --namespace ${NAMESPACE}

# Flatten/minify kubeconfig
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  view --flatten --minify > ${KUBECONFIG_FILE}

# Remove tmp
rm ${KUBECONFIG_FILE}.full.tmp
rm ${KUBECONFIG_FILE}.tmp
```

b. Geben Sie die Befehle an, um sie auf Ihren Kubernetes-Cluster anzuwenden.

```
source create-kubeconfig.sh
```

8. (Optional) Umbenennen Sie die kubeconfig auf einen aussagekräftigen Namen für Ihr Cluster.

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

Was kommt als Nächstes?

Nachdem Sie nun überprüft haben, ob die Voraussetzungen erfüllt sind, können Sie es jetzt tun Fügen Sie einen Cluster hinzu.

Cluster hinzufügen

Zum Management von Applikationen fügen Sie einen Kubernetes-Cluster hinzu und managen ihn als Computing-Ressource. Um Ihre Kubernetes-Applikationen zu ermitteln, müssen Sie einen Cluster hinzufügen, in dem Astra Control Center ausgeführt werden kann.

Wir empfehlen, dass Astra Control Center den Cluster, der zuerst bereitgestellt wird, verwaltet, bevor Sie zum Management weitere Cluster zum Astra Control Center hinzufügen. Das Management des anfänglichen Clusters ist erforderlich, um Kubemetrics-Daten und Cluster-zugeordnete Daten zur Metriken und Fehlerbehebung zu senden.

Bevor Sie beginnen

- Bevor Sie ein Cluster hinzufügen, überprüfen und führen Sie die erforderlichen Maßnahmen durch Erforderliche Aufgaben.
- Wenn Sie einen ONTAP SAN-Treiber verwenden, stellen Sie sicher, dass Multipath auf allen Kubernetes-Clustern aktiviert ist.

Schritte

1. Navigieren Sie entweder über das Dashboard oder über das Menü Cluster:
   - Wählen Sie in der Ressourcenübersicht aus **Dashboard** im Bereich Cluster die Option **Hinzufügen** aus.
   - Wählen Sie im linken Navigationsbereich **Cluster** und dann auf der Seite Cluster **Cluster hinzufügen** aus.
2. Laden Sie im Fenster **Cluster hinzufügen** ein `kubeconfig.yaml` Datei oder fügen Sie den Inhalt eines ein `kubeconfig.yaml` Datei:

   Der `kubeconfig.yaml` Die Datei sollte **nur die Cluster-Anmeldedaten für einen Cluster** enthalten.

   Wenn Sie Ihre eigenen erstellen `kubeconfig` Datei, Sie sollten nur ein **ein**-Kontext -Element darin definieren. Siehe "Kubernetes-Dokumentation" Weitere Informationen zum Erstellen `kubeconfig` Dateien: Wenn Sie ein kubeconfig für eine eingeschränkte Clusterrolle erstellt haben, die mit verwendet wird Das oben beschriebene Verfahren, Vergewissern Sie sich, dass in diesem Schritt kubeconfig hochgeladen oder eingefügt wird.
3. Geben Sie einen Namen für die Anmeldeinformationen an. Standardmäßig wird der Name der Anmeldeinformationen automatisch als Name des Clusters ausgefüllt.
4. Wählen Sie **Weiter**.
5. Wählen Sie die Standard-Storage-Klasse, die für diesen Kubernetes-Cluster verwendet werden soll, und wählen Sie **Next** aus.

   Sie sollten eine Astra Trident Storage-Klasse auswählen, die von ONTAP Storage unterstützt wird.
6. Überprüfen Sie die Informationen, und wenn alles gut aussieht, wählen Sie **Hinzufügen**.

Ergebnis

Der Cluster wechselt in den **Entdeckungs**-Zustand und dann in **gesund**. Sie managen jetzt das Cluster mit dem Astra Control Center.

Nachdem Sie einen Cluster hinzugefügt haben, der im Astra Control Center verwaltet werden soll, kann es in einigen Minuten dauern, bis der Monitoring-Operator implementiert ist. Bis dahin wird das Benachrichtigungssymbol rot und ein Ereignis **Überwachung Agent-Status-Prüfung fehlgeschlagen** protokolliert. Sie können dies ignorieren, da das Problem gelöst wird, wenn Astra Control Center den richtigen Status erhält. Wenn sich das Problem in wenigen Minuten nicht beheben lässt, wechseln Sie zum Cluster und führen Sie aus `oc get pods -n netapp-monitoring` Als Ausgangspunkt. Um das Problem zu beheben, müssen Sie sich die Protokolle des Überwachungsperbers ansehen.

Aktivieren Sie die Authentifizierung auf dem ONTAP Storage Back-End

Astra Control Center bietet zwei Arten der Authentifizierung eines ONTAP-Backends:

- **Credential-basierte Authentifizierung**: Der Benutzername und das Passwort an einen ONTAP-Benutzer mit den erforderlichen Berechtigungen. Sie sollten eine vordefinierte Sicherheits-Login-Rolle wie admin oder vsadmin verwenden, um maximale Kompatibilität mit ONTAP-Versionen zu gewährleisten.
- **Zertifikatbasierte Authentifizierung**: Astra Control Center kann auch mit einem ONTAP-Cluster kommunizieren, indem ein auf dem Backend installiertes Zertifikat verwendet wird. Verwenden Sie gegebenenfalls das Clientzertifikat, den Schlüssel und das Zertifikat der vertrauenswürdigen Zertifizierungsstelle (empfohlen).

Sie können später vorhandene Back-Ends aktualisieren, um von einem Authentifizierungstyp zu einer anderen zu wechseln. Es wird jeweils nur eine Authentifizierungsmethode unterstützt.

Aktivieren Sie die Anmeldeinformationsbasierte Authentifizierung

Astra Control Center erfordert die Anmeldeinformationen für einen Cluster-Scoped `admin` Zur Kommunikation mit dem ONTAP-Backend. Sie sollten standardmäßige, vordefinierte Rollen wie verwenden `admin`. So wird die Kompatibilität mit zukünftigen ONTAP Versionen sichergestellt, für die Funktionskompatibilität für zukünftige Astra Control Center Versionen zur Verfügung stehen könnte.

> Eine benutzerdefinierte Sicherheits-Login-Rolle kann erstellt und mit Astra Control Center verwendet werden, wird aber nicht empfohlen.

Eine Beispiel-Backend-Definition sieht so aus:

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "admin",
  "password": "secret"
}
```

Die Backend-Definition ist der einzige Ort, an dem die Anmeldeinformationen im Klartext gespeichert werden. Die Erstellung oder Aktualisierung eines Backend ist der einzige Schritt, der Kenntnisse über die Anmeldeinformationen erfordert. Daher handelt es sich um einen reinen Admin-Vorgang, der vom Kubernetes- oder Storage-Administrator ausgeführt werden kann.

Aktivieren Sie die zertifikatbasierte Authentifizierung

Astra Control Center kann mithilfe von Zertifikaten mit neuen und vorhandenen ONTAP Back-Ends kommunizieren. Geben Sie die folgenden Informationen in die Backend-Definition ein.

- `clientCertificate`: Kundenzertifikat.

- `clientPrivateKey`: Zugehöriger privater Schlüssel.
- `trustedCACertificate`: Trusted CA-Zertifikat. Bei Verwendung einer vertrauenswürdigen CA muss dieser Parameter angegeben werden. Dies kann ignoriert werden, wenn keine vertrauenswürdige CA verwendet wird.

Sie können einen der folgenden Zertifikatstypen verwenden:

- Selbstsigniertes Zertifikat
- Drittanbieter-Zertifikat

Aktivieren Sie die Authentifizierung mit einem selbstsignierten Zertifikat

Ein typischer Workflow umfasst die folgenden Schritte.

Schritte

1. Erzeugen eines Clientzertifikats und eines Schlüssels. Legen Sie beim Generieren den allgemeinen Namen (Common Name, CN) auf den ONTAP-Benutzer fest, der sich als authentifizieren soll.

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key
-out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=<common-name>"
```

2. Installieren Sie das Clientzertifikat des Typs `client-ca` Und drücken Sie auf dem ONTAP-Cluster.

```
security certificate install -type client-ca -cert-name <certificate-
name> -vserver <vserver-name>
security ssl modify -vserver <vserver-name> -client-enabled true
```

3. Vergewissern Sie sich, dass die ONTAP-Sicherheits-Anmeldungsrolle die Zertifikatauthentifizierung unterstützt.

```
security login create -user-or-group-name vsadmin -application ontapi
-authentication-method cert -vserver <vserver-name>
security login create -user-or-group-name vsadmin -application http
-authentication-method cert -vserver <vserver-name>
```

4. Testen Sie die Authentifizierung mithilfe des generierten Zertifikats. Ersetzen Sie <ONTAP Management LIF> und <vserver name> durch die Management-LIF-IP und den SVM-Namen. Sie müssen sicherstellen, dass die Service-Richtlinie für das LIF auf festgelegt ist `default-data-management`.

```
curl -X POST -Lk https://<ONTAP-Management-
LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key
--cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp
xmlns=http://www.netapp.com/filer/admin version="1.21" vfiler="<vserver-
name>"><vserver-get></vserver-get></netapp>
```

5. Fügen Sie mithilfe der Werte aus dem vorherigen Schritt das Speicher-Backend in der Astra Control Center-Benutzeroberfläche hinzu.

Aktivieren Sie die Authentifizierung mit einem Zertifikat eines Drittanbieters

Wenn Sie über ein Zertifikat eines Drittanbieters verfügen, können Sie mit diesen Schritten eine zertifikatbasierte Authentifizierung einrichten.

Schritte

1. Privaten Schlüssel und CSR generieren:

```
openssl req -new -newkey rsa:4096 -nodes -sha256 -subj "/" -outform pem
-out ontap_cert_request.csr -keyout ontap_cert_request.key -addext
"subjectAltName = DNS:<ONTAP_CLUSTER_FQDN_NAME>,IP:<ONTAP_MGMT_IP>”
```

2. Leiten Sie die CSR an die Windows-Zertifizierungsstelle (Drittanbieter-CA) weiter, und stellen Sie das signierte Zertifikat aus.
3. Laden Sie das signierte Zertifikat herunter und benennen Sie es mit `ontap_signed_cert.crt'.
4. Exportieren Sie das Stammzertifikat aus der Windows-CA (Drittanbieter-CA).
5. Benennen Sie diese Datei `ca_root.crt`

   Sie haben nun die folgenden drei Dateien:

   - **Privatschlüssel**: `ontap_signed_request.key` (Dies ist der entsprechende Schlüssel für das Serverzertifikat in ONTAP. Sie wird bei der Installation des Serverzertifikats benötigt.)
   - **Signiertes Zertifikat**: `ontap_signed_cert.crt` (Dies wird in ONTAP auch als *Server-Zertifikat* bezeichnet.)
   - **Stammzertifizierungsstelle**: `ca_root.crt` (In ONTAP wird dies auch als *Server-CA-Zertifikat* bezeichnet.)
6. Installieren Sie diese Zertifikate in ONTAP. Generieren und installieren `server` Und `server-ca` Zertifikate auf ONTAP.

Erweitern für Sample.yaml

```
# Copy the contents of ca_root.crt and use it here.

security certificate install -type server-ca

Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----
<certificate details>
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:

CA:
serial:

The certificate's generated name for reference:


===

# Copy the contents of ontap_signed_cert.crt and use it here. For
key, use the contents of ontap_cert_request.key file.
security certificate install -type server
Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----
<certificate details>
-----END CERTIFICATE-----

Please enter Private Key: Press <Enter> when done

-----BEGIN PRIVATE KEY-----
<private key details>
-----END PRIVATE KEY-----

Enter certificates of certification authorities (CA) which form the
certificate chain of the server certificate. This starts with the
issuing CA certificate of the server certificate and can range up to
the root CA certificate.
Do you want to continue entering root and/or intermediate
```

```
certificates {y|n}: n

The provided certificate does not have a common name in the subject
field.
Enter a valid common name to continue installation of the
certificate: <ONTAP_CLUSTER_FQDN_NAME>

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
The installed certificate's CA and serial number for reference:
CA:
serial:
The certificate's generated name for reference:


==
# Modify the vserver settings to enable SSL for the installed
certificate

ssl modify -vserver <vserver_name> -ca <CA>  -server-enabled true
-serial <serial number>       (security ssl modify)

==
# Verify if the certificate works fine:

openssl s_client -CAfile ca_root.crt -showcerts -servername server
-connect <ONTAP_CLUSTER_FQDN_NAME>:443
CONNECTED(00000005)
depth=1 DC = local, DC = umca, CN = <CA>
verify return:1
depth=0
verify return:1
write W BLOCK
---
Certificate chain
0 s:
   i:/DC=local/DC=umca/<CA>

-----BEGIN CERTIFICATE-----
<Certificate details>
```

7. Erstellen Sie das Clientzertifikat für denselben Host für die passwortlose Kommunikation. Astra Control Center kommuniziert anhand dieses Verfahrens mit ONTAP.
8. Generieren und installieren Sie die Clientzertifikate auf ONTAP:

Erweitern für Sample.yaml

```
# Use /CN=admin or use some other account which has privileges.
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout
ontap_test_client.key -out ontap_test_client.pem -subj "/CN=admin"

Copy the content of ontap_test_client.pem file and use it in the
below command:
security certificate install -type client-ca -vserver <vserver_name>

Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----
<Certificate details>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.
The installed certificate's CA and serial number for reference:

CA:
serial:
The certificate's generated name for reference:


==

ssl modify -vserver <vserver_name> -client-enabled true
(security ssl modify)

# Setting permissions for certificates
security login create -user-or-group-name admin -application ontapi
-authentication-method cert -role admin -vserver <vserver_name>

security login create -user-or-group-name admin -application http
-authentication-method cert -role admin -vserver <vserver_name>

==

#Verify passwordless communication works fine with the use of only
certificates:

curl --cacert ontap_signed_cert.crt  --key ontap_test_client.key
--cert ontap_test_client.pem
https://<ONTAP_CLUSTER_FQDN_NAME>/api/storage/aggregates
{
```

```
"records": [
{
"uuid": "f84e0a9b-e72f-4431-88c4-4bf5378b41bd",
"name": "<aggr_name>",
"node": {
"uuid": "7835876c-3484-11ed-97bb-d039ea50375c",
"name": "<node_name>",
"_links": {
"self": {
"href": "/api/cluster/nodes/7835876c-3484-11ed-97bb-d039ea50375c"
}
}
},
"_links": {
"self": {
"href": "/api/storage/aggregates/f84e0a9b-e72f-4431-88c4-
4bf5378b41bd"
}
}
}
],
"num_records": 1,
"_links": {
"self": {
"href": "/api/storage/aggregates"
}
}
}%
```


9. Fügen Sie das Storage-Backend in der Astra Control Center-Benutzeroberfläche hinzu und geben Sie die folgenden Werte an:
   - **Client-Zertifikat**: ontap_Test_Client.pem
   - **Private Key**: ontap_test_client.key
   - **Vertrauenswürdiges CA-Zertifikat**: ontap_Signed_cert.crt

Fügen Sie ein Storage-Back-End hinzu

Nachdem Sie die Anmeldeinformationen oder Zertifikatauthentifizierungsinformationen eingerichtet haben, können Sie ein vorhandenes ONTAP-Storage-Back-End zu Astra Control Center hinzufügen, um seine Ressourcen zu managen.

Durch das Management von Storage-Clustern in Astra Control als Storage-Backend können Sie Verbindungen zwischen persistenten Volumes (PVS) und dem Storage-Backend sowie zusätzliche Storage-Kennzahlen abrufen.

nur Astra Control Provisioner: Das Hinzufügen und Managen von ONTAP-Storage-Back-Ends in Astra

Control Center ist bei Verwendung der NetApp SnapMirror Technologie optional, wenn Sie Astra Control Provisioner mit Astra Control Center 23.10 oder höher aktiviert haben.

Schritte

1. Wählen Sie im Dashboard im linken Navigationsbereich **Backend** aus.
2. Wählen Sie **Hinzufügen**.
3. Wählen Sie im Bereich vorhandene verwenden auf der Seite Speicher-Backend hinzufügen **ONTAP** aus.
4. Wählen Sie eine der folgenden Optionen:
   - **Administrator-Anmeldeinformationen verwenden**: Geben Sie die ONTAP Cluster Management IP-Adresse und die Admin-Anmeldeinformationen ein. Die Anmeldedaten müssen Cluster-weite Anmeldedaten aufweisen.

     Der Benutzer, dessen Anmeldeinformationen Sie hier eingeben, muss über den verfügen `ontapi` Aktivieren der Zugriffsmethode für die Anmeldung beim Benutzer in ONTAP System Manager auf dem ONTAP Cluster. Wenn Sie Vorhaben, SnapMirror Replizierung zu verwenden, wenden Sie Benutzeranmeldeinformationen auf die Rolle „Admin“ an, die über die Zugriffsmethoden verfügt `ontapi` Und `http`, Auf Quell- und Ziel-ONTAP Clustern. Siehe "Managen von Benutzerkonten in der ONTAP Dokumentation" Finden Sie weitere Informationen.

   - **Ein Zertifikat** verwenden: Das Zertifikat hochladen `.pem` Datei, dem Zertifikatschlüssel `.key` Datei und optional die Zertifizierungsdatei.
5. Wählen Sie **Weiter**.
6. Bestätigen Sie die Backend-Details und wählen Sie **Verwalten**.

Ergebnis

Das Backend wird im angezeigt `online` Status in der Liste mit Zusammenfassungsinformationen.

Möglicherweise müssen Sie die Seite aktualisieren, damit das Backend angezeigt wird.

Fügen Sie einen Bucket hinzu

Sie können einen Bucket über die Astra Control UI oder hinzufügen "Astra Control API". Das Hinzufügen von Objektspeicher-Bucket-Providern ist wichtig, wenn Sie Ihre Applikationen und Ihren persistenten Storage sichern möchten oder Applikationen über Cluster hinweg klonen möchten. Astra Control speichert diese Backups oder Klone in den von Ihnen definierten Objektspeicher-Buckets.

Wenn Sie Ihre Applikationskonfiguration und Ihren persistenten Storage im selben Cluster klonen, benötigen Sie in Astra Control keinen Bucket. Für die Funktionalität von Applikations-Snapshots ist kein Bucket erforderlich.

Bevor Sie beginnen

- Stellen Sie sicher, dass ein Bucket vorhanden ist, der von den von Astra Control Center gemanagten Clustern erreichbar ist.
- Stellen Sie sicher, dass Sie über Anmeldedaten für den Bucket verfügen.
- Stellen Sie sicher, dass es sich bei dem Bucket um einen der folgenden Typen handelt:
  - NetApp ONTAP S3
  - NetApp StorageGRID S3

- Microsoft Azure
- Allgemein S3

Amazon Web Services (AWS) und Google Cloud Platform (GCP) verwenden den Bucket-Typ Generic S3.

Obwohl Astra Control Center Amazon S3 als Generic S3 Bucket-Provider unterstützt, unterstützt Astra Control Center unter Umständen nicht alle Objektspeicher-Anbieter, die die Unterstützung von Amazon S3 beanspruchen.

Schritte

1. Wählen Sie im linken Navigationsbereich **Buckets** aus.
2. Wählen Sie **Hinzufügen**.
3. Wählen Sie den Bucket-Typ aus.

   Wenn Sie einen Bucket hinzufügen, wählen Sie den richtigen Bucket-Provider aus und geben die richtigen Anmeldedaten für diesen Provider an. 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.

4. Geben Sie einen vorhandenen Bucket-Namen und eine optionale Beschreibung ein.

   Der Name und die Beschreibung des Buckets werden als Backupspeicherort angezeigt, den Sie später bei der Erstellung eines Backups auswählen können. Der Name wird auch während der Konfiguration der Schutzrichtlinien angezeigt.

5. Geben Sie den Namen oder die IP-Adresse des S3-Endpunkts ein.
6. Wählen Sie unter **Anmeldeinformationen auswählen** die Registerkarte **Hinzufügen** oder **vorhandene verwenden**.
   - Wenn Sie sich für **Hinzufügen** entschieden haben:
     i. Geben Sie einen Namen für die Anmeldedaten ein, der sie von anderen Anmeldeinformationen in Astra Control unterscheidet.
     ii. Geben Sie die Zugriffs-ID und den geheimen Schlüssel ein, indem Sie den Inhalt aus der Zwischenablage einfügen.
   - Wenn Sie sich für **vorhandenes** verwenden:
     i. Wählen Sie die vorhandenen Anmeldedaten aus, die Sie mit dem Bucket verwenden möchten.
7. Wählen Sie `Add`.

   Wenn Sie einen Bucket hinzufügen, markiert Astra Control einen Bucket mit der Standard-Bucket-Anzeige. Der erste von Ihnen erstellte Bucket wird der Standard-Bucket. Wenn Sie Buckets hinzufügen, können Sie sich später entscheiden "Legen Sie einen weiteren Standard-Bucket fest".

Was kommt als Nächstes?

Nachdem Sie sich jetzt angemeldet haben und Cluster zum Astra Control Center hinzugefügt haben, können Sie die Applikationsdatenmanagement-Funktionen von Astra Control Center nutzen.

- "Managen Sie lokale Benutzer und Rollen"
- "Starten Sie das Anwendungsmanagement"
- "Schützen von Applikationen"
- "Benachrichtigungen verwalten"
- "Verbinden Sie sich mit Cloud Insights"
- "Fügen Sie ein benutzerdefiniertes TLS-Zertifikat hinzu"
- "Ändern der Standard-Storage-Klasse"

Weitere Informationen

- "Verwenden Sie die Astra Control API"
- "Bekannte Probleme"

Häufig gestellte Fragen zum Astra Control Center

Diese FAQ kann Ihnen helfen, wenn Sie nur nach einer schnellen Antwort auf eine Frage suchen.

Überblick

In den folgenden Abschnitten finden Sie Antworten auf einige zusätzliche Fragen, die Sie bei der Verwendung von Astra Control Center interessieren könnten. Weitere Erläuterungen erhalten Sie von astra.feedback@netapp.com

Zugang zum Astra Control Center

Was ist die Astra Control URL?

Astra Control Center verwendet lokale Authentifizierung und eine spezifische URL für jede Umgebung.

Geben Sie für die URL in einem Browser den vollständig qualifizierten Domänennamen (FQDN) ein, den Sie im Feld spec.astraAddress (astra_control_Center.yaml Custom Resource (CR)) festgelegt haben, wenn Sie Astra Control Center installiert haben. Die E-Mail ist der Wert, den Sie im Feld Spec.email im astra_Control_Center.yaml CR festgelegt haben.

Lizenzierung

Ich verwende eine Evaluierungslizenz. Wie ändere ich die Volllizenz?

Sie können ganz einfach zu einer vollständigen Lizenz wechseln, indem Sie die NetApp Lizenzdatei (NetApp License File, NLF) von NetApp beziehen.

Schritte

1. Wählen Sie in der linken Navigationsleiste **Konto** > **Lizenz**.
2. Wählen Sie in der Lizenzübersicht rechts neben den Lizenzinformationen das Menü Optionen.
3. Wählen Sie **Ersetzen**.
4. Navigieren Sie zu der Lizenzdatei, die Sie heruntergeladen haben, und wählen Sie **Hinzufügen**.

Ich verwende eine Evaluierungslizenz. Kann ich trotzdem Apps verwalten?

Ja, Sie können die Funktionalität zum Verwalten von Apps mit einer Evaluierungslizenz testen (einschließlich der standardmäßig installierten integrierten Evaluierungslizenz). Zwischen einer Evaluierungslizenz und einer vollständigen Lizenz gibt es keinen Unterschied in den Funktionen oder der Funktionalität; die Evaluierungslizenz hat einfach eine kürzere Lebensdauer. Siehe "Lizenzierung" Finden Sie weitere Informationen.

Kubernetes Cluster werden registriert

Nach dem Hinzufügen von Astra Control müssen ich die Worker-Nodes zu meinem Kubernetes Cluster hinzufügen. Was soll ich tun?

Vorhandenen Pools können neue Worker Nodes hinzugefügt werden. Diese werden automatisch von Astra Control entdeckt. Wenn die neuen Knoten in Astra Control nicht sichtbar sind, prüfen Sie, ob auf den neuen Worker Nodes der unterstützte Bildtyp ausgeführt wird. Sie können den Zustand der neuen Worker-Nodes auch mit überprüfen `kubectl get nodes` Befehl.

Wie entnehme ich einen Cluster richtig?

1. "Lösen Sie die Anwendungen von Astra Control".
2. "Lösen Sie das Cluster über Astra Control".

Was passiert mit meinen Anwendungen und Daten, nachdem ich den Kubernetes Cluster aus Astra Control entfernt habe?

Das Entfernen eines Clusters aus Astra Control führt keine Änderungen an der Cluster-Konfiguration (Applikationen und persistenter Storage) durch. Astra Control Snapshots oder Backups, die von Applikationen auf diesem Cluster erstellt werden, sind zur Wiederherstellung nicht verfügbar. Die von Astra Control erstellten persistenten Storage Backups bleiben innerhalb des Astra Control, sind aber nicht für die Wiederherstellung verfügbar.

> Entfernen Sie immer einen Cluster aus Astra Control, bevor Sie ihn mit anderen Methoden löschen. Das Löschen eines Clusters mithilfe eines anderen Tools, während es noch von Astra Control gemanagt wird, kann zu Problemen mit Ihrem Astra Control Konto führen.

Wird NetApp Astra Trident automatisch aus einem Cluster deinstalliert, wenn ich es entmanage?
Wenn Sie ein Cluster aus Astra Control Center deinstallieren, wird Astra Trident nicht automatisch aus dem Cluster deinstalliert. Um Astra Trident zu deinstallieren, müssen Sie es benötigen "Folgen Sie den Schritten in der Dokumentation von Astra Trident".

Management von Applikationen

Kann Astra Control eine Anwendung bereitstellen?

Astra Control implementiert keine Applikationen. Applikationen müssen außerhalb von Astra Control bereitgestellt werden.

Was passiert mit Anwendungen, nachdem ich sie von Astra Control aus verwaltet habe?

Alle bestehenden Backups oder Snapshots werden gelöscht. Applikationen und Daten sind weiterhin verfügbar. Datenmanagement-Vorgänge stehen nicht für nicht verwaltete Anwendungen oder für Backups oder Snapshots zur Verfügung, die dazu gehören.

Kann Astra Control eine Applikation managen, die sich auf Storage anderer Anbieter befindet?

Nein Astra Control kann zwar Applikationen erkennen, die Storage anderer Anbieter verwenden, aber eine Applikation, die Storage anderer Anbieter verwendet, kann die IT nicht managen.

Sollte ich Astra Control selbst managen?

Astra Control Center wird standardmäßig nicht als Anwendung angezeigt, die Sie managen können, aber Sie können es "Backup und Restore" Eine Astra Control Center-Instanz, die eine andere Astra Control Center-Instanz verwendet.

Wirken sich ungesunde Pods auf das App-Management aus?

Nein, der Zustand von Pods beeinträchtigt das App-Management nicht.

Datenmanagement-Vorgänge

Meine Anwendung verwendet mehrere PVS. Wird Astra Control Snapshots und Backups dieser PVS erstellen?

Ja. Ein Snapshot-Vorgang auf einer Anwendung von Astra Control umfasst die Momentaufnahme aller VES, die an die VES der Anwendung gebunden sind.

Kann ich die von Astra Control erstellten Snapshots direkt über eine andere Schnittstelle oder Objekt-Storage managen?

Nein Von Astra Control angenommene Snapshots und Backups können nur mit Astra Control gemanagt werden.

Astra Control Provisioner

Wie unterscheiden sich die Funktionen zur Storage-Bereitstellung von Astra Control von denen in Astra Trident?

Astra Control Provisioner unterstützt als Teil von Astra Control übergeordnete Funktionen für die Storage-Bereitstellung, die in Open-Source-Funktionen von Astra Trident nicht verfügbar sind. Diese Funktionen stehen zusätzlich zu allen Features, die für den Open-Source-Trident zur Verfügung stehen.

Ersetzt Astra Control Provisioner Astra Trident?

Bei den nächsten Updates für Astra Control wird der Provisioner Astra Trident als Storage-bereitstellung und -Orchestrierung in der Architektur von Astra Control ersetzen. Aus diesem Grund wird Astra Control besonders empfohlen "Astra Control Provisioner aktivieren". Astra Trident wird weiterhin Open Source bleiben und mit neuen CSI- und anderen Funktionen von NetApp veröffentlicht, gepflegt, unterstützt und auf dem neuesten Stand sein.

Muss ich für Astra Trident bezahlen?

Nein Astra Trident ist weiterhin Open-Source-Software und kann kostenlos heruntergeladen werden.

Kann ich die Funktionen zur Speicherverwaltung und Bereitstellung in Astra Control nutzen, ohne Astra Control zu installieren und zu verwenden?

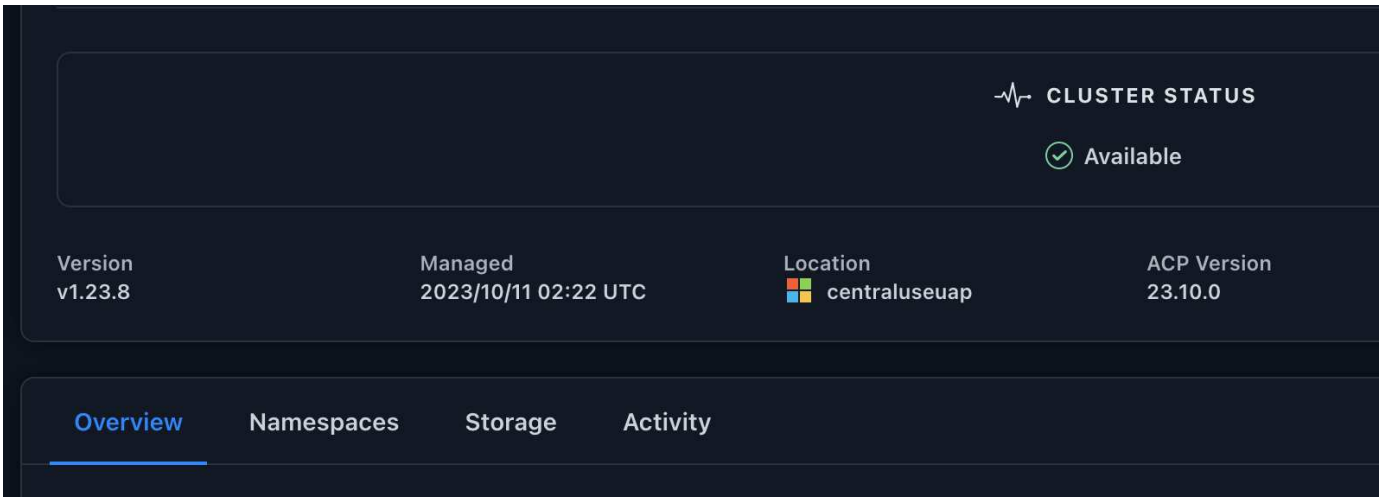
Ja, Sie können ein Upgrade auf Astra Trident 23.10 oder höher durchführen und die Astra Control Provisioner-Funktion aktivieren, selbst wenn Sie nicht den gesamten Funktionsumfang des Astra Control Datenmanagements nutzen möchten.

Wie kann ich von einem vorhandenen Trident-Benutzer zu Astra Control wechseln, um erweiterte Storage-Management- und Bereitstellungsfunktionen zu nutzen?

Wenn Sie bereits Trident verwenden (einschließlich Benutzer von Astra Trident in der Public Cloud), müssen Sie zuerst eine Astra Control Lizenz erwerben. Anschließend können Sie das Bundle für Astra Control Provisioner herunterladen, das Upgrade von Astra Trident und durchführen "Aktivieren Sie die Funktionen für die Astra Control Provisionierung".

Wie kann ich feststellen, ob Astra Control Provisioner Astra Trident in meinem Cluster ersetzt hat?

Nach der Installation von Astra Control Provisioner wird für das Host-Cluster in der Astra Control UI ein angezeigt `ACP version` Und nicht `Trident version` Feld und aktuelle installierte Versionsnummer.



Wenn Sie keinen Zugriff auf die Benutzeroberfläche haben, können Sie die erfolgreiche Installation mithilfe der folgenden Methoden bestätigen:

Astra Trident Betreiber

Überprüfen Sie die `trident-acp` Container läuft und das `acpVersion` Ist `23.10.0` Mit dem Status `Installed`:

```
kubectl get torc -o yaml
```

Antwort:

```
status:
  acpVersion: 23.10.0
  currentInstallationParams:
    ...
    acpImage: <my_custom_registry>/trident-acp:23.10.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

Tridentctl

Aktivieren Sie die Astra Control Provisioner-Funktion:

```
./tridentctl -n trident version
```

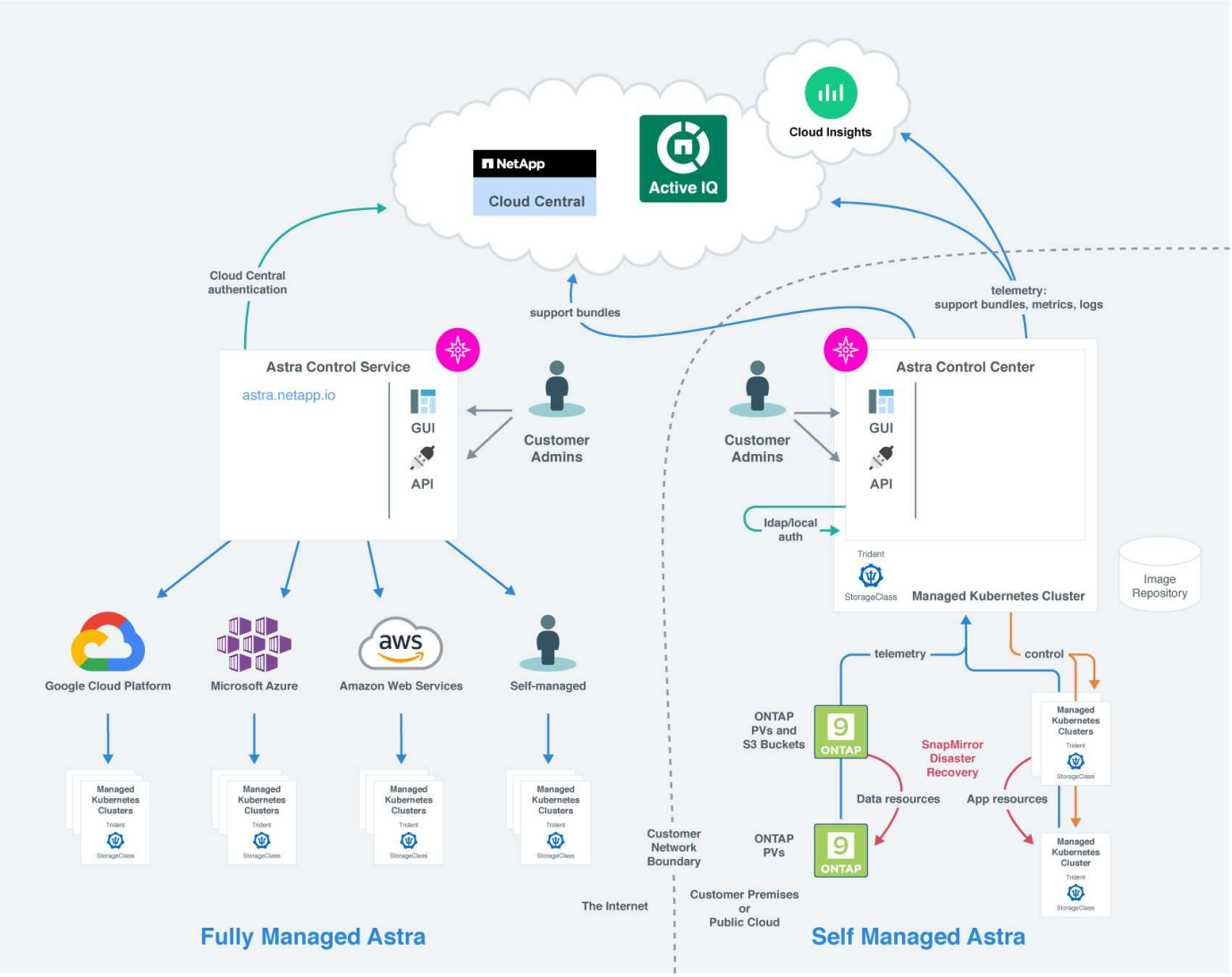
Antwort:

```
+----------------+----------------+-------------+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +----------------+----------------
+-------------+ | 23.10.0 | 23.10.0 | 23.10.0. | +----------------
+----------------+-------------+
```

Konzepte

Architektur und Komponenten

Hier ist ein Überblick über die verschiedenen Komponenten der Astra Control-Umgebung.



Komponenten des Astra Control

- **Kubernetes-Cluster**: Kubernetes ist eine portable, erweiterbare Open-Source-Plattform für das Management von Workloads und Services in Containern, die sowohl deklarative Konfigurationen als auch Automatisierung ermöglicht. Astra bietet Managementservices für Applikationen, die in einem Kubernetes-Cluster gehostet werden.
- **Astra Trident**: Als vollständig unterstützte Open-Source-Storage-bereitstellung und -Orchestrierung mit NetApp ermöglicht Ihnen Astra Trident die Erstellung von Storage Volumes für Container-Applikationen, die von Docker und Kubernetes verwaltet werden. Astra Trident ist mit dem Astra Control Center implementiert und umfasst ein konfiguriertes ONTAP Storage-Back-End.
- **Speicher-Backend**:

    - Astra Control Service nutzt folgende Storage-Back-Ends:
        - "NetApp Cloud Volumes Service für Google Cloud" Oder Google Persistent Disk als Speicher-Backend für GKE-Cluster
        - "Azure NetApp Dateien" Oder von Azure verwaltete Festplatten als Storage-Backend für AKS-Cluster.
        - "Amazon Elastic Block Store (EBS)" Oder "Amazon FSX für NetApp ONTAP" Als Back-End-Speicheroptionen für EKS-Cluster.
    - Astra Control Center nutzt folgende Storage-Back-Ends:
        - ONTAP AFF, FAS und ASA. Als Storage-Software- und Hardware-Plattform bietet ONTAP wichtige Storage-Services, Unterstützung für mehrere Storage-Zugriffsprotokolle und Storage-Managementfunktionen wie Snapshots und Spiegelung.
        - Cloud Volumes ONTAP
- **Cloud Insights**: Mit Cloud Insights, einem Monitoring-Tool für die Cloud-Infrastruktur von NetApp, können Sie die Performance und Auslastung für Ihre Kubernetes-Cluster überwachen, die vom Astra Control Center gemanagt werden. Cloud Insights korreliert die Storage-Auslastung mit Workloads. Wenn Sie die Cloud Insights-Verbindung im Astra Control Center aktivieren, werden Telemetriedaten auf den UI-Seiten des Astra Control Center angezeigt.

Astra Control-Schnittstellen

Sie können Aufgaben über verschiedene Schnittstellen ausführen:

- **Web-Benutzeroberfläche (UI)**: Sowohl Astra Control Service als auch Astra Control Center nutzen die gleiche webbasierte Benutzeroberfläche, in der Sie Apps verwalten, migrieren und schützen können. Verwenden Sie die UI auch zum Verwalten von Benutzerkonten und Konfigurationseinstellungen.
- **API**: Sowohl Astra Control Service als auch Astra Control Center nutzen die gleiche Astra Control API. Mit der API können Sie die gleichen Aufgaben ausführen, die Sie über die UI ausgeführt haben.

Mit Astra Control Center können Sie auch Kubernetes Cluster in VM-Umgebungen managen, migrieren und schützen.

Finden Sie weitere Informationen

- "Dokumentation des Astra Control Service"
- "Astra Control Center-Dokumentation"
- "Astra Trident-Dokumentation"
- "Verwenden Sie die Astra Control API"
- "Cloud Insights-Dokumentation"
- "ONTAP-Dokumentation"

Datensicherung

Lernen Sie die verfügbaren Datensicherungsarten im Astra Control Center kennen und erfahren Sie, wie Sie diese am besten für den Schutz Ihrer Applikationen nutzen.

Snapshots, Backups und Sicherungsrichtlinien

Sowohl Snapshots als auch Backups sichern die folgenden Datentypen:

- Der Applikation selbst.
- Alle persistenten Daten-Volumes, die mit der Applikation in Verbindung stehen
- Alle zu der Applikation gehörenden Ressourcenartefakte

A *Snapshot* ist eine zeitpunktgenaue Kopie einer Applikation, die auf demselben bereitgestellten Volume wie die Applikation gespeichert ist. In der Regel sind sie schnell. Sie können lokale Snapshots verwenden, um die Anwendung auf einen früheren Zeitpunkt wiederherzustellen. Snapshots sind nützlich für schnelle Klone. Snapshots enthalten alle Kubernetes-Objekte für die App, einschließlich Konfigurationsdateien. Snapshots sind nützlich zum Klonen oder Wiederherstellen einer Anwendung innerhalb desselben Clusters.

Ein *Backup* basiert auf einem Snapshot. Er wird im externen Objektspeicher gespeichert und kann daher im Vergleich zu lokalen Snapshots langsamer erstellt werden. Sie können ein Applikations-Backup in demselben Cluster wiederherstellen oder eine Applikation migrieren, indem Sie dessen Backup auf ein anderes Cluster wiederherstellen. Sie können auch eine längere Aufbewahrungsdauer für Backups wählen. Da diese im externen Objektspeicher gespeichert werden, bieten Backups in der Regel besseren Schutz als Snapshots bei Serverausfällen oder Datenverlusten.

Eine *Schutzrichtlinie* ist eine Möglichkeit zum Schutz einer App, indem automatisch Snapshots, Backups oder beides gemäß einem von Ihnen für die App definierten Zeitplan erstellt werden. Eine Sicherungsrichtlinie erlaubt Ihnen außerdem festzulegen, wie viele Snapshots und Backups im Zeitplan aufbewahrt werden sollen, und verschiedene granulare Zeitplanebenen festzulegen. Die Automatisierung von Backups und Snapshots mit einer Sicherungsrichtlinie ist die beste Methode, um sicherzustellen, dass jede Applikation gemäß den Anforderungen Ihres Unternehmens und der SLA-Anforderungen (Service Level Agreement) geschützt ist.

> _Sie können erst dann vollständig geschützt sein, wenn Sie ein kürzlich gesichertes Backup haben. Das ist wichtig, da Backups abseits der persistenten Volumes in einem Objektspeicher gespeichert werden. Wenn ein Ausfall das Cluster und der damit verbundene persistente Storage entfernt, muss ein Backup wiederhergestellt werden. Ein Snapshot würde es Ihnen nicht ermöglichen, eine Wiederherstellung durchzuführen.

Unveränderliche Backups

Ein unveränderliches Backup ist ein Backup, das innerhalb eines festgelegten Zeitraums nicht geändert oder gelöscht werden kann. Beim Erstellen eines unveränderlichen Backups überprüft Astra Control, ob es sich bei dem verwendeten Bucket um einen WORM-Bucket (Write Once Read Many) handelt. Falls ja, stellt er sicher, dass das Backup in Astra Control unveränderlich ist.
Astra Control Center unterstützt das Erstellen unveränderlicher Backups mit den folgenden Plattformen und Bucket-Typen:

- Amazon Web Services verwenden einen Amazon S3 Bucket mit konfigurierter S3 Object Lock
- NetApp StorageGRID mithilfe eines S3 Buckets mit konfigurierter S3 Object Lock-Funktion

Beachten Sie beim Arbeiten mit unveränderlichen Backups Folgendes:

- Wenn ein Backup auf einem WORM-Bucket in einer nicht unterstützten Plattform oder auf einem nicht unterstützten Bucket-Typ durchgeführt wird, können unvorhersehbare Ergebnisse wie das Löschen von Backups sogar dann angezeigt werden, wenn die Aufbewahrungszeit abgelaufen ist.
- Astra Control unterstützt keine Management-Richtlinien für den Daten-Lebenszyklus oder das manuelle

Löschen von Objekten in den Buckets, die Sie mit unveränderlichen Backups verwenden. Stellen Sie sicher, dass Ihr Storage-Backend nicht für das Management des Lebenszyklus von Astra Control Snapshots oder gesicherten Daten konfiguriert ist.

Klone

Ein *Clone* ist ein exaktes Duplikat einer App, ihrer Konfiguration und ihrer persistenten Daten-Volumes. Sie können einen Klon entweder manuell auf demselben Kubernetes-Cluster oder auf einem anderen Cluster erstellen. Das Klonen einer Applikation kann nützlich sein, wenn Sie Applikationen und Storage von einem Kubernetes Cluster zu einem anderen verschieben müssen.

Replizierung zwischen Storage-Back-Ends

Mithilfe von Astra Control können Sie mit den asynchronen Replizierungsfunktionen der NetApp SnapMirror Technologie Business Continuity für Ihre Applikationen erzielen: Mit Low-RPO (Recovery Point Objective) und Low-RTO (Recovery Time Objective). Nach der Konfiguration können Ihre Applikationen auf diese Weise Daten und Applikationsänderungen von einem Storage-Back-End auf ein anderes replizieren, sowohl im selben Cluster als auch zwischen verschiedenen Clustern.

Sie können zwischen zwei ONTAP SVMs auf demselben ONTAP Cluster oder in verschiedenen ONTAP Clustern replizieren.

Astra Control repliziert App-Snapshot-Kopien asynchron an ein Ziel-Cluster. Der Replizierungsprozess umfasst Daten in den persistenten Volumes, die von SnapMirror repliziert werden, und die durch Astra Control geschützten App-Metadaten.

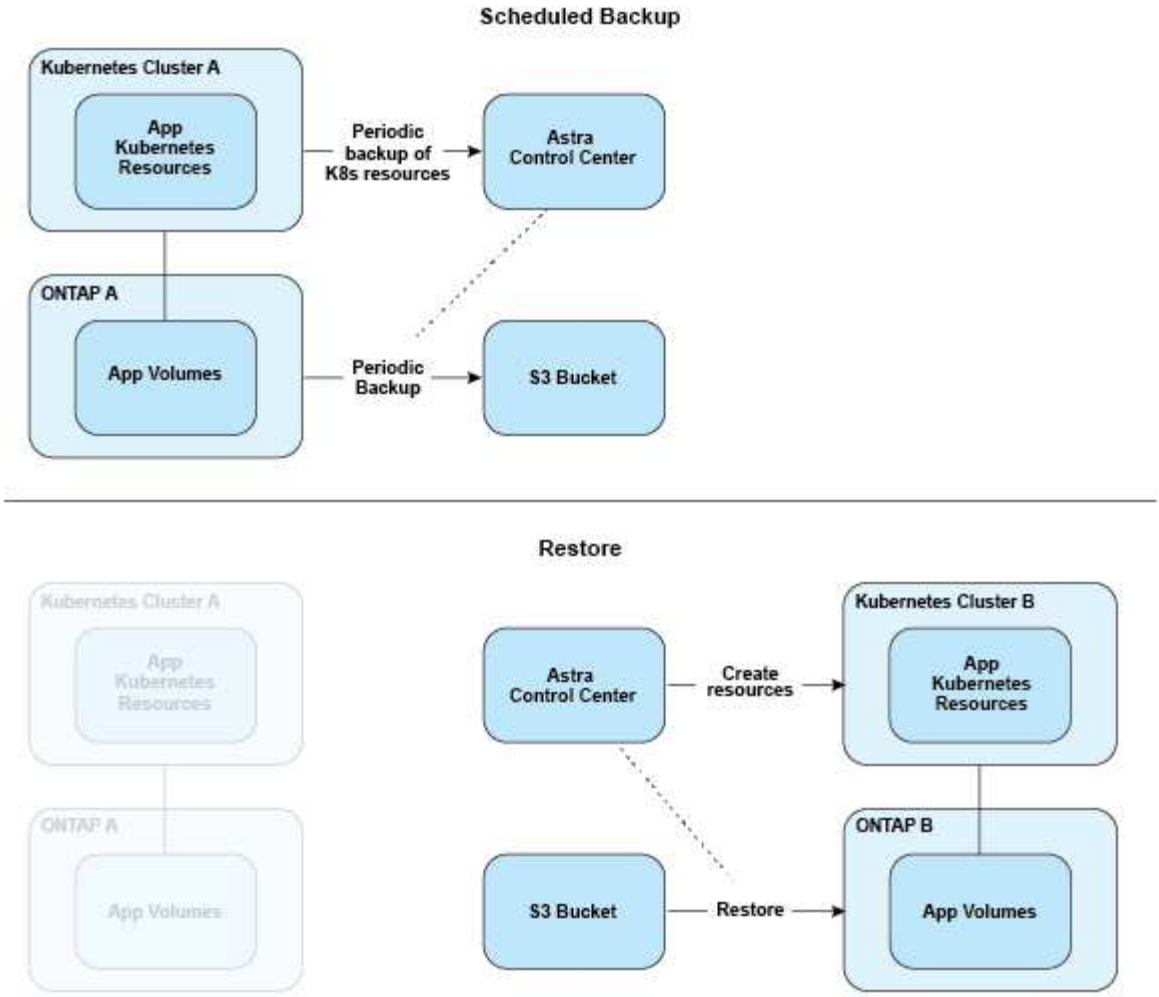
Die Replizierung von Applikationen unterscheidet sich folgendermaßen von Backup und Restore von Applikationen:

- **App-Replizierung**: Für Astra Control müssen die Kubernetes Quell- und Ziel-Cluster (die dasselbe Cluster sein können) verfügbar sein und mit ihren jeweiligen ONTAP Storage-Back-Ends gemanagt werden, die für die Aktivierung von NetApp SnapMirror konfiguriert sind. Astra Control repliziert den richtlinienbasierten Applikations-Snapshot auf das Ziel-Storage-Back-End. NetApp SnapMirror wird zur Replizierung der persistenten Volume-Daten eingesetzt. Zum Failover kann Astra Control die replizierte Applikation online schalten, indem die Applikationsobjekte auf dem Kubernetes Ziel-Cluster mit den replizierten Volumes auf dem ONTAP Ziel-Cluster neu erstellt werden. Da die persistenten Volume-Daten bereits auf dem Ziel-ONTAP-Cluster vorhanden sind, kann Astra Control schnelle Recovery-Zeiten für Failover bieten.
- **App-Backup und -Wiederherstellung**: Beim Backup von Anwendungen erstellt Astra Control einen Snapshot der App-Daten und speichert diesen in einem Objekt-Storage-Bucket. Wenn eine Wiederherstellung erforderlich ist, müssen die Daten in dem Bucket auf ein persistentes Volume auf dem ONTAP Cluster kopiert werden. Der Backup-/Restore-Vorgang erfordert nicht, dass der sekundäre Kubernetes/ONTAP Cluster verfügbar und gemanagt wird. Die zusätzliche Datenkopie kann jedoch zu längeren Restore-Zeiten führen.

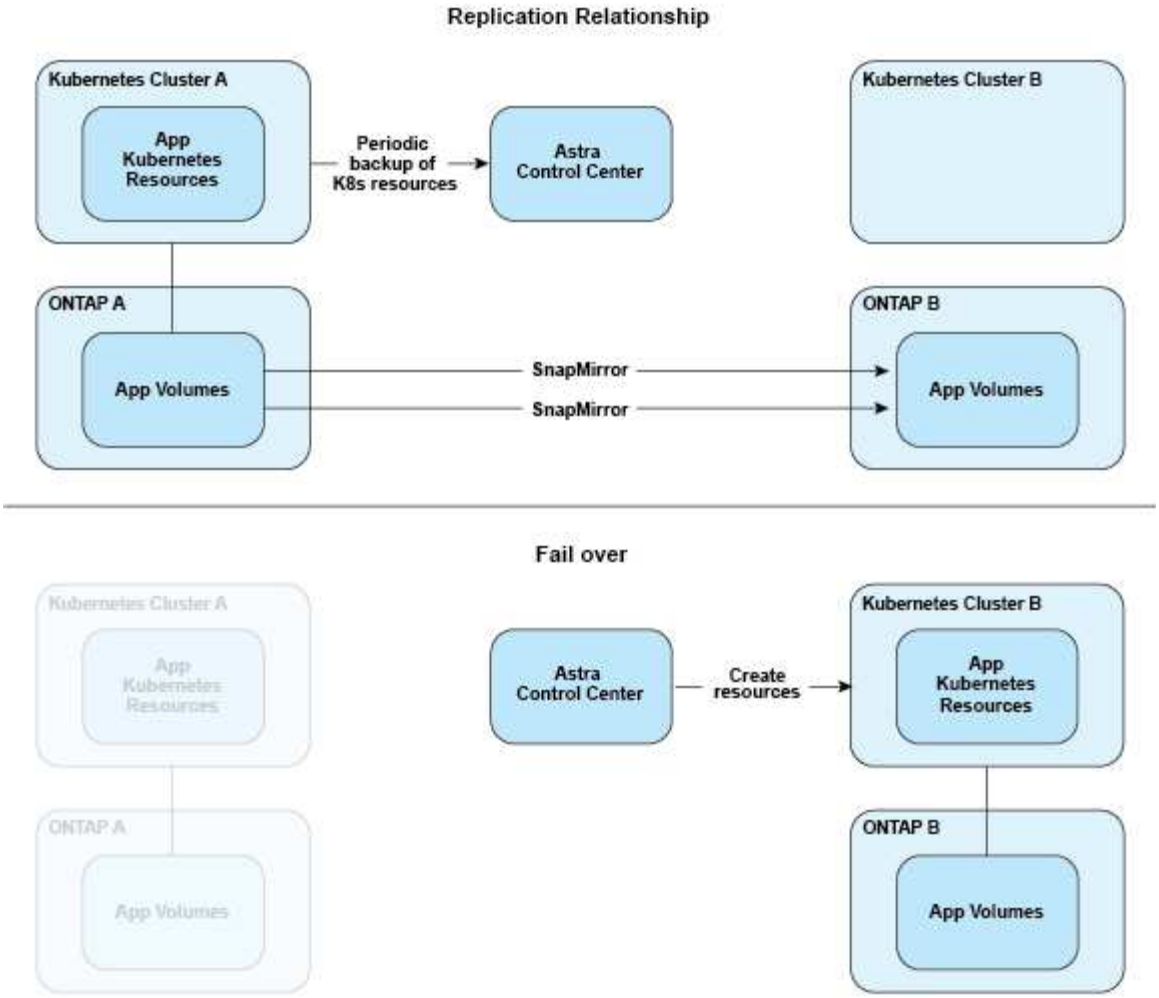
Weitere Informationen zum Replizieren von Apps finden Sie unter "Replizieren von Applikationen auf einem Remote-System mit SnapMirror Technologie".

Die folgenden Images zeigen den geplanten Backup- und Wiederherstellungsprozess im Vergleich zum Replikationsprozess.

Der Backup-Prozess kopiert Daten in S3 Buckets und Restores aus S3 Buckets:



Andererseits wird die Replizierung zu ONTAP durchgeführt. Durch ein Failover werden die Kubernetes-Ressourcen erzeugt:



Backups, Snapshots und Klone mit abgelaufener Lizenz

Wenn Ihre Lizenz abläuft, können Sie nur dann eine neue Applikation hinzufügen oder Vorgänge zum Schutz von Applikationen (wie Snapshots, Backups, Klone und Wiederherstellungsvorgänge) durchführen, wenn die hinzugefügte oder zu schützende Applikation eine weitere Astra Control Center-Instanz ist.

Lizenzierung

Bei der Bereitstellung von Astra Control Center wird es mit einer eingebetteten 90-Tage-Evaluierungslizenz für 4,800 CPU-Einheiten installiert. Wenn Sie mehr Kapazität oder einen längeren Evaluierungszeitraum benötigen oder auf eine komplette Lizenz aktualisieren möchten, können Sie eine andere Evaluierungslizenz oder eine komplette Lizenz von NetApp beziehen.

Sie erhalten eine Lizenz auf eine der folgenden Arten:

- Wenn Sie Astra Control Center evaluieren und andere Evaluierungsbedingungen als in der eingebetteten Evaluierungslizenz benötigen, wenden Sie sich an NetApp, um eine andere Evaluierungslizenzdatei zu anfordern.
- "Wenn Sie Astra Control Center bereits gekauft haben, generieren Sie Ihre NetApp Lizenzdatei (NLF)." Melden Sie sich dazu auf der NetApp Support-Website an und navigieren Sie zu Ihren Softwarelizenzen im

Menü „Systeme“.

Details zu Lizenzen, die für ONTAP Storage Back-Ends erforderlich sind, finden Sie unter "Unterstützte Storage-Back-Ends".

> Stellen Sie sicher, dass Ihre Lizenz mindestens so viele CPU-Einheiten wie erforderlich aktiviert. Wenn die Anzahl der CPU-Einheiten, die Astra Control Center derzeit verwaltet, die verfügbaren CPU-Einheiten in der neuen Lizenz überschreitet, können Sie die neue Lizenz nicht anwenden.

Evaluierungslizenzen und Volllizenzen

Eine eingebettete Evaluierungslizenz wird mit der neuen Astra Control Center-Installation bereitgestellt. Eine Evaluierungslizenz ermöglicht über einen begrenzten Zeitraum (90 Tage) dieselben Funktionen und Funktionen wie eine Volllizenz. Nach dem Evaluierungszeitraum ist eine vollständige Lizenz erforderlich, um mit voller Funktionalität fortzufahren.

Ablauf der Lizenz

Wenn die aktive Astra Control Center-Lizenz abläuft, sind die UI- und API-Funktionen für die folgenden Funktionen nicht verfügbar:

- Manuelle lokale Snapshots und Backups
- Geplante lokale Snapshots und Backups
- Wiederherstellen aus einem Snapshot oder einem Backup
- Klonen aus einem Snapshot oder aktuellem Status
- Managen neuer Applikationen
- Konfigurieren von Replikationsrichtlinien

Berechnung der Lizenznutzung

Wenn Sie dem Astra Control Center einen neuen Cluster hinzufügen, zählen diese nicht auf verbrauchte Lizenzen, bis mindestens eine auf dem Cluster ausgeführte Applikation vom Astra Control Center verwaltet wird.

Wenn Sie eine App auf einem Cluster verwalten, sind alle CPU-Einheiten dieses Clusters im Lizenzverbrauch von Astra Control Center enthalten, mit Ausnahme der CPU-Einheiten des Red hat OpenShift-Cluster-Node, die von einem mit dem Label gemeldet werden `node-role.kubernetes.io/infra: ""`.

> Red hat OpenShift Infrastruktur-Nodes nutzen keine Lizenzen in Astra Control Center. Um einen Node als Infrastruktur-Node zu markieren, wenden Sie die Beschriftung an `node-role.kubernetes.io/infra: ""` Auf den Node.

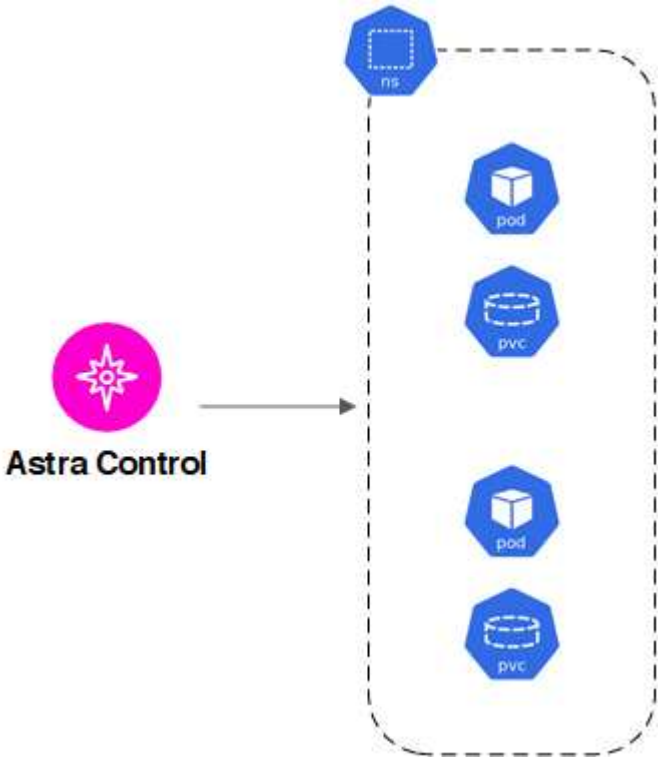
Weitere Informationen

- "Fügen Sie beim ersten Einrichten des Astra Control Center eine Lizenz hinzu"
- "Aktualisieren einer vorhandenen Lizenz"

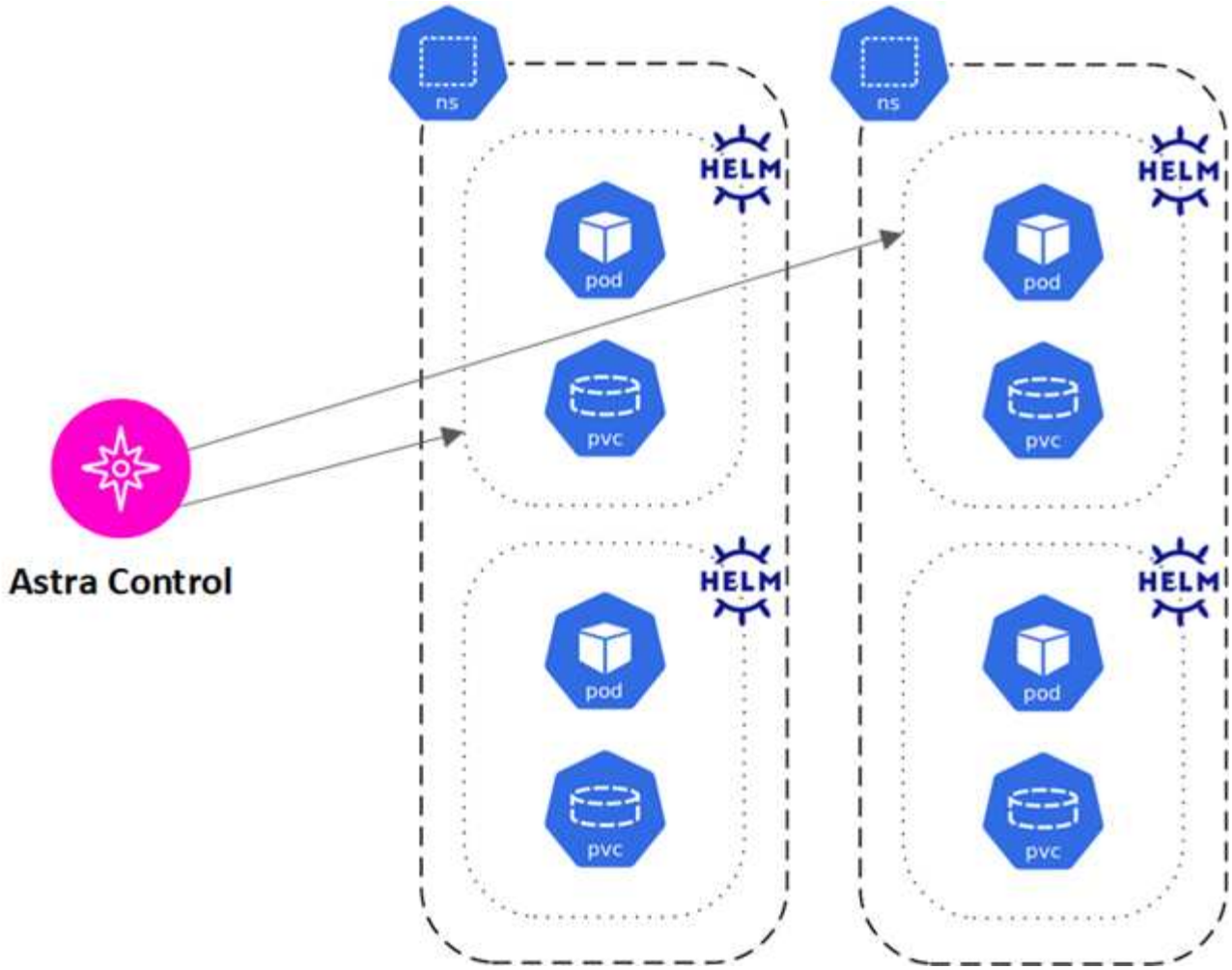
Applikationsmanagement

Wenn Astra Control Ihre Cluster erkennt, werden die Apps auf diesen Clustern solange nicht verwaltet, bis Sie das gewünschte Management wählen. Eine verwaltete Anwendung in Astra Control kann eine der folgenden sein:

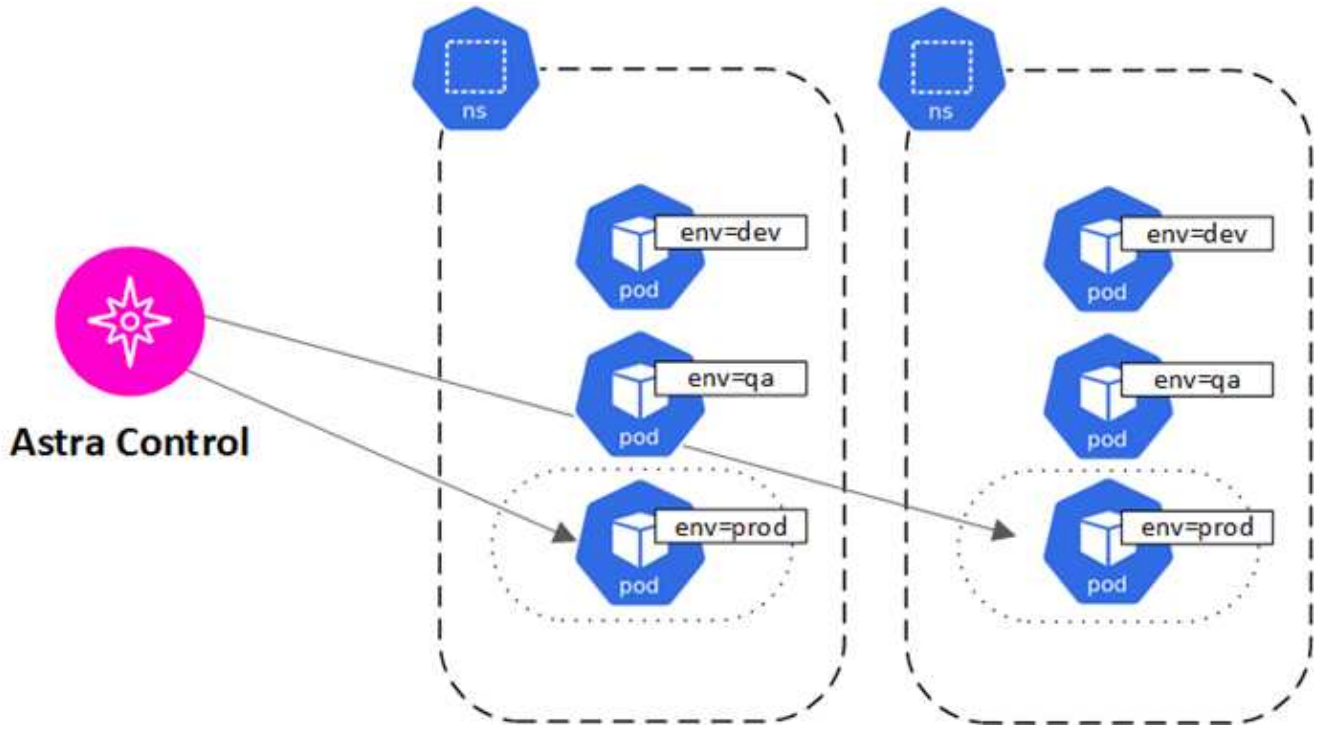
- Einen Namespace, einschließlich aller Ressourcen in diesem Namespace



- Eine individuelle Anwendung, die innerhalb einer oder mehrerer Namespaces bereitgestellt wird (in diesem Beispiel wird helm3 verwendet)



- Eine Gruppe von Ressourcen, die innerhalb eines oder mehrerer Namespaces durch ein Kubernetes-Label identifiziert werden



Storage-Klassen und persistente Volume-Größe

Astra Control Center unterstützt NetApp ONTAP und Longhorn als Storage-Back-Ends.

Überblick

Das Astra Control Center unterstützt Folgendes:

- **Von ONTAP Storage unterstützte Astra Trident Storage-Klassen**: Wenn Sie ein ONTAP-Backend verwenden, bietet Astra Control Center die Möglichkeit, das ONTAP-Backend zu importieren und verschiedene Monitoring-Informationen zu melden.
- **CSI-basierte Speicherklassen mit Longhorn**: Sie können Longhorn mit dem Longhorn Container Storage Interface (CSI) Treiber verwenden.

Astra Trident Storage-Klassen sollten außerhalb des Astra Control Center vorkonfiguriert werden.

Speicherklassen

Wenn Sie dem Astra Control Center einen Cluster hinzufügen, werden Sie aufgefordert, eine zuvor konfigurierte Storage-Klasse auf diesem Cluster als Standard-Storage-Klasse auszuwählen. Diese Storage-Klasse wird verwendet, wenn in einem persistent Volume Claim (PVC) keine Storage-Klasse angegeben ist. Die Standard-Speicherklasse kann jederzeit im Astra Control Center geändert werden und jede Speicherklasse kann jederzeit verwendet werden, indem der Name der Speicherklasse im PVC- oder Helm-Diagramm angegeben wird. Stellen Sie sicher, dass nur eine einzelne Standard-Storage-Klasse für Ihr Kubernetes-Cluster definiert ist.

Finden Sie weitere Informationen

- "Astra Trident-Dokumentation"

Benutzerrollen und Namespaces

Informieren Sie sich über Benutzerrollen und Namespaces in Astra Control und darüber, wie Sie mit ihnen den Zugriff auf Ressourcen in Ihrem Unternehmen steuern können.

Benutzerrollen

Sie können Rollen verwenden, um den Zugriff von Benutzern auf Ressourcen oder Funktionen von Astra Control zu steuern. Im Folgenden sind die Benutzerrollen in Astra Control aufgeführt:

- Ein **Viewer** kann Ressourcen anzeigen.
- Ein **Mitglied** verfügt über Berechtigungen für Viewer-Rollen und kann Apps und Cluster verwalten, Apps verwalten und Snapshots und Backups löschen.
- Ein **Admin** verfügt über Berechtigungen für die Mitgliederrolle und kann alle anderen Benutzer außer dem Eigentümer hinzufügen und entfernen.
- Ein **Owner** hat Administratorrechte und kann beliebige Benutzerkonten hinzufügen und entfernen.

Sie können einem Mitglied oder Viewer-Benutzer Einschränkungen hinzufügen, um den Benutzer auf einen oder mehrere Benutzer zu beschränken Namespaces.

Namespaces

Ein Namespace ist ein Umfang, den Sie bestimmten Ressourcen innerhalb eines von Astra Control gemanagten Clusters zuweisen können. Astra Control erkennt Namespaces eines Clusters, wenn Sie das Cluster zu Astra Control hinzufügen. Sobald die Namespaces erkannt wurden, können sie Benutzern als Bedingungen zuweisen. Nur Mitglieder, die Zugriff auf diesen Namespace haben, können diese Ressource nutzen. Sie können Namespaces verwenden, um den Zugriff auf Ressourcen anhand eines Paradigmas zu steuern, das für Ihr Unternehmen sinnvoll ist, z. B. nach physischen Regionen oder Abteilungen innerhalb eines Unternehmens. Wenn Sie einem Benutzer Einschränkungen hinzufügen, können Sie diesen Benutzer so konfigurieren, dass er Zugriff auf alle Namespaces oder nur auf bestimmte Namespaces hat. Sie können auch Namespace-Einschränkungen mithilfe von Namespace-Etiketten zuweisen.

Weitere Informationen

"Managen Sie lokale Benutzer und Rollen"

Nutzen Sie Das Astra Control Center

Starten Sie das Anwendungsmanagement

Nach Ihnen "Fügen Sie dem Astra Control Management einen Cluster hinzu", Sie können Apps auf dem Cluster installieren (außerhalb von Astra Control) und dann auf der Seite Anwendungen in Astra Control, um die Apps und ihre Ressourcen zu definieren.

Sie können Apps definieren und managen, die Storage-Ressourcen mit laufenden Pods umfassen, oder Applikationen mit Storage-Ressourcen, ohne laufende Pods auszuführen. Applikationen, auf denen keine Pods ausgeführt werden, werden als reine Daten-Applikationen bezeichnet.

Anforderungen für das Applikationsmanagement

Astra Control verfügt über folgende Anforderungen an das Applikationsmanagement:

- **Lizenzierung**: Um Anwendungen mit Astra Control Center zu verwalten, benötigen Sie entweder die eingebettete Astra Control Center-Evaluierungslizenz oder eine Volllizenz.
- **Namesaces**: Apps können mit Astra Control innerhalb eines oder mehrerer spezifizierter Namespaces auf einem einzigen Cluster definiert werden. Eine App kann Ressourcen enthalten, die mehrere Namespaces innerhalb desselben Clusters umfassen. Astra Control unterstützt nicht die Möglichkeit, Applikationen über mehrere Cluster hinweg zu definieren.
- **Speicherklasse**: Wenn Sie eine Anwendung installieren, die eine Speicherklasse explizit festgelegt hat und Sie die App klonen müssen, muss das Zielcluster für den Klonvorgang die ursprünglich angegebene Speicherklasse haben. Das Klonen einer Applikation mit einer explizit festgelegten Storage-Klasse auf ein Cluster ohne dieselbe Storage-Klasse schlägt fehl.
- **Kubernetes-Ressourcen**: Applikationen, die nicht mit Astra Control gesammelte Kubernetes-Ressourcen verwenden, verfügen unter Umständen nicht über umfassende Funktionen zum App-Datenmanagement. Astra Control sammelt die folgenden Kubernetes-Ressourcen:

`ClusterRole`	`ClusterRoleBinding`	`ConfigMap`
`CronJob`	`CustomResourceDefinition`	`CustomResource`
`DaemonSet`	`DeploymentConfig`	`HorizontalPodAutoscaler`
`Ingress`	`MutatingWebhook`	`NetworkPolicy`
`PersistentVolumeClaim`	`Pod`	`PodDisruptionBudget`
`PodTemplate`	`ReplicaSet`	`Role`
`RoleBinding`	`Route`	`Secret`
`Service`	`ServiceAccount`	`StatefulSet`
`ValidatingWebhook`		

Unterstützte Installationsmethoden für Anwendungen

Astra Control unterstützt folgende Installationsmethoden für Anwendungen:

- **Manifest-Datei**: Astra Control unterstützt Apps, die aus einer Manifest-Datei mit kubectl installiert wurden. Beispiel:

```
kubectl apply -f myapp.yaml
```

- **Helm 3**: Wenn Sie Helm zur Installation von Apps verwenden, benötigt Astra Control Helm Version 3. Das Management und Klonen von Apps, die mit Helm 3 installiert sind (oder ein Upgrade von Helm 2 auf Helm 3), wird vollständig unterstützt. Das Verwalten von mit Helm 2 installierten Apps wird nicht unterstützt.
- **Vom Betreiber bereitgestellte Apps**: Astra Control unterstützt Apps, die mit Namespace-Scoped Operatoren installiert sind und im Allgemeinen mit einer "Pass-by-value" anstatt einer "Pass-by-reference" Architektur konzipiert sind. Ein Operator und die App, die er installiert, müssen denselben Namespace verwenden. Möglicherweise müssen Sie die YAML-Bereitstellungsdatei für den Operator ändern, um sicherzustellen, dass dies der Fall ist.

  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.

Installation von Apps auf dem Cluster

Nach dem haben "Hat den Cluster hinzugefügt" Bei Astra Control können Sie Apps installieren oder vorhandene Apps auf dem Cluster managen. Jede Anwendung, die einem oder mehreren Namespaces zugeordnet ist, kann verwaltet werden.

Definieren von Apps

Nachdem Astra Control Namespaces auf den Clustern ermittelt hat, können Sie Anwendungen definieren, die Sie managen möchten. Sie können wählen die als Applikation gemanagt werden sollen,Verwalten einer App, die einen oder mehrere Namespaces umfasst Oder der als App gemanagt werden soll,Management eines gesamten Namespace als einzelne Applikation. All dies kommt auf die Granularität zurück, die Sie für Datensicherungsvorgänge benötigen.

Astra Control ermöglicht es Ihnen zwar, beide Ebenen der Hierarchie (den Namespace und die Apps in diesem Namespace oder den überspannenden Namespaces) separat zu verwalten, aber die beste Vorgehensweise ist es, eine oder andere zu wählen. Aktionen, die Sie in Astra Control nehmen, können fehlschlagen, wenn die Aktionen gleichzeitig sowohl auf Namespace- als auch auf App-Ebene stattfinden.

Beispielsweise könnten Sie eine Backup-Policy für „maria“ setzen, die über ein wöchentliches Kadenz verfügt, aber vielleicht müssen Sie „mariadb“ (die sich im selben Namespace befindet) häufiger sichern. Basierend auf diesen Anforderungen müssen die Applikationen separat gemanagt werden und nicht als Single Namespace App.

Bevor Sie beginnen

- Astra Control ist ein Kubernetes Cluster.
- Eine oder mehrere installierte Applikationen auf dem Cluster. Weitere Informationen zu unterstützten App-Installationsmethoden.
- Namespaces sind auf dem Kubernetes-Cluster vorhanden, die Sie Astra Control hinzugefügt haben.
- (Optional) ein Kubernetes-Etikett auf jeder beliebigen "Unterstützte Kubernetes-Ressourcen".

Eine Bezeichnung ist ein Schlüssel-/Wertpaar, das Sie Kubernetes-Objekten zur Identifizierung zuweisen können. Etiketten erleichtern das Sortieren, Organisieren und Auffinden Ihrer Kubernetes-Objekte. Weitere Informationen zu Kubernetes-Labels: "In der offiziellen Kubernetes-Dokumentation finden Sie weitere Informationen".

Über diese Aufgabe

- Bevor Sie beginnen, sollten Sie auch verstehen "Verwalten von Standard- und Systemnames".
- Wenn Sie in Astra Control mehrere Namespaces mit Ihren Apps verwenden möchten, "Ändern Sie Benutzerrollen mit Namespace-Einschränkungen" Nach dem Upgrade auf eine Astra Control Center-Version mit Unterstützung für mehrere Namespace.
- Anweisungen zum Verwalten von Apps mit der Astra Control API finden Sie im "Astra Automation und API-Informationen".

Optionen für Applikationsmanagement

- die als Applikation gemanagt werden sollen
- der als App gemanagt werden soll

Definition von Ressourcen, die als Applikation gemanagt werden sollen

Sie können den angeben "Kubernetes-Ressourcen bilden eine Applikation" Die Sie mit Astra Control verwalten möchten. Durch die Definition einer App können Sie Elemente Ihres Kubernetes Clusters zu einer einzelnen Applikation gruppieren. Diese Sammlung von Kubernetes-Ressourcen ist nach Namespace und Auswahlkriterien für Labels organisiert.

Mit der Definition einer App haben Sie eine granularere Kontrolle über die Auswirkungen einer Astra Control Operation, einschließlich Klonen, Snapshots und Backups.

Stellen Sie bei der Definition von Applikationen sicher, dass Sie keine Kubernetes-Ressource in mehrere Applikationen mit Sicherungsrichtlinien aufnehmen. Überlappende Sicherungsrichtlinien für Kubernetes-Ressourcen können zu Datenkonflikten führen. Lesen Sie mehr in einem Beispiel.

Erweitern Sie, um weitere Informationen über das Hinzufügen von Ressourcen mit Clusterbereich zu Ihren App-Namespaces zu erhalten.

Außerdem können Sie Clusterressourcen importieren, die den Namespace-Ressourcen zugeordnet sind und die automatisch mit Astra Control integriert sind. Sie können eine Regel hinzufügen, die Ressourcen einer bestimmten Gruppe, Art, Version und optional eine Bezeichnung enthält. Dies sollten Sie tun, wenn Astra Control nicht automatisch Ressourcen enthält.

Sie können keine Ressourcen mit Cluster-Umfang ausschließen, die automatisch von Astra Control enthalten sind.

Sie können Folgendes hinzufügen `apiVersions` (Welche Gruppen sind mit der API-Version kombiniert):

RessourcArt	ApiVersions (Gruppe + Version)
`ClusterRole`	rbac.authorization.k8s.io/v1
`ClusterRoleBinding`	rbac.authorization.k8s.io/v1
`CustomResource`	Apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
`CustomResourceDefinition`	Apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
`MutatingWebhookConfiguration`	Zulassungsregistrierung.k8s.io/v1
`ValidatingWebhookConfiguration`	Zulassungsregistrierung.k8s.io/v1

Schritte

1. Wählen Sie auf der Seite Anwendungen die Option **Definieren**.
2. Geben Sie im Fenster **Anwendung definieren** den App-Namen ein.
3. Wählen Sie den Cluster aus, auf dem Ihre Anwendung ausgeführt wird, in der Dropdown-Liste * Cluster* aus.
4. Wählen Sie aus der Dropdown-Liste **Namespace** einen Namespace für Ihre Anwendung aus.

   Apps können mit Astra Control in einem oder mehreren festgelegten Namespaces auf einem einzigen Cluster definiert werden. Eine App kann Ressourcen enthalten, die mehrere Namespaces innerhalb desselben Clusters umfassen. Astra Control unterstützt nicht die Möglichkeit, Applikationen über mehrere Cluster hinweg zu definieren.

5. (Optional) Geben Sie in jedem Namespace ein Etikett für die Kubernetes-Ressourcen ein. Sie können ein einzelnes Etikett oder ein Label-Auswahlkriterium (Abfrage) festlegen.

   Weitere Informationen zu Kubernetes-Labels: "In der offiziellen Kubernetes-Dokumentation finden Sie weitere Informationen".

6. (Optional) Fügen Sie zusätzliche Namespaces für die App hinzu, indem Sie **Namespace hinzufügen** und den Namespace aus der Dropdown-Liste auswählen.
7. (Optional) Geben Sie für alle weiteren Namespaces, die Sie hinzufügen, die Kriterien für eine einzelne Beschriftung oder eine Labelauswahl ein.

8. (Optional) um Ressourcen mit Cluster-Umfang zusätzlich zu den Ressourcen von Astra Control automatisch einzubeziehen, überprüfen Sie **zusätzliche Ressourcen mit Cluster-Umfang** und füllen Sie Folgendes aus:
   a. Wählen Sie **Add include Rule**.
   b. **Gruppe**: Wählen Sie aus der Dropdown-Liste die API-Ressourcengruppe aus.
   c. **Art**: Wählen Sie aus der Dropdown-Liste den Namen des Objektschemas aus.
   d. **Version**: Geben Sie die API-Version ein.
   e. **Label selector**: Optional ein Etikett enthalten, das der Regel hinzugefügt werden soll. Mit diesem Etikett werden nur die Ressourcen abgerufen, die diesem Etikett entsprechen. Wenn Sie kein Etikett bereitstellen, sammelt Astra Control alle Instanzen der für diesen Cluster angegebenen Ressourcenkartart.
   f. Überprüfen Sie die Regel, die auf Ihren Einträgen erstellt wird.
   g. Wählen Sie **Hinzufügen**.

   Sie können die gewünschten Ressourcenregeln mit dem Cluster-Umfang erstellen. Die Regeln werden in der Anwendungsübersicht definieren angezeigt.

9. Wählen Sie **Definieren**.
10. Nachdem Sie **Definieren** ausgewählt haben, wiederholen Sie den Vorgang für andere Apps, je nach Bedarf.

Nachdem Sie die Definition einer App abgeschlossen haben, wird die App in angezeigt `Healthy` Geben Sie in der Liste der Apps auf der Seite Anwendungen an. Sie können sie jetzt klonen und erstellen Backups und Snapshots.

Die gerade hinzugefügte App verfügt möglicherweise über ein Warnsymbol unter der Spalte „geschützt“, das angibt, dass sie nicht gesichert ist und noch keine Backups geplant sind.

Um Details zu einer bestimmten App anzuzeigen, wählen Sie den App-Namen aus.

Um die Ressourcen anzuzeigen, die dieser App hinzugefügt wurden, wählen Sie die Registerkarte **Ressourcen** aus. Wählen Sie in der Spalte Ressource die Nummer nach dem Ressourcennamen aus, oder geben Sie den Ressourcennamen in die Suche ein, um die zusätzlichen Ressourcen anzuzeigen, die im Cluster enthalten sind.

Definieren Sie einen Namespace, der als App gemanagt werden soll

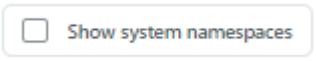
Sie können alle Kubernetes-Ressourcen im Namespace zum Astra Control Management hinzufügen, indem Sie die Ressourcen dieses Namespace als Applikation definieren. Diese Methode ist es besser, Apps einzeln zu definieren, wenn Sie alle Ressourcen in einem bestimmten Namespace ähnlich und in gemeinsamen Abständen verwalten und schützen wollen.

Schritte

1. Wählen Sie auf der Seite Cluster einen Cluster aus.
2. Wählen Sie die Registerkarte **Namesaces** aus.
3. Wählen Sie das Menü Aktionen für den Namespace aus, der die Anwendungsressourcen enthält, die Sie verwalten möchten, und wählen Sie **als Anwendung definieren** aus.

Wenn Sie mehrere Anwendungen definieren möchten, wählen Sie in der Namensliste die Schaltfläche **Aktionen** in der linken oberen Ecke aus und wählen Sie **als Anwendung definieren** aus. Damit werden mehrere einzelne Anwendungen in ihren einzelnen Namespaces definiert. Informationen zu Multi-Namespace-Anwendungen finden Sie unter die als Applikation gemanagt werden sollen.

Aktivieren Sie das Kontrollkästchen **System-Namespaces**, um Systemnamenpaces anzuzeigen, die in der Regel nicht standardmäßig in der App-Verwaltung verwendet werden.



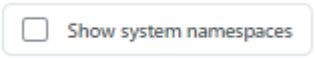
"Weitere Informationen".

Nach Abschluss des Prozesses werden die dem Namespace zugeordneten Anwendungen im angezeigt `Associated applications` Spalte.

Und wie sieht es mit System-Namespaces aus?

Astra Control erkennt auch Systemnames auf einem Kubernetes Cluster. Wir zeigen Ihnen diese System-Namespaces standardmäßig nicht, da es selten ist, dass Sie die Ressourcen der System-App sichern müssen.

Sie können Systemnames auf der Registerkarte Namespaces für ein ausgewähltes Cluster anzeigen, indem Sie das Kontrollkästchen **System-Namespaces** anzeigen auswählen.



Astra Control Center wird standardmäßig nicht als eine Applikation angezeigt, die Sie managen können. Sie können jedoch eine Astra Control Center-Instanz sichern und wiederherstellen.

Beispiel: Separate Sicherungsrichtlinie für verschiedene Versionen

In diesem Beispiel managt das devops Team eine Implementierung der Version „canary“. Der Cluster des Teams verfügt über drei Pods mit nginx. Zwei der Stative sind der stabilen Freisetzung gewidmet. Der dritte POD ist für den canary Release.

Der Kubernetes Administrator des devops-Teams fügt das Label hinzu `deployment=stable` Zu den stabilen Entriegelungstativen. Das Team fügt das Label hinzu `deployment=canary` Zum canary Release POD.

Die stabile Version des Teams umfasst eine Notwendigkeit für stündliche Snapshots und tägliche Backups. Die version von canary ist kurzlebig, deshalb wollen sie für alles, was gekennzeichnet ist, eine weniger aggressive, kurzfristige Schutzpolitik erstellen `deployment=canary`.

Um mögliche Datenkonflikte zu vermeiden, erstellt der Admin zwei Apps: Eine für die "canary"-Version und eine für die "Stable"-Version. Hierdurch werden Backups, Snapshots und Klonvorgänge für die beiden Gruppen von Kubernetes-Objekten getrennt.

Weitere Informationen

- "Verwenden Sie die Astra Control API"
- "Verwaltung einer Anwendung aufheben"

Schützen von Applikationen

Sicherungsübersicht

Mit Astra Control Center können Sie Backups, Klone, Snapshots und Sicherungsrichtlinien für Ihre Applikationen erstellen. Durch das Backup Ihrer Applikationen sind Ihre Services und zugehörigen Daten so verfügbar wie möglich. Bei einem Disaster-Szenario ist durch die Wiederherstellung aus einem Backup die vollständige Recovery einer Applikation und der zugehörigen Daten bei minimalen Unterbrechungen sichergestellt. Backups, Klone und Snapshots schützen vor gängigen Bedrohungen wie Ransomware, versehentlichen Datenverlusten und Umweltnotfällen. "Informieren Sie sich über die verfügbaren Arten von Datensicherung im Astra Control Center und wann Sie diese einsetzen können".

Darüber hinaus können Sie Applikationen zur Vorbereitung auf das Disaster Recovery auf ein Remote-Cluster replizieren.

Workflow für Applikationssicherung

Anhand des folgenden Beispielworkflows können Sie Ihre Apps schützen.

[Eins] Sicherung aller Applikationen

Um sicherzustellen, dass Ihre Apps sofort geschützt sind, "Erstellen Sie ein manuelles Backup aller Apps".

[Zwei] Konfigurieren Sie für jede Applikation eine Sicherungsrichtlinie

Zur Automatisierung zukünftiger Backups und Snapshots "Konfigurieren Sie für jede Applikation eine Sicherungsrichtlinie". Sie können beispielsweise mit wöchentlichen Backups und täglichen Snapshots beginnen und jeweils mit einer Monatsaufbewahrung beginnen. Für manuelle Backups und Snapshots wird dringend die Automatisierung von Backups und Snapshots mit einer Schutzrichtlinie empfohlen.

[Drittens] Passen Sie die Sicherungsrichtlinien an

Wenn Applikationen und ihre Nutzungsmuster sich ändern, passen Sie die Sicherungsrichtlinien nach Bedarf an, um einen bestmöglichen Schutz zu gewährleisten.

[Vier] Replizieren von Applikationen in einem Remote-Cluster

"Replizierung von Applikationen" Erstellen eines Remote-Clusters mithilfe von NetApp SnapMirror. Astra Control repliziert Snapshots in einen Remote-Cluster und bietet damit asynchrone Disaster Recovery-Funktion.

[Fünf] Stellen Sie im Notfall Ihre Applikationen mit dem neuesten Backup oder der neuesten Replizierung auf ein Remote-System wieder her

Im Falle eines Datenverlustes sind Recoverys bis möglich "Wiederherstellung des aktuellen Backups" Zuerst für jede Anwendung. Sie können dann den letzten Snapshot wiederherstellen (falls verfügbar). Sie können die Replikation zu einem Remote-System verwenden.

Sichern von Applikationen durch Snapshots und Backups

Alle Applikationen werden gesichert, indem Snapshots und Backups über eine

automatisierte Sicherungsrichtlinie oder im Ad-hoc-Verfahren erstellt werden. Sie können die Astra Control Center-UI oder verwenden "Die Astra Control API" Um Anwendungen zu schützen.

Über diese Aufgabe

- **Helm implementierte Apps**: Wenn Sie Helm zum Bereitstellen von Apps verwenden, benötigt 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. Mit Helm 2 implementierte Apps werden nicht unterstützt.
- **(nur OpenShift-Cluster) Richtlinien hinzufügen**: Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder Kubernetes-Namespace) eine SecurityContext-UID zugewiesen. Um Astra Control Center zum Schutz Ihrer App zu aktivieren und die App in ein anderes Cluster oder Projekt in OpenShift zu verschieben, müssen Sie Richtlinien hinzufügen, mit denen die App als beliebige UID ausgeführt werden kann. Als Beispiel erteilen die folgenden OpenShift-CLI-Befehle der WordPress-App die entsprechenden Richtlinien.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Sie können die folgenden Aufgaben zum Schutz Ihrer Applikationsdaten ausführen:

- Konfigurieren einer Sicherungsrichtlinie
- Erstellen Sie einen Snapshot
- Erstellen Sie ein Backup
- Backup und Restore für den wirtschaftlichen Betrieb von ontap-nas
- Unveränderliches Backup erstellen
- Anzeigen von Snapshots und Backups
- Snapshots löschen
- Abbrechen von Backups
- Backups löschen

Konfigurieren einer Sicherungsrichtlinie

Eine Sicherungsrichtlinie sichert eine Applikation, indem Snapshots, Backups oder beides nach einem definierten Zeitplan erstellt werden. Sie können Snapshots und Backups stündlich, täglich, wöchentlich und monatlich erstellen. Außerdem können Sie die Anzahl der beizubehaltenden Kopien festlegen.

Wenn Sie Backups oder Snapshots öfter als einmal pro Stunde benötigen, können Sie dies tun "Erstellen Sie mithilfe der Astra Control REST API Snapshots und Backups".

> Wenn Sie eine Schutzrichtlinie definieren, die unveränderliche Backups für WORM-Buckets (Write Once Read Many) erstellt, stellen Sie sicher, dass die Aufbewahrungszeit für die Backups nicht kürzer ist als der für den Bucket konfigurierte Aufbewahrungszeitraum.

Verschieben Sie Backup- und Replikationspläne, um Zeitplanüberschneidungen zu vermeiden. Führen Sie beispielsweise jede Stunde Backups oben in der Stunde durch, und planen Sie die Replikation, um mit einem Offset von 5 Minuten und einem Intervall von 10 Minuten zu beginnen.

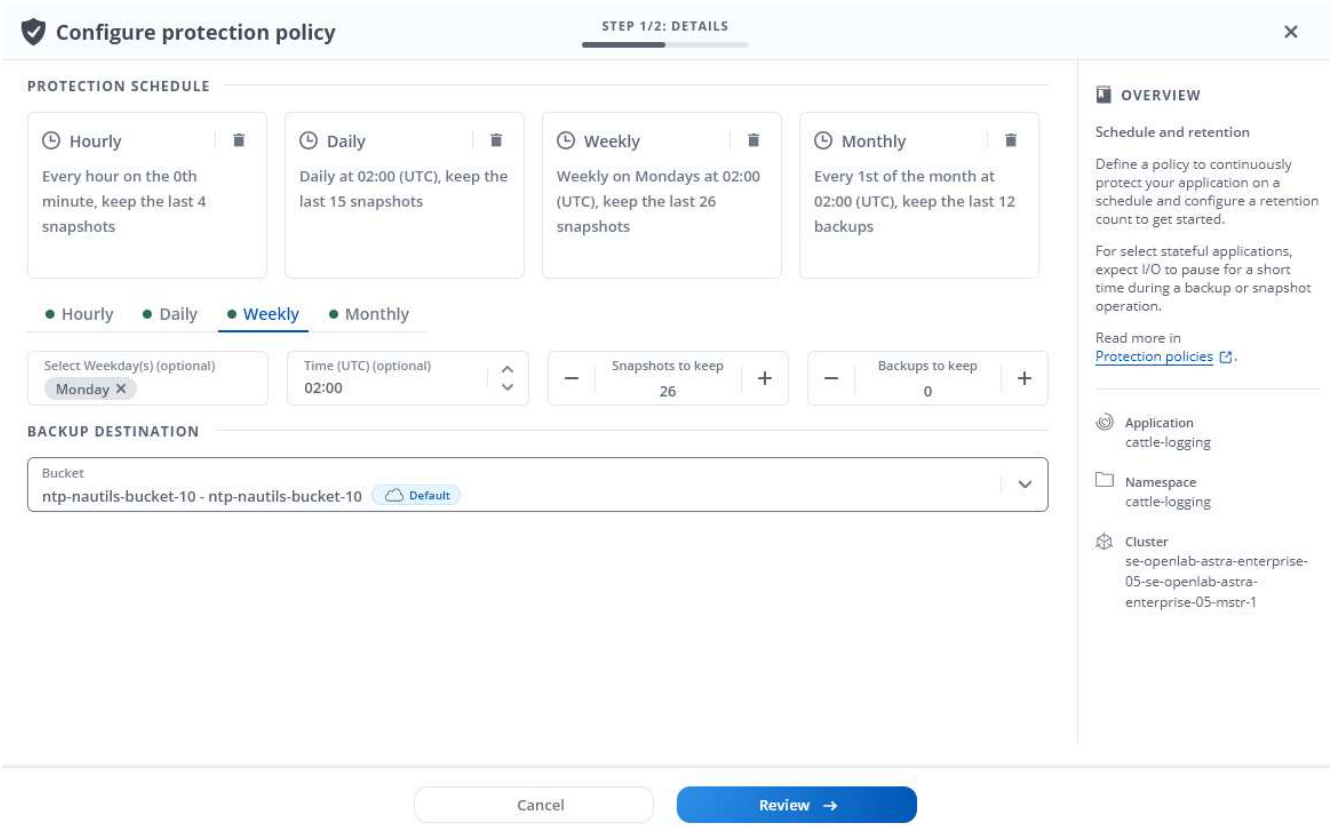
Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie **Datenschutz**.
3. Wählen Sie **Schutzrichtlinie Konfigurieren**.
4. Legen Sie einen Sicherungszeitplan fest, indem Sie die Anzahl der Snapshots und Backups auswählen, die stündlich, täglich, wöchentlich und monatlich erstellt werden sollen.

   Sie können die stündlichen, täglichen, wöchentlichen und monatlichen Zeitpläne gleichzeitig festlegen. Ein Zeitplan wird erst aktiviert, wenn Sie eine Aufbewahrungsstufe festlegen.

   Wenn Sie ein Aufbewahrungsniveau für Backups festlegen, können Sie den Bucket auswählen, auf dem Sie die Backups speichern möchten.

   Im folgenden Beispiel sind vier Sicherungspläne definiert: Stündlich, täglich, wöchentlich und monatlich für Snapshots und Backups.



5. Wählen Sie **Bewertung**.
6. Wählen Sie **Schutzrichtlinie Festlegen.**

Ergebnis

Astra Control implementiert die Datensicherungsrichtlinien, indem Snapshots und Backups mithilfe der von

Ihnen definierten Zeitplan und Aufbewahrungsrichtlinie erstellt und aufbewahrt werden.

Erstellen Sie einen Snapshot

Sie können jederzeit einen On-Demand-Snapshot erstellen.

Über diese Aufgabe

Astra Control unterstützt die Snapshot-Erstellung mithilfe von Storage-Klassen, die von den folgenden Treibern unterstützt werden:

- `ontap-nas`
- `ontap-san`
- `ontap-san-economy`

> Wenn Ihre App eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Treiber, Snapshots können nicht erstellt werden. Verwenden Sie eine alternative Storage-Klasse für Snapshots.

Schritte

1. Wählen Sie **Anwendungen**.
2. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für die gewünschte App die Option **Snapshot** aus.
3. Passen Sie den Namen des Snapshots an und wählen Sie dann **Weiter**.
4. Überprüfen Sie die Snapshot-Zusammenfassung und wählen Sie **Snapshot**.

Ergebnis

Der Snapshot-Prozess beginnt. Ein Snapshot ist erfolgreich, wenn der Status in der Spalte **Zustand** auf der Seite **Datenschutz** > **Snapshots** in der Spalte **Zustand** angegeben ist.

Erstellen Sie ein Backup

Sie können eine App jederzeit sichern.

Über diese Aufgabe

Buckets in Astra Control berichten nicht über die verfügbare Kapazität. Bevor Sie von Astra Control gemanagte Applikationen sichern oder klonen, überprüfen Sie Bucket-Informationen im entsprechenden Storage-Managementsystem.

Wenn Ihre App eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Fahrer, müssen Sie Aktivieren Sie Backup und Restore Funktionalität. Stellen Sie sicher, dass Sie einen definiert haben `backendType` Parameter in im "Kubernetes Storage-Objekt" Mit einem Wert von `ontap-nas-economy` Bevor Sie Schutzmaßnahmen durchführen.

Astra Control unterstützt die Backup-Erstellung mithilfe von Storage-Klassen, die von den folgenden Treibern unterstützt werden:

- `ontap-nas`
- `ontap-nas-economy`
- `ontap-san`
- `ontap-san-economy`

Schritte

1. Wählen Sie **Anwendungen**.
2. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für die gewünschte App die Option **Sichern** aus.
3. Passen Sie den Namen des Backups an.
4. Wählen Sie aus, ob die Anwendung aus einem vorhandenen Snapshot gesichert werden soll. Wenn Sie diese Option auswählen, können Sie aus einer Liste vorhandener Snapshots auswählen.
5. Wählen Sie aus der Liste der Storage-Buckets einen Ziel-Bucket für das Backup aus.
6. Wählen Sie **Weiter**.
7. Überprüfen Sie die Backup-Zusammenfassung und wählen Sie **Backup**.

Ergebnis

Astra Control erstellt ein Backup der App.

- Wenn Ihr Netzwerk ausfällt oder ungewöhnlich langsam ist, kann es zu einer Zeit für einen Backup-Vorgang kommen. Dies führt zum Fehlschlagen der Datensicherung.
- Wenn Sie eine laufende Sicherung abbrechen müssen, befolgen Sie die Anweisungen unter Abbrechen von Backups. Um das Backup zu löschen, warten Sie, bis es abgeschlossen ist, und befolgen Sie die Anweisungen unter Backups löschen.
- 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. Der Datensicherungsvorgang ist innerhalb von Minuten erfolgreich und Sie können mit der Management Software für das Storage-Backend die Änderung der Volume-Größe bestätigen.

Backup und Restore für den wirtschaftlichen Betrieb von ontap-nas

Astra Control Provisioner bietet Backup- und Restore-Funktionen für Storage-Back-Ends, die das verwenden `ontap-nas-economy` Storage-Klasse.

Bevor Sie beginnen

- Das ist schon "Astra Control Provisioner wurde aktiviert".
- Sie haben eine Anwendung in Astra Control definiert. Diese Anwendung verfügt nur über begrenzte Schutzfunktionen, bis Sie diesen Vorgang abgeschlossen haben.
- Das ist schon `ontap-nas-economy` Ausgewählt als Standard-Storage-Klasse für Ihr Storage-Back-End.

Erweitern Sie für Konfigurationsschritte

1. Gehen Sie auf dem ONTAP Storage Back-End folgendermaßen vor:

   a. Finden Sie die SVM, die den hostet `ontap-nas-economy`-Basierte Volumen der Anwendung.

   b. Melden Sie sich bei einem Terminal an, das mit ONTAP verbunden ist, wo die Volumes erstellt werden.

   c. Snapshot-Verzeichnis für SVM ausblenden:

   > Diese Änderung wirkt sich auf die gesamte SVM aus. Auf das verborgene Verzeichnis kann weiterhin zugegriffen werden.

   ```
   nfs modify -vserver <svm name> -v3-hide-snapshot enabled
   ```

   +

   > Vergewissern Sie sich, dass das Snapshot-Verzeichnis auf dem ONTAP-Speicher-Back-End verborgen ist. Das Ausblenden dieses Verzeichnisses kann zu einem Verlust des Zugriffs auf Ihre Anwendung führen, insbesondere wenn es NFSv3 verwendet.

2. Gehen Sie in Astra Trident wie folgt vor:

   a. Aktivieren Sie das Snapshot-Verzeichnis für jedes PV, das ist `ontap-nas-economy` Basiert und mit der Applikation verknüpft:

   ```
   tridentctl update volume <pv name> --snapshot-dir=true --pool
   -level=true -n trident
   ```

   b. Vergewissern Sie sich, dass das Snapshot-Verzeichnis für jedes zugeordnete PV aktiviert wurde:

   ```
   tridentctl get volume <pv name> -n trident -o yaml | grep
   snapshotDir
   ```

   Antwort:

   ```
   snapshotDirectory: "true"
   ```

3. Aktualisieren Sie in Astra Control die Applikation nach Aktivierung aller zugehörigen Snapshot-Verzeichnisse, damit Astra Control den geänderten Wert erkennt.

Ergebnis

Die Applikation ist bereit für Backups und Restores mit Astra Control. Jede PVC kann auch von anderen Anwendungen für Backups und Wiederherstellungen verwendet werden.

Unveränderliches Backup erstellen

Ein unveränderliches Backup kann nicht geändert, gelöscht oder überschrieben werden, solange die Aufbewahrungsrichtlinie auf dem Bucket, der das Backup speichert, dies verbietet. Erstellen Sie unveränderliche Backups, indem Sie Applikationen in Buckets sichern, für die eine Aufbewahrungsrichtlinie konfiguriert ist. Siehe "Datensicherung" Finden Sie wichtige Informationen zum Arbeiten mit unveränderlichen Backups.

Bevor Sie beginnen

Sie müssen den Ziel-Bucket mit einer Aufbewahrungsrichtlinie konfigurieren. Je nachdem, welchen Storage-Anbieter Sie verwenden, hängt die Vorgehensweise davon ab. Weitere Informationen finden Sie in der Dokumentation des Speicheranbieters:

- **Amazon Web Services**: "Aktivieren Sie S3 Object Lock beim Erstellen des Buckets und legen Sie den Standardaufbewahrungsmodus „Governance“ mit einer Standardaufbewahrungszeit fest".
- **NetApp StorageGRID**: "Aktivieren Sie S3 Object Lock beim Erstellen des Buckets und legen Sie den Standardaufbewahrungsmodus „Compliance“ mit einer Standardaufbewahrungsdauer fest".

> Buckets in Astra Control berichten nicht über die verfügbare Kapazität. Bevor Sie von Astra Control gemanagte Applikationen sichern oder klonen, überprüfen Sie Bucket-Informationen im entsprechenden Storage-Managementsystem.

> Wenn Ihre App eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Treiber, stellen Sie sicher, dass Sie einen definiert haben `backendType` Parameter in im "Kubernetes Storage-Objekt" Mit einem Wert von `ontap-nas-economy` Bevor Sie Schutzmaßnahmen durchführen.

Schritte

1. Wählen Sie **Anwendungen**.
2. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für die gewünschte App die Option **Sichern** aus.
3. Passen Sie den Namen des Backups an.
4. Wählen Sie aus, ob die Anwendung aus einem vorhandenen Snapshot gesichert werden soll. Wenn Sie diese Option auswählen, können Sie aus einer Liste vorhandener Snapshots auswählen.
5. Wählen Sie aus der Liste der Storage-Buckets einen Ziel-Bucket für das Backup aus. Ein WORM-Bucket (Write Once Read Many) wird neben dem Bucket-Namen mit dem Status „gesperrt“ angezeigt.

   > Wenn es sich bei dem Bucket um einen nicht unterstützten Typ handelt, wird dies angezeigt, wenn Sie den Mauszeiger über den Bucket bewegen oder ihn auswählen.

6. Wählen Sie **Weiter**.
7. Überprüfen Sie die Backup-Zusammenfassung und wählen Sie **Backup**.

Ergebnis

Astra Control erstellt eine unveränderliche Sicherung der App.

- Wenn Ihr Netzwerk ausfällt oder ungewöhnlich langsam ist, kann es zu einer Zeit für einen Backup-Vorgang kommen. Dies führt zum Fehlschlagen der Datensicherung.
- Wenn Sie versuchen, zwei unveränderliche Backups derselben App gleichzeitig im selben Bucket zu erstellen, verhindert Astra Control, dass das zweite Backup gestartet wird. Warten Sie, bis die erste Sicherung abgeschlossen ist, bevor Sie eine andere starten.
- Sie können ein auslaufendes unveränderliches Backup nicht abbrechen.
- 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. Der Datensicherungsvorgang ist innerhalb von Minuten erfolgreich und Sie können mit der Management Software für das Storage-Backend die Änderung der Volume-Größe bestätigen.

Anzeigen von Snapshots und Backups

Sie können die Snapshots und Backups einer Anwendung auf der Registerkarte Datenschutz anzeigen.

Ein unveränderliches Backup wird neben dem verwendeten Bucket mit dem Status „gesperrt“ angezeigt.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie **Datenschutz**.

   Die Snapshots werden standardmäßig angezeigt.
3. Wählen Sie **Backups**, um die Liste der Backups anzuzeigen.

Snapshots löschen

Löschen Sie die geplanten oder On-Demand Snapshots, die Sie nicht mehr benötigen.

Sie können keinen Snapshot löschen, der derzeit repliziert wird.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie **Datenschutz**.
3. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für den gewünschten Snapshot die Option **Snapshot löschen** aus.
4. Geben Sie das Wort „Löschen“ ein, um das Löschen zu bestätigen und wählen Sie dann **Ja, Snapshot löschen** aus.

Ergebnis

Astra Control löscht den Snapshot.

Abbrechen von Backups

Sie können ein gerade einlaufenden Backup abbrechen.

Um ein Backup abzubrechen, muss sich das Backup befinden `Running` Bundesland. Sie können ein Backup, das sich in befindet, nicht abbrechen `Pending` Bundesland.

Sie können ein auslaufendes unveränderliches Backup nicht abbrechen.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie **Datenschutz**.
3. Wählen Sie **Backups**.
4. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für das gewünschte Backup die Option **Abbrechen** aus.
5. Geben Sie das Wort „Abbrechen“ ein, um den Vorgang zu bestätigen, und wählen Sie dann **Ja, Sicherung abbrechen** aus.

Backups löschen

Löschen Sie die geplanten oder On-Demand-Backups, die Sie nicht mehr benötigen. Sie können ein Backup, das an einem unveränderlichen Bucket erstellt wurde, erst dann löschen, wenn dies durch die Aufbewahrungsrichtlinie des Buckets möglich ist.

Sie können ein unveränderliches Backup nicht vor Ablauf der Aufbewahrungsfrist löschen.

Wenn Sie eine laufende Sicherung abbrechen müssen, befolgen Sie die Anweisungen unter Abbrechen von Backups. Um das Backup zu löschen, warten Sie, bis es abgeschlossen ist, und befolgen Sie diese Anweisungen.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie **Datenschutz**.
3. Wählen Sie **Backups**.
4. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für das gewünschte Backup die Option **Backup löschen** aus.
5. Geben Sie das Wort „Löschen“ ein, um das Löschen zu bestätigen und wählen Sie dann **Ja, Sicherung löschen**.

Ergebnis

Astra Control löscht das Backup.

Wiederherstellung von Applikationen

Astra Control kann Ihre Applikation aus einem Snapshot oder einem Backup wiederherstellen. Das Wiederherstellen aus einem vorhandenen Snapshot erfolgt schneller, wenn die Anwendung auf dasselbe Cluster wiederhergestellt wird. Sie können die Astra Control UI oder verwenden "Astra Control API" Zur Wiederherstellung von Applikationen.

Bevor Sie beginnen

- **Schützen Sie Ihre Anwendungen zuerst**: Es wird dringend empfohlen, dass Sie einen Snapshot oder ein Backup Ihrer Anwendung vor der Wiederherstellung machen. Auf diese Weise können Sie aus dem Snapshot oder Backup klonen, wenn die Wiederherstellung nicht erfolgreich war.
- **Zieldatenträger prüfen**: Wenn Sie eine andere Speicherklasse wiederherstellen, stellen Sie sicher, dass die Speicherklasse den gleichen persistenten Zugriffsmodus für Volumes verwendet (z. B. ReadWriteMany). Der Wiederherstellungsvorgang schlägt fehl, wenn der Zugriffsmodus des Ziel-persistenten Volumes anders ist. Wenn das persistente Quell-Volume beispielsweise den RWX-Zugriffsmodus verwendet, wählen Sie eine Ziel-Storage-Klasse aus, die RWX nicht bereitstellen kann, wie z. B. Azure Managed Disks, AWS EBS, Google Persistent Disk oder `ontap-san`Wird dazu führen, dass der Wiederherstellungsvorgang fehlschlägt. Weitere Informationen zu den Zugriffsmodi für persistente Volumes finden Sie im "Kubernetes" Dokumentation.
- **Planung des Platzbedarfs**: Wenn Sie eine in-Place-Wiederherstellung einer Applikation durchführen, die NetApp ONTAP Storage nutzt, kann sich der von der wiederhergestellten Applikation genutzte Speicherplatz verdoppeln. Nachdem Sie eine in-Place-Wiederherstellung durchgeführt haben, entfernen Sie alle unerwünschten Snapshots aus der wiederhergestellten Applikation, um Speicherplatz freizugeben.
- **(nur Red hat OpenShift-Cluster) Richtlinien hinzufügen**: Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder Kubernetes-Namespace) eine SecurityContext-UID zugewiesen. Um Astra Control Center zum Schutz Ihrer App zu aktivieren und die App in ein anderes Cluster oder Projekt in OpenShift zu verschieben, müssen Sie Richtlinien hinzufügen, mit denen die App als beliebige UID ausgeführt werden kann. Als Beispiel erteilen die folgenden OpenShift-CLI-Befehle der WordPress-App die entsprechenden Richtlinien.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

- **Unterstützte Storage Class Treiber**: Astra Control unterstützt die Wiederherstellung von Backups mit Speicherklassen, die von den folgenden Treibern unterstützt werden:
  - `ontap-nas`
  - `ontap-nas-economy`
  - `ontap-san`
  - `ontap-san-economy`
- **(nur ontap-nas-Economy-Treiber) Backups und Wiederherstellungen**: Vor dem Backup oder der Wiederherstellung einer App, die eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Überprüfen Sie, ob der "Das snapshot Verzeichnis auf dem ONTAP Storage-Backend ist verborgen". Das Ausblenden dieses Verzeichnisses kann zu einem Verlust des Zugriffs auf Ihre Anwendung führen, insbesondere wenn es NFSv3 verwendet.
- **Helm bereitgestellte Apps**: Apps, die mit Helm 3 (oder von Helm 2 auf Helm 3 aktualisiert) bereitgestellt werden, werden vollständig unterstützt. Mit Helm 2 implementierte Apps werden nicht unterstützt.

> Die Durchführung einer in-Place-Wiederherstellung in einer Anwendung, in der Ressourcen mit einer anderen Anwendung geteilt werden, kann unbeabsichtigte Ergebnisse haben. Alle Ressourcen, die von den Applikationen gemeinsam genutzt werden, werden ersetzt, wenn eine in-Place-Wiederherstellung für eine der Applikationen durchgeführt wird. Weitere Informationen finden Sie unter bei der Ressourcen mit einer anderen App geteilt werden,Dieses Beispiel.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie im Menü Optionen in der Spalte Aktionen die Option **Wiederherstellen** aus.
3. Wählen Sie den Wiederherstellungstyp aus:
   - **Wiederherstellen auf ursprünglichen Namespaces**: Verwenden Sie dieses Verfahren, um die App an Ort und Stelle auf dem ursprünglichen Cluster wiederherzustellen.

     > Wenn Ihre App eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Treiber, müssen Sie die App mithilfe der ursprünglichen Speicherklassen wiederherstellen. Sie können keine andere Storage-Klasse angeben, wenn Sie die App im gleichen Namespace wiederherstellen.

     i. Wählen Sie den Snapshot oder das Backup aus, mit dem die App direkt wiederhergestellt werden soll. Dadurch wird die App auf eine frühere Version von selbst zurückgesetzt.

     ii. Wählen Sie **Weiter**.

     > Wenn Sie in einem zuvor gelöschten Namespace wiederherstellen, wird im Rahmen des Wiederherstellungsprozesses ein neuer Namespace mit demselben Namen erstellt. Alle Benutzer, die über Berechtigungen zum Verwalten von Apps im zuvor gelöschten Namespace verfügen, müssen die Rechte für den neu erstellten Namespace manuell wiederherstellen.

   - **Wiederherstellen auf neuen Namespaces**: Verwenden Sie dieses Verfahren, um die App auf einem anderen Cluster oder mit verschiedenen Namespaces von der Quelle wiederherzustellen.

     i. Geben Sie den Namen für die wiederhergestellte App an.

     ii. Wählen Sie das Ziel-Cluster für die Anwendung aus, die Sie wiederherstellen möchten.

     iii. Geben Sie für jeden mit der App verknüpften Quell-Namespace einen Ziel-Namespace ein.

     > Astra Control erstellt als Teil dieser Wiederherstellungsoption neue Ziel-Namespaces. Die angegebenen Ziel-Namespaces dürfen nicht bereits im Ziel-Cluster vorhanden sein.

     iv. Wählen Sie **Weiter**.

     v. Wählen Sie den Snapshot oder das Backup aus, mit dem die App wiederhergestellt werden soll.

     vi. Wählen Sie **Weiter**.

     vii. Folgenden Optionen wählbar:

     - **Wiederherstellung unter Verwendung der ursprünglichen Speicherklassen**: Die Anwendung verwendet die ursprünglich zugeordnete Speicherklasse, es sei denn, sie existiert nicht auf dem Zielcluster. In diesem Fall wird die Standard-Storage-Klasse für das Cluster verwendet.
     - **Wiederherstellen mit einer anderen Storage-Klasse**: Wählen Sie eine Storage-Klasse aus, die auf dem Ziel-Cluster vorhanden ist. Alle Applikations-Volumes, unabhängig von den ursprünglich zugewiesenen Storage-Klassen, werden im Rahmen der Wiederherstellung in diese andere Storage-Klasse migriert.

     viii. Wählen Sie **Weiter**.
4. Wählen Sie die Ressourcen aus, die gefiltert werden sollen:
   - **Alle Ressourcen wiederherstellen**: Alle mit der ursprünglichen App verknüpften Ressourcen

wiederherstellen.

- **Ressourcen filtern**: Geben Sie Regeln an, um einen Untersatz der ursprünglichen Anwendungsressourcen wiederherzustellen:
  i. Wählen Sie diese Option, um Ressourcen aus der wiederhergestellten Anwendung einzuschließen oder auszuschließen.
  ii. Wählen Sie entweder **Include rule** oder **Add exclude rule** aus und konfigurieren Sie die Regel, um die richtigen Ressourcen während der Anwendungswiederherstellung zu filtern. Sie können eine Regel bearbeiten oder entfernen und eine Regel erneut erstellen, bis die Konfiguration korrekt ist.

> Weitere Informationen zum Konfigurieren von Einschließen- und Ausschlussregeln finden Sie unter Filtern Sie Ressourcen während einer Anwendungswiederherstellung.

5. Wählen Sie **Weiter**.
6. Lesen Sie die Details zur Wiederherstellungsaktion sorgfältig durch, geben Sie „Restore“ ein (falls Sie dazu aufgefordert werden), und wählen Sie **Restore**.

Ergebnis

Astra Control stellt die App basierend auf den von Ihnen angegebenen Informationen wieder her. Wenn Sie die Applikation bereits wiederhergestellt haben, wird der Inhalt vorhandener persistenter Volumes durch den Inhalt persistenter Volumes aus der wiederhergestellten App ersetzt.

> Nach einer Datensicherungsoperation (Klonen, Backup oder Wiederherstellung) und einer anschließenden Anpassung des persistenten Volumes beträgt die Verzögerung bis zu zwanzig Minuten, bevor die neue Volume-Größe in der Web-Benutzeroberfläche angezeigt wird. Der Datensicherungsvorgang ist innerhalb von Minuten erfolgreich und Sie können mit der Management Software für das Storage-Backend die Änderung der Volume-Größe bestätigen.

> Jeder Mitgliedsbenutzer mit Namespace-Einschränkungen nach Namespace-Name/ID oder anhand von Namespace-Bezeichnungen kann eine Applikation in einem neuen Namespace im selben Cluster oder einem anderen Cluster in seinem Unternehmenskonto 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 das Mitgliedskonto bearbeiten und Rolleneinschränkungen aktualisieren, damit der betroffene Benutzer Zugriff auf den neuen Namespace gewährt.

Filtern Sie Ressourcen während einer Anwendungswiederherstellung

Sie können eine Filterregel zu einem hinzufügen "Wiederherstellen" Vorgang, bei dem vorhandene Anwendungsressourcen angegeben werden, die in die wiederhergestellte Anwendung einbezogen oder von ihr ausgeschlossen werden sollen. Sie können Ressourcen basierend auf einem bestimmten Namespace, Label oder GVK (GroupVersionRind) ein- oder ausschließen.

Erweitern Sie die Erweiterung, um weitere Informationen über ein- und Ausschlussszenarien zu erhalten

- **Sie wählen eine Include-Regel mit ursprünglichen Namespaces (in-Place-Wiederherstellung)**: Vorhandene Anwendungsressourcen, die Sie in der Regel definieren, werden gelöscht und durch jene aus dem ausgewählten Snapshot oder Backup ersetzt, den Sie für die Wiederherstellung verwenden. Alle Ressourcen, die Sie nicht in der Include-Regel angeben, bleiben unverändert.
- **Sie wählen eine Include-Regel mit neuen Namespaces**: Verwenden Sie die Regel, um die spezifischen Ressourcen auszuwählen, die Sie in der wiederhergestellten Anwendung benötigen. Alle Ressourcen, die Sie nicht in der Include-Regel angeben, werden nicht in die wiederhergestellte Anwendung aufgenommen.
- **Sie wählen eine Ausschlussregel mit ursprünglichen Namespaces (in-Place-Wiederherstellung)**: Die von Ihnen angegebenen Ressourcen werden nicht wiederhergestellt und bleiben unverändert. Ressourcen, die Sie nicht ausschließen möchten, werden vom Snapshot oder Backup wiederhergestellt. Alle Daten auf persistenten Volumes werden gelöscht und neu erstellt, wenn das entsprechende StatefulSet Teil der gefilterten Ressourcen ist.
- **Sie wählen eine Ausschlussregel mit neuen Namespaces** aus: Wählen Sie mit der Regel die Ressourcen aus, die Sie aus der wiederhergestellten Anwendung entfernen möchten. Ressourcen, die Sie nicht ausschließen möchten, werden vom Snapshot oder Backup wiederhergestellt.

Regeln sind entweder Einschließen oder Ausschließen von Typen. Regeln, die Ressourceneinschluss und -Ausschluss kombinieren, sind nicht verfügbar.

Schritte

1. Nachdem Sie die Option Ressourcen filtern und im Assistenten zum Wiederherstellen von Apps eine Option ein- oder ausschließen ausgewählt haben, wählen Sie **Einschlussregel hinzufügen** oder **Ausschlussregel hinzufügen** aus.

   Sie können keine im Cluster enthaltenen Ressourcen ausschließen, die von Astra Control automatisch berücksichtigt werden.

2. Konfigurieren Sie die Filterregel:

   Sie müssen mindestens einen Namespace, eine Bezeichnung oder GVK angeben. Stellen Sie sicher, dass alle Ressourcen, die Sie behalten, nachdem die Filterregeln angewendet wurden, ausreichend sind, um die wiederhergestellte Anwendung in einem ordnungsgemäßen Zustand zu halten.

   a. Wählen Sie einen bestimmten Namespace für die Regel aus. Wenn Sie keine Auswahl treffen, werden alle Namespaces im Filter verwendet.

      Wenn Ihre Anwendung ursprünglich mehrere Namespaces enthielt und Sie sie in neuen Namespaces wiederherstellen, werden alle Namespaces erstellt, auch wenn sie keine Ressourcen enthalten.

   b. (Optional) Geben Sie einen Ressourcennamen ein.

   c. (Optional) **Etikettenauswahl**: A einschließen "Etikettenauswahl" Um der Regel hinzuzufügen. Mit der Etikettenauswahl werden nur die Ressourcen gefiltert, die der ausgewählten Bezeichnung entsprechen.

   d. (Optional) Wählen Sie **Use GVK (GroupVersionRind) Set, um Ressourcen zu filtern**, um weitere

Filteroptionen zu erhalten.

> Wenn Sie einen GVK-Filter verwenden, müssen Sie Version und Art angeben.

i. (Optional) **Gruppe**: Wählen Sie aus der Dropdown-Liste die Kubernetes API-Gruppe aus.
ii. **Kind**: Wählen Sie aus der Dropdown-Liste das Objektschema für den Kubernetes-Ressourcentyp aus, der im Filter verwendet werden soll.
iii. **Version**: Wählen Sie die Kubernetes API Version.

3. Überprüfen Sie die Regel, die auf Ihren Einträgen erstellt wird.
4. Wählen Sie **Hinzufügen**.

> Sie können beliebig viele Regeln für ein- und Ausschlussressourcen erstellen. Die Regeln werden in der Zusammenfassung der Wiederherstellungsanwendung angezeigt, bevor Sie den Vorgang starten.

In-Place-Wiederherstellungskomplikationen für eine App, bei der Ressourcen mit einer anderen App geteilt werden

Sie können einen in-Place-Wiederherstellungsvorgang für eine App durchführen, die Ressourcen mit einer anderen App teilt und unbeabsichtigte Ergebnisse liefert. Alle Ressourcen, die von den Applikationen gemeinsam genutzt werden, werden ersetzt, wenn eine in-Place-Wiederherstellung für eine der Applikationen durchgeführt wird.

Im Folgenden sehen Sie ein Beispielszenario, das eine unerwünschte Situation verursacht, wenn die NetApp SnapMirror Replizierung für eine Wiederherstellung verwendet wird:

1. Sie definieren die Anwendung `app1` Verwenden des Namespace `ns1`.
2. Sie konfigurieren eine Replikationsbeziehung für `app1`.
3. Sie definieren die Anwendung `app2` (Auf demselben Cluster) mit den Namespaces `ns1` Und `ns2`.
4. Sie konfigurieren eine Replikationsbeziehung für `app2`.
5. Die Replizierung wird für rückgängig gemacht `app2`. Das verursacht das `app1` App auf dem Quellcluster zu deaktivieren.

Replizierung von Applikationen zwischen Storage Back-Ends mithilfe von SnapMirror Technologie

Mithilfe von Astra Control können Sie mit den asynchronen Replizierungsfunktionen der NetApp SnapMirror Technologie Business Continuity für Ihre Applikationen erzielen: Mit Low-RPO (Recovery Point Objective) und Low-RTO (Recovery Time Objective). Nach der Konfiguration können Ihre Applikationen auf diese Weise Daten und Applikationsänderungen von einem Storage-Back-End auf ein anderes replizieren, sowohl im selben Cluster als auch zwischen verschiedenen Clustern.

Einen Vergleich zwischen Backups/Wiederherstellungen und Replikation finden Sie unter "Konzepte zur Datensicherung".

Applikationen lassen sich in unterschiedlichen Szenarien replizieren, z. B. nur on-Premises, in Hybrid- und

Multi-Cloud-Szenarien:

- Standort A vor Ort zu Standort A
- On-Premises-Standort A auf On-Premises-Standort B
- On-Premises- und Cloud-Umgebungen mit Cloud Volumes ONTAP
- Cloud mit Cloud Volumes ONTAP auf On-Premises-Umgebungen
- Cloud mit Cloud Volumes ONTAP in die Cloud (zwischen verschiedenen Regionen desselben Cloud-Providers oder verschiedener Cloud-Provider)

Astra Control kann Applikationen über On-Premises-Cluster, On-Premises-Cluster und Cloud (mithilfe von Cloud Volumes ONTAP) oder zwischen Clouds (Cloud Volumes ONTAP auf Cloud Volumes ONTAP) replizieren.

> Sie können gleichzeitig eine andere App in die entgegengesetzte Richtung replizieren. So können beispielsweise Applikationen A, B und C von Datacenter 1 nach Datacenter 2 repliziert werden. Applikationen X, Y und Z können von Datacenter 2 zu Datacenter 1 repliziert werden.

Mit Astra Control können Sie die folgenden Aufgaben für die Replikation von Anwendungen ausführen:

- Richten Sie eine Replikationsbeziehung ein
- Online-Funktion einer replizierten Anwendung auf dem Ziel-Cluster (Failover)
- Resynchronisierung einer fehlgeschlagenen Überreplikation
- Replizierung der Applikation wird rückgängig gemacht
- Führen Sie ein Failback von Anwendungen auf das ursprüngliche Quellcluster durch
- Löschen einer Replikationsbeziehung für Anwendungen

Replikationsvoraussetzungen

Für die Replizierung der Astra Control Applikation müssen vor Beginn die folgenden Voraussetzungen erfüllt sein:

ONTAP Cluster

- **Astra Trident**: Astra Trident Version 22.10 oder höher muss sowohl auf den Quell- als auch auf den Ziel-Kubernetes-Clustern vorhanden sein, die ONTAP als Backend nutzen. Astra Control unterstützt die Replizierung mit NetApp SnapMirror Technologie unter Verwendung von Storage-Klassen, die von den folgenden Treibern unterstützt werden:
  - `ontap-nas`
  - `ontap-san`
- **Lizenzen**: Asynchrone Lizenzen von ONTAP SnapMirror, die das Datensicherungspaket verwenden, müssen sowohl auf den Quell- als auch auf den Ziel-ONTAP-Clustern aktiviert sein. Siehe "Übersicht über die SnapMirror Lizenzierung in ONTAP" Finden Sie weitere Informationen.

Peering

- **Cluster und SVM**: Die ONTAP Speicher-Back-Ends müssen aktiviert werden. Siehe "Übersicht über Cluster- und SVM-Peering" Finden Sie weitere Informationen.

Vergewissern Sie sich, dass die in der Replizierungsbeziehung zwischen zwei ONTAP-Clustern verwendeten SVM-Namen eindeutig sind.

- **Astra Trident und SVM**: Die Peering von Remote-SVMs müssen für Astra Trident auf dem Ziel-Cluster verfügbar sein.

Astra Control Center

- **Managed Back-Ends**: Sie müssen ONTAP Storage Back-Ends in Astra Control Center hinzufügen und verwalten, um eine Replikationsbeziehung zu erstellen.

  nur Astra Control Provisioner: Das Hinzufügen und Managen von ONTAP-Storage-Back-Ends in Astra Control Center ist optional, wenn Sie die Astra Control Provisioner für Astra Control Center 23.10 oder höher aktiviert haben.

- **Verwaltete Cluster**: Fügen Sie mit Astra Control die folgenden Cluster hinzu und verwalten Sie sie idealerweise an verschiedenen Ausfalldomänen oder Standorten:
  - Quell-Kubernetes-Cluster
  - Kubernetes Ziel-Cluster
  - Zugeordnete ONTAP-Cluster
- **Benutzerkonten**: Wenn Sie ein ONTAP-Speicher-Backend zu Astra Control Center hinzufügen, wenden Sie die Anmeldeinformationen des Benutzers mit der Rolle "admin" an. Diese Rolle verfügt über Zugriffsmethoden `http` Und `ontapi` Sowohl auf ONTAP Quell- als auch auf Ziel-Clustern aktiviert. Siehe "Managen von Benutzerkonten in der ONTAP Dokumentation" Finden Sie weitere Informationen.

  nur Astra Control Provisioner: Wenn Sie die Astra Control Provisioner-Funktion aktiviert haben, müssen Sie zum Managen von Clustern in Astra Control Center keine spezielle „Admin“-Rolle mehr definieren, da diese Zugangsdaten in Astra Control Center nicht mehr erforderlich sind.

"Implementieren Sie Astra Control Center" In einer dritten Fehlerdomäne oder an einem sekundären Standort für nahtloses Disaster Recovery

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

Konfiguration von Astra Trident/ONTAP

Für Astra Control Center müssen Sie mindestens ein Storage-Back-End konfigurieren, das die Replizierung sowohl für die Quell- als auch für die Ziel-Cluster unterstützt. Wenn die Quell- und Ziel-Cluster identisch sind, sollte die Zielanwendung ein anderes Speicher-Back-End als die Quellanwendung verwenden, um die beste Ausfallsicherheit zu erreichen.

Die Astra Control Replizierung unterstützt Applikationen, die eine einzige Storage-Klasse verwenden. Wenn Sie eine App zu einem Namespace hinzufügen, stellen Sie sicher, dass die App dieselbe Storage-Klasse wie andere Apps im Namespace hat. Wenn Sie eine PVC zu einer replizierten App hinzufügen, stellen Sie sicher, dass die neue PVC die gleiche Speicherklasse hat wie andere VES im Namespace.

Richten Sie eine Replikationsbeziehung ein

Die Einrichtung einer Replikationsbeziehung umfasst Folgendes:

- Festlegen der Häufigkeit, mit der Astra Control einen App-Snapshot erstellen soll (einschließlich der Kubernetes-Ressourcen der Applikation sowie der Volume-Snapshots für die jeweiligen Volumes der Applikation)
- Auswahl des Replizierungszeitplans (einschließlich Kubernetes-Ressourcen und persistente Volume-Daten)
- Einstellen der Uhrzeit für die Erstellung des Snapshots

Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie die Registerkarte **Data Protection** > **Replication** aus.
3. Wählen Sie **Configure Replication Policy** aus. Oder wählen Sie im Feld Anwendungsschutz die Option Aktionen aus, und wählen Sie **Replikationsrichtlinie konfigurieren** aus.
4. Geben Sie die folgenden Informationen ein, oder wählen Sie sie aus:
   - **Ziel-Cluster**: Geben Sie einen Ziel-Cluster ein (dies kann mit dem Quell-Cluster identisch sein).
   - **Ziel-Storage-Klasse**: Wählen oder geben Sie die Storage-Klasse ein, die die Peering-SVM auf dem Ziel-ONTAP-Cluster verwendet. Als Best Practice sollte die Ziel-Storage-Klasse auf ein anderes Storage-Back-End verweisen als die Quell-Storage-Klasse.
   - **Replikationstyp**: `Asynchronous` Ist derzeit der einzige verfügbare Replikationstyp.
   - **Ziel-Namespace**: Geben Sie neue oder vorhandene Ziel-Namespaces für das Ziel-Cluster ein.
   - (Optional) Fügen Sie zusätzliche Namespaces hinzu, indem Sie **Namespace hinzufügen** und den Namespace aus der Dropdown-Liste auswählen.
   - **Replikationsfrequenz**: Legen Sie fest, wie oft Astra Control einen Snapshot erstellen und an das Ziel replizieren soll.
   - **Offset**: Legen Sie die Anzahl der Minuten von der Spitze der Stunde fest, die Astra Control für einen Snapshot verwenden soll. Möglicherweise möchten Sie einen Offset verwenden, sodass er nicht mit anderen geplanten Vorgängen übereinstimmt.

   Verschieben Sie Backup- und Replikationspläne, um Zeitplanüberschneidungen zu vermeiden. Führen Sie beispielsweise jede Stunde Backups oben in der Stunde durch, und planen Sie die Replikation, um mit einem Offset von 5 Minuten und einem Intervall von 10 Minuten zu beginnen.

5. Wählen Sie **Weiter**, lesen Sie die Zusammenfassung und wählen Sie **Speichern**.

   Zunächst wird der Status „App-Mirror“ angezeigt, bevor der erste Zeitplan stattfindet.

   Astra Control erstellt einen Applikations-Snapshot, der für die Replizierung verwendet wird.

6. Um den Snapshot-Status der Anwendung anzuzeigen, wählen Sie die Registerkarte **Anwendungen** > **Snapshots** aus.

   Der Snapshot-Name verwendet das Format von `replication-schedule-<string>`. Astra Control behält den letzten Snapshot bei, der für die Replizierung verwendet wurde. Alle älteren Replikations-Snapshots werden nach erfolgreichem Abschluss der Replikation gelöscht.

Ergebnis

Dadurch wird die Replikationsbeziehung erstellt.

Astra Control führt die folgenden Maßnahmen durch, die auf dem Aufbau der Beziehung resultieren:

- Erstellt einen Namespace auf dem Ziel (wenn er nicht vorhanden ist)
- Erstellt eine PVC auf dem Ziel-Namespace, der den PVCs der Quell-App entspricht.
- Erstellt einen ersten applikationskonsistenten Snapshot.
- Erstellt mithilfe des ersten Snapshots die SnapMirror Beziehung für persistente Volumes.

Die Seite **Data Protection** zeigt den Status und den Status der Replikationsbeziehung an:
<Health status>, <Relationship life cycle state>

Beispiel:
Normal

Erfahren Sie am Ende dieses Themas mehr über Replikationszustände und -Status.

Online-Funktion einer replizierten Anwendung auf dem Ziel-Cluster (Failover)

Mit Astra Control können Sie ein Failover replizierter Applikationen auf ein Ziel-Cluster durchführen. Durch dieses Verfahren wird die Replikationsbeziehung angehalten und die App wird auf dem Ziel-Cluster online geschaltet. Durch dieses Verfahren wird die App nicht auf dem Quell-Cluster angehalten, wenn sie betriebsbereit war.

Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie die Registerkarte **Data Protection** > **Replication** aus.
3. Wählen Sie im Menü Aktionen die Option **Failover**.
4. Überprüfen Sie auf der Seite Failover die Informationen, und wählen Sie **Failover**.

Ergebnis

Die folgenden Aktionen werden als Ergebnis des Failover-Verfahrens durchgeführt:

- Die Zielanwendung wird basierend auf dem zuletzt replizierten Snapshot gestartet.
- Das Quellcluster und die App (falls betriebsbereit) werden nicht angehalten und werden weiterhin ausgeführt.
- Der Replikationsstatus ändert sich zu „Failover“ und dann zu „Failover“, wenn er abgeschlossen ist.
- Die Schutzrichtlinie der Quell-App wird auf Basis der zum Zeitpunkt des Failovers auf der Quell-App vorhandenen Zeitpläne in die Ziel-App kopiert.
- Wenn in der Quell-App mindestens eine Ausführungshaken nach der Wiederherstellung aktiviert ist, werden diese Ausführungshaken für die Ziel-App ausgeführt.
- Astra Control zeigt die App sowohl auf den Quell- und Ziel-Clustern und deren jeweiligen Zustand.

Resynchronisierung einer fehlgeschlagenen Überreplikation

Durch den Neusynchronisierung wird die Replikationsbeziehung wiederhergestellt. Sie können die Quelle der Beziehung auswählen, um die Daten im Quell- oder Ziel-Cluster aufzubewahren. Durch diesen Vorgang werden die SnapMirror Beziehungen neu erstellt, um die Volume-Replizierung in Richtung ihrer Wahl zu starten.

Dabei wird die App auf dem neuen Ziel-Cluster angehalten, bevor die Replizierung neu erstellt wird.

Während der Resynchronisierung wird der Lebenszyklusstatus als „Einrichten“ angezeigt.

Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie die Registerkarte **Data Protection** > **Replication** aus.
3. Wählen Sie im Menü Aktionen die Option **Resync**.
4. Wählen Sie auf der Seite Resync entweder die Quell- oder Ziel-App-Instanz aus, die die zu bewahrenden Daten enthält.

   Wählen Sie die Quelle sorgfältig neu synchronisieren, da die Daten auf dem Ziel überschrieben werden.

5. Wählen Sie **Resync**, um fortzufahren.
6. Geben Sie zur Bestätigung „Resynchronisieren“ ein.
7. Wählen Sie **Ja, Resynchronisierung**, um den Vorgang abzuschließen.

Ergebnis

- Die Seite „Replikation“ zeigt den Replikationsstatus „Einrichten“ an.
- Astra Control stoppt die Applikation auf dem neuen Ziel-Cluster.
- Astra Control stellt mithilfe der SnapMirror-Resynchronisierung die persistente Volume-Replikation in die ausgewählte Richtung wieder her.
- Auf der Seite Replikation wird die aktualisierte Beziehung angezeigt.

Replizierung der Applikation wird rückgängig gemacht

Dies ist der geplante Vorgang, mit dem die Applikation auf das Ziel-Storage Back-End verschoben und gleichzeitig weiterhin zurück auf das ursprüngliche Quell-Storage Back-End repliziert werden soll. Astra Control stoppt die Quellapplikation und repliziert die Daten zum Ziel, bevor ein Failover zur Ziel-App durchgeführt wird.

In dieser Situation tauschen Sie Quelle und Ziel aus.

Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie die Registerkarte **Data Protection** > **Replication** aus.
3. Wählen Sie im Menü Aktionen die Option **Reverse Replication**.
4. Überprüfen Sie auf der Seite „Replikation umkehren“ die Informationen und wählen Sie zum Fortfahren **Replikation umkehren** aus.

Ergebnis

Die folgenden Aktionen sind auf das Ergebnis der umgekehrten Replikation zurückzuführen:

- Von den Kubernetes-Ressourcen der ursprünglichen Quell-Applikation wird ein Snapshot erstellt.
- Die PODs der ursprünglichen Quell-App werden mit sanfter Weise gestoppt, indem die Kubernetes-Ressourcen der App gelöscht werden (wodurch PVCs und PVS aktiviert bleiben).
- Nach dem Herunterfahren der Pods werden Snapshots der Volumes der App erstellt und repliziert.

- Die SnapMirror Beziehungen sind beschädigt, wodurch die Zieldatenträger für Lese-/Schreibvorgänge bereit sind.
- Die Kubernetes-Ressourcen der App werden aus dem Snapshot vor dem Herunterfahren wiederhergestellt. Dabei werden die Volume-Daten verwendet, die nach dem Herunterfahren der ursprünglichen Quell-App repliziert wurden.
- Die Replizierung wird in umgekehrter Richtung wieder hergestellt.

Führen Sie ein Failback von Anwendungen auf das ursprüngliche Quellcluster durch

Mit Astra Control können Sie nach einem Failover-Vorgang mithilfe der folgenden Sequenz von Vorgängen „Failback“ erreichen. In diesem Workflow zur Wiederherstellung der ursprünglichen Replikationsrichtung repliziert (synchronisiert) Astra Control alle Anwendungsänderungen zurück zur ursprünglichen Quellanwendung, bevor die Replikationsrichtung umkehrt.

Dieser Prozess beginnt mit einer Beziehung, bei der ein Failover zu einem Ziel durchgeführt wurde, und umfasst die folgenden Schritte:

- Starten Sie mit einem Failover-Status fehlgeschlagen.
- Beziehung neu synchronisieren.
- Die Replikation wird rückgängig gemacht.

Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie die Registerkarte **Data Protection** > **Replication** aus.
3. Wählen Sie im Menü Aktionen die Option **Resync**.
4. Wählen Sie für einen Failback-Vorgang die Failoveranwendung als Quelle für den Resync-Vorgang aus (unter Beibehaltung der nach dem Failover geschriebenen Daten).
5. Geben Sie zur Bestätigung „Resynchronisieren“ ein.
6. Wählen Sie **Ja, Resynchronisierung**, um den Vorgang abzuschließen.
7. Nach Abschluss der Resynchronisierung wählen Sie im Menü Aktionen auf der Registerkarte Data Protection > Replication die Option **Replikation umkehren** aus.
8. Überprüfen Sie auf der Seite „Replikation umkehren“ die Informationen und wählen Sie **Replikation umkehren**.

Ergebnis

Dies kombiniert die Ergebnisse aus den „Resync“- und „umgekehrten Beziehungs“-Vorgängen, um die Applikation auf dem ursprünglichen Quell-Cluster online zu schalten und die Replizierung wieder auf das ursprüngliche Ziel-Cluster zu übertragen.

Löschen einer Replikationsbeziehung für Anwendungen

Das Löschen der Beziehung führt zu zwei separaten Apps ohne Beziehung zwischen ihnen.

Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie die Registerkarte **Data Protection** > **Replication** aus.
3. Wählen Sie im Feld Anwendungsschutz oder im Beziehungsdiagramm **Replikationsbeziehung löschen** aus.

Ergebnis

Die folgenden Aktionen treten beim Löschen einer Replikationsbeziehung auf:

- Wenn die Beziehung aufgebaut ist, aber die App noch nicht auf dem Ziel-Cluster online gestellt wurde (Failover fehlgeschlagen), behält Astra Control während der Initialisierung erstellte PVCs bei, hinterlässt eine „leere“ gemanagte App auf dem Ziel-Cluster und behält die Ziel-App bei, alle Backups zu behalten, die möglicherweise erstellt wurden.
- Wenn die App auf dem Ziel-Cluster online geschaltet wurde (Failover), behält Astra Control PVCs und Ziel-Applikationen bei. Quell- und Zielapplikationen werden jetzt als unabhängige Apps behandelt. Die Backup-Zeitpläne bleiben auf beiden Applikationen, sind jedoch nicht miteinander verknüpft.

Status des Integritätsstatus der Replikationsbeziehung und Lebenszyklusstatus der Beziehungen

Astra Control zeigt den Zustand der Beziehung und die Zustände des Lebenszyklus der Replikationsbeziehung an.

Integritätsstatus von Replikationsbeziehungen

Die folgenden Status geben den Zustand der Replikationsbeziehung an:

- **Normal**: Die Beziehung wird entweder aufgebaut oder hat sich etabliert, und der letzte Snapshot wurde erfolgreich übertragen.
- **Warnung**: Die Beziehung wird entweder überschlagen oder ist gescheitert (und somit schützt die Quell-App nicht mehr).
- * Kritisch*
  - Die Beziehung wird erstellt oder fehlgeschlagen, und der letzte Versuch der Abstimmung ist fehlgeschlagen.
  - Die Beziehung wird hergestellt, und der letzte Versuch, die Hinzufügung eines neuen PVC zu vereinbaren, ist gescheitert.
  - Die Beziehung wird hergestellt (so dass ein erfolgreicher Snapshot repliziert wurde und Failover möglich ist), aber der aktuelle Snapshot ist fehlgeschlagen oder konnte nicht repliziert werden.

Lebenszyklusstatus der Replikation

Die folgenden Zustände spiegeln die verschiedenen Phasen des Replikationslebenszyklus wider:

- **Aufbau**: Es wird eine neue Replikationsbeziehung erstellt. Astra Control erstellt bei Bedarf einen Namespace, erstellt PVCs (persistente Volume Claims) auf neuen Volumes im Ziel-Cluster und erstellt SnapMirror Beziehungen. Dieser Status kann auch darauf hinweisen, dass die Replikation neu synchronisiert wird oder die Replikation rückgängig gemacht wird.
- **Etabliert**: Es besteht eine Replikationsbeziehung. Astra Control überprüft regelmäßig, ob die VES verfügbar sind, überprüft die Replizierungsbeziehung, erstellt regelmäßig Snapshots der App und identifiziert neue Quell-VES in der App. Wenn ja, erstellt Astra Control die Ressourcen, die sie in die Replikation aufnehmen.
- **Failover**: Astra Control bricht die SnapMirror-Beziehungen und stellt die Kubernetes-Ressourcen der App aus dem zuletzt erfolgreich replizierten App-Snapshot wieder her.
- **Failover**: Astra Control stoppt die Replikation vom Quellcluster, verwendet den neuesten (erfolgreichen) replizierten App-Snapshot auf dem Ziel und stellt die Kubernetes-Ressourcen wieder her.
- **Resyncing**: Astra Control resynchronisiert die neuen Daten auf der Resynchronisierungsquelle mit SnapMirror Resynchronisierung auf das Resynchronisierungsziel. Bei diesem Vorgang werden

möglicherweise einige Daten auf dem Ziel basierend auf der Synchronisationsrichtung überschrieben. Astra Control stoppt die Ausführung der Applikation auf dem Ziel-Namespace und entfernt die Kubernetes App. Während der Resynchronisierung wird der Status als „Einrichten“ angezeigt.

- **Umkehrung**: Der ist der geplante Vorgang, um die Anwendung auf das Ziel-Cluster zu verschieben, während die Replikation zurück zum ursprünglichen Quellcluster fortgesetzt wird. Astra Control stoppt die Anwendung auf dem Quell-Cluster, repliziert die Daten auf dem Ziel, bevor ein Failover über die App zum Ziel-Cluster erfolgt. Während der umgekehrten Replikation wird der Status als „Einrichten“ angezeigt.
- **Löschen**:
  - Wenn die Replikationsbeziehung hergestellt wurde, aber noch nicht Failover durchgeführt wurde, entfernt Astra Control PVCs, die während der Replikation erstellt wurden, und löscht die Ziel-verwaltete App.
  - Wenn die Replikation bereits gescheitert ist, behält Astra Control die PVCs und die Ziel-App bei.

Klonen und Migrieren von Applikationen

Eine vorhandene Applikation kann geklont werden, um eine doppelte Applikation auf demselben Kubernetes-Cluster oder einem anderen Cluster zu erstellen. Wenn Astra Control eine Applikation klonen, wird ein Klon Ihrer Applikationskonfiguration und des persistenten Storage erstellt.

Das Klonen kann sich leisten, wenn Sie Applikationen und Storage von einem Kubernetes Cluster zu einem anderen verschieben müssen. So möchten Sie beispielsweise Workloads über eine CI/CD-Pipeline und über Kubernetes-Namespaces verschieben. Sie können die Astra Control Center-UI oder verwenden "Astra Control API" Zum Klonen und Migrieren von Applikationen

Bevor Sie beginnen

- **Zieldatenträger prüfen**: Wenn Sie in eine andere Speicherklasse klonen, stellen Sie sicher, dass die Speicherklasse den gleichen persistenten Zugriffsmodus für Volumes verwendet (z. B. ReadWriteMany). Der Klonvorgang schlägt fehl, wenn der Zugriffsmodus des persistenten Volume-Ziels anders ist. Wenn das persistente Quell-Volume beispielsweise den RWX-Zugriffsmodus verwendet, wählen Sie eine Ziel-Storage-Klasse aus, die RWX nicht bereitstellen kann, wie z. B. Azure Managed Disks, AWS EBS, Google Persistent Disk oder `ontap-san`, Führt dazu, dass der Klonvorgang fehlschlägt. Weitere Informationen zu den Zugriffsmodi für persistente Volumes finden Sie im "Kubernetes" Dokumentation.
- Um Applikationen in einem anderen Cluster zu klonen, müssen Sie sicherstellen, dass die Cloud-Instanzen, die die Quell- und Ziel-Cluster enthalten (wenn sie nicht identisch sind), einen Standard-Bucket haben. Für jede Cloud-Instanz müssen Sie einen Standard-Bucket zuweisen.
- 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.

> Beim Klonen von Applikationen in OpenShift-Umgebungen muss das Astra Control Center OpenShift erlauben, Volumes anzuhängen und die Eigentümerschaft von Dateien zu ändern. Daher müssen Sie eine ONTAP Volume Export-Richtlinie konfigurieren, damit diese Vorgänge möglich sind. Sie können dies mit folgenden Befehlen tun:
>
> 1. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sys`
> 2. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -anon 65534`

Einschränkungen beim Klonen

- **Explicit Storage class**: Wenn Sie eine App mit einer explizit eingestellten Speicherklasse bereitstellen und die App klonen müssen, muss das Ziel-Cluster über die ursprünglich angegebene Speicherklasse verfügen. Das Klonen einer Applikation mit einer explizit festgelegten Storage-Klasse auf ein Cluster ohne dieselbe Storage-Klasse schlägt fehl.
- **Anwendungen mit Unterstützung der ontap-nas-Wirtschaft**: Klonvorgänge können nicht verwendet werden, wenn die Storage-Klasse Ihrer Applikation von unterstützt wird `ontap-nas-economy` Treiber. Sie können es jedoch "Backup und Restore für den wirtschaftlichen Betrieb von ontap-nas".
- **Klone und Benutzerbeschränkungen**: Jeder Mitgliedsbenutzer mit Namespace-Beschränkungen durch Namespace-Name/ID oder durch Namespace-Labels kann eine Anwendung in einem neuen Namespace im selben Cluster oder einem anderen Cluster im Konto ihres 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 das Mitgliedskonto bearbeiten und Rolleneinschränkungen aktualisieren, damit der betroffene Benutzer Zugriff auf den neuen Namespace gewährt.
- **Klone verwenden Standard-Buckets**: Während einer App-Sicherung oder App-Wiederherstellung 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.
- **Mit Jenkins CI**: Wenn Sie eine vom Betreiber implementierte Instanz von Jenkins CI klonen, müssen Sie die persistenten Daten manuell wiederherstellen. Dies ist eine Einschränkung des Bereitstellungsmodells der Applikation.
- **Mit S3 Buckets**: S3 Buckets im Astra Control Center melden keine 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.
- **Mit einer bestimmten Version von PostgreSQL**: App-Klone innerhalb desselben Clusters schlagen mit dem Bitnami PostgreSQL 11.5.0-Chart konsequent fehl. Um erfolgreich zu klonen, verwenden Sie eine frühere oder höhere Version des Diagramms.

OpenShift-Überlegungen

- **Cluster und OpenShift Versionen**: Wenn Sie eine App zwischen Clustern klonen, müssen die Quell- und Ziel-Cluster die gleiche Verteilung von OpenShift sein. Wenn Sie beispielsweise eine App aus einem OpenShift 4.7-Cluster klonen, verwenden Sie ein Ziel-Cluster, das auch OpenShift 4.7 ist.
- **Projekte und UIDs**: Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder Kubernetes-Namespace) eine SecurityContext-UID zugewiesen. Um Astra Control Center zum Schutz Ihrer App zu aktivieren und die App in ein anderes Cluster oder Projekt in OpenShift zu verschieben, müssen Sie Richtlinien hinzufügen, mit denen die App als beliebige UID ausgeführt werden kann. Als Beispiel erteilen die folgenden OpenShift-CLI-Befehle der WordPress-App die entsprechenden Richtlinien.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Schritte

1. Wählen Sie **Anwendungen**.
2. Führen Sie einen der folgenden Schritte aus:

- Wählen Sie das Menü Optionen in der Spalte **Aktionen** für die gewünschte App aus.
- Wählen Sie den Namen der gewünschten App aus, und wählen Sie rechts oben auf der Seite die Dropdown-Liste Status aus.

3. Wählen Sie **Clone**.
4. Geben Sie Details für den Klon an:
   - Geben Sie einen Namen ein.
   - Wählen Sie ein Ziel-Cluster für den Klon.
   - Geben Sie die Ziel-Namespaces für den Klon ein. Jeder mit der App verknüpfte Quell-Namespace ordnet den von Ihnen definierten Ziel-Namespace zu.

     Astra Control erstellt im Rahmen des Klonvorgangs neue Ziel-Namespaces. Die angegebenen Ziel-Namespaces dürfen nicht bereits im Ziel-Cluster vorhanden sein.

   - Wählen Sie **Weiter**.
   - Wählen Sie aus, ob die der App zugeordnete ursprüngliche Storage-Klasse beibehalten oder eine andere Storage-Klasse ausgewählt werden soll.

     Sie können die Storage-Klasse einer App zu einer Storage-Klasse eines nativen Cloud-Providers oder einer anderen unterstützten Storage-Klasse migrieren und eine App von einer Storage-Klasse migrieren, die von unterstützt wird `ontap-nas-economy` Zu einer Storage-Klasse, die von unterstützt wird `ontap-nas` Oder kopieren Sie die App in ein anderes Cluster mit einer Storage-Klasse, die von der unterstützt wird `ontap-nas-economy` Treiber.

   Wenn Sie eine andere Storage-Klasse auswählen und diese Storage-Klasse zum Zeitpunkt der Wiederherstellung nicht vorhanden ist, wird ein Fehler zurückgegeben.

5. Wählen Sie **Weiter**.
6. Überprüfen Sie die Informationen über den Klon und wählen Sie **Clone**.

Ergebnis

Astra Control klont die App basierend auf den von Ihnen angegebenen Informationen. Der Klonvorgang ist erfolgreich, wenn der neue Applikationsklon ausgeführt wird `Healthy` Geben Sie auf der Seite **Anwendungen** an.

Nachdem durch einen Klon- oder Wiederherstellungsvorgang ein neuer Namespace erstellt wurde, kann der Kontoadministrator/Kontoinhaber das Mitgliedskonto bearbeiten und Rolleneinschränkungen aktualisieren, damit der betroffene Benutzer Zugriff auf den neuen Namespace gewährt.

Nach einer Datensicherungsoperation (Klonen, Backup oder Wiederherstellung) und einer anschließenden Größenanpassung des persistenten Volumes beträgt die Verzögerung bis zu zwanzig Minuten, bevor die neue Volume-Größe in der UI angezeigt wird. Der Datensicherungsvorgang ist innerhalb von Minuten erfolgreich und Sie können mit der Management Software für das Storage-Backend die Änderung der Volume-Größe bestätigen.

Anwendungsausführungshaken verwalten

Ein Execution Hook ist eine benutzerdefinierte Aktion, die Sie so konfigurieren können, dass sie zusammen mit einem Datenschutzvorgang einer verwalteten App ausgeführt wird. Wenn Sie beispielsweise über eine Datenbank-App verfügen, können Sie mit einem Execution-Hook alle Datenbanktransaktionen vor einem Snapshot anhalten und die Transaktionen nach Abschluss des Snapshots wieder aufnehmen. Dies gewährleistet applikationskonsistente Snapshots.

Arten von Ausführungshaken

Astra Control Center unterstützt die folgenden Typen von Ausführungshaken, je nachdem, wann sie ausgeführt werden können:

- Vor dem Snapshot
- Nach dem Snapshot
- Vor dem Backup
- Nach dem Backup
- Nach dem Wiederherstellen
- Nach Failover

Filter für Testausführungshaken

Wenn Sie einer Anwendung einen Ausführungshaken hinzufügen oder bearbeiten, können Sie einem Ausführungshaken Filter hinzufügen, um zu verwalten, mit welchen Containern der Hook übereinstimmt. Filter sind für Applikationen nützlich, die in allen Containern dasselbe Container-Image nutzen. Jedes Image kann jedoch für einen anderen Zweck (wie Elasticsearch) verwendet werden. Mit Filtern können Sie Szenarien erstellen, in denen Ausführungshaken auf einigen, aber nicht unbedingt allen identischen Containern ausgeführt werden. Wenn Sie mehrere Filter für einen einzelnen Testausführungshaken erstellen, werden diese mit einem logischen UND einem Operator kombiniert. Pro Testsuite können Sie bis zu 10 aktive Filter haben.

Jeder Filter, den Sie einem Execution Hook hinzufügen, verwendet einen regulären Ausdruck, um Container in Ihrem Cluster zu entsprechen. Wenn ein Haken einem Container entspricht, führt der Haken sein zugehöriges Skript auf diesem Container aus. Reguläre Ausdrücke für Filter verwenden die Syntax des regulären Ausdrucks 2 (RE2), die das Erstellen eines Filters nicht unterstützt, der Container aus der Liste der Übereinstimmungen ausschließt. Informationen zur Syntax, die Astra Control für regelmäßige Ausdrücke in Hook-Filter unterstützt, finden Sie unter "Syntaxunterstützung für regulären Ausdruck 2 (RE2)".

> Wenn Sie einem Ausführungs-Hook einen Namespace-Filter hinzufügen, der nach einer Wiederherstellung oder einem Klonvorgang ausgeführt wird, und die Wiederherstellungs- oder Klonquelle und das Ziel in verschiedenen Namespaces liegen, wird der Namespace-Filter nur auf den Ziel-Namespace angewendet.

Wichtige Hinweise zu benutzerdefinierten Testausführungshaken

Bei der Planung von Testausführungshooks für Ihre Apps sollten Sie Folgendes berücksichtigen:

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.
Wenn Sie eine Backup- oder Snapshot-Operation mit zugeordneten Testsuiten starten, diese aber dann abbrechen, können die Haken trotzdem ausgeführt werden, wenn der Backup- oder Snapshot-Vorgang bereits gestartet wurde. Das bedeutet, dass die in einem Testsuite nach dem Backup verwendete Logik nicht davon ausgehen kann, dass das Backup abgeschlossen wurde.

- Die Ausführungshaken-Funktion ist bei neuen Astra Control-Bereitstellungen standardmäßig deaktiviert.
  - Sie müssen die Funktion „Ausführungshaken“ aktivieren, bevor Sie Ausführungshaken verwenden können.
  - Benutzer von Eigentümer oder Administrator können die Funktion „Ausführungshaken“ für alle Benutzer aktivieren oder deaktivieren, die im aktuellen Astra Control-Konto definiert sind. Siehe Aktivieren Sie die Funktion „Ausführungshaken“ Und Deaktivieren Sie die Funktion Ausführungshaken Weitere Anweisungen.
  - Der Status der Funktionsunterstützung bleibt bei Astra Control Upgrades erhalten.
- Ein Testsuite muss ein Skript verwenden, um Aktionen durchzuführen. Viele Testsuitehaoks können auf dasselbe Skript verweisen.
- Astra Control erfordert, dass die Skripte, mit denen Ausführungshaken ausgeführt werden, im Format ausführbarer Shell-Skripte geschrieben werden.
- Die Skriptgröße ist auf 96 KB begrenzt.
- Astra Control verwendet Hook-Einstellungen für die Ausführung und alle übereinstimmenden Kriterien, um festzustellen, welche Haken für einen Snapshot-, Backup- oder Wiederherstellungsvorgang gelten.
- Alle Fehler bei den Testausführungshaken sind weiche Ausfälle, andere Haken und der Datenschutzvorgang werden immer noch versucht, auch wenn ein Haken ausfällt. Wenn ein Haken jedoch ausfällt, wird ein Warnereignis im Ereignisprotokoll der Seite * aufgezeichnet.
- Um Testsuiten zu erstellen, zu bearbeiten oder zu löschen, müssen Sie Benutzer mit den Berechtigungen Eigentümer, Administrator oder Mitglied sein.
- 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 wird als fehlgeschlagen markiert, und ein resultierender Eintrag im Ereignisprotokoll weist auf das Timeout hin.
- Für Ad-hoc-Datenschutzvorgänge werden alle Hook-Ereignisse generiert und im Ereignisprotokoll der Seite **Aktivität** gespeichert. Bei geplanten Datenschutzvorgängen werden jedoch nur Hook-Failure-Ereignisse im Ereignisprotokoll aufgezeichnet (Ereignisse, die von den geplanten Datenschutzvorgängen selbst generiert werden, werden noch aufgezeichnet).
- Wenn Astra Control Center einen Failover über eine replizierte Quell-App an die Ziel-App ausführt, werden nach dem Failover alle für die Quell-App aktivierten Ausführungs-Hooks für die Ziel-App ausgeführt.

Wenn Sie nach der Wiederherstellung Hooks mit Astra Control Center 23.04 ausgeführt und Ihr Astra Control Center auf 23.07 oder höher aktualisiert haben, werden die Hooks für die Ausführung nach der Wiederherstellung nach einer Failover-Replizierung nicht mehr ausgeführt. Sie müssen neue Ausführungshaken nach dem Failover für Ihre Apps erstellen. Alternativ können Sie den Operationstyp vorhandener Hooks nach der Wiederherstellung ändern, die für Failover von „nach der Wiederherstellung“ zu „nach dem Failover“ gedacht sind.

Ausführungsreihenfolge

Wenn ein Datenschutzvorgang ausgeführt wird, finden Hakenereignisse in der folgenden Reihenfolge statt:

1. Alle entsprechenden benutzerdefinierten Testhaken für die Ausführung vor dem Betrieb werden auf den entsprechenden Containern ausgeführt. Sie können beliebig viele benutzerdefinierte Hooks für die Vorbedienung erstellen und ausführen, aber die Reihenfolge der Ausführung dieser Haken vor der Operation ist weder garantiert noch konfigurierbar.
2. Der Vorgang der Datensicherung wird durchgeführt.
3. Alle entsprechenden benutzerdefinierten Testhaken für die Ausführung nach der Operation werden auf den entsprechenden Containern ausgeführt. Sie können beliebig viele benutzerdefinierte Haken für die Nachbearbeitung erstellen und ausführen, aber die Reihenfolge der Ausführung dieser Haken nach der Operation ist weder garantiert noch konfigurierbar.

Wenn Sie mehrere Testausführungshaken desselben Typs erstellen (z. B. Pre-Snapshot), ist die Reihenfolge der Ausführung dieser Haken nicht garantiert. Die Reihenfolge der Ausführung von Haken unterschiedlicher Art ist jedoch garantiert. Die Reihenfolge der Ausführung einer Konfiguration mit allen verschiedenen Hooks sieht beispielsweise folgendermaßen aus:

1. Hooks vor dem Backup wurden ausgeführt
2. Hooks vor dem Snapshot wurden ausgeführt
3. Hooks nach dem Snapshot wurden ausgeführt
4. Hooks nach dem Backup ausgeführt
5. Haken nach der Wiederherstellung ausgeführt

Ein Beispiel für diese Konfiguration finden Sie in Szenario 2 aus der Tabelle in ob ein Haken läuft.

> Sie sollten Ihre Hook-Skripte immer testen, bevor Sie sie in einer Produktionsumgebung aktivieren. Mit dem Befehl 'kubectl exec' können Sie die Skripte bequem testen. Nachdem Sie die Testausführungshaken in einer Produktionsumgebung aktiviert haben, testen Sie die erstellten Snapshots und Backups, um sicherzustellen, dass sie konsistent sind. Dazu klonen Sie die Applikation in einem temporären Namespace, stellen den Snapshot oder das Backup wieder her und testen anschließend die App.

Bestimmen Sie, ob ein Haken läuft

Verwenden Sie die folgende Tabelle, um zu ermitteln, ob ein benutzerdefinierter Testsuite für Ihre Anwendung ausgeführt wird.

Alle grundlegenden Applikationsvorgänge müssen eine der grundlegenden Vorgänge – Snapshot, Backup oder Wiederherstellung – ausgeführt werden. Je nach Szenario kann ein Klonvorgang aus verschiedenen Kombinationen dieser Operationen bestehen, sodass die Ausführungsooks für einen Klonvorgang variieren.

Für Wiederherstellungen ohne Backup ist ein vorhandener Snapshot oder Backup erforderlich, sodass bei diesen Vorgängen keine Snapshot- oder Backup-Hooks ausgeführt werden.

Wenn Sie starten, aber dann brechen Sie ein Backup, das einen Snapshot enthält und es sind zugewiesene Testausführungshaken, einige Haken laufen, und andere möglicherweise nicht. Das bedeutet, dass ein Testinaper nach dem Backup nicht davon ausgehen kann, dass die Sicherung abgeschlossen wurde. Beachten Sie die folgenden Punkte für abgebrochene Backups mit zugehörigen Testsuiten:

- Die Hooks vor dem Backup und nach dem Backup laufen immer.
- Wenn das Backup einen neuen Snapshot enthält und der Snapshot gestartet wurde, werden die Hooks vor dem Snapshot und nach dem Snapshot ausgeführt.
- Wenn die Sicherung vor dem Start des Snapshots abgebrochen wird, werden die Hooks vor dem Snapshot und nach dem Snapshot nicht ausgeführt.

Szenario	Betrieb	Vorhandener Snapshot	Vorhandenes Backup	Namespace	Cluster	Snapshot Hooks laufen	Backup Hooks laufen	Hooks Run wiederherstellen	Failover Hooks werden ausgeführt
1	Klon	N	N	Neu	Gleich	Y	N	Y	N
2	Klon	N	N	Neu	Anders	Y	Y	Y	N
3	Klonen oder Wiederherstellen	Y	N	Neu	Gleich	N	N	Y	N
4	Klonen oder Wiederherstellen	N	Y	Neu	Gleich	N	N	Y	N
5	Klonen oder Wiederherstellen	Y	N	Neu	Anders	N	N	Y	N
6	Klonen oder Wiederherstellen	N	Y	Neu	Anders	N	N	Y	N
7	Wiederherstellen	Y	N	Vorhanden	Gleich	N	N	Y	N
8	Wiederherstellen	N	Y	Vorhanden	Gleich	N	N	Y	N
9	Snapshot	K. A.	K. A.	K. A.	K. A.	Y	K. A.	K. A.	N
10	Backup	N	K. A.	K. A.	K. A.	Y	Y	K. A.	N
11	Backup	Y	K. A.	K. A.	K. A.	N	N	K. A.	N
12	Failover	Y	K. A.	Durch Replikation erstellt	Anders	N	N	N	Y

Szenario	Betrieb	Vorhandener Snapshot	Vorhandenes Backup	Namespace	Cluster	Snapshot Hooks laufen	Backup Hooks laufen	Hooks Run wiederherstellen	Failover Hooks werden ausgeführt
13	Failover	Y	K. A.	Durch Replikation erstellt	Gleich	N	N	N	Y

Beispiele für Testausführungshaken

Besuchen Sie das "NetApp Verda GitHub Projekt" Zum Herunterladen von Real-Execution-Hooks für beliebte Apps wie Apache Cassandra und Elasticsearch. Sie können auch Beispiele sehen und Ideen für die Strukturierung Ihrer eigenen benutzerdefinierten Execution Hooks erhalten.

Aktivieren Sie die Funktion „Ausführungshaken“

Wenn Sie Eigentümer oder Admin-Benutzer sind, können Sie die Funktion Ausführungshaken aktivieren. Wenn Sie die Funktion aktivieren, können alle in diesem Astra Control-Konto definierten Benutzer Ausführungshaken verwenden und vorhandene Ausführungshaken und Hook-Skripte anzeigen.

Schritte

1. Gehen Sie zu **Anwendungen** und wählen Sie dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie **Ausführungshaken aktivieren**.

   Die Registerkarte **Account** > **feature settings** wird angezeigt.
4. Wählen Sie im Bereich **Ausführungshaken** das Einstellungsmenü aus.
5. Wählen Sie **Enable**.
6. Beachten Sie die Sicherheitswarnung, die angezeigt wird.
7. Wählen Sie **Ja, Ausführungshaken aktivieren**.

Deaktivieren Sie die Funktion Ausführungshaken

Wenn Sie ein Benutzer von Eigentümer oder Administrator sind, können Sie die Funktion „Ausführungshaken“ für alle Benutzer deaktivieren, die in diesem Astra Control-Konto definiert sind. Sie müssen alle vorhandenen Ausführungshaken löschen, bevor Sie die Funktion „Ausführungshaken“ deaktivieren können. Siehe Löschen Sie einen Testsuite-Haken Für Anweisungen zum Löschen einer vorhandenen Ausführungsöse.

Schritte

1. Gehen Sie zu **Account** und wählen Sie dann die Registerkarte **Feature settings**.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie im Bereich **Ausführungshaken** das Einstellungsmenü aus.
4. Wählen Sie **Deaktivieren**.
5. Beachten Sie die Warnmeldung, die angezeigt wird.
6. Typ `disable` Um zu bestätigen, dass Sie die Funktion für alle Benutzer deaktivieren möchten.

7. Wählen Sie **Ja, deaktivieren**.

Vorhandene Testsuiten anzeigen

Sie können vorhandene benutzerdefinierte Testsuiten für eine App anzeigen.

Schritte

1. Gehen Sie zu **Anwendungen** und wählen Sie dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.

   In der Ergebnisliste können Sie alle aktivierten oder deaktivierten Testausführungshaken anzeigen. Sie sehen den Status eines Hakens, die Anzahl der passenden Container, die Erstellungszeit und den Ablauf (vor- oder Nachbetrieb). Sie können die auswählen + Symbol neben dem Hook-Namen, um die Liste der Container, auf denen es ausgeführt wird, zu erweitern. Um die Ereignisprotokolle zu den Testausführungshaken für diese Anwendung anzuzeigen, gehen Sie zur Registerkarte **Aktivität**.

Vorhandene Skripte anzeigen

Sie können die bereits hochgeladenen Skripte anzeigen. Auf dieser Seite können Sie auch sehen, welche Skripte verwendet werden und welche Haken sie verwenden.

Schritte

1. Gehen Sie zu **Konto**.
2. Wählen Sie die Registerkarte **Skripts** aus.

   Auf dieser Seite sehen Sie eine Liste mit bereits hochgeladenen Skripten. Die Spalte **used by** zeigt an, welche Testsuitehaoks die einzelnen Skripte verwenden.

Fügen Sie ein Skript hinzu

Jeder Execution Hook muss ein Skript verwenden, um Aktionen durchzuführen. Sie können einen oder mehrere Skripte hinzufügen, auf die Testausführungshaken verweisen können. Viele Ausführungshaken können auf dasselbe Skript verweisen. Dadurch können Sie viele Ausführungshaken aktualisieren, indem Sie nur ein Skript ändern.

Schritte

1. Stellen Sie sicher, dass die Funktion Ausführungshaken aktiviert ist Aktiviert.
2. Gehen Sie zu **Konto**.
3. Wählen Sie die Registerkarte **Skripts** aus.
4. Wählen Sie **Hinzufügen**.
5. Führen Sie einen der folgenden Schritte aus:
   - Laden Sie ein benutzerdefiniertes Skript hoch.
     i. Wählen Sie die Option **Datei hochladen**.
     ii. Navigieren Sie zu einer Datei, und laden Sie sie hoch.
     iii. Geben Sie dem Skript einen eindeutigen Namen.
     iv. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.
     v. Wählen Sie **Skript speichern**.

- Fügen Sie in ein benutzerdefiniertes Skript aus der Zwischenablage ein.
  i. Wählen Sie die Option **Einfügen oder Typ** aus.
  ii. Wählen Sie das Textfeld aus, und fügen Sie den Skripttext in das Feld ein.
  iii. Geben Sie dem Skript einen eindeutigen Namen.
  iv. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.

6. Wählen Sie **Skript speichern**.

Ergebnis

Das neue Skript erscheint in der Liste auf der Registerkarte **Scripts**.

Ein Skript löschen

Sie können ein Skript aus dem System entfernen, wenn es nicht mehr benötigt wird und nicht von Testsuiten verwendet wird.

Schritte

1. Gehen Sie zu **Konto**.
2. Wählen Sie die Registerkarte **Skripts** aus.
3. Wählen Sie ein Skript aus, das Sie entfernen möchten, und wählen Sie das Menü in der Spalte **Aktionen** aus.
4. Wählen Sie **Löschen**.

> Wenn das Skript mit einem oder mehreren Testsuiten verknüpft ist, ist die Aktion **Löschen** nicht verfügbar. Um das Skript zu löschen, bearbeiten Sie zunächst die zugehörigen Testausführungshaken und ordnen Sie sie einem anderen Skript zu.

Erstellen Sie einen benutzerdefinierten Testsuite-Haken

Sie können einen benutzerdefinierten Ausführungshaken für eine App erstellen und ihn zu Astra Control hinzufügen. Siehe Beispiele für Testausführungshaken Beispiele für Haken. Sie müssen über die Berechtigungen Eigentümer, Administrator oder Mitglied verfügen, um Testausführungshaken zu erstellen.

> Wenn Sie ein benutzerdefiniertes Shell-Skript erstellen, das als Execution Hook verwendet werden soll, denken Sie daran, die entsprechende Shell am Anfang der Datei anzugeben, es sei denn, Sie führen bestimmte Befehle aus oder geben den vollständigen Pfad zu einer ausführbaren Datei an.

Schritte

1. Stellen Sie sicher, dass die Funktion Ausführungshaken aktiviert ist Aktiviert.
2. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
3. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
4. Wählen Sie **Hinzufügen**.
5. Im Bereich **Klettdetails**:
   a. Bestimmen Sie, wann der Haken ausgeführt werden soll, indem Sie im Dropdown-Menü * Operation* einen Operationstyp auswählen.
   b. Geben Sie einen eindeutigen Namen für den Haken ein.

c. (Optional) Geben Sie alle Argumente ein, um während der Ausführung an den Haken weiterzuleiten. Drücken Sie nach jedem eingegebenen Argument die Eingabetaste, um jedes Argument aufzuzeichnen.

6. (Optional) im Bereich **Hook Filter Details** können Sie Filter hinzufügen, um zu steuern, auf welchen Behältern der Execution Hook läuft:
   a. Wählen Sie **Filter hinzufügen**.
   b. Wählen Sie in der Spalte **Hook Filtertyp** ein Attribut aus, nach dem Sie im Dropdown-Menü filtern möchten.
   c. Geben Sie in der Spalte **Regex** einen regulären Ausdruck ein, der als Filter verwendet werden soll. Astra Control verwendet den "Regex-Syntax für regulären Ausdruck 2 (RE2)".

      Wenn Sie nach dem genauen Namen eines Attributs (z. B. einem Pod-Namen) filtern, ohne dass im Feld Regulärer Ausdruck ein anderer Text enthalten ist, wird eine Substring-Übereinstimmung durchgeführt. Verwenden Sie zum Abgleich eines genauen Namens und nur des Namens die exakte Syntax für die Übereinstimmung der Zeichenfolge (z. B. `^exact_podname$`).

   d. Um weitere Filter hinzuzufügen, wählen Sie **Filter hinzufügen**.

      Mehrere Filter für einen Execution Hook werden mit einem logischen UND einem Operator kombiniert. Pro Testsuite können Sie bis zu 10 aktive Filter haben.

7. Wählen Sie anschließend **Weiter** aus.
8. Führen Sie im Bereich **Script** einen der folgenden Schritte aus:
   - Fügen Sie ein neues Skript hinzu.
     i. Wählen Sie **Hinzufügen**.
     ii. Führen Sie einen der folgenden Schritte aus:
       - Laden Sie ein benutzerdefiniertes Skript hoch.
         I. Wählen Sie die Option **Datei hochladen**.
         II. Navigieren Sie zu einer Datei, und laden Sie sie hoch.
         III. Geben Sie dem Skript einen eindeutigen Namen.
         IV. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.
         V. Wählen Sie **Skript speichern**.
       - Fügen Sie in ein benutzerdefiniertes Skript aus der Zwischenablage ein.
         I. Wählen Sie die Option **Einfügen oder Typ** aus.
         II. Wählen Sie das Textfeld aus, und fügen Sie den Skripttext in das Feld ein.
         III. Geben Sie dem Skript einen eindeutigen Namen.
         IV. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.
   - Wählen Sie ein vorhandenes Skript aus der Liste aus.

     Hiermit wird der Testsuitelink angewiesen, dieses Skript zu verwenden.

9. Wählen Sie **Weiter**.
10. Überprüfen Sie die Konfiguration der Testsuite.
11. Wählen Sie **Hinzufügen**.

Überprüfen Sie den Status eines Testablaufanhängees

Nachdem ein Snapshot-, Backup- oder Wiederherstellungsvorgang abgeschlossen wurde, können Sie den Status der Testsuiten überprüfen, die im Rahmen des Vorgangs ausgeführt wurden. Mit diesen Statusinformationen können Sie festlegen, ob der Testsuite beibehalten, geändert oder gelöscht werden soll.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Datenschutz** aus.
3. Wählen Sie **Snapshots** aus, um die laufenden Snapshots zu sehen, oder **Backups**, um die laufenden Backups zu sehen.

   Der **Hook-Status** zeigt den Status der Ausführung Hakenlauf nach Abschluss des Vorgangs an. Sie können den Mauszeiger auf den Status bewegen, um weitere Details zu erhalten. Wenn z. B. beim Snapshot Fehler beim Ausführen von Hakenabfällen auftreten, wird beim Mauszeiger über den Hakenzustand für diesen Snapshot eine Liste mit fehlgeschlagenen Testsuitelhaken angezeigt. Um die Gründe für jeden Fehler zu sehen, können Sie die Seite **Aktivität** im linken Navigationsbereich überprüfen.

Skriptverwendung anzeigen

In der Web-Benutzeroberfläche von Astra Control können Sie sehen, welche Testausführungshaken ein bestimmtes Skript verwenden.

Schritte

1. Wählen Sie **Konto**.
2. Wählen Sie die Registerkarte **Skripts** aus.

   Die Spalte **used by** in der Liste der Skripte enthält Details darüber, welche Haken die einzelnen Skripte in der Liste verwenden.

3. Wählen Sie die Informationen in der Spalte **used by** für ein Skript aus, das Sie interessieren.

   Eine detailliertere Liste mit den Namen der Haken, die das Skript verwenden, und der Art der Operation, mit der sie konfiguriert sind.

Bearbeiten Sie einen Testsuite-Haken

Sie können einen Testsuite-Haken bearbeiten, wenn Sie die Attribute, Filter oder das verwendete Skript ändern möchten. Sie müssen über die Berechtigungen Eigentümer, Administrator oder Mitglied verfügen, um Testausführungshaken bearbeiten zu können.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie in der Spalte **Aktionen** das Menü Optionen für einen Haken, den Sie bearbeiten möchten.

4. Wählen Sie **Bearbeiten**.
5. Nehmen Sie alle erforderlichen Änderungen vor, und wählen Sie nach Abschluss jedes Abschnitts **Weiter** aus.
6. Wählen Sie **Speichern**.

Deaktivieren Sie einen Testsuite-Haken

Sie können einen Testsuite-Hook deaktivieren, wenn Sie ihn vorübergehend vor oder nach einem Snapshot einer App nicht ausführen möchten. Sie müssen über die Berechtigung Eigentümer, Administrator oder Mitglied verfügen, um Testsuiten zu deaktivieren.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie in der Spalte **Aktionen** das Menü Optionen für einen Haken, den Sie deaktivieren möchten.
4. Wählen Sie **Deaktivieren**.

Löschen Sie einen Testsuite-Haken

Sie können einen Execution Hook ganz entfernen, wenn Sie ihn nicht mehr benötigen. Sie müssen über die Berechtigung Eigentümer, Administrator oder Mitglied verfügen, um Testausführungshaken zu löschen.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie in der Spalte **Aktionen** das Menü Optionen für einen Haken, den Sie löschen möchten.
4. Wählen Sie **Löschen**.
5. Geben Sie im Dialogfeld „Ergebnis“ zur Bestätigung „Löschen“ ein.
6. Wählen Sie **Ja, Testsuite löschen**.

Finden Sie weitere Informationen

- "NetApp Verda GitHub Projekt"

Astra Control Center kann über Astra Control Center geschützt werden

Schützen Sie die Astra Control Center-Anwendung selbst, um die Ausfallsicherheit im Kubernetes-Cluster, auf dem Astra Control Center ausgeführt wird, besser vor schwerwiegenden Fehlern zu schützen. Sie können für ein Backup und Restore von Astra Control Center eine sekundäre Astra Control Center-Instanz verwenden oder die Astra-Replizierung verwenden, wenn der zugrunde liegende Storage ONTAP verwendet.

In diesen Szenarien wird eine zweite Instanz von Astra Control Center in einer anderen Fehlerdomäne bereitgestellt und konfiguriert und auf einem anderen zweiten Kubernetes-Cluster ausgeführt als die primäre Astra Control Center-Instanz. Die zweite Astra Control Instanz wird verwendet, um Backups und potenziell die primäre Astra Control Center Instanz wiederherzustellen. Eine wiederhergestellte oder replizierte Astra Control Center Instanz stellt weiterhin das Management von Applikationsdaten für die Applikations-Cluster-Applikationen bereit und stellt den Zugriff auf Backups und Snapshots dieser Applikationen wieder her.

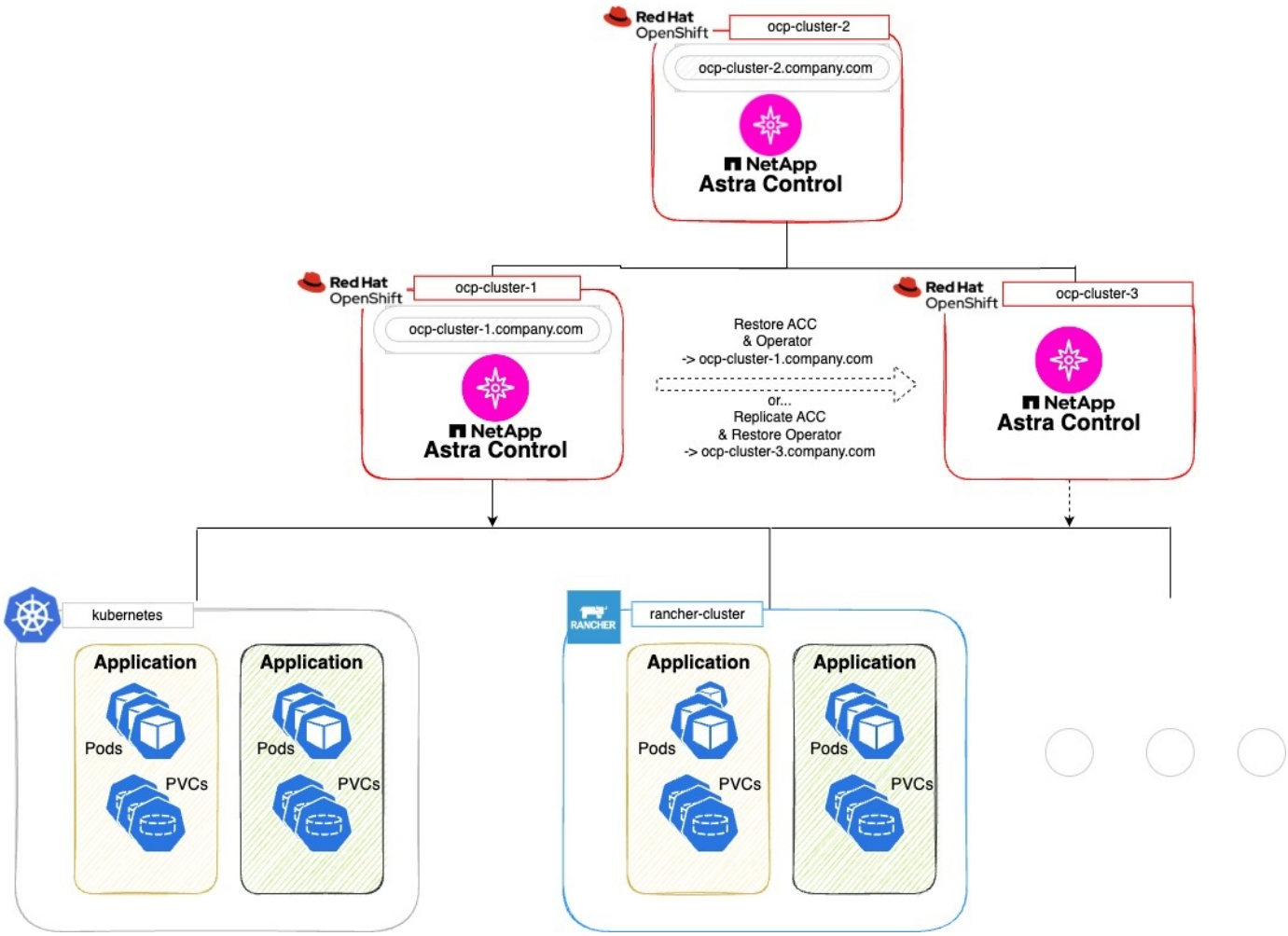
Bevor Sie beginnen

Stellen Sie sicher, dass Sie die folgenden Informationen haben, bevor Sie Schutzszenarien für Astra Control Center einrichten:

- **Ein Kubernetes-Cluster, auf dem die primäre Astra Control Center-Instanz ausgeführt wird**: Dieser Cluster hostet die primäre Astra Control Center-Instanz, die Anwendungscluster verwaltet.
- **Ein zweiter Kubernetes-Cluster desselben Kubernetes-Verteilungstyps wie der primäre, auf dem die sekundäre Astra Control Center-Instanz ausgeführt wird**: Dieser Cluster hostet die Astra Control Center-Instanz, die die primäre Astra Control Center-Instanz verwaltet.
- **Ein dritter Kubernetes-Cluster desselben Kubernetes-Verteilungstyps wie der primäre**: In diesem Cluster wird die wiederhergestellte oder replizierte Instanz von Astra Control Center gehostet. Er muss denselben Astra Control Center Namespace zur Verfügung haben, der derzeit auf dem primären System bereitgestellt wird. Wenn beispielsweise Astra Control Center im Namespace bereitgestellt wird `netapp-acc` Auf dem Quellcluster, dem Namespace `netapp-acc` Der Service muss verfügbar und nicht von Applikationen auf dem Kubernetes-Ziel-Cluster verwendet werden.
- **S3-kompatible Buckets**: Jede Astra Control Center Instanz verfügt über einen zugänglichen S3-kompatiblen Objektspeicher-Bucket.
- **Ein konfigurierter Load Balancer**: Der Load Balancer stellt eine IP-Adresse für Astra bereit und muss über eine Netzwerkverbindung zu den Anwendungsclustern und beiden S3 Buckets verfügen.
- **Cluster erfüllen die Anforderungen für Astra Control Center**: Jeder Cluster, der in Astra Control Center verwendet wird, erfüllt "Allgemeine Anforderungen für Astra Control Center".

Über diese Aufgabe

In diesen Verfahren werden die erforderlichen Schritte beschrieben, um Astra Control Center mithilfe eines der beiden Cluster auf einem neuen Cluster wiederherzustellen Backup und Restore Oder Replizierung. Die Schritte basieren auf der hier dargestellten Beispielkonfiguration:



In dieser Beispielkonfiguration wird Folgendes angezeigt:

- **Ein Kubernetes-Cluster, auf dem die primäre Astra Control Center-Instanz ausgeführt wird**:
  - OpenShift-Cluster: `ocp-cluster-1`
  - Primäre Astra Control Center-Instanz: `ocp-cluster-1.company.com`
  - Dieser Cluster verwaltet die Anwendungscluster.
- **Der zweite Kubernetes-Cluster desselben Kubernetes-Distributionstyps wie der primäre, auf dem die sekundäre Astra Control Center-Instanz ausgeführt wird**:
  - OpenShift-Cluster: `ocp-cluster-2`
  - Sekundäre Astra Control Center-Instanz: `ocp-cluster-2.company.com`
  - Dieser Cluster wird verwendet, um die primäre Astra Control Center-Instanz zu sichern oder die Replikation in einem anderen Cluster zu konfigurieren (in diesem Beispiel der `ocp-cluster-3` Cluster).
- **Ein dritter Kubernetes-Cluster mit demselben Kubernetes-Verteilungstyp wie der primäre, der für Wiederherstellungsvorgänge verwendet wird**:
  - OpenShift-Cluster: `ocp-cluster-3`
  - Astra Control Center dritte Instanz: `ocp-cluster-3.company.com`
  - Dieser Cluster wird für die Wiederherstellung oder das Replizierungs-Failover von Astra Control Center

verwendet.

> Idealerweise sollte sich der Applikations-Cluster außerhalb der drei Astra Control Center Cluster befinden, wie in der Abbildung oben in kubernetes und Rancher Clustern dargestellt.

Nicht im Diagramm dargestellt:

- Auf allen Clustern sind ONTAP-Back-Ends mit installiertem Trident installiert.
- In dieser Konfiguration verwenden die OpenShift-Cluster MetalLB als Load Balancer.
- Der Snapshot-Controller und die VolumeSnapshotClass sind auch auf allen Clustern installiert, wie in beschrieben "Voraussetzungen".

Schritt 1 Option: Backup und Wiederherstellung von Astra Control Center

In diesem Verfahren werden die erforderlichen Schritte beschrieben, um Astra Control Center mithilfe von Backup und Restore auf einem neuen Cluster wiederherzustellen.

In diesem Beispiel wird Astra Control Center immer unter installiert `netapp-acc` Namespace und der Operator wird unter installiert `netapp-acc-operator` Namespace.

> Obwohl nicht beschrieben, kann der Astra Control Center-Operator auch im selben Namespace wie der Astra CR eingesetzt werden.

Bevor Sie beginnen

- Sie haben das primäre Astra Control Center auf einem Cluster installiert.
- Sie haben das sekundäre Astra Control Center auf einem anderen Cluster installiert.

Schritte

1. Management der primären Astra Control Center-Applikation und des Ziel-Clusters über die sekundäre Astra Control Center-Instanz (auf der ausgeführt wird `ocp-cluster-2` Cluster):
   a. Melden Sie sich bei der sekundären Astra Control Center-Instanz an.
   b. "Fügen Sie das primäre Astra Control Center-Cluster hinzu" (`ocp-cluster-1`).
   c. "Fügen Sie das dritte Zielcluster hinzu" (`ocp-cluster-3`), die für die Wiederherstellung verwendet werden.
2. Astra Control Center und den Astra Control Center Betreiber im sekundären Astra Control Center managen:
   a. Wählen Sie auf der Seite Anwendungen die Option **Definieren**.
   b. Geben Sie im Fenster **Anwendung definieren** den neuen Anwendungsnamen ein (`netapp-acc`).
   c. Wählen Sie den Cluster aus, auf dem das primäre Astra Control Center ausgeführt wird (`ocp-cluster-1`) Aus der Dropdown-Liste **Cluster**.
   d. Wählen Sie die aus `netapp-acc` Namespace für Astra Control Center aus der Dropdown-Liste **Namespace**.
   e. Aktivieren Sie auf der Seite „Cluster-Ressourcen“ die Option **zusätzliche Cluster-Ressourcen einschließen**.
   f. Wählen Sie **Add include Rule**.

g. Wählen Sie diese Einträge aus, und wählen Sie **Hinzufügen**:
   - Etikettenauswahl: <label name>
   - Gruppe: Apiextensions.k8s.io
   - Stand: v1
   - Art: CustomResourceDefinition

h. Bestätigen Sie die Anwendungsinformationen.

i. Wählen Sie **Definieren**.

   Nachdem Sie **define** ausgewählt haben, wiederholen Sie den Prozess Anwendung definieren für den Operator `netapp-acc-operator`) Und wählen Sie die aus `netapp-acc-operator` Namespace im Assistenten „Anwendung definieren“.

3. Astra Control Center und den Bediener sichern:
   a. Navigieren Sie im sekundären Astra Control Center zur Seite Anwendungen, indem Sie die Registerkarte Anwendungen auswählen.
   b. "Backup" Astra Control Center (`netapp-acc`).
   c. "Backup" Der Bediener (`netapp-acc-operator`).
4. Nachdem Sie Astra Control Center und den Operator gesichert haben, simulieren Sie durch ein Disaster Recovery-Szenario (DR) "Astra Control Center wird deinstalliert" Vom primären Cluster aus.

   Sie stellen Astra Control Center in einem neuen Cluster (dem dritten in diesem Verfahren beschriebenen Kubernetes-Cluster) wieder her und verwenden denselben DNS wie das primäre Cluster für das neu installierte Astra Control Center.

5. Mit dem sekundären Astra Control Center "Wiederherstellen" Die primäre Instanz der Astra Control Center-Anwendung aus ihrem Backup:
   a. Wählen Sie **Applications** aus und wählen Sie dann den Namen der Astra Control Center-Anwendung aus.
   b. Wählen Sie im Menü Optionen in der Spalte Aktionen die Option **Wiederherstellen** aus.
   c. Wählen Sie als Wiederherstellungstyp die Option **in neue Namespaces wiederherstellen**.
   d. Geben Sie den Wiederherstellungsnamen ein (`netapp-acc`).
   e. Wählen Sie das dritte Zielcluster aus (`ocp-cluster-3`).
   f. Aktualisieren Sie den Ziel-Namespace so, dass es sich um den gleichen Namespace wie das Original handelt.
   g. Wählen Sie auf der Seite Quelle wiederherstellen das Anwendungsbackup aus, das als Wiederherstellungsquelle verwendet werden soll.
   h. Wählen Sie **Restore using original Storage classes**.
   i. Wählen Sie **Alle Ressourcen wiederherstellen**.
   j. Überprüfen Sie die Restore-Informationen und wählen Sie dann **Restore** aus, um den Wiederherstellungsprozess zu starten, der Astra Control Center auf dem Ziel-Cluster wiederherstellt (`ocp-cluster-3`). Die Wiederherstellung ist abgeschlossen, wenn die Anwendung eingibt `available` Bundesland.
6. Astra Control Center auf dem Ziel-Cluster konfigurieren:

a. Öffnen Sie ein Terminal, und stellen Sie mithilfe von kubeconfig eine Verbindung zum Ziel-Cluster her (`ocp-cluster-3`), das das wiederhergestellte Astra Control Center enthält.

b. Bestätigen Sie das `ADDRESS` Spalte in der Astra Control Center-Konfiguration verweist auf den DNS-Namen des primären Systems:

```
kubectl get acc -n netapp-acc
```

Antwort:

```
NAME  UUID                                   VERSION    ADDRESS
READY
astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.10.0-68 ocp-cluster-
1.company.com           True
```

a. Wenn der `ADDRESS` Feld in der obigen Antwort weist nicht den FQDN der primären Astra Control Center-Instanz auf. Aktualisieren Sie die Konfiguration, um auf den Astra Control Center-DNS zu verweisen:

```
kubectl edit acc -n netapp-acc
```

i. Ändern Sie das `astraAddress` Unter `spec:` Zum FQDN (`ocp-cluster-1.company.com` In diesem Beispiel) der primären Astra Control Center-Instanz.

ii. Speichern Sie die Konfiguration.

iii. Bestätigen Sie, dass die Adresse aktualisiert wurde:

```
kubectl get acc -n netapp-acc
```

b. Wechseln Sie zum Stellen Sie den Astra Control Center Operator wieder her Abschnitt dieses Dokuments, um den Wiederherstellungsprozess abzuschließen.

Schritt 1: Astra Control Center mit Replizierung schützen

Dieses Verfahren beschreibt die erforderlichen Schritte zur Konfiguration "Astra Control Center-Replizierung" Zum Schutz der primären Astra Control Center-Instanz.

In diesem Beispiel wird Astra Control Center immer unter installiert `netapp-acc` Namespace und der Operator wird unter installiert `netapp-acc-operator` Namespace.

Bevor Sie beginnen

- Sie haben das primäre Astra Control Center auf einem Cluster installiert.
- Sie haben das sekundäre Astra Control Center auf einem anderen Cluster installiert.

Schritte

1. Management der primären Astra Control Center-Applikation und des Ziel-Clusters über die sekundäre

Astra Control Center-Instanz:

a. Melden Sie sich bei der sekundären Astra Control Center-Instanz an.

b. "Fügen Sie das primäre Astra Control Center-Cluster hinzu" (`ocp-cluster-1`).

c. "Fügen Sie das dritte Zielcluster hinzu" (`ocp-cluster-3`), das für die Replikation verwendet wird.

2. Astra Control Center und den Astra Control Center Betreiber im sekundären Astra Control Center managen:

a. Wählen Sie **Cluster** aus und wählen Sie den Cluster aus, der das primäre Astra Control Center enthält (`ocp-cluster-1`).

b. Wählen Sie die Registerkarte **Namesaces** aus.

c. Wählen Sie `netapp-acc` Und `netapp-acc-operator` Namespaces.

d. Wählen Sie im Menü Aktionen die Option **als Anwendungen definieren**.

e. Wählen Sie **in Anwendungen anzeigen**, um die definierten Anwendungen anzuzeigen.

3. Back-Ends für Replikation konfigurieren:

> Für die Replizierung sind das primäre Astra Control Center-Cluster und das Ziel-Cluster erforderlich (`ocp-cluster-3`) Verwenden Sie verschiedene peered ONTAP-Speicher-Backends.
> Nachdem jedes Backend zu Astra Control hinzugefügt wurde, erscheint das Backend auf der Seite Backends auf der Registerkarte **Discovered**.

a. "Fügen Sie ein Peering-Backend hinzu" Zum Astra Control Center auf dem primären Cluster.

b. "Fügen Sie ein Peering-Backend hinzu" Zum Astra Control Center auf dem Ziel-Cluster.

4. Replikation konfigurieren:

a. Wählen Sie im Bildschirm Anwendungen die aus `netapp-acc` Applikation.

b. Wählen Sie **Configure Replication Policy** aus.

c. Wählen Sie `ocp-cluster-3` Als Ziel-Cluster.

d. Wählen Sie die Storage-Klasse aus.

e. Eingabe `netapp-acc` Als Ziel-Namespace.

f. Ändern Sie bei Bedarf die Replizierungshäufigkeit.

g. Wählen Sie **Weiter**.

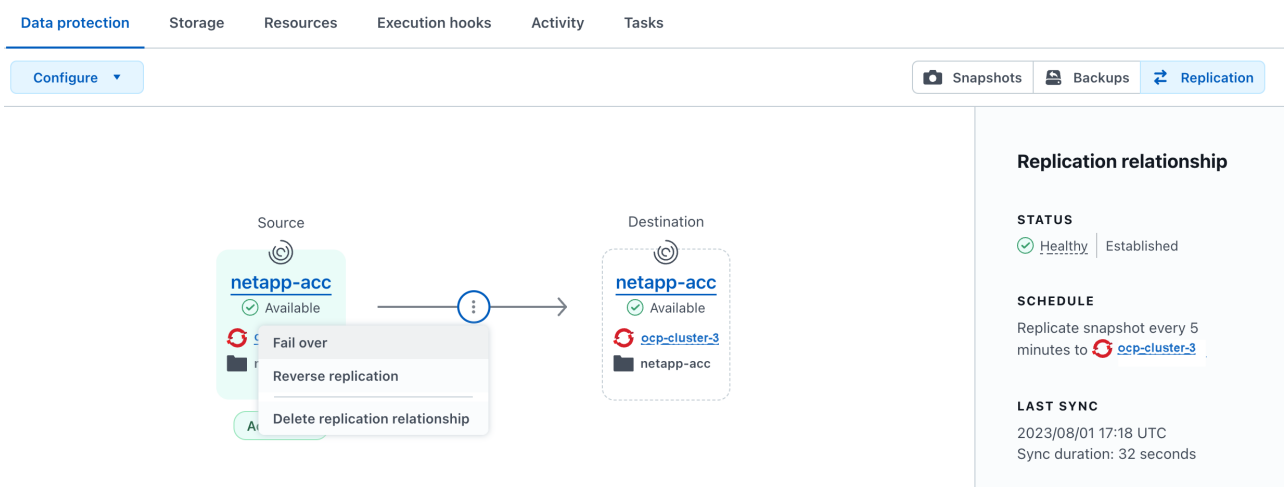
h. Bestätigen Sie, dass die Konfiguration korrekt ist, und wählen Sie **Speichern**.

Die Replikationsbeziehung wechselt von `Establishing` Bis `Established`. Wenn diese Replikation aktiv ist, erfolgt sie alle fünf Minuten, bis die Replikationskonfiguration gelöscht wird.

5. Failover der Replikation auf den anderen Cluster, wenn das primäre System beschädigt ist oder nicht mehr darauf zugegriffen werden kann:

> Stellen Sie sicher, dass auf dem Ziel-Cluster Astra Control Center nicht installiert ist, um einen erfolgreichen Failover zu gewährleisten.

a. Wählen Sie das Symbol für vertikale Ellipsen und dann **Failover**.



b. Bestätigen Sie die Details, und wählen Sie **Failover**, um den Failover-Prozess zu starten.

   Der Status der Replikationsbeziehung ändert sich in `Failing over` Und dann `Failed over` Nach Abschluss.

6. Schließen Sie die Failover-Konfiguration ab:

   a. Öffnen Sie ein Terminal, und verbinden Sie es mit dem kubeconfig des dritten Clusters (`ocp-cluster-3`). Auf diesem Cluster ist jetzt Astra Control Center installiert.

   b. Bestimmen Sie den FQDN des Astra Control Center auf dem dritten Cluster (`ocp-cluster-3`).

   c. Aktualisieren Sie die Konfiguration, um auf den Astra Control Center-DNS zu verweisen:

```
kubectl edit acc -n netapp-acc
```

      i. Ändern Sie das `astraAddress` Unter `spec:` Mit dem FQDN (`ocp-cluster-3.company.com`) Des dritten Zielclusters.

      ii. Speichern Sie die Konfiguration.

      iii. Bestätigen Sie, dass die Adresse aktualisiert wurde:

```
kubectl get acc -n netapp-acc
```

   d. Bestätigen Sie, dass alle erforderlichen traefik-CRDs vorhanden sind:

```
kubectl get crds | grep traefik
```

   Erforderliche Traefik CRDS:

```
ingressroutes.traefik.containo.us
ingressroutes.traefik.io
ingressroutetcps.traefik.containo.us
ingressroutetcps.traefik.io
ingressrouteudps.traefik.containo.us
ingressrouteudps.traefik.io
middlewares.traefik.containo.us
middlewares.traefik.io
middlewaretcps.traefik.containo.us
middlewaretcps.traefik.io
serverstransports.traefik.containo.us
serverstransports.traefik.io
tlsoptions.traefik.containo.us
tlsoptions.traefik.io
tIsstores.traefik.containo.us
tIsstores.traefik.io
traefikservices.traefik.containo.us
traefikservices.traefik.io
```

a. Wenn einige der oben genannten CRDs fehlen:
   i. Gehen Sie zu "Traefik-Dokumentation".
   ii. Kopieren Sie den Bereich „Definitionen“ in eine Datei.
   iii. Änderungen übernehmen:

```
kubectl apply -f <file name>
```

   iv. Traefik neu starten:

```
kubectl get pods -n netapp-acc | grep -e "traefik" | awk '{print
$1}' | xargs kubectl delete pod -n netapp-acc
```

b. Wechseln Sie zum Stellen Sie den Astra Control Center Operator wieder her Abschnitt dieses Dokuments, um den Wiederherstellungsprozess abzuschließen.

Schritt 2: Wiederherstellen des Bedieners des Astra Control Centers

Stellen Sie mithilfe des sekundären Astra Control Center den primären Astra Control Center-Operator aus dem Backup wieder her. Der Ziel-Namespace muss mit dem Quell-Namespace übereinstimmen. Wenn Astra Control Center aus dem primären Quell-Cluster gelöscht wurde, sind Backups weiterhin vorhanden, um dieselben Wiederherstellungsschritte auszuführen.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen der Operator-App aus (`netapp-acc-operator`).

2. Wählen Sie im Menü Optionen in der Spalte Aktionen die Option **Wiederherstellen** aus
3. Wählen Sie als Wiederherstellungstyp die Option **in neue Namespaces wiederherstellen**.
4. Wählen Sie das dritte Zielcluster aus (`ocp-cluster-3`).
5. Ändern Sie den Namespace so, dass er mit dem Namespace identisch ist, der mit dem primären Quellcluster verknüpft ist (`netapp-acc-operator`).
6. Wählen Sie das Backup aus, das zuvor als Wiederherstellungsquelle erstellt wurde.
7. Wählen Sie **Restore using original Storage classes**.
8. Wählen Sie **Alle Ressourcen wiederherstellen**.
9. Überprüfen Sie die Details und klicken Sie dann auf * Wiederherstellen*, um den Wiederherstellungsprozess zu starten.

   Auf der Seite Anwendungen wird der Astra Control Center-Operator angezeigt, der auf dem dritten Zielcluster wiederhergestellt wird (`ocp-cluster-3`). Wenn der Prozess abgeschlossen ist, wird der Status als angezeigt `Available`. Innerhalb von zehn Minuten sollte die DNS-Adresse auf der Seite aufgelöst werden.

Ergebnis

Astra Control Center, die registrierten Cluster sowie gemanagte Applikationen mit ihren Snapshots und Backups sind jetzt auf dem Ziel-Third-Cluster verfügbar (`ocp-cluster-3`). Alle Sicherungsrichtlinien, die Sie auf dem Original hatten, sind auch auf der neuen Instanz vorhanden. Sie können weiterhin geplante oder On-Demand-Backups und Snapshots erstellen.

Fehlerbehebung

Bestimmen Sie den Systemzustand und ob die Schutzprozesse erfolgreich waren.

- **Pods laufen nicht**: Vergewissern Sie sich, dass alle Pods ausgeführt werden:

  ```
  kubectl get pods -n netapp-acc
  ```

  Wenn sich einige Pods im befinden `CrashLookBackOff` Geben Sie den Status ein, und starten Sie sie neu. Sie sollten dann zu wechseln `Running` Bundesland.

- **Systemstatus bestätigen**: Bestätigen Sie, dass sich das Astra Control Center-System in befindet `ready` Bundesland:

  ```
  kubectl get acc -n netapp-acc
  ```

  Antwort:

  ```
  NAME  UUID                                   VERSION    ADDRESS
  READY
  astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.10.0-68 ocp-cluster-
  1.company.com           True
  ```

- **Bereitstellungsstatus bestätigen**: Zeigt Informationen zur Astra Control Center-Bereitstellung an, um dies zu bestätigen `Deployment State` Ist `Deployed`.

```
kubectl describe acc astra -n netapp-acc
```

- **Wiederhergestellte Astra Control Center UI gibt einen 404 Fehler** zurück: Wenn dies geschieht, wenn Sie ausgewählt haben `AccTraefik` Aktivieren Sie als Eindringen die Option Traefik-CRDs Um sicherzustellen, dass alle installiert sind.

Monitoring des Applikations- und Cluster-Systemzustands

Zeigen Sie eine Zusammenfassung des Applikations- und Cluster-Zustands an

Wählen Sie das **Dashboard** aus, um eine übergeordnete Ansicht Ihrer Apps, Cluster, Storage-Back-Ends und deren Integrität anzuzeigen.

Dabei handelt es sich nicht nur um statische Zahlen oder Statusangaben, sondern Sie können von jedem einzelnen Detail aus darauf aufgehen. Wenn Apps beispielsweise nicht vollständig geschützt sind, können Sie mit dem Mauszeiger auf das Symbol zeigen, um zu ermitteln, welche Apps nicht vollständig geschützt sind. Dies gibt einen Grund dafür.

Auf Applikationen Kachel

Mit der Kachel * Applications* können Sie Folgendes identifizieren:

- Wie viele Applikationen managen Sie aktuell mit Astra?
- Ob diese verwalteten Apps gesund sind.
- Gibt an, ob die Applikationen vollständig gesichert sind (sie sind geschützt, wenn neueste Backups verfügbar sind).
- Die Anzahl der Anwendungen, die erkannt, aber noch nicht verwaltet wurden.

  Idealerweise wäre diese Zahl null, da Sie Apps nach dem Entstehen verwalten oder ignorieren würden. Anschließend sollten Sie die Anzahl der im Dashboard ermittelten Apps überwachen, um zu ermitteln, wann Entwickler neue Apps zu einem Cluster hinzufügen.

Cluster-Tile

Die Kachel **Cluster** bietet ähnliche Details über die Integrität der Cluster, die Sie mit dem Astra Control Center verwalten, und Sie können detaillierte Informationen abrufen, wie Sie es mit einer App möglich sind.

Storage Back-Ends

Die Kachel **Storage Back-Ends** enthält Informationen, die Ihnen bei der Identifizierung des Zustands von Storage-Back-Ends helfen. Dazu gehören:

- Wie viele Storage-Back-Ends werden gemanagt
- Gibt an, ob diese gemanagten Backends gesund sind
- Gibt an, ob die Back-Ends vollständig geschützt sind

- Die Anzahl der Back-Ends, die zwar erkannt, aber noch nicht gemanagt werden.

Zeigen Sie den Cluster-Zustand an und managen Sie Storage-Klassen

Nachdem Sie Cluster hinzugefügt haben, die von Astra Control Center gemanagt werden können, können Sie Details zum Cluster anzeigen, beispielsweise den Speicherort, die Worker-Nodes, die persistenten Volumes und die Storage-Klassen. Sie können auch die Standard-Storage-Klasse für verwaltete Cluster ändern.

Zeigen Sie den Cluster-Zustand und die Details an

Sie können Details zum Cluster anzeigen, z. B. seinen Standort, die Worker-Nodes, persistente Volumes und Storage-Klassen.

Schritte

1. Wählen Sie in der Astra Control Center-Benutzeroberfläche **Cluster** aus.
2. Wählen Sie auf der Seite **Cluster** den Cluster aus, dessen Details Sie anzeigen möchten.

> 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".

3. Zeigen Sie die Informationen auf den Registerkarten **Übersicht**, **Speicher** und **Aktivität** an, um die gewünschten Informationen zu finden.
   - **Übersicht**: Details zu den Arbeiterknoten, einschließlich ihres Status.
   - **Storage**: Die persistenten Volumes, die mit dem Computing verbunden sind, einschließlich der Speicherklasse und des Status.
   - **Aktivität**: Zeigt die Aktivitäten im Zusammenhang mit dem Cluster an.

> Sie können auch Clusterinformationen anzeigen, die Sie über das Astra Control Center **Dashboard** starten. Auf der Registerkarte **Cluster** unter **Resource summary** können Sie die verwalteten Cluster auswählen, die Sie zur Seite **Cluster** führen. Nachdem Sie die Seite **Cluster** aufgerufen haben, befolgen Sie die oben beschriebenen Schritte.

Ändern der Standard-Storage-Klasse

Sie können die Standard-Storage-Klasse für ein Cluster ändern. Wenn Astra Control einen Cluster verwaltet, wird die Standard-Storage-Klasse des Clusters überwacht.

> Ändern Sie die Storage-Klasse nicht mit kubectl-Befehlen. Verwenden Sie stattdessen diese Prozedur. Astra Control setzt die Änderungen zurück, wenn sie mit kubectl vorgenommen werden.

Schritte

1. Wählen Sie in der Web-UI des Astra Control Center die Option **Cluster** aus.

2. Wählen Sie auf der Seite **Cluster** den Cluster aus, den Sie ändern möchten.
3. Wählen Sie die Registerkarte **Storage** aus.
4. Wählen Sie die Kategorie **Speicherklassen** aus.
5. Wählen Sie das Menü **Aktionen** für die Speicherklasse aus, die Sie als Standard festlegen möchten.
6. Wählen Sie **als Standard**.

Anzeigen des Funktionszustands und der Details einer App

Astra Control bietet nach dem Management einer App Details zu der App, mit der Sie den Kommunikationsstatus (ob Astra Control mit der App kommunizieren kann), den Sicherungsstatus (unabhängig davon, ob die App bei Ausfällen vollständig geschützt ist), die Pods, persistenten Storage usw. ermitteln können.

Schritte

1. Wählen Sie in der Astra Control Center-UI **Anwendungen** und dann den Namen einer App aus.
2. Überprüfen Sie die Informationen.

Anwendungsstatus

Zeigt einen Status an, der angibt, ob Astra Control mit der Applikation kommunizieren kann.

- **App Protection Status**: Gibt einen Status, wie gut die App geschützt ist:
  - **Vollständig geschützt**: Die App verfügt über einen aktiven Backup-Zeitplan und ein erfolgreiches Backup, das weniger als eine Woche alt ist
  - **Teilweise geschützt**: Die App verfügt über einen aktiven Backup-Zeitplan, einen aktiven Snapshot-Zeitplan oder einen erfolgreichen Backup oder Snapshot
  - **Ungeschützt**: Apps, die weder vollständig geschützt noch teilweise geschützt sind.

    _Sie können erst dann vollständig geschützt sein, wenn Sie ein kürzlich gesichertes Backup haben. Das ist wichtig, da Backups abseits der persistenten Volumes in einem Objektspeicher gespeichert werden. Wenn ein Ausfall das Cluster herauswischt und es sich um den persistenten Storage handelt, muss das Backup wiederhergestellt werden. Ein Snapshot würde es Ihnen nicht ermöglichen, eine Wiederherstellung durchzuführen.
- **Übersicht**: Informationen über den Zustand der Pods, die mit der App verbunden sind.
- **Datenschutz**: Ermöglicht die Konfiguration einer Datenschutzrichtlinie und die Anzeige der vorhandenen Snapshots und Backups.
- **Storage**: Zeigt dir die persistenten Volumes auf App-Ebene. Der Zustand eines persistenten Volumes befindet sich aus der Perspektive des Kubernetes Clusters.
- **Ressourcen**: Ermöglicht es Ihnen, zu überprüfen, welche Ressourcen gesichert und verwaltet werden.
- **Aktivität**: Zeigt die Aktivitäten im Zusammenhang mit der App an.

> Sie können auch App-Informationen ab dem Astra Control Center **Dashboard** anzeigen. Auf der Registerkarte **Anwendungen** unter **Ressourcenzusammenfassung** können Sie die verwalteten Apps auswählen, die Sie zur Seite **Anwendungen** führen. Nachdem Sie die Seite **Applikationen** aufgerufen haben, befolgen Sie die oben beschriebenen Schritte.

Konto verwalten

Managen Sie lokale Benutzer und Rollen

Sie können Benutzer Ihrer Astra Control Center-Installation über die Astra Control-Benutzeroberfläche hinzufügen, entfernen und bearbeiten. Sie können die Astra Control UI oder verwenden "Astra Control API" Um Benutzer zu managen.

Sie können LDAP auch zur Authentifizierung für ausgewählte Benutzer verwenden.

LDAP verwenden

LDAP ist ein branchenübliches Protokoll für den Zugriff auf verteilte Verzeichnisinformationen und eine beliebte Wahl für die Unternehmensauthentifizierung. Sie können Astra Control Center mit einem LDAP-Server verbinden, um die Authentifizierung für ausgewählte Astra Control-Benutzer durchzuführen. Auf hohem Niveau beinhaltet die Konfiguration die Integration von Astra mit LDAP und die Definition der Astra Control Benutzer und Gruppen entsprechend der LDAP-Definitionen. Sie können die Astra Control API oder die Web-Benutzeroberfläche verwenden, um die LDAP-Authentifizierung und LDAP-Benutzer und -Gruppen zu konfigurieren. Weitere Informationen finden Sie in der folgenden Dokumentation:

- "Mit der Astra Control API können Sie die Remote-Authentifizierung und -Benutzer verwalten"
- "Verwenden Sie die Astra Control-Benutzeroberfläche, um Remote-Benutzer und -Gruppen zu verwalten"
- "Verwenden Sie die Astra Control-Benutzeroberfläche, um die Remote-Authentifizierung zu verwalten"

Benutzer hinzufügen

Kontoinhaber und -Administratoren können weitere Benutzer zur Installation des Astra Control Center hinzufügen.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Wählen Sie die Registerkarte **Benutzer** aus.
3. Wählen Sie **Benutzer Hinzufügen**.
4. Geben Sie den Namen des Benutzers, die E-Mail-Adresse und ein temporäres Kennwort ein.

   Der Benutzer muss das Passwort bei der ersten Anmeldung ändern.

5. Wählen Sie eine Benutzerrolle mit den entsprechenden Systemberechtigungen aus.

   Jede Rolle bietet die folgenden Berechtigungen:

   - Ein **Viewer** kann Ressourcen anzeigen.
   - Ein **Mitglied** verfügt über Berechtigungen für Viewer-Rollen und kann Apps und Cluster verwalten, Apps verwalten und Snapshots und Backups löschen.
   - Ein **Admin** verfügt über Berechtigungen für die Mitgliederrolle und kann alle anderen Benutzer außer dem Eigentümer hinzufügen und entfernen.
   - Ein **Owner** hat Administratorrechte und kann beliebige Benutzerkonten hinzufügen und entfernen.

6. Um einem Benutzer mit einer Mitglied- oder Viewer-Rolle Einschränkungen hinzuzufügen, aktivieren Sie das Kontrollkästchen * Rolle auf Einschränkungen beschränken*.

Weitere Informationen zum Hinzufügen von Einschränkungen finden Sie unter "Managen Sie lokale Benutzer und Rollen".

7. Wählen Sie **Hinzufügen**.

Passwörter verwalten

Sie können Passwörter für Benutzerkonten im Astra Control Center verwalten.

Passwort ändern

Sie können das Passwort Ihres Benutzerkontos jederzeit ändern.

Schritte

1. Klicken Sie oben rechts auf dem Bildschirm auf das Symbol Benutzer.
2. Wählen Sie **Profil**.
3. Wählen Sie im Menü Optionen in der Spalte **Aktionen** die Option **Passwort ändern** aus.
4. Geben Sie ein Passwort ein, das den Anforderungen des Passworts entspricht.
5. Geben Sie das Kennwort zur Bestätigung erneut ein.
6. Wählen Sie **Passwort ändern**.

Kennwort eines anderen Benutzers zurücksetzen

Wenn Ihr Konto über Berechtigungen für die Administrator- oder Eigentümerrolle verfügt, können Sie Passwörter für andere Benutzerkonten sowie für Ihre eigenen zurücksetzen. Wenn Sie ein Kennwort zurücksetzen, weisen Sie ein temporäres Kennwort zu, das der Benutzer bei der Anmeldung ändern muss.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Wählen Sie die Dropdown-Liste **Aktionen** aus.
3. Wählen Sie **Passwort Zurücksetzen**.
4. Geben Sie ein temporäres Kennwort ein, das den Anforderungen des Passworts entspricht.
5. Geben Sie das Kennwort zur Bestätigung erneut ein.

> ⓘ Wenn sich der Benutzer beim nächsten Mal anmeldet, wird er aufgefordert, das Passwort zu ändern.

6. Wählen Sie **Passwort zurücksetzen**.

Benutzer entfernen

Benutzer mit der Eigentümer- oder Administratorrolle können jederzeit andere Benutzer aus dem Konto entfernen.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Aktivieren Sie auf der Registerkarte **Benutzer** das Kontrollkästchen in der Zeile jedes Benutzers, den Sie entfernen möchten.

3. Wählen Sie im Menü Optionen in der Spalte **Aktionen** die Option **Benutzer/s entfernen** aus.
4. Wenn Sie aufgefordert werden, bestätigen Sie den Löschvorgang, indem Sie das Wort "Entfernen" eingeben und dann **Ja, Benutzer entfernen** wählen.

Ergebnis

Astra Control Center entfernt den Benutzer aus dem Konto.

Rollen managen

Sie können Rollen managen, indem Sie Namespace-Einschränkungen hinzufügen und Benutzerrollen auf diese Einschränkungen beschränken. So können Sie den Zugriff auf Ressourcen in Ihrem Unternehmen kontrollieren. Sie können die Astra Control UI oder verwenden "Astra Control API" Rollen managen.

Fügen Sie einer Rolle eine Namespace-Einschränkung hinzu

Ein Administrator oder Benutzer des Eigentümers kann den Mitglied- oder Viewer-Rollen Namespace-Einschränkungen hinzufügen.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Wählen Sie die Registerkarte **Benutzer** aus.
3. Wählen Sie in der Spalte **Actions** die Menü-Schaltfläche für einen Benutzer mit der Rolle Mitglied oder Viewer.
4. Wählen Sie **Rolle bearbeiten**.
5. Aktivieren Sie das Kontrollkästchen * Rolle auf Einschränkungen beschränken*.

   Das Kontrollkästchen ist nur für Mitglieder- oder Viewer-Rollen verfügbar. Aus der Dropdown-Liste **Rolle** können Sie eine andere Rolle auswählen.

6. Wählen Sie **Bedingung hinzufügen**.

   Sie können die Liste der verfügbaren Einschränkungen nach Namespace oder Namensraum-Bezeichnung anzeigen.

7. Wählen Sie in der Dropdown-Liste **Constraint type** je nach Konfiguration Ihrer Namespaces entweder **Kubernetes Namespace** oder **Kubernetes Namespace Label** aus.
8. Wählen Sie eine oder mehrere Namespaces oder Labels aus der Liste aus, um eine Beschränkung zu erstellen, die Rollen auf diese Namespaces beschränkt.
9. Wählen Sie **Bestätigen**.

   Auf der Seite * Rolle bearbeiten* wird die Liste der für diese Rolle ausgewählten Einschränkungen angezeigt.

10. Wählen Sie **Bestätigen**.

    Auf der Seite **Konto** können Sie die Einschränkungen für beliebige Mitglieder- oder Viewer-Rollen in der Spalte **Role** anzeigen.

Wenn Sie Einschränkungen für eine Rolle aktivieren und **Bestätigen** wählen, ohne dass Einschränkungen hinzugefügt werden müssen, gilt die Rolle als uneingeschränkt eingeschränkt (die Rolle wird dem Zugriff auf alle Ressourcen verweigert, die Namespaces zugewiesen sind).

Entfernen Sie eine Namespace-Beschränkung aus einer Rolle

Ein Administrator oder Benutzer eines Eigentümers kann eine Namespace-Einschränkung aus einer Rolle entfernen.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Wählen Sie die Registerkarte **Benutzer** aus.
3. Wählen Sie in der Spalte **Aktionen** die Menütaste für einen Benutzer mit der Rolle Mitglied oder Viewer mit aktiven Einschränkungen.
4. Wählen Sie **Rolle bearbeiten**.

   Im Dialogfeld **Rolle bearbeiten** werden die aktiven Einschränkungen für die Rolle angezeigt.

5. Wählen Sie das **X** rechts neben der Bedingung aus, die Sie entfernen müssen.
6. Wählen Sie **Bestätigen**.

Finden Sie weitere Informationen

- "Benutzerrollen und Namespaces"

Managen Sie die Remote-Authentifizierung

LDAP ist ein branchenübliches Protokoll für den Zugriff auf verteilte Verzeichnisinformationen und eine beliebte Wahl für die Unternehmensauthentifizierung. Sie können Astra Control Center mit einem LDAP-Server verbinden, um die Authentifizierung für ausgewählte Astra Control-Benutzer durchzuführen.

Auf hohem Niveau beinhaltet die Konfiguration die Integration von Astra mit LDAP und die Definition der Astra Control Benutzer und Gruppen entsprechend der LDAP-Definitionen. Sie können die Astra Control API oder die Web-Benutzeroberfläche verwenden, um die LDAP-Authentifizierung und LDAP-Benutzer und -Gruppen zu konfigurieren.

Astra Control Center verwendet das bei aktivierter Remote-Authentifizierung konfigurierte Attribut für die Benutzeranmeldung, um Remote-Benutzer zu suchen und zu verfolgen. Für jeden Remote-Benutzer, den Sie im Astra Control Center anzeigen möchten, muss in diesem Feld ein Attribut einer E-Mail-Adresse („Mail“) oder eines Hauptnamens des Benutzers („userPrincipalName“) vorhanden sein. Dieses Attribut wird als Benutzername in Astra Control Center für die Authentifizierung und bei der Suche nach Remote-Benutzern verwendet.

Fügen Sie ein Zertifikat für die LDAPS-Authentifizierung hinzu

Fügen Sie das private TLS-Zertifikat für den LDAP-Server hinzu, damit sich Astra Control Center bei Verwendung einer LDAPS-Verbindung mit dem LDAP-Server authentifizieren kann. Sie müssen dies nur einmal tun, oder wenn das Zertifikat, das Sie installiert haben, abläuft.

Schritte

1. Gehen Sie zu **Konto**.
2. Wählen Sie die Registerkarte **Zertifikate** aus.
3. Wählen Sie **Hinzufügen**.
4. Laden Sie entweder die hoch `.pem` Datei oder fügen Sie den Inhalt der Datei aus der Zwischenablage ein.
5. Aktivieren Sie das Kontrollkästchen * Trusted*.
6. Wählen Sie **Zertifikat hinzufügen**.

Aktivieren Sie die Remote-Authentifizierung

Sie können die LDAP-Authentifizierung aktivieren und die Verbindung zwischen Astra Control und dem Remote LDAP-Server konfigurieren.

Bevor Sie beginnen

Wenn Sie LDAPS verwenden möchten, stellen Sie sicher, dass das private TLS-Zertifikat für den LDAP-Server im Astra Control Center installiert ist, damit sich Astra Control Center mit dem LDAP-Server authentifizieren kann. Siehe Fügen Sie ein Zertifikat für die LDAPS-Authentifizierung hinzu Weitere Anweisungen.

Schritte

1. Gehen Sie zu **Konto > Verbindungen**.
2. Wählen Sie im Fenster **Remote Authentication** das Konfigurationsmenü aus.
3. Wählen Sie **Verbinden**.
4. Geben Sie die IP-Adresse, den Port und das bevorzugte Verbindungsprotokoll (LDAP oder LDAPS) des Servers ein.

   Verwenden Sie als Best Practice LDAPS, wenn Sie eine Verbindung zum LDAP-Server herstellen. Vor der Verbindung mit LDAPS müssen Sie das private TLS-Zertifikat des LDAP-Servers in Astra Control Center installieren.

5. Geben Sie die Anmeldeinformationen für das Servicekonto im E-Mail-Format ein (administrator@example.com). Astra Control verwendet diese Anmeldeinformationen, wenn Sie eine Verbindung mit dem LDAP-Server herstellen.
6. Gehen Sie im Abschnitt **User Match** wie folgt vor:
   a. Geben Sie den Basis-DN und einen entsprechenden Benutzersuchfilter ein, der beim Abrufen von Benutzerinformationen vom LDAP-Server verwendet werden soll.
   b. (Optional) Wenn Ihr Verzeichnis das Benutzeranmeldungsattribut verwendet `userPrincipalName` Statt `mail`, Geben Sie ein `userPrincipalName` Geben Sie im Feld **Benutzer-Login-Attribut** das richtige Attribut ein.
7. Geben Sie im Abschnitt **Gruppenvergleich** den Gruppen-Suchsockel-DN und einen entsprechenden benutzerdefinierten Gruppensuchfilter ein.

   Verwenden Sie unbedingt den richtigen Basisnamen (DN) und einen entsprechenden Suchfilter für **User Match** und **Group Match**. Der Basis-DN teilt Astra Control mit, auf welcher Ebene der Verzeichnisstruktur die Suche gestartet werden soll, und der Suchfilter begrenzt die Teile des Verzeichnisbaums Astra Control Suchanfragen.

8. Wählen Sie **Senden**.

Ergebnis

Der Fensterstatus **Remote-Authentifizierung** wechselt zu **Ausstehend** und dann zu **verbunden**, wenn die Verbindung zum LDAP-Server hergestellt wird.

Deaktivieren Sie die Remote-Authentifizierung

Sie können eine aktive Verbindung zum LDAP-Server vorübergehend deaktivieren.

> Wenn Sie eine Verbindung zu einem LDAP-Server deaktivieren, werden alle Einstellungen gespeichert und alle Remote-Benutzer und -Gruppen, die von diesem LDAP-Server zu Astra Control hinzugefügt wurden, bleiben erhalten. Sie können jederzeit eine Verbindung zu diesem LDAP-Server herstellen.

Schritte

1. Gehen Sie zu **Konto > Verbindungen**.
2. Wählen Sie im Fenster **Remote Authentication** das Konfigurationsmenü aus.
3. Wählen Sie **Deaktivieren**.

Ergebnis

Der Status des Fensterbereichs **Remote Authentication** wechselt zu **deaktivierte**. Alle Einstellungen für die Remote-Authentifizierung, Remote-Benutzer und Remote-Gruppen bleiben erhalten, und Sie können die Verbindung jederzeit wieder aktivieren.

Remote-Authentifizierungseinstellungen bearbeiten

Wenn Sie die Verbindung zum LDAP-Server deaktiviert haben oder sich der Fensterbereich **Remote Authentication** im Status „Verbindungsfehler“ befindet, können Sie die Konfigurationseinstellungen bearbeiten.

> Sie können die URL oder IP-Adresse des LDAP-Servers nicht bearbeiten, wenn sich der Bereich **Remote Authentication** im Status „deaktiviert“ befindet. Sie müssen Trennen Sie die Remote-Authentifizierung Zunächst.

Schritte

1. Gehen Sie zu **Konto > Verbindungen**.
2. Wählen Sie im Fenster **Remote Authentication** das Konfigurationsmenü aus.
3. Wählen Sie **Bearbeiten**.
4. Nehmen Sie die erforderlichen Änderungen vor, und wählen Sie **Bearbeiten**.

Trennen Sie die Remote-Authentifizierung

Sie können die Verbindung zu einem LDAP-Server trennen und die Konfigurationseinstellungen von Astra Control entfernen.

> Wenn Sie ein LDAP-Benutzer sind und die Verbindung trennen, wird Ihre Sitzung sofort beendet Wenn Sie die Verbindung zum LDAP-Server trennen, werden alle Konfigurationseinstellungen für diesen LDAP-Server aus Astra Control sowie alle Remote-Benutzer und -Gruppen entfernt, die diesem LDAP-Server hinzugefügt wurden.

Schritte

1. Gehen Sie zu **Konto > Verbindungen**.
2. Wählen Sie im Fenster **Remote Authentication** das Konfigurationsmenü aus.
3. Wählen Sie **Trennen**.

Ergebnis

Der Status des Fensterbereichs **Remote Authentication** wechselt zu **nicht verbunden**. Remote-Authentifizierungseinstellungen, Remote-Benutzer und Remote-Gruppen werden aus Astra Control entfernt.

Verwalten von Remote-Benutzern und -Gruppen

Wenn Sie die LDAP-Authentifizierung auf Ihrem Astra Control System aktiviert haben, können Sie nach LDAP-Benutzern und -Gruppen suchen und diese in die genehmigten Benutzer des Systems aufnehmen.

Fügen Sie einen Remote-Benutzer hinzu

Kontoinhaber und -Administratoren können Remote-Benutzer zu Astra Control hinzufügen. Astra Control Center unterstützt bis zu 10,000 LDAP Remote-Benutzer.

> Astra Control Center verwendet das bei aktivierter Remote-Authentifizierung konfigurierte Attribut für die Benutzeranmeldung, um Remote-Benutzer zu suchen und zu verfolgen. Für jeden Remote-Benutzer, den Sie im Astra Control Center anzeigen möchten, muss in diesem Feld ein Attribut einer E-Mail-Adresse („Mail“) oder eines Hauptnamens des Benutzers („userPrincipalName“) vorhanden sein. Dieses Attribut wird als Benutzername in Astra Control Center für die Authentifizierung und bei der Suche nach Remote-Benutzern verwendet.

> Sie können keinen Remote-Benutzer hinzufügen, wenn bereits ein lokaler Benutzer mit derselben E-Mail-Adresse (basierend auf dem Attribut „Mail“ oder „user principal Name“) auf dem System vorhanden ist. Um den Benutzer als Remote-Benutzer hinzuzufügen, löschen Sie zuerst den lokalen Benutzer aus dem System.

Schritte

1. Gehen Sie zum Bereich **Konto**.
2. Wählen Sie die Registerkarte **Benutzer & Gruppen** aus.
3. Wählen Sie rechts auf der Seite die Option **Remote Users**.
4. Wählen Sie **Hinzufügen**.
5. Sie können auch nach einem LDAP-Benutzer suchen, indem Sie die E-Mail-Adresse des Benutzers im Feld **Filtern nach E-Mail** eingeben.
6. Wählen Sie einen oder mehrere Benutzer aus der Liste aus.
7. Weisen Sie dem Benutzer eine Rolle zu.

> Wenn Sie einem Benutzer und der Gruppe des Benutzers verschiedene Rollen zuweisen, hat die Rolle eine größere Priorität.

8. Weisen Sie diesem Benutzer optional eine oder mehrere Namespace-Einschränkungen zu und wählen Sie **Rolle auf Einschränkungen beschränken** aus, um sie durchzusetzen. Sie können eine neue Namespace-Einschränkung hinzufügen, indem Sie **Bedingung hinzufügen** auswählen.

Wenn einem Benutzer mehrere Rollen durch die LDAP-Gruppenmitgliedschaft zugewiesen werden, sind die Einschränkungen in der am stärksten permissivsten Rolle die einzigen, die wirksam werden. Wenn z. B. ein Benutzer mit einer lokalen Viewer-Rolle drei Gruppen verbindet, die an die Rolle Mitglied gebunden sind, wird die Summe der Einschränkungen aus den Mitgliederrollen wirksam, und alle Einschränkungen aus der Viewer-Rolle werden ignoriert.

9. Wählen Sie **Hinzufügen**.

Ergebnis

Der neue Benutzer wird in der Liste der Remote-Benutzer angezeigt. In dieser Liste können Sie aktive Einschränkungen für den Benutzer sehen und den Benutzer über das Menü **Aktionen** verwalten.

Fügen Sie eine externe Gruppe hinzu

Wenn Sie viele Remote-Benutzer gleichzeitig hinzufügen möchten, können Kontoinhaber und -Administratoren Remote-Gruppen zu Astra Control hinzufügen. Wenn Sie eine Remote-Gruppe hinzufügen, können sich alle Remote-Benutzer in dieser Gruppe bei Astra Control anmelden und übernehmen die gleiche Rolle wie die Gruppe.

Astra Control Center unterstützt bis zu 5,000 LDAP-Remote-Gruppen.

Schritte

1. Gehen Sie zum Bereich **Konto**.
2. Wählen Sie die Registerkarte **Benutzer & Gruppen** aus.
3. Wählen Sie rechts auf der Seite **Remote-Gruppen** aus.
4. Wählen Sie **Hinzufügen**.

   In diesem Fenster sehen Sie eine Liste der gemeinsamen Namen und Distinguished Names der LDAP-Gruppen, die Astra Control aus dem Verzeichnis abgerufen hat.

5. Suchen Sie optional nach einer LDAP-Gruppe, indem Sie den gemeinsamen Namen der Gruppe in das Feld **Filter nach gemeinsamem Namen** eingeben.
6. Wählen Sie eine oder mehrere Gruppen aus der Liste aus.
7. Weisen Sie den Gruppen eine Rolle zu.

   Die ausgewählte Rolle ist allen Benutzern in dieser Gruppe zugewiesen. Wenn Sie einem Benutzer und der Gruppe des Benutzers verschiedene Rollen zuweisen, hat die Rolle eine größere Priorität.

8. Weisen Sie dieser Gruppe optional eine oder mehrere Namespace-Einschränkungen zu und wählen Sie **Rolle auf Einschränkungen beschränken** aus, um sie durchzusetzen. Sie können eine neue Namespace-Einschränkung hinzufügen, indem Sie **Bedingung hinzufügen** auswählen.

   Wenn einem Benutzer mehrere Rollen durch die LDAP-Gruppenmitgliedschaft zugewiesen werden, sind die Einschränkungen in der am stärksten permissivsten Rolle die einzigen, die wirksam werden. Wenn z. B. ein Benutzer mit einer lokalen Viewer-Rolle drei Gruppen verbindet, die an die Rolle Mitglied gebunden sind, wird die Summe der Einschränkungen aus den Mitgliederrollen wirksam, und alle Einschränkungen aus der Viewer-Rolle werden ignoriert.

9. Wählen Sie **Hinzufügen**.

Ergebnis

Die neue Gruppe wird in der Liste der Remote-Gruppen angezeigt. Remote-Benutzer in dieser Gruppe werden erst dann in der Liste der Remote-Benutzer angezeigt, wenn sich jeder Remote-Benutzer anmeldet. In dieser Liste können Sie Details über die Gruppe anzeigen und die Gruppe über das Menü **Aktionen** verwalten.

Anzeigen und Managen von Benachrichtigungen

Astra benachrichtigt Sie, wenn Aktionen abgeschlossen oder fehlgeschlagen sind. Beispielsweise wird eine Benachrichtigung angezeigt, wenn ein Backup einer Anwendung erfolgreich abgeschlossen wurde.

Sie können diese Benachrichtigungen oben rechts auf der Schnittstelle verwalten:

Schritte

1. Wählen Sie oben rechts die Anzahl der ungelesenen Benachrichtigungen aus.
2. Überprüfen Sie die Benachrichtigungen und wählen Sie dann **als gelesen markieren** oder **Alle Benachrichtigungen anzeigen**.

   Wenn Sie **Alle Benachrichtigungen anzeigen** ausgewählt haben, wird die Seite Benachrichtigungen geladen.

3. Zeigen Sie auf der Seite **Benachrichtigungen** die Benachrichtigungen an, wählen Sie die Benachrichtigungen aus, die Sie als gelesen markieren möchten, wählen Sie **Aktion** und wählen Sie **als gelesen markieren**.

Anmeldeinformationen hinzufügen und entfernen

Fügen Sie Anmeldedaten für lokale Private-Cloud-Provider wie ONTAP S3, mit OpenShift gemanagte Kubernetes-Cluster oder nicht gemanagte Kubernetes-Cluster jederzeit in Ihrem Konto hinzu und entfernen Sie sie. Astra Control Center verwendet diese Zugangsdaten, um Kubernetes-Cluster und die Applikationen auf den Clustern zu erkennen und Ressourcen in Ihrem Auftrag bereitzustellen.

Beachten Sie, dass alle Benutzer im Astra Control Center dieselben Anmeldedaten verwenden.

Anmeldedaten hinzufügen

Wenn Sie Cluster verwalten, können Sie Astra Control Center Anmeldeinformationen hinzufügen. Informationen zum Hinzufügen von Anmeldeinformationen durch Hinzufügen eines neuen Clusters finden Sie unter "Fügen Sie einen Kubernetes-Cluster hinzu".

> Wenn Sie Ihre eigene kubeconfig-Datei erstellen, sollten Sie nur **ein** Kontextelement in ihr definieren. Siehe "Kubernetes-Dokumentation" Für Informationen über das Erstellen von kubeconfig-Dateien.

Anmeldedaten entfernen

Entfernen Sie die Anmeldeinformationen jederzeit aus einem Konto. Sie sollten erst nach dem Entfernen von Anmeldeinformationen verwenden "Verwalten aller zugehörigen Cluster wird aufgehoben".

> Der erste Satz von Anmeldeinformationen, die Sie dem Astra Control Center hinzufügen, wird immer verwendet, da Astra Control Center die Zugangsdaten für die Authentifizierung beim Backup-Bucket verwendet. Diese Anmeldedaten sollten am besten nicht entfernt werden.

Schritte

1. Wählen Sie **Konto**.
2. Wählen Sie die Registerkarte **Anmeldeinformationen** aus.
3. Wählen Sie in der Spalte **Status** das Menü Optionen für die Anmeldeinformationen aus, die Sie entfernen möchten.
4. Wählen Sie **Entfernen**.
5. Geben Sie das Wort „Entfernen“ ein, um den Löschvorgang zu bestätigen, und wählen Sie dann **Ja, Anmeldedaten entfernen** aus.

Ergebnis

Astra Control Center entfernt die Anmeldeinformationen aus dem Konto.

Überwachen der Kontoaktivität

Details zu den Aktivitäten können Sie in Ihrem Astra Control Konto anzeigen. Beispiel: Beim Einladen neuer Benutzer, beim Hinzufügen eines Clusters oder beim Erstellen eines Snapshots. Sie haben auch die Möglichkeit, Ihre Kontoaktivität in eine CSV-Datei zu exportieren.

> Wenn Sie Kubernetes-Cluster über Astra Control verwalten und Astra Control mit Cloud Insights verbunden ist, sendet Astra Control Ereignisprotokolle an Cloud Insights. Die Protokollinformationen, einschließlich Informationen über die Pod-Implementierung und PVC-Anhänge, werden im Astra Control Activity Log angezeigt. Mithilfe dieser Informationen können Sie alle zu verwaltenden Kubernetes-Cluster Fehler ermitteln.

Alle Kontoaktivitäten in Astra Control anzeigen

1. Wählen Sie **Aktivität**.
2. Verwenden Sie die Filter, um die Liste der Aktivitäten einzugrenzen, oder verwenden Sie das Suchfeld, um das gesuchte zu finden.
3. Wählen Sie **in CSV exportieren** aus, um Ihre Kontoaktivität in eine CSV-Datei herunterzuladen.

Zeigen Sie die Kontoaktivität für eine bestimmte App an

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie **Aktivität**.

Zeigen Sie die Kontoaktivität für Cluster an

1. Wählen Sie **Cluster** und dann den Namen des Clusters aus.
2. Wählen Sie **Aktivität**.

Ergreifen Sie Maßnahmen, um Ereignisse zu lösen, die Aufmerksamkeit erfordern

1. Wählen Sie **Aktivität**.
2. Wählen Sie ein Ereignis aus, das Aufmerksamkeit erfordert.
3. Wählen Sie die Dropdown-Option **Aktion** aus.

   In dieser Liste finden Sie mögliche Korrekturmaßnahmen, die Sie ergreifen können, eine Dokumentation zum Problem anzeigen und Support zur Behebung des Problems erhalten.

Aktualisieren einer vorhandenen Lizenz

Sie können eine Evaluierungslizenz in eine vollständige Lizenz umwandeln oder eine bestehende Evaluierung oder Volllizenz mit einer neuen Lizenz aktualisieren. Wenn Sie keine vollständige Lizenz besitzen, wenden Sie sich an Ihren NetApp Ansprechpartner, um eine vollständige Lizenz und eine Seriennummer zu erhalten. Sie können die Astra Control Center-UI oder verwenden "Astra Control API" Um eine vorhandene Lizenz zu aktualisieren.

Schritte

1. Melden Sie sich bei an "NetApp Support Website".
2. Rufen Sie die Download-Seite des Astra Control Center auf, geben Sie die Seriennummer ein und laden Sie die vollständige NetApp Lizenzdatei (NLF) herunter.
3. Melden Sie sich in der UI des Astra Control Center an.
4. Wählen Sie in der linken Navigationsleiste **Konto** > **Lizenz**.
5. Wählen Sie auf der Seite **Konto** > **Lizenz** das Dropdown-Menü Status der vorhandenen Lizenz aus und wählen Sie **Replace**.
6. Navigieren Sie zu der Lizenzdatei, die Sie heruntergeladen haben.
7. Wählen Sie **Hinzufügen**.

Auf der Seite **Konto** > **Lizenzen** werden Lizenzinformationen, Ablaufdatum, Lizenzseriennummer, Konto-ID und verwendete CPU-Einheiten angezeigt.

Finden Sie weitere Informationen

- "Astra Control Center-Lizenzierung"

Buckets verwalten

Ein Objektspeicher-Bucket-Provider ist äußerst wichtig, wenn Sie Ihre Applikationen und Ihren persistenten Storage sichern möchten oder Applikationen über Cluster hinweg klonen möchten. Fügen Sie mithilfe des Astra Control Center einen Objektspeicher-Provider als externes Backup-Ziel für Ihre Applikationen hinzu.

Sie benötigen keinen Bucket, wenn Sie die Applikationskonfiguration und Ihren persistenten Storage auf dasselbe Cluster klonen.

Verwenden Sie einen der folgenden Amazon Simple Storage Service (S3) Bucket-Provider:

- NetApp ONTAP S3
- NetApp StorageGRID S3
- Microsoft Azure
- Allgemein S3

> Amazon Web Services (AWS) und Google Cloud Platform (GCP) verwenden den Bucket-Typ Generic S3.

> Obwohl Astra Control Center Amazon S3 als Generic S3 Bucket-Provider unterstützt, unterstützt Astra Control Center unter Umständen nicht alle Objektspeicher-Anbieter, die die Unterstützung von Amazon S3 beanspruchen.

Ein Bucket kann sich in einem dieser Zustände befinden:

- Ausstehend: Der Bucket ist für die Erkennung geplant.
- Verfügbar: Der Bucket ist zur Verwendung verfügbar.
- Entfernt: Der Bucket ist derzeit nicht zugänglich.

Anweisungen zum Verwalten von Buckets mithilfe der Astra Control API finden Sie im "Astra Automation und API-Informationen".

Sie können die folgenden Aufgaben zum Verwalten von Buckets ausführen:

- "Fügen Sie einen Bucket hinzu"
- Bearbeiten eines Buckets
- Legen Sie den Standard-Bucket fest
- Bucket-Anmeldedaten drehen oder entfernen
- Entfernen Sie einen Bucket

> 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.

Bearbeiten eines Buckets

Sie können die Zugangsdaten für einen Bucket ändern und ändern, ob ein ausgewählter Bucket der Standard-Bucket ist.

> Wenn Sie einen Bucket hinzufügen, wählen Sie den richtigen Bucket-Provider aus und geben die richtigen Anmeldedaten für diesen Provider an. 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. Siehe "Versionshinweise".

Schritte

1. Wählen Sie in der linken Navigationsleiste **Buckets** aus.
2. Wählen Sie im Menü in der Spalte **Aktionen** die Option **Bearbeiten**.

3. Ändern Sie alle Informationen außer dem Bucket-Typ.

   Sie können den Bucket-Typ nicht ändern.

4. Wählen Sie **Aktualisieren**.

Legen Sie den Standard-Bucket fest

Wenn Sie einen Cluster-übergreifenden Klon durchführen, benötigt Astra Control einen Standard-Bucket. Führen Sie diese Schritte aus, um einen Standard-Bucket für alle Cluster festzulegen.

Schritte

1. Gehen Sie zu **Cloud-Instanzen**.
2. Wählen Sie das Menü in der Spalte **Aktionen** für die Cloud-Instanz in der Liste aus.
3. Wählen Sie **Bearbeiten**.
4. Wählen Sie in der Liste **Bucket** den Bucket aus, der als Standard verwendet werden soll.
5. Wählen Sie **Speichern**.

Bucket-Anmeldedaten drehen oder entfernen

Astra Control verwendet Bucket-Zugangsdaten, um Zugriff zu erhalten und geheime Schlüssel für einen S3-Bucket bereitzustellen, damit Astra Control Center mit dem Bucket kommunizieren kann.

Bucket-Anmeldedaten rotieren

Wenn Sie die Anmeldeinformationen drehen, drehen Sie sie während eines Wartungsfensters, wenn keine Backups ausgeführt werden (geplant oder auf Anforderung).

Schritte zum Bearbeiten und Drehen von Anmeldeinformationen

1. Wählen Sie in der linken Navigationsleiste **Buckets** aus.
2. Wählen Sie im Menü Optionen in der Spalte **Aktionen** die Option **Bearbeiten** aus.
3. Erstellen Sie die neuen Anmeldedaten.
4. Wählen Sie **Aktualisieren**.

Bucket-Anmeldedaten entfernen

Sie sollten die Bucket-Anmeldedaten nur entfernen, wenn auf einen Bucket neue Zugangsdaten angewendet wurden oder der Bucket nicht mehr aktiv verwendet wird.

Der erste Satz von Anmeldeinformationen, die Sie Astra Control hinzufügen, wird immer verwendet, da Astra Control zur Authentifizierung des Backup-Buckets die Zugangsdaten verwendet. Entfernen Sie diese Anmeldedaten nicht, wenn der Bucket aktiv ist, da dies zu Backup-Ausfällen und Nichtverfügbarkeit von Backups führen kann.

Wenn Sie die aktiven Bucket-Anmeldedaten entfernen, finden Sie unter "Fehlerbehebung beim Entfernen der Bucket-Anmeldeinformationen".

Anweisungen zum Entfernen von S3-Anmeldeinformationen mithilfe der Astra Control API finden Sie im "Astra Automation und API-Informationen".

Entfernen Sie einen Bucket

Sie können einen Eimer entfernen, der nicht mehr verwendet wird oder nicht ordnungsgemäß ist. Dies könnte Sie nutzen, um die Konfiguration Ihres Objektspeicher einfach und aktuell zu halten.

- Sie können keinen Standard-Bucket entfernen. Wenn Sie diesen Bucket entfernen möchten, wählen Sie zuerst einen anderen Bucket als Standard aus.
- Sie können einen WORM-Bucket (Write Once Read Many) nicht entfernen, bevor die Aufbewahrungsfrist des Cloud-Providers abgelaufen ist. WORM-Buckets werden neben dem Bucket-Namen mit „gesperrt“ gekennzeichnet.

- Sie können keinen Standard-Bucket entfernen. Wenn Sie diesen Bucket entfernen möchten, wählen Sie zuerst einen anderen Bucket als Standard aus.

Bevor Sie beginnen

- Sie sollten vor Beginn sicherstellen, dass keine Backups für diesen Bucket ausgeführt oder abgeschlossen wurden.
- Sie sollten prüfen, ob der Bucket nicht in einer aktiven Schutzrichtlinie verwendet wird.

Wenn dies der Fall ist, können Sie nicht fortfahren.

Schritte

1. Wählen Sie in der linken Navigationsleiste **Buckets** aus.
2. Wählen Sie im Menü **Aktionen** die Option **Entfernen**.

   Astra Control stellt zunächst sicher, dass es keine Planungsrichtlinien gibt, die den Bucket für Backups verwenden und dass keine aktiven Backups im Bucket vorhanden sind, den Sie entfernen möchten.

3. Geben Sie „Entfernen“ ein, um die Aktion zu bestätigen.
4. Wählen Sie **Ja, entfernen Sie den Eimer**.

Weitere Informationen

- "Verwenden Sie die Astra Control API"

Management des Storage-Backends

Durch das Management von Storage-Clustern in Astra Control als Storage-Backend können Sie Verbindungen zwischen persistenten Volumes (PVS) und dem Storage-Backend sowie zusätzliche Storage-Kennzahlen abrufen. Sie können Storage-Kapazität und -Integritätsdetails überwachen, beispielsweise die Performance, wenn Astra Control Center mit Cloud Insights verbunden ist.

Eine Anleitung zum Managen von Storage-Back-Ends mithilfe der Astra Control API finden Sie im "Astra Automation und API-Informationen".

Sie können die folgenden Aufgaben zur Verwaltung eines Storage-Backends ausführen:

- "Fügen Sie ein Storage-Back-End hinzu"
- Details zum Storage-Back-End
- Bearbeiten Sie die Details der Storage-Back-End-Authentifizierung
- Management eines erkannten Storage-Backends
- Unmanagement eines Storage-Backends
- Entfernen Sie ein Speicher-Back-End

Details zum Storage-Back-End

Sie können Speicher-Backend-Informationen über das Dashboard oder über die Option Back-Ends anzeigen.

Details zum Storage-Back-End können Sie über das Dashboard anzeigen

Schritte

1. Wählen Sie in der linken Navigationsleiste **Dashboard** aus.
2. Überprüfen Sie den Back-End-Bereich Speicher des Dashboards, der den Status anzeigt:
   - **Ungesund**: Die Lagerung befindet sich nicht im optimalen Zustand. Dies kann durch ein Latenzproblem oder eine Applikation aufgrund eines Container-Problems, z. B., beeinträchtigt sein.
   - **Alles gesund**: Die Lagerung wurde verwaltet und ist in einem optimalen Zustand.
   - **Entdeckt**: Der Speicher wurde entdeckt, aber nicht von Astra Control verwaltet.

Details zum Speicher-Backend über die Option „Backend“ anzeigen

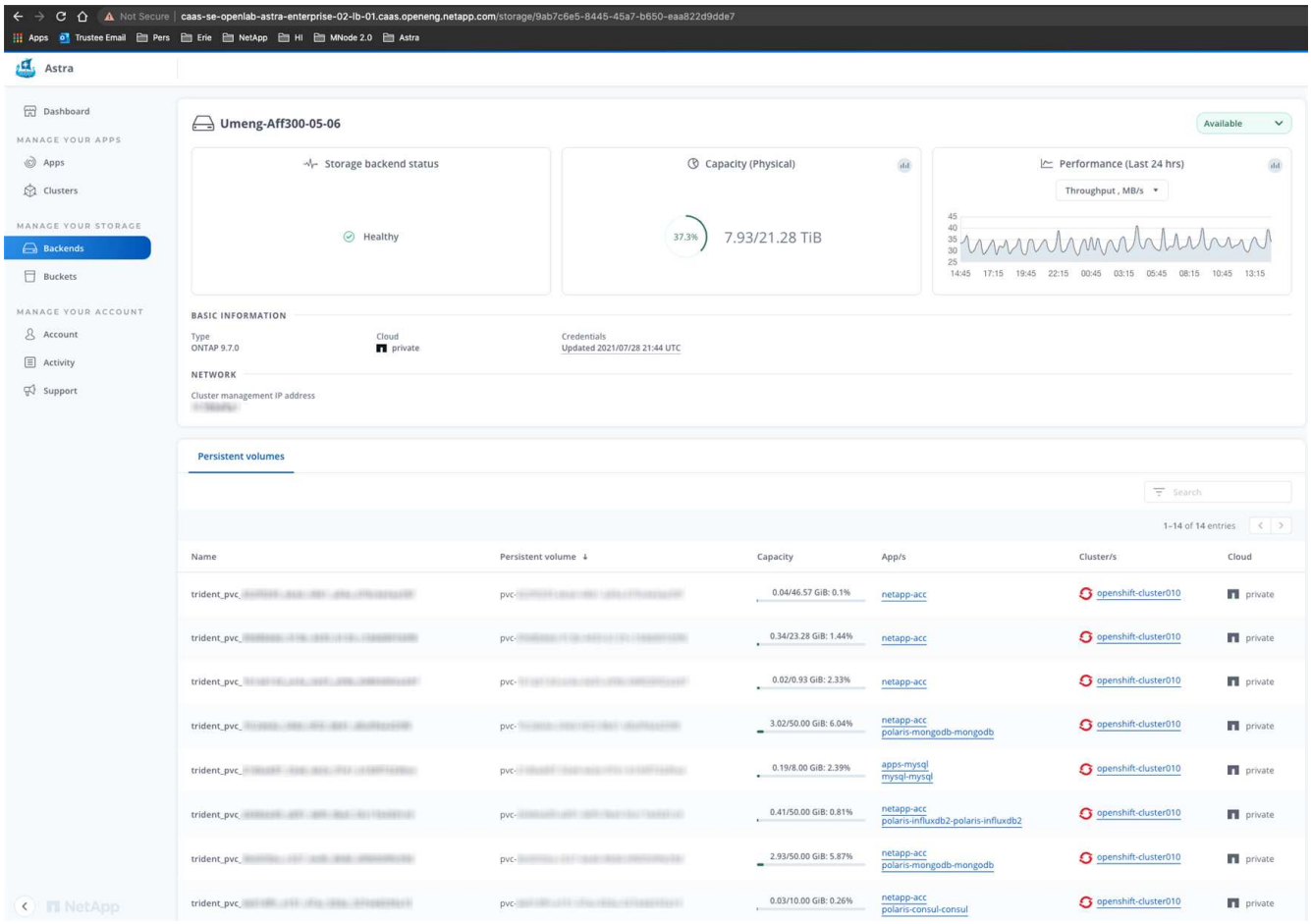
Informationen zum Zustand, Kapazität und Performance des Backend (IOPS-Durchsatz und/oder Latenz)

Sie sehen die Volumes, die die Kubernetes-Apps verwenden, die in einem ausgewählten Storage-Backend gespeichert sind. Mit Cloud Insights werden zusätzliche Informationen angezeigt. Siehe "Cloud Insights-Dokumentation".

Schritte

1. Wählen Sie im linken Navigationsbereich **Backend** aus.
2. Wählen Sie das Storage-Back-End aus.

Wenn Sie eine Verbindung zum NetApp Cloud Insights hergestellt haben, werden auf der Seite „Back-Ends“ Auszüge aus Cloud Insights angezeigt.



3. Um direkt zu Cloud Insights zu gelangen, wählen Sie neben dem Kennzahlenbild das Symbol **Cloud Insights** aus.

Bearbeiten Sie die Details der Storage-Back-End-Authentifizierung

Astra Control Center bietet zwei Arten der Authentifizierung eines ONTAP-Backends.

- **Credential-basierte Authentifizierung**: Der Benutzername und das Passwort an einen ONTAP-Benutzer mit den erforderlichen Berechtigungen. Sie sollten eine vordefinierte Sicherheits-Login-Rolle wie admin verwenden, um maximale Kompatibilität mit ONTAP-Versionen zu gewährleisten.
- **Zertifikatbasierte Authentifizierung**: Astra Control Center kann auch mit einem ONTAP-Cluster kommunizieren, indem ein auf dem Backend installiertes Zertifikat verwendet wird. Verwenden Sie gegebenenfalls das Clientzertifikat, den Schlüssel und das Zertifikat der vertrauenswürdigen Zertifizierungsstelle (empfohlen).

Sie können vorhandene Back-Ends aktualisieren, um von einem Authentifizierungstyp zu einer anderen zu wechseln. Es wird jeweils nur eine Authentifizierungsmethode unterstützt.

Weitere Informationen zum Aktivieren der zertifikatbasierten Authentifizierung finden Sie unter "Aktivieren Sie die Authentifizierung auf dem ONTAP Storage Back-End".

Schritte

1. Wählen Sie in der linken Navigationsleiste **Backend** aus.
2. Wählen Sie das Storage-Back-End aus.

3. Wählen Sie im Feld Anmeldeinformationen das Symbol **Bearbeiten** aus.
4. Wählen Sie auf der Seite Bearbeiten eine der folgenden Optionen aus.
   - **Administrator-Anmeldeinformationen verwenden**: Geben Sie die ONTAP Cluster Management IP-Adresse und die Admin-Anmeldeinformationen ein. Die Anmeldedaten müssen Cluster-weite Anmeldedaten aufweisen.

     Der Benutzer, dessen Anmeldeinformationen Sie hier eingeben, muss über den verfügen `ontapi` Aktivieren der Zugriffsmethode für die Anmeldung beim Benutzer in ONTAP System Manager auf dem ONTAP Cluster. Wenn Sie Vorhaben, SnapMirror Replizierung zu verwenden, wenden Sie Benutzeranmeldeinformationen auf die Rolle „Admin“ an, die über die Zugriffsmethoden verfügt `ontapi` Und `http`, Auf Quell- und Ziel-ONTAP Clustern. Siehe "Managen von Benutzerkonten in der ONTAP Dokumentation" Finden Sie weitere Informationen.

   - **Ein Zertifikat** verwenden: Das Zertifikat hochladen `.pem` Datei, dem Zertifikatschlüssel `.key` Datei und optional die Zertifizierungsdatei.
5. Wählen Sie **Speichern**.

Management eines erkannten Storage-Backends

Sie können auswählen, wie ein nicht verwaltetes, aber dennoch ermitteltes Storage-Back-End verwaltet werden soll. Wenn Sie ein Storage-Backend verwalten, gibt Astra Control an, ob ein Authentifizierungszertifikat abgelaufen ist.

Schritte

1. Wählen Sie in der linken Navigationsleiste **Backend** aus.
2. Wählen Sie die Option **entdeckt**.
3. Wählen Sie das Storage-Back-End aus.
4. Wählen Sie im Menü Optionen in der Spalte **Aktionen Verwalten** aus.
5. Nehmen Sie die Änderungen vor.
6. Wählen Sie **Speichern**.

Unmanagement eines Storage-Backends

Sie können das Backend verwalten.

Schritte

1. Wählen Sie in der linken Navigationsleiste **Backend** aus.
2. Wählen Sie das Storage-Back-End aus.
3. Wählen Sie im Menü Optionen in der Spalte **Aktionen** die Option **Verwaltung aufheben** aus.
4. Geben Sie „unverwalten“ ein, um die Aktion zu bestätigen.
5. Wählen Sie **Ja, verwalten Sie das Speicher-Backend**.

Entfernen Sie ein Speicher-Back-End

Sie können ein nicht mehr verwendenden Storage-Back-End entfernen. Nutzen Sie dies, um Ihre Konfiguration auf dem neuesten Stand zu halten.

Bevor Sie beginnen

- Stellen Sie sicher, dass das Storage-Back-End nicht gemanagt wird.
- Stellen Sie sicher, dass dem Cluster keine Volumes im Speicher-Backend zugewiesen sind.

Schritte

1. Wählen Sie in der linken Navigationsleiste **Backend** aus.
2. Wenn das Backend verwaltet wird, managen Sie es rückgängig.
   a. Wählen Sie **Verwaltet**.
   b. Wählen Sie das Storage-Back-End aus.
   c. Wählen Sie in der Option **actions Unmanage** aus.
   d. Geben Sie „unverwalten“ ein, um die Aktion zu bestätigen.
   e. Wählen Sie **Ja, verwalten Sie das Speicher-Backend**.
3. Wählen Sie **Entdeckt**.
   a. Wählen Sie das Storage-Back-End aus.
   b. Wählen Sie in der Option **actions** die Option **Remove** aus.
   c. Geben Sie „Entfernen“ ein, um die Aktion zu bestätigen.
   d. Wählen Sie **Ja, Speicher-Backend entfernen**.

Weitere Informationen

- "Verwenden Sie die Astra Control API"

Überwachen Sie laufende Aufgaben

Sie können Details über die Ausführung von Aufgaben und Aufgaben anzeigen, die in den letzten 24 Stunden in Astra Control abgeschlossen, fehlgeschlagen oder abgebrochen wurden. Beispielsweise können Sie den Status eines laufenden Backups, Restores oder Klonvorgangs anzeigen, und Details wie den Prozentsatz abgeschlossen und die geschätzte verbleibende Zeit angezeigt werden. Sie können den Status eines geplanten Vorgangs anzeigen, der ausgeführt wurde, oder einen manuell gestarteten Vorgang.

Während Sie eine laufende oder abgeschlossene Aufgabe anzeigen, können Sie die Aufgabendetails erweitern, um den Status der einzelnen Unteraufgaben anzuzeigen. Die Fortschrittsleiste der Aufgabe ist grün für laufende oder abgeschlossene Aufgaben, blau für stornierte Aufgaben und rot für Aufgaben, die aufgrund eines Fehlers fehlgeschlagen sind.

Bei Klonvorgängen bestehen die Unteraufgaben der Aufgabe aus einem Snapshot und einem Snapshot-Wiederherstellungsvorgang.

Weitere Informationen zu fehlgeschlagenen Aufgaben finden Sie unter "Überwachen der Kontoaktivität".

Schritte

1. Während eine Aufgabe ausgeführt wird, gehen Sie zu **Anwendungen**.

2. Wählen Sie den Namen einer Anwendung aus der Liste aus.
3. Wählen Sie in den Details der Anwendung die Registerkarte **Aufgaben** aus.

   Sie können Details zu aktuellen oder früheren Aufgaben anzeigen und nach Aufgabenstatus filtern.

Aufgaben werden bis zu 24 Stunden in der Liste **Aufgaben** aufbewahrt. Sie können diese Begrenzung und andere Einstellungen für die Aufgabenüberwachung mit dem konfigurieren "Astra Control API".

Infrastruktur mit Cloud Insights-, Prometheus- oder Fluentd-Verbindungen überwachen

Sie können mehrere optionale Einstellungen konfigurieren, um Ihre Astra Control Center-Erfahrung zu verbessern. Um Ihre komplette Infrastruktur zu überwachen und Erkenntnisse zu erhalten, stellen Sie eine Verbindung zu NetApp Cloud Insights her, konfigurieren Sie Prometheus oder fügen Sie eine Fluentd-Verbindung hinzu.

Wenn das Netzwerk, in dem Astra Control Center ausgeführt wird, einen Proxy für die Verbindung zum Internet benötigt (um Support-Bundles auf die NetApp Support Site hochzuladen oder eine Verbindung zu Cloud Insights herzustellen), sollten Sie einen Proxy Server in Astra Control Center konfigurieren.

- Verbinden Sie sich mit Cloud Insights
- Verbinden Sie sich mit Prometheus
- Mit Fluentd verbinden

Fügen Sie einen Proxy-Server für Verbindungen zu Cloud Insights oder zur NetApp Support-Website hinzu

Wenn das Netzwerk, in dem Astra Control Center ausgeführt wird, einen Proxy für die Verbindung zum Internet benötigt (um Support-Bundles auf die NetApp Support Site hochzuladen oder eine Verbindung zu Cloud Insights herzustellen), sollten Sie einen Proxy Server in Astra Control Center konfigurieren.

Astra Control Center überprüft nicht die von Ihnen eingegebenen Details für Ihren Proxy-Server. Stellen Sie sicher, dass Sie korrekte Werte eingeben.

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Verbinden** aus, um einen Proxyserver hinzuzufügen.

4. Geben Sie den Proxy-Servernamen oder die IP-Adresse und die Proxy-Portnummer ein.
5. Wenn Ihr Proxy-Server eine Authentifizierung erfordert, aktivieren Sie das Kontrollkästchen, und geben Sie den Benutzernamen und das Kennwort ein.
6. Wählen Sie **Verbinden**.

Ergebnis

Wenn die eingegebenen Proxydaten gespeichert wurden, zeigt der Abschnitt **HTTP Proxy** der Seite **Konto** > **Verbindungen** an, dass sie verbunden sind, und zeigt den Servernamen an.

Proxy-Server-Einstellungen bearbeiten

Sie können die Proxy-Server-Einstellungen bearbeiten.

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie **Bearbeiten** aus der Dropdown-Liste, um die Verbindung zu bearbeiten.
4. Bearbeiten Sie die Serverdetails und die Authentifizierungsinformationen.
5. Wählen Sie **Speichern**.

Deaktivieren Sie die Proxy-Serververbindung

Sie können die Proxy-Server-Verbindung deaktivieren. Bevor Sie diese Option deaktivieren, werden Sie gewarnt, dass mögliche Unterbrechungen bei anderen Verbindungen auftreten können.

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Trennen** aus, um die Verbindung zu deaktivieren.
4. Bestätigen Sie im Dialogfeld, das geöffnet wird, den Vorgang.

Verbinden Sie sich mit Cloud Insights

Überwachen Sie Ihre komplette Infrastruktur, und verschaffen Sie sich so einen Überblick über Ihre komplette Infrastruktur. Verbinden Sie NetApp Cloud Insights mit Ihrer Astra Control Center Instanz. Cloud Insights ist in Ihrer Astra Control Center-Lizenz enthalten.

Cloud Insights sollte über das Netzwerk, das Astra Control Center verwendet, oder indirekt über einen Proxy-Server zugänglich sein.

Wenn Astra Control Center mit Cloud Insights verbunden ist, wird ein Pod für die Akquisitionseinheit erstellt. Dieser POD sammelt Daten aus den Storage-Back-Ends, die vom Astra Control Center gemanagt werden, und schiebt diese an Cloud Insights. Dieser POD benötigt 8 GB RAM und 2 CPU-Kerne.

Wenn Astra Control Center mit Cloud Insights gekoppelt ist, sollten Sie die Option **Bereitstellung ändern** in Cloud Insights nicht verwenden.

Nachdem Sie die Cloud Insights-Verbindung aktiviert haben, können Sie die Durchsatzinformationen auf der Seite **Backends** anzeigen sowie nach Auswahl eines Storage-Backends eine Verbindung zu Cloud Insights herstellen. Sie können auch die Informationen im **Dashboard** im Bereich Cluster finden und sich von dort mit Cloud Insights verbinden.

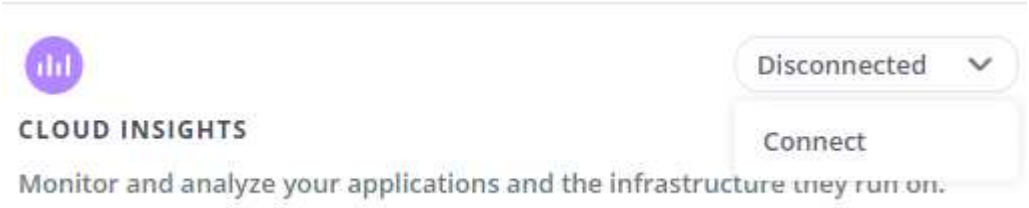
Bevor Sie beginnen

- Ein Astra Control Center-Konto mit **admin**/**Owner** Privilegien.
- Eine gültige Astra Control Center-Lizenz.
- Ein Proxy-Server, wenn das Netzwerk, in dem Sie Astra Control Center verwenden, einen Proxy für die Verbindung zum Internet benötigt.

Falls Sie neu bei Cloud Insights sind, sollten Sie sich mit den Funktionen und Features vertraut machen. Siehe "Cloud Insights-Dokumentation".

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Verbinden**, wo es **getrennt** angezeigt wird, um die Verbindung hinzuzufügen.



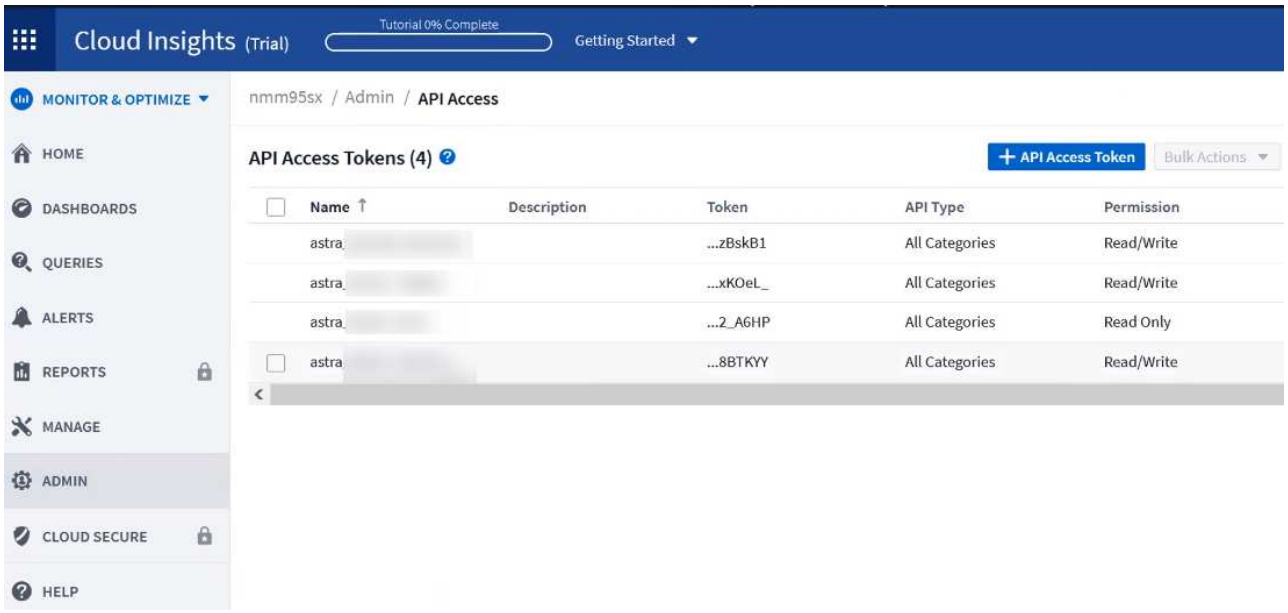
4. Geben Sie die Cloud Insights-API-Token und die Mandanten-URL ein. Die Mandanten-URL weist beispielsweise das folgende Format auf:

```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

Sie erhalten die Mandanten-URL, wenn Sie die Cloud Insights-Lizenz erhalten. Wenn die Mandanten-URL nicht vorhanden ist, lesen Sie den "Cloud Insights-Dokumentation".

a. Um die zu bekommen "API-Token", Loggen Sie sich bei Ihrer Cloud Insights-Mandanten-URL ein.

b. Generieren Sie in Cloud Insights durch Klicken auf **Admin** > **API-Zugriff** sowohl ein **Lesen/Schreiben** als auch ein **schreibgeschütztes** API-Zugriffstoken.



c. Kopieren Sie die Taste * nur Lesen*. Sie müssen es in das Fenster Astra Control Center einfügen, um die Cloud Insights-Verbindung zu aktivieren. Wählen Sie für die Hauptberechtigungen Lese-API-Zugriffstoken die Option Assets, Alerts, Acquisition Unit und Data Collection aus.

d. Kopieren Sie die Taste **Lesen/Schreiben**. Sie müssen es in das Astra Control Center **Connect Cloud Insights** Fenster einfügen. Wählen Sie für die Hauptberechtigungen Lese-/Schreib-API-Zugriffstoken die Option Datenaufnahme, Protokollaufnahme, Erfassungseinheit und Datenerfassung aus.

> Wir empfehlen Ihnen, einen **Read Only**-Schlüssel und einen **Read/Write**-Schlüssel zu generieren und nicht den gleichen Schlüssel für beide Zwecke zu verwenden. Standardmäßig ist der Ablauf des Tokens auf ein Jahr festgelegt. Wir empfehlen, dass Sie die Standardauswahl beibehalten, um dem Token die maximale Dauer zu geben, bevor es abläuft. Wenn Ihr Token abläuft, wird die Telemetrie angehalten.

e. Fügen Sie die Tasten ein, die Sie von Cloud Insights in Astra Control Center kopiert haben.

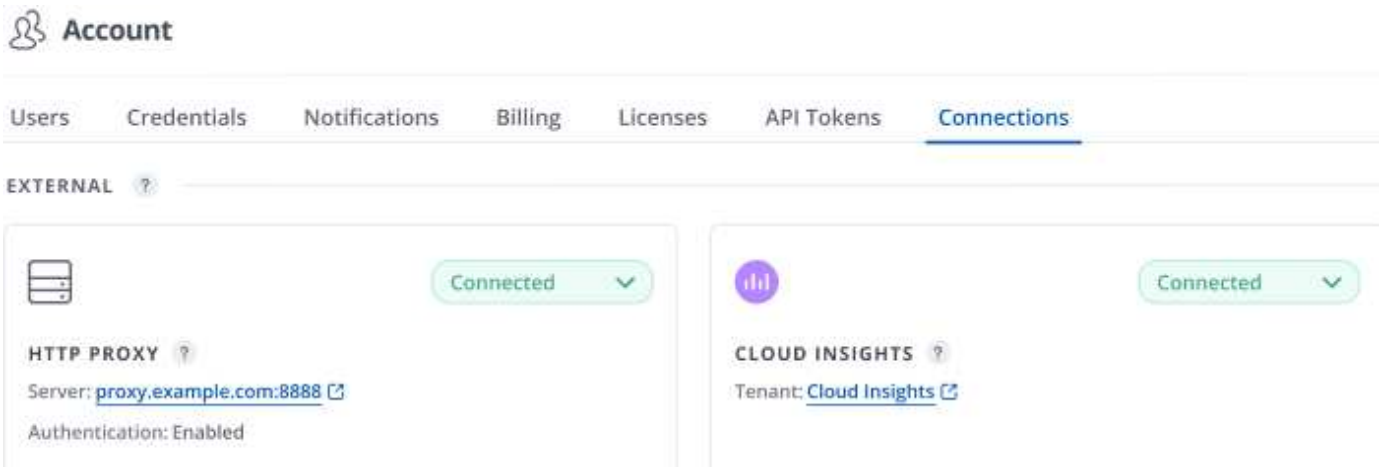
5. Wählen Sie **Verbinden**.

> Nach der Auswahl von **Verbinden** ändert sich der Status der Verbindung auf der Seite **Konto** > **Verbindungen** auf der Seite **Cloud Insights** auf **ausstehend**. Es kann einige Minuten dauern, bis die Verbindung aktiviert ist und der Status auf **verbunden** geändert wird.

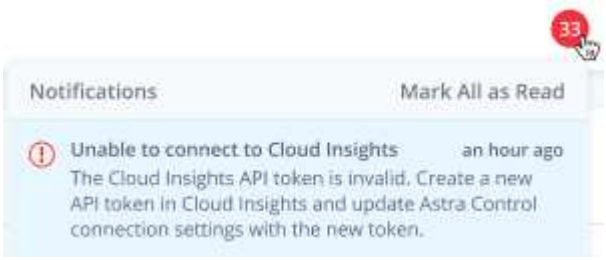
> Um zwischen dem Astra Control Center und den Cloud Insights UIs hin und her zu gehen, stellen Sie sicher, dass Sie bei beiden angemeldet sind.

Daten im Cloud Insights anzeigen

Wenn die Verbindung erfolgreich war, zeigt der Abschnitt **Cloud Insights** auf der Seite **Konto** > **Verbindungen** an, dass sie verbunden ist, und zeigt die Mandanten-URL an. Sie können Cloud Insights besuchen, um zu sehen, dass Daten erfolgreich empfangen und angezeigt werden.

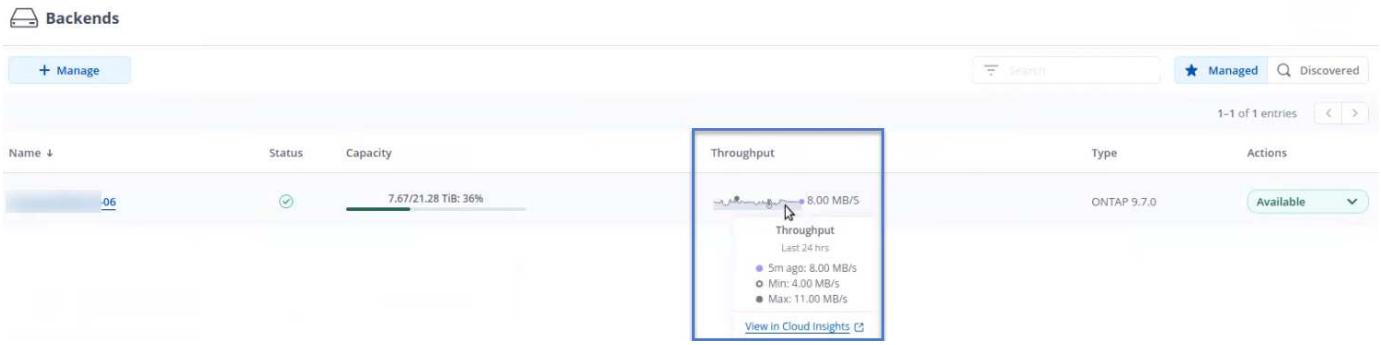


Wenn die Verbindung aus irgendeinem Grund fehlgeschlagen ist, wird im Status **failed** angezeigt. Den Grund für Fehlschlag finden Sie unter **Benachrichtigungen** auf der rechten oberen Seite des UI.



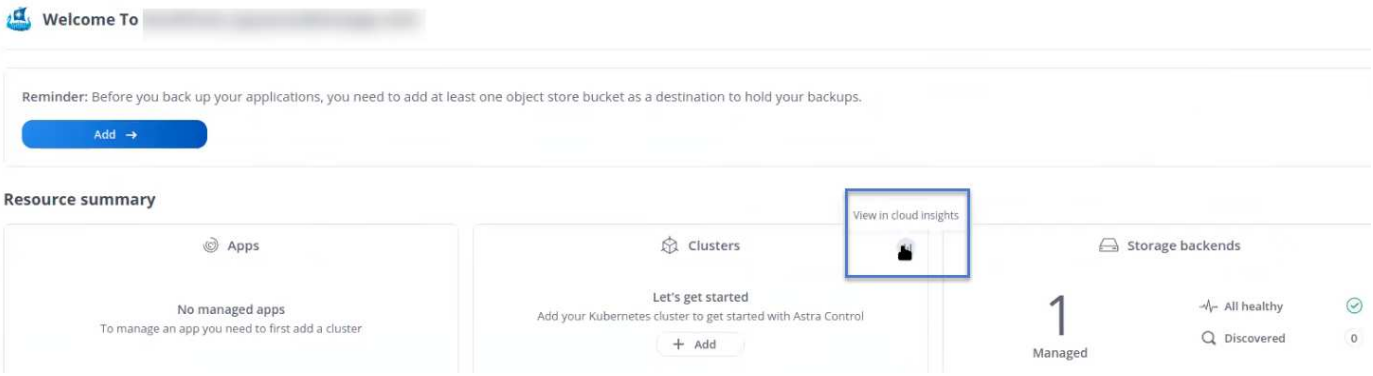
Die gleichen Informationen finden Sie auch unter **Konto** > **Benachrichtigungen**.

Vom Astra Control Center können Sie Durchsatzinformationen auf der Seite **Backend** anzeigen sowie von hier aus eine Verbindung zu Cloud Insights herstellen, nachdem Sie ein Storage-Backend ausgewählt haben.



Um direkt zu Cloud Insights zu gelangen, wählen Sie neben dem Kennzahlenbild das Symbol **Cloud Insights** aus.

Die Informationen finden Sie auch auf dem **Dashboard**.



Wenn Sie nach Aktivierung der Cloud Insights-Verbindung die Back-Ends entfernen, die Sie im Astra Control Center hinzugefügt haben, werden die Back-Ends nicht mehr an Cloud Insights gemeldet.

Cloud Insights-Verbindung bearbeiten

Sie können die Cloud Insights-Verbindung bearbeiten.

Sie können nur die API-Schlüssel bearbeiten. Um die Cloud Insights-Mandanten-URL zu ändern, sollten Sie die Cloud Insights-Verbindung trennen und eine Verbindung mit der neuen URL herstellen.

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie **Bearbeiten** aus der Dropdown-Liste, um die Verbindung zu bearbeiten.
4. Bearbeiten Sie die Cloud Insights-Verbindungseinstellungen.
5. Wählen Sie **Speichern**.

Deaktivieren Sie die Cloud Insights-Verbindung

Sie können die Cloud Insights-Verbindung für einen Kubernetes Cluster deaktivieren, der von Astra Control Center gemanagt wird. Wenn Sie die Cloud Insights-Verbindung deaktivieren, werden die bereits auf Cloud Insights hochgeladenen Telemetriedaten nicht gelöscht.

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Trennen** aus, um die Verbindung zu deaktivieren.
4. Bestätigen Sie im Dialogfeld, das geöffnet wird, den Vorgang.
   Nachdem Sie den Vorgang bestätigt haben, ändert sich der Cloud Insights-Status auf der Seite **Konto** > **Verbindungen** in **Ausstehend**. Es dauert ein paar Minuten, bis der Status in **nicht verbunden** geändert wird.

Verbinden Sie sich mit Prometheus

Sie können Astra Control Center Daten mit Prometheus überwachen. Sie können Prometheus so

konfigurieren, dass Kennzahlen vom Kubernetes Cluster-Metriken-Endpunkt erfasst werden, und Sie können Prometheus auch zur Visualisierung der Kennzahlendaten verwenden.

Weitere Informationen zur Verwendung von Prometheus finden Sie in der Dokumentation unter "Erste Schritte mit Prometheus".

Was Sie benötigen

Stellen Sie sicher, dass Sie das Prometheus-Paket auf dem Astra Control Center-Cluster oder einem anderen Cluster heruntergeladen und installiert haben, der mit dem Astra Control Center-Cluster kommunizieren kann.

Befolgen Sie die Anweisungen in der offiziellen Dokumentation zu "Installation Von Prometheus".

Prometheus muss in der Lage sein, mit dem Astra Control Center Kubernetes Cluster zu kommunizieren. Wenn Prometheus nicht auf dem Astra Control Center Cluster installiert ist, müssen Sie sicherstellen, dass sie mit dem Kennzahlendienst kommunizieren können, der auf dem Astra Control Center Cluster ausgeführt wird.

Konfigurieren Sie Prometheus

Astra Control Center stellt einen Kennzahlungsservice für TCP-Port 9090 im Kubernetes-Cluster bereit. Sie müssen Prometheus konfigurieren, um Kennzahlen aus diesem Service zu sammeln.

Schritte

1. Melden Sie sich beim Prometheus-Server an.
2. Fügen Sie den Cluster-Eintrag in das hinzu `prometheus.yml` Datei: Im `yml` Fügen Sie im einen Eintrag wie der folgende für Ihr Cluster hinzu `scrape_configs section`:

```
job_name: '<Add your cluster name here. You can abbreviate. It just
needs to be a unique name>'
  metrics_path: /accounts/<replace with your account ID>/metrics
  authorization:
     credentials: <replace with your API token>
  tls_config:
     insecure_skip_verify: true
  static_configs:
    - targets: ['<replace with your astraAddress. If using FQDN, the
prometheus server has to be able to resolve it>']
```

> Wenn Sie die einstellen `tls_config insecure_skip_verify` Bis `true`, Das TLS-Verschlüsselungsprotokoll ist nicht erforderlich.

3. Starten Sie den Prometheus-Service neu:

```
sudo systemctl restart prometheus
```

Zugang Prometheus

Rufen Sie die Prometheus-URL auf.

Schritte

1. Geben Sie in einem Browser die Prometheus-URL mit Port 9090 ein.
2. Überprüfen Sie Ihre Verbindung, indem Sie **Status** > **Ziele** wählen.

Daten in Prometheus anzeigen

Sie können Prometheus verwenden, um Astra Control Center-Daten anzuzeigen.

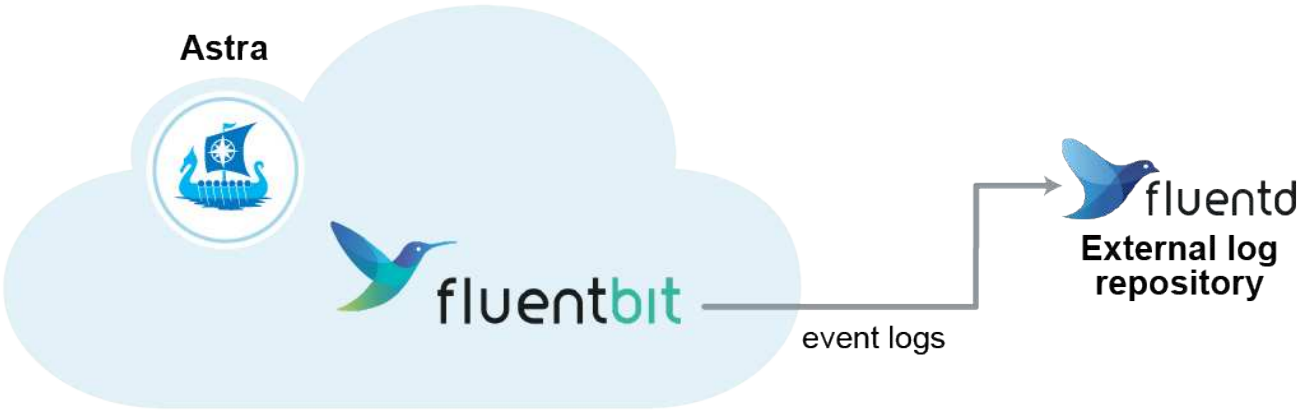
Schritte

1. Geben Sie in einem Browser die Prometheus-URL ein.
2. Wählen Sie im Menü Prometheus die Option **Grafik** aus.
3. Um den Metrics Explorer zu verwenden, wählen Sie das Symbol neben **Ausführen** aus.
4. Wählen Sie `scrape_samples_scraped` Und wählen Sie **Ausführen**.
5. Wenn Sie das Scraping von Proben im Laufe der Zeit anzeigen möchten, wählen Sie **Grafik**.

Wenn mehrere Cluster-Daten erfasst wurden, werden die Metriken jedes Clusters in einer anderen Farbe angezeigt.

Mit Fluentd verbinden

Sie können Protokolle (Kubernetes-Ereignisse) von einem System, das von Astra Control Center überwacht wird, an Ihren Fluentd-Endpunkt senden. Die Fluentd-Verbindung ist standardmäßig deaktiviert.



Nur die Ereignisprotokolle von verwalteten Clustern werden an Fluentd weitergeleitet.

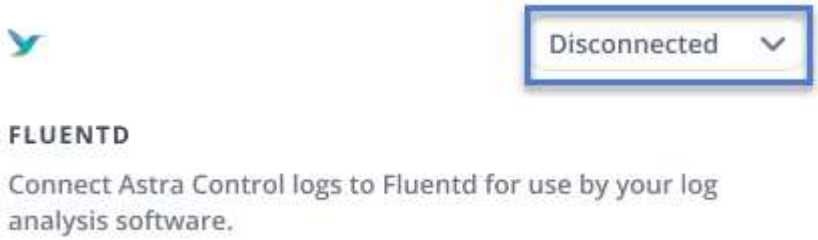
Bevor Sie beginnen

- Ein Astra Control Center-Konto mit **admin**/**Owner** Privilegien.
- Astra Control Center ist auf einem Kubernetes-Cluster installiert und läuft.

Astra Control Center überprüft nicht die Details, die Sie für Ihren Fluentd-Server eingeben. Stellen Sie sicher, dass Sie die richtigen Werte eingeben.

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **nicht verbunden** aus, um die Verbindung hinzuzufügen.



4. Geben Sie die Host-IP-Adresse, die Portnummer und den freigegebenen Schlüssel für Ihren Fluentd-Server ein.
5. Wählen Sie **Verbinden**.

Ergebnis

Wenn die für den Fluentd-Server eingegebenen Details gespeichert wurden, zeigt der Abschnitt **Fluentd** auf der Seite **Konto** > **Verbindungen** an, dass er verbunden ist. Jetzt können Sie den Fluentd-Server besuchen, mit dem Sie verbunden sind, und die Ereignisprotokolle anzeigen.

Wenn die Verbindung aus irgendeinem Grund fehlgeschlagen ist, wird im Status **failed** angezeigt. Den Grund für Fehlschlag finden Sie unter **Benachrichtigungen** auf der rechten oberen Seite des UI.

Die gleichen Informationen finden Sie auch unter **Konto** > **Benachrichtigungen**.

Wenn Sie Probleme mit der Protokollerfassung haben, sollten Sie sich bei Ihrem Worker-Knoten anmelden und sicherstellen, dass Ihre Protokolle in verfügbar sind `/var/log/containers/`.

Bearbeiten Sie die Fluentd-Verbindung

Sie können die Fluentd-Verbindung zu Ihrer Astra Control Center-Instanz bearbeiten.

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie **Bearbeiten** aus der Dropdown-Liste, um die Verbindung zu bearbeiten.
4. Ändern Sie die Einstellungen für den Fluentd-Endpunkt.
5. Wählen Sie **Speichern**.

Deaktivieren Sie die Fluentd-Verbindung

Sie können die Fluentd-Verbindung zu Ihrer Astra Control Center-Instanz deaktivieren.

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Trennen** aus, um die Verbindung zu deaktivieren.

4. Bestätigen Sie im Dialogfeld, das geöffnet wird, den Vorgang.

Heben Sie das Management von Applikationen und Clustern auf

Entfernen Sie alle Apps oder Cluster, die Sie nicht mehr über das Astra Control Center managen möchten.

Verwaltung einer Anwendung aufheben

Sie müssen nicht mehr Apps managen, die Sie nicht mehr Backups, Snapshots oder Klone von Astra Control Center erstellen möchten.

Wenn Sie die Verwaltung einer Anwendung aufheben:

- Alle bestehenden Backups und Snapshots werden gelöscht.
- Applikationen und Daten sind weiterhin verfügbar.

Schritte

1. Wählen Sie in der linken Navigationsleiste die Option **Anwendungen**.
2. Wählen Sie die App aus.
3. Wählen Sie im Menü Optionen in der Spalte Aktionen die Option **Verwaltung aufheben** aus.
4. Überprüfen Sie die Informationen.
5. Geben Sie zur Bestätigung „nicht verwalten“ ein.
6. Wählen Sie **Ja, Anwendung verwalten** aus.

Ergebnis

Astra Control Center beendet die Verwaltung der App.

Aufheben des Managements eines Clusters

Sie müssen den Cluster nicht mehr über das Astra Control Center managen.

> Bevor Sie das Management des Clusters aufheben, sollten Sie die dem Cluster zugeordnete Applikationen aufheben.

Wenn Sie das Management eines Clusters aufheben:

- Dadurch wird das Management des Clusters durch das Astra Control Center verhindert. Die Konfiguration des Clusters ändert sich nicht, und das Cluster wird nicht gelöscht.
- Astra Trident wird nicht vom Cluster deinstalliert. "Erfahren Sie, wie Sie Astra Trident deinstallieren".

Schritte

1. Wählen Sie in der linken Navigationsleiste **Cluster** aus.
2. Aktivieren Sie das Kontrollkästchen für den Cluster, den Sie nicht mehr managen möchten.
3. Wählen Sie im Menü Optionen in der Spalte **Aktionen** die Option **Verwaltung aufheben** aus.

4. Bestätigen Sie, dass Sie die Verwaltung des Clusters aufheben möchten und wählen Sie dann **Ja, Cluster verwalten** aus.

Ergebnis

Der Status des Clusters ändert sich in **Entfernen**. Danach wird der Cluster aus der Seite **Cluster** entfernt und wird nicht mehr vom Astra Control Center verwaltet.

Wenn Astra Control Center und Cloud Insights nicht verbunden sind, entfernt die Unverwaltung des Clusters alle Ressourcen, die zum Senden von Telemetriedaten installiert wurden. **Wenn Astra Control Center und Cloud Insights verbunden sind**, löscht die Entsteuerung des Clusters nur das `fluentbit` Und `event-exporter` Behälter.

Upgrade Astra Control Center

Laden Sie zum Upgrade des Astra Control Center das Installationspaket von der NetApp Support Site herunter, und füllen Sie die folgenden Anweisungen aus. Mit diesem Verfahren können Sie das Astra Control Center in internetverbundenen oder luftgekapderten Umgebungen aktualisieren.

Diese Anweisungen beschreiben den Upgrade-Prozess für Astra Control Center von der zweitneuesten Version auf diese aktuelle Version. Sie können kein direktes Upgrade von einer Version durchführen, die zwei oder mehr Versionen hinter der aktuellen Version enthält. Wenn Ihre installierte Astra Control Center-Version viele Versionen hinter der aktuellen Version zurückliegt, müssen Sie möglicherweise Kettenaktualisierungen auf neuere Versionen durchführen, bis Ihr installiertes Astra Control Center nur eine Version hinter der neuesten Version zurückliegt. Eine vollständige Liste der freigegebenen Versionen finden Sie im "Versionshinweise".

Bevor Sie beginnen

Stellen Sie vor dem Upgrade sicher, dass Ihre Umgebung weiterhin die Anforderungen erfüllt "Mindestanforderungen für die Implementierung des Astra Control Center". Ihre Umgebung sollte Folgendes haben:

- **A "Unterstützt" Die Version Astra Trident**

  Für Schritte erweitern

  Bestimmen Sie die ausgeführte Trident-Version:

  ```
  kubectl get tridentversion -n trident
  ```

  Führen Sie bei Bedarf ein Upgrade von Astra Trident durch. Verwenden Sie diese "Anweisungen".

Version 23.10 ist die letzte Version von Astra Control Center, die Astra Trident unterstützt. Es wird dringend empfohlen, dass Sie "Astra Control Provisioner aktivieren" Zugriff auf Funktionen für erweitertes Management und Storage-Bereitstellung, die über die von Astra Trident hinausgehen Zur Nutzung dieser erweiterten Funktion müssen Sie sowohl ein Upgrade auf Astra Control Center 23.10 als auch Astra Control Provisioner aktivieren. Astra Control Provisioner ist nicht mit älteren Versionen von Astra Control Center möglich.

- **Eine unterstützte Kubernetes-Distribution**

  Für Schritte erweitern

  Bestimmen Sie die Kubernetes-Version, die Sie ausführen:

  ```
  kubectl get nodes -o wide
  ```

- **Ausreichende Clusterressourcen**

  Für Schritte erweitern

  Ermitteln der verfügbaren Clusterressourcen:

  ```
  kubectl describe node <node name>
  ```

- **Eine Registrierung, mit der Sie Astra Control Center-Bilder per Push und Upload hochladen können**
- **Eine Standard-Speicherklasse**

  Für Schritte erweitern

  Bestimmen Sie Ihre Standard-Storage-Klasse:

  ```
  kubectl get storageclass
  ```

- **Gesunde und verfügbare API-Dienste**

  Für Schritte erweitern

  Stellen Sie sicher, dass alle API-Services in einem ordnungsgemäßen Zustand und verfügbar sind:

  ```
  kubectl get apiservices
  ```

- **(nur OpenShift) gesunde und verfügbare Clusteroperatoren**

Für Schritte erweitern

Stellen Sie sicher, dass alle Cluster Operator in einem ordnungsgemäßen Zustand und verfügbar sind.

```
kubectl get clusteroperators
```

- **Zugriff auf die NetApp Astra Control Image Registry**:
  Sie haben die Möglichkeit, Installations-Images und Funktionserweiterungen für Astra Control, wie z. B. Astra Control Provisioner, aus der NetApp-Image-Registrierung zu beziehen.

  Für Schritte erweitern

  a. Notieren Sie Ihre Astra Control Account-ID, die Sie zur Anmeldung in der Registrierung benötigen.

     Ihre Konto-ID wird in der Web-UI des Astra Control Service angezeigt. Wählen Sie das Symbol oben rechts auf der Seite aus, wählen Sie **API Access** aus und notieren Sie sich Ihre Konto-ID.

  b. Wählen Sie auf derselben Seite **API-Token generieren** aus und kopieren Sie die API-Token-Zeichenfolge in die Zwischenablage und speichern Sie sie in Ihrem Editor.

  c. Melden Sie sich in der Astra Control Registry an:

     ```
     docker login cr.astra.netapp.io -u <account-id> -p <api-token>
     ```

Über diese Aufgabe

Der Astra Control Center Upgrade-Prozess führt Sie durch die folgenden grundlegenden Schritte:

Melden Sie sich von der Astra Control Center-Benutzeroberfläche ab, bevor Sie das Upgrade starten.

- Laden Sie das Astra Control Center herunter und extrahieren Sie es
- Entfernen Sie das NetApp Astra kubectl Plugin und installieren Sie es erneut
- Fügen Sie die Bilder Ihrer lokalen Registrierung hinzu
- Installieren Sie den aktualisierten Astra Control Center-Operator
- Upgrade Astra Control Center
- Überprüfen Sie den Systemstatus

Löschen Sie den Operator Astra Control Center nicht (z. B. `kubectl delete -f astra_control_center_operator_deploy.yaml`) Zu jeder Zeit während des Astra Control Center Upgrades oder Betrieb, um zu vermeiden, dass Pods gelöscht werden.

Führen Sie Upgrades in einem Wartungsfenster durch, wenn Zeitpläne, Backups und Snapshots nicht ausgeführt werden.

Laden Sie das Astra Control Center herunter und extrahieren Sie es

Sie können das Bundle von Astra Control Center von der NetApp Support-Website herunterladen oder das Bundle mithilfe von Docker aus der Image-Registrierung des Astra Control Service abrufen.

NetApp Support Website

1. Laden Sie das Bundle mit Astra Control Center herunter (`astra-control-center-[version].tar.gz`) Vom "Download-Seite für Astra Control Center".
2. (Empfohlen, aber optional) Laden Sie das Zertifikaten- und Unterschriftenpaket für Astra Control Center herunter (`astra-control-center-certs-[version].tar.gz`) Um die Signatur des Bündels zu überprüfen.

   Erweitern Sie, um Details anzuzeigen

   ```
   tar -vxzf astra-control-center-certs-[version].tar.gz
   ```

   ```
   openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub
   -signature certs/astra-control-center-[version].tar.gz.sig
   astra-control-center-[version].tar.gz
   ```

   Die Ausgabe wird angezeigt `Verified OK` Nach erfolgreicher Überprüfung.

3. Extrahieren Sie die Bilder aus dem Astra Control Center Bundle:

   ```
   tar -vxzf astra-control-center-[version].tar.gz
   ```

Astra Control-Image-Registrierung

1. Melden Sie sich beim Astra Control Service an.
2. Wählen Sie im Dashboard **Deploy a self-Managed Instance of Astra Control** aus.
3. Folgen Sie den Anweisungen, um sich bei der Astra Control-Image-Registrierung anzumelden, das Astra Control Center-Installationsabbild zu ziehen und das Image zu extrahieren.

Entfernen Sie das NetApp Astra kubectl Plugin und installieren Sie es erneut

Sie können das NetApp Astra kubectl Befehlszeilenschnittstelle-Plug-in verwenden, um Images in ein lokales Docker Repository zu verschieben.

1. Ermitteln Sie, ob das Plug-in installiert ist:

   ```
   kubectl astra
   ```

2. Führen Sie eine der folgenden Aktionen durch:
   - Wenn das Plugin installiert ist, sollte der Befehl die kubectl Plugin-Hilfe zurückgeben und Sie können die vorhandene Version von kubectl-astra entfernen: `delete /usr/local/bin/kubectl-astra`.
   - Wenn der Befehl einen Fehler zurückgibt, ist das Plugin nicht installiert und Sie können mit dem nächsten Schritt fortfahren, um es zu installieren.
3. Installieren Sie das Plugin:
   a. Geben Sie die verfügbaren Plug-ins-Binärdateien von NetApp Astra kubectl an und notieren Sie sich den Namen der für Ihr Betriebssystem und die CPU-Architektur erforderlichen Datei:

      Die kubectl Plugin-Bibliothek ist Teil des tar-Bündels und wird in den Ordner extrahiert `kubectl-astra`.

```
ls kubectl-astra/
```

   a. Verschieben Sie die richtige Binärdatei in den aktuellen Pfad, und benennen Sie sie in um `kubectl-astra`:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Fügen Sie die Bilder Ihrer lokalen Registrierung hinzu

1. Führen Sie die entsprechende Schrittfolge für Ihre Container-Engine durch:

Docker

1. Wechseln Sie in das Stammverzeichnis des Tarballs. Sie sollten den sehen `acc.manifest.bundle.yaml` Datei und diese Verzeichnisse:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Übertragen Sie die Paketbilder im Astra Control Center-Bildverzeichnis in Ihre lokale Registrierung. Führen Sie die folgenden Ersetzungen durch, bevor Sie den ausführen `push-images` Befehl:
   - Ersetzen Sie <BUNDLE_FILE> durch den Namen der Astra Control Bundle-Datei (`acc.manifest.bundle.yaml`).
   - <MY_FULL_REGISTRY_PATH> durch die URL des Docker Repositorys ersetzen, beispielsweise "<a href="https://<docker-registry>"" class="bare">https://<docker-registry>".
   - Ersetzen Sie <MY_REGISTRY_USER> durch den Benutzernamen.
   - Ersetzen Sie <MY_REGISTRY_TOKEN> durch ein autorisiertes Token für die Registrierung.

     ```
     kubectl astra packages push-images -m <BUNDLE_FILE> -r
     <MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
     <MY_REGISTRY_TOKEN>
     ```

Podman

1. Wechseln Sie in das Stammverzeichnis des Tarballs. Sie sollten diese Datei und das Verzeichnis sehen:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Melden Sie sich bei Ihrer Registrierung an:

   ```
   podman login <YOUR_REGISTRY>
   ```

3. Vorbereiten und Ausführen eines der folgenden Skripts, das für die von Ihnen verwendete Podman-Version angepasst ist. Ersetzen Sie <MY_FULL_REGISTRY_PATH> durch die URL Ihres Repositorys, die alle Unterverzeichnisse enthält.

   ```
   <strong>Podman 4</strong>
   ```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

Der Bildpfad, den das Skript erstellt, sollte abhängig von Ihrer Registrierungskonfiguration wie folgt aussehen:

```
https://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/23.10.0-68/image:version
```

Installieren Sie den aktualisierten Astra Control Center-Operator

1. Telefonbuch ändern:

```
cd manifests
```

2. Bearbeiten Sie die yaml-Implementierung des Astra Control Center-Bedieners (`astra_control_center_operator_deploy.yaml`) Zu Ihrem lokalen Register und Geheimnis zu verweisen.

```
vim astra_control_center_operator_deploy.yaml
```

   a. Wenn Sie eine Registrierung verwenden, die eine Authentifizierung erfordert, ersetzen oder bearbeiten Sie die Standardzeile von `imagePullSecrets: []` Mit folgenden Optionen:

```
imagePullSecrets: [{name: astra-registry-cred}]
```

   b. Ändern `ASTRA_IMAGE_REGISTRY` Für das `kube-rbac-proxy` Bild zum Registrierungspfad, in dem Sie die Bilder in ein geschoben haben Vorheriger Schritt.

   c. Ändern `ASTRA_IMAGE_REGISTRY` Für das `acc-operator` Bild zum Registrierungspfad, in dem Sie die Bilder in ein geschoben haben Vorheriger Schritt.

   d. Fügen Sie dem die folgenden Werte hinzu `env` Abschnitt:

```
- name: ACCOP_HELM_UPGRADETIMEOUT
  value: 300m
```

Beispiel für astra_Control_Center_Operator_deploy.yaml:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: ASTRA_IMAGE_REGISTRY/kube-rbac-proxy:v4.8.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_UPGRADETIMEOUT
          value: 300m
        image: ASTRA_IMAGE_REGISTRY/acc-operator:23.10.72
        imagePullPolicy: IfNotPresent
        livenessProbe:
          httpGet:
            path: /healthz
```

```
            port: 8081
          initialDelaySeconds: 15
          periodSeconds: 20
        name: manager
        readinessProbe:
          httpGet:
            path: /readyz
            port: 8081
          initialDelaySeconds: 5
          periodSeconds: 10
        resources:
          limits:
            cpu: 300m
            memory: 750Mi
          requests:
            cpu: 100m
            memory: 75Mi
        securityContext:
          allowPrivilegeEscalation: false
      imagePullSecrets: []
      securityContext:
        runAsUser: 65532
      terminationGracePeriodSeconds: 10
```

3. Installieren Sie den aktualisierten Astra Control Center-Operator:

```
kubectl apply -f astra_control_center_operator_deploy.yaml
```

Beispielantwort:

```
namespace/netapp-acc-operator unchanged
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.as
tra.netapp.io configured
role.rbac.authorization.k8s.io/acc-operator-leader-election-role
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role
configured
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role
unchanged
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding unchanged
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding configured
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding unchanged
configmap/acc-operator-manager-config unchanged
service/acc-operator-controller-manager-metrics-service unchanged
deployment.apps/acc-operator-controller-manager configured
```

4. Überprüfen Sie, ob Pods ausgeführt werden:

```
kubectl get pods -n netapp-acc-operator
```

Upgrade Astra Control Center

1. Bearbeiten der benutzerdefinierten Ressource des Astra Control Center (CR):

```
kubectl edit AstraControlCenter -n [netapp-acc or custom namespace]
```

2. Ändern Sie die Versionsnummer des Astra (`astraVersion` Innerhalb von `spec`) Aus Richtung `23.07.0` Bis `23.10.0`:

> Sie können kein direktes Upgrade von einer Version durchführen, die zwei oder mehr Versionen hinter der aktuellen Version enthält. Eine vollständige Liste der freigegebenen Versionen finden Sie im "Versionshinweise".

```
spec:
  accountName: "Example"
  astraVersion: "[Version number]"
```

3. Überprüfen Sie, ob Ihr Image-Registrierungspfad mit dem von Ihnen gedrückten Registrierungspfad übereinstimmt Vorheriger Schritt. Aktualisierung `imageRegistry` Innerhalb von `spec` Wenn sich die Registrierung seit Ihrer letzten Installation geändert hat.

```
  imageRegistry:
    name: "[your_registry_path]"
```

4. Fügen Sie Folgendes zu Ihrem hinzu `crds` Konfiguration in `spec`:

```
crds:
  shouldUpgrade: true
```

5. Fügen Sie die folgenden Zeilen in hinzu `additionalValues` Innerhalb von `spec` Im Astra Control Center CR:

```
additionalValues:
    nautilus:
      startupProbe:
        periodSeconds: 30
        failureThreshold: 600
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
```

6. Speichern und beenden Sie den Dateieditor. Die Änderungen werden übernommen und das Upgrade beginnt.
7. (Optional) Stellen Sie sicher, dass die Pods beendet werden und wieder verfügbar sind:

```
watch kubectl get pods -n [netapp-acc or custom namespace]
```

8. Warten Sie, bis die Statusbedingungen des Astra Control angezeigt werden, um anzuzeigen, dass das Upgrade abgeschlossen und bereit ist (`True`):

```
kubectl get AstraControlCenter -n [netapp-acc or custom namespace]
```

Antwort:

```
NAME    UUID                                   VERSION     ADDRESS
READY
astra   9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f   23.10.0-68
10.111.111.111  True
```

Führen Sie den folgenden Befehl aus, um den Upgrade-Status während des Vorgangs zu überwachen: `kubectl get AstraControlCenter -o yaml -n [netapp-acc or custom namespace]`

Führen Sie den folgenden Befehl aus, um die Bedienerprotokolle des Astra Control Center zu überprüfen:
`kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f`

Überprüfen Sie den Systemstatus

1. Melden Sie sich beim Astra Control Center an.
2. Überprüfen Sie, ob die Version aktualisiert wurde. Weitere Informationen finden Sie auf der Seite **Support** in der Benutzeroberfläche.
3. Vergewissern Sie sich, dass alle gemanagten Cluster und Applikationen weiterhin vorhanden und geschützt sind.

Astra Control Provisioner Aktivieren

In Astra Trident Version 23.10 und höher können Sie Astra Control Provisioner verwenden, damit lizenzierte Benutzer von Astra Control auf erweiterte Storage-Bereitstellungsfunktionen zugreifen können. Astra Control Provisioner bietet diese erweiterte Funktionalität zusätzlich zu den auf Astra Trident basierenden Standardfunktionen.

Bei den nächsten Updates für Astra Control wird der Provisioner Astra Trident als Storage-bereitstellung und -Orchestrierung in der Architektur von Astra Control ersetzen. Aus diesem Grund wird dringend empfohlen, Astra Control Benutzer für die Astra Control-Bereitstellung zu verwenden. Astra Trident wird weiterhin Open Source bleiben und mit neuen CSI- und anderen Funktionen von NetApp veröffentlicht, gepflegt, unterstützt und auf dem neuesten Stand sein.

Über diese Aufgabe

Befolgen Sie dieses Verfahren, wenn Sie als lizenzierter Astra Control Center-Benutzer die Astra Control Provisioner-Funktion verwenden möchten. Wenn Sie Astra Trident verwenden und die zusätzlichen Funktionen von Astra Control Provisioner verwenden möchten, sollten Sie dieses Verfahren auch befolgen.

In allen Fällen ist die bereitstellungsfunktion in Astra Trident 23.10 standardmäßig nicht aktiviert, kann jedoch mit diesem Prozess aktiviert werden.

Bevor Sie beginnen

Wenn Sie die Astra Control Provisioner aktivieren, gehen Sie wie folgt vor:

Astra Control Provisioniert Benutzer mit Astra Control Center

- **Bewirke eine Astra Control Center Lizenz**: Du benötigst eine "Astra Control Center-Lizenz" Um Astra Control Provisioner zu aktivieren und auf die enthaltenen Funktionen zuzugreifen.
- **Installation oder Upgrade auf Astra Control Center 23.10**: Sie benötigen diese Version, wenn Sie Astra Control Provisioner mit Astra Control verwenden möchten.
- **Bestätigen Sie, dass Ihr Cluster über eine AMD64-Systemarchitektur verfügt**: Das Astra Control Provisioner-Image wird sowohl in AMD64- als auch in ARM64-CPU-Architekturen bereitgestellt, aber nur AMD64 wird von Astra Control Center unterstützt.
- **Erhalten Sie ein Astra Control Service-Konto für den Registrierungszugriff**: Wenn Sie beabsichtigen, die Astra Control-Registrierung anstelle der NetApp-Support-Website zu verwenden, um das Astra Control-Provisioner-Image herunterzuladen, schließen Sie die Registrierung für einen ab "Astra Control Service Konto". Nachdem Sie das Formular ausgefüllt, übermittelt und ein BlueXP Konto erstellt haben, erhalten Sie eine Willkommens-E-Mail für Astra Control Service.
- **Wenn Sie Astra Trident installiert haben, bestätigen Sie, dass seine Version innerhalb eines Fensters mit vier Versionen ist**: Sie können ein direktes Upgrade auf Astra Trident 23.10 mit Astra Control Provisioner durchführen, wenn Ihr Astra Trident innerhalb eines Fensters mit vier Versionen von Version 23.10 ist. Sie können beispielsweise direkt von Astra Trident 22.10 auf 23.10 aktualisieren.

Astra Control Provisioner nur Benutzer

- **Bewirke eine Astra Control Center Lizenz**: Du benötigst eine "Astra Control Center-Lizenz" Um Astra Control Provisioner zu aktivieren und auf die enthaltenen Funktionen zuzugreifen.
- **Wenn Sie Astra Trident installiert haben, bestätigen Sie, dass seine Version innerhalb eines Fensters mit vier Versionen ist**: Sie können ein direktes Upgrade auf Astra Trident 23.10 mit Astra Control Provisioner durchführen, wenn Ihr Astra Trident innerhalb eines Fensters mit vier Versionen von Version 23.10 ist. Sie können beispielsweise direkt von Astra Trident 22.10 auf 23.10 aktualisieren.
- **Sie können ein Astra Control Service-Konto für den Registrierungszugriff abrufen**: Sie benötigen Zugriff auf die Registrierung, um Astra Control Provisioner-Bilder herunterladen zu können. Um zu beginnen, füllen Sie die Registrierung für einen aus "Astra Control Service Konto". Nachdem Sie das Formular ausgefüllt, übermittelt und ein BlueXP Konto erstellt haben, erhalten Sie eine Willkommens-E-Mail für Astra Control Service.

(Schritt 1) Laden Sie die Astra Control Provisioner herunter und extrahieren Sie sie

Benutzer von Astra Control Center können das Image entweder über die NetApp Support Site oder die Astra Control Registry-Methode herunterladen. Für Astra Trident Benutzer, die Astra Control Provisioner ohne Astra Control verwenden möchten, sollte die Registrierungsmethode verwendet werden.

(Optional) NetApp Support-Website

1. Laden Sie das Bundle für die Astra Control Bereitstellung herunter (`trident-acp-[version].tar`) Vom "Download-Seite für Astra Control Center".
2. (Empfohlen, aber optional) Laden Sie das Paket Zertifikate und Signaturen für Astra Control Center (astra-control-Center-certs-[Version].tar.gz) herunter, um die Signatur des tar-Bundles tar von trident-acp-[Version] zu überprüfen.

Erweitern Sie, um Details anzuzeigen

```
tar -vxzf astra-control-center-certs-[version].tar.gz
```

```
openssl dgst -sha256 -verify certs/AstraControlCenterDockerImages-public.pub -signature certs/trident-acp-[version].tar.sig trident-acp-[version].tar
```

3. Laden Sie das Astra Control Provisioner-Bild:

```
docker load < trident-acp-23.10.0.tar
```

Antwort:

```
Loaded image: trident-acp:23.10.0-linux-amd64
```

4. Markieren Sie das Bild:

```
docker tag trident-acp:23.10.0-linux-amd64 <my_custom_registry>/trident-acp:23.10.0
```

5. Laden Sie das Bild in Ihre benutzerdefinierte Registrierung:

```
docker push <my_custom_registry>/trident-acp:23.10.0
```

(Optional) Astra Control-Image-Registrierung

Bei diesem Verfahren können Sie Podman anstelle von Docker für die Befehle verwenden. Wenn Sie eine Windows-Umgebung verwenden, wird PowerShell empfohlen.

1. Rufen Sie die NetApp Astra Control Image-Registry auf:
   a. Melden Sie sich bei der Astra Control Service Web-UI an, und wählen Sie das Symbol oben rechts auf der Seite aus.
   b. Wählen Sie **API-Zugriff**.
   c. Notieren Sie sich Ihre Konto-ID.
   d. Wählen Sie auf derselben Seite **API-Token generieren** aus und kopieren Sie die API-Token-Zeichenfolge in die Zwischenablage und speichern Sie sie in Ihrem Editor.
   e. Melden Sie sich über Ihre bevorzugte Methode in der Astra Control Registry an:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

```
crane auth login cr.astra.netapp.io -u <account-id> -p <api-token>
```

2. Wenn Sie über eine benutzerdefinierte Registrierung verfügen, führen Sie die folgenden Schritte aus, um das Bild in Ihre benutzerdefinierte Registrierung zu verschieben. Wenn Sie keine Registrierung verwenden, befolgen Sie die Schritte des Trident-Operators in "Nächster Abschnitt".

> Sie können Podman anstelle von Docker für die folgenden Befehle verwenden. Wenn Sie eine Windows-Umgebung verwenden, wird PowerShell empfohlen.

Docker

a. Rufen Sie das Astra Control Provisioner-Image aus der Registrierung ab:

> Das abgezogene Image unterstützt nicht mehrere Plattformen und unterstützt nur die gleiche Plattform wie der Host, der das Image gezogen hat, wie z. B. Linux AMD64.

```
docker pull cr.astra.netapp.io/astra/trident-acp:23.10.0
--platform <cluster platform>
```

Beispiel:

```
docker pull cr.astra.netapp.io/astra/trident-acp:23.10.0
--platform linux/amd64
```

b. Markieren Sie das Bild:

```
docker tag cr.astra.netapp.io/astra/trident-acp:23.10.0
<my_custom_registry>/trident-acp:23.10.0
```

c. Laden Sie das Bild in Ihre benutzerdefinierte Registrierung:

```
docker push <my_custom_registry>/trident-acp:23.10.0
```

Kran

a. Kopieren Sie das Astra Control Provisioner-Manifest in Ihre benutzerdefinierte Registry:

```
crane copy cr.astra.netapp.io/astra/trident-acp:23.10.0
<my_custom_registry>/trident-acp:23.10.0
```

(Schritt 2) Aktivieren Sie die Astra Control-Bereitstellung in Astra Trident

Stellen Sie fest, ob die ursprüngliche Installationsmethode einen verwendet hat Und führen Sie die entsprechenden Schritte entsprechend Ihrer ursprünglichen Methode durch.

> Verwenden Sie Helm nicht, um die Astra Control Provisioner zu aktivieren. Wenn Sie Helm für die ursprüngliche Installation verwendet haben und ein Upgrade auf 23.10 durchführen, müssen Sie entweder den Trident-Operator oder tridentctl verwenden, um die Aktivierung von Astra Control Provisioner durchzuführen.

Astra Trident Betreiber

1. "Laden Sie das Astra Trident Installationsprogramm herunter und extrahieren Sie es".
2. Führen Sie diese Schritte aus, wenn Sie Astra Trident noch nicht installiert haben oder den Operator aus der ursprünglichen Astra Trident-Implementierung entfernt haben:
   a. Erstellen des CRD:

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.y
aml
```

   b. Erstellen Sie den Namespace für Trident (`kubectl create namespace trident`) Oder bestätigen Sie, dass der Namensraum Dreizack noch existiert (`kubectl get all -n trident`). Wenn der Namespace entfernt wurde, erstellen Sie ihn erneut.
3. Update von Astra Trident auf 23.10.0:

> Verwenden Sie für Cluster mit Kubernetes 1.24 oder früheren Versionen `bundle_pre_1_25.yaml`. Verwenden Sie für Cluster mit Kubernetes 1.25 oder höher `bundle_post_1_25.yaml`.

```
kubectl -n trident apply -f trident-installer-
23.10.0/deploy/<bundle-name.yaml>
```

4. Überprüfen Sie, ob Astra Trident ausgeführt wird:

```
kubectl get torc -n trident
```

   Antwort:

```
NAME      AGE
trident   21m
```

5. Wenn Sie eine Registry mit Geheimnissen haben, erstellen Sie ein Geheimnis, mit dem Sie das Astra Control Provisioner-Bild abrufen können:

```
kubectl create secret docker-registry <secret_name> -n trident
--docker-server=<my_custom_registry> --docker-username=<username>
--docker-password=<token>
```

6. Bearbeiten Sie den TridentOrchestrator CR, und nehmen Sie die folgenden Änderungen vor:

```
kubectl edit torc trident -n trident
```

a. Legen Sie einen benutzerdefinierten Registrierungsport für das Astra Trident Image fest oder ziehen Sie es aus der Astra Control Registry (`tridentImage: <my_custom_registry>/trident:23.10.0` Oder `tridentImage: netapp/trident:23.10.0`).

b. Astra Control Provisioner Aktivieren (`enableACP: true`).

c. Legen Sie den benutzerdefinierten Registrierungsport für das Astra Control Provisioner-Image fest oder ziehen Sie es aus der Astra Control Registry (`acpImage: <my_custom_registry>/trident-acp:23.10.0` Oder `acpImage: cr.astra.netapp.io/astra/trident-acp:23.10.0`).

d. Wenn Sie sich etabliert haben Geheimnisse der Bildausziehung Sie können diese hier einstellen (`imagePullSecrets: - <secret_name>`). Verwenden Sie den gleichen geheimen Namen, den Sie in den vorherigen Schritten festgelegt haben.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  tridentImage: <registry>/trident:23.10.0
  enableACP: true
  acpImage: <registry>/trident-acp:23.10.0
  imagePullSecrets:
  - <secret_name>
```

7. Speichern und beenden Sie die Datei. Der Bereitstellungsprozess wird automatisch gestartet.
8. Überprüfen Sie, ob der Operator, die Bereitstellung und Replikasets erstellt wurden.

```
kubectl get all -n trident
```

Es sollte nur eine Instanz* des Operators in einem Kubernetes-Cluster geben. Erstellen Sie nicht mehrere Implementierungen des Astra Trident Operators.

9. Überprüfen Sie die `trident-acp` Container läuft und das `acpVersion` Ist `23.10.0` Mit dem Status `Installed`:

```
kubectl get torc -o yaml
```

Antwort:

```
status:
  acpVersion: 23.10.0
  currentInstallationParams:
    ...
    acpImage: <registry>/trident-acp:23.10.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

Tridentctl

1. "Laden Sie das Astra Trident Installationsprogramm herunter und extrahieren Sie es".
2. "Wenn Sie bereits Astra Trident verwenden, deinstallieren Sie ihn aus dem Cluster, das ihn hostet".
3. Installieren Sie Astra Trident mit aktiviertem Astra Control Provisioner (`--enable-acp=true`):

```
./tridentctl -n trident install --enable-acp=true --acp
-image=mycustomregistry/trident-acp:23.10
```

4. Aktivieren Sie die Astra Control Provisioner-Funktion:

```
./tridentctl -n trident version
```

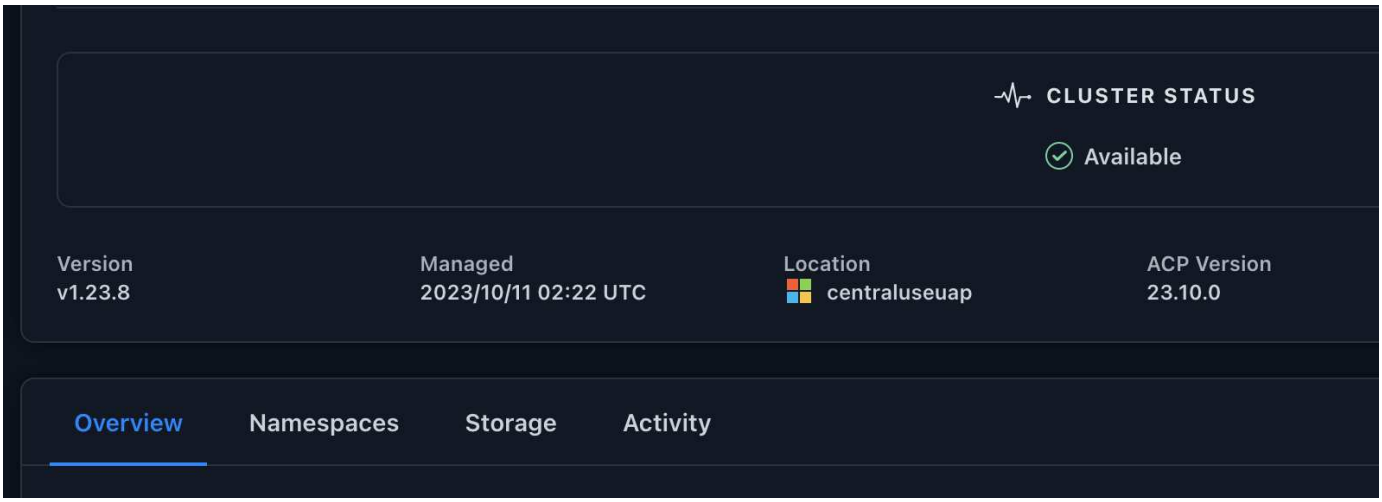
Antwort:

```
+----------------+----------------+-------------+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +----------------+----------------
+-------------+ | 23.10.0 | 23.10.0 | 23.10.0. | +----------------
+----------------+-------------+
```

Ergebnis

Die Bereitstellungsfunktion von Astra Control ist aktiviert und Sie können alle Funktionen der verwendeten Version verwenden.

(Nur für Astra Control Center Benutzer) nach der Installation von Astra Control wird für das Cluster, das die provisionierung in der Astra Control Center UI hostet, ein angezeigt `ACP version` Und nicht `Trident version` Feld und aktuelle installierte Versionsnummer.



Finden Sie weitere Informationen

- "Dokumentation für Astra Trident Upgrades"

Deinstallieren Sie Astra Control Center

Möglicherweise müssen Sie die Komponenten des Astra Control Center entfernen, wenn Sie ein Upgrade von einer Testversion auf eine Vollversion des Produkts durchführen. Um Astra Control Center und den Astra Control Center Operator zu entfernen, führen Sie die in diesem Verfahren beschriebenen Befehle nacheinander aus.

Wenn Sie Probleme mit der Deinstallation haben, lesen Sie Fehlerbehebung bei Deinstallationsproblemen.

Bevor Sie beginnen

1. "Heben Sie die Verwaltung aller Apps auf" Auf den Clustern.
2. "Heben Sie die Verwaltung aller Cluster auf".

Schritte

1. Löschen Sie Das Astra Control Center. Der folgende Beispielbefehl basiert auf einer Standardinstallation. Ändern Sie den Befehl, wenn Sie benutzerdefinierte Konfigurationen erstellt haben.

   ```
   kubectl delete -f astra_control_center.yaml -n netapp-acc
   ```

   Ergebnis:

   ```
   astracontrolcenter.astra.netapp.io "astra" deleted
   ```

2. Löschen Sie den mit dem folgenden Befehl `netapp-acc` (Oder benutzerdefinierter Name) Namespace:

   ```
   kubectl delete ns [netapp-acc or custom namespace]
   ```

   Beispielergebnis:

```
namespace "netapp-acc" deleted
```

3. Löschen Sie die Komponenten des Astra Control Center-Bedienersystems mit dem folgenden Befehl:

```
kubectl delete -f astra_control_center_operator_deploy.yaml
```

Ergebnis:

```
namespace/netapp-acc-operator deleted
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.astra.
netapp.io deleted
role.rbac.authorization.k8s.io/acc-operator-leader-election-role deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role deleted
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding deleted
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding deleted
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding deleted
configmap/acc-operator-manager-config deleted
service/acc-operator-controller-manager-metrics-service deleted
deployment.apps/acc-operator-controller-manager deleted
```

Fehlerbehebung bei Deinstallationsproblemen

Verwenden Sie die folgenden Problemumgehungen, um Probleme bei der Deinstallation von Astra Control Center zu beheben.

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:

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

Ergebnis:

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

2. Löschen Sie den Namespace:

```
kubectl delete ns netapp-monitoring
```

Ergebnis:

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

3. Bestätigen der entfernten Ressourcen:

```
kubectl get pods -n netapp-monitoring
```

Ergebnis:

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

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

```
kubectl get crd|grep agent
```

Beispielergebnis:

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

5. Informationen zur benutzerdefinierten Ressourcendefinition löschen:

```
kubectl 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

- "Bekannte Probleme bei der Deinstallation"

Verwenden Sie Astra Control Provisioner

Konfiguration der Storage-Back-End-Verschlüsselung

Mit Astra Control Provisioner können Sie die Datensicherheit verbessern, indem Sie die Verschlüsselung für den Datenverkehr zwischen dem gemanagten Cluster und dem Storage-Back-End aktivieren.

Astra Control Provisioner unterstützt Kerberos-Verschlüsselung für zwei Arten von Storage-Back-Ends:

- **On-Premises-ONTAP** – Astra Control Provisioner unterstützt Kerberos-Verschlüsselung über NFSv3- und NFSv4-Verbindungen von Red hat OpenShift und Upstream-Kubernetes-Clustern zu lokalen ONTAP-Volumes.
- **Azure NetApp Files** – Astra Control Provisioner unterstützt Kerberos-Verschlüsselung über NFSv4.1-Verbindungen von Upstream-Kubernetes-Clustern zu Azure NetApp Files Volumes.

Sie können Snapshots, Klone, schreibgeschütztes Klonen und Importieren von Volumes mit NFS-Verschlüsselung.

Konfiguration der in-Flight-Kerberos-Verschlüsselung mit lokalen ONTAP-Volumes

Sie können die Kerberos-Verschlüsselung auf dem Storage-Datenverkehr zwischen dem verwalteten Cluster und einem lokalen ONTAP-Storage-Back-End aktivieren.

Kerberos-Verschlüsselung für NFS-Datenverkehr mit lokalen ONTAP-Storage-Back-Ends wird nur mithilfe des unterstützt `ontap-nas` Storage-Treiber:

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie die Astra Control-Bereitstellung im verwalteten Cluster aktiviert haben. Siehe "Astra Control Provisioner Aktivieren" Weitere Anweisungen.
- Stellen Sie sicher, dass Sie Zugriff auf haben `tridentctl` Utility:
- Stellen Sie sicher, dass Sie Administratorzugriff auf das ONTAP Storage Back-End haben.
- Stellen Sie sicher, dass Sie den Namen des Volumes oder der Volumes kennen, die Sie über das ONTAP-Speicher-Back-End freigeben werden.
- Stellen Sie sicher, dass Sie die ONTAP-Storage-VM auf die Unterstützung der Kerberos-Verschlüsselung für NFS-Volumes vorbereitet haben. Siehe "Aktivieren Sie Kerberos auf einer Daten-LIF" Weitere Anweisungen.
- Stellen Sie sicher, dass alle NFSv4-Volumes, die Sie mit Kerberos-Verschlüsselung verwenden, korrekt konfiguriert sind. Weitere Informationen finden Sie im Abschnitt NetApp NFSv4-Domänenkonfiguration (Seite 13) des "NetApp Leitfaden zu NFSv4-Verbesserungen und Best Practices".

ONTAP-Exportrichtlinien hinzufügen oder ändern

Sie müssen bestehenden ONTAP-Exportrichtlinien Regeln hinzufügen oder neue Exportrichtlinien erstellen, die Kerberos-Verschlüsselung für das ONTAP Storage-VM-Root-Volume sowie alle mit dem Upstream-Kubernetes-Cluster gemeinsam genutzten ONTAP-Volumes unterstützen. Die von Ihnen hinzugefügten Regeln für die Exportrichtlinie oder neu erstellte Richtlinien für den Export müssen die folgenden Zugriffsprotokolle und Zugriffsberechtigungen unterstützen:

Zugriffsprotokolle

Konfigurieren Sie die Exportrichtlinie mit NFS-, NFSv3- und NFSv4-Zugriffsprotokollen.

Zugriffsdetails

Sie können eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung konfigurieren, je nach Ihren Anforderungen für das Volume:

- **Kerberos 5** - (Authentifizierung und Verschlüsselung)
- **Kerberos 5i** - (Authentifizierung und Verschlüsselung mit Identitätsschutz)
- **Kerberos 5p** - (Authentifizierung und Verschlüsselung mit Identitäts- und Datenschutz)

Konfigurieren Sie die ONTAP-Exportrichtlinie mit den entsprechenden Zugriffsberechtigungen. Wenn beispielsweise Cluster die NFS-Volumes mit einer Mischung aus Kerberos 5i- und Kerberos 5p-Verschlüsselung mounten, verwenden Sie die folgenden Zugriffseinstellungen:

Typ	Schreibgeschützter Zugriff	Lese-/Schreibzugriff	Superuser-Zugriff
UNIX	Aktiviert	Aktiviert	Aktiviert
Kerberos 5i	Aktiviert	Aktiviert	Aktiviert
Kerberos 5p	Aktiviert	Aktiviert	Aktiviert

Informationen zum Erstellen von ONTAP Exportrichtlinien und Exportrichtlinienregeln finden Sie in der folgenden Dokumentation:

- "Erstellen Sie eine Exportrichtlinie"
- "Fügen Sie eine Regel zu einer Exportrichtlinie hinzu"

Erstellen eines Storage-Backends

Sie können eine Astra Control Provisioner-Storage-Back-End-Konfiguration erstellen, die Kerberos Verschlüsselungsfunktionen umfasst.

Über diese Aufgabe

Wenn Sie eine Speicher-Back-End-Konfigurationsdatei erstellen, die die Kerberos-Verschlüsselung konfiguriert, können Sie eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung mithilfe des angeben `spec.nfsMountOptions` Parameter:

- `spec.nfsMountOptions: sec=krb5` (Authentifizierung und Verschlüsselung)
- `spec.nfsMountOptions: sec=krb5i` (Authentifizierung und Verschlüsselung mit Identitätsschutz)
- `spec.nfsMountOptions: sec=krb5p` (Authentifizierung und Verschlüsselung mit Identitäts- und Datenschutz)

Geben Sie nur eine Kerberos-Ebene an. Wenn Sie in der Parameterliste mehr als eine Kerberos-Verschlüsselungsebene angeben, wird nur die erste Option verwendet.

Schritte

1. Erstellen Sie auf dem verwalteten Cluster mithilfe des folgenden Beispiels eine Speicher-Back-End-Konfigurationsdatei. Ersetzen Sie Werte in Klammern <> durch Informationen aus Ihrer Umgebung:

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-ontap-nas-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-ontap-nas
spec:
  version: 1
  storageDriverName: "ontap-nas"
  managementLIF: <STORAGE_VM_MGMT_LIF_IP_ADDRESS>
  dataLIF: <PROTOCOL_LIF_FQDN_OR_IP_ADDRESS>
  svm: <STORAGE_VM_NAME>
  username: <STORAGE_VM_USERNAME_CREDENTIAL>
  password: <STORAGE_VM_PASSWORD_CREDENTIAL>
  nasType: nfs
  nfsMountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
  qtreesPerFlexvol:
  credentials:
    name: backend-ontap-nas-secret
```

2. Verwenden Sie die Konfigurationsdatei, die Sie im vorherigen Schritt erstellt haben, um das Backend zu erstellen:

```
tridentctl create backend -f <backend-configuration-file>
```

Wenn die Backend-Erstellung fehlschlägt, ist mit der Back-End-Konfiguration ein Fehler aufgetreten. Sie können die Protokolle zur Bestimmung der Ursache anzeigen, indem Sie den folgenden Befehl ausführen:

```
tridentctl logs
```

Nachdem Sie das Problem mit der Konfigurationsdatei identifiziert und korrigiert haben, können Sie den Befehl „Erstellen“ erneut ausführen.

Erstellen Sie eine Speicherklasse

Sie können eine Storage-Klasse für die Bereitstellung von Volumes mit Kerberos-Verschlüsselung erstellen.

Über diese Aufgabe

Wenn Sie ein Storage-Klasse-Objekt erstellen, können Sie eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung mithilfe des angeben `mountOptions` Parameter:

- `mountOptions: sec=krb5` (Authentifizierung und Verschlüsselung)
- `mountOptions: sec=krb5i` (Authentifizierung und Verschlüsselung mit Identitätsschutz)
- `mountOptions: sec=krb5p` (Authentifizierung und Verschlüsselung mit Identitäts- und Datenschutz)

Geben Sie nur eine Kerberos-Ebene an. Wenn Sie in der Parameterliste mehr als eine Kerberos-Verschlüsselungsebene angeben, wird nur die erste Option verwendet. Wenn die in der Storage-Backend-Konfiguration angegebene Verschlüsselungsebene von der Ebene abweicht, die Sie im Storage-Klasse-Objekt angeben, hat das Storage-Klasse-Objekt Vorrang.

Schritte

1. Erstellen Sie mithilfe des folgenden Beispiels ein StorageClass-Kubernetes-Objekt:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas-sc
provisioner: csi.trident.netapp.io
mountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
parameters:
  backendType: "ontap-nas"
  storagePools: "ontapnas_pool"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: True
```

2. Speicherklasse erstellen:

```
kubectl create -f sample-input/storage-class-ontap-nas-sc.yaml
```

3. Stellen Sie sicher, dass die Storage-Klasse erstellt wurde:

```
kubectl get sc ontap-nas-sc
```

   Sie sollten eine Ausgabe wie die folgende sehen:

```
NAME          PROVISIONER             AGE
ontap-nas-sc    csi.trident.netapp.io   15h
```

Bereitstellen von Volumes

Nachdem Sie ein Storage-Back-End und eine Storage-Klasse erstellt haben, können Sie nun ein Volume bereitstellen. Anweisungen finden Sie unter "Bereitstellen eines Volumes".

Konfiguration der Verschlüsselung von Kerberos während der Übertragung mit Azure NetApp Files Volumes

Sie können die Kerberos-Verschlüsselung für den Storage-Datenverkehr zwischen dem gemanagten Cluster und einem einzelnen Azure NetApp Files Storage-Back-End oder einem virtuellen Pool von Azure NetApp Files Storage-Back-Ends aktivieren.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie Astra Control Provisioner auf dem verwalteten Red hat OpenShift-Cluster aktiviert haben. Siehe "Astra Control Provisioner Aktivieren" Weitere Anweisungen.
- Stellen Sie sicher, dass Sie Zugriff auf haben `tridentctl` Utility:
- Stellen Sie sicher, dass Sie das Azure NetApp Files-Speicher-Back-End für die Kerberos-Verschlüsselung vorbereitet haben, indem Sie die Anforderungen beachten und die Anweisungen in befolgen "Azure NetApp Files-Dokumentation".
- Stellen Sie sicher, dass alle NFSv4-Volumes, die Sie mit Kerberos-Verschlüsselung verwenden, korrekt konfiguriert sind. Weitere Informationen finden Sie im Abschnitt NetApp NFSv4-Domänenkonfiguration (Seite 13) des "NetApp Leitfaden zu NFSv4-Verbesserungen und Best Practices".

Erstellen eines Storage-Backends

Sie können eine Azure NetApp Files-Storage-Back-End-Konfiguration mit Kerberos Verschlüsselungsfunktionen erstellen.

Über diese Aufgabe

Wenn Sie eine Speicher-Backend-Konfigurationsdatei erstellen, die die Kerberos-Verschlüsselung konfiguriert, können Sie sie so definieren, dass sie auf einer der zwei möglichen Ebenen angewendet werden sollte:

- Die **Speicher-Backend-Ebene** unter Verwendung der `spec.kerberos` Feld
- Die **virtuelle Pool-Ebene** mit dem `spec.storage.kerberos` Feld

Wenn Sie die Konfiguration auf der Ebene des virtuellen Pools definieren, wird der Pool mithilfe der Beschriftung in der Speicherklasse ausgewählt.

Auf beiden Ebenen können Sie eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung angeben:

- `kerberos: sec=krb5` (Authentifizierung und Verschlüsselung)
- `kerberos: sec=krb5i` (Authentifizierung und Verschlüsselung mit Identitätsschutz)
- `kerberos: sec=krb5p` (Authentifizierung und Verschlüsselung mit Identitäts- und Datenschutz)

Schritte

1. Erstellen Sie auf dem verwalteten Cluster eine Speicher-Backend-Konfigurationsdatei mit einem der folgenden Beispiele, je nachdem, wo Sie das Speicher-Back-End definieren müssen (Speicher-Back-End-Ebene oder virtuelle Pool-Ebene). Ersetzen Sie Werte in Klammern <> durch Informationen aus Ihrer Umgebung:

Beispiel auf Storage-Back-End-Ebene

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-anf-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-anf-secret
```

Beispiel auf Ebene des virtuellen Pools

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-anf-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  storage:
    - labels:
        type: encryption
      kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-anf-secret
```

2. Verwenden Sie die Konfigurationsdatei, die Sie im vorherigen Schritt erstellt haben, um das Backend zu erstellen:

```
tridentctl create backend -f <backend-configuration-file>
```

Wenn die Backend-Erstellung fehlschlägt, ist mit der Back-End-Konfiguration ein Fehler aufgetreten. Sie können die Protokolle zur Bestimmung der Ursache anzeigen, indem Sie den folgenden Befehl ausführen:

```
tridentctl logs
```

Nachdem Sie das Problem mit der Konfigurationsdatei identifiziert und korrigiert haben, können Sie den Befehl „Erstellen“ erneut ausführen.

Erstellen Sie eine Speicherklasse

Sie können eine Storage-Klasse für die Bereitstellung von Volumes mit Kerberos-Verschlüsselung erstellen.

Schritte

1. Erstellen Sie mithilfe des folgenden Beispiels ein StorageClass-Kubernetes-Objekt:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "nfs"
  selector: "type=encryption"
```

2. Speicherklasse erstellen:

```
kubectl create -f sample-input/storage-class-anf-sc-nfs.yaml
```

3. Stellen Sie sicher, dass die Storage-Klasse erstellt wurde:

```
kubectl get sc anf-sc-nfs
```

Sie sollten eine Ausgabe wie die folgende sehen:

```
NAME          PROVISIONER             AGE
anf-sc-nfs    csi.trident.netapp.io   15h
```

Bereitstellen von Volumes

Nachdem Sie ein Storage-Back-End und eine Storage-Klasse erstellt haben, können Sie nun ein Volume bereitstellen. Anweisungen finden Sie unter "Bereitstellen eines Volumes".

Wiederherstellen von Volume-Daten mithilfe eines Snapshots

Astra Control Provisioner ermöglicht die schnelle Wiederherstellung von Volumes aus einem Snapshot mithilfe von `TridentActionSnapshotRestore` (TASR) CR. Dieser CR fungiert als eine zwingend notwendige Kubernetes-Aktion und bleibt nach Abschluss des Vorgangs nicht erhalten.

Astra Control Provisioner unterstützt die Wiederherstellung von Snapshots auf dem `ontap-san`, `ontap-san-economy`, `ontap-nas`, `ontap-nas-flexgroup`, `azure-netapp-files`, `gcp-cvs`, und `solidfire-san` Treiber.

Bevor Sie beginnen

Sie müssen über einen gebundenen PVC-Snapshot und einen verfügbaren Volume-Snapshot verfügen.

- Vergewissern Sie sich, dass der PVC-Status gebunden ist.

```
kubectl get pvc
```

- Überprüfen Sie, ob der Volume-Snapshot einsatzbereit ist.

```
kubectl get vs
```

Schritte

1. Erstellen Sie den TASR CR. In diesem Beispiel wird ein CR für PVC erstellt `pvc1` Und Volume-Snapshot `pvc1-snapshot`.

```
cat tasr-pvc1-snapshot.yaml

apiVersion: trident.netapp.io/v1
kind: TridentActionSnapshotRestore
metadata:
  name: this-doesnt-matter
  namespace: trident
spec:
  pvcName: pvc1
  volumeSnapshotName: pvc1-snapshot
```

2. Wenden Sie den CR an, um ihn aus dem Snapshot wiederherzustellen. Dieses Beispiel wird aus einem Snapshot wiederhergestellt `pvc1`.

```
kubectl create -f tasr-pvc1-snapshot.yaml

tridentactionsnapshotrestore.trident.netapp.io/this-doesnt-matter
created
```

Ergebnisse

Mit Astra Control Provisioner werden die Daten aus dem Snapshot wiederhergestellt. Sie können den Status der Snapshot-Wiederherstellung überprüfen.

```
kubectl get tasr -o yaml

apiVersion: trident.netapp.io/v1
items:
- apiVersion: trident.netapp.io/v1
  kind: TridentActionSnapshotRestore
  metadata:
    creationTimestamp: "2023-04-14T00:20:33Z"
    generation: 3
    name: this-doesnt-matter
    namespace: trident
    resourceVersion: "3453847"
    uid: <uid>
  spec:
    pvcName: pvc1
    volumeSnapshotName: pvc1-snapshot
  status:
    startTime: "2023-04-14T00:20:34Z"
    completionTime: "2023-04-14T00:20:37Z"
    state: Succeeded
kind: List
metadata:
  resourceVersion: ""
```

- In den meisten Fällen versucht die Astra Control Provisioner bei einem Ausfall nicht automatisch einen weiteren Vorgang auszuführen. Sie müssen den Vorgang erneut ausführen.
- Kubernetes-Benutzer ohne Administratorzugriff müssen möglicherweise vom Administrator zum Erstellen eines TASR CR in ihrem Applikations-Namespace erhalten.

Replizieren Sie Volumes mit SnapMirror

Mit Astra Control Provisioner können Sie Spiegelungsbeziehungen zwischen einem Quell-Volume auf einem Cluster und dem Ziel-Volume auf dem Peering-Cluster erstellen,

um Daten für die Disaster Recovery zu replizieren. Sie können eine benutzerdefinierte Ressourcendefinition (CRD, Namested Custom Resource Definition) verwenden, um die folgenden Vorgänge auszuführen:

- Erstellen von Spiegelbeziehungen zwischen Volumes (VES)
- Entfernen Sie Spiegelungsbeziehungen zwischen Volumes
- Brechen Sie die Spiegelbeziehungen auf
- Bewerben des sekundären Volumes bei Ausfällen (Failover)
- Verlustfreie Transition von Applikationen von Cluster zu Cluster (während geplanter Failover oder Migrationen)

Replikationsvoraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie beginnen:

ONTAP Cluster

- **Astra Control Provisioner**: Astra Control Provisioner Version 22.10 oder höher muss sowohl auf den Quell- als auch auf den Ziel-Kubernetes-Clustern vorhanden sein, die ONTAP als Backend verwenden.
- **Lizenzen**: Asynchrone Lizenzen von ONTAP SnapMirror, die das Datensicherungspaket verwenden, müssen sowohl auf den Quell- als auch auf den Ziel-ONTAP-Clustern aktiviert sein. Siehe "Übersicht über die SnapMirror Lizenzierung in ONTAP" Finden Sie weitere Informationen.

Peering

- **Cluster und SVM**: Die ONTAP Speicher-Back-Ends müssen aktiviert werden. Siehe "Übersicht über Cluster- und SVM-Peering" Finden Sie weitere Informationen.

> Vergewissern Sie sich, dass die in der Replizierungsbeziehung zwischen zwei ONTAP-Clustern verwendeten SVM-Namen eindeutig sind.

- **Astra Control Provisioner und SVM**: Die Peering von Remote-SVMs müssen für die Astra Control Bereitstellung im Ziel-Cluster verfügbar sein.

Unterstützte Treiber

- Die Volume-Replizierung wird von ontap-nas und ontap-san Treibern unterstützt.

Erstellen Sie eine gespiegelte PVC

Führen Sie die folgenden Schritte aus, und verwenden Sie die CRD-Beispiele, um eine Spiegelungsbeziehung zwischen primären und sekundären Volumes zu erstellen.

Schritte

1. Führen Sie auf dem primären Kubernetes-Cluster die folgenden Schritte aus:
   a. Erstellen Sie ein StorageClass-Objekt mit dem `trident.netapp.io/replication: true` Parameter.

Beispiel

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  fsType: "nfs"
  trident.netapp.io/replication: "true"
```

b. PVC mit zuvor erstellter StorageClass erstellen.

Beispiel

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
spec:
  accessModes:
  - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: csi-nas
```

c. Erstellen Sie eine MirrorRelation CR mit lokalen Informationen.

Beispiel

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
```

Astra Control Provisioner ruft die internen Informationen für das Volume und den aktuellen DP-Status des Volumes ab und füllt dann das Statusfeld der MirrorRelationship aus.

d. Holen Sie sich den TridentMirrorRelationship CR, um den internen Namen und die SVM der PVC zu erhalten.

```
kubectl get tmr csi-nas
```

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
  generation: 1
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
status:
  conditions:
  - state: promoted
    localVolumeHandle:
"datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
    localPVCName: csi-nas
    observedGeneration: 1
```

2. Führen Sie auf dem sekundären Kubernetes-Cluster die folgenden Schritte aus:
   a. Erstellen Sie eine StorageClass mit dem Parameter trident.netapp.io/replication: true.

      Beispiel

      ```
      apiVersion: storage.k8s.io/v1
      kind: StorageClass
      metadata:
        name: csi-nas
      provisioner: csi.trident.netapp.io
      parameters:
        trident.netapp.io/replication: true
      ```

   b. Erstellen Sie eine MirrorRelationship-CR mit Ziel- und Quellinformationen.

Beispiel

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  state: established
  volumeMappings:
  - localPVCName: csi-nas
    remoteVolumeHandle:
"datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
```

Astra Control Provisioner erstellt eine SnapMirror Beziehung zum Namen der konfigurierten Beziehungsrichtlinie (oder dem Standard für ONTAP) und initialisiert sie.

c. PVC mit zuvor erstellter StorageClass erstellen, um als sekundäres Ziel zu fungieren (SnapMirror Ziel).

Beispiel

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
  annotations:
    trident.netapp.io/mirrorRelationship: csi-nas
spec:
  accessModes:
  - ReadWriteMany
resources:
  requests:
    storage: 1Gi
storageClassName: csi-nas
```

Astra Control Provisioner überprüft die CRD für die TridentMirrorRelationship und erstellt das Volume nicht, wenn die Beziehung nicht vorhanden ist. Falls die Beziehung besteht, stellt Astra Control Provisioner sicher, dass das neue FlexVol Volume auf eine SVM platziert wird, die mit der in MirrorRelation definierten Remote SVM verbunden ist.

Volume-Replikationsstatus

Eine Trident Mirror-Beziehung (TMR) ist eine CRD, die ein Ende einer Replizierungsbeziehung zwischen PVCs darstellt. Das Ziel-TMR verfügt über einen Status, der Astra Control Provisioner über den gewünschten Status informiert. Das Ziel-TMR hat die folgenden Zustände:

- **Etabliert**: Die lokale PVC ist das Zielvolumen einer Spiegelbeziehung, und das ist eine neue Beziehung.
- **Befördert**: Die lokale PVC ist ReadWrite und montierbar, ohne dass aktuell eine Spiegelbeziehung besteht.

- **Wiederhergestellt**: Die lokale PVC ist das Zielvolumen einer Spiegelbeziehung und war zuvor auch in dieser Spiegelbeziehung.
  - Der neu eingerichtete Status muss verwendet werden, wenn das Ziel-Volume jemals in einer Beziehung zum Quell-Volume stand, da es den Inhalt des Ziel-Volume überschreibt.
  - Der neu eingerichtete Status schlägt fehl, wenn das Volume zuvor nicht in einer Beziehung zur Quelle stand.

Fördern Sie die sekundäre PVC während eines ungeplanten Failover

Führen Sie den folgenden Schritt auf dem sekundären Kubernetes-Cluster aus:

- Aktualisieren Sie das Feld *spec.State* von TridentMirrorRelationship auf `promoted`.

Fördern Sie die sekundäre PVC während eines geplanten Failover

Führen Sie während eines geplanten Failover (Migration) die folgenden Schritte durch, um die sekundäre PVC hochzustufen:

Schritte

1. Erstellen Sie auf dem primären Kubernetes-Cluster einen Snapshot der PVC und warten Sie, bis der Snapshot erstellt wurde.
2. Erstellen Sie auf dem primären Kubernetes-Cluster SnapshotInfo CR, um interne Details zu erhalten.

   Beispiel

   ```
   kind: SnapshotInfo
   apiVersion: trident.netapp.io/v1
   metadata:
     name: csi-nas
   spec:
     snapshot-name: csi-nas-snapshot
   ```

3. Aktualisieren Sie im sekundären Kubernetes-Cluster das Feld *spec.State* des *tridentMirrorRelationship* CR auf *promoted* und *spec.promotedSnapshotHandle* als InternalName des Snapshots.
4. Bestätigen Sie auf sekundärem Kubernetes-Cluster den Status (Feld Status.State) von TridentMirrorRelationship auf hochgestuft.

Stellen Sie nach einem Failover eine gespiegelte Beziehung wieder her

Wählen Sie vor dem Wiederherstellen einer Spiegelbeziehung die Seite aus, die Sie als neuen primären festlegen möchten.

Schritte

1. Stellen Sie auf dem sekundären Kubernetes-Cluster sicher, dass die Werte für das Feld *spec.remoteVolumeHandle* auf dem TridentMirrorRelationship aktualisiert werden.
2. Aktualisieren Sie im sekundären Kubernetes-Cluster das Feld *spec.mirror* von TridentMirrorRelationship auf `reestablished`.

Zusätzliche Vorgänge

Astra Control Provisioner unterstützt die folgenden Vorgänge für primäre und sekundäre Volumes:

Replizieren der primären PVC auf eine neue sekundäre PVC

Stellen Sie sicher, dass Sie bereits über eine primäre PVC und eine sekundäre PVC verfügen.

Schritte

1. Löschen Sie die CRDs PersistentVolumeClaim und TridentMirrorRelationship aus dem eingerichteten sekundären Cluster (Ziel).
2. Löschen Sie die CRD für TridentMirrorRelationship aus dem primären (Quell-) Cluster.
3. Erstellen Sie eine neue TRIdentMirrorRelationship CRD auf dem primären (Quell-) Cluster für die neue sekundäre (Ziel-) PVC, die Sie einrichten möchten.

Ändern der Größe einer gespiegelten, primären oder sekundären PVC

Die PVC-Größe kann wie gewohnt geändert werden. ONTAP erweitert automatisch alle Zielflvxole, wenn die Datenmenge die aktuelle Größe überschreitet.

Entfernen Sie die Replikation aus einer PVC

Um die Replikation zu entfernen, führen Sie einen der folgenden Vorgänge auf dem aktuellen sekundären Volume aus:

- Löschen Sie MirrorRelation auf der sekundären PVC. Dadurch wird die Replikationsbeziehung unterbrochen.
- Oder aktualisieren Sie das Feld spec.State auf *promoted*.

Löschen einer PVC (die zuvor gespiegelt wurde)

Astra Control Provisioner überprüft nach replizierten PVCs und gibt die Replizierungsbeziehung frei, bevor versucht wird, das Volume zu löschen.

Löschen eines TMR

Das Löschen eines TMR auf einer Seite einer gespiegelten Beziehung führt dazu, dass der verbleibende TMR in den Status *promoted* übergeht, bevor Astra Control Provisioner den Löschvorgang abgeschlossen hat. Wenn der für den Löschvorgang ausgewählte TMR bereits den Status *promoted* hat, gibt es keine bestehende Spiegelbeziehung und der TMR wird entfernt und Astra Control Provisioner wird die lokale PVC auf *ReadWrite* hochstufen. Durch dieses Löschen werden SnapMirror Metadaten für das lokale Volume in ONTAP freigegeben. Wenn dieses Volume in Zukunft in einer Spiegelbeziehung verwendet wird, muss es beim Erstellen der neuen Spiegelbeziehung ein neues TMR mit einem *established* Volume-Replikationsstatus verwenden.

Aktualisieren Sie Spiegelbeziehungen, wenn ONTAP online ist

Spiegelbeziehungen können jederzeit nach ihrer Einrichtung aktualisiert werden. Sie können das verwenden `state: promoted` Oder `state: reestablished` Felder zum Aktualisieren der Beziehungen.
Wenn Sie ein Zielvolume auf ein reguläres ReadWrite-Volume heraufstufen, können Sie *promotedSnapshotHandle* verwenden, um einen bestimmten Snapshot anzugeben, auf dem das aktuelle Volume wiederhergestellt werden soll.

Aktualisieren Sie Spiegelbeziehungen, wenn ONTAP offline ist

Sie können ein CRD verwenden, um ein SnapMirror Update durchzuführen, ohne dass Astra Control direkt mit dem ONTAP Cluster verbunden ist. Im folgenden Beispielformat finden Sie das TridentActionMirrorUpdate:

Beispiel

```
apiVersion: trident.netapp.io/v1
kind: TridentActionMirrorUpdate
metadata:
  name: update-mirror-b
spec:
  snapshotHandle: "pvc-1234/snapshot-1234"
  tridentMirrorRelationshipName: mirror-b
```

`status.state` Gibt den Status von TridentActionMirrorUpdate CRD wieder. Es kann einen Wert von *suileded*, *in progress* oder *failed* annehmen.

Automatisierung mit Astra Control REST-API

Automatisierung mit der Astra Control REST-API

Astra Control verfügt über EINE REST-API, mit der Sie über eine Programmiersprache oder ein Dienstprogramm wie Curl direkt auf die Astra Control-Funktionalität zugreifen können. Astra Control Implementierungen lassen sich auch über Ansible und andere Automatisierungstechnologien managen.

Zur Einrichtung und zum Management Ihrer Kubernetes-Applikationen können Sie entweder die Astra Control Center-UI oder die Astra Control API verwenden.

Weitere Informationen erhalten Sie im "Astra Automation Dokumentation".

Wissen und Support

Fehlerbehebung

Lernen Sie, wie Sie mit einigen häufigen Problemen umgehen können.

"NetApp Knowledge Base für Astra Control"

Weitere Informationen

- "Hochladen einer Datei an NetApp (Anmeldung erforderlich)"
- "Wie kann ich Dateien manuell auf NetApp hochladen? (Anmeldung erforderlich)"

Holen Sie sich Hilfe

NetApp bietet Unterstützung für Astra Control auf verschiedene Weise. Umfangreiche kostenlose Self-Support-Optionen stehen rund um die Uhr zur Verfügung, wie z. B. Knowledge Base-Artikel (KB) und ein Einseilkanal. Ihr Astra Control-Konto umfasst technischen Remote-Support über eine Web-Ticketausstellung.

Wenn Sie eine Evaluierungslizenz für Astra Control Center haben, können Sie technischen Support erhalten. Eine Case-Erstellung über die NetApp Support Site (NSS) ist jedoch nicht verfügbar. Sie können sich über die Feedback-Option mit dem Support in Verbindung setzen oder den Abschnur-Kanal für den Self-Service nutzen.

Zunächst müssen Sie "Sie aktivieren den Support für Ihre NetApp Seriennummer" Um diese nicht-Self-Service-Support-Optionen zu nutzen. Für Chat- und WebTicketing sowie die Case-Verwaltung ist ein SSO-Konto auf der NetApp Support Site (NSS) erforderlich.

Self-Support-Optionen

Über die Benutzeroberfläche des Astra Control Center können Sie auf Support-Optionen zugreifen, indem Sie im Hauptmenü auf die Registerkarte **Support** klicken.

Diese Optionen stehen rund um die Uhr kostenlos zur Verfügung:

- "**Nutzung der Wissensdatenbank** (Anmeldung erforderlich)": Suchen Sie nach Artikeln, FAQs oder Break Fix Informationen in Bezug auf Astra Control.
- **Siehe die Produktdokumentation**: Dies ist die Dokumentseite, die Sie gerade sehen.
- "* Hilfe erhalten Sie über Discord*": Gehen Sie zum Astra in der Kategorie Pub, um sich mit Kollegen und Experten auszutauschen.
- **Erstellen Sie einen Support Case**: Generieren Sie Support-Bundles, um NetApp Support für die Fehlerbehebung zur Verfügung zu stellen.
- **Geben Sie Feedback zu Astra Control**: Senden Sie eine E-Mail an astra.feedback@netapp.com, um uns Ihre Gedanken, Ideen oder Bedenken mitzuteilen.

Ermöglichen Sie den täglichen Upload geplanter Support-Bundles an NetApp Support

Bei der Installation des Astra Control Center, falls Sie dies angeben `enrolled: true` Für `autoSupport` In der Datei Astra Control Center Custom Resource (CR) (`astra_control_center.yaml`) Werden täglich Support-Pakete automatisch auf die hochgeladen "NetApp Support Website".

Generieren Sie Support Bundle für NetApp Support

Mit Astra Control Center können die Admin-Benutzer Bundles generieren, die Informationen für den NetApp Support enthalten, einschließlich Protokollen, Ereignissen für alle Komponenten der Astra-Implementierung, Kennzahlen und Topologiedaten zu den zu verwaltenden Clustern und Applikationen. Wenn Sie mit dem Internet verbunden sind, können Sie Support Bundles direkt über die Benutzeroberfläche des Astra Control Center auf die NetApp Support Site (NSS) hochladen.

> Die Zeit, die Astra Control Center für die Erstellung des Pakets benötigt, hängt von der Größe Ihrer Astra Control Center-Installation sowie den Parametern des gewünschten Support-Pakets ab. Die Dauer, die Sie bei der Anforderung eines Support-Pakets angegeben haben, gibt die Zeit an, die für die Erzeugung des Pakets benötigt wird (z. B. durch einen kürzeren Zeitraum wird eine schnellere Paketgenerierung beschleunigt).

Bevor Sie beginnen

Ermitteln Sie, ob eine Proxy-Verbindung erforderlich ist, um Pakete auf NSS hochzuladen. Wenn eine Proxy-Verbindung erforderlich ist, überprüfen Sie, ob Astra Control Center für die Verwendung eines Proxy-Servers konfiguriert wurde.

1. Wählen Sie **Konten** > **Verbindungen**.
2. Überprüfen Sie die Proxy-Einstellungen unter **Verbindungseinstellungen**.

Schritte

1. Erstellen Sie einen Fall auf dem NSS-Portal mithilfe der Lizenzseriennummer, die auf der Seite **Support** der Astra Control Center-Benutzeroberfläche aufgeführt ist.
2. Führen Sie die folgenden Schritte durch, um das Support Bundle mithilfe der Astra Control Center-UI zu erstellen:

   a. Wählen Sie auf der Seite **Support** in der Kachel Support Bundle die Option **Erstellen** aus.

   b. Wählen Sie im Fenster **Support Bundle erzeugen** den Zeitrahmen aus.

      Es stehen schnelle oder benutzerdefinierte Zeitrahmen zur Auswahl.

      > Sie können einen benutzerdefinierten Datumsbereich auswählen und einen benutzerdefinierten Zeitraum für den Datumsbereich festlegen.

   c. Nachdem Sie die Auswahl getroffen haben, wählen Sie **Bestätigen**.

   d. Aktivieren Sie das Kontrollkästchen **Paket nach dem Generieren** auf die NetApp Support Site hochladen.

   e. Wählen Sie **Paket Generieren**.

      Wenn das Supportpaket fertig ist, wird eine Benachrichtigung auf der Seite **Konten** > **Benachrichtigung** im Bereich Benachrichtigungen, auf der Seite **Aktivität** und auch in der Benachrichtigungsliste angezeigt (über das Symbol rechts oben in der Benutzeroberfläche).

Wenn die Generierung fehlgeschlagen ist, wird auf der Seite „Paket erstellen“ ein Symbol angezeigt. Klicken Sie auf das Symbol, um die Nachricht anzuzeigen.

Das Benachrichtigungssymbol oben rechts in der Benutzeroberfläche bietet Informationen über Ereignisse im Zusammenhang mit dem Support-Bundle, z. B. wenn das Paket erfolgreich erstellt wurde, wenn die Bundle-Erstellung fehlschlägt, das Bundle nicht hochgeladen werden konnte, wenn das Paket nicht heruntergeladen werden konnte usw.

Wenn Sie eine luftvergoppte Installation haben

Wenn Sie über eine Luftvergast-Installation verfügen, führen Sie die folgenden Schritte aus, nachdem das Support-Paket erstellt wurde.
Wenn das Paket zum Download verfügbar ist, wird das Download-Symbol neben **Erzeugen** im Abschnitt **Support-Pakete** der Seite **Support** angezeigt.

Schritte

1. Klicken Sie auf das Download-Symbol, um das Bundle lokal herunterzuladen.
2. Laden Sie das Paket manuell auf NSS hoch.

   Dazu können Sie eine der folgenden Methoden verwenden:

   - Nutzung "Hochladen von NetApp authentifizierten Dateien (Anmeldung erforderlich)".
   - Befestigen Sie das Paket direkt am NSS-Gehäuse.
   - Verwenden Sie Digital Advisor.

Weitere Informationen

- "Hochladen einer Datei an NetApp (Anmeldung erforderlich)"
- "Wie kann ich Dateien manuell auf NetApp hochladen? (Anmeldung erforderlich)"

Frühere Versionen der Astra Control Center-Dokumentation

Für vorherige Versionen steht eine Dokumentation zur Verfügung.

- "Dokumentation zu Astra Control Center 23.04"
- "Astra Control Center 22.11-Dokumentation"
- "Astra Control Center 22.08-Dokumentation"
- "Astra Control Center 22.04-Dokumentation"
- "Astra Control Center 21.12-Dokumentation"
- "Astra Control Center 21.08-Dokumentation"

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

- "Hinweis für Astra Control Center"

Astra Control API-Lizenz

https://docs.netapp.com/us-en/astra-automation/media/astra-api-license.pdf