Astra Control Center 22.08-Dokumentation

Astra Control Center

NetApp
November 21, 2023

Inhalt

Astra Control Center 22.08-Dokumentation

Versionshinweise

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

- "In dieser Version des Astra Control Center"
- "Bekannte Probleme"
- "Bekannte Probleme bei Astra Data Store und dieser Version des Astra Control Center"
- "Bekannte Einschränkungen"

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

Was ist neu in dieser Version des Astra Control Center

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

8. September 2022 (22.08.1)

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

August 10 2022 (22.08.0)

Neue Funktionen und Support

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

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

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

Bekannte Probleme und Einschränkungen

- "Bekannte Probleme in diesem Release"
- "Bekannte Probleme bei Astra Data Store und dieser Version des Astra Control Center"
- "Bekannte Einschränkungen für diese Version"

26. April 2022 (22.04.0)

Details

Neue Funktionen und Support

- "Implementierung des Astra Data Stores über das Astra Control Center"
- "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 Probleme bei Astra Data Store und dieser Version des Astra Control Center"
- "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 Data Store: Backend-Management und -Monitoring in der Vorschau"
- "Astra Control Center-Upgrades"
- "Red hat OperatorHub-Option zur Installation"

Behobene Probleme

- "Probleme in diesem Release wurden behoben"

Bekannte Probleme und Einschränkungen

- "Bekannte Probleme in diesem Release"
- "Bekannte Probleme mit der Vorschau des Astra Data Stores und dieser Version des Astra Control Center"
- "Bekannte Einschränkungen für diese Version"

August 5 2021 (21.08)

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"
- "Astra Data Store-Dokumentation"
- "Frühere Versionen der Astra Control Center-Dokumentation"

Bekannte Probleme

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

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

Anwendungen

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

Cluster

- wenn die standardmäßige kubeconfig-Datei mehr als einen Kontext enthält

Andere Probleme

- wenn Astra Trident offline ist
- Snapshots können mit Snapshot-Controller-Version 4.2.0 fehlschlagen

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

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

Applikationsklone können nicht mit einer bestimmten Version von PostgreSQL verwendet werden

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

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

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

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

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

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

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

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

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

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.

Snapshots können mit Snapshot-Controller-Version 4.2.0 fehlschlagen

Wenn Sie Kubernetes Snapshot-Controller (auch bekannt als externer Snapshot) Version 4.2.0 mit Kubernetes 1.20 oder 1.21 verwenden, können Snapshots irgendwann fehlschlagen. Um dies zu verhindern, verwenden Sie ein anderes "Unterstützte Version" Von externen Snapshots, wie Version 4.2.1, mit Kubernetes Versionen 1.20 oder 1.21.

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

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

Weitere Informationen

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

Bekannte Probleme bei Astra Data Store und dieser Version des Astra Control Center

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

"Sehen Sie sich diese zusätzlichen bekannten Probleme bei Astra Data Store an" Das könnte sich mit der aktuellen Version des Astra Control Center auch auf das Management des Astra Data Stores auswirken.

Die Volume-Details des Astra Data Store werden auf der Seite Storage Backends der Astra Control Center-Benutzeroberfläche nicht angezeigt

Details wie Kapazität und Durchsatz werden nicht in der UI angezeigt. Wenn dieses Problem auftritt, heben Sie die Verwaltung des Storage-Back-End von und fügen Sie es erneut hinzu.

Um einen Cluster mit Astra Data Store zu verwalten, muss zunächst eine gemanagte System-App entfernt werden

Wenn Sie einem Astra Control Center-Cluster einen Cluster mit Astra Data Store hinzugefügt haben, wird die astrads-System-App standardmäßig als versteckte Anwendung verwaltet. Um das Cluster zu verwalten, müssen Sie zuerst die Astrads-System-App rückgängig machen. Die Verwaltung dieser App kann mit der Astra Control Center-Benutzeroberfläche nicht aufgehoben werden. Verwenden Sie stattdessen eine Astra Control API-Anfrage, um die App manuell zu entfernen:

Details

Schritte

1. Holen Sie sich die ID für den verwalteten Cluster mithilfe dieser API:

```
/accounts/{account_id}/topology/v1/managedClusters
```

Antwort:

```
{
"items": [
{
"type": "application/astra-managedCluster",
"version": "1.1",
"id": "123ab987-0bc0-00d0-a00a-1234567abd8d",
"name": "astrads-cluster-1234567",
...
```

2. Abrufen der App „Managed astrads-System“:

```
/accounts/{account_id}/topology/v2/managedClusters/{managedCluster_id}/apps
```

Antwort:

```
{
  "items": [
    [
      "1b011d11-bb88-40c7-a1a1-ab1234c123d3",
      "astrads-system",
      "ready"
    ]
  ],
  "metadata": {}
}
```

3. Löschen Sie die App astrads-System mit der App-ID, die Sie im vorherigen Schritt erworben haben (`1b011d11-bb88-40c7-a1a1-ab1234c123d3`).

```
/accounts/{account_id}/k8s/v2/apps/{astrads-system_app_id}
```

Weitere Informationen

- "Bekannte Probleme"
- "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

- Klone von über Benutzer mit Pass-by-Reference installierten Applikationen können fehlschlagen
- die einen Zertifikatmanager verwenden, werden nicht unterstützt
- Vom Betreiber bereitgestellte Apps mit OLM-Enabled und Cluster-Scoped werden nicht unterstützt
- Mit Helm 2 implementierte Apps werden nicht unterstützt

Allgemeine Einschränkungen

- S3 Buckets im Astra Control Center berichten nicht über die verfügbare Kapazität
- Astra Control Center überprüft nicht die von Ihnen eingegebenen Details für Ihren Proxy-Server
- Bestehende Verbindungen zu einem Postgres-Pod führen zu Fehlern
- Backups und Snapshots werden während der Entfernung einer Astra Control Center-Instanz nicht aufbewahrt

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 die Konfigurationskarte für kubeadm-config:

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

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

   ```
   apiVersion: v1
   clusters:
   - cluster:
       certificate-authority-data:
   ExAmPLERb2tCcjZ5K3E2Njk4eQotLExAMpLEORCBDRVJUSUZJQ0FURS0txxxxXX==
       server: https://x.x.x.x:6443
     name: xyz-cluster
   contexts:
   - context:
       cluster: xyz-cluster
       namespace: default
       user: kubernetes-admin
     name: kubernetes-admin@kubernetes
   current-context: kubernetes-admin@kubernetes
   ```

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

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

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

Alle `member` Benutzer mit rollenbasierter Zugriffssteuerung nach Namespace-Name/ID können eine

Applikation in einem neuen Namespace im selben Cluster oder einem anderen Cluster im Konto des Unternehmens klonen oder wiederherstellen. Derselbe Benutzer kann jedoch nicht auf die geklonte oder wiederhergestellte Anwendung im neuen Namespace zugreifen. Nachdem ein neuer Namespace durch einen Klon- oder Wiederherstellungsvorgang erstellt wurde, kann der Account-Administrator/-Eigentümer den bearbeiten `member` Benutzerkonto und Aktualisierung von Rollenbeschränkungen für den betroffenen Benutzer, um den Zugriff auf den neuen Namespace zu gewähren.

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.

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

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

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

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

Mit Helm 2 implementierte Apps werden nicht unterstützt

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

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

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

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

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

Bestehende Verbindungen zu einem Postgres-Pod führen zu Fehlern

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

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

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

Weitere Informationen

- "Bekannte Probleme"
- "Bekannte Probleme bei Astra Data Store und dieser Version des Astra Control Center"

Konzepte

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
- Replizierung von Applikationen auf einem Remote-System mit NetApp SnapMirror Technologie
- Migrieren Sie Applikationen und Daten von einem Kubernetes-Cluster zu einem anderen
- Einfaches Klonen von Applikationen aus der Produktion bis hin zur Staging
- Darstellung des Anwendungszustands und des Schutzstatus
- Verwenden Sie eine Benutzeroberfläche oder eine API zur Implementierung Ihrer Backup- und Migrations-Workflows

Implementierungsmodelle

Astra Control ist in zwei Implementierungsmodellen erhältlich:

- **Astra Control Service**: Ein von NetApp gemanagter Service, der applikationskonsistentes Datenmanagement von Kubernetes-Clustern in der Google Kubernetes Engine (GKE) und Azure Kubernetes Service (AKS) ermöglicht.
- **Astra Control Center**: Gemanagte Software für applikationsgerechtes Datenmanagement von Kubernetes-Clustern, die in Ihrer On-Premises-Umgebung ausgeführt 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
Wo wird sie gehostet?	In einer Public Cloud von NetApp ihrer Wahl	In Ihrem bereitgestellten Kubernetes-Cluster
Wie wird sie aktualisiert?	Gemanagt von NetApp	Sie verwalten jegliche Updates

	Astra Control Service	Astra Control Center
Welche Funktionen stehen für das Applikationsdaten management zur Verfügung?	Auf beiden Plattformen laufen dieselben Funktionen, mit Ausnahme des Storage-Backend oder zu externen Services	Auf beiden Plattformen laufen dieselben Funktionen, mit Ausnahme des Storage-Backend oder zu externen Services
Was ist die Back-End-Unterstützung für Storage?	NetApp Cloud-Serviceangebote	• NetApp ONTAP AFF und FAS Systeme • Astra Data Store als Storage-Backend • Cloud Volumes ONTAP Storage Back-End

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 Azure Disk Storage 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 Azure NetApp Files oder NetApp Cloud Volumes Service für Google Cloud als Storage-Backend nutzen, verwendet der Astra Control Service Astra Trident, um persistente Volumes für Ihre Applikationen bereitzustellen.
- 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 Free Plan von Astra Control können Sie bis zu 10 Apps in Ihrem Konto verwalten. Wenn Sie mehr als 10 Apps 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:

- Trident Storage-Back-Ends mit ONTAP 9.5 und höher
- Astra Data Store Storage-Back-Ends

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 AutoSupport und Active IQ Ecosystem integriert, damit Benutzer und NetApp Support Fehlerbehebungs- und Verwendungsinformationen liefern können.

Sie können Astra Control Center mit einer 90-Tage-Evaluierungslizenz ausprobieren. Die Evaluierungsversion wird durch E-Mail- und Community-Optionen (Slack-Kanal) unterstützt. 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".

Astra Control Center erreicht dies:

- Ermittelt Details zum Cluster einschließlich Namespaces und ermöglicht das Definieren und Schützen der Apps.
- Erkennt die Konfiguration Ihrer Astra Trident oder Astra Data Store auf den Clustern, die Sie managen möchten, und ermöglicht Ihnen das Monitoring der Storage-Back-Ends.

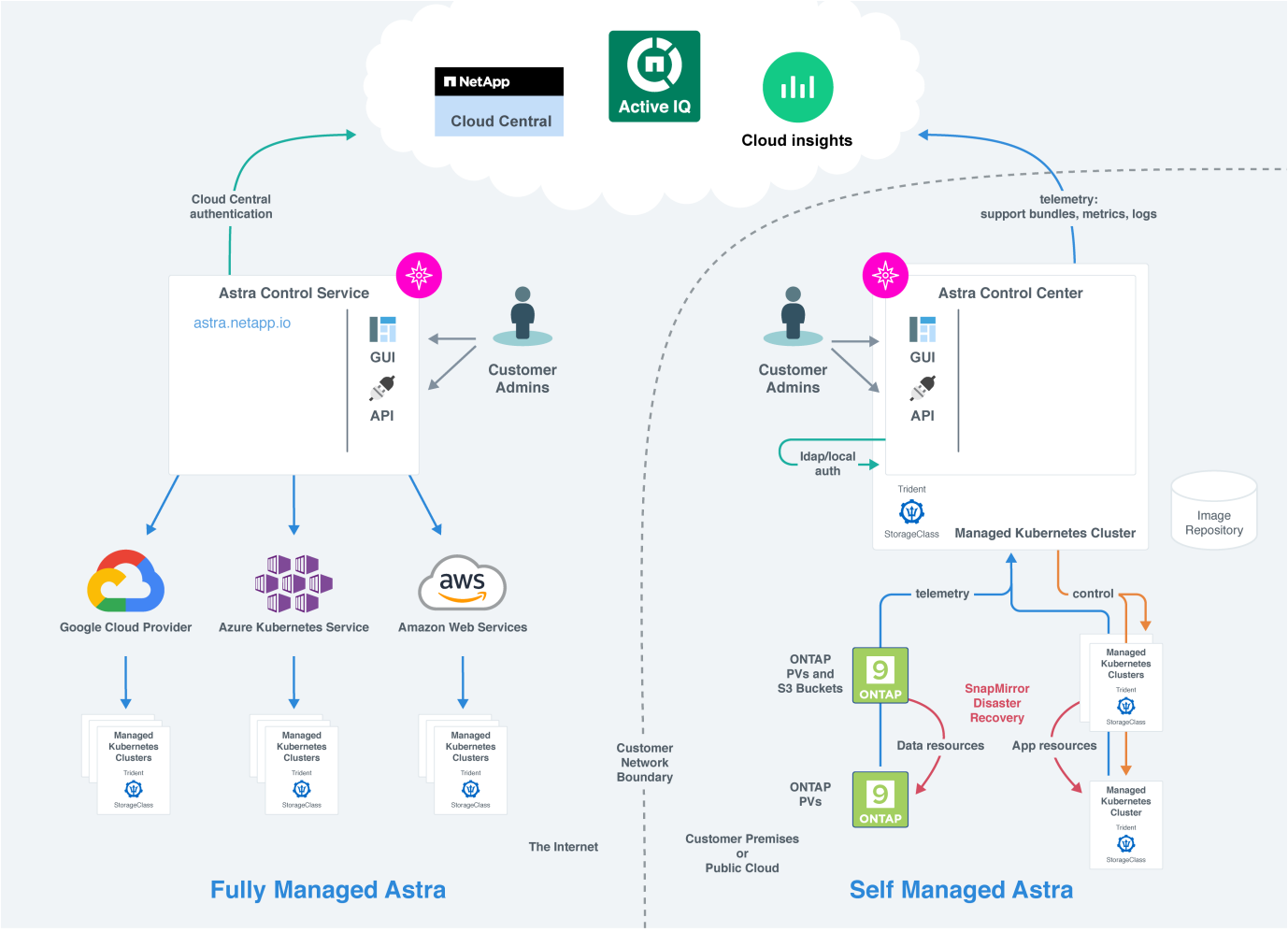
Sie können Applikationen zu Ihrem Cluster hinzufügen. Wenn auch einige Applikationen bereits im Cluster gemanagt werden, können Sie sie mit dem Astra Control Center managen. Nutzen Sie dann das Astra Control Center, um Snapshots, Backups, Klone und Replizierungsbeziehungen zu erstellen.

Finden Sie weitere Informationen

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

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**: Trident ist eine vollständig unterstützte Open-Source-Storage-bereitstellung und -Orchestrierung mit Hilfe von NetApp. Mit Trident können Sie Storage Volumes für Container-Applikationen erstellen, die von Docker und Kubernetes verwaltet werden. Bei der Implementierung mit Astra Control Center umfasst Trident 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 UND FAS. 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 Cloud-Infrastruktur-Monitoring-Tool, überwachen Sie die Performance und Auslastung Ihrer Kubernetes-Cluster und werden von Astra Control Center gemanagt. 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

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.

Ein *Backup* wird im externen Objektspeicher gespeichert und kann 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 Schutzrichtlinie ermöglicht Ihnen darüber hinaus die Auswahl der Anzahl der Snapshots und Backups, die im Zeitplan aufbewahrt werden sollen. Die Automatisierung Ihrer Backups und Snapshots mithilfe einer Schutzrichtlinie stellt sicher, dass jede Applikation den Anforderungen Ihres Unternehmens entsprechend 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.

Klone

Ein *Clone* ist ein exaktes Duplikat einer Applikation, ihrer Konfiguration und des persistenten Storage. 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 in ein Remote-Cluster

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). Sobald Ihre Applikationen konfiguriert sind, können sie Daten und Applikationsänderungen von einem Cluster auf ein anderes replizieren.

Astra Control repliziert asynchron App-Snapshot-Kopien in einem Remote-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**: Astra Control erfordert, dass die Quell- und Ziel-Kubernetes-Cluster mit den

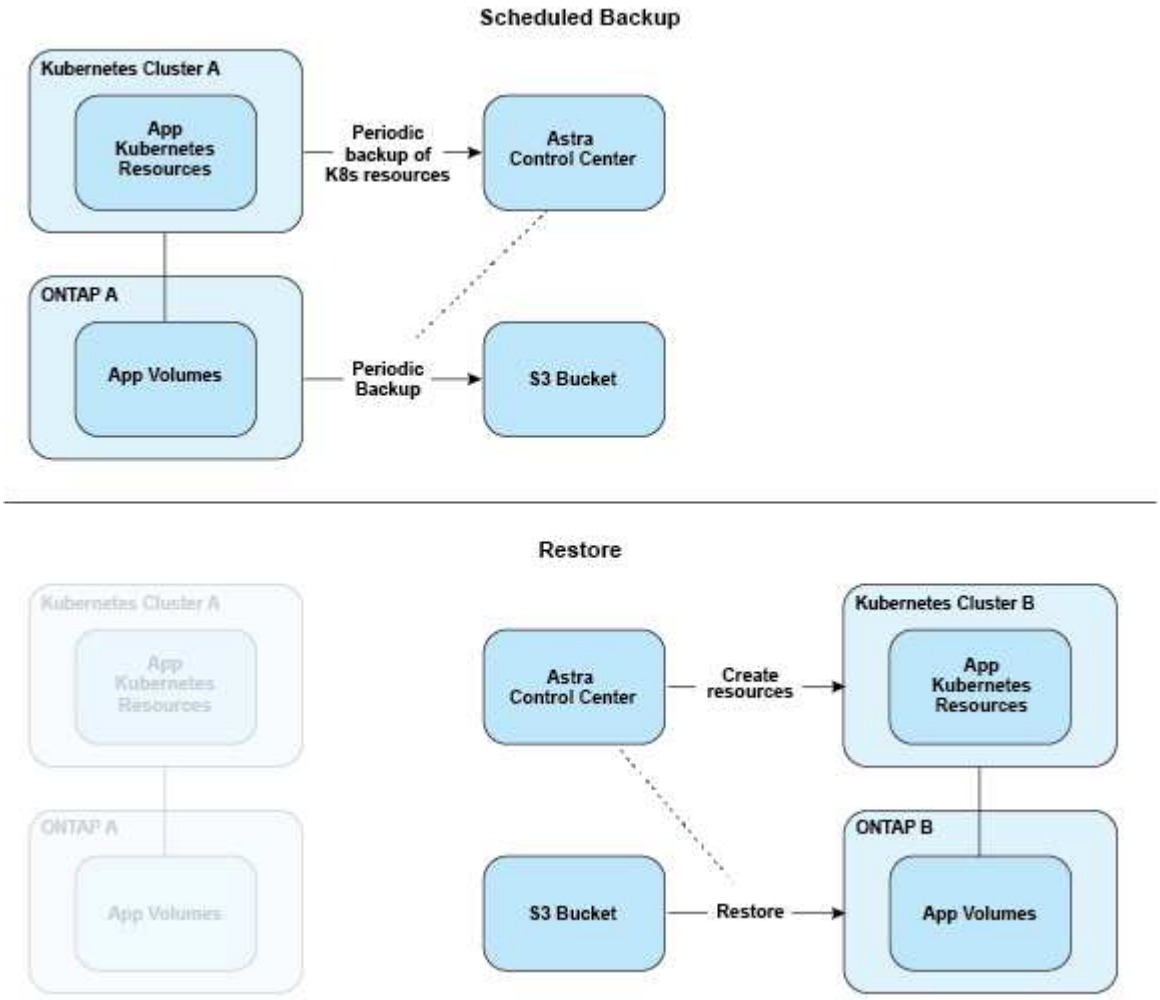
entsprechenden ONTAP Storage-Back-Ends verfügbar und gemanagt werden, die für NetApp SnapMirror konfiguriert sind. Astra Control repliziert den richtlinienbasierten Applikations-Snapshot auf dem Remote-Cluster. NetApp SnapMirror Technologie wird zur Replizierung der Daten des persistenten Volumes verwendet. 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 Daten des persistenten Volumes bereits auf dem Ziel-ONTAP Cluster vorhanden sind, bietet Astra Control kurze Recovery-Zeiten für Failover.

- **App-Backup und -Restore**: Beim Backup von Applikationen erstellt Astra Control einen Snapshot der Applikationsdaten und speichert diese 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 zur Replizierung von Applikationen finden Sie unter "Replizieren von Applikationen auf einem Remote-System mit SnapMirror Technologie".

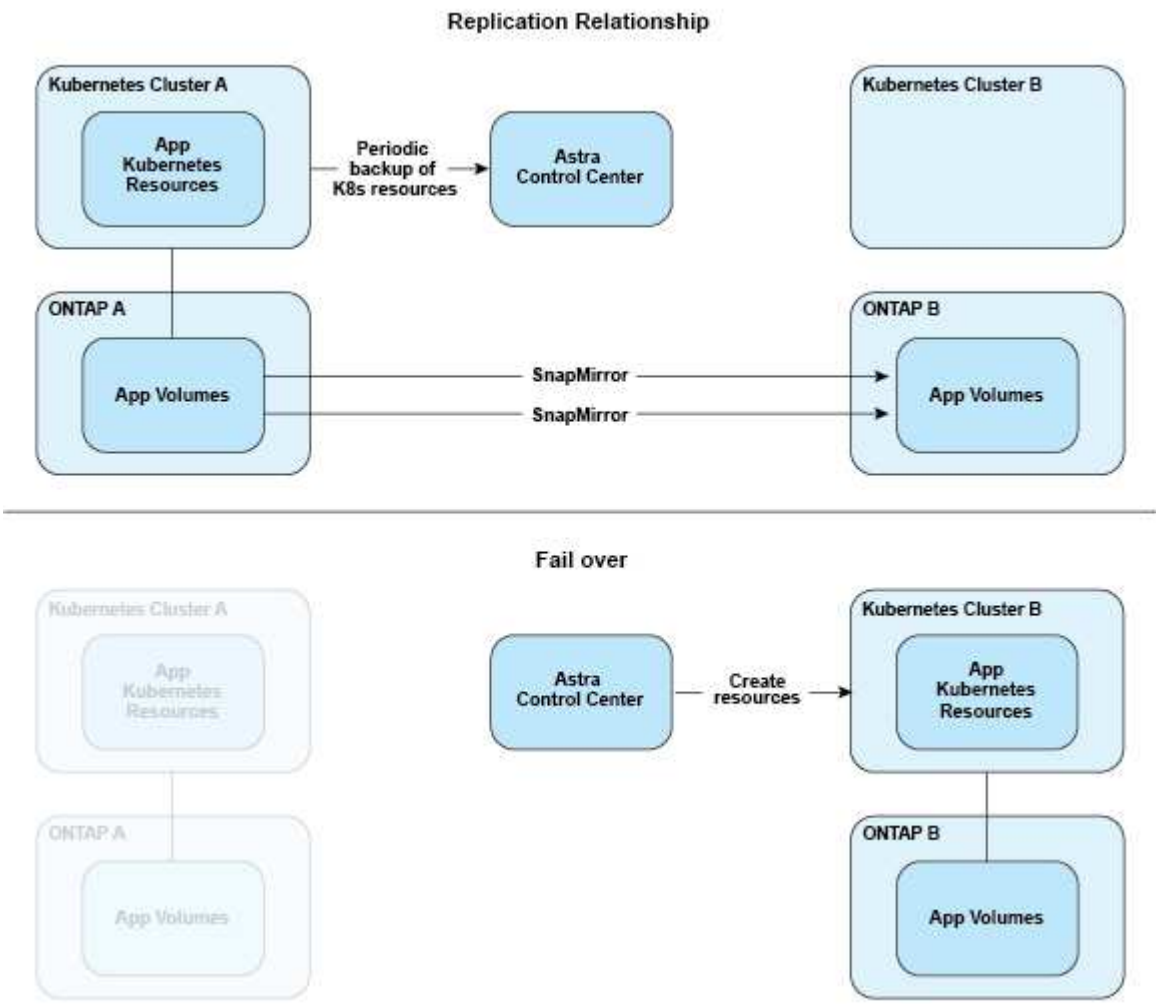
Die folgenden Images zeigen den geplanten Backup- und Wiederherstellungsprozess im Vergleich zum Replikationsprozess.

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



Zum anderen erfolgt die Replizierung auf ONTAP. Bei einem Failover werden die Kubernetes-Ressourcen

erstellt:



Lizenzierung

Astra Control Center erfordert die Installation einer Lizenz, damit die vollständige App-Datenmanagement-Funktion aktiviert werden kann. Wenn Sie Astra Control Center ohne Lizenz bereitstellen, wird in der Web-UI ein Banner angezeigt, in dem Sie darauf hingewiesen werden, dass die Systemfunktionalität begrenzt ist.

Sie benötigen eine Lizenz zum Schutz Ihrer Applikationen und Daten. Siehe Astra Control Center "Funktionen" Entsprechende Details.

Nach dem Kauf des Produkts erhalten Sie eine Seriennummer und eine Lizenz. Sie können die NetApp Lizenzdatei (NetApp License File, NLF) von generieren "NetApp Support Website".

Sie können das Astra Control Center auch mit einer Evaluierungslizenz ausprobieren, mit der Sie das Astra Control Center 90 Tage ab dem Tag, an dem Sie die Lizenz herunterladen, nutzen können. Weitere Informationen finden Sie unter "Anforderungen".

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

Sie können ohne Lizenz ein Cluster hinzufügen, einen Bucket hinzufügen und ein Storage-Backend verwalten.

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 des Astra Control Center enthalten.

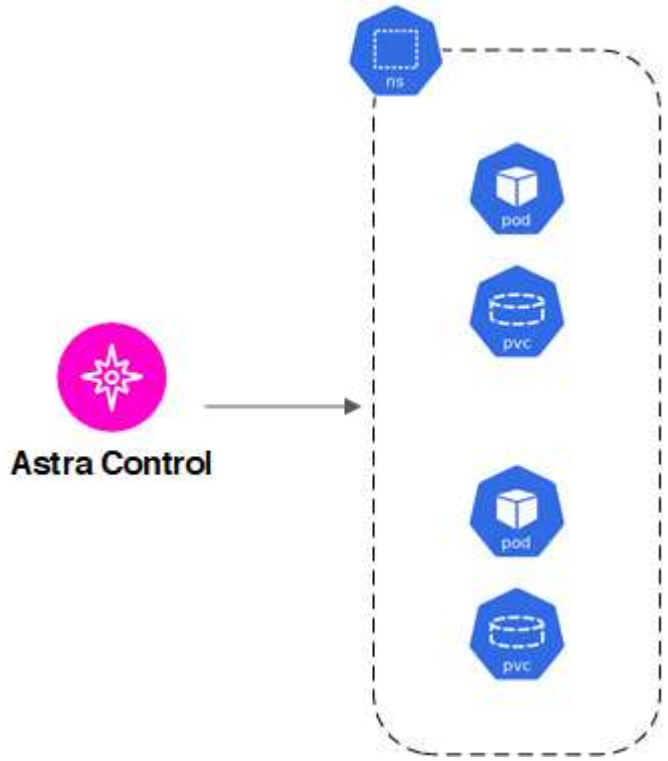
Weitere Informationen

- "Aktualisieren einer vorhandenen Lizenz"

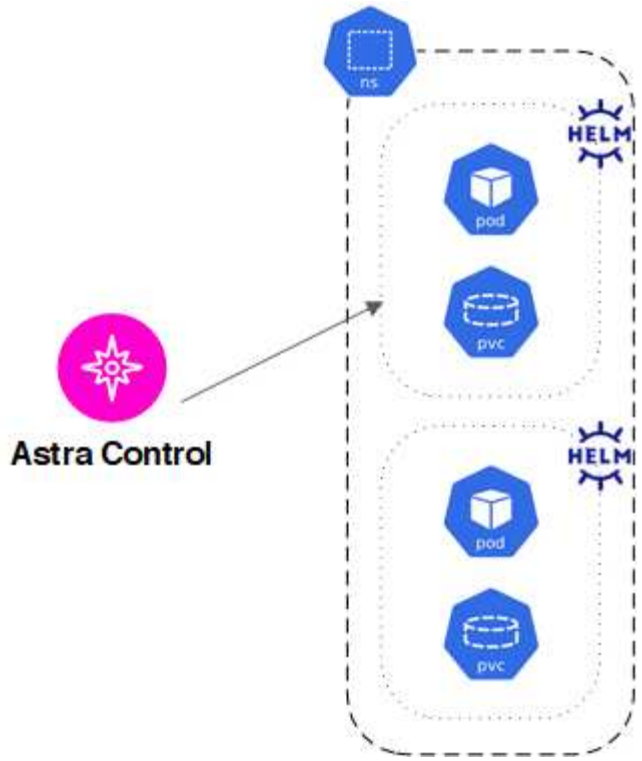
Allgemeines zum Applikationsmanagement

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:

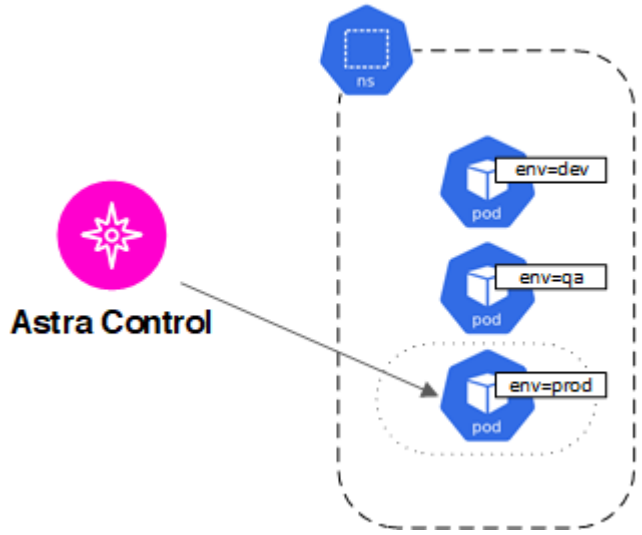
- Einen Namespace, einschließlich aller Ressourcen in diesem Namespace



- Eine individuelle Anwendung innerhalb eines Namespace (in diesem Beispiel wird helm3 verwendet)



- Eine Gruppe von Ressourcen, die innerhalb eines Namespace durch ein Kubernetes-Label identifiziert werden



Storage-Klassen und persistente Volume-Größe

Astra Control Center unterstützt ONTAP oder Astra Data Store als Storage-Backend.

Überblick

Das Astra Control Center unterstützt Folgendes:

- **Trident Storage-Klassen mit Unterstützung von Astra Data Store Storage**: Wenn Sie einen oder mehrere Astra Data Store Cluster manuell installiert haben, bietet Astra Control Center die Möglichkeit,

diese zu importieren und ihre Topologie (Nodes, Festplatten) sowie verschiedene Status abzurufen.

Astra Control Center zeigt das zugrunde liegende Kubernetes Cluster aus der Astra Data Store-Konfiguration, der Cloud, der dem Kubernetes-Cluster angehört, beliebigen persistenten Volumes, die durch Astra Data Store bereitgestellt werden, dem Namen des entsprechenden internen Volumes, der Applikation mit dem persistenten Volume und dem Cluster mit der App an.

- **Trident Storage-Klassen mit ONTAP-Storage**: Wenn Sie ein ONTAP-Back-End verwenden, bietet Astra Control Center die Möglichkeit, das ONTAP-Back-End zu importieren, um verschiedene Monitoring-Informationen zu melden.

Trident Storage-Kurse sollten außerhalb des Astra Control Center vorkonfiguriert sein.

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.

Wenn Sie Astra Control Center nutzen, das mit einem Astra Data Store Storage-Backend integriert ist, sind nach der Installation keine Storage-Klassen definiert. Sie müssen die Standard-Storage-Klasse Trident erstellen und sie auf das Storage-Back-End anwenden. Siehe "Astra Data Store – die ersten Schritte" Um eine Standard-Storage-Klasse Astra Data Store zu erstellen.

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

"Rollen managen"

Los geht’s

Anforderungen des Astra Control Centers

Prüfen Sie zunächst die Bereitschaft Ihrer Betriebsumgebung, Anwendungscluster, Applikationen, Lizenzen und Ihres Webbrowsers.

- Anforderungen an die Betriebsumgebung
- Unterstützte Storage-Back-Ends
- Anforderungen für Applikationscluster
- Anforderungen für das Applikationsmanagement
- Replikationsvoraussetzungen
- Zugang zum Internet
- Lizenz
- Ingress für lokale Kubernetes Cluster
- Netzwerkanforderungen
- Unterstützte Webbrowser

Anforderungen an die Betriebsumgebung

Astra Control Center wurde mit folgenden Typen von Betriebsumgebungen validiert:

- Google Anthos 1.10 oder 1.11
- Kubernetes 1.22 auf 1.24
- Rancher Kubernetes Engine (RKE):
  - RKE 1.2.16 mit Rancher 2.5.12 und RKE 1.3.3 mit 2.6.3
  - RKE 2 (v1.23,6+rke2r2) mit Rancher 2.6.3
- Red hat OpenShift Container Platform 4.8, 4.9 oder 4.10
- VMware Tanzu Kubernetes Grid 1.4 oder 1.5
- VMware Tanzu Kubernetes Grid Integrated Edition 1.12.2 oder 1.13

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
Storage-Back-End-Kapazität	Mindestens 500 GB verfügbar
Worker-Nodes	Insgesamt mindestens 3 Worker-Nodes mit 4 CPU-Kernen und jeweils 12 GB RAM
FQDN-Adresse	Eine FQDN-Adresse für Astra Control Center

Komponente	Anforderungen
Astra Trident	Astra Trident 21.10.1 oder höher ist installiert und konfiguriert Astra Trident 22.07 oder höher für SnapMirror-basierte Applikationsreplizierung

> 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.

- **Image Registry**: Sie benötigen eine bereits vorhandene private Docker-Image-Registry, mit der Sie Astra Control Center-Bilder erstellen können. Sie müssen die URL der Bildregistrierung angeben, in der Sie die Bilder hochladen.
- **Astra Trident / ONTAP Konfiguration**: Astra Control Center erfordert, dass eine Storage-Klasse erstellt und als Standard-Storage-Klasse eingestellt wird. Astra Control Center unterstützt die folgenden ONTAP-Treiber von Astra Trident:
  - ontap-nas
  - ontap-san
  - ontap-san-Ökonomie

> 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`

> Wenn Sie eine zweite OpenShift-Betriebsumgebung als gemanagte Computing-Ressource hinzufügen möchten, müssen Sie sicherstellen, dass die Astra Trident Volume Snapshot-Funktion aktiviert ist. Um Volume Snapshots mit Astra Trident zu aktivieren und zu testen, "Sehen Sie sich die offiziellen Anweisungen von Astra Trident an".

Cluster-Anforderungen für VMware Tanzu Kubernetes Grid

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.

- 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.
- Im Rahmen der Installation von Astra Control Center werden die folgenden Ressourcen in einer Pod Security Policy (PSP)-Umgebung mit eingeschränkter Sicherheit erstellt:
  - POD-Sicherheitsrichtlinie

    - RBAC-Rolle
    - RBAC Rolle und rollenbindende Ressourcen werden in der erstellt `netapp-acc` Namespace.
- 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".

> 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."

Cluster-Anforderungen für Google Anthos

Wenn Sie Astra Control Center auf einem Google Anthos Cluster hosten, beachten Sie, dass Google Anthos standardmäßig den MetalLB Load Balancer und den Istio Ingress Gateway-Dienst enthält. So können Sie die generischen Ingress-Funktionen von Astra Control Center während der Installation einfach nutzen. Siehe "Konfigurieren Sie Astra Control Center" Entsprechende Details.

Unterstützte Storage-Back-Ends

Astra Control Center unterstützt folgende Storage-Back-Ends.

- NetApp ONTAP 9.5 oder neuere AFF und FAS Systeme
- NetApp ONTAP 9.8 oder neuere AFF und FAS Systeme für SnapMirror-basierte Applikationsreplizierung
- NetApp Cloud Volumes ONTAP

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

Sie können überprüfen, ob Ihr ONTAP System über die erforderlichen Lizenzen verfügt. Siehe "Managen Sie ONTAP Lizenzen".

Anforderungen für Applikationscluster

Astra Control Center hat folgende Anforderungen für Cluster, die Sie über das Astra Control Center verwalten möchten. Diese Anforderungen gelten auch, wenn der zu verwaltende Cluster der Betriebsumgebung ist, der das Astra Control Center hostet.

- Die neueste Version von Kubernetes "snapshot-Controller-Komponente" Installiert ist
- Astra Trident "Objekt der Volumesnapshotklasse" Wurde von einem Administrator definiert
- Im Cluster ist eine standardmäßige Kubernetes-Storage-Klasse vorhanden
- Mindestens eine Storage-Klasse ist für die Verwendung von Astra Trident konfiguriert

Ihr Applikations-Cluster sollte einen haben `kubeconfig.yaml` Datei, die nur ein *context* -Element definiert. In der Kubernetes-Dokumentation für finden Sie "Informationen zum Erstellen von kubeconfig-Dateien".

Wenn Sie Anwendungscluster in einer Rancher-Umgebung verwalten, ändern Sie den Standardkontext des Anwendungsclusters im `kubeconfig` Die von Rancher bereitgestellte Datei verwendet anstelle des Rancher API-Serverkontexts einen Steuerebenen-Kontext. So wird die Last auf dem Rancher API Server reduziert und die Performance verbessert.

Anforderungen für das Applikationsmanagement

Astra Control verfügt über folgende Anforderungen an das Applikationsmanagement:

- **Lizenzierung**: Zur Verwaltung von Anwendungen mit dem Astra Control Center benötigen Sie eine Astra Control Center-Lizenz.
- **Namesaces**: Astra Control erfordert, dass eine App nicht mehr als einen Single Namespace umfasst, aber ein Namespace kann mehr als eine App enthalten.
- **StorageClass**: Wenn Sie eine Anwendung mit einem explizit eingestellten StorageClass installieren und die App klonen müssen, muss das Zielcluster für den Klonvorgang die ursprünglich angegebene StorageClass haben. Das Klonen einer Applikation, deren StorageClass explizit auf ein Cluster festgelegt ist, das nicht über dieselbe StorageClass verfügt, 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:

ClusterCole	ClusterrollenBding	Konfigmap
Kronjob	KundenressourcenDefinition	Benutzerressource
DemonSet	BereitstellungConfig	Horizon PodAutoscaler
Eindringen	MutatingWebhook	Netzwerkrichtlinie
PersistentVolumeClaim	Pod	PodDisruptionBudget
PodTemplate	ReplicaSet	Rolle
Rollenverschwarten	Route	Geheim
Service	Service Account	StatfulSet
ValidierenWebhook		

Replikationsvoraussetzungen

Die Astra Control Applikationsreplizierung erfordert, dass die folgenden Voraussetzungen erfüllt sein müssen, bevor Sie beginnen:

- Um eine nahtlose Disaster Recovery zu erreichen, empfehlen wir Ihnen, Astra Control Center in einer dritten Fehlerdomäne oder an einem sekundären Standort einzusetzen.
- Das Kubernetes-Cluster der Applikation und ein Kubernetes Ziel-Cluster müssen verfügbar und mit zwei ONTAP Clustern verbunden sein, im Idealfall für unterschiedliche Ausfall-Domains oder Standorte.

- ONTAP-Cluster und die Host-SVM müssen gekoppelt sein. Siehe "Übersicht über Cluster- und SVM-Peering".
- Die gekoppelte Remote SVM muss für Trident auf dem Ziel-Cluster verfügbar sein.
- Trident Version 22.07 oder höher muss sowohl auf den Quell- als auch Ziel-ONTAP Clustern vorhanden sein.
- Asynchrone ONTAP SnapMirror Lizenzen mit dem Datensicherungs-Bundle müssen sowohl auf den Quell- als auch auf den Ziel-ONTAP Clustern aktiviert werden. Siehe "Übersicht über die SnapMirror Lizenzierung in ONTAP".
- Wenn Sie dem Astra Control Center ein ONTAP-Speicher-Backend hinzufügen, wenden Sie die Benutzeranmeldeinformationen auf die Rolle „Admin“ an, die über Zugriffsmethoden verfügt `http` Und `ontapi` Auf beiden ONTAP Clustern aktiviert. Siehe "Benutzerkonten Verwalten" Finden Sie weitere Informationen.
- Sowohl Quell- als auch Ziel-Kubernetes-Cluster als auch ONTAP-Cluster müssen von Astra Control gemanagt werden.

> Sie können gleichzeitig eine andere Applikation (auf dem anderen Cluster oder Standort ausgeführt) 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.

Erfahren Sie, wie Sie "Replizieren von Applikationen auf einem Remote-System mit SnapMirror Technologie".

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 Betreibern mit Namespace-Scoped installiert sind. Im Folgenden sind einige Apps aufgeführt, die für dieses Installationsmodell validiert wurden:
  - "Apache K8ssandra"
  - "Jenkins CI"
  - "Percona XtraDB Cluster"

> Ein Operator und die von ihm zu installieren App müssen denselben Namespace verwenden. Möglicherweise müssen Sie die yaml-Bereitstellungsdatei ändern, um sicherzustellen, dass dies der Fall ist.

Zugang zum Internet

Sie sollten feststellen, ob Sie einen externen Zugang zum Internet 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".

Lizenz

Astra Control Center erfordert eine Astra Control Center-Lizenz für die volle Funktionalität. Anfordern einer Evaluierungslizenz oder Volllizenz von NetApp. Sie benötigen eine Lizenz zum Schutz Ihrer Applikationen und Daten. Siehe "Funktionen des Astra Control Center" Entsprechende Details.

Sie können Astra Control Center mit einer Evaluierungslizenz ausprobieren, mit der Sie das Astra Control Center 90 Tage ab dem Tag, an dem Sie die Lizenz herunterladen, nutzen können. Sie können sich durch die Anmeldung für eine kostenlose Testversion anmelden "Hier".

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

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

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 mit dem MetalLB Load Balancer dem Dienst automatisch eine externe IP-Adresse zuweisen. In der Konfiguration des internen DNS-Servers sollten Sie den ausgewählten DNS-Namen für Astra Control Center auf die Load-Balanced IP-Adresse verweisen.

> Wenn Sie Astra Control Center auf einem Tanzu Kubernetes Grid Cluster hosten, nutzen Sie den `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.

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

Netzwerkanforderungen

Die Betriebsumgebung, die als Host für Astra Control Center fungiert, 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 auf beiden Wegen zwischen dem Cluster geöffnet ist, der Astra Control Center hostet, und jedem verwalteten Cluster
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)
Astra Control Center	Gehosteter Cloud Insights Service	443	HTTPS	Cloud Insights Kommunikation
Astra Control Center	Amazon S3 Storage-Bucket-Provider	443	HTTPS	Amazon S3 Storage-Kommunikation
Astra Control Center	NetApp AutoSupport	443	HTTPS	Kommunikation zwischen NetApp AutoSupport

Unterstützte Webbrowser

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

Wie es weiter geht

Sehen Sie sich die an "Schnellstart" Überblick.

Schnellstart für Astra Control Center

Diese Seite bietet einen Überblick 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.

Probieren Sie es aus! Wenn Sie Astra Control Center ausprobieren möchten, können Sie eine 90-Tage-Evaluierungslizenz verwenden. Siehe "Lizenzierungsinformationen" Entsprechende Details.

1 Kubernetes-Cluster-Anforderungen prüfen

- Astra arbeitet mit Kubernetes-Clustern mit einem in Trident konfigurierten ONTAP-Storage-Back-End oder einem Astra Data Store Storage-Backend.
- Cluster müssen in einem ordnungsgemäßen Zustand mit mindestens drei Online-Worker-Nodes ausgeführt werden.
- Der Cluster muss Kubernetes ausführen.

Erfahren Sie mehr über das "Anforderungen des Astra Control Centers".

2 Laden Sie Astra Control Center herunter und installieren Sie es

- Laden Sie das Astra Control Center von der herunter "NetApp Support Site Astra Control Center Download-Seite".
- Installieren Sie Astra Control Center in Ihrer lokalen Umgebung.

  Optional können Sie Astra Control Center mit Red hat OperatorHub installieren.

  Optional kann Astra Control Center mit einem Cloud Volumes ONTAP Storage-Backend installiert werden.

Weitere Informationen zu "Installieren des Astra Control Center".

3 Führen Sie einige erste Setup-Aufgaben aus

- Fügen Sie eine Astra Control-Lizenz und alle unterstützenden ONTAP-Lizenzen hinzu.
- Ein Kubernetes Cluster hinzufügen und Astra Control Center erkennt Details.
- Fügen Sie ein ONTAP-Storage-Back-End hinzu.
- Optional können Sie einen Objektspeicher-Bucket hinzufügen, der Ihre Applikations-Backups speichert.

Erfahren Sie mehr über das "Initialer Einrichtungsvorgang".

4 Nutzen Sie Das Astra Control Center

Nachdem Sie das Astra Control Center eingerichtet haben, können Sie folgende Schritte ausführen:

- Eine App verwalten. Erfahren Sie mehr darüber, wie Sie "Applikationsmanagement".
- Schützen Sie Applikationen durch die Konfiguration von Sicherheitsrichtlinien für Applikationen, das Replizieren von Applikationen auf Remote-Systeme und das Klonen und Migrieren von Applikationen. Erfahren Sie mehr darüber, wie Sie "Schützen von Applikationen".
- Konten verwalten (einschließlich Benutzer, Rollen, LDAP zur Benutzerauthentifizierung, Anmeldedaten, Repository-Verbindungen usw.). Erfahren Sie mehr darüber, wie Sie "Benutzer managen".
- Optional können Sie eine Verbindung zu NetApp Cloud Insights herstellen, um Kennzahlen zum Zustand von System, Kapazität und Durchsatz innerhalb der Astra Control Center UI anzuzeigen. Weitere Informationen zu "Verbindung zu Cloud Insights wird hergestellt".

5 **Fahren Sie mit dieser Schnellstartanleitung fort**

"Installieren Sie Astra Control Center".

Weitere Informationen

- "Verwenden Sie die Astra Control API"

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"

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, um Astra Control Center Operator und Astra Control Center in Ihrer Umgebung zu installieren. Mit diesem Verfahren können Sie Astra Control Center in Internet-angeschlossenen oder luftgekapderten Umgebungen installieren.

Für Red hat OpenShift-Umgebungen können Sie ein verwenden "Alternativverfahren" So installieren Sie Astra Control Center mithilfe des OpenShift OperatorHub.

Was Sie benötigen

- "Bevor Sie mit der Installation beginnen, bereiten Sie Ihre Umgebung auf die Implementierung des Astra Control Center vor".
- Wenn Sie POD-Sicherheitsrichtlinien in Ihrer Umgebung konfiguriert haben oder konfigurieren möchten, sollten Sie sich mit den POD-Sicherheitsrichtlinien vertraut machen und wie diese sich auf die Installation des Astra Control Center auswirken. Siehe "Einschränkungen der POD-Sicherheitsrichtlinie verstehen".
- Stellen Sie sicher, dass alle Cluster Operator in einem ordnungsgemäßen Zustand und verfügbar sind.

  ```
  kubectl get clusteroperators
  ```

- Stellen Sie sicher, dass alle API-Services in einem ordnungsgemäßen Zustand und verfügbar sind:

  ```
  kubectl get apiservices
  ```

- Stellen Sie sicher, dass der Astra FQDN, den Sie verwenden möchten, für diesen Cluster routingfähig ist. Das bedeutet, dass Sie entweder einen DNS-Eintrag in Ihrem internen DNS-Server haben oder eine bereits registrierte Core URL-Route verwenden.
- Wenn bereits ein Zertifikat-Manager im Cluster vorhanden ist, müssen Sie einen Teil durchführen "Erforderliche Schritte" Damit Astra Control Center nicht seinen eigenen Cert-Manager installiert.

Über diese Aufgabe

Der Astra Control Center-Installationsprozess führt Folgendes aus:

- Installiert die Astra-Komponenten im `netapp-acc` (Oder Name des benutzerdefinierten Namespace).
- Erstellt ein Standardkonto.
- Richtet eine standardmäßige E-Mail-Adresse für Administratorbenutzer und ein Standardpasswort ein. Diesem Benutzer wird die Owner-Rolle im System zugewiesen, die für die erste Anmeldung bei der UI erforderlich ist.
- Hilft Ihnen bei der Ermittlung, dass alle Astra Control Center-Pods ausgeführt werden.
- Installiert die Astra UI

> (Gilt nur für die Version des Astra Data Store Early Access Program (EAP). Wenn Sie den Astra Data Store über das Astra Control Center verwalten und VMware-Workflows aktivieren möchten, implementieren Sie Astra Control Center nur auf dem `pcloud` Und nicht auf dem `netapp-acc` Namespace oder ein benutzerdefinierter Namespace, der in den Schritten dieses Verfahrens beschrieben wird.

> Führen Sie den folgenden Befehl während der gesamten Installation nicht aus, um zu vermeiden, dass alle Astra Control Center Pods gelöscht werden: `kubectl delete -f astra_control_center_operator_deploy.yaml`

> Wenn Sie Podman von Red hat anstelle von Docker Engine verwenden, können Podman-Befehle anstelle von Docker-Befehlen verwendet werden.

Schritte

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

- Laden Sie das Astra Control Center Bundle herunter und entpacken Sie es aus
- 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

Laden Sie das Astra Control Center Bundle herunter und entpacken Sie es aus

1. Laden Sie das Astra Control Center Bundle herunter (`astra-control-center-[version].tar.gz`) Vom "NetApp Support Website".
2. Laden Sie den Zip der Astra Control Center Zertifikate und Schlüssel aus dem herunter "NetApp Support Website".
3. (Optional) Überprüfen Sie mit dem folgenden Befehl die Signatur des Pakets:

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

4. Extrahieren Sie die Bilder:

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

Installieren Sie das NetApp Astra kubectl Plug-in

Der NetApp Astra `kubectl` Kommandozeilen-Plugin spart Zeit bei der Ausführung von Routineaufgaben im Zusammenhang mit der Bereitstellung und dem Upgrade von Astra Control Center.

Was Sie benötigen

NetApp bietet Binärdateien für das Plug-in für verschiedene CPU-Architekturen und Betriebssysteme. Sie müssen wissen, welche CPU und welches Betriebssystem Sie haben, bevor Sie diese Aufgabe ausführen. Unter Linux- und Mac-Betriebssystemen können Sie die verwenden `uname -a` Befehl zum Sammeln dieser Informationen.

Schritte

1. Nennen Sie den verfügbaren NetApp Astra `kubectl` Plugin-Binärdateien, und notieren Sie den Namen der Datei, die Sie für Ihr Betriebssystem und CPU-Architektur benötigen:

```
ls kubectl-astra/
```

2. Kopieren Sie die Datei an denselben Speicherort wie der Standard `kubectl` Utility: In diesem Beispiel ist der `kubectl` Das Dienstprogramm befindet sich im `/usr/local/bin` Verzeichnis. Austausch `<binary-name>` Mit dem Namen der benötigten Datei:

```
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 Astra-Verzeichnis:

```
cd acc
```

2. Schieben Sie die Paketbilder im Astra Control Center-Bildverzeichnis in Ihre lokale Registrierung. Führen Sie folgende Ersetzungen durch, bevor Sie den Befehl ausführen:
   - ERSETZEN SIE DIE BUNDLE_FILE durch den Namen der Astra Control Bundle-Datei (z. B. `acc.manifest.yaml`).
   - ERSETZEN SIE MY_REGISTRY durch die URL des Docker Repositorys.
   - 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_REGISTRY
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

Podman

1. Melden Sie sich bei Ihrer Registrierung an:

```
podman login [your_registry_path]
```

2. Führen Sie das folgende Skript aus und machen Sie die Substitution <YOUR_REGISTRY> wie in den Kommentaren angegeben:

```
# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
  # Load to local cache
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')

  # Remove path and keep imageName.
  astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')

  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

  # Push to the local repo.
  podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

Einrichten von Namespace und Geheimdienstraum für Registrys mit auth Anforderungen

1. Exportieren Sie den KUBECONFIG für den Hostcluster Astra Control Center:

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

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

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

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

   Antwort:

```
namespace/netapp-acc-operator created
```

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/22.08.1-26`).

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

Beispielantwort:

```
secret/astra-registry-cred created
```

> Wenn Sie den Namespace löschen, nachdem das Geheimnis generiert wurde, müssen Sie das Geheimnis für den Namespace neu generieren, nachdem der Namespace neu erstellt wurde.

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

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

Beispielantwort:

```
namespace/netapp-acc created
```

d. Erstellen Sie ein Geheimnis für das `netapp-acc` (Oder benutzerdefinierter Name) 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]
```

Antwort

```
secret/astra-registry-cred created
```

a. (Optional) Wenn Sie möchten, dass der Cluster nach der Installation automatisch vom Astra Control Center verwaltet wird, stellen Sie sicher, dass Sie den kubeconfig als Geheimnis innerhalb des Astra Control Center Namespace angeben, in dem Sie diesen Befehl einsetzen möchten:

```
kubectl create secret generic [acc-kubeconfig-cred or custom secret
name] --from-file=<path-to-your-kubeconfig> -n [netapp-acc or custom
namespace]
```

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 `[your_registry_path]` Für das `kube-rbac-proxy` Bild zum Registrierungspfad, in dem Sie die Bilder in ein geschoben haben Vorheriger Schritt.

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

d. (Für Installationen mit Astra Data Store Vorschau) Siehe dieses bekannte Problem bzgl. "Provisorer der Speicherklasse und zusätzliche Änderungen, die Sie an der YAML vornehmen müssen".

```
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
  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: [your_registry_path]/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
        command:
        - /manager
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        image: [your_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

3. Installieren Sie den Astra Control Center-Operator:

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

Beispielantwort:

```
namespace/netapp-acc-operator created
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.astra.
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_min.yaml`) Um Konto, AutoSupport, Registrierung und andere notwendige Konfigurationen zu machen:

> `astra_control_center_min.yaml` Ist die Standard-CR und ist für die meisten Installationen geeignet. Machen Sie sich mit allen vertraut "CR-Optionen und ihre potenziellen Werte" Damit Sie Astra Control Center richtig für Ihre Umgebung einsetzen können. Falls für Ihre Umgebung zusätzliche Anpassungen erforderlich sind, können Sie dies verwenden `astra_control_center.yaml` Als Alternative CR.

```
vim astra_control_center_min.yaml
```

> Wenn Sie eine Registrierung verwenden, für die keine Autorisierung erforderlich ist, müssen Sie das löschen `secret` Zeile in `imageRegistry` Oder die Installation schlägt fehl.

a. Ändern `[your_registry_path]` Zum Registrierungspfad, in dem Sie die Bilder im vorherigen Schritt verschoben haben.

b. Ändern Sie das `accountName` Zeichenfolge an den Namen, den Sie dem Konto zuordnen möchten.

c. Ändern Sie das `astraAddress` Zeichenfolge an den FQDN, den Sie in Ihrem Browser für den Zugriff auf Astra verwenden möchten. Verwenden Sie es nicht `http://` Oder `https://` In der Adresse. Kopieren Sie diesen FQDN zur Verwendung in einem Später Schritt.

d. Ändern Sie das `email` Zeichenfolge zur standardmäßigen ursprünglichen Administratoradresse. Kopieren Sie diese E-Mail-Adresse zur Verwendung in A Später Schritt.

e. Ändern `enrolled` Für AutoSupport bis `false` Für Websites ohne Internetverbindung oder Aufbewahrung `true` Für verbundene Standorte.

f. Wenn Sie einen externen Zertifikaten-Manager verwenden, fügen Sie folgende Zeilen zu hinzu `spec`:

```
spec:
  crds:
    externalCertManager: true
```

g. (Optional) Geben Sie einen Vornamen ein `firstName` Und Nachname `lastName` Des Benutzers, der dem Konto zugeordnet ist. Sie können diesen Schritt jetzt oder später in der Benutzeroberfläche ausführen.

h. (Optional) Ändern Sie den `storageClass` Nutzen Sie bei Bedarf für Ihre Installation einen anderen Trident Storage Class-Mitarbeiter.

i. (Optional) Wenn der Cluster nach der Installation automatisch von Astra Control Center verwaltet werden soll und schon vorhanden ist Schuf das Geheimnis, das den kubeconfig für diesen Cluster enthältGeben Sie den Namen des Geheimnisses an, indem Sie dieser YAML-Datei ein neues Feld hinzufügen `astraKubeConfigSecret: "acc-kubeconfig-cred or custom secret name"`

j. Führen Sie einen der folgenden Schritte aus:

- **Anderer Ingress-Controller (ingressType:Generic)**: Dies ist die Standard-Aktion mit Astra Control Center. Nachdem Astra Control Center bereitgestellt wurde, müssen Sie den Ingress-Controller so konfigurieren, dass Astra Control Center mit einer URL verfügbar ist.

  Die standardmäßige Astra Control Center-Installation stellt das Gateway ein (`service/traefik`) Vom Typ zu sein `ClusterIP`. Bei dieser Standardinstallation müssen Sie zusätzlich einen Kubernetes ProgressController/Ingress einrichten, um den Datenverkehr dorthin zu leiten. Wenn Sie ein Ingress verwenden möchten, lesen Sie "Eindringen für den Lastenausgleich einrichten".

- **Service Load Balancer (ingressType:AccTraefik)**: Wenn Sie keinen IngressController installieren oder eine Ingress-Ressource erstellen möchten, stellen Sie ein `ingressType` Bis `AccTraefik`.

  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 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 nicht eine 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.

Einzelheiten zum Servicetyp von „loadbalancer“ und Ingress finden Sie unter "Anforderungen".

```
apiVersion: astra.netapp.io/v1
kind: AstraControlCenter
metadata:
  name: astra
spec:
  accountName: "Example"
  astraVersion: "ASTRA_VERSION"
  astraAddress: "astra.example.com"
  astraKubeConfigSecret: "acc-kubeconfig-cred or custom secret name"
  ingressType: "Generic"
  autoSupport:
    enrolled: true
  email: "[admin@example.com]"
  firstName: "SRE"
  lastName: "Admin"
  imageRegistry:
    name: "[your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
```

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]
   ```

   Beispielantwort:

   ```
   namespace/netapp-acc created
   ```

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

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

   Beispielantwort:

```
astracontrolcenter.astra.netapp.io/astra created
```

Überprüfen Sie den Systemstatus

> Wenn Sie OpenShift verwenden möchten, können Sie vergleichbare oc-Befehle für Verifizierungsschritte verwenden.

1. 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.

Beispielantwort

```
NAME                                        READY   STATUS    RESTARTS
AGE
acc-helm-repo-6b44d68d94-d8m55              1/1     Running   0
13m
activity-78f99ddf8-hltct                    1/1     Running   0
10m
api-token-authentication-457nl              1/1     Running   0
9m28s
api-token-authentication-dgwsz              1/1     Running   0
9m28s
api-token-authentication-hmqqc              1/1     Running   0
9m28s
asup-75fd554dc6-m6qzh                       1/1     Running   0
9m38s
authentication-6779b4c85d-92gds             1/1     Running   0
8m11s
bucketservice-7cc767f8f8-lqwr8              1/1     Running   0
9m31s
certificates-549fd5d6cb-5kmd6               1/1     Running   0
9m56s
certificates-549fd5d6cb-bkjh9               1/1     Running   0
9m56s
cloud-extension-7bcb7948b-hn8h2             1/1     Running   0
10m
cloud-insights-service-56ccf86647-fgg69     1/1     Running   0
9m46s
composite-compute-677685b9bb-7vgsf          1/1     Running   0
10m
composite-volume-657d6c5585-dnq79           1/1     Running   0
9m49s
credentials-755fd867c8-vrlmt                1/1     Running   0
11m
entitlement-86495cdf5b-nwhh2                1/1     Running   2
10m
features-5684fb8b56-8d6s8                   1/1     Running   0
10m
fluent-bit-ds-rhx7v                         1/1     Running   0
7m48s
fluent-bit-ds-rjms4                         1/1     Running   0
7m48s
fluent-bit-ds-zf5ph                         1/1     Running   0
7m48s
graphql-server-66d895f544-w6hjd             1/1     Running   0
3m29s
```

```
identity-744df448d5-rlcmm                1/1     Running   0
10m
influxdb2-0                              1/1     Running   0
13m
keycloak-operator-75c965cc54-z7csw       1/1     Running   0
8m16s
krakend-798d6df96f-9z2sk                 1/1     Running   0
3m26s
license-5fb7d75765-f8mjg                 1/1     Running   0
9m50s
login-ui-7d5b7df85d-l2s7s                1/1     Running   0
3m20s
loki-0                                   1/1     Running   0
13m
metrics-facade-599b9d7fcc-gtmgl          1/1     Running   0
9m40s
monitoring-operator-67cc74f844-cdplp     2/2     Running   0
8m11s
nats-0                                   1/1     Running   0
13m
nats-1                                   1/1     Running   0
13m
nats-2                                   1/1     Running   0
12m
nautilus-769f5b74cd-k5jxm                1/1     Running   0
9m42s
nautilus-769f5b74cd-kd9gd                1/1     Running   0
8m59s
openapi-84f6ccd8ff-76kvp                 1/1     Running   0
9m34s
packages-6f59fc67dc-4g2f5                1/1     Running   0
9m52s
polaris-consul-consul-server-0           1/1     Running   0
13m
polaris-consul-consul-server-1           1/1     Running   0
13m
polaris-consul-consul-server-2           1/1     Running   0
13m
polaris-keycloak-0                       1/1     Running   0
8m7s
polaris-keycloak-1                       1/1     Running   0
5m49s
polaris-keycloak-2                       1/1     Running   0
5m15s
polaris-keycloak-db-0                    1/1     Running   0
8m6s
```

```
polaris-keycloak-db-1                     1/1     Running   0
5m49s
polaris-keycloak-db-2                     1/1     Running   0
4m57s
polaris-mongodb-0                         2/2     Running   0
13m
polaris-mongodb-1                         2/2     Running   0
12m
polaris-mongodb-2                         2/2     Running   0
12m
polaris-ui-565f56bf7b-zwr8b               1/1     Running   0
3m19s
polaris-vault-0                           1/1     Running   0
13m
polaris-vault-1                           1/1     Running   0
13m
polaris-vault-2                           1/1     Running   0
13m
public-metrics-6d86d66444-2wbzl           1/1     Running   0
9m30s
storage-backend-metrics-77c5d98dcd-dbhg5 1/1     Running   0
9m44s
storage-provider-78c885f57c-6zcv4         1/1     Running   0
9m36s
telegraf-ds-2l2m9                         1/1     Running   0
7m48s
telegraf-ds-qfzgh                         1/1     Running   0
7m48s
telegraf-ds-shrms                         1/1     Running   0
7m48s
telegraf-rs-bjpkt                         1/1     Running   0
7m48s
telemetry-service-6684696c64-qzfdf        1/1     Running   0
10m
tenancy-6596b6c54d-vmpsm                  1/1     Running   0
10m
traefik-7489dc59f9-6mnst                  1/1     Running   0
3m19s
traefik-7489dc59f9-xrkgg                  1/1     Running   0
3m4s
trident-svc-6c8dc458f5-jswcl              1/1     Running   0
10m
vault-controller-6b954f9b76-gz9nm         1/1     Running   0
11m
```

2. (Optional) um sicherzustellen, dass die Installation abgeschlossen ist, können Sie sich die ansehen `acc-operator` Protokolle mit dem folgenden Befehl

```
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. Sollte ein Cluster-Registrierungsfehler in den Protokollen gemeldet werden, können Sie die Registrierung erneut durch den Add-Cluster-Workflow versuchen "In der UI" Oder API.

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

```
kubectl get AstraControlCenter -n netapp-acc
```

Antwort:

```
NAME    UUID                                      VERSION     ADDRESS
READY
astra   ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f  22.08.1-26
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, wie etwa den Lastausgleich in einem Cluster, managt.

Dieses Verfahren erklärt, wie ein Ingress-Controller eingerichtet wird (`ingressType:Generic`). Dies ist die Standardaktion mit Astra Control Center. Nachdem Astra Control Center bereitgestellt wurde, müssen Sie den Ingress-Controller so konfigurieren, dass Astra Control Center mit einer URL verfügbar ist.

> Wenn Sie keinen Ingress-Controller einrichten möchten, können Sie ihn einstellen `ingressType:AccTraefik`). 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 nicht eine 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. Einzelheiten zum Servicetyp von „loadbalancer“ und Ingress finden Sie unter "Anforderungen".

Die Schritte unterscheiden sich je nach Art des Ingress-Controllers, den Sie verwenden:

- Istio Ingress
- Nginx-Ingress-Controller
- OpenShift-Eingangs-Controller

Was Sie benötigen

- Erforderlich "Eingangs-Controller" Sollte bereits eingesetzt werden.
- Der "Eingangsklasse" Entsprechend der Eingangs-Steuerung sollte bereits erstellt werden.
- Sie verwenden Kubernetes-Versionen zwischen und v1.19 und v1.22.

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 in `netapp-acc` (Oder Custom-Name) Namespace mit entweder dem v1beta1 (veraltet in Kubernetes Version weniger als oder 1.22) oder v1 Ressourcentyp für entweder ein deprecated oder ein neues Schema:

   Ausgabe:

```
apiVersion: networking.k8s.io/v1beta1
kind: IngressClass
metadata:
  name: istio
spec:
  controller: istio.io/ingress-controller
---
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
  name: ingress
  namespace: istio-system
spec:
  ingressClassName: istio
  tls:
  - hosts:
    - <ACC addess>
    secretName: [tls secret name]
  rules:
  - host: [ACC addess]
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          serviceName: traefik
          servicePort: 80
```

Für das neue Schema v1 gehen Sie wie folgt vor:

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

Ausgabe:

```
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: istio-system
spec:
  ingressClassName: istio
  tls:
  - hosts:
    - <ACC addess>
    secretName: [tls secret name]
  rules:
  - host: [ACC addess]
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: traefik
            port:
              number: 80
```

5. Implementieren Sie wie gewohnt Astra Control Center.
6. Überprüfen Sie den Status des Eingangs:

```
kubectl get ingress -n netapp-acc
```

Antwort:

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

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 mit entweder dem `v1beta1` (Veraltet in Kubernetes Version kleiner als oder 1.22) oder `v1` Ressourcentyp für ein deprecated oder ein neues Schema:

   a. Für A `v1beta1` Veraltete Schemas, folgen Sie diesem Beispiel:

```
apiVersion: extensions/v1beta1
Kind: IngressClass
metadata:
  name: ingress-acc
  namespace: [netapp-acc or custom namespace]
  annotations:
    kubernetes.io/ingress.class: [class name for nginx controller]
spec:
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - backend:
        serviceName: traefik
        servicePort: 80
        pathType: ImplementationSpecific
```

   b. Für das `v1` Neues Schema, folgen Sie diesem Beispiel:

```yaml
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 addess>
    http:
      paths:
        - path:
          backend:
            service:
              name: traefik
              port:
                number: 80
          pathType: ImplementationSpecific
```

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, den Sie in verwendet haben `astraAddress` Im `astra_control_center_min.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_min.yaml` CR, wenn Sie haben das Astra Control Center installiert, Gefolgt von dem Einzeitkennwort (`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 es sich um Ihre erste Anmeldung handelt und Sie das Passwort vergessen haben und noch keine anderen Administratorkonten erstellt wurden, wenden Sie sich an den NetApp Support, um Unterstützung bei der Passwortwiederherstellung zu erhalten.

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.

Schritte

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

```
kubectl logs --follow -n netapp-acc-operator $(kubectl get pods -n
netapp-acc-operator -o name) -c manager
```

Wie es weiter geht

Führen Sie die Implementierung durch "Setup-Aufgaben".

=
:allow-uri-read:

Einschränkungen der POD-Sicherheitsrichtlinie verstehen

Astra Control Center unterstützt die Einschränkung von Berechtigungen durch POD-Sicherheitsrichtlinien (PSPs). Mithilfe der POD-Sicherheitsrichtlinien können Sie begrenzen, welche Benutzer oder Gruppen Container ausführen können und welche Berechtigungen diese Container haben können.

Einige Kubernetes Distributionen, wie z. B. RKE2, verfügen über eine Standard-Pod-Sicherheitsrichtlinie, die zu restriktiv ist und bei der Installation von Astra Control Center Probleme verursacht.

Anhand der hier enthaltenen Informationen und Beispiele können Sie die von Astra Control Center erstellten POD-Sicherheitsrichtlinien verstehen und die Richtlinien für die POD-Sicherheit konfigurieren, die den erforderlichen Schutz bieten, ohne die Funktionen des Astra Control Center zu beeinträchtigen.

PSPs, die vom Astra Control Center installiert werden

Astra Control Center erstellt während der Installation mehrere POD-Sicherheitsrichtlinien. Einige davon sind dauerhaft, und einige von ihnen werden während bestimmter Operationen erstellt und werden entfernt, sobald der Vorgang abgeschlossen ist.

PSPs, die während der Installation erstellt wurden

Bei der Installation von Astra Control Center installiert der Astra Control Center-Operator eine benutzerdefinierte POD-Sicherheitsrichtlinie, ein Rollenobjekt und ein rollenbindendes Objekt, um die Implementierung von Astra Control Center-Diensten im Astra Control Center-Namespace zu unterstützen.

Die neue Richtlinie und die neuen Objekte haben folgende Attribute:

```
kubectl get psp

NAME                            PRIV    CAPS          SELINUX    RUNASUSER
FSGROUP     SUPGROUP    READONLYROOTFS   VOLUMES
avp-psp                         false                 RunAsAny   RunAsAny
RunAsAny    RunAsAny    false            *
netapp-astra-deployment-psp     false                 RunAsAny   RunAsAny
RunAsAny    RunAsAny    false            *

kubectl get role

NAME                                     CREATED AT
netapp-astra-deployment-role             2022-06-27T19:34:58Z

kubectl get rolebinding

NAME                                     ROLE
AGE
netapp-astra-deployment-rb               Role/netapp-astra-deployment-role
32m
```

Während des Backup-Betriebs erstellte PSPs

Astra Control Center erstellt während des Backup-Betriebs eine dynamische Pod-Sicherheitsrichtlinie, ein ClusterRollenobjekt und ein rollenbindendes Objekt. Diese unterstützen den Backup-Prozess, der in einem separaten Namespace geschieht.

Die neue Richtlinie und die neuen Objekte haben folgende Attribute:

```
kubectl get psp

NAME                            PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-astra-backup             false   DAC_READ_SEARCH
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false            *

kubectl get role

NAME                   CREATED AT
netapp-astra-backup    2022-07-21T00:00:00Z

kubectl get rolebinding

NAME                   ROLE                        AGE
netapp-astra-backup    Role/netapp-astra-backup    62s
```

PSPs, die während des Clustermanagements erstellt wurden

Wenn Sie einen Cluster verwalten, installiert Astra Control Center den netapp Monitoring Operator im Managed Cluster. Dieser Operator erstellt eine Pod-Sicherheitsrichtlinie, ein ClusterRole-Objekt und ein RoleBending-Objekt, um Telemetrieservices im Namespace von Astra Control Center bereitzustellen.

Die neue Richtlinie und die neuen Objekte haben folgende Attribute:

```
kubectl get psp

NAME                            PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-monitoring-psp-nkmo      true    AUDIT_WRITE,NET_ADMIN,NET_RAW
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false            *

kubectl get role

NAME                                            CREATED AT
netapp-monitoring-role-privileged               2022-07-21T00:00:00Z

kubectl get rolebinding

NAME                                                    ROLE
AGE
netapp-monitoring-role-binding-privileged               Role/netapp-
monitoring-role-privileged              2m5s
```

Aktivieren der Netzwerkkommunikation zwischen Namespaces

Einige Umgebungen verwenden NetworkPolicy-Konstrukte, um den Datenverkehr zwischen Namespaces zu beschränken. Der Astra Control Center Operator, Astra Control Center und das Astra Plugin für VMware vSphere sind allesamt in verschiedenen Namespaces. Die Dienste in diesen verschiedenen Namespaces müssen in der Lage sein, miteinander zu kommunizieren. Gehen Sie wie folgt vor, um diese Kommunikation zu aktivieren.

Schritte

1. Löschen Sie alle im Astra Control Center Namespace vorhandenen NetworkPolicy-Ressourcen:

```
kubectl get networkpolicy -n netapp-acc
```

2. Verwenden Sie für jedes NetworkPolicy-Objekt, das vom vorhergehenden Befehl zurückgegeben wird, den folgenden Befehl, um es zu löschen. Ersetzen Sie <OBJECT_NAME> durch den Namen des zurückgegebenen Objekts:

```
kubectl delete networkpolicy <OBJECT_NAME> -n netapp-acc
```

3. Wenden Sie die folgende Ressourcendatei an, um das ACC-avp-Netzwerk-Policy-Objekt zu konfigurieren, damit das Astra Plugin für VMware vSphere Services Anfragen an die Astra Control Center Services stellen kann. Ersetzen Sie die Informationen in Klammern <> durch Informationen aus Ihrer Umgebung:

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-avp-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
        - namespaceSelector:
            matchLabels:
              kubernetes.io/metadata.name: <PLUGIN_NAMESPACE_NAME> #
REPLACE THIS WITH THE ASTRA PLUGIN FOR VMWARE VSPHERE NAMESPACE NAME
```

4. Wenden Sie die folgende Ressourcendatei an, um das ACC-Operator-Network-Policy-Objekt so zu konfigurieren, dass der Astra Control Center-Operator mit den Astra Control Center-Diensten kommunizieren kann. Ersetzen Sie die Informationen in Klammern <> durch Informationen aus Ihrer Umgebung:

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-operator-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
        - namespaceSelector:
            matchLabels:
              kubernetes.io/metadata.name: <NETAPP-ACC-OPERATOR> #
REPLACE THIS WITH THE OPERATOR NAMESPACE NAME
```

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. Sie müssen sie 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. Holen Sie sich die Ressourcenkontingente im netapp-ACC Namespace:

   ```
   kubectl get quota -n netapp-acc
   ```

   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
```

```
kubectl delete resourcequota  pods-low -n netapp-acc
```

```
kubectl delete resourcequota  pods-medium -n netapp-acc
```

3. Grenzbereiche im netapp-ACC Namespace abrufen:

```
kubectl get limits -n netapp-acc
```

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
```

=
:allow-uri-read:

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.

Was Sie benötigen

- "Bevor Sie mit der Installation beginnen, bereiten Sie Ihre Umgebung auf die Implementierung des Astra Control Center vor".
- Stellen Sie in Ihrem OpenShift-Cluster sicher, dass sich alle Clusterbetreiber in einem ordnungsgemäßen Zustand befinden (`available` Ist `true`):

```
oc get clusteroperators
```

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

sind (`available` Ist `true`):

```
oc get apiservices
```

- Erstellen Sie in Ihrem Rechenzentrum eine FQDN-Adresse für Astra Control Center.
- Erhalten Sie die erforderlichen Berechtigungen und den Zugriff auf die Red hat OpenShift Container Platform, um die beschriebenen Installationsschritte durchzuführen.
- Wenn bereits ein Zertifikat-Manager im Cluster vorhanden ist, müssen Sie einen Teil durchführen "Erforderliche Schritte" Damit Astra Control Center nicht seinen eigenen Cert-Manager installiert.

Schritte

- Laden Sie das Astra Control Center Bundle herunter und entpacken Sie es aus
- 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 Bundle herunter und entpacken Sie es aus

1. Laden Sie das Astra Control Center Bundle herunter (`astra-control-center-[version].tar.gz`) Vom "NetApp Support Website".
2. Laden Sie den Zip der Astra Control Center Zertifikate und Schlüssel aus dem herunter "NetApp Support Website".
3. (Optional) Überprüfen Sie mit dem folgenden Befehl die Signatur des Pakets:

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

4. Extrahieren Sie die Bilder:

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

Installieren Sie das NetApp Astra kubectl Plug-in

Der NetApp Astra `kubectl` Kommandozeilen-Plugin spart Zeit bei der Ausführung von Routineaufgaben im Zusammenhang mit der Bereitstellung und dem Upgrade von Astra Control Center.

Was Sie benötigen

NetApp bietet Binärdateien für das Plug-in für verschiedene CPU-Architekturen und Betriebssysteme. Sie müssen wissen, welche CPU und welches Betriebssystem Sie haben, bevor Sie diese Aufgabe ausführen. Unter Linux- und Mac-Betriebssystemen können Sie die verwenden `uname -a` Befehl zum Sammeln dieser

Informationen.

Schritte

1. Nennen Sie den verfügbaren NetApp Astra `kubectl` Plugin-Binärdateien, und notieren Sie den Namen der Datei, die Sie für Ihr Betriebssystem und CPU-Architektur benötigen:

```
ls kubectl-astra/
```

2. Kopieren Sie die Datei an denselben Speicherort wie der Standard `kubectl` Utility: In diesem Beispiel ist der `kubectl` Das Dienstprogramm befindet sich im `/usr/local/bin` Verzeichnis. Austausch `<binary-name>` Mit dem Namen der benötigten Datei:

```
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 Astra-Verzeichnis:

```
cd acc
```

2. Schieben Sie die Paketbilder im Astra Control Center-Bildverzeichnis in Ihre lokale Registrierung. Führen Sie folgende Ersetzungen durch, bevor Sie den Befehl ausführen:
   - ERSETZEN SIE DIE BUNDLE_FILE durch den Namen der Astra Control Bundle-Datei (z. B. `acc.manifest.yaml`).
   - ERSETZEN SIE MY_REGISTRY durch die URL des Docker Repositorys.
   - 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_REGISTRY
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

Podman

1. Melden Sie sich bei Ihrer Registrierung an:

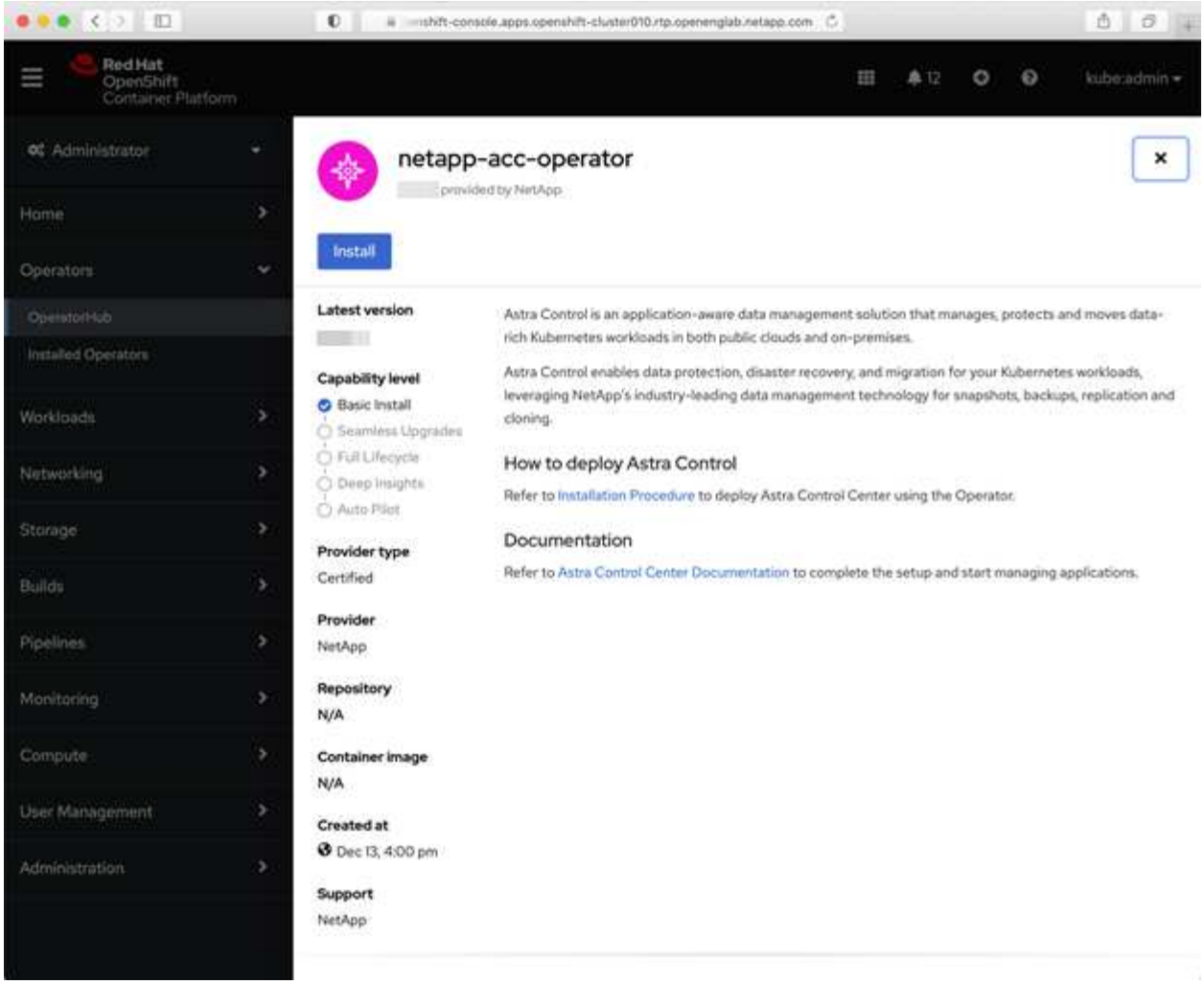
```
podman login [your_registry_path]
```

2. Führen Sie das folgende Skript aus und machen Sie die Substitution <YOUR_REGISTRY> wie in den Kommentaren angegeben:

```
# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
  # Load to local cache
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')

  # Remove path and keep imageName.
  astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')

  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

  # Push to the local repo.
  podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

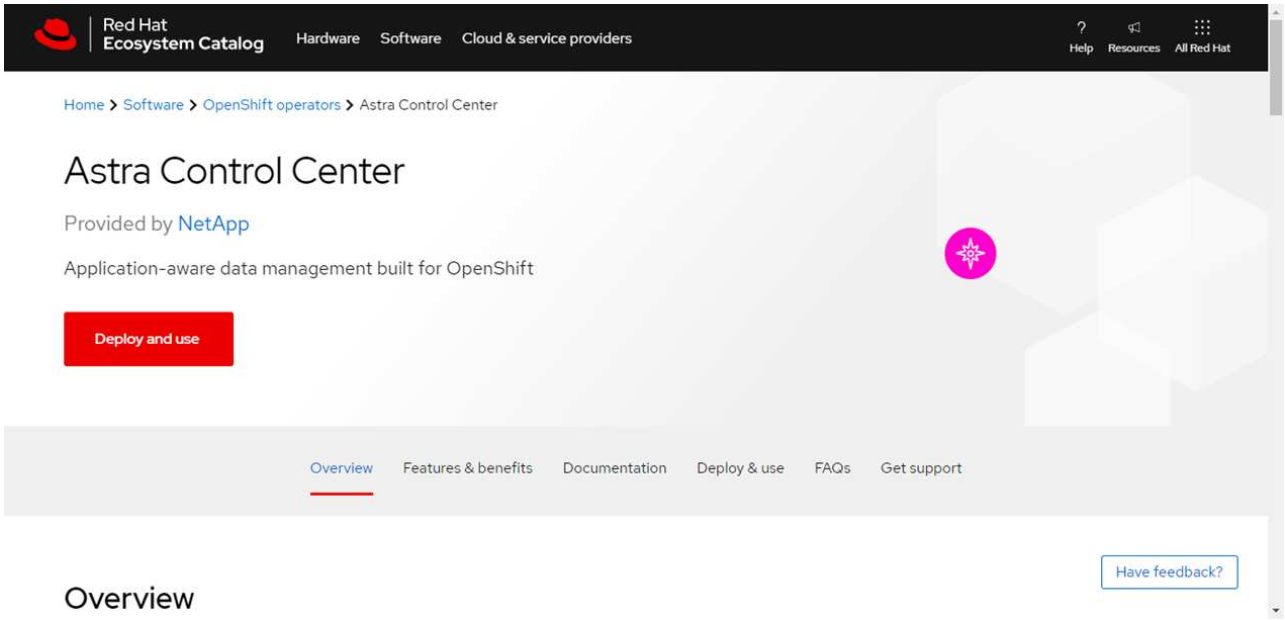
Suchen Sie die Installationsseite des Bedieners

1. Führen Sie eines der folgenden Verfahren aus, um auf die Installationsseite des Bedieners zuzugreifen:
   - Von der Red hat OpenShift-Webkonsole
     aus:



i. Melden Sie sich in der OpenShift Container Platform UI an.
ii. Wählen Sie im Seitenmenü die Option **Operatoren > OperatorHub** aus.
iii. Wählen Sie den Operator des NetApp Astra Control Center aus.
iv. Wählen Sie **Installieren**.

- 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 in der Detailansicht des Bedieners Astra Control Center die Option aus `Create instance` Im Abschnitt über die bereitgestellten APIs.

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

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

   b. (Optional) Aktivieren oder Deaktivieren von Auto Support. Es wird empfohlen, die Auto Support-Funktion beizubehalten.

c. Geben Sie die Astra Control Center-Adresse ein. Kommen Sie nicht herein `http://` Oder `https://` In der Adresse.

d. Geben Sie die Astra Control Center-Version ein, z. B. 21.12.60.

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

f. Beibehaltung der Standard-Richtlinie zur Rückgewinnung von Volumes

g. Geben Sie in **Image Registry** Ihren lokalen Container Image Registry-Pfad ein. Kommen Sie nicht herein `http://` Oder `https://` In der Adresse.

h. Wenn Sie eine Registrierung verwenden, für die eine Authentifizierung erforderlich ist, geben Sie das Geheimnis ein.

i. Geben Sie den Vornamen des Administrators ein.

j. Konfiguration der Ressourcenskalierung

k. Behalten Sie die Standard-Storage-Klasse bei.

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

3. Wählen Sie `Create`.

Wie es weiter geht

Überprüfen Sie die erfolgreiche Installation von Astra Control Center und führen Sie die "Verbleibende Schritte" Um sich anzumelden. Darüber hinaus wird die Implementierung abgeschlossen, indem Sie auch die Ausführung durchführen "Setup-Aufgaben".

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 ist die gehostete AWS Zone und der Eintrag Route 53 erforderlich

Anforderungen der Betriebsumgebung für AWS

Astra Control Center erfordert die folgende Betriebsumgebung für AWS:

- Red hat OpenShift Container Platform 4.8

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

Das Astra Control Center benötigt 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
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 als Teil der Kubernetes Cluster Discovery in NetApp Cloud Manager)	Astra Trident 21.04 oder höher ist installiert und konfiguriert und NetApp ONTAP Version 9.5 oder höher als Storage-Backend

Komponente	Anforderungen
Bildregistrierung	Sie müssen über eine vorhandene private Registry, wie AWS Elastic Container Registry, mit der Sie Astra Control Center Build-Images 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 ONTAP Kubernetes Storage-Klassen, die beim Importieren des Kubernetes Clusters in NetApp 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. NetApp Cloud Manager konfigurieren.

5. Installieren Sie Astra Control Center.

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

Stellen Sie sicher, dass die IAM-Rollen und -Berechtigungen ausreichend sind, damit ein RedHat OpenShift-Cluster und ein NetApp Cloud Manager Connector installiert werden 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 dann AWS für die Erstellung eines virtuellen Netzwerks, richten Sie EC2 Computing-Instanzen ein, erstellen Sie einen AWS S3-Bucket, erstellen Sie ein Elastic Container Register (ECR), um die Astra Control Center Images zu hosten und übertragen Sie die Images auf diese Registrierung.

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

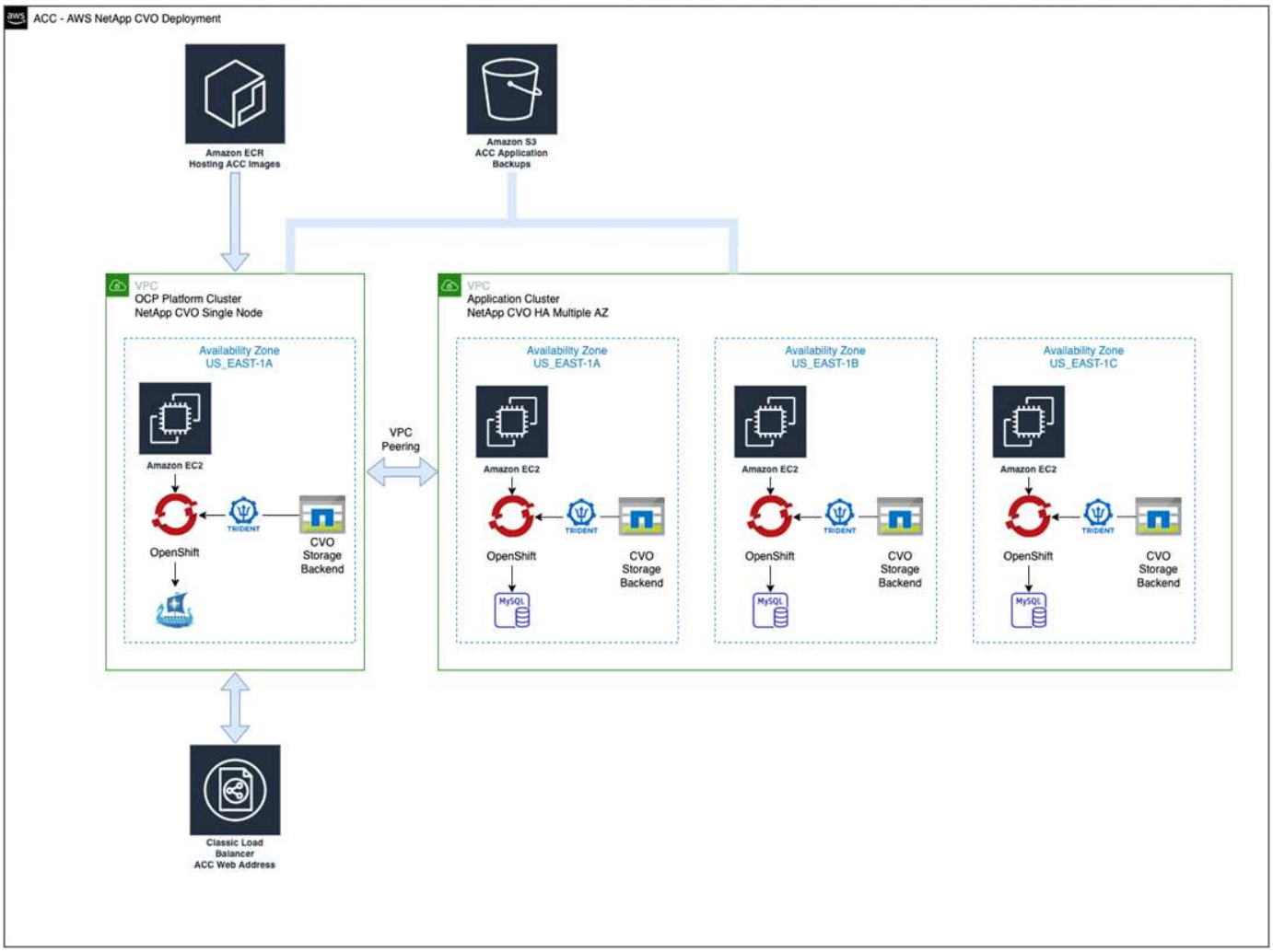
1. Virtuelles AWS Netzwerk erstellen.
2. EC2 Computing-Instanzen prüfen. Dabei können es sich um einen Bare Metal Server oder VMs in AWS handelt.
3. Wenn der Instanztyp nicht bereits den Mindestanforderungen für Ressourcen von Astra für Master- und Worker-Nodes entspricht, ändern Sie den Instanztyp in 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. AWS Elastic Container Registry (ECR) erstellen, um alle ACC-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.

6. Drücken Sie die ACC-Bilder auf die 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:



NetApp Cloud Manager konfigurieren

Erstellen Sie mit Cloud Manager einen Workspace, fügen Sie eine Connector zu AWS hinzu, erstellen Sie eine Arbeitsumgebung und importieren Sie den Cluster.

Folgen Sie der Dokumentation zum Cloud Manager, um die folgenden Schritte auszuführen. Siehe folgendes:

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

Schritte

1. Fügen Sie Ihre Zugangsdaten zu Cloud Manager 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 oben rechts die 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. Trident wird automatisch im Rahmen des Import- und Erkennungsvorgangs 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

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) 4.10
- 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 der Betriebsumgebung für GCP

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

Das Astra Control Center benötigt 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 als Teil der Kubernetes Cluster Discovery in NetApp Cloud Manager)	Astra Trident 21.04 oder höher ist installiert und konfiguriert und NetApp ONTAP Version 9.5 oder höher als Storage-Backend
Bildregistrierung	Sie müssen über eine bestehende private Registrierung, wie Google Container Registry, zu denen Sie Astra Control Center Bilder erstellen 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 Importieren des Kubernetes Clusters in NetApp 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.

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. Installation eines RedHat OpenShift-Clusters in GCP.
2. Erstellung eines GCP-Projekts und einer virtuellen Private Cloud.
3. dass Sie über ausreichende IAM-Berechtigungen verfügen.
4. GCP konfigurieren.
5. NetApp Cloud Manager konfigurieren.
6. Installation und Konfiguration des Astra Control Center.

Installation eines RedHat OpenShift-Clusters in 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 die IAM-Rollen und -Berechtigungen ausreichend sind, damit ein RedHat OpenShift-Cluster und ein NetApp Cloud Manager Connector installiert werden können.

Siehe "Erste GCP-Zugangsdaten und -Berechtigungen".

GCP konfigurieren

Konfigurieren Sie dann GCP zur Erstellung einer VPC, zur Einrichtung von Computing-Instanzen, zur Erstellung eines Google Cloud Objekt-Storage, zur Erstellung eines Google-Container-Registers für das Hosten der Astra Control Center-Images und zum Senden der Bilder an diese Registry.

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 Mindestanforderungen für Ressourcen von Astra 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. Erstellen Sie eine Google Container-Registry, um alle Astra Control Center-Bilder zu hosten.
7. Richten Sie Google Container Registry-Zugriff für Docker Push/Pull für alle Astra Control Center-Bilder ein.

   Beispiel: ACC-Bilder können durch Eingabe des folgenden Skripts in diese Registrierung verschoben werden:

   ```
   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=astra-control-center-<version>.manifest
   GCP_CR_REGISTRY=<target image repository>
   ASTRA_REGISTRY=<source ACC image repository>

   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 < astra-control-center-22.04.41.manifest
   ```

8. Richten Sie DNS-Zonen ein.

NetApp Cloud Manager konfigurieren

Erstellen Sie mit Cloud Manager einen Workspace, fügen Sie einen Connector zu GCP hinzu, erstellen Sie eine Arbeitsumgebung und importieren Sie den Cluster.

Folgen Sie der Dokumentation zum Cloud Manager, um die folgenden Schritte auszuführen. Siehe "Erste Schritte mit Cloud Volumes ONTAP in GCP".

Was Sie benötigen

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

Schritte

1. Fügen Sie Ihre Zugangsdaten zu Cloud Manager 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 Konnektors in GCP von Cloud Manager".
   c. Stellen Sie sicher, dass der Anschluss läuft, und wechseln Sie zu diesem Anschluss.
3. Schaffen Sie eine Arbeitsumgebung für Ihre Cloud-Umgebung.
   a. Speicherort: „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. Trident wird automatisch im Rahmen des Import- und Erkennungsvorgangs 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.

Installieren Sie Astra Control Center

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) 4.8
- 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 Anforderungen an die Ressourcen entspricht, die in der offiziellen Dokumentation der Umgebung aufgeführt sind.

Das Astra Control Center benötigt 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 als Teil der Kubernetes Cluster Discovery in NetApp Cloud Manager)	Astra Trident 21.04 oder neuer installiert und konfiguriert und NetApp ONTAP Version 9.5 oder neuer wird als Storage-Backend verwendet
Bildregistrierung	Sie müssen über eine vorhandene private Registry, wie z. B. Azure Container Registry (ACR) verfügen, in die Sie Bilder vom Astra Control Center erstellen 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 Importieren des Kubernetes Clusters in NetApp 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.

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. NetApp Cloud Manager konfigurieren.
6. Installation und Konfiguration des Astra Control Center.

Installieren Sie einen RedHat OpenShift-Cluster auf Azure

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

Installationsanweisungen finden Sie in der Dokumentation zu RedHat auf "Installation von OpenShift-Cluster auf Azure" Und "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 die IAM-Rollen und -Berechtigungen ausreichend sind, damit ein RedHat OpenShift-Cluster und ein NetApp Cloud Manager Connector installiert werden können.

Siehe "Azure Zugangsdaten und Berechtigungen".

Konfigurieren Sie Azure

Konfigurieren Sie dann Azure für die Erstellung eines virtuellen Netzwerks, richten Sie Computing-Instanzen ein, erstellen Sie einen Azure Blob Container, erstellen Sie ein Azure Container Register (ACR), um die Astra Control Center Images zu hosten und übertragen Sie die Bilder auf diese Registrierung.

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. Erstellen Sie eine Azure Container Registry (ACR), um alle Astra Control Center-Images zu hosten.
8. ACR-Zugriff für Docker-Push/Pull-alle Astra Control Center-Images einrichten.
9. Drücken Sie die ACC-Bilder in diese Registrierung, indem Sie das folgende Skript eingeben:

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

   - Beispiel*:

```
manifestfile=astra-control-center-<version>.manifest
AZ_ACR_REGISTRY=<target image repository>
ASTRA_REGISTRY=<source ACC image repository>

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 $AZ_ACR_REGISTRYY/$image
    docker push $AZ_ACR_REGISTRY/$image
done < astra-control-center-22.04.41.manifest
```

10. Richten Sie DNS-Zonen ein.

NetApp Cloud Manager konfigurieren

Erstellen Sie mit Cloud Manager einen Workspace, fügen Sie einen Connector zu Azure hinzu, erstellen Sie eine Arbeitsumgebung und importieren Sie den Cluster.

Folgen Sie der Dokumentation zum Cloud Manager, um die folgenden Schritte auszuführen. Siehe "Erste Schritte mit Cloud Manager in Azure".

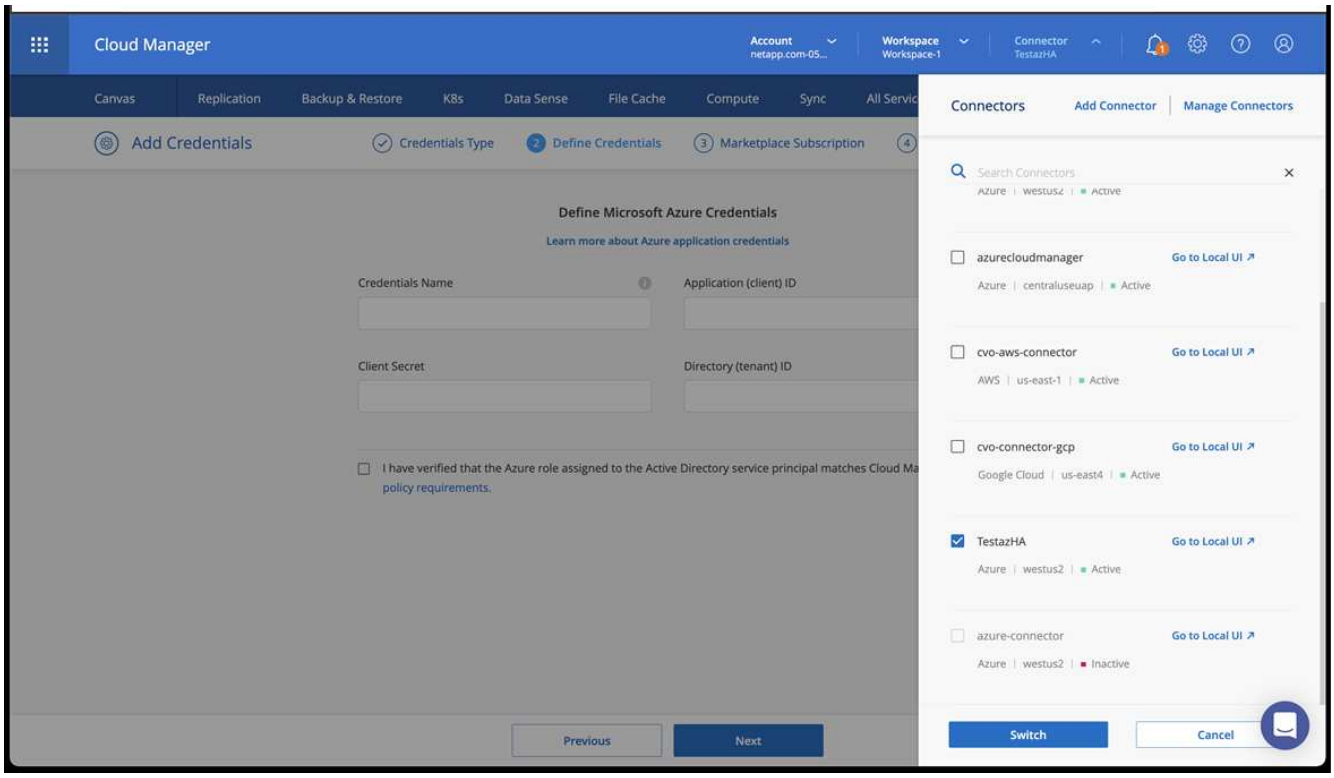
Was Sie benötigen

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

Schritte

1. Fügen Sie Ihre Zugangsdaten zu Cloud Manager hinzu.
2. Fügen Sie einen Connector für Azure hinzu. Siehe "Richtlinien für Cloud Manager".
   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).

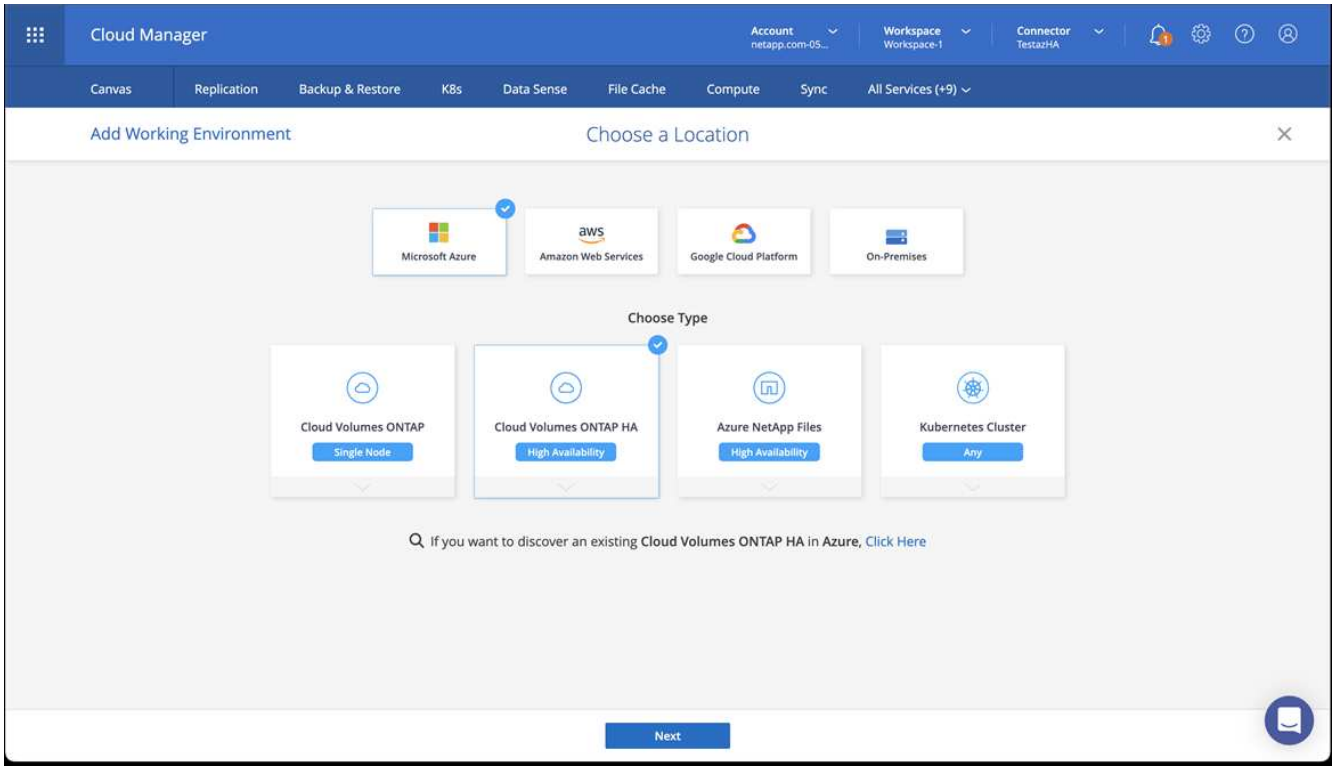
      Siehe "Erstellen eines Konnektors in Azure aus Cloud Manager".
3. Stellen Sie sicher, dass der Anschluss läuft, und wechseln Sie zu diesem Anschluss.



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

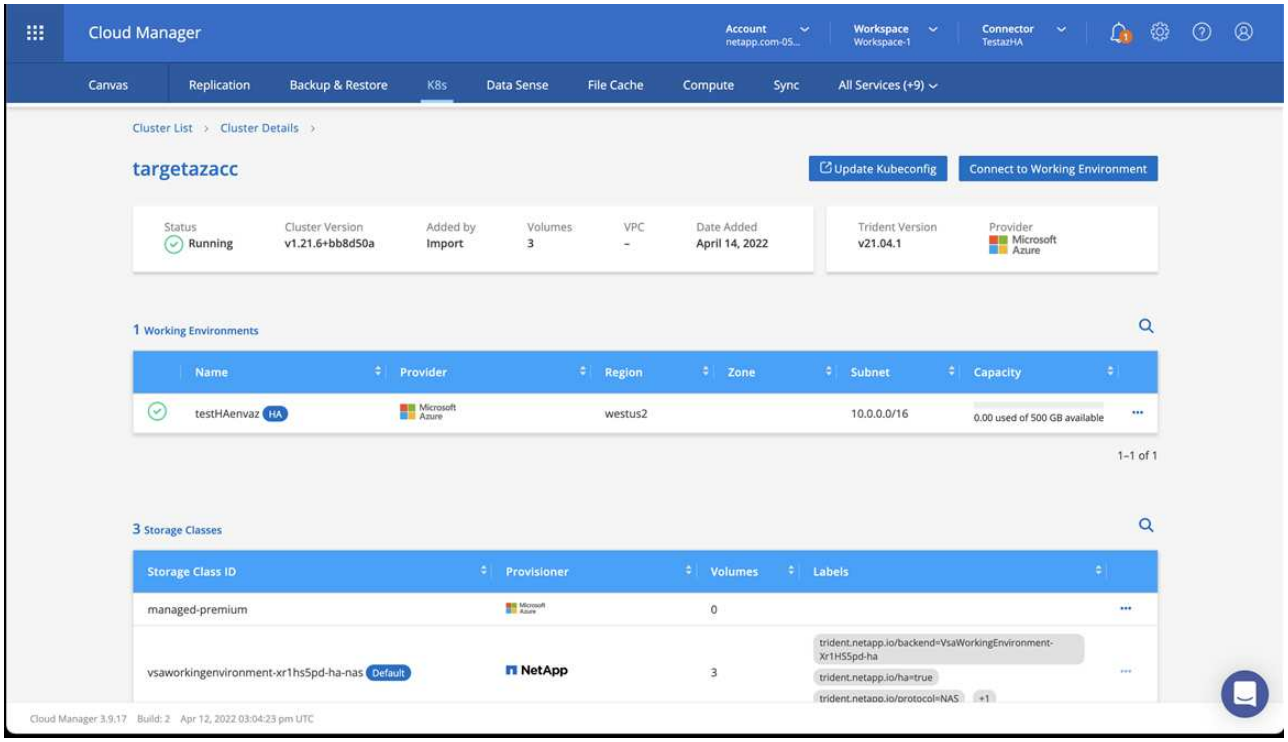
   a. Ort: „Microsoft Azure“.

   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 oben rechts die 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. Trident wird automatisch im Rahmen des Import- und Erkennungsvorgangs 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 des Astra Control Center

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".

Einrichten des Astra Control Center

Astra Control Center unterstützt und überwacht ONTAP und Astra Data Store als Storage-Backend. Nach der Installation von Astra Control Center, melden Sie sich in der UI an und ändern Sie Ihr Passwort, Sie möchten eine Lizenz einrichten, Cluster hinzufügen, Speicher verwalten und Buckets hinzufügen.

Aufgaben

- Fügen Sie eine Lizenz für Astra Control Center hinzu
- Cluster hinzufügen

- Fügen Sie ein Storage-Back-End hinzu
- Fügen Sie einen Bucket hinzu

Fügen Sie eine Lizenz für Astra Control Center hinzu

Sie können eine neue Lizenz über die UI oder hinzufügen "API" Um die Funktionalität des Astra Control Center voll zu nutzen. Ohne Lizenz ist Ihre Verwendung von Astra Control Center auf das Management von Benutzern und das Hinzufügen neuer Cluster beschränkt.

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

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

Astra Control Center Lizenzen messen die CPU-Ressourcen mithilfe von Kubernetes CPU-Einheiten. Die Lizenz muss die CPU-Ressourcen berücksichtigen, die den Worker-Nodes aller verwalteten Kubernetes-Cluster zugewiesen sind. Bevor Sie eine Lizenz hinzufügen, müssen Sie die Lizenzdatei (NLF) vom beziehen "NetApp Support Website".

Sie können das Astra Control Center auch mit einer Evaluierungslizenz ausprobieren, mit der Sie das Astra Control Center 90 Tage ab dem Tag, an dem Sie die Lizenz herunterladen, nutzen können. Sie können sich durch die Anmeldung für eine kostenlose Testversion anmelden "Hier".

> 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.

Was Sie benötigen

Wenn Sie Astra Control Center von heruntergeladen "NetApp Support Website", Sie haben auch die NetApp Lizenzdatei (NLF) heruntergeladen. Stellen Sie sicher, dass Sie Zugriff auf diese Lizenzdatei haben.

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

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. Bei Astra Data Store möchten Sie den Kubernetes App-

Cluster hinzufügen, der Applikationen enthält, die von Astra Data Store bereitgestellte Volumes verwenden.

> 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. Sie können die * Cluster hinzufügen* Funktion verwenden, um einen Cluster mit Astra Control Center zu verwalten.

> Wenn Astra Control einen Cluster verwaltet, wird die Standard-Storage-Klasse des Clusters überwacht. Wenn Sie die Speicherklasse mit ändern `kubectl` Befehle, Astra Control setzt die Änderung zurück. Verwenden Sie eine der folgenden Methoden, um die Standard-Storage-Klasse in einem von Astra Control gemanagten Cluster zu ändern:
>
> - Verwenden Sie die Astra Control API `PUT /managedClusters` endpunkt, und weisen Sie dem eine andere Standard-Speicherklasse zu `DefaultStorageClass` Parameter.
> - Verwenden Sie die Web-UI von Astra Control, um eine andere Standard-Storage-Klasse zuzuweisen. Siehe Ändern der Standard-Storage-Klasse.

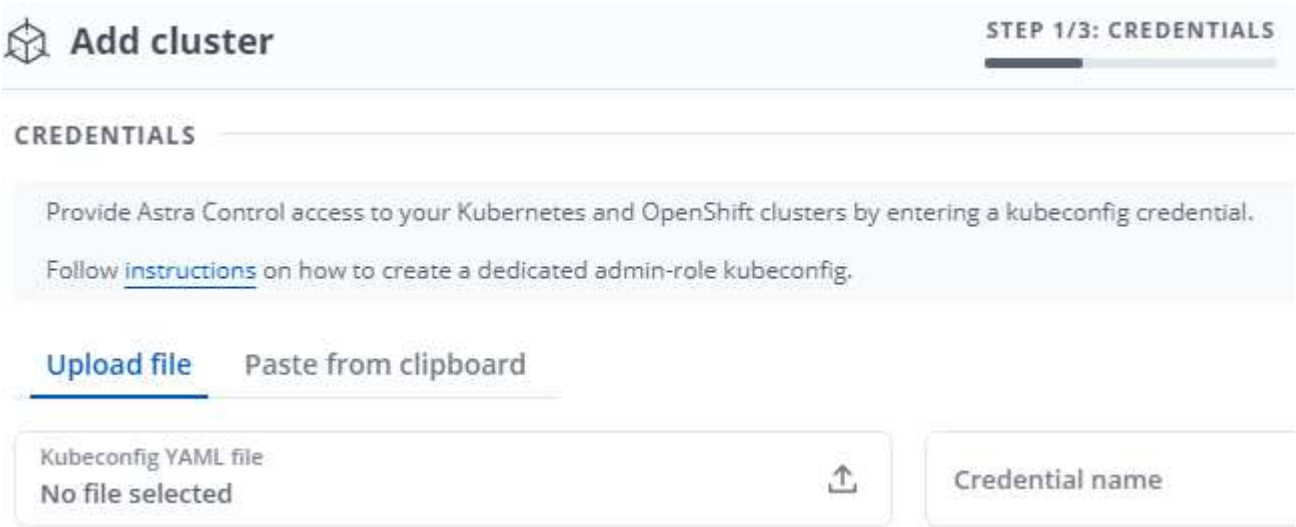
Was Sie benötigen

- Bevor Sie ein Cluster hinzufügen, überprüfen und führen Sie die erforderlichen Maßnahmen durch "Erforderliche Aufgaben".

Schritte

1. Wählen Sie in der Astra Control Center-Benutzeroberfläche auf dem Dashboard * im Bereich Cluster die Option **Add** aus.
2. Laden Sie im Fenster **Cluster hinzufügen** ein `kubeconfig.yaml` Datei oder fügen Sie den Inhalt eines ein `kubeconfig.yaml` Datei:

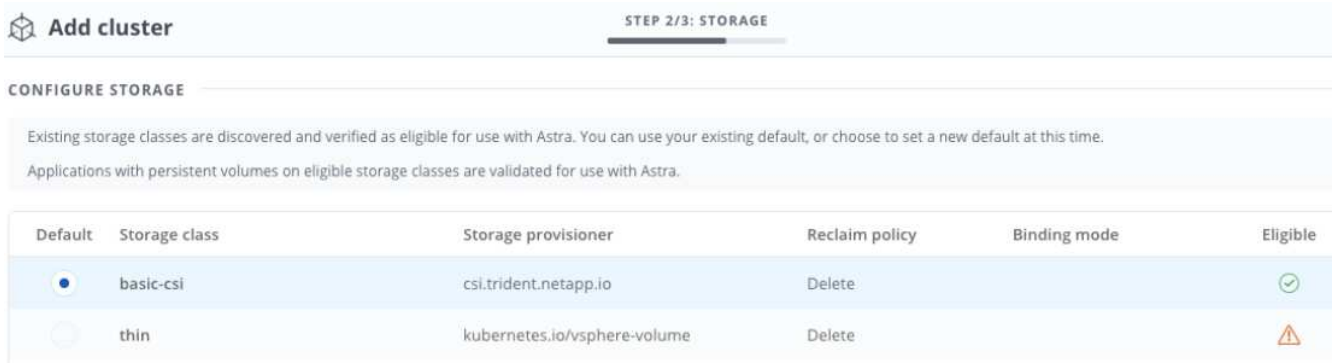
> Der `kubeconfig.yaml` Die Datei sollte **nur die Cluster-Anmeldedaten für einen Cluster** enthalten.



> 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:

3. Geben Sie einen Namen für die Anmeldeinformationen an. Standardmäßig wird der Name der Anmeldeinformationen automatisch als Name des Clusters ausgefüllt.
4. Wählen Sie * Storage konfigurieren* aus.
5. Wählen Sie die Storage-Klasse aus, die für diesen Kubernetes-Cluster verwendet werden soll, und wählen Sie **Review** aus.

> Sie sollten sich für einen Trident-Storage-Kurs entscheiden, der von ONTAP Storage oder Astra Data Store unterstützt wird.



6. Überprüfen Sie die Informationen, und wenn alles gut aussieht, wählen Sie **Cluster hinzufügen**.

Ergebnis

Der Cluster wechselt in den **Entdeckungs**-Status und dann in **running**. Sie haben erfolgreich ein Kubernetes-Cluster hinzugefügt und verwalten es jetzt im 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.

Fügen Sie ein Storage-Back-End hinzu

Sie können ein Storage-Backend hinzufügen, sodass Astra Control die Ressourcen managen kann. Sie können ein Storage-Back-End auf einem gemanagten Cluster implementieren oder ein vorhandenes Storage-Back-End verwenden.

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.

Was Sie für bestehende Implementierungen von Astra Data Store benötigen

- Sie haben Ihren Kubernetes-App-Cluster und das zugrunde liegende Computing-Cluster hinzugefügt.

> Nachdem Sie Ihren Kubernetes App-Cluster für Astra Data Store hinzugefügt haben und er durch Astra Control gemanagt wird, erscheint der Cluster wie `unmanaged` In der Liste der entdeckten Back-Ends. Als Nächstes müssen Sie das Computing-Cluster hinzufügen, das Astra Data Store enthält und das Kubernetes App-Cluster untermauert. Dies können Sie über **Backends** in der UI tun. Wählen Sie das Menü Aktionen für den Cluster aus `Manage`, und "Fügen Sie den Cluster hinzu". Nach dem Status des Clusters von `unmanaged` Änderungen am Namen des Kubernetes-Clusters können Sie mit dem Hinzufügen eines Backend fortfahren.

Was Sie für die neuen Astra Data Store Implementierungen benötigen

- Das ist schon "Die Version des Installationspakets, das Sie bereitstellen möchten, hochgeladen haben" Zu einem Ort, der für Astra Control zugänglich ist.
- Sie haben den Kubernetes-Cluster hinzugefügt, den Sie für die Implementierung verwenden möchten.
- Sie haben die hochgeladen Astra Data Store-Lizenz Für Ihre Implementierung an einen Standort, auf den Astra Control zugreifen kann.

Optionen

- Implementieren von Storage-Ressourcen
- Verwenden Sie ein vorhandenes Storage-Back-End

Implementieren von Storage-Ressourcen

Sie können einen neuen Astra Data Store implementieren und das zugehörige Storage-Backend verwalten.

Schritte

1. Navigieren Sie im Dashboard oder im Menü „Backend“:
   - Aus **Dashboard**: Wählen Sie in der Ressourcenübersicht einen Link aus dem Fensterbereich Speicherrückseite aus und wählen Sie im Bereich Back Ends **Add** aus.
   - Von **Backends**:
     i. Wählen Sie im linken Navigationsbereich **Backend** aus.
     ii. Wählen Sie **Hinzufügen**.
2. Wählen Sie auf der Registerkarte **Bereitstellen** die Option * Astra Data Store* Deployment aus.
3. Wählen Sie das zu implementierende Astra Data Store-Paket aus:
   a. Geben Sie einen Namen für die Astra Data Store-Anwendung ein.
   b. Wählen Sie die Version des Astra Data Stores, die Sie implementieren möchten.

   > Wenn Sie die Version, die Sie bereitstellen möchten, noch nicht hochgeladen haben, können Sie die Option **Paket hinzufügen** verwenden oder den Assistenten beenden und verwenden "Paketmanagement" Um das Installationspaket hochzuladen.

4. Wählen Sie eine Astra Data Store-Lizenz aus, die Sie bereits hochgeladen haben, oder laden Sie die **Lizenz hinzufügen**-Option ein, die Sie mit der Anwendung verwenden können.

> Astra Data Store-Lizenzen mit vollständigen Berechtigungen sind mit Ihrem Kubernetes-Cluster verknüpft. Die zugehörigen Cluster sollten automatisch angezeigt werden. Wenn kein verwalteter Cluster vorhanden ist, können Sie die Option **Cluster hinzufügen** zur Astra Control-Verwaltung hinzufügen wählen. Für Astra Data Store-Lizenzen können Sie diese Verknüpfung auf der nächsten Seite des Assistenten definieren, wenn keine Verbindung zwischen Lizenz und Cluster hergestellt wurde.

5. Wenn Sie dem Astra Control Management noch kein Kubernetes-Cluster hinzugefügt haben, müssen Sie dies auf der Seite * Kubernetes Cluster* tun. Wählen Sie einen vorhandenen Cluster aus der Liste aus, oder wählen Sie **Hinzufügen des zugrunde liegenden Clusters** aus, um ein Cluster zum Astra Control Management hinzuzufügen.
6. Wählen Sie eine Vorlagengröße für den Kubernetes Cluster aus, die Ressourcen für Astra Data Store bereitstellen wird. Sie können eine der folgenden Optionen auswählen:
   - Wenn Sie sich entscheiden `Recommended Kubernetes worker node requirements`, Wählen Sie eine Vorlage von groß zu klein basierend auf, was Ihre Lizenz erlaubt.
   - Wenn Sie sich entscheiden `Custom Kubernetes worker node requirements`, Wählen Sie die Anzahl der Kerne und den gesamten Arbeitsspeicher aus, die Sie für jeden Cluster-Knoten benötigen. Sie können auch die zulässige Anzahl von Nodes im Cluster anzeigen, die die Auswahlkriterien für Kerne und Speicher erfüllen.

> Wählen Sie bei der Auswahl einer Vorlage größere Nodes mit mehr Arbeitsspeicher und Kernen für größere Workloads oder eine größere Anzahl an Nodes für kleinere Workloads aus. Wählen Sie eine Vorlage basierend auf den von Ihrer Lizenz zulässt aus. Bei jeder empfohlenen Vorlagenoption wird die Anzahl der qualifizierten Nodes angegeben, die dem Vorlagenmuster für Arbeitsspeicher und Kerne sowie der Kapazität für jeden Node entsprechen.

7. Konfigurieren der Nodes:
   a. Fügen Sie eine Node-Bezeichnung hinzu, um den Pool der Worker-Nodes zu identifizieren, die diesen Astra Data Store-Cluster unterstützen.

> Das Label muss jedem einzelnen Node im Cluster hinzugefügt werden, der vor Beginn der Implementierung oder der Implementierung von Astra Data Store genutzt wird.

   b. Konfigurieren Sie die Kapazität (gib) pro Node manuell, oder wählen Sie die maximal zulässige Node-Kapazität aus.
   c. Konfigurieren Sie eine Höchstzahl der im Cluster zulässigen Nodes oder zulassen die maximale Anzahl der Nodes im Cluster.
8. (Nur Astra Data Store Volllizenzen) Geben Sie den Schlüssel des Etiketts ein, das Sie für Protection Domains verwenden möchten.

> Erstellen Sie für jeden Node mindestens drei eindeutige Beschriftungen für den Schlüssel. Beispiel: Wenn Ihr Schlüssel lautet `astra.datastore.protection.domain`, Sie können die folgenden Etiketten erstellen: `astra.datastore.protection.domain=domain1`,`astra.datastore.protection.domain=domain2`, und `astra.datastore.protection.domain=domain3`.

9. Konfigurieren des Managementnetzwerks:

a. Geben Sie eine Management-IP-Adresse für die interne Verwaltung von Astra Data Store ein, die sich im gleichen Subnetz wie die IP-Adressen der Worker-Nodes befindet.
b. Sie können dieselbe NIC sowohl für Management- als auch für Datennetzwerke verwenden oder sie separat konfigurieren.
c. Geben Sie den Daten-Netzwerk-IP-Adressenpool, die Subnetzmaske und das Gateway für den Storage-Zugriff ein.

10. Überprüfen Sie die Konfiguration und wählen Sie **Bereitstellen**, um mit der Installation zu beginnen.

Ergebnis

Nach erfolgreicher Installation erscheint das Backend in `available` Geben Sie in der Back-Ends-Liste zusammen mit aktiven Performance-Informationen an.

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

Verwenden Sie ein vorhandenes Storage-Back-End

Sie können ein entdecktes ONTAP oder Astra Data Store Storage Back-End in das Astra Control Center Management integrieren.

Schritte

1. Navigieren Sie im Dashboard oder im Menü „Backend“:
   - Aus **Dashboard**: Wählen Sie in der Ressourcenübersicht einen Link aus dem Fensterbereich Speicherrückseite aus und wählen Sie im Bereich Back Ends **Add** aus.
   - Von **Backends**:
     i. Wählen Sie im linken Navigationsbereich **Backend** aus.
     ii. Wählen Sie **Verwalten** auf einem ermittelten Backend aus dem verwalteten Cluster oder wählen Sie **Hinzufügen**, um ein zusätzliches vorhandenes Backend zu verwalten.
2. Wählen Sie die Registerkarte **vorhandene** verwenden.
3. Je nach Backend-Typ:
   - **Astra Data Store**:
     i. Wählen Sie **Astra Data Store**.
     ii. Wählen Sie das verwaltete Compute-Cluster aus und wählen Sie **Next** aus.
     iii. Bestätigen Sie die Back-End-Details und wählen Sie **Add Storage Backend**.
   - **ONTAP**:
     i. Wählen Sie **ONTAP** und wählen Sie **Weiter**.
     ii. Geben Sie die IP-Adresse und die Administrator-Anmeldedaten für das ONTAP-Cluster-Management ein.

> 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, aktivieren Sie die Zugriffsmethoden `ontapi` Und `http` Für den Benutzer auf beiden ONTAP Clustern. Siehe "Benutzerkonten Verwalten" Finden Sie weitere Informationen.

iii. Wählen Sie **Bewertung**.

iv. Bestätigen Sie die Back-End-Details und wählen Sie **Add Storage Backend**.

Ergebnis

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

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

Fügen Sie einen Bucket hinzu

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 einen Bucket hinzufügen, markiert Astra Control einen Bucket als Standard-Bucket-Indikator. Der erste von Ihnen erstellte Bucket wird der Standard-Bucket.

Sie brauchen keinen Eimer, wenn Sie Ihre Anwendungskonfiguration und Ihren persistenten Storage im selben Cluster klonen.

Verwenden Sie einen der folgenden Bucket-Typen:

- NetApp ONTAP S3
- NetApp StorageGRID S3
- Allgemein S3

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

- Microsoft Azure

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

- Microsoft Azure

Anweisungen zum Hinzufügen von Buckets mithilfe der Astra Control API finden Sie unter "Astra Automation und API-Informationen".

Schritte

1. Wählen Sie im linken Navigationsbereich **Buckets** aus.
   a. Wählen Sie **Hinzufügen**.
   b. 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.

c. Erstellen Sie einen neuen Bucket-Namen oder geben Sie einen vorhandenen Bucket-Namen und eine optionale Beschreibung ein.

> Der Bucket-Name und die Beschreibung erscheinen als Backup-Speicherort, den Sie später wählen können, wenn Sie ein Backup erstellen. Der Name wird auch während der Konfiguration der Schutzrichtlinien angezeigt.

d. Geben Sie den Namen oder die IP-Adresse des S3-Endpunkts ein.

e. Wenn dieser Bucket der Standard-Bucket für alle Backups sein soll, prüfen Sie den `Make this bucket the default bucket for this private cloud` Option.

> Diese Option wird nicht für den ersten von Ihnen erstellten Bucket angezeigt.

f. Mit Hinzufügen fortfahren Anmeldeinformationen.

Fügen Sie S3-Zugriffsdaten hinzu

Fügen Sie Ihre Zugangsdaten für S3-Zugriff jederzeit hinzu.

Schritte

1. Wählen Sie im Dialogfeld Buckets entweder die Registerkarte **Hinzufügen** oder **vorhandene verwenden** aus.
   a. Geben Sie einen Namen für die Anmeldedaten ein, der sie von anderen Anmeldeinformationen in Astra Control unterscheidet.
   b. Geben Sie die Zugriffs-ID und den geheimen Schlüssel ein, indem Sie den Inhalt aus der Zwischenablage einfügen.

Ändern der Standard-Storage-Klasse

Sie können die Standard-Storage-Klasse für ein Cluster ändern.

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**.

Was kommt als Nächstes?

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

- "Benutzer managen"
- "Starten Sie das Anwendungsmanagement"
- "Schützen von Applikationen"

- "Applikationen klonen"
- "Benachrichtigungen verwalten"
- "Verbinden Sie sich mit Cloud Insights"
- "Fügen Sie ein benutzerdefiniertes TLS-Zertifikat hinzu"

Weitere Informationen

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

Voraussetzungen für das Hinzufügen eines Clusters

Sie sollten sicherstellen, dass die Voraussetzungen erfüllt sind, bevor Sie ein Cluster hinzufügen. Außerdem sollten Sie die Eignungskontrollen durchführen, um sicherzustellen, dass Ihr Cluster zum Astra Control Center hinzugefügt werden kann.

Was benötigen Sie vor dem Hinzufügen eines Clusters

Vergewissern Sie sich, dass Ihr Cluster die in aufgeführten Anforderungen erfüllt "Anforderungen für Applikationscluster".

> Wenn Sie planen, als verwaltete Computing-Ressource einen zweiten OpenShift 4.6, 4.7 oder 4.8 hinzuzufügen, sollten Sie sicherstellen, dass die Astra Trident Volume Snapshot-Funktion aktiviert ist. Sehen Sie den offiziellen Astra Trident an "Anweisungen" Um Volume Snapshots mit Astra Trident zu aktivieren und zu testen.

- Astra Trident StorageClasses ist mit einem konfiguriert "Unterstütztes Storage-Backend" (Erforderlich für jeden Cluster-Typ)
- Der Superuser und die Benutzer-ID sind auf dem ONTAP-System eingerichtet, um Apps mit Astra Control Center zu sichern und wiederherzustellen. Führen Sie den folgenden Befehl in der ONTAP-Befehlszeile aus:
  `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sysm --anon 65534`
- Astra Trident `volumesnapshotclass` Objekt, das von einem Administrator definiert wurde. Astra Trident ist der Anfang "Anweisungen" Um Volume Snapshots mit Astra Trident zu aktivieren und zu testen.
- Stellen Sie sicher, dass nur eine einzelne Standard-Storage-Klasse für Ihr Kubernetes-Cluster definiert ist.

Führen Sie Eignungsprüfungen durch

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

Schritte

1. Überprüfen Sie die Trident Version.

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

   Wenn Trident vorhanden ist, wird eine Ausgabe ähnlich der folgenden ausgegeben:

```
NAME      VERSION
trident   21.04.0
```

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

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

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

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

```
kubectl get sc
NAME                    PROVISIONER                    RECLAIMPOLICY
VOLUMEBINDINGMODE   ALLOWVOLUMEEXPANSION   AGE
ontap-gold (default)    csi.trident.netapp.io          Delete
Immediate           true                   5d23h
thin                    kubernetes.io/vsphere-volume   Delete
Immediate           false                  6d
```

Erstellen Sie ein „admin-Role“-kubeconfig

Stellen Sie sicher, dass Sie die folgenden Schritte auf Ihrem Gerät ausführen:

- `kubectl` v1.19 oder höher installiert
- Ein aktiver kubeconfig mit Clusteradministratorrechten für den aktiven Kontext

Schritte

1. Erstellen Sie ein Service-Konto wie folgt:

   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>
```

+

```yaml
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. (Optional) Wenn Ihr Cluster eine restriktive Pod-Sicherheitsrichtlinie verwendet, die die Erstellung privilegierter Pods nicht zulässt oder Vorgänge innerhalb der Pod-Container als Root-Benutzer ausgeführt werden können, erstellen Sie eine benutzerdefinierte Pod-Sicherheitsrichtlinie für den Cluster, durch die Astra Control Pods erstellen und managen kann. Anweisungen hierzu finden Sie unter "Erstellen einer benutzerdefinierten POD-Sicherheitsrichtlinie".
3. Gewähren Sie Cluster-Admin-Berechtigungen wie folgt:

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>
```

+

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astracontrol-admin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
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. 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-vhz87"},
{ "name": "astracontrol-service-account-token-r59kr"}
]
```

Die Indizes für jedes Element im `secrets` Array beginnt mit 0. Im obigen Beispiel der Index für `astracontrol-service-account-dockercfg-vhz87` Wäre 0 und der Index für `astracontrol-service-account-token-r59kr` Sind es 1. Notieren Sie in Ihrer Ausgabe den Index für den Namen des Dienstkontos, der das Wort „Token“ darin enthält.

5. 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
```

6. (**Optional**) Umbenennen Sie die kubeconfig in einen aussagekräftigen Namen für Ihren Cluster. Schützen Sie die Cluster-Anmeldedaten.

```
chmod 700 create-kubeconfig.sh
mv kubeconfig-sa.txt YOUR_CLUSTER_NAME_kubeconfig
```

Was kommt als Nächstes?

Jetzt, wo du überprüft hast, dass die Voraussetzungen erfüllt sind, bist du bereit "Fügen Sie einen Cluster hinzu".

Weitere Informationen

- "Trident Dokumentation"
- "Verwenden Sie die Astra Control API"

Fügen Sie ein benutzerdefiniertes TLS-Zertifikat hinzu

Sie können das vorhandene selbst signierte TLS-Zertifikat entfernen und durch ein TLS-Zertifikat ersetzen, das von einer Zertifizierungsstelle (CA) signiert ist.

Was Sie benötigen

- 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 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>
....

#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>
....

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:

```yaml
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: <certificate-name>
  namespace: <ACC-deployment-namespace>
spec:
  secretName: <certificate-secret-name>
  duration: 2160h # 90d
  renewBefore: 360h # 15d
  dnsNames:
  - <astra.dnsname.example.com> #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>
....

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 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.containo.us -n <ACC-deployment-
namespace>
....

# tls:
#    options:
#      name: default
#    secretName: secure-testing-cert
#    store:
#      name: default

 tls:
    options:
      name: default
    secretName: <certificate-secret-name>
    store:
      name: default
```

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

Erstellen einer benutzerdefinierten POD-Sicherheitsrichtlinie

Astra Control muss Kubernetes Pods auf den gemanagten Clustern erstellen und managen. Wenn Ihr Cluster eine restriktive Pod-Sicherheitsrichtlinie verwendet, die die Erstellung privilegierter Pods nicht zulässt oder Vorgänge innerhalb der Pod-Container nicht als Root-Benutzer ausgeführt werden können, müssen Sie eine weniger restriktive POD-Sicherheitsrichtlinie erstellen, damit Astra Control diese Pods erstellen und verwalten kann.

Schritte

1. Erstellen Sie eine Pod-Sicherheitsrichtlinie für den Cluster, die weniger restriktiv ist als der Standard, und speichern Sie sie in einer Datei. Beispiel:

```yaml
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: astracontrol
  annotations:
    seccomp.security.alpha.kubernetes.io/allowedProfileNames: '*'
spec:
  privileged: true
  allowPrivilegeEscalation: true
  allowedCapabilities:
  - '*'
  volumes:
  - '*'
  hostNetwork: true
  hostPorts:
  - min: 0
    max: 65535
  hostIPC: true
  hostPID: true
  runAsUser:
    rule: 'RunAsAny'
  seLinux:
    rule: 'RunAsAny'
  supplementalGroups:
    rule: 'RunAsAny'
  fsGroup:
    rule: 'RunAsAny'
```

2. Erstellen Sie eine neue Rolle für die POD-Sicherheitsrichtlinie.

```bash
kubectl-admin create role psp:astracontrol \
    --verb=use \
    --resource=podsecuritypolicy \
    --resource-name=astracontrol
```

3. Binden Sie die neue Rolle an das Dienstkonto.

```bash
kubectl-admin create rolebinding default:psp:astracontrol \
    --role=psp:astracontrol \
    --serviceaccount=astracontrol-service-account:default
```

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 in der Datei astra_control_Center_min.yaml Custom Resource Definition (CRD) 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_min.yaml CRD festgelegt haben.

Lizenzierung

Ich verwende die Evaluierungslizenz. Wie ändere ich die Volllizenz?

Sie können die vollständige Lizenz ganz einfach von der NetApp Lizenzdatei (NetApp License File, NLF) erhalten.

Schritte

- Wählen Sie in der linken Navigationsleiste **Konto** > **Lizenz**.
- Wählen Sie **Lizenz hinzufügen**.
- Navigieren Sie zu der Lizenzdatei, die Sie heruntergeladen haben, und wählen Sie **Hinzufügen**.

Ich verwende die Evaluierungslizenz. Kann ich trotzdem Apps verwalten?

Ja, Sie können die Funktionalität Apps verwalten mit der Evaluierungslizenz testen.

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 Trident bei Unmanagement automatisch von einem Cluster deinstalliert? Wenn Sie das Management eines Clusters aus dem Astra Control Center aufheben, wird Trident nicht automatisch aus dem Cluster deinstalliert. Um Trident zu deinstallieren, müssen Sie es benötigen "Befolgen Sie die folgenden Schritte in der Trident-Dokumentation".

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 nutzen, aber keine Applikation managen, die Storage von anderen Anbietern verwendet.

Sollte ich Astra Control selbst verwalten? Nein, Sie sollten Astra Control nicht selbst verwalten, weil es sich um eine "System-App" handelt.

Beeinträchtigen ungesunde Pods das App-Management? Wenn eine verwaltete App Pods in einem ungesunden Zustand hat, kann Astra Control keine neuen Backups und Klone erstellen.

Datenmanagement-Vorgänge

Es gibt Schnappschüsse in meinem Konto, die ich nicht erstellt habe. Woher kamen sie?

In manchen Situationen erstellt Astra Control automatisch einen Snapshot im Rahmen eines Backup-, Klon- oder Wiederherstellungsprozesses.

Meine Anwendung verwendet mehrere PVS. Wird Astra Control Snapshots und Backups all dieser VES machen?

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 Snapshots und Backups von Astra Control können nur mit Astra Control verwaltet werden.

Nutzen Sie Astra

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 Applikationen in Astra Control auf die Verwaltung der Apps und ihrer Ressourcen zu starten.

Weitere Informationen finden Sie unter "Anforderungen für das Applikationsmanagement".

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), werden vollständig unterstützt. Das Verwalten von mit Helm 2 installierten Apps wird nicht unterstützt.
- **Vom Betreiber implementierte Apps**: Astra Control unterstützt Apps, die mit Betreibern mit Namespace-Scoped installiert sind, die im Allgemeinen mit einer "Pass-by-Value"-Architektur statt mit "Pass-by-reference"-Architektur konzipiert sind. Ein Operator und die von ihm zu installieren App müssen denselben Namespace verwenden. Möglicherweise müssen Sie die yaml-Bereitstellungsdatei 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 einzelnen Namespace zugeordnet ist, kann verwaltet werden.

Applikationsmanagement

Nachdem Astra Control Namespaces auf den Clustern ermittelt hat, können Sie Anwendungen definieren, die Sie managen möchten. Sie können wählen "Sie managen einen gesamten Namespace als eine einzelne Applikation oder managen eine oder mehrere Applikationen im Namespace individuell". All dies kommt auf die Granularität zurück, die Sie für Datensicherungsvorgänge benötigen.

Obwohl Astra Control ermöglicht Ihnen, beide Ebenen der Hierarchie (den Namespace und die Apps in diesem Namespace) getrennt zu verwalten, ist die beste Praxis, 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.

Was Sie benötigen

- Astra Control ist ein Kubernetes Cluster.
- Eine oder mehrere installierte Applikationen auf dem Cluster. Weitere Informationen zu unterstützten App-Installationsmethoden.
- Ein oder mehrere aktive Pods.
- Namespaces wurden auf dem Kubernetes-Cluster angegeben, den Sie Astra Control hinzugefügt haben.
- (Optional) Kubernetes-Etikett auf jedem 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".

Bevor Sie beginnen, sollten Sie auch verstehen "Verwalten von Standard- und Systemnames".

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

Zusätzliche Optionen für Applikationsmanagement

- Das Management von Apps wird aufgehoben

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. Erfahren Sie mehr über Best Practices.

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** den Namespace Ihrer Anwendung aus.

   > Apps können nur innerhalb eines bestimmten Namespace auf einem einzelnen Cluster definiert werden. Astra Control unterstützt nicht die Möglichkeit, dass Apps mehrere Namespaces oder Cluster umfassen.

5. Geben Sie eine Bezeichnung für die App und den Namespace 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. 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 auf der Seite Anwendungen in der Liste der Apps angezeigt. 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.

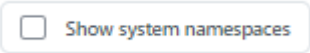
Definieren Sie einen Namespace, der als App gemanagt werden soll

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 Namespaces verwalten möchten, wählen Sie die Namespaces aus, und wählen Sie die Schaltfläche **Aktionen** in der linken oberen Ecke aus, und wählen Sie **Verwalten**.

> 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.

Das Management von Apps wird aufgehoben

Wenn Sie keine Backups, Snapshots oder Klone mehr erstellen möchten, können Sie deren Management beenden.

> Wenn Sie die Verwaltung einer Anwendung aufheben, gehen alle Backups oder Snapshots verloren, die zuvor erstellt wurden.

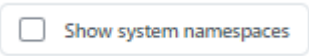
Schritte

1. Wählen Sie in der linken Navigationsleiste die Option **Anwendungen**.
2. Wählen Sie die App aus.
3. Wählen Sie im Menü 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 Nicht Verwalten**.

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 selbst ist keine Standard-App, sondern eine „System-App“. Sie sollten nicht versuchen, Astra Control selbst zu verwalten. Astra Control selbst wird für das Management nicht standardmäßig angezeigt.

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"

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" Zu einem Remote-Cluster mit NetApp SnapMirror Technologie 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 UI oder verwenden "Die Astra Control API" Um Anwendungen zu schützen.

Wenn Sie Helm zur Implementierung von Apps verwenden, erfordert Astra Control Center Helm Version 3. Das Management und Klonen von mit Helm 3 bereitgestellten Apps (oder ein Upgrade von Helm 2 auf Helm 3) werden vollständig unterstützt. Mit Helm 2 implementierte Apps werden nicht unterstützt.

Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder dem 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
- 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. Eine

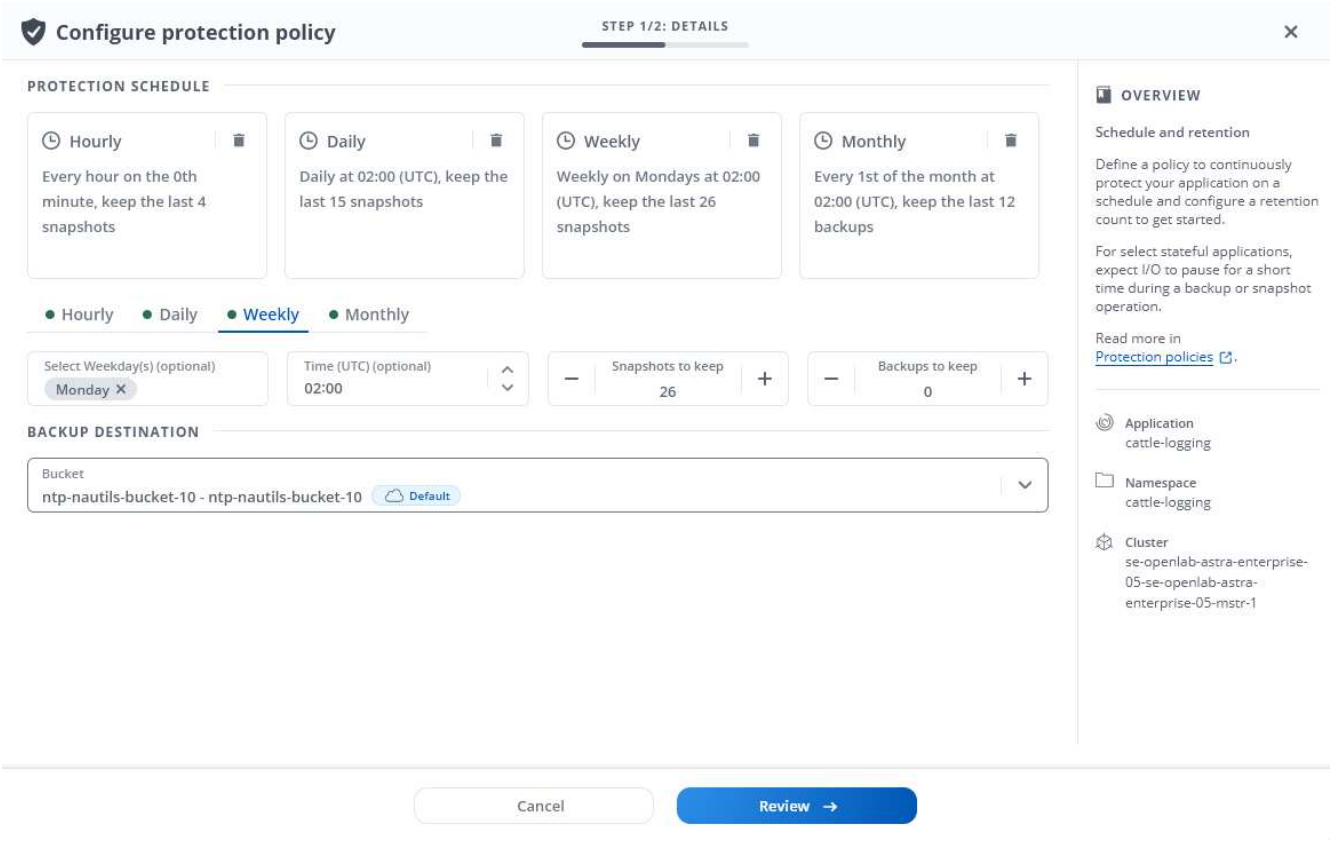
Sicherungsrichtlinie kann beispielsweise wöchentliche Backups und tägliche Snapshots erstellen und die Backups und Snapshots einen Monat lang aufbewahren. Wie oft Sie Snapshots und Backups erstellen und wie lange Sie sie behalten, hängt von den Anforderungen Ihres Unternehmens ab.

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.

   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 Center 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.

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 **Review**.
4. Überprüfen Sie die Snapshot-Zusammenfassung und wählen Sie **Snapshot**.

Ergebnis

Der Snapshot-Prozess beginnt. Ein Snapshot ist erfolgreich, wenn der Status **verfügbar** in der Spalte **Aktionen** auf der Seite **Datenschutz** > **Snapshots** steht.

Erstellen Sie ein Backup

Sie können eine App auch jederzeit sichern.

> 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.

Schritte

1. Wählen Sie **Anwendungen**.
2. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für die gewünschte App die Option **Backup** 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 ein Ziel für das Backup aus der Liste der Speicher-Buckets aus.
6. Wählen Sie **Bewertung**.
7. Überprüfen Sie die Backup-Zusammenfassung und wählen Sie **Backup**.

Ergebnis

Astra Control Center 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.

> Es gibt keine Möglichkeit, ein ausgelaufes Backup zu stoppen. Wenn Sie das Backup löschen müssen, warten Sie, bis es abgeschlossen ist, und befolgen Sie die Anweisungen unter Backups löschen. So löschen Sie ein fehlgeschlagenes Backup: "Verwenden Sie die Astra Control API".

> 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.

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.

> Eine Snapshot Kopie, die derzeit repliziert wird, kann nicht gelöscht werden.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer 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 Center löscht den Snapshot.

Abbrechen von Backups

Sie können ein gerade einlaufenden Backup abbrechen.

> Um ein Backup abzubrechen, muss sich das Backup im laufenden Zustand befinden. Sie können ein Backup, das sich im Status „Ausstehend“ befindet, 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 Löschvorgang 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.

Es gibt keine Möglichkeit, ein ausgelaufes Backup zu stoppen. Wenn Sie das Backup löschen müssen, warten Sie, bis es abgeschlossen ist, und befolgen Sie diese Anweisungen. So löschen Sie ein fehlgeschlagenes Backup: "Verwenden Sie die Astra Control API".

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 Center 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 "Die Astra Control API" Zur Wiederherstellung von Applikationen.

Über diese Aufgabe

- Es wird dringend empfohlen, einen Snapshot von Ihrer Anwendung zu erstellen oder zu sichern, bevor Sie sie wiederherstellen. Dadurch können Sie den Snapshot oder die Datensicherung klonen, wenn die Wiederherstellung nicht erfolgreich war.
- Wenn Sie Helm zur Implementierung von Apps verwenden, erfordert Astra Control Center Helm Version 3. Das Management und Klonen von mit Helm 3 bereitgestellten Apps (oder ein Upgrade von Helm 2 auf Helm 3) werden vollständig unterstützt. Mit Helm 2 implementierte Apps werden nicht unterstützt.
- Wenn Sie ein anderes Cluster wiederherstellen, stellen Sie sicher, dass das Cluster denselben Zugriffsmodus für persistente Volumes verwendet (z. B. ReadWriteManche). Der Wiederherstellungsvorgang schlägt fehl, wenn der Zugriffsmodus des Ziel-persistenten Volumes anders ist.
- Jeder Mitgliedsbenutzer mit Namespace-Einschränkungen nach Namespace-Name/ID oder durch Namespace-Bezeichnungen kann eine App in einem neuen Namespace auf demselben 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 ein neuer Namespace durch einen Klon- oder Wiederherstellungsvorgang erstellt wurde, kann der Account-Administrator/-Eigentümer das Mitglied-Benutzerkonto bearbeiten und Rolleneinschränkungen für den betroffenen Benutzer aktualisieren, um dem neuen Namespace Zugriff zu gewähren.
- Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder dem 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** und dann den Namen einer App aus.
2. Wählen Sie **Datenschutz**.
3. Wenn Sie von einem Snapshot wiederherstellen möchten, lassen Sie das **Snapshots** -Symbol ausgewählt. Andernfalls wählen Sie das Symbol **Backups** aus, um aus einem Backup wiederherzustellen.
4. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für den Snapshot oder die Datensicherung, aus der Sie wiederherstellen möchten, **Anwendung wiederherstellen** aus.
5. **Restore Details**: Geben Sie Details für die wiederhergestellte App an. Standardmäßig werden das aktuelle Cluster und der aktuelle Namespace angezeigt. Lassen Sie diese Werte intakt, um eine App an Ort und Stelle wiederherzustellen, die die App auf eine frühere Version von selbst zurücksetzt. Ändern Sie diese Werte, wenn Sie die Daten in einem anderen Cluster oder Namespace wiederherstellen möchten.
   - Geben Sie einen Namen und einen Namespace für die App ein.
   - Wählen Sie das Ziel-Cluster für die App aus.
   - Wählen Sie **Bewertung**.

   > 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.

6. **Zusammenfassung wiederherstellen**: Überprüfen Sie die Details über die Wiederherstellungsaktion, geben Sie "wiederherstellen" ein und wählen Sie **Wiederherstellen**.

Ergebnis

Astra Control Center stellt die App basierend auf den von Ihnen bereitgestellten Informationen wieder her. Wenn Sie die Applikation bereits wiederhergestellt haben, werden die Inhalte vorhandener persistenter Volumes durch den Inhalt persistenter Volumes aus der wiederhergestellten App ersetzt.

> 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 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.

Replizieren von Applikationen auf einem Remote-System mit 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). Sobald Ihre Applikationen konfiguriert sind, können sie Daten und Applikationsänderungen von einem Cluster auf ein anderes replizieren.

Einen Vergleich zwischen Backups/Wiederherstellungen und der Replizierung finden Sie unter "Konzepte zur Datensicherung".

Applikationen lassen sich in unterschiedlichen Szenarien replizieren, z. B. nur on-Premises, in Hybrid- und Multi-Cloud-Szenarien:

- 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 Applikation (auf dem anderen Cluster oder Standort ausgeführt) 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-Betrieb einer replizierten App 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

Siehe "Replikationsvoraussetzungen" Bevor Sie beginnen.

Richten Sie eine Replikationsbeziehung ein

Die Einrichtung einer Replikationsbeziehung umfasst Folgendes, die die Replikationsrichtlinie enthält;

- Wählen Sie, wie häufig Astra Control einen App Snapshot erstellen soll (einschließlich der Kubernetes-Ressourcen der Applikation und der Volume-Snapshots für die einzelnen Applikations-Volumes).
- Auswahl des Replizierungszeitplans (einschließlich Kubernetes-Ressourcen und persistente Volume-Daten)
- Einstellen der Zeit, die für die Erstellung des Snapshots verwendet werden soll

Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie auf der Seite Anwendung die Registerkarte **Datenschutz** > **Replikation** aus.
3. Wählen Sie auf der Registerkarte Data Protection > Replication die Option **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
   - **Zielspeicherklasse**: Wählen Sie die Speicherklasse aus, die die gekoppelte SVM auf dem Ziel-ONTAP-Cluster verwendet.
   - **Replikationstyp**: "Asynchron" ist derzeit der einzige verfügbare Replikationstyp.
   - **Ziel-Namespace**: Geben Sie einen neuen oder bestehenden Ziel-Namespace für das Ziel-Cluster ein.

     Alle in Konflikt stehenden Ressourcen im ausgewählten Namespace werden überschrieben.

   - **Frequenz der Replikation**: Legen Sie fest, wie oft Astra Control einen Snapshot machen und ihn an sein Ziel replizieren soll.
   - **Offset**: Stellen Sie die Anzahl der Minuten von der Stunde her, die Sie möchten, dass Astra Control einen Schnappschuss machen soll. Möglicherweise möchten Sie einen Offset verwenden, sodass er nicht mit anderen geplanten Vorgängen übereinstimmt. Wenn Sie beispielsweise den Snapshot alle 5 Minuten ab 10:02 Uhr aufnehmen möchten, geben Sie als Offset-Minuten „02“ ein. Das Ergebnis sind 10:02, 10:07, 10:12 usw.
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**.

   Der Snapshot-Name verwendet das Format „Replication-Schedule-<string>“. Astra Control behält den letzten Snapshot, der für die Replizierung verwendet wurde. Alle älteren Replizierungs-Snapshots werden nach 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.
- Ersten applikationskonsistenten Snapshot
- Legt mithilfe des ersten Snapshots die SnapMirror Beziehung für persistente Volumes fest

Auf der Seite Datensicherung werden der Status und der Status der Replikationsbeziehung angezeigt: <Status> <Lebenszyklus der Beziehung>

Zum Beispiel: Normal

Weitere Informationen zu Replikationsstatus und -Status finden Sie unten.

Online-Betrieb einer replizierten App auf dem Ziel-Cluster (Failover)

Mit Astra Control können Sie ein „Failover“ Ihrer replizierten Applikationen auf ein Ziel-Cluster ausführen. 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 auf der Seite Anwendung die Registerkarte **Datenschutz** > **Replikation** aus.
3. Wählen Sie auf der Registerkarte Datenschutz > Replikation im Menü Aktionen die Option **Failover** aus.
4. Überprüfen Sie auf der Seite Failover die Informationen, und wählen Sie **Failover**.

Ergebnis

Die folgenden Aktionen ergeben sich aus dem Failover-Verfahren:

- Auf dem Ziel-Cluster wird die Applikation 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 basierend auf den Zeitplänen in der Quell-App zum Zeitpunkt des Failover in die Ziel-App kopiert.
- 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 auf der Seite Anwendung die Registerkarte **Datenschutz** > **Replikation** aus.
3. Wählen Sie auf der Registerkarte Datenschutz > Replikation im Menü Aktionen die Option **Resync** aus.
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 ein geplanter Vorgang, bei dem die Applikation zum Ziel-Cluster verschoben und anschließend wieder zurück auf das ursprüngliche Quell-Cluster repliziert wird. Astra Control stoppt die Applikation auf dem Quell-Cluster und repliziert die Daten zum Ziel, bevor ein Failover der App zum Ziel-Cluster erfolgt.

In dieser Situation tauschen Sie Quelle und Ziel aus. Der ursprüngliche Quellcluster wird zum neuen Ziel-Cluster, und das ursprüngliche Ziel-Cluster wird zum neuen Quellcluster.

Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie auf der Seite Anwendung die Registerkarte **Datenschutz** > **Replikation** aus.
3. Wählen Sie auf der Registerkarte Datenschutz > Replikation im Menü Aktionen die Option **Replikation umkehren** aus.
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:

- Es wird ein Snapshot der Kubernetes-Ressourcen der ursprünglichen Quell-Applikation 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 Applikation erstellt und repliziert.
- Die SnapMirror Beziehungen sind beschädigt, wodurch die Zieldatenträger für Lese-/Schreibvorgänge bereit sind.
- Die Kubernetes-Ressourcen der Applikation werden aus dem vor dem Herunterfahren-Snapshot wiederhergestellt. Dabei werden die Volume-Daten repliziert, nachdem die ursprüngliche Quell-App heruntergefahren wurde.
- 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 „Failback“ erreichen, indem Sie die folgende Reihenfolge der Vorgänge verwenden. In diesem Workflow repliziert (neu synchronisiert) Astra Control alle Anwendungen, die in die ursprüngliche Replikationsrichtung geändert werden, zurück zum ursprünglichen Quell-Cluster, bevor die Replikationsrichtung umkehrt.

Dieser Prozess beginnt mit einer Beziehung, die ein Failover zu einem Ziel abgeschlossen hat und die folgenden Schritte umfasst:

- 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 auf der Seite Anwendung die Registerkarte **Datenschutz** > **Replikation** aus.
3. Wählen Sie auf der Registerkarte Datenschutz > Replikation im Menü Aktionen die Option **Resync** aus.
4. Für einen Fail-Back-Vorgang wählen Sie die Failover-App als Quelle für den Resynchronisierungsvorgang aus (wobei Daten nach dem Failover beim Schreiben beibehalten werden).
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 auf der Seite Anwendung die Registerkarte **Datenschutz** > **Replikation** aus.
3. Wählen Sie auf der Registerkarte Datenschutz > Replikation im Feld Anwendungsschutz oder im Beziehungsdiagramm die Option **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 hergestellt oder hat sich etabliert, und der jüngste 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 steht fest (also, ein erfolgreicher Snapshot wurde repliziert, und ein Failover ist möglich), aber der neueste Snapshot ist ausgefallen oder zur Replizierung fehlgeschlagen.

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 PVCs verfügbar sind, überprüft die Replikationsbeziehung, erstellt regelmäßig Snapshots der App und identifiziert alle neuen Quell-VES in der App. Wenn ja, erstellt Astra Control die Ressourcen, die sie in die Replikation aufnehmen.
- **Failover**: Astra Control durchbricht die SnapMirror Beziehungen und stellt die Kubernetes-Ressourcen der App aus dem letzten erfolgreich replizierten App-Snapshot wieder her.
- **Failover**: Astra Control stoppt die Replizierung vom Quell-Cluster, 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 klonen, um eine doppelte Applikation auf demselben Kubernetes-Cluster oder einem anderen Cluster zu erstellen. Wenn Astra Control Center eine Applikation geklont, 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 UI oder verwenden "Die Astra Control API" Zum Klonen und Migrieren von Applikationen

Was Sie benötigen

Zum Klonen von Applikationen auf einem anderen Cluster benötigen Sie einen Standard-Bucket. Wenn Sie einen ersten Bucket hinzufügen, wird dieser zum Standard-Bucket.

Über diese Aufgabe

- Wenn Sie eine App implementieren, die explizit auf StorageClass gesetzt ist und Sie die Applikation klonen müssen, muss das Ziel-Cluster über die ursprünglich angegebene StorageClass verfügen. Das Klonen einer Applikation, deren StorageClass explizit auf ein Cluster festgelegt ist, das nicht über dieselbe StorageClass verfügt, schlägt fehl.
- 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.
- 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.
- Während eines Applikations-Backups oder Applikations-Restores können Sie optional eine Bucket-ID angeben. Ein Applikationsklonvorgang verwendet jedoch immer den definierten Standard-Bucket. Es besteht keine Möglichkeit, die Buckets für einen Klon zu ändern. Wenn Sie die Kontrolle darüber haben möchten, welcher Bucket verwendet wird, können Sie entweder "Ändern Sie den Bucket-Standard" Oder machen Sie ein "Backup" Gefolgt von A "Wiederherstellen" Separat.
- Jeder Mitgliedsbenutzer mit Namespace-Einschränkungen nach Namespace-Name/ID oder durch Namespace-Bezeichnungen kann eine App in einem neuen Namespace auf demselben 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 ein neuer Namespace durch einen Klon- oder Wiederherstellungsvorgang erstellt wurde, kann der Account-Administrator/-Eigentümer das Mitglied-Benutzerkonto bearbeiten und Rolleneinschränkungen für den betroffenen Benutzer aktualisieren, um dem neuen Namespace Zugriff zu gewähren.

OpenShift-Überlegungen

- Wenn Sie eine App zwischen Clustern klonen, müssen die Quell- und Ziel-Cluster dieselbe Verteilung von OpenShift aufweisen. Wenn Sie beispielsweise eine App aus einem OpenShift 4.7-Cluster klonen, verwenden Sie ein Ziel-Cluster, das auch OpenShift 4.7 ist.
- Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder dem 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. **Clone Details**: Geben Sie Details für den Klon an:
   - Geben Sie einen Namen ein.
   - Geben Sie einen Namespace für den Klon ein.
   - Wählen Sie ein Ziel-Cluster für den Klon.
   - Wählen Sie aus, ob Sie den Klon aus einem vorhandenen Snapshot oder einem vorhandenen Backup erstellen möchten. Wenn Sie diese Option nicht wählen, erstellt Astra Control Center den Klon aus dem aktuellen Status der App.
5. **Quelle**: Wenn Sie sich für das Klonen aus einem vorhandenen Snapshot oder Backup entscheiden, wählen Sie den Snapshot oder die Sicherung, die Sie verwenden möchten.
6. Wählen Sie **Bewertung**.
7. **Clone Summary**: Überprüfen Sie die Details über den Klon und wählen Sie **Clone**.

Ergebnis

Astra Control Center klont die App basierend auf den von Ihnen angegebenen Informationen. Der Klonvorgang ist erfolgreich, wenn der neue Applikationsklon im ausgeführt wird `Available` Geben Sie auf der Seite **Anwendungen** an.

> 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.

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 mithilfe von Testsuiten alle Datenbanktransaktionen vor dem Snapshot anhalten und die Transaktionen nach Abschluss des Snapshots fortsetzen. Dies gewährleistet applikationskonsistente Snapshots.

Arten von Ausführungshaken

Astra Control unterstützt die folgenden Arten von Ausführungshaken, je nachdem, wann sie ausgeführt werden können:

- Vor dem Snapshot
- Nach dem Snapshot
- Vor dem Backup
- Nach dem Backup
- Nach dem Wiederherstellen

Wichtige Hinweise zu benutzerdefinierten Testausführungshaken

Bei der Planung von Testausführungshooks für Ihre Apps sollten Sie Folgendes berücksichtigen:

- 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.
- Bei Ad-hoc-Datenschutzvorgängen werden alle Hook-Ereignisse im Ereignisprotokoll auf der Seite * erzeugt und 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).

> Da die 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 ein Testinaper nach dem Backup nicht davon ausgehen kann, dass die Sicherung abgeschlossen wurde.

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. So würde beispielsweise die Reihenfolge der Ausführung einer Konfiguration mit allen fünf verschiedenen Hooks aussehen:

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
1	Klon	N	N	Neu	Gleich	Y	N	Y
2	Klon	N	N	Neu	Anders	Y	Y	Y
3	Klonen oder Wiederherstellen	Y	N	Neu	Gleich	N	N	Y
4	Klonen oder Wiederherstellen	N	Y	Neu	Gleich	N	N	Y
5	Klonen oder Wiederherstellen	Y	N	Neu	Anders	N	Y	Y
6	Klonen oder Wiederherstellen	N	Y	Neu	Anders	N	N	Y
7	Wiederherstellen	Y	N	Vorhanden	Gleich	N	N	Y
8	Wiederherstellen	N	Y	Vorhanden	Gleich	N	N	Y
9	Snapshot	K. A.	K. A.	K. A.	K. A.	Y	K. A.	K. A.
10	Backup	N	K. A.	K. A.	K. A.	Y	Y	K. A.
11	Backup	Y	K. A.	K. A.	K. A.	N	Y	K. A.

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, die Quelle und den Ablauf eines Hakens (vor oder nach dem Betrieb). Um Ereignisprotokolle zu den Testausführungshaken anzuzeigen, gehen Sie zur Seite **Aktivität** im linken Navigationsbereich.

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

Sie können einen oder mehrere Skripte hinzufügen, auf die Testausführungshaken verweisen können. Viele Testsuitehaoks können auf dasselbe Skript verweisen. So können Sie viele Testsuiten aktualisieren, indem Sie nur ein Skript ändern.

Schritte

1. Gehen Sie zu **Konto**.
2. Wählen Sie die Registerkarte **Skripts** aus.
3. Wählen Sie **Hinzufügen**.
4. 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.
5. 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 Testsuite-Haken für eine App erstellen. 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. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie **Hinzufügen**.
4. Legen Sie im Bereich **Hook Details** fest, wann der Haken ausgeführt werden soll, indem Sie im Dropdown-Menü **Operation** einen Operationstyp auswählen.
5. Geben Sie einen eindeutigen Namen für den Haken ein.
6. (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.
7. Wenn der Haken im Bereich **Container Images** auf alle Container-Bilder in der Anwendung laufen soll, aktivieren Sie das Kontrollkästchen **auf alle Container-Bilder** anwenden. Sollte der Haken stattdessen nur auf ein oder mehrere angegebene Container-Images wirken, geben Sie die Container-Bildnamen in das Feld **Container-Bildnamen ein, die mit** übereinstimmen.
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 **Haken 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.

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**.

Beispiele für Testausführungshaken

Nutzen Sie die folgenden Beispiele, um eine Vorstellung davon zu erhalten, wie Sie Ihre Testausführungshaken strukturieren. Sie können diese Haken als Vorlagen oder als Testskripte verwenden.

Einfaches Erfolgsbeispiel

Dies ist ein Beispiel für einen einfachen Haken, der erfolgreich ist und eine Nachricht in die Standardausgabe und Standardfehler schreibt.

```
#!/bin/sh

# success_sample.sh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#



#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}
```

```
#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample.sh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Einfaches Erfolgsbeispiel (Bash-Version)

Dies ist ein Beispiel für einen einfachen Haken, der erfolgreich ist und eine Nachricht in die Standardausgabe und Standardfehler schreibt, für bash geschrieben.

```
#!/bin/bash

# success_sample.bash
#
# A simple noop success hook script for testing purposes.
#
# args: None


#
```

```
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample.bash"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Einfaches Erfolgsbeispiel (zsh-Version)

Dies ist ein Beispiel für einen einfachen Haken, der erfolgreich ist und eine Nachricht in Standardausgabe und Standardfehler schreibt, geschrieben für Z Shell.

```
#!/bin/zsh
```

```
# success_sample.zsh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}

#
# main
#

# log something to stdout
info "running success_sample.zsh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Erfolg mit Argumenten Beispiel

Das folgende Beispiel zeigt, wie Sie in einem Haken Aargliste verwenden können.

```
#!/bin/sh

# success_sample_args.sh
#
# A simple success hook script with args for testing purposes.
#
# args: Up to two optional args that are echoed to stdout

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample_args.sh"
```

```
# collect args
arg1=$1
arg2=$2

# output args and arg count to stdout
info "number of args: $#"
info "arg1 ${arg1}"
info "arg2 ${arg2}"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Beispiel für Haken vor dem Snapshot/nach dem Snapshot

Das folgende Beispiel zeigt, wie dasselbe Skript sowohl für einen Pre-Snapshot als auch für einen Post-Snapshot-Haken verwendet werden kann.

```
#!/bin/sh

# success_sample_pre_post.sh
#
# A simple success hook script example with an arg for testing purposes
# to demonstrate how the same script can be used for both a prehook and
posthook
#
# args: [pre|post]

# unique error codes for every error case
ebase=100
eusage=$((ebase+1))
ebadstage=$((ebase+2))
epre=$((ebase+3))
epost=$((ebase+4))


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}
```

```
#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# Would run prehook steps here
#
prehook() {
    info "Running noop prehook"
    return 0
}

#
# Would run posthook steps here
#
posthook() {
    info "Running noop posthook"
    return 0
}


#
# main
#

# check arg
stage=$1
if [ -z "${stage}" ]; then
    echo "Usage: $0 <pre|post>"
```

```
    exit ${eusage}
fi

if [ "${stage}" != "pre" ] && [ "${stage}" != "post" ]; then
    echo "Invalid arg: ${stage}"
    exit ${ebadstage}
fi

# log something to stdout
info "running success_sample_pre_post.sh"

if [ "${stage}" = "pre" ]; then
    prehook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during prehook"
    fi
fi

if [ "${stage}" = "post" ]; then
    posthook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during posthook"
    fi
fi

exit ${rc}
```

Fehlerbeispiel

Das folgende Beispiel zeigt, wie Sie Fehler in einem Haken handhaben können.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#



#
# Writes the given message to standard output
#
```

```
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

Beispiel für ausführlichen Fehler

Das folgende Beispiel zeigt, wie Sie Fehler in einem Haken mit detaillierteren Protokollierung behandeln können.

```
#!/bin/sh

# failure_sample_verbose.sh
#
# A simple failure hook script with args for testing purposes.
#
# args: [The number of lines to output to stdout]


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_verbose.sh"


# output arg value to stdout
```

```
linecount=$1
info "line count ${linecount}"

# write out a line to stdout based on line count arg
i=1
while [ "$i" -le ${linecount} ]; do
    info "This is line ${i} from failure_sample_verbose.sh"
    i=$(( i + 1 ))
done

error "exiting with error code 8"
exit 8
```

Fehler bei einem Beispiel für den Exit-Code

Das folgende Beispiel zeigt, dass ein Haken mit einem Exit-Code ausfällt.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#



#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}



#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}
```

```
#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

Beispiel Erfolg nach Ausfall

Das folgende Beispiel zeigt, dass bei der ersten Ausführung ein Haken versagt, der jedoch nach dem zweiten Lauf erfolgreich ist.

```
#!/bin/sh

# failure_then_success_sample.sh
#
# A hook script that fails on initial run but succeeds on second run for
testing purposes.
#
# Helpful for testing retry logic for post hooks.
#
# args: None
#

#
# Writes the given message to standard output
#
# $* - The message to write
```

```
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_success sample.sh"


if [ -e /tmp/hook-test.junk ] ; then
    info "File does exist.  Removing /tmp/hook-test.junk"
    rm /tmp/hook-test.junk
    info "Second run so returning exit code 0"
    exit 0
else
    info "File does not exist.  Creating /tmp/hook-test.junk"
    echo "test" > /tmp/hook-test.junk
    error "Failed first run, returning exit code 5"
    exit 5
fi
```

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.

Anzeigen des Systemzustands und der Details von Clustern

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.

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.

Anzeigen des Funktionszustands und der Details einer App

Nachdem Sie mit dem Management der Applikation begonnen haben, stellt Astra detaillierte Informationen zur Applikation bereit, mit der Sie den Status (unabhängig davon, ob er sich gesund ist), den Sicherungsstatus (ob er im Falle eines Ausfalls vollständig geschützt ist), die Behälter, den persistenten Storage und vieles mehr ermitteln können.

Schritte

1. Wählen Sie in der Astra Control Center-UI **Anwendungen** und dann den Namen einer App aus.
2. Hier finden Sie die gewünschten Informationen:

   Anwendungsstatus

   Gibt einen Status an, der den Status der App in Kubernetes wiedergibt. Sind Pods und persistente Volumes beispielsweise online? Wenn eine Applikation fehlerhaft ist, müssen Sie mit den Kubernetes-Protokollen zum Beheben des Problems im Cluster wechseln. Astra stellt keine Informationen zur Verfügung, die Ihnen bei der Behebung einer defekten App helfen.

   App-Schutzstatus

   Gibt den Status an, 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.

Überblick

Informationen über den Status der Pods, die mit der App verknüpft sind.

Datensicherung

Hiermit können Sie eine Datenschutzrichtlinie konfigurieren und die vorhandenen Snapshots und Backups anzeigen.

Storage

Zeigt Ihnen die persistenten Volumes auf App-Ebene. Der Zustand eines persistenten Volumes befindet sich aus der Perspektive des Kubernetes Clusters.

Ressourcen

Hiermit können Sie überprüfen, welche Ressourcen gesichert und gemanagt 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

Benutzer managen

Sie können Benutzer Ihrer Astra Control Center-Installation über die Astra Control-Benutzeroberfläche einladen, hinzufügen, entfernen und bearbeiten. Sie können die Astra Control UI oder verwenden "Die 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-Benutzer durchzuführen. Auf hohem Niveau beinhaltet die Konfiguration die Integration von Astra mit LDAP und die Definition der Astra-Benutzer und -Gruppen entsprechend der LDAP-Definitionen. Siehe "LDAP-Authentifizierung" Finden Sie weitere Informationen.

Benutzer einladen

Kontoinhaber und -Administratoren können neue Benutzer zum Astra Control Center einladen.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Wählen Sie die Registerkarte **Benutzer** aus.
3. Wählen Sie **Benutzer Einladen**.
4. Geben Sie den Namen und die E-Mail-Adresse des Benutzers ein.
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 "Rollen managen".

7. Wählen Sie **Benutzer einladen**.

   Der Benutzer erhält eine E-Mail, in der er darüber informiert wird, dass er zum Astra Control Center eingeladen wurde. Die E-Mail enthält ein temporäres Passwort, das sie bei der ersten Anmeldung ändern müssen.

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 "Rollen managen".

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**.

Ändern Sie die Rolle eines Benutzers

Benutzer mit der Rolle „Eigentümer“ können die Rolle aller Benutzer ändern, während Benutzer mit der Administratorrolle die Rolle von Benutzern ändern können, die die Rolle „Administrator“, „Mitglied“ oder „Viewer“ haben.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Wählen Sie die Dropdown-Liste **Aktionen** aus.
3. Wählen Sie **Rolle bearbeiten**.
4. Wählen Sie eine neue Rolle aus.
5. Um Einschränkungen auf die Rolle anzuwenden, aktivieren Sie das Kontrollkästchen **Rolle auf Einschränkungen beschränken** und wählen Sie eine Bedingung aus der Liste aus.

   Wenn es keine Einschränkungen gibt, können Sie eine Bedingung hinzufügen. Weitere Informationen finden Sie unter "Rollen managen".

6. Wählen Sie **Bestätigen**.

Ergebnis

Astra Control Center aktualisiert die Benutzerberechtigungen auf der Grundlage der neuen Rolle, die Sie ausgewählt haben.

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 "Die Astra Control API" Rollen managen.

Fügen Sie einer Rolle eine Namespace-Einschränkung hinzu

Ein Administrator oder Eigentümer kann 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"

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 eigenen erstellen `kubeconfig` Datei, Sie sollten nur ein **ein**-Kontext-Element darin definieren. Siehe "Kubernetes-Dokumentation" Weitere Informationen zum Erstellen `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 UI oder verwenden "Die 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"

Repository-Verbindungen verwalten

Repositories können mit Astra Control verbunden werden, um als Referenz für Installationsabbilder und Artefakte für Softwarepakete zu verwenden. Beim Importieren von Softwarepaketen verweist Astra Control auf Installationsabbilder im Image Repository sowie auf Binärdateien und andere Artefakte im Artefakt-Repository.

Was Sie benötigen

- Kubernetes-Cluster mit installiertem Astra Control Center
- Ein ausgelaufes Docker Repository, auf das Sie zugreifen können
- Ein ausgeführten Artefakt-Repository (z. B. Artifactory), auf das Sie zugreifen können

Verbinden eines Docker Image-Repositorys

Sie können ein Docker-Image-Repository anschließen, um Installations-Images für Pakete wie die für Astra Data Store zu speichern. Bei der Installation von Paketen importiert Astra Control die Paket-Image-Dateien aus dem Image-Repository.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Wählen Sie die Registerkarte **Connections**.
3. Wählen Sie im Abschnitt * Docker Image Repository* das Menü oben rechts aus.
4. Wählen Sie **Verbinden**.
5. Fügen Sie die URL und den Port für das Repository hinzu.

6. Geben Sie die Anmeldeinformationen für das Repository ein.
7. Wählen Sie **Verbinden**.

Ergebnis

Das Repository ist verbunden. Im Abschnitt * Docker Image Repository* sollte im Repository ein verbundener Status angezeigt werden.

Trennen Sie ein Docker Image-Repository

Sie können die Verbindung zu einem Docker-Image-Repository entfernen, wenn sie nicht mehr benötigt wird.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Wählen Sie die Registerkarte **Connections**.
3. Wählen Sie im Abschnitt * Docker Image Repository* das Menü oben rechts aus.
4. Wählen Sie **Trennen**.
5. Wählen Sie **Ja, Docker Image Repository trennen**.

Ergebnis

Das Repository ist getrennt. Im Abschnitt * Docker Image Repository* sollte der Status „nicht verbunden“ angezeigt werden.

Verbinden eines Artefakt-Repository

Ein Artefakt-Repository kann mit Host-Artefakten wie Binärdateien verbunden werden. Bei der Installation von Paketen importiert Astra Control die Artefakte für die Softwarepakete aus dem Image-Repository.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Wählen Sie die Registerkarte **Connections**.
3. Wählen Sie im Abschnitt **Artefakt-Repository** das Menü oben rechts aus.
4. Wählen Sie **Verbinden**.
5. Fügen Sie die URL und den Port für das Repository hinzu.
6. Wenn eine Authentifizierung erforderlich ist, aktivieren Sie das Kontrollkästchen **Authentifizierung verwenden** und geben Sie die Anmeldeinformationen für das Repository ein.
7. Wählen Sie **Verbinden**.

Ergebnis

Das Repository ist verbunden. Im Abschnitt **Artefakt-Repository** sollte im Repository ein verbundener Status angezeigt werden.

Trennen Sie ein Artefakt-Repository

Sie können die Verbindung zu einem Artefakt-Repository entfernen, wenn es nicht mehr benötigt wird.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.

2. Wählen Sie die Registerkarte **Connections**.
3. Wählen Sie im Abschnitt **Artefakt-Repository** das Menü oben rechts aus.
4. Wählen Sie **Trennen**.
5. Wählen Sie **Ja, trennen Sie das Artefakt-Repository**.

Ergebnis

Das Repository ist getrennt. Im Abschnitt **Artefakt-Repository** sollte im Repository ein verbundener Status angezeigt werden.

Weitere Informationen

- "Managen von Softwarepaketen"

Managen von Softwarepaketen

NetApp bietet zusätzliche Funktionen für Astra Control Center mit Software-Paketen, die Sie von der NetApp Support-Website herunterladen können. Nachdem Sie Docker- und Artefakt-Repositorys verbunden haben, können Sie Pakete hochladen und importieren, um diese Funktion dem Astra Control Center hinzuzufügen. Sie können Softwarepakete über die CLI oder die Weboberfläche des Astra Control Center verwalten.

Was Sie benötigen

- Kubernetes-Cluster mit installiertem Astra Control Center
- Ein verbundenes Docker-Image-Repository zur Speicherung von Software-Paket-Images. Weitere Informationen finden Sie unter "Repository-Verbindungen verwalten".
- Ein verbundenes Artefakt-Repository zur Speicherung von Binärdateien und Artefakten für Softwarepakete Weitere Informationen finden Sie unter "Repository-Verbindungen verwalten".
- Ein Software-Paket von der NetApp Support Site

Laden Sie Software-Paketbilder in die Repositorys hoch

Astra Control Center verweist auf Paketbilder und -Artefakte in angeschlossenen Repositorys. Sie können Bilder und Artefakte mithilfe der CLI in die Repositorys hochladen.

Schritte

1. Laden Sie das Software-Paket von der NetApp Support-Website herunter und speichern Sie es auf einem System, auf dem es installiert ist `kubectl` Dienstprogramm installiert.
2. Extrahieren Sie die komprimierte Paketdatei und wechseln Sie das Verzeichnis zum Speicherort der Astra Control Bundle-Datei (z. B. `acc.manifest.yaml`).
3. Übertragen Sie die Paket-Images auf das Docker Repository. Nehmen Sie folgende Ersetzungen vor:
   - ERSETZEN SIE DIE BUNDLE_FILE durch den Namen der Astra Control Bundle-Datei (z. B. `acc.manifest.yaml`).
   - ERSETZEN SIE MY_REGISTRY durch die URL des Docker Repositorys.
   - 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_REGISTRY -u
MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

4. Wenn das Paket Artefakte enthält, kopieren Sie die Artefakte in das Artefakt-Repository. ERSETZEN SIE BUNDLE_FILE durch den Namen der Astra Control Bundle-Datei und NETWORK_LOCATION durch den Netzwerkspeicherort, um die Artefaktdateien zu kopieren:

```
kubectl astra packages copy-artifacts -m BUNDLE_FILE -n NETWORK_LOCATION
```

Fügen Sie ein Softwarepaket hinzu

Sie können Softwarepakete mit einer Astra Control Center-Paketdatei importieren. Dadurch wird das Paket installiert und die Software für Astra Control Center zur Verfügung gestellt.

Fügen Sie mithilfe der Web-Benutzeroberfläche von Astra Control ein Softwarepaket hinzu

Über die Web-Benutzeroberfläche von Astra Control Center können Sie ein Softwarepaket hinzufügen, das in die angeschlossenen Repositories hochgeladen wurde.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Wählen Sie die Registerkarte **Pakete** aus.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**.
4. Wählen Sie im Dialogfeld Dateiauswahl das Symbol Hochladen aus.
5. Wählen Sie in eine Astra Control Bundle-Datei `.yaml` Format für Upload.
6. Wählen Sie **Hinzufügen**.

Ergebnis

Wenn die Bundle-Datei gültig ist und sich die Paketbilder und Artefakte in den angeschlossenen Repositorys befinden, wird das Paket dem Astra Control Center hinzugefügt. Wenn der Status in der Spalte **Status** in **verfügbar** wechselt, können Sie das Paket verwenden. Sie können den Mauszeiger auf den Status eines Pakets bewegen, um weitere Informationen zu erhalten.

> Wenn ein oder mehrere Bilder oder Artefakte für ein Paket nicht im Repository gefunden werden, wird eine Fehlermeldung für dieses Paket angezeigt.

Fügen Sie mithilfe der CLI ein Softwarepaket hinzu

Sie können über die CLI ein Softwarepaket importieren, das Sie in die angeschlossenen Repositories hochgeladen haben. Dazu müssen Sie zunächst Ihre Astra Control Center-Konto-ID und ein API-Token aufzeichnen.

Schritte

1. Melden Sie sich über einen Webbrowser bei der Web-UI von Astra Control Center an.
2. Wählen Sie im Dashboard das Benutzersymbol rechts oben aus.

3. Wählen Sie **API-Zugriff**.
4. Notieren Sie sich die Konto-ID im oberen Bereich des Bildschirms.
5. Wählen Sie **API-Token generieren** aus.
6. Wählen Sie im daraufhin angezeigten Dialogfeld **API-Token generieren** aus.
7. Notieren Sie das resultierende Token, und wählen Sie **Schließen**. Ändern Sie in der CLI die Verzeichnisse in den Speicherort des `.yaml` Paketdatei im extrahierten Paketinhalt.
8. Importieren Sie das Paket mithilfe der Bundle-Datei, indem Sie folgende Ersetzungen vornehmen:
   - ERSETZEN SIE DIE BUNDLE_FILE durch den Namen der Astra Control Bundle-Datei.
   - ERSETZEN SIE DEN SERVER durch den DNS-Namen der Astra Control-Instanz.
   - ERSETZEN SIE ACCOUNT_ID und TOKEN durch die Konto-ID und das API-Token, das Sie zuvor aufgezeichnet haben.

   ```
   kubectl astra packages import -m BUNDLE_FILE -u SERVER -a ACCOUNT_ID
   -k TOKEN
   ```

Ergebnis

Wenn die Bundle-Datei gültig ist und sich die Paketbilder und Artefakte in den angeschlossenen Repositorys befinden, wird das Paket dem Astra Control Center hinzugefügt.

> Wenn ein oder mehrere Bilder oder Artefakte für ein Paket nicht im Repository gefunden werden, wird eine Fehlermeldung für dieses Paket angezeigt.

Entfernen eines Softwarepakets

Sie können die Web-Benutzeroberfläche von Astra Control Center verwenden, um ein Softwarepaket zu entfernen, das Sie zuvor in Astra Control Center importiert haben.

Schritte

1. Wählen Sie im Navigationsbereich * Konto verwalten* die Option **Konto**.
2. Wählen Sie die Registerkarte **Pakete** aus.

   Auf dieser Seite sehen Sie die Liste der installierten Pakete und deren Status.

3. Öffnen Sie in der Spalte **Aktionen** des Pakets das Menü Aktionen.
4. Wählen Sie **Löschen**.

Ergebnis

Das Paket wird aus dem Astra Control Center gelöscht, aber die Bilder und Artefakte für das Paket verbleiben in Ihren Repositorys.

Weitere Informationen

- "Repository-Verbindungen verwalten"

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 brauchen keinen Eimer, wenn Sie Ihre Anwendungskonfiguration und Ihren persistenten Storage im selben 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 möglicherweise nicht alle Objektspeicher-Anbieter, die die S3-Unterstützung von Amazon 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: Auf den Bucket ist derzeit nicht zugegriffen werden können.

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
- 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 Optionen in der Spalte **Aktionen** die Option **Bearbeiten** aus.
3. Ändern Sie alle Informationen außer dem Bucket-Typ.

   Sie können den Bucket-Typ nicht ändern.

4. Wählen Sie **Aktualisieren**.

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.

Was Sie benötigen

- 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
- Unmanagement eines Storage-Backends
- Aktualisieren einer Astra Data Store Storage-Backend-Lizenz
- Upgrade eines Astra Data Store Storage-Backends
- Entfernen Sie ein Speicher-Back-End

- Fügen Sie Nodes zu einem Storage-Back-End-Cluster hinzu
- Entfernen Sie die Nodes aus einem Storage-Back-End-Cluster

Details zum Storage-Back-End

Sie können Speicher-Backend-Informationen über das Dashboard oder über die Option Back-Ends anzeigen.

Auf der Seite Storage Back-End-Details für Astra Data Store sehen Sie die folgenden Informationen:

- Astra Data Store Cluster
  - Durchsatz, IOPS und Latenz
  - Genutzte Kapazität im Vergleich zur Gesamtkapazität
- Für jedes Astra Data Store Cluster Volume
  - Genutzte Kapazität im Vergleich zur Gesamtkapazität
  - Durchsatz

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 Abschnitt Storage Backend, 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

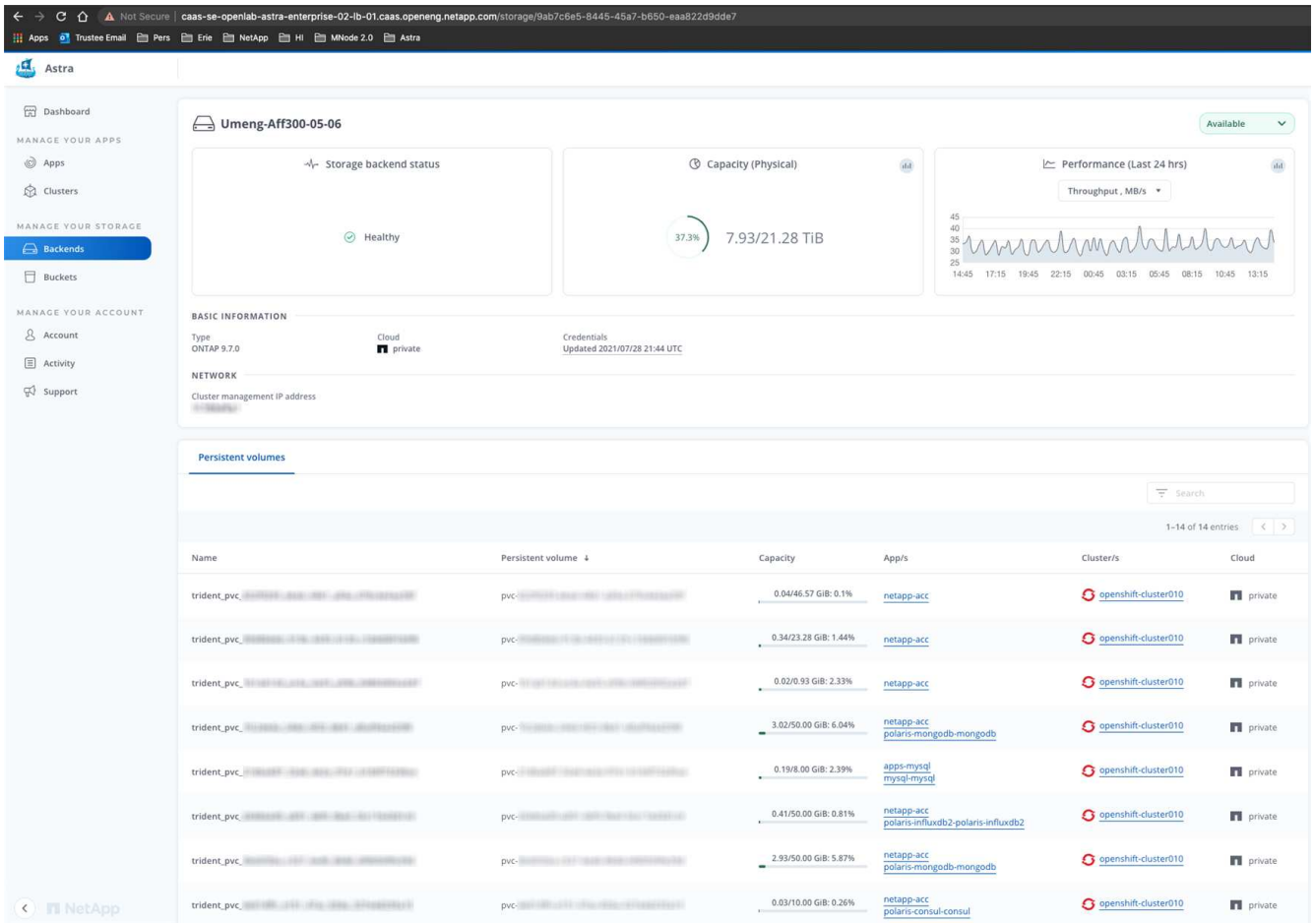
Informationen zum Zustand, Kapazität und Performance des Backend (IOPS-Durchsatz und/oder Latenz)

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.

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.

> Wenn Sie ein Astra Data Store Backend entfernen, darf es nicht vom vCenter erstellt worden sein.

Was Sie benötigen

- Stellen Sie sicher, dass das Storage-Back-End nicht gemanagt wird.
- Stellen Sie sicher, dass im Storage-Backend keine Volumes zum Astra Data Store Cluster zugeordnet 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 aus der Option **Aktionen** die Option **Verwaltung aufheben** 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 aus der Option **Aktionen** die Option **Entfernen**.
   c. Geben Sie „Entfernen“ ein, um die Aktion zu bestätigen.
   d. Wählen Sie **Ja, Speicher-Backend entfernen**.

Aktualisieren einer Astra Data Store Storage-Backend-Lizenz

Sie können die Lizenz für ein Astra Data Store Storage-Backend aktualisieren, um eine größere Implementierung oder erweiterte Funktionen zu unterstützen.

Was Sie benötigen

- Ein implementierbares und gemanagtes Astra Data Store Storage-Back-End
- Lizenzdatei von Astra Data Store (wenden Sie sich an Ihren NetApp Vertriebsmitarbeiter, um eine Lizenz für den Astra Data Store zu erwerben).

Schritte

1. Wählen Sie in der linken Navigationsleiste **Backend** aus.
2. Wählen Sie den Namen eines Storage-Backends aus.
3. Unter **Basisinformationen** können Sie den Lizenztyp anzeigen.

   Wenn Sie den Mauszeiger über die Lizenzinformationen bewegen, wird ein Popup mit weiteren Informationen angezeigt, z. B. zum Ablauf und zu Berechtigungen.

4. Wählen Sie unter **Lizenz** das Bearbeitungssymbol neben dem Lizenznamen aus.
5. Führen Sie auf der Seite **Lizenz aktualisieren** einen der folgenden Schritte aus:

Lizenzstatus	Aktion
Mindestens eine Lizenz wurde dem Astra Data Store hinzugefügt.	Wählen Sie eine Lizenz aus der Liste aus.

Lizenzstatus	Aktion
Dem Astra Data Store wurden keine Lizenzen hinzugefügt.	a. Klicken Sie auf die Schaltfläche **Hinzufügen**. b. Wählen Sie eine Lizenzdatei zum Hochladen aus. c. Wählen Sie **Hinzufügen**, um die Lizenzdatei hochzuladen.

6. Wählen Sie **Aktualisieren**.

Upgrade eines Astra Data Store Storage-Backends

Sie können Ihr Backend mit dem Astra Data Store über das Astra Control Center aktualisieren. Dazu müssen Sie zunächst ein Upgrade-Paket hochladen. Astra Control Center wird dieses Upgrade-Paket verwenden, um den Astra Data Store zu aktualisieren.

Was Sie benötigen

- Ein Managed Astra Data Store Storage-Backend
- Ein hochgeladenes Astra Data Store Upgrade-Paket (siehe "Managen von Softwarepaketen")

Schritte

1. Wählen Sie **Backends**.
2. Wählen Sie aus der Liste ein Astra Data Store Storage Backend aus und wählen Sie das entsprechende Menü in der Spalte **Actions** aus.
3. Wählen Sie **Upgrade**.
4. Wählen Sie eine Upgrade-Version aus der Liste aus.

   Wenn Sie mehrere Upgrade-Pakete in Ihrem Repository haben, die unterschiedliche Versionen sind, können Sie die Dropdown-Liste öffnen, um die gewünschte Version auszuwählen.

5. Wählen Sie **Weiter**.
6. Wählen Sie **Upgrade Starten**.

Ergebnis

Auf der Seite **Backends** wird in der Spalte **Status** ein **Upgrade**-Status angezeigt, bis das Upgrade abgeschlossen ist.

Fügen Sie Nodes zu einem Storage-Back-End-Cluster hinzu

Sie können einem Astra Data Store Cluster Nodes bis zur Anzahl der Nodes hinzufügen, die von dem für Astra Data Store installierten Lizenztyp unterstützt werden.

Was Sie benötigen

- Ein implementiertes und lizenziertes Astra Data Store Storage-Back-End
- Sie haben das Astra Data Store Softwarepaket im Astra Control Center hinzugefügt
- Ein oder mehrere neue Nodes, die dem Cluster hinzugefügt werden müssen

Schritte

1. Wählen Sie in der linken Navigationsleiste **Backend** aus.
2. Wählen Sie den Namen eines Storage-Backends aus.
3. Unter „Basisinformationen“ können Sie die Anzahl der Knoten in diesem Speicher-Backend-Cluster sehen.
4. Wählen Sie unter **Nodes** das Bearbeitungssymbol neben der Anzahl der Knoten aus.
5. Geben Sie auf der Seite **Nodes hinzufügen** Informationen zum neuen Knoten oder Knoten ein:
   a. Weisen Sie jedem Node eine Node-Bezeichnung zu.
   b. Führen Sie einen der folgenden Schritte aus:
      - Wenn Sie möchten, dass Astra Data Store stets die maximal verfügbare Anzahl der Knoten entsprechend Ihrer Lizenz verwenden soll, aktivieren Sie das Kontrollkästchen **immer bis maximal maximal zulässige Knoten verwenden**.
      - Wenn Astra Data Store nicht immer die maximale verfügbare Anzahl an Nodes nutzen soll, wählen Sie die gewünschte Anzahl an Nodes insgesamt aus.
   c. Wenn Sie Astra Data Store mit aktivierten Protection Domains implementiert haben, weisen Sie den neuen Node oder die neuen Nodes den Protection Domains zu.
6. Wählen Sie **Weiter**.
7. Geben Sie für jeden neuen Node die IP-Adresse und Netzwerkinformationen ein. Geben Sie eine einzelne IP-Adresse für einen einzelnen neuen Node oder einen IP-Adressenpool für mehrere neue Nodes ein.

   Wenn Astra Data Store die während der Bereitstellung konfigurierten IP-Adressen verwenden kann, müssen Sie keine IP-Adressinformationen eingeben.

8. Wählen Sie **Weiter**.
9. Überprüfen der Konfiguration für den neuen Node oder die neuen Nodes
10. Wählen Sie **Knoten hinzufügen**.

Entfernen Sie die Nodes aus einem Storage-Back-End-Cluster

Sie können Nodes aus einem Astra Data Store Cluster entfernen. Diese Nodes können einen ordnungsgemäßen Zustand oder einen fehlerhaften Node haben.

Durch Entfernen eines Node aus einem Astra Data Store Cluster werden die Daten auf andere Nodes im Cluster verschoben und der Node wird aus dem Astra Data Store entfernt.

Der Prozess erfordert folgende Bedingungen:

- In den anderen Nodes muss ausreichend freier Speicherplatz vorhanden sein, um die Daten zu empfangen.
- Der Cluster muss 4 oder mehr Nodes vorhanden sein.

Schritte

1. Wählen Sie in der linken Navigationsleiste **Backend** aus.
2. Wählen Sie den Namen eines Storage-Backends aus.
3. Wählen Sie die Registerkarte **Nodes** aus.
4. Wählen Sie im Menü Aktionen die Option **Entfernen**.
5. Bestätigen Sie den Löschvorgang, indem Sie „Entfernen“ eingeben.

6. Wählen Sie **Ja, Knoten entfernen**.

Weitere Informationen

- "Verwenden Sie die Astra Control API"

Überwachen Sie Ihre Infrastruktur mit Cloud Insights und Fluentd Verbindungen

Sie können mehrere optionale Einstellungen konfigurieren, um Ihre Astra Control Center-Erfahrung zu verbessern. Um Ihre gesamte Infrastruktur zu überwachen und Erkenntnisse zu erhalten, verwenden Sie eine Verbindung zu NetApp Cloud Insights. Um Kubernetes-Ereignisse von Systemen zu erfassen, die vom Astra Control Center überwacht werden, 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 im Astra Control Center konfigurieren.

Über die Seite Astra Control Center Storage Back-Ends können Sie auch den Back-End-Durchsatz, IOPS und die Kapazität von Astra Data Store überwachen. Siehe "Managen von Storage-Back-Ends".

Fügen Sie einen Proxy-Server für Verbindungen zu Cloud Insight 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 im Astra Control Center konfigurieren.

> Astra Control Center überprüft nicht die von Ihnen eingegebenen Details für Ihren Proxy-Server. 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 **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 in der Dropdown-Liste **Bearbeiten** aus, 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 Sie Astra Data Store-Cluster auf Astra Control (mit Cloud Insights verbunden) verwalten, wird im Astra Data Store für jeden Astra Data Store-Cluster ein Pod für die Datenerfassungseinheit erstellt. Die Kennzahlen werden vom Astra Data Store an das gepaarte Cloud Insights-System gesendet. Jeder POD benötigt 8 GB

RAM und 2 CPU-Kerne.

> Nach Aktivierung der Cloud Insights-Verbindung können Sie Durchsatzinformationen auf der Seite **Backend** anzeigen sowie von hier aus eine Verbindung zu Cloud Insights herstellen, nachdem Sie ein Speicher-Backend ausgewählt haben. Die Informationen finden Sie auch auf dem **Dashboard** im Clusterbereich, und von dort aus können Sie auch eine Verbindung zu Cloud Insights herstellen.

Was Sie benötigen

- 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

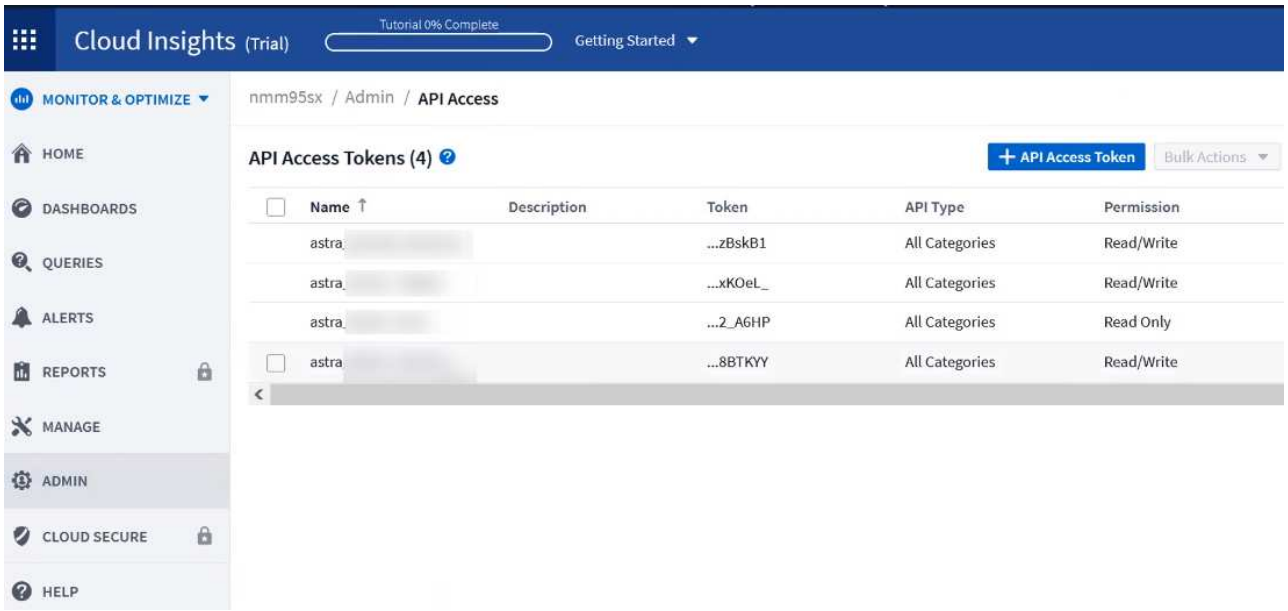
1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Verbinden**, wo es **getrennt** angezeigt wird, um die Verbindung hinzuzufügen.

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. Für die Hauptberechtigungen Lese-/Schreibzugriff auf API-Zugriffstoken wählen Sie: Assets, Datenaufnahme, Log-Ingestion, Acquisition Unit, Und Datenerfassung.

> 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.

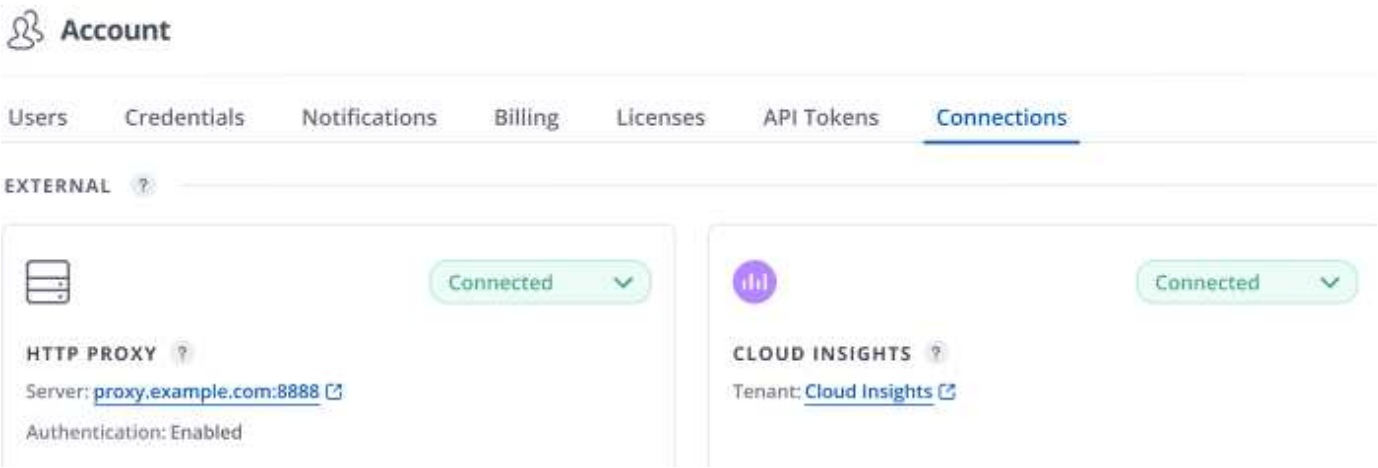
5. Wählen Sie **Verbinden**.

> 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.

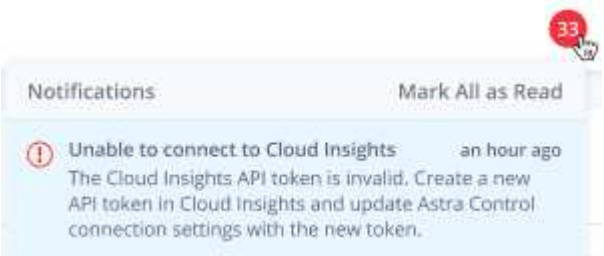
> Um zwischen dem Astra Control Center und den Cloud Insights UIs hin und her zu gehen, stellen Sie sicher, dass Sie bei beiden angemeldet sind.

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.

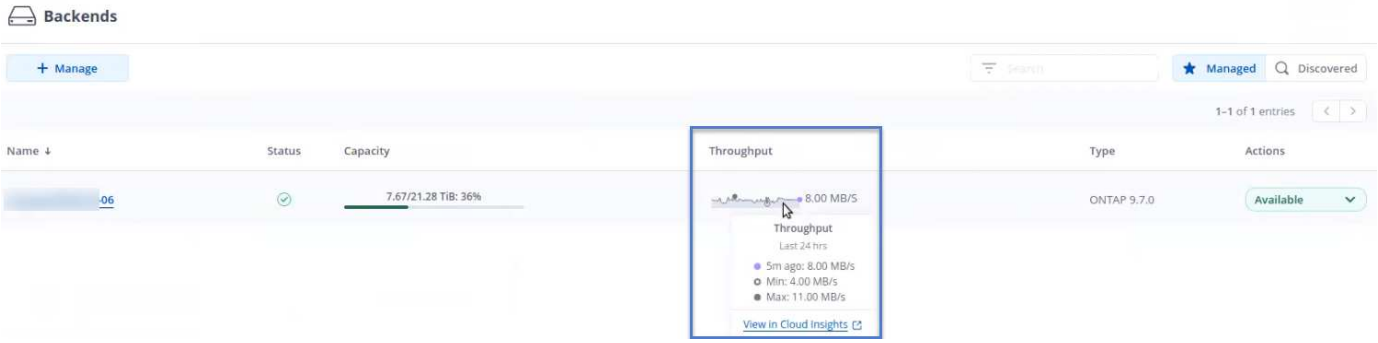


Wenn die Verbindung aus irgendeinem Grund fehlgeschlagen ist, wird im Status **failed** angezeigt. Den Grund für Fehlschlag finden Sie unter **Benachrichtigungen** auf der rechten oberen Seite des UI.



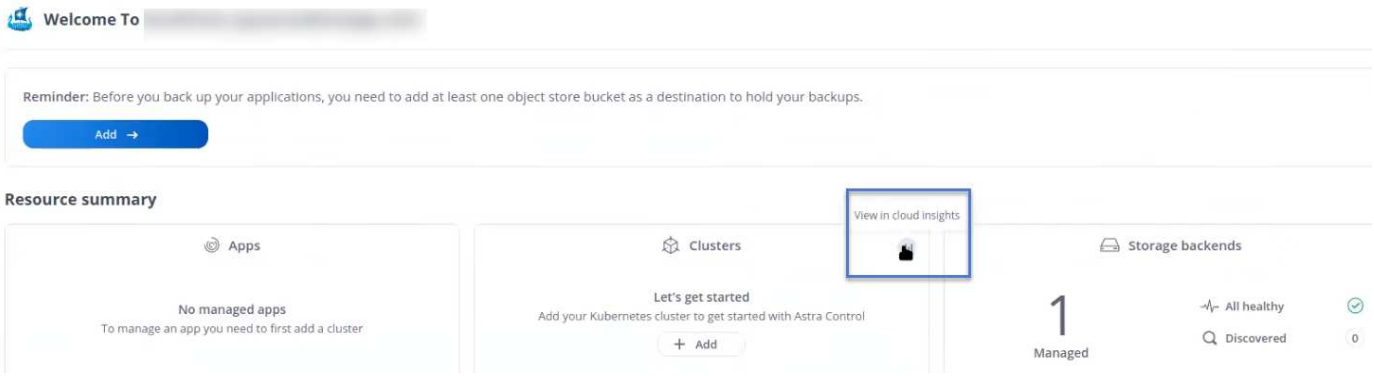
Die gleichen Informationen finden Sie auch unter **Konto** > **Benachrichtigungen**.

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 in der Dropdown-Liste **Bearbeiten** aus, um die Verbindung zu bearbeiten.
4. Bearbeiten Sie die Cloud Insights-Verbindungseinstellungen.
5. Wählen Sie **Speichern**.

Deaktivieren Sie die Cloud Insights-Verbindung

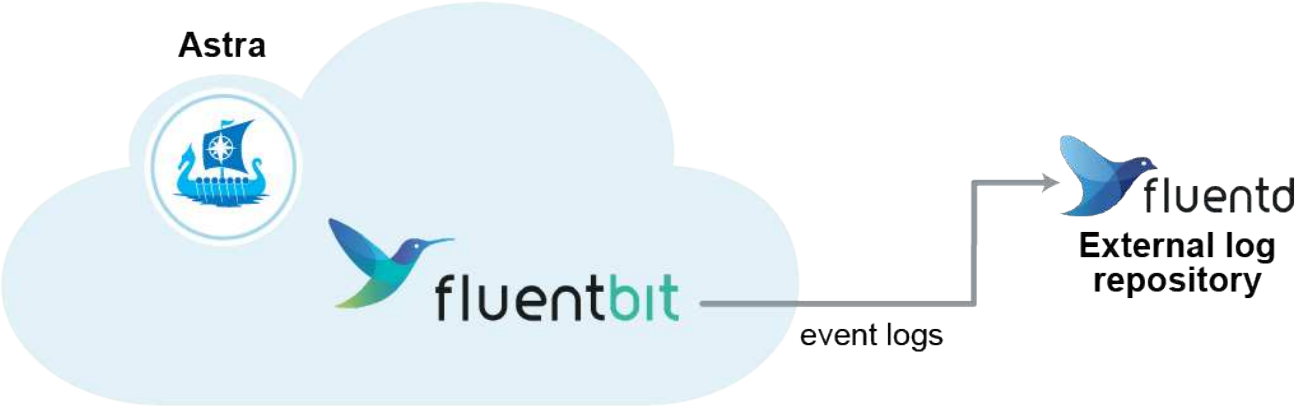
Sie können die Cloud Insights-Verbindung für einen Kubernetes Cluster deaktivieren, der von Astra Control Center gemanagt wird. Wenn Sie die Cloud Insights-Verbindung deaktivieren, werden die bereits auf Cloud Insights hochgeladenen Telemetriedaten nicht gelöscht.

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.

Mit Fluentd verbinden

Sie können Protokolle (Kubernetes-Ereignisse) vom Astra Control Center an Ihren Fluentd Endpunkt senden. Die Fluentd-Verbindung ist standardmäßig deaktiviert.



Nur die Ereignisprotokolle von verwalteten Clustern werden an Fluentd weitergeleitet.

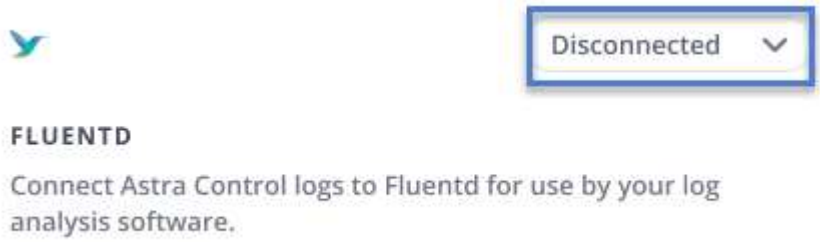
Was Sie benötigen

- 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 in der Dropdown-Liste **Bearbeiten** aus, 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.

- 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. Aktivieren Sie das Kontrollkästchen für die Apps, die Sie nicht mehr verwalten möchten.
3. Wählen Sie im Menü **Aktion** die Option **Entverwalten**.
4. Geben Sie zur Bestätigung „nicht verwalten“ ein.
5. Bestätigen Sie, dass Sie die Verwaltung der Apps aufheben möchten, und wählen Sie dann **Ja, Anwendung verwalten** aus.

Ergebnis

Astra Control Center beendet die Verwaltung der App.

Aufheben des Managements eines Clusters

Entmanagement des Clusters, den Sie nicht mehr über das Astra Control Center managen möchten.

- 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.
- Trident wird nicht vom Cluster deinstalliert. "Lesen Sie, wie Trident deinstalliert wird".

> Bevor Sie das Management des Clusters aufheben, sollten Sie die dem Cluster zugeordnete Applikationen aufheben.

Schritte

1. Wählen Sie in der linken Navigationsleiste **Cluster** aus.
2. Aktivieren Sie das Kontrollkästchen für den Cluster, den Sie nicht mehr im Astra Control Center 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 **removing** und danach wird der Cluster von der Seite **Clusters** entfernt und wird nicht mehr von 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 führen Sie diese Anweisungen aus, um die Komponenten des Astra Control Center in Ihrer Umgebung zu aktualisieren. Mit diesem Verfahren können Sie das Astra Control Center in internetverbundenen oder luftgekapderten Umgebungen aktualisieren.

Was Sie benötigen

- "Bevor Sie mit dem Upgrade beginnen, stellen Sie sicher, dass Ihre Umgebung auch die Mindestanforderungen für die Implementierung des Astra Control Center erfüllt".
- Stellen Sie sicher, dass alle Cluster Operator in einem ordnungsgemäßen Zustand und verfügbar sind.

```
kubectl get clusteroperators
```

- Stellen Sie sicher, dass alle API-Services in einem gesunden Zustand und verfügbar sind.

```
kubectl get apiservices
```

- Melden Sie sich von Ihrem Astra Control Center ab.

Über diese Aufgabe

Der Astra Control Center Upgrade-Prozess führt Sie durch die folgenden grundlegenden Schritte:

- Laden Sie das Astra Control Center Bundle herunter
- Packen Sie das Paket aus und ändern Sie das Verzeichnis
- Fügen Sie die Bilder Ihrer lokalen Registrierung hinzu
- Installieren Sie den aktualisierten Astra Control Center-Operator
- Upgrade Astra Control Center
- Upgrade von Services von Drittanbietern (optional)
- Überprüfen Sie den Systemstatus
- Eindringen für den Lastenausgleich einrichten

Führen Sie den folgenden Befehl während der gesamten Dauer des Upgrades nicht aus, um zu vermeiden, dass alle Astra Control Center Pods gelöscht werden: `kubectl delete -f astra_control_center_operator_deploy.yaml`

Führen Sie Upgrades in einem Wartungsfenster durch, wenn Zeitpläne, Backups und Snapshots nicht ausgeführt werden.

Podman-Befehle können anstelle von Docker-Befehlen verwendet werden, wenn Sie den Podman von Red hat anstelle von Docker Engine verwenden.

Laden Sie das Astra Control Center Bundle herunter

1. Laden Sie das Astra Control Center-Upgrade-Bundle herunter (`astra-control-center-[version].tar.gz`) Von der Support-Website https:mysupport.netapp.com/site/products/all/details/astra-control-center/downloads-tab[NetApp^].
2. (Optional) Überprüfen Sie mit dem folgenden Befehl die Signatur des Pakets:

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

Packen Sie das Paket aus und ändern Sie das Verzeichnis

1. Extrahieren Sie die Bilder:

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

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 Astra-Verzeichnis:

```
cd acc
```

2. Schieben Sie die Paketbilder im Astra Control Center-Bildverzeichnis in Ihre lokale Registrierung. Führen Sie folgende Ersetzungen durch, bevor Sie den Befehl ausführen:
   - ERSETZEN SIE DIE BUNDLE_FILE durch den Namen der Astra Control Bundle-Datei (z. B. `acc.manifest.yaml`).
   - ERSETZEN SIE MY_REGISTRY durch die URL des Docker Repositorys.
   - 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_REGISTRY
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

Podman

1. Melden Sie sich bei Ihrer Registrierung an:

```
podman login [your_registry_path]
```

2. Führen Sie das folgende Skript aus und machen Sie die Substitution <YOUR_REGISTRY> wie in den Kommentaren angegeben:

```
# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
  # Load to local cache
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')

  # Remove path and keep imageName.
  astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')

  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

  # Push to the local repo.
  podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

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, für die eine Authentifizierung erforderlich ist, ersetzen Sie die Standardzeile von `imagePullSecrets: []` Mit folgenden Optionen:

```
imagePullSecrets:
- name: <name_of_secret_with_creds_to_local_registry>
```

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

c. Ändern `[your_registry_path]` Für das `acc-operator-controller-manager` 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
```

```
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
  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: [your_registry_path]/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
        command:
        - /manager
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_UPGRADETIMEOUT
          value: 300m
        image: [your_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

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.astra.
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) (`astra_control_center_min.yaml`) Und ändern Sie die Astra-Version (`astraVersion` Innerhalb von `Spec`) Nummer auf die neueste:

```
kubectl edit acc -n [netapp-acc or custom namespace]
```

> Ihr Registrierungspfad muss mit dem Registrierungspfad übereinstimmen, in dem Sie die Bilder in A verschoben haben Vorheriger Schritt.

2. Fügen Sie die folgenden Zeilen in hinzu `additionalValues` Innerhalb von `Spec` Im Astra Control Center CR:

```
additionalValues:
    nautilus:
      startupProbe:
        periodSeconds: 30
        failureThreshold: 600
```

3. Führen Sie einen der folgenden Schritte aus:
   a. Wenn Sie nicht über Ihren eigenen IngressController oder Ingress verfügen und das Astra Control Center mit seinem Traefik Gateway als Lastausgleichsdienst verwenden und mit diesem Setup fortfahren möchten, geben Sie ein anderes Feld an `ingressType` (Falls noch nicht vorhanden) und auf einstellen `AccTraefik`.

      ```
      ingressType: AccTraefik
      ```

   b. Wenn Sie zur standardmäßigen Ingress-Bereitstellung von Astra Control Center wechseln möchten, stellen Sie Ihr eigenes Einstellungen für den IngressController/Ingress (mit TLS-Terminierung usw.) bereit, öffnen Sie eine Route zum Astra Control Center und stellen Sie sie ein `ingressType` Bis `Generic`.

      ```
      ingressType: Generic
      ```

      Wenn Sie das Feld nicht angeben, wird der Prozess zur allgemeinen Bereitstellung. Wenn die allgemeine Bereitstellung nicht gewünscht ist, fügen Sie das Feld hinzu.

4. (Optional) Stellen Sie sicher, dass die Pods beendet werden und wieder verfügbar sind:

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

5. Warten Sie, bis die Statusbedingungen des Astra angezeigt werden, dass das Upgrade abgeschlossen und bereit ist:

```
kubectl get -o yaml -n [netapp-acc or custom namespace]
astracontrolcenters.astra.netapp.io astra
```

Antwort:

```
conditions:
  - lastTransitionTime: "2021-10-25T18:49:26Z"
    message: Astra is deployed
    reason: Complete
    status: "True"
    type: Ready
  - lastTransitionTime: "2021-10-25T18:49:26Z"
    message: Upgrading succeeded.
    reason: Complete
    status: "False"
    type: Upgrading
```

6. Melden Sie sich erneut an, und überprüfen Sie, ob alle gemanagten Cluster und Apps weiterhin vorhanden und geschützt sind.
7. Wenn der Betreiber den Cert-Manager nicht aktualisiert hat, aktualisieren Sie als nächstes die Dienste von Drittanbietern.

Upgrade von Services von Drittanbietern (optional)

Die Drittanbieter-Services Traefik und Cert-Manager werden während früherer Aktualisierungsschritte nicht aktualisiert. Sie können sie optional mithilfe der hier beschriebenen Vorgehensweise aktualisieren oder vorhandene Servicestversionen beibehalten, wenn es vom System benötigt wird.

- **Traefik**: Standardmäßig verwaltet Astra Control Center den Lebenszyklus der Traefik-Bereitstellung. Einstellung `externalTraefik` Bis `false` (Standard) zeigt an, dass im System keine externe Traefik vorhanden ist und dass Traefik vom Astra Control Center installiert und verwaltet wird. In diesem Fall `externalTraefik` Ist auf festgelegt `false`.

  Wenn Sie hingegen Ihre eigene Traefik-Bereitstellung haben, stellen Sie fest `externalTraefik` Bis `true`. In diesem Fall erhalten Sie die Bereitstellung, und Astra Control Center wird nicht aktualisieren die CRDs, es sei denn `shouldUpgrade` Ist auf festgelegt `true`.

- **Cert-Manager**: Astra Control Center installiert standardmäßig den Cert-Manager (und CRDs), es sei denn, Sie haben es eingestellt `externalCertManager` Bis `true`. Einstellen `shouldUpgrade` Bis `true` Astra Control Center auf die CRDs aktualisieren zu lassen.

Traefik wird aktualisiert, wenn eine der folgenden Bedingungen erfüllt ist:

- Externer Traefik: Falsch
- Externer Traefik: Wahr UND sollte Upgrade: Wahr.

Schritte

1. Bearbeiten Sie das `acc` CR:

```
kubectl edit acc -n [netapp-acc or custom namespace]
```

2. Ändern Sie das `externalTraefik` Feld und das `shouldUpgrade` Feld an `true` Oder `false` Nach

Bedarf.

```
crds:
    externalTraefik: false
    externalCertManager: false
    shouldUpgrade: false
```

Überprüfen Sie den Systemstatus

1. Melden Sie sich beim Astra Control Center an.
2. Vergewissern Sie sich, dass alle gemanagten Cluster und Applikationen weiterhin vorhanden und geschützt sind.

Eindringen für den Lastenausgleich einrichten

Sie können ein Kubernetes Ingress-Objekt einrichten, das den externen Zugriff auf die Services, wie etwa den Lastausgleich in einem Cluster, managt.

- Beim Standard-Upgrade wird die allgemeine Ingress-Bereitstellung verwendet. In diesem Fall müssen Sie außerdem einen Ingress-Controller oder eine Ingress-Ressource einrichten.
- Wenn Sie keinen Ingress-Controller möchten und das beibehalten möchten, was Sie bereits haben, setzen Sie die Einstellung ein `ingressType` Bis `AccTraefik`.

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

Die Schritte unterscheiden sich je nach Art des Ingress-Controllers, den Sie verwenden:

- Nginx-Ingress-Controller
- OpenShift-Eingangs-Controller

Was Sie benötigen

- In der CR-Spezifikation
  - Wenn `crd.externalTraefik` Ist vorhanden, sollte auf festgelegt werden `false` ODER
  - Wenn `crd.externalTraefik` Ist `true`, `crd.shouldUpgrade` Sollte auch so sein `true`.
- Erforderlich "Eingangs-Controller" Sollte bereits eingesetzt werden.
- Der "Eingangsklasse" Entsprechend der Eingangs-Steuerung sollte bereits erstellt werden.
- Sie verwenden Kubernetes-Versionen zwischen und v1.19 und v1.21.

Schritte für Nginx Ingress Controller

1. Verwenden Sie das vorhandene Geheimnis `secure-testing-cert` Oder 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 benutzerdefinierter Name) Namespace für ein überkommenes oder ein neues Schema:

a. Führen Sie für ein deprecated Schema folgende Beispiel aus:

```
apiVersion: extensions/v1beta1
kind: IngressClass
metadata:
  name: ingress-acc
  namespace: [netapp-acc or custom namespace]
  annotations:
    kubernetes.io/ingress.class: nginx
spec:
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - backend:
        serviceName: traefik
        servicePort: 80
        pathType: ImplementationSpecific
```

b. Führen Sie für ein neues Schema das folgende Beispiel aus:

```
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
```

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
```

Überprüfen Sie, ob die Eindringen eingerichtet ist

Sie können den Ingress überprüfen, bevor Sie fortfahren.

1. Stellen Sie sicher, dass Traefik in geändert wurde `clusterIP` Vom Loadbalancer:

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

2. Überprüfen Sie Routen in Traefik:

```
Kubectl get ingressroute ingressroutetls -n [netapp-acc or custom
namespace]
-o yaml | grep "Host("
```

Das Ergebnis sollte leer sein.

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.

Was Sie benötigen

- Verwenden Sie die Benutzeroberfläche von Astra Control Center, um das Management aller zu lösen "Cluster".

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_min.yaml -n netapp-acc
   ```

   Ergebnis:

   ```
   astracontrolcenter.astra.netapp.io "astra" deleted
   ```

2. Löschen Sie den mit dem folgenden Befehl `netapp-acc` Namespace:

   ```
   kubectl delete ns netapp-acc
   ```

   Ergebnis:

   ```
   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"

Automatisierung mit 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.

Zum Einrichten und Managen Ihrer Kubernetes-Applikationen können Sie entweder die Astra-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"

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:

- "**Knowledge Base** (Anmeldung erforderlich)": Suchen Sie nach Artikeln, FAQs oder Break Fix Informationen in Bezug auf Astra Control.
- **Documentation Center**: Dies ist die doc-Site, 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 Definition (CRD) (`astra_control_center_min.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.
   - Nutzen Sie die NetApp Active IQ.

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.

- "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"
- "Hinweis zum Astra Data Store"

Astra Control API-Lizenz

https://docs.netapp.com/us-en/astra-automation/media/astra-api-license.pdf