Nutzen Sie Den Astra Control Service

Astra Control Service

NetApp
July 29, 2024

Inhalt

Nutzen Sie Den Astra Control Service

Melden Sie sich beim Astra Control Service an

Der Zugriff auf Astra Control Service erfolgt über eine SaaS-basierte Benutzeroberfläche über die von Ihnen zu bedienende Benutzeroberfläche https://astra.netapp.io.

Sie können sich mit Single Sign-On über Anmeldedaten aus Ihrem Unternehmensverzeichnis (föderierte Identität) anmelden. Weitere Informationen erhalten Sie im "Hilfe-Center" Und wählen Sie dann **Cloud Central Anmelde-Optionen**.

Bevor Sie beginnen

- "Eine BlueXP Benutzer-ID".
- "Ein neues Astra Control Konto" Oder "Einladung zu einem bestehenden Account".
- Einen unterstützten Webbrowser.

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

Schritte

1. Öffnen Sie einen Webbrowser, und gehen Sie zu https://astra.netapp.io.
2. Melden Sie sich mit Ihren NetApp BlueXP Zugangsdaten an.

Management und Sicherung von Applikationen

Starten Sie das Anwendungsmanagement

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

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

Anforderungen für das Applikationsmanagement

Astra Control verfügt über folgende Anforderungen an das Applikationsmanagement:

- **Lizenzierung**: Um mehr als 10 Namespaces zu verwalten, benötigen Sie ein Astra Control Abonnement.
- **Namesaces**: Apps können mit Astra Control innerhalb eines oder mehrerer spezifizierter Namespaces auf einem einzigen Cluster definiert werden. Eine App kann Ressourcen enthalten, die mehrere Namespaces innerhalb desselben Clusters umfassen. Astra Control unterstützt nicht die Möglichkeit, Applikationen über mehrere Cluster hinweg zu definieren.
- **Speicherklasse**: Wenn Sie eine App installieren, die eine Speicherklasse explizit festgelegt hat und Sie die App klonen müssen, muss das Zielcluster für den Klonvorgang die ursprünglich angegebene Speicherklasse haben. Das Klonen einer Applikation mit einer explizit festgelegten Storage-Klasse auf ein

Cluster ohne dieselbe Storage-Klasse schlägt fehl.

- **Kubernetes-Ressourcen**: Applikationen, die nicht von Astra Control gesammelte Kubernetes-Ressourcen verwenden, verfügen unter Umständen nicht über umfassende Funktionen zum App-Datenmanagement. Astra Control sammelt die folgenden Kubernetes-Ressourcen:

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

Unterstützte Installationsmethoden für Anwendungen

Astra Control unterstützt folgende Installationsmethoden für Anwendungen:

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

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

- **Helm 3**: Wenn Sie Helm zur Installation von Apps verwenden, benötigt Astra Control Helm Version 3. Das Management und Klonen von Apps, die mit Helm 3 installiert sind (oder ein Upgrade von Helm 2 auf Helm 3), 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 oder mehreren Namespaces zugeordnet ist, kann verwaltet werden.

Astra Control verwaltet statusorientierte Applikationen nur dann, wenn sich der Storage auf einer Storage-Klasse befindet, die von Astra Control unterstützt wird. Astra Control Service unterstützt alle Storage-Klassen, die von Astra Control Provisioner oder einem allgemeinen CSI-Treiber unterstützt werden.

- "Erfahren Sie mehr über Speicherklassen für GKE-Cluster"
- "Erfahren Sie mehr über Speicherklassen für AKS-Cluster"
- "Erfahren Sie mehr über Storage-Klassen für AWS Cluster"

Definieren von Apps

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

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

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

Bevor Sie beginnen

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

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

Über diese Aufgabe

- Bevor Sie beginnen, sollten Sie auch verstehen "Verwalten von Standard- und Systemnames".
- Wenn Sie in Astra Control mehrere Namespaces mit Ihren Apps verwenden möchten, sollten Sie dies in Betracht ziehen "Ändern von Benutzerrollen mit Namespace-Einschränkungen" Vor dem Definieren von Apps.
- Anweisungen zum Verwalten von Apps mit der Astra Control API finden Sie im "Astra Automation und API-Informationen".

Optionen für Applikationsmanagement

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

Definition von Ressourcen, die als Applikation gemanagt werden sollen

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

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

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

Erfahren Sie mehr über das Hinzufügen von Ressourcen im Cluster-Umfang zu Ihren Applikationsnamensräumen.

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

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

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

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

Schritte

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

   Apps können mit Astra Control in einem oder mehreren festgelegten Namespaces auf einem einzigen Cluster definiert werden. Eine App kann Ressourcen enthalten, die mehrere Namespaces innerhalb desselben Clusters umfassen. Astra Control unterstützt nicht die Möglichkeit, Applikationen über mehrere Cluster hinweg zu definieren.

5. (Optional) Geben Sie in jedem Namespace ein Etikett für die Kubernetes-Ressourcen ein. Sie können ein einzelnes Etikett oder ein Label-Auswahlkriterium (Abfrage) festlegen.

   Weitere Informationen zu Kubernetes-Labels: "In der offiziellen Kubernetes-Dokumentation finden Sie weitere Informationen".

6. (Optional) Fügen Sie zusätzliche Namespaces für die App hinzu, indem Sie **Namespace hinzufügen** und den Namespace aus der Dropdown-Liste auswählen.
7. (Optional) Geben Sie für alle weiteren Namespaces, die Sie hinzufügen, die Kriterien für eine einzelne Beschriftung oder eine Labelauswahl ein.

8. (Optional) um Ressourcen mit Cluster-Umfang zusätzlich zu den Ressourcen von Astra Control automatisch einzubeziehen, überprüfen Sie **zusätzliche Ressourcen mit Cluster-Umfang** und füllen Sie Folgendes aus:
   a. Wählen Sie **Add include Rule**.
   b. **Gruppe**: Wählen Sie aus der Dropdown-Liste die API-Ressourcengruppe aus.
   c. **Art**: Wählen Sie aus der Dropdown-Liste den Namen des Objektschemas aus.
   d. **Version**: Geben Sie die API-Version ein.
   e. **Label selector**: Optional ein Etikett enthalten, das der Regel hinzugefügt werden soll. Mit diesem Etikett werden nur die Ressourcen abgerufen, die diesem Etikett entsprechen. Wenn Sie kein Etikett bereitstellen, sammelt Astra Control alle Instanzen der für diesen Cluster angegebenen Ressourcenkartart.
   f. Überprüfen Sie die Regel, die auf Ihren Einträgen erstellt wird.
   g. Wählen Sie **Hinzufügen**.

   Sie können die gewünschten Ressourcenregeln mit dem Cluster-Umfang erstellen. Die Regeln werden in der Anwendungsübersicht definieren angezeigt.

9. Wählen Sie **Definieren**.
10. Nachdem Sie **Definieren** ausgewählt haben, wiederholen Sie den Vorgang für andere Apps, je nach Bedarf.

Nachdem Sie die Definition einer App abgeschlossen haben, wird die App in angezeigt `Healthy` Geben Sie in der Liste der Apps auf der Seite Anwendungen an. Sie können sie jetzt klonen und erstellen Backups und Snapshots.

Die gerade hinzugefügte App verfügt möglicherweise über ein Warnsymbol unter der Spalte „geschützt“, das angibt, dass sie nicht gesichert ist und noch keine Backups geplant sind.

Um Details zu einer bestimmten App anzuzeigen, wählen Sie den App-Namen aus.

Um die Ressourcen anzuzeigen, die dieser App hinzugefügt wurden, wählen Sie die Registerkarte **Ressourcen** aus. Wählen Sie in der Spalte „Ressource“ die Nummer nach dem Ressourcennamen aus, oder geben Sie den Ressourcennamen in „Suche“ ein, um die zusätzlichen Ressourcen anzuzeigen, die im Cluster-Umfang enthalten sind.

Definieren Sie einen Namespace, der als App gemanagt werden soll

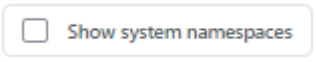
Sie können alle Kubernetes-Ressourcen im Namespace zum Astra Control Management hinzufügen, indem Sie die Ressourcen dieses Namespace als Applikation definieren. Diese Methode ist vorzuziehen, Apps einzeln zu definieren, wenn Sie "Alle Ressourcen in einem bestimmten Namespace managen und schützen sollen" Auf ähnliche Weise und in gemeinsamen Abständen.

Schritte

1. Wählen Sie auf der Seite Cluster einen Cluster aus.
2. Wählen Sie die Registerkarte **Namesaces** aus.
3. Wählen Sie das Menü Aktionen für den Namespace aus, der die Anwendungsressourcen enthält, die Sie verwalten möchten, und wählen Sie **als Anwendung definieren** aus.

Wenn Sie mehrere Anwendungen definieren möchten, wählen Sie in der Namensliste die Schaltfläche **Aktionen** in der linken oberen Ecke aus und wählen Sie **als Anwendung definieren** aus. Damit werden mehrere einzelne Anwendungen in ihren einzelnen Namespaces definiert. Informationen zu Applikationen mit mehreren Namespaces finden Sie unter die als Applikation gemanagt werden sollen.

Aktivieren Sie das Kontrollkästchen **System-Namespaces**, um Systemnamenpaces anzuzeigen, die in der Regel nicht standardmäßig in der App-Verwaltung verwendet werden.



"Weitere Informationen".

Nach Abschluss des Prozesses werden die dem Namespace zugeordneten Anwendungen im angezeigt `Associated applications` Spalte.

[Tech Preview] Definieren Sie eine Applikation mithilfe einer benutzerdefinierten Kubernetes-Ressource

Sie können die Kubernetes-Ressourcen angeben, die Sie mit Astra Control managen möchten, indem Sie sie als Applikation mithilfe einer benutzerdefinierten Ressource definieren. Sie können Ressourcen mit Cluster-Umfang hinzufügen, wenn Sie diese Ressourcen einzeln oder alle Kubernetes-Ressourcen in einem Namespace managen möchten, wenn Sie beispielsweise alle Ressourcen in einem bestimmten Namespace auf ähnliche Weise und in gängigen Intervallen managen und schützen möchten.

Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie (z. B. `astra_mysql_app.yaml`).
2. Benennen Sie die Anwendung in `metadata.name`.
3. Definieren Sie die zu verwaltenden Anwendungsressourcen:

spec.includedClusterScopedResources

Hinzufügen von Ressourcentypen mit Cluster-Umfang zusätzlich zu den von Astra Control automatisch enthaltenen Ressourcen:

- **spec.includedClusterScopedResources**: *(Optional)* Eine Liste der im Cluster enthaltenen Ressourcentypen.
  - **GroupVersionRind**: *(Optional)* eindeutig identifiziert eine Art.
    - **Group**: *(erforderlich, wenn groupVersionRind verwendet wird)* API-Gruppe der einzuschließen Ressource.
    - **Version**: *(erforderlich, wenn groupVersionRind verwendet wird)* API-Version der einzubauenden Ressource.
    - **Kind**: *(erforderlich, wenn groupVersionRind verwendet wird)* Art der Ressource, die einbezogen werden soll.
  - **LabelSelector**: *(Optional)* Eine Label-Abfrage für eine Gruppe von Ressourcen. Es wird verwendet, um nur die Ressourcen abzurufen, die der Bezeichnung entsprechen. Wenn Sie kein Etikett bereitstellen, sammelt Astra Control alle Instanzen der für diesen Cluster angegebenen Ressourcenkartart. Das Ergebnis von matchLabels und matchExpressions ist ANDed.
    - **MatchLabels**: *(Optional)* Eine Karte von {key,value} Paaren. Ein einzelner {key,value} in der matchLabels-Karte entspricht einem Element von matchExpressions, das ein Schlüsselfeld von "key", Operator als "in" und Values-Array enthält, das nur "value" enthält. Die Anforderungen sind ANDed.
    - **MatchExpressions**: *(Optional)* Eine Liste der Anforderungen an die Etikettenauswahl. Die Anforderungen sind ANDed.
      - **Key**: *(erforderlich, wenn matchExpressions verwendet wird)* der Label-Schlüssel, der mit dem Label-Selektor verknüpft ist.
      - **Operator**: *(erforderlich, wenn matchExpressions verwendet wird)* stellt die Beziehung eines Schlüssels zu einem Satz von Werten dar. Gültige Operatoren sind `In`, `NotIn`, `Exists` Und `DoesNotExist`.
      - **Values**: *(erforderlich, wenn matchExpressions verwendet wird)_ein Array von String-Werten. Wenn der Operator ist `In` Oder `NotIn`, Das Wertearray darf _Not* leer sein. Wenn der Operator ist `Exists` Oder `DoesNotExist`, Das Werte-Array muss leer sein.

spec.includedNamespaces

Fügen Sie Namespaces und Ressourcen in diesen Ressourcen in der Anwendung ein:

- **spec.includedNamespaces**: _(required)_definiert den Namespace und optionale Filter für die Ressourcenauswahl.
  - **Namespace**: *(erforderlich)* der Namespace, der die App-Ressourcen enthält, die Sie mit Astra Control managen möchten.
  - **LabelSelector**: *(Optional)* Eine Label-Abfrage für eine Gruppe von Ressourcen. Es wird verwendet, um nur die Ressourcen abzurufen, die der Bezeichnung entsprechen. Wenn Sie kein Etikett bereitstellen, sammelt Astra Control alle Instanzen der für diesen Cluster angegebenen Ressourcenkartart. Das Ergebnis von matchLabels und matchExpressions ist ANDed.
    - **MatchLabels**: *(Optional)* Eine Karte von {key,value} Paaren. Ein einzelner {key,value} in

der matchLabels-Karte entspricht einem Element von matchExpressions, das ein Schlüsselfeld von "key", Operator als "in" und Values-Array enthält, das nur "value" enthält. Die Anforderungen sind ANDed.

- **MatchExpressions**: *(Optional)* Eine Liste der Anforderungen an die Etikettenauswahl. `key` Und `operator` Erforderlich sind. Die Anforderungen sind ANDed.
  - **Key**: *(erforderlich, wenn matchExpressions verwendet wird)* der Label-Schlüssel, der mit dem Label-Selektor verknüpft ist.
  - **Operator**: *(erforderlich, wenn matchExpressions verwendet wird)* stellt die Beziehung eines Schlüssels zu einem Satz von Werten dar. Gültige Operatoren sind `In`, `NotIn`, `Exists` Und `DoesNotExist`.
  - **Values**: *(erforderlich, wenn matchExpressions verwendet wird)* ein Array von String-Werten. Wenn der Operator ist `In` Oder `NotIn`, Das Wertearray darf *Not* leer sein. Wenn der Operator ist `Exists` Oder `DoesNotExist`, Das Werte-Array muss leer sein.

Beispiel YAML:

```
apiVersion: astra.netapp.io/v1
kind: Application
metadata:
  name: astra_mysql_app
spec:
  includedNamespaces:
    - namespace: astra_mysql_app
      labelSelector:
        matchLabels:
          app: nginx
          env: production
        matchExpressions:
          - key: tier
            operator: In
            values:
              - frontend
              - backend
```

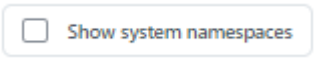
4. Nachdem Sie das ausgefüllt haben `astra_mysql_app.yaml` Datei mit den richtigen Werten, CR anwenden:

```
kubectl apply -f astra_mysql_app.yaml -n astra-connector
```

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.

Sichern von Applikationen durch Snapshots und Backups

Schützen Sie Ihre Applikationen, indem Sie Snapshots und Backups über eine automatisierte Sicherungsrichtlinie oder Ad-hoc-Erstellung erstellen. Sie können die Astra UI oder verwenden "Die Astra Control API" Um Anwendungen zu schützen.

Weitere Informationen zu "Datensicherung in Astra Control".

Sie können die folgenden Aufgaben zum Schutz Ihrer Applikationsdaten ausführen:

- Konfigurieren einer Sicherungsrichtlinie
- Erstellen Sie einen Snapshot
- Erstellen Sie ein Backup
- Backup und Restore für den wirtschaftlichen Betrieb von ontap-nas
- Unveränderliches Backup erstellen
- Anzeigen von Snapshots und Backups
- Snapshots löschen
- Abbrechen von Backups
- Backups löschen

Konfigurieren einer Sicherungsrichtlinie

Eine Sicherungsrichtlinie sichert eine Applikation, indem Snapshots, Backups oder beides nach einem definierten Zeitplan erstellt werden. Sie können Snapshots und Backups stündlich, täglich, wöchentlich und monatlich erstellen. Außerdem können Sie die Anzahl der beizubehaltenden Kopien festlegen. Sie können eine Schutzrichtlinie entweder über die Astra Control Web-UI oder über eine benutzerdefinierte Ressourcendatei (CR) definieren.

Wenn Sie Backups oder Snapshots öfter als einmal pro Stunde benötigen, können Sie dies tun "Erstellen Sie mithilfe der Astra Control REST API Snapshots und Backups".

Wenn Sie eine Schutzrichtlinie definieren, die unveränderliche Backups für WORM-Buckets (Write Once Read Many) erstellt, stellen Sie sicher, dass die Aufbewahrungszeit für die Backups nicht kürzer ist als der für den Bucket konfigurierte Aufbewahrungszeitraum.

Verschieben Sie Backup- und Replikationspläne, um Zeitplanüberschneidungen zu vermeiden. Führen Sie beispielsweise jede Stunde Backups oben in der Stunde durch, und planen Sie die Replikation, um mit einem Offset von 5 Minuten und einem Intervall von 10 Minuten zu beginnen.

Konfigurieren Sie eine Schutzrichtlinie über die Web-Benutzeroberfläche

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. Wählen Sie dazu die Anzahl der Snapshots und Backups aus, die stündlich, täglich, wöchentlich und monatlich erstellt werden sollen.

   Sie können die stündlichen, täglichen, wöchentlichen und monatlichen Zeitpläne gleichzeitig festlegen. Ein Zeitplan wird erst aktiviert, wenn Sie eine Aufbewahrungsstufe festlegen.

   Wenn Sie ein Aufbewahrungsniveau für Backups festlegen, können Sie den Bucket auswählen, auf dem Sie die Backups speichern möchten.

   Im folgenden Beispiel sind vier Sicherungspläne definiert: Stündlich, täglich, wöchentlich und monatlich für Snapshots und Backups.

   [Einen Screenshot einer Beispielkonfigurationsrichtlinie, in der Sie Snapshots und Backups stündlich, täglich, wöchentlich oder monatlich erstellen können.]

5. [**Tech Preview**] Wählen Sie einen Ziel-Bucket für die Backups oder Snapshots aus der Liste der Speicher-Buckets.
6. Wählen Sie **Bewertung**.
7. Wählen Sie **Schutzrichtlinie Festlegen.**

[Tech Preview] Konfigurieren Sie eine Schutzrichtlinie mit einem CR

Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie `astra-control-schedule-cr.yaml`. Aktualisieren Sie die Werte in Klammern <>, um sie an die Anforderungen Ihrer Astra Control-Umgebung, Cluster-Konfiguration und Datensicherung anzupassen:
   - <CR_NAME>: Der Name dieser benutzerdefinierten Ressource; wählen Sie einen eindeutigen und vernünftigen Namen für Ihre Umgebung.
   - <APPLICATION_NAME>: Der Kubernetes-Name der zu Back-up-Applikation.
   - <APPVAULT_NAME>: Der Name des AppVault, in dem der Backup-Inhalt gespeichert werden soll.
   - <BACKUPS_RETAINED>: Die Anzahl der beizubehaltenden Backups. Null bedeutet, dass keine Backups erstellt werden sollen.
   - <SNAPSHOTS_RETAINED>: Die Anzahl der beizubehaltenden Snapshots. Null bedeutet, dass keine Snapshots erstellt werden sollen.
   - <GRANULARITY>: Die Häufigkeit, mit der der Zeitplan ausgeführt werden soll. Mögliche Werte, zusammen mit den erforderlichen zugeordneten Feldern:
     - `hourly` (Erfordert, dass Sie angeben `spec.minute`)
     - `daily` (Erfordert, dass Sie angeben `spec.minute` Und `spec.hour`)
     - `weekly` (Erfordert, dass Sie angeben `spec.minute`, `spec.hour`, und `spec.dayOfWeek`)
     - `monthly` (Erfordert, dass Sie angeben `spec.minute`, `spec.hour`, und

`spec.dayOfMonth`)

- <DAY_OF_MONTH>: *(Optional)* der Tag des Monats (1 - 31), an dem der Zeitplan ausgeführt werden soll. Dieses Feld ist erforderlich, wenn die Granularität auf festgelegt ist `monthly`.
- <DAY_OF_WEEK>: *(Optional)* der Wochentag (0 - 7), an dem der Zeitplan ausgeführt werden soll. Werte von 0 oder 7 zeigen Sonntag an. Dieses Feld ist erforderlich, wenn die Granularität auf festgelegt ist `weekly`.
- <HOUR_OF_DAY>: *(Optional)* die Stunde des Tages (0 - 23), die der Zeitplan ausführen soll. Dieses Feld ist erforderlich, wenn die Granularität auf festgelegt ist `daily`, `weekly`, Oder `monthly`.
- <MINUTE_OF_HOUR>: *(Optional)* die Minute der Stunde (0 - 59), die der Zeitplan ausführen soll. Dieses Feld ist erforderlich, wenn die Granularität auf festgelegt ist `hourly`, `daily`, `weekly`, Oder `monthly`.

```
apiVersion: astra.netapp.io/v1
kind: Schedule
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  backupRetention: "<BACKUPS_RETAINED>"
  snapshotRetention: "<SNAPSHOTS_RETAINED>"
  granularity: <GRANULARITY>
  dayOfMonth: "<DAY_OF_MONTH>"
  dayOfWeek: "<DAY_OF_WEEK>"
  hour: "<HOUR_OF_DAY>"
  minute: "<MINUTE_OF_HOUR>"
```

2. Nachdem Sie das ausgefüllt haben `astra-control-schedule-cr.yaml` Datei mit den richtigen Werten, CR anwenden:

```
kubectl apply -f astra-control-schedule-cr.yaml
```

Ergebnis

Astra Control implementiert die Datensicherungsrichtlinien, indem Snapshots und Backups mithilfe der von Ihnen definierten Zeitplan und Aufbewahrungsrichtlinie erstellt und aufbewahrt werden.

Erstellen Sie einen Snapshot

Sie können jederzeit einen On-Demand-Snapshot erstellen.

Über diese Aufgabe

Astra Control unterstützt die Snapshot-Erstellung mithilfe von Storage-Klassen, die von den folgenden Treibern

unterstützt werden:

- `ontap-nas`
- `ontap-san`
- `ontap-san-economy`

> Wenn Ihre App eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Treiber, Snapshots können nicht erstellt werden. Verwenden Sie eine alternative Storage-Klasse für Snapshots.

Erstellen Sie mithilfe der Web-Benutzeroberfläche einen Snapshot

Schritte

1. Wählen Sie **Anwendungen**.
2. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für die gewünschte App die Option **Snapshot** aus.
3. Passen Sie den Namen des Snapshots an und wählen Sie dann **Weiter**.
4. [**Tech Preview**] Wählen Sie einen Ziel-Bucket für den Snapshot aus der Liste der Speicher-Buckets.
5. Überprüfen Sie die Snapshot-Zusammenfassung und wählen Sie **Snapshot**.

[Tech Preview] Erstellen Sie einen Snapshot mit einem CR

Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie `astra-control-snapshot-cr.yaml`. Aktualisieren Sie die Werte in Klammern <>, um sie an die Astra Control-Umgebung und die Cluster-Konfiguration anzupassen:
   - <CR_NAME>: Der Name dieser benutzerdefinierten Ressource; wählen Sie einen eindeutigen und vernünftigen Namen für Ihre Umgebung.
   - <APPLICATION_NAME>: Der Kubernetes-Name der Applikation, für die ein Snapshot erstellt werden soll.
   - <APPVAULT_NAME>: Der Name des AppVault, in dem der Snapshot-Inhalt gespeichert werden soll.
   - <RECLAIM_POLICY>: *(Optional)* definiert, was mit einem Snapshot passiert, wenn der Snapshot CR gelöscht wird. Gültige Optionen:
     - `Retain`
     - `Delete` (Standard)

     ```
     apiVersion: astra.netapp.io/v1
     kind: Snapshot
     metadata:
       namespace: astra-connector
       name: <CR_NAME>
     spec:
       applicationRef: <APPLICATION_NAME>
       appVaultRef: <APPVAULT_NAME>
       reclaimPolicy: <RECLAIM_POLICY>
     ```

2. Nachdem Sie das ausgefüllt haben `astra-control-snapshot-cr.yaml` Datei mit den richtigen Werten, CR anwenden:

   ```
   kubectl apply -f astra-control-snapshot-cr.yaml
   ```

Ergebnis

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

Erstellen Sie ein Backup

Sie können eine App auch jederzeit sichern.

Achten Sie darauf, wie Speicherplatz verarbeitet wird, wenn Sie eine Applikation sichern, die auf Azure NetApp Files Storage gehostet wird. Siehe "Applikations-Backups" Finden Sie weitere Informationen.

Astra Control unterstützt die Backup-Erstellung mithilfe von Storage-Klassen, die von den folgenden Treibern unterstützt werden:

- `ontap-nas`
- `ontap-nas-economy`
- `ontap-san`
- `ontap-san-economy`

Über diese Aufgabe

Buckets in Astra Control berichten nicht über die verfügbare Kapazität. Bevor Sie von Astra Control gemanagte Applikationen sichern oder klonen, überprüfen Sie Bucket-Informationen im entsprechenden Storage-Managementsystem.

Wenn Ihre App eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Fahrer, müssen Sie Aktivieren Sie Backup und Restore Funktionalität. Stellen Sie sicher, dass Sie einen definiert haben `backendType` Parameter in im "Kubernetes Storage-Objekt" Mit einem Wert von `ontap-nas-economy` Bevor Sie Schutzmaßnahmen durchführen.

Erstellen Sie mithilfe der Web-Benutzeroberfläche ein Backup

Schritte

1. Wählen Sie **Anwendungen**.
2. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für die gewünschte App die Option **Sichern** aus.
3. Passen Sie den Namen des Backups an.
4. Wählen Sie aus, ob die Anwendung aus einem vorhandenen Snapshot gesichert werden soll. Wenn Sie diese Option auswählen, können Sie aus einer Liste vorhandener Snapshots auswählen.
5. [**Tech Preview**] Wählen Sie einen Ziel-Bucket für das Backup aus der Liste der Speicher-Buckets.
6. Wählen Sie **Weiter**.
7. Überprüfen Sie die Backup-Zusammenfassung und wählen Sie **Backup**.

[Tech Preview] Erstellen Sie ein Backup mit einem CR

Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie `astra-control-backup-cr.yaml`. Aktualisieren Sie die Werte in Klammern <>, um sie an die Astra Control-Umgebung und die Cluster-Konfiguration anzupassen:
   - <CR_NAME>: Der Name dieser benutzerdefinierten Ressource; wählen Sie einen eindeutigen und vernünftigen Namen für Ihre Umgebung.
   - <APPLICATION_NAME>: Der Kubernetes-Name der zu Back-up-Applikation.
   - <APPVAULT_NAME>: Der Name des AppVault, in dem der Backup-Inhalt gespeichert werden soll.

   ```
   apiVersion: astra.netapp.io/v1
   kind: Backup
   metadata:
     namespace: astra-connector
     name: <CR_NAME>
   spec:
     applicationRef: <APPLICATION_NAME>
     appVaultRef: <APPVAULT_NAME>
   ```

2. Nachdem Sie das ausgefüllt haben `astra-control-backup-cr.yaml` Datei mit den richtigen Werten, CR anwenden:

   ```
   kubectl apply -f astra-control-backup-cr.yaml
   ```

Ergebnis

Astra Control erstellt ein Backup der App.

- Wenn Ihr Netzwerk ausfällt oder ungewöhnlich langsam ist, kann es zu einer Zeit für einen Backup-Vorgang kommen. Dies führt zum Fehlschlagen der Datensicherung.
- Wenn Sie eine laufende Sicherung abbrechen müssen, befolgen Sie die Anweisungen unter Abbrechen von Backups. Um das Backup zu löschen, warten Sie, bis es abgeschlossen ist, und befolgen Sie die Anweisungen unter Backups löschen.
- Nach einer Datensicherungsoperation (Klonen, Backup, Restore) und einer anschließenden Anpassung des persistenten Volumes beträgt die Verzögerung bis zu zwanzig Minuten, bevor die neue Volume-Größe in der UI angezeigt wird. Der Datensicherungsvorgang ist innerhalb von Minuten erfolgreich und Sie können mit der Management Software für das Storage-Backend die Änderung der Volume-Größe bestätigen.

Backup und Restore für den wirtschaftlichen Betrieb von ontap-nas

Astra Control Provisioner bietet Backup- und Restore-Funktionen für Storage-Back-Ends, die das verwenden `ontap-nas-economy` Storage-Klasse.

Bevor Sie beginnen

- Astra Control Provisioner oder Astra Trident ist aktiviert.
- Sie haben eine Anwendung in Astra Control definiert. Diese Anwendung verfügt nur über begrenzte Schutzfunktionen, bis Sie diesen Vorgang abgeschlossen haben.
- Das ist schon `ontap-nas-economy` Ausgewählt als Standard-Storage-Klasse für Ihr Storage-Back-End.

Erweitern Sie für Konfigurationsschritte

1. Gehen Sie auf dem ONTAP Storage Back-End folgendermaßen vor:

   a. Finden Sie die SVM, die den hostet `ontap-nas-economy`-Basierte Volumen der Anwendung.

   b. Melden Sie sich bei einem Terminal an, das mit ONTAP verbunden ist, wo die Volumes erstellt werden.

   c. Snapshot-Verzeichnis für SVM ausblenden:

   > Diese Änderung wirkt sich auf die gesamte SVM aus. Auf das verborgene Verzeichnis kann weiterhin zugegriffen werden.

   ```
   nfs modify -vserver <svm name> -v3-hide-snapshot enabled
   ```

   +

   > Vergewissern Sie sich, dass das Snapshot-Verzeichnis auf dem ONTAP-Speicher-Back-End verborgen ist. Das Ausblenden dieses Verzeichnisses kann zu einem Verlust des Zugriffs auf Ihre Anwendung führen, insbesondere wenn es NFSv3 verwendet.

2. Gehen Sie in Astra Control Provisioner oder Astra Trident wie folgt vor:

   a. Aktivieren Sie das Snapshot-Verzeichnis für jedes PV, das auf ontap-nas-Economy basiert und der Applikation zugeordnet ist:

   ```
   tridentctl update volume <pv name> --snapshot-dir=true --pool
   -level=true -n trident
   ```

   b. Vergewissern Sie sich, dass das Snapshot-Verzeichnis für jedes zugeordnete PV aktiviert wurde:

   ```
   tridentctl get volume <pv name> -n trident -o yaml | grep
   snapshotDir
   ```

   Antwort:

   ```
   snapshotDirectory: "true"
   ```

3. Aktualisieren Sie in Astra Control die Applikation nach Aktivierung aller zugehörigen Snapshot-Verzeichnisse, damit Astra Control den geänderten Wert erkennt.

Ergebnis

Die Applikation ist bereit für Backups und Restores mit Astra Control. Jede PVC kann auch von anderen Anwendungen für Backups und Wiederherstellungen verwendet werden.

Unveränderliches Backup erstellen

Ein unveränderliches Backup kann nicht geändert, gelöscht oder überschrieben werden, solange die Aufbewahrungsrichtlinie auf dem Bucket, der das Backup speichert, dies verbietet. Erstellen Sie unveränderliche Backups, indem Sie Applikationen in Buckets sichern, für die eine Aufbewahrungsrichtlinie konfiguriert ist. Siehe "Datensicherung" Finden Sie wichtige Informationen zum Arbeiten mit unveränderlichen Backups.

Bevor Sie beginnen

Sie müssen den Ziel-Bucket mit einer Aufbewahrungsrichtlinie konfigurieren. Je nachdem, welchen Storage-Anbieter Sie verwenden, hängt die Vorgehensweise davon ab. Weitere Informationen finden Sie in der Dokumentation des Speicheranbieters:

- **Amazon Web Services**: "Aktivieren Sie S3 Object Lock beim Erstellen des Buckets und legen Sie den Standardaufbewahrungsmodus „Governance“ mit einer Standardaufbewahrungszeit fest".
- **Google Cloud**: "Konfigurieren Sie einen Bucket mit einer Aufbewahrungsrichtlinie und geben Sie einen Aufbewahrungszeitraum an".
- **Microsoft Azure**: "Konfigurieren Sie einen Blob-Storage-Bucket mit einer zeitbasierten Aufbewahrungsrichtlinie im Umfang von Containern".
- **NetApp StorageGRID**: "Aktivieren Sie S3 Object Lock beim Erstellen des Buckets und legen Sie den Standardaufbewahrungsmodus „Compliance“ mit einer Standardaufbewahrungsdauer fest".

> Buckets in Astra Control berichten nicht über die verfügbare Kapazität. Bevor Sie von Astra Control gemanagte Applikationen sichern oder klonen, überprüfen Sie Bucket-Informationen im entsprechenden Storage-Managementsystem.

> Wenn Ihre App eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Treiber, stellen Sie sicher, dass Sie einen definiert haben `backendType` Parameter in im "Kubernetes Storage-Objekt" Mit einem Wert von `ontap-nas-economy` Bevor Sie Schutzmaßnahmen durchführen.

Schritte

1. Wählen Sie **Anwendungen**.
2. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für die gewünschte App die Option **Sichern** aus.
3. Passen Sie den Namen des Backups an.
4. Wählen Sie aus, ob die Anwendung aus einem vorhandenen Snapshot gesichert werden soll. Wenn Sie diese Option auswählen, können Sie aus einer Liste vorhandener Snapshots auswählen.
5. Wählen Sie aus der Liste der Storage-Buckets einen Ziel-Bucket für das Backup aus. Ein WORM-Bucket (Write Once Read Many) wird neben dem Bucket-Namen mit dem Status „gesperrt“ angezeigt.

   > Wenn es sich bei dem Bucket um einen nicht unterstützten Typ handelt, wird dies angezeigt, wenn Sie den Mauszeiger über den Bucket bewegen oder ihn auswählen.

6. Wählen Sie **Weiter**.
7. Überprüfen Sie die Backup-Zusammenfassung und wählen Sie **Backup**.

Ergebnis

Astra Control erstellt eine unveränderliche Sicherung der App.

- Wenn Ihr Netzwerk ausfällt oder ungewöhnlich langsam ist, kann es zu einer Zeit für einen Backup-Vorgang kommen. Dies führt zum Fehlschlagen der Datensicherung.
- Wenn Sie versuchen, zwei unveränderliche Backups derselben App gleichzeitig im selben Bucket zu erstellen, verhindert Astra Control, dass das zweite Backup gestartet wird. Warten Sie, bis die erste Sicherung abgeschlossen ist, bevor Sie eine andere starten.
- Sie können ein auslaufendes unveränderliches Backup nicht abbrechen.
- Nach einer Datensicherungsoperation (Klonen, Backup, Restore) und einer anschließenden Anpassung des persistenten Volumes beträgt die Verzögerung bis zu zwanzig Minuten, bevor die neue Volume-Größe in der UI angezeigt wird. Der Datensicherungsvorgang ist innerhalb von Minuten erfolgreich und Sie können mit der Management Software für das Storage-Backend die Änderung der Volume-Größe bestätigen.

Anzeigen von Snapshots und Backups

Sie können die Snapshots und Backups einer Anwendung auf der Registerkarte Datenschutz anzeigen.

Ein unveränderliches Backup wird neben dem verwendeten Bucket mit dem Status „gesperrt“ angezeigt.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie **Datenschutz**.

   Die Snapshots werden standardmäßig angezeigt.
3. Wählen Sie **Backups** aus, um auf die Liste der Backups zu verweisen.

Snapshots löschen

Löschen Sie die geplanten oder On-Demand Snapshots, die Sie nicht mehr benötigen.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie **Datenschutz**.
3. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für den gewünschten Snapshot die Option **Snapshot löschen** aus.
4. Geben Sie das Wort „Löschen“ ein, um das Löschen zu bestätigen und wählen Sie dann **Ja, Snapshot löschen** aus.

Ergebnis

Astra Control löscht den Snapshot.

Abbrechen von Backups

Sie können ein gerade einlaufenden Backup abbrechen.

Um ein Backup abzubrechen, muss sich das Backup befinden `Running` Bundesland. Sie können ein Backup, das sich in befindet, nicht abbrechen `Pending` Bundesland.

Sie können ein auslaufendes unveränderliches Backup nicht abbrechen.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie **Datenschutz**.
3. Wählen Sie **Backups**.
4. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für das gewünschte Backup die Option **Abbrechen** aus.
5. Geben Sie das Wort „Abbrechen“ ein, um den Vorgang zu bestätigen, und wählen Sie dann **Ja, Sicherung abbrechen** aus.

Backups löschen

Löschen Sie die geplanten oder On-Demand-Backups, die Sie nicht mehr benötigen.

Wenn Sie eine laufende Sicherung abbrechen müssen, befolgen Sie die Anweisungen unter Abbrechen von Backups. Um das Backup zu löschen, warten Sie, bis es abgeschlossen ist, und befolgen Sie diese Anweisungen.

Sie können ein unveränderliches Backup nicht vor Ablauf der Aufbewahrungsfrist löschen.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie **Datenschutz**.
3. Wählen Sie **Backups**.
4. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für das gewünschte Backup die Option **Backup löschen** aus.
5. Geben Sie das Wort „Löschen“ ein, um das Löschen zu bestätigen und wählen Sie dann **Ja, Sicherung löschen**.

Ergebnis

Astra Control löscht das Backup.

[Tech Preview] Schützen Sie einen gesamten Cluster

Sie können ein geplantes, automatisches Backup von beliebigen oder allen nicht gemanagten Namespaces in einem Cluster erstellen. Diese Workflows werden von NetApp als Kubernetes-Servicekonto, als Rollenbindung und als cron-Job bereitgestellt, orchestriert mit einem Python Skript.

So funktioniert es

Wenn Sie den vollständigen Cluster-Backup-Workflow konfigurieren und installieren, wird ein Cron-Job regelmäßig ausgeführt und schützt alle noch nicht verwalteten Namespaces. Dabei werden automatisch Schutzrichtlinien basierend auf Zeitplänen erstellt, die Sie während der Installation auswählen.

Wenn Sie nicht jeden nicht verwalteten Namespace auf dem Cluster mit dem vollständigen Cluster-Backup-

Workflow schützen möchten, können Sie stattdessen den labelbasierten Backup-Workflow verwenden. Der labelbasierte Backup-Workflow verwendet auch eine Cron-Aufgabe, aber anstatt alle nicht verwalteten Namespaces zu schützen, identifiziert er Namespaces durch von Ihnen zur Verfügung gestellt Labels, um optional die Namespaces auf Basis von Bronze-, Silber- oder Gold-Backup-Richtlinien zu schützen.

Wenn ein neuer Namespace erstellt wird, der in den Umfang des von Ihnen gewählten Workflows fällt, wird er automatisch und ohne Administratoraktionen geschützt. Diese Workflows werden auf Cluster-Basis implementiert. Je nach Cluster-Bedeutung können unterschiedliche Cluster einen der beiden Workflows mit individuellen Sicherungsstufen nutzen.

Beispiel: Vollständige Cluster-Sicherung

Wenn Sie beispielsweise den vollständigen Cluster-Backup-Workflow konfigurieren und installieren, werden alle Applikationen in einem Namespace regelmäßig und ohne weiteren Aufwand durch den Administrator gemanagt und geschützt. Der Namespace muss bei der Installation des Workflows nicht vorhanden sein; wenn ein Namespace in der Zukunft hinzugefügt wird, wird er geschützt.

Beispiel: Label-basierter Schutz

Für eine größere Granularität können Sie den labelbasierten Workflow verwenden. Sie können beispielsweise diesen Workflow installieren und Ihren Benutzern mitteilen, je nach Schutzstufe eine von mehreren Labels auf alle Namespaces anzuwenden, die sie schützen möchten. Auf diese Weise können Benutzer den Namespace mit einem dieser Labels erstellen, ohne dass sie einen Administrator benachrichtigen müssen. Der neue Namespace und alle darin Apps werden automatisch geschützt.

Erstellen Sie ein geplantes Backup aller Namespaces

Sie können mithilfe des vollständigen Cluster-Backup-Workflows ein geplantes Backup aller Namespaces auf einem Cluster erstellen.

Schritte

1. Laden Sie die folgenden Dateien auf einen Computer herunter, der über Netzwerkzugriff auf den Cluster verfügt:
   - "Components.yaml CRD-Datei"
   - "protectCluster.py Python-Skript"
2. So konfigurieren und installieren Sie das Toolkit: "Befolgen Sie die im Lieferumfang enthaltenen Anweisungen".

Erstellen Sie ein geplantes Backup bestimmter Namespaces

Sie können mithilfe des labelbasierten Backup-Workflows ein geplantes Backup bestimmter Namespaces anhand ihrer Labels erstellen.

Schritte

1. Laden Sie die folgenden Dateien auf einen Computer herunter, der über Netzwerkzugriff auf den Cluster verfügt:
   - "Components.yaml CRD-Datei"
   - "protectCluster.py Python-Skript"
2. So konfigurieren und installieren Sie das Toolkit: "Befolgen Sie die im Lieferumfang enthaltenen Anweisungen".

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.

Wenn Sie einem Ausführungs-Hook einen Namespace-Filter hinzufügen, der nach einer Wiederherstellung oder einem Klonvorgang ausgeführt wird, und die Wiederherstellungs- oder Klonquelle und das Ziel in verschiedenen Namespaces liegen, wird der Namespace-Filter nur auf den Ziel-Namespace angewendet.

Bevor Sie beginnen

- **Schützen Sie Ihre Anwendungen zuerst**: Es wird dringend empfohlen, dass Sie einen Snapshot oder ein Backup Ihrer Anwendung vor der Wiederherstellung machen. Auf diese Weise können Sie aus dem Snapshot oder Backup klonen, wenn die Wiederherstellung nicht erfolgreich war.
- **Zieldatenträger prüfen**: Wenn Sie eine andere Speicherklasse wiederherstellen, stellen Sie sicher, dass die Speicherklasse den gleichen persistenten Zugriffsmodus für Volumes verwendet (z. B. ReadWriteMany). Der Wiederherstellungsvorgang schlägt fehl, wenn der Zugriffsmodus des Ziel-persistenten Volumes anders ist. Wenn das persistente Quell-Volume beispielsweise den RWX-Zugriffsmodus verwendet, wählen Sie eine Ziel-Storage-Klasse aus, die RWX nicht bereitstellen kann, wie z. B. Azure Managed Disks, AWS EBS, Google Persistent Disk oder `ontap-san`Wird dazu führen, dass der Wiederherstellungsvorgang fehlschlägt. Weitere Informationen zu den Zugriffsmodi für persistente Volumes finden Sie im "Kubernetes" Dokumentation.
- **Planung des Platzbedarfs**: Wenn Sie eine in-Place-Wiederherstellung einer Applikation durchführen, die NetApp ONTAP Storage nutzt, kann sich der von der wiederhergestellten Applikation genutzte Speicherplatz verdoppeln. Nachdem Sie eine in-Place-Wiederherstellung durchgeführt haben, entfernen Sie alle unerwünschten Snapshots aus der wiederhergestellten Applikation, um Speicherplatz freizugeben.
- **Unterstützte Storage Class Treiber**: Astra Control unterstützt die Wiederherstellung von Backups mit Speicherklassen, die von den folgenden Treibern unterstützt werden:
  - `ontap-nas`
  - `ontap-nas-economy`
  - `ontap-san`
  - `ontap-san-economy`
- **(nur ontap-nas-Economy-Treiber) Backups und Wiederherstellungen**: Vor dem Backup oder der Wiederherstellung einer App, die eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Überprüfen Sie, ob der "Das snapshot Verzeichnis auf dem ONTAP Storage-Backend ist verborgen". Das Ausblenden dieses Verzeichnisses kann zu einem Verlust des Zugriffs auf Ihre Anwendung führen, insbesondere wenn es NFSv3 verwendet.

Die Durchführung einer in-Place-Wiederherstellung in einer Anwendung, in der Ressourcen mit einer anderen Anwendung geteilt werden, kann unbeabsichtigte Ergebnisse haben. Alle Ressourcen, die von den Applikationen gemeinsam genutzt werden, werden ersetzt, wenn eine in-Place-Wiederherstellung für eine der Applikationen durchgeführt wird.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie im Menü Optionen in der Spalte Aktionen die Option **Wiederherstellen** aus.
3. Wählen Sie den Wiederherstellungstyp aus:
   - **Wiederherstellen auf ursprünglichen Namespaces**: Verwenden Sie dieses Verfahren, um die App an Ort und Stelle auf dem ursprünglichen Cluster wiederherzustellen.
     i. Wählen Sie den Snapshot oder das Backup aus, mit dem die App direkt wiederhergestellt werden soll. Dadurch wird die App auf eine frühere Version von selbst zurückgesetzt.
     ii. Wählen Sie **Weiter**.

     > Wenn Sie in einem zuvor gelöschten Namespace wiederherstellen, wird im Rahmen des Wiederherstellungsprozesses ein neuer Namespace mit demselben Namen erstellt. Alle Benutzer, die über Berechtigungen zum Verwalten von Apps im zuvor gelöschten Namespace verfügen, müssen die Rechte für den neu erstellten Namespace manuell wiederherstellen.

   - **Wiederherstellen auf neuen Namespaces**: Verwenden Sie dieses Verfahren, um die App auf einem anderen Cluster oder mit verschiedenen Namespaces von der Quelle wiederherzustellen. Mit diesem Verfahren können Sie auch eine App zu einer anderen Storage-Klasse migrieren.
     i. Geben Sie den Namen für die wiederhergestellte App an.
     ii. Wählen Sie das Ziel-Cluster für die Anwendung aus, die Sie wiederherstellen möchten.
     iii. Geben Sie für jeden mit der App verknüpften Quell-Namespace einen Ziel-Namespace ein.

     > Astra Control erstellt als Teil dieser Wiederherstellungsoption neue Ziel-Namespaces. Die angegebenen Ziel-Namespaces dürfen nicht bereits im Ziel-Cluster vorhanden sein.

     iv. Wählen Sie **Weiter**.
     v. Wählen Sie den Snapshot oder das Backup aus, mit dem die App wiederhergestellt werden soll.
     vi. Wählen Sie **Weiter**.
     vii. Folgenden Optionen wählbar:
       - **Wiederherstellung unter Verwendung der ursprünglichen Speicherklassen**: Die Anwendung verwendet die ursprünglich zugeordnete Speicherklasse, es sei denn, sie existiert nicht auf dem Zielcluster. In diesem Fall wird die Standard-Storage-Klasse für das Cluster verwendet.
       - **Wiederherstellen mit einer anderen Storage-Klasse**: Wählen Sie eine Storage-Klasse aus, die auf dem Ziel-Cluster vorhanden ist. Alle Applikations-Volumes, unabhängig von den ursprünglich zugewiesenen Storage-Klassen, werden im Rahmen der Wiederherstellung in diese andere Storage-Klasse migriert.

     viii. Wählen Sie **Weiter**.
4. Wählen Sie die Ressourcen aus, die gefiltert werden sollen:
   - **Alle Ressourcen wiederherstellen**: Alle mit der ursprünglichen App verknüpften Ressourcen wiederherstellen.
   - **Ressourcen filtern**: Geben Sie Regeln an, um einen Untersatz der ursprünglichen Anwendungsressourcen wiederherzustellen:
     i. Wählen Sie diese Option, um Ressourcen aus der wiederhergestellten Anwendung einzuschließen

oder auszuschließen.

ii. Wählen Sie entweder **Include rule** oder **Add exclude rule** aus und konfigurieren Sie die Regel, um die richtigen Ressourcen während der Anwendungswiederherstellung zu filtern. Sie können eine Regel bearbeiten oder entfernen und eine Regel erneut erstellen, bis die Konfiguration korrekt ist.

Weitere Informationen zum Konfigurieren von Einschließen- und Ausschlussregeln finden Sie unter Filtern Sie Ressourcen während einer Anwendungswiederherstellung.

5. Wählen Sie **Weiter**.
6. Lesen Sie die Details zur Wiederherstellungsaktion sorgfältig durch, geben Sie „Restore“ ein (falls Sie dazu aufgefordert werden), und wählen Sie **Restore**.

[Tech Preview] Wiederherstellen von Backups mithilfe einer benutzerdefinierten Ressource (CR)

Sie können Daten aus einem Backup mithilfe einer benutzerdefinierten Ressourcendatei (CR) entweder in einem anderen Namespace oder im ursprünglichen QuellNamespace wiederherstellen.

Mit einem CR-System aus der Sicherung wiederherstellen

Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie `astra-control-backup-restore-cr.yaml`. Aktualisieren Sie die Werte in Klammern <>, um sie an die Astra Control-Umgebung und die Cluster-Konfiguration anzupassen:
   - <CR_NAME>: Der Name dieser CR-Operation; wählen Sie einen vernünftigen Namen für Ihre Umgebung.
   - <APPVAULT_NAME>: Der Name des AppVault, in dem der Backup-Inhalt gespeichert ist.
   - <BACKUP_PATH>: Der Pfad innerhalb von AppVault, wo die Backup-Inhalte gespeichert werden. Beispiel:

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE>: Der Quell-Namespace des Wiederherstellungsvorgangs.
   - <DESTINATION_NAMESPACE>: Der Ziel-Namespace des Wiederherstellungsvorgangs.

     ```
     apiVersion: astra.netapp.io/v1
     kind: BackupRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appVaultRef: <APPVAULT_NAME>
       appArchivePath: <BACKUP_PATH>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

Ungelöste Direktive in <stdin> - include::../_include/selective-Restore-cr.adoc[]

1. Nachdem Sie das ausgefüllt haben `astra-control-backup-restore-cr.yaml` Datei mit den richtigen Werten, CR anwenden:

   ```
   kubectl apply -f astra-control-backup-restore-cr.yaml
   ```

Wiederherstellung aus dem Backup in den ursprünglichen Namespace mit einem CR

Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie `astra-control-backup-ipr-cr.yaml`. Aktualisieren Sie die Werte in Klammern <>, um sie an die Astra Control-Umgebung und die Cluster-Konfiguration anzupassen:
   - <CR_NAME>: Der Name dieser CR-Operation; wählen Sie einen vernünftigen Namen für Ihre Umgebung.

- <APPVAULT_NAME>: Der Name des AppVault, in dem der Backup-Inhalt gespeichert ist.
- <BACKUP_PATH>: Der Pfad innerhalb von AppVault, wo die Backup-Inhalte gespeichert werden. Beispiel:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
20231213023800_94347756-9d9b-401d-a0c3
```

```
apiVersion: astra.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appVaultRef: <APPVAULT_NAME>
  appArchivePath: <BACKUP_PATH>
```

Ungelöste Direktive in <stdin> - include::../_include/selective-Restore-cr.adoc[]

1. Nachdem Sie das ausgefüllt haben `astra-control-backup-ipr-cr.yaml` Datei mit den richtigen Werten, CR anwenden:

```
kubectl apply -f astra-control-backup-ipr-cr.yaml
```

[Tech Preview] Wiederherstellen von Snapshots mithilfe einer benutzerdefinierten Ressource (CR)

Sie können Daten aus einem Snapshot mithilfe einer benutzerdefinierten Ressourcendatei (CR) entweder in einem anderen Namespace oder im ursprünglichen QuellNamespace wiederherstellen.

Mit einem CR-System aus Snapshot wiederherstellen

Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie `astra-control-snapshot-restore-cr.yaml`. Aktualisieren Sie die Werte in Klammern <>, um sie an die Astra Control-Umgebung und die Cluster-Konfiguration anzupassen:
   - <CR_NAME>: Der Name dieser CR-Operation; wählen Sie einen vernünftigen Namen für Ihre Umgebung.
   - <APPVAULT_NAME>: Der Name des AppVault, in dem der Backup-Inhalt gespeichert ist.
   - <BACKUP_PATH>: Der Pfad innerhalb von AppVault, wo die Backup-Inhalte gespeichert werden. Beispiel:

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE>: Der Quell-Namespace des Wiederherstellungsvorgangs.
   - <DESTINATION_NAMESPACE>: Der Ziel-Namespace des Wiederherstellungsvorgangs.

     ```
     apiVersion: astra.netapp.io/v1
     kind: SnapshotRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appArchivePath: <BACKUP_PATH>
       appVaultRef: <APPVAULT_NAME>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

Ungelöste Direktive in <stdin> - include::../_include/selective-Restore-cr.adoc[]

1. Nachdem Sie das ausgefüllt haben `astra-control-snapshot-restore-cr.yaml` Datei mit den richtigen Werten, CR anwenden:

   ```
   kubectl apply -f astra-control-snapshot-restore-cr.yaml
   ```

Wiederherstellen von Snapshots in den ursprünglichen Namespace mit einem CR

Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie `astra-control-snapshot-ipr-cr.yaml`. Aktualisieren Sie die Werte in Klammern <>, um sie an die Astra Control-Umgebung und die Cluster-Konfiguration anzupassen:
   - <CR_NAME>: Der Name dieser CR-Operation; wählen Sie einen vernünftigen Namen für Ihre Umgebung.

- <APPVAULT_NAME>: Der Name des AppVault, in dem der Backup-Inhalt gespeichert ist.
- <BACKUP_PATH>: Der Pfad innerhalb von AppVault, wo die Backup-Inhalte gespeichert werden. Beispiel:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
20231213023800_94347756-9d9b-401d-a0c3
```

```
apiVersion: astra.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appArchivePath: <BACKUP_PATH>
  appVaultRef: <APPVAULT_NAME>
```

Ungelöste Direktive in <stdin> - include::../_include/selective-Restore-cr.adoc[]

1. Nachdem Sie das ausgefüllt haben `astra-control-snapshot-ipr-cr.yaml` Datei mit den richtigen Werten, CR anwenden:

```
kubectl apply -f astra-control-snapshot-ipr-cr.yaml
```

Ergebnis

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

Nach einer Datensicherungsoperation (Klonen, Backup oder Wiederherstellung) und einer anschließenden Anpassung des persistenten Volumes beträgt die Verzögerung bis zu zwanzig Minuten, bevor die neue Volume-Größe in der Web-Benutzeroberfläche angezeigt wird. Der Datensicherungsvorgang ist innerhalb von Minuten erfolgreich und Sie können mit der Management Software für das Storage-Backend die Änderung der Volume-Größe bestätigen.

Jeder Mitgliedsbenutzer mit Namespace-Einschränkungen nach Namespace-Name/ID oder anhand von Namespace-Bezeichnungen kann eine Applikation in einem neuen Namespace im selben Cluster oder einem anderen Cluster in seinem Unternehmenskonto klonen oder wiederherstellen. Derselbe Benutzer kann jedoch nicht auf die geklonte oder wiederhergestellte Anwendung im neuen Namespace zugreifen. Nachdem durch einen Klon- oder Wiederherstellungsvorgang ein neuer Namespace erstellt wurde, kann der Kontoadministrator/Kontoinhaber das Mitgliedskonto bearbeiten und Rolleneinschränkungen aktualisieren, damit der betroffene Benutzer Zugriff auf den neuen Namespace gewährt.

Filtern Sie Ressourcen während einer Anwendungswiederherstellung

Sie können eine Filterregel zu einem hinzufügen "Wiederherstellen" Vorgang, bei dem vorhandene Anwendungsressourcen angegeben werden, die in die wiederhergestellte Anwendung einbezogen oder von ihr ausgeschlossen werden sollen. Sie können Ressourcen basierend auf einem bestimmten Namespace, Label oder GVK (GroupVersionRind) ein- oder ausschließen.

Lesen Sie mehr über ein- und Ausschlussszenarien

- **Sie wählen eine Include-Regel mit ursprünglichen Namespaces (in-Place-Wiederherstellung)**: Vorhandene Anwendungsressourcen, die Sie in der Regel definieren, werden gelöscht und durch jene aus dem ausgewählten Snapshot oder Backup ersetzt, den Sie für die Wiederherstellung verwenden. Alle Ressourcen, die Sie nicht in der Include-Regel angeben, bleiben unverändert.
- **Sie wählen eine Include-Regel mit neuen Namespaces**: Verwenden Sie die Regel, um die spezifischen Ressourcen auszuwählen, die Sie in der wiederhergestellten Anwendung benötigen. Alle Ressourcen, die Sie nicht in der Include-Regel angeben, werden nicht in die wiederhergestellte Anwendung aufgenommen.
- **Sie wählen eine Ausschlussregel mit ursprünglichen Namespaces (in-Place-Wiederherstellung)**: Die von Ihnen angegebenen Ressourcen werden nicht wiederhergestellt und bleiben unverändert. Ressourcen, die Sie nicht ausschließen möchten, werden vom Snapshot oder Backup wiederhergestellt. Alle Daten auf persistenten Volumes werden gelöscht und neu erstellt, wenn das entsprechende StatefulSet Teil der gefilterten Ressourcen ist.
- **Sie wählen eine Ausschlussregel mit neuen Namespaces** aus: Wählen Sie mit der Regel die Ressourcen aus, die Sie aus der wiederhergestellten Anwendung entfernen möchten. Ressourcen, die Sie nicht ausschließen möchten, werden vom Snapshot oder Backup wiederhergestellt.

Regeln sind entweder Einschließen oder Ausschließen von Typen. Regeln, die Ressourceneinschluss und -Ausschluss kombinieren, sind nicht verfügbar.

Schritte

1. Nachdem Sie die Option Ressourcen filtern und im Assistenten zum Wiederherstellen von Apps eine Option ein- oder ausschließen ausgewählt haben, wählen Sie **Einschlussregel hinzufügen** oder **Ausschlussregel hinzufügen** aus.

   Sie können keine im Cluster enthaltenen Ressourcen ausschließen, die von Astra Control automatisch berücksichtigt werden.

2. Konfigurieren Sie die Filterregel:

   Sie müssen mindestens einen Namespace, eine Bezeichnung oder GVK angeben. Stellen Sie sicher, dass alle Ressourcen, die Sie behalten, nachdem die Filterregeln angewendet wurden, ausreichend sind, um die wiederhergestellte Anwendung in einem ordnungsgemäßen Zustand zu halten.

   a. Wählen Sie einen bestimmten Namespace für die Regel aus. Wenn Sie keine Auswahl treffen, werden alle Namespaces im Filter verwendet.

      Wenn Ihre Anwendung ursprünglich mehrere Namespaces enthielt und Sie sie in neuen Namespaces wiederherstellen, werden alle Namespaces erstellt, auch wenn sie keine Ressourcen enthalten.

b. (Optional) Geben Sie einen Ressourcennamen ein.

c. (Optional) **Etikettenauswahl**: A einschließen "Etikettenauswahl" Um der Regel hinzuzufügen. Mit der Etikettenauswahl werden nur die Ressourcen gefiltert, die der ausgewählten Bezeichnung entsprechen.

d. (Optional) Wählen Sie **Use GVK (GroupVersionRind) Set, um Ressourcen zu filtern**, um weitere Filteroptionen zu erhalten.

> Wenn Sie einen GVK-Filter verwenden, müssen Sie Version und Art angeben.

i. (Optional) **Gruppe**: Wählen Sie aus der Dropdown-Liste die Kubernetes API-Gruppe aus.

ii. **Kind**: Wählen Sie aus der Dropdown-Liste das Objektschema für den Kubernetes-Ressourcentyp aus, der im Filter verwendet werden soll.

iii. **Version**: Wählen Sie die Kubernetes API Version.

3. Überprüfen Sie die Regel, die auf Ihren Einträgen erstellt wird.
4. Wählen Sie **Hinzufügen**.

> Sie können beliebig viele Regeln für ein- und Ausschlussressourcen erstellen. Die Regeln werden in der Zusammenfassung der Wiederherstellungsanwendung angezeigt, bevor Sie den Vorgang starten.

Klonen und Migrieren von Applikationen

Eine vorhandene Applikation kann geklont werden, um eine doppelte Applikation auf demselben Kubernetes-Cluster oder einem anderen Cluster zu erstellen. Wenn Astra Control eine Applikation klonen, wird ein Klon Ihrer Applikationskonfiguration und des persistenten Storage erstellt.

Das Klonen kann sich leisten, wenn Sie Applikationen und Storage von einem Kubernetes Cluster zu einem anderen verschieben müssen. So möchten Sie beispielsweise Workloads über eine CI/CD-Pipeline und über Kubernetes-Namespaces verschieben.

> Wenn Sie einem Ausführungs-Hook einen Namespace-Filter hinzufügen, der nach einer Wiederherstellung oder einem Klonvorgang ausgeführt wird, und die Wiederherstellungs- oder Klonquelle und das Ziel in verschiedenen Namespaces liegen, wird der Namespace-Filter nur auf den Ziel-Namespace angewendet.

Bevor Sie beginnen

- **Zieldatenträger prüfen**: Wenn Sie in eine andere Speicherklasse klonen, stellen Sie sicher, dass die Speicherklasse den gleichen persistenten Zugriffsmodus für Volumes verwendet (z. B. ReadWriteMany). Der Klonvorgang schlägt fehl, wenn der Zugriffsmodus des persistenten Volume-Ziels anders ist. Wenn das persistente Quell-Volume beispielsweise den RWX-Zugriffsmodus verwendet, wählen Sie eine Ziel-Storage-Klasse aus, die RWX nicht bereitstellen kann, wie z. B. Azure Managed Disks, AWS EBS, Google Persistent Disk oder `ontap-san`, Führt dazu, dass der Klonvorgang fehlschlägt. Weitere Informationen zu den Zugriffsmodi für persistente Volumes finden Sie im "Kubernetes" Dokumentation.
- Um Apps einem anderen Cluster zu klonen, müssen Sie sicherstellen, dass Sie einen Standard-Bucket für die Cloud-Instanz zugewiesen haben, die das Quell-Cluster enthält. Wenn die Quell-Cloud-Instanz keinen Standard-Bucket-Satz hat, schlägt der Cluster-übergreifende Klonvorgang fehl.

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

Einschränkungen beim Klonen

- **Explicit Storage class**: Wenn Sie eine App mit einer explizit eingestellten Speicherklasse bereitstellen und die App klonen müssen, muss das Ziel-Cluster über die ursprünglich angegebene Speicherklasse verfügen. Das Klonen einer Applikation mit einer explizit festgelegten Storage-Klasse auf ein Cluster ohne dieselbe Storage-Klasse schlägt fehl.
- **Anwendungen mit Unterstützung der ontap-nas-Wirtschaft**: Klonvorgänge können nicht verwendet werden, wenn die Storage-Klasse Ihrer Applikation von unterstützt wird `ontap-nas-economy` Treiber. Sie können es jedoch "Backup und Restore für den wirtschaftlichen Betrieb von ontap-nas".
- **Klone und Benutzerbeschränkungen**: Jeder Mitgliedsbenutzer mit Namespace-Beschränkungen durch Namespace-Name/ID oder durch Namespace-Labels kann eine Anwendung in einem neuen Namespace im selben Cluster oder einem anderen Cluster im Konto ihres Unternehmens klonen oder wiederherstellen. Derselbe Benutzer kann jedoch nicht auf die geklonte oder wiederhergestellte Anwendung im neuen Namespace zugreifen. Nachdem durch einen Klon- oder Wiederherstellungsvorgang ein neuer Namespace erstellt wurde, kann der Kontoadministrator/Kontoinhaber das Mitgliedskonto bearbeiten und Rolleneinschränkungen aktualisieren, damit der betroffene Benutzer Zugriff auf den neuen Namespace gewährt.
- **Klone verwenden Standardcontainer**:
  - Während eines Applikations-Backups oder Applikations-Restores können Sie einen Bucket angeben, der verwendet werden soll. Sie müssen einen Standard-Bucket angeben, wenn Sie über die Cluster hinweg klonen, aber die Angabe eines Buckets ist optional, wenn Sie innerhalb desselben Clusters klonen.
  - Wenn Sie über Cluster hinweg klonen, muss die Cloud-Instanz, die das Quell-Cluster des Klonvorgangs enthält, einen Standard-Bucket-Satz aufweisen.
  - Es besteht keine Möglichkeit, die Buckets für einen Klon zu ändern. Wenn Sie die Kontrolle darüber haben möchten, welcher Bucket verwendet wird, können Sie entweder "Ändern Sie den Bucket-Standard" Oder machen Sie ein "Backup" Gefolgt von A "Wiederherstellen" Separat.
- **Mit Jenkins CI**: Wenn Sie eine vom Betreiber implementierte Instanz von Jenkins CI klonen, müssen Sie die persistenten Daten manuell wiederherstellen. Dies ist eine Einschränkung des Bereitstellungsmodells der Applikation.

Schritte

1. Wählen Sie **Anwendungen**.
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie das Menü Optionen in der Spalte **Aktionen** für die gewünschte App aus.
   - Wählen Sie den Namen der gewünschten App aus, und wählen Sie rechts oben auf der Seite die Dropdown-Liste Status aus.
3. Wählen Sie **Clone**.
4. Geben Sie Details für den Klon an:
   - Geben Sie einen Namen ein.
   - Wählen Sie ein Ziel-Cluster für den Klon.
   - Geben Sie die Ziel-Namespaces für den Klon ein. Jeder mit der App verknüpfte Quell-Namespace wird einem Ziel-Namespace zugeordnet.

Astra Control erstellt im Rahmen des Klonvorgangs neue Ziel-Namespaces. Die angegebenen Ziel-Namespaces dürfen nicht bereits im Ziel-Cluster vorhanden sein.

- Wählen Sie **Weiter**.
- Wählen Sie aus, ob die der App zugeordnete ursprüngliche Storage-Klasse beibehalten oder eine andere Storage-Klasse ausgewählt werden soll.

Sie können die Storage-Klasse einer App zu einer Storage-Klasse eines nativen Cloud-Providers oder einer anderen unterstützten Storage-Klasse migrieren und eine App von einer Storage-Klasse migrieren, die von unterstützt wird `ontap-nas-economy` Zu einer Storage-Klasse, die von unterstützt wird `ontap-nas` Oder kopieren Sie die App in ein anderes Cluster mit einer Storage-Klasse, die von der unterstützt wird `ontap-nas-economy` Treiber.

Wenn Sie eine andere Storage-Klasse auswählen und diese Storage-Klasse zum Zeitpunkt der Wiederherstellung nicht vorhanden ist, wird ein Fehler zurückgegeben.

5. Wählen Sie **Weiter**.
6. Überprüfen Sie die Informationen über den Klon und wählen Sie **Clone**.

Ergebnis

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

Nachdem durch einen Klon- oder Wiederherstellungsvorgang ein neuer Namespace erstellt wurde, kann der Kontoadministrator/Kontoinhaber das Mitgliedskonto bearbeiten und Rolleneinschränkungen aktualisieren, damit der betroffene Benutzer Zugriff auf den neuen Namespace gewährt.

Anwendungsausführungshaken verwalten

Ein Execution Hook ist eine benutzerdefinierte Aktion, die Sie so konfigurieren können, dass sie zusammen mit einem Datenschutzvorgang einer verwalteten App ausgeführt wird. Wenn Sie beispielsweise über eine Datenbank-App verfügen, können Sie mit einem Execution-Hook alle Datenbanktransaktionen vor einem Snapshot anhalten und die Transaktionen nach Abschluss des Snapshots wieder aufnehmen. Dies gewährleistet applikationskonsistente Snapshots.

Arten von Ausführungshaken

Astra Control Service unterstützt die folgenden Typen von Execution Hooks, je nachdem, wann sie ausgeführt werden können:

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

Filter für Testausführungshaken

Wenn Sie einer Anwendung einen Ausführungshaken hinzufügen oder bearbeiten, können Sie einem Ausführungshaken Filter hinzufügen, um zu verwalten, mit welchen Containern der Hook übereinstimmt. Filter sind für Applikationen nützlich, die in allen Containern dasselbe Container-Image nutzen. Jedes Image kann jedoch für einen anderen Zweck (wie Elasticsearch) verwendet werden. Mit Filtern können Sie Szenarien erstellen, in denen Ausführungshaken auf einigen, aber nicht unbedingt allen identischen Containern ausgeführt werden. Wenn Sie mehrere Filter für einen einzelnen Testausführungshaken erstellen, werden diese mit einem logischen UND einem Operator kombiniert. Pro Testsuite können Sie bis zu 10 aktive Filter haben.

Jeder Filter, den Sie einem Execution Hook hinzufügen, verwendet einen regulären Ausdruck, um Container in Ihrem Cluster zu entsprechen. Wenn ein Haken einem Container entspricht, führt der Haken sein zugehöriges Skript auf diesem Container aus. Reguläre Ausdrücke für Filter verwenden die Syntax des regulären Ausdrucks 2 (RE2), die das Erstellen eines Filters nicht unterstützt, der Container aus der Liste der Übereinstimmungen ausschließt. Informationen zur Syntax, die Astra Control für regelmäßige Ausdrücke in Hook-Filter unterstützt, finden Sie unter "Syntaxunterstützung für regulären Ausdruck 2 (RE2)".

> Wenn Sie einem Ausführungs-Hook einen Namespace-Filter hinzufügen, der nach einer Wiederherstellung oder einem Klonvorgang ausgeführt wird, und die Wiederherstellungs- oder Klonquelle und das Ziel in verschiedenen Namespaces liegen, wird der Namespace-Filter nur auf den Ziel-Namespace angewendet.

Wichtige Hinweise zu benutzerdefinierten Testausführungshaken

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

> Da Testsuitehingel die Funktionalität der Anwendung, für die sie ausgeführt werden, oft reduzieren oder vollständig deaktivieren, sollten Sie immer versuchen, die Zeit zu minimieren, die Ihre benutzerdefinierten Testausführungshaken für die Ausführung benötigt.
> Wenn Sie eine Backup- oder Snapshot-Operation mit zugeordneten Testsuiten starten, diese aber dann abbrechen, können die Haken trotzdem ausgeführt werden, wenn der Backup- oder Snapshot-Vorgang bereits gestartet wurde. Das bedeutet, dass die in einem Testsuite nach dem Backup verwendete Logik nicht davon ausgehen kann, dass das Backup abgeschlossen wurde.

- Die Ausführungshaken-Funktion ist bei neuen Astra Control-Bereitstellungen standardmäßig deaktiviert.
  - Sie müssen die Funktion „Ausführungshaken“ aktivieren, bevor Sie Ausführungshaken verwenden können.
  - Benutzer von Eigentümer oder Administrator können die Funktion „Ausführungshaken“ für alle Benutzer aktivieren oder deaktivieren, die im aktuellen Astra Control-Konto definiert sind. Siehe Aktivieren Sie die Funktion „Ausführungshaken“ Und Deaktivieren Sie die Funktion Ausführungshaken Weitere Anweisungen.
  - Der Status der Funktionsunterstützung bleibt bei Astra Control Upgrades erhalten.
- Ein Testsuite muss ein Skript verwenden, um Aktionen durchzuführen. Viele Testsuitehaoks können auf dasselbe Skript verweisen.
- Astra Control erfordert, dass die Skripte, mit denen Ausführungshaken ausgeführt werden, im Format ausführbarer Shell-Skripte geschrieben werden.
- Die Skriptgröße ist auf 96 KB begrenzt.
- Astra Control verwendet Hook-Einstellungen für die Ausführung und alle übereinstimmenden Kriterien, um festzustellen, welche Haken für einen Snapshot-, Backup- oder Wiederherstellungsvorgang gelten.

- Alle Fehler bei den Testausführungshaken sind weiche Ausfälle, andere Haken und der Datenschutzvorgang werden immer noch versucht, auch wenn ein Haken ausfällt. Wenn ein Haken jedoch ausfällt, wird ein Warnereignis im Ereignisprotokoll der Seite * aufgezeichnet.
- Um Testsuiten zu erstellen, zu bearbeiten oder zu löschen, müssen Sie Benutzer mit den Berechtigungen Eigentümer, Administrator oder Mitglied sein.
- Wenn ein Execution Hook länger als 25 Minuten dauert, schlägt der Hook fehl und erstellt einen Ereignisprotokolleintrag mit einem Rückgabecode von „N/A“. Jeder betroffene Snapshot wird als fehlgeschlagen markiert, und ein resultierender Eintrag im Ereignisprotokoll weist auf das Timeout hin.
- Für Ad-hoc-Datenschutzvorgänge werden alle Hook-Ereignisse generiert und im Ereignisprotokoll der Seite **Aktivität** gespeichert. Bei geplanten Datenschutzvorgängen werden jedoch nur Hook-Failure-Ereignisse im Ereignisprotokoll aufgezeichnet (Ereignisse, die von den geplanten Datenschutzvorgängen selbst generiert werden, werden noch aufgezeichnet).

Ausführungsreihenfolge

Wenn ein Datenschutzvorgang ausgeführt wird, finden Hakenereignisse in der folgenden Reihenfolge statt:

1. Alle entsprechenden benutzerdefinierten Testhaken für die Ausführung vor dem Betrieb werden auf den entsprechenden Containern ausgeführt. Sie können beliebig viele benutzerdefinierte Hooks für die Vorbedienung erstellen und ausführen, aber die Reihenfolge der Ausführung dieser Haken vor der Operation ist weder garantiert noch konfigurierbar.
2. Der Vorgang der Datensicherung wird durchgeführt.
3. Alle entsprechenden benutzerdefinierten Testhaken für die Ausführung nach der Operation werden auf den entsprechenden Containern ausgeführt. Sie können beliebig viele benutzerdefinierte Haken für die Nachbearbeitung erstellen und ausführen, aber die Reihenfolge der Ausführung dieser Haken nach der Operation ist weder garantiert noch konfigurierbar.

Wenn Sie mehrere Testausführungshaken desselben Typs erstellen (z. B. Pre-Snapshot), ist die Reihenfolge der Ausführung dieser Haken nicht garantiert. Die Reihenfolge der Ausführung von Haken unterschiedlicher Art ist jedoch garantiert. Die Reihenfolge der Ausführung einer Konfiguration mit allen verschiedenen Hooks sieht beispielsweise folgendermaßen aus:

1. Hooks vor dem Backup wurden ausgeführt
2. Hooks vor dem Snapshot wurden ausgeführt
3. Hooks nach dem Snapshot wurden ausgeführt
4. Hooks nach dem Backup ausgeführt
5. Haken nach der Wiederherstellung ausgeführt

Ein Beispiel für diese Konfiguration finden Sie in Szenario 2 aus der Tabelle in ob ein Haken läuft.

> Sie sollten Ihre Hook-Skripte immer testen, bevor Sie sie in einer Produktionsumgebung aktivieren. Mit dem Befehl 'kubectl exec' können Sie die Skripte bequem testen. Nachdem Sie die Testausführungshaken in einer Produktionsumgebung aktiviert haben, testen Sie die erstellten Snapshots und Backups, um sicherzustellen, dass sie konsistent sind. Dazu klonen Sie die Applikation in einem temporären Namespace, stellen den Snapshot oder das Backup wieder her und testen anschließend die App.

Bestimmen Sie, ob ein Haken läuft

Verwenden Sie die folgende Tabelle, um zu ermitteln, ob ein benutzerdefinierter Testsuite für Ihre Anwendung

ausgeführt wird.

Alle grundlegenden Applikationsvorgänge müssen eine der grundlegenden Vorgänge – Snapshot, Backup oder Wiederherstellung – ausgeführt werden. Je nach Szenario kann ein Klonvorgang aus verschiedenen Kombinationen dieser Operationen bestehen, sodass die Ausführungsooks für einen Klonvorgang variieren.

Für Wiederherstellungen ohne Backup ist ein vorhandener Snapshot oder Backup erforderlich, sodass bei diesen Vorgängen keine Snapshot- oder Backup-Hooks ausgeführt werden.

Wenn Sie starten, aber dann brechen Sie ein Backup, das einen Snapshot enthält und es sind zugewiesene Testausführungshaken, einige Haken laufen, und andere möglicherweise nicht. Das bedeutet, dass ein Testinaper nach dem Backup nicht davon ausgehen kann, dass die Sicherung abgeschlossen wurde. Beachten Sie die folgenden Punkte für abgebrochene Backups mit zugehörigen Testsuiten:

- Die Hooks vor dem Backup und nach dem Backup laufen immer.
- Wenn das Backup einen neuen Snapshot enthält und der Snapshot gestartet wurde, werden die Hooks vor dem Snapshot und nach dem Snapshot ausgeführt.
- Wenn die Sicherung vor dem Start des Snapshots abgebrochen wird, werden die Hooks vor dem Snapshot und nach dem Snapshot nicht ausgeführt.

Szenario	Betrieb	Vorhandener Snapshot	Vorhandenes Backup	Namespace	Cluster	Snapshot Hooks laufen	Backup Hooks laufen	Hooks Run wiederherstellen
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	N	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

Szenario	Betrieb	Vorhandener Snapshot	Vorhandenes Backup	Namespace	Cluster	Snapshot Hooks laufen	Backup Hooks laufen	Hooks Run wiederherstellen
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	N	K. A.

Beispiele für Testausführungshaken

Besuchen Sie das "NetApp Verda GitHub Projekt" Zum Herunterladen von Real-Execution-Hooks für beliebte Apps wie Apache Cassandra und Elasticsearch. Sie können auch Beispiele sehen und Ideen für die Strukturierung Ihrer eigenen benutzerdefinierten Execution Hooks erhalten.

Aktivieren Sie die Funktion „Ausführungshaken“

Wenn Sie Eigentümer oder Admin-Benutzer sind, können Sie die Funktion Ausführungshaken aktivieren. Wenn Sie die Funktion aktivieren, können alle in diesem Astra Control-Konto definierten Benutzer Ausführungshaken verwenden und vorhandene Ausführungshaken und Hook-Skripte anzeigen.

Schritte

1. Gehen Sie zu **Anwendungen** und wählen Sie dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie **Ausführungshaken aktivieren**.

   Die Registerkarte **Account** > **feature settings** wird angezeigt.
4. Wählen Sie im Bereich **Ausführungshaken** das Einstellungsmenü aus.
5. Wählen Sie **Enable**.
6. Beachten Sie die Sicherheitswarnung, die angezeigt wird.
7. Wählen Sie **Ja, Ausführungshaken aktivieren**.

Deaktivieren Sie die Funktion Ausführungshaken

Wenn Sie ein Benutzer von Eigentümer oder Administrator sind, können Sie die Funktion „Ausführungshaken“ für alle Benutzer deaktivieren, die in diesem Astra Control-Konto definiert sind. Sie müssen alle vorhandenen Ausführungshaken löschen, bevor Sie die Funktion „Ausführungshaken“ deaktivieren können. Siehe Löschen Sie einen Testsuite-Haken Für Anweisungen zum Löschen einer vorhandenen Ausführungsöse.

Schritte

1. Gehen Sie zu **Account** und wählen Sie dann die Registerkarte **Feature settings**.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie im Bereich **Ausführungshaken** das Einstellungsmenü aus.
4. Wählen Sie **Deaktivieren**.
5. Beachten Sie die Warnmeldung, die angezeigt wird.
6. Typ `disable` Um zu bestätigen, dass Sie die Funktion für alle Benutzer deaktivieren möchten.

7. Wählen Sie **Ja, deaktivieren**.

Vorhandene Testsuiten anzeigen

Sie können vorhandene benutzerdefinierte Testsuiten für eine App anzeigen.

Schritte

1. Gehen Sie zu **Anwendungen** und wählen Sie dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.

   In der Ergebnisliste können Sie alle aktivierten oder deaktivierten Testausführungshaken anzeigen. Sie sehen den Status eines Hakens, die Anzahl der passenden Container, die Erstellungszeit und den Ablauf (vor- oder Nachbetrieb). Sie können die auswählen + Symbol neben dem Hook-Namen, um die Liste der Container, auf denen es ausgeführt wird, zu erweitern. Um die Ereignisprotokolle zu den Testausführungshaken für diese Anwendung anzuzeigen, gehen Sie zur Registerkarte **Aktivität**.

Vorhandene Skripte anzeigen

Sie können die bereits hochgeladenen Skripte anzeigen. Auf dieser Seite können Sie auch sehen, welche Skripte verwendet werden und welche Haken sie verwenden.

Schritte

1. Gehen Sie zu **Konto**.
2. Wählen Sie die Registerkarte **Skripts** aus.

   Auf dieser Seite sehen Sie eine Liste mit bereits hochgeladenen Skripten. Die Spalte **used by** zeigt an, welche Testsuitehaoks die einzelnen Skripte verwenden.

Fügen Sie ein Skript hinzu

Jeder Execution Hook muss ein Skript verwenden, um Aktionen durchzuführen. Sie können einen oder mehrere Skripte hinzufügen, auf die Testausführungshaken verweisen können. Viele Ausführungshaken können auf dasselbe Skript verweisen. Dadurch können Sie viele Ausführungshaken aktualisieren, indem Sie nur ein Skript ändern.

Schritte

1. Stellen Sie sicher, dass die Funktion Ausführungshaken aktiviert ist Aktiviert.
2. Gehen Sie zu **Konto**.
3. Wählen Sie die Registerkarte **Skripts** aus.
4. Wählen Sie **Hinzufügen**.
5. Führen Sie einen der folgenden Schritte aus:
   - Laden Sie ein benutzerdefiniertes Skript hoch.
     i. Wählen Sie die Option **Datei hochladen**.
     ii. Navigieren Sie zu einer Datei, und laden Sie sie hoch.
     iii. Geben Sie dem Skript einen eindeutigen Namen.
     iv. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.
     v. Wählen Sie **Skript speichern**.

- Fügen Sie in ein benutzerdefiniertes Skript aus der Zwischenablage ein.
  i. Wählen Sie die Option **Einfügen oder Typ** aus.
  ii. Wählen Sie das Textfeld aus, und fügen Sie den Skripttext in das Feld ein.
  iii. Geben Sie dem Skript einen eindeutigen Namen.
  iv. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.

6. Wählen Sie **Skript speichern**.

Ergebnis

Das neue Skript erscheint in der Liste auf der Registerkarte **Scripts**.

Ein Skript löschen

Sie können ein Skript aus dem System entfernen, wenn es nicht mehr benötigt wird und nicht von Testsuiten verwendet wird.

Schritte

1. Gehen Sie zu **Konto**.
2. Wählen Sie die Registerkarte **Skripts** aus.
3. Wählen Sie ein Skript aus, das Sie entfernen möchten, und wählen Sie das Menü in der Spalte **Aktionen** aus.
4. Wählen Sie **Löschen**.

> Wenn das Skript mit einem oder mehreren Testsuiten verknüpft ist, ist die Aktion **Löschen** nicht verfügbar. Um das Skript zu löschen, bearbeiten Sie zunächst die zugehörigen Testausführungshaken und ordnen Sie sie einem anderen Skript zu.

Erstellen Sie einen benutzerdefinierten Testsuite-Haken

Sie können einen benutzerdefinierten Ausführungshaken für eine App erstellen und ihn zu Astra Control hinzufügen. Siehe Beispiele für Testausführungshaken Beispiele für Haken. Sie müssen über die Berechtigungen Eigentümer, Administrator oder Mitglied verfügen, um Testausführungshaken zu erstellen.

> Wenn Sie ein benutzerdefiniertes Shell-Skript erstellen, das als Execution Hook verwendet werden soll, denken Sie daran, die entsprechende Shell am Anfang der Datei anzugeben, es sei denn, Sie führen bestimmte Befehle aus oder geben den vollständigen Pfad zu einer ausführbaren Datei an.

Schritte

1. Stellen Sie sicher, dass die Funktion Ausführungshaken aktiviert ist Aktiviert.
2. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
3. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
4. Wählen Sie **Hinzufügen**.
5. Im Bereich **Klettdetails**:
   a. Bestimmen Sie, wann der Haken ausgeführt werden soll, indem Sie im Dropdown-Menü * Operation* einen Operationstyp auswählen.
   b. Geben Sie einen eindeutigen Namen für den Haken ein.

c. (Optional) Geben Sie alle Argumente ein, um während der Ausführung an den Haken weiterzuleiten. Drücken Sie nach jedem eingegebenen Argument die Eingabetaste, um jedes Argument aufzuzeichnen.

6. (Optional) im Bereich **Hook Filter Details** können Sie Filter hinzufügen, um zu steuern, auf welchen Behältern der Execution Hook läuft:
   a. Wählen Sie **Filter hinzufügen**.
   b. Wählen Sie in der Spalte **Hook Filtertyp** ein Attribut aus, nach dem Sie im Dropdown-Menü filtern möchten.
   c. Geben Sie in der Spalte **Regex** einen regulären Ausdruck ein, der als Filter verwendet werden soll. Astra Control verwendet den "Regex-Syntax für regulären Ausdruck 2 (RE2)".

      Wenn Sie den genauen Namen eines Attributs (z. B. einen Pod-Namen) ohne anderen Text im Feld „regulärer Ausdruck“ filtern, wird ein Teilstring-Match durchgeführt. Verwenden Sie zum Abgleich eines genauen Namens und nur des Namens die exakte Syntax für die Übereinstimmung der Zeichenfolge (z. B. `^exact_podname$`).

   d. Um weitere Filter hinzuzufügen, wählen Sie **Filter hinzufügen**.

      Mehrere Filter für einen Execution Hook werden mit einem logischen UND einem Operator kombiniert. Pro Testsuite können Sie bis zu 10 aktive Filter haben.

7. Wählen Sie anschließend **Weiter** aus.
8. Führen Sie im Bereich **Script** einen der folgenden Schritte aus:
   - Fügen Sie ein neues Skript hinzu.
     i. Wählen Sie **Hinzufügen**.
     ii. Führen Sie einen der folgenden Schritte aus:
       - Laden Sie ein benutzerdefiniertes Skript hoch.
         I. Wählen Sie die Option **Datei hochladen**.
         II. Navigieren Sie zu einer Datei, und laden Sie sie hoch.
         III. Geben Sie dem Skript einen eindeutigen Namen.
         IV. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.
         V. Wählen Sie **Skript speichern**.
       - Fügen Sie in ein benutzerdefiniertes Skript aus der Zwischenablage ein.
         I. Wählen Sie die Option **Einfügen oder Typ** aus.
         II. Wählen Sie das Textfeld aus, und fügen Sie den Skripttext in das Feld ein.
         III. Geben Sie dem Skript einen eindeutigen Namen.
         IV. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.
   - Wählen Sie ein vorhandenes Skript aus der Liste aus.

     Hiermit wird der Testsuitelink angewiesen, dieses Skript zu verwenden.

9. Wählen Sie **Weiter**.

10. Überprüfen Sie die Konfiguration der Testsuite.
11. Wählen Sie **Hinzufügen**.

Überprüfen Sie den Status eines Testablaufanhängees

Nachdem ein Snapshot-, Backup- oder Wiederherstellungsvorgang abgeschlossen wurde, können Sie den Status der Testsuiten überprüfen, die im Rahmen des Vorgangs ausgeführt wurden. Mit diesen Statusinformationen können Sie festlegen, ob der Testsuite beibehalten, geändert oder gelöscht werden soll.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Datenschutz** aus.
3. Wählen Sie **Snapshots** aus, um die laufenden Snapshots zu sehen, oder **Backups**, um die laufenden Backups zu sehen.

   Der **Hook-Status** zeigt den Status der Ausführung Hakenlauf nach Abschluss des Vorgangs an. Sie können den Mauszeiger auf den Status bewegen, um weitere Details zu erhalten. Wenn z. B. beim Snapshot Fehler beim Ausführen von Hakenabfällen auftreten, wird beim Mauszeiger über den Hakenzustand für diesen Snapshot eine Liste mit fehlgeschlagenen Testsuitelhaken angezeigt. Um die Gründe für jeden Fehler zu sehen, können Sie die Seite **Aktivität** im linken Navigationsbereich überprüfen.

Skriptverwendung anzeigen

In der Web-Benutzeroberfläche von Astra Control können Sie sehen, welche Testausführungshaken ein bestimmtes Skript verwenden.

Schritte

1. Wählen Sie **Konto**.
2. Wählen Sie die Registerkarte **Skripts** aus.

   Die Spalte **used by** in der Liste der Skripte enthält Details darüber, welche Haken die einzelnen Skripte in der Liste verwenden.

3. Wählen Sie die Informationen in der Spalte **used by** für ein Skript aus, das Sie interessieren.

   Eine detailliertere Liste mit den Namen der Haken, die das Skript verwenden, und der Art der Operation, mit der sie konfiguriert sind.

Bearbeiten Sie einen Testsuite-Haken

Sie können einen Testsuite-Haken bearbeiten, wenn Sie die Attribute, Filter oder das verwendete Skript ändern möchten. Sie müssen über die Berechtigungen Eigentümer, Administrator oder Mitglied verfügen, um Testausführungshaken bearbeiten zu können.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie in der Spalte **Aktionen** das Menü Optionen für einen Haken, den Sie bearbeiten möchten.
4. Wählen Sie **Bearbeiten**.

5. Nehmen Sie alle erforderlichen Änderungen vor, und wählen Sie nach Abschluss jedes Abschnitts **Weiter** aus.
6. Wählen Sie **Speichern**.

Deaktivieren Sie einen Testsuite-Haken

Sie können einen Testsuite-Hook deaktivieren, wenn Sie ihn vorübergehend vor oder nach einem Snapshot einer App nicht ausführen möchten. Sie müssen über die Berechtigung Eigentümer, Administrator oder Mitglied verfügen, um Testsuiten zu deaktivieren.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie in der Spalte **Aktionen** das Menü Optionen für einen Haken, den Sie deaktivieren möchten.
4. Wählen Sie **Deaktivieren**.

Löschen Sie einen Testsuite-Haken

Sie können einen Execution Hook ganz entfernen, wenn Sie ihn nicht mehr benötigen. Sie müssen über die Berechtigung Eigentümer, Administrator oder Mitglied verfügen, um Testausführungshaken zu löschen.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie in der Spalte **Aktionen** das Menü Optionen für einen Haken, den Sie löschen möchten.
4. Wählen Sie **Löschen**.
5. Geben Sie im Dialogfeld „Ergebnis“ zur Bestätigung „Löschen“ ein.
6. Wählen Sie **Ja, Testsuite löschen**.

Finden Sie weitere Informationen

- "NetApp Verda GitHub Projekt"

Zeigen Sie den Zustand von Applikationen und Computing an

Zeigen Sie eine Zusammenfassung des Applikations- und Cluster-Zustands an

Klicken Sie auf das **Dashboard**, um eine allgemeine Ansicht Ihrer Apps, Cluster und deren Gesundheit anzuzeigen.

Mithilfe der Kachel „Apps“ können Sie Folgendes identifizieren:

- Wie viele Anwendungen verwalten Sie aktuell.
- Ob diese verwalteten Apps gesund sind.
- Gibt an, ob die Applikationen vollständig gesichert sind (sie sind geschützt, wenn neueste Backups verfügbar sind).

Beachten Sie, dass es sich dabei nicht nur um Zahlen oder Statusangaben handelt, sondern dass Sie auf jeden einzelnen Aspekt detaillierte Informationen abrufen können. 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.

Die Kachel Cluster bietet ähnliche Details zum Zustand des Clusters. Zudem können Sie auch unsere Angaben im Detail anzeigen, wie dies bei einer App möglich ist.

Anzeigen des Systemzustands und der Details von Clustern

Nachdem Sie Astra Control um Kubernetes Cluster erweitert haben, können Sie Details zum Cluster anzeigen, beispielsweise seinen Speicherort, die Worker-Nodes, persistente Volumes und Storage-Klassen.

Schritte

1. Wählen Sie in der Astra Control Service-UI **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**: Die Aktivitäten im Zusammenhang mit dem Cluster.

> Sie können auch Cluster-Informationen anzeigen, die vom Astra Control Service **Dashboard** aus gestartet werden. 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

Astra Control bietet nach dem Management einer App Details zu der App, mit der Sie den Kommunikationsstatus (ob Astra Control mit der App kommunizieren kann), den Sicherungsstatus (unabhängig davon, ob die App bei Ausfällen vollständig geschützt ist), die Pods, persistenten Storage usw. ermitteln können.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Hier finden Sie die gewünschten Informationen:

Anwendungsstatus
Zeigt einen Status an, der angibt, ob Astra Control mit der Applikation kommunizieren kann.

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
Die Astra Control Aktivitäten im Zusammenhang mit der App.

Buckets verwalten

Sie können die Buckets managen, die Astra für Backups und Klone verwendet. Sie können zusätzliche Buckets hinzufügen, vorhandene Buckets entfernen und den Standard-Bucket für die Kubernetes-Cluster in einer Cloud-Instanz ändern.

Nur Eigentümer und Administratoren können Buckets managen.

So verwendet Astra Control Buckets

Wenn Sie Ihr erstes Kubernetes-Cluster für eine Cloud-Instanz managen, erstellt Astra Control Service den ersten Bucket dafür "Cloud-Instanz".

Sie können einen Bucket manuell als Standardbucket für eine Cloud-Instanz festlegen. Astra Control Service verwendet diesen Bucket standardmäßig für die Backups und Klone, die Sie auf einem beliebigen gemanagten

Cluster in dieser Cloud-Instanz erstellen (Sie können einen anderen Bucket für Backups auswählen). Wenn Sie einen Live-Klon einer Applikation von einem der gemanagten Cluster in einer Cloud-Instanz in ein anderes Cluster ausführen, verwendet Astra Control Service den Standard-Bucket für die Cloud-Quell-Instanz, um den Klonvorgang auszuführen.

Sie können denselben Bucket wie den Standard-Bucket für mehrere Cloud-Instanzen festlegen.

Sie können aus beliebigen Buckets auswählen, wenn Sie eine Schutzrichtlinie erstellen oder ein Ad-hoc-Backup starten.

Astra Control Service überprüft vor dem Start eines Backups oder Klons, ob auf einen Ziel-Bucket zugegriffen werden kann.

Vorhandene Buckets anzeigen

In der Liste der Buckets, die für Astra Control Service verfügbar sind, können Sie ihren Status ermitteln und den Standard-Bucket (sofern definiert) für Ihre Cloud-Instanz identifizieren.

Ein Bucket kann einen der folgenden Zustände haben:

Ausstehend

Nachdem Sie einen Bucket hinzugefügt haben, wird er im ausstehenden Status gestartet, während Astra Control ihn erkennt.

Verfügbar

Der Eimer ist für Astra Control verfügbar.

Entfernt

Der Bucket ist momentan nicht einsatzbereit. Bewegen Sie die Maus über das Statussymbol, um zu ermitteln, was das Problem ist.

Wenn ein Bucket den Status „entfernt“ aufweist, können Sie ihn immer noch als Standard-Bucket festlegen und ihn einem Sicherungszeitplan zuweisen. Wenn der Bucket jedoch zum Start eines Datensicherungsvorgangs nicht im Status „verfügbar“ steht, schlägt dieser Vorgang fehl.

Schritt

1. Gehen Sie zu **Buckets**.

   Die Liste der für Astra Control Service verfügbaren Buckets wird angezeigt.

Fügen Sie einen zusätzlichen Bucket hinzu

Sie können jederzeit weitere Buckets hinzufügen. Dadurch können Sie beim Erstellen einer Sicherungsrichtlinie oder beim Starten eines Ad-hoc-Backups zwischen Buckets wählen und den Standard-Bucket ändern, den eine Cloud-Instanz verwendet.

Sie können die folgenden Buckets hinzufügen:

- Amazon Web Services
- Allgemein S3
- Google Cloud Platform

- Microsoft Azure
- NetApp ONTAP S3
- NetApp StorageGRID S3

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie den Namen eines vorhandenen Buckets kennen.
- Stellen Sie sicher, dass Sie über Anmeldedaten für den Bucket verfügen, die Astra Control die erforderlichen Berechtigungen zum Management des Buckets zur Verfügung stellen.
- Wenn sich Ihr Bucket in Microsoft Azure befindet:
  - Der Bucket muss zur Ressourcengruppe *astra-Backup-rg* gehören.
  - Wenn die Performance der Azure Storage-Kontoinstanz auf „Premium“ eingestellt ist, muss die Einstellung „Premium-Kontotyp“ auf „Block-Blobs“ gesetzt werden.

Schritte

1. Gehen Sie zu **Buckets**.
2. Wählen Sie **Hinzufügen** und folgen Sie den Anweisungen, um den Eimer hinzuzufügen.
   - **Typ**: Wählen Sie Ihren Cloud-Anbieter.
   - **Vorhandener Bucket-Name**: Geben Sie den Namen des Buckets ein.
   - **Beschreibung**: Geben Sie optional eine Beschreibung des Eimers ein.
     - **Storage-Konto** (nur Azure): Geben Sie den Namen Ihres Azure-Speicherkontos ein. Dieser Bucket muss zur Ressourcengruppe namens *astra-Backup-rg* gehören.
     - **S3-Servername oder IP-Adresse** (nur AWS- und S3-Bucket-Typen): Geben Sie den vollständig qualifizierten Domainnamen des S3-Endpunkts ein, der Ihrer Region entspricht, ohne `https://`. Siehe "Die Amazon-Dokumentation" Finden Sie weitere Informationen.
     - **Select credentials**: Geben Sie die Zugangsdaten ein, die Astra Control Service mit den Berechtigungen zur Verwaltung des Buckets zur Verfügung stellen. Die Informationen, die Sie bereitstellen müssen, hängen vom Bucket-Typ ab.
       a. Wählen Sie **Hinzufügen**, um den Eimer hinzuzufügen.

Ergebnis

Der Bucket wird mit Astra Control Service hinzugefügt. Sie können diesen Bucket jetzt auswählen, wenn Sie eine Schutzrichtlinie erstellen oder ein Ad-hoc-Backup durchführen. Sie können diesen Bucket auch als Standardbucket für eine Cloud-Instanz festlegen.

Ändern des Standard-Bucket

Sie können den Standard-Bucket für eine Cloud-Instanz ändern. Astra Control Service verwendet diesen Bucket standardmäßig für Backups und Klone. Jede Cloud-Instanz verfügt über einen eigenen Standard-Bucket.

Astra Control weist keinem Cloud-Instanz automatisch einen Standard-Bucket zu. Sie müssen einen Standard-Bucket für eine Cloud-Instanz manuell festlegen, bevor Sie Applikationsklonvorgänge zwischen zwei Clustern durchführen.

Schritte

1. Gehen Sie zu **Cloud-Instanzen**.

2. Wählen Sie das Konfigurationsmenü in der Spalte **Aktionen** für die Cloud-Instanz, die Sie bearbeiten möchten.
3. Wählen Sie **Bearbeiten**.
4. Wählen Sie in der Liste der Buckets den Bucket aus, der als Standard-Bucket für diese Cloud-Instanz verwendet werden soll.
5. Wählen Sie **Aktualisieren**.

Entfernen Sie einen Bucket

Sie können einen Eimer entfernen, der nicht mehr verwendet wird oder nicht ordnungsgemäß ist. Dies könnte Sie nutzen, um die Konfiguration Ihres Objektspeicher einfach und aktuell zu halten.

- Sie können keinen Standard-Bucket entfernen. Wenn Sie diesen Bucket entfernen möchten, wählen Sie zuerst einen anderen Bucket als Standard aus.
- Sie können einen WORM-Bucket (Write Once Read Many) nicht entfernen, bevor die Aufbewahrungsfrist des Cloud-Providers abgelaufen ist. WORM-Buckets werden neben dem Bucket-Namen mit „gesperrt“ gekennzeichnet.

Bevor Sie beginnen

- Sie sollten vor Beginn sicherstellen, dass keine Backups für diesen Bucket ausgeführt oder abgeschlossen wurden.
- Sie sollten prüfen, ob der Bucket nicht für geplante Backups verwendet wird.

Wenn dies der Fall ist, können Sie nicht fortfahren.

Schritte

1. Gehen Sie zu **Buckets**.
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**.

[Tech Preview] Verwalten Sie einen Bucket mithilfe einer benutzerdefinierten Ressource

Sie können einen Bucket mithilfe einer benutzerdefinierten Astra Control-Ressource (CR) im Anwendungscluster hinzufügen. 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 die benutzerdefinierte Ressourcenmethode verwenden, erfordert die Funktionalität von Anwendungs-Snapshots einen Bucket.

Wenn Sie Ihre Applikationskonfiguration und Ihren persistenten Storage im selben Cluster klonen, benötigen Sie in Astra Control keinen Bucket.

Die benutzerdefinierte Bucket-Ressource für Astra Control ist AppVault genannt. Dieser CR enthält die Konfigurationen, die für die Verwendung eines Eimers bei Schutzmaßnahmen erforderlich sind.

Bevor Sie beginnen

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

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

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

Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie (z. B. `astra-appvault.yaml`).
2. Konfigurieren Sie die folgenden Attribute:
   - **metadata.name**: *(erforderlich)* der Name der benutzerdefinierten AppVault-Ressource.
   - **Spec.prefix**: *(Optional)* Ein Pfad, der den Namen aller im AppVault gespeicherten Entitäten vorangestellt ist.
   - **spec.providerConfig**: *(erforderlich)* speichert die Konfiguration, die für den Zugriff auf AppVault unter Verwendung des angegebenen Anbieters erforderlich ist.
   - **spec.providerCredentials**: *(erforderlich)* speichert Verweise auf alle Anmeldeinformationen, die für den Zugriff auf AppVault unter Verwendung des angegebenen Anbieters erforderlich sind.
     - **spec.providerCredentials.valueFromSecret**: *(Optional)* gibt an, dass der Wert der Zugangsdaten von einem Geheimschlüssel stammen soll.
       - **Schlüssel**: *(erforderlich, wenn valueFromSecret verwendet wird)* der gültige Schlüssel des zu wählenden Geheimnisses.
       - **Name**: *(erforderlich, wenn valueFromSecret verwendet wird)* Name des Geheimnisses, das den Wert für dieses Feld enthält. Muss sich im gleichen Namespace befinden.
   - **spec.providerType**: *(erforderlich)* legt fest, was das Backup zur Verfügung stellt, zum Beispiel NetApp ONTAP S3 oder Microsoft Azure.

     Beispiel YAML:

```
apiVersion: astra.netapp.io/v1
kind: AppVault
metadata:
  name: astra-appvault
spec:
  providerType: generic-s3
  providerConfig:
    path: testpath
    endpoint: 192.168.1.100:80
    bucketName: bucket1
    secure: "false"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        name: s3-creds
        key: accessKeyID
    secretAccessKey:
      valueFromSecret:
        name: s3-creds
        key: secretAccessKey
```

3. Nachdem Sie das ausgefüllt haben `astra-appvault.yaml` Datei mit den richtigen Werten, CR anwenden:

```
kubectl apply -f astra-appvault.yaml -n astra-connector
```

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

Weitere Informationen

- "Verwenden Sie die Astra Control API"

Überwachen Sie laufende Aufgaben

Sie können Details über die Ausführung von Aufgaben und Aufgaben anzeigen, die in den letzten 24 Stunden in Astra Control abgeschlossen, fehlgeschlagen oder abgebrochen wurden. Beispielsweise können Sie den Status eines laufenden Backups, Restores oder Klonvorgangs anzeigen, und Details wie den Prozentsatz abgeschlossen und die geschätzte verbleibende Zeit angezeigt werden. Sie können den Status eines geplanten Vorgangs anzeigen, der ausgeführt wurde, oder einen manuell gestarteten Vorgang.

Während Sie eine laufende oder abgeschlossene Aufgabe anzeigen, können Sie die Aufgabendetails erweitern, um den Status der einzelnen Unteraufgaben anzuzeigen. Die Fortschrittsleiste der Aufgabe ist grün für laufende oder abgeschlossene Aufgaben, blau für stornierte Aufgaben und rot für Aufgaben, die aufgrund eines Fehlers fehlgeschlagen sind.

Bei Klonvorgängen bestehen die Unteraufgaben der Aufgabe aus einem Snapshot und einem Snapshot-Wiederherstellungsvorgang.

Weitere Informationen zu fehlgeschlagenen Aufgaben finden Sie unter "Überwachen der Kontoaktivität".

Schritte

1. Während eine Aufgabe ausgeführt wird, gehen Sie zu **Anwendungen**.
2. Wählen Sie den Namen einer Anwendung aus der Liste aus.
3. Wählen Sie in den Details der Anwendung die Registerkarte **Aufgaben** aus.

   Sie können Details zu aktuellen oder früheren Aufgaben anzeigen und nach Aufgabenstatus filtern.

Aufgaben werden bis zu 24 Stunden in der Liste **Aufgaben** aufbewahrt. Sie können diese Begrenzung und andere Einstellungen für die Aufgabenüberwachung mit dem konfigurieren "Astra Control API".

Konto verwalten

Abrechnung einrichten

Sie können für die Verwaltung Ihrer Astra Control Service-Kontoabrechnung mehrere Methoden verwenden. Wenn Sie Azure oder Amazon AWS nutzen, können Sie einen Astra Control Service-Plan über den Microsoft Azure Marketplace oder AWS Marketplace abonnieren. Wenn Sie dies tun, können Sie Ihre Rechnungsdetails über den Marktplatz verwalten. Sie können sich auch direkt für NetApp anmelden. Wenn Sie sich direkt bei NetApp anmelden, können Sie über den Astra Control Service Ihre Rechnungsdetails verwalten. Wenn Sie den Astra Control Service ohne Abonnement nutzen, werden Sie automatisch beim Free Plan angemeldet.

Mit dem Astra Control Service Free Plan können Sie bis zu 10 Namespaces in Ihrem Konto verwalten. Wenn Sie mehr als 10 Namespaces verwalten möchten, müssen Sie Rechnungen einrichten. Dazu müssen Sie ein Upgrade vom Free Plan auf den Premium Plan durchführen oder den Azure Marketplace oder AWS Marketplace abonnieren.

Übersicht über die Abrechnung

Mit dem Astra Control Service stehen zwei Kostenarten zur Verfügung: Die Kosten für den Astra Control Service fallen durch NetApp an. Die Kosten für persistenten Volumes und Objekt-Storage fallen vom Cloud-Provider an.

Fakturierung des Astra Control Service

Der Astra Control Service umfasst drei Pläne:

Kostenloser Plan

Verwalten Sie bis zu 10 Namespaces kostenlos.

Premium-PAYGO

Managen Sie eine unbegrenzte Anzahl von Namespaces zu einer bestimmten Rate pro Namespace.

Premium-Abonnement

Mit einem Jahresabonnement, mit dem Sie bis zu 20 Namespaces pro *Namespace Pack* verwalten können, können Sie vorab zu einem ermäßigten Preis zahlen. Wenden Sie sich an den NetApp Vertrieb, um so viele Pakete wie nötig zu erwerben. Erwerben Sie beispielsweise 3 Pakete, um 60 Namespaces über Astra Control Service zu managen. Wenn Sie mehr Namespaces verwalten als von Ihrem Jahresabonnement erlaubt, werden Ihnen die Abonnementgebühr für einen zusätzlichen Namespace berechnet. Wenn Sie noch kein Astra Control Konto haben, erstellt der Kauf des Premium Subscription automatisch ein Astra Control-Konto für Sie. Wenn Sie bereits einen kostenlosen Plan besitzen, werden Sie automatisch in das Premium-Abonnement konvertiert.

Wenn Sie ein Astra Control-Konto erstellen, sind Sie automatisch beim Free Plan angemeldet. Das Dashboard von Astra Control zeigt Ihnen, wie viele Namespaces Sie derzeit aus den 10 freien Namespaces verwalten, die Sie zugelassen haben. Die Abrechnung beginnt für einen Namespace, wenn die erste App, die den Namespace enthält, verwaltet wird und stoppt für diesen Namespace, wenn die letzte App, die den Namespace enthält, nicht verwaltet wird.

Wenn Sie versuchen, einen 11. Namespace zu verwalten, benachrichtigt Astra Control Sie, dass Sie die Grenze des Freiplans erreicht haben. Anschließend werden Sie aufgefordert, ein Upgrade vom kostenlosen Plan auf einen Premium-Plan durchzuführen. Sie erhalten die Gebühr für die abonnementabhängige Überalterrate pro zusätzlichem Namespace.

Sie können jederzeit ein Upgrade auf einen Premium Plan durchführen. Nach dem Upgrade beginnt Astra Control Sie mit dem Aufladen von *all* Namespaces im Konto. Die ersten 10 Namensräume bleiben nicht im Free Plan.

Google Cloud Rechnungen

Persistente Volumes werden durch NetApp Cloud Volumes Service gesichert und Backups von Applikationen werden in einem Google Cloud-Bucket gespeichert.

- "Weitere Informationen zur Preisgestaltung für Cloud Volumes Service".

  Beachten Sie, dass der Astra Control Service alle Servicetypen und Servicelevel unterstützt. Der von Ihnen verwendete Servicetyp hängt von Ihrem ab "Google Cloud-Region".

- "Hier finden Sie Preisdetails für Google Cloud Storage Buckets".

Microsoft Azure Abrechnung

Persistente Volumes werden durch Azure NetApp Files gesichert und Backups Ihrer Applikationen werden in einem Azure Blob-Container gespeichert.

- "Weitere Informationen zur Preisgestaltung für Azure NetApp Files".
- "Sehen Sie sich Preisdetails für Microsoft Azure Blob Storage an".
- "Sehen Sie sich die Pläne und Preise für Astra Control Service im Azure Marketplace an"

Der Azure-Abrechnungssatz für den Astra Control Service gilt pro Stunde, nach Ablauf der 29 Minuten der Nutzungsstunde beginnt eine neue Abrechnungsstunde.

Amazon Web Services Abrechnung

Persistente Volumes werden durch EBS oder FSX for NetApp ONTAP gesichert und Backups Ihrer Applikationen werden in einem AWS-Bucket gespeichert.

- "Preisdetails zu Amazon Web Services anzeigen".

Abonnieren Sie den Astra Control Service im Azure Marketplace

Astra Control Service können Sie über den Azure Marketplace abonnieren. Ihre Konto- und Rechnungsdaten werden über den Marketplace verwaltet.

Eine Videoeingangsfunktion zum Abonnement von Azure Marketplace finden Sie unter "NetApp TV".

Schritte

1. Wechseln Sie zum "Azure Marketplace".
2. Wählen Sie **Jetzt Holen**.
3. Befolgen Sie die Anweisungen, um einen Plan zu abonnieren.

Abonnieren Sie den Astra Control Service im AWS Marketplace

Sie können den Astra Control Service über den AWS Marketplace abonnieren. Ihre Konto- und Rechnungsdaten werden über den Marketplace verwaltet.

Schritte

1. Wechseln Sie zum "AWS Marketplace".
2. Wählen Sie **Kaufoptionen anzeigen**.
3. Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem AWS-Konto an, oder erstellen Sie ein neues Konto.
4. Befolgen Sie die Anweisungen, um einen Plan zu abonnieren.

Abonnieren Sie den Astra Control Service direkt mit NetApp

Sie können den Astra Control Service über die Astra Control Service UI abonnieren oder sich an den NetApp Sales wenden.

Upgrade vom kostenlosen Plan auf den Premium PAYGO Plan

Aktualisieren Sie Ihren Rechnungsplan jederzeit, um mehr als 10 Namespaces von Astra Control zu verwalten, indem Sie bezahlen, wie Sie gehen. Sie brauchen nur eine gültige Kreditkarte.

Schritte

1. Wählen Sie **Konto** und dann **Abrechnung**.
2. Gehen Sie unter **Pläne** zu **Premium PAYGO** und wählen Sie **Upgrade Now**.
3. Geben Sie Zahlungsdetails für eine gültige Kreditkarte an und wählen Sie **Upgrade auf Premium Plan**.

Astra Control sendet Ihnen eine E-Mail, wenn sich die Kreditkarte dem Ablauf nähert.

Ergebnis

Sie können jetzt mehr als 10 Namespaces verwalten. Astra Control lädt Sie für alle Namespaces, die Sie derzeit verwalten.

Upgrade vom kostenlosen Plan auf das Premium-Abonnement

Wenden Sie sich an NetApp Sales, um im Rahmen eines Jahresabonnements eine Vorlaufzeit zu einem reduzierten Preis zu erhalten.

Schritte

1. Wählen Sie **Konto** und dann **Abrechnung**.
2. Gehen Sie unter **Pläne** zu **Premium-Abonnement** und wählen Sie **Vertrieb kontaktieren**.
3. Geben Sie dem Vertriebsteam Details an, um den Prozess zu starten.

Ergebnis

Ein NetApp Vertriebsmitarbeiter wird sich mit Ihnen in Verbindung setzen, um Ihre Bestellung zu bearbeiten. Nachdem die Bestellung abgeschlossen ist, wird Astra Control Ihren aktuellen Plan auf der Registerkarte **Abrechnung** widerspiegeln.

Zeigt den aktuellen Kosten- und Abrechnungsverlauf an

Astra Control zeigt Ihnen Ihre aktuellen monatlichen Kosten sowie einen detaillierten Abrechnungsverlauf per Namespace. Wenn Sie einen Plan über einen Marktplatz abonniert haben, ist der Rechnungsverlauf nicht sichtbar (Sie können ihn aber anzeigen, indem Sie sich am Marktplatz anmelden.)

Schritte

1. Wählen Sie **Konto** und dann **Abrechnung**.

   Ihre aktuellen Kosten werden in der Übersicht über die Abrechnung angezeigt.

2. Um den Abrechnungsverlauf nach Namespace anzuzeigen, wählen Sie **Abrechnungsverlauf** aus.

   Astra Control zeigt Ihnen die Nutzungsminuten und die Kosten für jeden Namespace. Eine Nutzungsminute ist, wie viele Minuten Astra Control Ihren Namespace in einem Abrechnungszeitraum verwaltet hat.

3. Wählen Sie die Dropdown-Liste aus, um einen vorherigen Monat auszuwählen.

Ändern Sie die Kreditkarte für Premium PAYGO

Bei Bedarf können Sie die Kreditkarte, die Astra Control zur Abrechnung hat, ändern.

Schritte

1. Wählen Sie **Konto > Abrechnung > Zahlungsart**.
2. Wählen Sie das Symbol Konfigurieren.
3. Ändern Sie die Kreditkarte.

Wichtige Hinweise

- Ihr Rechnungsplan ist per Astra Control Konto.

  Wenn Sie mehrere Konten haben, hat jeder seinen eigenen Abrechnungsplan.

- Ihre Astra Control-Rechnung enthält Gebühren für die Verwaltung Ihrer Namespaces. Für das Storage-Back-End für persistente Volumes werden Sie von Ihrem Cloud-Provider separat berechnet.

  "Erfahren Sie mehr über die Astra Control-Preise".

- Jeder Abrechnungszeitraum endet am letzten Tag des Monats.
- Sie können nicht von einem Premium-Plan auf den kostenlosen Plan herunterstufen.

Benutzer einladen und entfernen

Laden Sie Benutzer ein, sich Ihrem Astra Control-Konto anzuschließen und entfernen Sie Benutzer, die keinen Zugriff mehr auf das Konto haben sollten.

Benutzer einladen

Kontoinhaber und -Administratoren können andere Benutzer einladen, sich dem Astra Control-Konto anzuschließen.

Schritte

1. Stellen Sie sicher, dass der Benutzer über einen verfügt "BlueXP Anmeldung".
2. Wählen Sie **Konto**.
3. Wählen Sie auf der Registerkarte **Benutzer** die Option **Einladung** aus.
4. Geben Sie den Namen, die E-Mail-Adresse und die Rolle des Benutzers ein.

   Beachten Sie Folgendes:

   - Die E-Mail-Adresse muss mit der E-Mail-Adresse übereinstimmen, die der Benutzer zur Anmeldung bei BlueXP verwendet hat.
   - Jede Rolle bietet die folgenden Berechtigungen:
     - Ein **Eigentümer** hat Administratorrechte und kann Konten löschen.
     - Ein **Admin** hat Mitgliederberechtigungen und kann andere Benutzer einladen.
     - Ein **Mitglied** kann Apps und Cluster vollständig verwalten.
     - Ein **Viewer** kann Ressourcen anzeigen.
5. 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".

6. Um einen anderen Benutzer einzuladen, wählen Sie **Weitere Benutzer hinzufügen** und geben Sie Informationen für den neuen Benutzer ein.

   Sie können bis zu 10 Benutzer gleichzeitig einladen. Sie können zwischen den Nutzern, die Sie einladen, auf der linken Seite des Dialogfelds * Benutzer einladen* navigieren.

7. Wählen Sie **Benutzer einladen**.

Ergebnis

Der Benutzer oder die Benutzer erhalten eine E-Mail, die sie dazu einlädt, Ihrem Konto beizutreten.

Ändern Sie die Rolle eines Benutzers

Ein Kontoinhaber kann die Rolle aller Benutzer ändern, während ein Kontoadministrator die Rolle von Benutzern ändern kann, die über die Rolle „Administrator“, „Mitglied“ oder „Viewer“ verfügen.

Schritte

1. Wählen Sie **Konto**.
2. Wählen Sie auf der Registerkarte **Benutzer** das Menü in der Spalte **Aktionen** für den Benutzer aus.
3. Wählen Sie **Rolle bearbeiten**.
4. Wählen Sie eine neue Rolle aus.
5. 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".

6. Wählen Sie **Bestätigen**.

Ergebnis

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

Benutzer entfernen

Ein Benutzer mit der Owner-Rolle kann andere Benutzer jederzeit aus dem Konto entfernen.

Schritte

1. Wählen Sie **Konto**.
2. Wählen Sie auf der Registerkarte **Benutzer** die Benutzer aus, die Sie entfernen möchten.
3. Wählen Sie in der Spalte **Aktionen** das Menü aus und wählen Sie **Benutzer entfernen**.
4. Wenn Sie aufgefordert werden, bestätigen Sie den Löschvorgang, indem Sie „Entfernen“ eingeben und dann **Ja, Benutzer entfernen** wählen.

Ergebnis

Astra Control 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"

Anmeldeinformationen hinzufügen und entfernen

Fügen Sie Ihrem Konto Anmeldedaten für Cloud-Provider jederzeit hinzu und entfernen Sie sie. Astra Control verwendet diese Zugangsdaten, um einen Kubernetes Cluster, die Applikationen auf dem Cluster zu erkennen und Ressourcen in Ihrem Auftrag bereitzustellen.

Beachten Sie, dass alle Benutzer in Astra Control dieselben Anmeldedaten verwenden.

Anmeldedaten hinzufügen

Die häufigste Möglichkeit, Anmeldeinformationen zum Astra Control hinzuzufügen, ist, wenn Sie Cluster verwalten, aber Sie können auch Anmeldeinformationen von der Konto-Seite hinzufügen. Die Anmeldedaten stehen dann zur Verfügung, wenn Sie zusätzliche Kubernetes-Cluster managen.

Bevor Sie beginnen

- Bei Amazon Web Services sollten Sie über die JSON-Ausgabe der Anmeldedaten für das IAM-Konto verfügen, die zum Erstellen des Clusters verwendet werden. "Erfahren Sie, wie Sie einen IAM-Benutzer einrichten".
- Für GKE sollten Sie die Schlüssel-Datei für ein Servicekonto haben, das über die erforderlichen Berechtigungen verfügt. "Erfahren Sie, wie Sie ein Service-Konto einrichten".
- Bei AKS sollten Sie die JSON-Datei haben, die die Ausgabe aus der Azure CLI enthält, wenn Sie den Service-Principal erstellt haben. "Erfahren Sie, wie Sie einen Service-Principal einrichten".

  Außerdem benötigen Sie Ihre Azure Abonnement-ID, wenn Sie sie nicht zur JSON-Datei hinzugefügt haben.

Schritte

1. Wählen Sie **Konto > Anmeldeinformationen**.
2. Wählen Sie **Anmeldeinformationen Hinzufügen**.
3. Wählen Sie **Microsoft Azure**.
4. Wählen Sie **Google Cloud Platform**.
5. Wählen Sie **Amazon Web Services**.
6. Geben Sie einen Namen für die Anmeldeinformationen ein, der sie von anderen Anmeldeinformationen in Astra Control unterscheidet.
7. Geben Sie die erforderlichen Anmeldedaten ein.
8. **Microsoft Azure**: Geben Sie Astra Control Details über Ihren Azure Service Principal durch das Hochladen einer JSON-Datei oder durch Einfügen des Inhalts dieser JSON-Datei aus Ihrer Zwischenablage.

Die JSON-Datei sollte beim Erstellen des Service-Principal die Ausgabe aus der Azure CLI enthalten. Sie können auch Ihre Abonnement-ID angeben, damit sie automatisch in Astra Control hinzugefügt wird. Andernfalls müssen Sie die ID manuell eingeben, nachdem Sie den JSON bereitgestellt haben.

9. **Google Cloud Platform**: Stellen Sie die Kontoschlüsseldatei des Google Cloud-Dienstes entweder durch das Hochladen der Datei oder durch Einfügen des Inhalts aus Ihrer Zwischenablage bereit.
10. **Amazon Web Services**: Geben Sie die Zugangsdaten für den Amazon Web Services IAM-Benutzer entweder durch das Hochladen der Datei oder durch Einfügen der Inhalte aus Ihrer Zwischenablage an.
11. Wählen Sie **Anmeldeinformationen Hinzufügen**.

Ergebnis

Die Anmeldedaten stehen jetzt zur Verfügung, wenn Sie ein Cluster zu Astra Control hinzufügen.

Anmeldedaten entfernen

Entfernen Sie die Anmeldeinformationen jederzeit aus einem Konto. Sie sollten erst nach dem Entfernen von Anmeldeinformationen verwenden "Verwalten aller Cluster aufheben", Sofern Sie die Anmeldeinformationen nicht ändern (siehe Anmeldeinformationen drehen).

> Der erste Satz von Anmeldeinformationen, die Sie Astra Control hinzufügen, wird immer verwendet, da Astra Control die Zugangsdaten für die Authentifizierung im Backup-Bucket verwendet. Diese Anmeldedaten sollten am besten nicht entfernt werden.

Schritte

1. Wählen Sie **Konto > Anmeldeinformationen**.
2. Wählen Sie die Dropdown-Liste in der Spalte **Status** für die Anmeldeinformationen aus, die Sie entfernen möchten.
3. Wählen Sie **Entfernen**.
4. Geben Sie den Namen der Anmeldeinformationen ein, um das Löschen zu bestätigen, und wählen Sie dann **Ja, Anmeldeinformationen entfernen**.

Ergebnis

Astra Control entfernt die Anmeldeinformationen aus dem Konto.

Anmeldeinformationen drehen

Sie können die Anmeldeinformationen in Ihrem Konto ändern. Wenn Sie die Anmeldeinformationen drehen, drehen Sie sie während eines Wartungsfensters, wenn keine Backups ausgeführt werden (geplant oder auf Anforderung).

Schritte

1. Entfernen Sie die vorhandenen Anmeldeinformationen, indem Sie die Schritte unter ausführen Anmeldedaten entfernen.
2. Fügen Sie die neuen Anmeldeinformationen hinzu, indem Sie die Schritte unter ausführen Anmeldedaten hinzufügen.
3. Alle Buckets aktualisieren, um die neuen Anmeldedaten zu verwenden:
   a. Wählen Sie in der linken Navigationsleiste **Buckets** aus.
   b. Wählen Sie die Dropdown-Liste in der Spalte **Aktionen** für den Bucket aus, den Sie bearbeiten möchten.

c. Wählen Sie **Bearbeiten**.

d. Wählen Sie im Abschnitt **Anmeldeinformationen auswählen** die neuen Anmeldeinformationen aus, die Sie Astra Control hinzugefügt haben.

e. Wählen Sie **Aktualisieren**.

f. Wiederholen Sie die Schritte **b** bis **e** für alle übrigen Eimer auf Ihrem System.

Ergebnis

Astra Control nutzt die Zugangsdaten für den neuen Cloud-Provider.

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.

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**.

Anzeigen und Managen von Benachrichtigungen

Astra Control benachrichtigt Sie, wenn Aktionen abgeschlossen oder fehlgeschlagen sind. Beispielsweise wird eine Benachrichtigung angezeigt, wenn ein Backup einer Anwendung erfolgreich abgeschlossen wurde.

Die Anzahl der ungelesenen Benachrichtigungen ist oben rechts auf der Schnittstelle verfügbar.

Sie können diese Benachrichtigungen anzeigen und als gelesen markieren (dies kann nützlich sein, wenn Sie ungelesenen Benachrichtigungen löschen möchten, wie wir tun).

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**.

Schließen Sie Ihr Konto

Wenn Sie Ihr Astra Control-Konto nicht mehr benötigen, können Sie es jederzeit schließen.

Buckets, die Astra Control automatisch erstellt hat, werden automatisch gelöscht, wenn Sie Ihr Konto schließen.

Schritte

1. "Heben Sie das Management aller Applikationen und Cluster ab".
2. "Entfernen Sie die Zugangsdaten aus Astra Control".
3. Wählen Sie **Konto > Abrechnung > Zahlungsart**.
4. Wählen Sie **Konto Schließen**.
5. Geben Sie Ihren Kontonamen ein und bestätigen Sie, dass das Konto geschlossen wird.

Managen Sie Cloud-Instanzen

Eine Cloud-Instanz ist eine eindeutige Domäne innerhalb eines Cloud-Providers. Sie können für jeden Cloud-Provider mehrere Cloud-Instanzen erstellen, wobei jede Cloud-Instanz ihren eigenen Namen, ihre Anmeldedaten und zugehörigen Cluster hat.

Wenn Sie dem Astra Control ein neues Cluster hinzufügen, erstellen Sie eine Cloud-Instanz. Sie können eine Cloud-Instanz bearbeiten, um mit der Astra Control UI den Namen oder den Standard-Bucket zu ändern, und mithilfe der Astra Control API andere Aktionen mit der Cloud-Instanz durchführen.

Cloud-Instanz hinzufügen

Wenn Sie dem Astra Control ein neues Cluster hinzufügen, können Sie eine neue Cloud-Instanz hinzufügen. Siehe "Managen Sie Kubernetes Cluster über den Astra Control Service" Finden Sie weitere Informationen.

Bearbeiten einer Cloud-Instanz

Sie können eine vorhandene Cloud-Instanz für einen Cloud-Provider ändern.

Schritte

1. Gehen Sie zu **Cloud-Instanzen**.
2. Wählen Sie in der Liste der Cloud-Instanzen das Menü **Aktionen** für die Cloud-Instanz aus, die Sie bearbeiten möchten.
3. Wählen Sie **Bearbeiten**.

   Auf dieser Seite können Sie den Namen und den Standard-Bucket für die Cloud-Instanz aktualisieren.

   Jede Cloud-Instanz in Astra Control muss über einen eindeutigen Namen verfügen.

Anmeldedaten für eine Cloud-Instanz rotieren

Mit der Astra Control API können Sie die Anmeldedaten für eine Cloud-Instanz rotieren. Weitere Informationen "Besuchen Sie die Astra Automation Dokumentation".

Entfernen einer Cloud-Instanz

Mit der Astra Control API können Sie eine Cloud-Instanz vom Cloud-Provider entfernen. Weitere Informationen "Besuchen Sie die Astra Automation Dokumentation".

Astra Control Provisioner Aktivieren

In Astra Trident Version 23.10 und höher können Sie Astra Control Provisioner verwenden, damit lizenzierte Benutzer von Astra Control auf erweiterte Storage-Bereitstellungsfunktionen zugreifen können. Astra Control Provisioner bietet diese erweiterte Funktionalität zusätzlich zu den auf Astra Trident basierenden Standardfunktionen. Mit diesem Verfahren können Sie Astra Control Provisioner aktivieren und installieren.

Im Abonnement für Astra Control Service ist automatisch die Lizenz für die Nutzung von Astra Control Provisioner enthalten.

Bei den neuesten Updates für Astra Control wird Astra Control Provisioner Astra Trident als Storage-bereitstellung und -Orchestrierung ersetzen und für die Verwendung von Astra Control obligatorisch sein. Aus diesem Grund wird dringend empfohlen, Astra Control für die Astra Control-Bereitstellung zu aktivieren. Astra Trident wird weiterhin Open Source bleiben und mit neuen CSI- und anderen Funktionen von NetApp veröffentlicht, gepflegt, unterstützt und auf dem neuesten Stand sein.

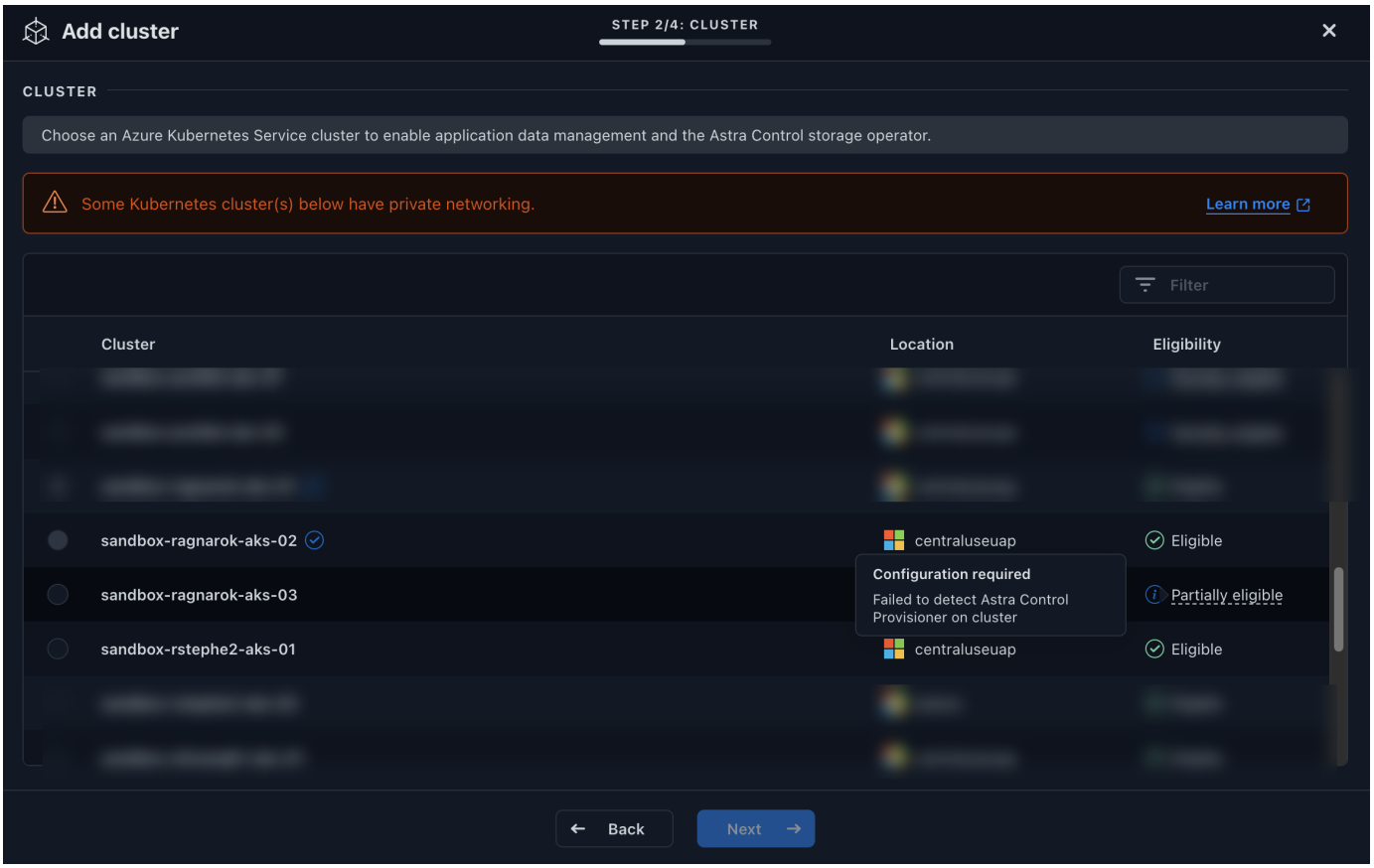
Wie kann ich feststellen, ob ich die Astra Control-Bereitstellung aktivieren muss?

Wenn Sie Astra Control Service einen Cluster hinzufügen, auf dem Astra Trident zuvor nicht installiert ist, wird der Cluster als markiert `Eligible`. Nach Ihnen "Fügen Sie den Cluster zu Astra Control hinzu", Astra Control Provisioner wird automatisch aktiviert.

Wenn der Cluster nicht markiert ist `Eligible`, Wird markiert `Partially eligible` Wegen einer der folgenden Gründe:

- Es verwendet eine ältere Version von Astra Trident
- In Astra Trident 23.10 wird noch nicht die bereitstellungsoption aktiviert
- Es handelt sich um einen Cluster-Typ, der keine automatische Aktivierung zulässt

Für `Partially eligible` In Fällen können Sie die Astra Control Provisioner für Ihr Cluster manuell aktivieren. Verwenden Sie diese Anweisungen, um



Bevor Sie Astra Control Provisioner aktivieren

Wenn Sie bereits Astra Trident ohne Astra Control Provisioner verwenden und Astra Control Provisioner aktivieren möchten, gehen Sie zuerst wie folgt vor:

- **Wenn Sie Astra Trident installiert haben, bestätigen Sie, dass seine Version innerhalb eines Fensters mit vier Versionen ist**: Sie können ein direktes Upgrade auf Astra Trident 24.02 mit Astra Control Provisioner durchführen, wenn Ihr Astra Trident innerhalb eines Fensters mit vier Versionen von Version 24.02 ist. Sie können beispielsweise direkt von Astra Trident 23.04 auf 24.02 aktualisieren.
- **Bestätigen Sie, dass Ihr Cluster über eine AMD64-Systemarchitektur verfügt**: Das Astra Control Provisioner-Image wird sowohl in AMD64- als auch in ARM64-CPU-Architekturen bereitgestellt, aber nur AMD64 wird von Astra Control unterstützt.

Schritte

1. Rufen Sie die NetApp Astra Control Image-Registry auf:
   a. Melden Sie sich an der Astra Control Service UI an und notieren Sie Ihre Astra Control Konto-ID.
      i. Wählen Sie das Symbol oben rechts auf der Seite.
      ii. Wählen Sie **API-Zugriff**.
      iii. Notieren Sie sich Ihre Konto-ID.
   b. Wählen Sie auf derselben Seite **API-Token generieren** aus und kopieren Sie die API-Token-Zeichenfolge in die Zwischenablage und speichern Sie sie in Ihrem Editor.
   c. Melden Sie sich über Ihre bevorzugte Methode in der Astra Control Registry an:

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

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

2. (Nur benutzerdefinierte Registrierungen) Befolgen Sie diese Schritte, um das Bild in Ihre benutzerdefinierte Registrierung zu verschieben. Wenn Sie keine Registrierung verwenden, befolgen Sie die Schritte des Trident-Operators in Nächster Abschnitt.

> Sie können Podman anstelle von Docker für die folgenden Befehle verwenden. Wenn Sie eine Windows-Umgebung verwenden, wird PowerShell empfohlen.

Docker

a. Rufen Sie das Astra Control Provisioner-Image aus der Registrierung ab:

> Das abgezogene Image unterstützt nicht mehrere Plattformen und unterstützt nur die gleiche Plattform wie der Host, der das Image gezogen hat, wie z. B. Linux AMD64.

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0
--platform <cluster platform>
```

Beispiel:

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0
--platform linux/amd64
```

b. Markieren Sie das Bild:

```
docker tag cr.astra.netapp.io/astra/trident-acp:24.02.0
<my_custom_registry>/trident-acp:24.02.0
```

c. Laden Sie das Bild in Ihre benutzerdefinierte Registrierung:

```
docker push <my_custom_registry>/trident-acp:24.02.0
```

Kran

a. Kopieren Sie das Astra Control Provisioner-Manifest in Ihre benutzerdefinierte Registry:

```
crane copy cr.astra.netapp.io/astra/trident-acp:24.02.0
<my_custom_registry>/trident-acp:24.02.0
```

3. Ermitteln, ob die ursprüngliche Astra Trident Installationsmethode einen verwendet hat.
4. Aktivieren Sie Astra Control Provisioner in Astra Trident mit der ursprünglich verwendeten Installationsmethode:

Astra Trident Betreiber

a. "Laden Sie das Astra Trident Installationsprogramm herunter und extrahieren Sie es".

b. Führen Sie diese Schritte aus, wenn Sie Astra Trident noch nicht installiert haben oder den Operator aus der ursprünglichen Astra Trident-Implementierung entfernt haben:

i. Erstellen des CRD:

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.1
6.yaml
```

ii. Erstellen Sie den Namespace für Trident (`kubectl create namespace trident`) Oder bestätigen Sie, dass der Namensraum Dreizack noch existiert (`kubectl get all -n trident`). Wenn der Namespace entfernt wurde, erstellen Sie ihn erneut.

c. Update von Astra Trident auf 24.02.0:

> Verwenden Sie für Cluster mit Kubernetes 1.24 oder früheren Versionen `bundle_pre_1_25.yaml`. Verwenden Sie für Cluster mit Kubernetes 1.25 oder höher `bundle_post_1_25.yaml`.

```
kubectl -n trident apply -f trident-installer/deploy/<bundle-
name.yaml>
```

d. Überprüfen Sie, ob Astra Trident ausgeführt wird:

```
kubectl get torc -n trident
```

Antwort:

```
NAME      AGE
trident   21m
```

e. Wenn Sie eine Registry mit Geheimnissen haben, erstellen Sie ein Geheimnis, mit dem Sie das Astra Control Provisioner-Bild abrufen können:

```
kubectl create secret docker-registry <secret_name> -n trident
--docker-server=<my_custom_registry> --docker-username=<username>
--docker-password=<token>
```

f. Bearbeiten Sie den TridentOrchestrator CR, und nehmen Sie die folgenden Änderungen vor:

```
kubectl edit torc trident -n trident
```

i. Legen Sie einen benutzerdefinierten Registrierungsport für das Astra Trident Image fest oder ziehen Sie es aus der Astra Control Registry (`tridentImage: <my_custom_registry>/trident:24.02.0` Oder `tridentImage: netapp/trident:24.02.0`).

ii. Astra Control Provisioner Aktivieren (`enableACP: true`).

iii. Legen Sie den benutzerdefinierten Registrierungsport für das Astra Control Provisioner-Image fest oder ziehen Sie es aus der Astra Control Registry (`acpImage: <my_custom_registry>/trident-acp:24.02.0` Oder `acpImage: cr.astra.netapp.io/astra/trident-acp:24.02.0`).

iv. Wenn Sie sich etabliert haben Geheimnisse der Bildausziehung Sie können diese hier einstellen (`imagePullSecrets: - <secret_name>`). Verwenden Sie den gleichen geheimen Namen, den Sie in den vorherigen Schritten festgelegt haben.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  tridentImage: <registry>/trident:24.02.0
  enableACP: true
  acpImage: <registry>/trident-acp:24.02.0
  imagePullSecrets:
  - <secret_name>
```

g. Speichern und beenden Sie die Datei. Der Bereitstellungsprozess wird automatisch gestartet.

h. Überprüfen Sie, ob der Operator, die Bereitstellung und Replikasets erstellt wurden.

```
kubectl get all -n trident
```

Es sollte nur eine Instanz* des Operators in einem Kubernetes-Cluster geben. Erstellen Sie nicht mehrere Implementierungen des Astra Trident Operators.

i. Überprüfen Sie die `trident-acp` Container läuft und das `acpVersion` Ist `24.02.0` Mit dem Status `Installed`:

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

Antwort:

```
status:
  acpVersion: 24.02.0
  currentInstallationParams:
    ...
    acpImage: <registry>/trident-acp:24.02.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

Tridentctl

a. "Laden Sie das Astra Trident Installationsprogramm herunter und extrahieren Sie es".

b. "Wenn Sie bereits Astra Trident verwenden, deinstallieren Sie ihn aus dem Cluster, das ihn hostet".

c. Installieren Sie Astra Trident mit aktiviertem Astra Control Provisioner (`--enable-acp=true`):

```
./tridentctl -n trident install --enable-acp=true --acp
-image=mycustomregistry/trident-acp:24.02
```

d. Aktivieren Sie die Astra Control Provisioner-Funktion:

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

Antwort:

```
+----------------+----------------+-------------+ | SERVER
VERSION | CLIENT VERSION | ACP VERSION | +----------------
+----------------+-------------+ | 24.02.0 | 24.02.0 | 24.02.0. |
+----------------+----------------+-------------+
```

Helm

a. Bei Astra Trident 23.07.1 oder einer früheren Version "Deinstallieren" Der Bediener und andere Komponenten.

b. Wenn auf dem Kubernetes-Cluster 1.24 oder eine frühere Version ausgeführt wird, löschen Sie psp:

```
kubectl delete psp tridentoperatorpod
```

c. Fügen Sie das Helm Repository von Astra Trident hinzu:

```
helm repo add netapp-trident https://netapp.github.io/trident-
helm-chart
```

d. Aktualisieren Sie das Helm-Diagramm:

```
helm repo update netapp-trident
```

Antwort:

```
Hang tight while we grab the latest from your chart
repositories...
...Successfully got an update from the "netapp-trident" chart
repository
Update Complete. □Happy Helming!□
```

e. Auflisten der Bilder:

```
./tridentctl images -n trident
```

Antwort:

```
| v1.28.0            | netapp/trident:24.02.0|
|                    | docker.io/netapp/trident-
autosupport:24.02|
|                    | registry.k8s.io/sig-storage/csi-
provisioner:v4.0.0|
|                    | registry.k8s.io/sig-storage/csi-
attacher:v4.5.0|
|                    | registry.k8s.io/sig-storage/csi-
resizer:v1.9.3|
|                    | registry.k8s.io/sig-storage/csi-
snapshotter:v6.3.3|
|                    | registry.k8s.io/sig-storage/csi-node-
driver-registrar:v2.10.0 |
|                    | netapp/trident-operator:24.02.0 (optional)
```

f. Stellen Sie sicher, dass Dreizack-Bediener 24.02.0 verfügbar ist:

```
helm search repo netapp-trident/trident-operator --versions
```

Antwort:

```
NAME                              CHART VERSION   APP VERSION
DESCRIPTION
netapp-trident/trident-operator 100.2402.0      24.02.0         A
```

g. Nutzung `helm install` Und führen Sie eine der folgenden Optionen aus, die diese Einstellungen enthalten:

- Ein Name für Ihren Bereitstellungsort
- Die Version Astra Trident
- Der Name des Bildes für die Astra Control-Bereitstellung
- Das Flag, mit dem die provisionierung aktiviert wird
- (Optional) Ein lokaler Registrierungspfad. Wenn Sie eine lokale Registrierung verwenden, wird Ihr "Trident Images" Kann in einer Registrierung oder in verschiedenen Registern gefunden werden, aber alle CSI-Images müssen sich in derselben Registrierung befinden.
- Der Trident Namespace

Optionen

◦ Bilder ohne Registrierung

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=cr.astra.netapp.io/astra/trident-
acp:24.02.0 --set enableACP=true --set operatorImage=netapp/trident-
operator:24.02.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02
--set tridentImage=netapp/trident:24.02.0 --namespace trident
```

◦ Bilder in einer oder mehreren Registern

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=<your-registry>:<acp image> --set
enableACP=true --set imageRegistry=<your-registry>/sig-storage --set
operatorImage=netapp/trident-operator:24.02.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02
--set tridentImage=netapp/trident:24.02.0 --namespace trident
```

Verwenden Sie können `helm list` So prüfen Sie Installationsdetails wie Name, Namespace, Diagramm, Status, App-Version, Und Revisionsnummer.

Falls Sie Probleme bei der Implementierung von Trident mit Helm haben, führen Sie diesen Befehl aus, um Astra Trident vollständig zu deinstallieren:

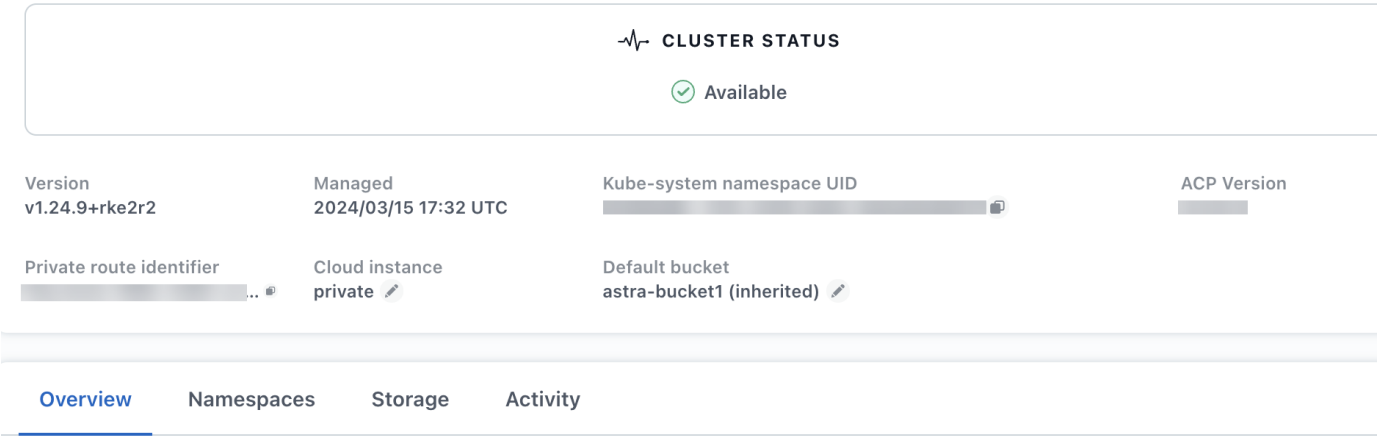
```
./tridentctl uninstall -n trident
```

Nicht "Astra Trident CRDs vollständig entfernen" Im Rahmen der Deinstallation vor dem erneuten Versuch, Astra Control Provisioner zu aktivieren.

Ergebnis

Die Bereitstellungsfunktion von Astra Control ist aktiviert und Sie können alle Funktionen der verwendeten Version verwenden.

Nach der Installation von Astra Control wird für das Cluster, das die bereitstellung in der Astra Control UI hostet, ein angezeigt `ACP version` Und nicht `Trident version` Feld und aktuelle installierte Versionsnummer.



Finden Sie weitere Informationen

- "Dokumentation für Astra Trident Upgrades"

Heben Sie das Management von Applikationen und Clustern auf

Entfernen Sie alle Applikationen oder Cluster, die Sie nicht mehr über Astra Control managen möchten.

Verwaltung einer Anwendung beenden

Sie müssen nicht mehr nur Apps managen, die Sie nicht mehr Backups, Snapshots oder Klone von Astra Control erstellen möchten.

Wenn Sie die Verwaltung einer Anwendung aufheben:

- Alle bestehenden Backups und Snapshots werden gelöscht.
- Applikationen und Daten sind weiterhin verfügbar.

Schritte

1. Wählen Sie in der linken Navigationsleiste die Option **Anwendungen**.
2. Wählen Sie die App aus.
3. Wählen Sie im Menü Optionen in der Spalte Aktionen die Option **Verwaltung aufheben** aus.

4. Überprüfen Sie die Informationen.
5. Geben Sie zur Bestätigung „nicht verwalten“ ein.
6. Wählen Sie **Ja, Anwendung Nicht Verwalten**.

Ergebnis

Astra Control beendet die Verwaltung der App.

Verwalten eines Clusters beenden

Sie müssen den Cluster nicht mehr über Astra Control managen.

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

Als Best Practice wird empfohlen, den Cluster aus Astra Control zu entfernen, bevor Sie ihn über GCP löschen.

Wenn Sie das Management eines Clusters aufheben:

- Dies verhindert, dass Ihr Cluster von Astra Control gemanagt wird. Die Konfiguration des Clusters ändert sich nicht, und das Cluster wird nicht gelöscht.
- Astra Control Provisioner oder Astra Trident werden nicht aus dem Cluster deinstalliert. "Erfahren Sie, wie Sie Astra Trident deinstallieren".

Schritte

1. Wählen Sie **Cluster**.
2. Aktivieren Sie das Kontrollkästchen für den Cluster, den Sie nicht mehr verwalten möchten.
3. Wählen Sie aus dem Optionsmenü in der Spalte **Aktionen** die Option **Unmanage**.
4. Bestätigen Sie, dass Sie die Verwaltung des Clusters aufheben möchten, und wählen Sie dann **Yes, unmanage** aus.

Ergebnis

Der Status des Clusters ändert sich in **Entfernen**. Danach wird der Cluster von der **Cluster** Seite entfernt und nicht mehr von Astra Control verwaltet.

Cluster werden von Ihrem Cloud-Provider gelöscht

Bevor Sie einen Kubernetes-Cluster mit persistenten Volumes (PV) in NetApp Storage-Klassen löschen, müssen Sie zunächst die Forderungen für das persistente Volume (PVC) löschen, und zwar nach einer der folgenden Methoden. Durch das Löschen der PVC und des PV vor dem Löschen des Clusters wird sichergestellt, dass Sie keine unerwarteten Rechnungen von Ihrem Cloud-Provider erhalten.

- **Methode #1**: Löschen Sie die Anwendungsarbeitslasten aus dem Cluster. Löschen Sie den Trident Namespace *Not*.
- **Methode #2**: Löschen Sie die VES und die Pods oder die Bereitstellung, an der die VES montiert sind.

Wenn Sie einen Kubernetes-Cluster über Astra Control managen, verwenden Applikationen auf diesem Cluster Ihren Cloud-Provider als Storage-Backend für persistente Volumes. Wenn Sie den Cluster von Ihrem Cloud-Provider löschen, ohne zuerst die PVS zu entfernen, werden die Backend-Volumes zusammen mit dem Cluster *Not* gelöscht.

Mit einer der oben genannten Methoden werden die entsprechenden PVS aus dem Cluster gelöscht. Stellen Sie sicher, dass sich auf NetApp Storage-Klassen im Cluster keine PVS befinden, bevor Sie es löschen.

Wenn Sie die persistenten Volumes nicht vor dem Löschen des Clusters gelöscht haben, müssen Sie die Backend-Volumes manuell von Ihrem Cloud-Provider löschen.

Selbstverwaltete Instanz von Astra Control implementieren

Wenn Sie eine selbst gemanagte Instanz von Astra Control innerhalb Ihres Netzwerks benötigen, können Sie Astra Control Center direkt vom Astra Control Service aus implementieren.

Schritte

1. Wählen Sie im Bereich erste Schritte im Dashboard **Deploy a self-Managed Instance of Astra Control** aus.
2. Führen Sie einen der folgenden Schritte aus:
   - Generieren Sie ein neues API-Token, indem Sie **Generate** auswählen.
   - Fügen Sie ein vorhandenes Astra Control REST-API-Token ein. Siehe "Dokumentation von Astra Automation" Anleitung zum Erstellen eines API-Tokens.
3. Folgen Sie den Anweisungen im Fenster **Deploy Astra Control Center**.