Nutzen Sie Astra

Astra Control Center

NetApp
June 06, 2024

Inhalt

Nutzen Sie Astra

Applikationsmanagement

Starten Sie das Anwendungsmanagement

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

Installation von Apps auf dem Cluster

Nachdem Sie jetzt Ihren Cluster zum Astra Control hinzugefügt haben, können Sie Apps installieren oder bestehende Apps auf dem Cluster managen. Jede Anwendung, die einem Namespace zugeordnet ist, kann verwaltet werden. Nachdem die Pods online sind, können Sie die App mit Astra Control verwalten.

Hilfe bei der Implementierung validierter Apps aus Helm Charts finden Sie in den folgenden Informationen:

- "Implementieren Sie MariaDB aus einem Helm-Diagramm"
- "MySQL aus einem Helm Diagramm implementieren"
- "Postgres aus einem Helm-Diagramm bereitstellen"
- "Jenkins aus einem Helm-Diagramm implementieren"

Applikationsmanagement

Astra Control ermöglicht das Management von Applikationen auf Namespace-Ebene oder über Kubernetes-Label.

Mit Helm 2 implementierte Apps werden nicht unterstützt.

Sie können die folgenden Aktivitäten zum Verwalten von Apps durchführen:

- Applikationsmanagement
  - Applikationen nach Namespace managen
  - Apps nach Kubernetes Label managen
- Apps ignorieren
- Das Management von Apps wird aufgehoben

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. Verwenden Sie den Filter „System-Apps anzeigen“, um Systemanwendungen anzuzeigen.

Anweisungen zum Verwalten von Apps mit der Astra API finden Sie im "Astra Automation und API-Informationen".

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.

Applikationen nach Namespace managen

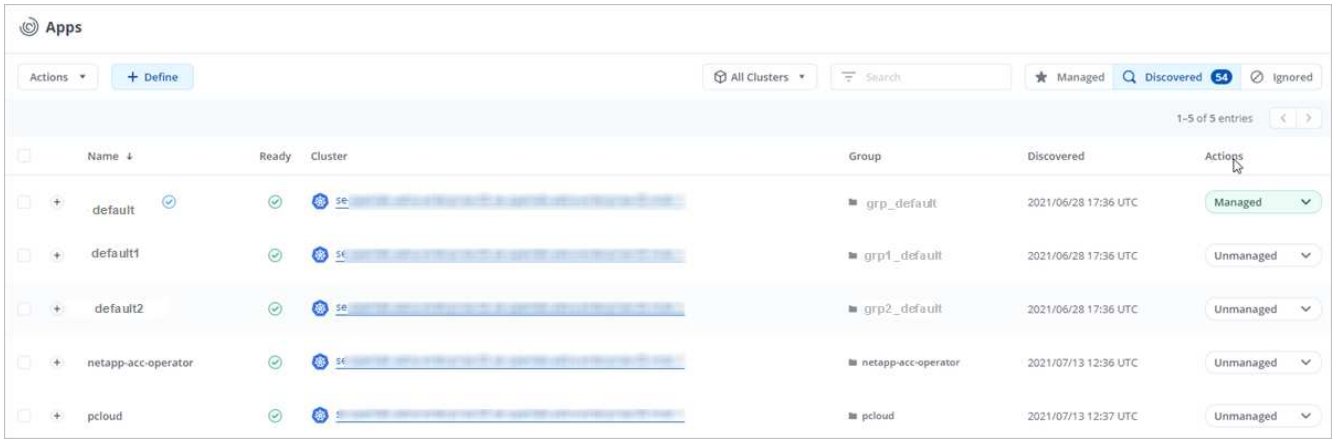
Der Abschnitt **entdeckt** der Seite Apps zeigt Namensräume und alle Helm-installierten Apps oder benutzerdefinierte Apps in diesen Namespaces. Sie können jede Applikation einzeln oder auf Namespace-Ebene managen. All dies kommt auf die Granularität zurück, die Sie für Datensicherungsvorgänge benötigen.

Vielleicht möchten Sie beispielsweise 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. Je nach Anforderungen müssen die Applikationen separat gemanagt werden und nicht unter dem Single Namespace.

Während Astra Control ermöglicht Ihnen, beide Ebenen der Hierarchie (der Namespace und die Apps in diesem Namespace) getrennt zu verwalten, ist die beste Praxis, eine oder andere zu wählen. Aktionen, die Sie in Astra Control nehmen, können fehlschlagen, wenn die Aktionen gleichzeitig sowohl auf Namespace- als auch auf App-Ebene stattfinden.

Schritte

1. Wählen Sie in der linken Navigationsleiste die Option **Apps** aus.
2. Wählen Sie **Entdeckt**.



3. Zeigen Sie die Liste der erkannten Namespaces an. Erweitern Sie den Namespace, um die Apps und zugehörigen Ressourcen anzuzeigen.

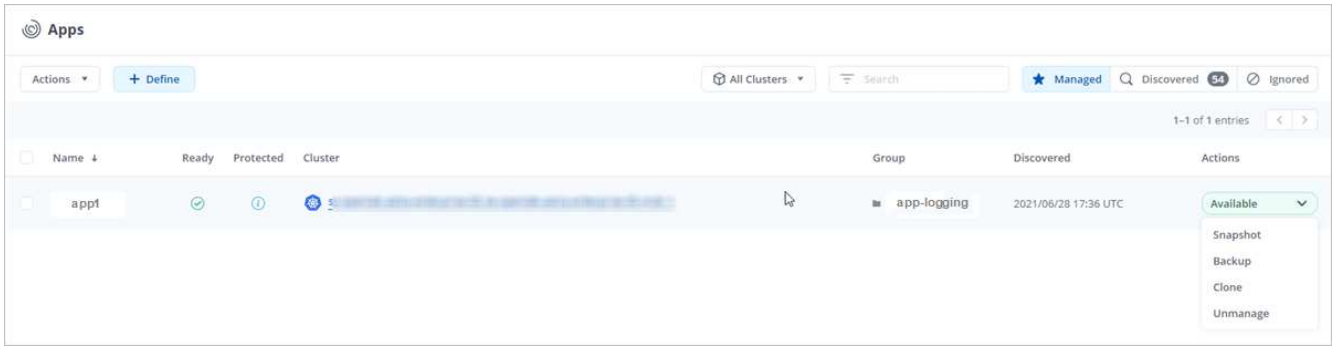
   Astra Control zeigt Ihnen die Helm-Apps und benutzerdefinierte Apps im Namespace. Wenn Helm-Labels verfügbar sind, sind sie mit einem Tag-Symbol gekennzeichnet.

4. Sehen Sie sich die Spalte **Gruppe** an, um zu sehen, in welchem Namespace die Anwendung ausgeführt wird (es ist mit dem Ordnersymbol gekennzeichnet).
5. Entscheiden Sie, ob Sie jede Applikation einzeln oder auf Namespace-Ebene verwalten möchten.
6. Suchen Sie die gewünschte App auf der gewünschten Ebene in der Hierarchie, und wählen Sie im Menü Aktionen die Option **Verwalten**.
7. Wenn Sie keine App verwalten möchten, wählen Sie im Menü Aktionen neben der App die Option

Ignorieren aus.

Wenn Sie beispielsweise alle Apps unter dem Namespace „maria“ verwalten möchten, so dass sie dieselben Snapshot- und Backup-Richtlinien haben, verwalten Sie den Namespace und ignorieren die Apps im Namespace.

8. Um die Liste der verwalteten Apps anzuzeigen, wählen Sie **verwaltet** als Anzeigefilter aus.



Beachten Sie, dass die soeben hinzugefügte App unter der Spalte „geschützt“ ein Warnsymbol enthält, das angibt, dass sie nicht gesichert ist und noch keine Backups geplant sind.

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

Ergebnis

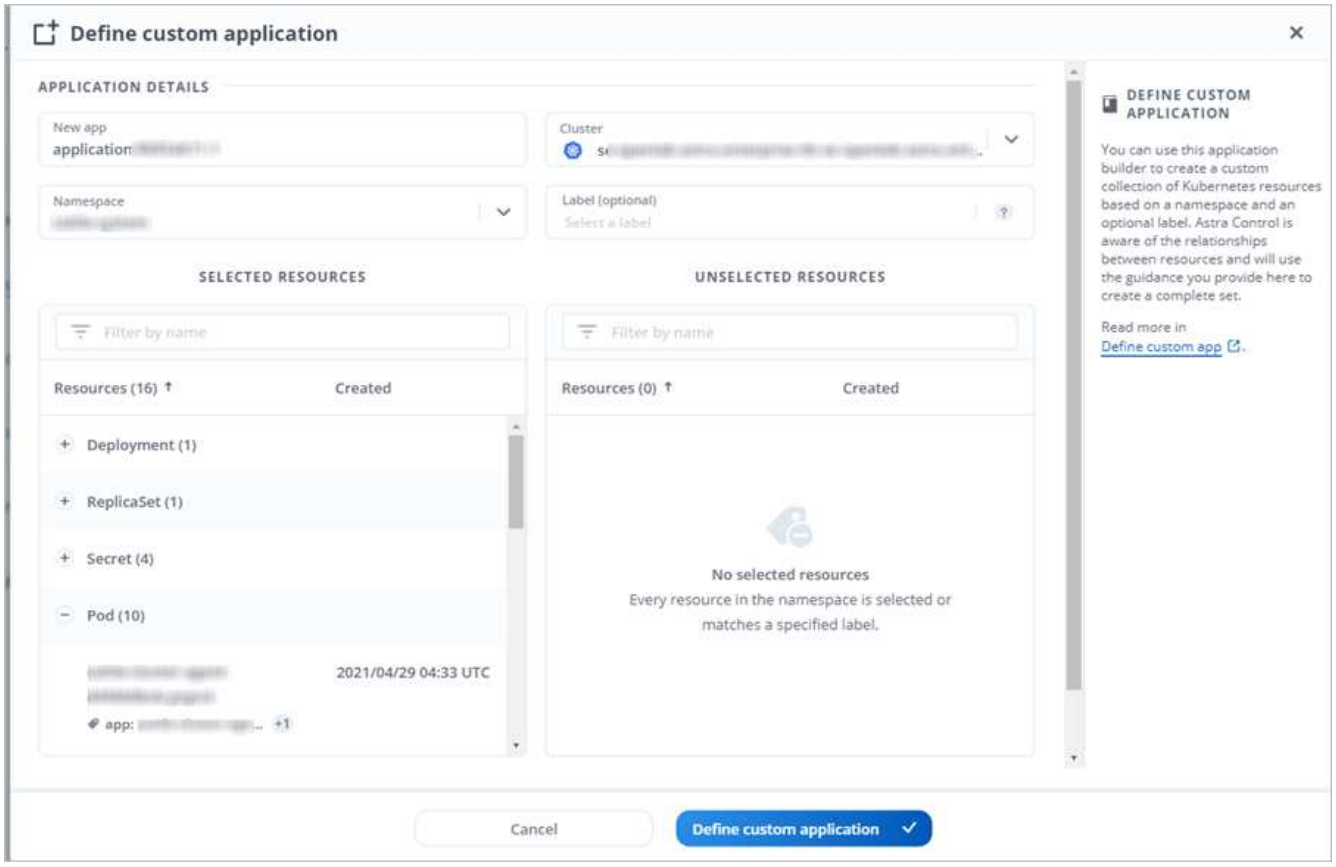
Apps, die Sie verwalten möchten, stehen jetzt auf der Registerkarte * Managed* zur Verfügung. Alle ignorierten Apps werden auf die Registerkarte **ignorierte** verschoben. Im Idealfall zeigt die Registerkarte „entdeckt“ keine Apps an, sodass neue Anwendungen leichter zu finden und zu verwalten sind.

Apps nach Kubernetes Label managen

Astra Control beinhaltet eine Aktion oben auf der Seite Apps mit dem Namen **Define Custom App**. Sie können diese Aktion zum Verwalten von Apps verwenden, die mit einem Kubernetes-Etikett gekennzeichnet sind. "Weitere Informationen über das Definieren benutzerdefinierter Applikationen nach dem Kubernetes Label".

Schritte

1. Wählen Sie in der linken Navigationsleiste die Option **Apps** aus.
2. Wählen Sie **Definieren**.



3. Geben Sie im Dialogfeld **benutzerdefinierte Anwendung definieren** die erforderlichen Informationen zur Verwaltung der App an:
   a. **Neue App**: Geben Sie den Anzeigenamen der App ein.
   b. **Cluster**: Wählen Sie den Cluster aus, in dem sich die App befindet.
   c. **Namespace:** Wählen Sie den Namespace für die App aus.
   d. **Beschriftung:** Geben Sie eine Beschriftung ein oder wählen Sie eine Beschriftung aus den unten stehenden Ressourcen aus.
   e. **Ausgewählte Ressourcen**: Zeigen Sie die ausgewählten Kubernetes-Ressourcen an, die Sie schützen möchten (Pods, Geheimnisse, persistente Volumes usw.) und managen Sie sie.
      - Zeigen Sie die verfügbaren Beschriftungen an, indem Sie eine Ressource erweitern und auf die Anzahl der Beschriftungen klicken.
      - Wählen Sie eine der Beschriftungen aus.

        Nachdem Sie eine Bezeichnung ausgewählt haben, wird sie im Feld **Etikett** angezeigt. Astra Control aktualisiert außerdem den Abschnitt **nicht ausgewählte Ressourcen**, um die Ressourcen anzuzeigen, die nicht mit dem ausgewählten Etikett übereinstimmen.
   f. **Nicht ausgewählte Ressourcen**: Überprüfen Sie die App-Ressourcen, die Sie nicht schützen möchten.
4. Klicken Sie auf **benutzerdefinierte Anwendung definieren**.

Ergebnis

Astra Control ermöglicht das Management der App. Sie finden es jetzt auf der Registerkarte **verwaltet**.

Apps ignorieren

Wenn eine App entdeckt wurde, wird sie in der Liste entdeckt angezeigt. In diesem Fall können Sie die entdeckte Liste aufräumen, damit neue, neu installierte Apps einfacher zu finden sind. Oder Sie haben unter Umständen Anwendungen, die Sie verwalten und entscheiden später, dass Sie sie nicht mehr verwalten möchten. Wenn Sie diese Apps nicht verwalten möchten, können Sie angeben, dass sie ignoriert werden sollen.

Möglicherweise möchten Sie auch Apps unter einem Namespace zusammen managen (Namespace-verwaltet). Sie können Apps ignorieren, die Sie vom Namespace ausschließen möchten.

Schritte

1. Wählen Sie in der linken Navigationsleiste die Option **Apps** aus.
2. Wählen Sie als Filter * entdeckt* aus.
3. Wählen Sie die App aus.
4. Wählen Sie im Menü Aktionen die Option **Ignorieren** aus.
5. Um das ignorieren rückgängig zu machen, wählen Sie im Menü Aktionen die Option **Unignore**.

Das Management von Apps wird aufgehoben

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

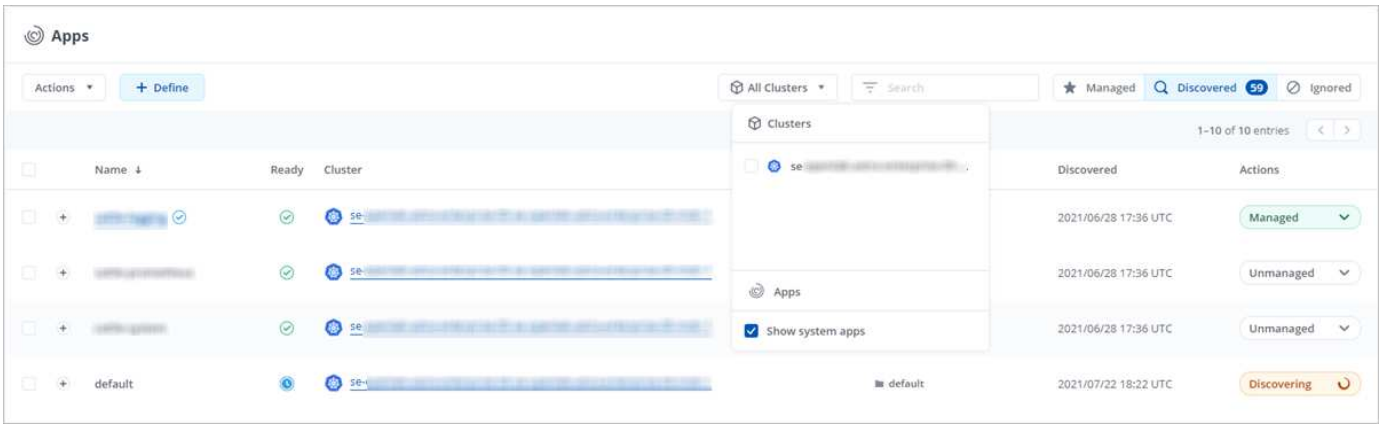
> Wenn Sie die Verwaltung einer Anwendung aufheben, gehen alle Backups oder Snapshots verloren, die zuvor erstellt wurden.

Schritte

1. Wählen Sie in der linken Navigationsleiste die Option **Apps** aus.
2. Wählen Sie als Filter * verwaltet* aus.
3. Wählen Sie die App aus.
4. Wählen Sie im Menü Aktionen die Option **Verwaltung aufheben** aus.
5. Überprüfen Sie die Informationen.
6. Geben Sie zur Bestätigung „nicht verwalten“ ein.
7. Wählen Sie **Ja, Anwendung Nicht Verwalten**.

Wie sieht es mit System-Applikationen aus?

Astra Control erkennt auch die System-Applikationen, die auf einem Kubernetes Cluster ausgeführt werden. Sie können Systemanwendungen anzeigen, indem Sie in der Symbolleiste unter dem Clusterfilter das Kontrollkästchen **System-Apps anzeigen** aktivieren.



Wir zeigen Ihnen diese System-Apps standardmäßig nicht, da es selten ist, dass Sie sie sichern müssen.

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. Verwenden Sie den Filter „System-Apps anzeigen“, um Systemanwendungen anzuzeigen.

Weitere Informationen

- "Verwenden Sie die Astra API"

Definieren Sie ein Beispiel für eine benutzerdefinierte Anwendung

Wenn Sie eine benutzerdefinierte App erstellen, können Sie Elemente Ihres Kubernetes Clusters zu einer einzelnen Applikation gruppieren.

Eine benutzerdefinierte App bietet Ihnen mehr granulare Kontrolle darüber, was in einem Astra Control-Betrieb enthalten ist, darunter:

- Klon
- Snapshot
- Backup
- Sicherungsrichtlinie

In den meisten Fällen möchten Sie die Funktionen von Astra Control in Ihrer gesamten App nutzen. Sie können jedoch auch eine benutzerdefinierte App erstellen, die diese Funktionen durch die Beschriftungen verwendet, die Sie Kubernetes-Objekten in einem Namespace zuweisen.

Um eine benutzerdefinierte App zu erstellen, gehen Sie zur Seite Apps und klicken Sie auf **+ definieren**.

Während Sie Ihre Auswahl treffen, zeigt Ihnen das Fenster Benutzerdefinierte App an, welche Ressourcen in Ihre benutzerdefinierte App aufgenommen oder von dieser ausgeschlossen werden. Dadurch können Sie sicherstellen, dass Sie die richtigen Kriterien für die Definition Ihrer benutzerdefinierten App auswählen.

Benutzerdefinierte Applikationen können nur innerhalb eines bestimmten Namespace auf einem einzelnen Cluster erstellt werden. Astra Control bietet keine Unterstützung für eine benutzerdefinierte App, die mehrere Namespaces oder Cluster umfasst.

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".

> Überlappende Richtlinien für dieselbe Ressource unter verschiedenen Namen können Datenkonflikte verursachen. Wenn Sie eine benutzerdefinierte App für eine Ressource erstellen, müssen Sie sicher sein, dass sie nicht unter anderen Richtlinien geklont oder gesichert wird.

Beispiel: Separate Schutzpolitik für kanarische Veröffentlichung

In diesem Beispiel managt das devops-Team eine implementierung für kanarische Versionen. Im Cluster befinden sich drei Pods mit nginx. Zwei der Stative sind der stabilen Freisetzung gewidmet. Der dritte POD ist für den canary Release.

Der Kubernetes Administrator des devops-Teams fügt das Label hinzu `deployment=stable` Zu den stabilen Entriegelungstativen. Das Team fügt das Label hinzu `deployment=canary` Zum canary Release POD.

Die stabile Version des Teams umfasst eine Notwendigkeit für stündliche Snapshots und tägliche Backups. Die version von canary ist kurzlebig, deshalb wollen sie für alles, was gekennzeichnet ist, eine weniger aggressive, kurzfristige Schutzpolitik erstellen `deployment=canary`.

Um mögliche Datenkonflikte zu vermeiden, erstellt der Admin zwei benutzerdefinierte Apps: Eine für die canary-Version und eine für die stabile Version. Hierdurch werden Backups, Snapshots und Klonvorgänge für die beiden Gruppen von Kubernetes-Objekten getrennt.

Schritte

1. Nachdem das Team den Cluster zu Astra Control hinzugefügt hat, besteht der nächste Schritt darin, eine benutzerdefinierte App zu definieren. Dazu klickt das Team auf die Schaltfläche **+ Definieren** auf der Seite Apps.
2. Im daraufhin angezeigten Pop-up-Fenster setzt das Team ein `devops-canary-deployment` Als App-Name. Das Team wählt den Cluster im Drop-down-Drop-Down-Menü **Namespace Cluster** aus, dann der Namensraum der App aus dem Drop-down **.
3. Das Team kann entweder eingeben `deployment=canary` Wählen Sie im Feld **Labels** das Etikett aus den unten aufgeführten Ressourcen aus.
4. Nach der Definition der benutzerdefinierten App für die canary-Bereitstellung wiederholt das Team den Prozess für die stabile Bereitstellung.

Wenn das Team die beiden benutzerdefinierten Apps erstellt hat, können diese Ressourcen als jede andere Astra Control Anwendung behandelt werden. Sie können sie klonen, Backups und Snapshots erstellen und für jede Gruppe von Ressourcen auf der Basis der Kubernetes-Labels eine individuelle Sicherungsrichtlinie erstellen.

Schützen von Applikationen

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 "Das Astra API" Um Anwendungen zu schützen.

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

Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder dem Kubernetes-Namespace) eine SecurityContext-UID zugewiesen. Um Astra Control Center zum Schutz Ihrer App zu aktivieren und die App in ein anderes Cluster oder Projekt in OpenShift zu verschieben, müssen Sie Richtlinien hinzufügen, mit denen die App als beliebige UID ausgeführt werden kann. Als Beispiel erteilen die folgenden OpenShift-CLI-Befehle der WordPress-App die entsprechenden Richtlinien.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Snapshots und Backups

A *Snapshot* ist eine zeitpunktgenaue Kopie einer Applikation, die auf demselben bereitgestellten Volume wie die Applikation gespeichert ist. In der Regel sind sie schnell. Lokale Snapshots werden verwendet, um die Applikation zu einem früheren Zeitpunkt wiederherzustellen. Snapshots sind nützlich für schnelle Klone. Snapshots enthalten alle Kubernetes-Objekte für die App, einschließlich Konfigurationsdateien.

Ein *Backup* wird im externen Objektspeicher gespeichert. Das Backup kann langsamer erstellt werden als lokale Snapshots. Sie können eine Applikation migrieren, indem Sie ihr Backup auf einen anderen Cluster wiederherstellen. Sie können auch eine längere Aufbewahrungsdauer für Backups wählen.

_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.

Konfigurieren einer Sicherungsrichtlinie

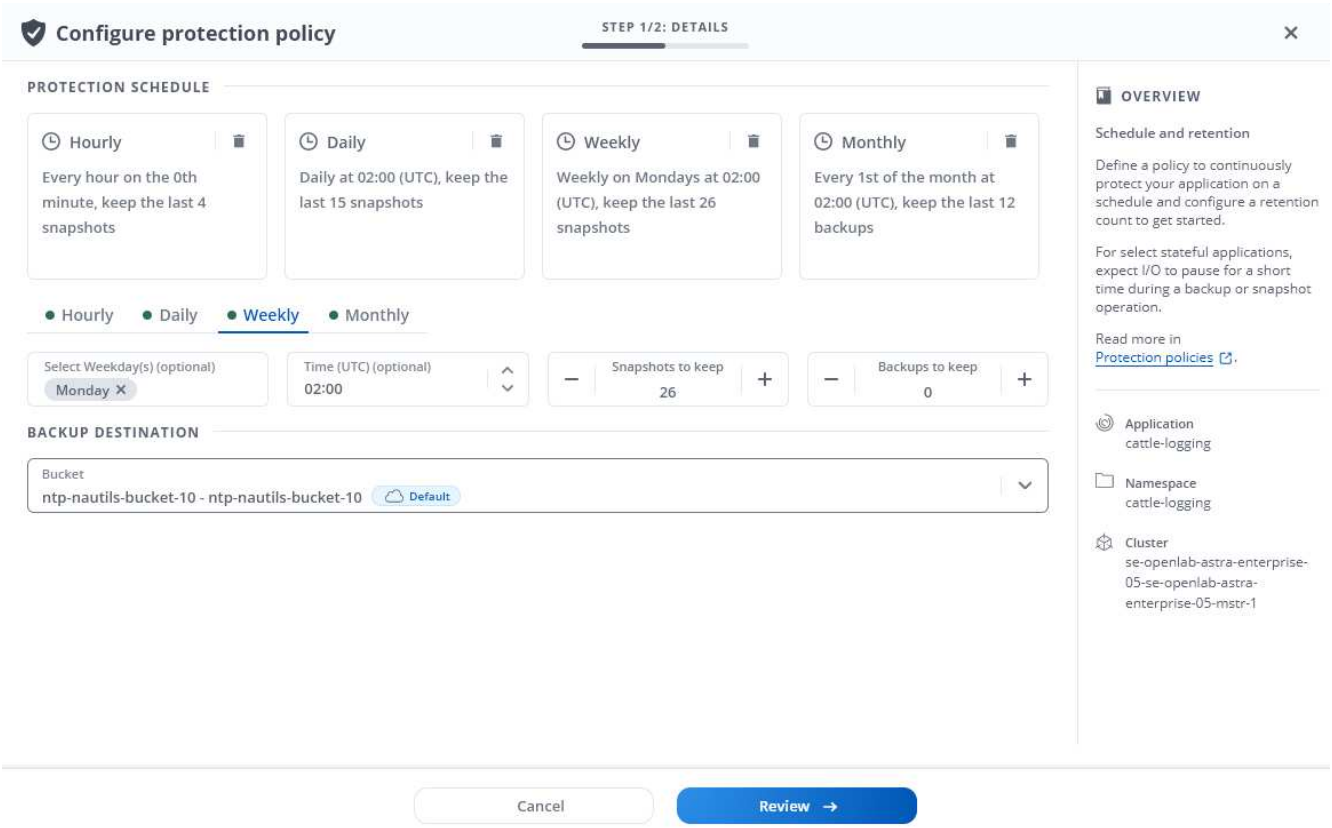
Eine Sicherungsrichtlinie sichert eine Applikation, indem Snapshots, Backups oder beides nach einem definierten Zeitplan erstellt werden. Sie können Snapshots und Backups stündlich, täglich, wöchentlich und monatlich erstellen. Außerdem können Sie die Anzahl der beizubehaltenden Kopien festlegen.

Schritte

1. Klicken Sie auf **Apps** und dann auf den Namen einer App.
2. Klicken Sie Auf **Datenschutz**.
3. Klicken Sie Auf **Schutzrichtlinie Konfigurieren**.
4. Legen Sie einen Sicherungszeitplan fest, indem Sie die Anzahl der Snapshots und Backups auswählen, die stündlich, täglich, wöchentlich und monatlich erstellt werden sollen.

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

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



5. Klicken Sie Auf **Review**.
6. Klicken Sie Auf **Schutzrichtlinie Festlegen.**

Ergebnis

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

Erstellen Sie einen Snapshot

Sie können jederzeit einen On-Demand-Snapshot erstellen.

Schritte

1. Klicken Sie Auf **Apps**.
2. Klicken Sie in der Spalte **Aktionen** für die gewünschte App auf die Dropdown-Liste.
3. Klicken Sie Auf **Snapshot**.
4. Passen Sie den Namen des Snapshots an und klicken Sie dann auf **Review**.
5. Überprüfen Sie die Snapshot-Übersicht und klicken Sie auf **Snapshot**.

Ergebnis

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

Erstellen Sie ein Backup

Sie können eine App auch jederzeit sichern.

S3 Buckets im Astra Control Center berichten nicht über die verfügbare Kapazität. Bevor Sie Backups oder Klonanwendungen durchführen, die von Astra Control Center gemanagt werden, sollten Sie die Bucket-Informationen im ONTAP oder StorageGRID Managementsystem prüfen.

Schritte

1. Klicken Sie Auf **Apps**.
2. Klicken Sie in der Spalte **Aktionen** für die gewünschte App auf die Dropdown-Liste.
3. Klicken Sie Auf **Backup**.
4. Passen Sie den Namen des Backups an.
5. 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.
6. Wählen Sie ein Ziel für das Backup aus der Liste der Speicher-Buckets aus.
7. Klicken Sie Auf **Review**.
8. Prüfen Sie die Backup-Zusammenfassung und klicken Sie auf **Backup**.

Ergebnis

Astra Control Center erstellt ein Backup der App.

Wenn Ihr Netzwerk ausfällt oder ungewöhnlich langsam ist, kann es zu einer Zeit für einen Backup-Vorgang kommen. Dies führt zum Fehlschlagen der Datensicherung.

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

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

Anzeigen von Snapshots und Backups

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

Schritte

1. Klicken Sie auf **Apps** und dann auf den Namen einer App.
2. Klicken Sie Auf **Datenschutz**.

   Die Snapshots werden standardmäßig angezeigt.

3. Klicken Sie auf **Backups**, um die Liste der Backups anzuzeigen.

Snapshots löschen

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

Schritte

1. Klicken Sie auf **Apps** und dann auf den Namen einer App.
2. Klicken Sie Auf **Datenschutz**.
3. Klicken Sie auf die Dropdown-Liste in der Spalte **Aktionen** für den gewünschten Snapshot.
4. Klicken Sie auf **Snapshot löschen**.
5. Geben Sie das Wort „Löschen“ ein, um das Löschen zu bestätigen und klicken Sie dann auf **Ja, Snapshot löschen**.

Ergebnis

Astra Control Center löscht den Snapshot.

Backups löschen

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

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

1. Klicken Sie auf **Apps** und dann auf den Namen einer App.
2. Klicken Sie Auf **Datenschutz**.
3. Klicken Sie Auf **Backups**.
4. Klicken Sie auf die Dropdown-Liste in der Spalte **Aktionen** für das gewünschte Backup.
5. Klicken Sie auf **Sicherung löschen**.
6. Geben Sie das Wort „Löschen“ ein, um den Löschvorgang zu bestätigen und klicken Sie dann auf **Ja, Sicherung löschen**.

Ergebnis

Astra Control Center löscht das Backup.

Wiederherstellung von Applikationen

Astra Control Center kann Ihre Applikation aus einem Snapshot oder Backup wiederherstellen. Persistente Storage-Backups und Snapshots werden von Ihrem Objektspeicher übertragen. Die Wiederherstellung von einem vorhandenen Snapshot in denselben Cluster erfolgt also schneller als mit anderen Methoden. Sie können die Astra UI oder verwenden "Das Astra API" Zur Wiederherstellung von Applikationen.

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

> Wenn Sie ein anderes Cluster wiederherstellen, stellen Sie sicher, dass das Cluster denselben Zugriffsmodus für persistente Volumes verwendet (z. B. ReadWriteManche). Der Wiederherstellungsvorgang schlägt fehl, wenn der Zugriffsmodus des Ziel-persistenten Volumes anders ist.

Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder dem Kubernetes-Namespace) eine SecurityContext-UID zugewiesen. Um Astra Control Center zum Schutz Ihrer App zu aktivieren und die App in ein anderes Cluster oder Projekt in OpenShift zu verschieben, müssen Sie Richtlinien hinzufügen, mit denen die App als beliebige UID ausgeführt werden kann. Als Beispiel erteilen die folgenden OpenShift-CLI-Befehle der WordPress-App die entsprechenden Richtlinien.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Schritte

1. Klicken Sie auf **Apps** und dann auf den Namen einer App.
2. Klicken Sie auf **Datenschutz**.
3. Wenn Sie von einem Snapshot wiederherstellen möchten, lassen Sie das **Snapshots** -Symbol ausgewählt. Klicken Sie andernfalls auf das Symbol **Backups**, um aus einem Backup wiederherzustellen.
4. Klicken Sie auf die Dropdown-Liste in der Spalte **Aktionen** für den Snapshot oder die Sicherung, aus der Sie wiederherstellen möchten.
5. Klicken Sie auf **Anwendung wiederherstellen**.
6. **Restore Details**: Geben Sie Details für die Wiederherstellung an:
   - Geben Sie einen Namen und einen Namespace für die App ein.

     Wenn Sie eine gelöschte Anwendung wiederherstellen, wählen Sie einen anderen Namen und einen anderen Namespace für die Anwendung als den ursprünglichen Namen aus. Wenn der Name der wiederhergestellten Anwendung mit der gelöschten Anwendung identisch ist, schlägt der Wiederherstellungsvorgang fehl.

   - Wählen Sie das Ziel-Cluster für die App aus.
   - Klicken Sie Auf **Review**.
7. **Zusammenfassung wiederherstellen**: Überprüfen Sie die Details zur Wiederherstellungsaktion und klicken Sie auf **Wiederherstellen**.

Ergebnis

Astra Control Center stellt die App basierend auf den von Ihnen bereitgestellten Informationen wieder her.

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.

Klonen und Migrieren von Applikationen

Eine vorhandene Applikation klonen, um eine doppelte Applikation auf demselben Kubernetes-Cluster oder einem anderen Cluster zu erstellen. Das Klonen kann sich leisten, wenn Sie Applikationen und Storage von einem Kubernetes Cluster zu einem anderen verschieben müssen. So möchten Sie beispielsweise Workloads über eine

CI/CD-Pipeline und über Kubernetes-Namespaces verschieben. Sie können die Astra UI oder verwenden "Das Astra API" Zum Klonen und Migrieren von Applikationen

> Wenn Sie eine App zwischen Clustern klonen, müssen die Quell- und Ziel-Cluster dieselbe Verteilung von OpenShift aufweisen. Wenn Sie beispielsweise eine App aus einem OpenShift 4.7-Cluster klonen, verwenden Sie ein Ziel-Cluster, das auch OpenShift 4.7 ist.

Wenn Astra Control Center eine Applikation geklont, wird ein Klon Ihrer Applikationskonfiguration und des persistenten Storage erstellt.

> S3 Buckets im Astra Control Center berichten nicht über die verfügbare Kapazität. Bevor Sie Backups oder Klonanwendungen durchführen, die von Astra Control Center gemanagt werden, sollten Sie die Bucket-Informationen im ONTAP oder StorageGRID Managementsystem prüfen.

> Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder dem Kubernetes-Namespace) eine SecurityContext-UID zugewiesen. Um Astra Control Center zum Schutz Ihrer App zu aktivieren und die App in ein anderes Cluster oder Projekt in OpenShift zu verschieben, müssen Sie Richtlinien hinzufügen, mit denen die App als beliebige UID ausgeführt werden kann. Als Beispiel erteilen die folgenden OpenShift-CLI-Befehle der WordPress-App die entsprechenden Richtlinien.
>
> ```
> oc new-project wordpress
> oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
> oc adm policy add-scc-to-user privileged -z default -n wordpress
> ```

Was Sie benötigen

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

Schritte

1. Klicken Sie Auf **Apps**.
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie in der Spalte **Aktionen** für die gewünschte App auf die Dropdown-Liste.
   - Klicken Sie auf den Namen der gewünschten App und wählen Sie rechts oben auf der Seite die Dropdown-Liste Status aus.
3. Klicken Sie Auf **Clone**.
4. **Clone Details**: Geben Sie Details für den Klon an:
   - Geben Sie einen Namen ein.
   - Geben Sie einen Namespace für den Klon ein.
   - Wählen Sie ein Ziel-Cluster für den Klon.
   - Wählen Sie aus, ob Sie den Klon aus einem vorhandenen Snapshot oder einem vorhandenen Backup erstellen möchten. Wenn Sie diese Option nicht wählen, erstellt Astra Control Center den Klon aus dem aktuellen Status der App.
5. **Quelle**: Wenn Sie sich für das Klonen aus einem vorhandenen Snapshot oder Backup entscheiden, wählen Sie den Snapshot oder die Sicherung, die Sie verwenden möchten.
6. Klicken Sie Auf **Review**.

7. **Clone Summary**: Überprüfen Sie die Details über den Klon und klicken Sie auf **Clone**.

Ergebnis

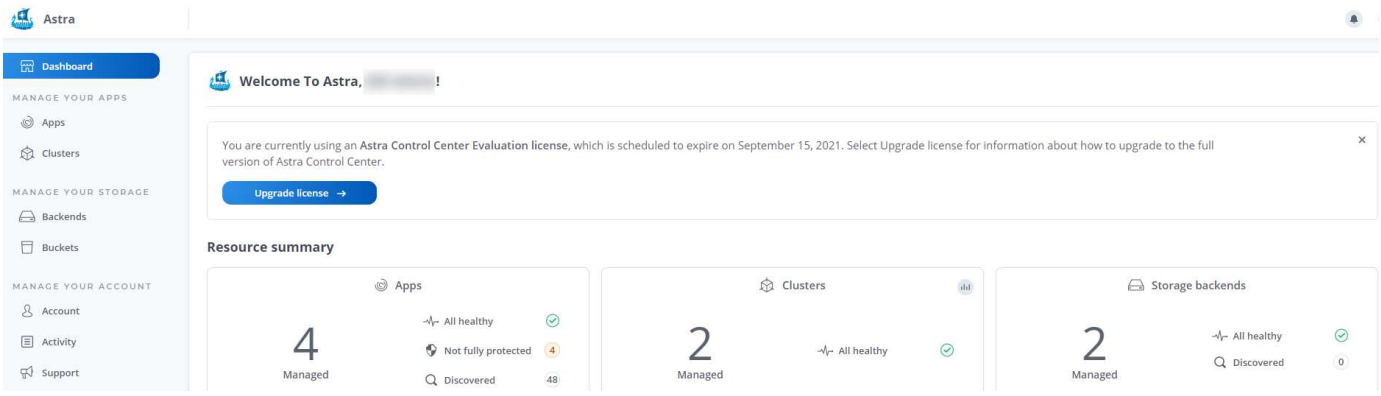
Astra Control Center klont die App basierend auf den von Ihnen angegebenen Informationen. Der Klonvorgang ist erfolgreich, wenn der neue Applikationsklon im ausgeführt wird `Available` Geben Sie auf der Seite * Apps* an.

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

Zeigen Sie den Applikations- und Cluster-Zustand an

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

Wählen Sie das **Dashboard** aus, um eine übergeordnete Ansicht Ihrer Apps, Cluster, Storage-Back-Ends und deren Integrität anzuzeigen.



Dabei handelt es sich nicht nur um statische Zahlen oder Statusangaben, sondern Sie können von jedem dieser Faktoren heruntergehen. 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.

Kachel „Apps“

Mit der Kachel * Apps* können Sie Folgendes identifizieren:

- Wie viele Applikationen managen Sie aktuell mit Astra?
- Ob diese verwalteten Apps gesund sind.
- Gibt an, ob die Applikationen vollständig gesichert sind (sie sind geschützt, wenn neueste Backups verfügbar sind).
- Die Anzahl der Anwendungen, die erkannt, aber noch nicht verwaltet wurden.

  Idealerweise wäre diese Zahl null, da Sie Apps nach dem Entstehen verwalten oder ignorieren würden. Anschließend sollten Sie die Anzahl der im Dashboard ermittelten Apps überwachen, um zu ermitteln, wann Entwickler neue Apps zu einem Cluster hinzufügen.

Cluster-Tile

Die Kachel **Cluster** bietet ähnliche Details über die Integrität der Cluster, die Sie mit dem Astra Control Center verwalten, und Sie können detaillierte Informationen abrufen, wie Sie es mit einer App möglich sind.

Storage Back-Ends

Die Kachel **Storage Back-Ends** enthält Informationen, die Ihnen bei der Identifizierung des Zustands von Storage-Back-Ends helfen. Dazu gehören:

- Wie viele Storage-Back-Ends werden gemanagt
- Gibt an, ob diese gemanagten Backends gesund sind
- Gibt an, ob die Back-Ends vollständig geschützt sind
- Die Anzahl der Back-Ends, die zwar erkannt, aber noch nicht gemanagt werden.

Anzeigen des Systemzustands und der Details von Clustern

Nachdem Sie Cluster hinzugefügt haben, die von Astra Control Center gemanagt werden können, können Sie Details zum Cluster anzeigen, beispielsweise den Speicherort, die Worker-Nodes, die persistenten Volumes und die Storage-Klassen.

Schritte

1. Wählen Sie in der Astra Control Center-Benutzeroberfläche **Cluster** aus.
2. Wählen Sie auf der Seite **Cluster** den Cluster aus, dessen Details Sie anzeigen möchten.
3. Zeigen Sie die Informationen auf den Registerkarten **Übersicht**, **Speicher** und **Aktivität** an, um die gewünschten Informationen zu finden.
   - **Übersicht**: Details zu den Arbeiterknoten, einschließlich ihres Status.
   - **Storage**: Die persistenten Volumes, die mit dem Computing verbunden sind, einschließlich der Speicherklasse und des Status.
   - **Aktivität**: Zeigt die Aktivitäten im Zusammenhang mit dem Cluster an.

> Sie können auch Clusterinformationen anzeigen, die Sie über das Astra Control Center **Dashboard** starten. Auf der Registerkarte **Cluster** unter **Resource summary** können Sie die verwalteten Cluster auswählen, die Sie zur Seite **Cluster** führen. Nachdem Sie die Seite **Cluster** aufgerufen haben, befolgen Sie die oben beschriebenen Schritte.

Anzeigen des Funktionszustands und der Details einer App

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

Schritte

1. Wählen Sie in der Astra Control Center-Benutzeroberfläche **Apps** aus, und wählen Sie dann den Namen einer App aus.

2. Klicken Sie hier, um alle gewünschten Informationen zu finden:

Anwendungsstatus

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

App-Schutzstatus

Gibt den Status an, wie gut die App geschützt ist:

- **Vollständig geschützt**: Die App verfügt über einen aktiven Backup-Zeitplan und ein erfolgreiches Backup, das weniger als eine Woche alt ist
- **Teilweise geschützt**: Die App verfügt über einen aktiven Backup-Zeitplan, einen aktiven Snapshot-Zeitplan oder einen erfolgreichen Backup oder Snapshot
- **Ungeschützt**: Apps, die weder vollständig geschützt noch teilweise geschützt sind.

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

Überblick

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

Datensicherung

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

Storage

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

Ressourcen

Hiermit können Sie überprüfen, welche Ressourcen gesichert und gemanagt werden.

Aktivität

Zeigt die Aktivitäten im Zusammenhang mit der App an.

Sie können auch App-Informationen ab dem Astra Control Center **Dashboard** anzeigen. Auf der Registerkarte **Apps** unter **Resource summary** können Sie die verwalteten Apps auswählen, die Sie zur Seite **Apps** bringen. Nachdem Sie die Seite **Apps** aufgerufen haben, befolgen Sie die oben beschriebenen Schritte.

Konto verwalten

Benutzer managen

Sie können Benutzer Ihrer Astra Control Center-Installation über die Astra Control Center-Benutzeroberfläche

hinzufügen, entfernen und bearbeiten. Sie können die Astra UI oder verwenden "Das Astra API" Um Benutzer zu managen.

Benutzer hinzufügen

Kontoinhaber und -Administratoren können weitere Benutzer zur Installation des Astra Control Center hinzufügen.

Schritte

1. Klicken Sie im Navigationsbereich * Konto verwalten* auf **Konto**.
2. Wählen Sie die Registerkarte **Benutzer** aus.
3. Wählen Sie **Benutzer Hinzufügen**.
4. Geben Sie den Namen des Benutzers, die E-Mail-Adresse und ein temporäres Kennwort ein.

   Der Benutzer muss das Passwort bei der ersten Anmeldung ändern.

5. Wählen Sie eine Benutzerrolle mit den entsprechenden Systemberechtigungen aus.

   Jede Rolle bietet die folgenden Berechtigungen:

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

Passwörter verwalten

Sie können Passwörter für Benutzerkonten im Astra Control Center verwalten.

Passwort ändern

Sie können das Passwort Ihres Benutzerkontos jederzeit ändern.

Schritte

1. Klicken Sie auf das Symbol Benutzer oben rechts im Bildschirm.
2. Wählen Sie **Profil**.
3. Klicken Sie auf die Dropdown-Liste **Aktionen** und wählen Sie **Passwort ändern**.
4. Geben Sie ein Passwort ein, das den Anforderungen des Passworts entspricht.
5. Geben Sie das Kennwort zur Bestätigung erneut ein.
6. Klicken Sie auf **Passwort ändern**.

Kennwort eines anderen Benutzers zurücksetzen

Wenn Ihr Konto über Berechtigungen für die Administrator- oder Eigentümerrolle verfügt, können Sie Passwörter für andere Benutzerkonten sowie für Ihre eigenen zurücksetzen. Wenn Sie ein Kennwort zurücksetzen, weisen Sie ein temporäres Kennwort zu, das der Benutzer bei der Anmeldung ändern muss.

Schritte

1. Klicken Sie im Navigationsbereich * Konto verwalten* auf **Konto**.
2. Wählen Sie auf der Registerkarte **Benutzer** die Dropdown-Liste in der Spalte **Status** für den Benutzer aus.
3. Wählen Sie **Passwort Zurücksetzen**.
4. Geben Sie ein temporäres Kennwort ein, das den Anforderungen des Passworts entspricht.
5. Geben Sie das Kennwort zur Bestätigung erneut ein.

   Wenn sich der Benutzer beim nächsten Mal anmeldet, wird er aufgefordert, das Passwort zu ändern.

6. Klicken Sie auf **Passwort zurücksetzen**.

Ändern Sie die Rolle eines Benutzers

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

Schritte

1. Klicken Sie im Navigationsbereich * Konto verwalten* auf **Konto**.
2. Wählen Sie auf der Registerkarte **Benutzer** die Dropdown-Liste in der Spalte **Rolle** für den Benutzer aus.
3. Wählen Sie eine neue Rolle aus, und klicken Sie dann auf **Rolle ändern**, wenn Sie dazu aufgefordert werden.

Ergebnis

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

Benutzer entfernen

Benutzer mit der Eigentümer- oder Administratorrolle können jederzeit andere Benutzer aus dem Konto entfernen.

Schritte

1. Klicken Sie im Navigationsbereich * Konto verwalten* auf **Konto**.
2. Aktivieren Sie auf der Registerkarte **Benutzer** das Kontrollkästchen in der Zeile jedes Benutzers, den Sie entfernen möchten.
3. Klicken Sie auf **Aktionen** und wählen Sie **Benutzer entfernen**.
4. Wenn Sie aufgefordert werden, bestätigen Sie den Löschvorgang, indem Sie das Wort "Entfernen" eingeben und dann auf **Ja, Benutzer entfernen** klicken.

Ergebnis

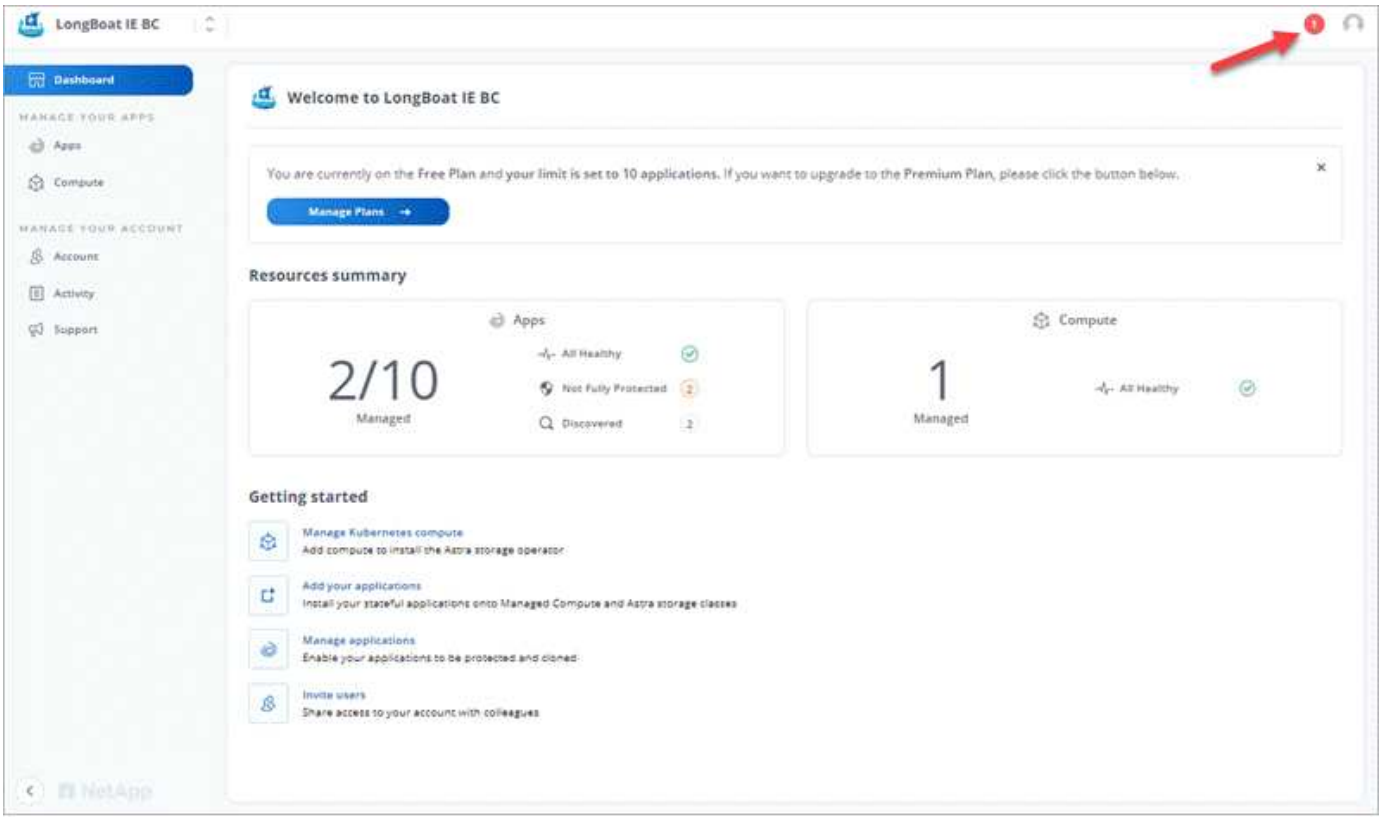
Astra Control Center entfernt den Benutzer aus dem Konto.

Anzeigen und Managen von Benachrichtigungen

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

Anwendung erfolgreich abgeschlossen wurde.

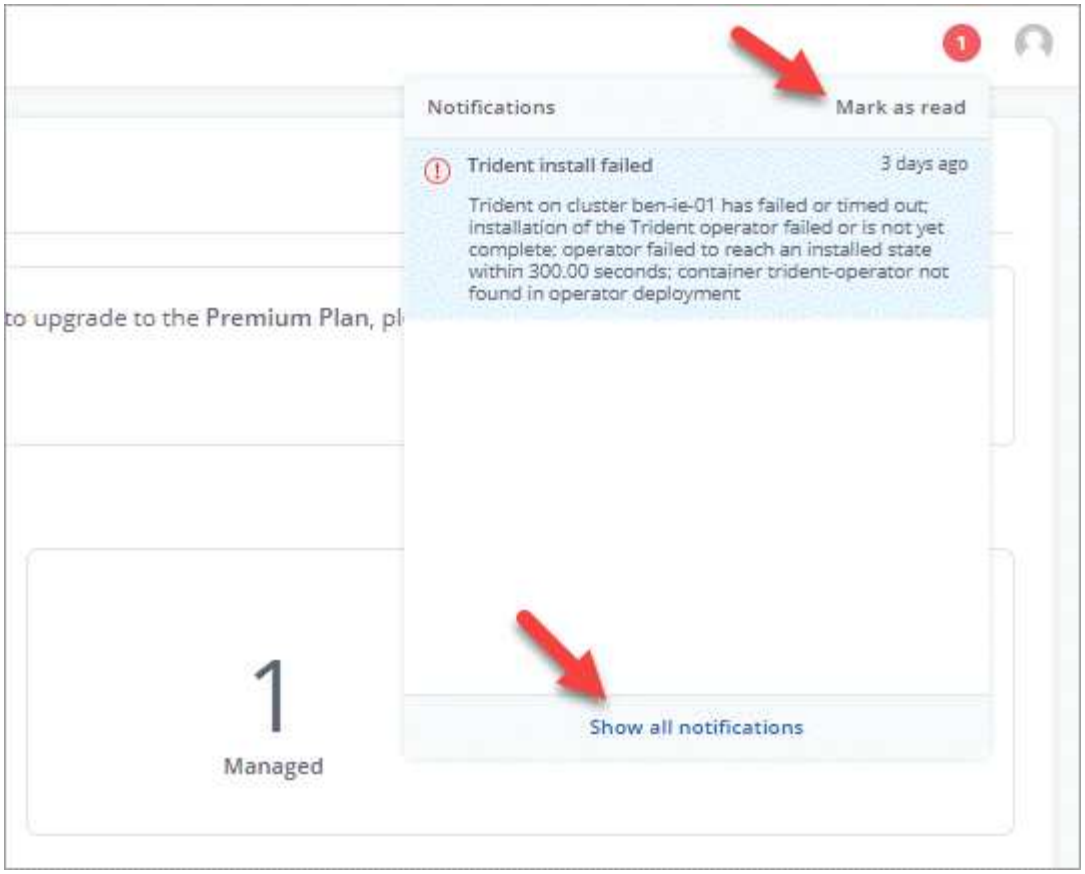
Die Anzahl der ungelesenen Benachrichtigungen ist oben rechts auf der Schnittstelle verfügbar:



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

Schritte

1. Klicken Sie oben rechts auf die Anzahl der ungelesenen Benachrichtigungen.



2. Überprüfen Sie die Benachrichtigungen und klicken Sie dann **als gelesen markieren** oder **Alle Benachrichtigungen anzeigen**.

   Wenn Sie auf **Alle Benachrichtigungen anzeigen** geklickt 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, klicken Sie auf **Aktion** und wählen Sie **als gelesen markieren**.

Anmeldeinformationen hinzufügen und entfernen

Fügen Sie Anmeldedaten für lokale Private-Cloud-Provider wie ONTAP S3, mit OpenShift gemanagte Kubernetes-Cluster oder nicht gemanagte Kubernetes-Cluster jederzeit in Ihrem Konto hinzu und entfernen Sie sie. Astra Control Center verwendet diese Zugangsdaten, um Kubernetes-Cluster und die Applikationen auf den Clustern zu erkennen und Ressourcen in Ihrem Auftrag bereitzustellen.

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

Anmeldedaten hinzufügen

Wenn Sie Cluster verwalten, können Sie Astra Control Center Anmeldeinformationen hinzufügen. Informationen zum Hinzufügen von Anmeldeinformationen durch Hinzufügen eines neuen Clusters finden Sie unter "Fügen Sie einen Kubernetes-Cluster hinzu".

Wenn Sie Ihre eigenen erstellen `kubeconfig` Datei, Sie sollten nur ein **ein**-Kontext-Element darin definieren. Siehe "Kubernetes-Dokumentation" Weitere Informationen zum Erstellen `kubeconfig` Dateien:

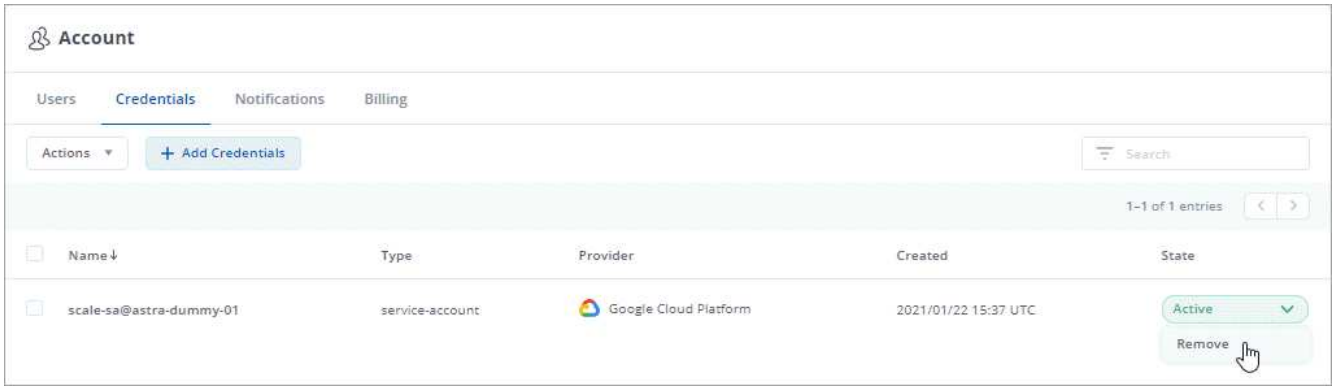
Anmeldedaten entfernen

Entfernen Sie die Anmeldeinformationen jederzeit aus einem Konto. Sie sollten erst nach dem Entfernen von Anmeldeinformationen verwenden "Verwalten aller zugehörigen Cluster wird aufgehoben".

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

Schritte

1. Klicken Sie Auf **Konto > Anmeldeinformationen**.
2. Klicken Sie in der Spalte **Status** auf die Dropdown-Liste für die Anmeldeinformationen, die Sie entfernen möchten.
3. Klicken Sie Auf **Entfernen**.



4. Geben Sie das Wort „Entfernen“ ein, um das Löschen zu bestätigen, und klicken Sie dann auf **Ja, Anmeldedaten entfernen**.

Ergebnis

Astra Control Center entfernt die Anmeldeinformationen aus dem Konto.

Aktualisieren einer vorhandenen Lizenz

Sie können eine Evaluierungslizenz in eine vollständige Lizenz umwandeln oder eine bestehende Evaluierung oder Volllizenz mit einer neuen Lizenz aktualisieren. Wenn Sie keine vollständige Lizenz besitzen, wenden Sie sich an Ihren NetApp Ansprechpartner, um eine vollständige Lizenz und eine Seriennummer zu erhalten. Sie können die Astra UI oder verwenden "Das Astra API" Um eine vorhandene Lizenz zu aktualisieren.

Schritte

1. Loggen Sie sich auf der NetApp Support Site ein.
2. Rufen Sie die Download-Seite des Astra Control Center auf, geben Sie die Seriennummer ein und laden Sie die vollständige NetApp Lizenzdatei (NLF) herunter.
3. Melden Sie sich in der UI des Astra Control Center an.

4. Wählen Sie in der linken Navigationsleiste **Konto** > **Lizenz**.
5. Klicken Sie auf der Seite **Konto** > **Lizenz** auf das Dropdown-Menü Status der vorhandenen Lizenz und wählen Sie **Replace**.
6. Navigieren Sie zu der Lizenzdatei, die Sie heruntergeladen haben.
7. Wählen Sie **Hinzufügen**.

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

Buckets verwalten

Ein Objektspeicher-Bucket-Provider ist äußerst wichtig, wenn Sie Ihre Applikationen und Ihren persistenten Storage sichern möchten oder Applikationen über Cluster hinweg klonen möchten. Fügen Sie mithilfe des Astra Control Center einen Objektspeicher-Provider als externes Backup-Ziel für Ihre Applikationen hinzu.

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

Nutzen Sie einen der folgenden Bucket-Provider:

- NetApp ONTAP S3
- NetApp StorageGRID S3
- Allgemein S3

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

Ein Bucket kann nicht gelöscht werden, Sie können ihn jedoch bearbeiten.

Ein Bucket kann sich in einem dieser Zustände befinden:

- Ausstehend: Der Bucket ist für die Erkennung geplant.
- Verfügbar: Der Bucket ist zur Verwendung verfügbar.
- Entfernt: Auf den Bucket ist derzeit nicht zugegriffen werden können.

Anweisungen zum Verwalten von Buckets mithilfe der Astra API finden Sie im "Astra Automation und API-Informationen".

Sie können die folgenden Aufgaben zum Verwalten von Buckets ausführen:

- "Fügen Sie einen Bucket hinzu"
- Bearbeiten eines Buckets

> S3 Buckets im Astra Control Center berichten nicht über die verfügbare Kapazität. Bevor Sie Backups oder Klonanwendungen durchführen, die von Astra Control Center gemanagt werden, sollten Sie die Bucket-Informationen im ONTAP oder StorageGRID Managementsystem prüfen.

Anmeldedaten entfernen

Entfernen Sie jederzeit S3-Anmeldeinformationen mithilfe der Astra Control API aus einem Konto.

Weitere Informationen finden Sie unter "Verwenden Sie die Astra Control API".

Der erste Satz von Anmeldeinformationen, die Sie Astra Control hinzufügen, wird immer verwendet, da Astra Control zur Authentifizierung des Backup-Buckets die Zugangsdaten verwendet. Es ist am besten, diese Anmeldeinformationen nicht zu entfernen.

Bearbeiten eines Buckets

Sie können die Zugangsdaten für einen Bucket ändern und ändern, ob ein ausgewählter Bucket der Standard-Bucket ist.

Wenn Sie einen Bucket hinzufügen, wählen Sie den richtigen Bucket-Provider-Typ mit den Zugangsdaten aus, die für diesen Provider korrekt sind. Die UI akzeptiert beispielsweise NetApp ONTAP S3 als Typ mit StorageGRID Zugangsdaten. Dies führt jedoch dazu, dass alle künftigen Applikations-Backups und -Wiederherstellungen mit diesem Bucket fehlschlagen. Siehe "Versionshinweise".

Schritte

1. Wählen Sie in der linken Navigationsleiste **Buckets** aus.
2. Wählen Sie im Menü Aktionen die Option **Bearbeiten**.
3. Ändern Sie alle Informationen außer dem Bucket-Typ.

   Sie können den Bucket-Typ nicht ändern.

4. Wählen Sie **Aktualisieren**.

Weitere Informationen

- "Verwenden Sie die Astra API"

Management des Storage-Backends

Durch das Management von Storage-Clustern in Astra Control als Storage-Backend können Sie Verbindungen zwischen persistenten Volumes (PVS) und dem Storage-Backend sowie zusätzliche Storage-Kennzahlen abrufen. Sie können Storage-Kapazität und -Integritätsdetails überwachen, beispielsweise die Performance, wenn Astra Control Center mit Cloud Insights verbunden ist.

Anweisungen zum Managen von Storage-Back-Ends mit der Astra API finden Sie im "Astra Automation und API-Informationen".

Sie können die folgenden Aufgaben zur Verwaltung eines Storage-Backends ausführen:

- "Fügen Sie ein Storage-Back-End hinzu"
- Details zum Storage-Back-End
- Unmanagement eines Storage-Backends

Details zum Storage-Back-End

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

Details zum Storage-Back-End können Sie über das Dashboard anzeigen

Schritte

1. Wählen Sie in der linken Navigationsleiste **Dashboard** aus.
2. Überprüfen Sie den Abschnitt Storage Backend, der den Status anzeigt:
   - **Ungesund**: Die Lagerung befindet sich nicht im optimalen Zustand. Dies kann durch ein Latenzproblem oder eine Applikation aufgrund eines Container-Problems, z. B., beeinträchtigt sein.
   - **Alles gesund**: Die Lagerung wurde verwaltet und ist in einem optimalen Zustand.
   - **Entdeckt**: Der Speicher wurde entdeckt, aber nicht von Astra Control verwaltet.

Details zum Speicher-Backend über die Option „Backend“ anzeigen

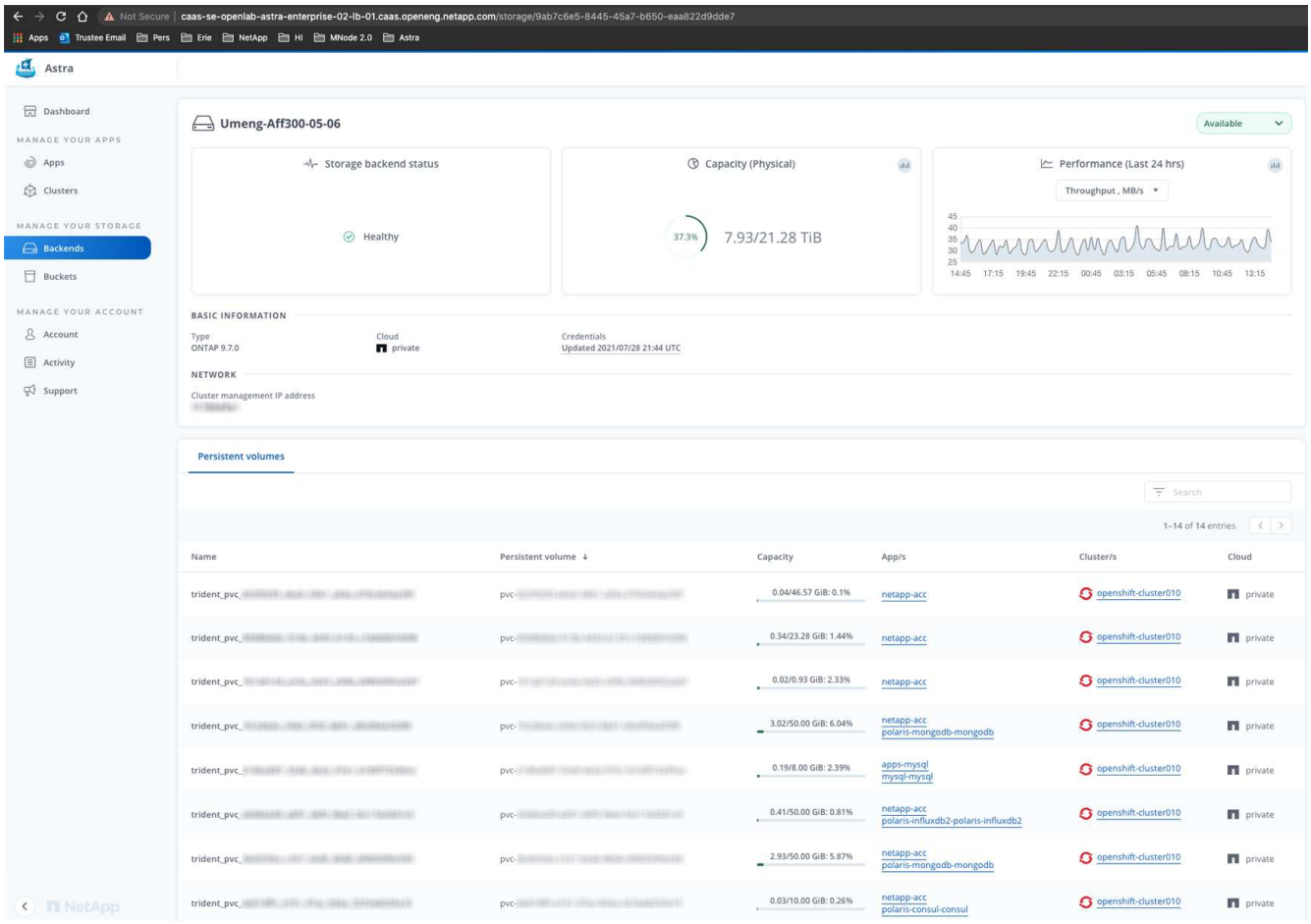
Informationen zum Zustand, Kapazität und Performance des Backend (IOPS-Durchsatz und/oder Latenz)

Bei der Verbindung zu Cloud Insights sehen Sie die Volumes, die die Kubernetes-Apps verwenden, die in einem ausgewählten Storage-Back-End gespeichert sind.

Schritte

1. Wählen Sie im linken Navigationsbereich **Backend** aus.
2. Wählen Sie das Storage-Back-End aus.

Wenn Sie eine Verbindung zum NetApp Cloud Insights hergestellt haben, werden auf der Seite „Back-Ends“ Auszüge aus Cloud Insights angezeigt.



3. Um direkt zu Cloud Insights zu gelangen, klicken Sie neben dem Kennzahlenbild auf das Symbol **Cloud Insights**.

Unmanagement eines Storage-Backends

Sie können das Backend verwalten.

Schritte

1. Wählen Sie in der linken Navigationsleiste **Backend** aus.
2. Wählen Sie den Back-End-Speicher aus.
3. Wählen Sie im Menü Aktionen die Option **Verwaltung aufheben** aus.
4. Geben Sie „unmanage“ ein, um das Entfernen zu bestätigen.
5. Wählen Sie **Ja, Speicher-Backend entfernen**.

Weitere Informationen

- "Verwenden Sie die Astra API"

Überwachung und Sicherung der Infrastruktur

Sie können mehrere optionale Einstellungen konfigurieren, um Ihre Astra Control Center-Erfahrung zu verbessern. Wenn das Netzwerk, in dem Astra Control Center ausgeführt wird, einen Proxy für die Verbindung zum Internet benötigt (um Support-Bundles auf die NetApp Support Site hochzuladen oder eine Verbindung zu

Cloud Insights herzustellen), sollten Sie einen Proxy-Server im Astra Control Center konfigurieren. Um Ihre gesamte Infrastruktur zu überwachen und Erkenntnisse zu erhalten, verwenden Sie eine Verbindung zu NetApp Cloud Insights. Um Kubernetes-Ereignisse von Systemen zu erfassen, die vom Astra Control Center überwacht werden, fügen Sie eine Fluentd-Verbindung hinzu.

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

Fügen Sie einen Proxyserver hinzu

Wenn das Netzwerk, in dem Astra Control Center ausgeführt wird, einen Proxy für die Verbindung zum Internet benötigt (um Support-Bundles auf die NetApp Support Site hochzuladen oder eine Verbindung zu Cloud Insights herzustellen), sollten Sie einen Proxy-Server im Astra Control Center konfigurieren.

Astra Control Center überprüft nicht die von Ihnen eingegebenen Details für Ihren Proxy-Server. Stellen Sie sicher, dass Sie die richtigen Werte eingeben.

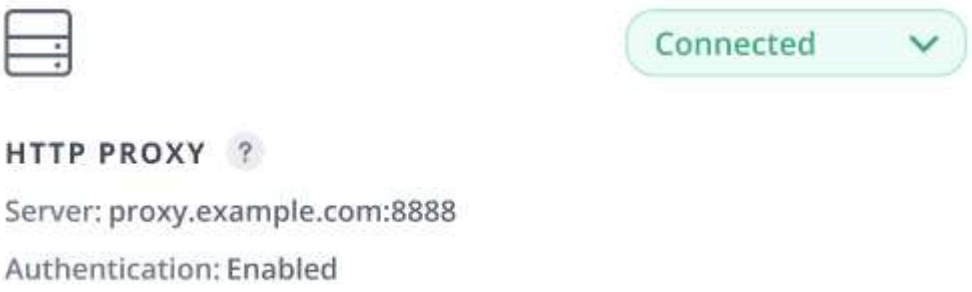
Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Verbinden** aus, um einen Proxyserver hinzuzufügen.

4. Geben Sie den Proxy-Servernamen oder die IP-Adresse und die Proxy-Portnummer ein.
5. Wenn Ihr Proxy-Server eine Authentifizierung erfordert, aktivieren Sie das Kontrollkästchen, und geben Sie den Benutzernamen und das Kennwort ein.
6. Wählen Sie **Verbinden**.

Ergebnis

Wenn die eingegebenen Proxydaten gespeichert wurden, zeigt der Abschnitt **HTTP Proxy** der Seite **Konto** > **Verbindungen** an, dass sie verbunden sind, und zeigt den Servernamen an.



Proxy-Server-Einstellungen bearbeiten

Sie können die Proxy-Server-Einstellungen bearbeiten.

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Bearbeiten** aus, um die Verbindung zu bearbeiten.
4. Bearbeiten Sie die Serverdetails und die Authentifizierungsinformationen.
5. Wählen Sie **Speichern**.

Deaktivieren Sie die Proxy-Serververbindung

Sie können die Proxy-Server-Verbindung deaktivieren. Bevor Sie diese Option deaktivieren, werden Sie gewarnt, dass mögliche Unterbrechungen bei anderen Verbindungen auftreten können.

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Trennen** aus, um die Verbindung zu deaktivieren.
4. Bestätigen Sie im Dialogfeld, das geöffnet wird, den Vorgang.

Verbinden Sie sich mit Cloud Insights

Überwachen Sie Ihre komplette Infrastruktur, und verschaffen Sie sich so einen Überblick über Ihre komplette Infrastruktur. Verbinden Sie NetApp Cloud Insights mit Ihrer Astra Control Center Instanz. Cloud Insights ist in Ihrer Astra Control Center-Lizenz enthalten.

Cloud Insights sollte über das Netzwerk, das Astra Control Center verwendet, oder indirekt über einen Proxy-Server zugänglich sein.

Wenn Astra Control Center mit Cloud Insights verbunden ist, wird ein Pod für die Akquisitionseinheit erstellt. Dieser POD sammelt Daten aus den Storage-Back-Ends, die vom Astra Control Center gemanagt werden, und schiebt diese an Cloud Insights. Dieser POD benötigt 8 GB RAM und 2 CPU-Kerne.

Was Sie benötigen

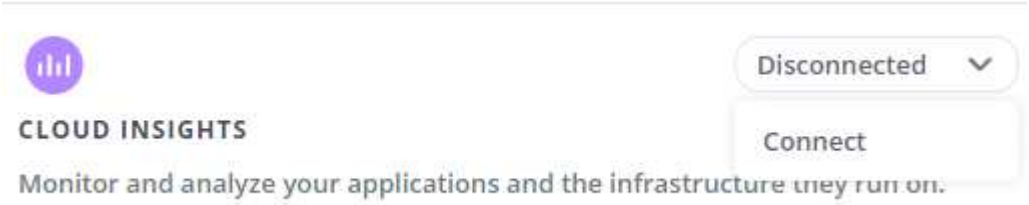
- Ein Astra Control Center-Konto mit **admin**/**Owner** Privilegien.
- Eine gültige Astra Control Center-Lizenz.
- Ein Proxy-Server, wenn das Netzwerk, in dem Sie Astra Control Center verwenden, einen Proxy für die Verbindung zum Internet benötigt.

Falls Sie neu bei Cloud Insights sind, sollten Sie sich mit den Funktionen und Features vertraut machen "Hier".

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.

2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Verbinden**, wo es **getrennt** angezeigt wird, um die Verbindung hinzuzufügen.



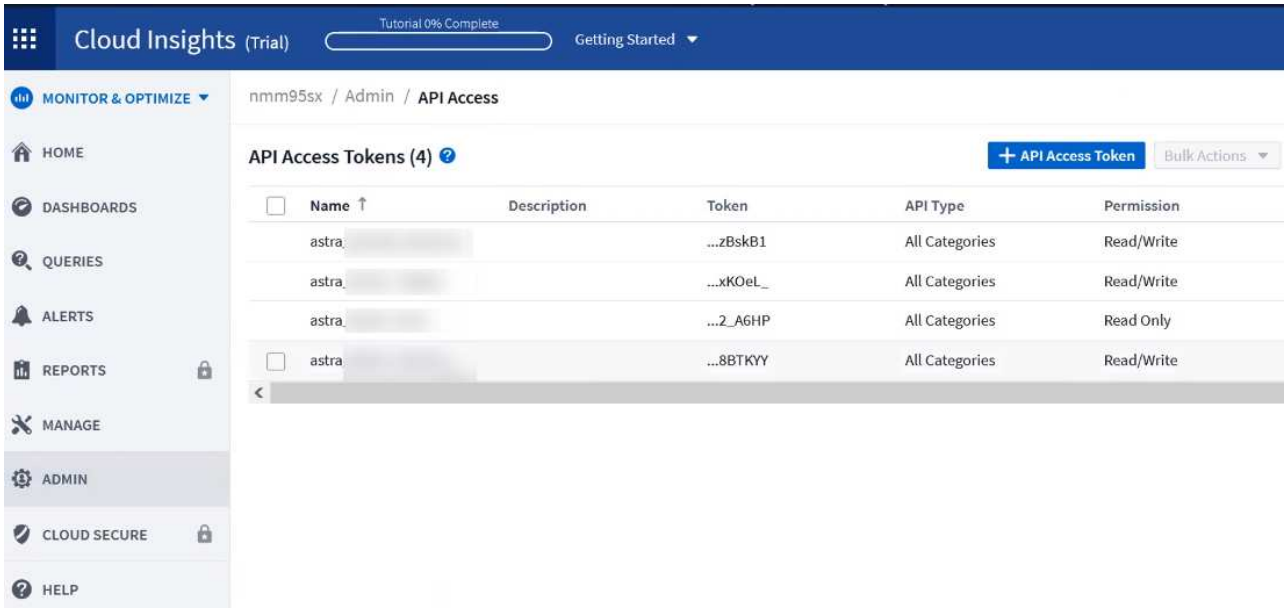
4. Geben Sie die Cloud Insights-API-Token und die Mandanten-URL ein. Die Mandanten-URL weist beispielsweise das folgende Format auf:

```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

Sie erhalten die Mandanten-URL, wenn Sie die Cloud Insights-Lizenz erhalten. Wenn die Mandanten-URL nicht vorhanden ist, lesen Sie den "Cloud Insights-Dokumentation".

a. Um die zu bekommen "API-Token", Loggen Sie sich bei Ihrer Cloud Insights-Mandanten-URL ein.

b. Generieren Sie in Cloud Insights ein API-Token vom Typ **schreibgeschützt**.



c. Kopieren Sie die Taste * nur Lesen*. Sie müssen es in das Fenster Astra Control Center einfügen, um die Cloud Insights-Verbindung zu aktivieren.

d. Generieren Sie in Cloud Insights ein API-Token vom Typ **Lesen/Schreiben**.

e. Kopieren Sie die Taste **Lesen/Schreiben**. Sie müssen es in das Astra Control Center **Connect Cloud Insights** Fenster einfügen.

Wir empfehlen Ihnen, einen **Read Only**-Schlüssel und einen **Read/Write**-Schlüssel zu generieren und nicht den gleichen Schlüssel für beide Zwecke zu verwenden. Standardmäßig ist der Ablauf des Tokens auf ein Jahr festgelegt. Wir empfehlen, dass Sie die Standardauswahl beibehalten, um dem Token die maximale Dauer zu geben, bevor es abläuft. Wenn Ihr Token abläuft, wird die Telemetrie angehalten.

f. Fügen Sie die Tasten ein, die Sie von Cloud Insights in Astra Control Center kopiert haben.

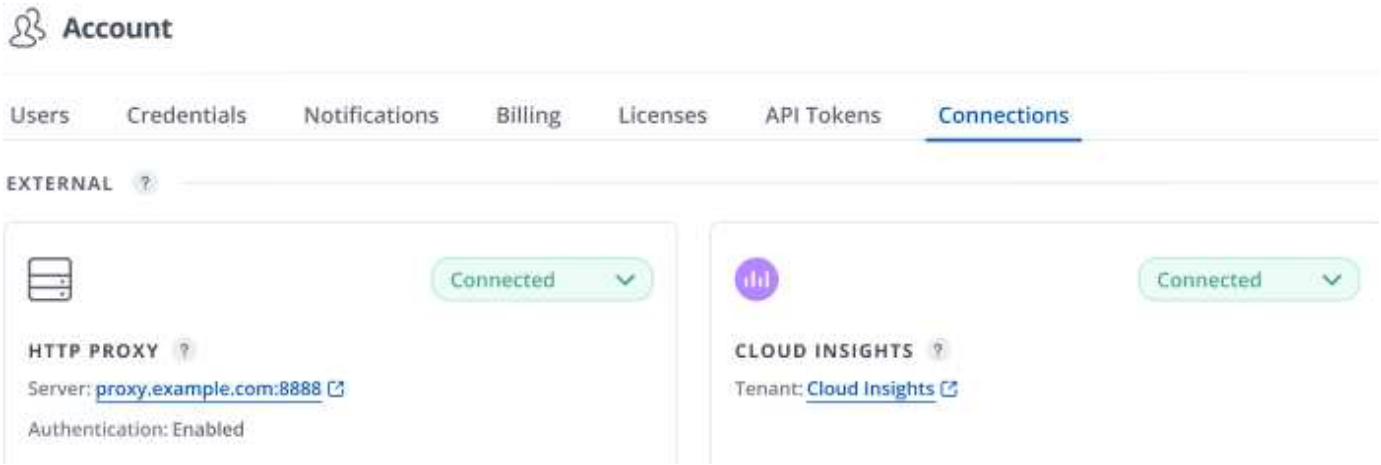
5. Wählen Sie **Verbinden**.

Nach der Auswahl von **Verbinden** ändert sich der Status der Verbindung auf der Seite **Konto** > **Verbindungen** auf der Seite **Cloud Insights** auf **ausstehend**. Es kann einige Minuten dauern, bis die Verbindung aktiviert ist und der Status auf **verbunden** geändert wird.

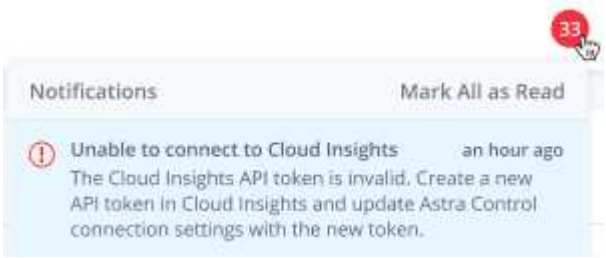
Um zwischen dem Astra Control Center und den Cloud Insights UIs hin und her zu gehen, stellen Sie sicher, dass Sie bei beiden angemeldet sind.

Daten im Cloud Insights anzeigen

Wenn die Verbindung erfolgreich war, zeigt der Abschnitt **Cloud Insights** auf der Seite **Konto** > **Verbindungen** an, dass sie verbunden ist, und zeigt die Mandanten-URL an. Sie können Cloud Insights besuchen, um zu sehen, dass Daten erfolgreich empfangen und angezeigt werden.



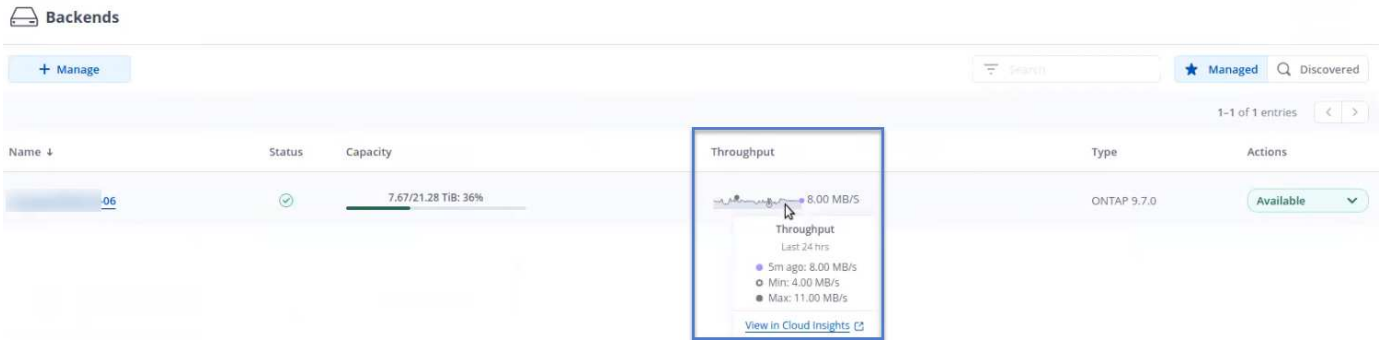
Wenn die Verbindung aus irgendeinem Grund fehlgeschlagen ist, wird im Status **failed** angezeigt. Den Grund für Fehlschlag finden Sie unter **Benachrichtigungen** auf der rechten oberen Seite des UI.



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

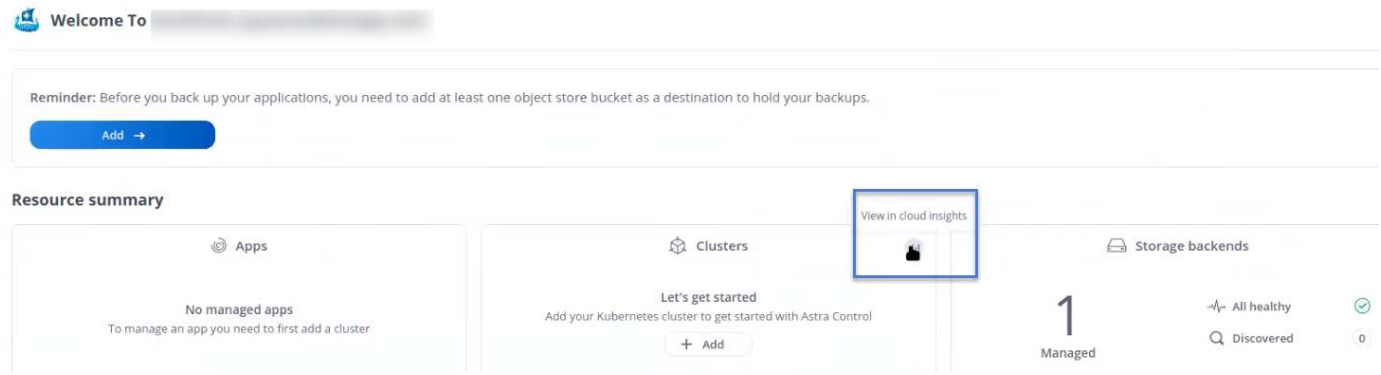
Vom Astra Control Center können Sie Durchsatzinformationen auf der Seite **Backend** anzeigen sowie von hier aus eine Verbindung zu Cloud Insights herstellen, nachdem Sie ein Storage-Backend ausgewählt

haben.



Um direkt zu Cloud Insights zu gelangen, wählen Sie neben dem Kennzahlenbild das Symbol **Cloud Insights** aus.

Die Informationen finden Sie auch auf dem **Dashboard**.



> Wenn Sie nach Aktivierung der Cloud Insights-Verbindung die Back-Ends entfernen, die Sie im Astra Control Center hinzugefügt haben, werden die Back-Ends nicht mehr an Cloud Insights gemeldet.

Cloud Insights-Verbindung bearbeiten

Sie können die Cloud Insights-Verbindung bearbeiten.

> Sie können nur die API-Schlüssel bearbeiten. Um die Cloud Insights-Mandanten-URL zu ändern, sollten Sie die Cloud Insights-Verbindung trennen und eine Verbindung mit der neuen URL herstellen.

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Bearbeiten** aus, um die Verbindung zu bearbeiten.
4. Bearbeiten Sie die Cloud Insights-Verbindungseinstellungen.
5. Wählen Sie **Speichern**.

Deaktivieren Sie die Cloud Insights-Verbindung

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

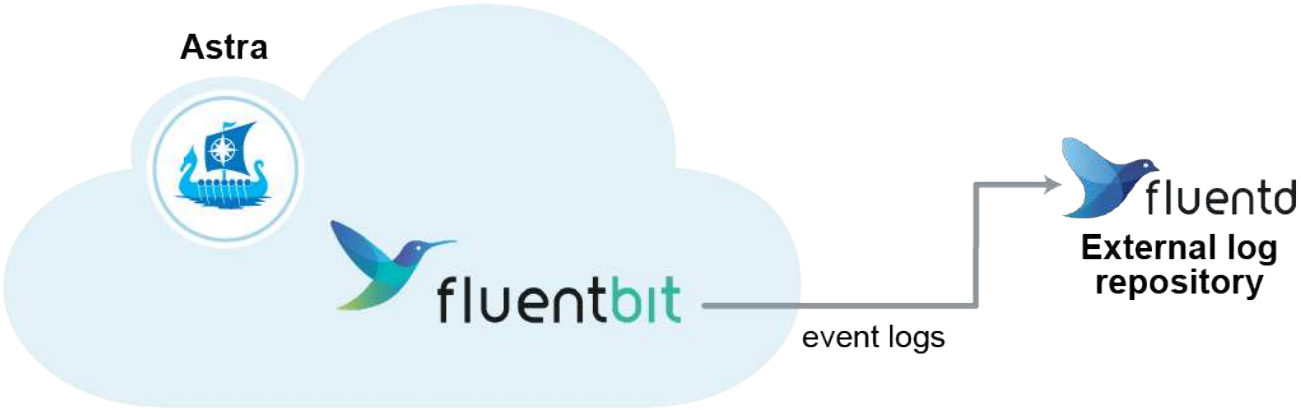
Insights hochgeladenen Telemetriedaten nicht gelöscht.

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Trennen** aus, um die Verbindung zu deaktivieren.
4. Bestätigen Sie im Dialogfeld, das geöffnet wird, den Vorgang. Nachdem Sie den Vorgang bestätigt haben, ändert sich der Cloud Insights-Status auf der Seite **Konto** > **Verbindungen** in **Ausstehend**. Es dauert ein paar Minuten, bis der Status in **nicht verbunden** geändert wird.

Mit Fluentd verbinden

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



Nur die Ereignisprotokolle von verwalteten Clustern werden an Fluentd weitergeleitet.

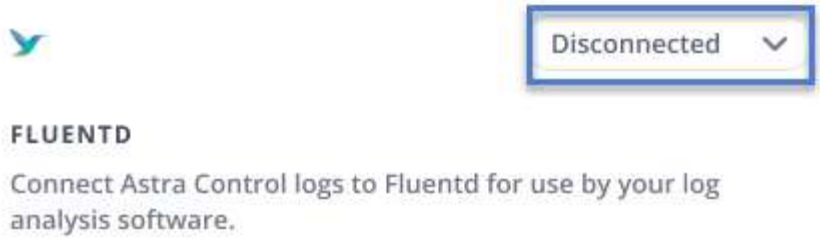
Was Sie benötigen

- Ein Astra Control Center-Konto mit **admin**/**Owner** Privilegien.
- Astra Control Center ist auf einem Kubernetes-Cluster installiert und läuft.

Astra Control Center überprüft nicht die Details, die Sie für Ihren Fluentd-Server eingeben. Stellen Sie sicher, dass Sie die richtigen Werte eingeben.

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **nicht verbunden** aus, um die Verbindung hinzuzufügen.



4. Geben Sie die Host-IP-Adresse, die Portnummer und den freigegebenen Schlüssel für Ihren Fluentd-Server ein.
5. Wählen Sie **Verbinden**.

Ergebnis

Wenn die für den Fluentd-Server eingegebenen Details gespeichert wurden, zeigt der Abschnitt **Fluentd** auf der Seite **Konto** > **Verbindungen** an, dass er verbunden ist. Jetzt können Sie den Fluentd-Server besuchen, mit dem Sie verbunden sind, und die Ereignisprotokolle anzeigen.

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

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

Wenn Sie Probleme mit der Protokollerfassung haben, sollten Sie sich bei Ihrem Worker-Knoten anmelden und sicherstellen, dass Ihre Protokolle in verfügbar sind `/var/log/containers/`.

Bearbeiten Sie die Fluentd-Verbindung

Sie können die Fluentd-Verbindung zu Ihrer Astra Control Center-Instanz bearbeiten.

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Bearbeiten** aus, um die Verbindung zu bearbeiten.
4. Ändern Sie die Einstellungen für den Fluentd-Endpunkt.
5. Wählen Sie **Speichern**.

Deaktivieren Sie die Fluentd-Verbindung

Sie können die Fluentd-Verbindung zu Ihrer Astra Control Center-Instanz deaktivieren.

Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin**/**Owner**-Berechtigung an.
2. Wählen Sie **Konto** > **Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Trennen** aus, um die Verbindung zu deaktivieren.
4. Bestätigen Sie im Dialogfeld, das geöffnet wird, den Vorgang.

Aktualisieren einer vorhandenen Lizenz

Sie können eine Evaluierungslizenz in eine vollständige Lizenz umwandeln oder eine bestehende Evaluierung oder Volllizenz mit einer neuen Lizenz aktualisieren. Wenn Sie keine vollständige Lizenz besitzen, wenden Sie sich an Ihren NetApp Ansprechpartner, um eine vollständige Lizenz und eine Seriennummer zu erhalten. Sie können die Astra UI oder verwenden "Das Astra API" Um eine vorhandene Lizenz zu aktualisieren.

Schritte

1. Loggen Sie sich auf der NetApp Support Site ein.
2. Rufen Sie die Download-Seite des Astra Control Center auf, geben Sie die Seriennummer ein und laden Sie die vollständige NetApp Lizenzdatei (NLF) herunter.
3. Melden Sie sich in der UI des Astra Control Center an.
4. Wählen Sie in der linken Navigationsleiste **Konto** > **Lizenz**.
5. Klicken Sie auf der Seite **Konto** > **Lizenz** auf das Dropdown-Menü Status der vorhandenen Lizenz und wählen Sie **Replace**.
6. Navigieren Sie zu der Lizenzdatei, die Sie heruntergeladen haben.
7. Wählen Sie **Hinzufügen**.

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

Heben Sie das Management von Applikationen und Clustern auf

Entfernen Sie alle Apps oder Cluster, die Sie nicht mehr über das Astra Control Center managen möchten.

Verwaltung einer Anwendung aufheben

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

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

Schritte

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

Ergebnis

Astra Control Center beendet die Verwaltung der App.

Aufheben des Managements eines Clusters

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

- Dadurch wird das Management des Clusters durch das Astra Control Center verhindert. Die Konfiguration des Clusters ändert sich nicht, und das Cluster wird nicht gelöscht.
- Trident wird nicht vom Cluster deinstalliert. "Lesen Sie, wie Trident deinstalliert wird".

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

Schritte

1. Wählen Sie in der linken Navigationsleiste **Cluster** aus.
2. Aktivieren Sie das Kontrollkästchen für den Cluster, den Sie in Astra Control Center nicht mehr verwalten möchten.
3. Wählen Sie im Menü **Aktionen** die Option **nicht verwalten**.
4. Bestätigen Sie, dass Sie die Verwaltung des Clusters aufheben möchten und wählen Sie dann **Ja, Cluster verwalten** aus.

Ergebnis

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

> **Wenn Astra Control Center und Cloud Insights nicht verbunden sind**, entfernt die Unverwaltung des Clusters alle Ressourcen, die zum Senden von Telemetriedaten installiert wurden. **Wenn Astra Control Center und Cloud Insights verbunden sind**, löscht die Entsteuerung des Clusters nur das `fluentbit` Und `event-exporter` Behälter.

Deinstallieren Sie Astra Control Center

Möglicherweise müssen Sie die Komponenten des Astra Control Center entfernen, wenn Sie ein Upgrade von einer Testversion auf eine Vollversion des Produkts durchführen. Um Astra Control Center und den Astra Control Center Operator zu entfernen, führen Sie die in diesem Verfahren beschriebenen Befehle nacheinander aus.

Was Sie benötigen

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

Schritte

1. Löschen Sie Das Astra Control Center. Der folgende Beispielbefehl basiert auf einer Standardinstallation. Ändern Sie den Befehl, wenn Sie benutzerdefinierte Konfigurationen erstellt haben.

   ```
   kubectl delete -f astra_control_center_min.yaml -n netapp-acc
   ```

   Ergebnis:

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

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

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

Ergebnis:

```
namespace "netapp-acc" deleted
```

3. Löschen Sie die Komponenten des Astra Control Center-Bedienersystems mit dem folgenden Befehl:

```
kubectl delete -f astra_control_center_operator_deploy.yaml
```

Ergebnis:

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

Weitere Informationen

- "Bekannte Probleme bei der Deinstallation"