



Applikationsmanagement

Astra Control Center

NetApp

November 21, 2023

Inhalt

- Applikationsmanagement 1
 - Starten Sie das Anwendungsmanagement 1
 - Definieren Sie ein Beispiel für eine benutzerdefinierte Anwendung 5

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.

Weitere Informationen finden Sie unter ["Anforderungen für das Applikationsmanagement"](#).

Unterstützte Installationsmethoden für Anwendungen

Astra Control unterstützt folgende Installationsmethoden für Anwendungen:

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

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

- **Helm 3:** Wenn Sie Helm zur Installation von Apps verwenden, benötigt Astra Control Helm Version 3. Das Management und Klonen von Apps, die mit Helm 3 installiert sind (oder ein Upgrade von Helm 2 auf Helm 3), werden vollständig unterstützt. Das Verwalten von mit Helm 2 installierten Apps wird nicht unterstützt.
- **Vom Betreiber bereitgestellte Apps:** Astra Control unterstützt Apps, die mit Betreibern mit Namespace-Scoped installiert sind. Diese Betreiber sind in der Regel mit einer "Pass-by-Value"-Architektur statt "Pass-by-reference"-Architektur ausgelegt. Im Folgenden sind einige Bedieneranwendungen aufgeführt, die folgende Muster befolgen:
 - ["Apache K8ssandra"](#)
 - ["Jenkins CI"](#)
 - ["Percona XtraDB Cluster"](#)

Astra Control ist möglicherweise nicht in der Lage, einen Operator zu klonen, der mit einer „Pass-by-reference“-Architektur entworfen wurde (z. B. der CockroachDB-Operator). Während dieser Art von Klonvorgängen versucht der geklonte Operator, Kubernetes Secrets vom Quelloperator zu beziehen, obwohl er im Zuge des Klonens ein eigenes neues Geheimnis hat. Der Klonvorgang kann fehlschlagen, da Astra Control die Kubernetes-Geheimnisse im Quelloperator nicht kennt.



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.

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 installierte 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 Control 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 **Anwendungen**.
2. Wählen Sie den Filter * entdeckt* aus.



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 Optionen in der Spalte **Aktionen** die Option **Verwalten** aus.
7. Wenn Sie keine App verwalten möchten, wählen Sie im Menü Optionen in der Spalte **Aktionen** 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.



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.

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 **Anwendungen**.
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 die Anzahl der Beschriftungen auswählen.
 - 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. Wählen Sie **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 **Anwendungen**.
2. Wählen Sie als Filter * entdeckt* aus.
3. Wählen Sie die App aus.
4. Wählen Sie im Menü Optionen in der Spalte **Aktionen** die Option **Ignorieren** aus.
5. Um das ignorieren rückgängig zu machen, wählen Sie **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.

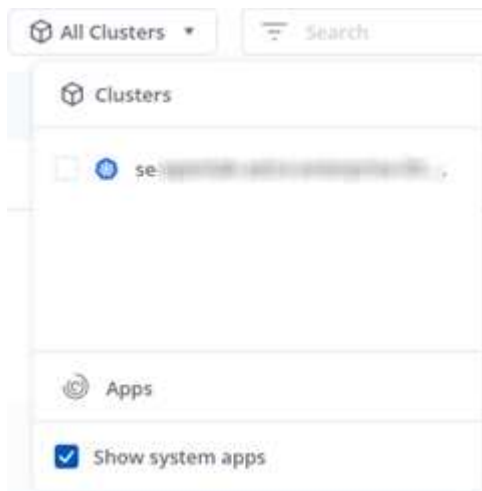
Schritte

1. Wählen Sie in der linken Navigationsleiste die Option **Anwendungen**.
2. Wählen Sie als Filter * verwaltet* aus.
3. Wählen Sie die App aus.
4. Wählen Sie im Menü Optionen in der Spalte **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. Wir zeigen Ihnen diese System-Apps standardmäßig nicht, da es selten ist, dass Sie sie sichern müssen.

Sie können Systemanwendungen auf der Seite Anwendungen anzeigen, indem Sie das Kontrollkästchen Systemanwendungen anzeigen* unter dem Filter Cluster in der Symbolleiste aktivieren.



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.

Weitere Informationen

- ["Verwenden Sie die Astra Control API"](#)

Definieren Sie ein Beispiel für eine benutzerdefinierte Anwendung

Wenn Sie eine benutzerdefinierte App erstellen, können Sie Elemente Ihres Kubernetes-Clusters zu einer einzelnen App gruppieren. Diese Sammlung von Kubernetes-Ressourcen basiert auf einem Namespace und einem Etikett.

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.



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.

Was Sie benötigen

- Astra Control ist ein Cluster

Schritte

1. Wählen Sie auf der Seite Apps die Option **+ Definieren** aus.

Im Fenster Benutzerdefinierte App wird angezeigt, 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.

2. Geben Sie im Popup-Fenster den App-Namen ein, wählen Sie den Cluster im Dropdown-Menü **Cluster** aus und wählen Sie den Namespace der App aus der Dropdown-Liste **Namespace** aus.
3. Wählen Sie aus der Dropdown-Liste **Label** eine Bezeichnung für die Apps und den Namespace aus.
4. Nachdem Sie die benutzerdefinierte Applikation für eine Implementierung definiert haben, wiederholen Sie den Prozess für andere Implementierungen je nach Bedarf.

Wenn Sie die Erstellung der beiden benutzerdefinierten Apps abgeschlossen haben, können Sie diese Ressourcen wie jede andere Astra Control Anwendung behandeln. Sie können sie klonen, Backups und Snapshots erstellen und für jede Gruppe von Ressourcen auf der Basis der Kubernetes-Labels eine individuelle Sicherungsrichtlinie erstellen.

Beispiel: Separate Sicherungsrichtlinie für verschiedene Versionen

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 "Stable"-Version. Hierdurch werden Backups, Snapshots und Klonvorgänge für die beiden Gruppen von Kubernetes-Objekten getrennt.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.