Konzepte

Astra Control Center

NetApp
November 21, 2023

This PDF was generated from https://docs.netapp.com/de-de/astra-control-center-2204/concepts/intro.html on November 21, 2023. Always check docs.netapp.com for the latest.

Inhalt

Konzepte . . . 1
Weitere Informationen zu Astra Control . . . 1
Architektur und Komponenten . . . 4
Datensicherung . . . 6
Lizenzierung . . . 7
Validiert gegenüber Standard-Applikationen . . . 8
Storage-Klassen und persistente Volume-Größe . . . 9
Benutzerrollen und Namespaces . . . 9

Konzepte

Weitere Informationen zu Astra Control

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

Funktionen

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

- Automatisches Management von persistentem Storage
- Erstellen Sie applikationsorientierte Snapshots und Backups nach Bedarf
- Automatisierung von richtlinienbasierten Snapshot- und Backup-Vorgängen
- Migrieren Sie Applikationen und Daten von einem Kubernetes-Cluster zu einem anderen
- Einfaches Klonen von Applikationen aus der Produktion bis hin zur Staging
- Darstellung des Anwendungszustands und des Schutzstatus
- Verwenden Sie eine Benutzeroberfläche oder eine API zur Implementierung Ihrer Backup- und Migrations-Workflows

Astra Control überwacht Ihr Computing kontinuierlich auf Zustandsänderungen, so ist es bewusst, dass neue Apps, die Sie auf dem Weg hinzufügen.

Implementierungsmodelle

Astra Control ist in zwei Implementierungsmodellen erhältlich:

- **Astra Control Service**: Ein von NetApp gemanagter Service, der applikationskonsistentes Datenmanagement von Kubernetes-Clustern in der Google Kubernetes Engine (GKE) und Azure Kubernetes Service (AKS) ermöglicht.
- **Astra Control Center**: Gemanagte Software für applikationsgerechtes Datenmanagement von Kubernetes-Clustern, die in Ihrer On-Premises-Umgebung ausgeführt werden.

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

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

Unterstützte Applikationen

NetApp hat einige Applikationen validiert, um die Sicherheit und Konsistenz der Snapshots und Backups zu gewährleisten.

- "Erfahren Sie mehr über den Unterschied zwischen einer validierten App und einer Standard-App in Astra Control".

Unabhängig von der Art der Applikation, die Sie mit Astra Control verwenden, sollten Sie den Backup- und Restore-Workflow immer selbst testen, um Ihre Disaster-Recovery-Anforderungen zu erfüllen.

Funktionsweise des Astra Control Service

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

Astra Control Service funktioniert auf hohem Niveau wie folgt:

- Starten Sie mit Astra Control Service, indem Sie Ihren Cloud-Provider einrichten und einen Astra Account anfordern.
  - Für GKE-Cluster verwendet der Astra Control Service "NetApp Cloud Volumes Service für Google Cloud" Oder Google Persistent Disks als Storage-Backend für Ihre persistenten Volumes.
  - Für AKS-Cluster nutzt der Astra Control Service "Azure NetApp Dateien" Oder Azure Disk Storage als Storage-Backend für Ihre persistenten Volumes.
- Sie fügen Ihre ersten Kubernetes-Computing-Ressourcen in den Astra Control Service ein. Astra Control Service übernimmt dann Folgendes:
  - Erstellung eines Objektspeicher in Ihrem Cloud-Provider-Konto, an dem Backup-Kopien gespeichert werden

    In Azure erstellt Astra Control Service außerdem eine Ressourcengruppe, ein Storage-Konto und Schlüssel für den Blob-Container.
  - Erstellt eine neue Administratorrolle und ein Kubernetes-Servicekonto auf dem Cluster.
  - Verwendet diese neue Administratorrolle für die Installation "Astra Trident" Auf dem Cluster und um eine oder mehrere Storage-Klassen zu erstellen.

    - Wenn Sie Azure NetApp Files oder NetApp Cloud Volumes Service für Google Cloud als Storage-Backend nutzen, verwendet der Astra Control Service Astra Trident, um persistente Volumes für Ihre Applikationen bereitzustellen.
- An dieser Stelle können Sie Ihrem Cluster Apps hinzufügen. Persistente Volumes werden auf der neuen Standard-Storage-Klasse bereitgestellt.
- Anschließend verwalten Sie diese Applikationen mithilfe des Astra Control Service und erstellen Snapshots, Backups und Klone.

  Astra Control Service überwacht Ihr Computing kontinuierlich auf Statusänderungen, sodass Sie sich über neue Applikationen im Klaren sind, die Sie unterwegs hinzufügen.

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

So funktioniert Astra Control Center

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

Astra Control Center unterstützt OpenShift Kubernetes Cluster mit:

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

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

Astra Control Center ist vollständig in das AutoSupport und Active IQ Ecosystem integriert, damit Benutzer und NetApp Support Fehlerbehebungs- und Verwendungsinformationen liefern können.

Sie können Astra Control Center mit einer 90-Tage-Evaluierungslizenz ausprobieren. Die Evaluierungsversion wird durch E-Mail- und Community-Optionen (Slack-Kanal) unterstützt. Zudem haben Sie über das Dashboard für den Produktsupport Zugriff auf Knowledgebase-Artikel und -Dokumentation.

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

Astra Control Center funktioniert auf hohem Niveau wie folgt:

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

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

Astra Control Center erreicht dies:

- Erkennung von Details zu gemanagten Kubernetes Clustern
- Erkennt die Konfiguration Ihrer Astra Trident oder Astra Data Store auf den Clustern, die Sie managen möchten, und ermöglicht Ihnen das Monitoring der Storage-Back-Ends.
- Erkennt Apps auf diesen Clustern und ermöglicht das Management und den Schutz der Apps.

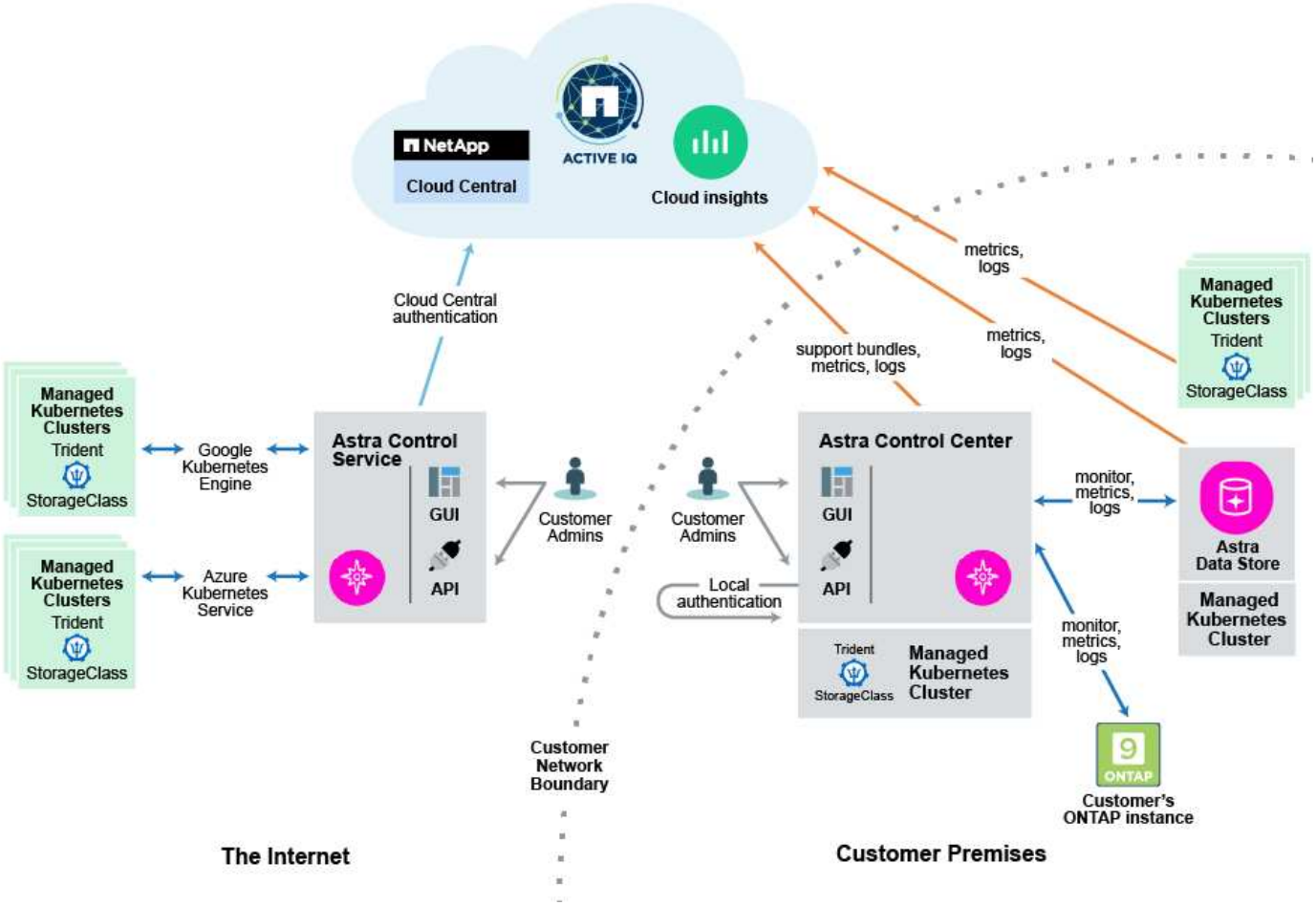
Sie können Applikationen zu Ihrem Cluster hinzufügen. Wenn Sie auch bereits einige Apps im Cluster verwalten, können Sie sie mit Astra Control Center erkennen und managen. Nutzen Sie dann das Astra Control Center, um Snapshots, Backups und Klone zu erstellen.

Finden Sie weitere Informationen

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

Architektur und Komponenten

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



Komponenten des Astra Control

- **Kubernetes-Cluster**: Kubernetes ist eine portable, erweiterbare Open-Source-Plattform für das Management von Workloads und Services in Containern, die sowohl deklarative Konfigurationen als auch Automatisierung ermöglicht. Astra bietet Managementservices für Applikationen, die in einem Kubernetes-Cluster gehostet werden.
- **Astra Trident**: Trident ist eine vollständig unterstützte Open-Source-Storage-bereitstellung und -Orchestrierung mit Hilfe von NetApp. Mit Trident können Sie Storage Volumes für Container-Applikationen erstellen, die von Docker und Kubernetes verwaltet werden. Trident ist mit dem Astra Control Center implementiert und bietet ein konfiguriertes ONTAP Storage-Backend sowie Support des Astra Data Store als Storage-Backend.
- **Speicher-Backend**:
  - Astra Control Service verwendet "NetApp Cloud Volumes Service für Google Cloud" Als Speicher-Backend für GKE-Cluster und "Azure NetApp Dateien" Als Speicher-Backend für AKS-Cluster.
  - Astra Control Service unterstützt auch Azure Managed Disks und Google Persistent Disk als Backend-Storage-Optionen.
  - Astra Control Center nutzt folgende Storage-Back-Ends:
    - Astra Data Store Storage-Back-End
    - ONTAP AFF und FAS Storage Back-End Als Storage-Software- und Hardware-Plattform bietet ONTAP wichtige Storage-Services, Unterstützung für mehrere Storage-Zugriffsprotokolle und Storage-Managementfunktionen wie Snapshots und Spiegelung.

    - Cloud Volumes ONTAP Storage Back-End
- **Cloud Insights**: Mit Cloud Insights, einem Cloud-Infrastruktur-Monitoring-Tool, überwachen Sie die Performance und Auslastung Ihrer Kubernetes-Cluster und werden von Astra Control Center gemanagt. Cloud Insights korreliert die Storage-Auslastung mit Workloads. Wenn Sie die Cloud Insights-Verbindung im Astra Control Center aktivieren, werden Telemetriedaten auf den UI-Seiten des Astra Control Center angezeigt.

Astra Control-Schnittstellen

Sie können Aufgaben über verschiedene Schnittstellen ausführen:

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

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

Finden Sie weitere Informationen

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

Datensicherung

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

Snapshots, Backups und Sicherungsrichtlinien

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

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

Eine *Schutzrichtlinie* ist eine Möglichkeit zum Schutz einer App, indem automatisch Snapshots, Backups oder beides gemäß einem von Ihnen für die App definierten Zeitplan erstellt werden. Eine Schutzrichtlinie

ermöglicht Ihnen darüber hinaus die Auswahl der Anzahl der Snapshots und Backups, die im Zeitplan aufbewahrt werden sollen. Die Automatisierung Ihrer Backups und Snapshots mithilfe einer Schutzrichtlinie stellt sicher, dass jede Applikation den Anforderungen Ihres Unternehmens entsprechend geschützt ist.

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

Klone

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

Lizenzierung

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

Für die folgenden Vorgänge ist eine gültige Lizenz erforderlich:

- Managen neuer Applikationen
- Snapshots oder Backups werden erstellt
- Konfigurieren einer Schutzrichtlinie zur Planung von Snapshots oder Backups
- Wiederherstellen aus einem Snapshot oder einem Backup
- Klonen aus einem Snapshot oder aktuellem Status

> Sie können ohne Lizenz ein Cluster hinzufügen, einen Bucket hinzufügen und ein Astra Data Store Storage-Backend verwalten. Sie benötigen jedoch eine gültige Astra Control Center-Lizenz für das Management von Applikationen mit Astra Data Store als Storage-Backend.

Berechnung der Lizenznutzung

Wenn Sie dem Astra Control Center einen neuen Cluster hinzufügen, zählen diese nicht auf verbrauchte Lizenzen, bis mindestens eine auf dem Cluster ausgeführte Applikation vom Astra Control Center verwaltet wird. Sie können das Astra Data Store Storage-Backend auch zum Astra Control Center hinzufügen, ohne den Lizenzverbrauch zu beeinträchtigen. So können Sie ein Astra Data Store Backend von einem nicht lizenzierten Astra Control Center System aus managen.

Wenn Sie eine App auf einem Cluster verwalten, sind die CPU-Einheiten des Clusters in der Berechnung des Lizenzverbrauchs des Astra Control Center enthalten.

Weitere Informationen

- "Aktualisieren einer vorhandenen Lizenz"

Validiert gegenüber Standard-Applikationen

Es gibt zwei Arten von Anwendungen für Astra Control: Validiert und Standard. Erfahren Sie mehr über die Unterschiede zwischen diesen beiden Kategorien und die potenziellen Auswirkungen auf Ihre Projekte und Ihre Strategie.

> Es ist verlockend, sich diese beiden Kategorien als „unterstützt“ und „nicht unterstützt“ zu betrachten. Aber wie Sie sehen werden, gibt es nicht so etwas wie eine "nicht unterstützte" App in Astra Control. Sie können jede beliebige Applikation in Astra Control integrieren, obwohl validierte Applikationen im Vergleich zu standardmäßigen Applikationen auf ihren Astra Control Workflows mehr Infrastruktur aufbauen.

Validierte Applikationen

Zu den validierten Applikationen für Astra Control gehören:

- MySQL 8.0.25
- MariaDB 10.5.9
- PostgreSQL 11.12
- Jenkins 2.277.4 LTS und 2.289.1 LTS

Die Liste validierter Applikationen stellt Applikationen dar, die Astra Control erkennt. Das Astra Control Team hat diese Apps analysiert und bestätigt, dass sie vollständig auf die Wiederherstellung getestet werden. Astra Control führt benutzerdefinierte Workflows aus, um die Konsistenz von Snapshots und Backups auf Applikationsebene zu gewährleisten.

Wenn eine App validiert wird, hat das Astra Control Team Maßnahmen identifiziert und implementiert, die ergriffen werden können, um die App stillzulegen, bevor ein Snapshot erstellt wird, um einen applikationskonsistenten Snapshot zu erhalten. Wenn Astra Control beispielsweise ein Backup einer PostgreSQL Datenbank erstellt, wird zunächst die Datenbank stillgelegt. Nach Abschluss der Sicherung stellt Astra Control die Datenbank in den normalen Betrieb wieder her.

Ganz gleich, welche Art von Applikation Sie mit Astra Control verwenden: Testen Sie den Backup- und Restore-Workflow immer selbst, um Ihre Disaster-Recovery-Anforderungen zu erfüllen.

Standard-Applikationen

Andere Apps, darunter auch benutzerdefinierte Programme, werden als Standard-Apps betrachtet. Sie können Standard-Apps über Astra Control hinzufügen und verwalten. Außerdem können Sie grundlegende, absturzkonsistente Snapshots und Backups einer Standard-App erstellen. Diese wurden jedoch nicht vollständig getestet, um die App in ihren ursprünglichen Zustand wiederherzustellen.

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

Storage-Klassen und persistente Volume-Größe

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

Überblick

Das Astra Control Center unterstützt Folgendes:

- **Trident Storage-Klassen mit Unterstützung von Astra Data Store Storage**: Wenn Sie einen oder mehrere Astra Data Store Cluster manuell installiert haben, bietet Astra Control Center die Möglichkeit, diese zu importieren und ihre Topologie (Nodes, Festplatten) sowie verschiedene Status abzurufen.

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

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

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

Speicherklassen

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

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

Finden Sie weitere Informationen

- "Astra Trident-Dokumentation"

Benutzerrollen und Namespaces

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

Benutzerrollen

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

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

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

Namespaces

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

Weitere Informationen

"Rollen managen"

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 IRGENDEINER 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.