Konzepte

Astra Control Center

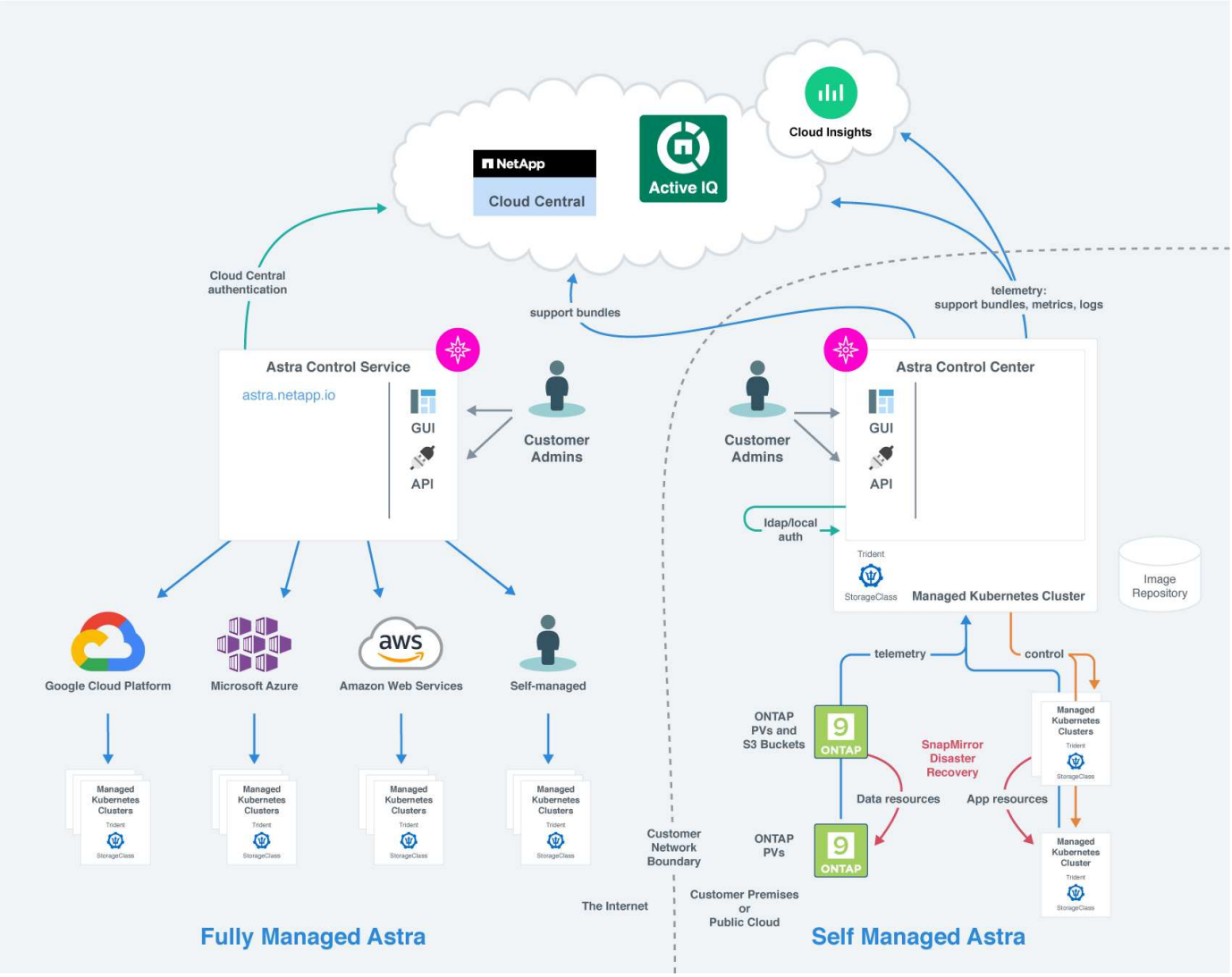
NetApp
November 27, 2023

Inhalt

Konzepte

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**: Als vollständig unterstützte Open-Source-Storage-bereitstellung und -Orchestrierung mit NetApp ermöglicht Ihnen Astra Trident die Erstellung von Storage Volumes für Container-Applikationen, die von Docker und Kubernetes verwaltet werden. Astra Trident ist mit dem Astra Control Center implementiert und umfasst ein konfiguriertes ONTAP Storage-Back-End.
- **Speicher-Backend**:

- Astra Control Service nutzt folgende Storage-Back-Ends:
  - "NetApp Cloud Volumes Service für Google Cloud" Oder Google Persistent Disk als Speicher-Backend für GKE-Cluster
  - "Azure NetApp Dateien" Oder von Azure verwaltete Festplatten als Storage-Backend für AKS-Cluster.
  - "Amazon Elastic Block Store (EBS)" Oder "Amazon FSX für NetApp ONTAP" Als Back-End-Speicheroptionen für EKS-Cluster.
- Astra Control Center nutzt folgende Storage-Back-Ends:
  - ONTAP AFF, FAS und ASA. Als Storage-Software- und Hardware-Plattform bietet ONTAP wichtige Storage-Services, Unterstützung für mehrere Storage-Zugriffsprotokolle und Storage-Managementfunktionen wie Snapshots und Spiegelung.
  - Cloud Volumes ONTAP

- **Cloud Insights**: Mit Cloud Insights, einem Monitoring-Tool für die Cloud-Infrastruktur von NetApp, können Sie die Performance und Auslastung für Ihre Kubernetes-Cluster überwachen, die vom Astra Control Center gemanagt werden. 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

Sowohl Snapshots als auch Backups sichern die folgenden Datentypen:

- Der Applikation selbst.
- Alle persistenten Daten-Volumes, die mit der Applikation in Verbindung stehen
- Alle zu der Applikation gehörenden Ressourcenartefakte

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. Snapshots sind nützlich zum Klonen oder Wiederherstellen einer Anwendung innerhalb desselben Clusters.

Ein *Backup* basiert auf einem Snapshot. Er wird im externen Objektspeicher gespeichert und kann daher 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 Sicherungsrichtlinie erlaubt Ihnen außerdem festzulegen, wie viele Snapshots und Backups im Zeitplan aufbewahrt werden sollen, und verschiedene granulare Zeitplanebenen festzulegen. Die Automatisierung von Backups und Snapshots mit einer Sicherungsrichtlinie ist die beste Methode, um sicherzustellen, dass jede Applikation gemäß den Anforderungen Ihres Unternehmens und der SLA-Anforderungen (Service Level Agreement) 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 App, ihrer Konfiguration und ihrer persistenten Daten-Volumes. Sie können einen Klon entweder manuell auf demselben Kubernetes-Cluster oder auf einem anderen Cluster erstellen. Das Klonen einer Applikation kann nützlich sein, wenn Sie Applikationen und Storage von einem Kubernetes Cluster zu einem anderen verschieben müssen.

Replizierung zwischen Storage-Back-Ends

Mithilfe von Astra Control können Sie mit den asynchronen Replizierungsfunktionen der NetApp SnapMirror Technologie Business Continuity für Ihre Applikationen erzielen: Mit Low-RPO (Recovery Point Objective) und Low-RTO (Recovery Time Objective). Nach der Konfiguration können Ihre Applikationen auf diese Weise Daten und Applikationsänderungen von einem Storage-Back-End auf ein anderes replizieren, sowohl im selben Cluster als auch zwischen verschiedenen Clustern.

Sie können zwischen zwei ONTAP SVMs auf demselben ONTAP Cluster oder in verschiedenen ONTAP Clustern replizieren.

Astra Control repliziert App-Snapshot-Kopien asynchron an ein Ziel-Cluster. Der Replizierungsprozess umfasst

Daten in den persistenten Volumes, die von SnapMirror repliziert werden, und die durch Astra Control geschützten App-Metadaten.

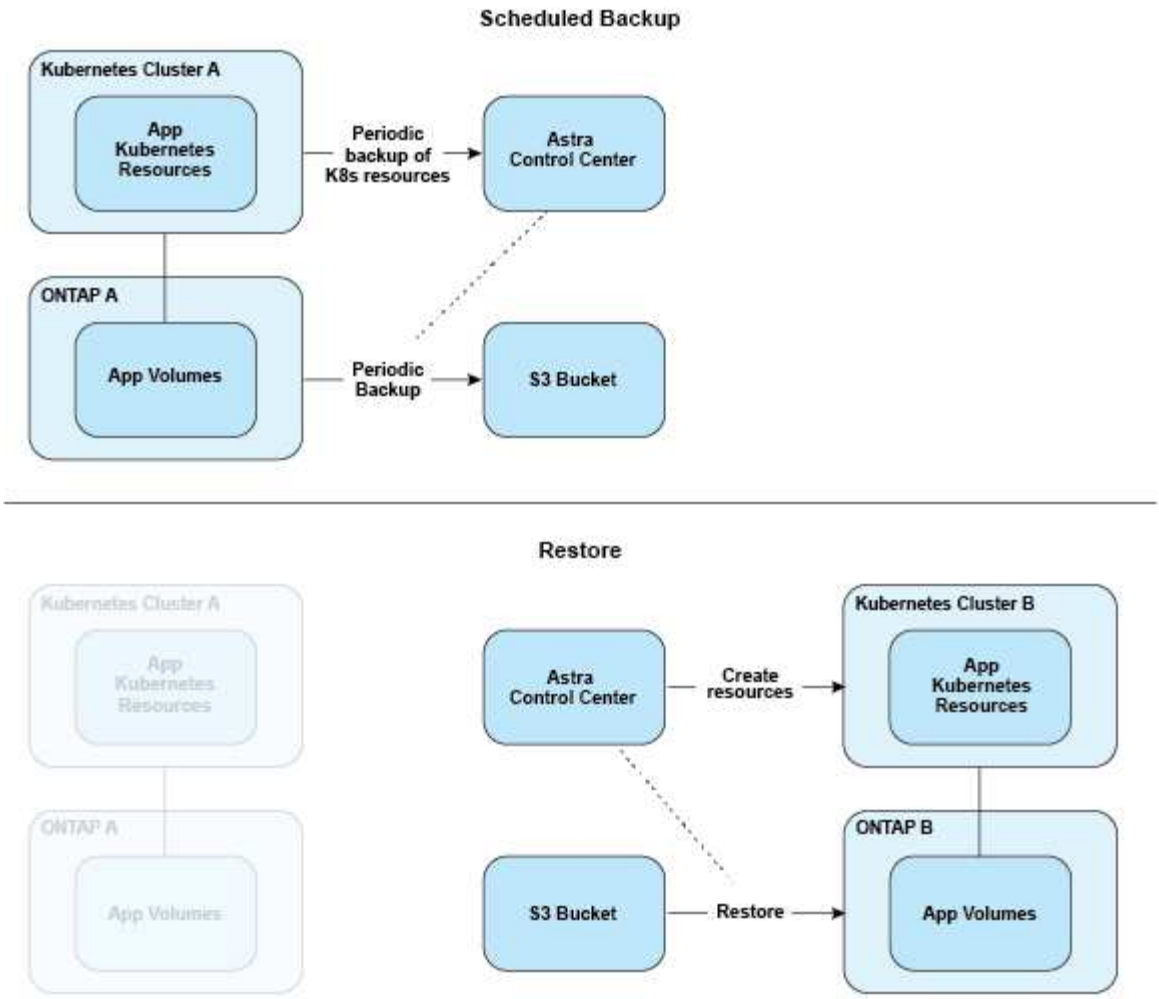
Die Replizierung von Applikationen unterscheidet sich folgendermaßen von Backup und Restore von Applikationen:

- **App-Replizierung**: Für Astra Control müssen die Kubernetes Quell- und Ziel-Cluster (die dasselbe Cluster sein können) verfügbar sein und mit ihren jeweiligen ONTAP Storage-Back-Ends gemanagt werden, die für die Aktivierung von NetApp SnapMirror konfiguriert sind. Astra Control repliziert den richtlinienbasierten Applikations-Snapshot auf das Ziel-Storage-Back-End. NetApp SnapMirror wird zur Replizierung der persistenten Volume-Daten eingesetzt. Zum Failover kann Astra Control die replizierte Applikation online schalten, indem die Applikationsobjekte auf dem Kubernetes Ziel-Cluster mit den replizierten Volumes auf dem ONTAP Ziel-Cluster neu erstellt werden. Da die persistenten Volume-Daten bereits auf dem Ziel-ONTAP-Cluster vorhanden sind, kann Astra Control schnelle Recovery-Zeiten für Failover bieten.
- **App-Backup und -Wiederherstellung**: Beim Backup von Anwendungen erstellt Astra Control einen Snapshot der App-Daten und speichert diesen in einem Objekt-Storage-Bucket. Wenn eine Wiederherstellung erforderlich ist, müssen die Daten in dem Bucket auf ein persistentes Volume auf dem ONTAP Cluster kopiert werden. Der Backup-/Restore-Vorgang erfordert nicht, dass der sekundäre Kubernetes/ONTAP Cluster verfügbar und gemanagt wird. Die zusätzliche Datenkopie kann jedoch zu längeren Restore-Zeiten führen.

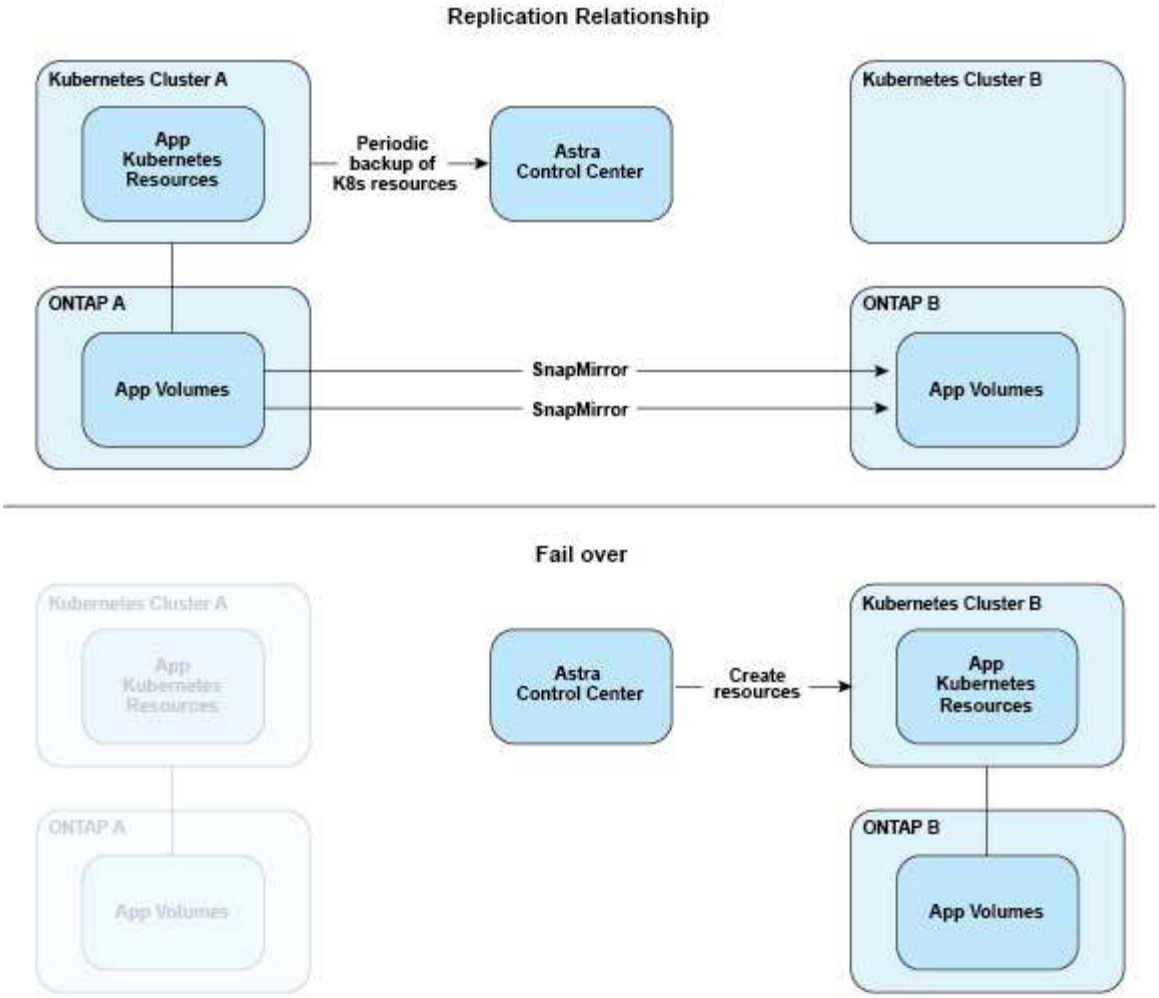
Weitere Informationen zum Replizieren von Apps finden Sie unter "Replizieren von Applikationen auf einem Remote-System mit SnapMirror Technologie".

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

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



Andererseits wird die Replizierung zu ONTAP durchgeführt. Durch ein Failover werden die Kubernetes-Ressourcen erzeugt:



Backups, Snapshots und Klone mit abgelaufener Lizenz

Wenn Ihre Lizenz abläuft, können Sie nur dann eine neue Applikation hinzufügen oder Vorgänge zum Schutz von Applikationen (wie Snapshots, Backups, Klone und Wiederherstellungsvorgänge) durchführen, wenn die hinzugefügte oder zu schützende Applikation eine weitere Astra Control Center-Instanz ist.

Lizenzierung

Bei der Bereitstellung von Astra Control Center wird es mit einer eingebetteten 90-Tage-Evaluierungslizenz für 4,800 CPU-Einheiten installiert. Wenn Sie mehr Kapazität oder einen längeren Evaluierungszeitraum benötigen oder auf eine komplette Lizenz aktualisieren möchten, können Sie eine andere Evaluierungslizenz oder eine komplette Lizenz von NetApp beziehen.

Sie erhalten eine Lizenz auf eine der folgenden Arten:

- Wenn Sie Astra Control Center evaluieren und andere Evaluierungsbedingungen als in der eingebetteten Evaluierungslizenz benötigen, wenden Sie sich an NetApp, um eine andere Evaluierungslizenzdatei zu anfordern.
- "Wenn Sie Astra Control Center bereits gekauft haben, generieren Sie Ihre NetApp Lizenzdatei (NLF)." Melden Sie sich dazu auf der NetApp Support-Website an und navigieren Sie zu Ihren Softwarelizenzen im

Menü „Systeme“.

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

> Stellen Sie sicher, dass Ihre Lizenz mindestens so viele CPU-Einheiten wie erforderlich aktiviert. Wenn die Anzahl der CPU-Einheiten, die Astra Control Center derzeit verwaltet, die verfügbaren CPU-Einheiten in der neuen Lizenz überschreitet, können Sie die neue Lizenz nicht anwenden.

Evaluierungslizenzen und Volllizenzen

Eine eingebettete Evaluierungslizenz wird mit der neuen Astra Control Center-Installation bereitgestellt. Eine Evaluierungslizenz ermöglicht über einen begrenzten Zeitraum (90 Tage) dieselben Funktionen und Funktionen wie eine Volllizenz. Nach dem Evaluierungszeitraum ist eine vollständige Lizenz erforderlich, um mit voller Funktionalität fortzufahren.

Ablauf der Lizenz

Wenn die aktive Astra Control Center-Lizenz abläuft, sind die UI- und API-Funktionen für die folgenden Funktionen nicht verfügbar:

- Manuelle lokale Snapshots und Backups
- Geplante lokale Snapshots und Backups
- Wiederherstellen aus einem Snapshot oder einem Backup
- Klonen aus einem Snapshot oder aktuellem Status
- Managen neuer Applikationen
- Konfigurieren von Replikationsrichtlinien

Berechnung der Lizenznutzung

Wenn Sie dem Astra Control Center einen neuen Cluster hinzufügen, zählen diese nicht auf verbrauchte Lizenzen, bis mindestens eine auf dem Cluster ausgeführte Applikation vom Astra Control Center verwaltet wird.

Wenn Sie eine App auf einem Cluster verwalten, sind alle CPU-Einheiten dieses Clusters im Lizenzverbrauch von Astra Control Center enthalten, mit Ausnahme der CPU-Einheiten des Red hat OpenShift-Cluster-Node, die von einem mit dem Label gemeldet werden `node-role.kubernetes.io/infra: ""`.

> Red hat OpenShift Infrastruktur-Nodes nutzen keine Lizenzen in Astra Control Center. Um einen Node als Infrastruktur-Node zu markieren, wenden Sie die Beschriftung an `node-role.kubernetes.io/infra: ""` Auf den Node.

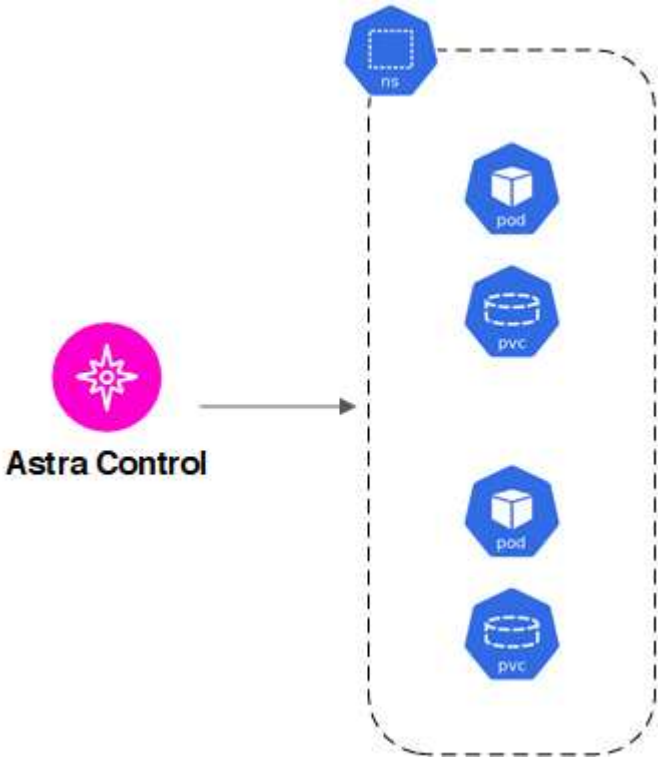
Weitere Informationen

- "Fügen Sie beim ersten Einrichten des Astra Control Center eine Lizenz hinzu"
- "Aktualisieren einer vorhandenen Lizenz"

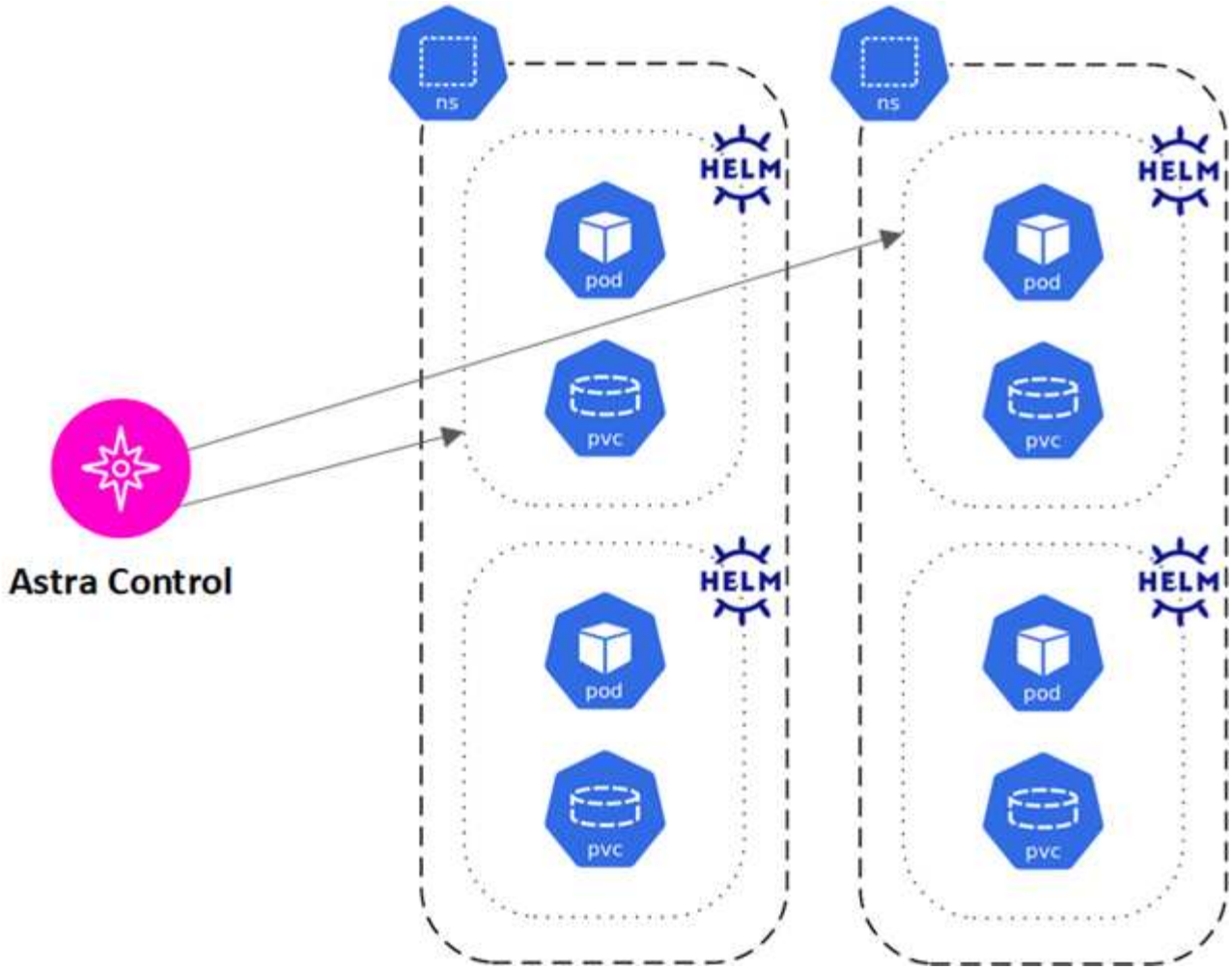
Applikationsmanagement

Wenn Astra Control Ihre Cluster erkennt, werden die Apps auf diesen Clustern solange nicht verwaltet, bis Sie das gewünschte Management wählen. Eine verwaltete Anwendung in Astra Control kann eine der folgenden sein:

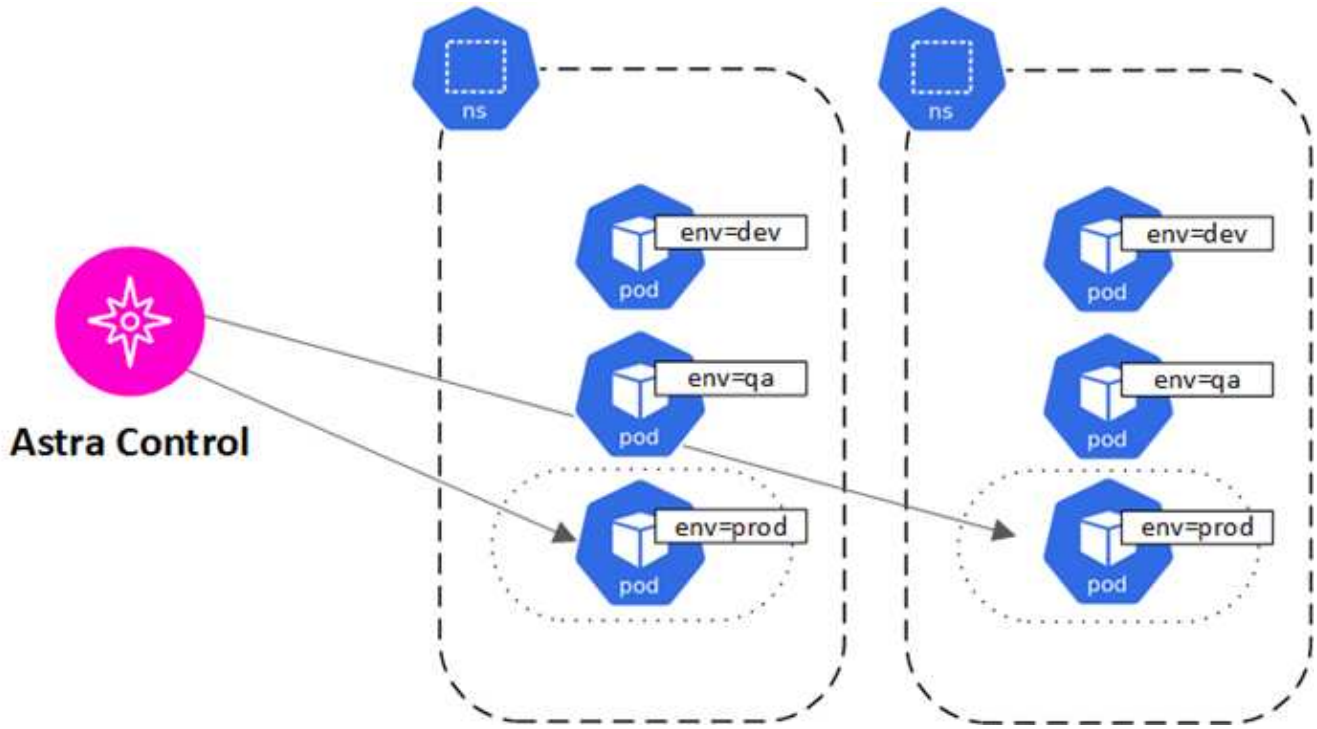
- Einen Namespace, einschließlich aller Ressourcen in diesem Namespace



- Eine individuelle Anwendung, die innerhalb einer oder mehrerer Namespaces bereitgestellt wird (in diesem Beispiel wird helm3 verwendet)



- Eine Gruppe von Ressourcen, die innerhalb eines oder mehrerer Namespaces durch ein Kubernetes-Label identifiziert werden



Storage-Klassen und persistente Volume-Größe

Astra Control Center unterstützt NetApp ONTAP und Longhorn als Storage-Back-Ends.

Überblick

Das Astra Control Center unterstützt Folgendes:

- **Von ONTAP Storage unterstützte Astra Trident Storage-Klassen**: Wenn Sie ein ONTAP-Backend verwenden, bietet Astra Control Center die Möglichkeit, das ONTAP-Backend zu importieren und verschiedene Monitoring-Informationen zu melden.
- **CSI-basierte Speicherklassen mit Longhorn**: Sie können Longhorn mit dem Longhorn Container Storage Interface (CSI) Treiber verwenden.

Astra Trident Storage-Klassen sollten außerhalb des Astra Control Center vorkonfiguriert werden.

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.

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

"Managen Sie lokale Benutzer und Rollen"

Pod-Sicherheit

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

Einige Kubernetes Distributionen verfügen möglicherweise über eine Standard-Pod-Sicherheitskonfiguration, die zu restriktiv ist und bei der Installation von Astra Control Center Probleme verursacht.

Anhand der hier enthaltenen Informationen und Beispiele können Sie die Sicherheitsänderungen des Behälters verstehen, die Astra Control Center vornimmt, und einen Pod-Sicherheitsansatz verwenden, der Ihnen den nötigen Schutz bietet, ohne die Funktionen des Astra Control Center zu beeinträchtigen.

PSAs durch Astra Control Center durchgesetzt

Astra Control Center ermöglicht die Durchsetzung einer Pod-Sicherheitsaufnahme, indem dem Namespace, auf dem Astra installiert ist, das folgende Label hinzugefügt wird (netapp-ACC oder benutzerdefinierter Namespace) und für Backups erstellte Namespaces.

```
pod-security.kubernetes.io/enforce: privileged
```

PSPs, die vom Astra Control Center installiert werden

Wenn Sie Astra Control Center auf Kubernetes 1.23 oder 1.24 installieren, werden während der Installation mehrere POD-Sicherheitsrichtlinien erstellt. Einige davon sind dauerhaft, und einige von ihnen werden während bestimmter Operationen erstellt und werden entfernt, sobald der Vorgang abgeschlossen ist. Astra Control Center versucht nicht, PSPs zu installieren, wenn auf dem Host-Cluster Kubernetes 1.25 oder höher ausgeführt wird, da diese nicht von diesen Versionen unterstützt werden.

PSPs, die während der Installation erstellt wurden

Während der Installation des Astra Control Center installiert der Astra Control Center-Operator eine benutzerdefinierte POD-Sicherheitsrichtlinie, A `Role` Objekt und A `RoleBinding` Soll die Implementierung

der Astra Control Center-Services im Astra Control Center Namespace unterstützen.

Die neue Richtlinie und die neuen Objekte haben folgende Attribute:

```
kubectl get psp

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

kubectl get role -n <namespace_name>

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

kubectl get rolebinding -n <namespace_name>

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

Während des Backup-Betriebs erstellte PSPs

Während des Backups erstellt Astra Control Center eine dynamische POD-Sicherheitsrichtlinie, A `ClusterRole` Objekt und A `RoleBinding` Objekt: Diese unterstützen den Backup-Prozess, der in einem separaten Namespace geschieht.

Die neue Richtlinie und die neuen Objekte haben folgende Attribute:

```
kubectl get psp

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

kubectl get role -n <namespace_name>

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

kubectl get rolebinding -n <namespace_name>

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

PSPs, die während des Clustermanagements erstellt wurden

Wenn Sie einen Cluster verwalten, installiert Astra Control Center den netapp Monitoring Operator im Managed Cluster. Dieser Operator erstellt eine POD-Sicherheitsrichtlinie, A `ClusterRole` Objekt und A `RoleBinding` Implementieren von Telemetrieservices im Astra Control Center Namespace

Die neue Richtlinie und die neuen Objekte haben folgende Attribute:

```
kubectl get psp

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

kubectl get role -n <namespace_name>

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

kubectl get rolebinding -n <namespace_name>

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

Copyright-Informationen

Markeninformationen