



Konzepte

Astra Control Service

NetApp
July 29, 2024

Inhalt

- Konzepte 1
 - Architektur und Komponenten 1
 - Datensicherung 6
 - Storage-Klassen und Performance für AWS Cluster 7
 - Speicherklassen und PV-Größe für AKS-Cluster 8
 - Servicetyp, Speicherklassen und PV-Größe für GKE-Cluster 9
- Applikationsmanagement 12
- Benutzerrollen und Namespaces 14

Konzepte

Architektur und Komponenten

Astra Control ist eine Kubernetes-Lösung für das übergreifende Lebenszyklusmanagement von Applikationsdaten. Sie vereinfacht den Betrieb zustandsbehafteter Applikationen und unterstützt Sie beim Speichern, Sichern und Verschieben Ihrer Kubernetes-Workloads zwischen Hybrid- und Multi-Cloud-Umgebungen.

Sorgen

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

Store:

- Dynamische Storage-Bereitstellung für Container-Workloads
- Verschlüsselung der Daten auf der Übertragungsstrecke aus Container zu persistenten Volumes
- Regionsübergreifende, zonenübergreifende Replizierung

Schutz:

- Automatische Erkennung und applikationsgerechte Sicherung einer gesamten Applikation und ihrer Daten
- Sofortige Wiederherstellung einer Applikation von einer beliebigen Snapshot-Version je nach den Anforderungen Ihres Unternehmens
- Schnelles Failover über Zonen, Regionen und Cloud-Provider hinweg

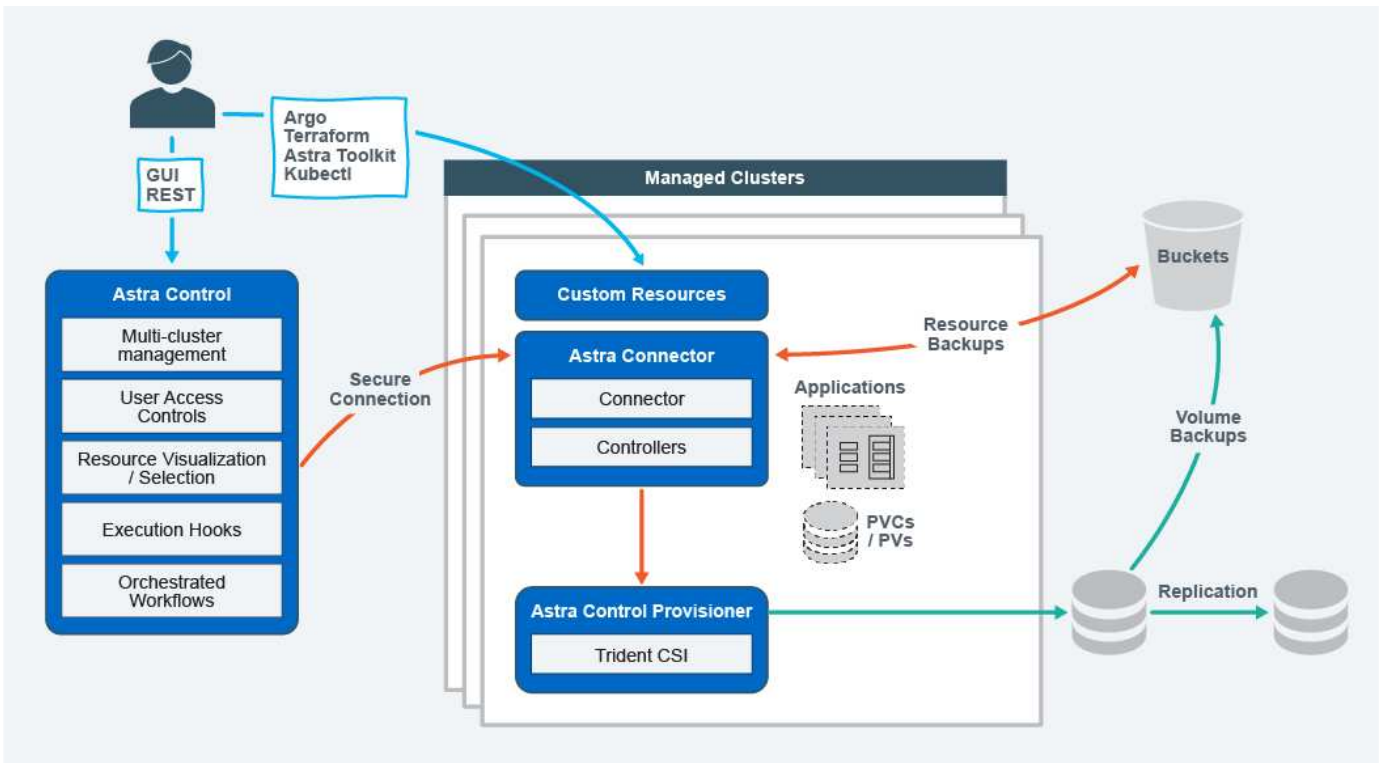
Verschieben:

- Vollständige Applikations- und Datenmobilität innerhalb und zwischen Kubernetes-Clustern und Clouds
- Sofortige Klone vollständiger Applikationen und Daten
- Migration von Anwendungen mit einem Klick über eine konsistente Web-UI und -API

Der Netapp Architektur Sind

Mit der Architektur von Astra Control bietet die IT erweiterte Datenmanagementfunktionen, die sowohl die Funktionalität als auch die Verfügbarkeit von Kubernetes-Applikationen verbessern. Sie vereinfacht das Management, den Schutz und die Verschiebung von Container-Workloads in Public Clouds und On-Premises-Umgebungen. Die Software bietet Automatisierungsfunktionen über ihre REST-API und sein SDK und ermöglicht einen programmatischen Zugriff für eine nahtlose Integration in vorhandene Workflows.

Astra Control ist Kubernetes-nativ und ermöglicht Datensicherungs-Workflows, die benutzerdefinierte Ressourcen verwenden und gleichzeitig rückwärtskompatibel mit der vorhandenen API und dem SDK bleiben. Die native Datensicherung von Kubernetes bietet deutliche Vorteile. Durch die nahtlose Integration in Kubernetes-APIs und -Ressourcen kann die Datensicherung über die vorhandenen CI/CD- und/oder GitOps-Tools eines Unternehmens zu einem integrierenden Bestandteil des Applikationslebenszyklus werden.



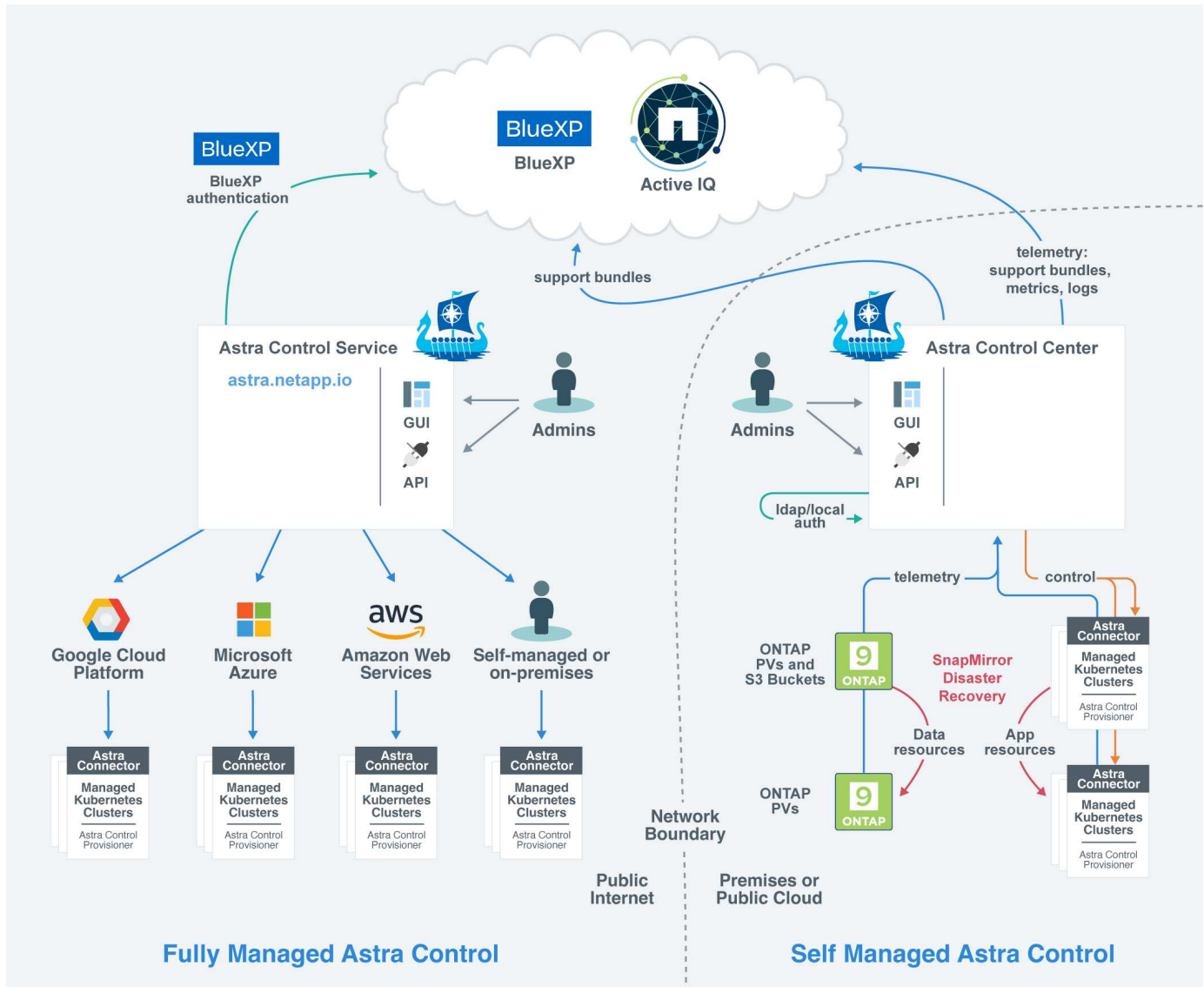
Astra Control basiert auf vier sich ergänzenden Komponenten:

- **Astra Control:** Astra Control ist der zentralisierte Management-Service für alle gemanagten Cluster und bietet orchestrierte Workloads für den Schutz und die Mobilität von Applikationen in der Cloud und On-Premises sowie folgende Funktionen:
 - Kombinierte Ansicht auf mehrere Cluster und Clouds
 - Schutz orchestrierter Workflows
 - Granulare Ressourcenvisualisierung und -Auswahl
- **Astra Connector:** Astra Connector arbeitet mit Astra Control zusammen, um eine sichere Verbindung zu jedem verwalteten Cluster bereitzustellen und so die lokale Ausführung geplanter Operationen unabhängig vom Verbindungsstatus sowie die folgenden Funktionen zu ermöglichen:
 - Lokale Ausführung geplanter Vorgänge unabhängig vom Verbindungsstatus
 - Lokale Abläufe, die die Nutzung von Astra Systemressourcen auf Cluster verteilen und optimieren
 - Lokale Installation, die den Zugriff auf das Cluster mit den geringsten Berechtigungen ermöglicht, um die Sicherheit zu erhöhen
- **Astra Control Provisioner:** Der Astra Control Provisioner bietet zentrale CSI-Bereitstellungsfunktionen und erweiterte Storage Management-Funktionen für zusätzliche Sicherheit und Disaster Recovery-Konfiguration sowie die folgenden Funktionen:
 - Dynamische Storage-Bereitstellung für Container-Workloads
 - Erweitertes Storage-Management:
 - Verschlüsselung der Daten während der Übertragung vom Container zum PV
 - SnapMirror Cloud Funktionalität mit regionsübergreifender Replizierung
- **Astra Custom-Ressourcen:** Auf jedem Cluster verwendete benutzerdefinierte Ressourcen bieten einen Kubernetes-nativen Ansatz für die lokale Ausführung von Vorgängen. Dies vereinfacht die Integration in andere Kubernetes-freundliche Tools und Automatisierungsfunktionen sowie folgende Funktionen:

- Direkte Integration und Workflows für die Automatisierung von Tools anderer Anbieter
- Primitive auf niedrigerer Ebene, die benutzerdefinierte Workflows ermöglichen

Implementierungsmodelle

Astra Control ist in zwei Implementierungsmodellen verfügbar.



- **Astra Control Service:** Ein von NetApp gemanagter Service, der applikationskonsistentes Datenmanagement für Kubernetes-Cluster in Umgebungen mehrerer Cloud-Provider sowie selbstverwaltete Kubernetes-Cluster bietet.

["Dokumentation des Astra Control Service"](#)

- **Astra Control Center:** Gemanagte Software für applikationsgerechtes Datenmanagement von Kubernetes-Clustern, die in Ihrer On-Premises-Umgebung ausgeführt werden. Astra Control Center kann auch auf mehreren Cloud-Provider-Umgebungen mit einem NetApp Cloud Volumes ONTAP Storage-Backend installiert werden.

["Astra Control Center-Dokumentation"](#)

	Astra Control Service	Astra Control Center
Wie wird das angeboten?	Vollständig gemanagter Cloud-Service von NetApp	Als Software, die Sie herunterladen, installieren und verwalten können
Wo wird sie gehostet?	In einer Public Cloud von NetApp ihrer Wahl	In Ihrem eigenen Kubernetes-Cluster
Wie wird sie aktualisiert?	Gemanagt von NetApp	Sie verwalten jegliche Updates
Welche Kubernetes-Distributionen werden unterstützt?	<ul style="list-style-type: none"> • Cloud-Provider <ul style="list-style-type: none"> ◦ Amazon Web Services <ul style="list-style-type: none"> ▪ Amazon Elastic Kubernetes Service (EKS) ◦ Google Cloud <ul style="list-style-type: none"> ▪ Google Kubernetes Engine (GKE) ◦ Microsoft Azure <ul style="list-style-type: none"> ▪ Azure Kubernetes-Service (AKS) • Selbstverwaltete Cluster <ul style="list-style-type: none"> ◦ Kubernetes (Vorgelagert) ◦ Rancher Kubernetes Engine (RKE) ◦ Red hat OpenShift Container Platform • On-Premises-Cluster <ul style="list-style-type: none"> ◦ Lokale Red hat OpenShift Container-Plattform 	<ul style="list-style-type: none"> • Azure Kubernetes Service für Azure Stack HCI • Google Anthos • Kubernetes (Vorgelagert) • Rancher Kubernetes Engine (RKE) • Red hat OpenShift Container Platform

	Astra Control Service	Astra Control Center
Welche Storage-Back-Ends werden unterstützt?	<ul style="list-style-type: none"> • Cloud-Provider <ul style="list-style-type: none"> ◦ Amazon Web Services <ul style="list-style-type: none"> ▪ Amazon EBS ▪ Amazon FSX für NetApp ONTAP ▪ "Cloud Volumes ONTAP" ◦ Google Cloud <ul style="list-style-type: none"> ▪ Google Persistent Disk ▪ NetApp Cloud Volumes Service ▪ "Cloud Volumes ONTAP" ◦ Microsoft Azure <ul style="list-style-type: none"> ▪ Über Azure Gemanagte Festplatten ▪ Azure NetApp Dateien ▪ "Cloud Volumes ONTAP" • Selbstverwaltete Cluster <ul style="list-style-type: none"> ◦ Amazon EBS ◦ Über Azure Gemanagte Festplatten ◦ Google Persistent Disk ◦ "Cloud Volumes ONTAP" ◦ NetApp MetroCluster ◦ "Longhorn" • On-Premises-Cluster <ul style="list-style-type: none"> ◦ NetApp MetroCluster ◦ NetApp ONTAP AFF und FAS Systeme ◦ NetApp ONTAP Select ◦ "Cloud Volumes ONTAP" ◦ "Longhorn" 	<ul style="list-style-type: none"> • NetApp ONTAP AFF und FAS Systeme • NetApp ONTAP Select • "Cloud Volumes ONTAP" • "Longhorn"

Finden Sie weitere Informationen

- ["Dokumentation des Astra Control Service"](#)
- ["Astra Control Center-Dokumentation"](#)
- ["Astra Trident-Dokumentation"](#)
- ["Astra Control API"](#)

- ["Cloud Insights-Dokumentation"](#)
- ["ONTAP-Dokumentation"](#)

Datensicherung

Informieren Sie sich über die verfügbaren Datensicherungsarten in Astra Control Service und über deren optimale Nutzung zum Schutz Ihrer Applikationen.

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.



Wenn Sie einen Snapshot oder eine Sicherung durchführen, aber der Vorgang mit dem Fehler „die Ressource wurde nicht wegen eines internen Serverproblems erstellt“ fehlschlägt, überprüfen Sie, ob im verwendeten Speicher-Backend die richtigen Treiber installiert sind. Einige Storage-Back-Ends benötigen Container-CSI-Treiber (Storage Interface), während andere einen externen Snapshot-Controller benötigen.

Unveränderliche Backups

Ein unveränderliches Backup ist ein Backup, das innerhalb eines festgelegten Zeitraums nicht geändert oder gelöscht werden kann. Beim Erstellen eines unveränderlichen Backups überprüft Astra Control, ob es sich bei dem verwendeten Bucket um einen WORM-Bucket (Write Once Read Many) handelt. Falls ja, stellt er sicher, dass das Backup in Astra Control unveränderlich ist.

Der Astra Control Service unterstützt das Erstellen unveränderlicher Backups mit den folgenden Plattformen und Bucket-Typen:

- Amazon Web Services verwenden einen Amazon S3 Bucket mit konfigurierter S3 Object Lock
- Microsoft Azure verwendet einen Azure-Bucket mit konfigurierter Aufbewahrungsrichtlinie
- Google Kubernetes Engine (GKE), die einen Google Cloud Storage-Bucket mit konfigurierter Aufbewahrungsrichtlinie verwendet
- NetApp StorageGRID mithilfe eines S3 Buckets mit konfigurierter S3 Object Lock-Funktion

Beachten Sie beim Arbeiten mit unveränderlichen Backups Folgendes:

- Wenn ein Backup auf einem WORM-Bucket in einer nicht unterstützten Plattform oder auf einem nicht unterstützten Bucket-Typ durchgeführt wird, können unvorhersehbare Ergebnisse wie das Löschen von Backups sogar dann angezeigt werden, wenn die Aufbewahrungszeit abgelaufen ist.
- Astra Control unterstützt keine Management-Richtlinien für den Daten-Lebenszyklus oder das manuelle Löschen von Objekten in den Buckets, die Sie mit unveränderlichen Backups verwenden. Stellen Sie sicher, dass Ihr Storage-Backend nicht für das Management des Lebenszyklus von Astra Control Snapshots oder gesicherten Daten konfiguriert ist.

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.

Storage-Klassen und Performance für AWS Cluster

Astra Control Service kann Amazon Elastic Block Store (EBS), Amazon FSX for NetApp ONTAP oder NetApp Cloud Volumes ONTAP als Storage-Backend für Amazon Elastic Kubernetes Service (EKS)-Cluster verwenden.

Amazon Elastic Block Store (EBS)

Ihre Cluster können eine Schnittstelle mit EBS über Container Storage Interface (CSI)-Treiber (Container Storage Interface) erstellen. Wenn Sie EBS als Speicher-Backend für EKS-Cluster verwenden, können Sie einige Speicherklassenparameter konfigurieren. Weitere Informationen über die Bedeutung der Parameter und deren Konfiguration finden Sie unter ["Die Kubernetes-Dokumentation"](#).

Sie können mit EBS mehrere verschiedene Volume-Typen verwenden:

- Solid State-Laufwerke (SSD)
- Festplattenlaufwerke (HDD)
- Vorherige Generation

Weitere Informationen zu den einzelnen Volume-Typen und ihrer Performance finden Sie unter ["Die Dokumentation zu Amazon EBS"](#). Preisinformationen finden Sie unter ["Amazon EBS Preis"](#).

Amazon FSX für NetApp ONTAP

Wenn Sie FSX für NetApp ONTAP als Storage-Backend für AWS Cluster verwenden, hängt die I/O-Performance von der Konfiguration des Dateisystems und den Eigenschaften Ihrer Workloads ab. Weitere Informationen zur Performance von NetApp ONTAP finden Sie unter FSX ["Amazon FSX für die Performance von NetApp ONTAP"](#). Preisinformationen finden Sie unter ["Amazon FSX für NetApp ONTAP-Preise"](#).

NetApp Cloud Volumes ONTAP

Genauere Informationen zur Konfiguration von NetApp Cloud Volumes ONTAP, einschließlich Performance-Empfehlungen, finden Sie im ["NetApp Cloud Volumes ONTAP-Dokumentation"](#).

Speicherklassen und PV-Größe für AKS-Cluster

Der Astra Control Service unterstützt Azure NetApp Files, von Azure gemanagte Festplatten oder NetApp Cloud Volumes ONTAP als Storage-Back-End für AKS-Cluster (Azure Kubernetes Service).

Azure NetApp Dateien

Astra Control Service unterstützt Azure NetApp Files als Storage-Backend für Azure Kubernetes Service-Cluster (AKS). Sie sollten verstehen, wie Sie mithilfe einer Storage-Klasse und einer persistenten Volume-Größe Ihre Performance-Ziele erreichen können.

Service Levels und Storage-Klassen

Azure NetApp Files unterstützt drei Service-Level: Ultra-Storage, Premium-Storage und Standard-Storage. Jedes dieser Service-Level ist für unterschiedliche Performance-Anforderungen konzipiert:

Ultra-Storage

Bietet einen Durchsatz von bis zu 128 MiB/s pro 1 tib.

Premium-Storage

Bietet einen Durchsatz von bis zu 64 MiB/s pro 1 tib.

Standard-Storage

Bietet einen Durchsatz von bis zu 16 MiB/s pro 1 tib.

Diese Service Levels sind die Attribute eines Kapazitäts-Pools. Sie müssen für jedes Service-Level, das Sie mit Ihren Kubernetes Clustern verwenden möchten, einen Kapazitäts-Pool einrichten. ["Erfahren Sie, wie Sie Kapazitäts-Pools einrichten"](#).

Astra Control Service verwendet diese Service-Level als Storage-Klassen für Ihre persistenten Volumes. Wenn Sie Kubernetes-Cluster zum Astra Control Service hinzufügen, werden Sie aufgefordert, Ultra, Premium oder Standard als Standard-Storage-Klasse auszuwählen. Die Namen der Storage-Klassen sind *netapp-anf-perf-ultra*, *netapp-anf-perf-Premium* und *netapp-anf-perf-Standard*.

["Weitere Informationen zu diesen Service Levels finden Sie in der Azure NetApp Files Dokumentation"](#).

Persistente Volume-Größe und -Performance

Wie oben beschrieben, beträgt der Durchsatz für jedes Service-Level 1 tib bereitgestellte Kapazität. Größere Volumes bieten also eine bessere Performance. Sie sollten also bei der Bereitstellung von Volumes sowohl Kapazitäts- als auch Performance-Anforderungen berücksichtigen.

Minimale Volume-Größe

Astra Control Service stellt persistente Volumes mit einer minimalen Volume-Größe von 100 gib bereit, selbst wenn das PVC eine kleinere Volume-Größe erfordert. Wenn beispielsweise das PVC in einem Helm-Diagramm 6 gib verlangt, stellt Astra Control Service automatisch ein Volumen von 100 gib bereit.

Applikations-Backups

Wenn Sie eine Applikation sichern, die sich auf dem Azure NetApp Files Storage befindet, erweitert Astra Control Service automatisch vorübergehend den Kapazitäts-Pool. Nach Abschluss des Backups verkleinert der Astra Control Service den Kapazitäts-Pool auf die vorherige Größe. Je nach Ihrem Azure-Abonnement fallen bei diesem Vorgang möglicherweise Storage-Gebühren an. Im Ereignisprotokoll der Seite **Aktivität** können Sie einen Verlauf der Größenänderung des Kapazitätspools sehen.

Wenn der Kapazitäts-Pool die maximal zulässige Größe des Azure-Abonnements während des Größenänderungsvorgangs überschreitet, schlägt der Backup-Vorgang fehl, und eine Warnung wird von der Azure-API ausgelöst.

Von Azure gemanagte Festplatten

Astra Control Service kann über Container Storage Interface (CSI)-Treiber eine Schnittstelle zu Azure Managed Disks als Storage-Backend verwenden. Dieser Service bietet Storage auf Block-Ebene, der von Azure gemanagt wird.

["Weitere Informationen über von Azure gemanagte Festplatten"](#).

NetApp Cloud Volumes ONTAP

Genauere Informationen zur Konfiguration von NetApp Cloud Volumes ONTAP, einschließlich Performance-Empfehlungen, finden Sie im ["NetApp Cloud Volumes ONTAP-Dokumentation"](#).

Servicetyp, Speicherklassen und PV-Größe für GKE-Cluster

Astra Control Service unterstützt NetApp Cloud Volumes Service für Google Cloud, Google Persistent Disk oder NetApp Cloud Volumes ONTAP als Storage-Backend-Optionen für persistente Volumes.

Cloud Volumes Service für Google Cloud

Astra Control Service kann Cloud Volumes Service für Google Cloud als Storage-Backend für persistente Volumes nutzen. Sie sollten verstehen, wie die Wahl eines Service-Typs, einer Storage-Klasse und einer persistenten Volume-Größe Sie dabei unterstützen kann, Ihre Performance-Ziele zu erreichen.

Überblick

Cloud Volumes Service für Google Cloud bietet zwei Servicetypen: *CVS* und *CVS-Performance*. Diese Servicetypen werden in bestimmten Google Cloud Regionen unterstützt. ["Wechseln Sie zu den Zuordnungen"](#)

von [NetApp BlueXP Regionen weltweit](#)" Ermitteln des Servicetyps, der in der Google Cloud-Region unterstützt wird, in der sich Ihre Cluster befinden.

Wenn Ihre Kubernetes-Cluster in einer bestimmten Region residieren müssen, verwenden Sie den in dieser Region unterstützten Servicetyp.

Wenn Sie jedoch flexibel zwischen Google Cloud Regionen wählen können, empfehlen wir auf Basis Ihrer Performance-Anforderungen Folgendes:

- Wählen Sie für K8s-Applikationen mit mittleren bis hohen Performance-Storage-Anforderungen eine Google Cloud-Region, die CVS-Performance unterstützt und die Premium- oder Extreme-Storage-Klasse verwendet. Zu diesen Workloads gehören KI/ML-Pipelines, CI/CD-Pipelines, Medienverarbeitung und Datenbanken wie relationale Workloads, NoSQL, Zeitreihen usw.
- Bei K8s-Applikationen mit geringen bis mittleren Storage-Performance-Anforderungen (Web-Applikationen, allgemeiner File-Storage usw.), wählen Sie eine Google Cloud-Region aus, die CVS oder CVS-Performance unterstützt – mit der Standard-Storage-Klasse.



Wenn Sie den CVS-Servicetyp mit Astra Control Provisioner verwenden, müssen Sie Speicherpools konfigurieren, bevor Sie Volumes bereitstellen können. Wenn Sie Volumes ohne konfigurierte Speicherpools bereitstellen, schlägt die Volume-Bereitstellung fehl. Siehe ["Cloud Volumes Service Dokumentation"](#) Weitere Informationen zum Erstellen von Volumes.

Die folgende Tabelle bietet einen schnellen Vergleich der auf dieser Seite beschriebenen Informationen.

Servicetyp	Anwendungsfall	Unterstützte Regionen	Speicherklassen	Minimale Volume-Größe
CVS-Performance	Applikationen mit mittleren bis hohen Storage-Performance-Anforderungen	"Unterstützte Google-Cloud-Regionen anzeigen"	<ul style="list-style-type: none">• netapp-cvs-Performance-Standard• netapp-cvs-perf-Premium• netapp-cvs-perf-extreme	100 gib
CVS	Applikationen mit geringen bis mittelgroßen Storage-Performance-Anforderungen	"Unterstützte Google-Cloud-Regionen anzeigen"	netapp-cvs-Standard	300 gib

CVS-Performance-Servicetyp

Erfahren Sie mehr über den CVS-Performance-Servicetyp, bevor Sie sich für eine Storage-Klasse entscheiden und persistente Volumes erstellen.

Speicherklassen

Der CVS-Performance-Servicetyp bietet drei Service Level: Standard, Premium und Extreme. Wenn Sie dem Astra Control Service ein Cluster hinzufügen, werden Sie aufgefordert, entweder Standard, Premium oder Extreme als Standard-Storage-Klasse für persistente Volumes auszuwählen. Jedes dieser Service-Levels ist

für unterschiedliche Kapazitäts- und Bandbreitenanforderungen konzipiert.

Die Namen der Storage-Klassen sind *netapp-cvs-perf-Standard*, *netapp-cvs-perf-Premium* und *netapp-cvs-perf-extreme*.

["Weitere Informationen zu diesen Service-Levels finden Sie in der Dokumentation zu Cloud Volumes Service für Google Cloud"](#).

Persistente Volume-Größe und -Performance

["Wie die Google Cloud Dokumente erklären"](#), Die zulässige Bandbreite für jedes Service-Level beträgt pro gib der bereitgestellten Kapazität. Das bedeutet, dass größere Volumes eine bessere Performance bieten.

Lesen Sie unbedingt die oben verlinkte Google Cloud-Seite durch. Es enthält Kostenvergleiche und Beispiele, damit Sie besser verstehen, wie Sie Service-Level mit Volume-Größe koppeln können, um Ihre Performance-Ziele zu erreichen.

Minimale Volume-Größe

Astra Control Service stellt persistente Volumes mit einer minimalen Volume-Größe von 100 gib beim Servicetyp CVS-Performance bereit, selbst wenn die PVC eine kleinere Volume-Größe erfordert. Wenn beispielsweise das PVC in einem Helm-Diagramm 6 gib verlangt, stellt Astra Control Service automatisch ein Volumen von 100 gib bereit.

CVS-Diensttyp

Erfahren Sie mehr über den CVS-Servicetyp, bevor Sie eine Storage-Klasse auswählen und persistente Volumes erstellen.

Storage-Klasse

Ein Service Level wird mit dem CVS-Servicetyp Standard unterstützt. Wenn Sie Cluster in Regionen managen, in denen der CVS-Servicetyp unterstützt wird, verwendet der Astra Control Service das Standard Service Level als Standard-Storage-Klasse für persistente Volumes. Die Storage-Klasse heißt *netapp-cvs-Standard*.

["Weitere Informationen zum Standard-Service finden Sie in der Dokumentation zu Cloud Volumes Service für Google Cloud"](#).

Persistente Volume-Größe und -Performance

Die zulässige Bandbreite für den CVS-Servicetyp beträgt pro gib der bereitgestellten Kapazität. Das bedeutet, dass größere Volumes eine bessere Performance bieten.

Minimale Volume-Größe

Astra Control Service stellt persistente Volumes mit einer Mindestvolumengröße von 300 gib beim CVS-Servicetyp bereit, selbst wenn das PVC eine kleinere Volume-Größe erfordert. Wenn z. B. 20 gib angefordert wird, stellt Astra Control Service automatisch ein Volumen von 300 gib bereit.

Wenn ein PVC ein Volumen zwischen 700-999 gib anfordert, stellt der Astra Control Service automatisch eine Volume-Größe von 1000 gib bereit.

Google Persistent Disk

Astra Control Service kann über CSI-Treiber (Container Storage Interface) eine Schnittstelle zu Google

Persistent Disk als Storage-Backend erstellen. Dieser Service bietet Storage auf Blockebene, der von Google gemanagt wird.

["Erfahren Sie mehr über Google Persistent Disk"](#).

["Erfahren Sie mehr über die verschiedenen Performance-Level von Google Persistent Disks"](#).

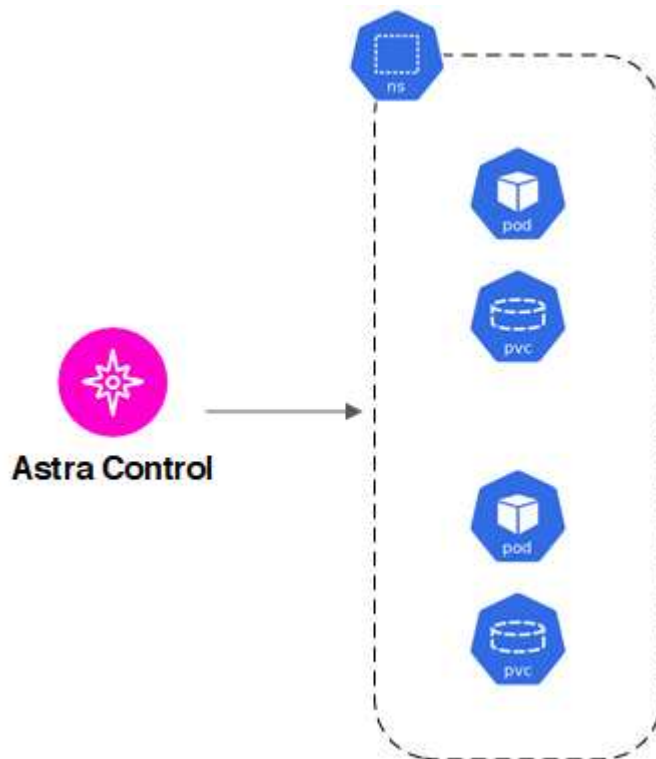
NetApp Cloud Volumes ONTAP

Genauere Informationen zur Konfiguration von NetApp Cloud Volumes ONTAP, einschließlich Performance-Empfehlungen, finden Sie im ["NetApp Cloud Volumes ONTAP-Dokumentation"](#).

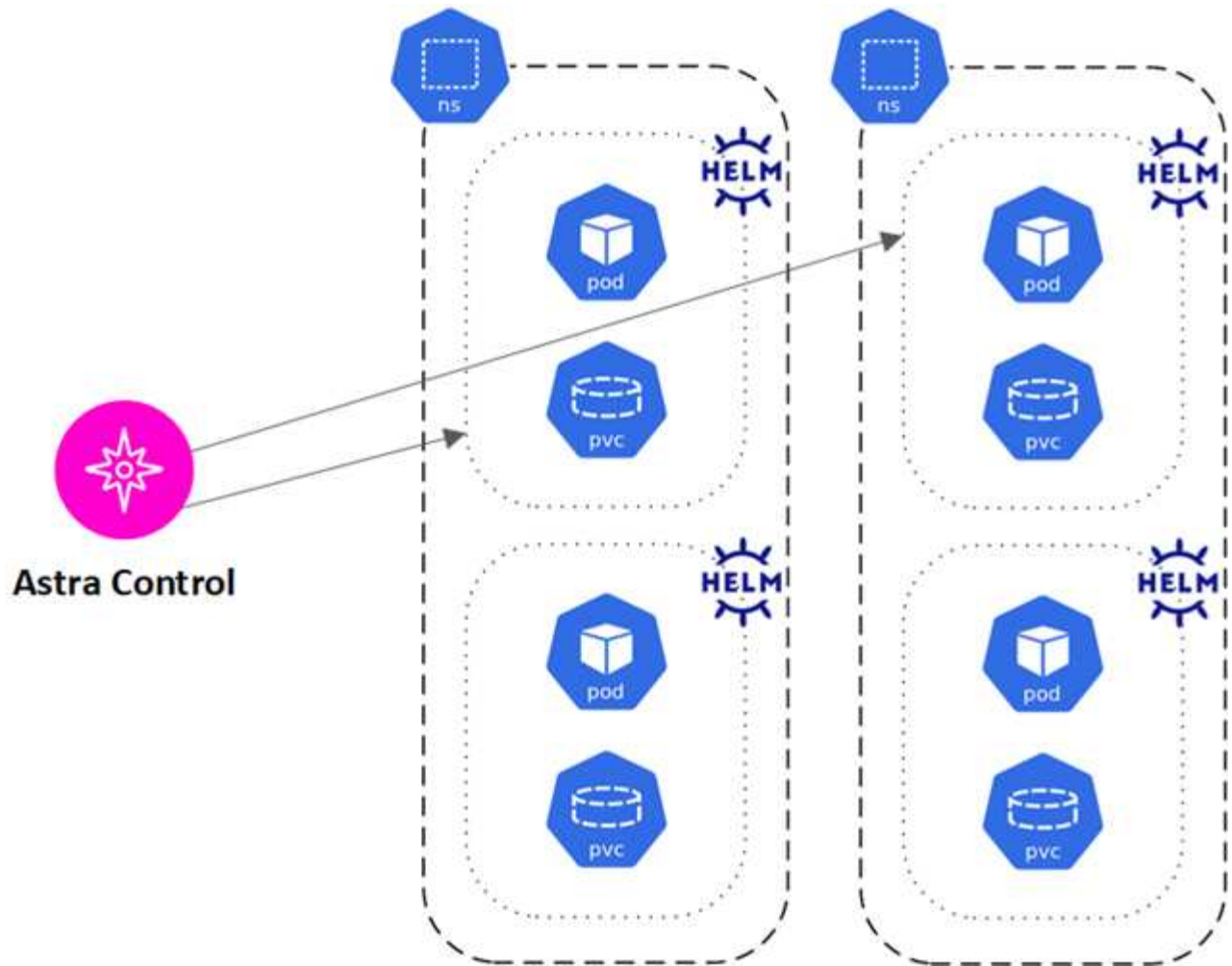
Applikationsmanagement

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:

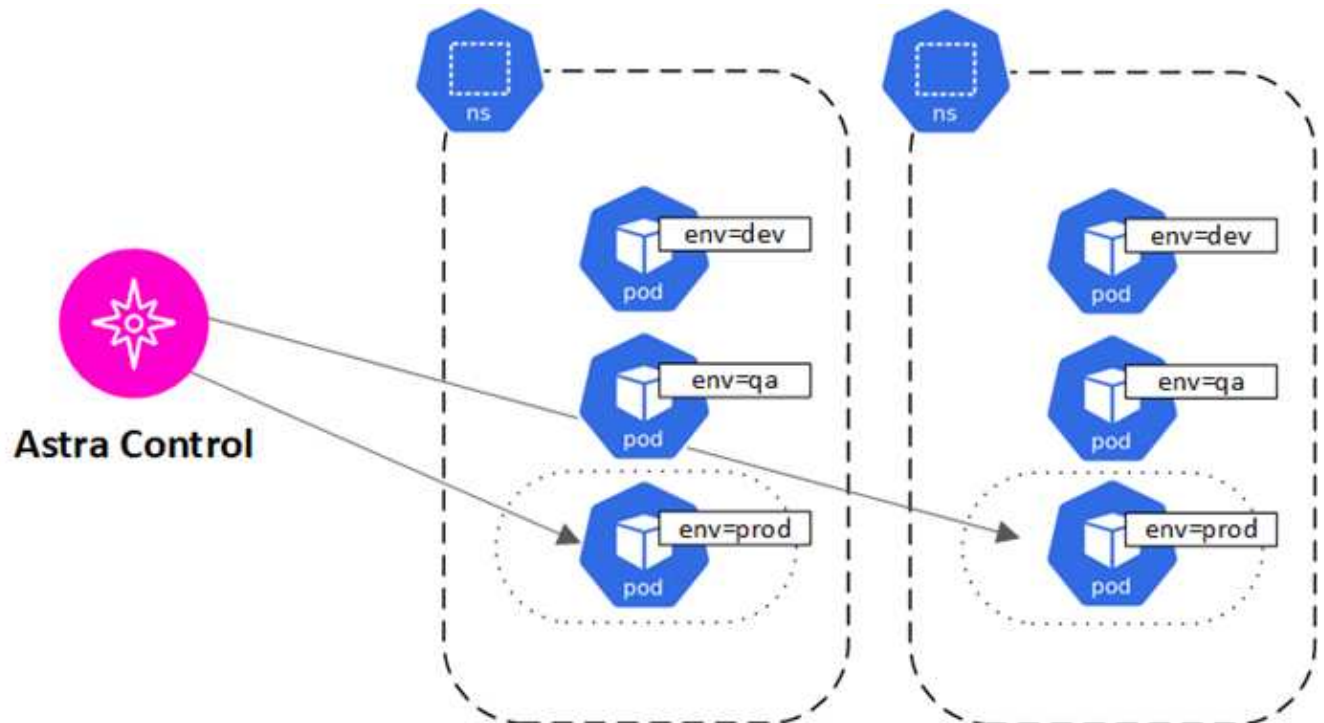
- Einen Namespace, einschließlich aller Ressourcen in diesem Namespace



- Eine einzelne Applikation, die innerhalb eines oder mehrerer Namespaces bereitgestellt wird (Helm 3 wird in diesem Beispiel verwendet).



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



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 **Eigentümer** hat Administratorrechte und kann Konten löschen.
- Ein **Admin** hat Mitgliederberechtigungen und kann andere Benutzer einladen.
- Ein **Mitglied** kann Apps und Cluster vollständig verwalten.
- Ein **Viewer** kann Ressourcen anzeigen.

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 © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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.