Know-How

Cloud Manager 3.8

NetApp
March 25, 2024

This PDF was generated from https://docs.netapp.com/de-de/occm38/concept_overview_cvo.html on March 25, 2024. Always check docs.netapp.com for the latest.

Inhalt

Know-How

Weitere Informationen zu Cloud Volumes ONTAP

Mit Cloud Volumes ONTAP können Sie Ihre Cloud Storage-Kosten und -Performance optimieren und gleichzeitig die Datensicherung, -Sicherheit und -Compliance verbessern.

Cloud Volumes ONTAP ist eine rein softwarebasierte Storage Appliance, auf der ONTAP Datenmanagement-Software in der Cloud ausgeführt wird. Das System bietet Storage der Enterprise-Klasse mit den folgenden wichtigen Funktionen:

- Storage-Effizienz

  Nutzen Sie integrierte Datendeduplizierung, Datenkomprimierung, Thin Provisioning und Klonen und minimieren Sie so die Storage-Kosten.

- Hochverfügbarkeit

  Zuverlässigkeit der Enterprise-Klasse und unterbrechungsfreien Betrieb bei Ausfällen in der Cloud-Umgebung sicherstellen.

- Datensicherung

  Cloud Volumes ONTAP nutzt SnapMirror, die branchenführende Replizierungstechnologie von NetApp, um On-Premises-Daten in der Cloud zu replizieren, sodass einfach sekundäre Kopien für diverse Anwendungsfälle verfügbar sind.

  Die Integration von Cloud Volumes ONTAP in Cloud Backup Service bietet zudem Backup- und Restore-Funktionen zur Sicherung und zur Langzeitarchivierung Ihrer Cloud-Daten.

- Daten-Tiering

  Wechseln Sie nach Bedarf zwischen hochperformanten Storage Pools, ohne Applikationen offline zu schalten.

- Applikationskonsistenz

  Konsistenz von NetApp Snapshot Kopien mit NetApp SnapCenter sicherstellen.

- Datensicherheit

  Cloud Volumes ONTAP unterstützt die Datenverschlüsselung und bietet Schutz vor Viren und Ransomware.

- Kontrolloptionen für die Einhaltung des Datenschutzes

  Durch die Integration in Cloud Compliance können Sie den Datenkontext verstehen und sensible Daten identifizieren.

Lizenzen für ONTAP Funktionen sind im Lieferumfang von Cloud Volumes ONTAP enthalten.

"Anzeigen der unterstützten Cloud Volumes ONTAP Konfigurationen"

"Erfahren Sie mehr über Cloud Volumes ONTAP"

Storage

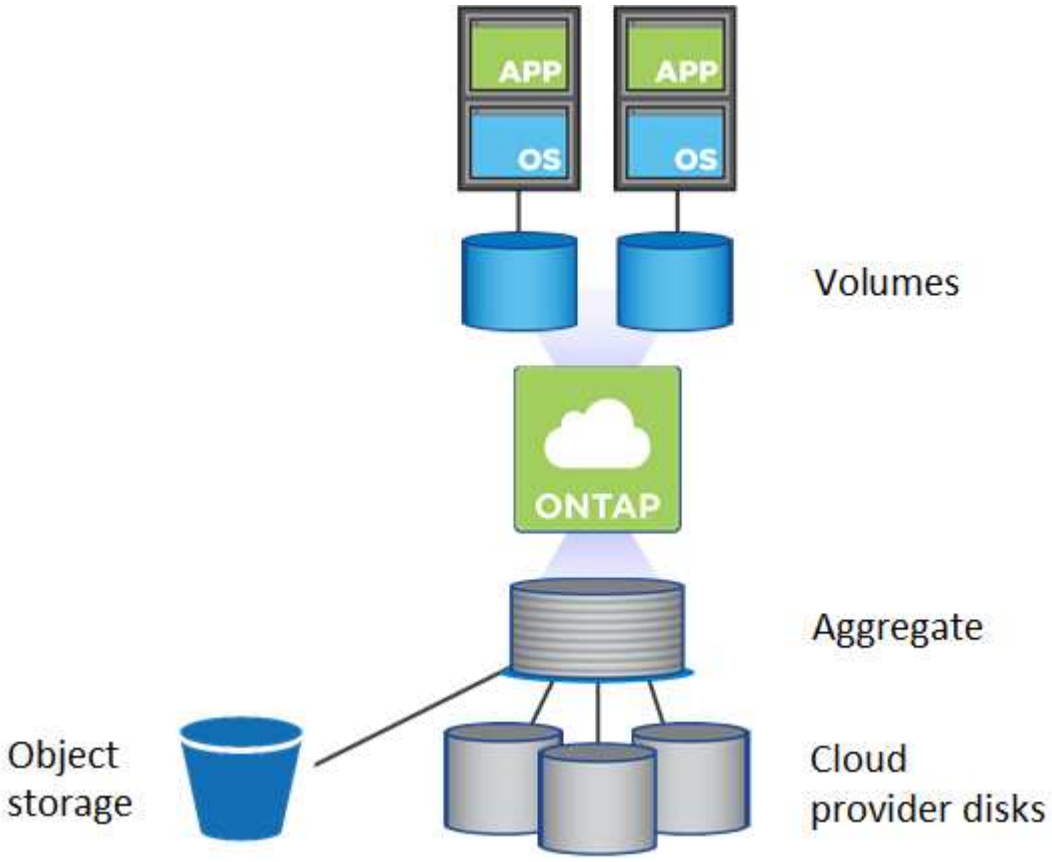
Festplatten und Aggregate

Wenn Sie verstehen, wie Cloud Volumes ONTAP Cloud Storage verwendet, können Sie Ihre Storage-Kosten besser verstehen.

Alle Festplatten und Aggregate müssen direkt aus Cloud Manager erstellt und gelöscht werden. Sie sollten diese Aktionen nicht über ein anderes Management-Tool ausführen. Dies kann sich auf die Systemstabilität auswirken, die Fähigkeit zum Hinzufügen von Festplatten in der Zukunft beeinträchtigen und möglicherweise Kosten für redundante Cloud-Provider verursachen.

Überblick

Cloud Volumes ONTAP verwendet Storage von Cloud-Providern als Festplatten und gruppiert diese in einem oder mehreren Aggregaten. Aggregate stellen Storage für ein oder mehrere Volumes bereit.



Es werden mehrere Arten von Cloud-Festplatten unterstützt. Bei der Implementierung von Cloud Volumes ONTAP wählen Sie den Festplattentyp bei der Erstellung eines Volume und der Standardfestplattengröße aus.

Der gesamte Storage, den ein Cloud-Provider erworben hat, ist die *Rohkapazität*. Die *nutzbare Kapazität* ist geringer, da etwa 12 bis 14 Prozent der für die Verwendung durch Cloud Volumes ONTAP reservierte Overhead sind. Wenn Cloud Manager beispielsweise ein 500-GB-Aggregat erstellt, beträgt die nutzbare Kapazität 442,94 GB.

AWS Storage

In AWS verwendet Cloud Volumes ONTAP EBS Storage für Benutzerdaten und lokalen NVMe Storage als Flash Cache auf einigen EC2 Instanztypen.

EBS Storage

In AWS kann ein Aggregat bis zu 6 Festplatten enthalten, die jeweils gleich groß sind. Die maximale Festplattengröße beträgt 16 TB.

Der zugrunde liegende EBS-Festplattentyp kann entweder eine Universal-SSD, eine bereitgestellte IOPS-SSD, eine für den Durchsatz optimierte Festplatte oder eine kalte Festplatte sein. Sie können eine EBS-Festplatte mit Amazon S3 zu koppeln "Verschieben inaktiver Daten in kostengünstigen Objektspeicher".

Die Unterschiede zwischen den EBS-Festplattentypen unterscheiden sich auf hohem Niveau wie folgt:

- *Universal SSD* Festplatten balancieren Kosten und Performance für ein breites Spektrum an Workloads aus. Die Performance wird in Bezug auf IOPS definiert.
- *Bereitgestellte IOPS SSD*-Festplatten sind für kritische Applikationen geeignet, die höchste Performance zu höheren Kosten erfordern.
- _Optimierte Festplatten mit hohem Durchsatz sind für häufig genutzte Workloads konzipiert, die einen schnellen und konsistenten Durchsatz zu einem niedrigeren Preis erfordern.
- *Cold HDD* Festplatten werden für Backups oder selten genutzte Daten gedacht, da die Performance nur sehr gering ist. Wie bei Festplatten mit Durchsatzoptimierung wird die Performance in Bezug auf den Durchsatz definiert.

> Festplatten mit kalten Daten werden von HA-Konfigurationen und Daten-Tiering nicht unterstützt.

Lokaler NVMe-Storage

Einige EC2-Instanztypen sind lokaler NVMe-Storage, der als Cloud Volumes ONTAP verwendet wird "Flash Cache".

Verwandte Links

- "AWS Dokumentation: EBS Volume-Typen"
- "Lesen Sie, wie Sie Festplattentypen und Festplattengrößen für Ihre Systeme in AWS auswählen"
- "Prüfen von Storage-Limits für Cloud Volumes ONTAP in AWS"
- "Unterstützte Konfigurationen für Cloud Volumes ONTAP in AWS prüfen"

Azure Storage

In Azure kann ein Aggregat bis zu 12 Festplatten enthalten, die dieselbe Größe aufweisen. Der Festplattentyp und die maximale Festplattengröße hängen davon ab, ob Sie ein Single-Node-System oder ein HA-Paar verwenden:

Systeme mit einzelnen Nodes

Systeme mit einem Node können drei Typen von Azure Managed Disks verwenden:

- *Premium SSD Managed Disks* bieten hohe Performance für I/O-intensive Workloads zu höheren Kosten.

- *Standard SSD Managed Disks* bieten konsistente Performance für Workloads, die niedrige IOPS erfordern.
- *Standard HDD Managed Disks* sind eine gute Wahl, wenn Sie keine hohen IOPS benötigen und Ihre Kosten senken möchten.

  Jeder verwaltete Festplattentyp hat eine maximale Festplattengröße von 32 TB.

  Sie können eine gemanagte Festplatte mit Azure Blob Storage kombinieren "Verschieben inaktiver Daten in kostengünstigen Objektspeicher".

HA-Paare

HA-Paare verwenden Premium Page Blobs, die eine maximale Festplattengröße von 8 TB haben.

Verwandte Links

- "Microsoft Azure-Dokumentation: Einführung in Microsoft Azure Storage"
- "Erfahren Sie, wie Sie Festplattentypen und Festplattengrößen für Ihre Systeme in Azure auswählen"
- "Prüfen Sie Storage-Limits für Cloud Volumes ONTAP in Azure"

GCP-Storage

In GCP kann ein Aggregat bis zu 6 Festplatten enthalten, die dieselbe Größe aufweisen. Die maximale Festplattengröße beträgt 16 TB.

Der Festplattentyp kann entweder *Zonal SSD Persistent Disks* oder *Zonal Standard Persistent Disks* sein. Sie können persistente Festplatten mit einem Google Storage Bucket kombinieren "Verschieben inaktiver Daten in kostengünstigen Objektspeicher".

Verwandte Links

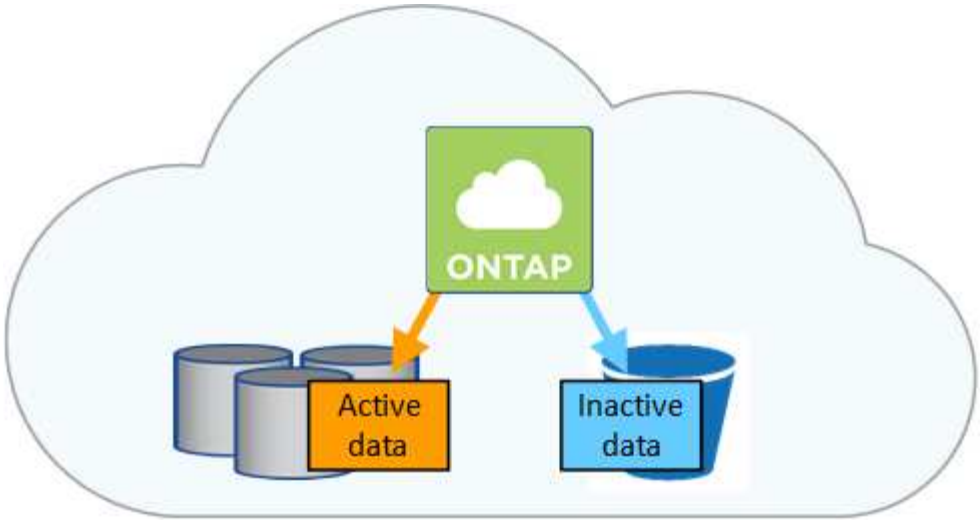
- "Dokumentation der Google Cloud Platform Storage Options"
- "Prüfen von Storage-Limits für Cloud Volumes ONTAP in GCP"

RAID-Typ

Der RAID-Typ für jedes Cloud Volumes ONTAP Aggregat ist RAID0 (Striping). Es werden keine anderen RAID-Typen unterstützt. Cloud Volumes ONTAP verlässt sich bei Festplattenverfügbarkeit und Langlebigkeit auf den Cloud-Provider.

Data Tiering - Übersicht

Senken Sie Ihre Storage-Kosten, indem Sie das automatisierte Tiering inaktiver Daten auf kostengünstigen Objekt-Storage ermöglichen. Aktive Daten bleiben auf hochperformanten SSDs oder HDDs, während inaktive Daten in kostengünstigen Objekt-Storage verschoben werden. Dadurch können Sie Speicherplatz auf Ihrem primären Storage zurückgewinnen und den sekundären Storage verkleinern.



Cloud Volumes ONTAP unterstützt Daten-Tiering in AWS, Azure und Google Cloud Platform. Data Tiering wird durch FabricPool Technologie unterstützt.

Sie müssen keine Funktionslizenz installieren, um Daten-Tiering (FabricPool) zu aktivieren.

Daten-Tiering in AWS

Wenn Sie Daten-Tiering in AWS aktivieren, verwendet Cloud Volumes ONTAP EBS als Performance-Tier für häufig benötigte Daten und AWS S3 als Kapazitäts-Tier für inaktive Daten.

Performance-Tier

Bei der Performance-Tier kann es sich um allgemeine SSDs, bereitgestellte IOPS-SSDs oder Throughput-optimierte HDDs handeln.

Kapazitäts-Tier

Ein Cloud Volumes ONTAP System verschiebt inaktive Daten mithilfe der Storage-Klasse *Standard* zu einem einzelnen S3 Bucket. Standard ist ideal für häufig aufgerufene Daten, die über mehrere Verfügbarkeitszonen gespeichert werden.

Cloud Manager erstellt für jede Arbeitsumgebung einen einzelnen S3 Bucket und nennt ihn Fabric-Pool-*Cluster-eindeutige Kennung*. Für jedes Volume wird kein anderer S3-Bucket erstellt.

Speicherklassen

Die Standard-Storage-Klasse für Tiered Daten in AWS ist *Standard*. Wenn Sie keinen Zugriff auf inaktive Daten planen, können Sie die Speicherkosten senken, indem Sie die Speicherklasse auf eine der folgenden Optionen ändern: *Intelligent Tiering*, *One-Zone infrequent Access* oder *Standard-infrequent Access*. Wenn Sie die Speicherklasse ändern, beginnen inaktive Daten in der Klasse Standard-Speicher und wechseln zu der von Ihnen ausgewählten Speicherklasse, wenn nach 30 Tagen kein Zugriff auf die Daten erfolgt.

Die Zugriffskosten sind höher, wenn Sie auf die Daten zugreifen. Berücksichtigen Sie dies also vor einem Wechsel der Storage-Klasse. "Erfahren Sie mehr über Amazon S3 Storage Classes".

Sie können eine Speicherklasse auswählen, wenn Sie die Arbeitsumgebung erstellen, und Sie können sie jederzeit danach ändern. Informationen zum Ändern der Speicherklasse finden Sie unter "Tiering inaktiver Daten in kostengünstigen Objektspeicher".

Die Storage-Klasse für Daten-Tiering beträgt die systemweite; nicht pro Volume.

Daten-Tiering in Azure

Wenn Sie Daten-Tiering in Azure aktivieren, verwendet Cloud Volumes ONTAP von Azure gemanagte Festplatten als Performance-Tier für häufig abgerufene Daten und Azure Blob Storage als Kapazitäts-Tier für inaktive Daten.

Performance-Tier

Der Performance-Tier kann entweder aus SSDs oder HDDs bestehen.

Kapazitäts-Tier

Ein Cloud Volumes ONTAP System schichtet inaktive Daten mithilfe der Storage-Tier Azure *Hot* in einem einzelnen Blob-Container aus. Der Hot Tier eignet sich ideal für häufig genutzte Daten.

Cloud Manager erstellt für jede Cloud Volumes ONTAP-Arbeitsumgebung ein neues Storage-Konto mit einem einzelnen Container. Der Name des Speicherkontos ist zufällig. Für jedes Volume wird kein anderer Container erstellt.

Storage-Zugriffstufen

Die Standard-Storage-Zugriffs-Tier für Tiered Daten in Azure ist die *Hot*-Tier. Wenn Sie nicht auf die inaktiven Daten zugreifen möchten, können Sie Ihre Storage-Kosten durch Wechsel zum „*cool* Storage Tier“ senken. Wenn Sie die Storage-Tier ändern, beginnen inaktive Daten im Storage-Tier. Diese werden auf den „coolen Storage“ verschoben, sofern nach 30 Tagen nicht mehr auf die Daten zugegriffen wird.

Die Zugriffskosten sind höher, wenn Sie auf die Daten zugreifen. Berücksichtigen Sie diese also vor einem Wechsel des Storage-Tiers. "Weitere Informationen zu Azure Blob Storage-Zugriffsklassen".

Sie können eine Speicherebene auswählen, wenn Sie die Arbeitsumgebung erstellen, und sie kann jederzeit danach geändert werden. Weitere Informationen zum Ändern der Speicherebene finden Sie unter "Tiering inaktiver Daten in kostengünstigen Objektspeicher".

Die Storage-Zugriffs-Tier für Daten-Tiering beträgt die systemweite; nicht pro Volume.

Daten-Tiering in GCP

Wenn Sie Daten-Tiering in GCP aktivieren, verwendet Cloud Volumes ONTAP persistente Festplatten als Performance-Tier für häufig abgerufene Daten und Google Cloud Storage-Buckets als Kapazitäts-Tier für inaktive Daten.

Performance-Tier

Das Performance-Tier kann entweder SSDs oder HDDs (Standard-Festplatten) sein.

Kapazitäts-Tier

Ein Cloud Volumes ONTAP System verschiebt inaktive Daten mithilfe der Storage-Klasse „*Regional*“ zu einem einzelnen Google Cloud-Storage-Bucket.

Cloud Manager erstellt für jede Arbeitsumgebung einen einzelnen Bucket und nennt ihn Fabric-Pool-*Cluster-eindeutige Kennung*. Für jedes Volume wird kein anderer Bucket erstellt.

Speicherklassen

Die Standard-Storage-Klasse für Tiered Daten ist die Klasse *Standard Storage*. Wenn nur selten auf die Daten zugegriffen wird, können Sie Ihre Storage-Kosten senken, indem Sie zu *Nearline Storage* oder

Coldline Storage wechseln. Wenn Sie die Speicherklasse ändern, beginnen inaktive Daten in der Klasse Standard-Speicher und wechseln zu der von Ihnen ausgewählten Speicherklasse, wenn nach 30 Tagen kein Zugriff auf die Daten erfolgt.

Die Zugriffskosten sind höher, wenn Sie auf die Daten zugreifen. Berücksichtigen Sie dies also vor einem Wechsel der Storage-Klasse. "Erfahren Sie mehr über Storage-Klassen für Google Cloud Storage".

Sie können eine Speicherebene auswählen, wenn Sie die Arbeitsumgebung erstellen, und sie kann jederzeit danach geändert werden. Informationen zum Ändern der Speicherklasse finden Sie unter "Tiering inaktiver Daten in kostengünstigen Objektspeicher".

Die Storage-Klasse für Daten-Tiering beträgt die systemweite; nicht pro Volume.

Daten-Tiering und Kapazitätsgrenzen

Wenn Sie Daten-Tiering aktivieren, bleibt die Kapazitätsgrenze eines Systems unverändert. Das Limit wird über die Performance- und die Kapazitäts-Tier verteilt.

Richtlinien für das Volume-Tiering

Um das Daten-Tiering zu aktivieren, müssen Sie beim Erstellen, Ändern oder Replizieren eines Volumes eine Volume-Tiering-Policy auswählen. Sie können für jedes Volume eine andere Richtlinie auswählen.

Einige Tiering Policies haben einen zugehörigen Mindestkühlzeitraum, der festlegt, wie lange Benutzerdaten in einem Volume inaktiv bleiben müssen, damit die Daten als "kalt" betrachtet und auf die Kapazitätsebene verschoben werden können.

Cloud Manager ermöglicht Ihnen bei der Erstellung oder Änderung eines Volume die Auswahl aus den folgenden Volume Tiering-Richtlinien:

Nur Snapshot

Nachdem ein Aggregat die Kapazität von 50 % erreicht hat, stuft Cloud Volumes ONTAP kalte Benutzerdaten von Snapshot Kopien ein, die nicht mit dem aktiven Filesystem der Kapazitäts-Tier verbunden sind. Die Abkühlzeit beträgt ca. 2 Tage.

Beim Lesen werden kalte Datenblöcke auf dem Kapazitäts-Tier heiß und werden auf den Performance-Tier verschoben.

Alle

Alle Daten (ohne Metadaten) werden sofort als „kalt“ markiert und in den Objektspeicher verschoben, sobald wie möglich. Es ist nicht mehr nötig, 48 Stunden auf neue Blöcke in einem Volume zu warten, die kalt werden. Beachten Sie, dass für Blöcke, die sich vor der Festlegung der All-Richtlinie im Volume befinden, 48 Stunden zum Kaltstart benötigt werden.

Beim Lesen bleiben kalte Datenblöcke auf der Cloud-Tier kalt und werden nicht zurück in die Performance-Tier geschrieben. Diese Richtlinie ist ab ONTAP 9.6 verfügbar.

Automatisch

Nachdem ein Aggregat die Kapazität von 50 % erreicht hat, stuft Cloud Volumes ONTAP kalte Datenblöcke in einem Volume auf einen Kapazitäts-Tier. Die kalten Daten umfassen nicht nur Snapshot Kopien, sondern auch kalte Benutzerdaten aus dem aktiven Dateisystem. Die Abkühlzeit beträgt ca. 31 Tage.

Diese Richtlinie wird ab Cloud Volumes ONTAP 9.4 unterstützt.

Wenn die Daten nach dem Zufallsprinzip gelesen werden, werden die kalten Datenblöcke in der

Kapazitätsebene heiß und werden auf die Performance-Ebene verschoben. Beim Lesen von sequenziellen Lesevorgängen, z. B. in Verbindung mit Index- und Antivirenscans, bleiben die kalten Datenblöcke kalt und wechseln nicht zur Performance-Ebene.

Keine

Die Daten eines Volumes werden in der Performance-Ebene gespeichert, sodass es nicht in die Kapazitäts-Ebene verschoben werden kann.

Bei der Replizierung eines Volume können Sie entscheiden, ob die Daten in einen Objekt-Storage verschoben werden sollen. In diesem Fall wendet Cloud Manager die **Backup**-Richtlinie auf das Datensicherungs-Volume an. Ab Cloud Volumes ONTAP 9.6 ersetzt die **All** Tiering Policy die Backup Policy.

Die Abschaltung von Cloud Volumes ONTAP beeinträchtigt die Kühlungszeit

Datenblöcke werden durch Kühlprüfungen gekühlt. Während dieses Prozesses werden Blöcke, die nicht verwendet wurden, die Blocktemperatur verschoben (gekühlt) auf den nächsten niedrigeren Wert. Die standardmäßige Kühlzeit hängt von der Volume Tiering-Richtlinie ab:

- Auto: 31 Tage
- Nur Snapshot: 2 Tage

Damit der Kühlscan funktioniert, muss Cloud Volumes ONTAP ausgeführt werden. Wenn die Cloud Volumes ONTAP ausgeschaltet ist, stoppt der Kühlbedarf ebenfalls. Auf diese Weise können die Kühlzeiten möglicherweise länger dauern.

Einrichten von Data Tiering

Anweisungen und eine Liste der unterstützten Konfigurationen finden Sie unter "Tiering inaktiver Daten in kostengünstigen Objektspeicher".

Storage-Management

Cloud Manager ermöglicht ein vereinfachtes und erweitertes Management von Cloud Volumes ONTAP Storage.

> Alle Festplatten und Aggregate müssen direkt aus Cloud Manager erstellt und gelöscht werden. Sie sollten diese Aktionen nicht über ein anderes Management-Tool ausführen. Dies kann sich auf die Systemstabilität auswirken, die Fähigkeit zum Hinzufügen von Festplatten in der Zukunft beeinträchtigen und möglicherweise Kosten für redundante Cloud-Provider verursachen.

Storage-Bereitstellung

Cloud Manager vereinfacht die Storage-Provisionierung für Cloud Volumes ONTAP durch den Kauf von Festplatten und das Management von Aggregaten. Sie müssen einfach Volumes erstellen. Sie können bei Bedarf eine erweiterte Zuweisungsoption verwenden, um Aggregate selbst bereitzustellen.

Vereinfachte Bereitstellung

Aggregate stellen Cloud-Storage für Volumes bereit. Cloud Manager erstellt Aggregate für Sie, wenn Sie eine Instanz starten und wenn Sie zusätzliche Volumes bereitstellen.

Wenn Sie ein Volume erstellen, führt Cloud Manager eine der drei folgenden Aufgaben aus:

- Das Volume wird auf einem vorhandenen Aggregat platziert, das über ausreichend freien Speicherplatz verfügt.
- Das Volume wird auf einem vorhandenen Aggregat platziert, indem mehr Festplatten für dieses Aggregat erworben werden.
- Es kauft Festplatten für ein neues Aggregat und platziert das Volume auf diesem Aggregat.

Cloud Manager ermittelt, wo ein neues Volume platziert werden soll, indem mehrere Faktoren betrachtet werden: Die maximale Größe eines Aggregats, ob Thin Provisioning aktiviert ist und freie Speicherplatzschwellenwerte für Aggregate.

Der Kontoadministrator kann die Schwellenwerte für freien Speicherplatz auf der Seite **Einstellungen** ändern.

Auswahl der Festplattengröße für Aggregate in AWS

Wenn Cloud Manager neue Aggregate für Cloud Volumes ONTAP in AWS erstellt, erhöht sich die Festplattengröße in einem Aggregat allmählich, wenn die Anzahl der Aggregate im System steigt. Cloud Manager stellt auf diese Weise sicher, dass Sie die maximale Kapazität des Systems nutzen können, bevor es die maximale Anzahl von Datenfestplatten erreicht, die von AWS zulässig sind.

Cloud Manager kann beispielsweise die folgenden Festplattengrößen für Aggregate in einem Cloud Volumes ONTAP Premium oder Byol System wählen:

Aggregatnummer	Festplattengröße	Max. Gesamtkapazität
1	500 MB	3 TB
4	1 TB	6 TB
6	2 TB	12 TB

Sie können die Festplattengröße selbst mithilfe der erweiterten Zuweisungsoption auswählen.

Erweiterte Zuweisung

Anstatt Cloud Manager Aggregate für Sie verwalten zu lassen, können Sie dies selbst tun. "Auf der Seite **Erweiterte Zuweisung**", Sie können neue Aggregate erstellen, die eine bestimmte Anzahl an Festplatten enthalten, einem vorhandenen Aggregat Festplatten hinzufügen und Volumes in bestimmten Aggregaten erstellen.

Kapazitätsmanagement

Der Account Admin kann entscheiden, ob Cloud Manager Sie über Storage-Kapazitätsentscheidungen informiert oder ob Cloud Manager die Kapazitätsanforderungen automatisch managt. Es könnte Ihnen dabei helfen, die Funktionsweise dieser Modi zu verstehen.

Automatisches Kapazitätsmanagement

Der Kapazitätsmanagement-Modus ist standardmäßig auf automatisch eingestellt. In diesem Modus kauft Cloud Manager automatisch neue Festplatten für Cloud Volumes ONTAP-Instanzen, wenn mehr Kapazität benötigt wird, löscht nicht verwendete Festplatten-Sammlungen (Aggregate), verschiebt Volumes zwischen Aggregaten nach Bedarf und versucht, Festplatten nicht ordnungsgemäß zurückzusetzen.

Die folgenden Beispiele veranschaulichen die Funktionsweise dieses Modus:

- Wenn ein Aggregat mit 5 oder weniger EBS-Festplatten den Kapazitätsschwellenwert erreicht, kauft Cloud Manager automatisch neue Festplatten für dieses Aggregat, damit Volumes weiter wachsen können.
- Wenn ein Aggregat mit 12 Azure Disks den Kapazitätsschwellenwert erreicht, verschiebt Cloud Manager automatisch ein Volume von diesem Aggregat in ein Aggregat mit verfügbarer Kapazität oder in ein neues Aggregat.

  Wenn Cloud Manager ein neues Aggregat für das Volume erstellt, wählt es eine Festplattengröße aus, die der Größe des Volumes entspricht.

  Beachten Sie, dass jetzt freier Speicherplatz auf dem ursprünglichen Aggregat verfügbar ist. Vorhandene Volumes oder neue Volumes können diesen Speicherplatz nutzen. Der Speicherplatz kann in diesem Szenario nicht in AWS, Azure oder GCP zurückgegeben werden.

- Wenn ein Aggregat mehr als 12 Stunden lang keine Volumes enthält, löscht Cloud Manager es.

Verwaltung von LUNs mit automatischem Kapazitätsmanagement

Das automatische Kapazitätsmanagement von Cloud Manager gilt nicht für LUNs. Wenn Cloud Manager eine LUN erstellt, wird die Autogrow Funktion deaktiviert.

Verwaltung von Inoden mit automatischem Kapazitätsmanagement

Cloud Manager überwacht die Inode-Nutzung auf einem Volume. Wenn 85 % der Inodes verwendet werden, erhöht Cloud Manager die Größe des Volumes, um die Anzahl der verfügbaren Inodes zu erhöhen. Die Anzahl der Dateien, die ein Volume enthalten kann, wird durch die Anzahl der Inodes bestimmt, die es hat.

Manuelles Kapazitätsmanagement

Wenn der Account-Administrator den Modus für das Kapazitätsmanagement auf manuell setzt, zeigt Cloud Manager Meldungen mit erforderlichen Maßnahmen an, wenn Kapazitätsentscheidungen getroffen werden müssen. Die gleichen Beispiele, die im automatischen Modus beschrieben werden, gelten für den manuellen Modus, aber Sie müssen die Aktionen akzeptieren.

Flash Cache

Einige Cloud Volumes ONTAP Konfigurationen in AWS und Azure beinhalten lokalen NVMe-Storage, den Cloud Volumes ONTAP als *Flash Cache* verwendet, um eine bessere Performance zu erzielen.

Was ist Flash Cache?

Flash Cache beschleunigt den Zugriff auf Daten durch intelligente Cache-Speicherung von kürzlich gelesenen Anwenderdaten und NetApp Metadaten in Echtzeit. Es bringt Vorteile bei Random Read-intensiven Workloads, einschließlich Datenbanken, E-Mail und File Services.

Unterstützte Instanzen in AWS

Wählen Sie einen der folgenden EC2-Instanztypen mit einem neuen oder vorhandenen Cloud Volumes ONTAP Premium- oder BYOL-System aus:

- C5d.4xlarge
- C5d.9xlarge

- C5d.18xlarge
- M5d.8xlarge
- M5d.12xlarge
- R5d.2xlarge

Unterstützter VM-Typ in Azure

Wählen Sie in Azure den VM-Typ Standard_L8S_v2 mit einem Cloud Volumes ONTAP BYOL-System mit einem einzelnen Node aus.

Einschränkungen

- Um die Performance-Verbesserungen von Flash Cache nutzen zu können, muss die Komprimierung für alle Volumes deaktiviert sein.

  Entscheiden Sie sich für keine Storage-Effizienz bei der Erstellung eines Volumes aus Cloud Manager, oder erstellen Sie ein Volume und dann "Deaktivieren Sie die Datenkomprimierung über die CLI".

- Cloud Volumes ONTAP unterstützt das Neustarten des Cache nicht, wenn ein Neustart nach einem Neustart erfolgen soll.

WORM-Storage

Sie können WORM-Storage (Write Once, Read Many) auf einem Cloud Volumes ONTAP System aktivieren, um Dateien für einen bestimmten Aufbewahrungszeitraum in unveränderter Form aufzubewahren. WORM Storage basiert auf der SnapLock Technologie im Enterprise-Modus, was bedeutet, dass WORM-Dateien auf Dateiebene geschützt sind.

Nachdem eine Datei in WORM-Storage festgeschrieben wurde, kann sie auch nach Ablauf der Aufbewahrungsfrist nicht mehr geändert werden. Eine manipulationssichere Uhr bestimmt, wann die Aufbewahrungsfrist für eine WORM-Datei abgelaufen ist.

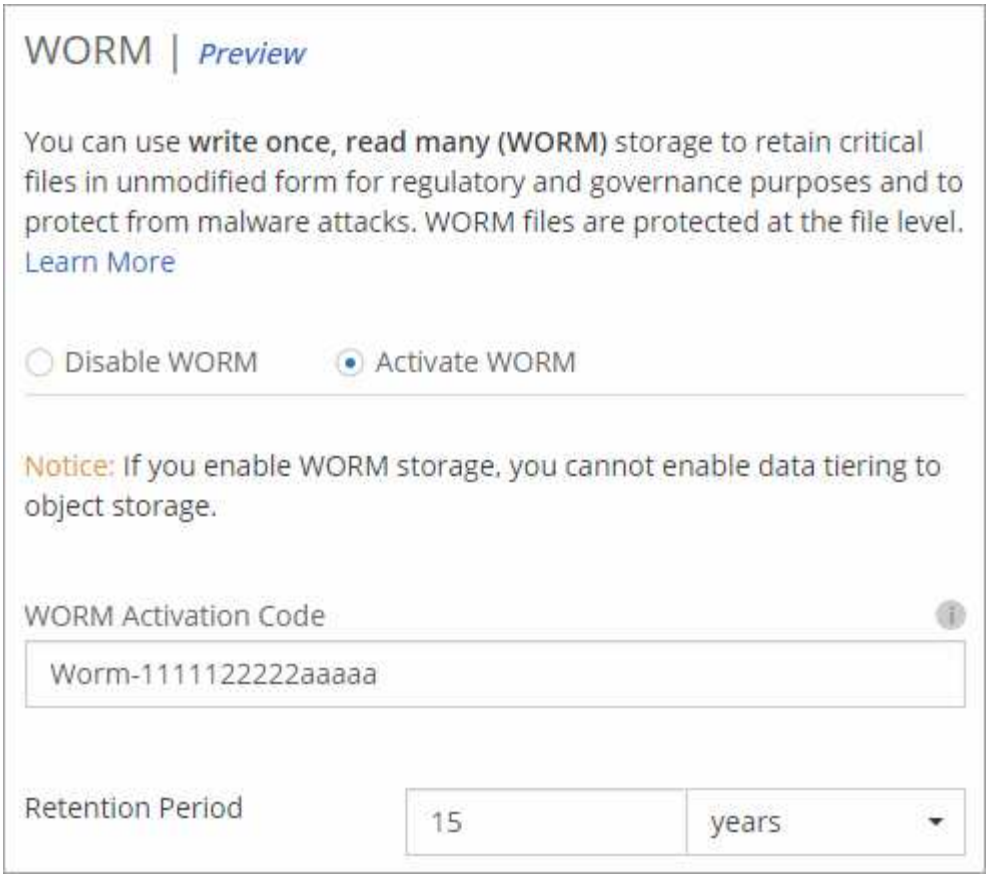
Nach Ablauf der Aufbewahrungsfrist sind Sie dafür verantwortlich, alle Dateien zu löschen, die Sie nicht mehr benötigen.

WORM-Storage wird aktiviert

Sie können WORM Storage auf einem Cloud Volumes ONTAP System aktivieren, wenn Sie eine neue Arbeitsumgebung erstellen. Dazu gehört die Angabe eines Aktivierungscodes und die Festlegung des standardmäßigen Aufbewahrungszeitraums für Dateien. Sie können einen Aktivierungscode erhalten, indem Sie das Chat-Symbol unten rechts in der Cloud Manager-Oberfläche verwenden.

SIE können WORM Storage nicht auf einzelnen Volumes aktivieren—WORM muss auf Systemebene aktiviert sein.

Die folgende Abbildung zeigt, wie WORM-Storage beim Erstellen einer Arbeitsumgebung aktiviert wird:



Dateien werden in WORM gespeichert

Sie können eine Applikation verwenden, um Dateien über NFS oder CIFS in WORM zu übergeben, oder die ONTAP CLI verwenden, um Dateien automatisch in WORM zu übertragen. Sie können auch eine WORM-Datei verwenden, die Daten speichert, die inkrementell geschrieben werden, z. B. Protokollinformationen.

Nachdem Sie WORM Storage auf einem Cloud Volumes ONTAP System aktiviert haben, müssen Sie die ONTAP CLI für das gesamte Management von WORM Storage verwenden. Anweisungen finden Sie unter "ONTAP-Dokumentation".

Cloud Volumes ONTAP Unterstützung für WORM Storage entspricht dem SnapLock Enterprise Modus.

Einschränkungen

- Wenn Sie eine Festplatte direkt aus AWS oder Azure löschen oder verschieben, kann ein Volume vor dem Ablaufdatum gelöscht werden.
- Wenn WORM-Storage aktiviert ist, kann das Daten-Tiering zu Objekt-Storage nicht aktiviert werden.
- Backup in die Cloud muss deaktiviert werden, um WORM-Speicher aktivieren zu können.

Hochverfügbarkeitspaare

Hochverfügbarkeitspaare in AWS

Eine Cloud Volumes ONTAP Hochverfügbarkeitskonfiguration (HA) bietet

unterbrechungsfreien Betrieb und Fehlertoleranz. In AWS werden die Daten zwischen den beiden Nodes synchron gespiegelt.

Überblick

In AWS umfassen die Cloud Volumes ONTAP HA-Konfigurationen die folgenden Komponenten:

- Zwei Cloud Volumes ONTAP Nodes, deren Daten synchron gespiegelt werden.
- Eine Mediatorinstanz, die einen Kommunikationskanal zwischen den Nodes bereitstellt, um die Storage-Übernahme und die Giveback-Prozesse zu unterstützen.

Die Mediatorinstanz führt das Linux-Betriebssystem auf einer t2.micro-Instanz aus und verwendet eine EBS-Magnetplatte mit ca. 8 GB.

Storage-Übernahme und -Giveback

Wenn ein Node ausfällt, kann der andere Node Daten für seinen Partner bereitstellen, um einen kontinuierlichen Datenservice bereitzustellen. Clients können vom Partner-Node aus auf dieselben Daten zugreifen, da die Daten synchron zum Partner gespiegelt wurden.

Nachdem der Node neu gestartet wurde, muss der Partner die Daten neu synchronisieren, bevor er den Storage zurückgeben kann. Die Zeit, die für die Neusynchronisierung von Daten benötigt wird, hängt davon ab, wie viele Daten während des Herunterfahrens des Node geändert wurden.

RPO und RTO

Eine HA-Konfiguration sorgt für eine hohe Verfügbarkeit Ihrer Daten wie folgt:

- Das Recovery Point Objective (RPO) beträgt 0 Sekunden. Ihre Daten sind transaktionskonsistent und ohne Datenverlust.
- Das Recovery Time Objective (RTO) beträgt 60 Sekunden. Im Falle eines Ausfalls sollten die Daten in maximal 60 Sekunden verfügbar sein.

Ha-Bereitstellungsmodelle

Sie können die Hochverfügbarkeit Ihrer Daten sicherstellen, indem Sie eine HA-Konfiguration über mehrere Verfügbarkeitszonen (AZS) oder in einer einzigen AZ bereitstellen. Sie sollten weitere Details zu jeder Konfiguration durchgehen, um zu entscheiden, welche für Ihre Anforderungen am besten geeignet ist.

Cloud Volumes ONTAP HA in mehreren Verfügbarkeitszonen

Durch die Implementierung einer HA-Konfiguration in mehreren Verfügbarkeitszonen (AZS) wird eine hohe Verfügbarkeit Ihrer Daten gewährleistet, wenn ein Ausfall bei einer AZ oder einer Instanz auftritt, die einen Cloud Volumes ONTAP Node ausführt. Sie sollten wissen, wie sich NAS-IP-Adressen auf den Datenzugriff und das Storage-Failover auswirken.

NFS- und CIFS-Datenzugriff

Wenn eine HA-Konfiguration über mehrere Verfügbarkeitszonen verteilt ist, aktivieren *fließende IP-Adressen* den NAS-Client-Zugriff. Die unverankerten IP-Adressen, die für alle VPCs in der Region außerhalb der CIDR-Blöcke liegen müssen, können bei Ausfällen zwischen Nodes migrieren. Für Clients außerhalb der VPC sind sie nicht nativ zugänglich, es sei denn, Sie "AWS Transit Gateway einrichten".

Wenn Sie kein Transit-Gateway einrichten können, sind private IP-Adressen für NAS-Clients außerhalb der VPC verfügbar. Diese IP-Adressen sind jedoch statisch und können nicht zwischen Nodes ein Failover ausführen.

Bevor Sie eine HA-Konfiguration über mehrere Verfügbarkeitszonen hinweg bereitstellen, sollten Sie die Anforderungen für unverankerte IP-Adressen und Weiterleitungstabellen überprüfen. Sie müssen die unverankerten IP-Adressen angeben, wenn Sie die Konfiguration bereitstellen. Die privaten IP-Adressen werden automatisch durch Cloud Manager erstellt.

Weitere Informationen finden Sie unter "AWS Netzwerkanforderungen für Cloud Volumes ONTAP HA in mehreren AZS".

ISCSI-Datenzugriff

VPC-übergreifende Datenkommunikation ist kein Problem, da iSCSI keine Floating-IP-Adressen verwendet.

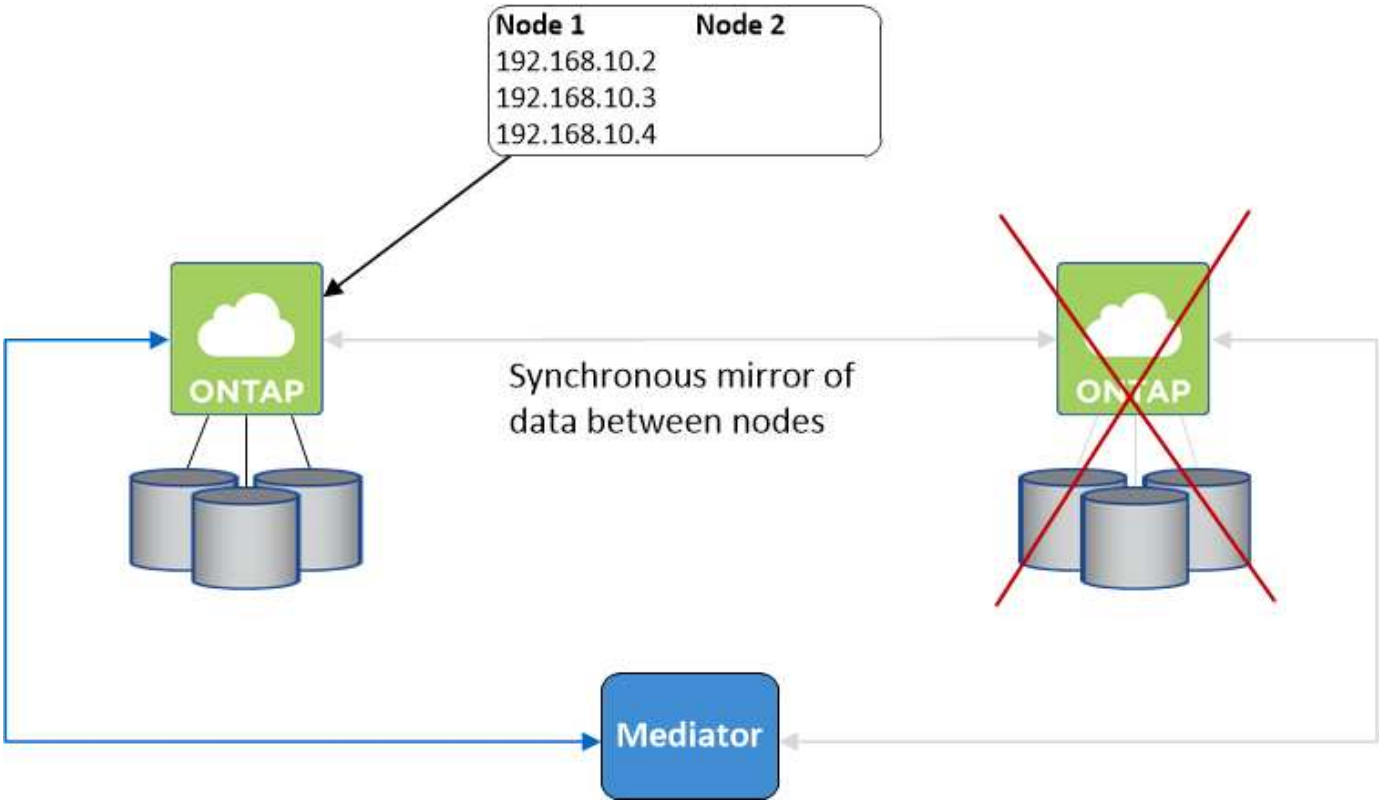
Storage-Übernahme und -Giveback für iSCSI

Für iSCSI verwendet Cloud Volumes ONTAP Multipath I/O (MPIO) und Asymmetric Logical Unit Access (ALUA), um das Pfad-Failover zwischen den Aktiv- und Nicht-optimierten Pfaden zu managen.

Informationen darüber, welche spezifischen Host-Konfigurationen ALUA unterstützen, finden Sie im "NetApp Interoperabilitäts-Matrix-Tool" Sowie das Installations- und Setup-Handbuch für Host Utilities für Ihr Host-Betriebssystem.

Storage-Übernahme und -Giveback für NAS

Wenn die Übernahme in einer NAS-Konfiguration mithilfe von Floating IPs erfolgt, stellt die fließende IP-Adresse des Node dar, über die Clients auf die zu verschiebenden Daten auf den anderen Node zugreifen. Die folgende Abbildung zeigt die Storage-Übernahme in einer NAS-Konfiguration mit Floating-IPs. Wenn Node 2 ausfällt, wird die unverankerte IP-Adresse für Node 2 zu Node 1 verschoben.



NAS-Daten-IPs, die für den externen VPC-Zugriff verwendet werden, können nicht zwischen Nodes migriert werden, wenn Fehler auftreten. Wenn ein Node offline geht, müssen Sie Volumes manuell über die IP-Adresse auf dem anderen Node auf Clients außerhalb des VPC neu mounten.

Nachdem der ausgefallene Node wieder online ist, mounten Sie Clients mit der ursprünglichen IP-Adresse erneut auf Volumes. Dieser Schritt ist erforderlich, um die Übertragung unnötiger Daten zwischen zwei HA-Nodes zu vermeiden, was erhebliche Auswirkungen auf die Performance und Stabilität haben kann.

Sie können einfach die richtige IP-Adresse aus Cloud Manager ermitteln, indem Sie das Volume auswählen und auf **Mount Command** klicken.

Cloud Volumes ONTAP HA in einer einzigen Verfügbarkeitszone

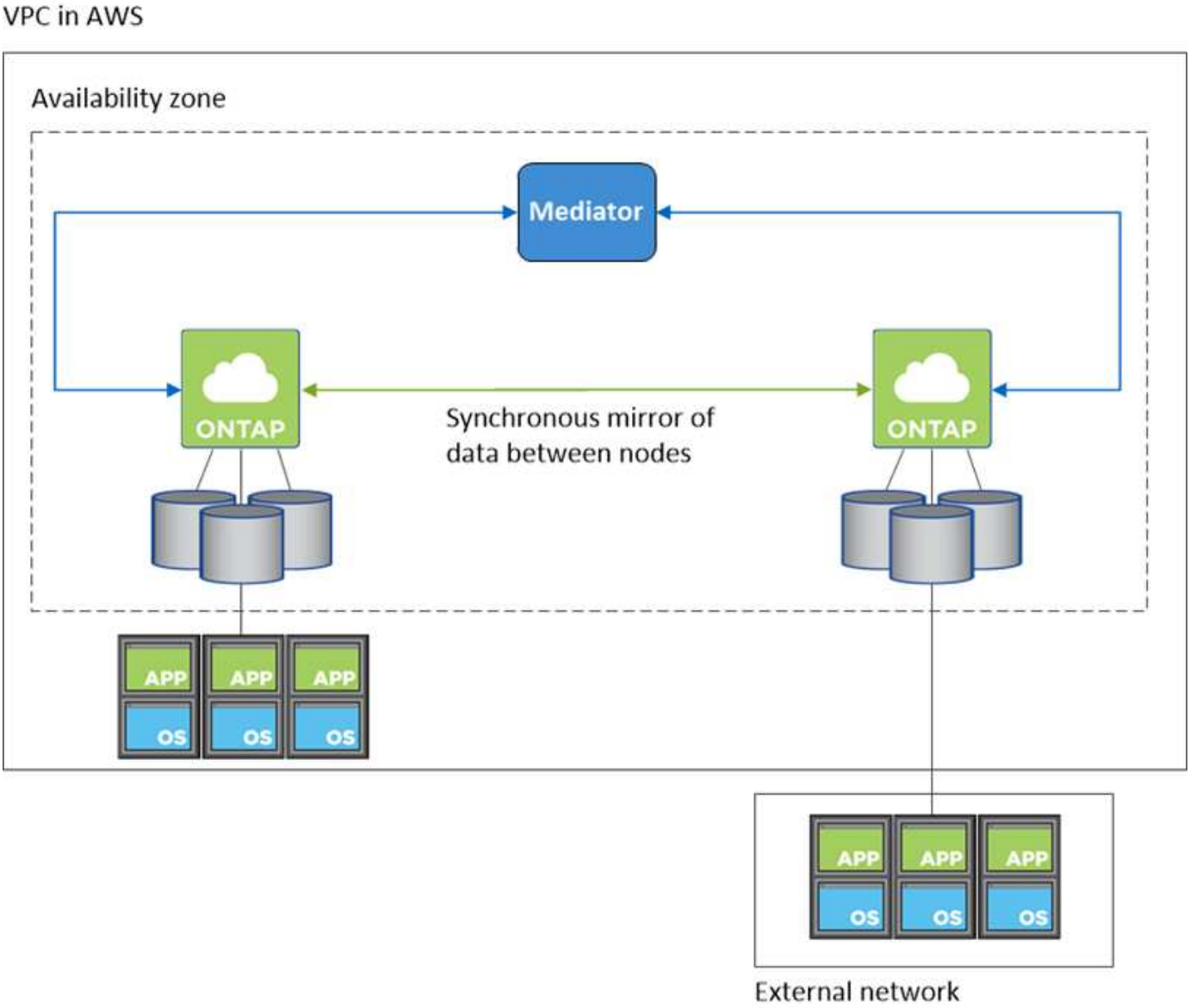
Durch die Implementierung einer HA-Konfiguration in einer einzelnen Verfügbarkeitszone (AZ) kann eine hohe Verfügbarkeit Ihrer Daten sichergestellt werden, wenn eine Instanz, auf der ein Cloud Volumes ONTAP Node ausgeführt wird, ausfällt. Alle Daten sind nativ von außerhalb des VPC zugänglich.

> Cloud Manager erstellt eine "AWS Spread-Platzierungsgruppe" Und startet die beiden HA-Nodes in dieser Platzierungsgruppe. Die Platzierungsgruppe verringert das Risiko gleichzeitiger Ausfälle, indem sie die Instanzen auf unterschiedliche zugrunde liegende Hardware verteilt. Diese Funktion verbessert die Redundanz aus Sicht des Computing und nicht aus Sicht des Festplattenausfalls.

Datenzugriff

Da sich diese Konfiguration in einer einzigen AZ befindet, sind keine gleitenden IP-Adressen erforderlich. Sie können dieselbe IP-Adresse für den Datenzugriff innerhalb des VPC und außerhalb des VPC verwenden.

Die folgende Abbildung zeigt eine HA-Konfiguration in einer einzigen AZ. Der Zugriff auf die Daten erfolgt innerhalb des VPC und außerhalb des VPC.



Storage-Übernahme und -Giveback

Für iSCSI verwendet Cloud Volumes ONTAP Multipath I/O (MPIO) und Asymmetric Logical Unit Access (ALUA), um das Pfad-Failover zwischen den Aktiv- und Nicht-optimierten Pfaden zu managen.

> Informationen darüber, welche spezifischen Host-Konfigurationen ALUA unterstützen, finden Sie im "NetApp Interoperabilitäts-Matrix-Tool" Sowie das Installations- und Setup-Handbuch für Host Utilities für Ihr Host-Betriebssystem.

Bei NAS-Konfigurationen können die Daten-IP-Adressen zwischen HA-Nodes migriert werden, wenn Fehler auftreten. Dadurch wird der Client-Zugriff auf Storage gewährleistet.

Funktionsweise von Storage in einem HA-Paar

Im Gegensatz zu einem ONTAP Cluster wird Storage in einem Cloud Volumes ONTAP HA Paar nicht zwischen Nodes geteilt. Stattdessen werden die Daten synchron zwischen den Nodes gespiegelt, sodass sie im Falle eines Ausfalls verfügbar sind.

Storage-Zuweisung

Wenn Sie ein neues Volume erstellen und zusätzliche Festplatten erforderlich sind, weist Cloud Manager beiden Nodes die gleiche Anzahl von Festplatten zu, erstellt ein gespiegeltes Aggregat und erstellt dann das neue Volume. Wenn beispielsweise zwei Festplatten für das Volume erforderlich sind, weist Cloud Manager zwei Festplatten pro Node für insgesamt vier Festplatten zu.

Storage-Konfigurationen

Sie können ein HA-Paar als Aktiv/Aktiv-Konfiguration verwenden, in der beide Nodes Daten an Clients bereitstellen, oder als Aktiv/Passiv-Konfiguration, bei der der passive Node nur dann auf Datenanforderungen reagiert, wenn er Storage für den aktiven Node übernommen hat.

Sie können eine Aktiv/Aktiv-Konfiguration nur einrichten, wenn Sie Cloud Manager in der Storage System View verwenden.

Performance-Erwartungen für eine HA-Konfiguration

Eine Cloud Volumes ONTAP HA-Konfiguration repliziert Daten synchron zwischen Nodes, wodurch Netzwerkbandbreite verbraucht wird. Daher können Sie im Vergleich zu einer Single Node Cloud Volumes ONTAP Konfiguration folgende Performance erwarten:

- Bei HA-Konfigurationen, die Daten von nur einem Node bereitstellen, ist die Lese-Performance mit der Lese-Performance einer Single-Node-Konfiguration vergleichbar, während die Schreib-Performance geringer ist.
- Bei HA-Konfigurationen, die Daten von beiden Nodes verarbeiten, ist die Lese-Performance höher als die Lese-Performance einer Single-Node-Konfiguration, und die Schreib-Performance ist gleich oder höher.

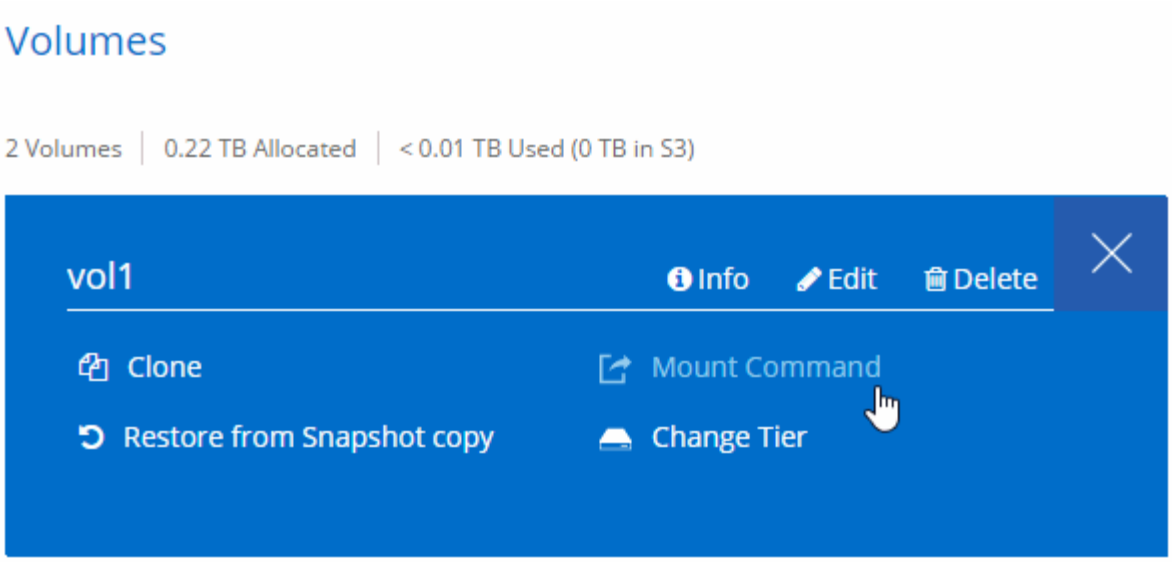
Weitere Informationen zur Performance von Cloud Volumes ONTAP finden Sie unter "Leistung".

Client-Zugriff auf Storage

Clients sollten über die Daten-IP-Adresse des Node, auf dem sich das Volume befindet, auf NFS- und CIFS-Volumes zugreifen. Wenn NAS-Clients über die IP-Adresse des Partner-Node auf ein Volume zugreifen, wird der Datenverkehr zwischen beiden Nodes geleitet, wodurch die Performance verringert wird.

Wenn Sie ein Volume zwischen Nodes in einem HA-Paar verschieben, sollten Sie das Volume mithilfe der IP-Adresse des anderen Node neu mounten. Andernfalls kann die Performance beeinträchtigt werden. Wenn Clients NFSv4-Verweise oder Ordnerumleitung für CIFS unterstützen, können Sie diese Funktionen auf den Cloud Volumes ONTAP Systemen aktivieren, um ein erneutes Mounten des Volumes zu vermeiden. Weitere Informationen finden Sie in der ONTAP Dokumentation.

Sie können einfach die richtige IP-Adresse aus Cloud Manager ermitteln:

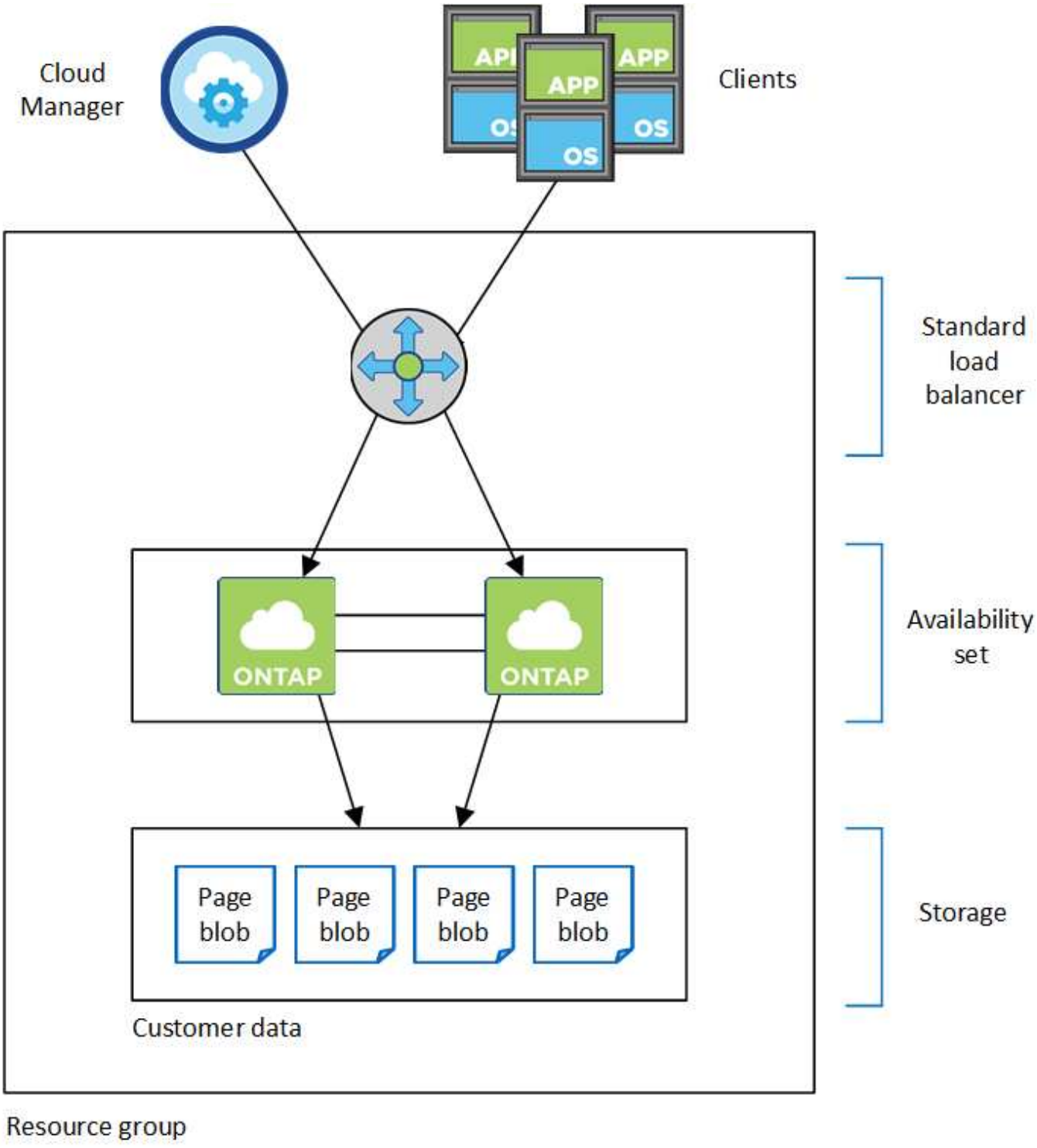


Hochverfügbarkeitspaare in Azure

Ein HA-Paar von Cloud Volumes ONTAP bietet Zuverlässigkeit der Enterprise-Klasse und unterbrechungsfreien Betrieb bei Ausfällen in Ihrer Cloud-Umgebung. In Azure wird der Storage zwischen den beiden Nodes gemeinsam genutzt.

HA-Komponenten

Eine Cloud Volumes ONTAP HA-Konfiguration in Azure umfasst die folgenden Komponenten:



Beachten Sie Folgendes über die Azure Komponenten, die Cloud Manager für Sie implementiert:

Azure Standard Load Balancer

Der Load Balancer managt den eingehenden Datenverkehr zum Cloud Volumes ONTAP HA-Paar.

Verfügbarkeitsgruppe

Das Verfügbarkeitsset stellt sicher, dass sich die Knoten in unterschiedlichen Fehler- und Updatedomänen befinden.

Festplatten

Die Kundendaten werden auf den Blobs für Premium Storage Seite gespeichert. Jeder Node hat Zugriff auf den Storage des anderen Nodes. Für ist auch zusätzlicher Speicher erforderlich "Boot-, Root- und Core-Daten".

Konten mit Storage-Systemen

- Für verwaltete Festplatten ist ein Speicherkonto erforderlich.
- Für die Blobs auf Premium Storage-Seite sind mindestens ein Storage-Konto erforderlich, da das Kapazitätslimit pro Storage-Konto erreicht wird.

  "Azure Dokumentation: Skalierbarkeit und Performance von Azure Storage-Konten".

- Für das Daten-Tiering zu Azure Blob Storage ist ein Storage-Konto erforderlich.
- Ab Cloud Volumes ONTAP 9.7 sind die Storage-Konten, die Cloud Manager für HA-Paare erstellt, allgemeine v2 Storage-Konten.
- Sie können bei der Erstellung einer Arbeitsumgebung eine HTTPS-Verbindung von einem Cloud Volumes ONTAP 9.7 HA-Paar zu Azure Storage-Konten aktivieren. Beachten Sie, dass die Aktivierung dieser Option sich auf die Schreib-Performance auswirken kann. Sie können die Einstellung nicht ändern, nachdem Sie die Arbeitsumgebung erstellt haben.

RPO und RTO

Eine HA-Konfiguration sorgt für eine hohe Verfügbarkeit Ihrer Daten wie folgt:

- Das Recovery Point Objective (RPO) beträgt 0 Sekunden. Ihre Daten sind transaktionskonsistent und ohne Datenverlust.
- Das Recovery Time Objective (RTO) beträgt 60 Sekunden. Im Falle eines Ausfalls sollten die Daten in maximal 60 Sekunden verfügbar sein.

Storage-Übernahme und -Giveback

Storage in einem Azure HA-Paar wird, ähnlich wie bei einem physischen ONTAP Cluster, von den Nodes gemeinsam genutzt. Durch Verbindungen zum Storage des Partners kann jeder Node im Falle einer Übernahme_ auf den Storage des anderen zugreifen. Durch Failover-Mechanismen von Netzwerkpfaden wird sichergestellt, dass Clients und Hosts weiterhin mit dem verbleibenden Node kommunizieren. Der Partner_gibt Back_ Storage zurück, wenn der Node wieder in den Online-Modus versetzt wird.

Bei NAS-Konfigurationen werden Daten-IP-Adressen bei Ausfällen automatisch zwischen HA Nodes migriert.

Für iSCSI verwendet Cloud Volumes ONTAP Multipath I/O (MPIO) und Asymmetric Logical Unit Access (ALUA), um das Pfad-Failover zwischen den Aktiv- und Nicht-optimierten Pfaden zu managen.

Informationen darüber, welche spezifischen Host-Konfigurationen ALUA unterstützen, finden Sie im "NetApp Interoperabilitäts-Matrix-Tool" Sowie das Installations- und Setup-Handbuch für Host Utilities für Ihr Host-Betriebssystem.

Storage-Konfigurationen

Sie können ein HA-Paar als Aktiv/Aktiv-Konfiguration verwenden, in der beide Nodes Daten an Clients bereitstellen, oder als Aktiv/Passiv-Konfiguration, bei der der passive Node nur dann auf Datenanforderungen reagiert, wenn er Storage für den aktiven Node übernommen hat.

HA-Einschränkungen

Die folgenden Einschränkungen betreffen Cloud Volumes ONTAP HA-Paare in Azure:

- HA-Paare werden mit Cloud Volumes ONTAP Standard, Premium und BYOL unterstützt. Explore wird nicht unterstützt.
- NFSv4 wird nicht unterstützt. NFSv3 wird unterstützt.
- HA-Paare werden in einigen Regionen nicht unterstützt.

  "Siehe die Liste der unterstützten Azure Regionen".

"So implementieren Sie ein HA-System in Azure".

Bewertung

Vor der Zahlung für die Software können Sie Cloud Volumes ONTAP auswerten. Am häufigsten starten Sie die PAYGO-Version Ihres ersten Cloud Volumes ONTAP-Systems, um eine kostenlose 30-Tage-Testversion zu erhalten. Auch eine Evaluation-BYOL-Lizenz ist eine Option.

Wenn Sie Hilfe bei Ihren Machbarkeitsstudien benötigen, wenden Sie sich an "Das Vertriebsteam" Oder wenden Sie sich an die Chat-Option, die über verfügbar ist "NetApp Cloud Central" Und aus Cloud Manager heraus.

30-Tage-Testversionen für PAYGO

Wenn Sie für Cloud Volumes ONTAP nutzungsbasiert bezahlen möchten, steht Ihnen eine kostenlose 30-Tage-Testversion zur Verfügung. Eine kostenlose 30-Tage-Testversion von Cloud Volumes ONTAP können Sie von Cloud Manager starten, indem Sie Ihr erstes Cloud Volumes ONTAP-System für einen Zahler erstellen.

Für die Instanz fallen keine stündlichen Lizenzgebühren für Software an, es gelten jedoch nach wie vor Gebühren für die Infrastruktur Ihres Cloud-Providers.

Eine kostenlose Testversion wird automatisch in ein kostenpflichtiges stündliches Abonnement umgewandelt, sobald diese abläuft. Wenn Sie die Instanz innerhalb des Zeitlimits beenden, ist die nächste Instanz, die Sie bereitstellen, nicht Teil der kostenlosen Testversion (selbst wenn sie innerhalb dieser 30 Tage bereitgestellt wird).

Die Very-As-you-go-Tests werden bei einem Cloud-Provider vergeben und können auf keinen Fall erweitert werden.

Evaluierungslizenzen für BYOL

Kunden, die mit dem Kauf einer NetApp Lizenz rechnen, erwerben Cloud Volumes ONTAP eine Evaluierungslizenz. Sie können eine Evaluierungslizenz von Ihrem Account-Team, Ihrem Sales Engineer oder Ihrem Partner erhalten.

Der Auswertungsschlüssel ist 30 Tage lang gut und kann mehrmals, jeweils für 30 Tage (unabhängig vom Erstellungstag) verwendet werden.

Nach 30 Tagen werden tägliche Abschaltungen stattfinden, daher ist es am besten, im Voraus zu planen. Für ein in-Place-Upgrade kann eine neue BYOL-Lizenz auf die Evaluierungslizenz angewendet werden (hierfür ist

ein Neustart einzelner Node-Systeme erforderlich). Ihre gehosteten Daten werden am Ende des Testzeitraums **nicht** gelöscht.

Sie können kein Upgrade der Cloud Volumes ONTAP Software mit einer Evaluierungslizenz durchführen.

Lizenzierung

Für jedes Cloud Volumes ONTAP BYOL-System muss eine Systemlizenz mit einem aktiven Abonnement installiert sein. Cloud Manager vereinfacht den Prozess, indem Sie Lizenzen für Sie verwalten und Sie vor Ablauf benachrichtigen. Byol-Lizenzen sind auch für Backup in der Cloud verfügbar.

Byol-Systemlizenzen

Sie können mehrere Lizenzen für ein Cloud Volumes ONTAP BYOL-System erwerben und so mehr als 368 TB Kapazität zuweisen. Beispielsweise können Sie zwei Lizenzen erwerben, um Cloud Volumes ONTAP bis zu 736 TB Kapazität zuzuweisen. Alternativ können Sie vier Lizenzen erwerben, um bis zu 1.4 PB zu erhalten.

Die Anzahl der Lizenzen, die Sie für ein Single Node-System oder ein HA-Paar erwerben können, ist unbegrenzt.

Beachten Sie, dass die Festplattenbeschränkungen verhindern können, dass Sie durch die Verwendung von Festplatten allein das Kapazitätslimit nicht erreichen. Sie können die Festplattengrenze um überschreiten "tiering inaktiver Daten in Objektspeicher". Weitere Informationen zu Festplattenlimits finden Sie unter "Speichergrenzwerte in den Versionshinweisen zu Cloud Volumes ONTAP".

Lizenzmanagement für ein neues System

Wenn Sie ein BYOL-System erstellen, werden Sie von Cloud Manager zur Seriennummer Ihrer Lizenz und Ihres NetApp Support Site Kontos aufgefordert. Cloud Manager verwendet das Konto, um die Lizenzdatei von NetApp herunterzuladen und auf dem Cloud Volumes ONTAP-System zu installieren.

"Erfahren Sie, wie Sie NetApp Support Site Konten in Cloud Manager hinzufügen".

Wenn Cloud Manager über die sichere Internetverbindung nicht auf die Lizenzdatei zugreifen kann, können Sie die Datei selbst beziehen und die Datei anschließend manuell auf Cloud Manager hochladen. Anweisungen hierzu finden Sie unter "Byol-Lizenzen für Cloud Volumes ONTAP verwalten".

Warnung zum Ablauf der Lizenz

Cloud Manager warnt Sie 30 Tage vor Ablauf einer Lizenz und erneut nach Ablauf der Lizenz. Die folgende Abbildung zeigt eine 30-Tage-Ablaufwarnung:

Sie können die Arbeitsumgebung auswählen, in der die Nachricht angezeigt werden soll.

Wenn Sie die Lizenz nicht rechtzeitig verlängern, wird das Cloud Volumes ONTAP System heruntergefahren. Wenn Sie ihn neu starten, fährt er sich wieder herunter.

> Cloud Volumes ONTAP kann Sie auch per E-Mail, SNMP Traphost oder Syslog-Server über EMS (Event Management System)-Ereignisbenachrichtigungen benachrichtigen. Anweisungen hierzu finden Sie im "ONTAP 9 EMS Configuration Express Guide".

Lizenzerneuerung

Wenn Sie ein Byol Abonnement erneuern, indem Sie sich an einen NetApp Vertreter wenden, erhält Cloud Manager automatisch die neue Lizenz von NetApp und installiert sie auf dem Cloud Volumes ONTAP System.

Wenn Cloud Manager über die sichere Internetverbindung nicht auf die Lizenzdatei zugreifen kann, können Sie die Datei selbst beziehen und die Datei anschließend manuell auf Cloud Manager hochladen. Anweisungen hierzu finden Sie unter "Byol-Lizenzen für Cloud Volumes ONTAP verwalten".

Byol-Backup-Lizenzen

Mit einer BYOL-Backup-Lizenz können Sie eine Lizenz von NetApp erwerben und Backup in der Cloud für einen bestimmten Zeitraum und für eine maximale Menge an Backup-Speicherplatz verwenden. Wenn eine der beiden Limits erreicht ist, müssen Sie die Lizenz erneuern.

"Weitere Informationen zur BYOL-Lizenz für Backup in der Cloud".

Sicherheit

Cloud Volumes ONTAP unterstützt die Datenverschlüsselung und bietet Schutz vor Viren und Ransomware.

Verschlüsselung von Daten im Ruhezustand

Cloud Volumes ONTAP unterstützt die folgenden Verschlüsselungstechnologien:

- NetApp Verschlüsselungslösungen (NVE und NAE)
- AWS Key Management Service
- Azure Storage Service Encryption
- Google Cloud Platform-Standardverschlüsselung

Sie können NetApp Verschlüsselungslösungen mit nativer Verschlüsselung von AWS, Azure oder GCP verwenden, die Daten auf Hypervisor-Ebene verschlüsseln. Auf diese Weise wäre eine doppelte Verschlüsselung möglich, die für sehr sensible Daten wünschenswert wäre. Wenn auf die verschlüsselten Daten zugegriffen wird, sind sie zweimal unverschlüsselt – einmal auf Hypervisor-Ebene (bei Verwendung von Schlüsseln des Cloud-Providers) und dann erneut mit NetApp Verschlüsselungslösungen (mit Schlüsseln von einem externen Schlüsselmanager).

NetApp Verschlüsselungslösungen (NVE und NAE)

Cloud Volumes ONTAP unterstützt sowohl NetApp Volume Encryption (NVE) als auch NetApp Aggregate Encryption (NAE) mit einem externen Schlüsselmanager. NVE und NAE sind softwarebasierte Lösungen, mit

denen die Verschlüsselung von Volumes im Ruhezustand (FIPS) 140-2-konform unterstützt wird.

- NVE verschlüsselt Daten im Ruhezustand nach einem Volume pro Zeit. Jedes Daten-Volume verfügt über einen eigenen eindeutigen Verschlüsselungsschlüssel.
- NAE ist eine Erweiterung von NVE, denn es verschlüsselt Daten für jedes Volume, und die Volumes teilen sich einen Schlüssel im gesamten Aggregat. NAE ermöglicht außerdem die Deduplizierung allgemeiner Blöcke aller Volumes im Aggregat.

Sowohl NVE als auch NAE nutzen 256-Bit-Verschlüsselung nach AES.

"Weitere Informationen erhalten Sie unter NetApp Volume Encryption und NetApp Aggregate Encryption".

Ab Cloud Volumes ONTAP 9.7 haben neue Aggregate die NetApp Aggregate Verschlüsselung (NAE) standardmäßig aktiviert, nachdem Sie einen externen Schlüsselmanager eingerichtet haben. Für neue Volumes, die nicht Teil eines NAE-Aggregats sind, ist standardmäßig NetApp Volume Encryption (NVE) aktiviert (bei vorhandenen Aggregaten, die vor dem Einrichten eines externen Schlüsselmanagers erstellt wurden).

Die Einrichtung eines unterstützten Schlüsselmanagers ist der einzige erforderliche Schritt. Anweisungen zur Einrichtung finden Sie unter "Verschlüsseln von Volumes mit NetApp Verschlüsselungslösungen".

AWS Key Management Service

Wenn Sie ein Cloud Volumes ONTAP System in AWS starten, können Sie die Datenverschlüsselung über das aktivieren "AWS KMS (Key Management Service)". Cloud Manager fordert Datenschlüssel mit einem Customer Master Key (CMK) an.

Sie können die AWS Datenverschlüsselungsmethode nicht ändern, nachdem Sie ein Cloud Volumes ONTAP System erstellt haben.

Wenn Sie diese Verschlüsselungsoption verwenden möchten, müssen Sie sicherstellen, dass AWS KMS ordnungsgemäß eingerichtet ist. Weitere Informationen finden Sie unter "Einrichten des AWS KMS".

Azure Storage Service Encryption

"Azure Storage Service Encryption" Für Daten im Ruhezustand ist Cloud Volumes ONTAP-Daten in Azure standardmäßig aktiviert. Es ist keine Einrichtung erforderlich.

Sie können von Azure gemanagte Festplatten auf Cloud Volumes ONTAP-Systemen mit einem einzelnen Node mit externen Schlüsseln von einem anderen Konto verschlüsseln. Diese Funktion wird durch Cloud Manager APIs unterstützt.

Beim Erstellen des Single-Node-Systems müssen Sie lediglich Folgendes zur API-Anforderung hinzufügen:

```
"azureEncryptionParameters": {
      "key": <azure id of encryptionset>
  }
```

Von Kunden verwaltete Schlüssel werden nicht durch Cloud Volumes ONTAP HA-Paare unterstützt.

Google Cloud Platform-Standardverschlüsselung

"Google Cloud-Plattform Verschlüsselung von Daten im Ruhezustand" Ist standardmäßig für Cloud Volumes ONTAP aktiviert. Es ist keine Einrichtung erforderlich.

Während Google Cloud Storage Ihre Daten immer verschlüsselt, bevor sie auf die Festplatte geschrieben werden, können Sie mithilfe der Cloud-Manager-APIs ein Cloud Volumes ONTAP-System erstellen, das *von Kunden gemanagte Verschlüsselungsschlüssel* verwendet. Diese Schlüssel werden in GCP mithilfe des Cloud Key Management Service generiert und gemanagt. "Weitere Informationen .".

ONTAP Virenscannen

Sie können integrierte Virenschutzfunktionen auf ONTAP Systemen verwenden, um Daten vor Viren oder anderem schädlichen Code zu schützen.

ONTAP Virus Scanning, genannt *Vscan*, kombiniert erstklassige Antivirensoftware von Drittanbietern mit ONTAP-Funktionen, die Ihnen die Flexibilität geben, die Sie benötigen, um zu kontrollieren, welche Dateien gescannt werden und wann.

Informationen zu den von Vscan unterstützten Herstellern, Software und Versionen finden Sie im "NetApp Interoperabilitätsmatrix".

Informationen zum Konfigurieren und Managen der Antivirenfunktionen auf ONTAP-Systemen finden Sie im "ONTAP 9 Antivirus Configuration Guide".

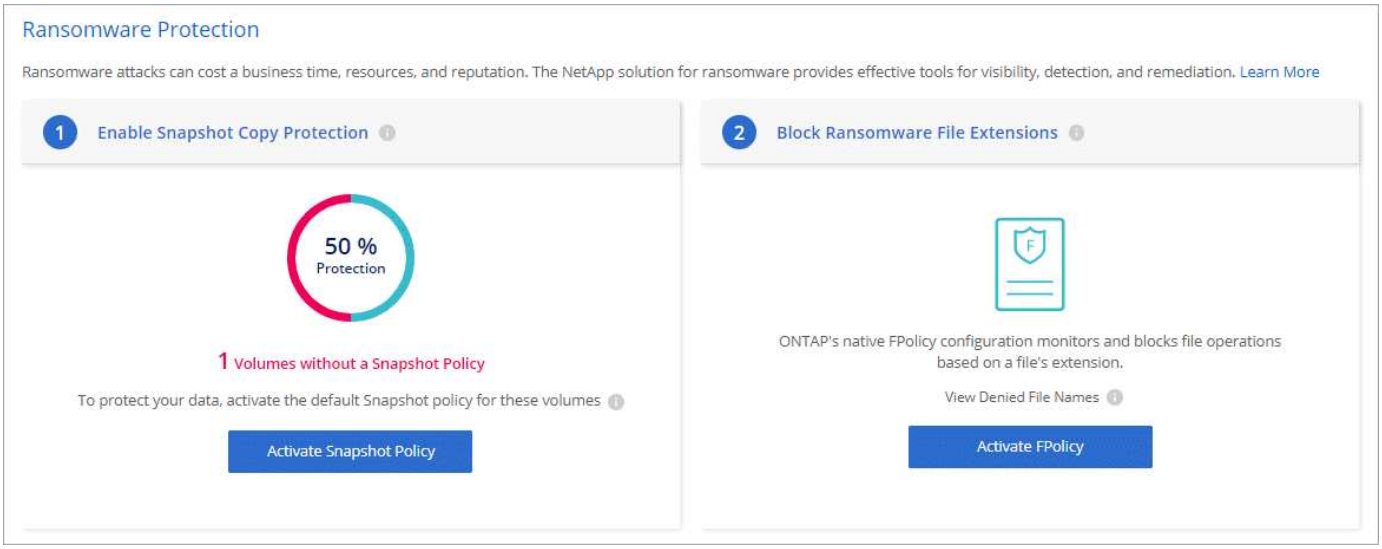
Schutz durch Ransomware

Ransomware-Angriffe können das Unternehmen Zeit, Ressourcen und Image-Schäden kosten. Cloud Manager ermöglicht die Implementierung der NetApp Lösung für Ransomware, die mit effektiven Tools für Transparenz, Erkennung und Korrektur ausgestattet ist.

- Cloud Manager ermittelt Volumes, die nicht durch eine Snapshot-Richtlinie geschützt sind, und ermöglicht Ihnen die Aktivierung der Standard-Snapshot-Richtlinie für diese Volumes.

  Snapshot Kopien sind schreibgeschützt, der Ransomware-Beschädigungen verhindert. Sie können außerdem die Granularität nutzen, um Images einer einzelnen Dateikopie oder einer kompletten Disaster-Recovery-Lösung zu erstellen.

- Cloud Manager ermöglicht es Ihnen auch, gängige Ransomware-Dateiendungen durch die Unterstützung der ONTAP FPolicy Lösung zu blockieren.



"So implementieren Sie die NetApp Lösung für Ransomware".

Leistung

Sie können die Performance-Ergebnisse überprüfen, um zu entscheiden, welche Workloads für Cloud Volumes ONTAP geeignet sind.

- Cloud Volumes ONTAP für AWS

  "NetApp Technical Report 4383: Performance Characterization of Cloud Volumes ONTAP in Amazon Web Services with Application Workloads".

- Cloud Volumes ONTAP für Microsoft Azure

  "Technischer Bericht von NetApp 4671: Performance-Charakterisierung von Cloud Volumes ONTAP in Azure mit Applikations-Workloads".

- Cloud Volumes ONTAP für Google Cloud

  "Technischer Bericht 4816: Performance-Merkmale von Cloud Volumes ONTAP für Google Cloud".

Standardkonfiguration für Cloud Volumes ONTAP

Wenn Sie verstehen, wie Cloud Volumes ONTAP standardmäßig konfiguriert ist, können Sie Ihre Systeme einrichten und verwalten. Dies gilt insbesondere, wenn Sie mit ONTAP vertraut sind, da sich das Standard-Setup für Cloud Volumes ONTAP von ONTAP unterscheidet.

Standardwerte

- Cloud Volumes ONTAP ist als Single-Node-System in AWS, Azure und GCP verfügbar und als HA-Paar in AWS und Azure.
- Cloud Manager erstellt bei der Implementierung von Cloud Volumes ONTAP eine Storage-VM mit Datenservice. Einige Konfigurationen unterstützen zusätzliche Storage VMs. "Erfahren Sie mehr über das

Management von Storage VMs".

- Cloud Manager installiert die folgenden ONTAP Funktionslizenzen automatisch auf Cloud Volumes ONTAP:
  - CIFS
  - FlexCache
  - FlexClone
  - ISCSI
  - NetApp Volume Encryption (nur für BYOL oder registrierte PAYGO Systeme)
  - NFS
  - SnapMirror
  - SnapRestore
  - SnapVault
- Standardmäßig werden mehrere Netzwerkschnittstellen erstellt:
  - Eine Cluster Management-LIF
  - Eine Intercluster-LIF
  - SVM-Management-LIF auf HA-Systemen in Azure, Single-Node-Systeme in AWS und optional auf HA-Systemen in mehreren AWS Availability Zones
  - Eine Node Management-LIF
  - Eine iSCSI-Daten-LIF
  - Eine CIFS- und NFS-Daten-LIF

  Aufgrund der EC2-Anforderungen ist das LIF-Failover für Cloud Volumes ONTAP standardmäßig deaktiviert. Durch die Migration einer LIF auf einen anderen Port wird die externe Zuordnung zwischen IP-Adressen und Netzwerkschnittstellen in der Instanz aufgehoben, sodass der LIF nicht mehr zugänglich ist.

- Cloud Volumes ONTAP sendet Konfigurations-Backups über HTTPS an den Connector.

  Auf die Backups kann über zugegriffen werden https://ipaddress/occm/offboxconfig/ Wobei *ipaddress* die IP-Adresse des Connector-Hosts ist.

- Cloud Manager legt einige Volume-Attribute anders fest als andere Management-Tools (z. B. System Manager oder CLI).

  In der folgenden Tabelle sind die Volume-Attribute aufgeführt, die Cloud Manager anders als die Standardeinstellungen festlegt:

Attribut	Vom Cloud Manager festgelegter Wert
AutoSize Modus	Wachsen

Attribut	Vom Cloud Manager festgelegter Wert
Maximale automatische Größe	1.000 Prozent Der Kontoadministrator kann diesen Wert auf der Seite Einstellungen ändern.
Sicherheitsstil	NTFS für CIFS-Volumes UNIX für NFS-Volumes
Platz garantiert Stil	Keine
UNIX-Berechtigungen (nur NFS)	777

Informationen zu diesen Attributen finden Sie auf der Seite „*Volume create* man“.

Boot- und Root-Daten für Cloud Volumes ONTAP

Zusätzlich zum Storage für Benutzerdaten erwirbt Cloud Manager auch Cloud Storage für Boot- und Root-Daten auf jedem Cloud Volumes ONTAP System.

AWS

- Zwei Festplatten pro Node für Boot- und Root-Daten:
  - 9.7: 160-GB-io1-Festplatte für Boot-Daten und eine 220-GB-gp2-Festplatte für Stammdaten
  - 9.6: 93-GB-io1-Festplatte für Boot-Daten und eine 140-GB-gp2-Festplatte für Stammdaten
  - 9.5: 45-GB-io1-Festplatte für Boot-Daten und eine 140-GB-gp2-Festplatte für Stammdaten
- Ein EBS-Snapshot für jede Boot- und Root-Festplatte
- Bei HA-Paaren ist ein EBS-Volume für die Mediator-Instanz, das ca. 8 GB beträgt

Azure (Single Node)

- Drei Premium-SSD-Festplatten:
  - Eine 10-GB-Festplatte für Boot-Daten
  - Eine 140-GB-Festplatte für Stammdaten
  - Eine 128-GB-Festplatte für NVRAM

    Wenn die virtuelle Maschine, die Sie für Cloud Volumes ONTAP ausgewählt haben, Ultra-SSDs unterstützt, verwendet das System statt einer Premium-SSD eine Ultra-SSD für NVRAM.
- Eine 1024-GB-Standardfestplatte zum Speichern der Kerne
- Ein Azure Snapshot für jedes Boot- und Root-Laufwerk

Azure (HA-Paare)

- Zwei 10-GB-Premium-SSD-Laufwerke für das Boot-Volume (eine pro Node)
- Zwei Blobs für 140 GB Premium-Storage für das Root-Volume (eine pro Node)

- Zwei 1024-GB-Standard-HDD-Festplatten zum Speichern der Cores (eine pro Node)
- Zwei 128-GB-Premium-SSD-Festplatten für NVRAM (eine pro Node)
- Ein Azure Snapshot für jedes Boot- und Root-Laufwerk

GCP

- Eine persistente 10-GB-Standardfestplatte für Boot-Daten
- Eine persistente 64-GB-Standardfestplatte für Stammdaten
- Eine persistente 500-GB-Standardfestplatte für NVRAM
- Eine persistente 216-GB-Standardfestplatte zum Speichern der Kerne
- Je ein GCP-Snapshot für die Boot-Festplatte und die Root-Festplatte

Wo sich die Festplatten befinden

Cloud Manager legt den Storage wie folgt vor:

- Boot-Daten befinden sich auf einem Laufwerk, das mit der Instanz oder Virtual Machine verbunden ist.

  Diese Festplatte, die das Boot-Image enthält, steht Cloud Volumes ONTAP nicht zur Verfügung.

- Die Stammdaten, die die Systemkonfiguration und die Protokolle enthalten, befinden sich in aggr0.
- Das Root-Volume der Storage Virtual Machine (SVM) befindet sich in aggr1.
- Daten-Volumes befinden sich auch in aggr1.

Verschlüsselung

Boot- und Root-Festplatten sind in Azure und Google Cloud Platform immer verschlüsselt, da bei diesen Cloud-Providern die Verschlüsselung standardmäßig aktiviert ist.

Wenn Sie die Datenverschlüsselung in AWS mithilfe des KMS (Key Management Service) aktivieren, werden sowohl Boot- als auch Root-Festplatten für Cloud Volumes ONTAP verschlüsselt. Dazu gehört die Boot-Festplatte für die Instanz des Mediators in einem HA-Paar. Die Laufwerke werden über das CMK verschlüsselt, das Sie bei der Erstellung der Arbeitsumgebung auswählen.

Copyright-Informationen

Copyright © 2024 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.