Managen Sie Cloud Volumes ONTAP

Cloud Manager 3.8

NetApp
March 25, 2024

Inhalt

Managen Sie Cloud Volumes ONTAP

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

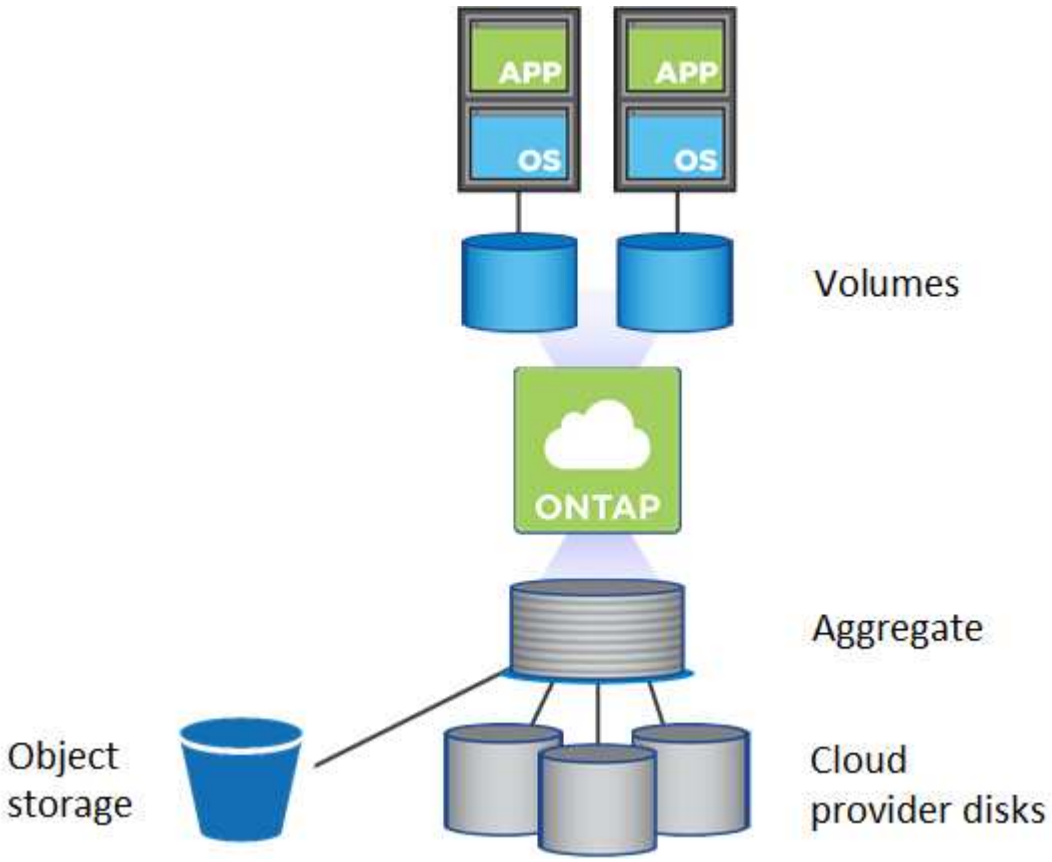
Festplatten und Aggregate

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

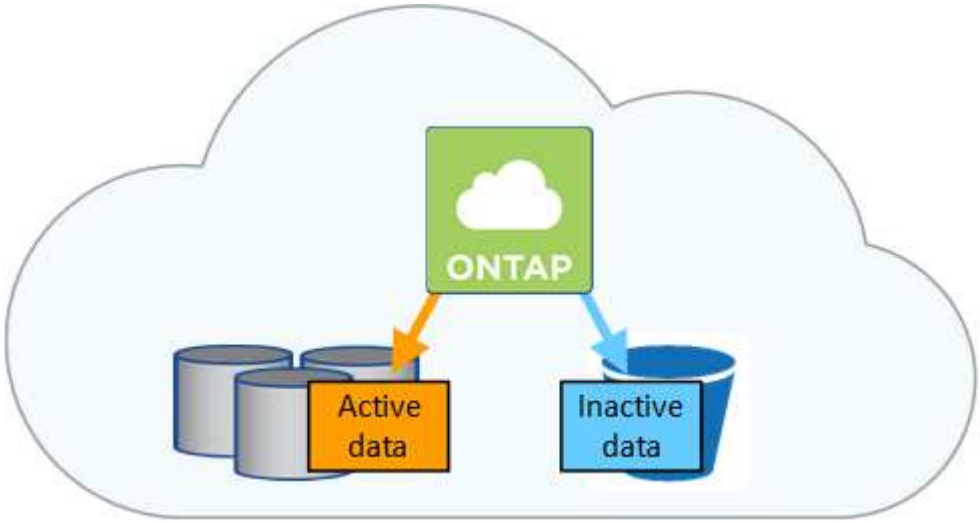
- "Dokumentation der Google Cloud Platform Storage Options"
- "Prüfen von Storage-Limits für Cloud Volumes ONTAP in GCP"

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.

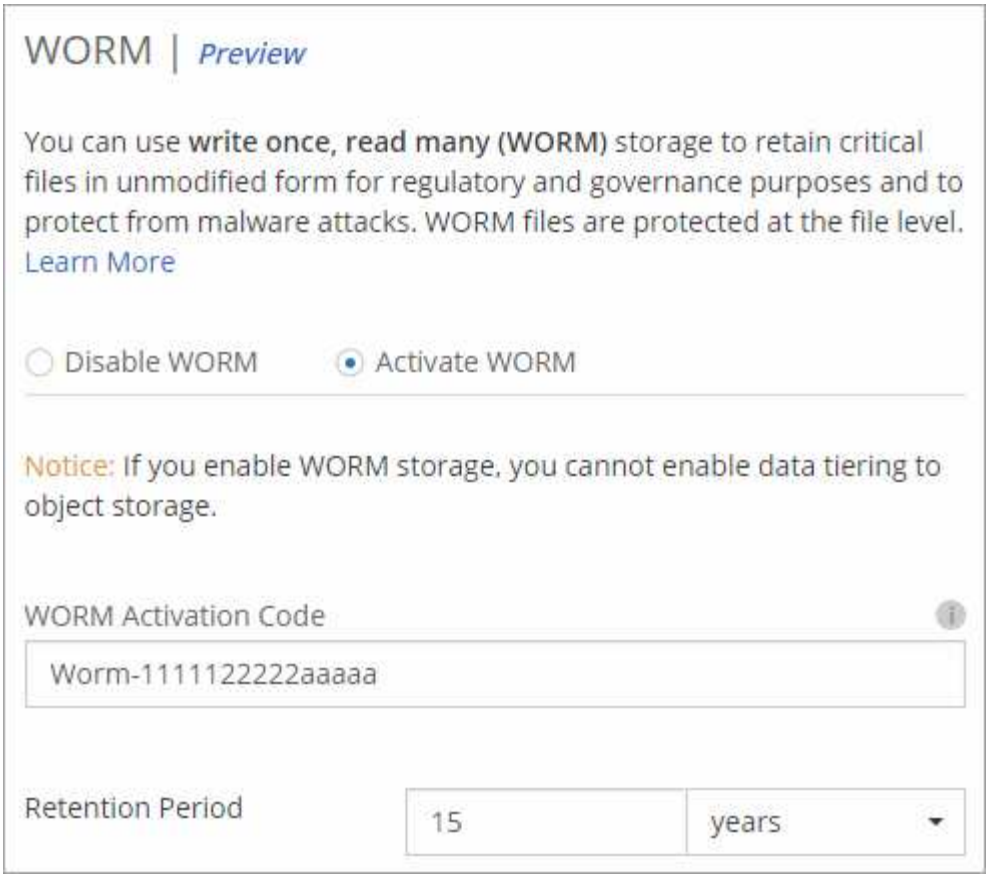
Nach Ablauf der Aufbewahrungsfrist sind Sie dafür verantwortlich, alle Dateien zu löschen, die Sie nicht mehr benötigen.

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.

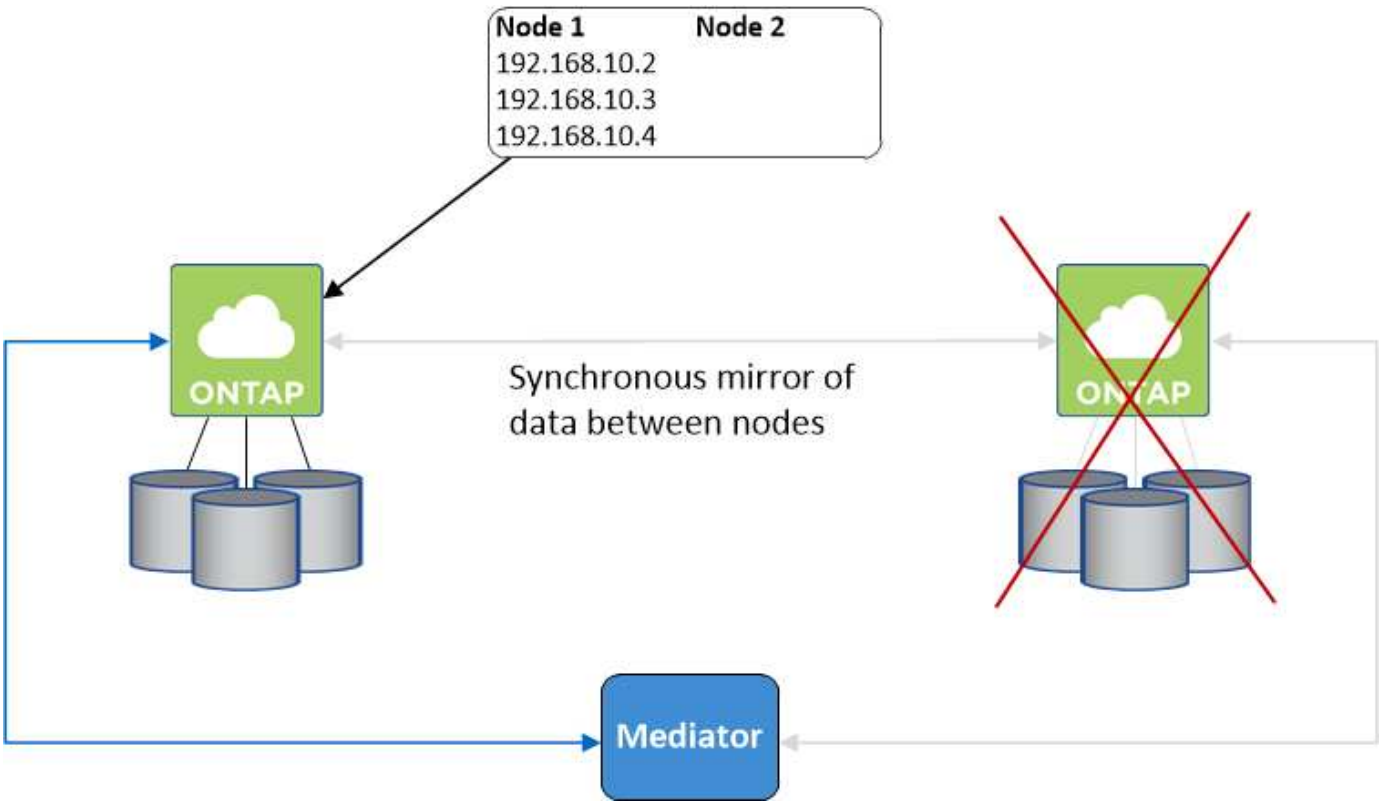
Storage-Übernahme und -Giveback für iSCSI

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

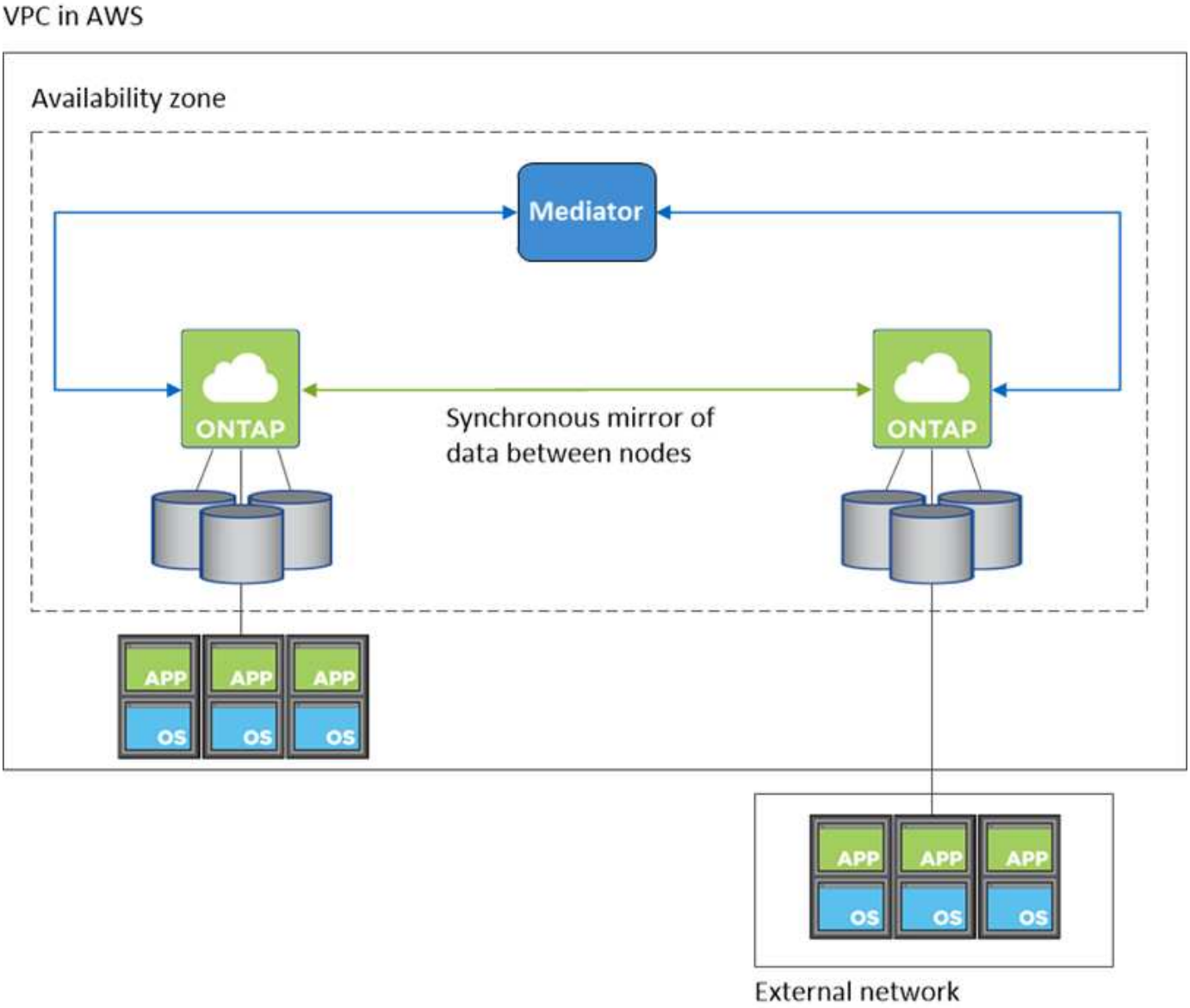
Durch die Implementierung einer HA-Konfiguration in einer einzelnen Verfügbarkeitszone (AZ) kann eine hohe Verfügbarkeit Ihrer Daten sichergestellt werden, wenn eine Instanz, auf der ein Cloud Volumes ONTAP Node ausgeführt wird, ausfällt. Alle Daten sind nativ von außerhalb des VPC zugänglich.

> 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.

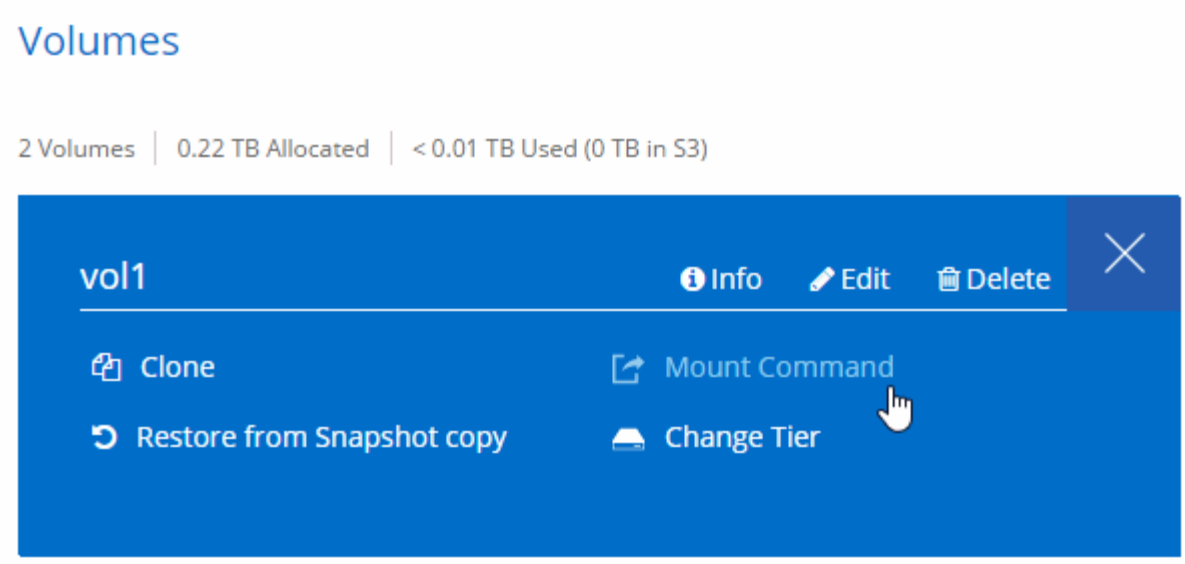
Weitere Informationen zur Performance von Cloud Volumes ONTAP finden Sie unter "Leistung".

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:

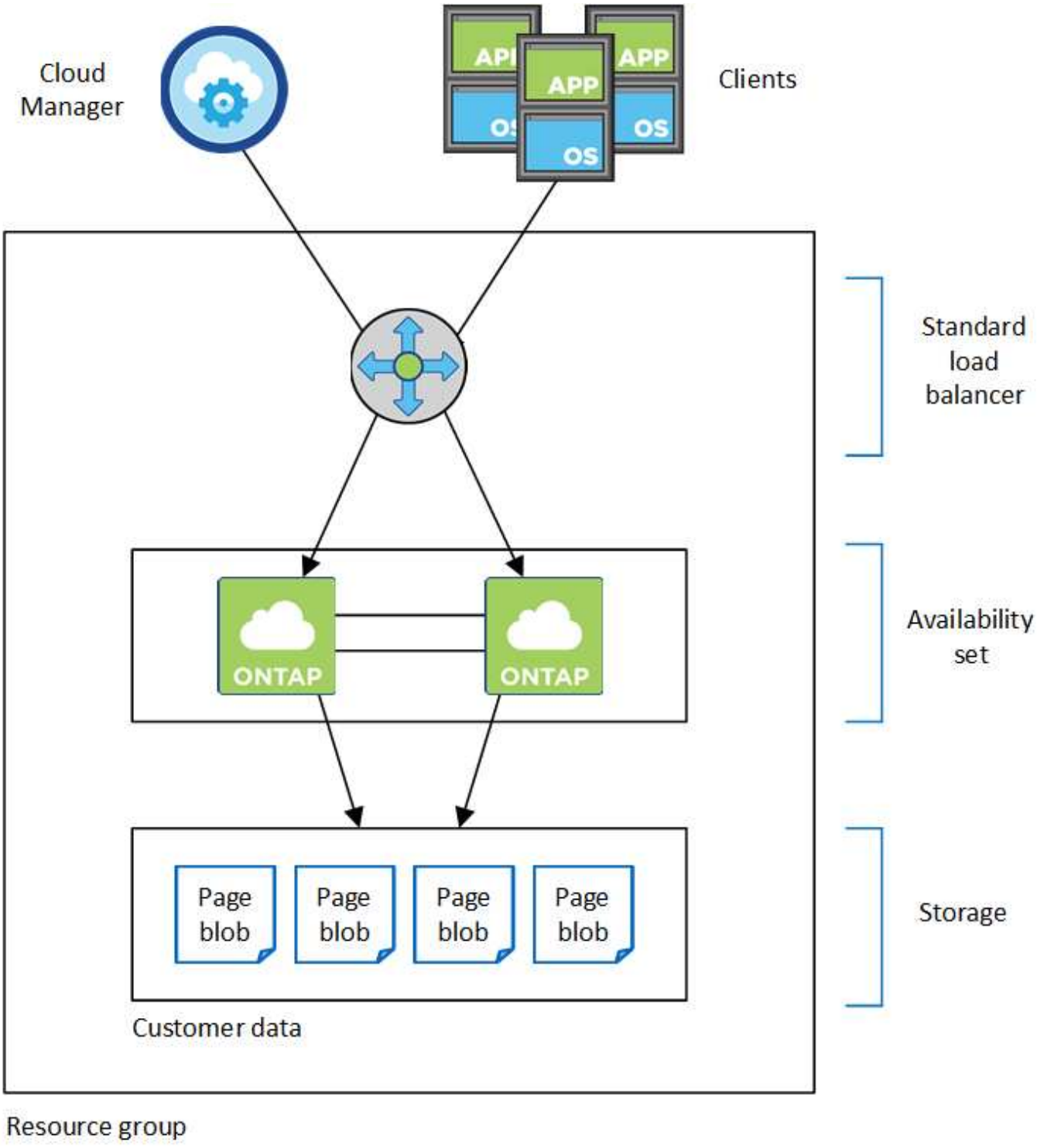


Hochverfügbarkeitspaare in Azure

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".

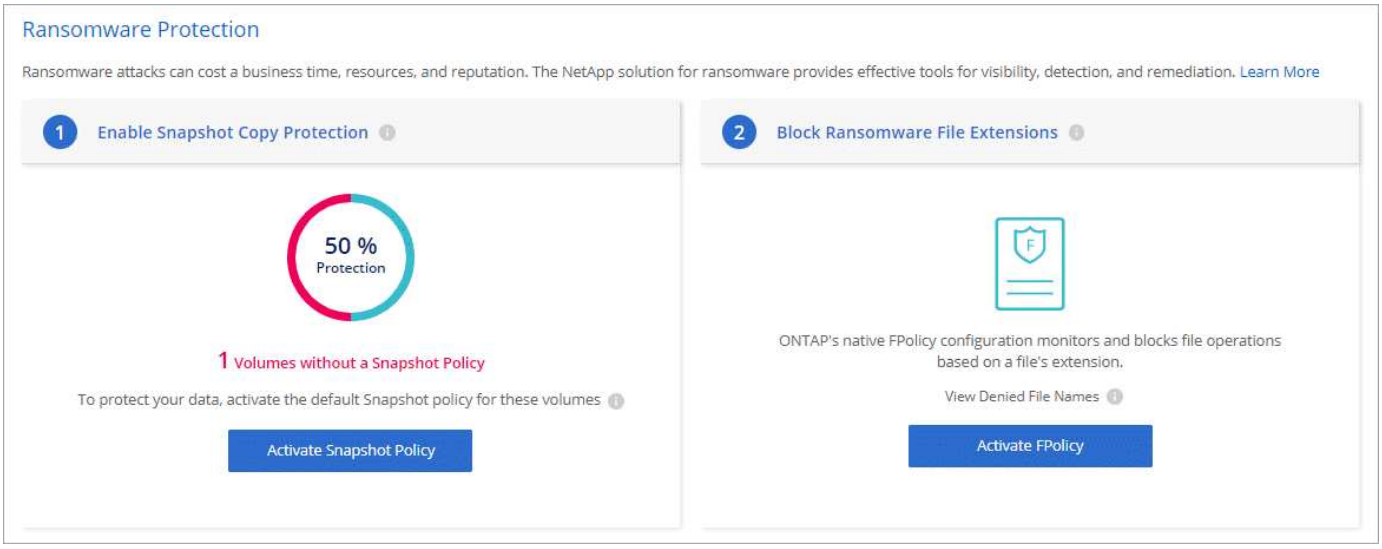
Schutz durch Ransomware

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
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.

Erste Schritte in AWS

Erste Schritte mit Cloud Volumes ONTAP für AWS

Erste Schritte mit Cloud Volumes ONTAP für AWS

Einen Konnektor erstellen

Wenn Sie keine haben "Stecker" Dennoch muss ein Kontoadministrator einen erstellen. "Erfahren Sie, wie Sie in AWS einen Connector erstellen können".

Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von Cloud Manager aufgefordert, einen Connector bereitzustellen, wenn Sie noch keinen haben.

Planen Sie Ihre Konfiguration

Cloud Manager bietet vorkonfigurierte Pakete, die Ihren Workload-Anforderungen entsprechen, oder Sie können eine eigene Konfiguration erstellen. Wenn Sie sich für eine eigene Konfiguration entscheiden, sollten Sie sich mit den verfügbaren Optionen vertraut machen. "Weitere Informationen .".

Richten Sie Ihr Netzwerk ein

1. Stellen Sie sicher, dass Ihre VPC und Subnetze die Konnektivität zwischen dem Connector und Cloud Volumes ONTAP unterstützen.
2. Aktivieren Sie den Outbound-Internetzugang über die Ziel-VPC, damit der Connector und der Cloud Volumes ONTAP mehrere Endpunkte kontaktieren können.

   Dieser Schritt ist wichtig, da der Connector Cloud Volumes ONTAP nicht ohne Outbound-Internetzugang verwalten kann. Wenn Sie die ausgehende Verbindung begrenzen müssen, lesen Sie die Liste der Endpunkte für "Anschluss und Cloud Volumes ONTAP".

3. Richten Sie einen VPC-Endpunkt für den S3-Dienst ein.

   Ein VPC-Endpunkt ist erforderlich, wenn Sie kalte Daten von Cloud Volumes ONTAP auf kostengünstigen Objekt-Storage einstufen möchten.

"Erfahren Sie mehr über Netzwerkanforderungen".

AWS KMS einrichten

Wenn Sie Amazon Verschlüsselung mit Cloud Volumes ONTAP verwenden möchten, müssen Sie sicherstellen, dass ein aktiver Kundenstammschlüssel (CMK) vorhanden ist. Außerdem müssen Sie die Schlüsselrichtlinie für jedes CMK ändern, indem Sie die IAM-Rolle hinzufügen, die dem Connector Berechtigungen als_Key-Benutzer_ bereitstellt. "Weitere Informationen .".

Starten Sie Cloud Volumes ONTAP mit Cloud Manager

Klicken Sie auf **Arbeitsumgebung hinzufügen**, wählen Sie den Systemtyp aus, den Sie bereitstellen möchten, und führen Sie die Schritte im Assistenten aus. "Lesen Sie Schritt-für-Schritt-Anleitungen".

Weiterführende Links

- "Bewertung"
- "Erstellen eines Connectors über Cloud Manager"
- "Einführen eines Connectors über den AWS Marketplace"
- "Installieren der Connector-Software auf einem Linux-Host"
- "Was Cloud Manager mit AWS-Berechtigungen macht"

Cloud Volumes ONTAP-Konfiguration in AWS planen

Wenn Sie Cloud Volumes ONTAP in AWS implementieren, können Sie entweder ein vorkonfiguriertes System wählen, das Ihren Workload-Anforderungen entspricht, oder Sie erstellen Ihre eigene Konfiguration. Wenn Sie sich für eine eigene Konfiguration entscheiden, sollten Sie sich mit den verfügbaren Optionen vertraut machen.

Auswahl eines Lizenztyps

Cloud Volumes ONTAP ist in zwei Preisoptionen erhältlich: Nutzungsbasiert und als BYOL-Modell (Bring-Your-Own-License). Für Pay-as-you-go können Sie zwischen drei Lizenzen wählen: Explore, Standard oder Premium. Jede Lizenz bietet verschiedene Kapazitäts- und Computing-Optionen.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP 9.7 in AWS"

Storage-Grenzen kennen

Die Rohkapazitätsgrenze für ein Cloud Volumes ONTAP System ist an die Lizenz gebunden. Zusätzliche Beschränkungen wirken sich auf die Größe von Aggregaten und Volumes aus. Sie sollten sich dieser Grenzen bei der Planung Ihrer Konfiguration bewusst sein.

"Storage-Limits für Cloud Volumes ONTAP 9.7 in AWS"

Dimensionierung Ihres Systems in AWS

Mit der Dimensionierung Ihres Cloud Volumes ONTAP Systems können Sie die Anforderungen an Performance und Kapazität erfüllen. Bei der Auswahl eines Instanztyps, des Festplattentyp und der Festplattengröße sollten Sie einige wichtige Punkte beachten:

Instanztyp

- Stimmen Sie die Workload-Anforderungen dem maximalen Durchsatz und IOPS für jeden EC2-Instanztyp ab.
- Wenn mehrere Benutzer gleichzeitig auf das System schreiben, wählen Sie einen Instanztyp aus, der über genügend CPUs verfügt, um die Anforderungen zu verwalten.
- Wenn Sie eine Anwendung haben, die hauptsächlich liest, dann wählen Sie ein System mit genügend RAM.
  - "AWS Dokumentation: Amazon EC2 Instanztypen"
  - "AWS Dokumentation: Für Amazon EBS optimierte Instanzen"

EBS-Festplattentyp

Allgemeine SSDs sind der am häufigsten verwendete Festplattentyp für Cloud Volumes ONTAP. Weitere Informationen zu den Anwendungsfällen für EBS-Festplatten finden Sie unter "AWS Dokumentation: EBS Volume-Typen".

EBS-Festplattengröße

Sie müssen beim Start eines Cloud Volumes ONTAP Systems die ursprüngliche Festplattengröße auswählen. Danach können Sie "Cloud Manager managt die Kapazität eines Systems für Sie", Aber wenn Sie wollen "Erstellen Sie Aggregate selbst", Verachten Sie auf folgende Punkte:

- Alle Festplatten in einem Aggregat müssen dieselbe Größe haben.
- Die Performance von EBS-Festplatten ist an die Festplattengröße gebunden. Die Größe bestimmt die IOPS-Basiswerte und die maximale Burst-Dauer für SSD-Festplatten sowie den Baseline- und Burst-Durchsatz für HDD-Festplatten.
- Am Ende sollten Sie die Festplattengröße wählen, die Ihnen die *dauerhafte Performance* bietet, die Sie benötigen.
- Selbst wenn Sie größere Festplatten wählen (z. B. sechs 4-TB-Festplatten), erhalten Sie möglicherweise nicht alle IOPS, da die EC2-Instanz ihr Bandbreitenlimit erreichen kann.

  Weitere Informationen zur Performance der EBS Festplatten finden Sie in "AWS Dokumentation: EBS Volume-Typen".

Sehen Sie sich das folgende Video an, um weitere Informationen zur Dimensionierung Ihres Cloud Volumes ONTAP-Systems in AWS zu erhalten:

[] | *https://img.youtube.com/vi/GELcXmOuYPw/maxresdefault.jpg*

Auswahl einer Konfiguration, die Flash Cache unterstützt

Einige Cloud Volumes ONTAP Konfigurationen in AWS enthalten lokalen NVMe-Storage, den Cloud Volumes ONTAP für bessere Performance als „ *Flash Cache*“ verwendet. "Weitere Informationen zu Flash Cache".

Arbeitsblatt mit Informationen zum AWS-Netzwerk

Wenn Sie Cloud Volumes ONTAP in AWS starten, müssen Sie Details zu Ihrem VPC-Netzwerk angeben. Sie können ein Arbeitsblatt verwenden, um die Informationen von Ihrem Administrator zu sammeln.

Netzwerkinformationen für Cloud Volumes ONTAP

AWS-Informationen	Ihr Wert
Region	
VPC	
Subnetz	
Sicherheitsgruppe (wenn Sie Ihre eigene verwenden)	

Netzwerkinformationen für ein HA-Paar in mehreren AZS

AWS-Informationen	Ihr Wert
Region	
VPC	
Sicherheitsgruppe (wenn Sie Ihre eigene verwenden)	
Verfügbarkeitszone von Node 1	
Subnetz von Node 1	
Verfügbarkeitszone von Node 2	
Subnetz von Node 2	
Mediator Verfügbarkeitszone	
Mediator Subnetz	
Schlüsselpaar für den Vermittler	
Floating-IP-Adresse für Cluster-Management-Port	
Unverankerte IP-Adresse für Daten auf Node 1	
Unverankerte IP-Adresse für Daten auf Node 2	
Routing-Tabellen für unverankerte IP-Adressen	

Auswählen einer Schreibgeschwindigkeit

Mit Cloud Manager können Sie eine Einstellung für die Schreibgeschwindigkeit für Cloud Volumes ONTAP Systeme mit einem Node wählen. Bevor Sie sich für eine Schreibgeschwindigkeit entscheiden, sollten Sie die Unterschiede zwischen den normalen und hohen Einstellungen sowie Risiken und Empfehlungen verstehen, wenn Sie eine hohe Schreibgeschwindigkeit verwenden.

Unterschied zwischen normaler Schreibgeschwindigkeit und hoher Schreibgeschwindigkeit

Wenn Sie sich für eine normale Schreibgeschwindigkeit entscheiden, werden die Daten direkt auf die Festplatte geschrieben, wodurch die Wahrscheinlichkeit eines Datenverlusts bei einem ungeplanten Systemausfall verringert wird.

Wenn Sie hohe Schreibgeschwindigkeit wählen, werden die Daten vor dem Schreiben auf die Festplatte im Speicher gepuffert, was eine schnellere Schreibleistung ermöglicht. Aufgrund dieses Cachings besteht die Gefahr eines Datenverlusts, wenn ein ungeplanter Systemausfall auftritt.

Die Datenmenge, die bei einem ungeplanten Systemausfall verloren gehen kann, entspricht der Spanne der letzten beiden Konsistenzpunkte. Ein Konsistenzpunkt ist das Schreiben gepufferter Daten auf die Festplatte. Ein Konsistenzpunkt tritt auf, wenn das Schreibprotokoll voll ist oder nach 10 Sekunden (je nachdem, was zuerst eintritt). Die Performance des AWS EBS-Volumes kann sich jedoch auf die Verarbeitungszeit des Konsistenzpunkts auswirken.

Wann wird hohe Schreibgeschwindigkeit verwendet

Hohe Schreibgeschwindigkeit ist eine gute Wahl, wenn für Ihre Workload eine schnelle Schreibleistung erforderlich ist und Sie das Risiko eines Datenverlusts bei einem ungeplanten Systemausfall überstehen können.

Empfehlungen bei hoher Schreibgeschwindigkeit

Wenn Sie die hohe Schreibgeschwindigkeit aktivieren, sollten Sie den Schreibschutz auf der Anwendungsebene sicherstellen.

Auswählen eines Volume-Nutzungsprofils

ONTAP umfasst mehrere Storage-Effizienzfunktionen, mit denen Sie die benötigte Storage-Gesamtmenge reduzieren können. Wenn Sie ein Volume in Cloud Manager erstellen, können Sie ein Profil auswählen, das diese Funktionen aktiviert, oder ein Profil, das sie deaktiviert. Sie sollten mehr über diese Funktionen erfahren, um zu entscheiden, welches Profil Sie verwenden möchten.

NetApp Storage-Effizienzfunktionen bieten folgende Vorteile:

Thin Provisioning

Bietet Hosts oder Benutzern mehr logischen Storage als in Ihrem physischen Storage-Pool. Anstatt Storage vorab zuzuweisen, wird jedem Volume beim Schreiben von Daten dynamisch Speicherplatz zugewiesen.

Deduplizierung

Verbessert die Effizienz, indem identische Datenblöcke lokalisiert und durch Verweise auf einen einzelnen gemeinsam genutzten Block ersetzt werden. Durch diese Technik werden die Storage-Kapazitätsanforderungen reduziert, da redundante Datenblöcke im selben Volume eliminiert werden.

Komprimierung

Reduziert die physische Kapazität, die zum Speichern von Daten erforderlich ist, indem Daten in einem Volume auf primärem, sekundärem und Archiv-Storage komprimiert werden.

Richten Sie Ihr Netzwerk ein

Netzwerkanforderungen für Cloud Volumes ONTAP in AWS

Richten Sie das AWS Netzwerk ein, um Cloud Volumes ONTAP Systeme ordnungsgemäß funktionieren zu können.

Allgemeine Anforderungen für Cloud Volumes ONTAP

Die folgenden Anforderungen müssen in AWS erfüllt sein.

Outbound-Internetzugang für Cloud Volumes ONTAP Nodes

Cloud Volumes ONTAP Nodes erfordern ausgehenden Internetzugang, um Nachrichten an NetApp AutoSupport zu senden, der proaktiv den Zustand Ihres Storage überwacht.

Routing- und Firewall-Richtlinien müssen AWS HTTP-/HTTPS-Datenverkehr an die folgenden Endpunkte ermöglichen, damit Cloud Volumes ONTAP AutoSupport-Meldungen senden kann:

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

  Wenn Sie über eine NAT-Instanz verfügen, müssen Sie eine eingehende Sicherheitsgruppenregel definieren, die HTTPS-Datenverkehr vom privaten Subnetz zum Internet zulässt.

  "Erfahren Sie, wie AutoSupport konfiguriert wird".

Outbound-Internetzugang für den HA Mediator

Die HA-Mediatorinstanz muss über eine ausgehende Verbindung zum AWS EC2-Service verfügen, damit sie beim Storage-Failover unterstützt werden kann. Um die Verbindung bereitzustellen, können Sie eine öffentliche IP-Adresse hinzufügen, einen Proxyserver angeben oder eine manuelle Option verwenden.

Die manuelle Option kann ein NAT-Gateway oder ein VPC-Endpunkt der Schnittstelle vom Ziel-Subnetz zum AWS EC2-Dienst sein. Details zu VPC-Endpunkten finden Sie unter "AWS Dokumentation: Interface VPC Endpunkte (AWS PrivateLink)".

Anzahl der IP-Adressen

Cloud Manager weist Cloud Volumes ONTAP in AWS die folgende Anzahl von IP-Adressen zu:

- Single Node: 6 IP-Adressen
- HA-Paare in einem AZS: 15 Adressen
- HA-Paare in mehreren AZS: 15 oder 16 IP-Adressen

  Beachten Sie, dass Cloud Manager auf Systemen mit einzelnen Nodes eine SVM-Management-LIF erstellt, jedoch nicht auf HA-Paaren in einer einzelnen Verfügbarkeitszone. Sie können festlegen, ob eine SVM-Management-LIF auf HA-Paaren in mehreren Verfügbarkeitszonen erstellt werden soll.

  Ein LIF ist eine IP-Adresse, die einem physischen Port zugewiesen ist. Für Managementtools wie SnapCenter ist eine SVM-Management-LIF erforderlich.

Sicherheitsgruppen

Sie müssen keine Sicherheitsgruppen erstellen, da Cloud Manager dies für Sie tut. Wenn Sie Ihr eigenes verwenden müssen, lesen Sie "Regeln für Sicherheitsgruppen".

Verbindung von Cloud Volumes ONTAP zu AWS S3 für Data Tiering

Wenn Sie EBS als Performance-Tier und AWS S3 als Kapazitäts-Tier verwenden möchten, müssen Sie sicherstellen, dass Cloud Volumes ONTAP eine Verbindung zu S3 hat. Die beste Möglichkeit, diese Verbindung bereitzustellen, besteht darin, einen VPC-Endpunkt für den S3-Dienst zu erstellen. Anweisungen hierzu finden Sie unter "AWS Dokumentation: Erstellen eines Gateway-Endpunkts".

Wenn Sie den VPC-Endpunkt erstellen, wählen Sie die Region, den VPC und die Routing-Tabelle aus, die der Cloud Volumes ONTAP Instanz entspricht. Sie müssen auch die Sicherheitsgruppe ändern, um eine ausgehende HTTPS-Regel hinzuzufügen, die Datenverkehr zum S3-Endpunkt ermöglicht. Andernfalls kann

Cloud Volumes ONTAP keine Verbindung zum S3-Service herstellen.

Informationen zu Problemen finden Sie unter "AWS Support Knowledge Center: Warum kann ich mich nicht über einen Gateway VPC Endpunkt mit einem S3-Bucket verbinden?"

Verbindungen zu ONTAP Systemen in anderen Netzwerken

Um Daten zwischen einem Cloud Volumes ONTAP System in AWS und ONTAP Systemen in anderen Netzwerken zu replizieren, müssen Sie eine VPN-Verbindung zwischen AWS VPC und dem anderen Netzwerk haben, z. B. ein Azure VNet oder Ihr Unternehmensnetzwerk. Anweisungen hierzu finden Sie unter "AWS Dokumentation: Einrichten einer AWS VPN-Verbindung".

DNS und Active Directory für CIFS

Wenn Sie CIFS-Storage bereitstellen möchten, müssen Sie DNS und Active Directory in AWS einrichten oder Ihre lokale Einrichtung auf AWS erweitern.

Der DNS-Server muss Namensauflösungsdienste für die Active Directory-Umgebung bereitstellen. Sie können DHCP-Optionssätze so konfigurieren, dass sie den Standard-EC2-DNS-Server verwenden, der nicht der von der Active Directory-Umgebung verwendete DNS-Server sein darf.

Anweisungen finden Sie unter "AWS Dokumentation: Active Directory Domain Services in der AWS Cloud: Quick Start Reference Deployment".

Anforderungen für HA-Paare in mehreren Verfügbarkeitszonen

Zusätzliche AWS Netzwerkanforderungen gelten für Cloud Volumes ONTAP HA-Konfigurationen, die mehrere Verfügbarkeitszonen (AZS) verwenden. Sie sollten diese Anforderungen prüfen, bevor Sie ein HA-Paar starten, da Sie die Netzwerkdetails in Cloud Manager eingeben müssen.

Informationen zur Funktionsweise von HA-Paaren finden Sie unter "Hochverfügbarkeitspaare".

Verfügbarkeitszonen

Dieses HA-Bereitstellungsmodell verwendet mehrere AZS, um eine hohe Verfügbarkeit Ihrer Daten zu gewährleisten. Sie sollten für jede Cloud Volumes ONTAP Instanz und die Mediatorinstanz eine dedizierte AZ verwenden, die einen Kommunikationskanal zwischen dem HA-Paar bereitstellt.

Fließende IP-Adressen für NAS- und Cluster-/SVM-Management

HA-Konfigurationen in mehreren Verfügbarkeitszonen verwenden fließende IP-Adressen, die bei einem Ausfall zwischen Nodes migriert werden. Außerhalb der VPC ist nicht nativ zugänglich. Es sei denn, Sie können darauf zugreifen "AWS Transit Gateway einrichten".

Eine Floating-IP-Adresse ist für das Cluster-Management, eine für NFS/CIFS-Daten auf Node 1 und eine für NFS/CIFS-Daten auf Node 2. Eine vierte Floating IP-Adresse für SVM-Management ist optional.

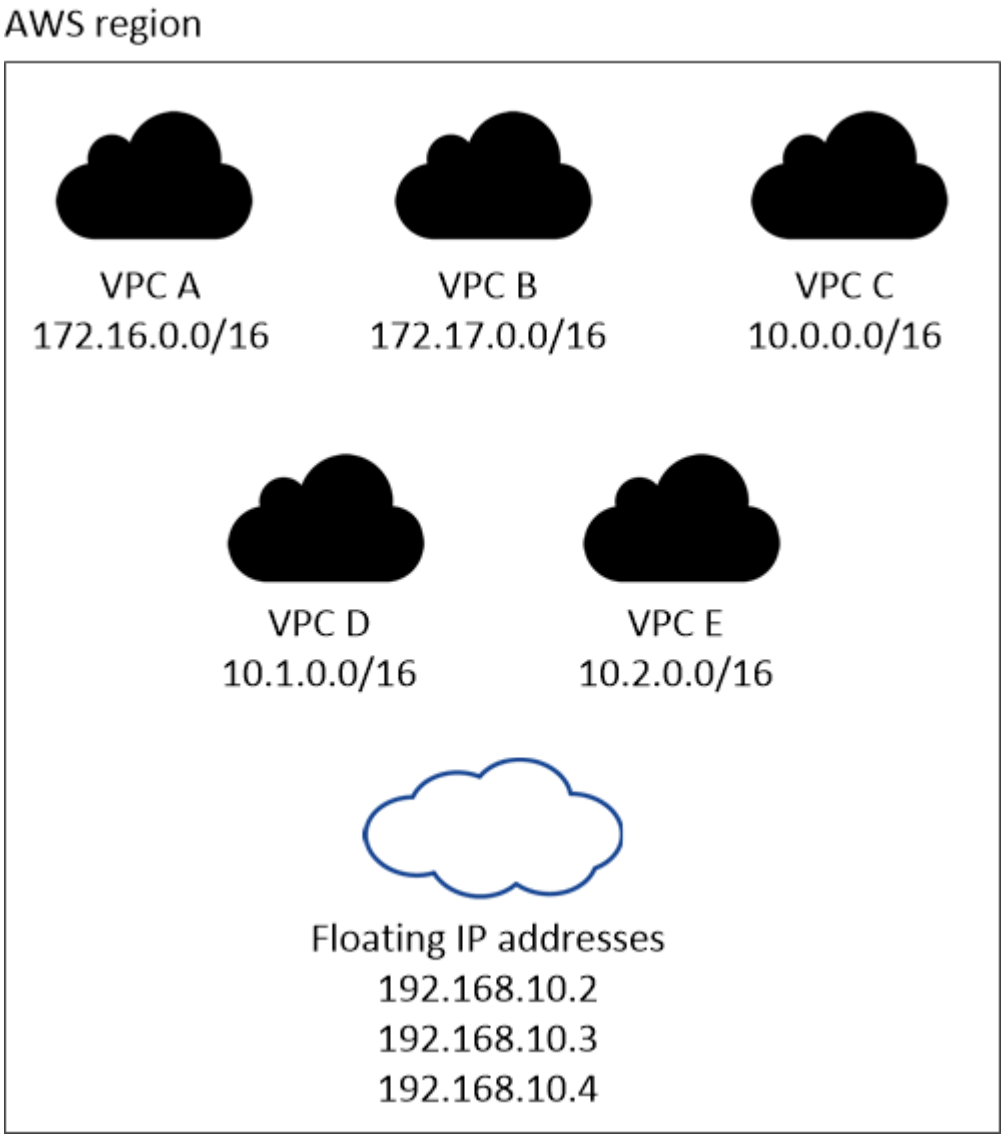
> Wenn Sie SnapDrive für Windows oder SnapCenter mit dem HA-Paar verwenden, ist eine unverankerte IP-Adresse für die SVM-Management-LIF erforderlich. Wenn Sie die IP-Adresse nicht angeben, wenn Sie das System implementieren, können Sie später die LIF erstellen. Weitere Informationen finden Sie unter "Einrichten von Cloud Volumes ONTAP".

Sie müssen die unverankerten IP-Adressen in Cloud Manager eingeben, wenn Sie eine Cloud Volumes ONTAP HA-Arbeitsumgebung erstellen. Cloud Manager weist dem HA-Paar die IP-Adressen zu, wenn es das System startet.

Die fließenden IP-Adressen müssen sich für alle VPCs in der AWS Region, in der Sie die HA-Konfiguration implementieren, außerhalb der CIDR-Blöcke befinden. Stellen Sie sich die fließenden IP-Adressen als

logisches Subnetz vor, das sich außerhalb der VPCs in Ihrer Region befindet.

Das folgende Beispiel zeigt die Beziehung zwischen Floating-IP-Adressen und den VPCs in einer AWS-Region. Während sich die fließenden IP-Adressen für alle VPCs außerhalb der CIDR-Blöcke befinden, sind sie über Routing-Tabellen in Subnetze routingfähig.



Cloud Manager erstellt automatisch statische IP-Adressen für den iSCSI-Zugriff und für den NAS-Zugriff von Clients außerhalb des VPC. Für diese Art von IP-Adressen müssen Sie keine Anforderungen erfüllen.

Transit-Gateway zur Aktivierung des Floating IP-Zugriffs von außerhalb der VPC

"AWS Transit Gateway einrichten" Um den Zugriff auf die unverankerten IP-Adressen eines HA-Paars von außerhalb der VPC zu ermöglichen, in der sich das HA-Paar befindet.

Routentabellen

Nachdem Sie in Cloud Manager die unverankerten IP-Adressen angegeben haben, müssen Sie die Routing-Tabellen auswählen, die Routen zu den Floating IP-Adressen enthalten sollen. Dies ermöglicht den Client-Zugriff auf das HA-Paar.

Wenn Sie nur eine Routing-Tabelle für die Subnetze in Ihrem VPC (der Hauptroutentabelle) haben, fügt

Cloud Manager dieser Routing-Tabelle automatisch die unverankerten IP-Adressen hinzu. Wenn Sie mehr als eine Routing-Tabelle haben, ist es sehr wichtig, beim Starten des HA-Paars die richtigen Routing-Tabellen auszuwählen. Andernfalls haben einige Clients möglicherweise keinen Zugriff auf Cloud Volumes ONTAP.

Sie können beispielsweise zwei Subnetze haben, die mit verschiedenen Routing-Tabellen verknüpft sind. Wenn Sie Routing-Tabelle A auswählen, jedoch nicht Route-Tabelle B, können Clients in der mit Routing-Tabelle A verknüpften Subnetz auf das HA-Paar zugreifen, die Clients im Subnetz der Routing-Tabelle B können jedoch nicht.

Weitere Informationen zu Routingtabellen finden Sie unter "AWS Documentation: Routingtabellen".

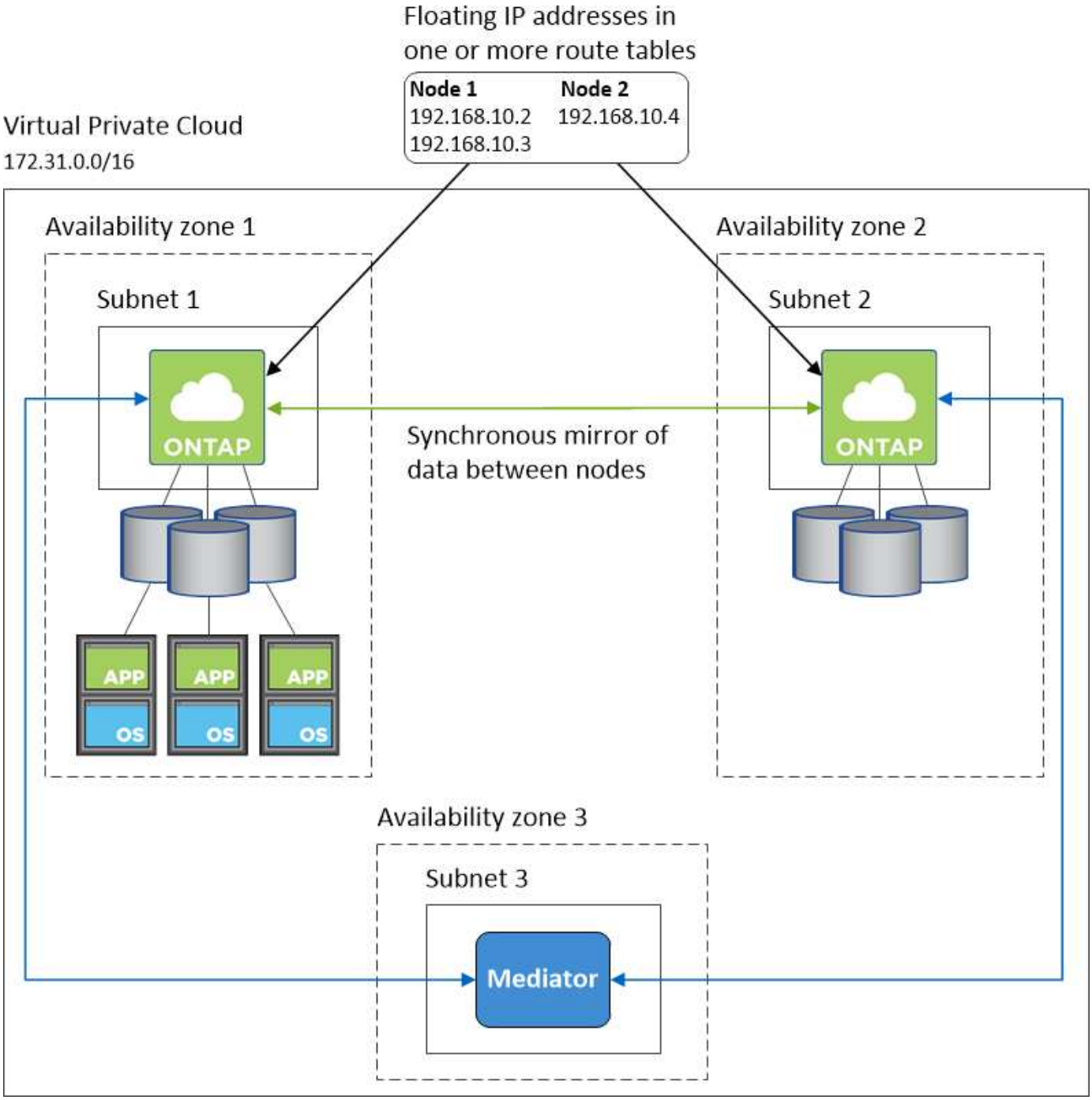
Anbindung an NetApp Management Tools

Für den Einsatz von NetApp Management Tools mit HA-Konfigurationen in mehreren Verfügbarkeitszonen stehen zwei Verbindungsoptionen zur Verfügung:

1. Die NetApp Management Tools in einer anderen VPC und implementieren "AWS Transit Gateway einrichten". Das Gateway ermöglicht den Zugriff auf die unverankerte IP-Adresse für die Cluster-Managementoberfläche von außerhalb der VPC aus.
2. Implementieren Sie die NetApp Management-Tools in derselben VPC mit einer ähnlichen Routing-Konfiguration wie NAS-Clients.

Beispiel für eine HA-Konfiguration

Die folgende Abbildung zeigt eine optimale HA-Konfiguration in AWS, die als Aktiv/Passiv-Konfiguration betrieben wird:



Anforderungen an den Steckverbinder

Richten Sie Ihr Netzwerk ein, damit der Connector Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen kann. Der wichtigste Schritt besteht darin, ausgehenden Internetzugriff auf verschiedene Endpunkte zu gewährleisten.

Wenn Ihr Netzwerk für die gesamte Kommunikation mit dem Internet einen Proxyserver verwendet, können Sie den Proxyserver über die Seite Einstellungen angeben. Siehe "Konfigurieren des Connectors für die Verwendung eines Proxy-Servers".

Verbindung zu Zielnetzwerken

Für einen Connector ist eine Netzwerkverbindung zu den VPCs und VNets erforderlich, in denen Cloud Volumes ONTAP bereitgestellt werden soll.

Wenn Sie beispielsweise einen Connector in Ihrem Unternehmensnetzwerk installieren, müssen Sie eine VPN-Verbindung zur VPC oder vnet einrichten, in der Sie Cloud Volumes ONTAP starten.

Outbound-Internetzugang

Für den Connector ist ein abgehender Internetzugang erforderlich, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung zu managen. Ein Connector kontaktiert die folgenden Endpunkte beim Management von Ressourcen in AWS:

Endpunkte	Zweck
AWS-Services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3) Der genaue Endpunkt hängt von der Region ab, in der Sie Cloud Volumes ONTAP implementieren. "Weitere Informationen finden Sie in der AWS-Dokumentation."	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in AWS.
https://api.services.cloud.netapp.com:443	API-Anfragen an NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://repo.cloud.support.netapp.com	Wird zum Herunterladen der Abhängigkeiten von Cloud Manager verwendet.
http://repo.mysql.com/	Zum Herunterladen von MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Cloud Manager kann Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images abrufen und herunterladen.
https://cloudmanagerinfraprod.azurecr.io	Zugriff auf Software-Images von Container-Komponenten für eine Infrastruktur, die Docker ausführt und eine Lösung für die Service-Integration mit Cloud Manager bietet.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cloudmanager.cloud.netapp.com	Kommunikation mit dem Cloud Manager-Service, der Cloud Central-Konten einschließt

Endpunkte	Zweck
https://netapp-cloud-account.auth0.com	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Wird verwendet, um Ihre AWS Konto-ID der Liste der zugelassenen Benutzer für die Sicherung in S3 hinzuzufügen.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Kommunikation mit NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Kommunikation mit NetApp bei Systemlizenzrechten und Support-Registrierung
https://ipa-signer.cloudmanager.netapp.com	Ermöglicht Cloud Manager die Generierung von Lizenzen (beispielsweise eine FlexCache Lizenz für Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Erforderlich, um Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster zu verbinden Mit den Endpunkten ist die Installation von NetApp Trident möglich.
Verschiedene Standorte von Drittanbietern, z. B.: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org An Standorten von Drittanbietern können Änderungen vorgenommen werden.	Während Upgrades lädt Cloud Manager die neuesten Pakete für Abhängigkeiten von Drittanbietern herunter.

Während Sie fast alle Aufgaben über die SaaS-Benutzeroberfläche ausführen sollten, steht auf dem Connector weiterhin eine lokale Benutzeroberfläche zur Verfügung. Die Maschine, auf der der Webbrowser ausgeführt wird, muss über Verbindungen zu den folgenden Endpunkten verfügen:

Endpunkte	Zweck
Der Connector-Host	Sie müssen die IP-Adresse des Hosts aus einem Webbrowser eingeben, um die Cloud Manager-Konsole zu laden. Je nach Ihrer Verbindung mit Ihrem Cloud-Provider können Sie die private IP oder eine dem Host zugewiesene öffentliche IP verwenden: • Eine private IP funktioniert, wenn Sie über ein VPN verfügen und direkten Zugriff auf Ihr virtuelles Netzwerk haben • Eine öffentliche IP funktioniert in jedem Netzwerkszenario In jedem Fall sollten Sie den Netzwerkzugriff sichern, indem Sie sicherstellen, dass die Sicherheitsgruppenregeln den Zugriff nur von autorisierten IPs oder Subnetzen ermöglichen.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Ihr Webbrowser stellt über NetApp Cloud Central eine Verbindung zu diesen Endpunkten her, um eine zentralisierte Benutzerauthentifizierung zu ermöglichen.
https://widget.intercom.io	Für Ihren Produkt-Chat, der Ihnen das Gespräch mit NetApp Cloud-Experten ermöglicht.

Einrichten eines AWS-Transit-Gateways für HA-Paare in mehreren Verfügbarkeitszonen

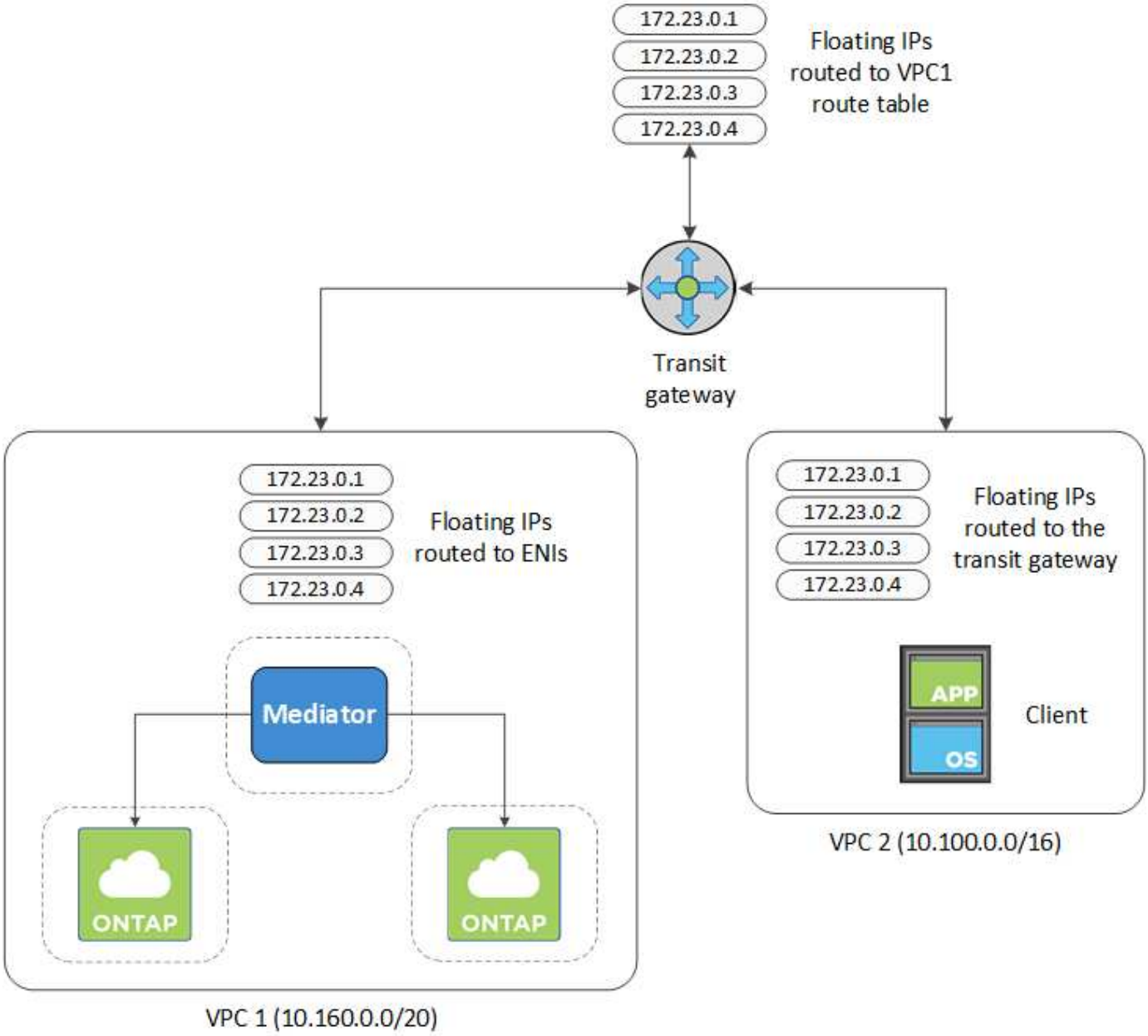
Einrichten eines AWS Transit-Gateways für den Zugriff auf HA-Paare "Floating-IP-Adressen" Von außerhalb der VPC, wo das HA-Paar residiert.

Wenn eine Cloud Volumes ONTAP-HA-Konfiguration über mehrere AWS-Verfügbarkeitszonen verteilt ist, sind unverankerte IP-Adressen für den NAS-Datenzugriff über die VPC erforderlich. Diese fließenden IP-Adressen können bei Ausfällen zwischen Nodes migriert werden, sind aber außerhalb der VPC nicht nativ zugänglich. Separate private IP-Adressen ermöglichen den Datenzugriff von außerhalb der VPC, bieten jedoch kein automatisches Failover.

Floating IP-Adressen sind außerdem für die Cluster-Managementoberfläche und die optionale SVM Management LIF erforderlich.

Wenn Sie ein AWS-Transit-Gateway einrichten, ermöglichen Sie den Zugriff auf die unverankerten IP-Adressen von außerhalb der VPC, wo sich das HA-Paar befindet. Das bedeutet, dass NAS-Clients und NetApp Managementtools außerhalb der VPC auf die fließenden IPs zugreifen können.

Das Beispiel zeigt zwei VPCs, die über ein Transit-Gateway verbunden sind. Ein HA-System befindet sich in einer VPC, während ein Client im anderen befindet. Sie können dann mithilfe der fließenden IP-Adresse ein NAS-Volume auf den Client mounten.

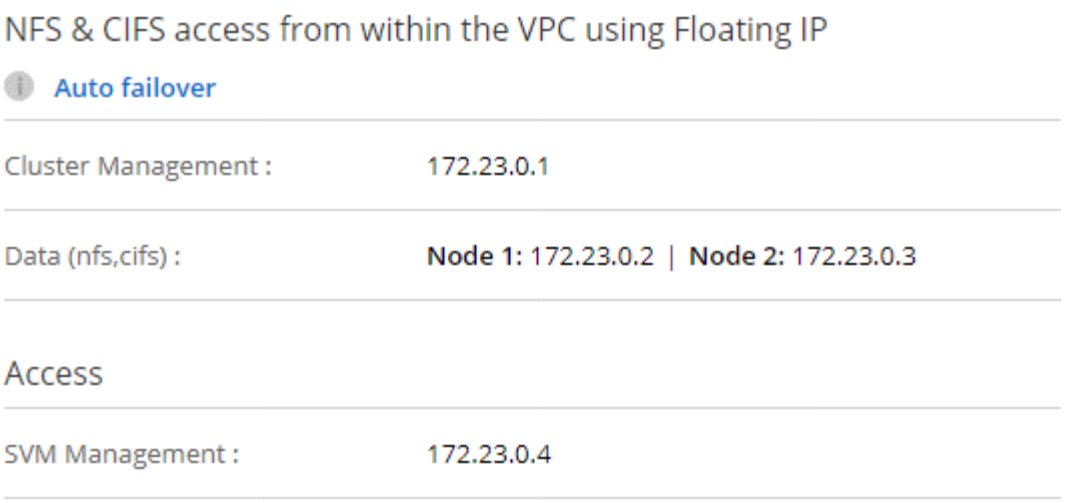


Die folgenden Schritte veranschaulichen die Einrichtung einer ähnlichen Konfiguration.

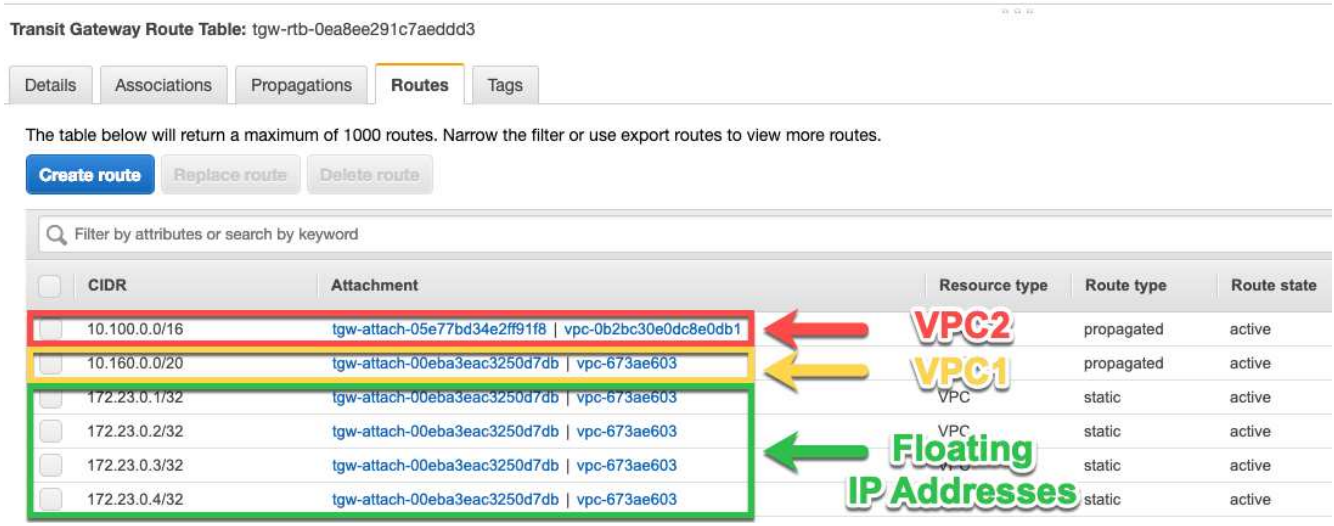
Schritte

1. "Erstellen Sie ein Transit-Gateway, und verbinden Sie die VPCs mit dem Gateway".
2. Erstellen Sie Routen in der Routing-Tabelle des Transit-Gateways durch Angabe der Floating-IP-Adressen des HA-Paars.

   Die unverankerten IP-Adressen finden Sie auf der Seite „Informationen zur Arbeitsumgebung“ in Cloud Manager. Hier ein Beispiel:



Das folgende Beispielbild zeigt die Routingtabelle für das Transit Gateway. Er umfasst Routen zu den CIDR-Blöcken der zwei VPCs und vier von Cloud Volumes ONTAP verwendete Floating IP-Adressen.

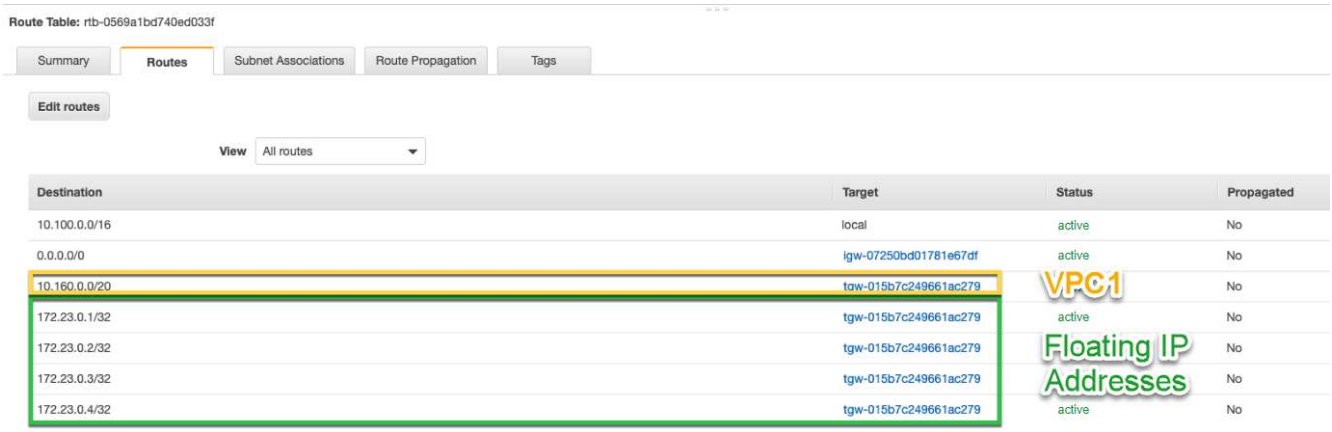


3. Ändern Sie die Routingtabelle von VPCs, die auf die fließenden IP-Adressen zugreifen müssen.

   a. Fügen Sie den unverankerten IP-Adressen Routeneinträge hinzu.

   b. Fügen Sie einen Routeneintrag zum CIDR-Block des VPC hinzu, wo das HA-Paar residiert.

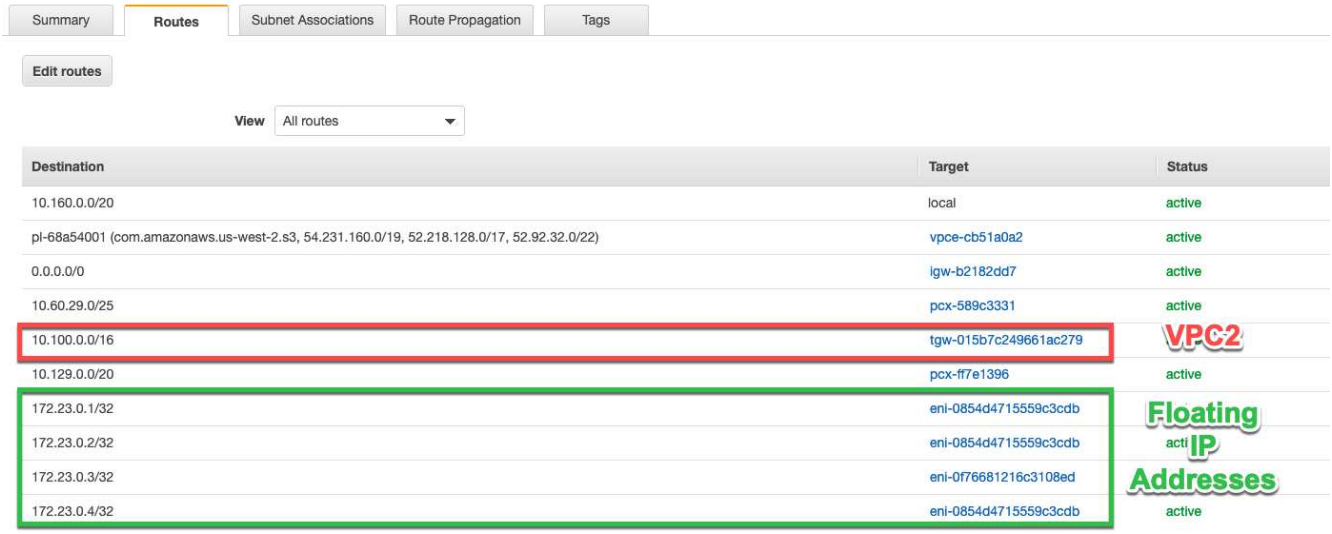
      Das folgende Beispielbild zeigt die Routingtabelle für VPC 2, die auch Routen zu VPC 1 und die fließenden IP-Adressen umfasst.



4. Ändern Sie die Routing-Tabelle für die VPC des HA-Paars, indem Sie der VPC eine Route hinzufügen, die Zugriff auf die fließenden IP-Adressen benötigt.

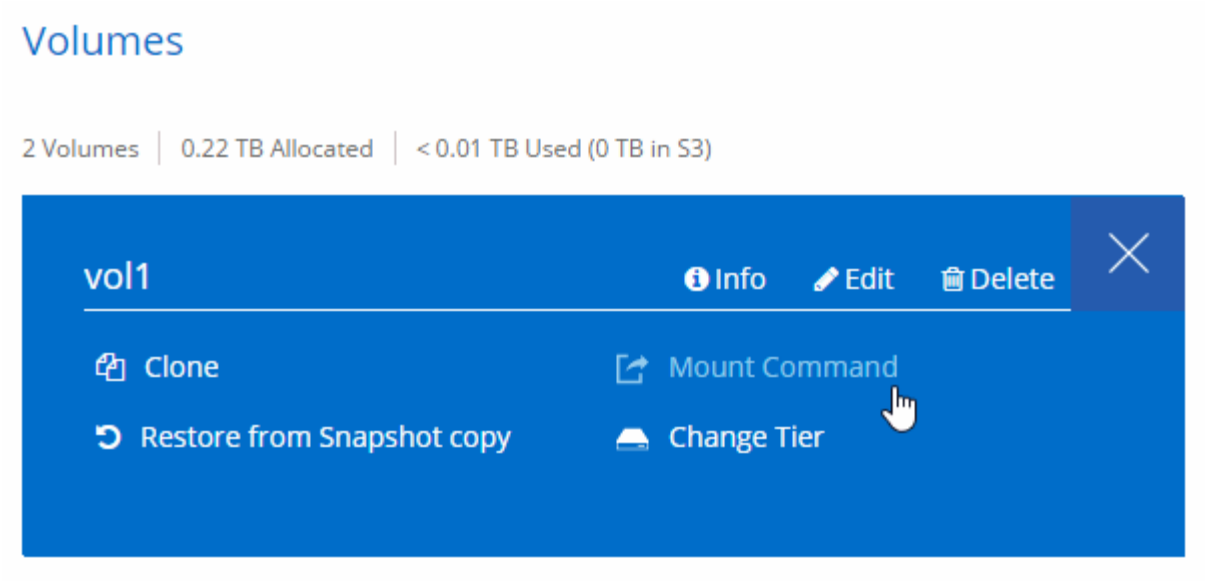
   Dieser Schritt ist wichtig, da er die Weiterleitung zwischen den VPCs abgeschlossen hat.

   Das folgende Beispielbild zeigt die Routing-Tabelle für VPC 1. Sie umfasst eine Route zu den unverankerten IP-Adressen und zu VPC 2, wo sich der Client befindet. Cloud Manager hat bei der Implementierung des HA-Paars automatisch die Floating IPs zur Routing-Tabelle hinzugefügt.



5. Volumes werden mithilfe der Floating IP-Adresse an Clients gemountet.

   Die richtige IP-Adresse finden Sie in Cloud Manager, indem Sie ein Volume auswählen und auf **Mount Command** klicken.



Verwandte Links

- "Hochverfügbarkeitspaare in AWS"
- "Netzwerkanforderungen für Cloud Volumes ONTAP in AWS"

Sicherheitsgruppenregeln für AWS

Cloud Manager erstellt AWS Sicherheitsgruppen mit den ein- und ausgehenden Regeln, die für den erfolgreichen Betrieb von Connector und Cloud Volumes ONTAP erforderlich sind. Sie können die Ports zu Testzwecken oder zur Verwendung eigener Sicherheitsgruppen verwenden.

Regeln für Cloud Volumes ONTAP

Die Sicherheitsgruppe für Cloud Volumes ONTAP erfordert sowohl eingehende als auch ausgehende Regeln.

Regeln für eingehende Anrufe

Die Quelle für eingehende Regeln in der vordefinierten Sicherheitsgruppe ist 0.0.0.0/0.

Protokoll	Port	Zweck
Alle ICMP	Alle	Pingen der Instanz
HTTP	80	HTTP-Zugriff auf die System Manager Webkonsole mit der IP-Adresse der Cluster-Management-LIF
HTTPS	443	HTTPS-Zugriff auf die System Manager-Webkonsole unter Verwendung der IP-Adresse der Cluster-Management-LIF
SSH	22	SSH-Zugriff auf die IP-Adresse der Cluster Management LIF oder einer Node Management LIF
TCP	111	Remote-Prozeduraufruf für NFS
TCP	139	NetBIOS-Servicesitzung für CIFS

Protokoll	Port	Zweck
TCP	161-162	Einfaches Netzwerkverwaltungsprotokoll
TCP	445	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
TCP	635	NFS-Mount
TCP	749	Kerberos
TCP	2049	NFS-Server-Daemon
TCP	3260	ISCSI-Zugriff über die iSCSI-Daten-LIF
TCP	4045	NFS-Sperr-Daemon
TCP	4046	Netzwerkstatusüberwachung für NFS
TCP	10.000	Backup mit NDMP
TCP	11104	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
TCP	11105	SnapMirror Datenübertragung über Cluster-interne LIFs
UDP	111	Remote-Prozeduraufruf für NFS
UDP	161-162	Einfaches Netzwerkverwaltungsprotokoll
UDP	635	NFS-Mount
UDP	2049	NFS-Server-Daemon
UDP	4045	NFS-Sperr-Daemon
UDP	4046	Netzwerkstatusüberwachung für NFS
UDP	4049	NFS rquotad-Protokoll

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle ICMP	Alle	Gesamter abgehender Datenverkehr
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie strenge Regeln für ausgehenden Datenverkehr benötigen, können Sie mit den folgenden Informationen nur die Ports öffnen, die für die ausgehende Kommunikation durch Cloud Volumes ONTAP erforderlich sind.

Die Quelle ist die Schnittstelle (IP-Adresse) auf dem Cloud Volumes ONTAP System.

Service	Protokoll	Port	Quelle	Ziel	Zweck
Active Directory	TCP	88	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Node Management-LIF	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Node Management-LIF	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	TCP	139	Node Management-LIF	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP UND UDP	389	Node Management-LIF	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Node Management-LIF	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	UDP	464	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	TCP	88	Daten-LIF (NFS, CIFS, iSCSI)	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	TCP	139	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP UND UDP	389	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	UDP	464	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V - Passwort ändern und festlegen (RPCSEC_GSS)

Service	Protokoll	Port	Quelle	Ziel	Zweck
Backup auf S3	TCP	5010	Intercluster-LIF	Backup-Endpunkt oder Wiederherstellungsendpunkt	Backup- und Restore-Vorgänge für die Funktion „Backup in S3“
Cluster	Gesamter Datenverkehr	Gesamter Datenverkehr	Alle LIFs auf einem Node	Alle LIFs auf dem anderen Node	Kommunikation zwischen Clustern (nur Cloud Volumes ONTAP HA)
	TCP	3000	Node Management-LIF	Ha Mediator	ZAPI-Aufrufe (nur Cloud Volumes ONTAP HA)
	ICMP	1	Node Management-LIF	Ha Mediator	Bleiben Sie am Leben (nur Cloud Volumes ONTAP HA)
DHCP	UDP	68	Node Management-LIF	DHCP	DHCP-Client für die erstmalige Einrichtung
DHCPS	UDP	67	Node Management-LIF	DHCP	DHCP-Server
DNS	UDP	53	Node Management LIF und Daten LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600-18699	Node Management-LIF	Zielserver	NDMP-Kopie
SMTP	TCP	25	Node Management-LIF	Mailserver	SMTP-Warnungen können für AutoSupport verwendet werden
SNMP	TCP	161	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	UDP	161	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	TCP	162	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	UDP	162	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
SnapMirror	TCP	11104	Intercluster-LIF	ONTAP Intercluster-LIFs	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
	TCP	11105	Intercluster-LIF	ONTAP Intercluster-LIFs	SnapMirror Datenübertragung
Syslog	UDP	514	Node Management-LIF	Syslog-Server	Syslog-Weiterleitungsmeldungen

Regeln für die externe Sicherheitsgruppe des HA Mediators

Die vordefinierte externe Sicherheitsgruppe für den Cloud Volumes ONTAP HA Mediator enthält die folgenden Regeln für ein- und ausgehende Anrufe.

Regeln für eingehende Anrufe

Die Quelle für eingehende Regeln ist 0.0.0.0/0.

Protokoll	Port	Zweck
SSH	22	SSH-Verbindungen zum HA-Vermittler
TCP	3000	RESTful API-Zugriff über den Connector

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den HA-Vermittler öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den HA-Vermittler enthält die folgenden Regeln für ausgehende Anrufe.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den HA-Vermittler erforderlich sind.

Protokoll	Port	Ziel	Zweck
HTTP	80	Anschluss-IP-Adresse	Lade Upgrades für den Mediator herunter
HTTPS	443	AWS API-Services	Unterstützung bei Storage Failover
UDP	53	AWS API-Services	Unterstützung bei Storage Failover

Anstatt die Ports 443 und 53 zu öffnen, können Sie einen VPC-Endpunkt des Zielsubnetzen zum AWS EC2 Service erstellen.

Regeln für die interne Sicherheitsgruppe des HA-Vermittlers

Die vordefinierte interne Sicherheitsgruppe für den Cloud Volumes ONTAP HA Mediator enthält die folgenden Regeln. Cloud Manager erstellt immer diese Sicherheitsgruppe. Sie haben nicht die Möglichkeit, Ihre eigenen zu verwenden.

Regeln für eingehende Anrufe

Die vordefinierte Sicherheitsgruppe enthält die folgenden Regeln für eingehende Anrufe.

Protokoll	Port	Zweck
Gesamter Datenverkehr	Alle	Kommunikation zwischen HA-Mediator und HA-Knoten

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Gesamter Datenverkehr	Alle	Kommunikation zwischen HA-Mediator und HA-Knoten

Regeln für den Konnektor

Die Sicherheitsgruppe für den Konnektor erfordert sowohl ein- als auch ausgehende Regeln.

Regeln für eingehende Anrufe

Die Quelle für eingehende Regeln in der vordefinierten Sicherheitsgruppe ist 0.0.0.0/0.

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche und Verbindungen von Cloud Compliance
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
TCP	3128	Bietet die Cloud Compliance-Instanz einen Internetzugang, wenn Ihr AWS-Netzwerk keine NAT oder Proxy verwendet

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Konnektor öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Connector enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.

Die Quell-IP-Adresse ist der Connector-Host.

Service	Protokoll	Port	Ziel	Zweck
Active Directory	TCP	88	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	TCP	139	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP	389	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	TCP	749	Active Directory-Gesamtstruktur	Active Directory Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	UDP	137	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	UDP	464	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe an AWS und ONTAP und Senden von AutoSupport Nachrichten an NetApp
API-Aufrufe	TCP	3000	ONTAP Cluster Management LIF	API-Aufrufe für ONTAP
	TCP	8088	Backup auf S3	API-Aufrufe zur Sicherung in S3

Service	Protokoll	Port	Ziel	Zweck
DNS	UDP	53	DNS	Wird für die DNS-Auflösung durch Cloud Manager verwendet
Cloud-Compliance	HTTP	80	Cloud Compliance Instanz	Cloud Compliance für Cloud Volumes ONTAP

Einrichten des AWS KMS

Wenn Sie die Amazon Verschlüsselung mit Cloud Volumes ONTAP verwenden möchten, müssen Sie den AWS KMS (Key Management Service) einrichten.

Schritte

1. Stellen Sie sicher, dass ein aktiver Kundenstammschlüssel (CMK) vorhanden ist.

   Bei CMK kann es sich um ein von AWS gemanagtes CMK oder um ein vom Kunden gemanagtes CMK handeln. Sie kann sich im selben AWS Konto wie Cloud Manager und Cloud Volumes ONTAP oder in einem anderen AWS Konto befinden.

   "AWS Dokumentation: Customer Master Keys (CMKs)"

2. Ändern Sie die Schlüsselrichtlinie für jedes CMK, indem Sie die IAM-Rolle hinzufügen, die Berechtigungen für Cloud Manager als *Key Benutzer* bereitstellt.

   Durch Hinzufügen der IAM-Rolle als Schlüsselbenutzer erhalten Cloud Manager Berechtigungen zur Verwendung des CMK mit Cloud Volumes ONTAP.

   "AWS Dokumentation: Schlüssel bearbeiten"

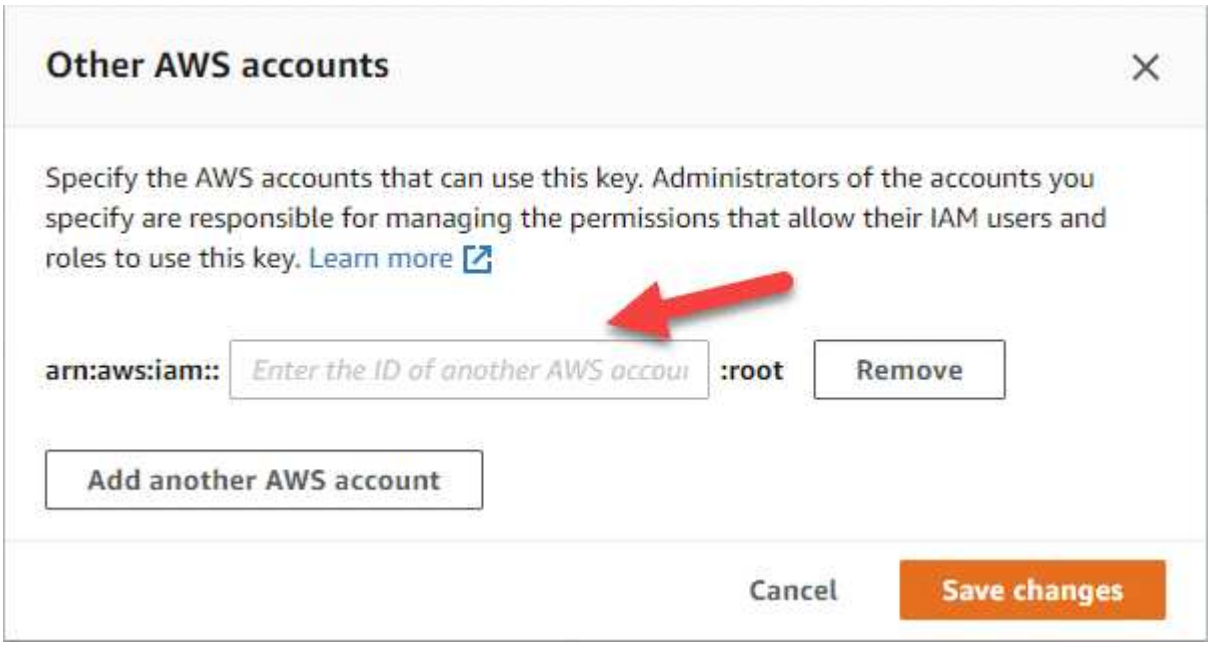
3. Wenn sich das CMK in einem anderen AWS Konto befindet, führen Sie folgende Schritte aus:

   a. Wechseln Sie von dem Konto, in dem sich der CMK befindet, zur KMS-Konsole.
   b. Wählen Sie die Taste.
   c. Kopieren Sie im Fenster **Allgemeine Konfiguration** den ARN des Schlüssels.

      Wenn Sie das Cloud Volumes ONTAP-System erstellen, müssen Sie dem Cloud Manager ARN zur Verfügung stellen.

   d. Fügen Sie im Fensterbereich **andere AWS-Konten** das AWS-Konto hinzu, das Cloud Manager mit Berechtigungen versorgt.

      In den meisten Fällen ist dies der Account, in dem sich Cloud Manager befindet. Falls Cloud Manager nicht in AWS installiert wurde, stellen Sie als Konto die AWS Zugriffsschlüssel für Cloud Manager bereit.



e. Wechseln Sie jetzt zum AWS Konto, das Cloud Manager über Berechtigungen verfügt, und öffnen Sie die IAM-Konsole.

f. Erstellen Sie eine IAM-Richtlinie, die die unten aufgeführten Berechtigungen enthält.

g. Hängen Sie die Richtlinie an die IAM-Rolle oder den IAM-Benutzer an, der Berechtigungen für Cloud Manager bereitstellt.

   Die folgende Richtlinie bietet die Berechtigungen, die Cloud Manager zur Verwendung des CMK aus dem externen AWS-Konto benötigt. Denken Sie daran, die Region und die Account-ID in den Abschnitten „Ressource“ zu ändern.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
Weitere Details zu diesem Prozess finden Sie unter "AWS Dokumentation: Zugriff auf einen CMK für externe AWS Konten".

Starten von Cloud Volumes ONTAP in AWS

Sie können Cloud Volumes ONTAP in einer Einzelsystemkonfiguration oder als HA-Paar in AWS starten.

Starten eines Cloud Volumes ONTAP Systems mit einem Node in AWS

Wenn Sie Cloud Volumes ONTAP in AWS starten möchten, müssen Sie eine neue Arbeitsumgebung in Cloud Manager erstellen.

Bevor Sie beginnen

- Sie sollten ein haben "Anschluss, der Ihrem Arbeitsbereich zugeordnet ist".

> Sie müssen ein Kontoadministrator sein, um einen Konnektor zu erstellen. Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, fordert Cloud Manager Sie auf, einen Connector zu erstellen, wenn Sie noch keinen haben.

- "Sie sollten darauf vorbereitet sein, den Konnektor jederzeit in Betrieb zu nehmen".
- Sie sollten eine Konfiguration ausgewählt und AWS-Netzwerkinformationen von Ihrem Administrator erhalten haben. Weitere Informationen finden Sie unter "Planung Ihrer Cloud Volumes ONTAP Konfiguration".
- Wenn Sie ein BYOL-System starten möchten, müssen Sie über die 20-stellige Seriennummer (Lizenzschlüssel) verfügen.
- Wenn Sie CIFS verwenden möchten, müssen Sie DNS und Active Directory eingerichtet haben. Weitere Informationen finden Sie unter "Netzwerkanforderungen für Cloud Volumes ONTAP in AWS".

Über diese Aufgabe

Unmittelbar nach dem Erstellen der Arbeitsumgebung startet Cloud Manager eine Testinstanz im angegebenen VPC, um die Konnektivität zu überprüfen. Wenn dies erfolgreich ist, beendet Cloud Manager die Instanz sofort und beginnt dann mit der Implementierung des Cloud Volumes ONTAP Systems. Wenn Cloud Manager die Konnektivität nicht überprüfen kann, schlägt die Erstellung der Arbeitsumgebung fehl. Die Testinstanz ist entweder t2.nano (für Standard-VPC-Mandantenfähigkeit) oder m3.medium (für dedizierte VPC-Mandantenfähigkeit).

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.
2. **Wählen Sie einen Standort**: Wählen Sie **Amazon Web Services** und **Cloud Volumes ONTAP Single Node**.
3. **Details und Anmeldeinformationen**: Optional können Sie die AWS-Anmeldeinformationen und das Abonnement ändern, einen Namen der Arbeitsumgebung eingeben, bei Bedarf Tags hinzufügen und dann ein Passwort eingeben.

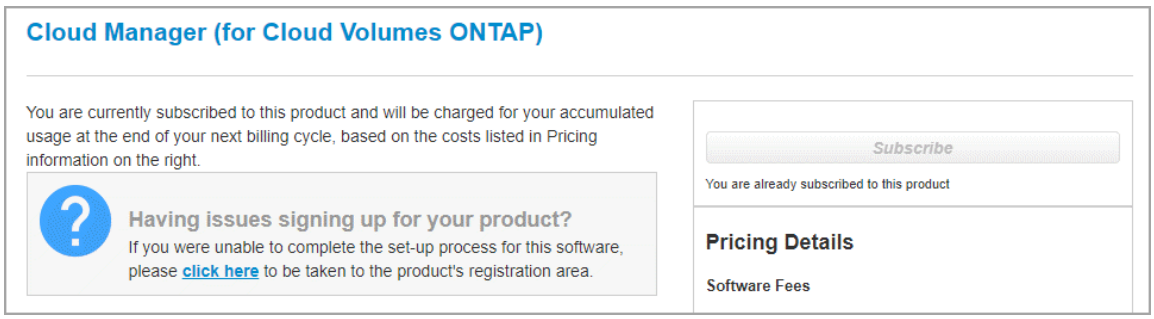
   Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Name der Arbeitsumgebung	Cloud Manager verwendet den Namen der Arbeitsumgebung, um sowohl das Cloud Volumes ONTAP System als auch die Amazon EC2 Instanz zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.
Tags hinzufügen	AWS-Tags sind Metadaten für Ihre AWS-Ressourcen. Cloud Manager fügt die Tags der Cloud Volumes ONTAP Instanz und jeder mit der Instanz verknüpften AWS Ressource hinzu. Sie können bis zu vier Tags aus der Benutzeroberfläche hinzufügen, wenn Sie eine Arbeitsumgebung erstellen. Nach der Erstellung können Sie weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen einer Arbeitsumgebung nicht auf vier Tags beschränkt. Informationen zu Tags finden Sie unter "AWS Dokumentation: Tagging der Amazon EC2 Ressourcen".
Benutzername und Passwort	Dies sind die Anmeldedaten für das Cloud Volumes ONTAP Cluster-Administratorkonto. Sie können diese Anmeldedaten verwenden, um über OnCommand System Manager oder seine CLI eine Verbindung zu Cloud Volumes ONTAP herzustellen.
Anmeldedaten Bearbeiten	AWS Zugangsdaten und das Marketplace-Abonnement für dieses Cloud Volumes ONTAP System auswählen Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen einem Abonnement zuzuordnen. Zum Erstellen eines nutzungsbasierten Cloud Volumes ONTAP Systems müssen Sie über AWS Marketplace AWS Zugangsdaten für ein Cloud Volumes ONTAP Abonnement auswählen. Sie erhalten für jedes von Ihnen erstellte Cloud Volumes ONTAP 9.6 und höhere PAYGO System und jede von Ihnen aktiviert erstellte Zusatzfunktion die Gebühr."Erfahren Sie, wie Sie Cloud Manager mit zusätzlichen AWS Zugangsdaten ergänzen".

Im folgenden Video wird gezeigt, wie Sie ein Pay-as-you-go Marketplace Abonnement mit Ihren AWS Zugangsdaten verknüpfen:

► https://docs.netapp.com/de-de/occm38//media/video_subscribing_aws.mp4 *(video)*

Wenn mehrere IAM-Benutzer im gleichen AWS-Konto arbeiten, muss jeder Benutzer sich anmelden. Wenn der erste Benutzer sich abonniert hat, informiert der AWS Marketplace die nachfolgenden Benutzer, dass sie bereits abonniert sind, wie in der Abbildung unten dargestellt. Während für das AWS *Account* ein Abonnement erfolgt, muss sich jeder IAM-Benutzer mit diesem Abonnement verknüpfen. Wenn die unten angezeigte Meldung angezeigt wird, klicken Sie auf den Link **click here**, um zu Cloud Central zu gelangen und den Vorgang
abzuschließen.



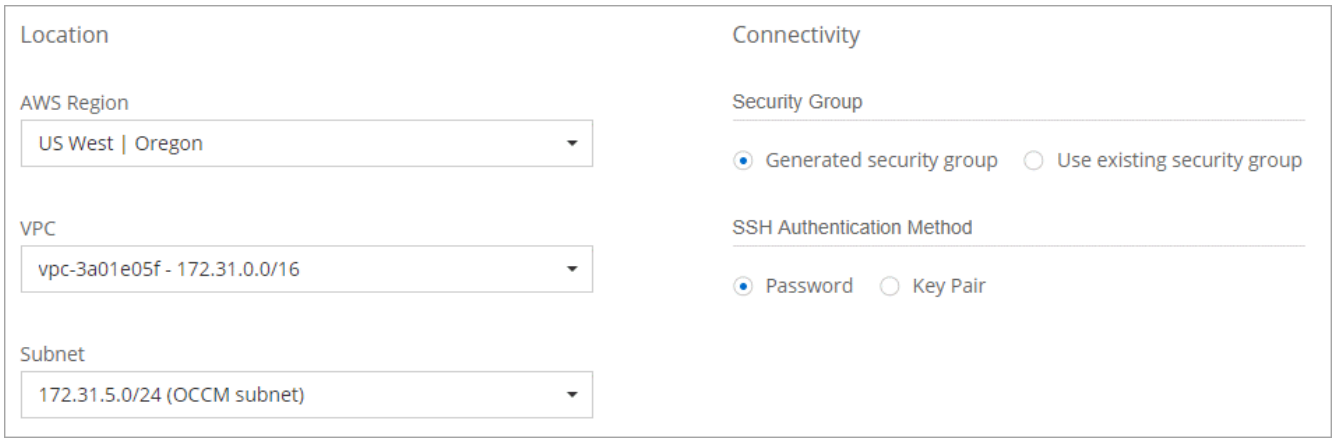
4. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie nicht mit

Cloud Volumes ONTAP verwenden möchten.

- "Erfahren Sie mehr über Cloud Compliance".
- "Weitere Informationen zu Backup in der Cloud".
- "Erfahren Sie mehr über Monitoring".

5. **Ort & Konnektivität**: Geben Sie die Netzwerkinformationen ein, die Sie im AWS-Arbeitsblatt aufgezeichnet haben.

   Das folgende Bild zeigt die ausgefüllte Seite:



6. **Datenverschlüsselung**: Wählen Sie keine Datenverschlüsselung oder Verschlüsselung von AWS.

   Für die von AWS gemanagte Verschlüsselung können Sie einen anderen Customer Master Key (CMK) von Ihrem Konto oder einem anderen AWS Konto auswählen.

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

   "So richten Sie AWS KMS für Cloud Volumes ONTAP ein".

   "Erfahren Sie mehr über unterstützte Verschlüsselungstechnologien".

7. **Lizenz- und Support-Site-Konto**: Geben Sie an, ob Sie Pay-as-you-go oder BYOL verwenden möchten, und legen Sie dann ein NetApp Support Site Konto fest.

   Informationen zur Funktionsweise von Lizenzen finden Sie unter "Lizenzierung".

   Ein NetApp Support Site Konto ist optional für „Pay-as-you-go“-Systeme erhältlich, wird aber für BYOL-Systeme benötigt. "Erfahren Sie, wie Sie Konten der NetApp Support Site hinzufügen".

8. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete aus, um schnell Cloud Volumes ONTAP zu starten, oder klicken Sie auf **eigene Konfiguration erstellen**.

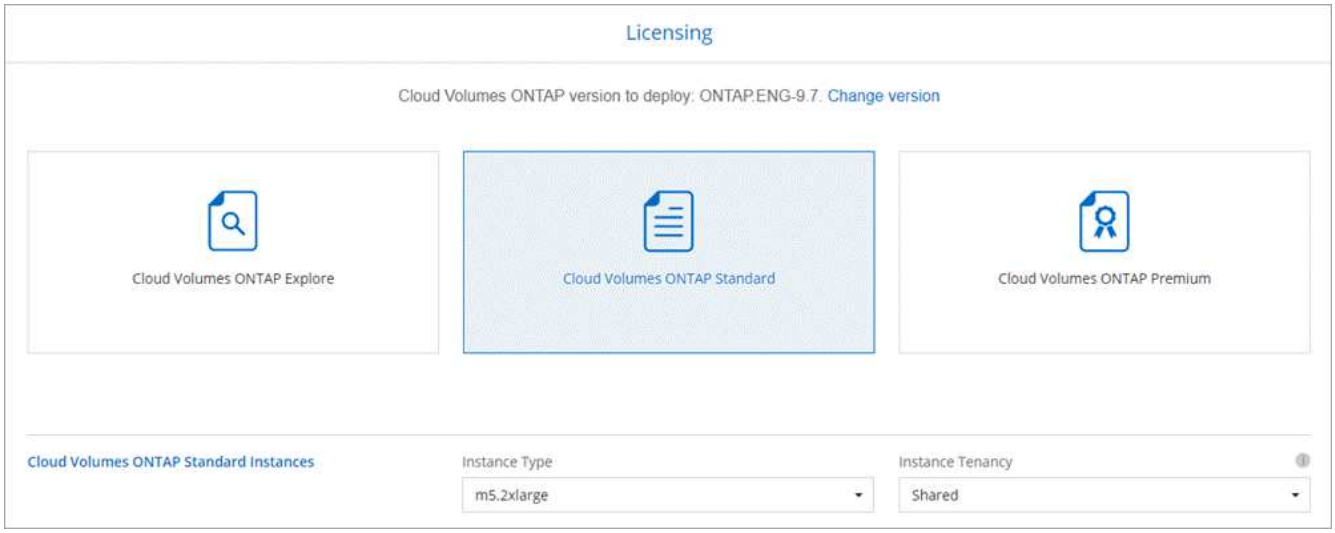
   Wenn Sie eines der Pakete auswählen, müssen Sie nur ein Volume angeben und dann die Konfiguration prüfen und genehmigen.

9. **IAM-Rolle**: Sie sollten die Standardoption beibehalten, damit Cloud Manager die Rolle für Sie erstellen kann.

   Wenn Sie Ihre eigene Richtlinie verwenden möchten, muss diese erfüllen "Richtlinienanforderungen für

Cloud Volumes ONTAP-Nodes".

10. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP-Version nach Bedarf, wählen Sie eine Lizenz, einen Instanztyp und die Instanzenfähigkeit aus.



Wenn sich Ihre Anforderungen nach dem Starten der Instanz ändern, können Sie die Lizenz oder den Instanztyp später ändern.

> Wenn für die ausgewählte Version ein neuer Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert Cloud Manager das System beim Erstellen der Arbeitsumgebung auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.6 RC1 und 9.6 GA auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.6 bis 9.7.

11. **Zugrunde liegende Speicherressourcen**: Wählen Sie die Einstellungen für das anfängliche Aggregat: Einen Datenträgertyp, eine Größe für jede Platte, und ob Daten-Tiering aktiviert werden soll.

    Beachten Sie Folgendes:

    - Der Festplattentyp ist für das anfängliche Volume. Sie können einen anderen Festplattentyp für nachfolgende Volumes auswählen.
    - Die Festplattengröße gilt für alle Festplatten im ursprünglichen Aggregat und für alle zusätzlichen Aggregate, die Cloud Manager erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuweisungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

      Hilfe bei der Auswahl von Festplattentyp und -Größe finden Sie unter "Dimensionierung Ihres Systems in AWS".

    - Sie können eine bestimmte Volume-Tiering-Richtlinie auswählen, wenn Sie ein Volume erstellen oder bearbeiten.
    - Wenn Sie das Daten-Tiering deaktivieren, können Sie es bei nachfolgenden Aggregaten aktivieren.

      "So funktioniert Daten-Tiering".

12. **Schreibgeschwindigkeit & WURM**: Wählen Sie **Normal** oder **hohe** Schreibgeschwindigkeit, und aktivieren Sie auf Wunsch den Schreib-Speicher, den WORM-Speicher.

Auswahl einer Schreibgeschwindigkeit wird nur bei Single-Node-Systemen unterstützt.

"Erfahren Sie mehr über Schreibgeschwindigkeit".

WORM kann nicht aktiviert werden, wenn Daten-Tiering aktiviert wurde.

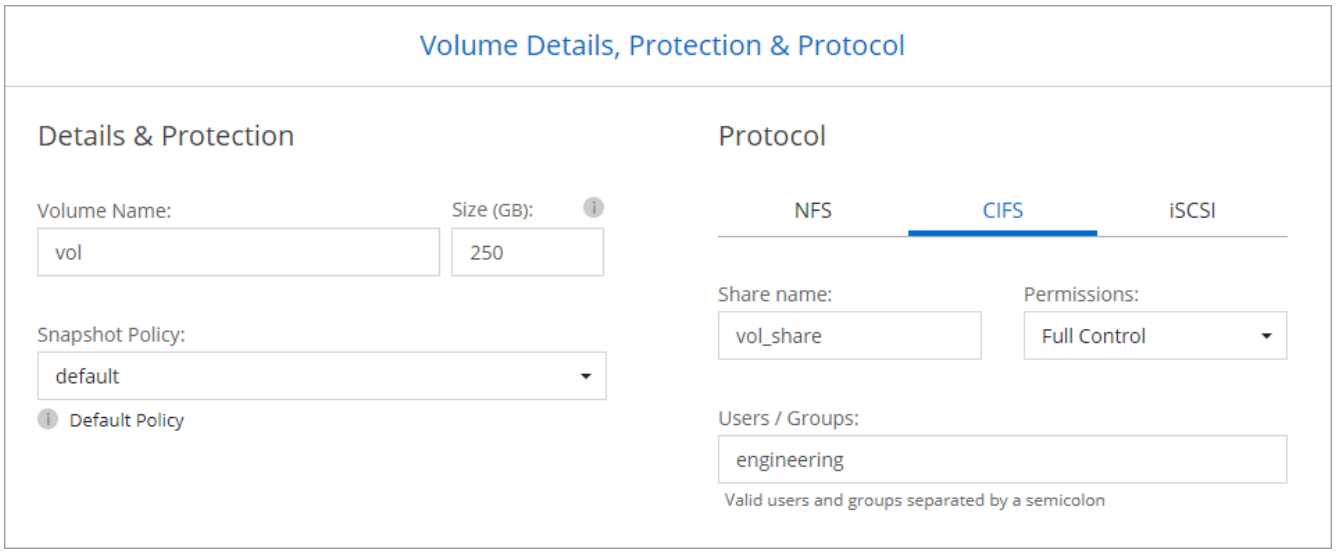
"Erfahren Sie mehr über WORM Storage".

13. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

    Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren, wodurch Sie ein Volume erstellen können, das größer ist als der derzeit verfügbare physische Storage.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt Cloud Manager einen Wert ein, der Zugriff auf alle Instanzen im Subnetz ermöglicht.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch Zugriffssteuerungslisten oder ACLs genannt). Sie können lokale oder domänenbasierte Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Domain-Windows-Benutzernamen angeben, müssen Sie die Domäne des Benutzers mit dem Format Domain\Benutzername einschließen.
Snapshot-Richtlinie	Eine Snapshot Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot Kopien an. Bei einer NetApp Snapshot Kopie handelt es sich um ein zeitpunktgenaues Filesystem Image, das keine Performance-Einbußen aufweist und minimalen Storage erfordert. Sie können die Standardrichtlinie oder keine auswählen. Sie können keine für transiente Daten auswählen, z. B. tempdb für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume: Entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt Cloud Manager automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Nachdem Sie das Volume erstellt haben, "Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen".

    Die folgende Abbildung zeigt die für das CIFS-Protokoll ausgefüllte Volume-Seite:



14. **CIFS Setup**: Wenn Sie das CIFS-Protokoll wählen, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. Wenn Sie von AWS verwaltete Microsoft AD als AD-Server für Cloud Volumes ONTAP konfigurieren, sollten Sie in diesem Feld **OU=Computers,OU=corp** eingeben.
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden** aus, um einen NTP-Server mit Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Siehe "Cloud Manager API-Entwicklerleitfaden" Entsprechende Details.

15. **Nutzungsprofil, Disk Type und Tiering Policy**: Wählen Sie, ob Sie Funktionen für die Storage-Effizienz aktivieren und die Volume Tiering Policy bei Bedarf bearbeiten möchten.

    Weitere Informationen finden Sie unter "Allgemeines zu Volume-Nutzungsprofilen" Und "Data Tiering - Übersicht".

16. **Überprüfen & Genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.

a. Überprüfen Sie die Details zur Konfiguration.

b. Klicken Sie auf **Weitere Informationen**, um Details zum Support und den von Cloud Manager erworbenen AWS Ressourcen anzuzeigen.

c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.

d. Klicken Sie Auf **Go**.

Ergebnis

Cloud Manager startet die Cloud Volumes ONTAP Instanz. Sie können den Fortschritt in der Timeline verfolgen.

Wenn beim Starten der Cloud Volumes ONTAP Instanz Probleme auftreten, lesen Sie die Fehlermeldung. Sie können auch die Arbeitsumgebung auswählen und auf Umgebung neu erstellen klicken.

Weitere Hilfe finden Sie unter "NetApp Cloud Volumes ONTAP Support".

Nachdem Sie fertig sind

- Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner, und überprüfen Sie, ob diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.
- Wenn Sie Kontingente auf Volumes anwenden möchten, verwenden Sie System Manager oder die CLI.

  Mithilfe von Quotas können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder qtree verwendeten Dateien einschränken oder nachverfolgen.

Starten eines Cloud Volumes ONTAP HA-Paars in AWS

Wenn Sie ein Cloud Volumes ONTAP HA-Paar in AWS starten möchten, müssen Sie eine HA-Arbeitsumgebung in Cloud Manager erstellen.

Bevor Sie beginnen

- Sie sollten ein haben "Anschluss, der Ihrem Arbeitsbereich zugeordnet ist".

  Sie müssen ein Kontoadministrator sein, um einen Konnektor zu erstellen. Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, fordert Cloud Manager Sie auf, einen Connector zu erstellen, wenn Sie noch keinen haben.

- "Sie sollten darauf vorbereitet sein, den Konnektor jederzeit in Betrieb zu nehmen".
- Sie sollten eine Konfiguration ausgewählt und AWS-Netzwerkinformationen von Ihrem Administrator erhalten haben. Weitere Informationen finden Sie unter "Planung Ihrer Cloud Volumes ONTAP Konfiguration".
- Wenn Sie BYOL-Lizenzen erworben haben, müssen Sie für jeden Node eine 20-stellige Seriennummer (Lizenzschlüssel) haben.
- Wenn Sie CIFS verwenden möchten, müssen Sie DNS und Active Directory eingerichtet haben. Weitere Informationen finden Sie unter "Netzwerkanforderungen für Cloud Volumes ONTAP in AWS".

Einschränkung

Derzeit werden HA-Paare nicht mit Ausposten von AWS unterstützt.

Über diese Aufgabe

Unmittelbar nach dem Erstellen der Arbeitsumgebung startet Cloud Manager eine Testinstanz im angegebenen VPC, um die Konnektivität zu überprüfen. Wenn dies erfolgreich ist, beendet Cloud Manager die Instanz sofort und beginnt dann mit der Implementierung des Cloud Volumes ONTAP Systems. Wenn Cloud Manager die Konnektivität nicht überprüfen kann, schlägt die Erstellung der Arbeitsumgebung fehl. Die Testinstanz ist entweder t2.nano (für Standard-VPC-Mandantenfähigkeit) oder m3.medium (für dedizierte VPC-Mandantenfähigkeit).

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.
2. **Wählen Sie einen Standort**: Wählen Sie **Amazon Web Services** und **Cloud Volumes ONTAP Single Node**.
3. **Details und Anmeldeinformationen**: Optional können Sie die AWS-Anmeldeinformationen und das Abonnement ändern, einen Namen der Arbeitsumgebung eingeben, bei Bedarf Tags hinzufügen und dann ein Passwort eingeben.

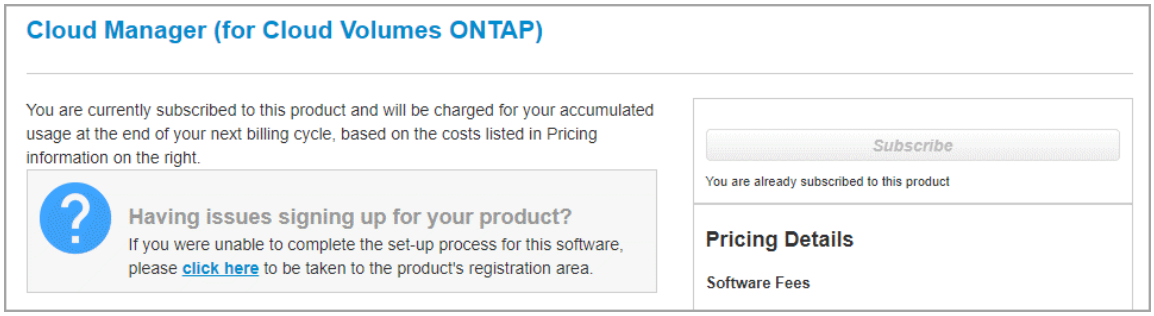
   Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Name der Arbeitsumgebung	Cloud Manager verwendet den Namen der Arbeitsumgebung, um sowohl das Cloud Volumes ONTAP System als auch die Amazon EC2 Instanz zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.
Tags hinzufügen	AWS-Tags sind Metadaten für Ihre AWS-Ressourcen. Cloud Manager fügt die Tags der Cloud Volumes ONTAP Instanz und jeder mit der Instanz verknüpften AWS Ressource hinzu. Sie können bis zu vier Tags aus der Benutzeroberfläche hinzufügen, wenn Sie eine Arbeitsumgebung erstellen. Nach der Erstellung können Sie weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen einer Arbeitsumgebung nicht auf vier Tags beschränkt. Informationen zu Tags finden Sie unter "AWS Dokumentation: Tagging der Amazon EC2 Ressourcen".
Benutzername und Passwort	Dies sind die Anmeldedaten für das Cloud Volumes ONTAP Cluster-Administratorkonto. Sie können diese Anmeldedaten verwenden, um über OnCommand System Manager oder seine CLI eine Verbindung zu Cloud Volumes ONTAP herzustellen.
Anmeldedaten Bearbeiten	AWS Zugangsdaten und das Marketplace-Abonnement für dieses Cloud Volumes ONTAP System auswählen Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen einem Abonnement zuzuordnen. Zum Erstellen eines nutzungsbasierten Cloud Volumes ONTAP Systems müssen Sie über AWS Marketplace AWS Zugangsdaten für ein Cloud Volumes ONTAP Abonnement auswählen. Sie erhalten für jedes von Ihnen erstellte Cloud Volumes ONTAP 9.6 und höhere PAYGO System und jede von Ihnen aktiviert erstellte Zusatzfunktion die Gebühr."Erfahren Sie, wie Sie Cloud Manager mit zusätzlichen AWS Zugangsdaten ergänzen".

   Im folgenden Video wird gezeigt, wie Sie ein Pay-as-you-go Marketplace Abonnement mit Ihren AWS Zugangsdaten verknüpfen:

   ► https://docs.netapp.com/de-de/occm38//media/video_subscribing_aws.mp4 *(video)*

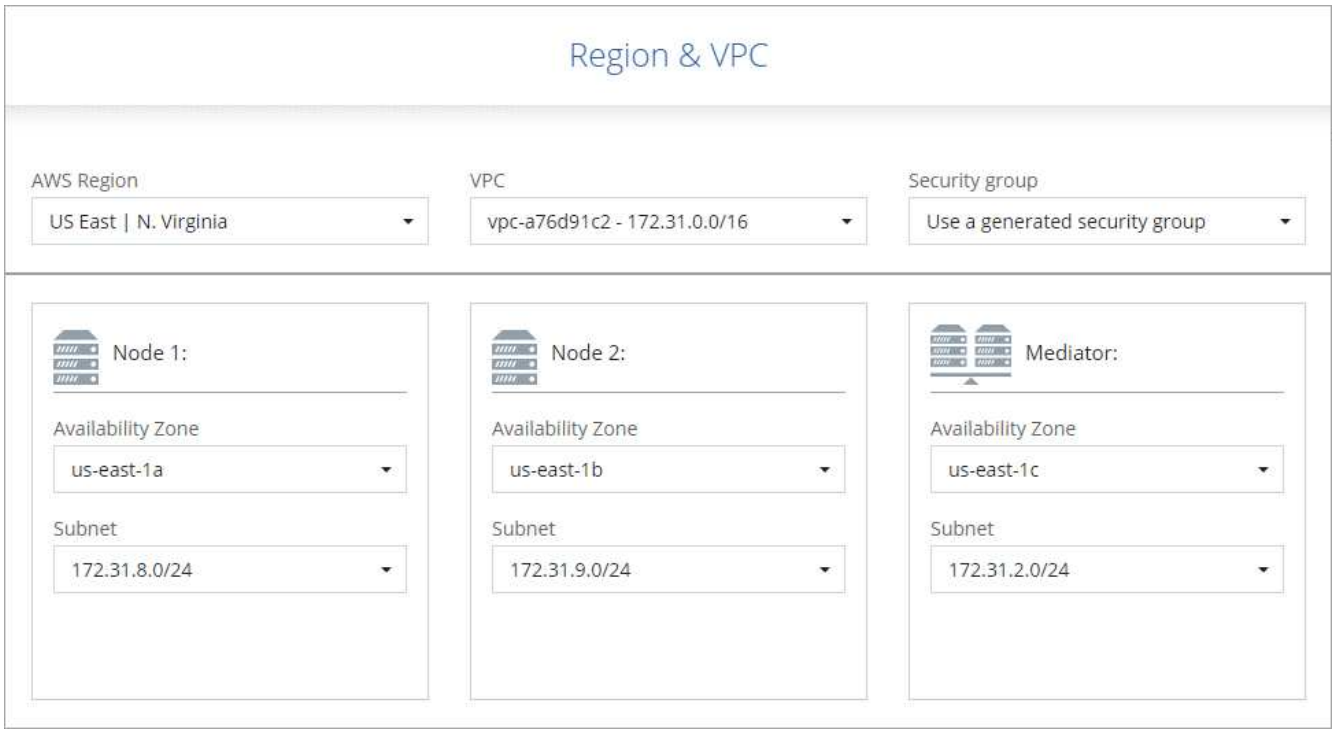
Wenn mehrere IAM-Benutzer im gleichen AWS-Konto arbeiten, muss jeder Benutzer sich anmelden. Wenn der erste Benutzer sich abonniert hat, informiert der AWS Marketplace die nachfolgenden Benutzer, dass sie bereits abonniert sind, wie in der Abbildung unten dargestellt. Während für das AWS *Account* ein Abonnement erfolgt, muss sich jeder IAM-Benutzer mit diesem Abonnement verknüpfen. Wenn die unten angezeigte Meldung angezeigt wird, klicken Sie auf den Link **click here**, um zu Cloud Central zu gelangen und den Vorgang
abzuschließen.



4. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie mit diesem Cloud Volumes ONTAP-System nicht verwenden möchten.
   - "Erfahren Sie mehr über Cloud Compliance".
   - "Weitere Informationen zu Backup in der Cloud".
   - "Erfahren Sie mehr über Monitoring".
5. **HA-Bereitstellungsmodelle**: Wählen Sie eine HA-Konfiguration.

   Einen Überblick über die Implementierungsmodelle finden Sie unter "Cloud Volumes ONTAP HA für AWS".
6. **Region & VPC**: Geben Sie die Netzwerkinformationen ein, die Sie im AWS-Arbeitsblatt aufgezeichnet haben.

   Das folgende Bild zeigt die Seite, die für eine Konfiguration mit mehreren AZ ausgefüllt wurde:



7. **Konnektivität und SSH Authentifizierung**: Wählen Sie Verbindungsmethoden für das HA-Paar und den Mediator.
8. **Schwebende IPs**: Wenn Sie mehrere AZS gewählt haben, geben Sie die fließenden IP-Adressen an.

   Die IP-Adressen müssen für alle VPCs in der Region außerhalb des CIDR-Blocks liegen. Weitere Informationen finden Sie unter "AWS Netzwerkanforderungen für Cloud Volumes ONTAP HA in mehreren AZS".

9. **Routentabellen**: Wenn Sie mehrere AZS gewählt haben, wählen Sie die Routentabellen aus, die Routen zu den schwimmenden IP-Adressen enthalten sollen.

   Wenn Sie mehr als eine Routentabelle haben, ist es sehr wichtig, die richtigen Routentabellen auszuwählen. Andernfalls haben einige Clients möglicherweise keinen Zugriff auf das Cloud Volumes ONTAP HA-Paar. Weitere Informationen zu Routingtabellen finden Sie unter "AWS Documentation: Routingtabellen".

10. **Datenverschlüsselung**: Wählen Sie keine Datenverschlüsselung oder Verschlüsselung von AWS.

    Für die von AWS gemanagte Verschlüsselung können Sie einen anderen Customer Master Key (CMK) von Ihrem Konto oder einem anderen AWS Konto auswählen.

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

    "So richten Sie AWS KMS für Cloud Volumes ONTAP ein".

    "Erfahren Sie mehr über unterstützte Verschlüsselungstechnologien".

11. **Lizenz- und Support-Site-Konto**: Geben Sie an, ob Sie Pay-as-you-go oder BYOL verwenden möchten, und legen Sie dann ein NetApp Support Site Konto fest.

    Informationen zur Funktionsweise von Lizenzen finden Sie unter "Lizenzierung".

Ein NetApp Support Site Konto ist optional für „Pay-as-you-go“-Systeme erhältlich, wird aber für BYOL-Systeme benötigt. "Erfahren Sie, wie Sie Konten der NetApp Support Site hinzufügen".

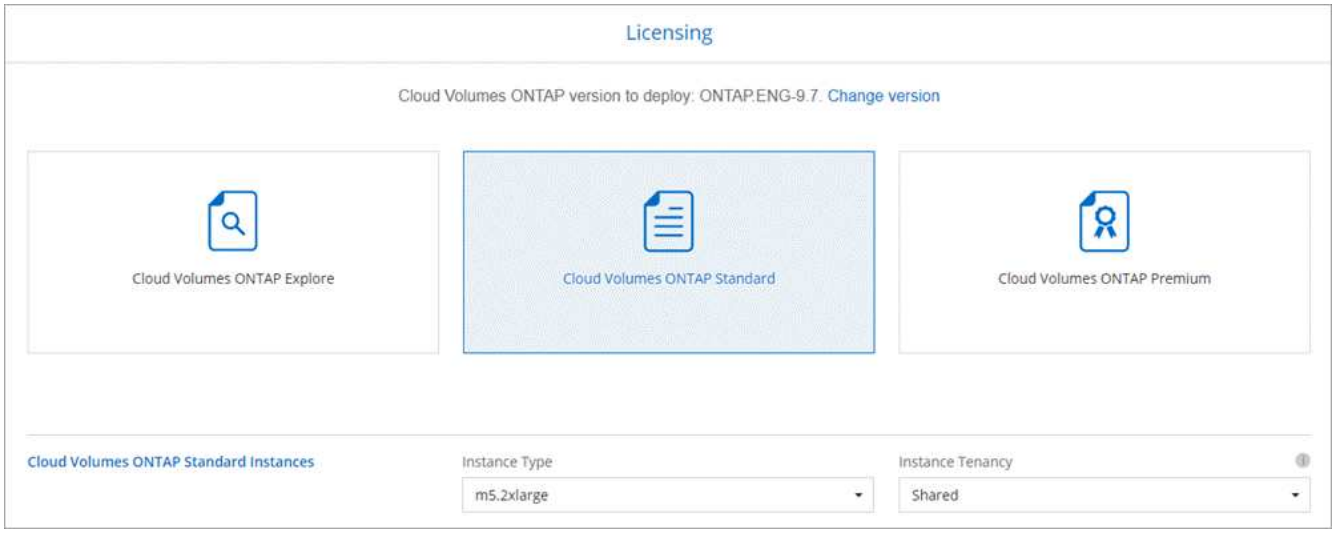
12. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete aus, um schnell ein Cloud Volumes ONTAP System zu starten, oder klicken Sie auf **eigene Konfiguration erstellen**.

    Wenn Sie eines der Pakete auswählen, müssen Sie nur ein Volume angeben und dann die Konfiguration prüfen und genehmigen.

13. **IAM-Rolle**: Sie sollten die Standardoption beibehalten, damit Cloud Manager die Rollen für Sie erstellen kann.

    Wenn Sie Ihre eigene Richtlinie verwenden möchten, muss diese erfüllen "Richtlinienanforderungen für Cloud Volumes ONTAP-Nodes und den HA-Mediator".

14. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP-Version nach Bedarf, wählen Sie eine Lizenz, einen Instanztyp und die Instanzenfähigkeit aus.



    Wenn sich Ihre Anforderungen nach dem Starten der Instanzen ändern, können Sie die Lizenz oder den Instanztyp später ändern.

    Wenn für die ausgewählte Version ein neuer Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert Cloud Manager das System beim Erstellen der Arbeitsumgebung auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.6 RC1 und 9.6 GA auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.6 bis 9.7.

15. **Zugrunde liegende Speicherressourcen**: Wählen Sie die Einstellungen für das anfängliche Aggregat: Einen Datenträgertyp, eine Größe für jede Platte, und ob Daten-Tiering aktiviert werden soll.

    Beachten Sie Folgendes:

    - Der Festplattentyp ist für das anfängliche Volume. Sie können einen anderen Festplattentyp für nachfolgende Volumes auswählen.
    - Die Festplattengröße gilt für alle Festplatten im ursprünglichen Aggregat und für alle zusätzlichen Aggregate, die Cloud Manager erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuweisungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

Hilfe bei der Auswahl von Festplattentyp und -Größe finden Sie unter "Dimensionierung Ihres Systems in AWS".

- Sie können eine bestimmte Volume-Tiering-Richtlinie auswählen, wenn Sie ein Volume erstellen oder bearbeiten.
- Wenn Sie das Daten-Tiering deaktivieren, können Sie es bei nachfolgenden Aggregaten aktivieren.

"So funktioniert Daten-Tiering".

16. **WORM**: Aktivieren Sie auf Wunsch den WORM-Speicher (write once, read many).

    WORM kann nicht aktiviert werden, wenn Daten-Tiering aktiviert wurde.

    "Erfahren Sie mehr über WORM Storage".

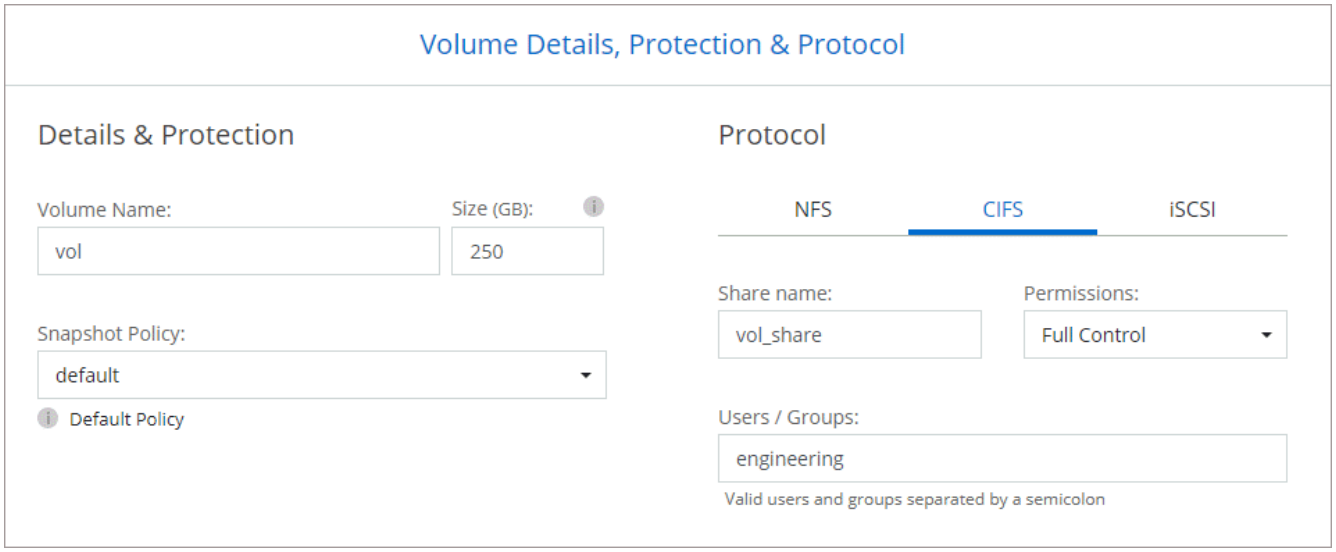
17. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

    Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren, wodurch Sie ein Volume erstellen können, das größer ist als der derzeit verfügbare physische Storage.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt Cloud Manager einen Wert ein, der Zugriff auf alle Instanzen im Subnetz ermöglicht.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch Zugriffssteuerungslisten oder ACLs genannt). Sie können lokale oder domänenbasierte Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Domain-Windows-Benutzernamen angeben, müssen Sie die Domäne des Benutzers mit dem Format Domain\Benutzername einschließen.
Snapshot-Richtlinie	Eine Snapshot Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot Kopien an. Bei einer NetApp Snapshot Kopie handelt es sich um ein zeitpunktgenaues Filesystem Image, das keine Performance-Einbußen aufweist und minimalen Storage erfordert. Sie können die Standardrichtlinie oder keine auswählen. Sie können keine für transiente Daten auswählen, z. B. tempdb für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume: Entweder NFSv3 oder NFSv4.

Feld	Beschreibung
Initiatorgruppe und IQN (nur für iSCSI)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt Cloud Manager automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Nachdem Sie das Volume erstellt haben, "Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen".

Die folgende Abbildung zeigt die für das CIFS-Protokoll ausgefüllte Volume-Seite:



18. **CIFS Setup**: Wenn Sie das CIFS-Protokoll ausgewählt haben, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.

Feld	Beschreibung
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. Wenn Sie von AWS verwaltete Microsoft AD als AD-Server für Cloud Volumes ONTAP konfigurieren, sollten Sie in diesem Feld **OU=Computers,OU=corp** eingeben.
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden** aus, um einen NTP-Server mit Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Siehe "Cloud Manager API-Entwicklerleitfaden" Entsprechende Details.

19. **Nutzungsprofil, Disk Type und Tiering Policy**: Wählen Sie, ob Sie Funktionen für die Storage-Effizienz aktivieren und die Volume Tiering Policy bei Bedarf bearbeiten möchten.

    Weitere Informationen finden Sie unter "Allgemeines zu Volume-Nutzungsprofilen" Und "Data Tiering - Übersicht".

20. **Überprüfen & Genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um Details zum Support und den von Cloud Manager erworbenen AWS Ressourcen anzuzeigen.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie Auf **Go**.

Ergebnis

Cloud Manager startet das Paar Cloud Volumes ONTAP HA. Sie können den Fortschritt in der Timeline verfolgen.

Wenn beim Starten des HA-Paars Probleme auftreten, überprüfen Sie die Fehlermeldung. Sie können auch die Arbeitsumgebung auswählen und auf Umgebung neu erstellen klicken.

Weitere Hilfe finden Sie unter "NetApp Cloud Volumes ONTAP Support".

Nachdem Sie fertig sind

- Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner, und überprüfen Sie, ob diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.
- Wenn Sie Kontingente auf Volumes anwenden möchten, verwenden Sie System Manager oder die CLI.

  Mithilfe von Quotas können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder qtree verwendeten Dateien einschränken oder nachverfolgen.

Erste Schritte in Azure

Erste Schritte mit Cloud Volumes ONTAP für Azure

Erste Schritte mit Cloud Volumes ONTAP für Azure

Einen Konnektor erstellen

Wenn Sie keine haben "Stecker" Dennoch muss ein Kontoadministrator einen erstellen. "Erfahren Sie, wie Sie in Azure einen Connector erstellen".

Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von Cloud Manager aufgefordert, einen Connector bereitzustellen, wenn Sie noch keinen haben.

Planen Sie Ihre Konfiguration

Cloud Manager bietet vorkonfigurierte Pakete, die Ihren Workload-Anforderungen entsprechen, oder Sie können eine eigene Konfiguration erstellen. Wenn Sie sich für eine eigene Konfiguration entscheiden, sollten Sie sich mit den verfügbaren Optionen vertraut machen. "Weitere Informationen .".

Richten Sie Ihr Netzwerk ein

1. Stellen Sie sicher, dass Ihre vnet und Subnetze Verbindungen zwischen dem Connector und Cloud Volumes ONTAP unterstützen.
2. Aktivieren Sie den ausgehenden Internetzugriff über das Ziel-vnet, damit der Konnektor und der Cloud Volumes ONTAP mehrere Endpunkte kontaktieren können.

   Dieser Schritt ist wichtig, da der Connector Cloud Volumes ONTAP nicht ohne Outbound-Internetzugang verwalten kann. Wenn Sie die ausgehende Verbindung begrenzen müssen, lesen Sie die Liste der Endpunkte für "Anschluss und Cloud Volumes ONTAP".

"Erfahren Sie mehr über Netzwerkanforderungen".

Starten Sie Cloud Volumes ONTAP mit Cloud Manager

Klicken Sie auf **Arbeitsumgebung hinzufügen**, wählen Sie den Systemtyp aus, den Sie bereitstellen möchten, und führen Sie die Schritte im Assistenten aus. "Lesen Sie Schritt-für-Schritt-Anleitungen".

Weiterführende Links

- "Bewertung"
- "Erstellen eines Connectors über Cloud Manager"
- "Erstellen eines Connectors über den Azure Marketplace"
- "Installieren der Connector-Software auf einem Linux-Host"
- "Was Cloud Manager mit Azure-Berechtigungen tut"

Planen Ihrer Cloud Volumes ONTAP-Konfiguration in Azure

Wenn Sie Cloud Volumes ONTAP in Azure implementieren, können Sie entweder ein vorkonfiguriertes System wählen, das Ihren Workload-Anforderungen entspricht, oder Sie erstellen Ihre eigene Konfiguration. Wenn Sie sich für eine eigene Konfiguration

entscheiden, sollten Sie sich mit den verfügbaren Optionen vertraut machen.

Auswahl eines Lizenztyps

Cloud Volumes ONTAP ist in zwei Preisoptionen erhältlich: Nutzungsbasiert und als BYOL-Modell (Bring-Your-Own-License). Für Pay-as-you-go können Sie zwischen drei Lizenzen wählen: Explore, Standard oder Premium. Jede Lizenz bietet verschiedene Kapazitäts- und Computing-Optionen.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP 9.7 in Azure"

Storage-Grenzen kennen

Die Rohkapazitätsgrenze für ein Cloud Volumes ONTAP System ist an die Lizenz gebunden. Zusätzliche Beschränkungen wirken sich auf die Größe von Aggregaten und Volumes aus. Sie sollten sich dieser Grenzen bei der Planung Ihrer Konfiguration bewusst sein.

"Storage-Höchstwerte für Cloud Volumes ONTAP 9.7 in Azure"

Dimensionierung Ihres Systems in Azure

Mit der Dimensionierung Ihres Cloud Volumes ONTAP Systems können Sie die Anforderungen an Performance und Kapazität erfüllen. Bei der Auswahl von VM-Typ, Festplattentyp und Festplattengröße sind einige wichtige Punkte zu beachten:

Typ der virtuellen Maschine

Sehen Sie sich die unterstützten Typen von Virtual Machines in an "Versionshinweise zu Cloud Volumes ONTAP" Und überprüfen Sie anschließend Details zu jedem unterstützten VM-Typ. Beachten Sie, dass jeder VM-Typ eine bestimmte Anzahl an Datenfestplatten unterstützt.

- "Azure-Dokumentation: Allgemeine Größe virtueller Maschinen"
- "Azure-Dokumentation: Für den Speicher optimierte Größen virtueller Maschinen"

Azure-Festplattentyp

Wenn Sie Volumes für Cloud Volumes ONTAP erstellen, müssen Sie den zugrunde liegenden Cloud-Storage auswählen, den Cloud Volumes ONTAP als Festplatte verwendet.

HA-Systeme verwenden Premium-Blobs auf Seite. In der Zwischenzeit können Systeme mit einem Node zwei Typen von Azure Managed Disks nutzen:

- *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.

  Weitere Details zu den Anwendungsfällen für diese Festplatten finden Sie unter "Microsoft Azure-Dokumentation: Welche Festplattentypen sind in Azure verfügbar?".

Festplattengröße Azure

Wenn Sie Cloud Volumes ONTAP Instanzen starten, müssen Sie die standardmäßige Festplattengröße für Aggregate auswählen. Cloud Manager verwendet diese Festplattengröße für das anfängliche Aggregat und

für alle zusätzlichen Aggregate, die es erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Sie können Aggregate erstellen, die eine Festplattengröße verwenden, die sich von der Standardgröße unterscheidet "Verwenden der erweiterten Zuweisungsoption".

Alle Festplatten in einem Aggregat müssen dieselbe Größe haben.

Bei der Auswahl der Festplattengröße sollten Sie mehrere Faktoren berücksichtigen. Die Festplattengröße wirkt sich darauf aus, wie viel Sie für Storage zahlen, wie viele Volumes Sie in einem Aggregat erstellen können, wie viel Kapazität insgesamt für Cloud Volumes ONTAP zur Verfügung steht und wie hoch die Storage-Performance ist.

Die Performance von Azure Premium Storage ist an die Festplattengröße gebunden. Größere Festplatten bieten höhere IOPS und einen höheren Durchsatz. Beispielsweise kann die Auswahl von 1-TB-Festplatten eine bessere Performance bieten als 500-GB-Festplatten zu höheren Kosten.

Es gibt keine Performance-Unterschiede zwischen den Festplattengrößen für Standard-Storage. Sie sollten die Festplattengröße basierend auf der benötigten Kapazität auswählen.

Unter Azure finden Sie IOPS und Durchsatz nach Festplattengröße:

- "Microsoft Azure: Preisgestaltung für Managed Disks"
- "Microsoft Azure: Page Blobs Pricing"

Auswahl einer Konfiguration, die Flash Cache unterstützt

Eine Cloud Volumes ONTAP-Konfiguration in Azure umfasst lokalen NVMe-Storage, den Cloud Volumes ONTAP zur Steigerung der Performance als *Flash Cache* verwendet. "Weitere Informationen zu Flash Cache".

Azure Network Information Worksheet

Wenn Sie Cloud Volumes ONTAP in Azure implementieren, müssen Sie Details zu Ihrem virtuellen Netzwerk angeben. Sie können ein Arbeitsblatt verwenden, um die Informationen von Ihrem Administrator zu sammeln.

Azure Informationen	Ihr Wert
Region	
Virtuelles Netzwerk (VNet)	
Subnetz	
Netzwerksicherheitsgruppe (wenn Sie Ihre eigene verwenden)	

Auswählen einer Schreibgeschwindigkeit

Mit Cloud Manager können Sie eine Einstellung für die Schreibgeschwindigkeit für Cloud Volumes ONTAP Systeme mit einem Node wählen. Bevor Sie sich für eine Schreibgeschwindigkeit entscheiden, sollten Sie die Unterschiede zwischen den normalen und hohen Einstellungen sowie Risiken und Empfehlungen verstehen, wenn Sie eine hohe Schreibgeschwindigkeit verwenden.

Unterschied zwischen normaler Schreibgeschwindigkeit und hoher Schreibgeschwindigkeit

Wenn Sie sich für eine normale Schreibgeschwindigkeit entscheiden, werden die Daten direkt auf die Festplatte geschrieben, wodurch die Wahrscheinlichkeit eines Datenverlusts bei einem ungeplanten Systemausfall verringert wird.

Wenn Sie hohe Schreibgeschwindigkeit wählen, werden die Daten vor dem Schreiben auf die Festplatte im Speicher gepuffert, was eine schnellere Schreibleistung ermöglicht. Aufgrund dieses Cachings besteht die Gefahr eines Datenverlusts, wenn ein ungeplanter Systemausfall auftritt.

Die Datenmenge, die bei einem ungeplanten Systemausfall verloren gehen kann, entspricht der Spanne der letzten beiden Konsistenzpunkte. Ein Konsistenzpunkt ist das Schreiben gepufferter Daten auf die Festplatte. Ein Konsistenzpunkt tritt auf, wenn das Schreibprotokoll voll ist oder nach 10 Sekunden (je nachdem, was zuerst eintritt). Die Performance des AWS EBS-Volumes kann sich jedoch auf die Verarbeitungszeit des Konsistenzpunkts auswirken.

Wann wird hohe Schreibgeschwindigkeit verwendet

Hohe Schreibgeschwindigkeit ist eine gute Wahl, wenn für Ihre Workload eine schnelle Schreibleistung erforderlich ist und Sie das Risiko eines Datenverlusts bei einem ungeplanten Systemausfall überstehen können.

Empfehlungen bei hoher Schreibgeschwindigkeit

Wenn Sie die hohe Schreibgeschwindigkeit aktivieren, sollten Sie den Schreibschutz auf der Anwendungsebene sicherstellen.

Auswählen eines Volume-Nutzungsprofils

ONTAP umfasst mehrere Storage-Effizienzfunktionen, mit denen Sie die benötigte Storage-Gesamtmenge reduzieren können. Wenn Sie ein Volume in Cloud Manager erstellen, können Sie ein Profil auswählen, das diese Funktionen aktiviert, oder ein Profil, das sie deaktiviert. Sie sollten mehr über diese Funktionen erfahren, um zu entscheiden, welches Profil Sie verwenden möchten.

NetApp Storage-Effizienzfunktionen bieten folgende Vorteile:

Thin Provisioning
: Bietet Hosts oder Benutzern mehr logischen Storage als in Ihrem physischen Storage-Pool. Anstatt Storage vorab zuzuweisen, wird jedem Volume beim Schreiben von Daten dynamisch Speicherplatz zugewiesen.

Deduplizierung
: Verbessert die Effizienz, indem identische Datenblöcke lokalisiert und durch Verweise auf einen einzelnen gemeinsam genutzten Block ersetzt werden. Durch diese Technik werden die Storage-Kapazitätsanforderungen reduziert, da redundante Datenblöcke im selben Volume eliminiert werden.

Komprimierung
: Reduziert die physische Kapazität, die zum Speichern von Daten erforderlich ist, indem Daten in einem Volume auf primärem, sekundärem und Archiv-Storage komprimiert werden.

Netzwerkanforderungen für die Implementierung und das Management von Cloud Volumes ONTAP in Azure

Richten Sie Ihr Azure Netzwerk ein, um Cloud Volumes ONTAP Systeme ordnungsgemäß funktionieren zu können. Dazu gehört auch die Vernetzung von

Connector und Cloud Volumes ONTAP.

Anforderungen für Cloud Volumes ONTAP

Die folgenden Netzwerkanforderungen müssen in Azure erfüllt werden.

Outbound-Internetzugang für Cloud Volumes ONTAP

Cloud Volumes ONTAP erfordert ausgehenden Internetzugang, um Nachrichten an NetApp AutoSupport zu senden, der proaktiv den Zustand Ihres Storage überwacht.

Routing- und Firewall-Richtlinien müssen HTTP-/HTTPS-Datenverkehr an die folgenden Endpunkte ermöglichen, damit Cloud Volumes ONTAP AutoSupport-Meldungen senden kann:

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

"Erfahren Sie, wie AutoSupport konfiguriert wird".

Sicherheitsgruppen

Sie müssen keine Sicherheitsgruppen erstellen, da Cloud Manager dies für Sie tut. Wenn Sie Ihre eigene Verwendung benötigen, lesen Sie die unten aufgeführten Sicherheitsgruppenregeln.

Anzahl der IP-Adressen

Cloud Manager weist Cloud Volumes ONTAP in Azure die folgende Anzahl von IP-Adressen zu:

- Single Node: 5 IP-Adressen
- HA-Paar: 16 IP-Adressen

Cloud Manager erstellt eine SVM-Management-LIF auf HA-Paare, jedoch nicht auf Systemen mit einem einzelnen Node in Azure.

Ein LIF ist eine IP-Adresse, die einem physischen Port zugewiesen ist. Für Managementtools wie SnapCenter ist eine SVM-Management-LIF erforderlich.

Verbindung von Cloud Volumes ONTAP zu Azure Blob Storage für Data Tiering

Wenn Sie „kalte“ Daten für den Azure Blob Storage Tiering möchten, müssen Sie keine Verbindung zwischen der Performance-Tier und der Kapazitäts-Tier einrichten, solange Cloud Manager über die erforderlichen Berechtigungen verfügt. Cloud Manager unterstützt ein vnet-Service-Endpunkt für Sie, wenn die Cloud Manager-Richtlinie über die folgenden Berechtigungen verfügt:

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Diese Berechtigungen sind in der neuesten enthalten "Cloud Manager-Richtlinie".

Weitere Informationen zum Einrichten von Daten-Tiering finden Sie unter "Tiering von kalten Daten auf kostengünstigen Objekt-Storage".

Verbindungen zu ONTAP Systemen in anderen Netzwerken

Um Daten zwischen einem Cloud Volumes ONTAP System in Azure und ONTAP Systemen in anderen Netzwerken zu replizieren, müssen Sie über eine VPN-Verbindung zwischen Azure VNet und dem anderen Netzwerk verfügen, z. B. einem AWS VPC oder Ihrem Unternehmensnetzwerk.

Anweisungen finden Sie unter "Microsoft Azure Dokumentation: Erstellen Sie eine Site-to-Site-Verbindung im Azure-Portal".

Anforderungen an den Steckverbinder

Richten Sie Ihr Netzwerk ein, damit der Connector Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen kann. Der wichtigste Schritt besteht darin, ausgehenden Internetzugriff auf verschiedene Endpunkte zu gewährleisten.

Wenn Ihr Netzwerk für die gesamte Kommunikation mit dem Internet einen Proxyserver verwendet, können Sie den Proxyserver über die Seite Einstellungen angeben. Siehe "Konfigurieren des Connectors für die Verwendung eines Proxy-Servers".

Verbindungen zu Zielnetzwerken

Für einen Connector ist eine Netzwerkverbindung zu den VPCs und VNets erforderlich, in denen Cloud Volumes ONTAP bereitgestellt werden soll.

Wenn Sie beispielsweise einen Connector in Ihrem Unternehmensnetzwerk installieren, müssen Sie eine VPN-Verbindung zur VPC oder vnet einrichten, in der Sie Cloud Volumes ONTAP starten.

Outbound-Internetzugang

Für den Connector ist ein abgehender Internetzugang erforderlich, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung zu managen. Ein Connector kontaktiert folgende Endpunkte beim Managen von Ressourcen in Azure:

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den meisten Azure Regionen.
https://management.microsoftazure.de https://login.microsoftonline.de	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den Azure Germany Regionen.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den Azure US Gov Regionen.
https://api.services.cloud.netapp.com:443	API-Anfragen an NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://repo.cloud.support.netapp.com	Wird zum Herunterladen der Abhängigkeiten von Cloud Manager verwendet.
http://repo.mysql.com/	Zum Herunterladen von MySQL.

Endpunkte	Zweck
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Cloud Manager kann Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images abrufen und herunterladen.
https://cloudmanagerinfraprod.azurecr.io	Zugriff auf Software-Images von Container-Komponenten für eine Infrastruktur, die Docker ausführt und eine Lösung für die Service-Integration mit Cloud Manager bietet.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cloudmanager.cloud.netapp.com	Kommunikation mit dem Cloud Manager-Service, der Cloud Central-Konten einschließt
https://netapp-cloud-account.auth0.com	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
https://mysupport.netapp.com	Kommunikation mit NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Kommunikation mit NetApp bei Systemlizenzrechten und Support-Registrierung
https://ipa-signer.cloudmanager.netapp.com	Ermöglicht Cloud Manager die Generierung von Lizenzen (beispielsweise eine FlexCache Lizenz für Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Erforderlich, um Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster zu verbinden Mit den Endpunkten ist die Installation von NetApp Trident möglich.
*.blob.core.windows.net	Bei Verwendung eines Proxy erforderlich für HA-Paare
Verschiedene Standorte von Drittanbietern, z. B.: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org An Standorten von Drittanbietern können Änderungen vorgenommen werden.	Während Upgrades lädt Cloud Manager die neuesten Pakete für Abhängigkeiten von Drittanbietern herunter.

Während Sie fast alle Aufgaben über die SaaS-Benutzeroberfläche ausführen sollten, steht auf dem Connector weiterhin eine lokale Benutzeroberfläche zur Verfügung. Die Maschine, auf der der Webbrowser ausgeführt wird, muss über Verbindungen zu den folgenden Endpunkten verfügen:

Endpunkte	Zweck
Der Connector-Host	Sie müssen die IP-Adresse des Hosts aus einem Webbrowser eingeben, um die Cloud Manager-Konsole zu laden. Je nach Ihrer Verbindung mit Ihrem Cloud-Provider können Sie die private IP oder eine dem Host zugewiesene öffentliche IP verwenden: • Eine private IP funktioniert, wenn Sie über ein VPN verfügen und direkten Zugriff auf Ihr virtuelles Netzwerk haben • Eine öffentliche IP funktioniert in jedem Netzwerkszenario In jedem Fall sollten Sie den Netzwerkzugriff sichern, indem Sie sicherstellen, dass die Sicherheitsgruppenregeln den Zugriff nur von autorisierten IPs oder Subnetzen ermöglichen.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Ihr Webbrowser stellt über NetApp Cloud Central eine Verbindung zu diesen Endpunkten her, um eine zentralisierte Benutzerauthentifizierung zu ermöglichen.
https://widget.intercom.io	Für Ihren Produkt-Chat, der Ihnen das Gespräch mit NetApp Cloud-Experten ermöglicht.

Regeln für Sicherheitsgruppen für Cloud Volumes ONTAP

Cloud Manager erstellt Azure-Sicherheitsgruppen mit den ein- und ausgehenden Regeln, die für den erfolgreichen Betrieb von Cloud Volumes ONTAP erforderlich sind. Sie können die Ports zu Testzwecken oder zur Verwendung eigener Sicherheitsgruppen verwenden.

Die Sicherheitsgruppe für Cloud Volumes ONTAP erfordert sowohl eingehende als auch ausgehende Regeln.

Eingehende Regeln für Single-Node-Systeme

Die unten aufgeführten Regeln erlauben den Datenverkehr, es sei denn, die Beschreibung stellt fest, dass bestimmte eingehende Daten blockiert werden.

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
1000 Inbound_SSH	22 TCP	Beliebige Art	SSH-Zugriff auf die IP-Adresse der Cluster Management LIF oder einer Node Management LIF
1001 Inbound_http	80 TCP	Beliebige Art	HTTP-Zugriff auf die System Manager Webkonsole mit der IP-Adresse der Cluster-Management-LIF
1002 Inbound_111_tcp	111 TCP	Beliebige Art	Remote-Prozeduraufruf für NFS

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
1003 Inbound_111_udp	111 UDP	Beliebige Art	Remote-Prozeduraufruf für NFS
1004 eingehend_139	139 TCP	Beliebige Art	NetBIOS-Servicesitzung für CIFS
1005 Inbound_161-162 _tcp	161-162 TCP	Beliebige Art	Einfaches Netzwerkverwaltungsprotokoll
1006 Inbound_161-162 _udp	161-162 UDP	Beliebige Art	Einfaches Netzwerkverwaltungsprotokoll
1007 eingehend_443	443 TCP	Beliebige Art	HTTPS-Zugriff auf die System Manager-Webkonsole unter Verwendung der IP-Adresse der Cluster-Management-LIF
1008 eingehend_445	445 TCP	Beliebige Art	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
1009 Inbound_635_tcp	635 TCP	Beliebige Art	NFS-Mount
1010 Inbound_635_udp	635 UDP	Beliebige Art	NFS-Mount
1011 eingehend_749	749 TCP	Beliebige Art	Kerberos
1012 Inbound_2049_tcp	2049 TCP	Beliebige Art	NFS-Server-Daemon
1013 Inbound_2049_udp	2049 UDP	Beliebige Art	NFS-Server-Daemon
1014 eingehend_3260	3260 TCP	Beliebige Art	ISCSI-Zugriff über die iSCSI-Daten-LIF
1015 Inbound_4045-4046_tcp	4045-4046 TCP	Beliebige Art	NFS Lock Daemon und Network Status Monitor
1016 Inbound_4045-4046_udp	4045-4046 UDP	Beliebige Art	NFS Lock Daemon und Network Status Monitor
1017 eingehend_10000	10000 TCP	Beliebige Art	Backup mit NDMP
1018 eingehend_11104-11105	11104-11105 TCP	Beliebige Art	SnapMirror Datenübertragung
3000 Inbound_Deny_all_tcp	Alle TCP-Ports	Beliebige Art	Blockieren Sie den gesamten anderen TCP-eingehenden Datenverkehr
3001 Inbound_Deny_all_udp	Alle Ports UDP	Beliebige Art	Alle anderen UDP-eingehenden Datenverkehr blockieren
65000 AllowVnetInBound	Alle Ports und Protokolle	VirtualNetwork zu VirtualNetwork	Eingehender Verkehr aus dem vnet

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
65001 AllowAzureLoad BalancerInBound	Alle Ports und Protokolle	AzureLoadBalancer zu jedem	Datenverkehr vom Azure Standard Load Balancer
65500 DenyAllInBound	Alle Ports und Protokolle	Beliebige Art	Alle anderen eingehenden Datenverkehr blockieren

Eingehende Regeln für HA-Systeme

Die unten aufgeführten Regeln erlauben den Datenverkehr, es sei denn, die Beschreibung stellt fest, dass bestimmte eingehende Daten blockiert werden.

HA-Systeme weisen weniger eingehende Regeln als Systeme mit einzelnen Nodes auf, da eingehender Datenverkehr durch den Azure Standard Load Balancer geleitet wird. Aus diesem Grund sollte der Verkehr aus dem Load Balancer geöffnet sein, wie in der Regel "AllowAzureLoadBalancerInBound" gezeigt.

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
100 eingehend_443	443 beliebiges Protokoll	Beliebige Art	HTTPS-Zugriff auf die System Manager-Webkonsole unter Verwendung der IP-Adresse der Cluster-Management-LIF
101 Inbound_111_tcp	111 beliebiges Protokoll	Beliebige Art	Remote-Prozeduraufruf für NFS
102 Inbound_2049_tcp	2049 beliebiges Protokoll	Beliebige Art	NFS-Server-Daemon
111 Inbound_SSH	22 beliebiges Protokoll	Beliebige Art	SSH-Zugriff auf die IP-Adresse der Cluster Management LIF oder einer Node Management LIF
121 eingehend_53	53 beliebiges Protokoll	Beliebige Art	DNS und CIFS
65000 AllowVnetInBound	Alle Ports und Protokolle	VirtualNetwork zu VirtualNetwork	Eingehender Verkehr aus dem vnet
65001 AllowAzureLoad BalancerInBound	Alle Ports und Protokolle	AzureLoadBalancer zu jedem	Datenverkehr vom Azure Standard Load Balancer
65500 DenyAllInBound	Alle Ports und Protokolle	Beliebige Art	Alle anderen eingehenden Datenverkehr blockieren

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP enthält die folgenden ausgehenden Regeln.

Port	Protokoll	Zweck
Alle	Alle TCP	Gesamter abgehender Datenverkehr
Alle	Alle UDP-Protokolle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie strenge Regeln für ausgehenden Datenverkehr benötigen, können Sie mit den folgenden Informationen nur die Ports öffnen, die für die ausgehende Kommunikation durch Cloud Volumes ONTAP erforderlich sind.

Die Quelle ist die Schnittstelle (IP-Adresse) auf dem Cloud Volumes ONTAP System.

Service	Port	Protokoll	Quelle	Ziel	Zweck
Active Directory	88	TCP	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	137	UDP	Node Management-LIF	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	138	UDP	Node Management-LIF	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	139	TCP	Node Management-LIF	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	389	TCP UND UDP	Node Management-LIF	Active Directory-Gesamtstruktur	LDAP
	445	TCP	Node Management-LIF	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	464	TCP	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	464	UDP	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	749	TCP	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	88	TCP	Daten-LIF (NFS, CIFS, iSCSI)	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	137	UDP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	138	UDP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	139	TCP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	389	TCP UND UDP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	LDAP
	445	TCP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	464	TCP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	464	UDP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	749	TCP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V - Passwort ändern und festlegen (RPCSEC_GSS)
DHCP	68	UDP	Node Management-LIF	DHCP	DHCP-Client für die erstmalige Einrichtung

Service	Port	Protokoll	Quelle	Ziel	Zweck
DHCPS	67	UDP	Node Management-LIF	DHCP	DHCP-Server
DNS	53	UDP	Node Management LIF und Daten LIF (NFS, CIFS)	DNS	DNS
NDMP	18600-18699	TCP	Node Management-LIF	Zielserver	NDMP-Kopie
SMTP	25	TCP	Node Management-LIF	Mailserver	SMTP-Warnungen können für AutoSupport verwendet werden
SNMP	161	TCP	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	161	UDP	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	162	TCP	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	162	UDP	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
SnapMirror	11104	TCP	Intercluster-LIF	ONTAP Intercluster-LIFs	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
	11105	TCP	Intercluster-LIF	ONTAP Intercluster-LIFs	SnapMirror Datenübertragung
Syslog	514	UDP	Node Management-LIF	Syslog-Server	Syslog-Weiterleitungsmeldungen

Sicherheitsgruppenregeln für den Konnektor

Die Sicherheitsgruppe für den Konnektor erfordert sowohl ein- als auch ausgehende Regeln.

Regeln für eingehende Anrufe

Die Quelle für eingehende Regeln in der vordefinierten Sicherheitsgruppe ist 0.0.0.0/0.

Port	Protokoll	Zweck
22	SSH	Bietet SSH-Zugriff auf den Connector-Host
80	HTTP	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
443	HTTPS	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Konnektor öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Connector enthält die folgenden ausgehenden Regeln.

Port	Protokoll	Zweck
Alle	Alle TCP	Gesamter abgehender Datenverkehr
Alle	Alle UDP-Protokolle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.

Die Quell-IP-Adresse ist der Connector-Host.

Service	Port	Protokoll	Ziel	Zweck
Active Directory	88	TCP	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	139	TCP	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	389	TCP	Active Directory-Gesamtstruktur	LDAP
	445	TCP	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	464	TCP	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	749	TCP	Active Directory-Gesamtstruktur	Active Directory Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	137	UDP	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	138	UDP	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	464	UDP	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
API-Aufrufe und AutoSupport	443	HTTPS	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe an AWS und ONTAP und Senden von AutoSupport Nachrichten an NetApp
API-Aufrufe	3000	TCP	ONTAP Cluster Management LIF	API-Aufrufe für ONTAP
DNS	53	UDP	DNS	Wird für die DNS-Auflösung durch Cloud Manager verwendet

Starten von Cloud Volumes ONTAP in Azure

Sie können ein Single-Node-System oder ein HA-Paar in Azure starten, indem Sie eine Cloud Volumes ONTAP-Arbeitsumgebung in Cloud Manager erstellen.

Bevor Sie beginnen

- Sie sollten ein haben "Anschluss, der Ihrem Arbeitsbereich zugeordnet ist".

Sie müssen ein Kontoadministrator sein, um einen Konnektor zu erstellen. Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, fordert Cloud Manager Sie auf, einen Connector zu erstellen, wenn Sie noch keinen haben.

- "Sie sollten darauf vorbereitet sein, den Konnektor jederzeit in Betrieb zu nehmen".
- Sie sollten eine Konfiguration auswählen und Azure Netzwerkinformationen von Ihrem Administrator erhalten haben. Weitere Informationen finden Sie unter "Planung Ihrer Cloud Volumes ONTAP Konfiguration".
- Für die Implementierung eines BYOL-Systems benötigen Sie für jeden Node die 20-stellige Seriennummer (Lizenzschlüssel).

Über diese Aufgabe

Wenn Cloud Manager ein Cloud Volumes ONTAP-System in Azure erstellt, werden mehrere Azure-Objekte wie eine Ressourcengruppe, Netzwerkschnittstellen und Storage-Konten erstellt. Sie können eine Zusammenfassung der Ressourcen am Ende des Assistenten überprüfen.

Risiko von Datenverlusten

Aufgrund des Risikos eines Datenverlusts wird die Bereitstellung von Cloud Volumes ONTAP in einer vorhandenen, gemeinsam genutzten Ressourcengruppe nicht empfohlen. Das Rollback ist derzeit standardmäßig deaktiviert, wenn die API zur Bereitstellung in einer vorhandenen Ressourcengruppe verwendet wird. Durch Löschen von Cloud Volumes ONTAP werden möglicherweise weitere Ressourcen aus dieser freigegebenen Gruppe gelöscht.

Als Best Practice empfiehlt es sich, eine neue, dedizierte Ressourcengruppe für Cloud Volumes ONTAP zu verwenden. Dies ist die Standard- und einzige empfohlene Option, wenn Sie Cloud Volumes ONTAP in Azure über Cloud Manager implementieren.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.
2. **Wählen Sie einen Standort**: Wählen Sie **Microsoft Azure** und **Cloud Volumes ONTAP Single Node** oder **Cloud Volumes ONTAP High Availability**.
3. **Details und Anmeldeinformationen**: Optional können Sie die Azure-Anmeldeinformationen und das Abonnement ändern, einen Cluster-Namen und einen Ressourcengruppennamen angeben, bei Bedarf Tags hinzufügen und dann Anmeldeinformationen angeben.

   In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Name der Arbeitsumgebung	Cloud Manager verwendet den Namen der Arbeitsumgebung, um sowohl das Cloud Volumes ONTAP System als auch die virtuelle Azure Maschine zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.

Feld	Beschreibung
Name der Ressourcengruppe	Behalten Sie den Standardnamen für die neue Ressourcengruppe bei, oder deaktivieren Sie **Standard verwenden** und geben Sie Ihren eigenen Namen für die neue Ressourcengruppe ein. Als Best Practice empfiehlt es sich, eine neue, dedizierte Ressourcengruppe für Cloud Volumes ONTAP zu verwenden. Es ist zwar möglich, Cloud Volumes ONTAP in einer vorhandenen, gemeinsam genutzten Ressourcengruppe mit Hilfe der API zu implementieren, es wird jedoch aufgrund des Risikos von Datenverlust nicht empfohlen. Weitere Informationen finden Sie in der oben stehenden Warnung.
Tags	Tags sind Metadaten für Ihre Azure Ressourcen. Wenn Sie in diesem Feld Tags eingeben, werden sie von Cloud Manager der Ressourcengruppe hinzugefügt, die dem Cloud Volumes ONTAP System zugeordnet ist. Sie können bis zu vier Tags aus der Benutzeroberfläche hinzufügen, wenn Sie eine Arbeitsumgebung erstellen. Nach der Erstellung können Sie weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen einer Arbeitsumgebung nicht auf vier Tags beschränkt. Informationen zu Tags finden Sie unter "Microsoft Azure-Dokumentation: Verwenden von Tags zur Organisation Ihrer Azure-Ressourcen".
Benutzername und Passwort	Dies sind die Anmeldedaten für das Cloud Volumes ONTAP Cluster-Administratorkonto. Sie können diese Anmeldedaten verwenden, um über OnCommand System Manager oder seine CLI eine Verbindung zu Cloud Volumes ONTAP herzustellen.
Anmeldeinformationen bearbeiten	Sie können verschiedene Azure Zugangsdaten und ein anderes Azure Abonnement für dieses Cloud Volumes ONTAP System wählen. Sie müssen ein Azure Marketplace Abonnement mit dem ausgewählten Azure Abonnement verknüpfen, um ein Pay-as-you-go Cloud Volumes ONTAP System zu implementieren. "Hier erfahren Sie, wie Sie Anmeldedaten hinzufügen".

Im folgenden Video wird gezeigt, wie Sie ein Marketplace-Abonnement zu einem Azure-Abonnement verknüpfen:

► https://docs.netapp.com/de-de/occm38//media/video_subscribing_azure.mp4 *(video)*

4. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie nicht mit Cloud Volumes ONTAP verwenden möchten.
   - "Erfahren Sie mehr über Cloud Compliance".
   - "Weitere Informationen zu Backup in der Cloud".
5. **Standort & Konnektivität**: Wählen Sie einen Standort und eine Sicherheitsgruppe aus und aktivieren Sie das Kontrollkästchen, um die Netzwerkverbindung zwischen Cloud Manager und dem Zielspeicherort zu bestätigen.
6. **Lizenz- und Support-Site-Konto**: Geben Sie an, ob Sie Pay-as-you-go oder BYOL verwenden möchten, und legen Sie dann ein NetApp Support Site Konto fest.

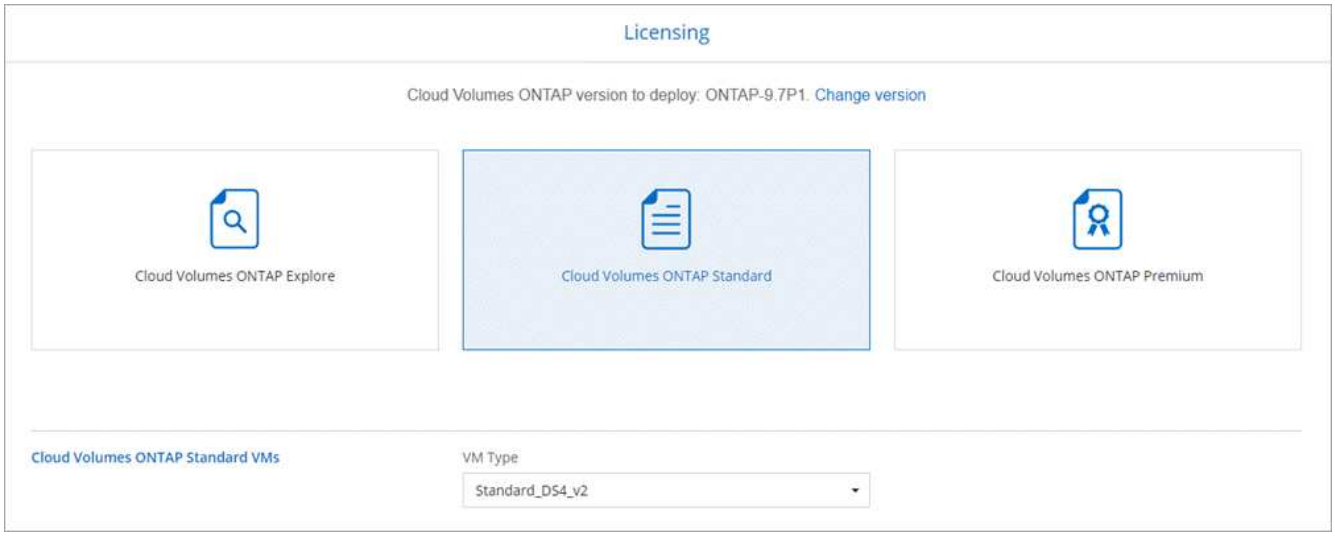
   Informationen zur Funktionsweise von Lizenzen finden Sie unter "Lizenzierung".

   Ein NetApp Support Site Konto ist optional für „Pay-as-you-go“-Systeme erhältlich, wird aber für BYOL-Systeme benötigt. "Erfahren Sie, wie Sie Konten der NetApp Support Site hinzufügen".

7. **Vorkonfigurierte Pakete**: Ein Paket zur schnellen Bereitstellung eines Cloud Volumes ONTAP-Systems einrichten oder auf **eigene Konfiguration erstellen** klicken.

Wenn Sie eines der Pakete auswählen, müssen Sie nur ein Volume angeben und dann die Konfiguration prüfen und genehmigen.

8. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP-Version nach Bedarf, wählen Sie eine Lizenz und wählen Sie einen virtuellen Maschinentyp.



Wenn sich Ihre Anforderungen nach dem Start des Systems ändern, können Sie die Lizenz oder den Typ der virtuellen Maschine später ändern.

> Wenn für die ausgewählte Version ein neuer Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert Cloud Manager das System beim Erstellen der Arbeitsumgebung auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.6 RC1 und 9.6 GA auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.6 bis 9.7.

9. **Vom Azure Marketplace abonnieren**: Folgen Sie den Schritten, wenn Cloud Manager programmatische Bereitstellungen von Cloud Volumes ONTAP nicht aktivieren könnte.
10. **Zugrunde liegende Storage-Ressourcen**: Wählen Sie die Einstellungen für das anfängliche Aggregat: Einen Festplattentyp, eine Größe für jede Festplatte und ob Daten-Tiering zu Blob-Storage aktiviert werden soll.

    Beachten Sie Folgendes:

    - Der Festplattentyp ist für das anfängliche Volume. Sie können einen anderen Festplattentyp für nachfolgende Volumes auswählen.
    - Die Festplattengröße gilt für alle Festplatten im ursprünglichen Aggregat und für alle zusätzlichen Aggregate, die Cloud Manager erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuweisungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

      Hilfe bei der Auswahl von Festplattentyp und -Größe finden Sie unter "Dimensionierung Ihres Systems in Azure".

    - Sie können eine bestimmte Volume-Tiering-Richtlinie auswählen, wenn Sie ein Volume erstellen oder bearbeiten.
    - Wenn Sie das Daten-Tiering deaktivieren, können Sie es bei nachfolgenden Aggregaten aktivieren.

"Weitere Informationen zum Daten-Tiering".

11. **Schreibgeschwindigkeit & WURM** (nur Systeme mit einem Knoten): Wählen Sie **normale** oder **hohe** Schreibgeschwindigkeit und aktivieren Sie ggf. den WORM-Speicher (Write Once, Read Many).

    Auswahl einer Schreibgeschwindigkeit wird nur bei Single-Node-Systemen unterstützt.

    "Erfahren Sie mehr über Schreibgeschwindigkeit".

    WORM kann nicht aktiviert werden, wenn Daten-Tiering aktiviert wurde.

    "Erfahren Sie mehr über WORM Storage".

12. **Secure Communication to Storage & WORM** (nur HA): Wählen Sie, ob eine HTTPS-Verbindung zu Azure-Speicherkonten aktiviert und ggf. WORM-Speicher (Write Once, Read Many) aktiviert werden soll.

    Die HTTPS-Verbindung besteht aus einem Cloud Volumes ONTAP 9.7 HA-Paar zu Azure Storage-Konten. 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.

    "Erfahren Sie mehr über WORM Storage".

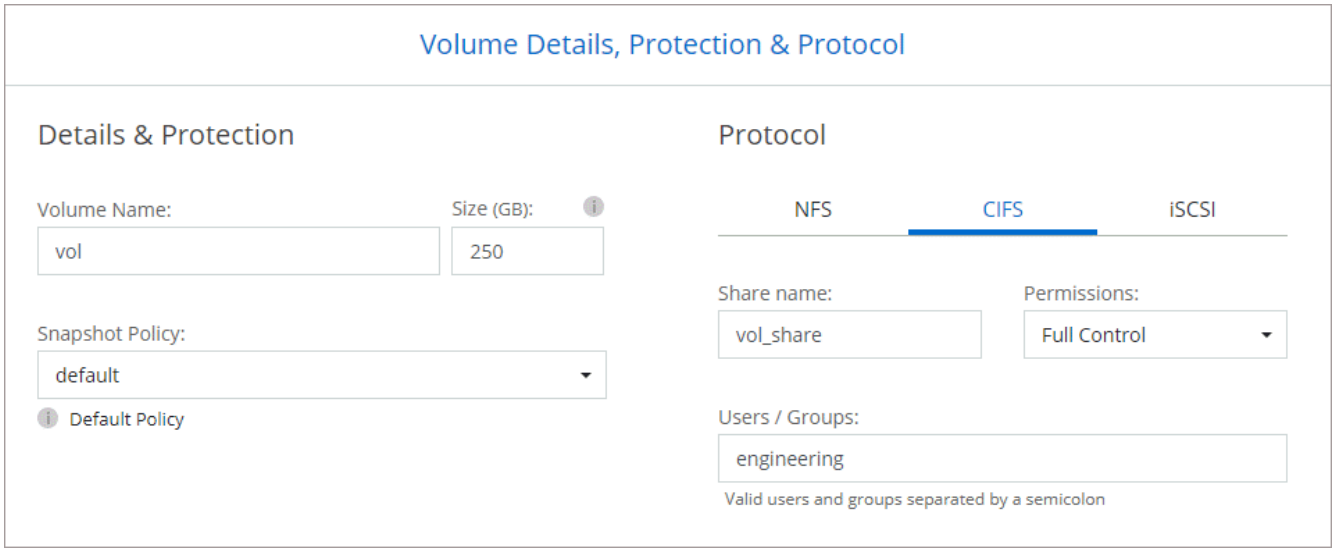
13. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

    Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren, wodurch Sie ein Volume erstellen können, das größer ist als der derzeit verfügbare physische Storage.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt Cloud Manager einen Wert ein, der Zugriff auf alle Instanzen im Subnetz ermöglicht.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch Zugriffssteuerungslisten oder ACLs genannt). Sie können lokale oder domänenbasierte Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Domain-Windows-Benutzernamen angeben, müssen Sie die Domäne des Benutzers mit dem Format Domain\Benutzername einschließen.
Snapshot-Richtlinie	Eine Snapshot Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot Kopien an. Bei einer NetApp Snapshot Kopie handelt es sich um ein zeitpunktgenaues Filesystem Image, das keine Performance-Einbußen aufweist und minimalen Storage erfordert. Sie können die Standardrichtlinie oder keine auswählen. Sie können keine für transiente Daten auswählen, z. B. tempdb für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume: Entweder NFSv3 oder NFSv4.

Feld	Beschreibung
Initiatorgruppe und IQN (nur für iSCSI)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt Cloud Manager automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Nachdem Sie das Volume erstellt haben, "Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen".

Die folgende Abbildung zeigt die für das CIFS-Protokoll ausgefüllte Volume-Seite:



14. **CIFS Setup**: Wenn Sie das CIFS-Protokoll wählen, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.

Feld	Beschreibung
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. Um Azure AD-Domänendienste als AD-Server für Cloud Volumes ONTAP zu konfigurieren, müssen Sie in diesem Feld **OU=AADDC-Computer** oder **OU=AADDC-Benutzer** eingeben.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure-Dokumentation: Erstellen Sie eine Organisationseinheit (Organisationseinheit, OU) in einer von Azure AD-Domänendiensten gemanagten Domäne"^]
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden** aus, um einen NTP-Server mit Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Siehe "Cloud Manager API-Entwicklerleitfaden" Entsprechende Details.

15. **Nutzungsprofil, Festplattentyp und Tiering-Richtlinie**: Wählen Sie aus, ob Sie Funktionen für die Storage-Effizienz aktivieren und gegebenenfalls die Volume Tiering-Richtlinie ändern möchten.

    Weitere Informationen finden Sie unter "Allgemeines zu Volume-Nutzungsprofilen" Und "Data Tiering - Übersicht".

16. **Überprüfen & Genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um Details zum Support und zu den von Cloud Manager erworbenen Azure Ressourcen anzuzeigen.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie Auf **Go**.

Ergebnis

Cloud Manager implementiert das Cloud Volumes ONTAP System. Sie können den Fortschritt in der Timeline verfolgen.

Wenn Sie Probleme bei der Implementierung des Cloud Volumes ONTAP Systems haben, lesen Sie die Fehlermeldung. Sie können auch die Arbeitsumgebung auswählen und auf **Umgebung neu erstellen** klicken.

Weitere Hilfe finden Sie unter "NetApp Cloud Volumes ONTAP Support".

Nachdem Sie fertig sind

- Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner, und überprüfen Sie, ob diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.
- Wenn Sie Kontingente auf Volumes anwenden möchten, verwenden Sie System Manager oder die CLI.

  Mithilfe von Quotas können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder qtree verwendeten Dateien einschränken oder nachverfolgen.

Erste Schritte in GCP

Erste Schritte mit Cloud Volumes ONTAP für Google Cloud

Erste Schritte mit Cloud Volumes ONTAP für GCP

Einen Konnektor erstellen

Wenn Sie keine haben "Stecker" Dennoch muss ein Kontoadministrator einen erstellen. "Connector in GCP erstellen".

Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von Cloud Manager aufgefordert, einen Connector bereitzustellen, wenn Sie noch keinen haben.

Planen Sie Ihre Konfiguration

Cloud Manager bietet vorkonfigurierte Pakete, die Ihren Workload-Anforderungen entsprechen, oder Sie können eine eigene Konfiguration erstellen. Wenn Sie sich für eine eigene Konfiguration entscheiden, sollten Sie sich mit den verfügbaren Optionen vertraut machen. "Weitere Informationen .".

Richten Sie Ihr Netzwerk ein

1. Stellen Sie sicher, dass Ihre VPC und Subnetze die Konnektivität zwischen dem Connector und Cloud Volumes ONTAP unterstützen.
2. Aktivieren Sie den Outbound-Internetzugang über die Ziel-VPC, damit der Connector und der Cloud Volumes ONTAP mehrere Endpunkte kontaktieren können.

   Dieser Schritt ist wichtig, da der Connector Cloud Volumes ONTAP nicht ohne Outbound-Internetzugang verwalten kann. Wenn Sie die ausgehende Verbindung begrenzen müssen, lesen Sie die Liste der Endpunkte für "Anschluss und Cloud Volumes ONTAP".

"Erfahren Sie mehr über Netzwerkanforderungen".

GCP für Daten-Tiering einrichten

Für das Tiering von kalten Daten von Cloud Volumes ONTAP auf kostengünstigen Objekt-Storage (ein Google Cloud-Storage-Bucket) müssen zwei Anforderungen erfüllt werden:

1. "Konfigurieren Sie das Cloud Volumes ONTAP-Subnetz für privaten Google-Zugriff".
2. "Service-Konto für Daten-Tiering einrichten":
   - Weisen Sie dem Tiering-Service-Konto die vordefinierte Rolle „*Storage Admin*“ zu.
   - Fügen Sie das Connector-Dienstkonto als *Service-Konto-Benutzer* zum Tiering-Dienstkonto hinzu.

     Sie können die Benutzerrolle angeben "In Schritt 3 des Assistenten, wenn Sie das Tiering Service-

Konto erstellen", Oder "Geben Sie die Rolle nach der Erstellung des Dienstkontos ein".

Sie müssen das Tiering Service-Konto später auswählen, wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen.

Wenn Sie kein Daten-Tiering aktivieren und bei der Erstellung des Cloud Volumes ONTAP-Systems ein Service-Konto auswählen, müssen Sie das System deaktivieren und das Service-Konto über die GCP-Konsole zu Cloud Volumes ONTAP hinzufügen.

Aktivieren Sie Google Cloud-APIs

"Aktivieren Sie die folgenden Google Cloud APIs in Ihrem Projekt". Diese APIs sind für die Implementierung des Connectors und der Cloud Volumes ONTAP erforderlich.

- Cloud Deployment Manager V2-API
- Cloud-ProtokollierungsAPI
- Cloud Resource Manager API
- Compute Engine-API
- IAM-API (Identitäts- und Zugriffsmanagement

Starten Sie Cloud Volumes ONTAP mit Cloud Manager

Klicken Sie auf **Arbeitsumgebung hinzufügen**, wählen Sie den Systemtyp aus, den Sie bereitstellen möchten, und führen Sie die Schritte im Assistenten aus. "Lesen Sie Schritt-für-Schritt-Anleitungen".

Weiterführende Links

- "Bewertung"
- "Erstellen eines Connectors über Cloud Manager"
- "Installieren der Connector-Software auf einem Linux-Host"
- "Was Cloud Manager mit GCP-Berechtigungen macht"

Cloud Volumes ONTAP-Konfiguration in Google Cloud planen

Wenn Sie Cloud Volumes ONTAP in Google Cloud implementieren, können Sie entweder ein vorkonfiguriertes System wählen, das Ihren Workload-Anforderungen entspricht, oder Sie erstellen Ihre eigene Konfiguration. Wenn Sie sich für eine eigene Konfiguration entscheiden, sollten Sie sich mit den verfügbaren Optionen vertraut machen.

Auswahl eines Lizenztyps

Cloud Volumes ONTAP ist in zwei Preisoptionen erhältlich: Nutzungsbasiert und als BYOL-Modell (Bring-Your-Own-License). Für Pay-as-you-go können Sie zwischen drei Lizenzen wählen: Explore, Standard oder Premium. Jede Lizenz bietet verschiedene Kapazitäts- und Computing-Optionen.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP 9.7 in GCP"

Storage-Grenzen kennen

Die Rohkapazitätsgrenze für ein Cloud Volumes ONTAP System ist an die Lizenz gebunden. Zusätzliche Beschränkungen wirken sich auf die Größe von Aggregaten und Volumes aus. Sie sollten sich dieser Grenzen bei der Planung Ihrer Konfiguration bewusst sein.

"Storage-Grenzen für Cloud Volumes ONTAP 9.7 in GCP"

Dimensionierung Ihres Systems in GCP

Mit der Dimensionierung Ihres Cloud Volumes ONTAP Systems können Sie die Anforderungen an Performance und Kapazität erfüllen. Bei der Auswahl von Maschinentyp, Festplattentyp und Festplattengröße sind einige wichtige Punkte zu beachten:

Maschinentyp

Sehen Sie sich die unterstützten Maschinentypen im an "Versionshinweise zu Cloud Volumes ONTAP" Und dann lesen Sie die Details von Google zu jedem unterstützten Maschinentyp durch. Passen Sie Ihre Workload-Anforderungen an die Anzahl an vCPUs und Speicher für den Maschinentyp an. Beachten Sie, dass jeder CPU-Kern die Netzwerk-Performance steigert.

Weitere Informationen finden Sie im Folgenden:

- "Google Cloud-Dokumentation: N1 Standard-Maschinentypen"
- "Google Cloud Dokumentation: Performance"

GCP-Festplattentyp

Bei der Erstellung von Volumes für Cloud Volumes ONTAP müssen Sie den zugrunde liegenden Cloud-Storage auswählen, den Cloud Volumes ONTAP für eine Festplatte verwendet. Der Festplattentyp kann entweder *Zonal SSD Persistent Disks* oder *Zonal Standard Persistent Disks* sein.

Persistente SSD-Festplatten eignen sich ideal für Workloads, die eine hohe Anzahl von zufälligen IOPS erfordern, während Standard-persistente Festplatten wirtschaftlich sind und sequenzielle Lese-/Schreibvorgänge verarbeiten können. Weitere Informationen finden Sie unter "Google Cloud-Dokumentation: Zonal Persistent Disks (Standard und SSD)".

GCP-Festplattengröße

Sie müssen bei der Implementierung eines Cloud Volumes ONTAP Systems die ursprüngliche Festplattengröße auswählen. Danach können Sie mit Cloud Manager die Kapazität eines Systems für Sie verwalten. Wenn Sie jedoch die Aggregate selbst erstellen möchten, beachten Sie Folgendes:

- Alle Festplatten in einem Aggregat müssen dieselbe Größe haben.
- Ermitteln Sie den Speicherplatz, den Sie benötigen, während Sie gleichzeitig die Performance in Betracht ziehen.
- Die Performance persistenter Festplatten lässt sich automatisch mit der Festplattengröße und der Anzahl der für das System verfügbaren vCPUs skalieren.

  Weitere Informationen finden Sie im Folgenden:

  - "Google Cloud-Dokumentation: Zonal Persistent Disks (Standard und SSD)"
  - "Google Cloud-Dokumentation: Optimierung von Persistent Disk und lokaler SSD-Performance"

Informationarbeitsblatt für das GCP-Netzwerk

Bei der Implementierung von Cloud Volumes ONTAP in GCP müssen Details zu Ihrem virtuellen Netzwerk angegeben werden. Sie können ein Arbeitsblatt verwenden, um die Informationen von Ihrem Administrator zu sammeln.

GCP-Informationen	Ihr Wert
Region	
Zone	
VPC-Netzwerk	
Subnetz	
Firewallrichtlinie (bei Nutzung eigener Richtlinien)	

Auswählen einer Schreibgeschwindigkeit

Mit Cloud Manager können Sie eine Einstellung für die Schreibgeschwindigkeit für Cloud Volumes ONTAP Systeme mit einem Node wählen. Bevor Sie sich für eine Schreibgeschwindigkeit entscheiden, sollten Sie die Unterschiede zwischen den normalen und hohen Einstellungen sowie Risiken und Empfehlungen verstehen, wenn Sie eine hohe Schreibgeschwindigkeit verwenden.

Unterschied zwischen normaler Schreibgeschwindigkeit und hoher Schreibgeschwindigkeit

Wenn Sie sich für eine normale Schreibgeschwindigkeit entscheiden, werden die Daten direkt auf die Festplatte geschrieben, wodurch die Wahrscheinlichkeit eines Datenverlusts bei einem ungeplanten Systemausfall verringert wird.

Wenn Sie hohe Schreibgeschwindigkeit wählen, werden die Daten vor dem Schreiben auf die Festplatte im Speicher gepuffert, was eine schnellere Schreibleistung ermöglicht. Aufgrund dieses Cachings besteht die Gefahr eines Datenverlusts, wenn ein ungeplanter Systemausfall auftritt.

Die Datenmenge, die bei einem ungeplanten Systemausfall verloren gehen kann, entspricht der Spanne der letzten beiden Konsistenzpunkte. Ein Konsistenzpunkt ist das Schreiben gepufferter Daten auf die Festplatte. Ein Konsistenzpunkt tritt auf, wenn das Schreibprotokoll voll ist oder nach 10 Sekunden (je nachdem, was zuerst eintritt). Die Performance des AWS EBS-Volumes kann sich jedoch auf die Verarbeitungszeit des Konsistenzpunkts auswirken.

Wann wird hohe Schreibgeschwindigkeit verwendet

Hohe Schreibgeschwindigkeit ist eine gute Wahl, wenn für Ihre Workload eine schnelle Schreibleistung erforderlich ist und Sie das Risiko eines Datenverlusts bei einem ungeplanten Systemausfall überstehen können.

Empfehlungen bei hoher Schreibgeschwindigkeit

Wenn Sie die hohe Schreibgeschwindigkeit aktivieren, sollten Sie den Schreibschutz auf der Anwendungsebene sicherstellen.

Auswählen eines Volume-Nutzungsprofils

ONTAP umfasst mehrere Storage-Effizienzfunktionen, mit denen Sie die benötigte Storage-Gesamtmenge

reduzieren können. Wenn Sie ein Volume in Cloud Manager erstellen, können Sie ein Profil auswählen, das diese Funktionen aktiviert, oder ein Profil, das sie deaktiviert. Sie sollten mehr über diese Funktionen erfahren, um zu entscheiden, welches Profil Sie verwenden möchten.

NetApp Storage-Effizienzfunktionen bieten folgende Vorteile:

Thin Provisioning

Bietet Hosts oder Benutzern mehr logischen Storage als in Ihrem physischen Storage-Pool. Anstatt Storage vorab zuzuweisen, wird jedem Volume beim Schreiben von Daten dynamisch Speicherplatz zugewiesen.

Deduplizierung

Verbessert die Effizienz, indem identische Datenblöcke lokalisiert und durch Verweise auf einen einzelnen gemeinsam genutzten Block ersetzt werden. Durch diese Technik werden die Storage-Kapazitätsanforderungen reduziert, da redundante Datenblöcke im selben Volume eliminiert werden.

Komprimierung

Reduziert die physische Kapazität, die zum Speichern von Daten erforderlich ist, indem Daten in einem Volume auf primärem, sekundärem und Archiv-Storage komprimiert werden.

Netzwerkanforderungen für die Implementierung und das Management von Cloud Volumes ONTAP in GCP

Richten Sie das Netzwerk Ihrer Google Cloud-Plattform ein, damit Cloud Volumes ONTAP-Systeme ordnungsgemäß funktionieren können. Dazu gehört auch die Vernetzung von Connector und Cloud Volumes ONTAP.

Anforderungen für Cloud Volumes ONTAP

Die folgenden Anforderungen müssen in GCP erfüllt sein.

Virtuelle Private Cloud

Cloud Volumes ONTAP und der Connector werden in einer gemeinsamen Google Cloud VPC und auch in nicht-freigegebenen VPCs unterstützt.

Mit einer gemeinsam genutzten VPC können Sie virtuelle Netzwerke über mehrere Projekte hinweg konfigurieren und zentral managen. Sie können freigegebene VPC-Netzwerke im_Host-Projekt_ einrichten und die Instanzen von Connector und Cloud Volumes ONTAP Virtual Machine in einem *Service-Projekt* implementieren. "Google Cloud-Dokumentation: Gemeinsame VPC-Übersicht".

Die einzige Anforderung bei der Verwendung einer gemeinsamen VPC ist die "Benutzerrolle für das Netzwerk wird berechnet" An das Konnektor-Dienstkonto. Cloud Manager benötigt diese Berechtigungen, um Firewalls, VPC und Subnetze im Host-Projekt abzufragen.

Outbound-Internetzugang für Cloud Volumes ONTAP

Cloud Volumes ONTAP erfordert ausgehenden Internetzugang, um Nachrichten an NetApp AutoSupport zu senden, der proaktiv den Zustand Ihres Storage überwacht.

Routing- und Firewall-Richtlinien müssen HTTP-/HTTPS-Datenverkehr an die folgenden Endpunkte ermöglichen, damit Cloud Volumes ONTAP AutoSupport-Meldungen senden kann:

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

"Erfahren Sie, wie AutoSupport konfiguriert wird".

Anzahl der IP-Adressen

Cloud Manager weist Cloud Volumes ONTAP in GCP 5 IP-Adressen zu.

Beachten Sie, dass Cloud Manager keine SVM-Management-LIF für Cloud Volumes ONTAP in GCP erstellt.

Ein LIF ist eine IP-Adresse, die einem physischen Port zugewiesen ist. Für Managementtools wie SnapCenter ist eine SVM-Management-LIF erforderlich.

Firewall-Regeln

Sie müssen keine Firewall-Regeln erstellen, weil Cloud Manager das für Sie macht. Wenn Sie Ihre eigene verwenden müssen, beachten Sie die unten aufgeführten Firewall-Regeln.

Verbindung von Cloud Volumes ONTAP zu Google Cloud Storage für Daten-Tiering

Wenn „kalte“ Daten in einen Google Cloud Storage Bucket verschoben werden sollen, muss das Subnetz, in dem Cloud Volumes ONTAP residiert, für privaten Google Zugriff konfiguriert sein. Anweisungen finden Sie unter "Google Cloud-Dokumentation: Privaten Google Access konfigurieren".

Weitere Schritte zur Einrichtung von Daten-Tiering in Cloud Manager finden Sie unter "Tiering von kalten Daten auf kostengünstigen Objekt-Storage".

Verbindungen zu ONTAP Systemen in anderen Netzwerken

Zur Replizierung von Daten zwischen einem Cloud Volumes ONTAP System in GCP und ONTAP Systemen in anderen Netzwerken müssen Sie eine VPN-Verbindung zwischen der VPC und dem anderen Netzwerk herstellen, beispielsweise mit dem Unternehmensnetzwerk.

Anweisungen finden Sie unter "Google Cloud Dokumentation: Cloud VPN Übersicht".

Anforderungen an den Steckverbinder

Richten Sie Ihr Netzwerk ein, damit der Connector Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen kann. Der wichtigste Schritt besteht darin, ausgehenden Internetzugriff auf verschiedene Endpunkte zu gewährleisten.

Wenn Ihr Netzwerk für die gesamte Kommunikation mit dem Internet einen Proxyserver verwendet, können Sie den Proxyserver über die Seite Einstellungen angeben. Siehe "Konfigurieren des Connectors für die Verwendung eines Proxy-Servers".

Verbindung zu Zielnetzwerken

Für einen Connector ist eine Netzwerkverbindung zu den VPCs und VNets erforderlich, in denen Cloud Volumes ONTAP bereitgestellt werden soll.

Wenn Sie beispielsweise einen Connector in Ihrem Unternehmensnetzwerk installieren, müssen Sie eine VPN-Verbindung zur VPC oder vnet einrichten, in der Sie Cloud Volumes ONTAP starten.

Outbound-Internetzugang

Für den Connector ist ein abgehender Internetzugang erforderlich, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung zu managen. Ein Connector kontaktiert die folgenden Endpunkte beim Management von Ressourcen in GCP:

Endpunkte	Zweck
https://www.googleapis.com	Ermöglicht dem Connector den Kontakt zu Google APIs für die Bereitstellung und das Management von Cloud Volumes ONTAP in GCP.
https://api.services.cloud.netapp.com:443	API-Anfragen an NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://repo.cloud.support.netapp.com	Wird zum Herunterladen der Abhängigkeiten von Cloud Manager verwendet.
http://repo.mysql.com/	Zum Herunterladen von MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Ermöglicht dem Connector, auf Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images zuzugreifen und diese herunterzuladen.
https://cloudmanagerinfraprod.azurecr.io	Zugriff auf Software-Images von Container-Komponenten für eine Infrastruktur, die Docker ausführt und eine Lösung für die Service-Integration mit Cloud Manager bietet.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cloudmanager.cloud.netapp.com	Kommunikation mit dem Cloud Manager-Service, der Cloud Central-Konten einschließt
https://netapp-cloud-account.auth0.com	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
https://mysupport.netapp.com	Kommunikation mit NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Kommunikation mit NetApp bei Systemlizenzrechten und Support-Registrierung
https://ipa-signer.cloudmanager.netapp.com	Ermöglicht Cloud Manager die Generierung von Lizenzen (beispielsweise eine FlexCache Lizenz für Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Erforderlich, um Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster zu verbinden Mit den Endpunkten ist die Installation von NetApp Trident möglich.

Endpunkte	Zweck
Verschiedene Standorte von Drittanbietern, z. B.: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org An Standorten von Drittanbietern können Änderungen vorgenommen werden.	Während Upgrades lädt Cloud Manager die neuesten Pakete für Abhängigkeiten von Drittanbietern herunter.

Während Sie fast alle Aufgaben über die SaaS-Benutzeroberfläche ausführen sollten, steht auf dem Connector weiterhin eine lokale Benutzeroberfläche zur Verfügung. Die Maschine, auf der der Webbrowser ausgeführt wird, muss über Verbindungen zu den folgenden Endpunkten verfügen:

Endpunkte	Zweck
Der Connector-Host	Sie müssen die IP-Adresse des Hosts aus einem Webbrowser eingeben, um die Cloud Manager-Konsole zu laden. Je nach Ihrer Verbindung mit Ihrem Cloud-Provider können Sie die private IP oder eine dem Host zugewiesene öffentliche IP verwenden: • Eine private IP funktioniert, wenn Sie über ein VPN verfügen und direkten Zugriff auf Ihr virtuelles Netzwerk haben • Eine öffentliche IP funktioniert in jedem Netzwerkszenario In jedem Fall sollten Sie den Netzwerkzugriff sichern, indem Sie sicherstellen, dass die Sicherheitsgruppenregeln den Zugriff nur von autorisierten IPs oder Subnetzen ermöglichen.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Ihr Webbrowser stellt über NetApp Cloud Central eine Verbindung zu diesen Endpunkten her, um eine zentralisierte Benutzerauthentifizierung zu ermöglichen.
https://widget.intercom.io	Für Ihren Produkt-Chat, der Ihnen das Gespräch mit NetApp Cloud-Experten ermöglicht.

Firewall-Regeln für Cloud Volumes ONTAP

Cloud Manager erstellt die GCP-Firewall-Regeln und enthält die ein- und ausgehenden Regeln, die für den erfolgreichen Betrieb von Cloud Manager und Cloud Volumes ONTAP gelten. Sie können die Ports zu Testzwecken oder zur Verwendung eigener Sicherheitsgruppen verwenden.

Die Firewall-Regeln für Cloud Volumes ONTAP erfordern sowohl ein- als auch ausgehende Regeln.

Regeln für eingehende Anrufe

Die Quelle für eingehende Regeln in der vordefinierten Sicherheitsgruppe ist 0.0.0.0/0.

Protokoll	Port	Zweck
Alle ICMP	Alle	Pingen der Instanz
HTTP	80	HTTP-Zugriff auf die System Manager Webkonsole mit der IP-Adresse der Cluster-Management-LIF
HTTPS	443	HTTPS-Zugriff auf die System Manager-Webkonsole unter Verwendung der IP-Adresse der Cluster-Management-LIF
SSH	22	SSH-Zugriff auf die IP-Adresse der Cluster Management LIF oder einer Node Management LIF
TCP	111	Remote-Prozeduraufruf für NFS
TCP	139	NetBIOS-Servicesitzung für CIFS
TCP	161-162	Einfaches Netzwerkverwaltungsprotokoll
TCP	445	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
TCP	635	NFS-Mount
TCP	749	Kerberos
TCP	2049	NFS-Server-Daemon
TCP	3260	ISCSI-Zugriff über die iSCSI-Daten-LIF
TCP	4045	NFS-Sperr-Daemon
TCP	4046	Netzwerkstatusüberwachung für NFS
TCP	10.000	Backup mit NDMP
TCP	11104	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
TCP	11105	SnapMirror Datenübertragung über Cluster-interne LIFs
UDP	111	Remote-Prozeduraufruf für NFS
UDP	161-162	Einfaches Netzwerkverwaltungsprotokoll
UDP	635	NFS-Mount
UDP	2049	NFS-Server-Daemon
UDP	4045	NFS-Sperr-Daemon
UDP	4046	Netzwerkstatusüberwachung für NFS
UDP	4049	NFS rquotad-Protokoll

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle ICMP	Alle	Gesamter abgehender Datenverkehr
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie strenge Regeln für ausgehenden Datenverkehr benötigen, können Sie mit den folgenden Informationen nur die Ports öffnen, die für die ausgehende Kommunikation durch Cloud Volumes ONTAP erforderlich sind.

Die Quelle ist die Schnittstelle (IP-Adresse) auf dem Cloud Volumes ONTAP System.

Service	Protokoll	Port	Quelle	Ziel	Zweck
Active Directory	TCP	88	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Node Management-LIF	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Node Management-LIF	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	TCP	139	Node Management-LIF	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP UND UDP	389	Node Management-LIF	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Node Management-LIF	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	UDP	464	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	TCP	88	Daten-LIF (NFS, CIFS, iSCSI)	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	TCP	139	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP UND UDP	389	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	UDP	464	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V - Passwort ändern und festlegen (RPCSEC_GSS)

Service	Protokoll	Port	Quelle	Ziel	Zweck
Cluster	Gesamter Datenverkehr	Gesamter Datenverkehr	Alle LIFs auf einem Node	Alle LIFs auf dem anderen Node	Kommunikation zwischen Clustern (nur Cloud Volumes ONTAP HA)
	TCP	3000	Node Management-LIF	Ha Mediator	ZAPI-Aufrufe (nur Cloud Volumes ONTAP HA)
	ICMP	1	Node Management-LIF	Ha Mediator	Bleiben Sie am Leben (nur Cloud Volumes ONTAP HA)
DHCP	UDP	68	Node Management-LIF	DHCP	DHCP-Client für die erstmalige Einrichtung
DHCPS	UDP	67	Node Management-LIF	DHCP	DHCP-Server
DNS	UDP	53	Node Management LIF und Daten LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600-18699	Node Management-LIF	Zielserver	NDMP-Kopie
SMTP	TCP	25	Node Management-LIF	Mailserver	SMTP-Warnungen können für AutoSupport verwendet werden
SNMP	TCP	161	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	UDP	161	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	TCP	162	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	UDP	162	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
SnapMirror	TCP	11104	Intercluster-LIF	ONTAP Intercluster-LIFs	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
	TCP	11105	Intercluster-LIF	ONTAP Intercluster-LIFs	SnapMirror Datenübertragung
Syslog	UDP	514	Node Management-LIF	Syslog-Server	Syslog-Weiterleitungsmeldungen

Firewall-Regeln für den Connector

Die Firewall-Regeln für den Connector erfordern sowohl ein- als auch ausgehende Regeln.

Regeln für eingehende Anrufe

Die Quelle für eingehende Regeln in den vordefinierten Firewall-Regeln ist 0.0.0.0/0.

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche

Regeln für ausgehende Anrufe

Die vordefinierten Firewall-Regeln für den Connector öffnen den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierten Firewall-Regeln für den Connector enthalten die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.

Die Quell-IP-Adresse ist der Connector-Host.

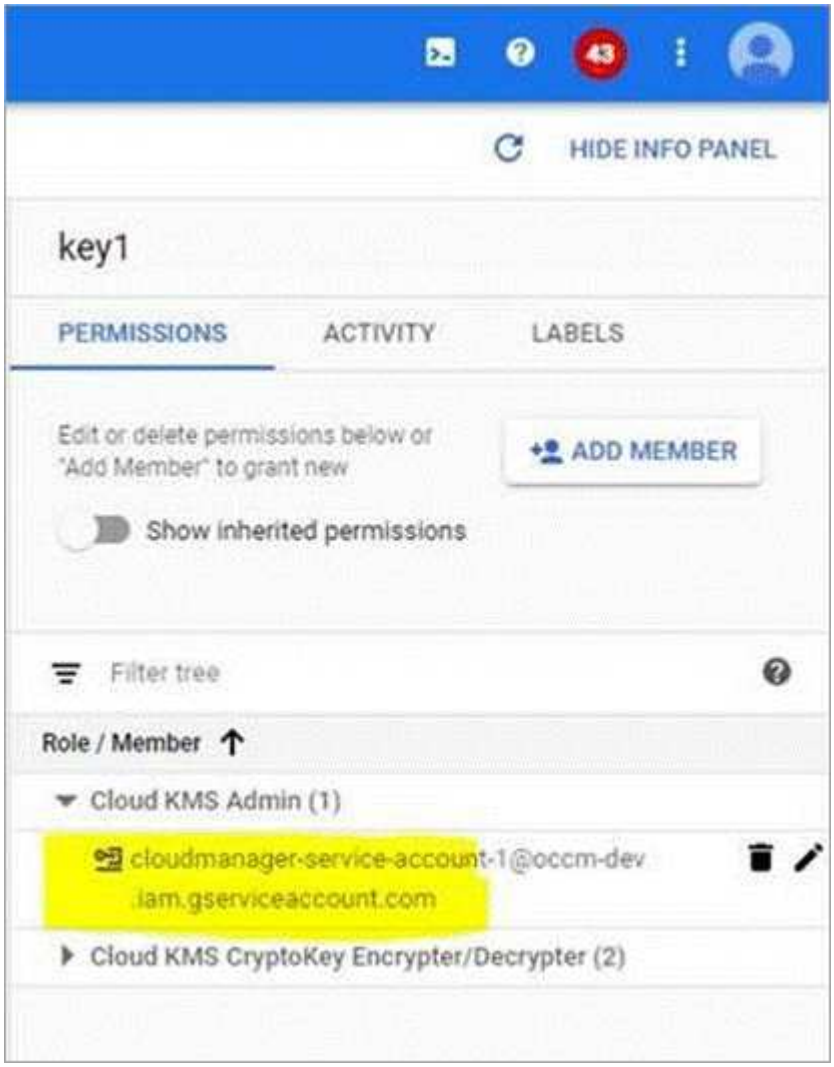
Service	Protokoll	Port	Ziel	Zweck
Active Directory	TCP	88	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	TCP	139	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP	389	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	TCP	749	Active Directory-Gesamtstruktur	Active Directory Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	UDP	137	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	UDP	464	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API ruft GCP und ONTAP ab und sendet AutoSupport Nachrichten an NetApp
API-Aufrufe	TCP	3000	ONTAP Cluster Management LIF	API-Aufrufe für ONTAP
DNS	UDP	53	DNS	Wird für die DNS-Auflösung durch Cloud Manager verwendet

Nutzung von vom Kunden gemanagten Schlüsseln mit Cloud Volumes ONTAP

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

Schritte

1. Geben Sie dem Connector-Dienstkonto die Berechtigung, den Verschlüsselungsschlüssel zu verwenden.



2. Rufen Sie die „id“ des Schlüssels auf, indem Sie den Befehl get für die API /gcp/vsa/Metadaten/gcp-Encryption-Keys aufrufen.
3. Verwenden Sie bei der Erstellung einer Arbeitsumgebung den Parameter „GcpEncryption“ in Verbindung mit Ihrer API-Anforderung.

   Beispiel

```
"gcpEncryptionParameters": {
    "key": "projects/tlv-support/locations/us-
east4/keyRings/Nikiskeys/cryptoKeys/generatedkey1"
  }
```

Siehe "API-Entwicklerhandbuch" Weitere Informationen zur Verwendung des Parameters „GcpEncryption“.

Einführung von Cloud Volumes ONTAP in GCP

In der GCP können Sie ein Single-Node-Cloud Volumes ONTAP-System einführen, indem Sie eine Arbeitsumgebung erstellen.

Was Sie benötigen

- Sie sollten ein haben "Anschluss, der Ihrem Arbeitsbereich zugeordnet ist".

> Sie müssen ein Kontoadministrator sein, um einen Konnektor zu erstellen. Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, fordert Cloud Manager Sie auf, einen Connector zu erstellen, wenn Sie noch keinen haben.

- "Sie sollten darauf vorbereitet sein, den Konnektor jederzeit in Betrieb zu nehmen".
- Sie sollten eine Konfiguration auswählen und GCP-Netzwerkinformationen von Ihrem Administrator erhalten haben. Weitere Informationen finden Sie unter "Planung Ihrer Cloud Volumes ONTAP Konfiguration".
- Für die Implementierung eines BYOL-Systems benötigen Sie für jeden Node die 20-stellige Seriennummer (Lizenzschlüssel).
- Die folgenden Google Cloud APIs sollten sein "In Ihrem Projekt aktiviert":
  - Cloud Deployment Manager V2-API
  - Cloud-ProtokollierungsAPI
  - Cloud Resource Manager API
  - Compute Engine-API
  - IAM-API (Identitäts- und Zugriffsmanagement

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.
2. **Wählen Sie einen Standort**: Wählen Sie **Google Cloud** und **Cloud Volumes ONTAP**.
3. **Details & Anmeldeinformationen**: Wählen Sie ein Projekt aus, geben Sie einen Clusternamen an, fügen Sie optional Labels hinzu und geben Sie dann Anmeldeinformationen an.

   In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Name der Arbeitsumgebung	Cloud Manager verwendet den Namen der Arbeitsumgebung, um sowohl das Cloud Volumes ONTAP System als auch die GCP VM-Instanz zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.

Feld	Beschreibung
Etiketten Hinzufügen	Beschriftungen sind Metadaten für Ihre GCP-Ressourcen. Cloud Manager fügt die Bezeichnungen dem Cloud Volumes ONTAP System und den GCP-Ressourcen hinzu, die dem System zugeordnet sind. Sie können bis zu vier Etiketten von der Benutzeroberfläche hinzufügen, wenn Sie eine Arbeitsumgebung erstellen, und dann können Sie weitere hinzufügen, nachdem sie erstellt wurde. Beachten Sie, dass Sie durch die API beim Erstellen einer Arbeitsumgebung nicht auf vier Labels beschränkt werden. Informationen zu Etiketten finden Sie unter "Google Cloud-Dokumentation: Ressourcen Zur Kennzeichnung".
Benutzername und Passwort	Dies sind die Anmeldedaten für das Cloud Volumes ONTAP Cluster-Administratorkonto. Sie können diese Anmeldedaten für die Verbindung mit Cloud Volumes ONTAP über System Manager oder dessen CLI verwenden.
Projekt Bearbeiten	Wählen Sie das Projekt aus, in dem Cloud Volumes ONTAP gespeichert werden soll. Das Standardprojekt ist das Projekt, in dem Cloud Manager residiert. Wenn in der Dropdown-Liste keine weiteren Projekte angezeigt werden, ist das Cloud Manager-Servicekonto noch nicht mit anderen Projekten verbunden. Rufen Sie die Google Cloud-Konsole auf, öffnen Sie den IAM-Service und wählen Sie das Projekt aus. Fügen Sie dem Projekt das Service-Konto mit der Rolle Cloud Manager hinzu. Sie müssen diesen Schritt für jedes Projekt wiederholen. Dies ist das Service-Konto, das Sie für Cloud Manager eingerichtet haben. "Wie in Schritt 2b auf dieser Seite beschrieben". Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen einem Abonnement zuzuordnen. Zum Erstellen eines nutzungsbasierten Cloud Volumes ONTAP Systems müssen Sie über GCP Marketplace ein GCP-Projekt für ein Cloud Volumes ONTAP Abonnement auswählen.

Das folgende Video zeigt, wie Sie ein Pay-as-you-go Marketplace Abonnement für Ihr GCP-Projekt verknüpfen:

► https://docs.netapp.com/de-de/occm38//media/video_subscribing_gcp.mp4 *(video)*

4. **Standort & Konnektivität**: Wählen Sie einen Speicherort, wählen Sie eine Firewall-Richtlinie und aktivieren Sie das Kontrollkästchen, um die Netzwerkverbindung zu Google Cloud Storage für Daten-Tiering zu bestätigen.

   Wenn „kalte“ Daten in einen Google Cloud Storage Bucket verschoben werden sollen, muss das Subnetz, in dem Cloud Volumes ONTAP residiert, für privaten Google Zugriff konfiguriert sein. Anweisungen finden Sie unter "Google Cloud Documentation: Configuring Private Google Access".

5. **Lizenz & Support Site Account**: Geben Sie an, ob Sie Pay-as-you-go oder BYOL verwenden möchten, und legen Sie dann ein NetApp Support Site Konto fest.

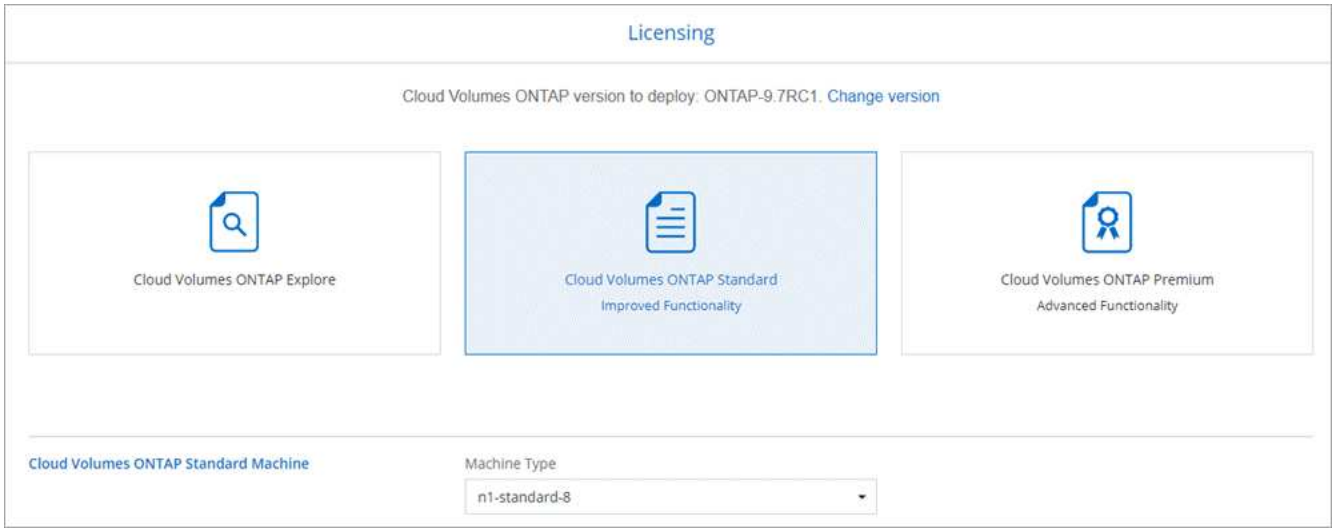
Informationen zur Funktionsweise von Lizenzen finden Sie unter "Lizenzierung".

Ein NetApp Support Site Konto ist optional für „Pay-as-you-go“-Systeme erhältlich, wird aber für BYOL-Systeme benötigt. "Erfahren Sie, wie Sie Konten der NetApp Support Site hinzufügen".

6. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete, um schnell ein Cloud Volumes ONTAP System bereitzustellen, oder klicken Sie auf **eigene Konfiguration erstellen**.

   Wenn Sie eines der Pakete auswählen, müssen Sie nur ein Volume angeben und dann die Konfiguration prüfen und genehmigen.

7. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP-Version nach Bedarf, wählen Sie eine Lizenz und wählen Sie einen virtuellen Maschinentyp.



   Wenn sich Ihre Anforderungen nach dem Start des Systems ändern, können Sie die Lizenz oder den Typ der virtuellen Maschine später ändern.

   Wenn für die ausgewählte Version ein neuer Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert Cloud Manager das System beim Erstellen der Arbeitsumgebung auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.6 RC1 und 9.6 GA auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.6 bis 9.7.

8. **Zugrunde liegende Speicherressourcen**: Wählen Sie die Einstellungen für das anfängliche Aggregat: Einen Datenträgertyp und die Größe für jede Platte.

   Der Festplattentyp ist für das anfängliche Volume. Sie können einen anderen Festplattentyp für nachfolgende Volumes auswählen.

   Die Festplattengröße gilt für alle Festplatten im ursprünglichen Aggregat und für alle zusätzlichen Aggregate, die Cloud Manager erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuweisungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

   Hilfe bei der Auswahl von Festplattentyp und -Größe finden Sie unter "Dimensionierung Ihres Systems in GCP".

9. **Schreibgeschwindigkeit & WURM**: Wählen Sie **Normal** oder **hohe** Schreibgeschwindigkeit, und

aktivieren Sie auf Wunsch den Schreib-Speicher, den WORM-Speicher.

Auswahl einer Schreibgeschwindigkeit wird nur bei Single-Node-Systemen unterstützt.

"Erfahren Sie mehr über Schreibgeschwindigkeit".

WORM kann nicht aktiviert werden, wenn Daten-Tiering aktiviert wurde.

"Erfahren Sie mehr über WORM Storage".

10. **Daten-Tiering in der Google Cloud Platform**: Wählen Sie, ob Daten-Tiering auf dem ursprünglichen Aggregat aktiviert werden soll, wählen Sie eine Storage-Klasse für die Tiered Daten, und wählen Sie dann entweder ein Service-Konto mit der vordefinierten Storage-Administratorrolle (erforderlich für Cloud Volumes ONTAP 9.7) oder wählen Sie ein GCP-Konto (erforderlich für Cloud Volumes ONTAP 9.6).

    Beachten Sie Folgendes:

    - Cloud Manager legt das Service-Konto auf der Cloud Volumes ONTAP Instanz fest. Dieses Servicekonto bietet Berechtigungen für Daten-Tiering zu einem Google Cloud Storage Bucket. Stellen Sie sicher, dass Sie das Cloud Manager-Servicekonto als Benutzer des Tiering-Dienstkontos hinzufügen, andernfalls können Sie es nicht aus Cloud Manager auswählen.
    - Hilfe zum Hinzufügen eines GCP-Kontos finden Sie unter "Einrichten und Hinzufügen von GCP-Konten für Daten-Tiering mit 9.6".
    - Sie können eine bestimmte Volume-Tiering-Richtlinie auswählen, wenn Sie ein Volume erstellen oder bearbeiten.
    - Wenn Sie das Daten-Tiering deaktivieren, können Sie es auf nachfolgenden Aggregaten aktivieren, jedoch müssen Sie das System deaktivieren und ein Service-Konto über die GCP-Konsole hinzufügen.

      "Weitere Informationen zum Daten-Tiering".

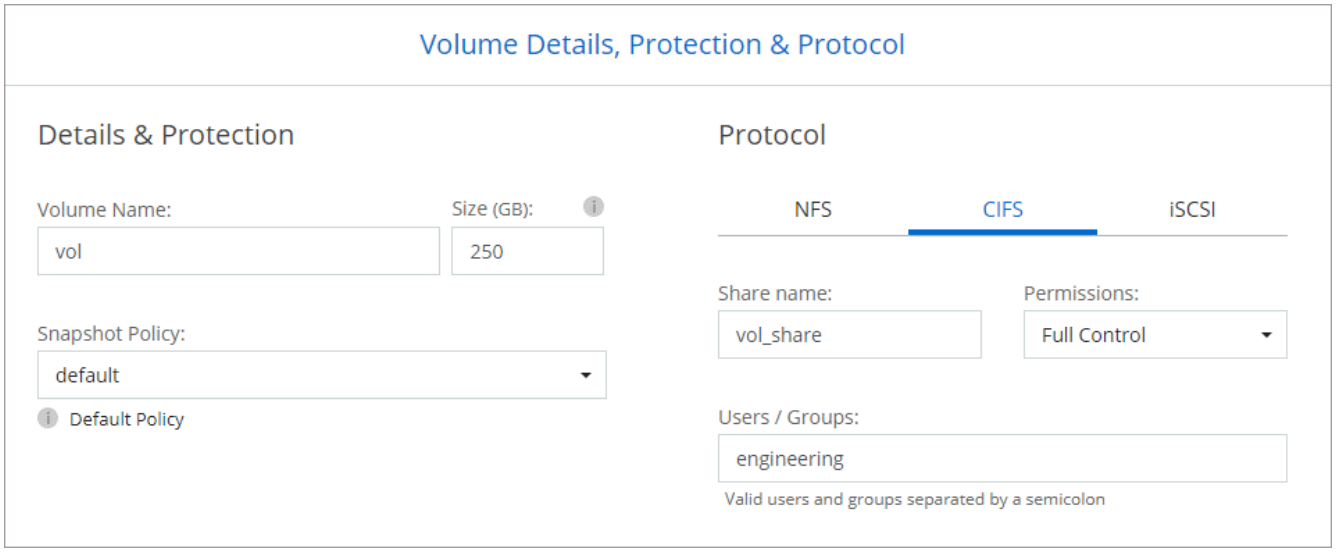
11. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

    Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren, wodurch Sie ein Volume erstellen können, das größer ist als der derzeit verfügbare physische Storage.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt Cloud Manager einen Wert ein, der Zugriff auf alle Instanzen im Subnetz ermöglicht.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch Zugriffssteuerungslisten oder ACLs genannt). Sie können lokale oder domänenbasierte Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Domain-Windows-Benutzernamen angeben, müssen Sie die Domäne des Benutzers mit dem Format Domain\Benutzername einschließen.

Feld	Beschreibung
Snapshot-Richtlinie	Eine Snapshot Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot Kopien an. Bei einer NetApp Snapshot Kopie handelt es sich um ein zeitpunktgenaues Filesystem Image, das keine Performance-Einbußen aufweist und minimalen Storage erfordert. Sie können die Standardrichtlinie oder keine auswählen. Sie können keine für transiente Daten auswählen, z. B. tempdb für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume: Entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt Cloud Manager automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Nachdem Sie das Volume erstellt haben, "Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen".

Die folgende Abbildung zeigt die für das CIFS-Protokoll ausgefüllte Volume-Seite:



12. **CIFS Setup**: Wenn Sie das CIFS-Protokoll wählen, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.

Feld	Beschreibung
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers.
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden** aus, um einen NTP-Server mit Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Siehe "Cloud Manager API-Entwicklerleitfaden" Entsprechende Details.

13. **Nutzungsprofil, Festplattentyp und Tiering-Richtlinie**: Wählen Sie aus, ob Sie Funktionen für die Storage-Effizienz aktivieren und gegebenenfalls die Volume Tiering-Richtlinie ändern möchten.

    Weitere Informationen finden Sie unter "Allgemeines zu Volume-Nutzungsprofilen" Und "Data Tiering - Übersicht".

14. **Überprüfen & Genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um weitere Informationen zum Support und zu den von Cloud Manager erworbenen GCP-Ressourcen zu erhalten.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie Auf **Go**.

Ergebnis

Cloud Manager implementiert das Cloud Volumes ONTAP System. Sie können den Fortschritt in der Timeline verfolgen.

Wenn Sie Probleme bei der Implementierung des Cloud Volumes ONTAP Systems haben, lesen Sie die Fehlermeldung. Sie können auch die Arbeitsumgebung auswählen und auf **Umgebung neu erstellen** klicken.

Weitere Hilfe finden Sie unter "NetApp Cloud Volumes ONTAP Support".

Nachdem Sie fertig sind

- Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner, und überprüfen Sie, ob diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.
- Wenn Sie Kontingente auf Volumes anwenden möchten, verwenden Sie System Manager oder die CLI.

  Mithilfe von Quotas können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder qtree verwendeten Dateien einschränken oder nachverfolgen.

Provisionierung und Management von Storage

Storage-Bereitstellung

Durch das Managen von Volumes und Aggregaten kann zusätzlicher Storage für die Cloud Volumes ONTAP Systeme vom Cloud Manager bereitgestellt werden.

> 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.

FlexVol Volumes werden erstellt

Wenn Sie nach dem Starten eines Cloud Volumes ONTAP Systems mehr Storage benötigen, können Sie aus Cloud Manager neue FlexVol Volumes für NFS, CIFS oder iSCSI erstellen.

Über diese Aufgabe

Wenn Sie ein iSCSI-Volume erstellen, erstellt Cloud Manager automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Nachdem Sie das Volume erstellt haben, Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen.

> Sie können weitere LUNs aus System Manager oder der CLI erstellen.

Bevor Sie beginnen

Wenn Sie CIFS in AWS verwenden möchten, müssen Sie DNS und Active Directory eingerichtet haben. Weitere Informationen finden Sie unter "Netzwerkanforderungen für Cloud Volumes ONTAP für AWS".

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf den Namen des Cloud Volumes ONTAP Systems, auf dem Sie FlexVol Volumes bereitstellen möchten.
2. Erstellen Sie ein neues Volume in einem beliebigen Aggregat oder in einem bestimmten Aggregat:

Aktion	Schritte
Erstellen Sie ein neues Volume, und lassen Sie Cloud Manager das enthaltende Aggregat auswählen	Klicken Sie Auf **Neues Volume Hinzufügen**.
Erstellen Sie ein neues Volume auf einem bestimmten Aggregat	a. Klicken Sie auf das Menüsymbol und dann auf **Erweitert > Erweiterte Zuweisung**. b. Klicken Sie auf das Menü für ein Aggregat. c. Klicken Sie auf **Create Volume**.

3. Geben Sie die Details für den neuen Volume ein, und klicken Sie dann auf **Weiter**.

   Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren, wodurch Sie ein Volume erstellen können, das größer ist als der derzeit verfügbare physische Storage.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt Cloud Manager einen Wert ein, der Zugriff auf alle Instanzen im Subnetz ermöglicht.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch Zugriffssteuerungslisten oder ACLs genannt). Sie können lokale oder domänenbasierte Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Domain-Windows-Benutzernamen angeben, müssen Sie die Domäne des Benutzers mit dem Format Domain\Benutzername einschließen.
Snapshot-Richtlinie	Eine Snapshot Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot Kopien an. Bei einer NetApp Snapshot Kopie handelt es sich um ein zeitpunktgenaues Filesystem Image, das keine Performance-Einbußen aufweist und minimalen Storage erfordert. Sie können die Standardrichtlinie oder keine auswählen. Sie können keine für transiente Daten auswählen, z. B. tempdb für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume: Entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt Cloud Manager automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Nachdem Sie das Volume erstellt haben, "Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen".

4. Wenn Sie das CIFS-Protokoll ausgewählt haben und der CIFS-Server noch nicht eingerichtet wurde, geben Sie im Dialogfeld Create a CIFS Server die Details für den Server an und klicken Sie dann auf **Save and Continue**:

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.

Feld	Beschreibung
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. • Um von AWS verwaltete Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, müssen Sie in diesem Feld **OU=Computers,OU=corp** eingeben. • Um Azure AD-Domänendienste als AD-Server für Cloud Volumes ONTAP zu konfigurieren, müssen Sie in diesem Feld **OU=AADDC-Computer** oder **OU=AADDC-Benutzer** eingeben.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure-Dokumentation: Erstellen Sie eine Organisationseinheit (Organisationseinheit, OU) in einer von Azure AD-Domänendiensten gemanagten Domäne"^]
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden** aus, um einen NTP-Server mit Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Siehe "Cloud Manager API-Entwicklerleitfaden" Entsprechende Details.

5. Wählen Sie auf der Seite Nutzungsprofil, Festplattentyp und Tiering-Richtlinie aus, ob Sie Funktionen der Storage-Effizienz aktivieren möchten, wählen Sie einen Festplattentyp aus und bearbeiten Sie die Tiering-Richtlinie falls erforderlich.

   Weitere Informationen finden Sie unter:

   - "Allgemeines zu Volume-Nutzungsprofilen"
   - "Dimensionierung Ihres Systems in AWS"
   - "Dimensionierung Ihres Systems in Azure"
   - "Data Tiering - Übersicht"

6. Klicken Sie Auf **Go**.

Ergebnis

Cloud Volumes ONTAP stellt das Volume bereit.

Nachdem Sie fertig sind

Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner, und überprüfen Sie, ob diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.

Wenn Sie Kontingente auf Volumes anwenden möchten, müssen Sie System Manager oder die CLI verwenden. Mithilfe von Quotas können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer

Gruppe oder qtree verwendeten Dateien einschränken oder nachverfolgen.

Erstellen von FlexVol Volumes auf dem zweiten Node in einer HA-Konfiguration

Standardmäßig erstellt Cloud Manager Volumes auf dem ersten Node in einer HA-Konfiguration. Wenn Sie eine Aktiv/Aktiv-Konfiguration benötigen, in der beide Nodes Daten für Clients bereitstellen, müssen Sie Aggregate und Volumes auf dem zweiten Node erstellen.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf den Namen der Cloud Volumes ONTAP Arbeitsumgebung, in der Sie Aggregate managen möchten.
2. Klicken Sie auf das Menü-Symbol und dann auf **Erweitert > Erweiterte Zuweisung**.
3. Klicken Sie auf **Aggregat hinzufügen** und erstellen Sie dann das Aggregat.
4. Wählen Sie für Home Node den zweiten Node im HA-Paar aus.
5. Nachdem Cloud Manager das Aggregat erstellt hat, wählen Sie es aus und klicken Sie dann auf **Create Volume**.
6. Geben Sie Details für den neuen Volume ein und klicken Sie dann auf **Erstellen**.

Nachdem Sie fertig sind

Sie können bei Bedarf weitere Volumes auf diesem Aggregat erstellen.

> Bei HA-Paaren, die in mehreren AWS Availability Zones implementiert sind, müssen Sie das Volume mithilfe der Floating-IP-Adresse des Node, auf dem sich das Volume befindet, an Clients mounten.

Aggregate werden erstellt

Sie können Aggregate selbst erstellen oder Cloud Manager bei der Erstellung von Volumes verwenden lassen. Der Vorteil der Erstellung von Aggregaten besteht darin, dass Sie die zugrunde liegende Festplattengröße wählen können, um das Aggregat an die Kapazität und Performance zu dimensionieren, die Sie benötigen.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf den Namen der Cloud Volumes ONTAP Instanz, auf der Sie Aggregate managen möchten.
2. Klicken Sie auf das Menüsymbol und dann auf **Erweitert > Erweiterte Zuweisung**.
3. Klicken Sie auf **Add Aggregate** und geben Sie dann Details für das Aggregat an.

   Hilfe zu Festplattentyp und Festplattengröße finden Sie unter "Planung Ihrer Konfiguration".

4. Klicken Sie auf **Go** und dann auf **Genehmigen und Kaufen**.

Verbinden einer LUN mit einem Host

Wenn Sie ein iSCSI-Volume erstellen, erstellt Cloud Manager automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Verwenden Sie nach dem Erstellen des Volumes den IQN, um von den Hosts eine Verbindung zur LUN herzustellen.

Beachten Sie Folgendes:

1. Das automatische Kapazitätsmanagement von Cloud Manager gilt nicht für LUNs. Wenn Cloud Manager eine LUN erstellt, wird die Autogrow Funktion deaktiviert.
2. Sie können weitere LUNs aus System Manager oder der CLI erstellen.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf die Arbeitsumgebung Cloud Volumes ONTAP, in der Sie Volumes managen möchten.
2. Wählen Sie ein Volume aus, und klicken Sie dann auf **Ziel-IQN**.
3. Klicken Sie auf **Kopieren**, um den IQN-Namen zu kopieren.
4. Richten Sie eine iSCSI-Verbindung vom Host zur LUN ein.
   - "ONTAP 9 iSCSI Express-Konfiguration für Red hat Enterprise Linux: Starten der iSCSI-Sitzungen mit dem Ziel"
   - "ONTAP 9 iSCSI Express-Konfiguration für Windows: Starten von iSCSI-Sitzungen mit dem Ziel"

Beschleunigen Sie den Datenzugriff mit FlexCache Volumes

Ein FlexCache Volume ist ein Storage Volume, das NFS-gelesene Daten aus einem Ursprungs-Volume (oder Quell-Volume) zwischenspeichert. Nachfolgende Lesezugriffe auf die zwischengespeicherten Daten führen zu einem schnelleren Zugriff auf diese Daten.

FlexCache Volumes beschleunigen den Zugriff auf Daten oder verlagern den Datenverkehr von Volumes, auf die stark zugegriffen wird. FlexCache Volumes tragen zu einer besseren Performance bei, insbesondere wenn Clients wiederholt auf dieselben Daten zugreifen müssen, da die Daten direkt ohne Zugriff auf das Ursprungs-Volume bereitgestellt werden können. FlexCache Volumes eignen sich gut für leseintensive System-Workloads.

Cloud Manager bietet derzeit kein Management von FlexCache Volumes, aber ONTAP CLI oder ONTAP System Manager ermöglicht die Erstellung und das Management von FlexCache Volumes:

- "FlexCache Volumes für schnelleren Datenzugriff – Power Guide"
- "FlexCache Volumes werden in System Manager erstellt"

Ab Version 3.7.2 generiert Cloud Manager eine FlexCache Lizenz für alle neuen Cloud Volumes ONTAP Systeme. Die Lizenz beinhaltet ein Nutzungslimit von 500 GB.

Zum Generieren der Lizenz muss Cloud Manager auf https://ipa-signer.cloudmanager.netapp.com zugreifen. Stellen Sie sicher, dass diese URL von Ihrer Firewall aus zugänglich ist.

Management von vorhandenem Storage

Mit Cloud Manager können Sie Volumes, Aggregate und CIFS-Server managen. Außerdem werden Sie aufgefordert, Volumes zu verschieben, um Kapazitätsprobleme zu vermeiden.

Management vorhandener Volumes

Sie können vorhandene Volumes managen, wenn sich Ihre Storage-Anforderungen ändern. Sie können Volumes anzeigen, bearbeiten, klonen, wiederherstellen und löschen.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf die Arbeitsumgebung Cloud Volumes ONTAP, in der Sie Volumes managen möchten.
2. Managen Sie Ihre Volumes:

Aufgabe	Aktion
Anzeigen von Informationen zu einem Volume	Wählen Sie ein Volume aus, und klicken Sie dann auf **Info**.

Aufgabe	Aktion
Bearbeiten eines Volumes (nur Volumes mit Lese-/Schreibzugriff)	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Bearbeiten**. b. Ändern Sie die Snapshot-Richtlinie des Volumes, die NFS-Protokollversion, die NFS-Zugriffskontrollliste oder die Freigabeberechtigungen und klicken Sie dann auf **Update**. Wenn Sie benutzerdefinierte Snapshot-Richtlinien benötigen, können Sie diese mit System Manager erstellen.
Klonen Sie ein Volume	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Clone**. b. Ändern Sie den Klonnamen nach Bedarf, und klicken Sie dann auf **Clone**. Bei diesem Prozess wird ein FlexClone Volume erstellt. Ein FlexClone Volume ist eine beschreibbare Point-in-Time-Kopie, die platzsparend ist, da es einen geringen Speicherplatz für Metadaten verbraucht und dann nur noch zusätzlichen Speicherplatz verbraucht, wenn Daten geändert oder hinzugefügt werden. Weitere Informationen zu FlexClone Volumes finden Sie im "ONTAP 9 Leitfaden für das Management von logischem Storage".
Wiederherstellen von Daten aus einer Snapshot Kopie auf einem neuen Volume	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Wiederherstellen aus Snapshot Kopie**. b. Wählen Sie eine Snapshot Kopie aus, geben Sie einen Namen für das neue Volume ein und klicken Sie dann auf **Wiederherstellen**.
Erstellen Sie bei Bedarf eine Snapshot Kopie	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Snapshot Kopie erstellen**. b. Ändern Sie ggf. den Namen und klicken Sie dann auf **Erstellen**.
Rufen Sie den NFS-Mount-Befehl ab	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Mount Command**. b. Klicken Sie Auf **Kopieren**.
Zeigen Sie die Ziel-IQN für ein iSCSI-Volume an	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Ziel-IQN**. b. Klicken Sie Auf **Kopieren**. c. "Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen".

Aufgabe	Aktion
Ändern Sie den zugrunde liegenden Festplattentyp	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Festplattentyp und Tiering Policy**. b. Wählen Sie den Laufwerkstyp aus und klicken Sie dann auf **Ändern**. Cloud Manager verschiebt das Volume in ein vorhandenes Aggregat, das den ausgewählten Festplattentyp verwendet, oder erstellt ein neues Aggregat für das Volume.
Ändern Sie die Tiering Policy	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Festplattentyp und Tiering Policy**. b. Klicken Sie Auf **Richtlinie Bearbeiten**. c. Wählen Sie eine andere Richtlinie aus und klicken Sie auf **Ändern**. Cloud Manager verschiebt das Volume in ein vorhandenes Aggregat, das den ausgewählten Festplattentyp mit Tiering verwendet, oder erstellt ein neues Aggregat für das Volume.
Löschen Sie ein Volume	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Löschen**. b. Klicken Sie zur Bestätigung erneut auf **Löschen**.

Management vorhandener Aggregate

Managen Sie Aggregate selbst, indem Sie Festplatten hinzufügen, Informationen über die Aggregate anzeigen und sie löschen.

Bevor Sie beginnen

Wenn Sie ein Aggregat löschen möchten, müssen Sie zunächst die Volumes im Aggregat gelöscht haben.

Über diese Aufgabe

Wenn einem Aggregat nicht mehr genügend Speicherplatz zur Verfügung steht, können Sie Volumes mithilfe von OnCommand System Manager in ein anderes Aggregat verschieben.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf die Arbeitsumgebung Cloud Volumes ONTAP, in der Sie Aggregate managen möchten.
2. Klicken Sie auf das Menü-Symbol und dann auf **Erweitert > Erweiterte Zuweisung**.
3. Verwalten Sie Ihre Aggregate:

Aufgabe	Aktion
Anzeigen von Informationen zu einem Aggregat	Wählen Sie ein Aggregat aus und klicken Sie auf **Info**.

Aufgabe	Aktion
Erstellen Sie ein Volume auf einem bestimmten Aggregat	Wählen Sie ein Aggregat aus und klicken Sie auf **Create Volume**.
Hinzufügen von Festplatten zu einem Aggregat	a. Wählen Sie ein Aggregat aus und klicken Sie auf **AWS-Festplatten hinzufügen** oder **Azure-Festplatten hinzufügen**. b. Wählen Sie die Anzahl der Festplatten aus, die Sie hinzufügen möchten, und klicken Sie auf **Hinzufügen**.  Alle Festplatten in einem Aggregat müssen dieselbe Größe haben.
Löschen Sie ein Aggregat	a. Wählen Sie ein Aggregat aus, das keine Volumes enthält, und klicken Sie auf **Löschen**. b. Klicken Sie zur Bestätigung erneut auf **Löschen**.

Ändern des CIFS-Servers

Wenn Sie Ihre DNS-Server oder Active Directory-Domain ändern, müssen Sie den CIFS-Server in Cloud Volumes ONTAP ändern, damit er weiterhin Storage für Clients bereitstellen kann.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Erweitert > CIFS-Setup**.
2. Geben Sie die Einstellungen für den CIFS-Server an:

Aufgabe	Aktion
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. Wenn Sie von AWS verwaltete Microsoft AD als AD-Server für Cloud Volumes ONTAP konfigurieren, sollten Sie in diesem Feld **OU=Computers,OU=corp** eingeben.
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.

Aufgabe	Aktion
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden** aus, um einen NTP-Server mit Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Siehe "Cloud Manager API-Entwicklerleitfaden" Entsprechende Details.

3. Klicken Sie Auf **Speichern**.

Ergebnis

Cloud Volumes ONTAP aktualisiert den CIFS-Server mit den Änderungen.

Verschieben eines Volumes

Verschieben Sie Volumes, um die Kapazitätsauslastung, die Performance zu verbessern und Service Level Agreements zu erfüllen.

Sie können ein Volume in System Manager verschieben, indem Sie ein Volume und das Zielaggregat auswählen, den Vorgang zur Volume-Verschiebung starten und optional den Auftrag zur Volume-Verschiebung überwachen. Bei Nutzung von System Manager wird die Verschiebung eines Volumes automatisch abgeschlossen.

Schritte

1. Verwenden Sie System Manager oder die CLI, um die Volumes in das Aggregat zu verschieben.

   In den meisten Fällen können Sie mit System Manager Volumes verschieben.

   Anweisungen hierzu finden Sie im "ONTAP 9 Volume Move Express Guide".

Durch das Verschieben eines Volumes, wenn Cloud Manager eine Meldung über die erforderliche Aktion angezeigt wird

Cloud Manager zeigt möglicherweise eine Meldung "Aktion erforderlich" an, die besagt, dass das Verschieben eines Volumes erforderlich ist, um Kapazitätsprobleme zu vermeiden, aber keine Empfehlungen zur Behebung des Problems geben kann. In diesem Fall müssen Sie herausfinden, wie das Problem behoben werden kann, und dann ein oder mehrere Volumes verschieben.

Schritte

1. wie Kapazitätsprobleme behoben werden,Identifizieren, wie das Problem behoben werden kann.
2. Verschieben Sie Volumes basierend auf Ihrer Analyse, um Kapazitätsprobleme zu vermeiden:
   - um Kapazitätsprobleme zu vermeiden,Volumes werden in ein anderes System verschoben.
   - um Kapazitätsprobleme zu vermeiden,Verschieben Sie Volumes zu einem anderen Aggregat auf demselben System.

Identifizieren, wie Kapazitätsprobleme behoben werden

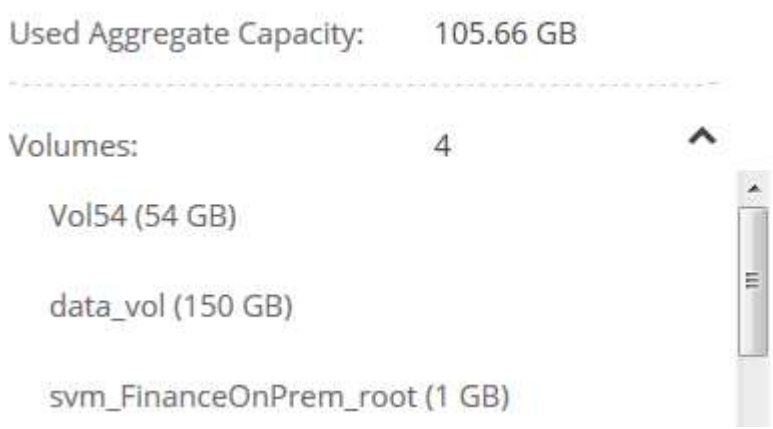
Wenn Cloud Manager keine Empfehlungen für das Verschieben eines Volumes zur Vermeidung von Kapazitätsproblemen geben kann, müssen Sie die Volumes identifizieren, die Sie verschieben müssen, und angeben, ob Sie sie in ein anderes Aggregat auf demselben System oder in ein anderes System verschieben sollten.

Schritte

1. Zeigen Sie die erweiterten Informationen in der Meldung Aktion erforderlich an, um das Aggregat zu identifizieren, das seine Kapazitätsgrenze erreicht hat.

   Die erweiterten Informationen sollten beispielsweise Folgendes enthalten: Aggregat aggr1 hat seine Kapazitätsgrenze erreicht.

2. Identifizieren Sie ein oder mehrere Volumes, die aus dem Aggregat verschoben werden sollen:
   a. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Erweiterte Zuweisung**.
   b. Wählen Sie das Aggregat aus und klicken Sie dann auf **Info**.
   c. Erweitern Sie die Liste der Volumes.



   d. Überprüfen Sie die Größe jedes Volumes, und wählen Sie ein oder mehrere Volumes aus, die aus dem Aggregat verschoben werden sollen.

      Sie sollten Volumes auswählen, die groß genug sind, um Speicherplatz im Aggregat freizugeben, damit Sie in Zukunft zusätzliche Kapazitätsprobleme vermeiden können.

3. Wenn das System die Festplattengrenze nicht erreicht hat, sollten Sie die Volumes in ein vorhandenes Aggregat oder ein neues Aggregat auf demselben System verschieben.

   Weitere Informationen finden Sie unter "Verschieben von Volumes in ein anderes Aggregat, um Kapazitätsprobleme zu vermeiden".

4. Wenn das System die Festplattengrenze erreicht hat, führen Sie einen der folgenden Schritte aus:
   a. Löschen Sie nicht verwendete Volumes.
   b. Ordnen Sie Volumes neu an, um Speicherplatz auf einem Aggregat freizugeben.

      Weitere Informationen finden Sie unter "Verschieben von Volumes in ein anderes Aggregat, um Kapazitätsprobleme zu vermeiden".

   c. Verschieben Sie zwei oder mehr Volumes auf ein anderes System mit Speicherplatz.

      Weitere Informationen finden Sie unter "Verschieben von Volumes auf ein anderes System, um Kapazitätsprobleme zu vermeiden".

Verschieben von Volumes auf ein anderes System, um Kapazitätsprobleme zu vermeiden

Sie können ein oder mehrere Volumes in ein anderes Cloud Volumes ONTAP System verschieben, um Kapazitätsprobleme zu vermeiden. Dies kann erforderlich sein, wenn das System die Festplattengrenze erreicht hat.

Über diese Aufgabe

Sie können die folgenden Schritte in dieser Aufgabe ausführen, um die folgende Meldung "Aktion erforderlich" zu korrigieren:

```
 Moving a volume is necessary to avoid capacity issues; however, Cloud
Manager cannot perform this action for you because the system has reached
the disk limit.
.Schritte
. Identifizieren Sie ein Cloud Volumes ONTAP System mit verfügbarer
Kapazität, oder implementieren Sie ein neues System.
. Ziehen Sie die Quellarbeitsumgebung per Drag & Drop in die
Zielarbeitsumgebung, um eine einmalige Datenreplizierung des Volumes
durchzuführen.
```

+
Weitere Informationen finden Sie unter "Replizierung von Daten zwischen Systemen".

1. Wechseln Sie zur Seite "Replication Status", und brechen Sie die SnapMirror Beziehung ab, um das replizierte Volume von einem Datensicherungsvolume in ein Lese-/Schreibvolume zu konvertieren.

   Weitere Informationen finden Sie unter "Managen von Plänen und Beziehungen zur Datenreplizierung".

2. Konfigurieren Sie das Volume für den Datenzugriff.

   Informationen über die Konfiguration eines Ziel-Volume für den Datenzugriff finden Sie unter "ONTAP 9 Express Guide für die Disaster Recovery von Volumes".

3. Löschen Sie das ursprüngliche Volume.

   Weitere Informationen finden Sie unter "Management vorhandener Volumes".

Verschieben von Volumes in ein anderes Aggregat, um Kapazitätsprobleme zu vermeiden

Sie können ein oder mehrere Volumes in ein anderes Aggregat verschieben, um Kapazitätsprobleme zu vermeiden.

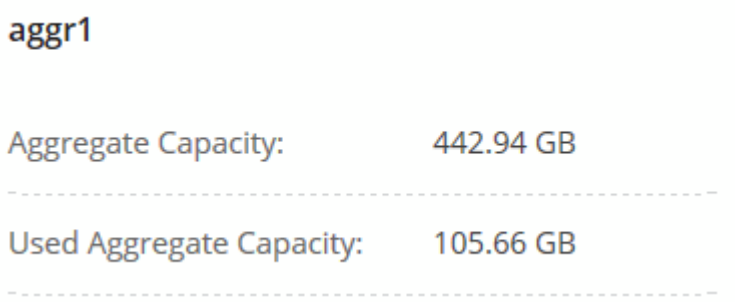
Über diese Aufgabe

Sie können die folgenden Schritte in dieser Aufgabe ausführen, um die folgende Meldung "Aktion erforderlich" zu korrigieren:

```
 Moving two or more volumes is necessary to avoid capacity issues;
however, Cloud Manager cannot perform this action for you.
.Schritte
. Überprüfen Sie, ob ein vorhandenes Aggregat über die verfügbare
Kapazität für die Volumes verfügt, die Sie verschieben müssen:
```

+
.. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Erweiterte Zuweisung**.
.. Wählen Sie jedes Aggregat aus, klicken Sie auf **Info** und sehen Sie dann die verfügbare Kapazität (Aggregatskapazität minus genutzte Aggregatskapazität).

+



1. Fügen Sie bei Bedarf Festplatten zu einem vorhandenen Aggregat hinzu:
   a. Wählen Sie das Aggregat aus und klicken Sie dann auf **Add Disks**.
   b. Wählen Sie die Anzahl der hinzuzufügenden Festplatten aus, und klicken Sie dann auf **Hinzufügen**.
2. Wenn keine Aggregate über verfügbare Kapazität verfügen, erstellen Sie ein neues Aggregat.

   Weitere Informationen finden Sie unter "Aggregate werden erstellt".
3. Verwenden Sie System Manager oder die CLI, um die Volumes in das Aggregat zu verschieben.
4. In den meisten Fällen können Sie mit System Manager Volumes verschieben.

   Anweisungen hierzu finden Sie im "ONTAP 9 Volume Move Express Guide".

Gründe, warum eine Volume-Verschiebung langsam durchführen könnte

Das Verschieben eines Volumes dauert möglicherweise länger, als erwartet wird, wenn eine der folgenden Bedingungen für Cloud Volumes ONTAP zutrifft:

- Das Volume ist ein Klon.
- Das Volume ist ein übergeordnetes Objekt eines Klons.
- Das Quell- oder Zielaggregat verfügt über eine einzige durchsatzoptimierte Festplatte (st1).
- Das Cloud Volumes ONTAP System befindet sich in AWS und ein Aggregat verwendet ein älteres Benennungsschema für Objekte. Beide Aggregate müssen das gleiche Namenformat verwenden.

  Ein älteres Benennungsschema wird verwendet, wenn das Daten-Tiering auf einem Aggregat in Version 9.4 oder früher aktiviert wurde.

- Die Verschlüsselungseinstellungen stimmen nicht mit den Quell- und Zielaggregaten überein. Zudem wird ein Rekey ausgeführt.
- Die Option *-Tiering-Richtlinie* wurde bei der Verschiebung des Volumes angegeben, um die Tiering-Richtlinie zu ändern.
- Die Option *-Generate-Destination-key* wurde für die Verschiebung des Volumes angegeben.

Tiering inaktiver Daten in kostengünstigen Objektspeicher

Sie können die Storage-Kosten für Cloud Volumes ONTAP senken, indem Sie eine SSD- oder HDD-Performance-Tier für häufig abgerufene Daten mit einem Objekt-Storage-Kapazitäts-Tier für inaktive Daten kombinieren. Eine allgemeine Übersicht finden Sie unter "Data Tiering - Übersicht".

Zum Einrichten von Data Tiering müssen Sie lediglich Folgendes tun:

Wählen Sie eine unterstützte Konfiguration aus

Die meisten Konfigurationen werden unterstützt. Wenn Sie über ein Cloud Volumes ONTAP Standard-, Premium- oder BYOL-System mit der aktuellsten Version verfügen, sollten Sie sich dafür entscheiden. "Weitere Informationen .".

Stellen Sie die Konnektivität zwischen Cloud Volumes ONTAP und Objekt-Storage sicher

- Für AWS ist ein VPC Endpunkt zu S3 erforderlich. Weitere Informationen ..
- Bei Azure sind keine Vorgänge mehr notwendig, solange Cloud Manager über die erforderlichen Berechtigungen verfügt. Weitere Informationen ..
- Für GCP müssen Sie das Subnetz für privaten Google Access konfigurieren und ein Service-Konto einrichten. Weitere Informationen ..

Wählen Sie eine Tiering-Richtlinie beim Erstellen, Ändern oder Replizieren eines Volume

Cloud Manager fordert Sie auf, beim Erstellen, Ändern oder Replizieren eines Volume eine Tiering-Richtlinie auszuwählen.

- "Tiering von Daten auf Lese-/Schreib-Volumes"
- "Tiering von Daten auf Data-Protection-Volumes"

Welche und#8217;s sind für das Daten-Tiering nicht erforderlich

- Für die Aktivierung von Daten-Tiering müssen Sie keine Funktionslizenz installieren.
- Es ist nicht erforderlich, die Kapazitäts-Tier (ein S3-Bucket, Azure Blob-Container oder GCP-Bucket) zu erstellen. Cloud Manager macht das für Sie.

Konfigurationen, die Daten-Tiering unterstützen

Sie können das Daten-Tiering aktivieren, wenn Sie bestimmte Konfigurationen und Funktionen verwenden:

- Das Daten-Tiering wird mit Cloud Volumes ONTAP Standard, Premium und BYOL unterstützt. Es beginnt mit den folgenden Versionen:
  - Version 9.2 in AWS
  - Version 9.4 in Azure mit Single-Node-Systemen
  - Version 9.6 in Azure mit HA-Paaren
  - Version 9.6 in GCP

  Data Tiering wird in Azure mit dem virtuellen Maschinentyp DS3_v2 nicht unterstützt.

- In AWS kann es sich um allgemeine SSDs, bereitgestellte IOPS SSDs oder Throughput Optimized HDDs handeln.
- In Azure kann die Performance-Tier Premium-Festplatten mit SSD-Management, von Standard-SSDs gemanagte Festplatten oder von Standard-HDDs gemanagte Festplatten sein.
- In der GCP kann die Performance-Tier entweder SSDs oder HDDs (Standard-Festplatten) sein.
- Daten-Tiering wird durch Verschlüsselungstechnologien unterstützt.
- Thin Provisioning muss auf Volumes aktiviert sein.

Anforderungen für das Tiering selten genutzter Daten in AWS S3

Stellen Sie sicher, dass Cloud Volumes ONTAP eine Verbindung zu S3 hat. Die beste Möglichkeit, diese Verbindung bereitzustellen, besteht darin, einen VPC-Endpunkt für den S3-Dienst zu erstellen. Anweisungen hierzu finden Sie unter "AWS Dokumentation: Erstellen eines Gateway-Endpunkts".

Wenn Sie den VPC-Endpunkt erstellen, wählen Sie die Region, den VPC und die Routing-Tabelle aus, die der Cloud Volumes ONTAP Instanz entspricht. Sie müssen auch die Sicherheitsgruppe ändern, um eine ausgehende HTTPS-Regel hinzuzufügen, die Datenverkehr zum S3-Endpunkt ermöglicht. Andernfalls kann Cloud Volumes ONTAP keine Verbindung zum S3-Service herstellen.

Informationen zu Problemen finden Sie unter "AWS Support Knowledge Center: Warum kann ich mich nicht über einen Gateway VPC Endpunkt mit einem S3-Bucket verbinden?".

Tiering selten genutzter Daten auf Azure Blob Storage

Es muss keine Verbindung zwischen der Performance-Tier und der Kapazitäts-Tier eingerichtet werden, sofern Cloud Manager über die erforderlichen Berechtigungen verfügt. Cloud Manager unterstützt ein vnet-Service-Endpunkt für Sie, wenn die Cloud Manager-Richtlinie über die folgenden Berechtigungen verfügt:

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Die Berechtigungen sind in der letzten enthalten "Cloud Manager-Richtlinie".

Anforderungen für das Tiering selten genutzter Daten in einen Google Cloud Storage Bucket

- Das Subnetz, in dem Cloud Volumes ONTAP residiert, muss für privaten Google-Zugriff konfiguriert werden. Anweisungen finden Sie unter "Google Cloud Documentation: Configuring Private Google Access".
- Sie benötigen ein Servicekonto mit der vordefinierten Storage-Administratorrolle. Wählen Sie dieses Servicekonto aus, wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen.

  "Richten Sie dieses Tiering-Dienstkonto wie folgt ein":

  a. Weisen Sie dem Tiering-Service-Konto die vordefinierte Rolle „*Storage Admin*“ zu.

  b. Fügen Sie das Connector-Dienstkonto als *Service-Konto-Benutzer* zum Tiering-Dienstkonto hinzu.

     Sie können die Benutzerrolle angeben "In Schritt 3 des Assistenten, wenn Sie das Tiering Service-Konto erstellen", Oder "Geben Sie die Rolle nach der Erstellung des Dienstkontos ein".

     Sie müssen das Tiering Service-Konto später auswählen, wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen.

  Wenn Sie kein Daten-Tiering aktivieren und bei der Erstellung des Cloud Volumes ONTAP-Systems ein Service-Konto auswählen, müssen Sie das System deaktivieren und das Service-Konto über die GCP-Konsole zu Cloud Volumes ONTAP hinzufügen.

Tiering von Daten aus Volumes mit Lese- und Schreibvorgängen

Cloud Volumes ONTAP kann inaktive Daten auf Volumes mit Lese- und Schreibvorgängen auf kostengünstigen Objekt-Storage verschieben und so den Performance-Tier für häufig abgerufene Daten freisetzen.

Schritte

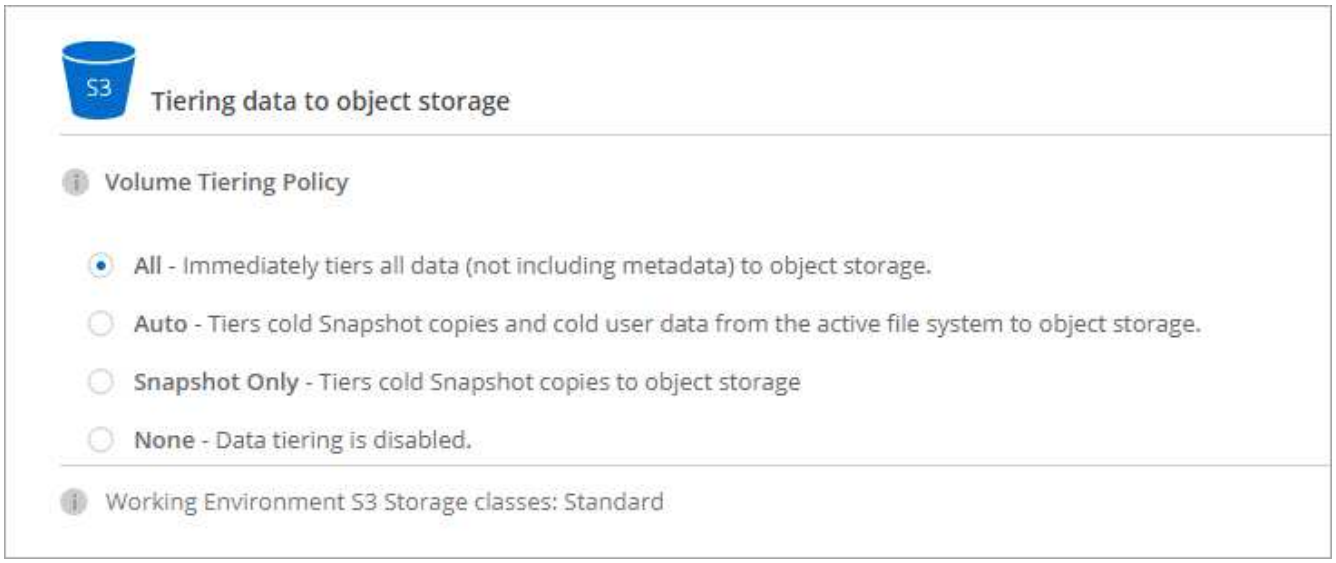
1. Erstellen Sie in der Arbeitsumgebung ein neues Volume, oder ändern Sie den Tier eines vorhandenen Volumes:

Aufgabe	Aktion
Erstellen Sie ein neues Volume	Klicken Sie Auf **Neues Volume Hinzufügen**.
Ändern Sie ein vorhandenes Volume	Wählen Sie das Volume aus und klicken Sie auf **Disk Type & Tiering Policy**.

2. Wählen Sie eine Tiering-Richtlinie aus.

   Eine Beschreibung dieser Richtlinien finden Sie unter "Data Tiering - Übersicht".

   Beispiel



Cloud Manager erstellt ein neues Aggregat für das Volume, wenn noch kein Daten Tiering-aktiviertes Aggregat vorhanden ist.

Wenn Sie Aggregate selbst erstellen möchten, können Sie beim Erstellen von Aggregaten das Daten-Tiering aktivieren.

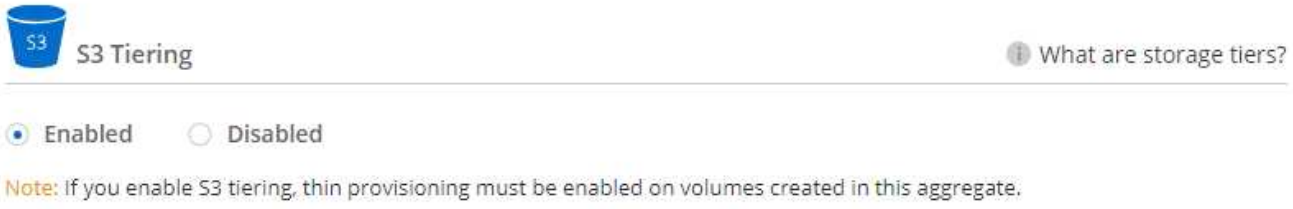
Tiering von Daten aus Datensicherungs-Volumes

Cloud Volumes ONTAP kann Daten von einem Daten-Protection-Volume auf eine Kapazitäts-Tier einstufen. Wenn Sie das Ziel-Volume aktivieren, werden die Daten beim Lesen schrittweise auf die Performance-Ebene verschoben.

Schritte

1. Wählen Sie auf der Seite Arbeitsumgebungen die Arbeitsumgebung aus, die das Quell-Volume enthält, und ziehen Sie es in die Arbeitsumgebung, in die Sie das Volume replizieren möchten.
2. Folgen Sie den Anweisungen, bis Sie die Seite Tiering aufrufen und Data Tiering für Objektspeicher aktivieren.

Beispiel



Unterstützung bei der Datenreplizierung finden Sie unter "Replizierung von Daten in die und aus der Cloud".

Änderung der Storage-Klasse für Tiered Daten

Nachdem Sie Cloud Volumes ONTAP implementiert haben, können Sie Ihre Storage-Kosten senken, indem Sie die Storage-Klasse für inaktive Daten ändern, auf die seit 30 Tagen nicht mehr zugegriffen wurde. Die

Zugriffskosten sind höher, wenn der Zugriff auf die Daten erfolgt. Berücksichtigen Sie diese also vor einem Wechsel der Storage-Klasse.

Die Storage-Klasse für Tiered Daten beträgt im gesamten System – nicht It pro Volume.

Informationen zu unterstützten Speicherklassen finden Sie unter "Data Tiering - Übersicht".

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Speicherklassen** oder **Blob Storage Tiering**.
2. Wählen Sie eine Speicherklasse aus und klicken Sie dann auf **Speichern**.

Kann ich Daten-Tiering auf einem vorhandenen Aggregat aktivieren?

Nein, Sie können das Daten-Tiering nicht auf einem vorhandenen Aggregat aktivieren. Sie können Daten-Tiering nur auf neuen Aggregaten aktivieren.

Sie können auch Daten-Tiering auf einem neuen Aggregat aktivieren "Indem Sie ein Aggregat selbst erstellen" Oder Indem ein neues Volume mit aktiviertem Daten-Tiering erstellt wird. Cloud Manager würde dann ein neues Aggregat für das Volume erstellen, wenn es bereits ein Daten-Tiering-fähiges Aggregat gibt.

Managen von Storage-VMs

Eine Storage VM ist eine Virtual Machine, die in ONTAP ausgeführt wird und Ihren Kunden Storage und Datenservices zur Verfügung stellt. Vielleicht wissen Sie das als *SVM* oder *vServer*. Cloud Volumes ONTAP ist standardmäßig mit einer Storage-VM konfiguriert, aber einige Konfigurationen unterstützen zusätzliche Storage-VMs.

Unterstützte Anzahl von Storage-VMs

Cloud Volumes ONTAP 9.7 unterstützt mehrere Storage-VMs in AWS mit bestimmten Konfigurationen und einer Add-on-Lizenz. "Anzeige der Anzahl der unterstützten Storage-VMs in AWS". Wenden Sie sich an Ihr Account-Team, um eine SVM-Add-on-Lizenz zu erhalten.

Alle anderen Cloud Volumes ONTAP Konfigurationen unterstützen eine Storage-VM mit Datenbereitstellung und eine Ziel-Storage-VM für die Disaster Recovery. Sie können die Ziel-Storage-VM für den Datenzugriff aktivieren, wenn es einen Ausfall auf der Quell-Storage-VM gibt.

Eine Storage-VM umfasst das gesamte Cloud Volumes ONTAP System (HA-Paar oder Single Node).

Erstellen von zusätzlichen Storage-VMs

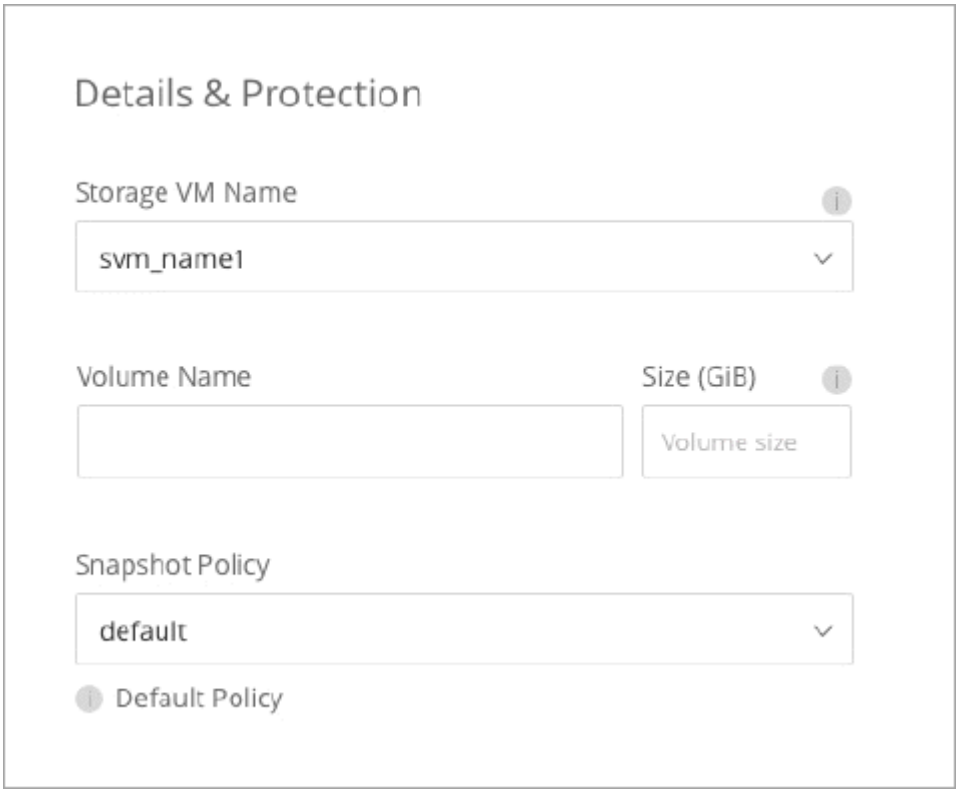
Wenn diese von Ihrer Konfiguration unterstützt werden, können Sie mit zusätzliche Storage-VMs erstellen "System Manager oder die CLI".

- "Erstellen einer SVM für SMB-Zugriff"
- "Erstellen einer SVM für NFS-Zugriff"
- "Erstellen einer SVM für iSCSI-Zugriff"
- "Erstellung einer Ziel-SVM für Disaster Recovery"

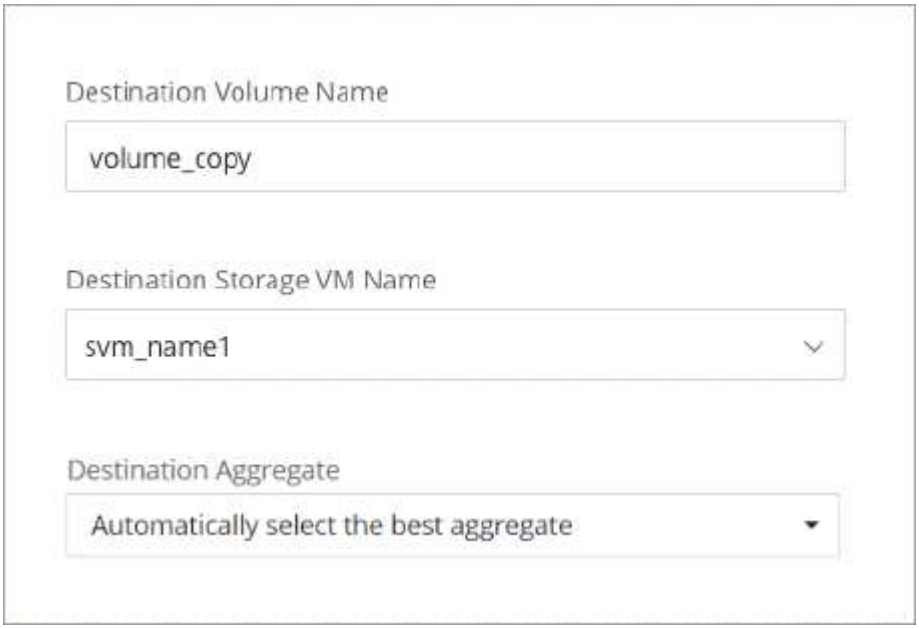
Arbeiten mit mehreren Storage VMs in Cloud Manager

Cloud Manager unterstützt alle zusätzlichen Storage-VMs, die Sie über System Manager oder die CLI erstellen.

Das folgende Bild zeigt beispielsweise, wie Sie beim Erstellen eines Volumes eine Storage-VM auswählen können.



Das folgende Bild zeigt, wie Sie bei der Replizierung eines Volumes in ein anderes System eine Storage VM auswählen können.



Management der Disaster Recovery für Storage VMs

Cloud Manager bietet keine Unterstützung für die Einrichtung oder Orchestrierung von Storage VM Disaster Recovery. Sie müssen System Manager oder die CLI verwenden.

- "Express Guide zur Vorbereitung des SVM-Disaster Recovery"
- "SVM Disaster Recovery Express Guide"

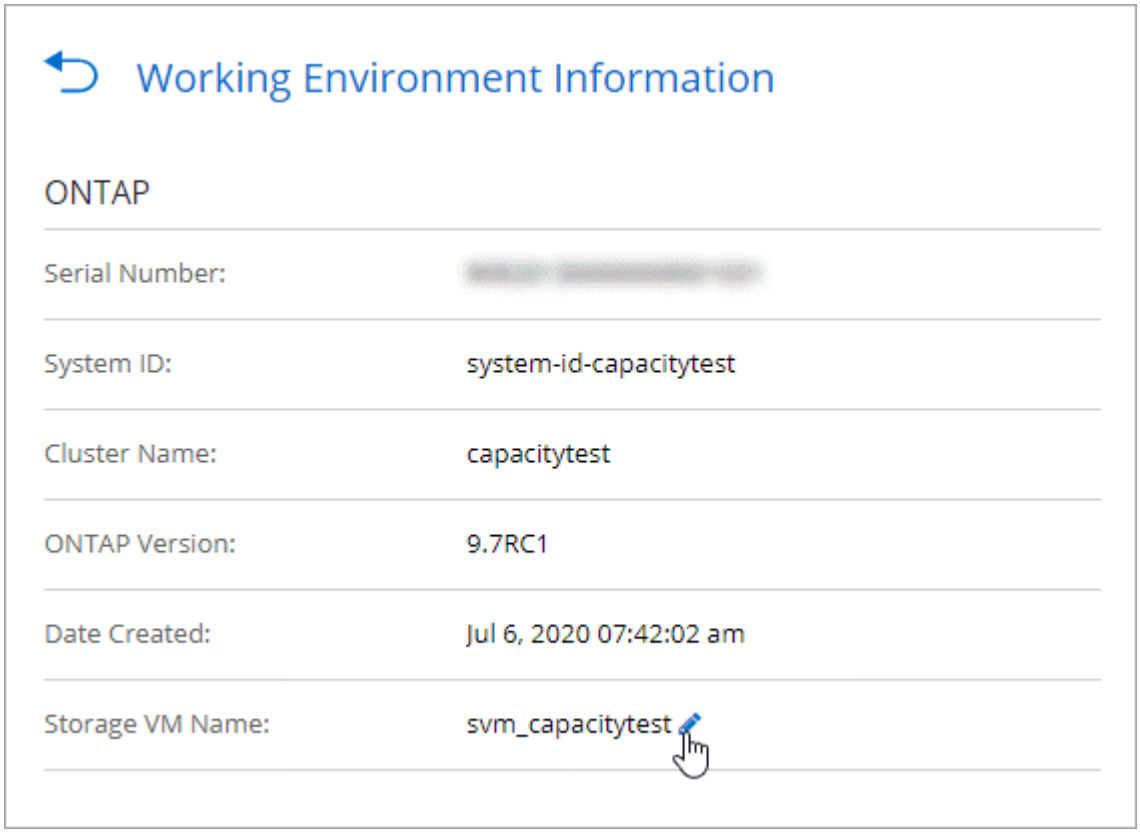
Ändern des Namens der Storage-VM

Cloud Manager benennt automatisch die einzelne Storage-VM, die sie für Cloud Volumes ONTAP erstellt. Sie können den Namen der Storage VM ändern, wenn Sie strenge Namensstandards haben. Beispielsweise möchte der Name Ihnen entsprechen, wie Sie die Storage-VMs für Ihre ONTAP Cluster benennen.

Wenn Sie zusätzliche Storage VMs für Cloud Volumes ONTAP erstellt haben, können Sie die Storage-VMs nicht aus Cloud Manager umbenennen. Sie müssen dies direkt von Cloud Volumes ONTAP mit System Manager oder der CLI ausführen.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Information**.
2. Klicken Sie rechts neben dem Namen der Storage-VM auf das Bearbeiten-Symbol.



3. Ändern Sie im Dialogfeld SVM-Name ändern den Namen und klicken Sie dann auf **Speichern**.

Verwendung von Cloud Volumes ONTAP als persistenter Storage für Kubernetes

Cloud Manager kann die Implementierung von NetApp Trident auf Kubernetes-Clustern automatisieren, sodass Sie Cloud Volumes ONTAP als persistenten Storage für

Container verwenden können.

Trident ist ein vollständig von NetApp unterstütztes Open-Source-Projekt. Trident lässt sich nativ mit Kubernetes und dessen Persistent Volume Framework integrieren und ermöglicht das nahtlose Bereitstellen und Managen von Volumes auf Systemen, die auf beliebigen Kombinationen von NetApp Storage-Plattformen ausgeführt werden. "Weitere Informationen zu Trident".

> Die Kubernetes-Funktion wird nicht durch lokale ONTAP-Cluster unterstützt. Es wird nur mit Cloud Volumes ONTAP unterstützt.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

Voraussetzungen prüfen

Stellen Sie sicher, dass Ihre Umgebung die Voraussetzungen erfüllt, einschließlich Konnektivität zwischen Kubernetes-Clustern und Cloud Volumes ONTAP, Konnektivität zwischen Kubernetes-Clustern und einem Connector, mindestens Kubernetes-Version von 1.14, mindestens einen Worker-Node in einem Cluster und mehr. Eine vollständige Liste finden Sie hier.

Fügen Sie Ihre Kubernetes Cluster zu Cloud Manager hinzu

Klicken Sie in Cloud Manager auf **Kubernetes**, um Cluster direkt aus dem Managed Service Ihres Cloud-Providers zu ermitteln, oder importieren Sie einen Cluster, indem Sie eine kubeconfig-Datei bereitstellen.

Verbinden Sie die Cluster mit Cloud Volumes ONTAP

Klicken Sie nach dem Hinzufügen eines Kubernetes-Clusters auf **Verbinden mit der Arbeitsumgebung**, um den Cluster mit einem oder mehreren Cloud Volumes ONTAP-Systemen zu verbinden.

Starten Sie die Bereitstellung persistenter Volumes

Persistente Volumes können über native Kubernetes-Schnittstellen und -Konstrukte angefordert und gemanagt werden. Cloud Manager erstellt NFS- und iSCSI-Storage-Klassen, die bei der Bereitstellung persistenter Volumes genutzt werden können.

"Erfahren Sie mehr über die Bereitstellung Ihres ersten Volumes mit Trident für Kubernetes".

Voraussetzungen prüfen

Bevor Sie beginnen, stellen Sie sicher, dass die Kubernetes-Cluster und der Connector bestimmte Anforderungen erfüllen.

Kubernetes-Cluster-Anforderungen

- Zwischen einem Kubernetes Cluster und dem Connector sowie zwischen einem Kubernetes Cluster und Cloud Volumes ONTAP ist eine Netzwerkverbindung erforderlich.

  Sowohl der Connector als auch der Cloud Volumes ONTAP benötigen eine Verbindung zum Kubernetes API Endpunkt:

  - Legen Sie für gemanagte Cluster eine Route zwischen der VPC eines Clusters und der VPC fest, an der sich der Connector und die Cloud Volumes ONTAP befinden.
  - Bei anderen Clustern muss die IP-Adresse des Hauptknotens oder des Load Balancer (wie in der kubeconfig-Datei angegeben) über den Connector und den Cloud Volumes ONTAP erreichbar sein, und es muss ein gültiges TLS-Zertifikat vorhanden sein.
- Ein Kubernetes-Cluster kann sich an jedem Ort befinden, an dem die oben aufgeführte Netzwerkverbindung vorhanden ist.
- Ein Kubernetes Cluster muss mindestens Version 1.14 ausführen.

  Die Version mit der maximalen Anzahl wird von Trident definiert. "Klicken Sie hier, um die maximal unterstützte Kubernetes-Version anzuzeigen".
- Ein Kubernetes-Cluster muss mindestens einen Worker-Node aufweisen.
- Für Cluster, die im Amazon Elastic Kubernetes Service (Amazon EKS) ausgeführt werden, benötigt jedes Cluster eine IAM-Rolle, um einen Berechtigungsfehler zu beheben. Nachdem Sie das Cluster hinzugefügt haben, werden Sie von Cloud Manager mit dem exact eksctl-Befehl aufgefordert, der den Fehler auflöst.

  "Erfahren Sie mehr über die Grenzen der IAM-Berechtigungen".
- Für Cluster, die im Azure Kubernetes Service (AKS) ausgeführt werden, müssen diesen Clustern die Rolle „*Azure Kubernetes Service RBAC für Cluster Admin*“ zugewiesen werden. Dies ist nötig, damit Cloud Manager Trident installieren und Storage-Klassen auf dem Cluster konfigurieren kann.
- Bei Clustern, die in der Google Kubernetes Engine (GKE) ausgeführt werden, dürfen diese Cluster nicht das standardmäßige für Container optimierte Betriebssystem verwenden. Sie sollten sie wechseln, um Ubuntu zu verwenden.

  GKE verwendet standardmäßig Google "Für Container optimiertes Image", Welches nicht über die Dienstprogramme verfügt, die Trident zum Mounten von Volumes benötigt.

Anforderungen an Steckverbinder

Stellen Sie sicher, dass die folgenden Netzwerk- und Berechtigungen für den Connector vorhanden sind.

Netzwerkbetrieb

- Für die Installation von Trident ist eine ausgehende Internetverbindung erforderlich, um auf die folgenden Endpunkte zuzugreifen:

  https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/

  Cloud Manager installiert Trident auf einem Kubernetes-Cluster, wenn Sie eine Arbeitsumgebung mit dem Cluster verbinden.

Erforderliche Berechtigungen zum ermitteln und Verwalten von EKS-Clustern

Für die Erkennung und das Management von Kubernetes-Clustern in Amazon Elastic Kubernetes Service (EKS) benötigt der Connector Administratorberechtigungen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "eks:*",
            "Resource": "*"
        }
    ]
}
```

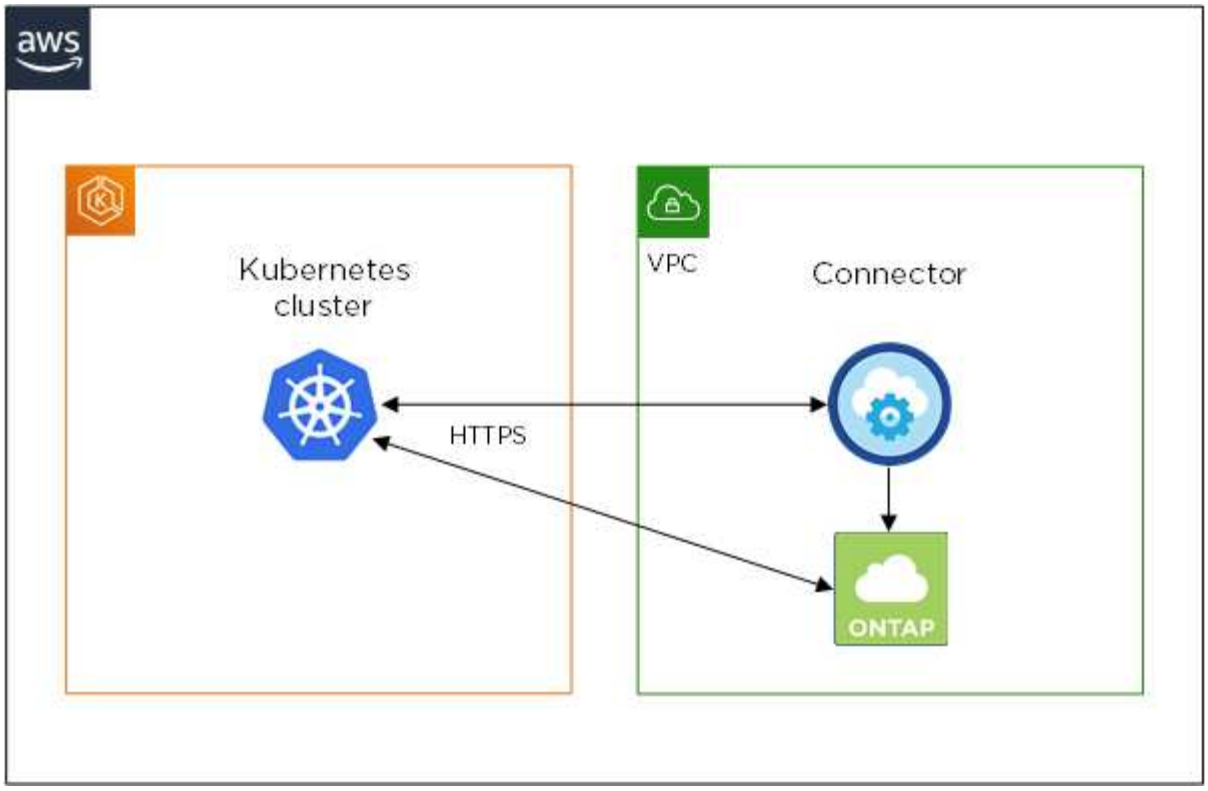
Erforderliche Berechtigungen zum ermitteln und Verwalten von GKE-Clustern

Für die Erkennung und das Management von Kubernetes-Clustern in der Google Kubernetes Engine (GKE) benötigt der Connector folgende Berechtigungen:

```
container.*
```

Beispiel für die Einrichtung

Das folgende Bild zeigt ein Beispiel für einen Kubernetes-Cluster mit Amazon Elastic Kubernetes Service (Amazon EKS) und dessen Verbindungen zum Connector und Cloud Volumes ONTAP.



Hinzufügen von Kubernetes Clustern

Fügen Sie Kubernetes-Cluster zu Cloud Manager hinzu, indem Sie die Cluster ermitteln, die im Managed Kubernetes Service des Cloud-Providers ausgeführt werden, oder indem Sie die kubeconfig-Datei eines Clusters importieren.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Kubernetes**.
2. Klicken Sie Auf **Cluster Hinzufügen**.
3. Wählen Sie eine der folgenden Optionen:
   - Klicken Sie auf **Cluster ermitteln**, um die verwalteten Cluster zu ermitteln, auf die Cloud Manager Zugriff hat, basierend auf den Berechtigungen, die Sie dem Connector bereitgestellt haben.

     Wenn Ihr Connector beispielsweise in Google Cloud ausgeführt wird, verwendet Cloud Manager die Berechtigungen aus dem Dienstkonto des Connectors, um Cluster zu ermitteln, die in der Google Kubernetes Engine (GKE) ausgeführt werden.

   - Klicken Sie auf **Cluster importieren**, um einen Cluster mit einer kubeconfig-Datei zu importieren.

     Nach dem Hochladen der Datei überprüft Cloud Manager die Verbindung zum Cluster und speichert eine verschlüsselte Kopie der kubeconfig-Datei.

Ergebnis

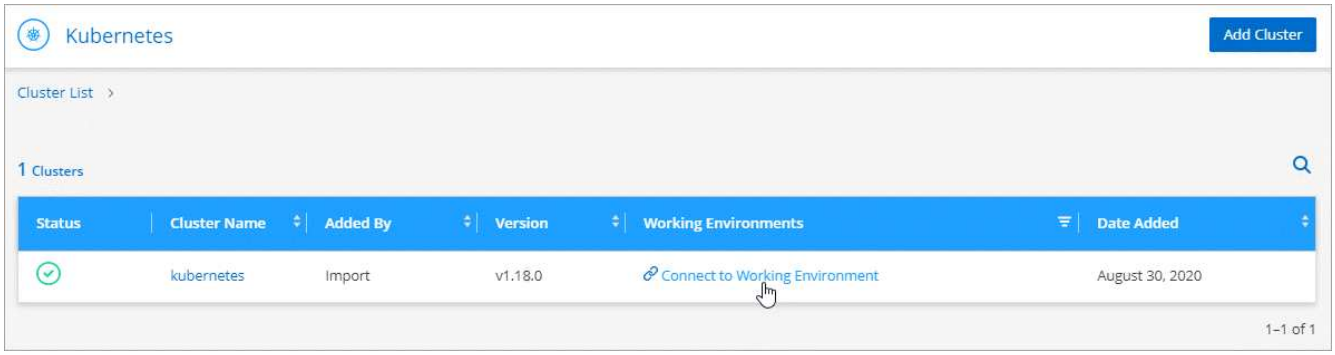
Cloud Manager fügt den Kubernetes-Cluster hinzu. Sie können das Cluster jetzt mit Cloud Volumes ONTAP verbinden.

Verbinden eines Clusters mit Cloud Volumes ONTAP

Verbinden Sie ein Kubernetes Cluster mit Cloud Volumes ONTAP, damit Sie Cloud Volumes ONTAP als persistenten Storage für Container verwenden können.

Schritte

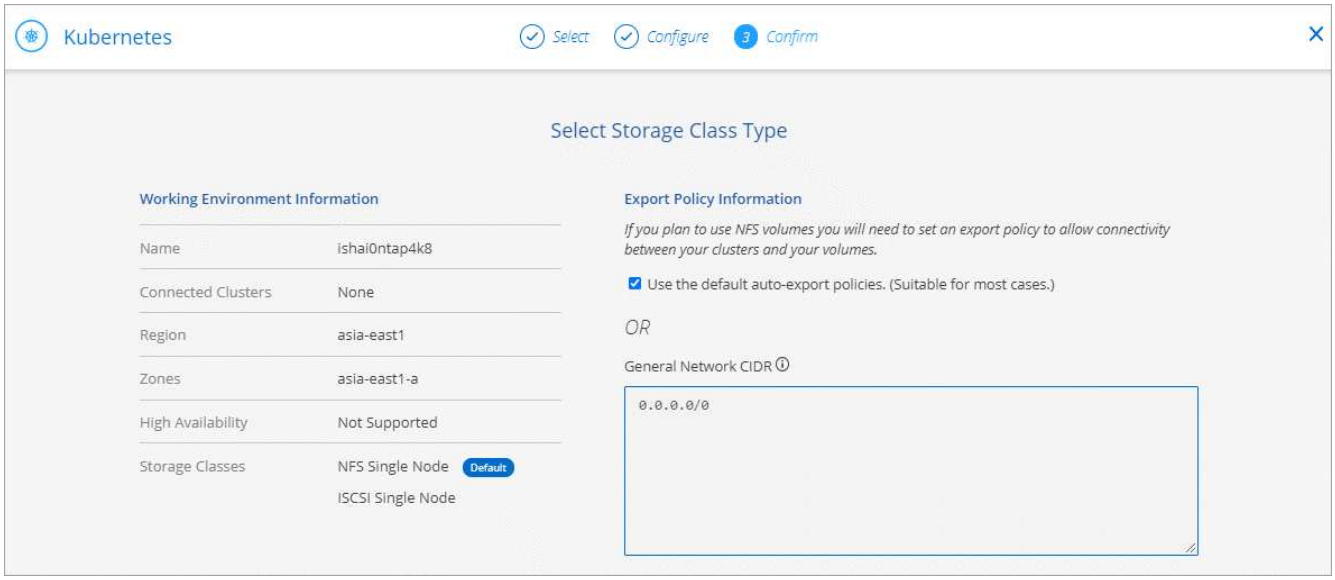
1. Klicken Sie oben im Cloud Manager auf **Kubernetes**.
2. Klicken Sie für den Cluster, den Sie gerade hinzugefügt haben, auf **mit der Arbeitsumgebung verbinden**.



3. Wählen Sie eine Arbeitsumgebung aus und klicken Sie auf **Weiter**.
4. Wählen Sie die NetApp Storage-Klasse als Standard-Storage-Klasse für den Kubernetes Cluster und klicken Sie auf **Weiter**.

   Wenn ein Benutzer ein persistentes Volume erstellt, kann der Kubernetes-Cluster diese Storage-Klasse standardmäßig als Back-End-Storage verwenden.

5. Wählen Sie, ob Sie die Standard-Richtlinien für den automatischen Export verwenden oder einen benutzerdefinierten CIDR-Block hinzufügen möchten.



6. Klicken Sie Auf **Arbeitsumgebung Hinzufügen**.

Ergebnis

Cloud Manager verbindet die Arbeitsumgebung mit dem Cluster, was bis zu 15 Minuten dauert.

Verwalten von Clustern

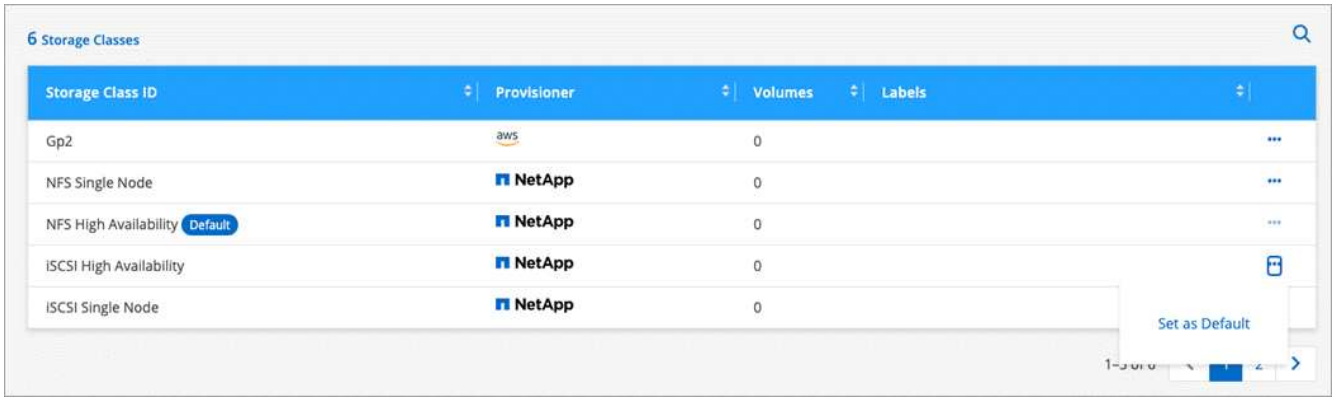
Mit Cloud Manager können Sie Ihre Kubernetes-Cluster managen, indem Sie die Standard-Storage-Klasse ändern, Trident aktualisieren und vieles mehr.

Ändern der Standard-Storage-Klasse

Stellen Sie sicher, dass Sie eine Cloud Volumes ONTAP Storage-Klasse als Standard-Storage-Klasse eingestellt haben, sodass Cluster Cloud Volumes ONTAP als Back-End Storage verwenden.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Kubernetes**.
2. Klicken Sie auf den Namen des Kubernetes-Clusters.
3. Klicken Sie in der Tabelle **Speicherklassen** ganz rechts auf das Menü Aktionen für die Speicherklasse, die Sie als Standard festlegen möchten.



4. Klicken Sie auf **als Standard festlegen**.

Upgrade Von Trident

Sie können Trident von Cloud Manager aktualisieren, wenn eine neue Version von Trident verfügbar ist.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Kubernetes**.
2. Klicken Sie auf den Namen des Kubernetes-Clusters.
3. Wenn eine neue Version verfügbar ist, klicken Sie neben der Trident-Version auf **Upgrade**.

Die kubeconfig-Datei wird aktualisiert

Wenn Sie den Cluster zum Cloud Manager hinzugefügt haben, indem Sie die kubeconfig-Datei importieren, können Sie die neueste kubeconfig-Datei jederzeit in Cloud Manager hochladen. Dies ist möglich, wenn Sie die Anmeldeinformationen aktualisiert haben, Benutzer oder Rollen geändert haben oder wenn sich etwas

geändert hat, das das Cluster, Benutzer, Namespaces oder die Authentifizierung betrifft.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Kubernetes**.
2. Klicken Sie auf den Namen des Kubernetes-Clusters.
3. Klicken Sie Auf **Kubeconfeigent Aktualisieren**.
4. Wenn Sie durch Ihren Webbrowser aufgefordert werden, wählen Sie die aktualisierte kubeconfg-Datei aus und klicken Sie auf **Öffnen**.

Ergebnis

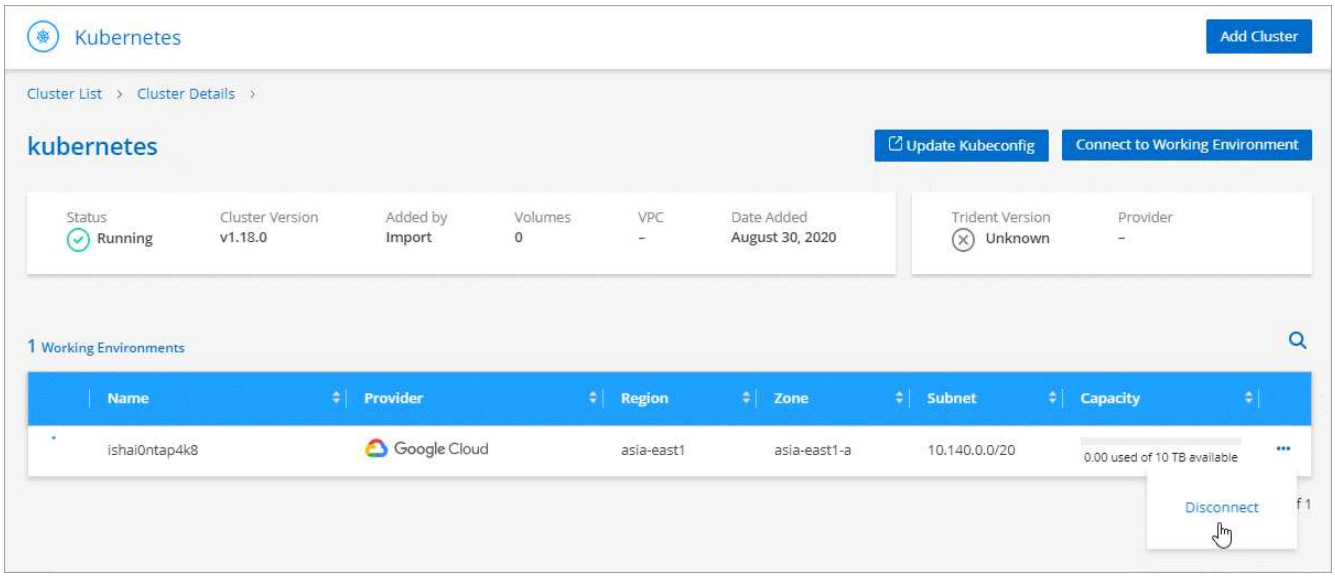
Cloud Manager aktualisiert die Informationen zum Kubernetes-Cluster auf der Grundlage der neuesten kubeconfig Datei.

Trennen eines Clusters

Wenn Sie ein Cluster von Cloud Volumes ONTAP trennen, können Sie dieses Cloud Volumes ONTAP System nicht mehr als persistenten Storage für Container verwenden. Vorhandene persistente Volumes werden nicht gelöscht.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Kubernetes**.
2. Klicken Sie auf den Namen des Kubernetes-Clusters.
3. Klicken Sie in der Tabelle **Arbeitsumgebungen** auf das Menü Aktionen ganz rechts für die Arbeitsumgebung, die Sie trennen möchten.



4. Klicken Sie Auf **Trennen**.

Ergebnis

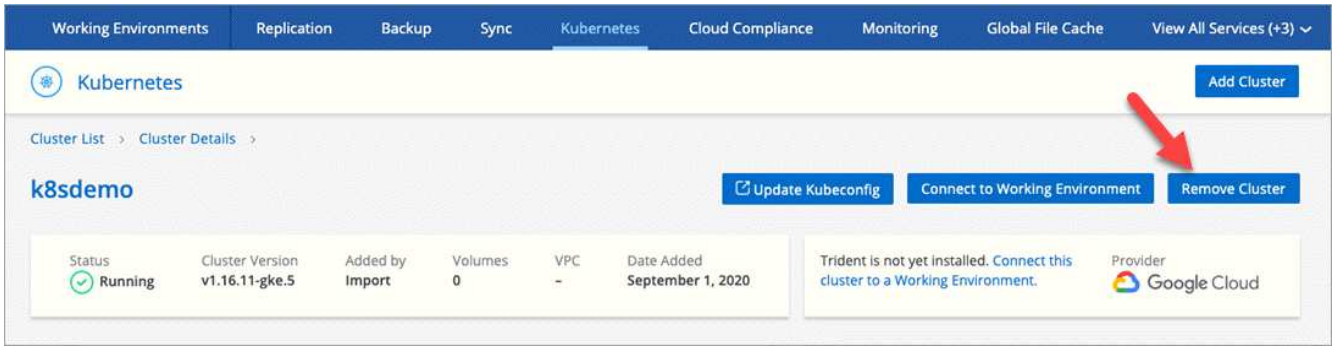
Cloud Manager trennt die Verbindung des Clusters vom Cloud Volumes ONTAP System.

Entfernen eines Clusters

Entfernen Sie stillgelegte Cluster aus dem Cloud Manager, nachdem Sie alle Arbeitsumgebungen vom Cluster getrennt haben.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Kubernetes**.
2. Klicken Sie auf den Namen des Kubernetes-Clusters.
3. Klicken Sie Auf **Cluster Entfernen**.



Verschlüsseln von Volumes mit NetApp Verschlüsselungslösungen

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. "Weitere Informationen zu diesen Verschlüsselungslösungen".

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

Cloud Volumes ONTAP unterstützt kein Onboard-Verschlüsselungsmanagement.

Was Sie benötigen

Ihr Cloud Volumes ONTAP System sollte beim NetApp Support registriert sein. Ab Cloud Manager 3.7 wird auf jedem Cloud Volumes ONTAP System, das beim NetApp Support registriert ist, automatisch eine NetApp Volume Encryption Lizenz installiert.

- "Hinzufügen von NetApp Support Site Konten zu Cloud Manager"
- "Registrieren von Pay-as-you-go-Systemen"

Cloud Manager installiert die NVE-Lizenz nicht auf Systemen, die sich in der Region China befinden.

Schritte

1. Überprüfen Sie die Liste der unterstützten Schlüsselmanager im "NetApp Interoperabilitäts-Matrix-Tool".

   Suchen Sie nach der **Key Manager**-Lösung.

2. "Stellen Sie eine Verbindung zur Cloud Volumes ONTAP-CLI her".
3. Installieren Sie SSL-Zertifikate und stellen Sie eine Verbindung zu den externen

Schlüsselverwaltungsservern her.

"ONTAP 9 NetApp Verschlüsselungs-Leitfaden: Konfiguration externer Verschlüsselungsmanagement"

Replizierung von Daten zwischen Systemen

Sie können Daten zwischen Arbeitsumgebungen replizieren, indem Sie eine einmalige Datenreplizierung für die Datenübertragung oder einen wiederkehrenden Zeitplan für Disaster Recovery oder langfristige Aufbewahrung wählen. Sie können beispielsweise die Datenreplizierung eines lokalen ONTAP-Systems auf Cloud Volumes ONTAP für Disaster Recovery einrichten.

Cloud Manager vereinfacht die Datenreplizierung zwischen Volumes auf separaten Systemen mithilfe von SnapMirror und SnapVault Technologien. Sie müssen lediglich das Quell-Volume und das Ziel-Volume identifizieren und dann eine Replizierungsrichtlinie und einen Zeitplan auswählen. Cloud Manager erwirbt die erforderlichen Festplatten, konfiguriert Beziehungen, wendet die Replizierungsrichtlinie an und initiiert dann den Basistransfer zwischen Volumes.

Die Basisplanübertragung enthält eine vollständige Kopie der Quelldaten. Nachfolgende Übertragungen enthalten differenzielle Kopien der Quelldaten.

Cloud Manager ermöglicht Datenreplizierung zwischen den folgenden Arbeitsumgebungen:

- Von einem Cloud Volumes ONTAP System zu einem anderen Cloud Volumes ONTAP System
- Zwischen einem Cloud Volumes ONTAP System und einem ONTAP-Cluster vor Ort
- Von einem ONTAP-Cluster vor Ort zu einem anderen ONTAP-Cluster vor Ort

Anforderungen an die Datenreplizierung

Bevor Sie Daten replizieren können, sollten Sie sicherstellen, dass sowohl für Cloud Volumes ONTAP Systeme als auch für ONTAP Cluster spezifische Anforderungen erfüllt sind.

Versionsanforderungen

Sie sollten überprüfen, ob die Quell- und Ziel-Volumes kompatible ONTAP Versionen ausführen, bevor Sie Daten replizieren. Weitere Informationen finden Sie im "Data Protection Power Guide".

Spezifische Anforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen ein- und ausgehenden Regeln enthalten: Speziell Regeln für ICMP und die Ports 11104 und 11105.

  Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.

- Um Daten zwischen zwei Cloud Volumes ONTAP Systemen in verschiedenen Subnetzen zu replizieren, müssen die Subnetze gemeinsam geroutet werden (dies ist die Standardeinstellung).
- Um Daten zwischen einem Cloud Volumes ONTAP System in AWS und einem System in Azure zu replizieren, müssen Sie über eine VPN-Verbindung zwischen AWS VPC und Azure VNet verfügen.

Spezifische Anforderungen für ONTAP Cluster

- Eine aktive SnapMirror Lizenz muss installiert sein.

- Wenn sich das Cluster in Ihrem Betrieb befindet, sollten Sie eine Verbindung von Ihrem Unternehmensnetzwerk zu AWS oder Azure haben, bei der es sich in der Regel um eine VPN-Verbindung handelt.
- ONTAP Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Cluster-Anforderungen erfüllen.

  Weitere Informationen finden Sie im Cluster and SVM Peering Express Guide für Ihre Version von ONTAP.

Datenreplikation zwischen Systemen einrichten

Sie können Daten zwischen Cloud Volumes ONTAP Systemen und ONTAP Clustern replizieren, indem Sie sich für eine einmalige Datenreplizierung entscheiden, mit der Sie Daten in die und aus der Cloud verschieben können, oder für einen wiederkehrenden Zeitplan, der zur Disaster Recovery oder langfristigen Aufbewahrung beitragen kann.

Über diese Aufgabe

Cloud Manager unterstützt einfache, fanout- und kaskadierende Datensicherungskonfigurationen:

- In einer einfachen Konfiguration erfolgt die Replizierung von Volume A auf Volume B.
- In einer Fanout-Konfiguration erfolgt die Replizierung von Volume A zu mehreren Zielen.
- Bei einer kaskadierten Konfiguration erfolgt die Replizierung von Volume A auf Volume B und von Volume B auf Volume C.

Sie können Fanout- und Kaskadenkonfigurationen in Cloud Manager konfigurieren, indem Sie mehrere Datenreplizierungen zwischen Systemen einrichten. Zum Beispiel durch Replizierung eines Volumes von System A auf System B und anschließendes Replizieren desselben Volumes von System B auf System C.

Schritte

1. Wählen Sie auf der Seite Arbeitsumgebungen die Arbeitsumgebung aus, die das Quell-Volume enthält, und ziehen Sie es in die Arbeitsumgebung, in die Sie das Volume replizieren möchten:

2. Wenn die Setup-Seiten für Quell- und Zielpeering angezeigt werden, wählen Sie alle Intercluster-LIFs für die Cluster-Peer-Beziehung aus.

   Das Cluster-übergreifende Netzwerk sollte so konfiguriert werden, dass Cluster-Peers *paarweise vollständige Mesh-Konnektivität* haben. Das bedeutet, dass jedes Cluster-Paar in einer Cluster-Peer-Beziehung über Konnektivität zwischen allen Intercluster LIFs verfügt.

   Diese Seiten werden angezeigt, wenn ein ONTAP Cluster mit mehreren LIFs Quelle oder Ziel ist.

3. Wählen Sie auf der Seite Quellvolumenauswahl das Volume aus, das Sie replizieren möchten.

4. Geben Sie auf der Seite Name und Tiering des Zieldatenträgers den Namen des Zieldatenträgers an, wählen Sie einen zugrunde liegenden Laufwerkstyp aus, ändern Sie eine der erweiterten Optionen, und klicken Sie dann auf **Weiter**.

   Wenn das Ziel ein ONTAP Cluster ist, müssen Sie auch das Ziel-SVM und das Aggregat angeben.

5. Geben Sie auf der Seite Max. Übertragungsrate die maximale Rate (in Megabyte pro Sekunde) an, mit der Daten übertragen werden können.
6. Wählen Sie auf der Seite Replikationsrichtlinie eine der Standardrichtlinien aus, oder klicken Sie auf **zusätzliche Richtlinien**, und wählen Sie dann eine der erweiterten Richtlinien aus.

   Hilfe finden Sie unter "Auswählen einer Replizierungsrichtlinie".

   Wenn Sie eine benutzerdefinierte Backup- (SnapVault-) Policy wählen, müssen die mit der Policy verknüpften Labels mit den Labels der Snapshot Kopien auf dem Quell-Volume übereinstimmen. Weitere Informationen finden Sie unter "Funktionsweise von Backup-Richtlinien".

7. Wählen Sie auf der Seite Zeitplan eine einmalige Kopie oder einen wiederkehrenden Zeitplan aus.

   Es stehen mehrere Standardzeitpläne zur Verfügung. Wenn Sie einen anderen Zeitplan möchten, müssen Sie mithilfe von System Manager einen neuen Zeitplan auf dem Cluster *Destination* erstellen.

8. Überprüfen Sie auf der Seite „Prüfen“ Ihre Auswahl und klicken Sie dann auf **Los**.

Ergebnis

Cloud Manager startet den Datenreplizierungsprozess. Details zur Replikation können Sie auf der Seite "Replication Status" anzeigen.

Managen von Plänen und Beziehungen zur Datenreplizierung

Nachdem Sie die Datenreplizierung zwischen zwei Systemen eingerichtet haben, können Sie den Zeitplan und die Beziehung für die Datenreplizierung über Cloud Manager managen.

Schritte

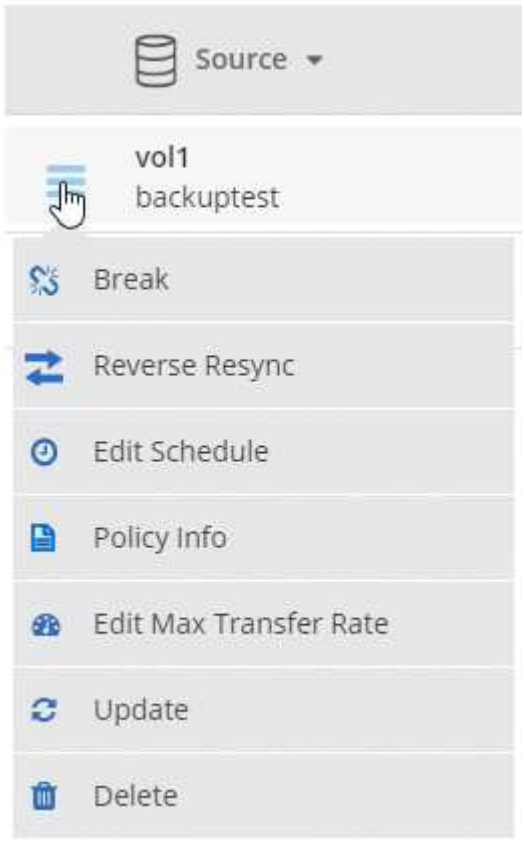
1. Zeigen Sie auf der Seite Arbeitsumgebungen den Replikationsstatus für alle Arbeitsumgebungen im Arbeitsbereich oder für eine bestimmte Arbeitsumgebung an:

Option	Aktion
Alle Arbeitsumgebungen im Arbeitsbereich	Klicken Sie oben im Cloud Manager auf **Replikation**.
Eine bestimmte Arbeitsumgebung	Öffnen Sie die Arbeitsumgebung und klicken Sie auf **Replikationen**.

2. Überprüfen Sie den Status der Datenreplizierungsbeziehungen, um sicherzustellen, dass sie in Ordnung sind.

Wenn der Status einer Beziehung inaktiv ist und der Spiegelungsstatus nicht initialisiert ist, müssen Sie die Beziehung vom Zielsystem initialisieren, damit die Datenreplizierung gemäß dem definierten Zeitplan ausgeführt werden kann. Sie können die Beziehung mit System Manager oder der Befehlszeilenschnittstelle (CLI) initialisieren. Diese Zustände können angezeigt werden, wenn das Zielsystem ausfällt und dann wieder online geht.

3. Wählen Sie das Menüsymbol neben dem Quellvolume und anschließend eine der verfügbaren Aktionen aus.



Die folgende Tabelle beschreibt die verfügbaren Aktionen:

Aktion	Beschreibung
Pause	Bricht die Beziehung zwischen Quell- und Ziel-Volumes und aktiviert das Ziel-Volume für den Datenzugriff. Diese Option wird in der Regel verwendet, wenn das Quell-Volume aufgrund von Ereignissen wie Datenbeschädigung, versehentlichem Löschen oder einem Offline-Status keine Daten bereitstellen kann. Informationen zum Konfigurieren eines Ziel-Volumes für den Datenzugriff und zur Reaktivierung eines Quell-Volumes finden Sie im ONTAP 9 Volume Disaster Recovery Express Guide.

Aktion	Beschreibung
Neu synchronisieren	Stellt eine unterbrochene Beziehung zwischen Volumes wieder her und setzt die Datenreplizierung gemäß dem definierten Zeitplan fort. Wenn Sie die Volumes erneut synchronisieren, werden die Inhalte auf dem Ziel-Volume durch die Inhalte auf dem Quell-Volume überschrieben. Informationen zur Neusynchronisierung, die die Daten vom Ziel-Volume zum Quell-Volume neu synchronisiert, finden Sie im "ONTAP 9 Express Guide für die Disaster Recovery von Volumes".
Reverse Resync	Kehrt die Rollen der Quell- und Ziel-Volumes um. Der Inhalt des ursprünglichen Quell-Volumes wird durch den Inhalt des Ziel-Volumes überschrieben. Dies ist hilfreich, wenn Sie ein Quell-Volume, das offline gegangen ist, reaktivieren möchten. Alle Daten, die zwischen der letzten Datenreplizierung und dem Zeitpunkt, zu dem das Quell-Volume deaktiviert wurde, auf das ursprüngliche Quell-Volume geschrieben wurden, bleiben nicht erhalten.
Zeitplan bearbeiten	Ermöglicht die Auswahl eines anderen Zeitplans für die Datenreplizierung.
Richtlinieninformationen	Zeigt die der Datenreplizierungsbeziehung zugewiesene Schutzrichtlinie an.
Max. Übertragungsrate bearbeiten	Hier können Sie die maximale Rate (in Kilobyte pro Sekunde) bearbeiten, mit der Daten übertragen werden können.
Aktualisierung	Startet einen inkrementellen Transfer, um das Zielvolume zu aktualisieren.
Löschen	Löscht die Data-Protection-Beziehung zwischen Quell- und Ziel-Volumes, d. H., die Datenreplizierung findet nicht mehr zwischen den Volumes statt. Durch diese Aktion wird das Ziel-Volume nicht für den Datenzugriff aktiviert. Durch diese Aktion werden auch die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung (Storage Virtual Machine) gelöscht, wenn keine anderen Data-Protection-Beziehungen zwischen den Systemen bestehen.

Ergebnis

Nachdem Sie eine Aktion ausgewählt haben, aktualisiert Cloud Manager die Beziehung oder den Zeitplan.

Auswählen einer Replizierungsrichtlinie

Möglicherweise benötigen Sie Hilfe bei der Auswahl einer Replizierungsrichtlinie, wenn Sie die Datenreplizierung in Cloud Manager einrichten. Eine Replizierungsrichtlinie definiert, wie das Storage-System Daten von einem Quell-Volume auf ein Ziel-Volume repliziert.

Was sind Replizierungsrichtlinien

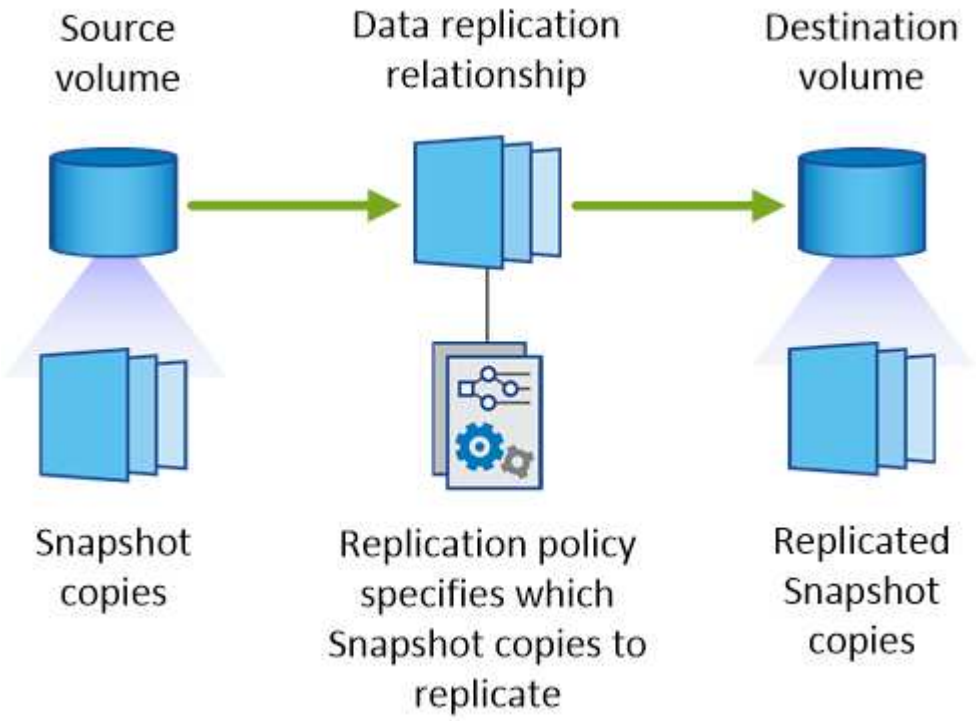
Das Betriebssystem ONTAP erstellt automatisch Backups mit dem Namen Snapshot Kopien. Eine Snapshot Kopie ist ein schreibgeschütztes Image eines Volumes, das den Status des Dateisystems zu einem bestimmten Zeitpunkt erfasst.

Wenn Sie Daten zwischen Systemen replizieren, replizieren Sie Snapshot Kopien von einem Quell-Volume zu einem Ziel-Volume. Eine Replizierungsrichtlinie gibt an, welche Snapshot Kopien vom Quell-Volume auf das

Ziel-Volume repliziert werden sollen.

Replizierungsrichtlinien werden auch als *Protection* -Richtlinien bezeichnet, da sie durch SnapMirror und SnapVault Technologien unterstützt werden, die Disaster Recovery-Schutz und Disk-to-Disk Backup und Recovery bieten.

Die folgende Abbildung zeigt die Beziehung zwischen Snapshot Kopien und Replizierungsrichtlinien:



Arten von Replizierungsrichtlinien

Es gibt drei Arten von Replizierungsrichtlinien:

- Eine *Mirror* Richtlinie repliziert neu erstellte Snapshot Kopien zu einem Ziel-Volume.

  Sie können diese Snapshot Kopien verwenden, um das Quell-Volume als Vorbereitung für die Disaster Recovery oder für die einmalige Datenreplizierung zu schützen. Sie können das Ziel-Volume jederzeit für den Datenzugriff aktivieren.

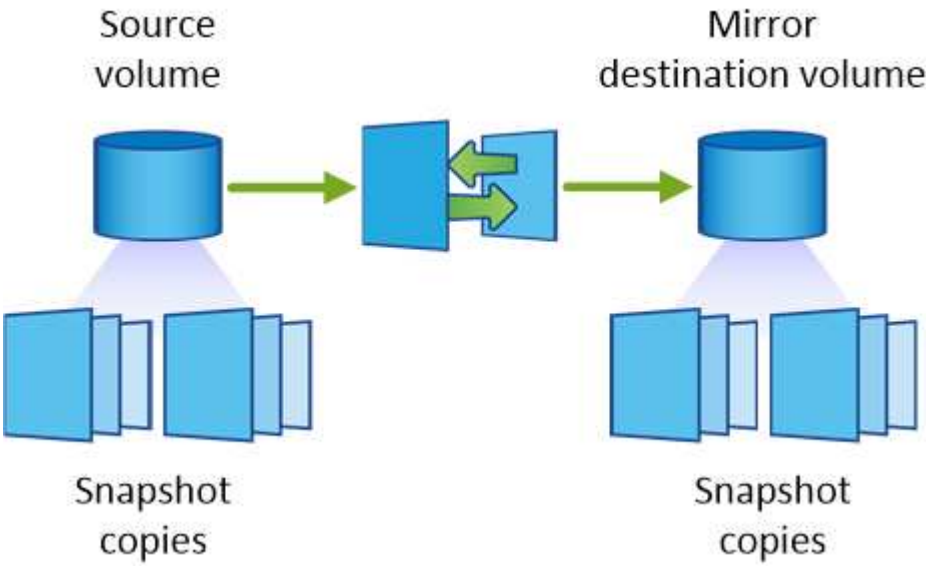
- Eine *Backup*-Richtlinie repliziert bestimmte Snapshot-Kopien zu einem Ziel-Volume und speichert diese in der Regel für einen längeren Zeitraum, als es auf dem Quell-Volume der Fall wäre.

  Sie können Daten aus diesen Snapshot Kopien wiederherstellen, wenn Daten beschädigt oder verloren gehen, und sie zur Einhaltung von Standards und zu anderen Governance-Zwecken aufbewahren.

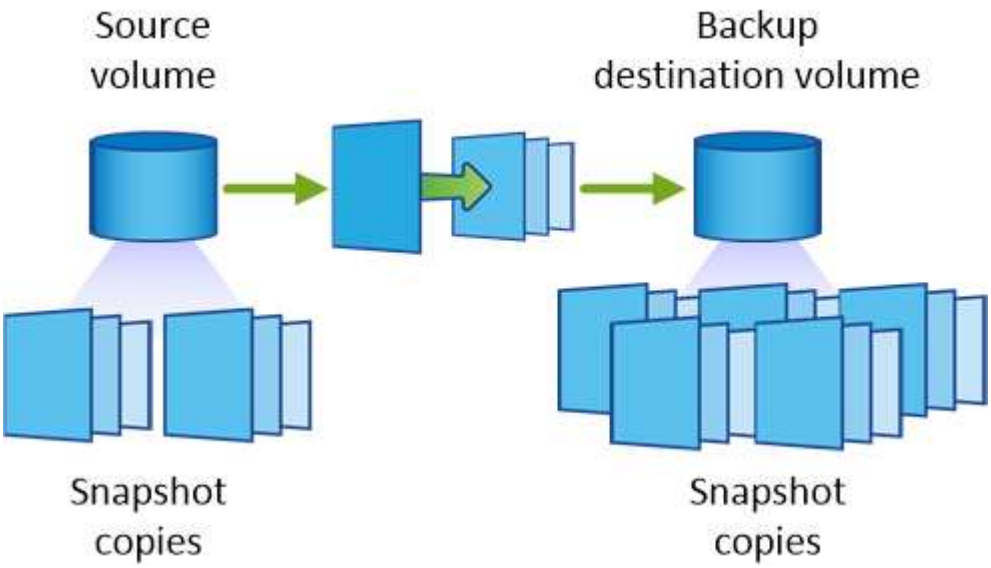
- Eine Richtlinie „ *Mirror und Backup*“ ermöglicht Disaster Recovery und langfristige Datenhaltung.

  Jedes System verfügt über eine standardmäßige Mirror- und Backup-Policy, die in vielen Situationen gut funktioniert. Wenn Sie benutzerdefinierte Richtlinien benötigen, können Sie mit System Manager eigene Richtlinien erstellen.

Die folgenden Abbildungen zeigen den Unterschied zwischen den Richtlinien für Spiegelung und Sicherung. Eine Spiegelungsrichtlinie spiegelt die auf dem Quell-Volume verfügbaren Snapshot Kopien wider.



Eine Backup-Policy behält Snapshot-Kopien in der Regel länger bei, als sie auf dem Quell-Volume aufbewahrt werden:



Funktionsweise von Backup-Richtlinien

Im Gegensatz zu Spiegelungsrichtlinien replizieren Backup-Richtlinien (SnapVault) bestimmte Snapshot Kopien auf ein Ziel-Volume. Es ist wichtig zu verstehen, wie Backup-Richtlinien funktionieren, wenn Sie Ihre eigenen Richtlinien anstelle der Standardrichtlinien verwenden möchten.

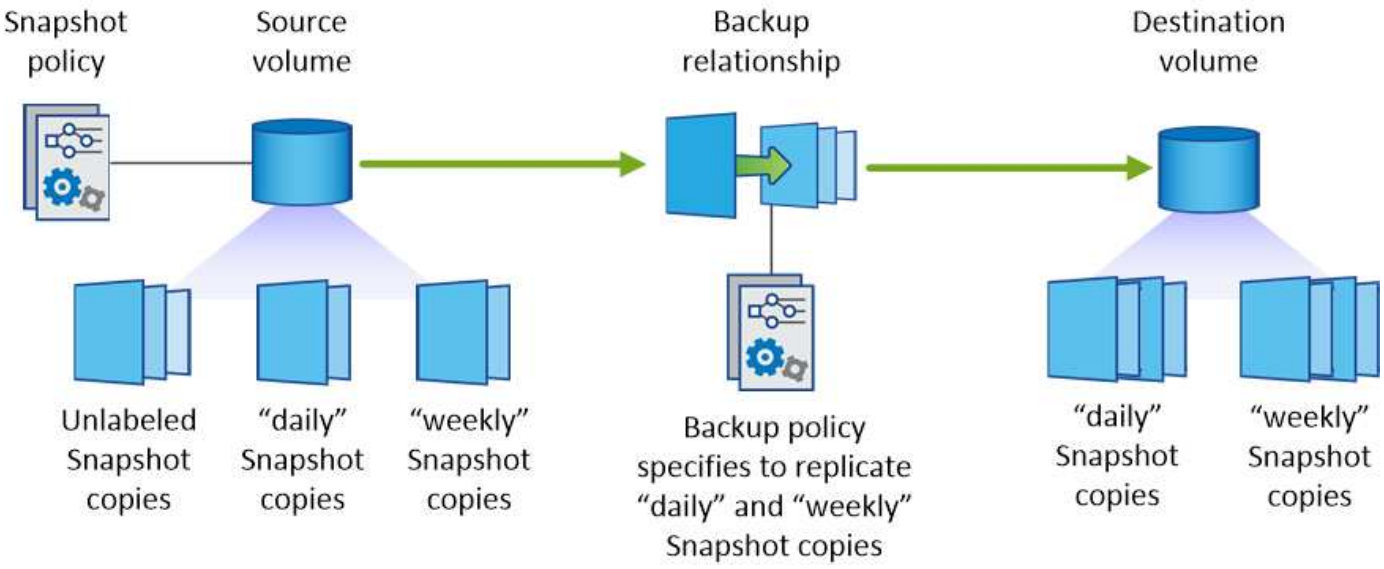
Verständnis der Beziehung zwischen Snapshot Copy Labels und Backup-Richtlinien

Eine Snapshot-Richtlinie definiert, wie das System Snapshot-Kopien von Volumes erstellt. Die Richtlinie gibt an, wann die Snapshot Kopien erstellt werden sollen, wie viele Kopien aufbewahrt werden sollen und wie sie beschriften werden. Ein System erstellt beispielsweise jeden Tag um 12:10 Uhr eine Snapshot Kopie, behält die beiden neuesten Kopien bei und kennzeichnet sie "täglich".

Eine Backup-Richtlinie enthält Regeln, die festlegen, welche benannten Snapshot Kopien auf ein Ziel-Volume repliziert werden sollen und wie viele Kopien aufbewahrt werden sollen. Die in einer Backup-Richtlinie definierten Bezeichnungen müssen mit einer oder mehreren Bezeichnungen übereinstimmen, die in einer

Snapshot-Richtlinie definiert sind. Andernfalls kann das System keine Snapshot Kopien replizieren.

Eine Backup-Policy, die beispielsweise die Bezeichnungen "täglich" und "wöchentlich" enthält, führt zur Replizierung von Snapshot Kopien, die nur diese Bezeichnungen enthalten. Es werden keine anderen Snapshot Kopien repliziert, wie im folgenden Bild dargestellt:



Standardrichtlinien und benutzerdefinierte Richtlinien

Die Standard-Snapshot-Richtlinie erstellt stündlich, täglich und wöchentlich Snapshot Kopien, wobei sechs Stunden, zwei Tage und zwei wöchentliche Snapshot Kopien aufbewahrt werden.

Sie können problemlos eine Standard-Backup-Richtlinie mit der Standard-Snapshot-Richtlinie verwenden. Die Standard-Backup-Richtlinien replizieren tägliche und wöchentliche Snapshot Kopien, wobei sieben tägliche und 52 wöchentliche Snapshot Kopien aufbewahrt werden.

Wenn Sie benutzerdefinierte Richtlinien erstellen, müssen die durch diese Richtlinien definierten Bezeichnungen übereinstimmen. Sie können benutzerdefinierte Richtlinien mit System Manager erstellen.

Datenreplizierung von NetApp HCI auf Cloud Volumes ONTAP

Wenn Sie versuchen, Daten von NetApp HCI zu Cloud Volumes ONTAP zu replizieren, können Sie dies auf einem NetApp HCI System tun, auf dem NetApp Element Software mit SnapMirror läuft. Alternativ können Sie Daten auf Volumes replizieren, die auf einem ONTAP Select System erstellt wurden, das als virtueller Gast in einer NetApp HCI Lösung ausgeführt wird, auf Cloud Volumes ONTAP.

Details finden Sie in den folgenden technischen Berichten:

- "Technischer Bericht 4641: NetApp HCI Datensicherung"
- "Technischer Bericht 4651: NetApp SolidFire SnapMirror Architektur und Konfiguration"

Monitoring der Performance

Erfahren Sie mehr über den Monitoring-Service

Durch die Nutzung der "NetApp Cloud Insights Service", Cloud Manager liefert Einblicke

in den Zustand und die Performance Ihrer Cloud Volumes ONTAP Instanzen und unterstützt Sie bei der Fehlerbehebung und Optimierung der Performance Ihrer Cloud-Storage-Umgebung.

Funktionen

- Automatische Überwachung aller Volumes
- Anzeige von Volume-Performance-Daten in Bezug auf IOPS, Durchsatz und Latenz
- Identifizieren von Performance-Problemen, um die Auswirkungen auf Benutzer und Applikationen zu minimieren

Unterstützte Cloud-Provider

Der Monitoring-Service wird mit Cloud Volumes ONTAP für AWS unterstützt.

Kosten

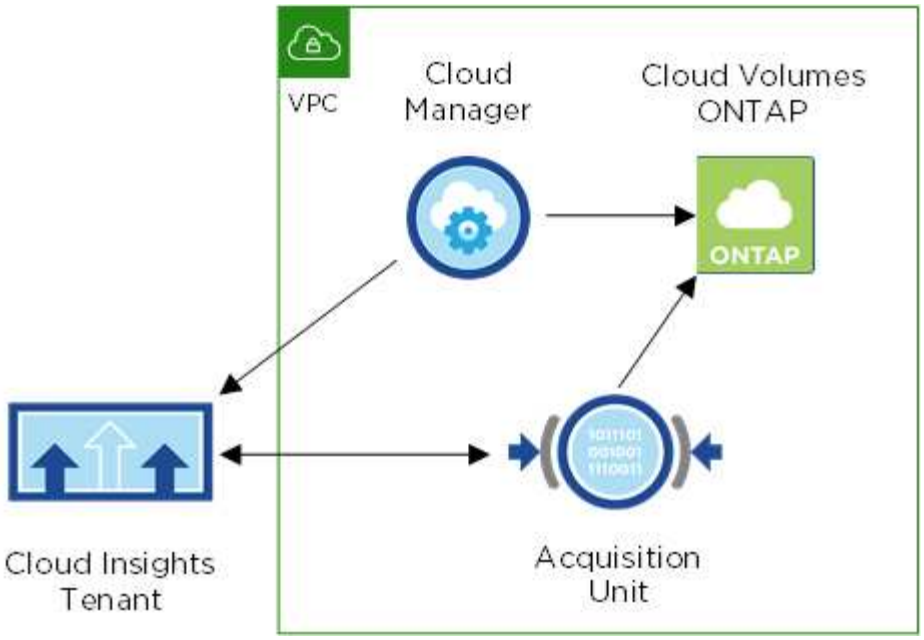
Die Überwachung ist derzeit als Vorschau verfügbar. Die Aktivierung ist zwar kostenlos, aber Cloud Manager startet eine Virtual Machine in der VPC, um die Überwachung zu erleichtern. Diese VM verursacht Gebühren von Ihrem Cloud-Provider.

Funktionsweise von Cloud Insights mit Cloud Manager

Die Cloud Insights Integration auf höherer Ebene in Cloud Manager funktioniert folgendermaßen:

1. Sie aktivieren den Überwachungsdienst auf Cloud Volumes ONTAP.
2. Cloud Manager konfiguriert Ihre Umgebung. Er führt folgende Maßnahmen durch:
    a. Erstellt einen Cloud Insights-Mandanten (auch „*Environment*“ genannt) und ordnet alle Benutzer in Ihrem Cloud Central-Konto dem Mandanten zu.
    b. Cloud Insights: 30 Tage kostenlos testen
    c. Implementiert eine Virtual Machine in der VPC, der als „Acquisition Unit“ bezeichnet wird, die das Monitoring von Volumes erleichtert (dies ist die VM, die im Abschnitt „Kosten“ oben erwähnt ist).
    d. Verbindet die Akquisitionseinheit mit Cloud Volumes ONTAP und mit dem Cloud Insights-Mandanten.
3. In Cloud Manager klicken Sie auf Monitoring und verwenden die Performance-Daten, um Fehler zu beheben und die Performance zu optimieren.

Die Beziehung zwischen diesen Komponenten wird in der folgenden Abbildung dargestellt:



Die Akquisitionseinheit

Wenn Sie Monitoring aktivieren, implementiert Cloud Manager eine Erfassungseinheit im selben Subnetz wie der Connector.

Eine *Acquisition Unit* sammelt Performancedaten von Cloud Volumes ONTAP und sendet sie an den Cloud Insights-Mandanten. Cloud Manager fragt diese Daten ab und stellt sie Ihnen zur Verfügung.

Beachten Sie Folgendes über die Instanz der Erfassungseinheit:

- Die Erfassungseinheit wird auf einer instanz mit t3.xlarge mit einem GP2-Volumen von 100 GB ausgeführt.
- Die Instanz heißt *AcquitionUnit* mit einem generierten Hash (UUID), der mit ihm verknüpft ist. Beispiel: *AcquitionUnit-FAN7FqeH*
- Pro Connector wird nur eine Akquisitionseinheit bereitgestellt.
- Die Instanz muss ausgeführt werden, um auf Leistungsinformationen auf der Registerkarte Überwachung zuzugreifen.

Cloud Insights-Mandant

Cloud Manager richtet bei der Aktivierung von Monitoring einen *Tenant* ein. Ein Cloud Insights-Mandant ermöglicht Ihnen den Zugriff auf die Leistungsdaten, die die Acquisition Unit sammelt. Der Mandant ist eine sichere Datenpartition innerhalb des NetApp Cloud Insights Service.

Cloud Insights Webschnittstelle

Die Registerkarte „Monitoring“ in Cloud Manager bietet grundlegende Performance-Daten für die Volumes. Über die Cloud Insights Weboberfläche können Sie in Ihrem Browser eine detailliertere Überwachung durchführen und Warnmeldungen für Ihre Cloud Volumes ONTAP Systeme konfigurieren.

Kostenlose Testversion und Abonnement

Cloud Manager ermöglicht eine kostenlose 30-Tage-Testversion von Cloud Insights zur Bereitstellung von Performance-Daten innerhalb von Cloud Manager. Sie können sich mit den Funktionen der Cloud Insights Standard Edition beschäftigen.

Sie müssen sich bis zum Ende der kostenlosen Testversion anmelden, anderenfalls wird Ihr Cloud Insights Mandant endgültig gelöscht. Sie können die Basic-, Standard- oder Premium-Edition abonnieren, um die Monitoring-Funktion in Cloud Manager fortzusetzen.

"Erfahren Sie, wie Sie Cloud Insights abonnieren".

Monitoring von Cloud Volumes ONTAP in AWS

Führen Sie einige Schritte durch, um mit der Überwachung der Cloud Volumes ONTAP-Performance zu beginnen.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

Überprüfen Sie die Unterstützung Ihrer Konfiguration

Sie benötigen eine Neuinstallation von Cloud Manager 3.8.4 oder höher in AWS, Cloud Volumes ONTAP in AWS und als neuer Cloud Insights Kunde.

Aktivieren Sie die Überwachung auf Ihrem neuen oder vorhandenen System

- Neue Arbeitsumgebungen: Achten Sie darauf, Monitoring aktiviert zu halten, wenn Sie die Arbeitsumgebung erstellen (es ist standardmäßig aktiviert).
- Bestehende Arbeitsumgebungen: Wählen Sie eine Arbeitsumgebung und klicken Sie auf **Monitoring starten**.

Anzeigen von Performance-Daten

Klicken Sie auf **Monitoring** und zeigen Sie Leistungsdaten für Ihre Volumes an.

Abonnieren Sie Cloud Insights

Wenn Sie sich für eine kostenlose 30-Tage-Testversion anmelden, werden auch weiterhin Performance-Daten in Cloud Manager und Cloud Insights gespeichert. "Erfahren Sie, wie Sie abonniert werden können".

Anforderungen

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen.

Unterstützte Cloud Manager Versionen

Sie benötigen eine neue Installation von Cloud Manager 3.8.4 oder höher. Es ist eine neue Installation erforderlich, weil für den Monitoring-Service eine neue Infrastruktur erforderlich ist. Die Infrastruktur ist bei Neuinstallationen von Cloud Manager 3.8 verfügbar 4.

Unterstützte Cloud Volumes ONTAP-Versionen

Jede Version von Cloud Volumes ONTAP in AWS.

Cloud Insights-Anforderungen

Sie müssen ein neuer Cloud Insights Kunde sein. Die Überwachung wird nicht unterstützt, wenn Sie bereits über einen Cloud Insights-Mandanten verfügen.

E-Mail-Adresse für Cloud Central

Die E-Mail-Adresse für Ihr Cloud Central-Benutzerkonto sollte Ihre geschäftliche E-Mail-Adresse sein. Kostenlose E-Mail-Domains wie gmail und Hotmail werden bei der Erstellung eines Cloud Insights-Mandanten nicht unterstützt.

Netzwerk für die Akquisitionseinheit

Die Akquisitionseinheit verwendet eine 2-Wege-/gegenseitige Authentifizierung, um eine Verbindung zum Cloud Insights-Server herzustellen. Das Clientzertifikat muss an den Cloud Insights-Server zur Authentifizierung übergeben werden. Dazu muss der Proxy eingerichtet werden, um die HTTP-Anforderung an den Cloud Insights-Server weiterzuleiten, ohne die Daten zu entschlüsseln.

Die Erfassungseinheit verwendet die folgenden beiden Endpunkte, um mit Cloud Insights zu kommunizieren. Wenn Sie eine Firewall zwischen dem Erfassungs- und dem Cloud Insights-Server besitzen, benötigen Sie diese Endpunkte, wenn Sie Firewall-Regeln konfigurieren:

```
https://aulogin.<Cloud Insights Domain>
https://<your-tenant-ID>.<Cloud Insights Domain>
```

Beispiel:

```
https://aulogin.c01.cloudinsights.netapp.com
https://cg0c586a-ee05-45rb-a5ac-
333b5ae7718d7.c01.cloudinsights.netapp.com
```

Kontaktieren Sie uns über den Chat in Product, wenn Sie Hilfe bei der Identifizierung Ihrer Cloud Insights-Domain und Mandanten-ID benötigen.

Vernetzung für den Connector

Ähnlich wie die Erfassungseinheit muss der Connector über eine ausgehende Verbindung zum Cloud Insights-Mandanten verfügen. Aber der Endpunkt, den der Connector kontaktiert, ist etwas anders. Die Mandantenhost-URL wird über die verkürzte Mandanten-ID kontaktiert:

```
 https://<your-short-tenant-ID>.<Cloud Insights Domain>
Beispiel:
```

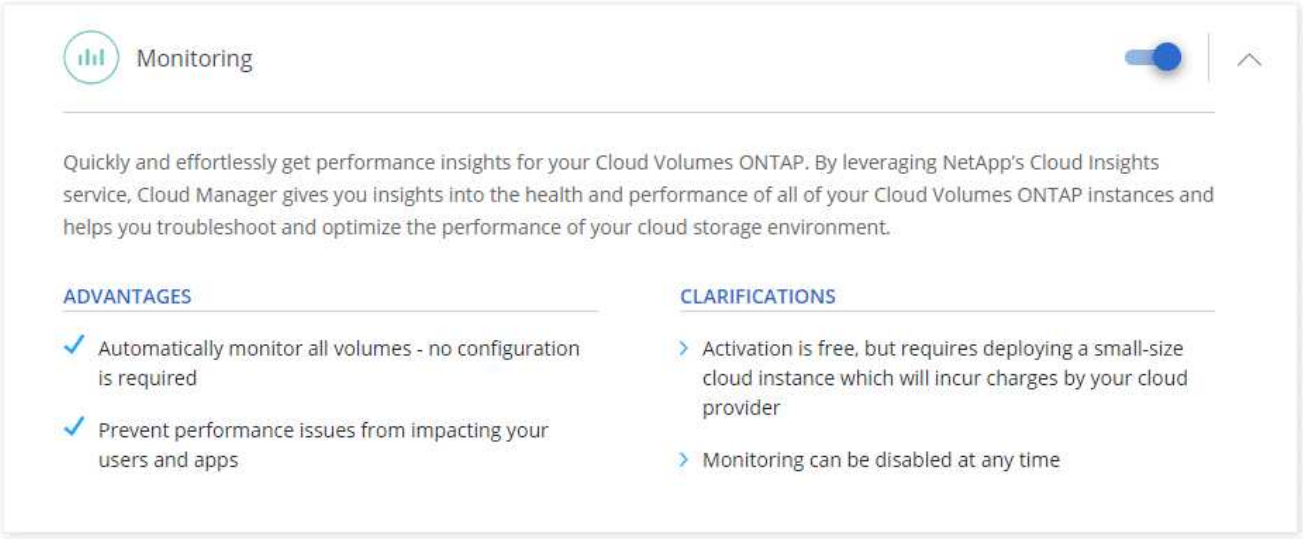
```
 https://abcd12345.c01.cloudinsights.netapp.com
Auch hier können Sie uns über den Produkt-Chat kontaktieren, wenn Sie
Hilfe bei der Ermittlung der Mandanten-Host-URL benötigen.
```

Aktivieren der Überwachung auf einem neuen System

Der Überwachungsdienst ist standardmäßig im Assistenten für die Arbeitsumgebung aktiviert. Achten Sie darauf, dass die Option aktiviert bleibt.

Schritte

1. Klicken Sie auf **Cloud Volumes ONTAP erstellen**.
2. Wählen Sie Amazon Web Services als Cloud-Provider und wählen Sie dann einen einzelnen Node oder ein HA-System.
3. Füllen Sie die Seite „Details & Credentials“ aus.
4. Lassen Sie auf der Seite Dienste den Dienst aktiviert, und klicken Sie auf **Weiter**.

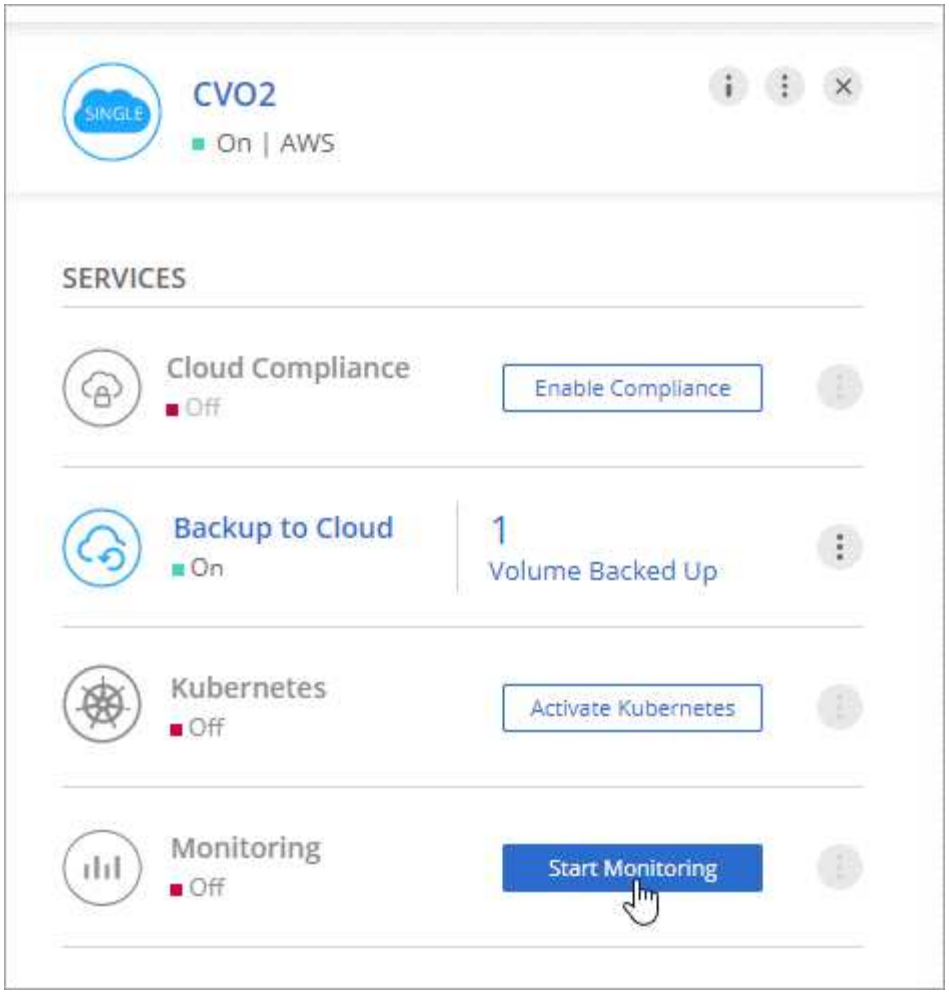


Aktivieren der Überwachung auf einem vorhandenen System

Ermöglichen Sie jederzeit die Überwachung aus der Arbeitsumgebung.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Arbeitsumgebungen**.
2. Wählen Sie eine Arbeitsumgebung aus.
3. Klicken Sie im rechten Fensterbereich auf **Überwachung starten**.



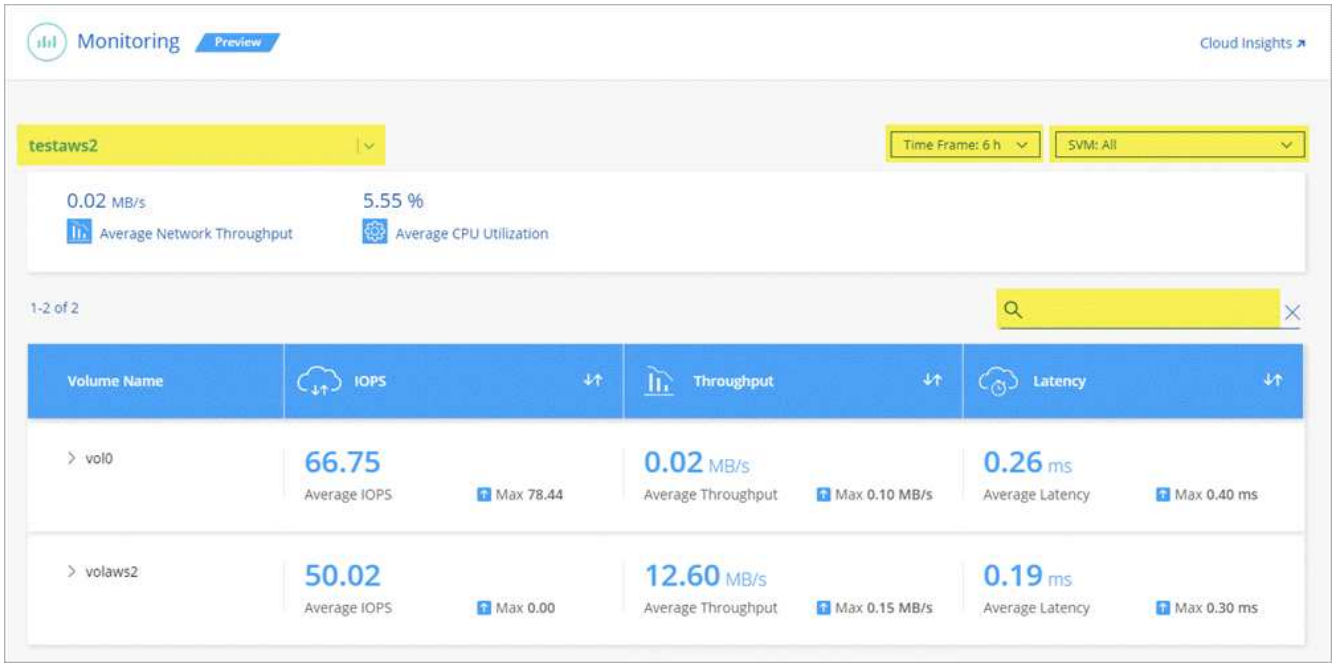
Monitoring Ihrer Volumes

Monitoring der Performance durch IOPS, Durchsatz und Latenz für jedes der Volumes

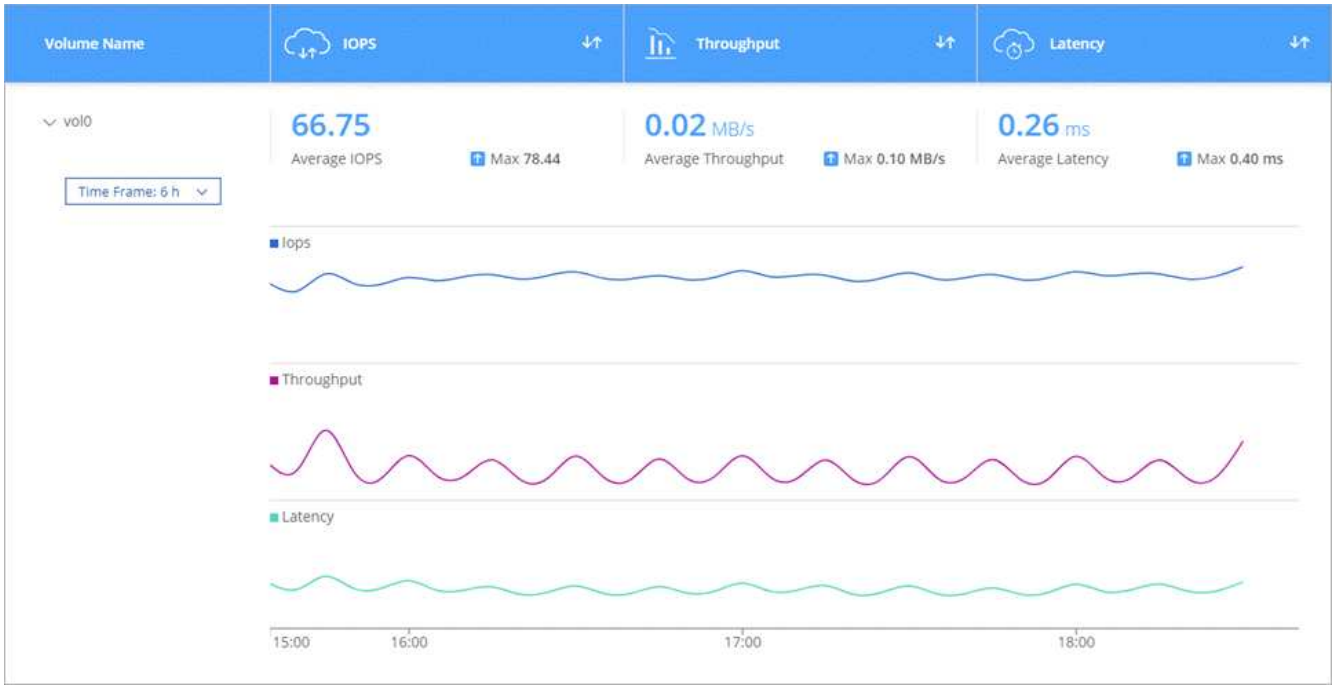
Schritte

1. Klicken Sie oben im Cloud Manager auf **Überwachung**.
2. Filtern Sie den Inhalt des Dashboards, um die gewünschten Informationen abzurufen.
    - Wählen Sie eine bestimmte Arbeitsumgebung aus.
    - Wählen Sie einen anderen Zeitrahmen aus.
    - Wählen Sie eine bestimmte SVM aus.
    - Suchen Sie nach einem bestimmten Volume.

    Die folgende Abbildung zeigt jede dieser Optionen:



3. Klicken Sie in der Tabelle auf ein Volume, um die Zeile zu erweitern und einen Zeitplan für IOPS, Durchsatz und Latenz anzuzeigen.



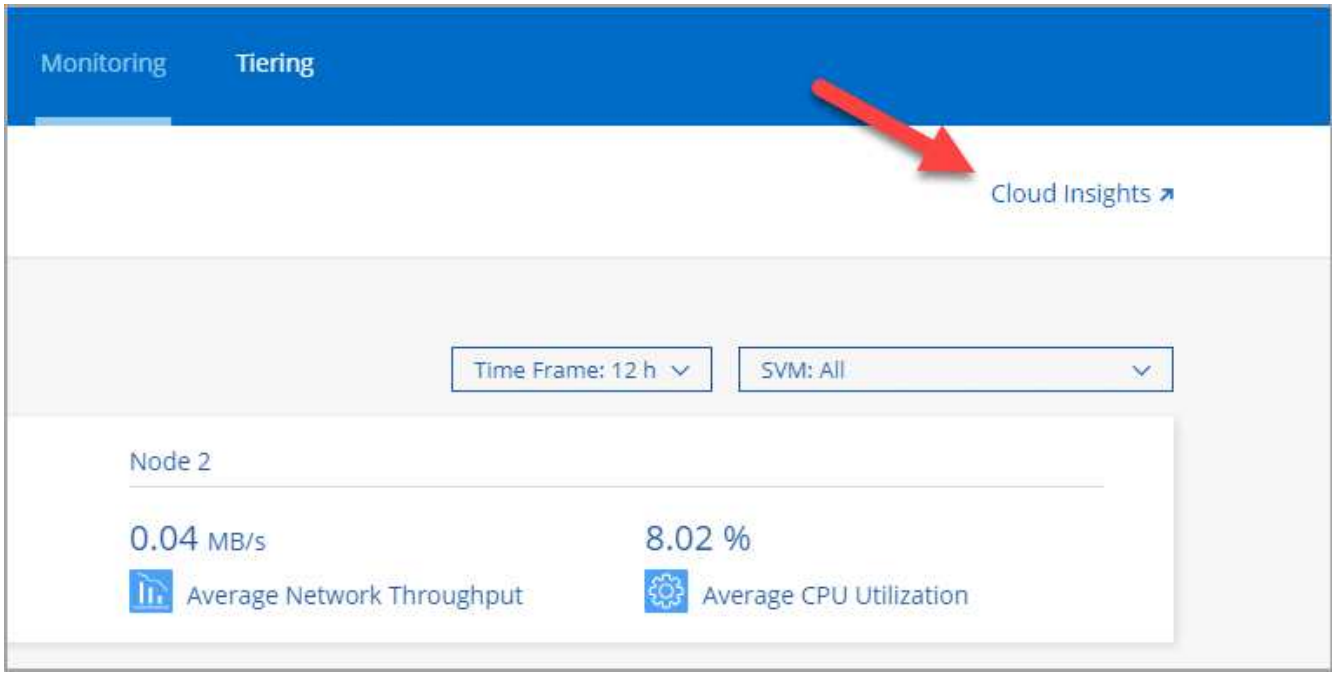
4. Ermitteln Sie mithilfe der Daten Performance-Probleme, um die Auswirkungen auf Benutzer und Applikationen zu minimieren.

Weitere Informationen von Cloud Insights

Die Registerkarte „Monitoring“ in Cloud Manager bietet grundlegende Performance-Daten für die Volumes. Über die Cloud Insights Weboberfläche können Sie in Ihrem Browser eine detailliertere Überwachung durchführen und Warnmeldungen für Ihre Cloud Volumes ONTAP Systeme konfigurieren.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Überwachung**.
2. Klicken Sie auf den Link **Cloud Insights**.



Ergebnis

Cloud Insights in einer neuen Browser-Registerkarte öffnen. Wenn Sie Hilfe benötigen, lesen Sie den "Cloud Insights-Dokumentation".

Überwachung wird deaktiviert

Wenn Sie Cloud Volumes ONTAP nicht mehr überwachen möchten, können Sie den Dienst jederzeit deaktivieren.

Wenn Sie das Monitoring in jeder Ihrer Arbeitsumgebungen deaktivieren, müssen Sie die EC2-Instanz selbst löschen. Die Instanz heißt *AcquitionUnit* mit einem generierten Hash (UUID), der mit ihm verknüpft ist. Beispiel: *AcquitionUnit-FAN7FqeH*

Schritte

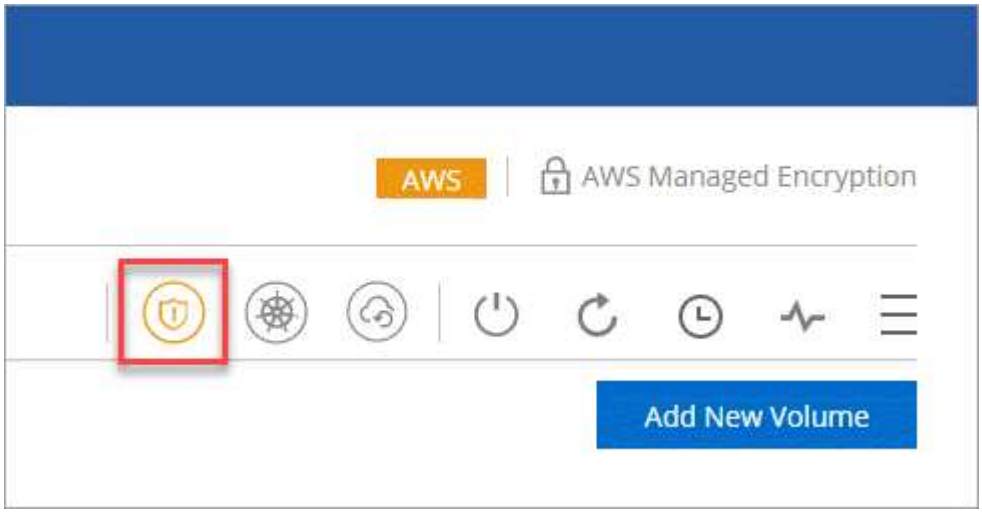
1. Klicken Sie oben im Cloud Manager auf **Arbeitsumgebungen**.
2. Wählen Sie eine Arbeitsumgebung aus.
3. Klicken Sie im rechten Fensterbereich auf das Symbol und wählen Sie **Scan deaktivieren**.

Besserer Schutz gegen 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.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Symbol **Ransomware**.

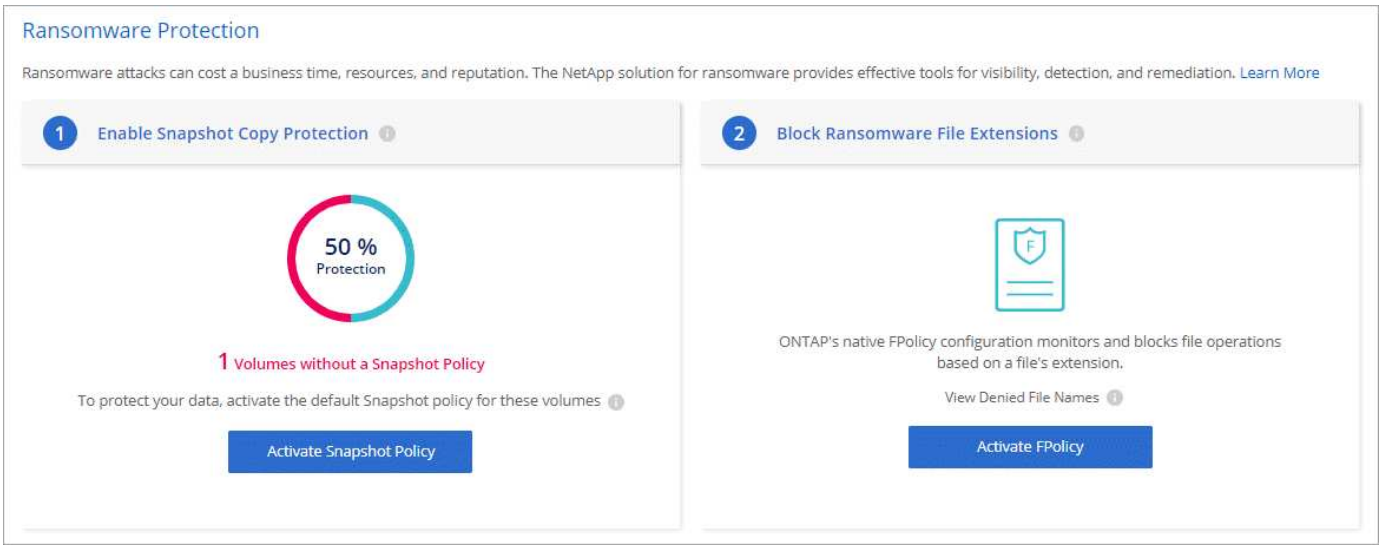


2. Implementierung der NetApp Lösung für Ransomware:
   a. Klicken Sie auf **Snapshot-Richtlinie aktivieren**, wenn Volumes ohne Snapshot-Richtlinie aktiviert sind.

      Die NetApp Snapshot-Technologie bietet die branchenweit beste Lösung zur Behebung von Ransomware. Der Schlüssel zu einer erfolgreichen Recovery liegt im Restore aus einem nicht infizierten Backup. 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.

   b. Klicken Sie auf **FPolicy** aktivieren, um die FPolicy Lösung von ONTAP zu aktivieren, die Dateivorgänge auf Basis der Dateierweiterung blockieren kann.

      Diese präventive Lösung verbessert den Schutz vor Ransomware-Angriffen, indem sie gängige Ransomware-Dateitypen blockiert.



Verwaltung

Registrieren von Pay-as-you-go-Systemen

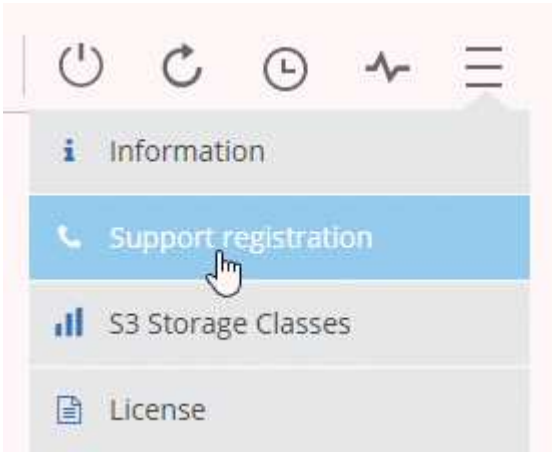
Cloud Volumes ONTAP Explore, Standard und Premium umfasst Support von NetApp. Sie müssen jedoch den Support erst aktivieren, wenn Sie die Systeme bei NetApp registrieren.

Schritte

1. Wenn Sie noch kein NetApp Support Site Konto zu Cloud Manager hinzugefügt haben, gehen Sie zu **Account Settings** und fügen Sie es jetzt hinzu.

   "Erfahren Sie, wie Sie Konten der NetApp Support Site hinzufügen".

2. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf den Namen des Systems, das Sie registrieren möchten.
3. Klicken Sie auf das Menü-Symbol und dann auf **Support-Registrierung**:



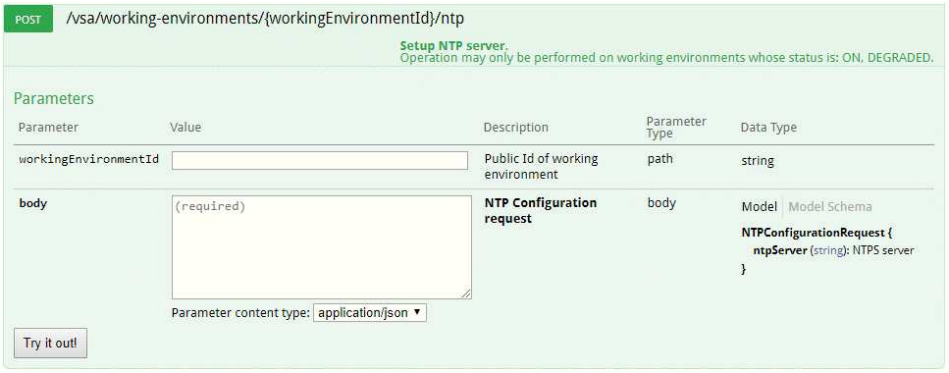
4. Wählen Sie ein NetApp Support Site Konto aus und klicken Sie auf **Registrieren**.

Ergebnis

Cloud Manager registriert das System bei NetApp.

Einrichten von Cloud Volumes ONTAP

Nachdem Sie Cloud Volumes ONTAP implementiert haben, können Sie diese einrichten, indem Sie die Systemzeit mithilfe von NTP synchronisieren und einige optionale Aufgaben entweder über den System Manager oder die CLI ausführen.

Aufgabe	Beschreibung
Synchronisieren Sie die Systemzeit mit NTP	Durch das Festlegen eines NTP-Servers wird die Zeit zwischen den Systemen im Netzwerk synchronisiert, wodurch Probleme aufgrund von Zeitunterschieden vermieden werden können. Geben Sie beim Einrichten eines CIFS-Servers einen NTP-Server mithilfe der Cloud Manager-API oder von der Benutzeroberfläche an. • "Ändern des CIFS-Servers" • "Cloud Manager API-Entwicklerleitfaden" Hier ist zum Beispiel die API für ein Single-Node-System in AWS: 
Optional: AutoSupport konfigurieren	AutoSupport überwacht proaktiv den Systemzustand und sendet standardmäßig automatisch Meldungen an den technischen Support von NetApp. Wenn der Kontoadministrator dem Cloud-Manager einen Proxyserver hinzugefügt hat, bevor Sie Ihre Instanz gestartet haben, ist Cloud Volumes ONTAP so konfiguriert, dass er diesen Proxyserver für AutoSupport-Nachrichten verwendet. Sie sollten AutoSupport testen, um sicherzustellen, dass Nachrichten gesendet werden können. Anweisungen hierzu finden Sie in der Hilfe zum System Manager oder in der "ONTAP 9 – Systemadministrationshandbuch".
Optional: Konfigurieren Sie Cloud-Manager als AutoSupport-Proxy	Wenn in Ihrer Umgebung ein Proxyserver zum Senden von AutoSupport Meldungen benötigt wird, können Sie Cloud Manager so konfigurieren, dass er als Proxy verwendet wird. Für Cloud Manager ist keine Konfiguration erforderlich – abgesehen vom Internet-Zugriff. Sie müssen einfach zur CLI für Cloud Volumes ONTAP gehen und den folgenden Befehl ausführen: `system node autosupport modify -proxy-url <cloud-manager-ip-address>`
Optional: EMS konfigurieren	Das Event Management System (EMS) erfasst und zeigt Informationen zu Ereignissen an, die auf Cloud Volumes ONTAP Systemen auftreten. Um Ereignisbenachrichtigungen zu erhalten, können Sie Ereignisziele (E-Mail-Adressen, SNMP-Trap-Hosts oder Syslog-Server) und Ereignisrouten für einen bestimmten Ereignisschweregrad festlegen. Sie können EMS über die CLI konfigurieren. Anweisungen hierzu finden Sie im "ONTAP 9 EMS Configuration Express Guide".

Aufgabe	Beschreibung
Optional: Erstellung einer SVM Management-Netzwerkschnittstelle (LIF) für HA-Systeme in mehreren AWS Verfügbarkeitszonen	Wenn Sie SnapCenter oder SnapDrive für Windows mit einem HA-Paar verwenden möchten, ist eine Storage Virtual Machine (SVM) Management Network Interface (LIF) erforderlich. Die SVM-Management-LIF muss bei Verwendung eines HA-Paars über mehrere AWS Availability Zones eine „*Floating* IP-Adresse“ verwenden. Cloud Manager fordert Sie auf, die unverankerte IP-Adresse anzugeben, wenn Sie das HA-Paar starten. Wenn Sie die IP-Adresse nicht angegeben haben, können Sie die SVM Management-LIF selbst über den System Manager oder die CLI erstellen. Das folgende Beispiel zeigt, wie Sie die LIF über die CLI erstellen: `network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home-port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall -policy mgmt`
Optional: Ändern Sie den Speicherort der Konfigurationsdateien	Cloud Volumes ONTAP erstellt automatisch Backup-Dateien für die Konfiguration, die Informationen zu den konfigurierbaren Optionen enthalten, die für einen ordnungsgemäßen Betrieb erforderlich sind. Standardmäßig sichert Cloud Volumes ONTAP die Dateien alle acht Stunden auf dem Connector-Host. Wenn Sie die Backups an einen anderen Speicherort senden möchten, können Sie den Speicherort auf einen FTP- oder HTTP-Server in Ihrem Datacenter oder in AWS ändern. Sie verfügen beispielsweise bereits über einen Backup-Speicherort für Ihre FAS Storage-Systeme. Sie können den Backup-Speicherort über die CLI ändern. Siehe "ONTAP 9 – Systemadministrationshandbuch".

Byol-Lizenzen für Cloud Volumes ONTAP verwalten

Fügen Sie eine Cloud Volumes ONTAP-BYOL-Systemlizenz hinzu, um zusätzliche Kapazität hinzuzufügen, eine vorhandene Systemlizenz zu aktualisieren und BYOL-Lizenzen für Backup in der Cloud zu managen.

Verwalten von 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.

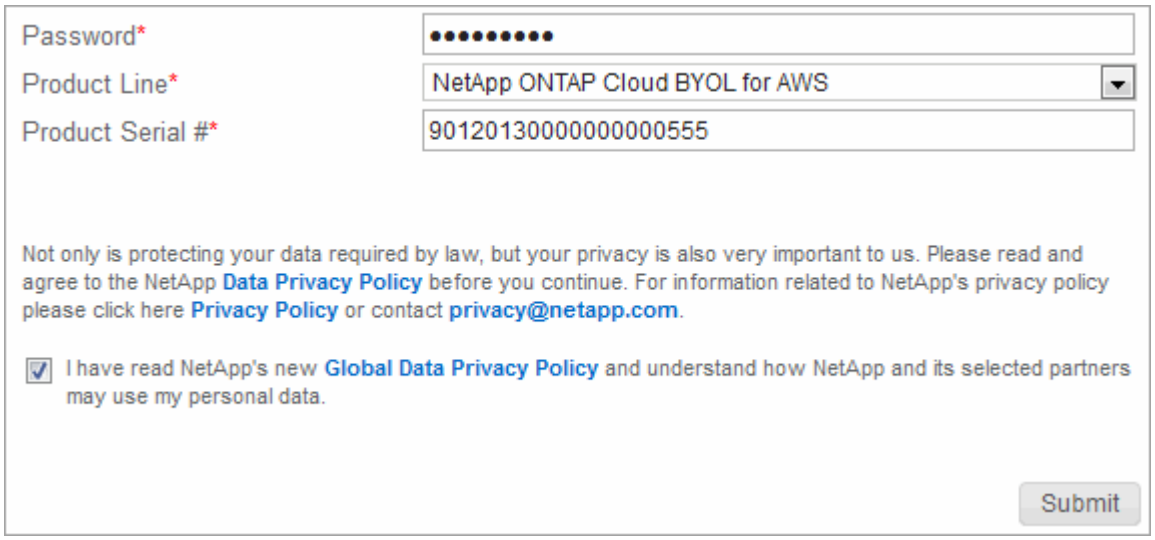
Abrufen einer Systemlizenzdatei

In den meisten Fällen kann Cloud Manager Ihre Lizenzdatei automatisch über Ihren NetApp Support Site Account beziehen. Aber wenn es nicht kann, dann müssen Sie die Lizenzdatei manuell hochladen. Wenn Sie die Lizenzdatei nicht haben, können Sie sie von netapp.com beziehen.

Schritte

1. Wechseln Sie zum "NetApp Lizenzdatei-Generator" Und loggen Sie sich mit Ihren Anmeldedaten für die NetApp Support Site ein.
2. Geben Sie Ihr Passwort ein, wählen Sie Ihr Produkt aus, geben Sie die Seriennummer ein, bestätigen Sie, dass Sie die Datenschutzrichtlinie gelesen und akzeptiert haben, und klicken Sie dann auf **Absenden**.

   Beispiel



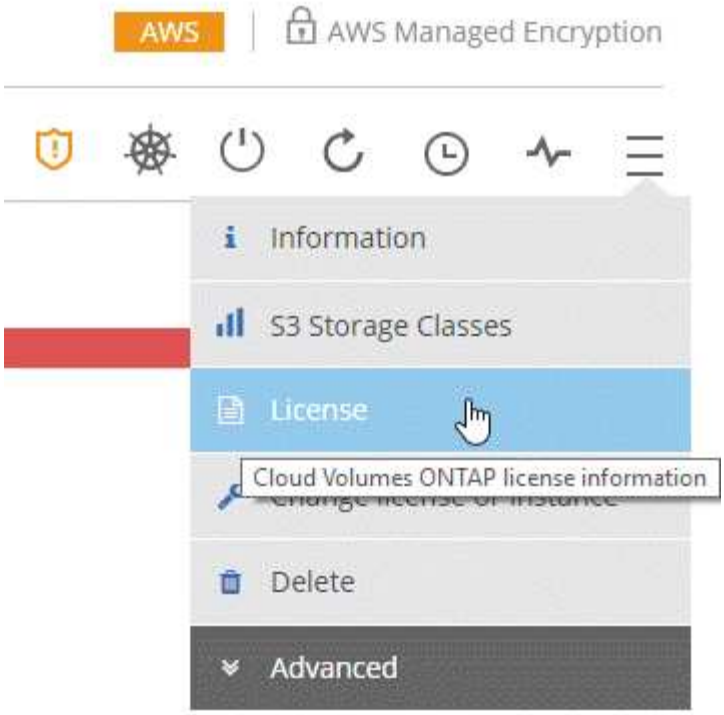
3. Wählen Sie aus, ob Sie die Datei serialnumber.NLF JSON per E-Mail oder direkt herunterladen möchten.

Hinzufügen einer neuen Systemlizenz

Fügen Sie jederzeit eine neue BYOL-Systemlizenz hinzu, um Ihrem Cloud Volumes ONTAP BYOL-System weitere 368 TB zusätzlicher Kapazität zuzuweisen.

Schritte

1. Öffnen Sie in Cloud Manager die BYOL-Arbeitsumgebung von Cloud Volumes ONTAP.
2. Klicken Sie auf das Menü-Symbol und dann auf **Lizenz**.



3. Klicken Sie auf **CVO-Systemlizenz hinzufügen**.

4. Geben Sie die Seriennummer ein oder laden Sie die Lizenzdatei hoch.
5. Klicken Sie Auf **Lizenz Hinzufügen**.

Ergebnis

Cloud Manager installiert die neue Lizenzdatei auf dem Cloud Volumes ONTAP System.

Aktualisieren einer Systemlizenz

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.

Schritte

1. Öffnen Sie in Cloud Manager die BYOL-Arbeitsumgebung von Cloud Volumes ONTAP.
2. Klicken Sie auf das Menü-Symbol und dann auf **Lizenz**.
3. Klicken Sie auf **Aktualisieren der CVO-Systemlizenz**.

4. Klicken Sie auf **Datei hochladen** und wählen Sie die Lizenzdatei aus.
5. Klicken Sie Auf **Lizenz Aktualisieren**.

Ergebnis

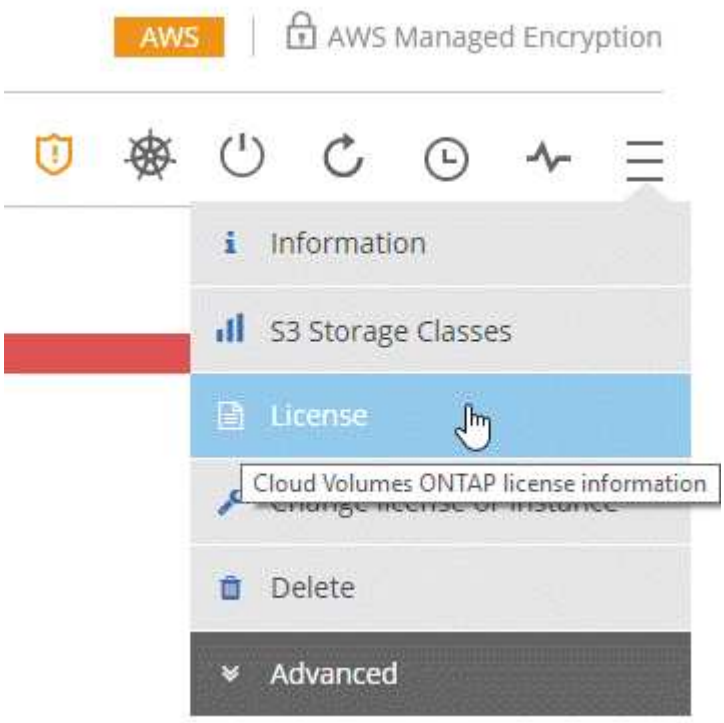
Cloud Manager aktualisiert die Lizenz auf dem Cloud Volumes ONTAP System.

Hinzufügen und Aktualisieren der Backup-BYOL-Lizenz

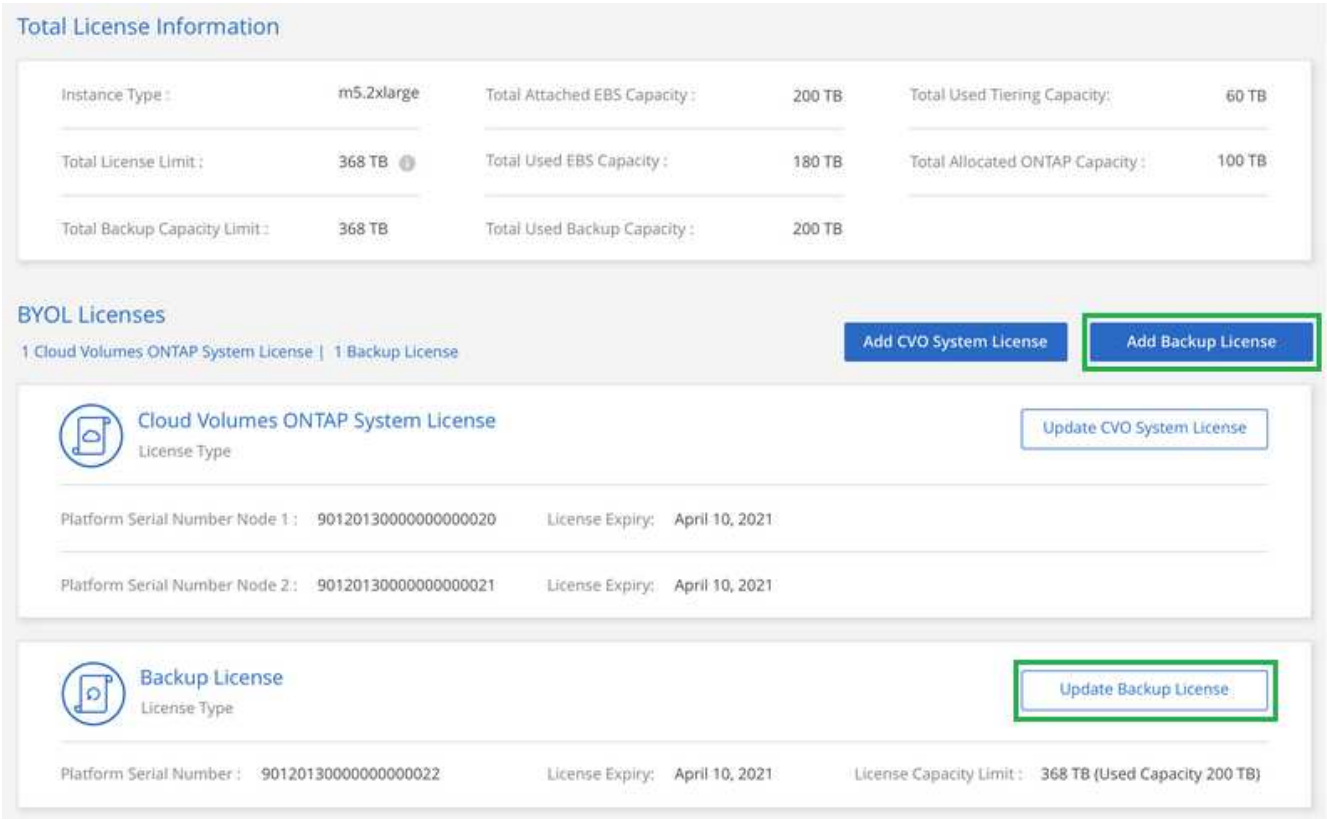
Auf der Seite „Byol Licenses“ können Sie Ihre BYOL-Lizenz für Backups hinzufügen oder aktualisieren.

Schritte

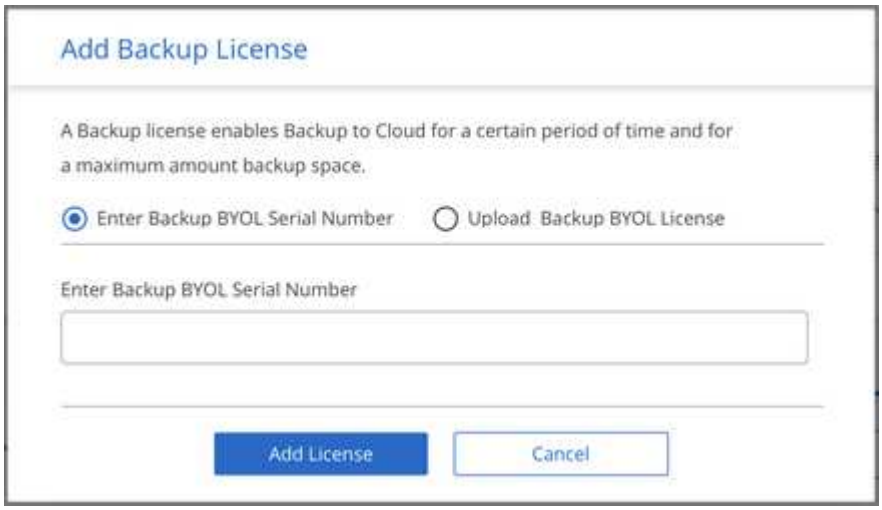
1. Öffnen Sie in Cloud Manager die BYOL-Arbeitsumgebung von Cloud Volumes ONTAP.
2. Klicken Sie auf das Menü-Symbol und dann auf **Lizenz**.



3. Klicken Sie abhängig davon, ob Sie eine neue Lizenz hinzufügen oder eine vorhandene Lizenz aktualisieren möchten, auf **Backup License** oder auf **Update Backup License**.



4. Geben Sie die Lizenzinformationen ein und klicken Sie auf **Lizenz hinzufügen**:
   - Wenn Sie die Seriennummer haben, wählen Sie die Option **Byol-Seriennummer eingeben** und geben Sie die Seriennummer ein.
   - Wenn Sie über die Backup-Lizenzdatei verfügen, wählen Sie die Option **BYOL-Lizenz hochladen** aus, und folgen Sie den Anweisungen, um die Datei anzuhängen.



Ergebnis

Cloud Manager fügt die Lizenz hinzu oder aktualisiert sie, sodass Ihr Cloud-Service für Backup aktiv ist.

Aktualisierung der Cloud Volumes ONTAP Software

Cloud Manager umfasst mehrere Optionen, mit denen Sie auf die aktuelle Version von

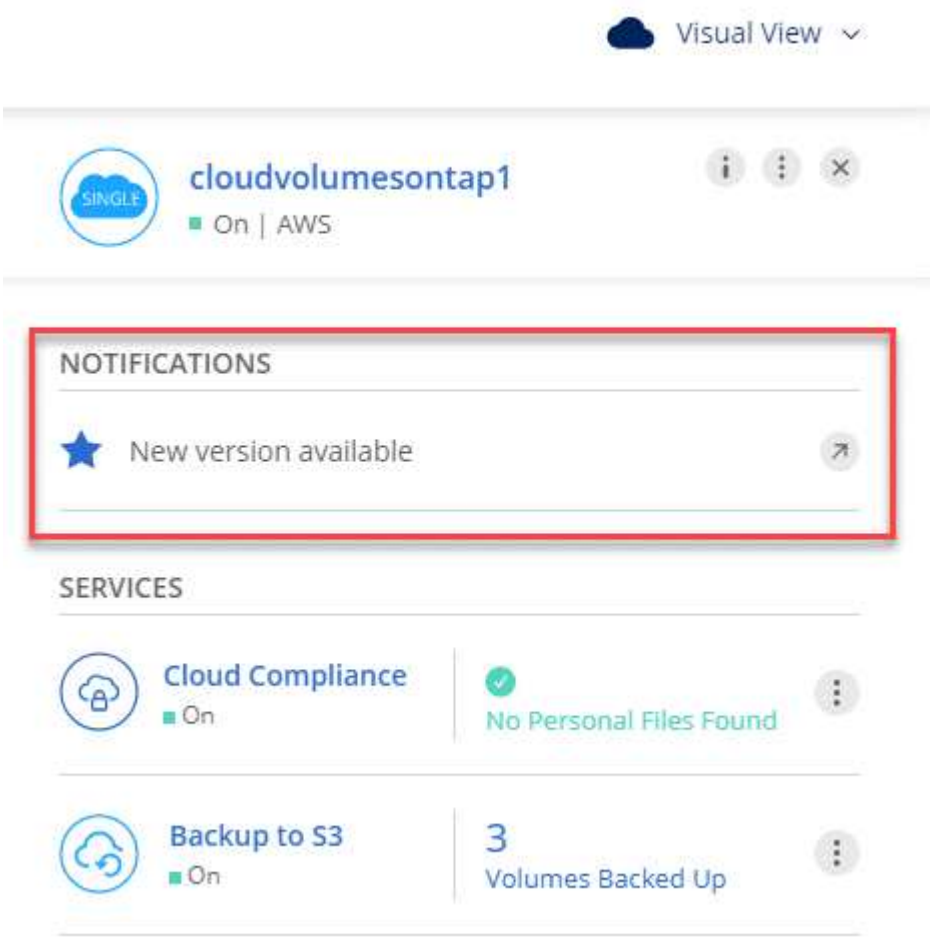
Cloud Volumes ONTAP aktualisieren oder Cloud Volumes ONTAP auf eine frühere Version herabstufen können. Sie sollten Cloud Volumes ONTAP Systeme vorbereiten, bevor Sie ein Upgrade oder Downgrade der Software durchführen.

Software-Updates müssen von Cloud Manager abgeschlossen werden

Upgrades von Cloud Volumes ONTAP müssen von Cloud Manager abgeschlossen werden. Sie sollten kein Cloud Volumes ONTAP-Upgrade mit System Manager oder der CLI durchführen. Dies kann die Stabilität des Systems beeinträchtigen.

Möglichkeiten zum Aktualisieren von Cloud Volumes ONTAP

Cloud Manager zeigt eine Benachrichtigung in den Arbeitsumgebungen von Cloud Volumes ONTAP an, wenn eine neue Version von Cloud Volumes ONTAP verfügbar ist:



Sie können den Upgrade-Prozess von dieser Benachrichtigung aus starten, die den Prozess automatisiert, indem Sie das Software-Image aus einem S3-Bucket beziehen, das Image installieren und das System dann neu starten. Weitere Informationen finden Sie unter Aktualisieren von Cloud Volumes ONTAP über Cloud Manager Benachrichtigungen.

Bei HA-Systemen in AWS kann Cloud Manager im Rahmen des Upgrades den HA-Mediator aktualisieren.

Erweiterte Optionen für Software-Updates

Cloud Manager bietet außerdem die folgenden erweiterten Optionen für die Aktualisierung der Cloud Volumes ONTAP Software:

- Software-Updates mit einem Bild auf einer externen URL

  Diese Option ist hilfreich, wenn Cloud Manager nicht auf den S3-Bucket zugreifen kann, um die Software zu aktualisieren, wenn Ihnen ein Patch zur Verfügung steht oder wenn Sie die Software auf eine bestimmte Version herunterstufen möchten.

  Weitere Informationen finden Sie unter Upgrade oder Downgrade von Cloud Volumes ONTAP mit einem HTTP- oder FTP-Server.

- Software-Updates mit dem alternativen Image auf dem System

  Mit dieser Option können Sie auf die vorherige Version zurückstufen, indem Sie das alternative Software-Image zum Standardbild machen. Diese Option ist für HA-Paare nicht verfügbar.

  Weitere Informationen finden Sie unter Downgrade von Cloud Volumes ONTAP mit einem lokalen Image.

Aktualisierung der Cloud Volumes ONTAP Software wird vorbereitet

Bevor Sie ein Upgrade oder Downgrade durchführen, müssen Sie sicherstellen, dass Ihre Systeme bereit sind, und alle erforderlichen Konfigurationsänderungen vornehmen.

- Planung von Ausfallzeiten
- Überprüfen der Versionsanforderungen
- dass das automatische Giveback weiterhin aktiviert ist
- SnapMirror Übertragungen werden ausgesetzt
- ob Aggregate online sind

Planung von Ausfallzeiten

Wenn Sie ein Single-Node-System aktualisieren, stellt der Upgrade-Prozess das System für bis zu 25 Minuten offline, während dieser I/O-Unterbrechung ausgeführt wird.

Das Upgrade eines HA-Paars erfolgt unterbrechungsfrei und die I/O wird unterbrochen. Während dieses unterbrechungsfreien Upgrade-Prozesses wird jeder Node entsprechend aktualisiert, um den I/O-Datenverkehr für die Clients weiterhin bereitzustellen.

Überprüfen der Versionsanforderungen

Die ONTAP Version, auf die Sie aktualisieren oder herunterstufen können, variiert abhängig von der Version von ONTAP, die derzeit auf Ihrem System ausgeführt wird.

Informationen zu Versionsanforderungen finden Sie unter "ONTAP 9 Dokumentation: Anforderungen für Cluster-Updates".

Es wird sichergestellt, dass das automatische Giveback weiterhin aktiviert ist

Automatisches Giveback muss auf einem Cloud Volumes ONTAP HA-Paar aktiviert sein (dies ist die Standardeinstellung). Wenn nicht, schlägt der Vorgang fehl.

"ONTAP 9 Dokumentation: Befehle zur Konfiguration von automatischem Giveback"

SnapMirror Übertragungen werden ausgesetzt

Wenn ein Cloud Volumes ONTAP System über aktive SnapMirror Beziehungen verfügt, sollten Sie die Übertragungen am besten unterbrechen, bevor Sie die Cloud Volumes ONTAP Software aktualisieren. Das Anhalten der Übertragungen verhindert SnapMirror Ausfälle. Sie müssen die Übertragungen vom Zielsystem anhalten.

Über diese Aufgabe

In diesen Schritten wird die Verwendung von System Manager für Version 9.3 und höher beschrieben.

Schritte

1. "Melden Sie sich bei System Manager an" Von dem Zielsystem stammen.
2. Klicken Sie Auf **Schutz > Beziehungen**.
3. Wählen Sie die Beziehung aus, und klicken Sie auf **Operationen > Quiesce**.

Überprüfen, ob Aggregate online sind

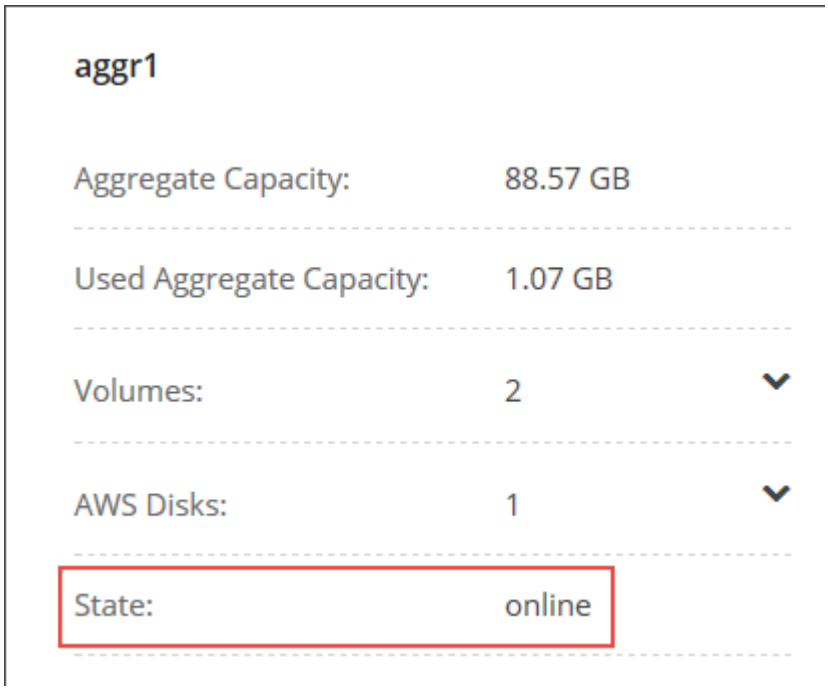
Aggregate für Cloud Volumes ONTAP muss online sein, bevor Sie die Software aktualisieren. Aggregate sollten in den meisten Konfigurationen online sein. Wenn dies nicht der Fall ist, sollten Sie sie jedoch online stellen.

Über diese Aufgabe

In diesen Schritten wird die Verwendung von System Manager für Version 9.3 und höher beschrieben.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Erweiterte Zuweisung**.
2. Wählen Sie ein Aggregat aus, klicken Sie auf **Info** und überprüfen Sie dann, ob der Status online ist.



3. Wenn das Aggregat offline ist, verwenden Sie System Manager, um das Aggregat online zu schalten:
   a. "Melden Sie sich bei System Manager an".
   b. Klicken Sie Auf **Storage > Aggregate & Disks > Aggregate**.
   c. Wählen Sie das Aggregat aus und klicken Sie dann auf **Weitere Aktionen > Status > Online**.

Aktualisieren von Cloud Volumes ONTAP über Cloud Manager Benachrichtigungen

Cloud Manager benachrichtigt Sie, wenn eine neue Version von Cloud Volumes ONTAP verfügbar ist. Klicken Sie auf die Benachrichtigung, um den Aktualisierungsprozess zu starten.

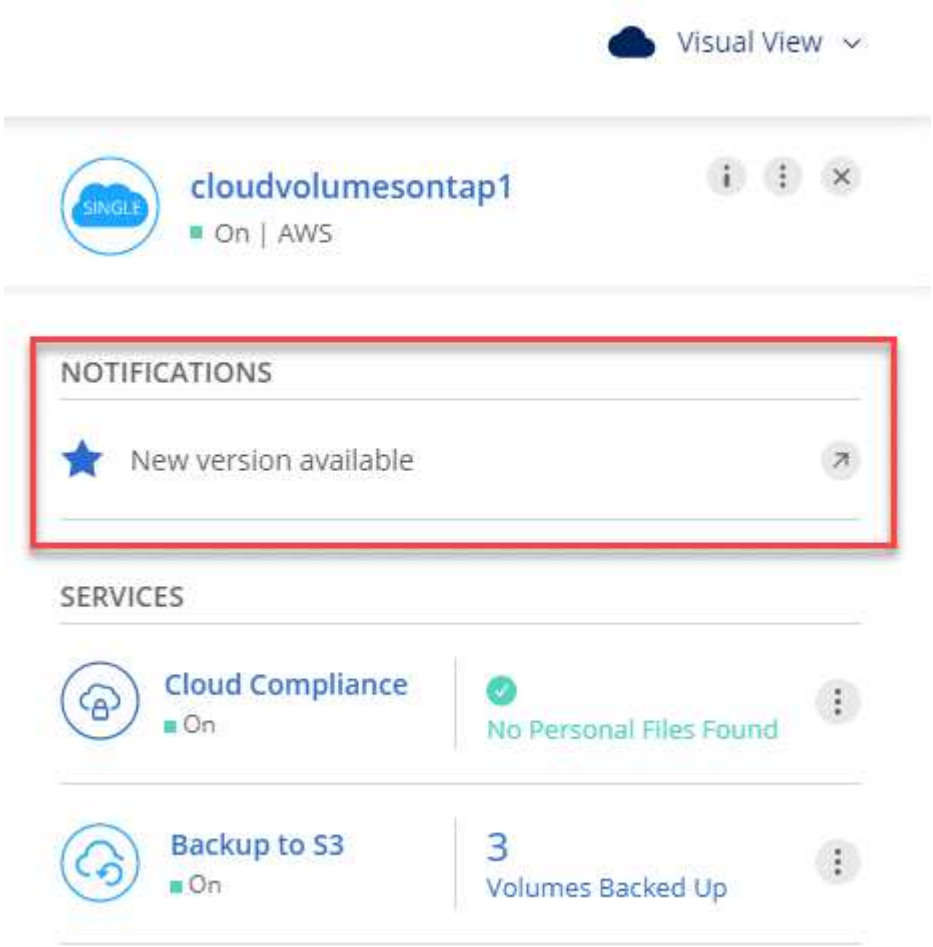
Bevor Sie beginnen

Cloud Manager-Vorgänge wie die Erstellung von Volumes oder Aggregaten dürfen für das Cloud Volumes ONTAP System nicht ausgeführt werden.

Schritte

1. Klicken Sie Auf **Arbeitsumgebungen**.
2. Wählen Sie eine Arbeitsumgebung aus.

   Im rechten Fensterbereich wird eine Benachrichtigung angezeigt, wenn eine neue Version verfügbar ist:



3. Wenn eine neue Version verfügbar ist, klicken Sie auf **Upgrade**.

4. Klicken Sie auf der Seite Release Information auf den Link, um die Versionshinweise für die angegebene Version zu lesen, und aktivieren Sie dann das Kontrollkästchen **Ich habe gelesen…**.
5. Lesen Sie auf der Seite Endbenutzer-Lizenzvereinbarung (EULA) die EULA, und wählen Sie dann **Ich habe die EULA gelesen und genehmigt**.
6. Lesen Sie auf der Seite Prüfen und genehmigen die wichtigen Hinweise, wählen Sie **Ich verstehe…** und klicken Sie dann auf **Go**.

Ergebnis

Cloud Manager startet das Software-Upgrade. Nach Abschluss der Softwareaktualisierung können Sie in der Arbeitsumgebung Aktionen ausführen.

Nachdem Sie fertig sind

Wenn Sie SnapMirror Transfers ausgesetzt haben, setzen Sie die Transfers mit System Manager fort.

Upgrade oder Downgrade von Cloud Volumes ONTAP mit einem HTTP- oder FTP-Server

Sie können das Cloud Volumes ONTAP Software-Image auf einem HTTP- oder FTP-Server platzieren und dann das Software-Update über Cloud Manager starten. Sie können diese Option verwenden, wenn Cloud Manager nicht auf den S3-Bucket zugreifen kann, um die Software zu aktualisieren, oder wenn Sie ein Downgrade der Software durchführen möchten.

Schritte

1. Richten Sie einen HTTP-Server oder FTP-Server ein, der das Cloud Volumes ONTAP Software-Image hosten kann.
2. Wenn Sie eine VPN-Verbindung zum virtuellen Netzwerk haben, können Sie das Cloud Volumes ONTAP Software-Image auf einem HTTP-Server oder FTP-Server in Ihrem eigenen Netzwerk platzieren. Andernfalls müssen Sie die Datei auf einem HTTP-Server oder FTP-Server in der Cloud platzieren.
3. Wenn Sie Ihre eigene Sicherheitsgruppe für Cloud Volumes ONTAP verwenden, stellen Sie sicher, dass die Outbound-Regeln HTTP- oder FTP-Verbindungen zulassen, damit Cloud Volumes ONTAP auf das Software-Image zugreifen kann.

   Die vordefinierte Sicherheitsgruppe Cloud Volumes ONTAP ermöglicht standardmäßig ausgehende HTTP- und FTP-Verbindungen.

4. Beziehen Sie das Software-Image von "Die NetApp Support Site".
5. Kopieren Sie das Software-Image in das Verzeichnis auf dem HTTP- oder FTP-Server, von dem die Datei bereitgestellt wird.
6. Klicken Sie in der Arbeitsumgebung des Cloud Managers auf das Menü-Symbol und dann auf **Erweitert > Cloud Volumes ONTAP aktualisieren**.
7. Wählen Sie auf der Seite Aktualisierungssoftware **Wählen Sie ein Bild aus einer URL** aus, geben Sie die URL ein und klicken Sie dann auf **Bild ändern**.
8. Klicken Sie zur Bestätigung auf **Weiter**.

Ergebnis

Cloud Manager startet das Softwareupdate. Nach Abschluss der Softwareaktualisierung können Sie in der Arbeitsumgebung Aktionen ausführen.

Nachdem Sie fertig sind

Wenn Sie SnapMirror Transfers ausgesetzt haben, setzen Sie die Transfers mit System Manager fort.

Downgrade von Cloud Volumes ONTAP mit einem lokalen Image

Der Wechsel von Cloud Volumes ONTAP auf eine frühere Version derselben Versionsfamilie (beispielsweise 9.5 bis 9.4) wird als Downgrade bezeichnet. Sie können ein Downgrade ohne Unterstützung durchführen, wenn Sie neue Cluster oder Testcluster herunterstufen möchten. Wenden Sie sich jedoch an den technischen Support, wenn Sie ein Downgrade eines Produktionsclusters durchführen möchten.

Jedes Cloud Volumes ONTAP System kann zwei Software-Images enthalten: Das aktuelle Image, das ausgeführt wird, und ein alternatives Image, das Sie booten können. Cloud Manager kann das alternative Bild als Standardbild ändern. Mit dieser Option können Sie auf die vorherige Version von Cloud Volumes ONTAP zurückstufen, wenn Probleme mit dem aktuellen Image auftreten.

Über diese Aufgabe

Dieser Downgrade-Prozess ist nur für einzelne Cloud Volumes ONTAP Systeme verfügbar. Es ist nicht für HA-Paare verfügbar.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Cloud Volumes ONTAP aktualisieren**.
2. Wählen Sie auf der Seite Aktualisierungssoftware das alternative Bild aus und klicken Sie dann auf **Bild ändern**.
3. Klicken Sie zur Bestätigung auf **Weiter**.

Ergebnis

Cloud Manager startet das Softwareupdate. Nach Abschluss der Softwareaktualisierung können Sie in der Arbeitsumgebung Aktionen ausführen.

Nachdem Sie fertig sind

Wenn Sie SnapMirror Transfers ausgesetzt haben, setzen Sie die Transfers mit System Manager fort.

Ändern von Cloud Volumes ONTAP Systemen

Möglicherweise müssen Sie die Konfiguration von Cloud Volumes ONTAP-Systemen ändern, wenn sich Ihre Storage-Anforderungen ändern. Sie können beispielsweise zwischen nutzungsbasierten Konfigurationen wechseln, den Instanz- oder VM-Typ ändern und vieles mehr.

Ändern des Instanz- oder Maschinentyps für Cloud Volumes ONTAP

Bei der Einführung von Cloud Volumes ONTAP in AWS, Azure oder GCP können Sie zwischen verschiedenen Instanzen oder Maschinentypen wählen. Sie können den Instanz- oder Maschinentyp jederzeit ändern, wenn Sie feststellen, dass er für Ihre Anforderungen unterdimensioniert oder überdimensioniert ist.

Über diese Aufgabe

- Automatisches Giveback muss auf einem Cloud Volumes ONTAP HA-Paar aktiviert sein (dies ist die Standardeinstellung). Wenn nicht, schlägt der Vorgang fehl.

  "ONTAP 9 Dokumentation: Befehle zur Konfiguration von automatischem Giveback"

- Eine Änderung des Instanz- oder Maschinentyps wirkt sich auf die Servicegebühren von Cloud-Providern aus.

- Der Vorgang startet Cloud Volumes ONTAP neu.

  Bei Systemen mit einem Node wird die I/O unterbrochen.

  Bei HA-Paaren ist die Änderung unterbrechungsfrei. Ha-Paare stellen weiterhin Daten bereit.

Cloud Manager ändert den Node nach dem anderen ordnungsgemäß, indem es Takeover und Warten auf Giveback initiiert. Das QA-Team von NetApp testete während dieses Prozesses sowohl das Schreiben als auch das Lesen der Dateien und sah keine Probleme auf Kundenseite. Wenn sich die Verbindungen änderten, wurden Wiederholungen auf I/O-Ebene gesehen, aber die Applikationsebene übergab diese kurze „Re-Wire“ der NFS/CIFS-Verbindungen.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Lizenz oder Instanz ändern** für AWS, **Lizenz ändern oder VM** für Azure oder **Lizenz oder Rechner ändern** für GCP.
2. Wenn Sie eine nutzungsbasierte Konfiguration verwenden, können Sie optional eine andere Lizenz auswählen.
3. Wählen Sie eine Instanz oder einen Maschinentyp aus, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Auswirkungen der Änderung verstehen, und klicken Sie dann auf **OK**.

Ergebnis

Cloud Volumes ONTAP wird mit der neuen Konfiguration neu gestartet.

Wechsel zwischen nutzungsbasierten Konfigurationen

Nachdem Sie Pay-as-you-go Cloud Volumes ONTAP Systeme gestartet haben, können Sie jederzeit zwischen den Konfigurationen Explore, Standard und Premium wechseln, indem Sie die Lizenz ändern. Das Ändern der Lizenz erhöht oder verringert die Obergrenze für die Rohkapazität und ermöglicht die Auswahl aus verschiedenen AWS Instanztypen oder Azure Virtual Machine-Typen.

In GCP ist für jede Pay-as-you-go-Konfiguration ein einziger Maschinentyp verfügbar. Sie können nicht zwischen verschiedenen Maschinentypen wählen.

Über diese Aufgabe

Beachten Sie Folgendes, um zwischen nutzungsbasierten Lizenzen zu wechseln:

- Der Vorgang startet Cloud Volumes ONTAP neu.

  Bei Systemen mit einem Node wird die I/O unterbrochen.

  Bei HA-Paaren ist die Änderung unterbrechungsfrei. Ha-Paare stellen weiterhin Daten bereit.

- Eine Änderung des Instanz- oder Maschinentyps wirkt sich auf die Servicegebühren von Cloud-Providern aus.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Lizenz oder Instanz ändern** für AWS, **Lizenz ändern oder VM** für Azure oder **Lizenz oder Rechner ändern** für GCP.
2. Wählen Sie einen Lizenztyp und einen Instanztyp oder Maschinentyp aus, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Auswirkungen der Änderung verstehen, und klicken Sie

dann auf **OK**.

Ergebnis

Cloud Volumes ONTAP wird mit der neuen Lizenz, dem Instanztyp oder dem Maschinentyp oder beides neu gebootet.

Wechsel zu einer alternativen Cloud Volumes ONTAP Konfiguration

Wenn Sie zwischen einem Pay-as-you-go-Abonnement und einem BYOL-Abonnement oder zwischen einem einzelnen Cloud Volumes ONTAP System und einem HA-Paar wechseln möchten, müssen Sie ein neues System implementieren und anschließend Daten aus dem vorhandenen System in das neue System replizieren.

Schritte

1. Erstellen Sie eine neue Cloud Volumes ONTAP Arbeitsumgebung.

   "Starten von Cloud Volumes ONTAP in AWS"
   "Starten von Cloud Volumes ONTAP in Azure"
   "Einführung von Cloud Volumes ONTAP in GCP"

2. "Einmalige Datenreplizierung einrichten" Zwischen den Systemen für jedes zu replizierende Volume wechseln.
3. Beenden Sie das Cloud Volumes ONTAP System, das Sie von nicht mehr benötigen "Die ursprüngliche Arbeitsumgebung wird gelöscht".

Ändern der Schreibgeschwindigkeit auf „Normal“ oder „hoch“

Mit Cloud Manager können Sie eine Einstellung für die Schreibgeschwindigkeit für Cloud Volumes ONTAP Systeme mit einem Node wählen. Die standardmäßige Schreibgeschwindigkeit ist normal. Wenn für Ihren Workload eine hohe Schreib-Performance erforderlich ist, kann die hohe Schreibgeschwindigkeit geändert werden. Bevor Sie die Schreibgeschwindigkeit ändern, sollten Sie dies tun "Die Unterschiede zwischen den normalen und den hohen Einstellungen verstehen".

Über diese Aufgabe

- Stellen Sie sicher, dass Vorgänge wie die Volume- oder Aggregaterstellung nicht ausgeführt werden.
- Beachten Sie, dass durch diese Änderung Cloud Volumes ONTAP neu gestartet wird, was bedeutet, dass I/O unterbrochen wird.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Schreibgeschwindigkeit**.
2. Wählen Sie **normal** oder **hoch**.

   Wenn Sie „hoch“ wählen, müssen Sie die „Ich verstehe…“-Aussage lesen und bestätigen, indem Sie das Kästchen aktivieren.

3. Klicken Sie auf **Speichern**, überprüfen Sie die Bestätigungsmeldung und klicken Sie dann auf **Weiter**.

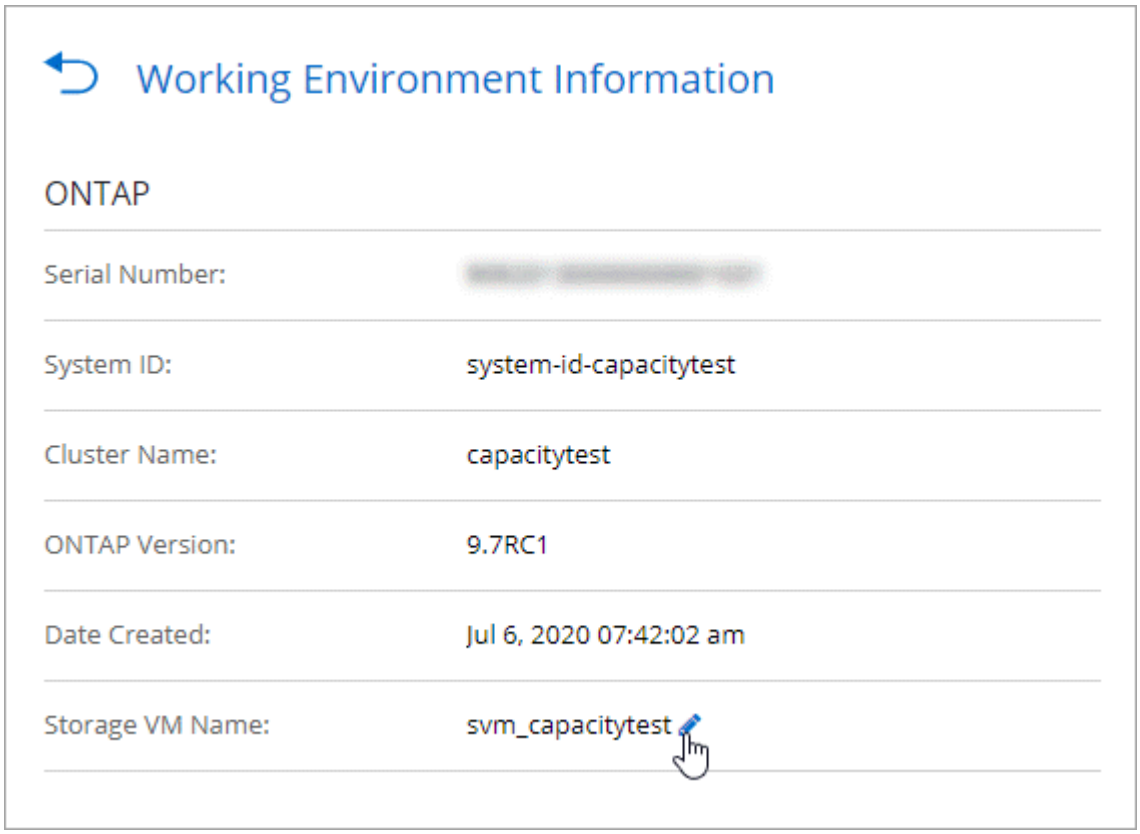
Ändern des Namens der Storage-VM

Cloud Manager benennt automatisch die einzelne Storage-VM (SVM), die für Cloud Volumes ONTAP erstellt wird. Sie können den Namen der SVM ändern, wenn Sie strenge Benennungsstandards haben. Beispielsweise sollte der Name Ihnen entsprechen, wie Sie die SVMs für Ihre ONTAP Cluster benennen.

Wenn Sie aber zusätzliche SVMs für Cloud Volumes ONTAP erstellen, können Sie die SVMs nicht aus Cloud Manager umbenennen. Sie müssen dies direkt von Cloud Volumes ONTAP mit System Manager oder der CLI ausführen.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Information**.
2. Klicken Sie rechts neben dem Namen der Storage-VM auf das Bearbeiten-Symbol.



3. Ändern Sie im Dialogfeld SVM-Name ändern den Namen und klicken Sie dann auf **Speichern**.

Ändern des Passworts für Cloud Volumes ONTAP

Cloud Volumes ONTAP enthält ein Cluster-Administratorkonto. Sie können das Kennwort für dieses Konto bei Bedarf über Cloud Manager ändern.

Sie sollten das Kennwort für das Administratorkonto nicht über System Manager oder die CLI ändern. Das Kennwort wird nicht in Cloud Manager angezeigt. Daher kann Cloud Manager die Instanz nicht ordnungsgemäß überwachen.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Passwort festlegen**.
2. Geben Sie das neue Passwort zweimal ein und klicken Sie dann auf **Speichern**.

   Das neue Kennwort muss sich von einem der letzten sechs Kennwörter unterscheiden.

Ändern der Netzwerk-MTU für c4.4xlarge und c4.8xlarge Instanzen

Standardmäßig ist Cloud Volumes ONTAP so konfiguriert, dass 9.000 MTU (auch Jumbo Frames genannt) verwendet werden, wenn Sie die c4.4xlarge Instanz oder die c4.8xlarge Instanz in AWS auswählen. Sie können die Netzwerk-MTU auf 1.500 Byte ändern, wenn dies für Ihre Netzwerkkonfiguration besser geeignet ist.

Über diese Aufgabe

Eine maximale Netzwerkübertragungseinheit (Maximum Transmission Unit, MTU) von 9.000 Byte bietet den höchstmöglichen Netzwerkdurchsatz für bestimmte Konfigurationen.

9.000 MTU ist eine gute Wahl, wenn Clients in demselben VPC mit dem Cloud Volumes ONTAP System kommunizieren und einige oder alle dieser Clients ebenfalls 9.000 MTU unterstützen. Wenn der Datenverkehr den VPC verlässt, kann es zu einer Paketfragmentierung kommen, die die Performance beeinträchtigt.

Eine Netzwerk-MTU von 1.500 Byte ist eine gute Wahl, wenn Clients oder Systeme außerhalb des VPC mit dem Cloud Volumes ONTAP System kommunizieren.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Netzwerknutzung**.
2. Wählen Sie **Standard** oder **Jumbo Frames**.
3. Klicken Sie Auf **Ändern**.

Ändern von Routingtabellen im Zusammenhang mit HA-Paaren in mehreren AWS AZS

Sie können die AWS-Routing-Tabellen mit Routen zu den unverankerten IP-Adressen für ein HA-Paar ändern. Vielleicht möchten Sie dies tun, wenn neue NFS- oder CIFS-Clients auf ein HA-Paar in AWS zugreifen müssen.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Information**.
2. Klicken Sie Auf **Routentabellen**.
3. Ändern Sie die Liste der ausgewählten Routentabellen und klicken Sie dann auf **Speichern**.

Ergebnis

Cloud Manager sendet eine AWS-Anforderung zum Ändern der Routentabellen.

Managen des Status von Cloud Volumes ONTAP

Sie können Cloud Volumes ONTAP über Cloud Manager anhalten und starten, um Ihre Cloud-Computing-Kosten zu managen.

Planen automatischer Abschaltungen von Cloud Volumes ONTAP

Sie sollten Cloud Volumes ONTAP in bestimmten Zeitintervallen herunterfahren, um Ihre Computing-Kosten zu senken. Statt dies manuell zu tun, können Sie Cloud Manager so konfigurieren, dass Systeme automatisch heruntergefahren und dann zu bestimmten Zeiten neu gestartet werden.

Über diese Aufgabe

Wenn Sie einen automatischen Shutdown des Cloud Volumes ONTAP Systems planen, verschiebt Cloud Manager das Herunterfahren vor, wenn ein aktiver Datentransfer stattfinden soll. Cloud Manager schaltet das

System nach Abschluss der Übertragung aus.

Diese Aufgabe plant das automatische Herunterfahren beider Nodes in einem HA-Paar.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Uhrsymbol:

2. Geben Sie den Zeitplan für das Herunterfahren an:

   a. Wählen Sie aus, ob Sie das System täglich, jeden Werktag, jedes Wochenende oder eine beliebige Kombination der drei Optionen herunterfahren möchten.

   b. Geben Sie an, wann und wie lange das System ausgeschaltet werden soll.

      Beispiel

      Die folgende Abbildung zeigt einen Zeitplan, in dem Cloud Manager angewiesen wird, das System jeden Samstag um 24:00 Uhr auszuschalten Für 48 Stunden. Cloud Manager startet das System jeden Montag um 12:00 Uhr neu

3. Klicken Sie Auf **Speichern**.

Ergebnis

Cloud Manager speichert den Zeitplan. Das Uhrensymbol ändert sich, um anzuzeigen, dass ein Zeitplan festgelegt wurde: 

Beenden von Cloud Volumes ONTAP

Stoppen von Cloud Volumes ONTAP erspart Ihnen das Ansteigen von Computing-Kosten und erstellt Snapshots der Root- und Boot-Festplatten, was bei der Fehlerbehebung hilfreich sein kann.

Über diese Aufgabe

Wenn Sie ein HA-Paar anhalten, fährt Cloud Manager beide Nodes herunter.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Symbol **Ausschalten**.

2. Behalten Sie die Option zum Erstellen von Snapshots aktiviert bei, da die Snapshots die System-Recovery ermöglichen können.
3. Klicken Sie Auf **Ausschalten**.

   Es kann bis zu einigen Minuten dauern, bis das System gestoppt wird. Sie können Systeme zu einem späteren Zeitpunkt von der Seite "Arbeitsumgebung" aus neu starten.

Überwachung der AWS-Ressourcenkosten

Mit Cloud Manager können Sie die Ressourcenkosten anzeigen, die mit der Ausführung von Cloud Volumes ONTAP in AWS verbunden sind. Außerdem erfahren Sie, wie viel Geld Sie durch den Einsatz von NetApp Funktionen zur Senkung der Storage-Kosten gespart haben.

Über diese Aufgabe

Cloud Manager aktualisiert die Kosten bei Aktualisierung der Seite. Die endgültigen Kostendetails finden Sie in AWS.

Schritt

1. Stellen Sie sicher, dass Cloud Manager Kosteninformationen von AWS beziehen kann:
   a. Vergewissern Sie sich, dass die IAM-Richtlinie, die Cloud Manager über Berechtigungen verfügt, die folgenden Aktionen umfasst:

      ```
      "ce:GetReservationUtilization",
      "ce:GetDimensionValues",
      "ce:GetCostAndUsage",
      "ce:GetTags"
      ```

      Diese Aktionen sind in den letzten enthalten "Cloud Manager-Richtlinie". Neue Systeme, die von NetApp Cloud Central implementiert werden, enthalten automatisch diese Berechtigungen.

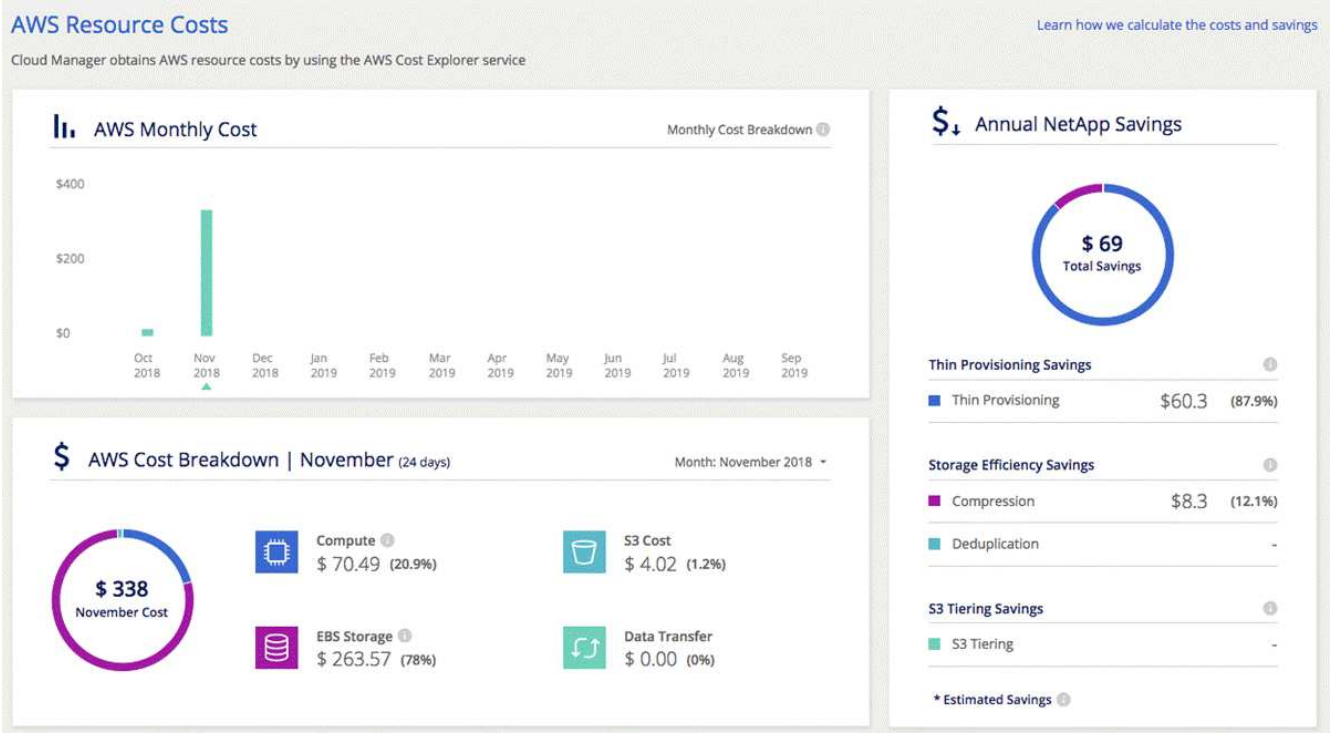
   b. "Aktivieren Sie das Tag **WorkingEnvironment ID**".

      Um die AWS-Kosten zu verfolgen, weist Cloud Manager Cloud Volumes ONTAP Instanzen ein Tag der Kostenzuteilung zu. Nachdem Sie Ihre erste Arbeitsumgebung erstellt haben, aktivieren Sie das Tag **WorkingEnvironment ID**. Benutzerdefinierte Tags werden erst in den AWS Abrechnungsberichten angezeigt, wenn Sie sie in der Konsole „Rechnungsstellung“ und „Kostenmanagement“ aktivieren.

2. Wählen Sie auf der Seite Arbeitsumgebungen eine Cloud Volumes ONTAP Arbeitsumgebung aus und klicken Sie dann auf **Kosten**.

   Auf der Kostenseite werden die Kosten für die aktuelle und die vorherigen Monate angezeigt sowie Ihre jährlichen NetApp Einsparungen angezeigt, wenn Sie die kostensparenden Funktionen von NetApp auf den Volumes aktiviert haben.

   Das folgende Bild zeigt eine Beispiel-Kostenseite:



Verbindung zu Cloud Volumes ONTAP

Wenn Sie ein erweitertes Management von Cloud Volumes ONTAP durchführen müssen, können Sie dies mit OnCommand System Manager oder der Befehlszeilenoberfläche tun.

Verbindung mit System Manager wird hergestellt

Möglicherweise müssen Sie einige Cloud Volumes ONTAP-Aufgaben aus System Manager ausführen. Hierbei handelt es sich um ein Browser-basiertes Managementtool, das auf dem Cloud Volumes ONTAP System ausgeführt wird. Sie müssen beispielsweise System Manager verwenden, wenn Sie LUNs erstellen möchten.

Bevor Sie beginnen

Der Computer, von dem aus Sie auf Cloud Manager zugreifen, muss über eine Netzwerkverbindung zu Cloud Volumes ONTAP verfügen. Sie müssen sich beispielsweise von einem Jump Host in AWS oder Azure bei Cloud Manager anmelden.

> Bei der Implementierung in mehreren AWS Availability Zones verwenden Cloud Volumes ONTAP HA-Konfigurationen eine Floating-IP-Adresse für die Cluster-Management-Schnittstelle, was bedeutet, dass externes Routing nicht verfügbar ist. Sie müssen eine Verbindung von einem Host herstellen, der Teil derselben Routingdomäne ist.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf das Cloud Volumes ONTAP System, das Sie mit System Manager managen möchten.
2. Klicken Sie auf das Menüsymbol und dann auf **Erweitert > System Manager**.
3. Klicken Sie Auf **Start**.

   System Manager wird in eine neue Browser-Registerkarte geladen.

4. Geben Sie im Anmeldebildschirm im Feld Benutzername * das Passwort ein, das Sie beim Erstellen der Arbeitsumgebung angegeben haben, und klicken Sie dann auf **Anmelden**.

Ergebnis

Die System Manager-Konsole wird geladen. Sie können es jetzt zum Managen von Cloud Volumes ONTAP verwenden.

Herstellen einer Verbindung zur Cloud Volumes ONTAP CLI

Die Cloud Volumes ONTAP CLI ermöglicht Ihnen die Ausführung aller administrativen Befehle und ist eine gute Wahl für erweiterte Aufgaben oder wenn Sie sich mit der CLI besser vertraut machen. Sie können über Secure Shell (SSH) eine Verbindung zur CLI herstellen.

Bevor Sie beginnen

Der Host, von dem aus Sie SSH für die Verbindung zu Cloud Volumes ONTAP verwenden, muss über eine Netzwerkverbindung zu Cloud Volumes ONTAP verfügen. Sie müssen beispielsweise SSH von einem Jump Host in AWS oder Azure verwenden.

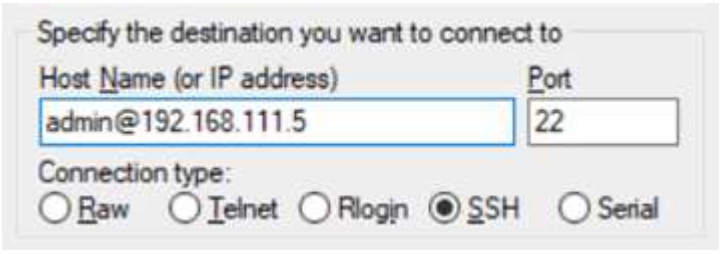
> Wenn Cloud Volumes ONTAP HA in mehreren AZS implementiert wird, verwenden sie eine Floating-IP-Adresse für die Cluster-Management-Schnittstelle, was bedeutet, dass externes Routing nicht verfügbar ist. Sie müssen eine Verbindung von einem Host herstellen, der Teil derselben Routingdomäne ist.

Schritte

1. Identifizieren Sie in Cloud Manager die IP-Adresse der Cluster-Management-Schnittstelle:
   a. Wählen Sie auf der Seite Arbeitsumgebungen das Cloud Volumes ONTAP System aus.
   b. Kopieren Sie die IP-Adresse der Clusterverwaltung, die im rechten Fensterbereich angezeigt wird.
2. Verwenden Sie SSH, um über das Administratorkonto eine Verbindung zur IP-Adresse der Cluster-Managementschnittstelle herzustellen.

   Beispiel

   Das folgende Bild zeigt ein Beispiel mit PuTTY:



3. Geben Sie an der Anmeldeaufforderung das Kennwort für das Administratorkonto ein.

   Beispiel

```
Password: ********
COT2::>
```

Hinzufügen vorhandener Cloud Volumes ONTAP Systeme zu Cloud Manager

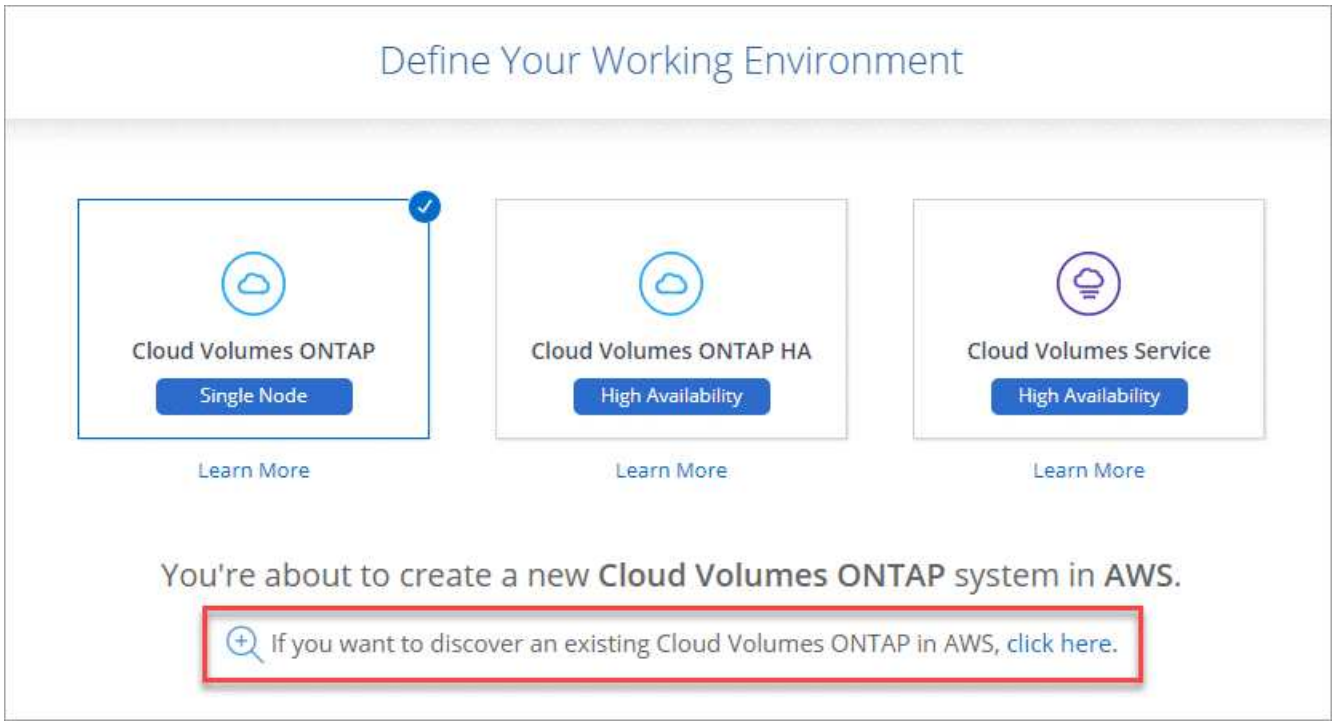
Sie können vorhandene Cloud Volumes ONTAP Systeme erkennen und zu Cloud Manager hinzufügen. Das könnte Sie erreichen, wenn Sie ein neues Cloud Manager System implementieren.

Bevor Sie beginnen

Sie müssen das Kennwort für das Cloud Volumes ONTAP Admin-Benutzerkonto kennen.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen**.
2. Wählen Sie den Cloud-Provider aus, in dem sich das System befindet.
3. Wählen Sie den Typ des Cloud Volumes ONTAP Systems aus.
4. Klicken Sie auf den Link, um ein vorhandenes System zu ermitteln.



5. Wählen Sie auf der Seite Region den Bereich aus, in dem die Instanzen ausgeführt werden, und wählen Sie dann die Instanzen aus.
6. Geben Sie auf der Seite Anmeldeinformationen das Kennwort für den Cloud Volumes ONTAP-Admin-Benutzer ein, und klicken Sie dann auf **Los**.

Ergebnis

Cloud Manager fügt den Arbeitsbereich die Cloud Volumes ONTAP-Instanzen hinzu.

Löschen einer Cloud Volumes ONTAP Arbeitsumgebung

Am besten löschen Sie die Cloud Volumes ONTAP Systeme aus dem Cloud Manager, nicht jedoch von der Konsole Ihres Cloud-Providers. Wenn Sie beispielsweise eine lizenzierte Cloud Volumes ONTAP-Instanz von AWS beenden, können Sie den

Lizenzschlüssel für eine andere Instanz nicht verwenden. Sie müssen die Arbeitsumgebung aus Cloud Manager löschen, um die Lizenz freizugeben.

Über diese Aufgabe

Wenn Sie eine Arbeitsumgebung löschen, beendet Cloud Manager Instanzen, löscht Festplatten und Snapshots.

> Cloud Volumes ONTAP Instanzen verfügen über einen aktivierten Kündigungsschutz, um eine versehentliche Beendigung von AWS zu verhindern. Wenn Sie jedoch eine Cloud Volumes ONTAP Instanz von AWS beenden, müssen Sie zur Konsole AWS CloudFormation wechseln und den Stack der Instanz löschen. Der Stack-Name ist der Name der Arbeitsumgebung.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Löschen**.
2. Geben Sie den Namen der Arbeitsumgebung ein und klicken Sie dann auf **Löschen**.

   Das Löschen der Arbeitsumgebung kann bis zu 5 Minuten dauern.