



Konzepte

Cloud Manager 3.6

NetApp
March 25, 2024

Inhalt

- Konzepte 1
 - Überblick über Cloud Manager und Cloud Volumes ONTAP 1
 - NetApp Cloud Central 2
 - Konten und Berechtigungen für Cloud-Provider 3
 - Storage 7
 - Hochverfügbarkeitspaare 21
 - Bewertung 30
 - Lizenzierung 30
 - Sicherheit 31
 - Leistung 33

Konzepte

Überblick über Cloud Manager und Cloud Volumes ONTAP

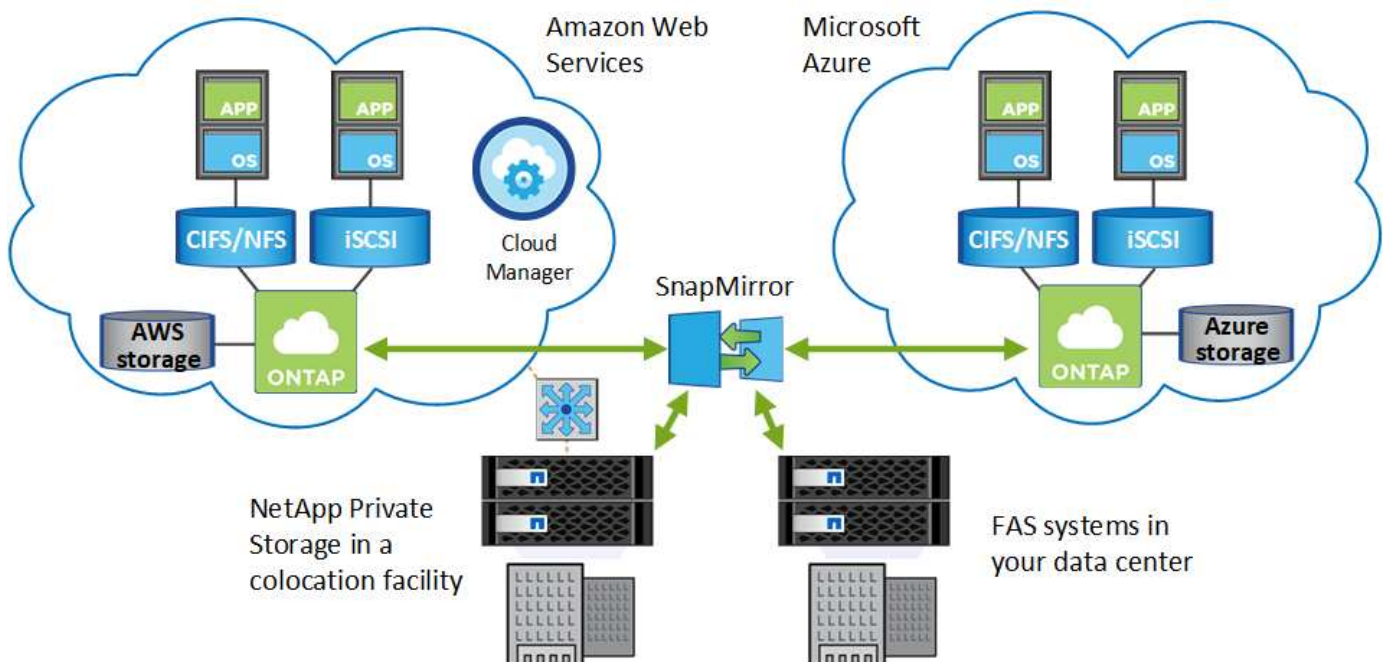
Mit OnCommand Cloud Manager können Sie Cloud Volumes ONTAP implementieren, das Funktionen der Enterprise-Klasse für Ihren Cloud-Storage bietet, und Daten einfach über Hybrid Clouds hinweg replizieren, die auf NetApp basieren.

Cloud Manager

Cloud Manager wurde mit Blick auf Einfachheit entwickelt. Sie führt Sie in wenigen Schritten durch die Cloud Volumes ONTAP Einrichtung und erleichtert das Datenmanagement durch vereinfachte Storage-Provisionierung und automatisiertes Kapazitätsmanagement, ermöglicht Datenreplizierung per Drag-and-Drop in einer Hybrid Cloud und vieles mehr.

Cloud Manager ist für die Implementierung und das Management von Cloud Volumes ONTAP erforderlich, kann aber auch Storage für On-Premises ONTAP Cluster erkennen und bereitstellen. Dies stellt einen zentralen Kontrollpunkt für Ihre Cloud und lokale Storage-Infrastruktur dar.

Sie können Cloud Manager in der Cloud oder in Ihrem Netzwerk ausführen. Sie benötigen lediglich eine Verbindung zu den Netzwerken, in denen Sie Cloud Volumes ONTAP implementieren möchten. Das folgende Bild zeigt Cloud Manager, der in AWS ausgeführt wird und Cloud Volumes ONTAP Systeme in AWS und Azure verwaltet. Außerdem wird die Datenreplizierung in einer Hybrid Cloud dargestellt.



["Erfahren Sie mehr über Cloud Manager"](#)

Cloud Volumes ONTAP

Cloud Volumes ONTAP ist eine reine Software-Storage Appliance, die die ONTAP Datenmanagement-Software in der Cloud ausführt. Sie können Cloud Volumes ONTAP für Produktions-Workloads, Disaster Recovery, DevOps, Dateifreigaben und Datenbankmanagement verwenden.

Cloud Volumes ONTAP erweitert Enterprise Storage mit den folgenden Hauptfunktionen auf die Cloud:

- Storage-Effizienz Nutzen Sie die integrierte Datendeduplizierung, Datenkomprimierung, Thin Provisioning und Klonen, um Storage-Kosten zu minimieren.
- Hochverfügbarkeit und Sicherstellung der Zuverlässigkeit der Enterprise-Klasse sowie eines unterbrechungsfreien Betriebs bei Ausfällen in der Cloud-Umgebung
- Datenreplizierung Cloud Volumes ONTAP nutzt SnapMirror, die branchenführende Replizierungstechnologie von NetApp, um lokale Daten in die Cloud zu replizieren. So ist es ganz einfach, sekundäre Kopien für mehrere Anwendungsfälle verfügbar zu haben.
- Daten-Tiering Wechsel zwischen hoch- und leistungsarmen Speicherpools nach Bedarf, ohne Applikationen offline zu schalten.
- Applikationskonsistenz stellen mit NetApp SnapCenter die Konsistenz von NetApp Snapshot Kopien sicher.



Lizenzen für ONTAP Funktionen sind in Cloud Volumes ONTAP enthalten, mit Ausnahme von NetApp Volume Encryption.

["Anzeigen der unterstützten Cloud Volumes ONTAP Konfigurationen"](#)

["Erfahren Sie mehr über Cloud Volumes ONTAP"](#)

NetApp Cloud Central

"NetApp Cloud Central" Zentraler Standort zum Zugriff auf NetApp Cloud Data Services und Management Mit diesen Services können Sie kritische Applikationen in der Cloud ausführen, automatisierte DR-Standorte erstellen, Ihre SaaS-Daten sichern und Daten effektiv über mehrere Clouds hinweg migrieren und steuern.

Die Integration von Cloud Manager in NetApp Cloud Central bietet verschiedene Vorteile, darunter eine vereinfachte Implementierung, ein zentraler Speicherort zum Anzeigen und Managen mehrerer Cloud Manager-Systeme und eine zentralisierte Benutzerauthentifizierung.

Mit der zentralisierten Benutzerauthentifizierung können Sie dieselben Anmeldedaten für Cloud Manager-Systeme und zwischen Cloud Manager und anderen Datenservices wie Cloud Sync verwenden. Sie können Ihr Passwort auch einfach zurücksetzen, wenn Sie es vergessen haben.

Das folgende Video bietet einen Überblick über NetApp Cloud Central:

Hi Kevin Hill, let's get started!



ONTAP Cloud

Loading...

[More Info](#)



Cloud Sync

Loading...

[More Info](#)



Cloud Control

[Go to Cloud Control](#)

[More Info](#)



Azure NFSaaS

[Register for Preview](#)

[More Info](#)



NFS Hybrid For AWS

[Register for Preview](#)

[More Info](#)

API

Konten und Berechtigungen für Cloud-Provider

Mit Cloud Manager können Sie das *Cloud-Provider-Konto* auswählen, in dem Sie ein Cloud Volumes ONTAP System implementieren möchten. Sie sollten die Berechtigungsanforderungen kennen, bevor Sie die Konten zu Cloud Manager hinzufügen.

AWS Konten und Berechtigungen

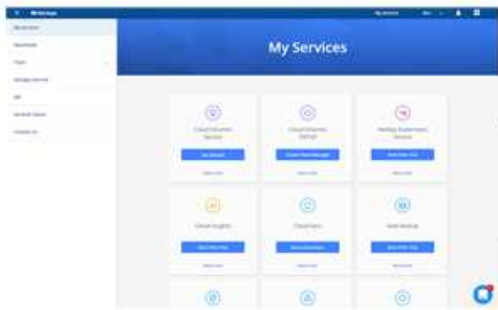
Sie können alle Ihre Cloud Volumes ONTAP Systeme über das erste AWS Konto oder weitere Konten einrichten.

Über das erste AWS Konto

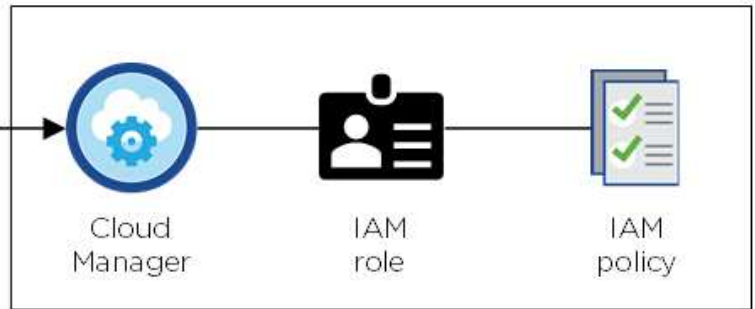
Wenn Sie Cloud Manager über NetApp Cloud Central implementieren, müssen Sie ein AWS Konto mit Berechtigungen zum Starten der Cloud Manager Instanz verwenden. Die erforderlichen Berechtigungen werden im aufgeführt "[NetApp Cloud Central-Richtlinie für AWS](#)".

Wenn Cloud Central die Cloud Manager Instanz in AWS startet, wird eine IAM-Rolle und ein Instanzprofil für die Instanz erstellt. Zudem wird eine Richtlinie angehängt, die Cloud Manager Berechtigungen für die Implementierung und das Management von Cloud Volumes ONTAP in diesem AWS-Konto bereitstellt. "[Überprüfen Sie, wie Cloud Manager die Berechtigungen verwendet](#)".

Cloud Central



AWS account



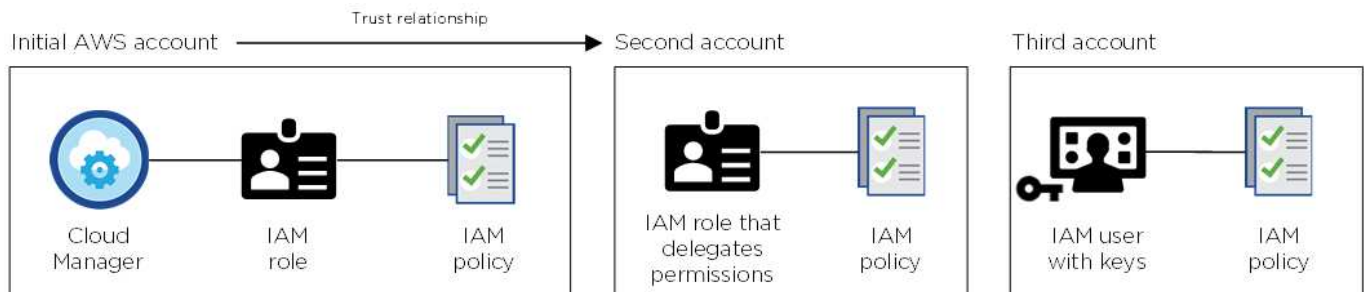
Cloud Manager wählt bei der Erstellung einer neuen Arbeitsumgebung standardmäßig dieses Cloud-Provider-Konto aus:

Details & Credentials

This working environment will be created in Cloud Provider Account: Instance Profile | Account ID: [REDACTED] | [Switch Account](#)

Weitere AWS Konten

Wenn Sie Cloud Volumes ONTAP in verschiedenen AWS Accounts starten möchten, haben Sie eine der Möglichkeiten "[AWS Schlüssel für einen IAM-Benutzer oder den ARN einer Rolle in einem vertrauenswürdigen Konto bereitstellen](#)". Die folgende Abbildung zeigt zwei zusätzliche Konten: Eines mit Berechtigungen über eine IAM-Rolle in einem vertrauenswürdigen Konto und ein weiteres über die AWS Schlüssel eines IAM-Benutzers:



Das würden Sie dann tun "[Fügen Sie die Cloud-Provider-Konten zu Cloud Manager hinzu](#)" indem Sie den Amazon Resource Name (ARN) der IAM-Rolle oder die AWS-Schlüssel für den IAM-Benutzer angeben.

Nachdem Sie ein weiteres Konto hinzugefügt haben, können Sie zu diesem wechseln, wenn Sie eine neue Arbeitsumgebung erstellen:

Cloud Provider Profile Name

QA | Account ID: [REDACTED]

Instance Profile | Account ID: [REDACTED]

To add a new AWS cloud provider account, go to the [Cloud Provider Account Settings](#).

Apply

Cancel

Azure-Konten und Berechtigungen

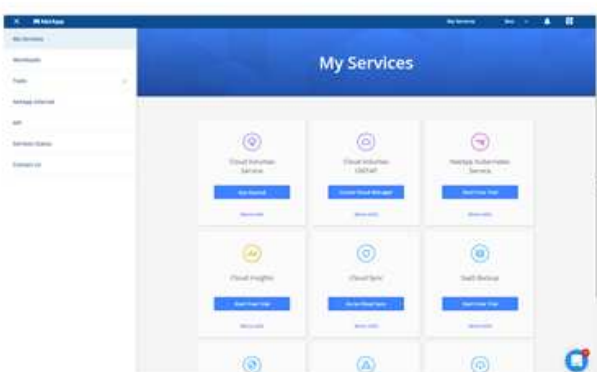
Sie können alle Ihre Cloud Volumes ONTAP Systeme über das erste Azure Konto oder weitere Konten einrichten.

Zunächst das Azure-Konto

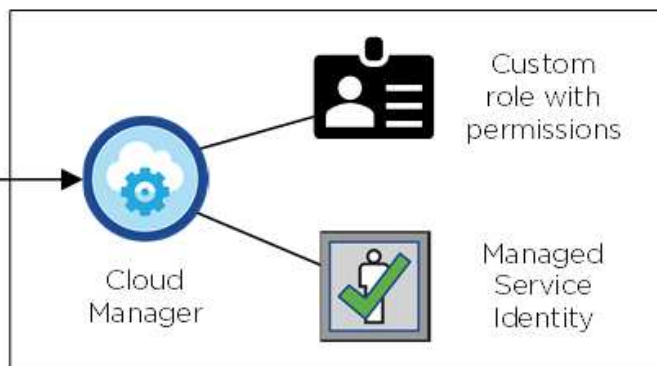
Wenn Sie Cloud Manager über NetApp Cloud Central implementieren, müssen Sie ein Azure Konto verwenden, das über Berechtigungen zum Bereitstellen der Virtual Machine von Cloud Manager verfügt. Die erforderlichen Berechtigungen werden im aufgeführt ["NetApp Cloud Central-Richtlinie für Azure"](#).

Wenn Cloud Central die Virtual Machine Cloud Manager in Azure implementiert, wird damit eine aktiviert ["Vom System zugewiesene verwaltete Identität"](#) Erstellt auf der Cloud Manager Virtual Machine eine benutzerdefinierte Rolle und weist sie der Virtual Machine zu. Die Rolle bietet Cloud Manager Berechtigungen für die Implementierung und das Management von Cloud Volumes ONTAP in diesem Azure Abonnement. ["Überprüfen Sie, wie Cloud Manager die Berechtigungen verwendet"](#).

Cloud Central



Azure account



Cloud Manager wählt bei der Erstellung einer neuen Arbeitsumgebung standardmäßig dieses Cloud-Provider-Konto aus:

Details & Credentials

This working environment will be created in Cloud Provider Account: [Managed Service Identity](#) | Azure Subscription: [OCCM QA1](#) | [Switch Account](#)

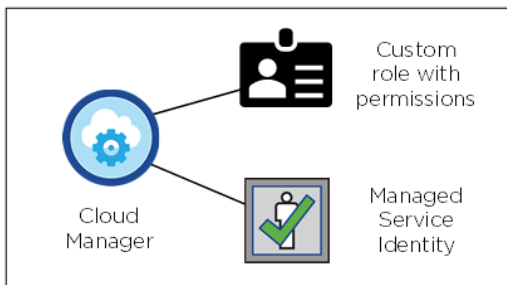
Zusätzliche Azure-Abonnements für das Erstkonto

Die verwaltete Identität ist mit dem Abonnement verknüpft, in dem Sie Cloud Manager gestartet haben. Wenn Sie ein anderes Azure Abonnement auswählen möchten, müssen Sie es ausführen "[Verknüpfen Sie die verwaltete Identität mit diesen Abonnements](#)".

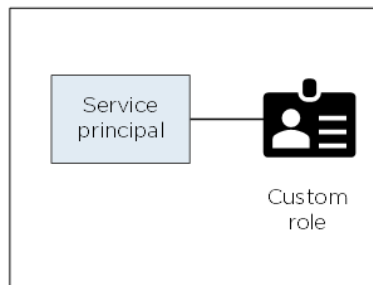
Zusätzliche Azure-Konten

Wenn Sie Cloud Volumes ONTAP in verschiedenen Azure Accounts implementieren möchten, müssen Sie die erforderlichen Berechtigungen von erteilen "[Erstellen und Einrichten eines Service Principal in Azure Active Directory](#)" Für jedes Azure Konto. Das folgende Bild zeigt zwei zusätzliche Konten, die jeweils mit einer Dienstprinzipal- und einer benutzerdefinierten Rolle eingerichtet sind, die Berechtigungen bereitstellt:

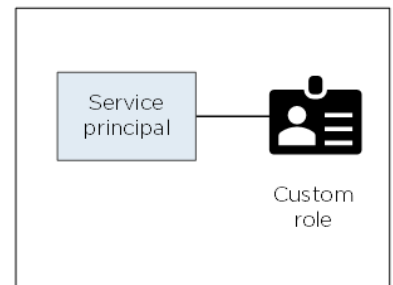
Initial Azure account



Second account



Third account



Das würden Sie dann tun "[Fügen Sie die Cloud-Provider-Konten zu Cloud Manager hinzu](#)" Durch Angabe von Details zum AD-Dienstprinzipal.

Nachdem Sie ein weiteres Konto hinzugefügt haben, können Sie zu diesem wechseln, wenn Sie eine neue Arbeitsumgebung erstellen:



Cloud Provider Profile Name

Azure Keys Application ID: [redacted] ...
Dev Keys Application ID: [redacted] ...
Managed Service Identity

To add a new Azure cloud provider account, go to the [Cloud Provider Account Settings](#).

Apply

Cancel

Wie sieht es mit Marketplace-Implementierungen und On-Premises-Implementierungen aus?

In den obigen Abschnitten wird die empfohlene Implementierungsmethode von NetApp Cloud Central beschrieben. Sie können Cloud Manager auch über die implementieren "[AWS Marketplace](#)", Das "[Azure Marketplace](#)", Und Sie können "[Installation von Cloud Manager vor Ort](#)".

Wenn Sie einen der Marktplätze verwenden, werden Berechtigungen auf die gleiche Weise bereitgestellt. Sie müssen lediglich die IAM-Rolle oder die gemanagte Identität für Cloud Manager manuell erstellen und einrichten und dann die Berechtigungen für weitere Konten bereitstellen.

Bei On-Premises-Implementierungen können Sie keine IAM-Rolle einrichten oder eine gemanagte Identität für das Cloud Manager System einrichten, Sie können jedoch Berechtigungen wie bei zusätzlichen Konten bereitstellen.

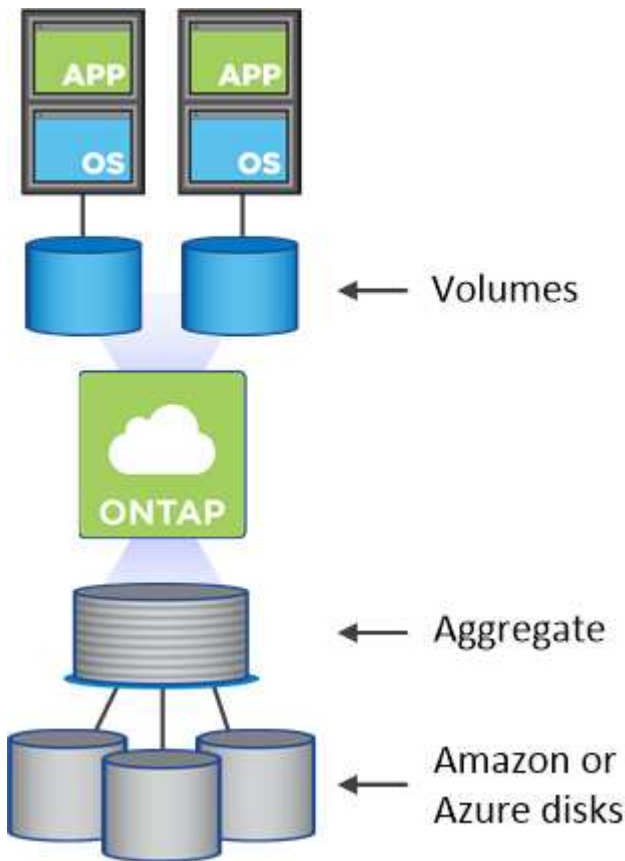
Storage

Wie Cloud Volumes ONTAP Cloud Storage verwendet

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

Überblick

Cloud Volumes ONTAP verwendet AWS und Azure Volumes als Back-End Storage. Diese Volumes werden als Festplatten betrachtet und in einem oder mehreren Aggregaten gruppiert. Aggregate stellen Storage für ein oder mehrere Volumes bereit.



Es werden mehrere Arten von Cloud-Festplatten unterstützt. Sie wählen beim Erstellen von Volumes den Festplattentyp und bei der Implementierung von Cloud Volumes ONTAP die Standardfestplattengröße aus.



Der gesamte Storage, der von AWS oder Azure gekauft wird, 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 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. Es ist auch möglich, eine EBS-Festplatte für zu koppeln "[Daten-Tiering](#)".

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.

Weitere Details zu den Anwendungsfällen für diese Festplatten finden Sie unter ["AWS Dokumentation: EBS Volume-Typen"](#).

["Lesen Sie, wie Sie Festplattentypen und Festplattengrößen für Ihre Systeme in AWS auswählen"](#).

["Prüfen der Storage-Limits für Cloud Volumes ONTAP"](#).

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 für kombinieren ["Daten-Tiering"](#).

HA-Paare

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

Weitere Details zu den Anwendungsfällen für diese Festplatten finden Sie unter ["Microsoft Azure-Dokumentation: Einführung in Microsoft Azure Storage"](#).

["Erfahren Sie, wie Sie Festplattentypen und Festplattengrößen für Ihre Systeme in Azure auswählen"](#).

["Prüfen der Storage-Limits für Cloud Volumes ONTAP"](#).

Data Tiering - Übersicht

Sie können Ihre Storage-Kosten senken, indem Sie das automatisierte Tiering inaktiver Daten auf kostengünstigen Objekt-Storage ermöglichen. Aktive Daten verbleiben in

hochperformanten SSDs oder HDDs (dem Performance-Tier), während inaktive Daten auf kostengünstigen Objektspeicher (dem Kapazitäts-Tier) gestaffelt werden. Dadurch können Sie Speicherplatz auf Ihrem primären Storage zurückgewinnen und den sekundären Storage verkleinern.

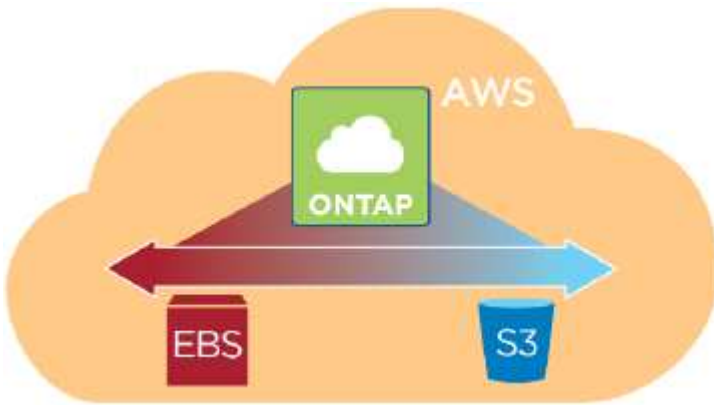
Cloud Volumes ONTAP unterstützt Daten-Tiering in AWS und in Microsoft Azure. Data Tiering wird durch FabricPool Technologie unterstützt.



Sie müssen keine Funktionslizenz installieren, um Data Tiering zu aktivieren.

Funktionsweise von Data 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 in AWS

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

Kapazitäts-Tier in AWS

Standardmäßig schichtet Cloud Volumes ONTAP inaktive Daten in die Storage-Klasse S3 *Standard* aus. Standard ist ideal für häufig aufgerufene Daten, die über mehrere Verfügbarkeitszonen gespeichert werden.

Wenn Sie keinen Zugriff auf inaktive Daten planen, können Sie Ihre Speicherkosten reduzieren, indem Sie die Tiering-Ebene eines Systems auf eine der folgenden Stufen ändern, nachdem Sie Cloud Volumes ONTAP bereitgestellt haben:

Intelligentes Tiering

Optimiert Storage-Kosten, indem bei sich ändernden Datenzugriffsmustern Daten zwischen zwei Tiers verschoben werden. Eine Ebene ist für häufigen Zugriff und die andere für unregelmäßigen Zugriff.

Ein einmaliger Zugriff

Für selten genutzte Daten, die in einer einzigen Verfügbarkeitszone gespeichert sind.

Standardzugriff

Für selten genutzte Daten, die über mehrere Verfügbarkeitszonen hinweg gespeichert werden.

Die Zugriffskosten sind höher, wenn Sie auf die Daten zugreifen. Daher müssen Sie dies berücksichtigen,

bevor Sie die Tiering Level ändern. Weitere Informationen zu S3-Speicherklassen finden Sie unter ["AWS-Dokumentation"](#).

Wenn Sie die Tiering-Ebene ändern, werden inaktive Daten in der Klasse Standard-Speicher gestartet und in die von Ihnen ausgewählte Speicherkategorie verschoben, sofern nach 30 Tagen kein Zugriff auf die Daten erfolgt. Weitere Informationen zum Ändern der Tiering-Ebene finden Sie unter ["Tiering inaktiver Daten in kostengünstigen Objektspeicher"](#).

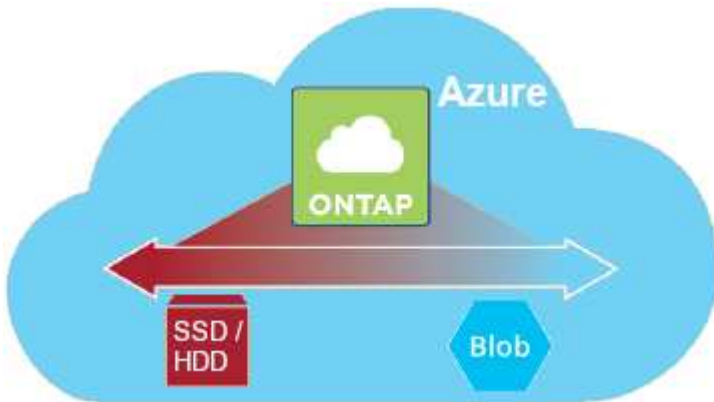
Die Tiering-Ebene ist systemweit, nicht pro Volume.



In einer Cloud Volumes ONTAP Arbeitsumgebung wird ein S3-Bucket für alle Tiered Data aus dem System verwendet. Für jedes Volume wird kein anderer S3-Bucket verwendet. Dazu gehört auch eine HA-Arbeitsumgebung. Cloud Manager erstellt einen S3-Bucket und nennt ihn Fabric-Pool-Cluster-eindeutige Kennung.

Funktionsweise von Data Tiering in Microsoft 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 in Azure

Die Performance-Ebene kann entweder Premium Storage (SSD) oder Standard Storage (HDD) sein.

Kapazitäts-Tier in Azure

Cloud Volumes ONTAP führt das Tiering inaktiver Daten standardmäßig auf den Azure Storage Tier mit Hot_ aus. Daher eignet es sich ideal für häufig genutzte Daten.

Wenn Sie keinen Zugriff auf inaktive Daten planen, können Sie nach der Implementierung von Cloud Volumes ONTAP die Storage-Kosten senken, indem Sie die Tiering-Ebene eines Systems zum Azure *cool* Storage Tier ändern. Die coole Tier eignet sich ideal für selten genutzte Daten, die sich mindestens 30 Tage in der Tier befinden.

Die Zugriffskosten sind höher, wenn Sie auf die Daten zugreifen. Daher müssen Sie dies berücksichtigen, bevor Sie die Tiering Level ändern. Weitere Informationen zu Azure Blob Storage-Tiers finden Sie unter ["Azure-Dokumentation"](#).

Wenn Sie das Tiering-Level ändern, beginnen inaktive Daten im Storage-Tier, und verschieben sich in den „kühlen“ Speicher-Tier, sofern nach 30 Tagen kein Zugriff auf die Daten erfolgt. Weitere Informationen zum Ändern der Tiering-Ebene finden Sie unter ["Tiering inaktiver Daten in kostengünstigen Objektspeicher"](#).

Die Tiering-Ebene ist systemweit, nicht pro Volume.



Eine Cloud Volumes ONTAP Arbeitsumgebung verwendet einen Azure Blob Container für alle Tiered Daten aus dem System. Für jedes Volume wird kein anderer Container verwendet. Cloud Manager erstellt ein neues Storage-Konto mit einem Container für jedes Cloud Volumes ONTAP System. Der Name des Speicherkontos ist zufällig.

Auswirkungen von Data Tiering auf 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 Volumes ONTAP unterstützt die folgenden Tiering Policies:

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.

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 Antivirenschans, bleiben die kalten Datenblöcke kalt und wechseln nicht zur Performance-Ebene.

Backup

Wenn Sie ein Volume für Disaster Recovery oder langfristige Aufbewahrung replizieren, beginnen die Daten für das Ziel-Volume in der Kapazitäts-Tier. Wenn Sie das Ziel-Volume aktivieren, werden die Daten beim Lesen schrittweise auf die Performance-Ebene verschoben.

Keine

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

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 Cloud Manager Administrator 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 Cloud Manager Admin kann wählen, ob Cloud Manager Sie über Entscheidungen zur Storage-Kapazität benachrichtigt oder ob Cloud Manager automatisch die Kapazitätsanforderungen für Sie managt. Es könnte Ihnen dabei helfen, die Funktionsweise dieser Modi zu verstehen.

Automatisches Kapazitätsmanagement

Wenn der Cloud Manager Administrator den Kapazitätsmanagement-Modus auf automatisch eingestellt hat, 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 bei Bedarf und versucht, Festplatten nicht ordnungsgemäß wiederherzustellen.

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 an AWS oder Azure zurückgegeben werden.

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

Manuelles Kapazitätsmanagement

Wenn der Cloud Manager Admin den Capacity Management-Modus auf "Manuell" setzt, zeigt Cloud Manager bei Kapazitätsentscheidungen Meldungen mit dem Status "Aktion erforderlich" an. Die gleichen Beispiele, die im automatischen Modus beschrieben werden, gelten für den manuellen Modus, aber Sie müssen die Aktionen akzeptieren.

Storage-Isolierung mithilfe von Mandanten

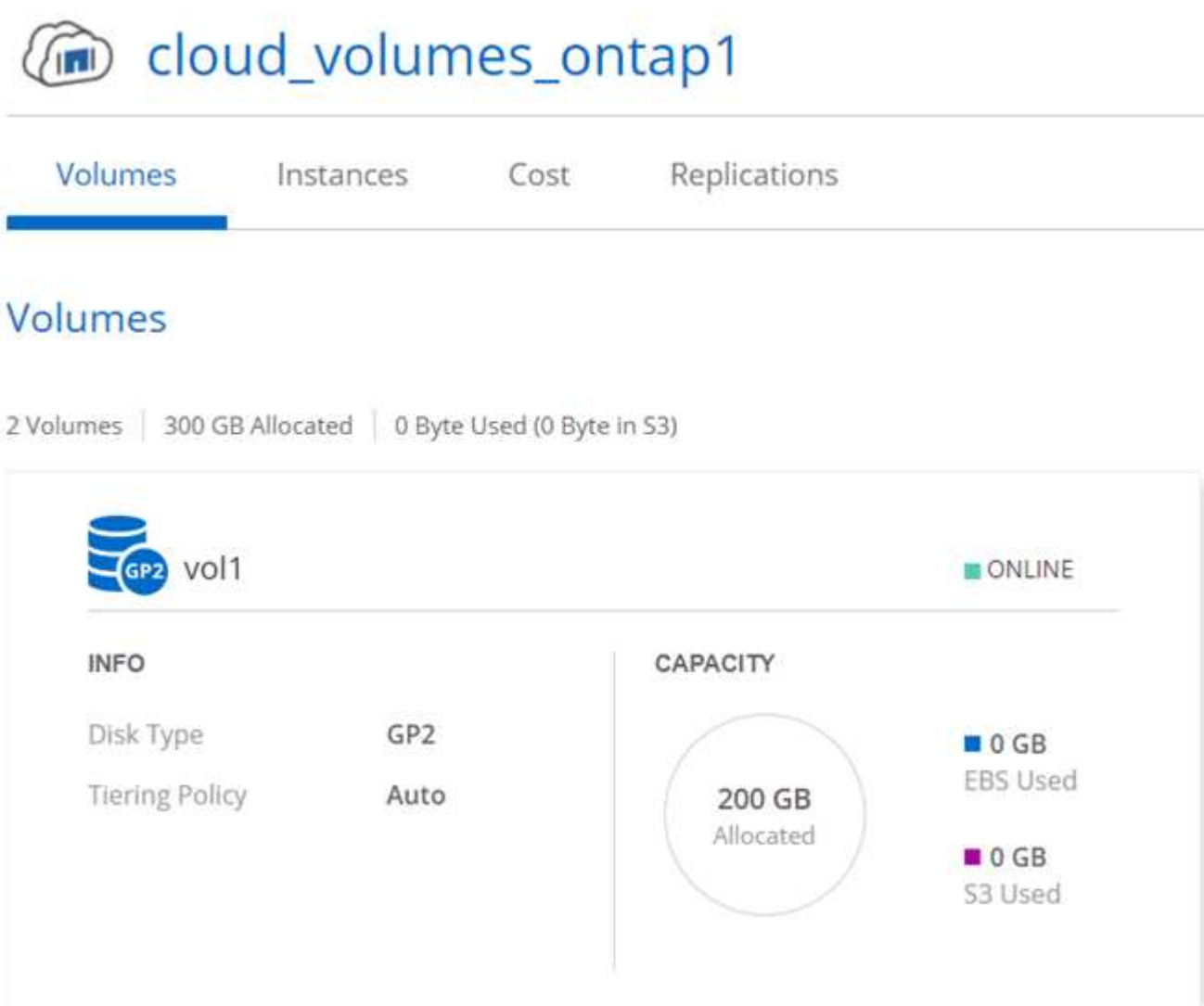
Mit Cloud Manager können Sie Storage in isolierten Gruppen, so genannten Mandanten, bereitstellen und managen. Sie müssen entscheiden, wie Cloud Manager-Benutzer und ihre Arbeitsumgebungen über Mandanten hinweg organisiert werden.

Arbeitsumgebungen

Cloud Manager repräsentiert Storage-Systeme als *Arbeitsumgebungen*. Eine Arbeitsumgebung hat folgende Eigenschaften:

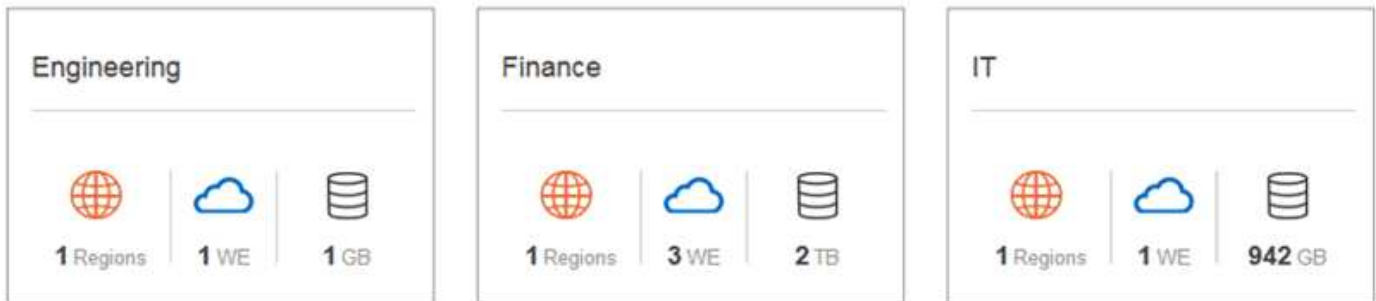
- Ein einzelnes Cloud Volumes ONTAP System oder ein HA-Paar
- Ein On-Premises ONTAP Cluster in Ihrem Netzwerk
- Ein ONTAP Cluster in einer NetApp Private Storage-Konfiguration

Das folgende Bild zeigt eine Cloud Volumes ONTAP Arbeitsumgebung:



Mandanten

A *Tenant* isoliert Arbeitsumgebungen in Gruppen. Sie erstellen eine oder mehrere Arbeitsumgebungen innerhalb eines Mandanten. Das folgende Bild zeigt drei Mandanten, die in Cloud Manager definiert sind:



Benutzerverwaltung von Mandanten und Arbeitsumgebungen

Die Mandanten und Arbeitsumgebungen, die Cloud Manager-Benutzer managen können, hängen von der Benutzerrolle und den Zuweisungen ab. Die drei unterschiedlichen Benutzerrollen sind:

Cloud Manager Admin

Verwaltet das Produkt und kann auf alle Mandanten und Arbeitsumgebungen zugreifen.

Mandantenverwaltung

Verwaltet einen einzelnen Mandanten. Kann alle Arbeitsumgebungen und Benutzer im Mandanten erstellen und verwalten.

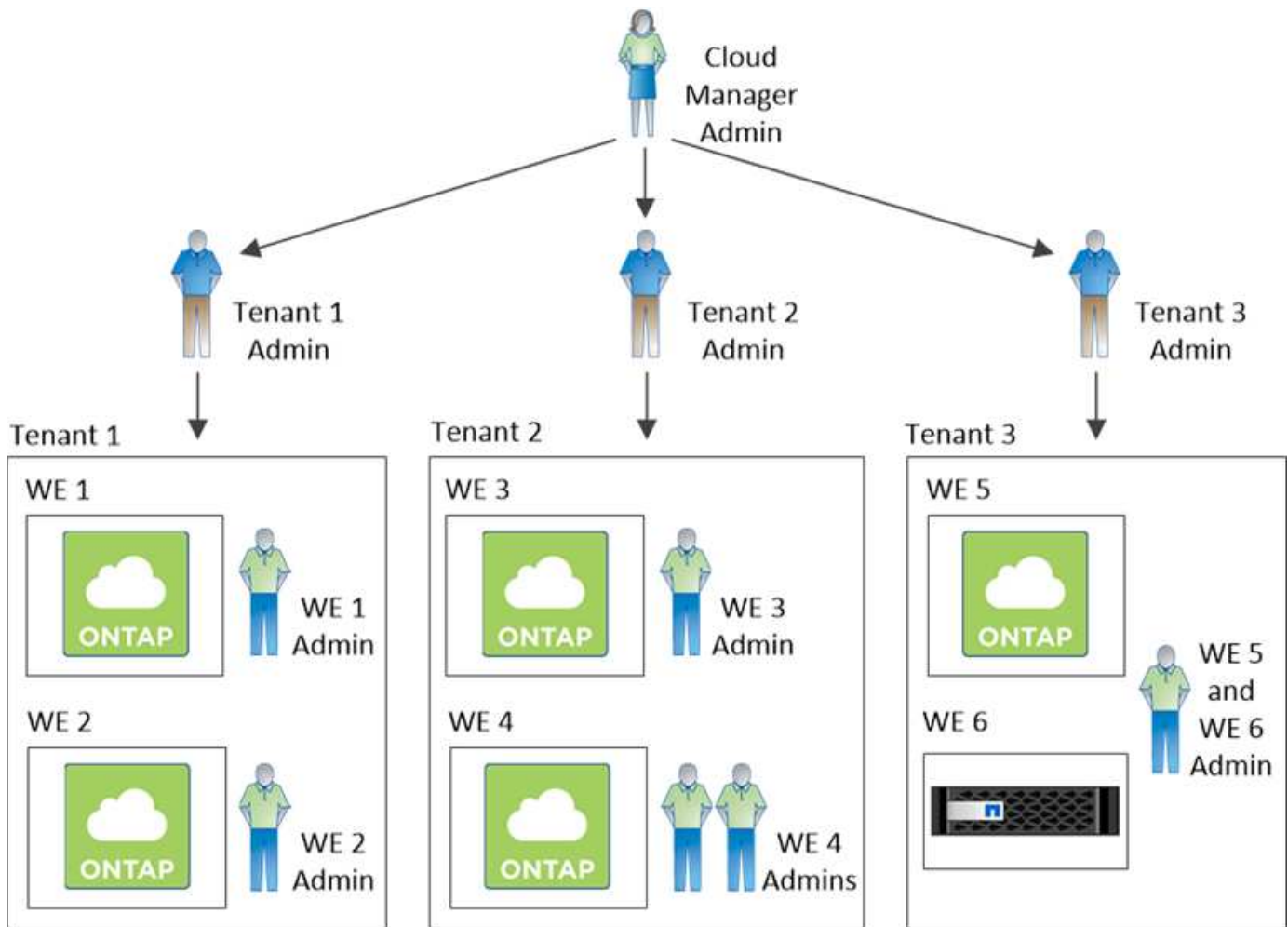
Administrator der Arbeitsumgebung

Kann eine oder mehrere Arbeitsumgebungen in einem Mandanten erstellen und managen.

Beispiel für das Erstellen von Mandanten und Benutzern

Wenn Ihr Unternehmen Abteilungen hat, die unabhängig voneinander arbeiten, ist es am besten, einen Mandanten für jede Abteilung zu haben.

Sie können beispielsweise drei Mandanten für drei separate Abteilungen erstellen. Anschließend erstellen Sie für jeden Mandanten einen Tenant Admin. Innerhalb jedes Mandanten wären ein oder mehrere Working Environment Admins, die Arbeitsumgebungen managen. Das folgende Bild zeigt dieses Szenario:

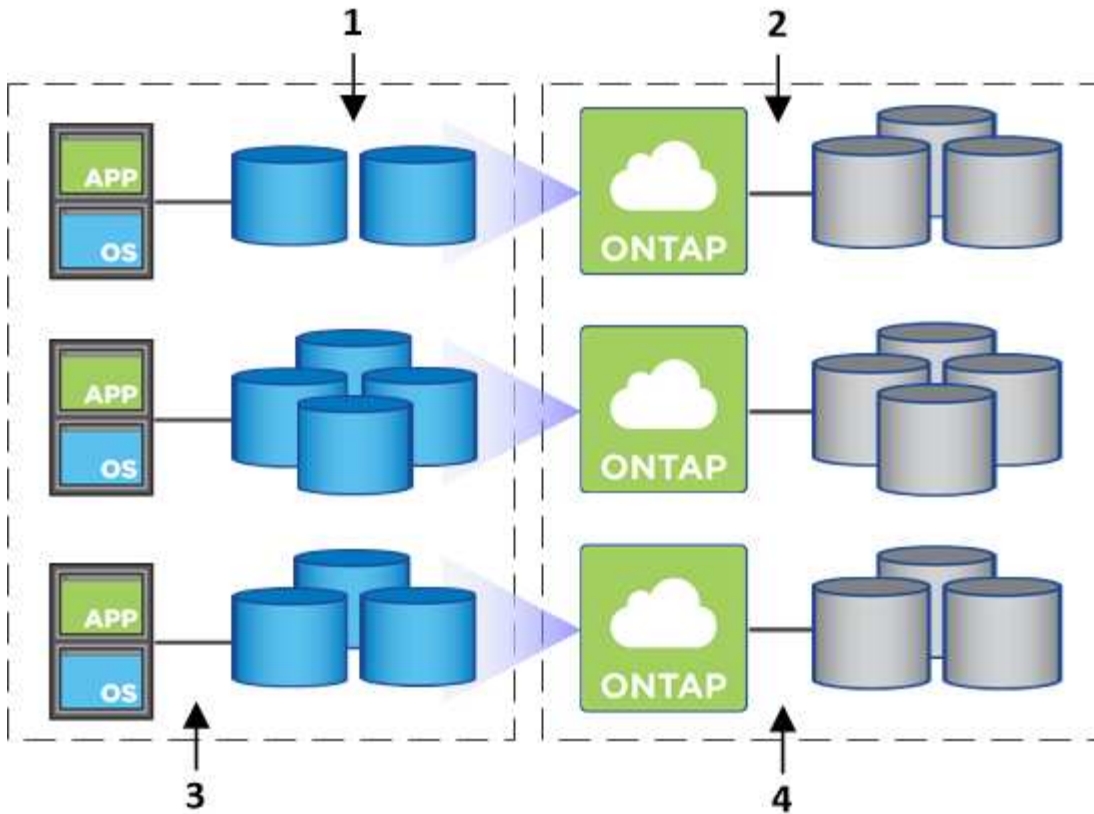


Vereinfachtes Storage-Management mit der Volume-Ansicht

Cloud Manager stellt eine separate Managementansicht namens „*Volume View*“ bereit, die das Storage-Management in AWS noch weiter vereinfacht.

Mit der Volume-Ansicht können Sie einfach die NFS-Volumes angeben, die Sie in AWS benötigen, und dann erledigt Cloud Manager den Rest: Cloud Volumes ONTAP Systeme werden nach Bedarf bereitgestellt, und die Kapazitätszuweisung wird bei wachsenden Volumes entschieden. Diese Ansicht bietet Ihnen die Vorteile von Storage der Enterprise-Klasse in der Cloud mit sehr geringem Storage-Management.

Die folgende Abbildung zeigt die Interaktion mit Cloud Manager in der Volume-Ansicht:

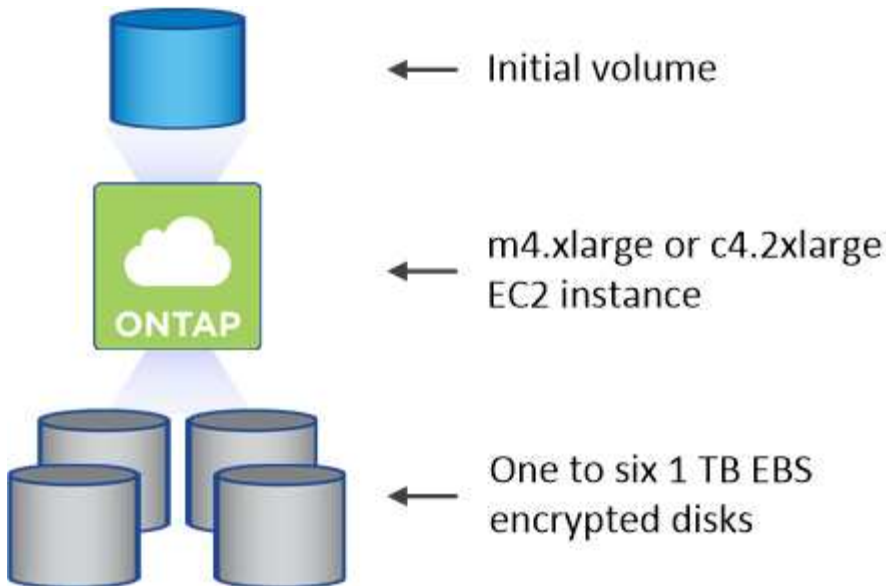


1. Sie erstellen NFS-Volumes.
2. Cloud Manager startet Cloud Volumes ONTAP Instanzen in AWS für neue Volumes oder erstellt Volumes auf vorhandenen Instanzen. Darüber hinaus wird physischer EBS Storage für die Volumes erworben.
3. Sie stellen die Volumes Ihren Hosts und Applikationen zur Verfügung.
4. Cloud Manager trifft Entscheidungen zur Kapazitätszuweisung, wenn Ihre Volumes wachsen.

Das bedeutet, dass Sie lediglich mit Volumes (das Bild links) interagieren müssen, während Cloud Manager mit dem Speichersystem und dem zugrunde liegenden Storage (das Bild rechts) interagiert.

Zuweisung von Cloud-Ressourcen für das anfängliche Volume

Wenn Sie Ihr erstes Volume erstellen, startet Cloud Manager eine Cloud Volumes ONTAP Instanz oder ein Cloud Volumes ONTAP HA Paar in AWS und kauft Amazon EBS Storage für das Volume:



Die Größe des initialen Volumes bestimmt den EC2-Instanztyp und die Anzahl der EBS-Festplatten.



Cloud Manager startet eine Cloud Volumes ONTAP Explore- oder Standardinstanz, je nach anfänglicher Volume-Größe. Wenn die Volumes wachsen, werden Sie möglicherweise von Cloud Manager aufgefordert, eine Änderung der AWS Instanz vorzunehmen, was bedeutet, dass die Lizenz der Instanz auf Standard oder Premium aktualisiert werden muss. Durch ein Upgrade wird die EBS-Rohkapazitätsgrenze erhöht, sodass Ihre Volumes wachsen können.



Cloud Manager startet Cloud Volumes ONTAP Byol Instanzen nicht in der Volume View. Sie sollten Cloud Manager in der Storage System View verwenden, wenn Sie eine Cloud Volumes ONTAP Lizenz erworben haben.

Zuweisung von Cloud-Ressourcen für zusätzliche Volumes

Wenn Sie zusätzliche Volumes erstellen, erstellt Cloud Manager die Volumes auf vorhandenen Cloud Volumes ONTAP Instanzen oder auf neuen Cloud Volumes ONTAP Instanzen. Cloud Manager kann auf einer vorhandenen Instanz ein Volume erstellen, wenn der AWS Standort und der Festplattentyp der Instanz dem angeforderten Volume entsprechen und genügend Speicherplatz zur Verfügung steht.

NetApp Storage-Effizienzfunktionen und Storage-Kosten

Cloud Manager aktiviert automatisch NetApp Storage-Effizienzfunktionen auf allen Volumes. Durch diese Effizienzsteigerungen können Sie die benötigte Storage-Gesamtmenge reduzieren. Möglicherweise unterscheiden sich Ihre zugewiesene Kapazität und die erworbene AWS-Kapazität, was zu Einsparungen bei den Storage-Kosten führen kann.

Entscheidungen zur Kapazitätzuweisung, die Cloud Manager automatisch übernimmt

- Cloud Manager erwirbt zusätzliche EBS-Festplatten, wenn Kapazitätsschwellenwerte überschritten werden. Dies geschieht, wenn Ihre Volumes wachsen.
- Cloud Manager löscht ungenutzte Sätze von EBS-Festplatten, wenn die Festplatten 12 Stunden lang keine Volumes enthalten.
- Cloud Manager verschiebt Volumes zwischen Festplattensätzen, um Kapazitätsprobleme zu vermeiden.

In einigen Fällen ist der Erwerb zusätzlicher EBS-Festplatten erforderlich. Außerdem wird Speicherplatz

auf dem ursprünglichen Satz von Festplatten für neue und vorhandene Volumes freigegeben.

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 Aktivierungscode 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:

WORM | *Preview*

You can use **write once, read many (WORM)** storage to retain critical files in unmodified form for regulatory and governance purposes and to protect from malware attacks. WORM files are protected at the file level. [Learn More](#)

Disable WORM Activate WORM

Notice: If you enable WORM storage, you cannot enable data tiering to object storage.

WORM Activation Code 

Worm-1111122222aaaaa

Retention Period

15

years 

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 auf Objekt-Storage nicht aktiviert werden.

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

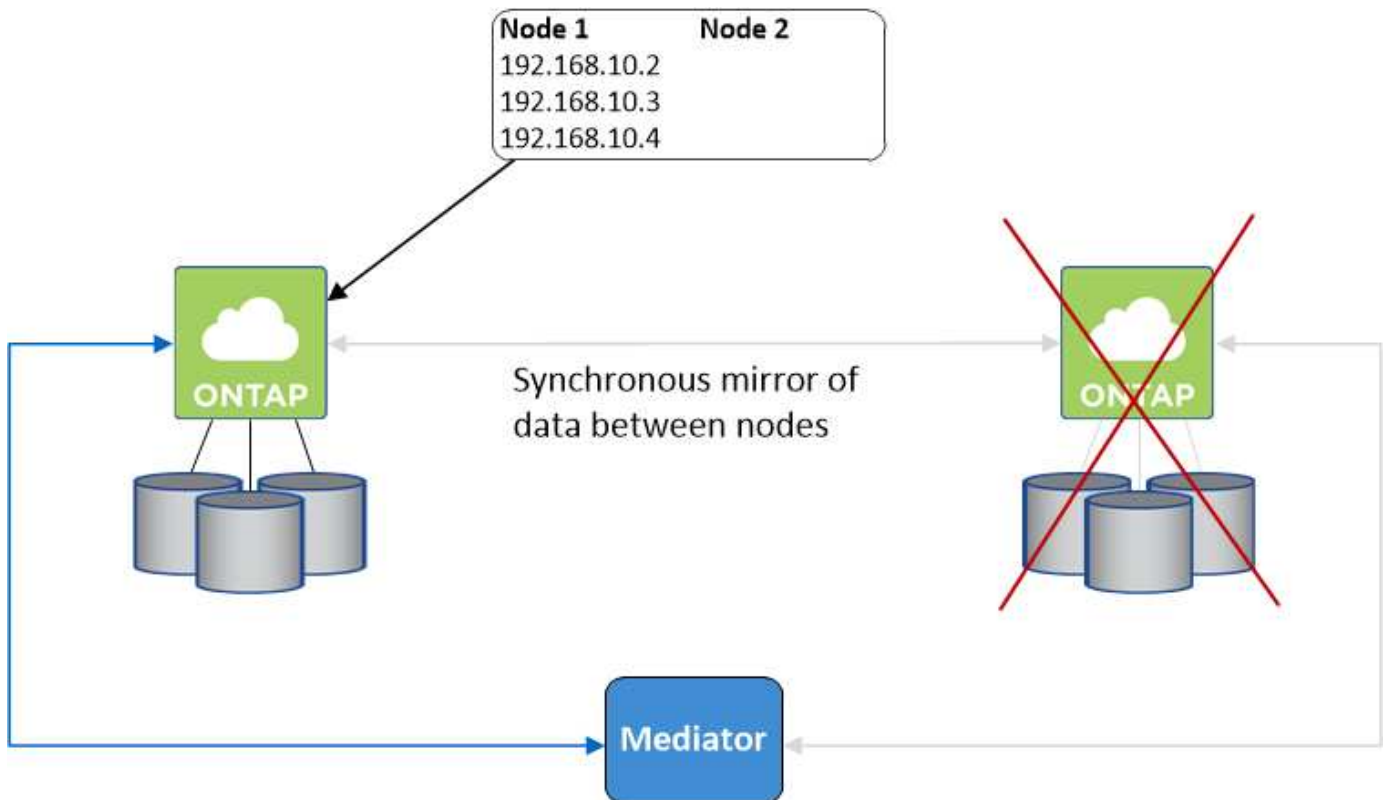
Für iSCSI verwendet Cloud Volumes ONTAP Multipath I/O (MPIO) und Asymmetric Logical Unit Access (ALUA), um das Pfad-Failover zwischen den Aktiv- und Nicht-optimierten Pfaden zu managen.



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.

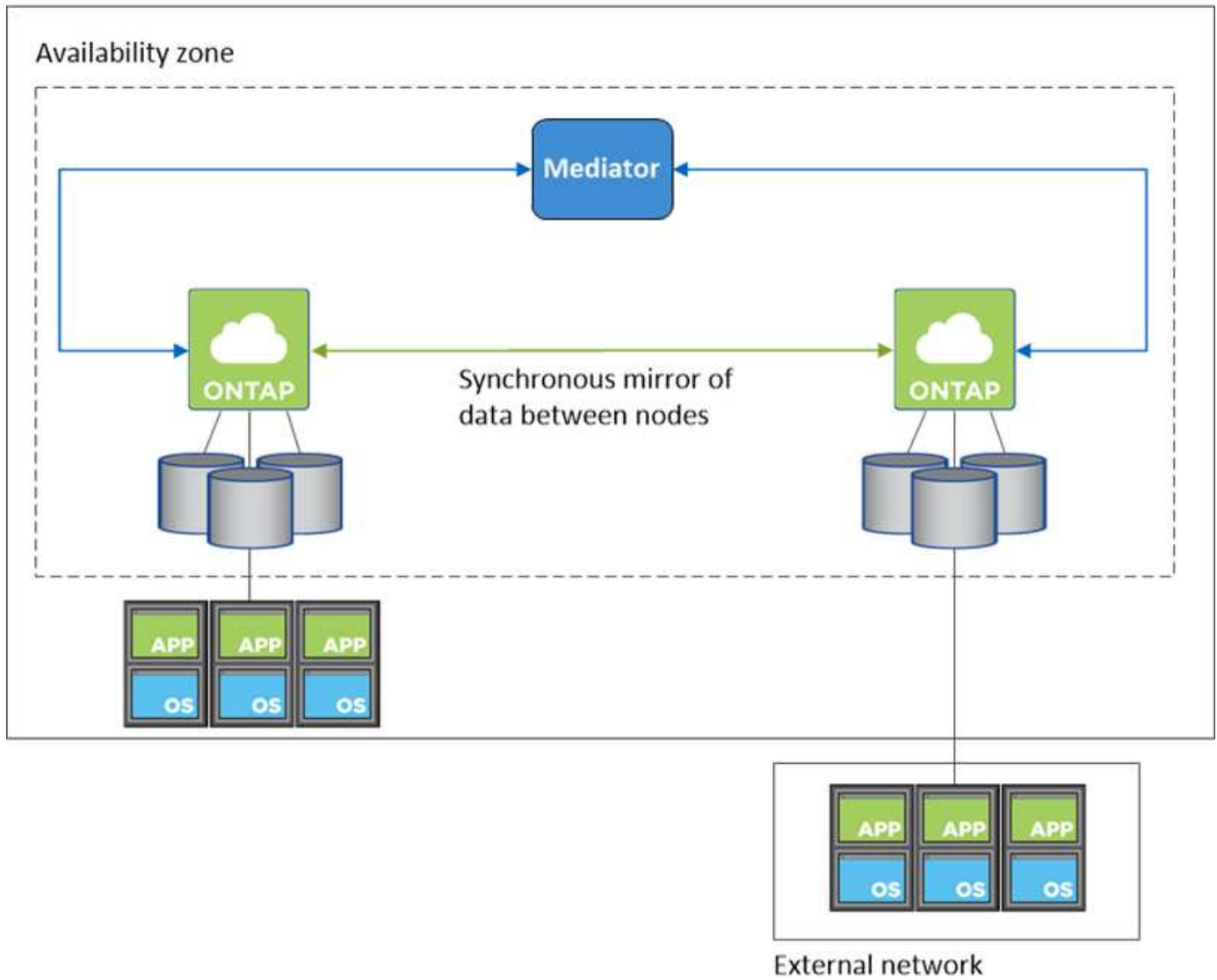


Cloud Manager erstellt eine "[AWS Spread-Platzierungsgruppe](#)" und startet die beiden HA-Nodes in dieser Platzierungsgruppe. Die Platzierungsgruppe verringert das Risiko gleichzeitiger Ausfälle, indem sie die Instanzen auf unterschiedliche zugrunde liegende Hardware verteilt. Diese Funktion verbessert 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.

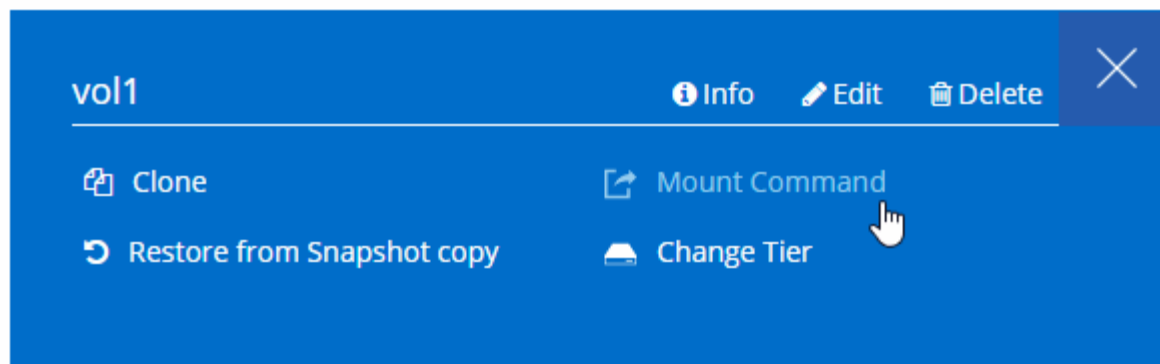


Wenn Sie ein Volume zwischen Nodes in einem HA-Paar verschieben, sollten Sie das Volume mithilfe der IP-Adresse des anderen Node neu mounten. Andernfalls kann die Performance beeinträchtigt werden. Wenn Clients NFSv4-Verweise oder Ordnerumleitung für CIFS unterstützen, können Sie diese Funktionen auf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

Die richtige IP-Adresse können Sie ganz einfach über Cloud Manager ermitteln. Die folgende Abbildung zeigt die Ansicht Storage System:

Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



Die folgende Abbildung zeigt die Volume-Ansicht:

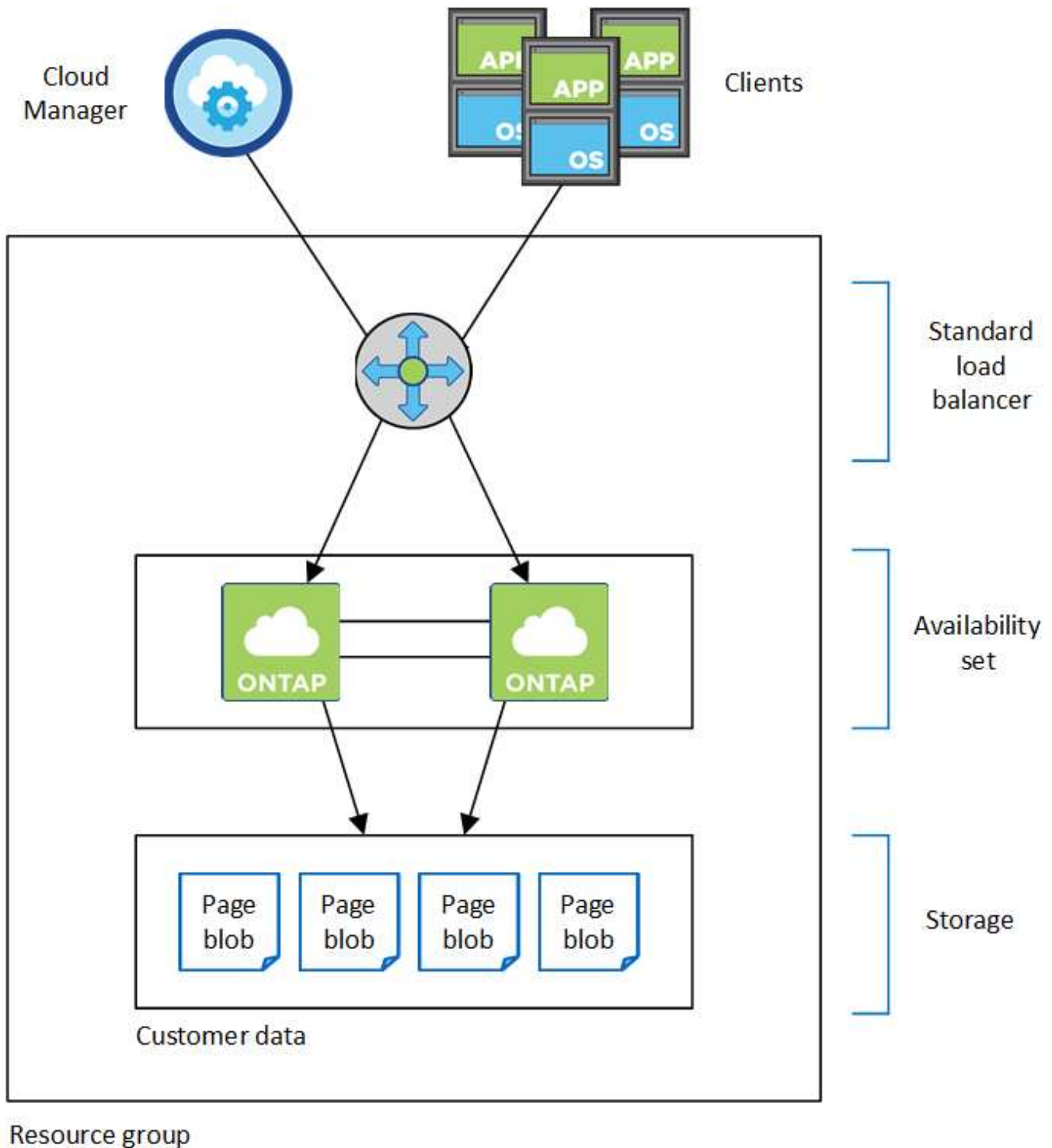
Volume Name	Capacity	Used Capacity	Disk Type	Exported as	Location	Status	
vol1	500 GB	188 KB	SSD	172.31.11.229:vol1	us-east-1, 172...	Online	
vol2	1,000 GB	188 KB	SSD	Mount	Manage Access	Clone	Delete

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.

Storage

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

- Die Boot-Daten eines Node befinden sich auf einer von Premium-SSDs gemanagten Festplatte.
- Die Stammdaten eines Node befinden sich auf einem Blob einer Premium-Storage-Seite.

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.
- Daten-Tiering 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.

Eine kostenlose 30-Tage-Testversion eines Cloud Volumes ONTAP Single Node-Systems ist ab erhältlich ["NetApp Cloud Central"](#). Es fallen keine Software-Gebühren pro Stunde an, doch für die Infrastruktur fallen weiterhin Gebühren an. Eine kostenlose Testversion wird automatisch in ein kostenpflichtiges stündliches Abonnement umgewandelt, sobald diese abläuft.

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.

Lizenzierung

Auf jedem Cloud Volumes ONTAP Byol System muss eine Lizenz mit einem aktiven Abonnement installiert sein. Wenn keine aktive Lizenz installiert ist, fährt das Cloud Volumes ONTAP System nach 30 Tagen herunter. Cloud Manager vereinfacht den Prozess, indem Sie Lizenzen für Sie verwalten und Sie vor Ablauf benachrichtigen.

Lizenzmanagement für ein neues System

Wenn Sie ein BYOL-System erstellen, werden Sie von Cloud Manager zu einem NetApp Support Site Konto 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 nicht über die sichere Internetverbindung auf die Lizenzdatei zugreifen kann, können Sie die Datei selbst abrufen und die Datei dann manuell in Cloud Manager hochladen. Anweisungen hierzu finden Sie unter ["Installation von Lizenzdateien auf Cloud Volumes ONTAP Byol Systemen"](#).

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 erneuern, 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 nicht über die sichere Internetverbindung auf die Lizenzdatei zugreifen kann, können Sie die Datei selbst abrufen und die Datei dann manuell in Cloud Manager hochladen. Anweisungen hierzu finden Sie unter ["Installation von Lizenzdateien auf Cloud Volumes ONTAP Byol Systemen"](#).

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 Volume Encryption (ab Cloud Volumes ONTAP 9.5)
- AWS Key Management Service
- Azure Storage Service Encryption

Sie können NetApp Volume Encryption mit nativer AWS und Azure Verschlüsselung verwenden, die Daten auf Hypervisor-Ebene verschlüsselt.

NetApp Volume Encryption

NetApp Volume Encryption (NVE) ist eine softwarebasierte Technologie, mit der Daten im Ruhezustand um ein Volume gleichzeitig verschlüsselt werden. Daten, Snapshot Kopien und Metadaten sind verschlüsselt. Der Zugriff auf die Daten erfolgt über einen eindeutigen XTS-AES-256-Schlüssel, einen pro Volume.

Cloud Volumes ONTAP unterstützt NetApp Volume Encryption mit einem externen Verschlüsselungsmanagement Server. Ein Onboard Key Manager wird nicht unterstützt. Die unterstützten Schlüsselmanager finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool"](#) Unter der **Key Manager**-Lösung.

Sie können die NetApp Volume Encryption auf einem neuen oder vorhandenen Volume mithilfe von CLI oder System Manager aktivieren. Cloud Manager unterstützt NetApp Volume Encryption nicht. Anweisungen hierzu finden Sie unter ["Verschlüsseln von Volumes mit NetApp Volume Encryption"](#).

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.

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.



Vom Kunden gemanagte Schlüssel werden mit Cloud Volumes ONTAP nicht unterstützt.

ONTAP Virenschannen

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.

The screenshot displays two configuration panels in the NetApp Cloud Manager interface:

- Panel 1: Enable Snapshot Copy Protection**
 - Shows a progress indicator: 40% Protection.
 - Text: 3 Volumes without a Snapshot Policy.
 - Text: To protect your data, activate the default Snapshot policy for these volumes.
 - Button: Activate Snapshot Policy.
- Panel 2: Block Ransomware File Extensions**
 - Shows an icon of a document with a shield and the letter 'F'.
 - Text: ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.
 - Text: View Denied File Names.
 - Button: Activate FPolicy.

"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.

Informationen zu Cloud Volumes ONTAP für AWS finden Sie unter ["NetApp Technical Report 4383: Performance Characterization of Cloud Volumes ONTAP in Amazon Web Services with Application Workloads"](#).

Informationen zu Cloud Volumes ONTAP für Microsoft Azure finden Sie unter ["Technischer Bericht von NetApp 4671: Performance-Charakterisierung von Cloud Volumes ONTAP in Azure mit Applikations-Workloads"](#).

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.