Cloud Manager und Cloud Volumes ONTAP Dokumentation

Cloud Manager 3.7

NetApp
October 23, 2024

Inhalt

Cloud Manager und Cloud Volumes ONTAP Dokumentation

Mit Cloud Manager können Sie NetApp Cloud Volumes ONTAP implementieren und managen – eine Datenmanagement-Lösung mit Schutz, Sichtbarkeit und Kontrolle für Ihre Cloud-basierten Workloads.

BlueXP

NetApp BlueXP erweitert und verbessert die über Cloud Manager bereitgestellten Funktionen.

"Rufen Sie die BlueXP Dokumentation auf"

Entdecken Sie die Neuigkeiten

- "Neuerungen in Cloud Manager"
- "Neuerungen in Cloud Volumes ONTAP"

Los geht’s

- "Erste Schritte in AWS"
- "Erste Schritte in Azure"
- "Erste Schritte mit der Google Cloud Platform"
- "Suchen Sie nach unterstützten Konfigurationen für Cloud Volumes ONTAP"
- "Netzwerkanforderungen für Cloud Manager prüfen"
- "Netzwerkanforderungen für Cloud Volumes ONTAP für AWS prüfen"
- "Netzwerkanforderungen für Cloud Volumes ONTAP für Azure prüfen"
- "Netzwerkanforderungen für Cloud Volumes ONTAP für GCP prüfen"
- "Planen Sie Ihre Cloud Volumes ONTAP Konfiguration"

Automatisierung mit APIs

- "API-Entwicklerhandbuch"
- "Automationsbeispiele"

Treten Sie mit Kollegen in Kontakt, holen Sie sich Hilfe und finden Sie weitere Informationen

- "NetApp Community: Cloud Data Services"
- "NetApp Cloud Volumes ONTAP Support"
- "Wo Sie Hilfe und weitere Informationen erhalten"

Versionshinweise

Cloud Manager

Neues in Cloud Manager 3.7

Cloud Manager stellt in der Regel jeden Monat eine neue Version vor, mit der Sie neue Funktionen, Verbesserungen und Fehlerbehebungen erhalten.

Suchen Sie nach einer früheren Version?"Neuerungen in 3.6"
"Neuerungen in 3.5"
"Neuerungen in 3.4"

Update zu Cloud Manager 3.7.5 (16. Dezember 2019)

Dieses Update enthält die folgenden Verbesserungen:

- Cloud Volumes ONTAP 9.7
- Cloud Compliance für Cloud Volumes ONTAP

Cloud Volumes ONTAP 9.7

Cloud Volumes ONTAP 9.7 ist jetzt auf der AWS, Azure und Google Cloud Platform verfügbar.

"Die neuesten Funktionen von Cloud Volumes ONTAP 9.7".

Cloud Compliance für Cloud Volumes ONTAP

Cloud Compliance ist ein Datenschutz- und Compliance-Service für Cloud Volumes ONTAP in AWS und Azure. Mithilfe von künstlicher Intelligenz (KI) hilft Cloud Compliance Unternehmen dabei, den Datenkontext zu verstehen und sensible Daten in Cloud Volumes ONTAP Systemen zu ermitteln.

Cloud Compliance ist derzeit als Version für kontrollierte Verfügbarkeit verfügbar.

"Erfahren Sie mehr über Cloud Compliance".

Cloud Manager 3.7.5 (3. Dezember 2019)

Cloud Manager 3.7.5 umfasst die folgenden Verbesserungen:

- Hohe Schreibgeschwindigkeit für Cloud Volumes ONTAP in GCP
- On-Premises-ONTAP-Cluster als persistenter Storage für Kubernetes
- Aktuelle Trident Version für Kubernetes
- Support für allgemeine Azure v2 Storage-Konten
- Präfixe in Azure-Storage-Kontonamen unter Verwendung von APIs

Hohe Schreibgeschwindigkeit für Cloud Volumes ONTAP in GCP

Auf neuen und bestehenden Cloud Volumes ONTAP Systemen können Sie als Google Cloud Platform jetzt hohe Schreibgeschwindigkeit aktivieren. Eine hohe Schreibgeschwindigkeit ist eine gute Wahl, wenn für Ihren

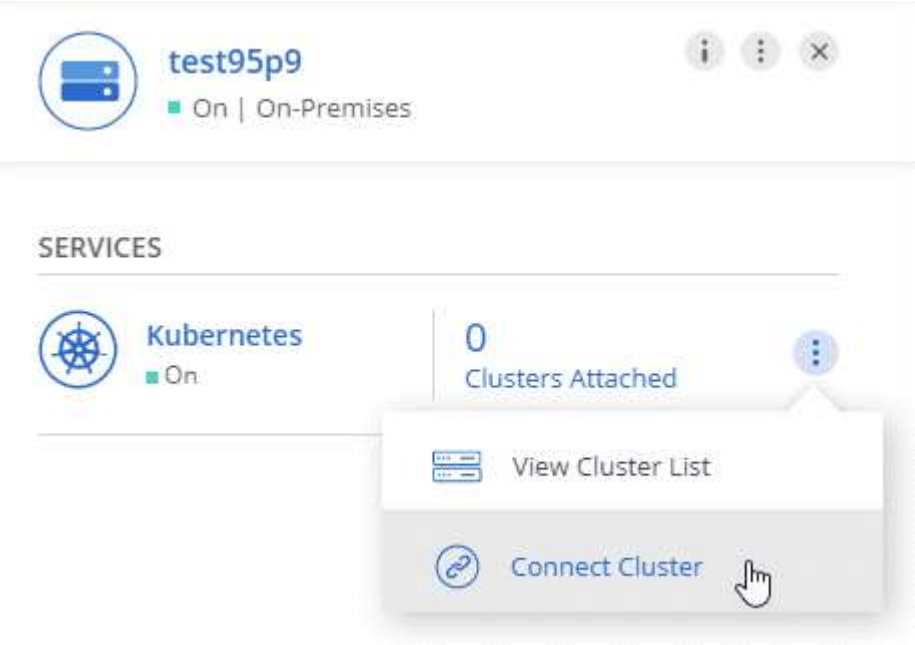
Workload eine hohe Schreib-Performance benötigt wird.

- "Hier erfahren Sie, wie Sie eine Schreibgeschwindigkeit auswählen"
- "Erfahren Sie, wie Sie die Schreibgeschwindigkeit bei vorhandenen Systemen ändern"

On-Premises-ONTAP-Cluster als persistenter Storage für Kubernetes

Mit Cloud Manager können Sie jetzt lokale ONTAP Cluster als persistenten Storage für Container verwenden. Ähnlich wie bei Cloud Volumes ONTAP automatisiert Cloud Manager die Implementierung von NetApp Trident und verbindet ONTAP mit Kubernetes-Clustern.

Nachdem Sie einem Cloud Manager ein Kubernetes Cluster hinzugefügt haben, können Sie es über die Seite „Arbeitsumgebung“ mit den lokalen ONTAP Clustern verbinden:



"Erste Schritte".

Aktuelle Trident Version für Kubernetes

Cloud Manager installiert jetzt eine aktuellere Version von Trident (Version 19.07.1), wenn Sie eine Arbeitsumgebung mit einem Kubernetes-Cluster verbinden.

Support für allgemeine Azure v2 Storage-Konten

Bei der Implementierung neuer Cloud Volumes ONTAP Systeme in Azure sind jetzt die Storage-Konten, die Cloud Manager für Diagnose und Daten-Tiering erstellt, allgemeine v2 Storage-Konten.

Präfixe in Azure-Storage-Kontonamen unter Verwendung von APIs

Sie können jetzt den Namen der Azure-Storage-Konten, die Cloud Manager für Cloud Volumes ONTAP erstellt, ein Präfix hinzufügen. Verwenden Sie einfach den Parameter *storageAccountPrefix*, wenn Sie ein neues Cloud Volumes ONTAP-System in Azure bereitstellen.

"Weitere Details zur Verwendung von APIs finden Sie im API-Entwicklerhandbuch".

Cloud Manager 3.7.4 (6. Okt. 2019)

Cloud Manager 3.7.4 umfasst die folgenden Verbesserungen:

- Unterstützung von Azure NetApp Files
- Cloud Volumes ONTAP für GCP-Verbesserungen
- Backup in S3-Verbesserungen
- Verschlüsselung von Boot- und Root-Festplatten in AWS
- Unterstützung für die Region AWS Bahrain
- Unterstützung für die Azure VAE Nord Region

Unterstützung von Azure NetApp Files

NFS Volumes für Azure NetApp Files können nun direkt über Cloud Manager angezeigt und erstellt werden. Diese Erweiterung setzt unser Ziel fort, Sie beim Management Ihres Cloud-Storage über eine einzige Benutzeroberfläche zu unterstützen.

"Erste Schritte".

Diese Funktion erfordert neue Berechtigungen, wie in der aktuellen gezeigt "Cloud Manager-Richtlinie für Azure".

```
"Microsoft.NetApp/netAppAccounts/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete"
```

Cloud Volumes ONTAP für GCP-Verbesserungen

Cloud Manager 3.7.4 ermöglicht die folgenden Verbesserungen an Cloud Volumes ONTAP für die Google Cloud Platform:

Pay-as-you-go-Abonnements im GCP Marketplace

Wenn Sie Cloud Volumes ONTAP im Google Cloud Platform Marketplace abonnieren, können Sie Cloud Volumes ONTAP jetzt bezahlen.

"Google Cloud Platform Marketplace: Cloud Manager für Cloud Volumes ONTAP"

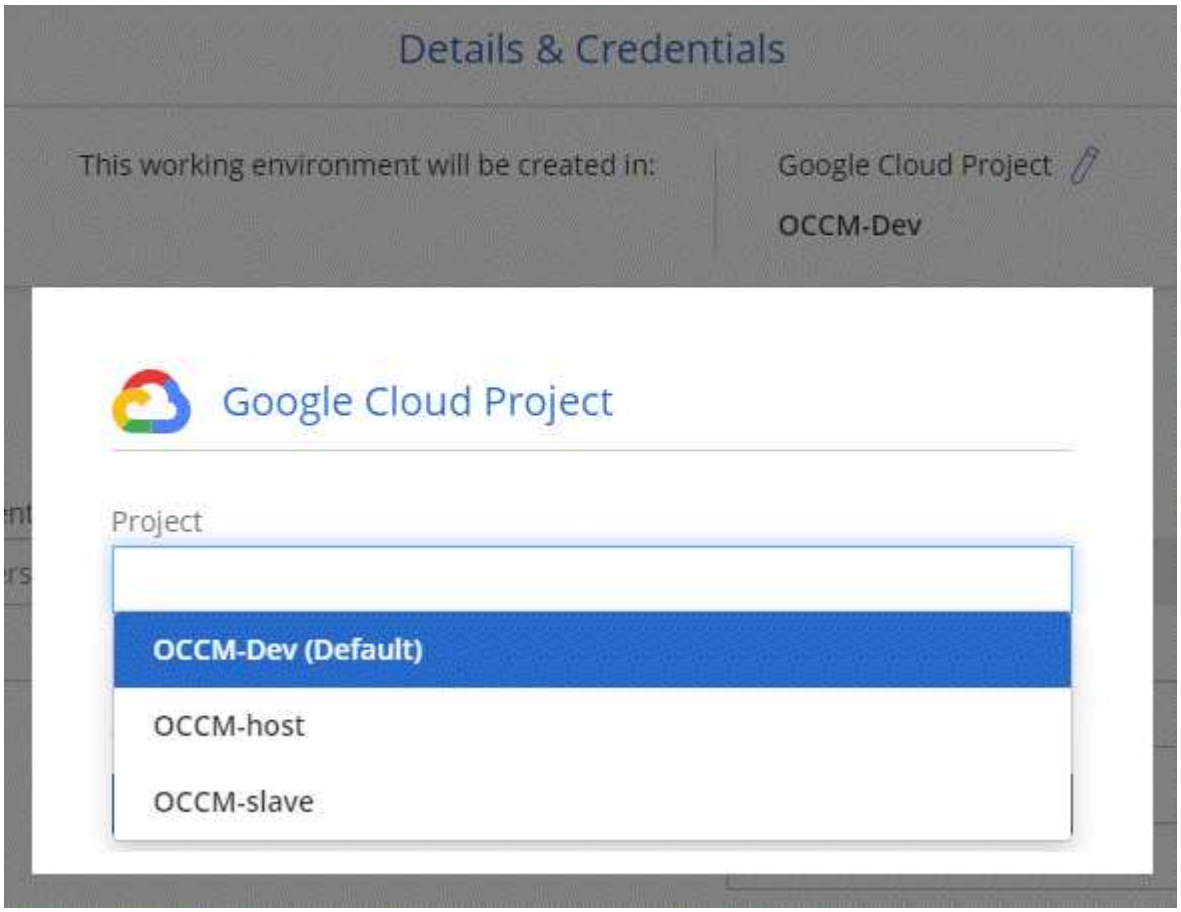
Gemeinsame VPC

Cloud Manager und Cloud Volumes ONTAP werden jetzt in einer gemeinsamen Google Cloud Platform VPC unterstützt.

Mit der Shared 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 Cloud Manager und Cloud Volumes ONTAP Virtual Machines in einem *Service-Projekt* implementieren. "Google Cloud-Dokumentation: Gemeinsame VPC-Übersicht".

Mehrere Google Cloud-Projekte

Cloud Volumes ONTAP muss sich nicht mehr im selben Projekt wie Cloud Manager befinden. Fügen Sie das Cloud Manager Service-Konto und die Rolle zu weiteren Projekten hinzu. Dann können Sie aus den Projekten auswählen, die Sie implementieren Cloud Volumes ONTAP.



Weitere Informationen zum Einrichten des Cloud Manager Servicekontos finden Sie unter "Siehe Schritt 4b auf dieser Seite".

Von Kunden gemanagte Verschlüsselungen bei Verwendung von Cloud Manager APIs

Während Google Cloud Storage Ihre Daten immer verschlüsselt, bevor sie auf die Festplatte geschrieben werden, können Sie mithilfe von Cloud-Manager-APIs ein neues 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.

Siehe "API-Entwicklerhandbuch" Weitere Informationen zur Verwendung der Parameter „GcpEncryption“.

Diese Funktion erfordert neue Berechtigungen, wie in der aktuellen gezeigt "Cloud Manager-Richtlinie für GCP":

```
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

Backup in S3-Verbesserungen

Sie können jetzt die Backups für vorhandene Volumes löschen. Früher konnten Sie nur die Backups für gelöschte Volumes löschen.

"Weitere Informationen zu Backup in S3".

Verschlüsselung von Boot- und Root-Festplatten in AWS

Wenn Sie die Datenverschlüsselung über den AWS KMS (Key Management Service) aktivieren, werden sowohl Boot- als auch Root-Festplatten für Cloud Volumes ONTAP jetzt 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.

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

Unterstützung für die Region AWS Bahrain

Cloud Manager und Cloud Volumes ONTAP werden jetzt auch in der Region AWS Middle East (Bahrain) unterstützt.

Unterstützung für die Azure VAE Nord Region

Cloud Manager und Cloud Volumes ONTAP werden nun in der Azure VAE Nord Region unterstützt.

"Alle unterstützten Regionen anzeigen".

Update für Cloud Manager 3.7.3 (15. Sept. 2019)

Mit Cloud Manager können Sie jetzt Daten-Backups von Cloud Volumes ONTAP in Amazon S3 erstellen.

Backup auf S3

Backup in S3 ist ein Add-on-Service für Cloud Volumes ONTAP, der vollumfängliche Backup- und Restore-Funktionen zum Schutz und Langzeitarchiv von Cloud-Daten bereitstellt. Die Backups werden im S3-Objekt-Storage gespeichert, unabhängig von Volume-Snapshot-Kopien für die kurzfristige Wiederherstellung oder das Klonen.

"Erste Schritte".

Für diese Funktion ist eine Aktualisierung des erforderlich "Cloud Manager-Richtlinie". Jetzt sind die folgenden VPC-Endpunktberechtigungen erforderlich:

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

Cloud Manager 3.7.3 (11. Sept. 2019)

Cloud Manager 3.7.3 umfasst die folgenden Verbesserungen:

- Bestandsaufnahme und Management von Cloud Volumes Service für AWS
- Im AWS Marketplace ist ein neues Abonnement erforderlich
- Unterstützung von AWS GovCloud (US-Ost)

Bestandsaufnahme und Management von Cloud Volumes Service für AWS

Mit Cloud Manager können Sie jetzt die Cloud Volumes in Ihrem erkennen "Cloud Volumes Service für AWS" Abonnement: Nach der Bestandsaufnahme können Sie zusätzliche Cloud Volumes direkt aus Cloud Manager hinzufügen. Diese Erweiterung ermöglicht das Management Ihres NetApp Cloud Storage über eine zentrale Konsole.

"Erste Schritte".

Im AWS Marketplace ist ein neues Abonnement erforderlich

"Ein neues Abonnement ist im AWS Marketplace erhältlich". Dieses einmalige Abonnement ist für die Implementierung von Cloud Volumes ONTAP 9.6 PAYGO erforderlich (außer für Ihr kostenloses 30-Tage-Testsystem). Mit dem Abonnement können wir auch Add-on-Funktionen für Cloud Volumes ONTAP PAYGO und BYOL anbieten. Sie erhalten für jedes von Ihnen erstellte Cloud Volumes ONTAP-PAYGO-System und jede von Ihnen erstellte Add-on-Funktion die Gebühr.

Ab Version 9.6 ersetzt diese neue Abonnementmethode die zwei vorhandenen AWS Marketplace-Abonnements für Cloud Volumes ONTAP PAYGO, für die Sie bereits angemeldet haben. Sie benötigen weiterhin Abonnements über das "Vorhandene AWS Marketplace-Seiten bei Implementierung von Cloud Volumes ONTAP BYOL".

"Weitere Informationen zu den einzelnen AWS Marketplace finden Sie auf dieser Seite".

Unterstützung von AWS GovCloud (US-Ost)

Cloud Manager und Cloud Volumes ONTAP werden nun von AWS GovCloud (US-Osten) unterstützt.

Allgemeine Verfügbarkeit von Cloud Volumes ONTAP in GCP (3. Sept. 2019)

Cloud Volumes ONTAP ist ab sofort in der Google Cloud Platform (GCP) verfügbar, wenn Sie Ihre eigene Lizenz (BYOL) verwenden. Außerdem ist eine Pay-as-you-go-Aktion verfügbar. Das Angebot bietet kostenlose Lizenzen für eine unbegrenzte Anzahl von Systemen und läuft Ende September 2019 ab.

- "Erste Schritte in GCP"
- "Zeigen Sie unterstützte Konfigurationen an"

Cloud Manager 3.7.2 (5. August 2019)

- FlexCache-Lizenzen
- Kubernetes Storage-Klassen für iSCSI
- Verwaltung von Inoden
- Unterstützung für die Region Hongkong in AWS
- Unterstützung der australischen Zentralregionen in Azure

FlexCache-Lizenzen

Cloud Manager generiert jetzt 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.

Kubernetes Storage-Klassen für iSCSI

Wenn Sie Cloud Volumes ONTAP mit einem Kubernetes Cluster verbinden, erstellt Cloud Manager jetzt zwei zusätzliche Kubernetes-Storage-Klassen, die mit persistenten iSCSI Volumes genutzt werden können:

- **netapp-File-san**: Zur Anbindung persistenter iSCSI-Volumes an Single-Node-Cloud Volumes ONTAP-Systeme
- **netapp-file-redundant-san**: Zur Anbindung persistenter iSCSI-Volumes an Cloud Volumes ONTAP HA-Paare

Verwaltung von Inoden

Cloud Manager überwacht jetzt 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.

Cloud Manager überwacht die Inode-Nutzung nur, wenn der Capacity Management-Modus auf automatisch eingestellt ist (dies ist die Standardeinstellung).

Unterstützung für die Region Hongkong in AWS

Cloud Manager und Cloud Volumes ONTAP werden jetzt auch im asiatisch-pazifischen Raum (Hongkong) in AWS unterstützt.

Unterstützung der australischen Zentralregionen in Azure

Cloud Manager und Cloud Volumes ONTAP werden jetzt in folgenden Azure Regionen unterstützt:

- Australien, Mitte
- Australien, Mitte 2

"Eine vollständige Liste der unterstützten Regionen ist verfügbar".

Update zur Sicherung und Wiederherstellung (15. Juli 2019)

Ab Version 3.7.1 unterstützt Cloud Manager nicht mehr das Herunterladen eines Backups und dessen Verwendung zum Wiederherstellen der Cloud Manager Konfiguration. "Führen Sie diese Schritte aus, um Cloud Manager wiederherzustellen".

Cloud Manager 3.7.1 (1. Juli 2019)

- Diese Version umfasst in erster Linie Bug Fixes.
- Es beinhaltet eine Verbesserung: Cloud Manager installiert nun eine Lizenz für NetApp Volume Encryption (NVE) auf jedem Cloud Volumes ONTAP System, das mit NetApp Support (neue und vorhandene Systeme) registriert ist.

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

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

Update zu Cloud Manager 3.7 (16. Juni 2019)

Cloud Volumes ONTAP 9.6 ist nun als private Vorschau in AWS, Azure und der Google Cloud Platform verfügbar. Um an der privaten Vorschau teilzunehmen, senden Sie eine Anfrage an ng-Cloud-Volume-ONTAP-preview@netapp.com.

"Die neuesten Funktionen von Cloud Volumes ONTAP 9.6"

Cloud Manager 3.7 (5. Juni 2019)

- Unterstützung für die kommende Version Cloud Volumes ONTAP 9.6
- NetApp Cloud Central Kunden
- Backup und Restore mit der Cloud Backup Service

Unterstützung für die kommende Version Cloud Volumes ONTAP 9.6

Cloud Manager 3.7 bietet Unterstützung für die neue Version Cloud Volumes ONTAP 9.6. Die Version 9.6 enthält eine exklusive Vorschau auf Cloud Volumes ONTAP in der Google Cloud Platform. Wir aktualisieren die Versionshinweise, sobald 9.6 verfügbar ist.

NetApp Cloud Central Kunden

Wir haben erweitert, wie Sie Ihre Cloud-Ressourcen managen. Jedem Cloud Manager System wird ein *NetApp Cloud Central Account* zugewiesen. Der Kunde ermöglicht Mandantenfähigkeit und ist zukünftig für andere NetApp Cloud-Datenservices geplant.

In Cloud Manager ist ein Cloud Central Konto ein Container für Ihre Cloud Manager Systeme und die „*Workspaces*“, in denen Benutzer Cloud Volumes ONTAP implementieren.

"Erfahren Sie, wie Cloud Central Accounts Mandantenfähigkeit ermöglichen".

> Für die Verbindung mit dem Cloud Central Account Service benötigt Cloud Manager Zugriff auf *https://cloudmanager.cloud.netapp.com*. Öffnen Sie diese URL in Ihrer Firewall, um sicherzustellen, dass Cloud Manager den Service kontaktieren kann.

Integration Ihres Systems mit Cloud Central Konten

Einige Zeit nach dem Upgrade auf Cloud Manager 3.7 wählt NetApp bestimmte Cloud Manager Systeme für die Integration mit Cloud Central Konten. Während dieses Prozesses erstellt NetApp einen Account, weist jedem Benutzer neue Rollen zu, erstellt Arbeitsbereiche und platziert bestehende Arbeitsumgebungen in diesen Arbeitsbereichen. Cloud Volumes ONTAP Systeme werden unterbrechungsfrei zugewiesen.

"Wenn Sie Fragen haben, lesen Sie diese FAQ".

Backup und Restore mit der Cloud Backup Service

NetApp Cloud Backup Service für Cloud Volumes ONTAP bietet vollständig gemanagte Backup- und Restore-Funktionen zum Schutz und zur langfristigen Archivierung Ihrer Cloud-Daten. Sie können die Cloud Backup Service in Cloud Volumes ONTAP für AWS integrieren. Die vom Service erstellten Backups werden im AWS S3 Objekt-Storage gespeichert.

"Erfahren Sie mehr über die Cloud Backup Service".

Um zu starten, installieren und konfigurieren Sie den Backup Agent und starten Sie dann Backup- und Restore-Vorgänge. Wenn Sie Hilfe benötigen, empfehlen wir Ihnen, uns über das Chat-Symbol in Cloud Manager zu kontaktieren.

Dieses manuelle Verfahren wird nicht mehr unterstützt. Die Funktion „Backup to S3“ wurde in Version 3.7.3 in Cloud Manager integriert.

Bekannte Probleme

Bekannte Probleme identifizieren Probleme, die Sie daran hindern könnten, diese Produktversion erfolgreich zu verwenden.

In dieser Version von Cloud Manager sind keine Probleme bekannt.

Bekannte Probleme für Cloud Volumes ONTAP finden Sie im "Versionshinweise zu Cloud Volumes ONTAP" Und für ONTAP-Software im Allgemeinen "Versionshinweise zu ONTAP".

Bekannte Einschränkungen

Bekannte Einschränkungen identifizieren Plattformen, Geräte oder Funktionen, die von dieser Version des Produkts nicht unterstützt werden oder nicht korrekt mit dem Produkt zusammenarbeiten. Lesen Sie diese Einschränkungen sorgfältig durch.

Cloud Manager sollte stets verfügbar sein

Cloud Manager ist eine Kernkomponente bei Systemzustand und Abrechnung von Cloud Volumes ONTAP. Wenn Cloud Manager heruntergefahren wird, werden Cloud Volumes ONTAP Systeme heruntergefahren, nachdem die Kommunikation mit Cloud Manager über mehr als 4 Tage lang unterbrochen wurde.

Freigegebene Linux-Hosts werden nicht unterstützt

Cloud Manager wird auf einem Host, der für andere Applikationen freigegeben ist, nicht unterstützt. Der Host muss ein dedizierter Host sein.

Cloud Manager unterstützt FlexGroup Volumes nicht

Cloud Volumes ONTAP unterstützt zwar FlexGroup Volumes, aber Cloud Manager nicht. Wenn Sie ein FlexGroup-Volume aus System Manager oder aus der CLI erstellen, sollten Sie den Modus „Kapazitätsmanagement“ von Cloud Manager auf „manuell“ setzen. Der automatische Modus funktioniert möglicherweise nicht ordnungsgemäß mit FlexGroup-Volumes.

Active Directory wird bei neuen Installationen von Cloud Manager standardmäßig nicht unterstützt

Ab Version 3.4 unterstützen neue Installationen von Cloud Manager nicht die Active Directory-Authentifizierung Ihres Unternehmens für die Benutzerverwaltung. Bei Bedarf kann NetApp Sie bei der Einrichtung von Active Directory mit Cloud Manager unterstützen. Klicken Sie auf das Chat-Symbol unten rechts im Cloud Manager, um Hilfe zu erhalten.

Einschränkungen in der AWS GovCloud (USA) Region

- Cloud Manager muss in der Region AWS GovCloud (USA) implementiert werden, wenn Sie Cloud Volumes ONTAP Instanzen in der Region AWS GovCloud (USA) starten möchten.
- Bei der Implementierung in der AWS GovCloud (USA)-Region kann Cloud Manager ONTAP Cluster in einer NetApp Private Storage für Microsoft Azure Konfiguration oder einer NetApp Private Storage für SoftLayer Konfiguration nicht erkennen.

Cloud Manager richtet keine iSCSI-Volumes ein

Wenn Sie ein Volume in Cloud Manager mithilfe der Storage System View erstellen, können Sie das NFS- oder CIFS-Protokoll auswählen. Sie müssen OnCommand System Manager verwenden, um ein Volume für iSCSI zu erstellen.

Storage Virtual Machine (SVM)-Einschränkung

Cloud Volumes ONTAP unterstützt eine SVM mit Datenbereitstellung und eine oder mehrere SVMs, die für Disaster Recovery verwendet werden. Die eine Datenservice-SVM umfasst das gesamte Cloud Volumes ONTAP System (HA-Paar oder ein Node).

Cloud Manager bietet keine Einrichtungs- oder Orchestrierungsunterstützung für SVM Disaster Recovery. Darüber hinaus werden Storage-bezogene Aufgaben auf zusätzlichen SVMs nicht unterstützt. Sie müssen System Manager oder die CLI für die SVM-Disaster Recovery verwenden.

Konzepte

Überblick über Cloud Manager und Cloud Volumes ONTAP

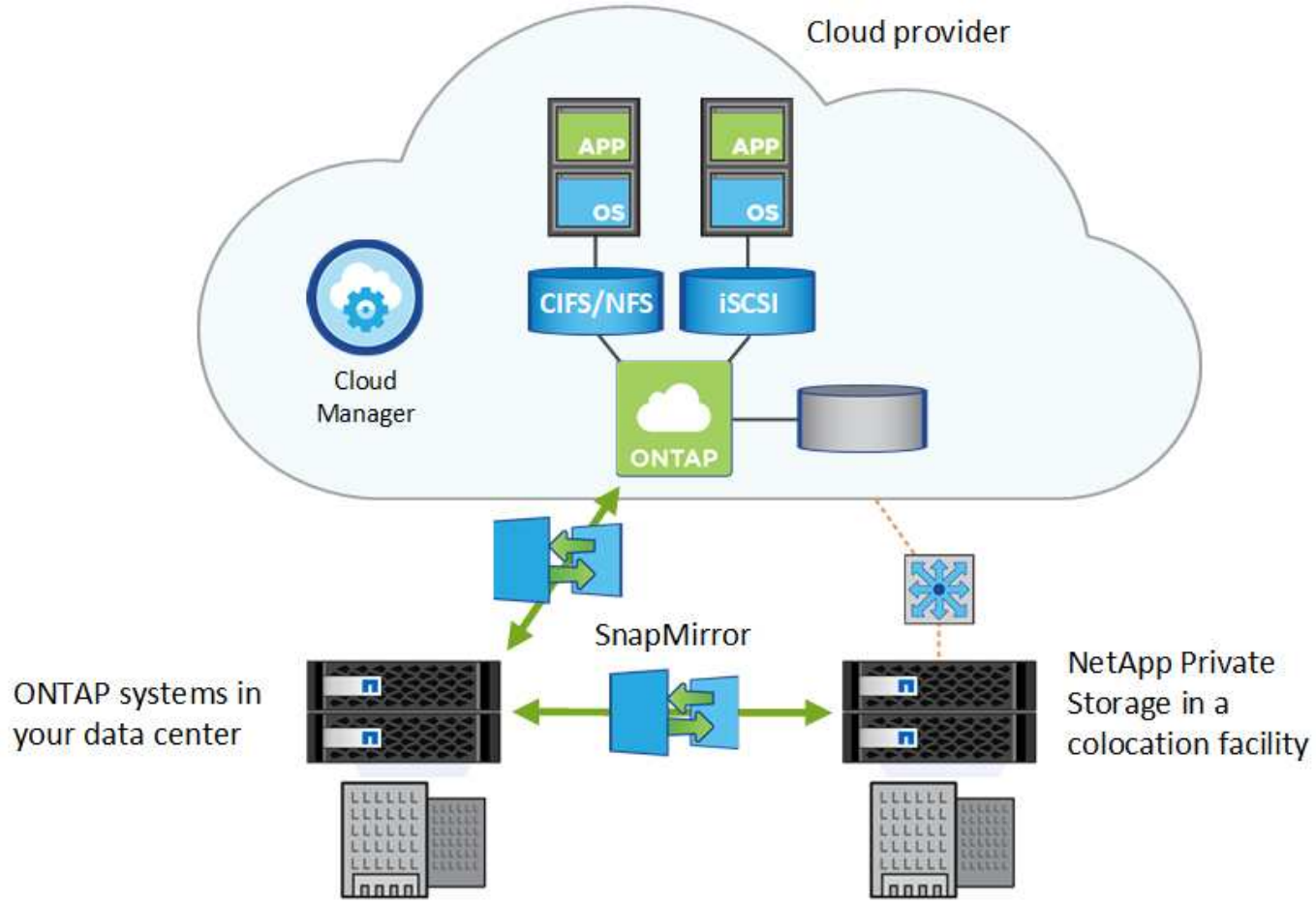
Mit Cloud Manager können Sie Cloud Volumes ONTAP implementieren, das Funktionen der Enterprise-Klasse für Ihren Cloud-Storage bietet und Daten einfach zwischen Hybrid Clouds basierend auf NetApp Technologie replizieren.

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 und Cloud Volumes ONTAP, die bei einem Cloud-Provider ausgeführt werden. 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 im Lieferumfang von Cloud Volumes ONTAP enthalten.

"Anzeigen der unterstützten Cloud Volumes ONTAP Konfigurationen"

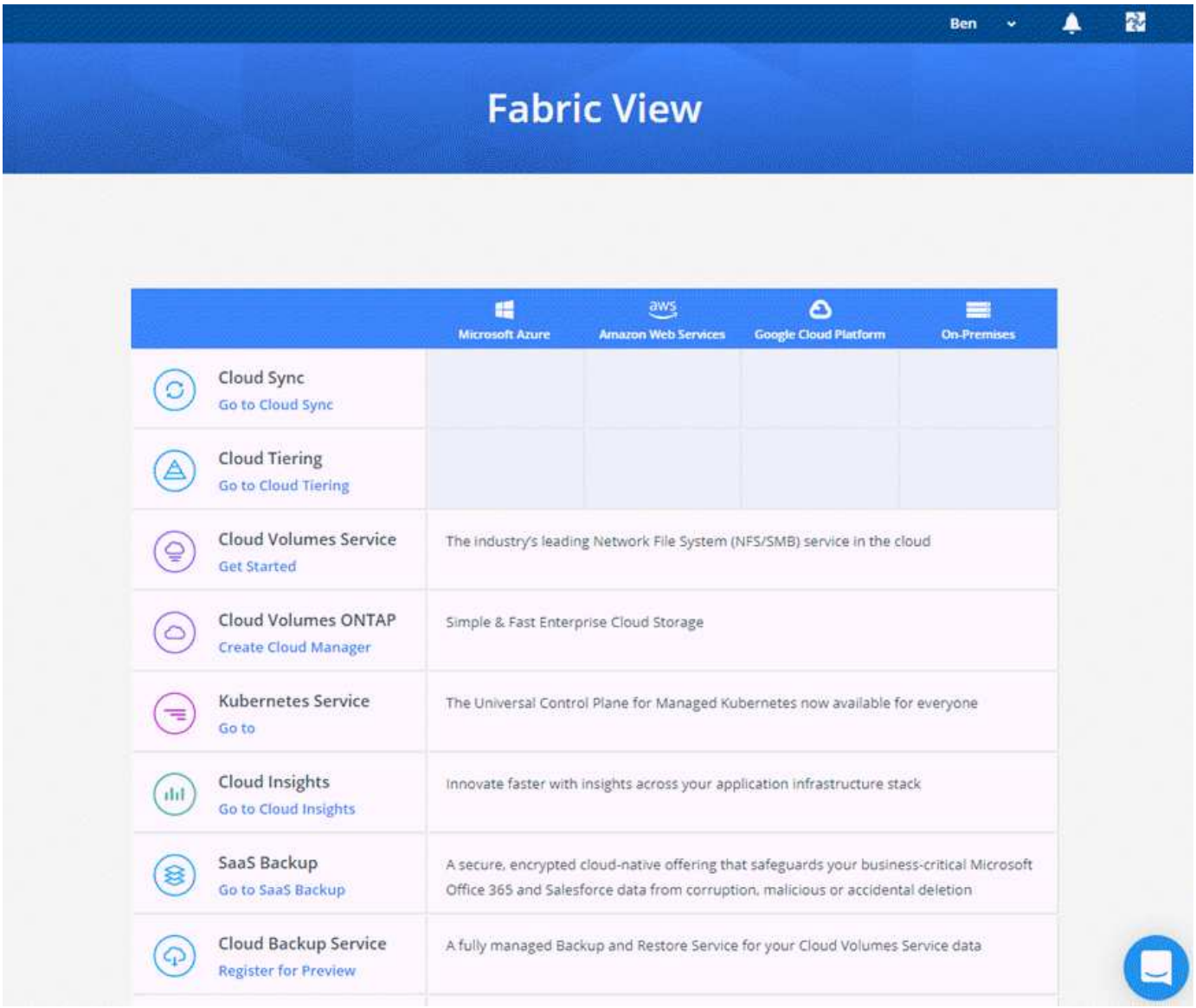
"Erfahren Sie mehr über Cloud Volumes ONTAP"

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.



Accounts in Cloud Central

Jedes Cloud Manager System ist einem *NetApp Cloud Central Account* zugeordnet. Ein Cloud Central Konto bietet Mandantenfähigkeit und ermöglicht es Ihnen, Benutzer und Ressourcen in isolierten Workspaces zu organisieren.

Ein Cloud Central Konto ermöglicht Mandantenfähigkeit:

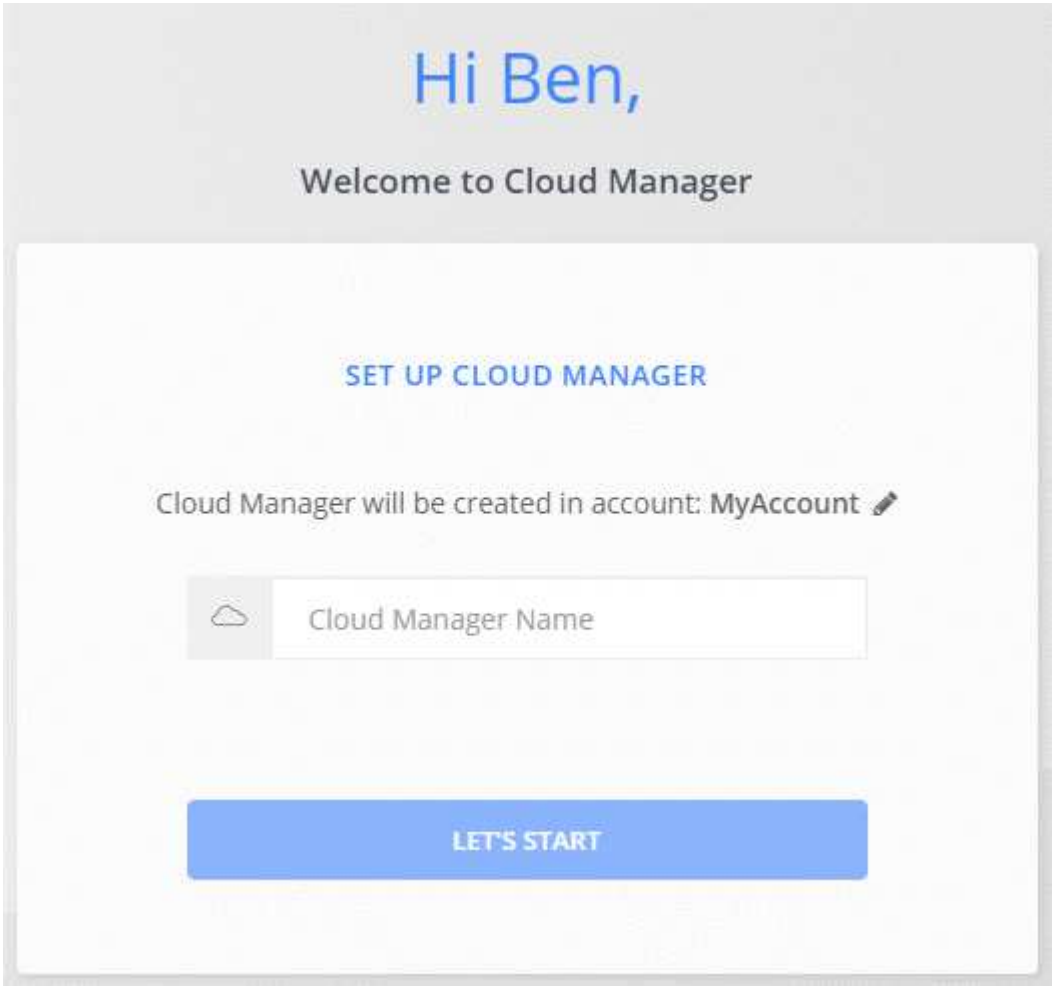
- Ein einzelnes Cloud Central Konto kann mehrere Cloud Manager Systeme enthalten, die unterschiedliche geschäftliche Anforderungen erfüllen.

  Da Benutzer mit dem Cloud Central Konto verknüpft sind, müssen keine Benutzer für jedes einzelne Cloud Manager System konfiguriert werden.

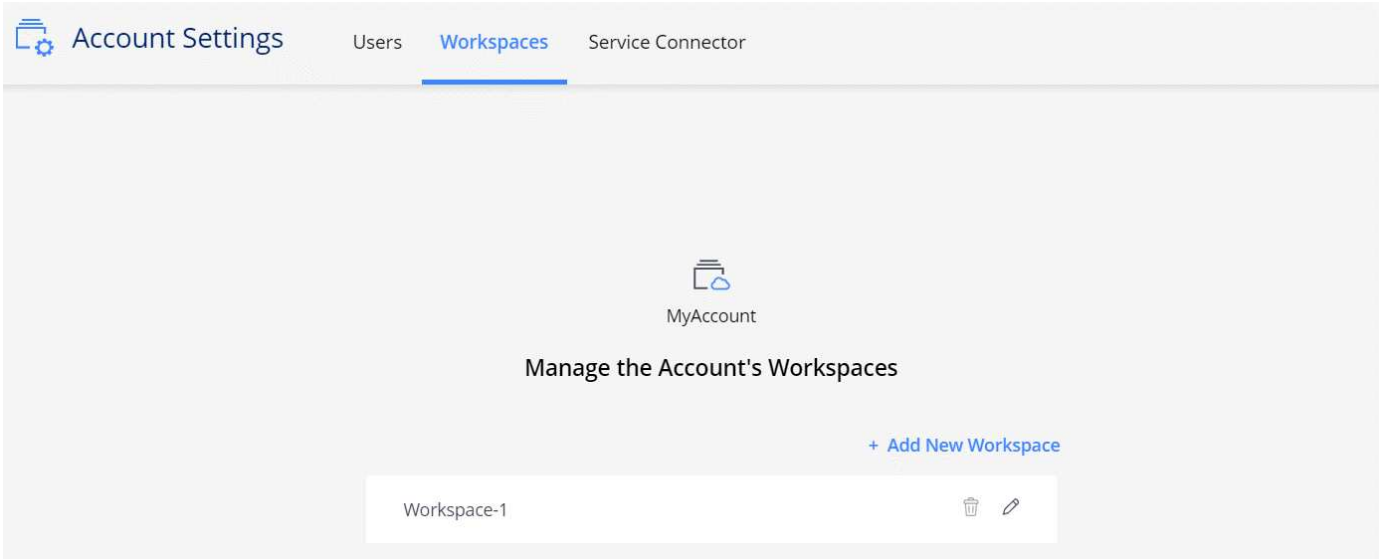
- Innerhalb jedes Cloud Manager Systems können mehrere Benutzer Cloud Volumes ONTAP Systeme in isolierten Umgebungen bereitstellen und managen, die als Workspaces bezeichnet werden.

  Diese Arbeitsbereiche sind für andere Benutzer unsichtbar, es sei denn, sie werden gemeinsam genutzt.

Wenn Sie Cloud Manager implementieren, wählen Sie das Cloud Central-Konto aus, das mit dem System verknüpft werden soll:



Kontoadministratoren können dann die Einstellungen für dieses Konto ändern, indem sie Benutzer, Arbeitsbereiche und Serviceanschlüsse verwalten:



Schritt-für-Schritt-Anweisungen finden Sie unter "Einrichten des Cloud Central Kontos".

Für die Verbindung mit dem Cloud Central Account Service benötigt Cloud Manager Zugriff auf *https://cloudmanager.cloud.netapp.com*. Öffnen Sie diese URL in Ihrer Firewall, um sicherzustellen, dass Cloud Manager den Service kontaktieren kann.

Benutzer, Arbeitsbereiche und Serviceanschlüsse

Im Widget „Account Settings“ in Cloud Manager können Kontoadministratoren ein Cloud Central Konto verwalten. Wenn Sie gerade Ihr Konto erstellt, dann beginnen Sie von Grund auf. Wenn Sie jedoch bereits ein Konto eingerichtet haben, sehen Sie *all* die Benutzer, Arbeitsbereiche und Dienstverbindungen, die mit dem Konto verknüpft sind.

Benutzer

Dies sind NetApp Cloud Central Benutzer, die Sie mit Ihrem Cloud Central Konto verknüpfen. Wenn ein Benutzer mit einem Konto und einem oder mehreren Arbeitsbereichen dieses Kontos verknüpft wird, können diese Benutzer Arbeitsumgebungen in Cloud Manager erstellen und verwalten.

Wenn Sie einen Benutzer zuordnen, weisen Sie ihm eine Rolle zu:

- *Account Admin*: Kann jede Aktion im Cloud Manager ausführen.
- *Workspace Admin*: Kann Ressourcen im zugewiesenen Arbeitsbereich erstellen und verwalten.

Arbeitsbereiche

In Cloud Manager isoliert ein Arbeitsbereich beliebig viele *Arbeitsumgebungen* aus anderen Arbeitsumgebungen. Workspace-Administratoren können nicht auf die Arbeitsumgebungen in einem Arbeitsbereich zugreifen, es sei denn, der Kontoadministrator ordnet den Administrator diesem Arbeitsbereich zu.

Eine Arbeitsumgebung ist ein Speichersystem:

- Single Node 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

Wartungsanschlüsse

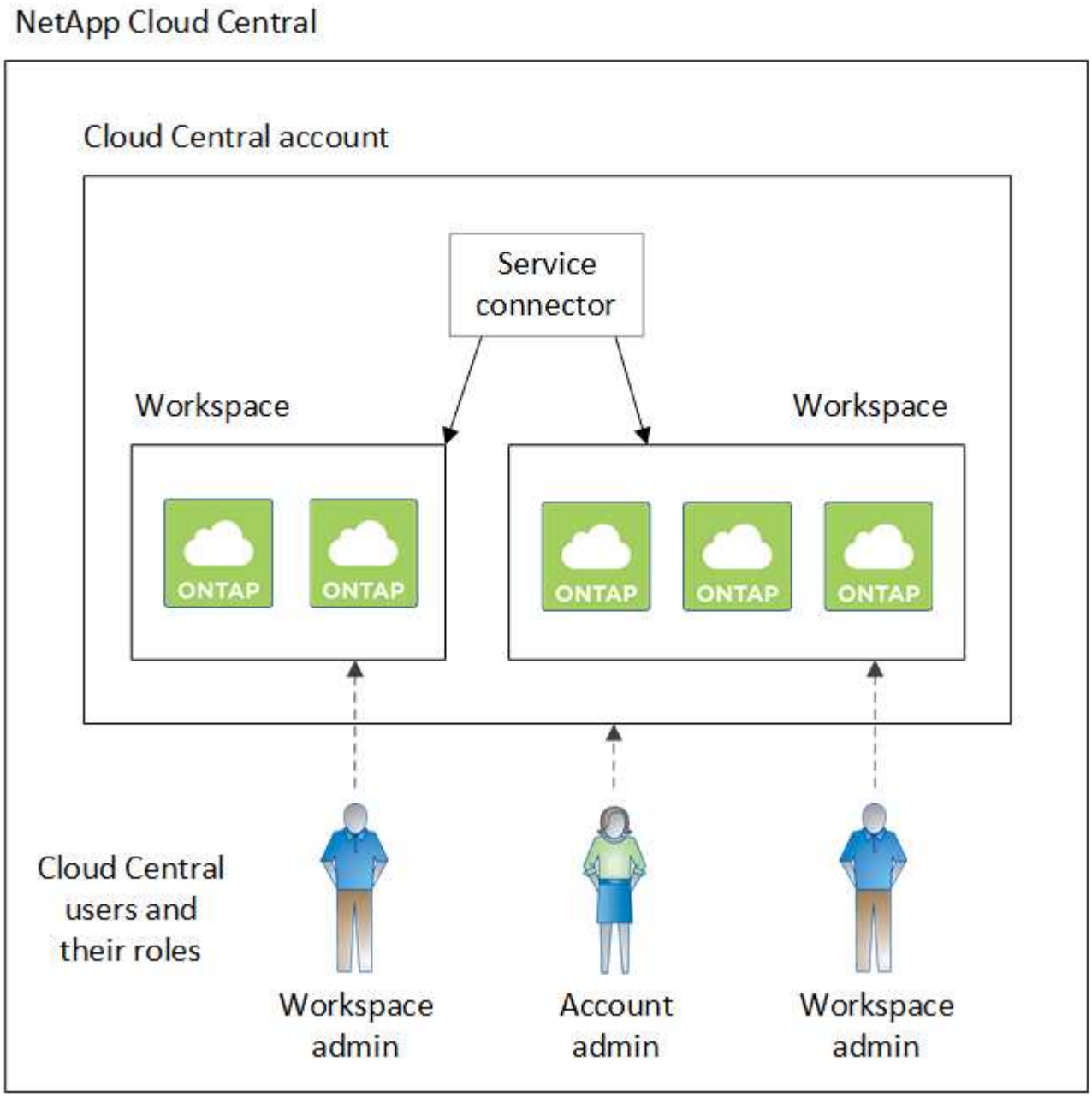
Ein Service-Connector ist Teil von Cloud Manager. Es wird ein Großteil der Cloud Manager-Software ausgeführt (wie die Benutzeroberfläche), mit Ausnahme einiger Cloud Central-Dienste, mit denen eine Verbindung hergestellt wird (auth0- und Cloud Central-Konten). Der Service-Connector wird auf der Virtual-Machine-Instanz ausgeführt, die bei Ihrem Cloud-Provider oder auf einem von Ihnen konfigurierten On-Premises-Host implementiert wurde.

Sie können einen Service-Connector mit mehr als einem NetApp Cloud-Datenservice verwenden. Wenn Sie beispielsweise bereits über einen Service-Connector für Cloud Manager verfügen, können Sie ihn beim Einrichten des Cloud Tiering-Service auswählen.

Beispiele

Das folgende Beispiel zeigt ein Konto, das zwei Arbeitsbereiche zum Erstellen isolierter Umgebungen für Cloud Volumes ONTAP-Systeme verwendet. Ein Arbeitsbereich könnte beispielsweise für eine Staging-Umgebung sein, der andere für eine Produktionsumgebung.

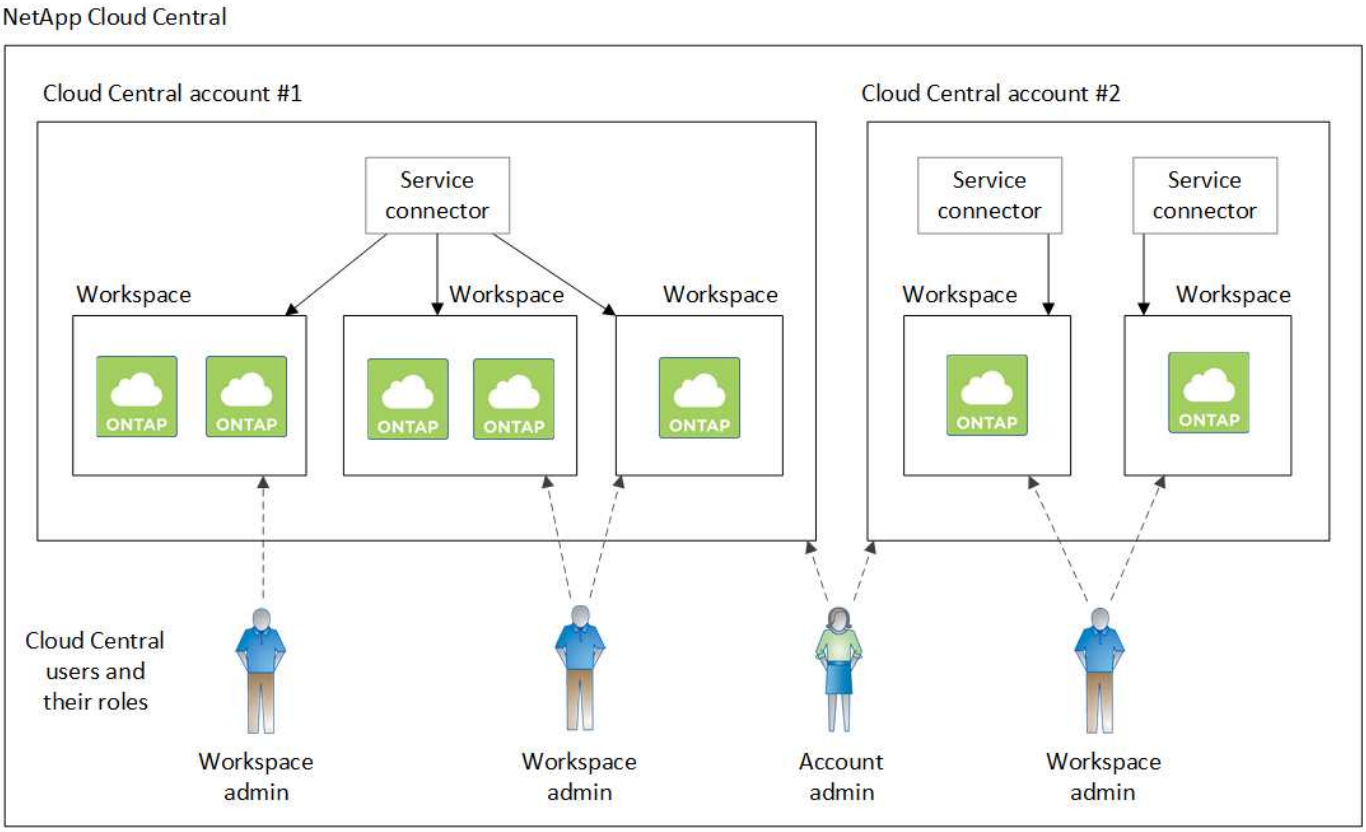
Cloud Manager und die Cloud Volumes ONTAP Systeme befinden sich nicht *in* dem NetApp Cloud Central Konto - sie laufen bei einem Cloud-Provider. Dies ist eine konzeptionelle Darstellung der Beziehung zwischen den einzelnen Komponenten.



Das hier ist ein weiteres Beispiel, das die höchste Mandantenfähigkeit mit zwei separaten Cloud Central Konten belegt. Ein Service-Provider kann beispielsweise Cloud Manager in einem Cloud Central Konto nutzen, um seinen Kunden Services bereitzustellen, während er ein anderes Konto verwendet, um eine Disaster Recovery für eine ihrer Geschäftsbereiche zu bieten.

Bitte beachten Sie, dass Konto 2 zwei separate Serviceanschlüsse enthält. Dies kann passieren, wenn Systeme in verschiedenen Regionen oder separaten Cloud-Providern vorhanden sind.

Und wieder: Cloud Manager und die Cloud Volumes ONTAP Systeme befinden sich nicht *in* dem NetApp Cloud Central Konto - sie laufen bei einem Cloud-Provider. Dies ist eine konzeptionelle Darstellung der Beziehung zwischen den einzelnen Komponenten.



FAQ zur Integration mit Cloud Central Accounts

Einige Zeit nach dem Upgrade auf Cloud Manager 3.7 wählt NetApp bestimmte Cloud Manager Systeme für die Integration mit Cloud Central Konten. In dieser FAQ können Sie Fragen zu diesem Prozess beantworten.

Wie lange dauert dieser Prozess?

In wenigen Minuten.

Ist Cloud Manager nicht verfügbar?

Nein, Sie können weiterhin auf Ihr Cloud Manager System zugreifen.

Wie sieht es mit Cloud Volumes ONTAP aus?

Cloud Volumes ONTAP Systeme werden unterbrechungsfrei zugewiesen.

Was passiert während dieses Prozesses?

NetApp führt während des Integrationsprozesses folgende Maßnahmen durch:

1. Erstellt ein neues Cloud Central-Konto und ordnet es Ihrem Cloud Manager-System zu.
2. Weist jedem vorhandenen Benutzer neue Rollen zu:
   - Cloud Manager-Administratoren werden zu Account-Administratoren
   - Mandantenadministratoren und -Umgebungadministratoren werden zu Workspace-Administratoren
3. Einrichtung von Workspaces, die vorhandene Mandanten ersetzen

4. Stellt Ihre Arbeitsumgebungen in diese Arbeitsbereiche.
5. Verknüpft den Serviceanschluss mit allen Arbeitsbereichen.

Spielt es eine Rolle, wo ich mein Cloud Manager-System installiert habe?

Nein NetApp integriert Systeme in Cloud Central Konten, unabhängig davon, wo sie sich befinden, ob in AWS, Azure oder vor Ort.

Accounts von Cloud-Providern

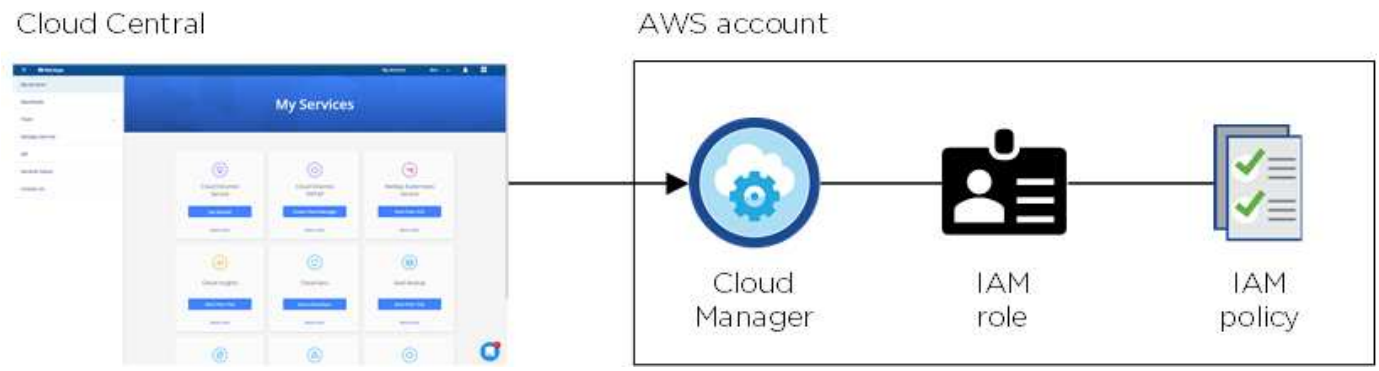
AWS Konten und Berechtigungen

Mit Cloud Manager können Sie das AWS Konto auswählen, in dem Sie ein Cloud Volumes ONTAP System implementieren möchten. 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".

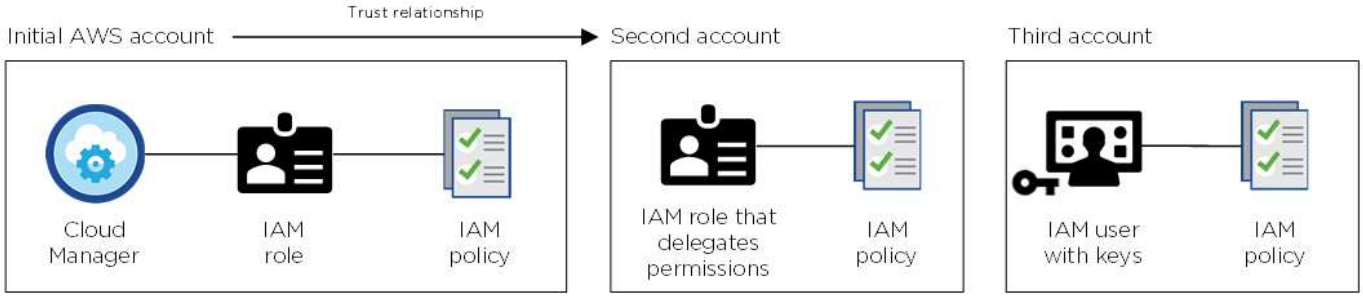


Cloud Manager wählt bei der Erstellung einer neuen Arbeitsumgebung standardmäßig dieses Cloud-Provider-Konto aus:

Weitere AWS Konten

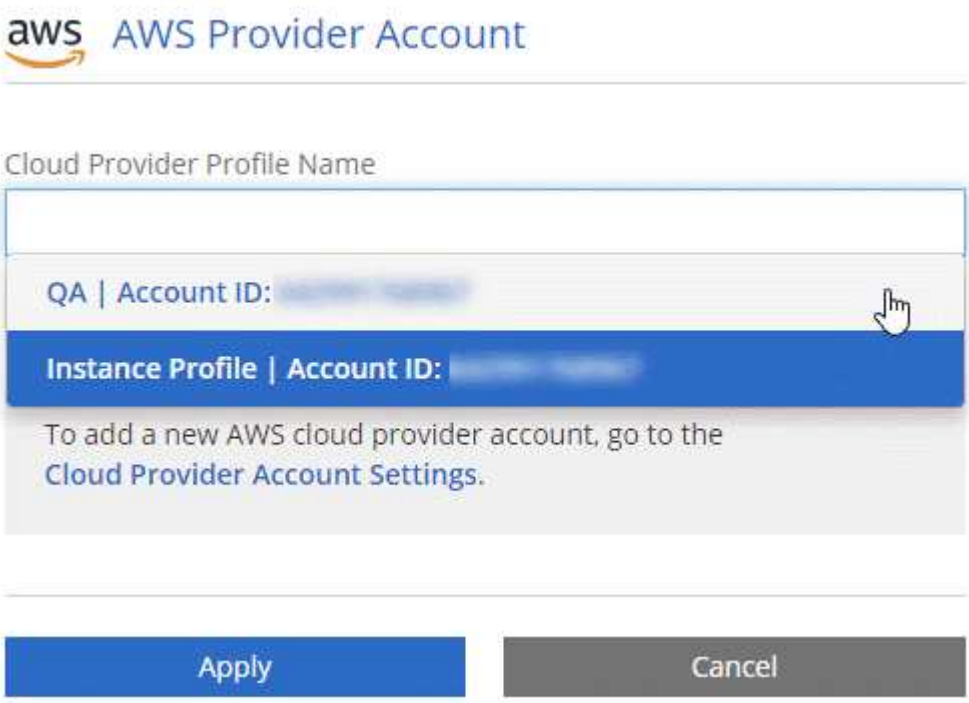
Wenn Sie Cloud Volumes ONTAP in verschiedenen AWS Accounts starten möchten, haben Sie eine der Möglichkeiten "AWS Schlüssel für einen IAM-Benutzer oder den ARN einer Rolle in einem vertrauenswürdigen

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:



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 in AWS über die implementieren "AWS Marketplace" Und das können Sie auch "Installation von Cloud Manager vor Ort".

Wenn Sie den Marktplatz nutzen, werden Berechtigungen auf die gleiche Weise bereitgestellt. Sie müssen lediglich die IAM-Rolle manuell erstellen und einrichten und dann Berechtigungen für weitere Konten bereitstellen.

Bei On-Premises-Implementierungen können nicht eine IAM-Rolle für das Cloud Manager-System eingerichtet werden, Sie können aber Berechtigungen wie bei zusätzlichen AWS-Konten bereitstellen.

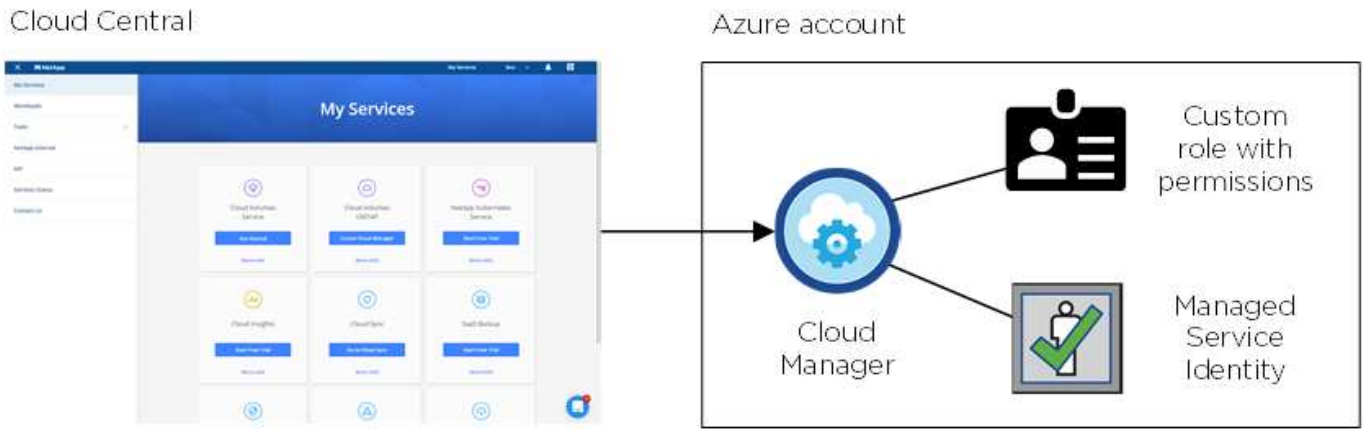
Azure-Konten und Berechtigungen

Mit Cloud Manager können Sie das Azure Konto auswählen, in dem Sie ein Cloud Volumes ONTAP System implementieren möchten. Sie können alle Ihre Cloud Volumes ONTAP Systeme über das erste Azure Konto oder weitere Konten einrichten.

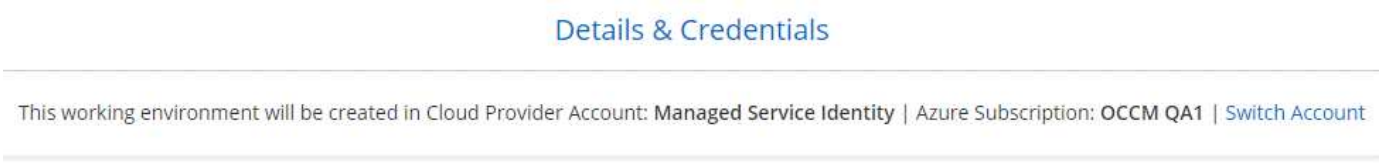
Zunächst das Azure-Konto

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

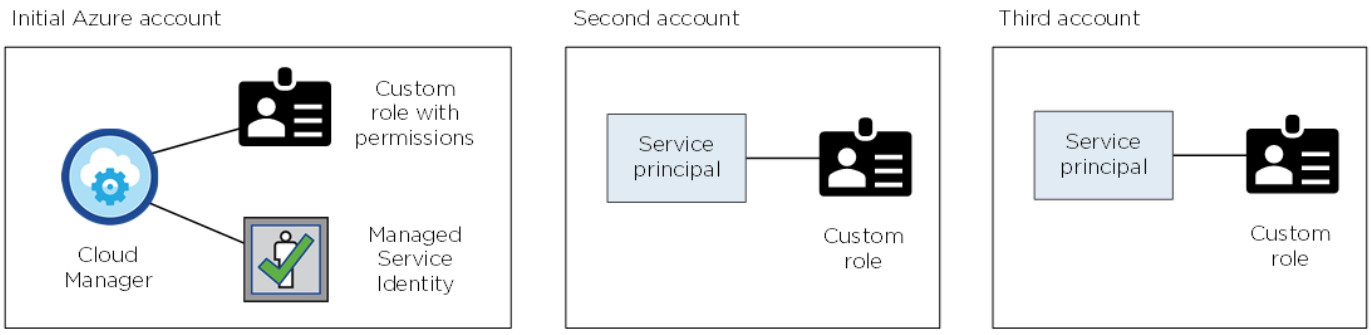


Zusätzliche Azure-Abonnements für das Erstkonto

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".

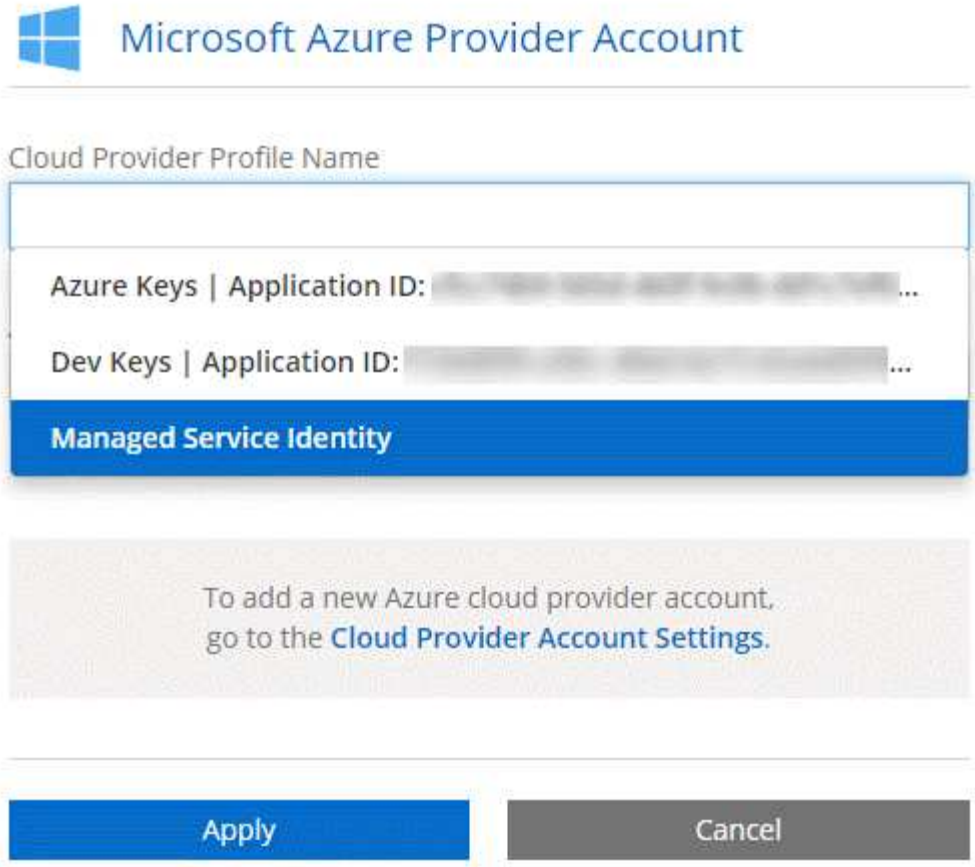
Zusätzliche Azure-Konten

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:



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:



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 in Azure über die implementieren "Azure Marketplace", Und Sie können "Installation von Cloud Manager vor Ort".

Wenn Sie den Marktplatz nutzen, werden Berechtigungen auf die gleiche Weise bereitgestellt. Sie müssen lediglich die verwaltete Identität für Cloud Manager manuell erstellen und einrichten und dann Berechtigungen für weitere Konten bereitstellen.

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

Google Cloud Projekte, Berechtigungen und Konten

Ein Service-Konto bietet Cloud Manager Berechtigungen für die Implementierung und das Management von Cloud Volumes ONTAP Systemen in demselben Projekt wie Cloud Manager oder in verschiedenen Projekten. Google Cloud-Konten, die Sie Cloud Manager hinzufügen, werden für das Daten-Tiering genutzt.

Projekt und Berechtigungen für Cloud Manager

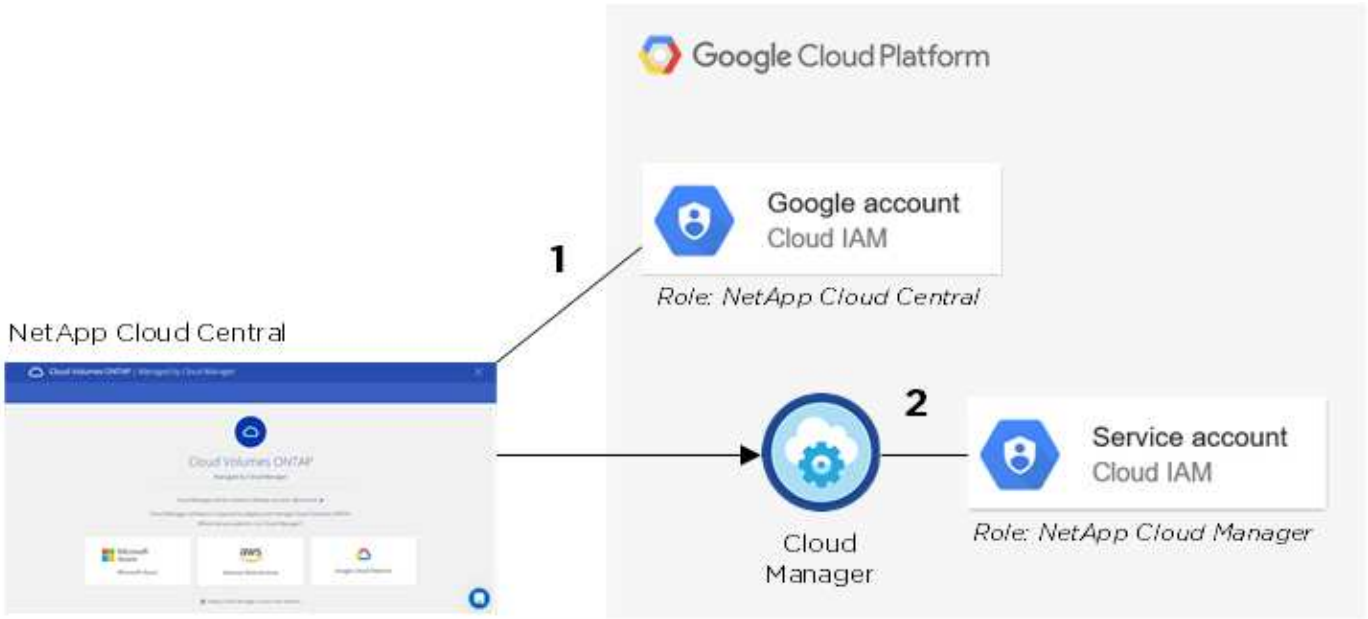
Bevor Cloud Volumes ONTAP in Google Cloud bereitgestellt werden kann, muss Cloud Manager zunächst in einem Google Cloud-Projekt implementiert werden. Cloud Manager kann nicht vor Ort oder bei einem anderen Cloud-Provider ausgeführt werden.

Es müssen zwei Gruppen von Berechtigungen vorhanden sein, bevor Sie Cloud Manager von implementieren "NetApp Cloud Central":

1. Sie müssen Cloud Manager mit einem Google-Konto implementieren, das über Berechtigungen verfügt, um die Cloud Manager VM-Instanz von Cloud Central zu starten.
2. Bei der Bereitstellung von Cloud Manager werden Sie aufgefordert, einen auszuwählen "Servicekonto" Für die VM-Instanz. Cloud Manager erhält Berechtigungen vom Service-Konto, um Cloud Volumes ONTAP Systeme in Ihrem Auftrag zu erstellen und zu managen. Berechtigungen werden durch Hinzufügen einer benutzerdefinierten Rolle an das Servicekonto bereitgestellt.

Wir haben zwei YAML-Dateien eingerichtet, die die erforderlichen Berechtigungen für den Benutzer und das Dienstkonto enthalten. "Erfahren Sie, wie Sie mit den YAML-Dateien Berechtigungen einrichten".

Das folgende Bild zeigt die in den Nummern 1 und 2 oben beschriebenen Berechtigungsanforderungen:



Projekt für Cloud Volumes ONTAP

Cloud Volumes ONTAP kann im selben Projekt wie Cloud Manager oder in einem anderen Projekt ausgeführt werden. Um Cloud Volumes ONTAP in einem anderen Projekt bereitzustellen, müssen Sie zunächst das Cloud Manager Service-Konto und die Rolle zu diesem Projekt hinzufügen.

- "Informationen zur Einrichtung des Cloud Manager Service-Kontos (siehe Schritt 4)".
- "Erfahren Sie, wie Cloud Volumes ONTAP in GCP implementiert und ein Projekt ausgewählt wird".

Konto für Daten-Tiering

Um Daten-Tiering auf einem Cloud Volumes ONTAP System zu ermöglichen, muss Cloud Manager ein Google Cloud Konto hinzufügen. Daten-Tiering verlagert selten genutzte Daten automatisch auf kostengünstigen Objekt-Storage, sodass Sie Speicherplatz auf dem primären Storage freigeben und den sekundären Storage

reduzieren können.

Wenn Sie das Konto hinzufügen, müssen Sie Cloud Manager mit einem Speicherzugriffsschlüssel für ein Servicekonto bereitstellen, das Storage Admin-Berechtigungen hat. Cloud Manager verwendet die Zugriffssteuerung zum Einrichten und Managen eines Cloud Storage-Buckets für Daten-Tiering.

Nachdem Sie ein Google Cloud Konto hinzugefügt haben, können Sie auf einzelnen Volumes das Daten-Tiering aktivieren, wenn Sie sie erstellen, ändern oder replizieren.

- "Erfahren Sie, wie Sie GCP-Konten in Cloud Manager einrichten und hinzufügen".
- "Verschieben Sie inaktive Daten auf kostengünstigen Objekt-Storage".

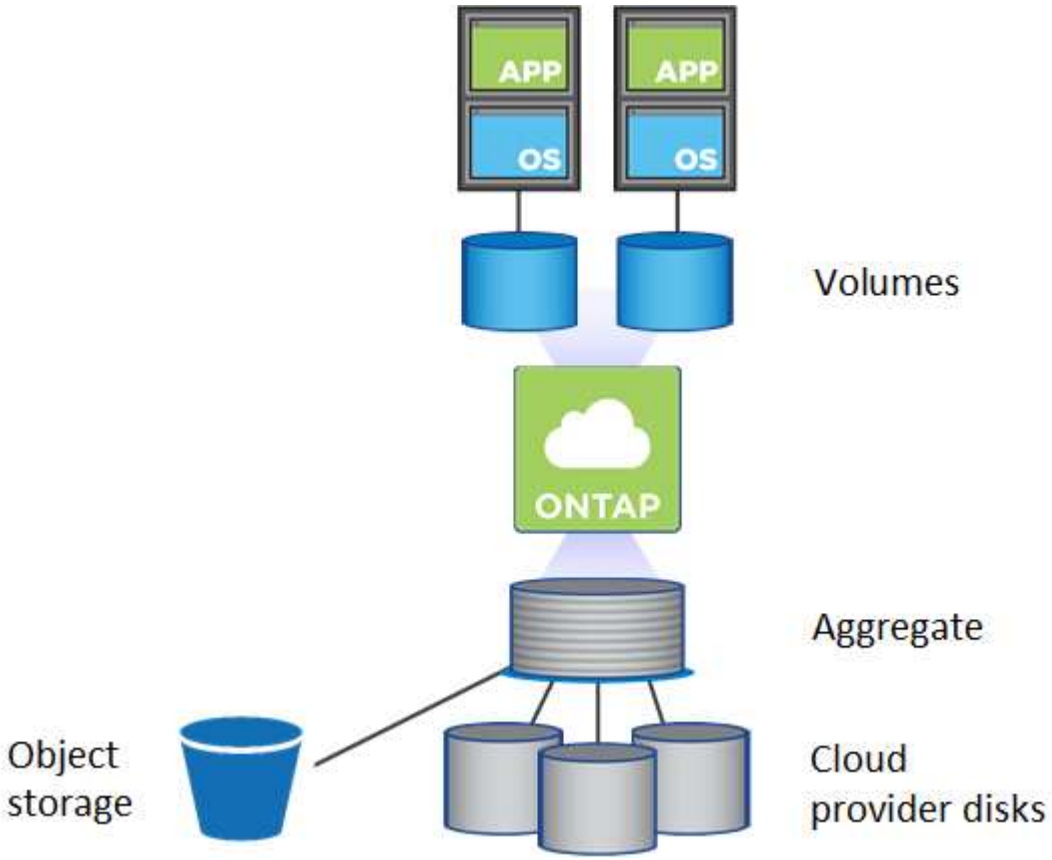
Storage

Festplatten und Aggregate

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

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"

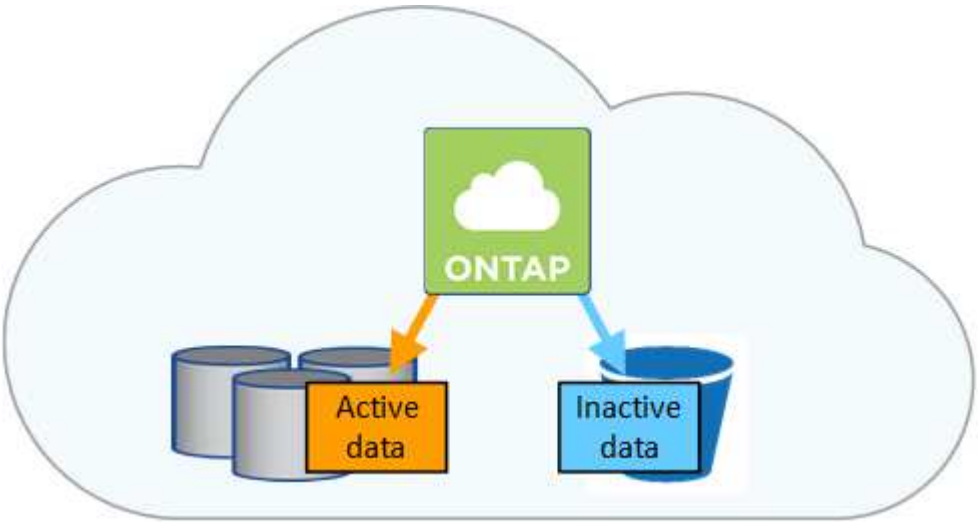
RAID-Typ

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. Wenn Sie die Tiering-Ebene eines Systems ändern, können Sie eine andere S3-Storage-Klasse wählen.

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.

Tiering-Ebenen

Wenn Sie keinen Zugriff auf inaktive Daten planen, können Sie Ihre Storage-Kosten senken, indem Sie die Tiering-Ebene eines Systems auf eine der folgenden Stufen ändern: *Intelligent Tiering*, *One-Zone infrequent Access* oder *Standard-infrequent Access*. Wenn Sie die Tiering-Ebene ändern, werden inaktive Daten in der Klasse Standard-Speicher gestartet und in die von Ihnen ausgewählte Speicherklasse verschoben, sofern nach 30 Tagen kein Zugriff auf die Daten erfolgt.

Die Zugriffskosten sind höher, wenn Sie auf die Daten zugreifen. Berücksichtigen Sie diese also, bevor Sie das Tiering-Level ändern. "Erfahren Sie mehr über Amazon S3 Storage Classes".

Nachdem Sie das System erstellt haben, ist es möglich, die Tiering-Ebene zu ändern. Weitere

Informationen finden Sie unter "Tiering inaktiver Daten in kostengünstigen Objektspeicher".

Die Tiering-Ebene ist systemweit, 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. Wenn Sie die Tiering-Ebene eines Systems ändern, können Sie einen anderen Azure Storage Tier wählen.

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.

Tiering-Ebenen

Wenn Sie keinen Zugriff auf die inaktiven Daten haben, können Sie Ihre Storage-Kosten senken, indem Sie die Tiering-Ebene eines Systems zum Azure *cool* Storage Tier ändern. 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.

Die Zugriffskosten sind höher, wenn Sie auf die Daten zugreifen. Berücksichtigen Sie diese also, bevor Sie das Tiering-Level ändern. "Weitere Informationen zu Azure Blob Storage-Zugriffsklassen".

Nachdem Sie das System erstellt haben, ist es möglich, die Tiering-Ebene zu ändern. Weitere Informationen finden Sie unter "Tiering inaktiver Daten in kostengünstigen Objektspeicher".

Die Tiering-Ebene ist systemweit, 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.

Tiering-Ebenen

Derzeit werden keine anderen GCP-Speicherklassen unterstützt.

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.

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 an AWS oder Azure zurückgegeben werden.

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

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.

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.

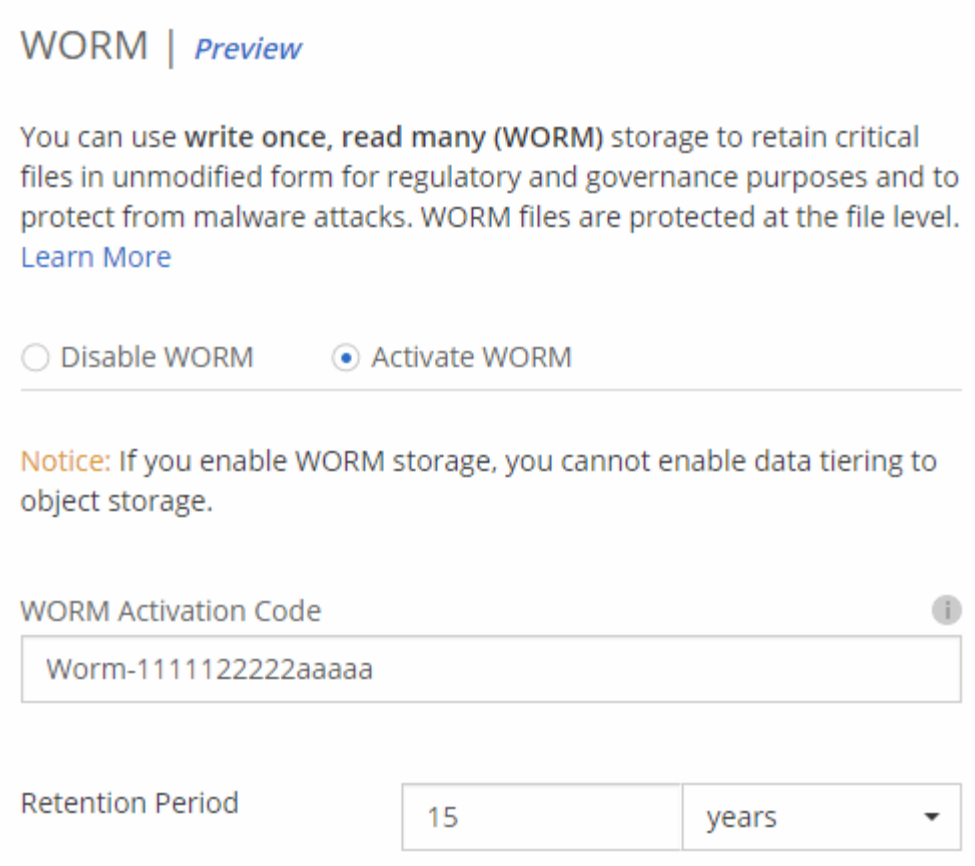
Nach Ablauf der Aufbewahrungsfrist sind Sie dafür verantwortlich, alle Dateien zu löschen, die Sie nicht mehr benötigen.

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 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.

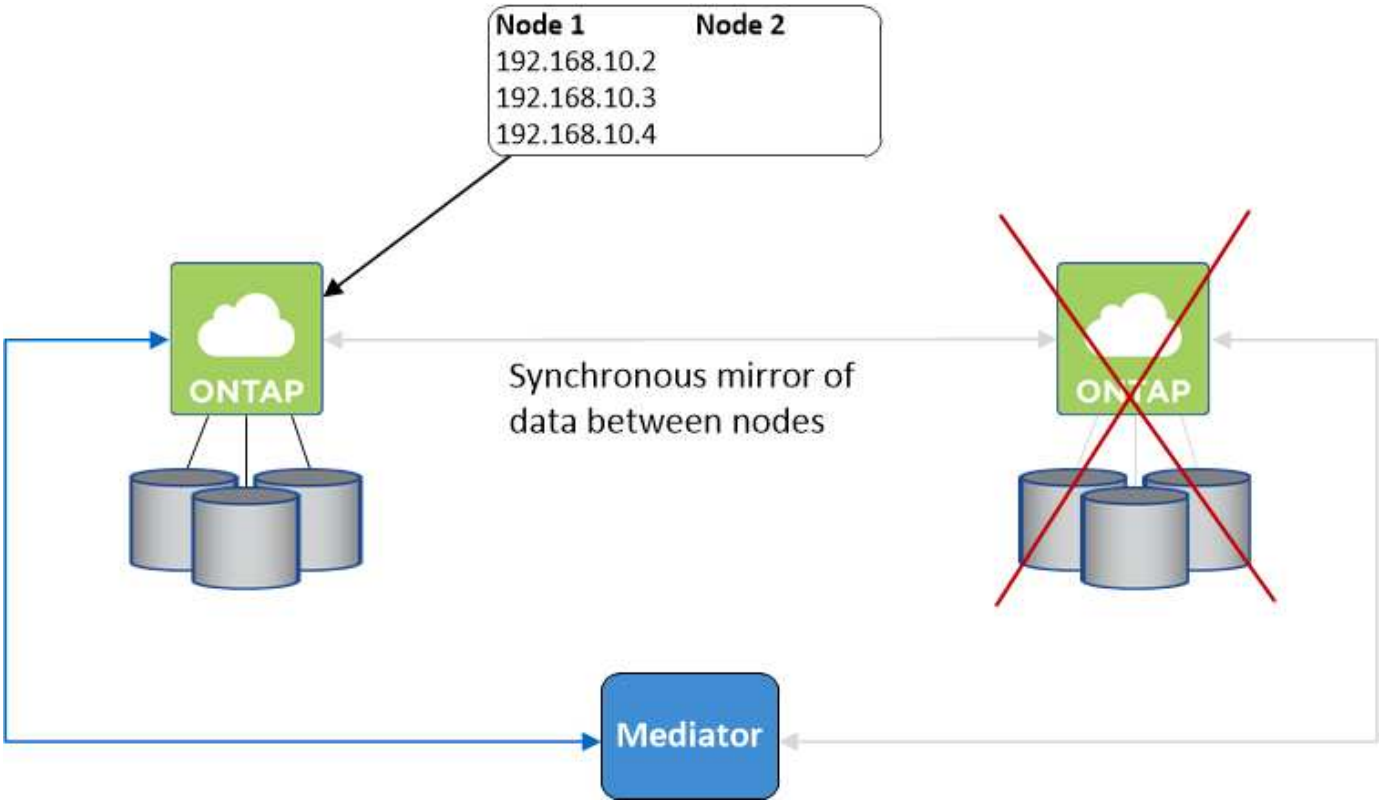
Storage-Übernahme und -Giveback für iSCSI

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

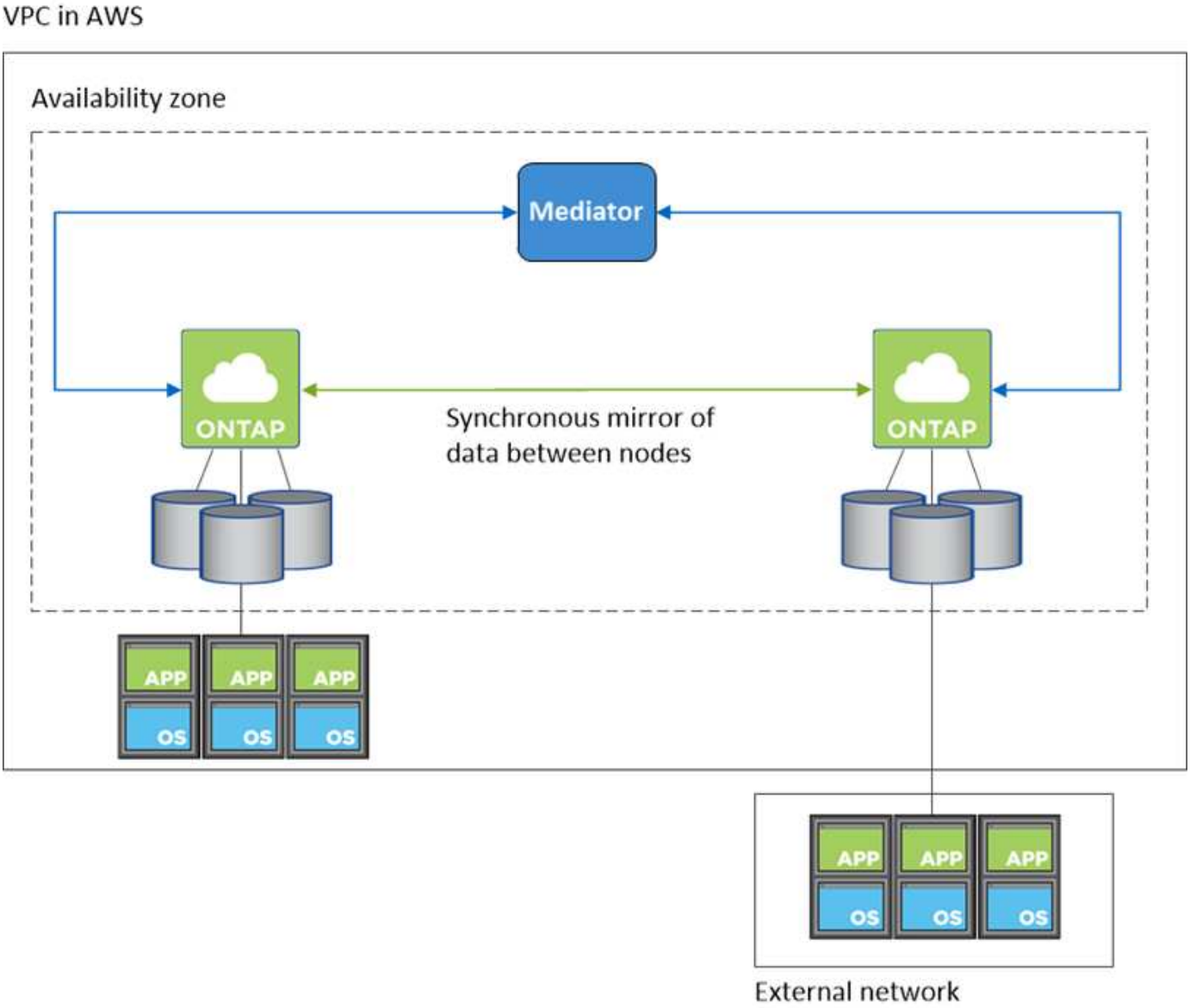
Durch die Implementierung einer HA-Konfiguration in einer einzelnen Verfügbarkeitszone (AZ) kann eine hohe Verfügbarkeit Ihrer Daten sichergestellt werden, wenn eine Instanz, auf der ein Cloud Volumes ONTAP Node ausgeführt wird, ausfällt. Alle Daten sind nativ von außerhalb des VPC zugänglich.

> 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.

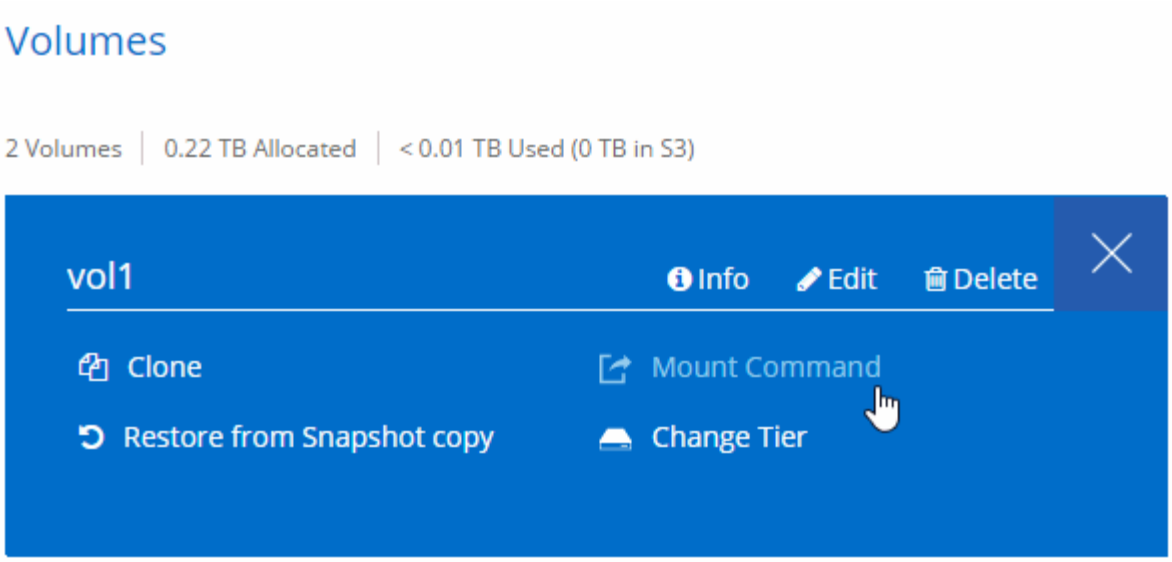
Weitere Informationen zur Performance von Cloud Volumes ONTAP finden Sie unter "Leistung".

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.

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

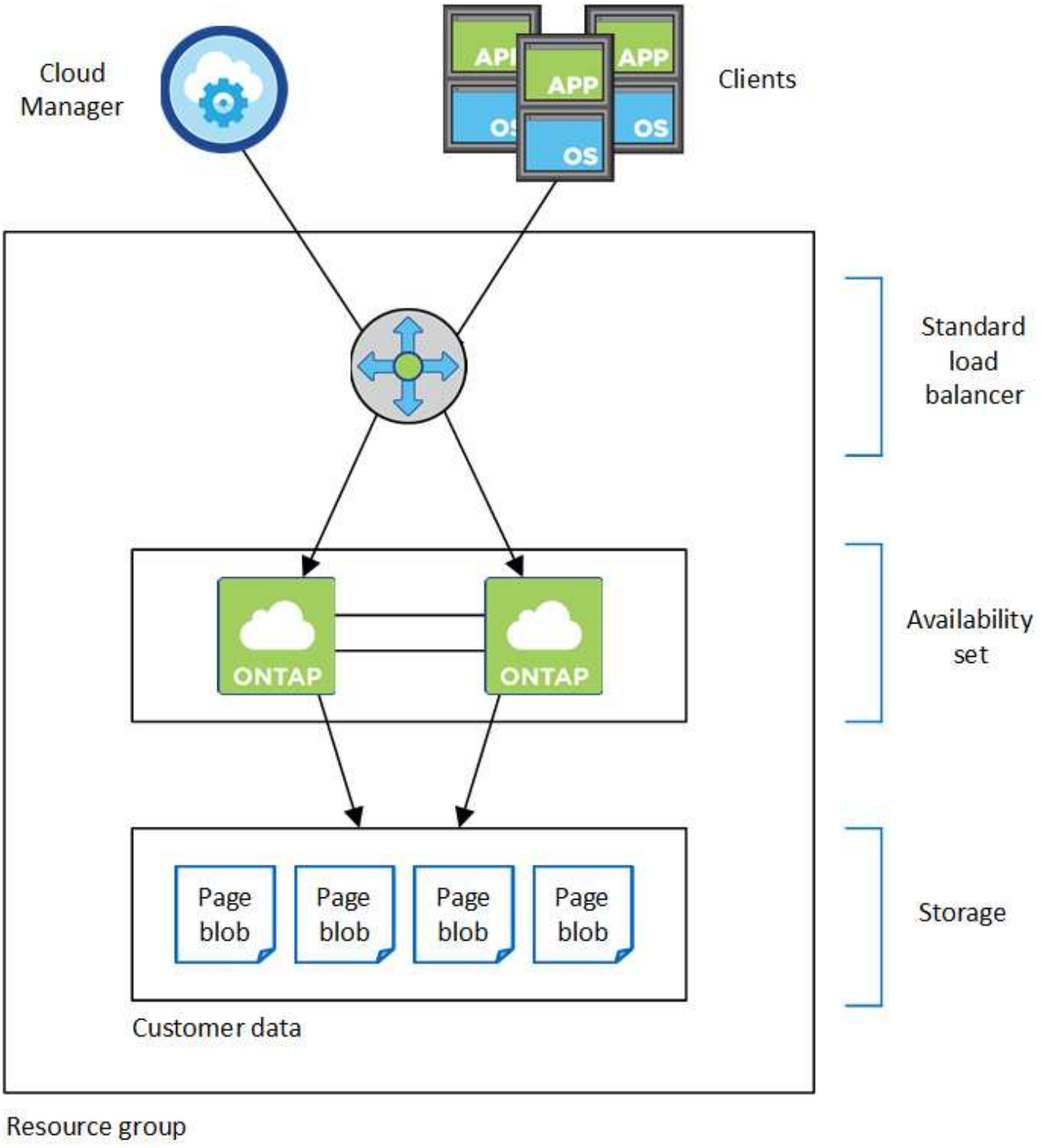


Hochverfügbarkeitspaare in Azure

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 Boot-, Root- und Kerndaten ist zusätzlicher Storage erforderlich:

- Zwei 90-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 128-GB-Standard-HDD-Festplatten zum Speichern der Cores (eine pro Node)

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.

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.

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
- Google Cloud Platform-Standardverschlüsselung

Sie können NetApp Volume Encryption mit nativer AWS, Azure oder GCP-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.

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.

Vom Kunden gemanagte Schlüssel werden mit Cloud Volumes ONTAP nicht 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.

Siehe "API-Entwicklerhandbuch" Weitere Informationen zur Verwendung der Parameter „GcpEncryption“.

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".

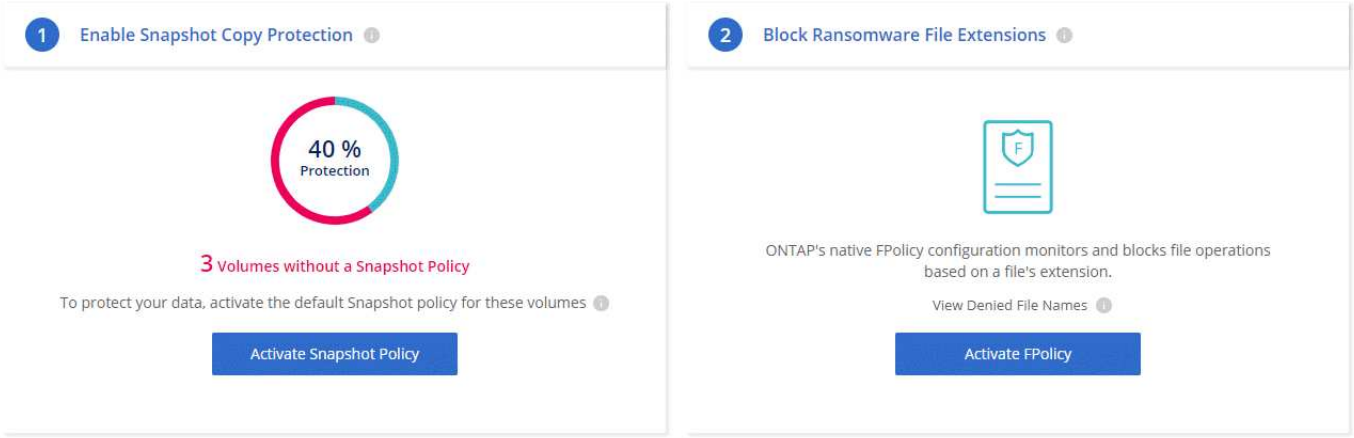
Schutz durch Ransomware

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.

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".

Los geht’s

Implementierungsübersicht

Bevor Sie beginnen, möchten Sie sich möglicherweise besser über Ihre Optionen für die Implementierung von Cloud Manager und Cloud Volumes ONTAP informieren.

Installation von Cloud Manager

Cloud Manager Software ist für die Implementierung und das Management von Cloud Volumes ONTAP erforderlich. Sie können Cloud Manager an einem der folgenden Standorte bereitstellen:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform

  Cloud Manager muss sich bei der Implementierung von Cloud Volumes ONTAP in GCP in der Google Cloud Platform befinden.

- IBM Cloud
- In Ihrem eigenen Netzwerk

Wie Sie Cloud Manager implementieren, hängt davon ab, für welchen Standort Sie sich entscheiden:

Standort für Cloud Manager	So implementieren Sie Cloud Manager
AWS	1. "Cloud Manager über NetApp Cloud Central implementieren" (Empfohlen) 2. "Implementierung über AWS Marketplace" 3. "Laden Sie die Software auf einem Linux-Host herunter, und installieren Sie sie"
AWS C2S	"Implementieren Sie Cloud Manager über den AWS Intelligence Community Marketplace"
Azure allgemein verfügbare Region	1. "Cloud Manager über NetApp Cloud Central implementieren" (Empfohlen) 2. "Implementieren Sie sie im Azure Marketplace" 3. "Laden Sie die Software auf einem Linux-Host herunter, und installieren Sie sie"
Azure Government	"Implementieren von Cloud Manager über den Azure US Government Marketplace"
Azure Deutschland	"Laden Sie die Software auf einem Linux-Host herunter, und installieren Sie sie"

Standort für Cloud Manager	So implementieren Sie Cloud Manager
Google Cloud Platform	1. "Cloud Manager über NetApp Cloud Central implementieren" (Empfohlen) 2. "Laden Sie die Software auf einem Linux-Host herunter, und installieren Sie sie" Die Implementierung von Cloud Manager in der Google Cloud ist über GCP Marketplace nicht möglich
IBM Cloud	"Laden Sie die Software auf einem Linux-Host herunter, und installieren Sie sie"
Des On-Premises-Netzwerks	"Laden Sie die Software auf einem Linux-Host herunter, und installieren Sie sie"

Einrichtung von Cloud Manager

Möglicherweise möchten Sie nach der Installation von Cloud Manager zusätzliche Einrichtung durchführen, z. B. das Hinzufügen weiterer Cloud-Provider-Konten, das Installieren eines HTTPS-Zertifikats und mehr.

- "Einrichten Ihres Cloud Central Kontos"
- "Hinzufügen von AWS Konten zu Cloud Manager"
- "Hinzufügen von Azure-Konten zu Cloud Manager"
- "Installieren eines HTTPS-Zertifikats"
- "Einrichten des AWS KMS"

Implementierung von Cloud Volumes ONTAP

Nachdem Cloud Manager betriebsbereit war, können Sie mit der Implementierung von Cloud Volumes ONTAP bei Ihrem Cloud-Provider beginnen.

"Erste Schritte in AWS", "Erste Schritte in Azure", und "Erste Schritte in GCP" Anweisungen zur schnellen Inbetriebnahme von Cloud Volumes ONTAP Weitere Hilfe finden Sie unter:

- "Unterstützte Konfigurationen für Cloud Volumes ONTAP 9.7 in AWS"
- "Unterstützte Konfigurationen für Cloud Volumes ONTAP 9.7 in Azure"
- "Unterstützte Konfigurationen für Cloud Volumes ONTAP 9.7 in GCP"
- "Planung Ihrer Konfiguration"
- "Starten von Cloud Volumes ONTAP in AWS"
- "Starten von Cloud Volumes ONTAP in Azure"
- "Einführung von Cloud Volumes ONTAP in GCP"

Erste Schritte mit Cloud Volumes ONTAP in AWS

Starten Sie mit Cloud Volumes ONTAP, indem Sie AWS einrichten und dann die Cloud Manager Software über NetApp Cloud Central starten. Für das erste Cloud Volumes

ONTAP System, das Sie in AWS starten, steht eine kostenlose 30-Tage-Testversion zur Verfügung.

Richten Sie Ihr Netzwerk ein

1. Aktivieren Sie ausgehenden Internetzugriff vom Ziel-VPC aus, sodass Cloud Manager und Cloud Volumes ONTAP mit mehreren Endpunkten in Verbindung treten können.

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

2. 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.

Stellen Sie die erforderlichen AWS-Berechtigungen bereit

Wenn Sie Cloud Manager über NetApp Cloud Central implementieren, müssen Sie ein AWS-Konto verwenden, das über die Berechtigung zum Bereitstellen der Instanz verfügt.

1. Gehen Sie zur AWS IAM-Konsole und erstellen Sie eine Richtlinie durch Kopieren und Einfügen der Inhalte des "NetApp Cloud Central-Richtlinie für AWS".
2. Hängen Sie die Richtlinie an den IAM-Benutzer an.

Abonnieren Sie ihn im AWS Marketplace

"Abonnieren Sie Cloud Manager über den AWS Marketplace" Um sicherzustellen, dass es nach der kostenlosen Testversion von Cloud Volumes ONTAP keine Serviceunterbrechung gibt. Sie erhalten für jedes von Ihnen erstellte Cloud Volumes ONTAP-PAYGO-System und jede von Ihnen erstellte Add-on-Funktion die Gebühr.

Wenn Sie Cloud Volumes ONTAP mit Ihrer eigenen Lizenz (BYOL) starten, "Anschließend müssen Sie das Angebot im AWS Marketplace abonnieren".

Starten Sie Cloud Manager über NetApp Cloud Central

Cloud Manager Software ist für die Implementierung und das Management von Cloud Volumes ONTAP erforderlich. Es dauert nur ein paar Minuten, um eine Cloud Manager Instanz von zu starten "Cloud Central".

Starten Sie Cloud Volumes ONTAP mit Cloud Manager

Wenn Cloud Manager fertig ist, klicken Sie einfach auf Erstellen, wählen Sie den Systemtyp aus, den Sie starten möchten, und führen Sie die Schritte im Assistenten aus. Nach 25 Minuten sollte Ihr erstes Cloud

Volumes ONTAP System betriebsbereit sein.

Sehen Sie sich das folgende Video an, um die folgenden Schritte durchzugehen:

► https://docs.netapp.com/de-de/occm37//media/video_getting_started_aws.mp4 *(video)*

Weiterführende Links

- "Bewertung"
- "Netzwerkanforderungen für Cloud Manager"
- "Netzwerkanforderungen für Cloud Volumes ONTAP in AWS"
- "Sicherheitsgruppenregeln für AWS"
- "Hinzufügen von AWS Konten zu Cloud Manager"
- "Was Cloud Manager mit AWS-Berechtigungen macht"
- "Starten von Cloud Volumes ONTAP in AWS"
- "Starten von Cloud Manager über den AWS Marketplace"

Erste Schritte mit Cloud Volumes ONTAP in Azure

Steigen Sie in das Cloud Volumes ONTAP ein, indem Sie Azure einrichten und dann die Cloud Manager Software von NetApp Cloud Central implementieren. Für die Implementierung von Cloud Manager in stehen separate Anweisungen zur Verfügung "Azure Regionen der US-Regierung" Und ein "Azure Deutschland Regionen".

Richten Sie Ihr Netzwerk ein

Aktivieren Sie ausgehenden Internetzugriff vom Ziel-VNet aus, sodass Cloud Manager und Cloud Volumes ONTAP mit mehreren Endpunkten in Verbindung treten können.

Dieser Schritt ist wichtig, da Cloud Manager Cloud Volumes ONTAP nicht ohne ausgehenden Internetzugang implementieren kann. Wenn Sie die ausgehende Verbindung begrenzen müssen, lesen Sie die Liste der Endpunkte für "Cloud Manager" Und "Cloud Volumes ONTAP".

Stellen Sie die erforderlichen Azure Berechtigungen bereit

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.

1. Laden Sie die herunter "NetApp Cloud Central-Richtlinie für Azure".
2. Ändern Sie die JSON-Datei, indem Sie im Feld "AssignableScopes" Ihre Azure Abonnement-ID hinzufügen.
3. Verwenden Sie die JSON-Datei, um in Azure namens *Azure SetupAsService* eine benutzerdefinierte Rolle zu erstellen.

   Beispiel: **Az Rollendefinition erstellen --Role-Definition C:\Policy_for_Setup_as_Service_Azure.json**

4. Weisen Sie die benutzerdefinierte Rolle über das Azure Portal dem Benutzer zu, der Cloud Manager über Cloud Central bereitstellt.

Starten Sie Cloud Manager über NetApp Cloud Central

Cloud Manager Software ist für die Implementierung und das Management von Cloud Volumes ONTAP erforderlich. Es dauert nur ein paar Minuten, um eine Cloud Manager Instanz von zu starten "Cloud Central".

Starten Sie Cloud Volumes ONTAP mit Cloud Manager

Sobald Cloud Manager bereit ist, klicken Sie einfach auf Erstellen, wählen Sie den Systemtyp aus, den Sie bereitstellen möchten, und führen Sie die Schritte im Assistenten aus. Nach 25 Minuten sollte Ihr erstes Cloud Volumes ONTAP System betriebsbereit sein.

Weiterführende Links

- "Bewertung"
- "Netzwerkanforderungen für Cloud Manager"
- "Netzwerkanforderungen für Cloud Volumes ONTAP in Azure"
- "Sicherheitsgruppenregeln für Azure"
- "Hinzufügen von Azure-Konten zu Cloud Manager"
- "Was Cloud Manager mit Azure-Berechtigungen tut"
- "Starten von Cloud Volumes ONTAP in Azure"
- "Cloud Manager über den Azure Marketplace starten"

Erste Schritte mit Cloud Volumes ONTAP in der Google Cloud Platform

Steigen Sie in die Cloud Volumes ONTAP ein, indem Sie GCP einrichten und dann die Cloud Manager Software von NetApp Cloud Central implementieren.

Cloud Manager muss in der Google Cloud Platform installiert sein, um Cloud Volumes ONTAP in GCP implementieren zu können.

Richten Sie Ihr Netzwerk ein

Aktivieren Sie ausgehenden Internetzugriff vom Ziel-VPC aus, sodass Cloud Manager und Cloud Volumes ONTAP mit mehreren Endpunkten in Verbindung treten können.

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

GCP-Berechtigungen und -Projekte einrichten

Stellen Sie sicher, dass zwei Gruppen von Berechtigungen vorhanden sind:

1. Stellen Sie sicher, dass der GCP-Benutzer, der Cloud Manager über NetApp Cloud Central implementiert, die Berechtigungen in hat "Cloud Central-Richtlinie für GCP".

   "Sie können eine benutzerdefinierte Rolle mit der YAML-Datei erstellen" Und verbinden Sie sie dann mit dem Benutzer. Sie müssen die gCloud-Befehlszeile verwenden, um die Rolle zu erstellen.

2. Richten Sie ein Service-Konto ein, das über die Berechtigungen verfügt, die Cloud Manager zum Erstellen und Managen von Cloud Volumes ONTAP-Systemen in Projekten benötigt.

   Dieses Service-Konto wird in Schritt 6 der Cloud Manager VM zugeordnet.

   - "Rolle in GCP anlegen" Dazu gehören die im definierten Berechtigungen "Cloud Manager-Richtlinie für GCP". Sie müssen die gCloud-Befehlszeile verwenden.

     Die in dieser YAML-Datei enthaltenen Berechtigungen unterscheiden sich von den Berechtigungen in Schritt 2a.

   - "Erstellen Sie ein GCP-Service-Konto und wenden Sie die benutzerdefinierte Rolle an, die Sie gerade erstellt haben".
   - Wenn Sie Cloud Volumes ONTAP in anderen Projekten implementieren möchten, "Sie gewähren Zugriff, indem Sie dem Projekt das Service-Konto mit der Rolle Cloud Manager hinzufügen". Sie müssen diesen Schritt für jedes Projekt wiederholen.

GCP für Daten-Tiering einrichten

Für das Tiering von kalten Daten von Cloud Volumes ONTAP 9.7 auf kostengünstigen Objekt-Storage (ein Google Cloud-Storage-Bucket) müssen zwei Anforderungen erfüllt werden:

1. "Erstellen eines Dienstkontos" Damit verfügt er über die vordefinierte Storage-Administratorrolle und das Cloud Manager-Servicekonto als Benutzer.

   Sie müssen dieses Servicekonto später auswählen, wenn Sie eine Cloud Volumes ONTAP Arbeitsumgebung erstellen. Dieses Servicekonto unterscheidet sich von dem Servicekonto, das Sie in Schritt 2 erstellt haben.

2. "Konfigurieren Sie das Cloud Volumes ONTAP-Subnetz für privaten Google-Zugriff".

Wenn Sie Daten-Tiering mit Cloud Volumes ONTAP 9.6 verwenden möchten, "Führen Sie dann diese Schritte aus".

Aktivieren Sie Google Cloud-APIs

"Aktivieren Sie die folgenden Google Cloud APIs in Ihrem Projekt". Für die Implementierung von Cloud Manager und Cloud Volumes ONTAP sind diese APIs erforderlich.

- Cloud Deployment Manager V2-API

- Cloud Resource Manager API
- Compute Engine-API
- Stackdriver Logging API

Abonnieren Sie ihn im GCP Marketplace

"Abonnieren Sie Cloud Volumes ONTAP über den GCP Marketplace" Um sicherzustellen, dass es keine Unterbrechung des Dienstes nach Ihrer kostenlosen Testversion endet. Sie werden von diesem Abonnement für jedes von Ihnen erstellte Cloud Volumes ONTAP PAYGO-System berechnet.

Starten Sie Cloud Manager über NetApp Cloud Central

Cloud Manager Software ist für die Implementierung und das Management von Cloud Volumes ONTAP erforderlich. Es dauert nur wenige Minuten, um eine Cloud Manager Instanz in GCP von zu starten "Cloud Central".

Wenn Sie sich für GCP als Cloud-Provider entscheiden, werden Sie von Google aufgefordert, sich bei Ihrem Konto anzumelden und Berechtigungen zu erteilen. Durch Klicken auf „Zulassen“ wird Zugriff auf die für die Implementierung von Cloud Manager erforderlichen Computing-APIs gewährt.

Starten Sie Cloud Volumes ONTAP mit Cloud Manager

Sobald Cloud Manager bereit ist, klicken Sie einfach auf Erstellen, wählen Sie den Systemtyp aus, den Sie bereitstellen möchten, und führen Sie die Schritte im Assistenten aus. Nach 25 Minuten sollte Ihr erstes Cloud Volumes ONTAP System betriebsbereit sein.

Weiterführende Links

- "Bewertung"
- "Netzwerkanforderungen für Cloud Manager"
- "Netzwerkanforderungen für Cloud Volumes ONTAP in GCP"
- "Firewall-Regeln für GCP"
- "Was Cloud Manager mit GCP-Berechtigungen macht"
- "Einführung von Cloud Volumes ONTAP in GCP"
- "Herunterladen und Installieren der Cloud Manager-Software auf einem Linux-Host"

Cloud Manager einrichten

Einrichtung von Workspaces und Benutzern im Cloud Central Konto

Jedes Cloud Manager System ist einem *NetApp Cloud Central Account* zugeordnet. Richten Sie das mit Ihrem Cloud Manager System verknüpfte Cloud Central Konto ein, damit Benutzer auf Cloud Manager zugreifen und Cloud Volumes ONTAP Systeme in Workspaces implementieren können. Fügen Sie einfach einen Benutzer hinzu oder fügen

Sie mehrere Benutzer und Arbeitsbereiche hinzu.

Das Konto wird in Cloud Central gewartet. Alle Änderungen, die Sie vornehmen, stehen also anderen Cloud Manager Systemen und anderen Cloud-Datenservices von NetApp zur Verfügung. "Erfahren Sie mehr über die Funktionsweise von Cloud Central-Accounts".

Arbeitsbereiche werden hinzugefügt

In Cloud Manager können Sie mithilfe von Workspaces eine Reihe von Arbeitsumgebungen von anderen Arbeitsumgebungen und anderen Benutzern isolieren. Sie können beispielsweise zwei Arbeitsbereiche erstellen und den Arbeitsbereichen separate Benutzer zuordnen.

Schritte

1. Klicken Sie Auf **Kontoeinstellungen**.

2. Klicken Sie Auf **Arbeitsbereiche**.
3. Klicken Sie Auf **Neuen Arbeitsbereich Hinzufügen**.
4. Geben Sie einen Namen für den Arbeitsbereich ein und klicken Sie auf **Hinzufügen**.

Nachdem Sie fertig sind

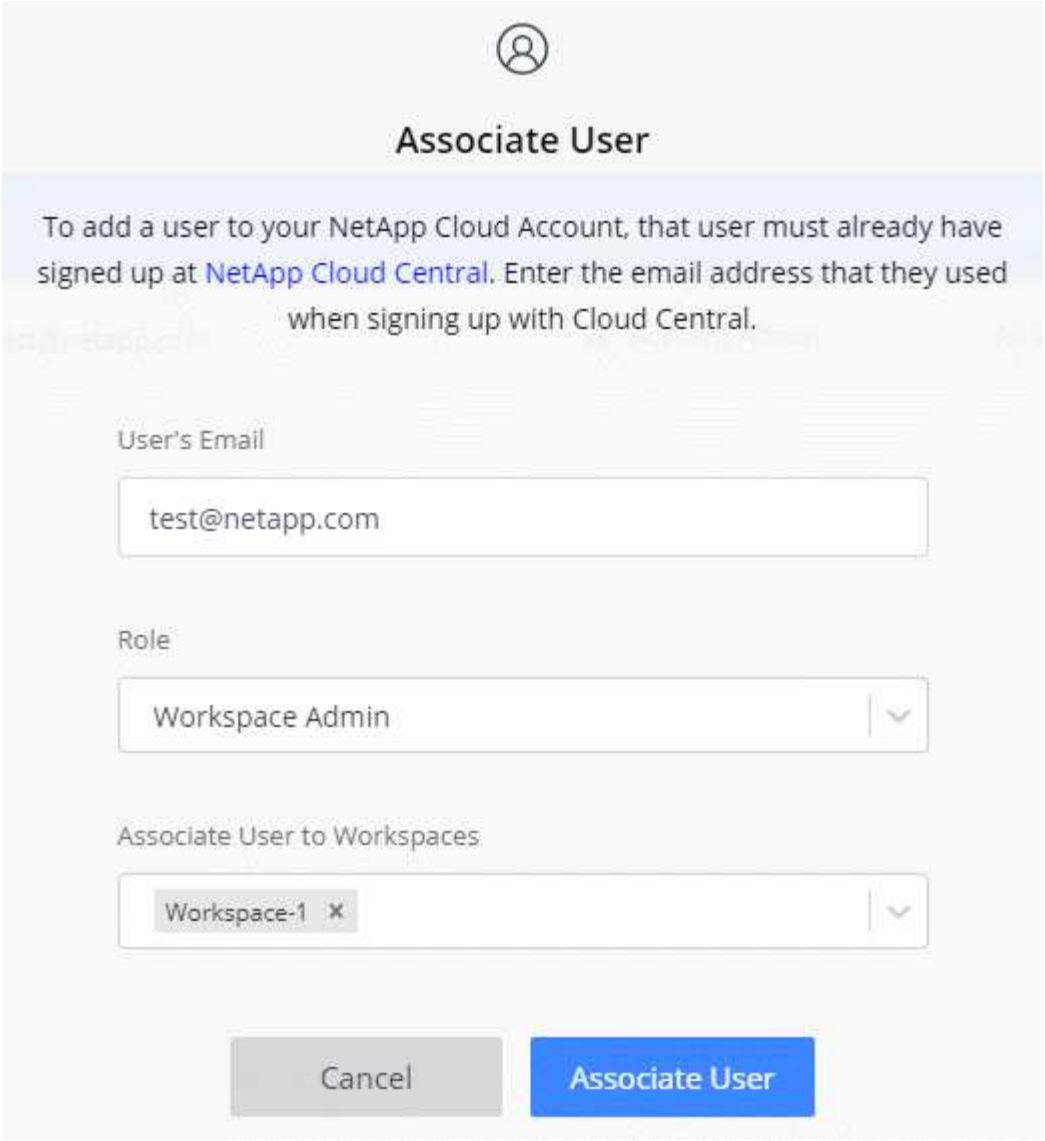
Sie können nun Benutzer und Service Connectors mit dem Arbeitsbereich verknüpfen.

Benutzer hinzufügen

Cloud Central Benutzer werden mit dem Cloud Central Konto verknüpft, damit diese Arbeitsumgebungen in Cloud Manager erstellen und verwalten können.

Schritte

1. Wenn der Benutzer dies noch nicht getan hat, bitten Sie den Benutzer, zu wechseln "NetApp Cloud Central" Und erstellen Sie ein Konto.
2. Klicken Sie in Cloud Manager auf **Kontoeinstellungen**.
3. Klicken Sie auf der Registerkarte Benutzer auf **Benutzer verknüpfen**.
4. Geben Sie die E-Mail-Adresse des Benutzers ein, und wählen Sie eine Rolle für den Benutzer aus:
   - **Account Admin**: Kann jede Aktion in Cloud Manager ausführen.
   - **Workspace Admin**: Kann Ressourcen in zugewiesenen Workspaces erstellen und verwalten.
5. Wenn Sie Workspace Admin ausgewählt haben, wählen Sie eine oder mehrere Arbeitsbereiche aus, die diesem Benutzer zugeordnet werden sollen.



6. Klicken Sie Auf * Benutzer Verknüpfen*.

Ergebnis

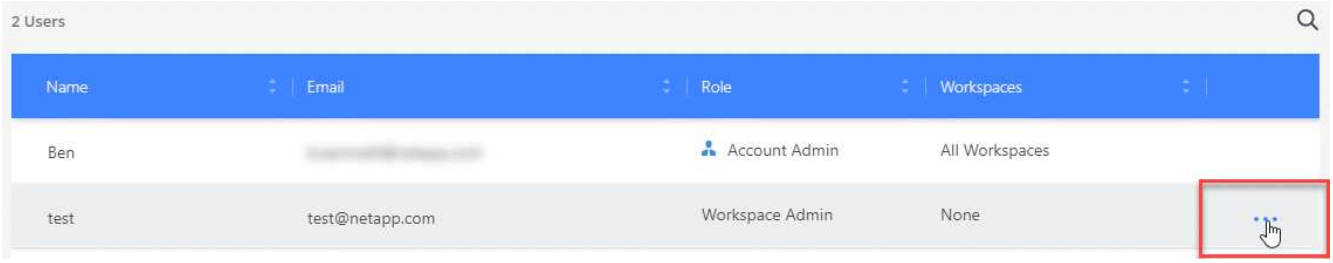
Der Benutzer sollte eine E-Mail von NetApp Cloud Central mit dem Titel „Account Association“ erhalten. Die E-Mail enthält die für den Zugriff auf Cloud Manager erforderlichen Informationen.

Verknüpfen von Workspace-Administratoren mit Arbeitsbereichen

Sie können Workspace-Administratoren jederzeit mit zusätzlichen Arbeitsbereichen verknüpfen. Durch die Verknüpfung des Benutzers können die Arbeitsumgebungen in diesem Arbeitsbereich erstellt und angezeigt werden.

Schritte

1. Klicken Sie Auf **Kontoeinstellungen**.
2. Klicken Sie auf das Aktionsmenü in der Zeile, die dem Benutzer entspricht.



3. Klicken Sie Auf **Arbeitsbereiche Verwalten**.
4. Wählen Sie einen oder mehrere Arbeitsbereiche aus, und klicken Sie auf **Anwenden**.

Ergebnis

Der Benutzer kann jetzt über Cloud Manager auf diese Arbeitsbereiche zugreifen, solange der Service Connector auch mit den Arbeitsbereichen verknüpft war.

Verknüpfen von Service Connectors mit Arbeitsbereichen

Ein Service-Anschluss ist Teil des Cloud Manager Systems. Es wird auf der Virtual-Machine-Instanz ausgeführt, die bei Ihrem Cloud-Provider oder auf einem von Ihnen konfigurierten On-Premises-Host implementiert wurde. Sie müssen diesen Service Connector mit Arbeitsbereichen verknüpfen, damit Workspace-Administratoren über Cloud Manager auf diese Arbeitsbereiche zugreifen können.

Wenn Sie nur Kontoadministratoren haben, ist es nicht erforderlich, den Service Connector mit Arbeitsbereichen zu verknüpfen. Account-Administratoren haben standardmäßig die Möglichkeit, auf alle Workspaces in Cloud Manager zuzugreifen.

"Erfahren Sie mehr über Benutzer, Arbeitsbereiche und Serviceanschlüsse".

Schritte

1. Klicken Sie Auf **Kontoeinstellungen**.
2. Klicken Sie Auf **Service Connector**.
3. Klicken Sie auf **Arbeitsbereiche verwalten** für den Service-Anschluss, den Sie verknüpfen möchten.
4. Wählen Sie einen oder mehrere Arbeitsbereiche aus, und klicken Sie auf **Anwenden**.

Ergebnis

Workspace-Administratoren können jetzt auf die zugehörigen Arbeitsbereiche zugreifen, solange der Benutzer auch mit dem Arbeitsbereich verknüpft war.

Einrichten und Hinzufügen von AWS Konten zu Cloud Manager

Wenn Sie Cloud Volumes ONTAP in verschiedenen AWS Konten implementieren möchten, müssen Sie die erforderlichen Berechtigungen angeben und die Details zu Cloud Manager hinzufügen. Wie Sie die Berechtigungen bereitstellen, hängt davon ab, ob Sie Cloud Manager mit AWS Schlüsseln oder dem ARN einer Rolle in einem vertrauenswürdigen Konto bereitstellen möchten.

Bei der Implementierung von Cloud Manager über Cloud Central fügt Cloud Manager automatisch das AWS Konto hinzu, in dem Sie Cloud Manager implementiert haben. Ein initiales Konto wird nicht hinzugefügt, wenn Sie die Cloud Manager Software manuell auf einem vorhandenen System installieren. "Erfahren Sie mehr über AWS Konten und Berechtigungen".

Auswahl

- Erteilen von Berechtigungen durch die Bereitstellung von AWS Schlüsseln
- Gewährung von Berechtigungen durch Annahme von IAM-Rollen in anderen Konten

Erteilen von Berechtigungen durch die Bereitstellung von AWS Schlüsseln

Wenn Sie Cloud Manager mit AWS Schlüsseln für einen IAM-Benutzer bereitstellen möchten, müssen Sie diesem Benutzer die erforderlichen Berechtigungen erteilen. Die Cloud Manager IAM-Richtlinie definiert die AWS-Aktionen und -Ressourcen, die Cloud Manager verwenden darf.

Schritte

1. Laden Sie die IAM-Richtlinie von Cloud Manager aus herunter "Seite „Cloud Manager Policies“ aufgeführt".
2. Erstellen Sie über die IAM-Konsole Ihre eigene Richtlinie, indem Sie den Text aus der Cloud Manager IAM-Richtlinie kopieren und einfügen.

   "AWS Dokumentation: Erstellung von IAM-Richtlinien"

3. Hängen Sie die Richtlinie an eine IAM-Rolle oder einen IAM-Benutzer an.
   - "AWS Documentation: Erstellung von IAM-Rollen"
   - "AWS Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"

Ergebnis

Das Konto verfügt nun über die erforderlichen Berechtigungen. Sie können es jetzt zu Cloud Manager hinzufügen.

Gewährung von Berechtigungen durch Annahme von IAM-Rollen in anderen Konten

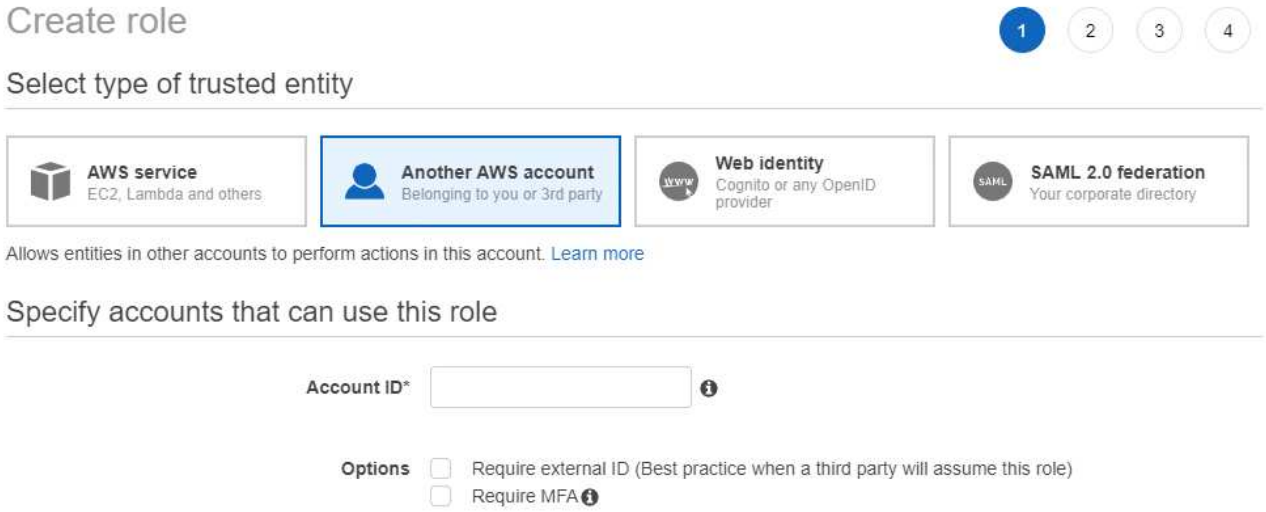
Sie können eine Vertrauensbeziehung zwischen dem Quell-AWS-Konto einrichten, in dem Sie die Cloud Manager-Instanz und anderen AWS-Konten mithilfe von IAM-Rollen bereitgestellt haben. Dann würden Sie Cloud Manager über die vertrauenswürdigen Konten mit dem ARN der IAM-Rollen versorgen.

Schritte

1. Rufen Sie das Zielkonto auf, in dem Sie Cloud Volumes ONTAP bereitstellen und eine IAM-Rolle erstellen möchten, indem Sie **ein weiteres AWS-Konto** auswählen.

   Gehen Sie wie folgt vor:

   - Geben Sie die ID des Kontos ein, auf dem sich die Cloud Manager Instanz befindet.
   - Hängen Sie die Cloud Manager IAM-Richtlinie an, die über die erhältlich ist "Seite „Cloud Manager Policies“ aufgeführt".



2. Wechseln Sie zum Quellkonto, in dem sich die Cloud Manager Instanz befindet, und wählen Sie die IAM-Rolle aus, die mit der Instanz verbunden ist.

   a. Klicken Sie auf **Vertrauensverhältnis > Vertrauensverhältnis bearbeiten**.

   b. Fügen Sie die Aktion „STS:AssumeRole“ und den ARN der Rolle hinzu, die Sie im Zielkonto erstellt haben.

      Beispiel

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
}
}
```

Ergebnis

Das Konto verfügt nun über die erforderlichen Berechtigungen. Sie können es jetzt zu Cloud Manager hinzufügen.

Hinzufügen von AWS Konten zu Cloud Manager

Nachdem Sie ein AWS Konto mit den erforderlichen Berechtigungen bereitgestellt haben, können Sie das Konto zu Cloud Manager hinzufügen. Damit können Sie Cloud Volumes ONTAP Systeme in diesem Konto starten.

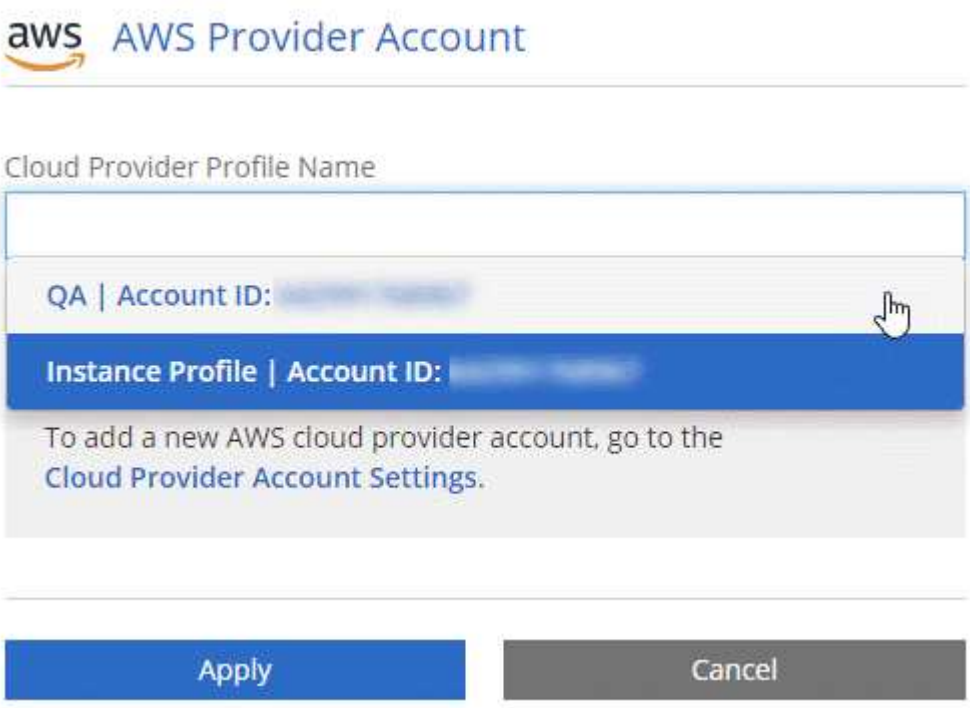
Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Cloud Provider & Support Accounts** aus.

2. Klicken Sie auf **Neues Konto hinzufügen** und wählen Sie **AWS**.
3. Sie können entscheiden, ob Sie AWS Schlüssel oder den ARN einer vertrauenswürdigen IAM-Rolle bereitstellen möchten.
4. Bestätigen Sie, dass die Richtlinienanforderungen erfüllt wurden, und klicken Sie dann auf **Konto erstellen**.

Ergebnis

Sie können jetzt auf der Seite Details und Anmeldeinformationen zu einem anderen Konto wechseln, wenn Sie eine neue Arbeitsumgebung erstellen:



Einrichten und Hinzufügen von Azure-Konten zu Cloud Manager

Wenn Sie Cloud Volumes ONTAP in verschiedenen Azure-Konten implementieren möchten, müssen Sie diese Konten die erforderlichen Berechtigungen erteilen und anschließend Details zu den Konten in Cloud Manager einfügen.

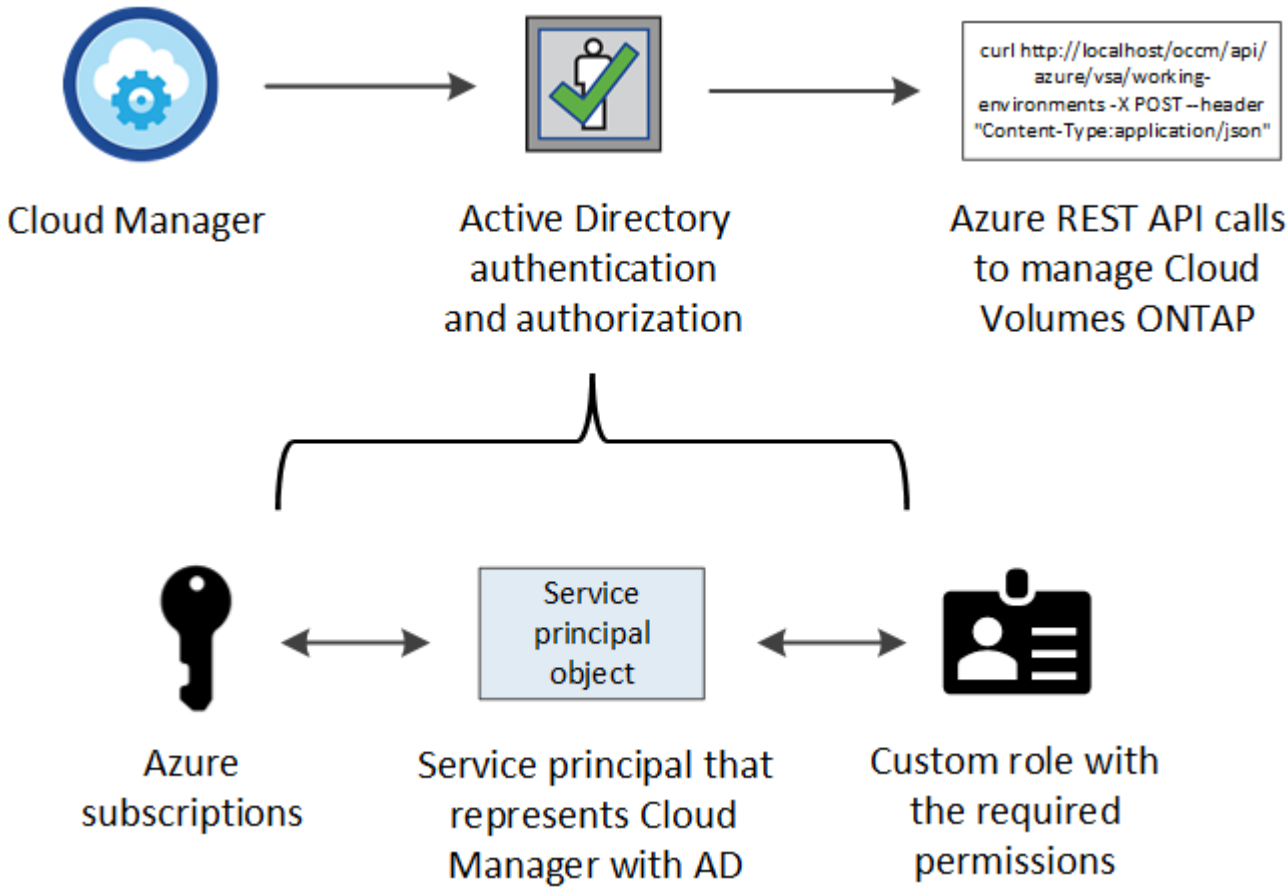
Bei der Implementierung von Cloud Manager über Cloud Central fügt Cloud Manager automatisch das Azure Konto hinzu, in dem Sie Cloud Manager implementiert haben. Ein initiales Konto wird nicht hinzugefügt, wenn Sie die Cloud Manager Software manuell auf einem vorhandenen System installieren. "Weitere Informationen zu Azure Konten und Berechtigungen".

Azure-Berechtigungen über einen Service-Principal gewähren

Cloud Manager benötigt Berechtigungen zum Ausführen von Aktionen in Azure. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie einen Service-Principal in Azure Active Directory erstellen und einrichten, sowie die für Cloud Manager erforderlichen Azure Zugangsdaten erhalten.

Über diese Aufgabe

In der folgenden Abbildung wird dargestellt, wie Cloud Manager Berechtigungen zum Ausführen von Vorgängen in Azure erhält. Ein Service-Prinzipalobjekt, das an ein oder mehrere Azure Subscriptions gebunden ist, stellt Cloud Manager in Azure Active Directory dar und wird einer benutzerdefinierten Rolle zugewiesen, die die erforderlichen Berechtigungen zulässt.



Schritte

1. Erstellen Sie eine Azure Active Directory-Anwendung.
2. Anwendung einer Rolle zuweisen.
3. Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu.
4. Holen Sie die Anwendungs-ID und die Verzeichnis-ID ab.
5. Erstellen Sie einen Clientschlüssel.

Erstellen einer Azure Active Directory-Anwendung

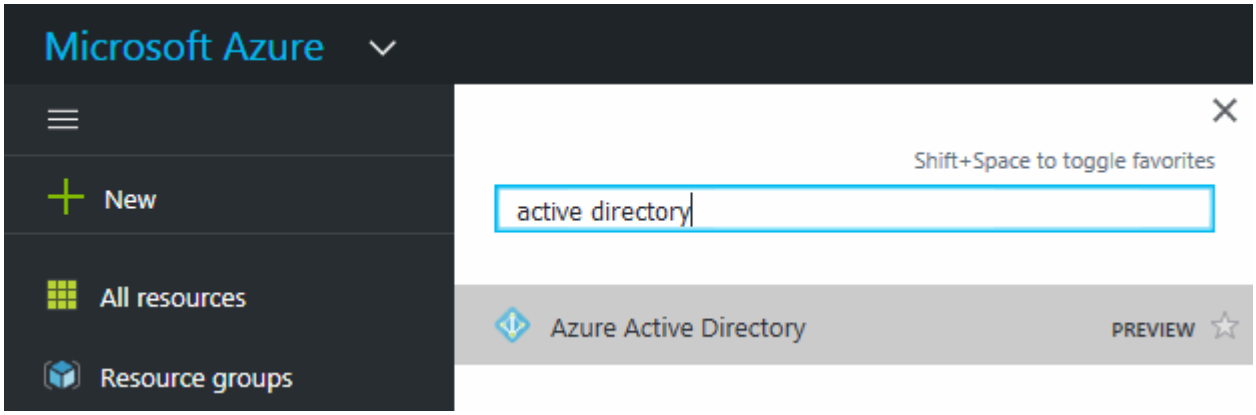
Erstellen einer Azure Active Directory (AD)-Applikation und eines Service-Principal, den Cloud Manager für die rollenbasierte Zugriffssteuerung nutzen kann

Bevor Sie beginnen

Sie müssen über die richtigen Berechtigungen in Azure verfügen, um eine Active Directory-Anwendung zu erstellen und die Anwendung einer Rolle zuzuweisen. Weitere Informationen finden Sie unter "Microsoft Azure-Dokumentation: Erforderliche Berechtigungen".

Schritte

1. Öffnen Sie über das Azure-Portal den **Azure Active Directory**-Service.



2. Klicken Sie im Menü auf **App-Registrierungen**.
3. Klicken Sie auf **Neue Registrierung**.
4. Geben Sie Details zur Anwendung an:
   - **Name**: Geben Sie einen Namen für die Anwendung ein.
   - **Kontotyp**: Wählen Sie einen Kontotyp aus (jeder funktioniert mit Cloud Manager).
   - **Redirect URI**: Wählen Sie **Web** und geben Sie dann eine beliebige URL ein – z. B. https://url
5. Klicken Sie Auf **Registrieren**.

Ergebnis

Sie haben die AD-Anwendung und den Service-Principal erstellt.

Anwendung einer Rolle zuweisen

Sie müssen den Service-Principal an ein oder mehrere Azure-Abonnements binden und ihm die benutzerdefinierte Rolle „OnCommand Cloud Manager Operator“ zuweisen, damit Cloud Manager über Berechtigungen in Azure verfügt.

Schritte

1. Erstellen einer benutzerdefinierten Rolle:

   a. Laden Sie die herunter "Cloud Manager Azure-Richtlinie".

   b. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

      Sie sollten die ID für jedes Azure Abonnement hinzufügen, aus dem Benutzer Cloud Volumes ONTAP Systeme erstellen.

      Beispiel

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

c. Verwenden Sie die JSON-Datei, um eine benutzerdefinierte Rolle in Azure zu erstellen.

   Im folgenden Beispiel wird gezeigt, wie eine benutzerdefinierte Rolle mithilfe der Azure CLI 2.0 erstellt wird:

   Az Rollendefinition erstellen --Role-Definition C:\Policy_for_Cloud_Manager_Azure_3.7.4.json

Sie sollten nun über eine benutzerdefinierte Rolle namens *OnCommand Cloud Manager Operator* verfügen.

2. Applikation der Rolle zuweisen:

   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.

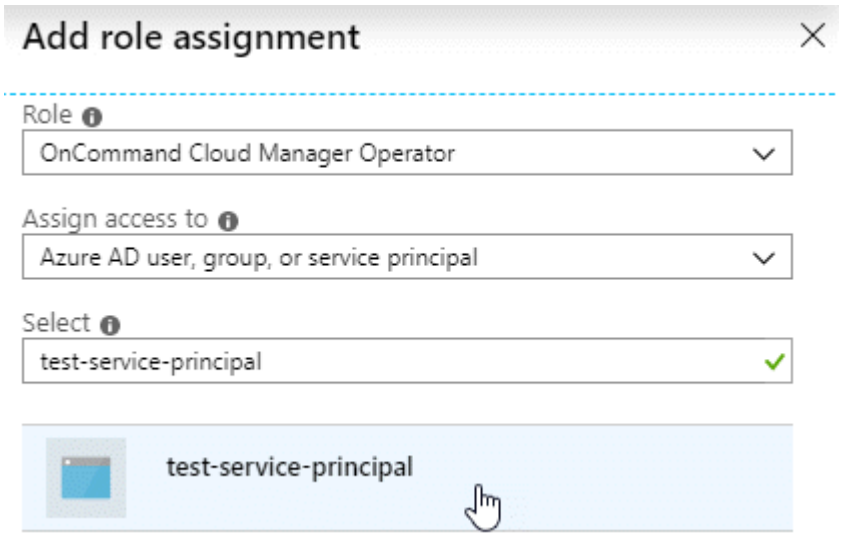
   b. Wählen Sie das Abonnement aus.

   c. Klicken Sie auf **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.

   d. Wählen Sie die Rolle **OnCommand Cloud Manager Operator** aus.

   e. * Azure AD Benutzer, Gruppe oder Serviceprincipal* ausgewählt lassen.

   f. Suchen Sie nach dem Namen der Anwendung (Sie finden sie nicht in der Liste durch Scrollen).



   g. Wählen Sie die Anwendung aus und klicken Sie auf **Speichern**.

      Der Service Principal für den Cloud Manager verfügt jetzt über die erforderlichen Azure Berechtigungen für das Abonnement.

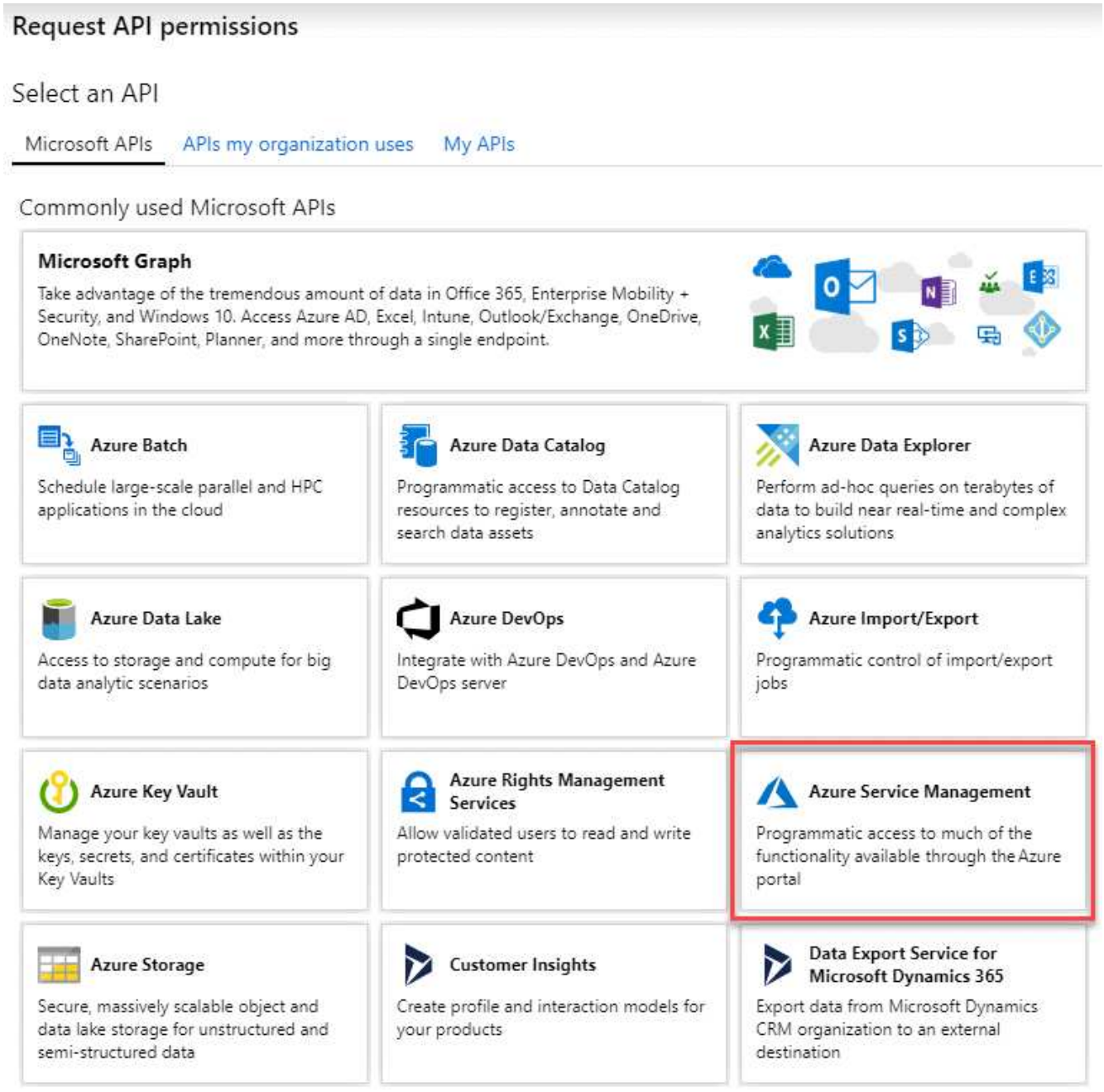
Wenn Sie Cloud Volumes ONTAP aus mehreren Azure Subscriptions bereitstellen möchten, müssen Sie den Service-Prinzipal an jedes dieser Subscriptions binden. Mit Cloud Manager können Sie das Abonnement auswählen, das Sie bei der Implementierung von Cloud Volumes ONTAP verwenden möchten.

Windows Azure Service Management-API-Berechtigungen werden hinzugefügt

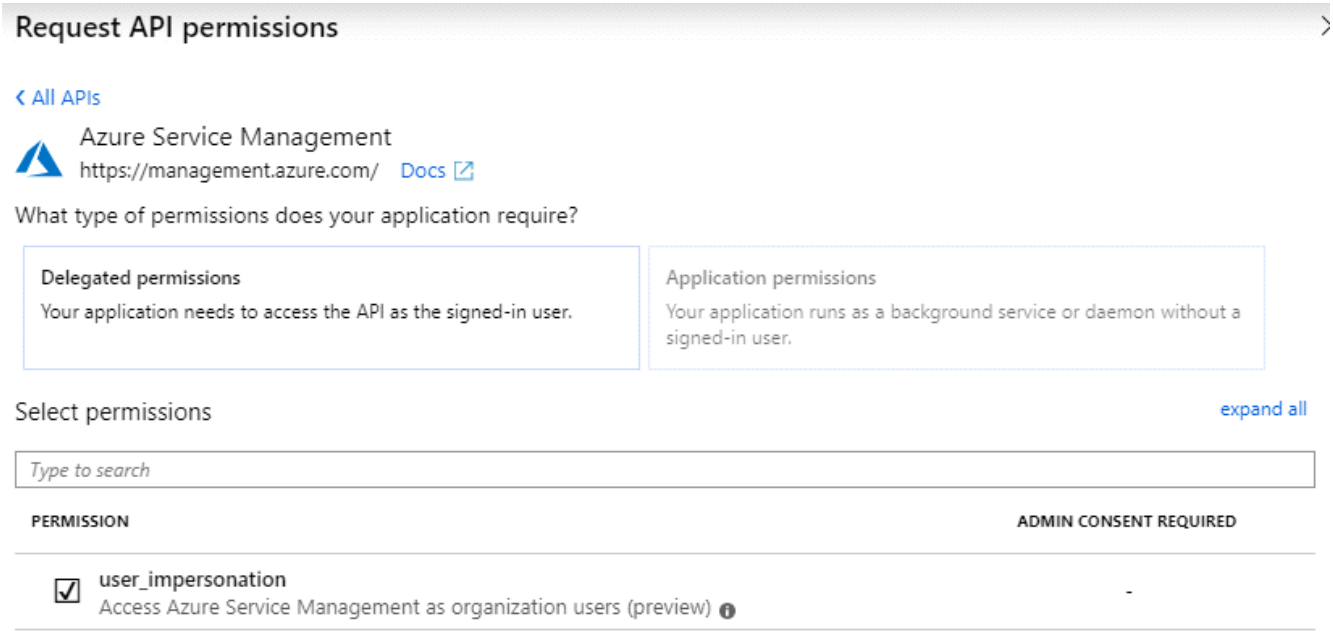
Der Service-Principal muss über die Berechtigungen „Windows Azure Service Management API“ verfügen.

Schritte

1. Klicken Sie im **Azure Active Directory**-Dienst auf **App-Registrierungen** und wählen Sie die Anwendung aus.
2. Klicken Sie auf **API-Berechtigungen > Berechtigung hinzufügen**.
3. Wählen Sie unter **Microsoft APIs Azure Service Management** aus.



4. Klicken Sie auf **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann auf **Berechtigungen hinzufügen**.

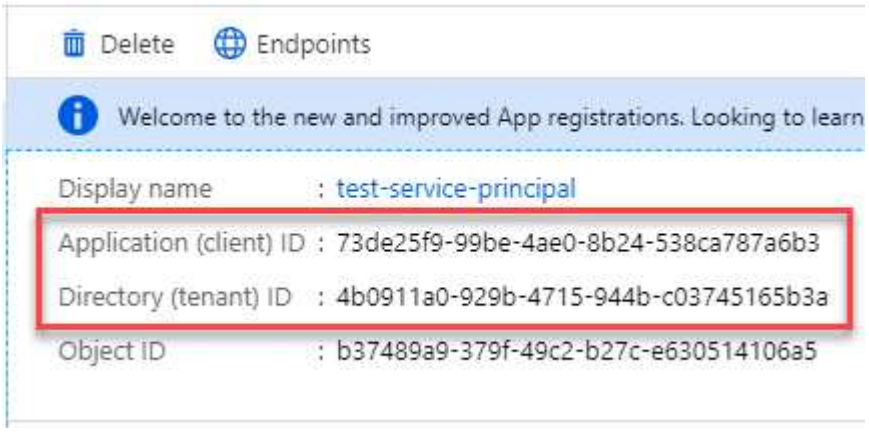


Abrufen der Anwendungs-ID und der Verzeichnis-ID

Wenn Sie dem Cloud Manager das Azure-Konto hinzufügen, müssen Sie die Anwendungs- (Client-) ID und die Verzeichnis- (Mandanten-)ID für die Applikation angeben. Cloud Manager verwendet die IDs, um sich programmatisch anzumelden.

Schritte

1. Klicken Sie im **Azure Active Directory**-Dienst auf **App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Application (Client) ID** und die **Directory (Tenant) ID**.



Erstellen eines Clientgeheimnisses

Sie müssen ein Client-Geheimnis erstellen und Cloud Manager dann den Wert des Geheimnisses zur Verfügung stellen, damit Cloud Manager es zur Authentifizierung mit Azure AD verwenden kann.

Wenn Sie das Konto zu Cloud Manager hinzufügen, bezieht sich Cloud Manager auf das Kundengeheimnis als Applikationsschlüssel.

Schritte

1. Öffnen Sie den Dienst **Azure Active Directory**.
2. Klicken Sie auf **App-Registrierungen** und wählen Sie Ihre Anwendung aus.
3. Klicken Sie auf **Zertifikate & Geheimnisse > Neuer Client Secret**.
4. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
5. Klicken Sie Auf **Hinzufügen**.
6. Kopieren Sie den Wert des Clientgeheimnisses.

Ergebnis

Ihr Service-Principal ist jetzt eingerichtet und Sie sollten die Anwendungs- (Client-)ID, die Verzeichnis- (Mandanten-)ID und den Wert des Clientgeheimnisses kopiert haben. Sie müssen diese Informationen in Cloud Manager eingeben, wenn Sie ein Azure-Konto hinzufügen.

Hinzufügen von Azure-Konten zu Cloud Manager

Nachdem Sie ein Azure Konto mit den erforderlichen Berechtigungen angegeben haben, können Sie das Konto zu Cloud Manager hinzufügen. Damit können Sie Cloud Volumes ONTAP Systeme in diesem Konto starten.

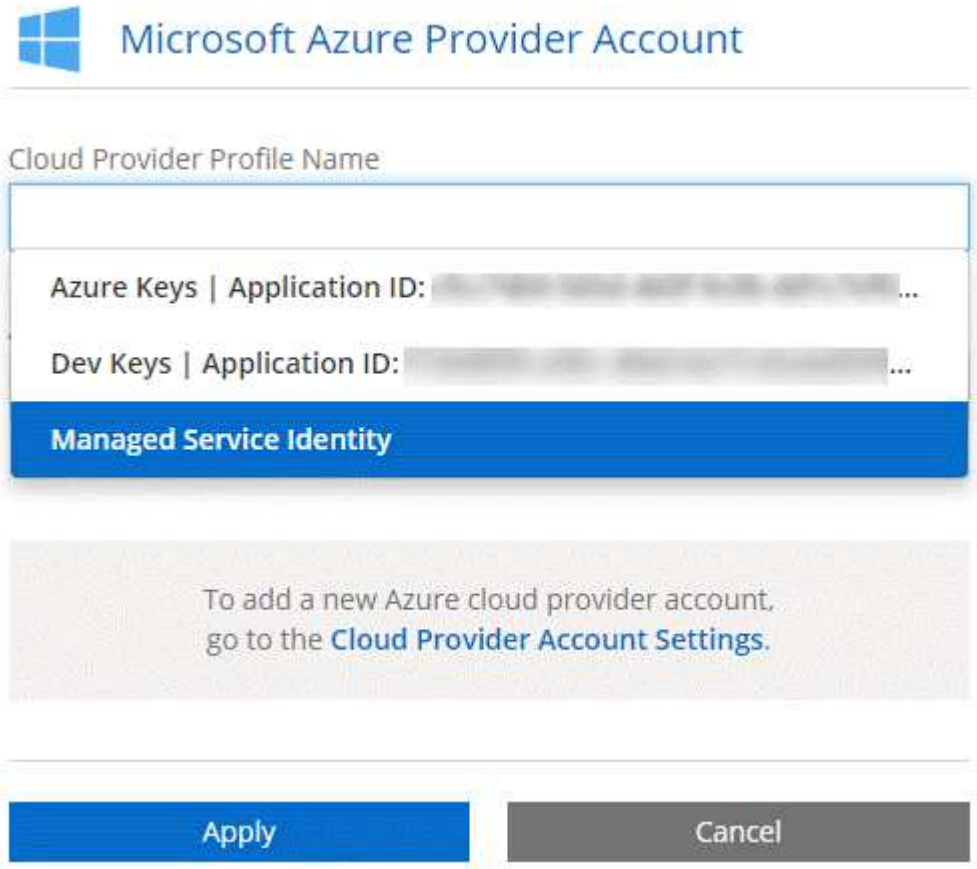
Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Cloud Provider & Support Accounts** aus.

2. Klicken Sie auf **Neues Konto hinzufügen** und wählen Sie **Microsoft Azure**.
3. Geben Sie Informationen zum Azure Active Directory Service Principal ein, der die erforderlichen Berechtigungen erteilt:
   - Anwendungs-ID: Siehe Abrufen der Anwendungs-ID und der Verzeichnis-ID.
   - Mandanten-ID (oder Verzeichnis-ID): Siehe Abrufen der Anwendungs-ID und der Verzeichnis-ID.
   - Anwendungsschlüssel (das Clientgeheimnis): Siehe Erstellen eines Clientgeheimnisses.
4. Bestätigen Sie, dass die Richtlinienanforderungen erfüllt wurden, und klicken Sie dann auf **Konto erstellen**.

Ergebnis

Sie können jetzt auf der Seite Details und Anmeldeinformationen zu einem anderen Konto wechseln, wenn Sie eine neue Arbeitsumgebung erstellen:



Verknüpfen weiterer Azure-Abonnements mit einer gemanagten Identität

Mit Cloud Manager können Sie das Azure Konto und das Abonnement auswählen, in dem Sie Cloud Volumes ONTAP implementieren möchten. Sie können kein anderes Azure-Abonnement für das verwaltete Identitätsprofil auswählen, es sei denn, Sie verknüpfen das "Verwaltete Identität" Mit diesen Abonnements.

Über diese Aufgabe

Eine verwaltete Identität ist "Zunächst das Azure-Konto" Wenn Sie Cloud Manager über NetApp Cloud Central implementieren. Bei der Implementierung von Cloud Manager erstellte Cloud Central die Rolle "OnCommand Cloud Manager Operator" und wies sie der virtuellen Cloud Manager-Maschine zu.

Schritte

1. Melden Sie sich beim Azure Portal an.
2. Öffnen Sie den Dienst **Abonnements** und wählen Sie dann das Abonnement aus, in dem Sie Cloud Volumes ONTAP-Systeme bereitstellen möchten.
3. Klicken Sie auf **Access Control (IAM)**.
   a. Klicken Sie auf **Hinzufügen** > **Rollenzuordnung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:
      - Wählen Sie die Rolle **OnCommand Cloud Manager Operator** aus.

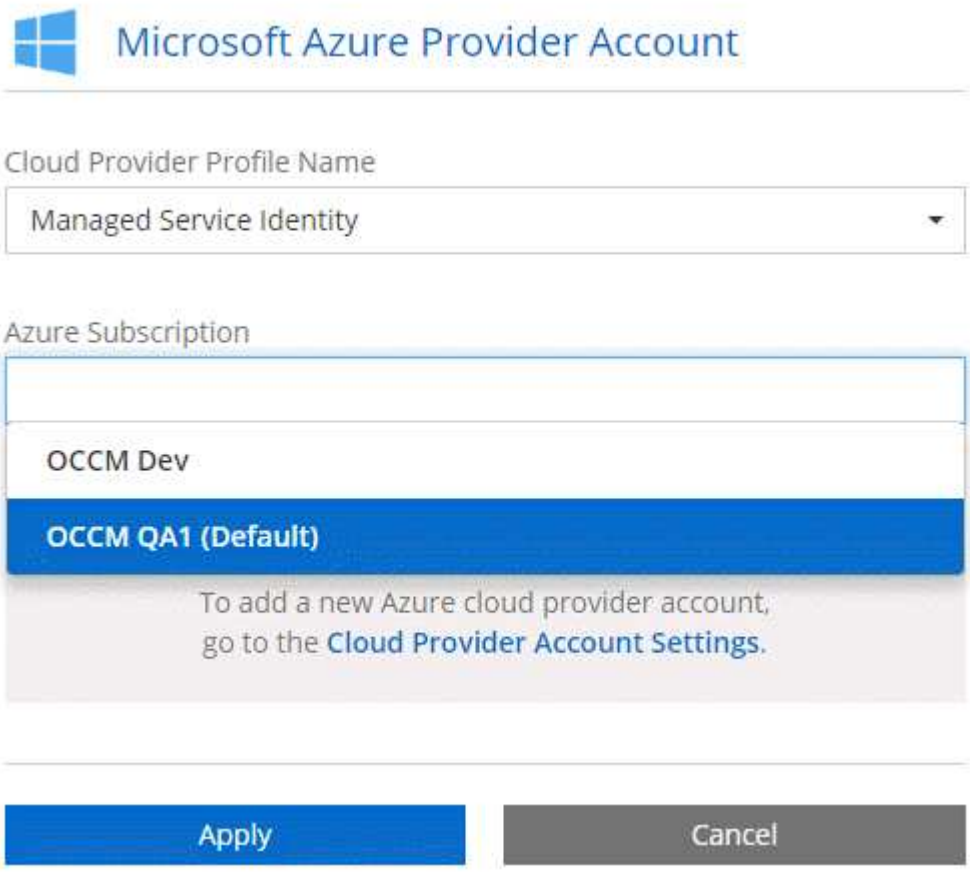
OnCommand Cloud Manager Operator ist der im angegebene Standardname "Cloud Manager-Richtlinie". Wenn Sie einen anderen Namen für die Rolle ausgewählt haben, wählen Sie stattdessen diesen Namen aus.

- Weisen Sie einer **virtuellen Maschine** Zugriff zu.
- Wählen Sie das Abonnement aus, in dem die virtuelle Cloud Manager-Maschine erstellt wurde.
- Wählen Sie die virtuelle Cloud Manager-Maschine aus.
- Klicken Sie Auf **Speichern**.

4. Wiederholen Sie diese Schritte für weitere Abonnements.

Ergebnis

Wenn Sie eine neue Arbeitsumgebung erstellen, sollten Sie nun über mehrere Azure-Abonnements für das verwaltete Identitätsprofil verfügen.



Einrichten und Hinzufügen von GCP-Konten zu Cloud Manager

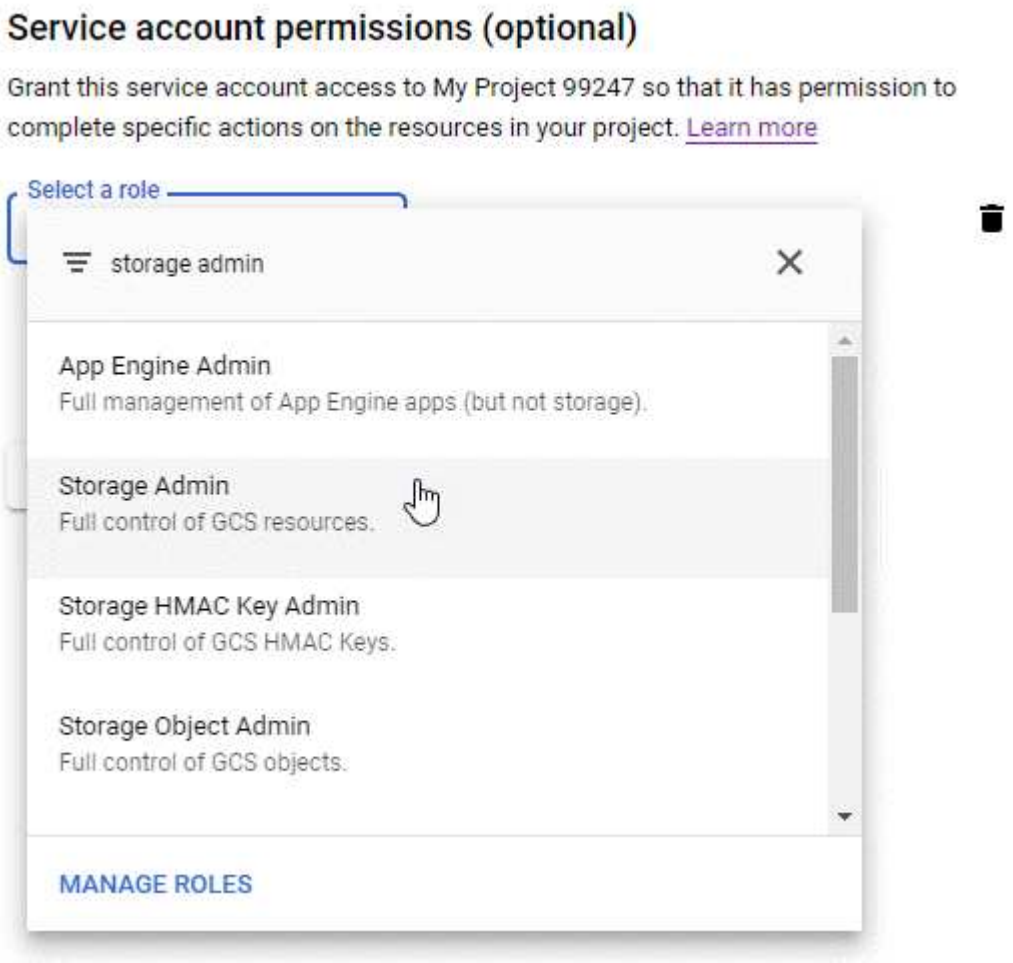
Wenn Sie aktivieren möchten "Daten-Tiering" Auf einem Cloud Volumes ONTAP System müssen Sie Cloud Manager mit einem Storage-Zugriffschlüssel für ein Servicekonto mit Storage-Admin-Berechtigungen bereitstellen. Cloud Manager verwendet die Zugriffssteuerung zum Einrichten und Managen eines Cloud Storage-Buckets für Daten-Tiering.

Einrichten eines Servicekontos und Zugriffsschlüssel für Google Cloud Storage

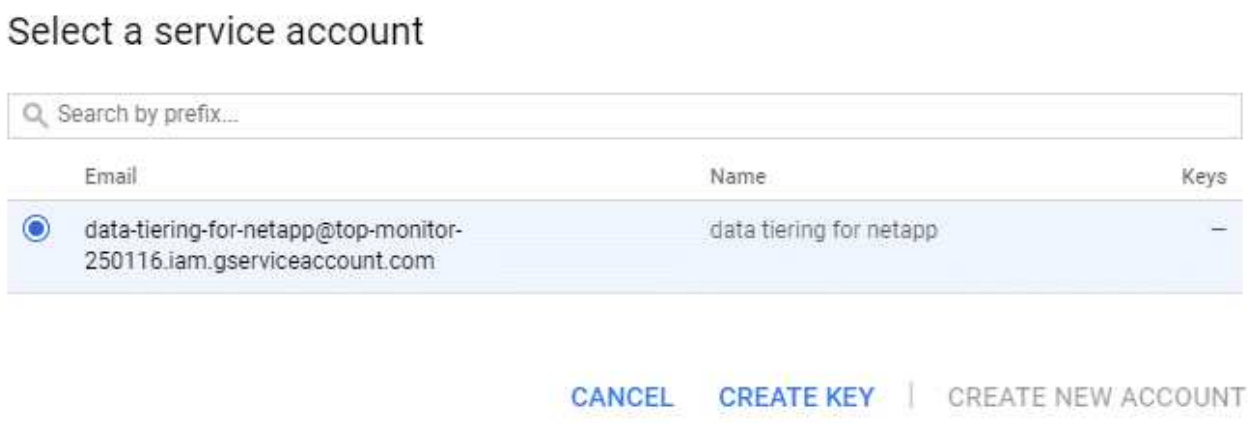
Mithilfe eines Service-Kontos kann Cloud Manager Cloud Storage-Buckets authentifizieren und auf sie zugreifen, die für Daten-Tiering verwendet werden. Die Schlüssel sind erforderlich, damit Google Cloud Storage weiß, wer die Anfrage stellt.

Schritte

1. Öffnen Sie die GCP IAM-Konsole und "Erstellen Sie ein Dienstkonto mit der Rolle Storage Admin".



2. Gehen Sie zu "GCP-Speichereinstellungen".
3. Wenn Sie aufgefordert werden, wählen Sie ein Projekt aus.
4. Klicken Sie auf die Registerkarte **Interoperabilität**.
5. Falls Sie dies noch nicht getan haben, klicken Sie auf **Interoperabilitätszugriff aktivieren**.
6. Klicken Sie unter **Zugriffsschlüssel für Servicekonten** auf **Schlüssel für ein Servicekonto erstellen**.
7. Wählen Sie das Servicekonto aus, das Sie in Schritt 1 erstellt haben.



8. Klicken Sie Auf **Schlüssel Erstellen**.
9. Kopieren Sie den Zugriffsschlüssel und den Schlüssel.

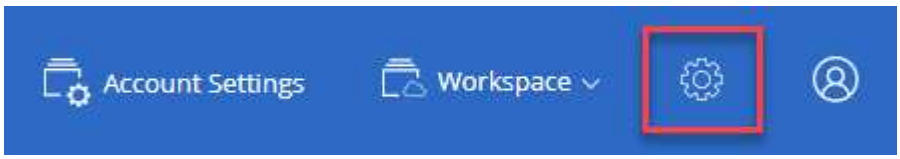
   Sie müssen diese Informationen in Cloud Manager eingeben, wenn Sie das GCP-Konto für das Daten-Tiering hinzufügen.

Hinzufügen eines GCP-Kontos zu Cloud Manager

Nachdem Sie nun über einen Zugriffsschlüssel für ein Service-Konto verfügen, können Sie ihn dem Cloud Manager hinzufügen.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Cloud Provider & Support Accounts** aus.



2. Klicken Sie auf **Neues Konto hinzufügen** und wählen Sie **GCP**.
3. Geben Sie den Zugriffsschlüssel und den Schlüssel für das Servicekonto ein.

   Mithilfe der Schlüssel kann Cloud Manager einen Cloud Storage-Bucket für das Daten-Tiering einrichten.

4. Bestätigen Sie, dass die Richtlinienanforderungen erfüllt wurden, und klicken Sie dann auf **Konto erstellen**.

Was kommt als Nächstes?

Sie können jetzt Daten-Tiering für einzelne Volumes aktivieren, wenn Sie sie erstellen, ändern oder replizieren. Weitere Informationen finden Sie unter "Tiering inaktiver Daten in kostengünstigen Objektspeicher".

Bevor Sie jedoch das tun, stellen Sie sicher, dass das Subnetz, in dem sich Cloud Volumes ONTAP befindet, für privaten Google-Zugriff konfiguriert ist. Anweisungen finden Sie unter "Google Cloud Documentation: Configuring Private Google Access".

Hinzufügen von NetApp Support Site Konten zu Cloud Manager

Um ein BYOL-System zu implementieren, muss ein NetApp Support Site Konto in Cloud Manager hinzugefügt werden. Zudem müssen Pay-as-you-go-Systeme registriert und ein Upgrade der ONTAP Software durchgeführt werden.

Sehen Sie sich das folgende Video an und erfahren Sie, wie Sie NetApp Support Site Accounts in Cloud Manager hinzufügen. Oder blättern Sie nach unten, um die Schritte zu lesen.

[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

Schritte

1. Wenn Sie noch keinen NetApp Support Site Account haben, "Eine anmeldung".
2. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Cloud Provider & Support Accounts** aus.

3. Klicken Sie auf **Neues Konto hinzufügen** und wählen Sie **NetApp Support Site** aus.
4. Geben Sie einen Namen für das Konto an, und geben Sie dann den Benutzernamen und das Kennwort ein.
   - Das Konto muss ein Kundenkonto auf Kundenebene sein (kein Gast- oder Temporkonto).
   - Wenn Sie Byol-Systeme implementieren möchten:
     - Das Konto muss für den Zugriff auf die Seriennummern der BYOL-Systeme autorisiert sein.
     - Wenn Sie ein sicheres BYOL-Abonnement erworben haben, ist ein sicheres NSS-Konto erforderlich.
5. Klicken Sie Auf **Konto Erstellen.**

Was kommt als Nächstes?

Benutzer können jetzt das Konto beim Erstellen neuer Cloud Volumes ONTAP Systeme und bei der Registrierung vorhandener Systeme auswählen.

- "Starten von Cloud Volumes ONTAP in AWS"
- "Starten von Cloud Volumes ONTAP in Azure"
- "Registrieren von Pay-as-you-go-Systemen"
- "Cloud Manager managt Lizenzdateien"

Installieren eines HTTPS-Zertifikats für sicheren Zugriff

Standardmäßig verwendet Cloud Manager ein selbstsigniertes Zertifikat für den HTTPS-Zugriff auf die Webkonsole. Sie können ein Zertifikat installieren, das von einer Zertifizierungsstelle (CA) signiert wurde. Dies bietet einen besseren Sicherheitsschutz als ein selbstsigniertes Zertifikat.

Schritte

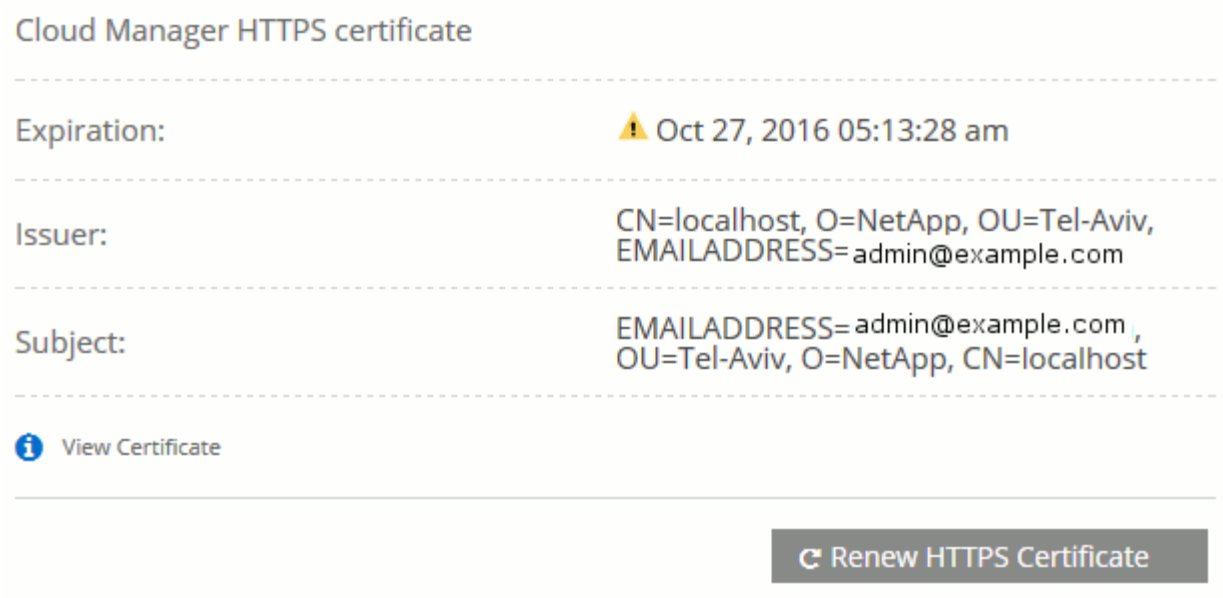
1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **HTTPS-Setup**.

2. Installieren Sie auf der Seite HTTPS Setup ein Zertifikat, indem Sie eine Zertifikatsignierungsanforderung (CSR) erstellen oder Ihr eigenes, von der Zertifizierungsstelle signiertes Zertifikat installieren:

Option	Beschreibung
Erstellen Sie eine CSR	a. Geben Sie den Hostnamen oder DNS des Cloud Manager-Hosts (dessen allgemeiner Name) ein, und klicken Sie dann auf **CSR generieren**. Cloud Manager zeigt eine Zertifikatsignierungsanforderung an. b. Verwenden Sie die CSR, um eine SSL-Zertifikatsanforderung an eine Zertifizierungsstelle zu senden. Das Zertifikat muss das mit Privacy Enhanced Mail (PEM) Base-64 codierte X.509-Format verwenden. c. Kopieren Sie den Inhalt des signierten Zertifikats, fügen Sie es in das Feld Zertifikat ein und klicken Sie dann auf **Installieren**.
Installieren Sie Ihr eigenes CA-signiertes Zertifikat	a. Wählen Sie **CA-signiertes Zertifikat installieren**. b. Laden Sie sowohl die Zertifikatdatei als auch den privaten Schlüssel und klicken Sie dann auf **Installieren**. Das Zertifikat muss das mit Privacy Enhanced Mail (PEM) Base-64 codierte X.509-Format verwenden.

Ergebnis

Cloud Manager verwendet jetzt das CA-signierte Zertifikat, um sicheren HTTPS-Zugriff zu ermöglichen. Die folgende Abbildung zeigt ein Cloud Manager-System, das für den sicheren Zugriff konfiguriert ist:



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:

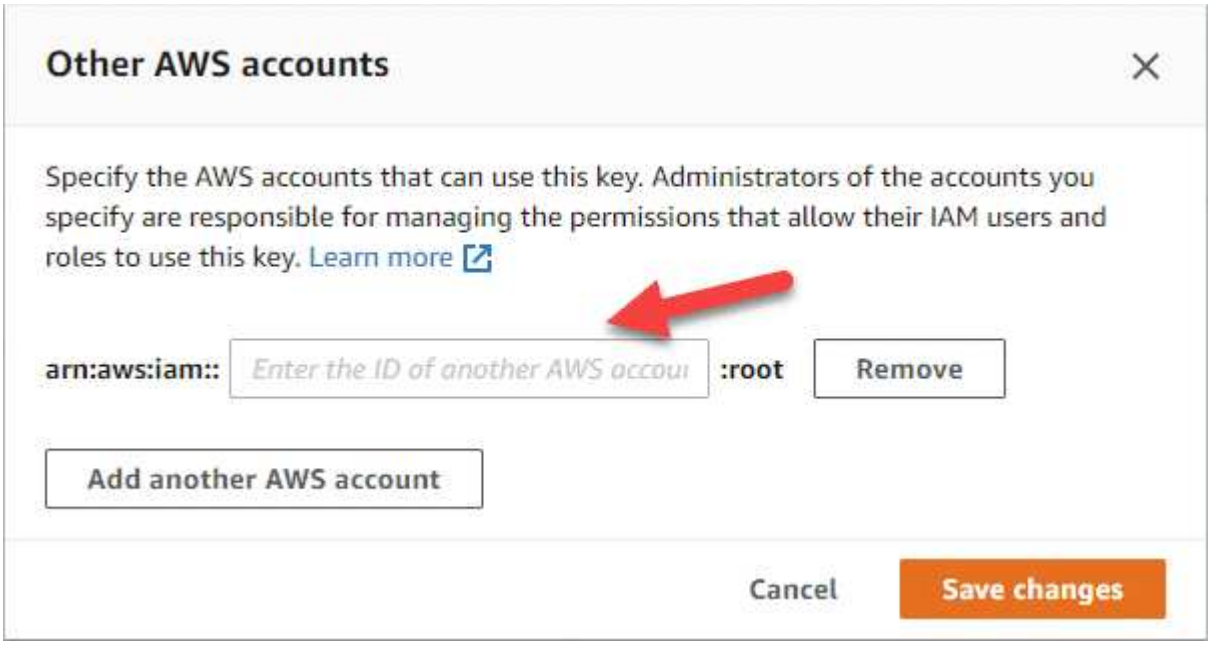
   a. Wechseln Sie von dem Konto, in dem sich der CMK befindet, zur KMS-Konsole.
   b. Wählen Sie die Taste.
   c. Kopieren Sie im Fenster **Allgemeine Konfiguration** den ARN des Schlüssels.

      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".

Netzwerkanforderungen

Netzwerkanforderungen für Cloud Manager

Richten Sie Ihr Netzwerk ein, damit Cloud Manager Cloud Volumes ONTAP Systeme in AWS, Microsoft Azure oder Google Cloud Platform implementieren kann. Der wichtigste Schritt besteht darin, ausgehenden Internetzugriff auf verschiedene Endpunkte zu gewährleisten.

Wenn Ihr Netzwerk einen Proxyserver für die gesamte Kommunikation mit dem Internet verwendet, fordert Cloud Manager Sie auf, den Proxy während der Einrichtung anzugeben. Sie können den Proxyserver auch auf der Seite Einstellungen angeben. Siehe "Konfigurieren von Cloud Manager für die Verwendung eines Proxyservers".

Verbindung zu Zielnetzwerken

Cloud Manager benötigt eine Netzwerkverbindung zu den VPCs und VNets, in denen Cloud Volumes ONTAP implementiert werden soll.

Wenn Sie beispielsweise Cloud Manager in Ihrem Unternehmensnetzwerk installieren, müssen Sie eine VPN-Verbindung zu der VPC oder vnet einrichten, in dem Cloud Volumes ONTAP gestartet wird.

Outbound-Internetzugang

Cloud Manager erfordert ausgehenden Internetzugang, um Cloud Volumes ONTAP bereitzustellen und zu managen. Outbound-Internetzugang ist auch erforderlich, wenn Sie über Ihren Webbrowser auf Cloud Manager zugreifen und das Cloud Manager-Installationsprogramm auf einem Linux-Host ausführen.

In den folgenden Abschnitten werden die spezifischen Endpunkte beschrieben.

Endpunkte für das Management von Cloud Volumes ONTAP in AWS

Cloud Manager erfordert ausgehenden Internetzugang, um bei der Implementierung und dem Management von Cloud Volumes ONTAP in AWS die folgenden Endpunkte zu kontaktieren:

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.

Endpunkte	Zweck
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://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Cloud Manager kann Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images abrufen und herunterladen.
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://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	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.

Endpunkte zum Management von Cloud Volumes ONTAP in Azure

Cloud Manager erfordert ausgehenden Internetzugang, um bei der Bereitstellung und Verwaltung von Cloud Volumes ONTAP in Microsoft Azure folgende Endpunkte zu kontaktieren:

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://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com	Cloud Manager kann Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images abrufen und herunterladen.
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	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.

Endpunkte zum Management von Cloud Volumes ONTAP in GCP

Für die Implementierung und das Management von Cloud Volumes ONTAP in GCP ist für Cloud Manager ein abgehender Internetzugang erforderlich, damit Sie die folgenden Endpunkte kontaktieren können:

Endpunkte	Zweck
https://www.googleapis.com	Ermöglicht Cloud Manager den Kontakt zu Google APIs für die Implementierung 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://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com	Cloud Manager kann Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images abrufen und herunterladen.
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	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.

Endpunkte, auf die über Ihren Webbrowser zugegriffen wird

Benutzer müssen über einen Webbrowser auf Cloud Manager zugreifen. Die Maschine, auf der der Webbrowser ausgeführt wird, muss über Verbindungen zu den folgenden Endpunkten verfügen:

Endpunkte	Zweck
Der Cloud Manager-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.

Endpunkte zum Installieren von Cloud Manager auf einem Linux-Host

Das Cloud Manager-Installationsprogramm muss während des Installationsvorgangs auf die folgenden URLs zugreifen:

- http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

Ports und Sicherheitsgruppen

- Wenn Sie Cloud Manager über Cloud Central oder über Marktplatz-Images bereitstellen, lesen Sie Folgendes:
  - "Sicherheitsgruppenregeln für Cloud Manager in AWS"
  - "Sicherheitsgruppenregeln für Cloud Manager in Azure"
  - "Firewall-Regeln für Cloud Manager in GCP"
- Wenn Sie Cloud Manager auf einem vorhandenen Linux-Host installieren, lesen Sie "Anforderungen an den Cloud Manager Host".

Netzwerkanforderungen für Cloud Volumes ONTAP in AWS

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

Allgemeine AWS Netzwerkanforderungen 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.

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".

AWS Netzwerkanforderungen für Cloud Volumes ONTAP HA in mehreren AZS

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".

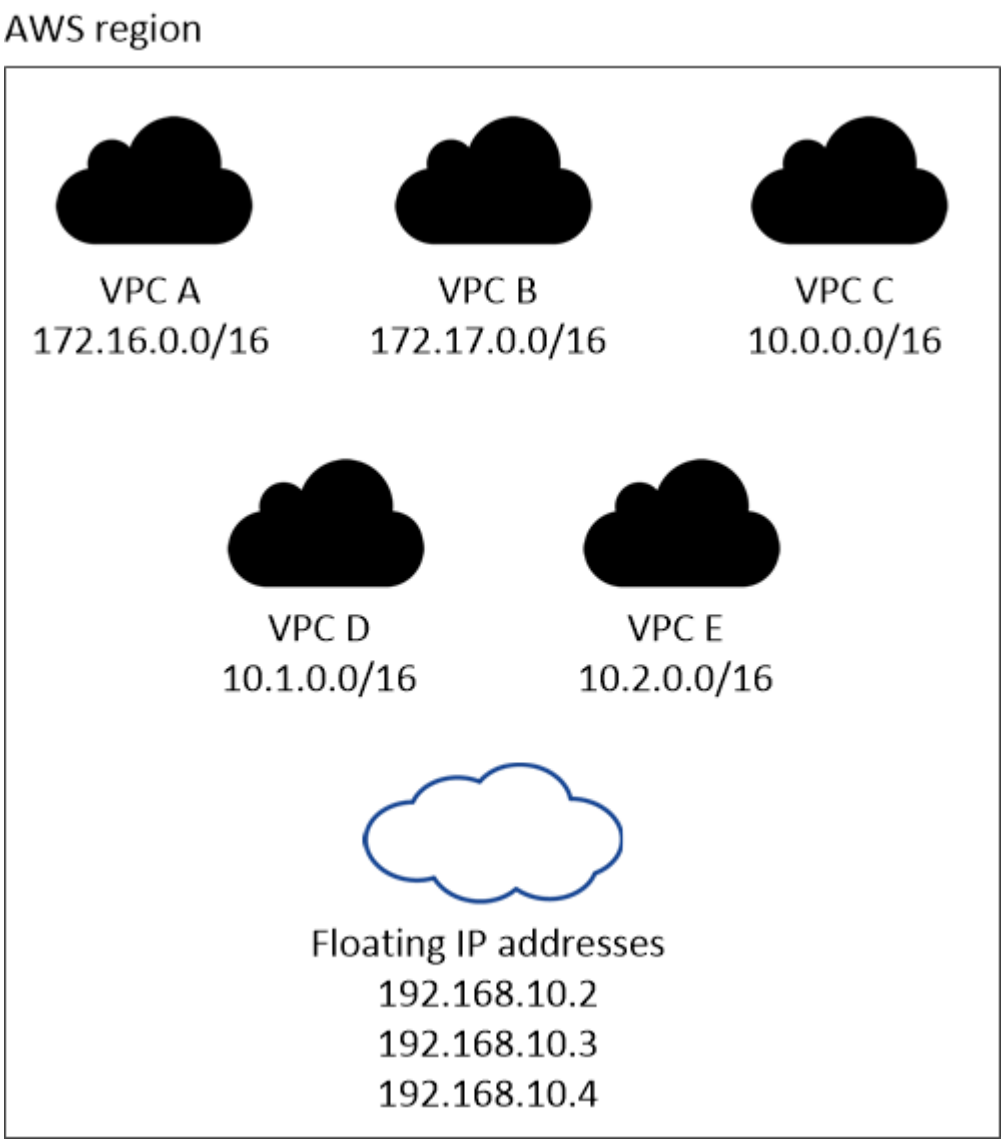
Eine Floating-IP-Adresse ist für das Cluster-Management, eine für NFS/CIFS-Daten auf Node 1 und eine für NFS/CIFS-Daten auf Node 2. Eine vierte Floating IP-Adresse für SVM-Management ist optional.

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".

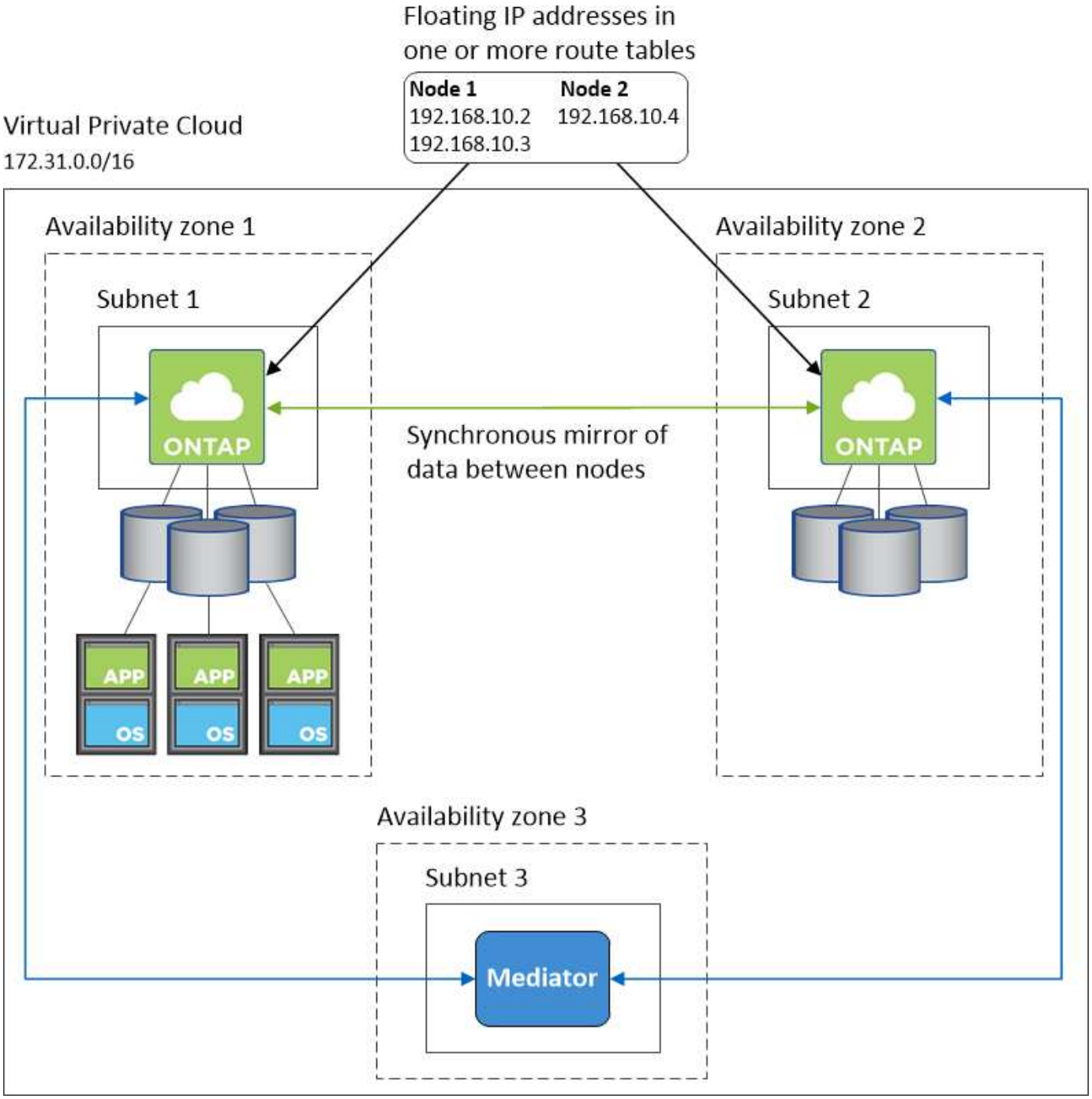
Anbindung an NetApp Management Tools

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.

Beispielkonfiguration

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



Beispiele für VPC-Konfigurationen

Um besser zu verstehen, wie Sie Cloud Manager und Cloud Volumes ONTAP in AWS implementieren können, sollten Sie sich die gängigsten VPC-Konfigurationen ansehen.

- Ein VPC mit öffentlichen und privaten Subnetzen und einem NAT-Gerät
- Ein VPC mit einem privaten Subnetz und einer VPN-Verbindung zu Ihrem Netzwerk

Ein VPC mit öffentlichen und privaten Subnetzen und einem NAT-Gerät

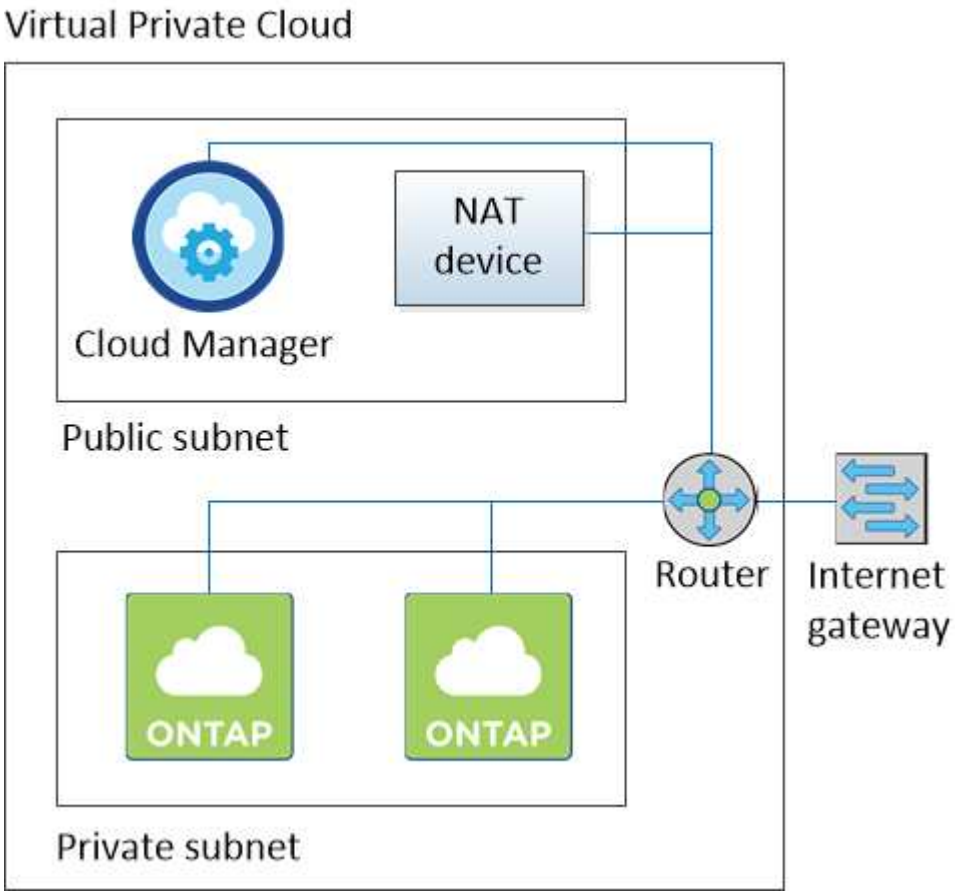
Diese VPC-Konfiguration umfasst öffentliche und private Subnetze, ein Internet-Gateway, das den VPC mit dem Internet verbindet, und ein NAT-Gateway oder eine NAT-Instanz im öffentlichen Subnetz, die

ausgehenden Internetverkehr vom privaten Subnetz aus ermöglicht. In dieser Konfiguration können Sie Cloud Manager in einem öffentlichen oder privaten Subnetz ausführen. Das öffentliche Subnetz wird jedoch empfohlen, da es den Zugriff von Hosts außerhalb des VPC ermöglicht. Sie können dann Cloud Volumes ONTAP Instanzen im privaten Subnetz starten.

Anstelle eines NAT-Geräts können Sie einen HTTP-Proxy verwenden, um Internetverbindungen bereitzustellen.

Weitere Informationen zu diesem Szenario finden Sie unter "AWS Dokumentation: Szenario 2: VPC mit öffentlichen und privaten Subnetzen (NAT)".

Die folgende Grafik zeigt Cloud Manager, der in einem öffentlichen Subnetz und in Einzelknoten-Systemen in einem privaten Subnetz ausgeführt wird:



Ein VPC mit einem privaten Subnetz und einer VPN-Verbindung zu Ihrem Netzwerk

Bei dieser VPC-Konfiguration handelt es sich um eine Hybrid Cloud-Konfiguration, bei der Cloud Volumes ONTAP zu einer Erweiterung Ihrer privaten Umgebung wird. Die Konfiguration umfasst ein privates Subnetz und ein virtuelles privates Gateway mit einer VPN-Verbindung zu Ihrem Netzwerk. Durch das Routing über den VPN-Tunnel können EC2-Instanzen über das Netzwerk und Firewalls auf das Internet zugreifen. Sie können Cloud Manager im privaten Subnetz oder in Ihrem Datacenter ausführen. Sie starten dann Cloud Volumes ONTAP im privaten Subnetz.

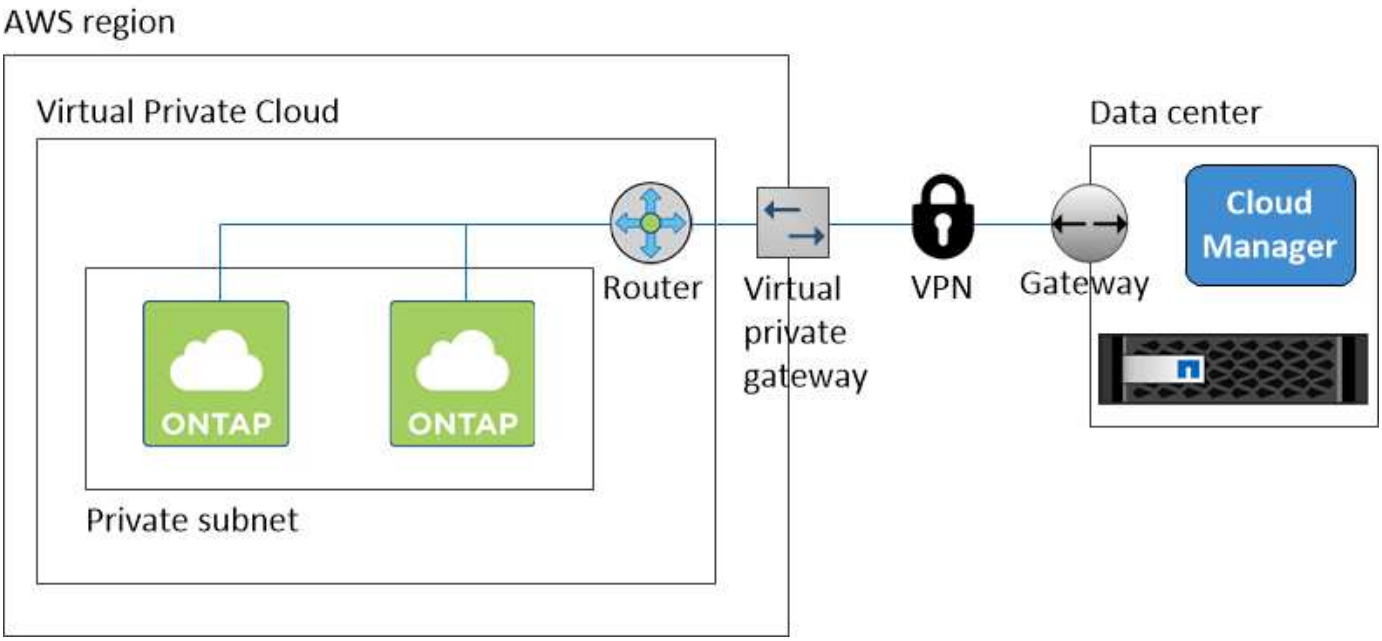
Sie können in dieser Konfiguration auch einen Proxyserver verwenden, um den Internetzugang zu ermöglichen. Der Proxy-Server kann sich in Ihrem Datacenter oder in AWS befinden.

Wenn Sie Daten zwischen FAS Systemen in Ihrem Datacenter und Cloud Volumes ONTAP Systemen in AWS

replizieren möchten, sollten Sie eine VPN-Verbindung verwenden, damit die Verbindung sicher ist.

Weitere Informationen zu diesem Szenario finden Sie unter "AWS Dokumentation: Szenario 4: VPC mit privatem Subnetz und von AWS gemanagtem VPN-Zugriff".

Die folgende Grafik zeigt Cloud Manager, der in Ihrem Datacenter und in Einzelknotensystemen in einem privaten Subnetz ausgeführt wird:



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

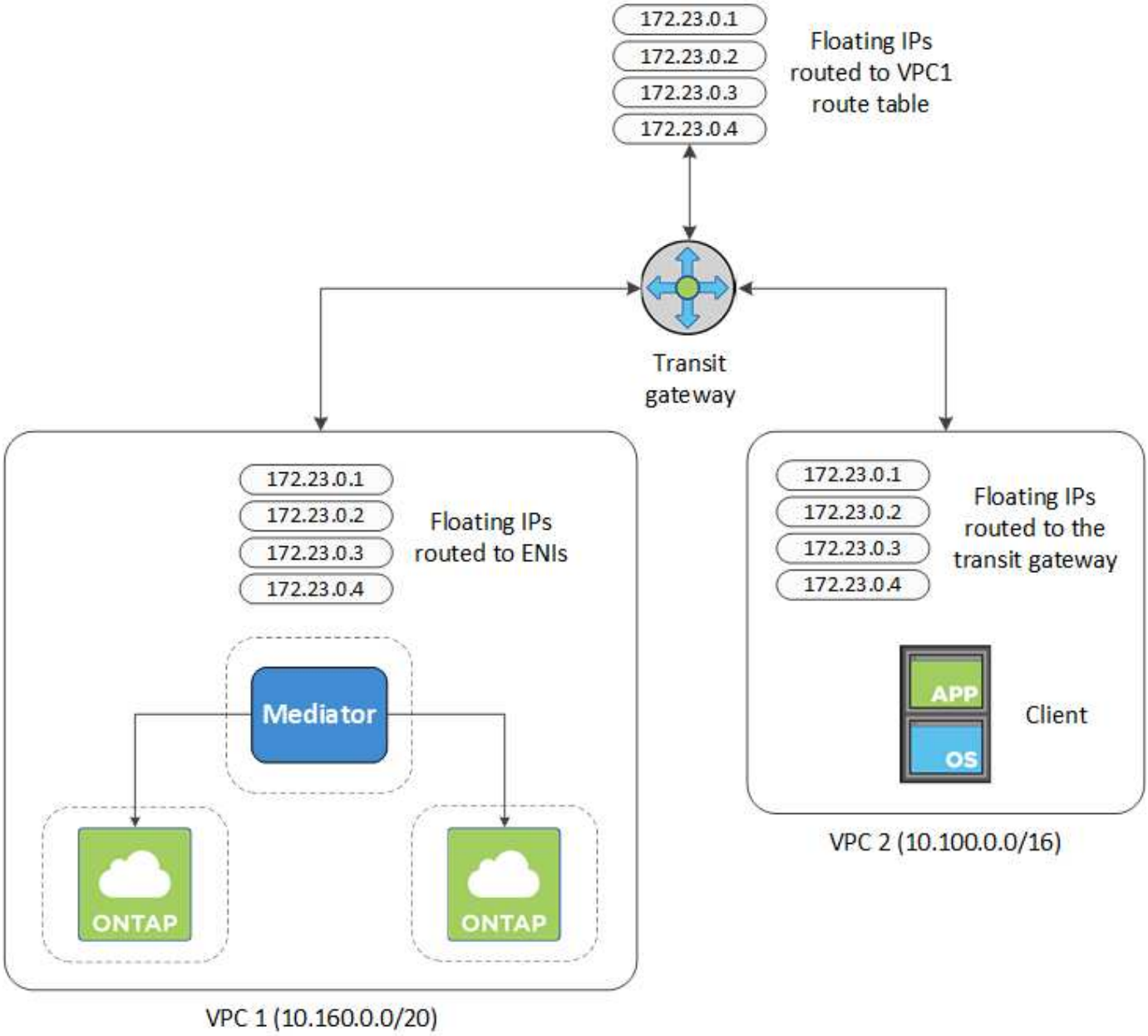
Einrichten eines AWS-Transit-Gateways für den Zugriff auf die unverankerten IP-Adressen eines HA-Paars von außerhalb der VPC aus, wo sich das HA-Paar befindet.

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.

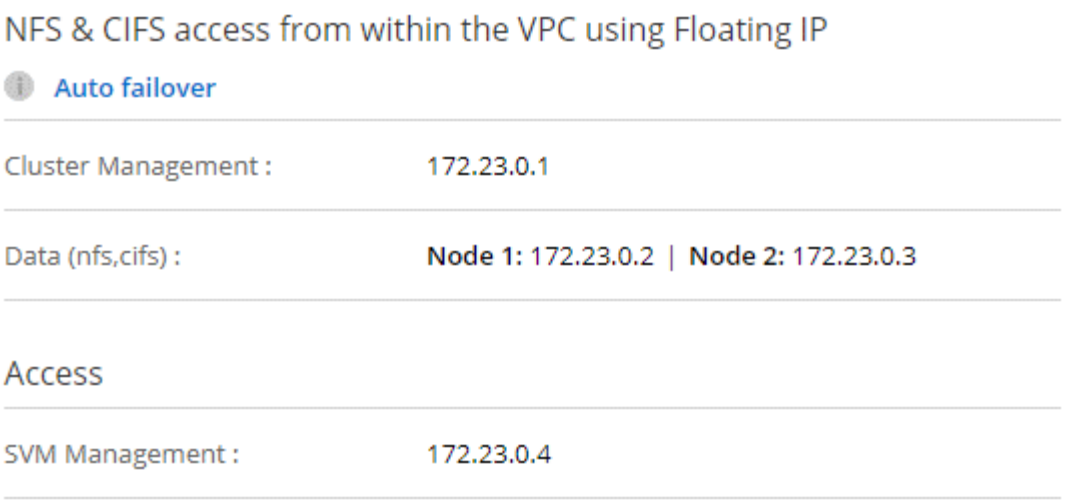


Die folgenden Schritte veranschaulichen die Einrichtung einer ähnlichen Konfiguration.

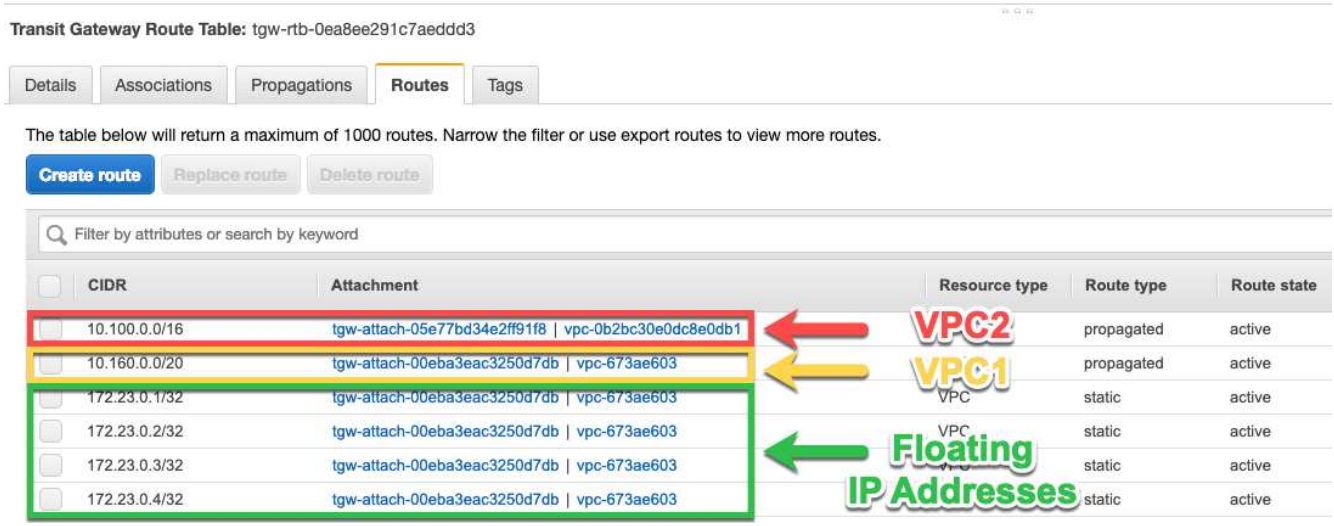
Schritte

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:

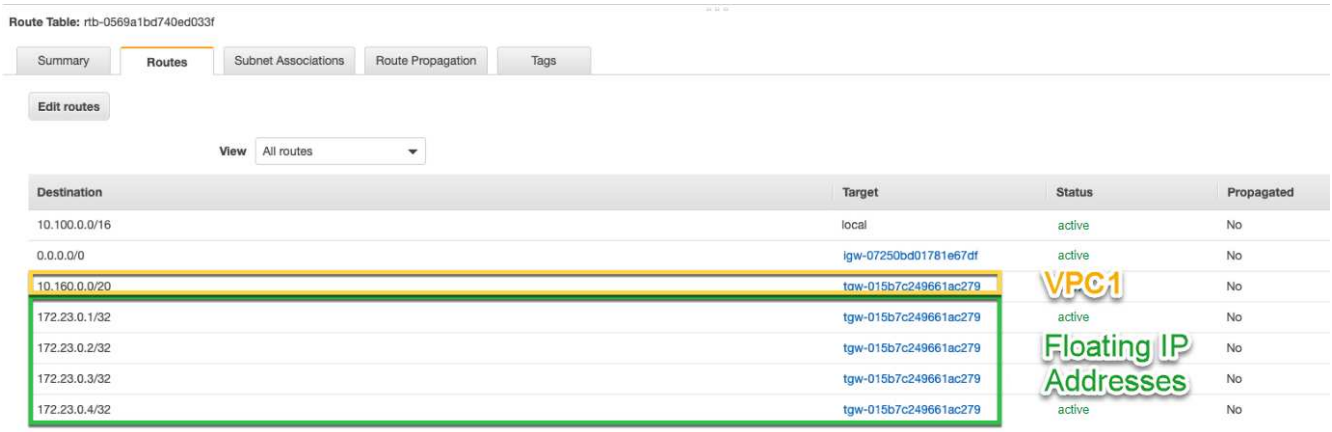


Das folgende Beispielbild zeigt die Routingtabelle für das Transit Gateway. Er umfasst Routen zu den CIDR-Blöcken der zwei VPCs und vier von Cloud Volumes ONTAP verwendete Floating IP-Adressen.



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.

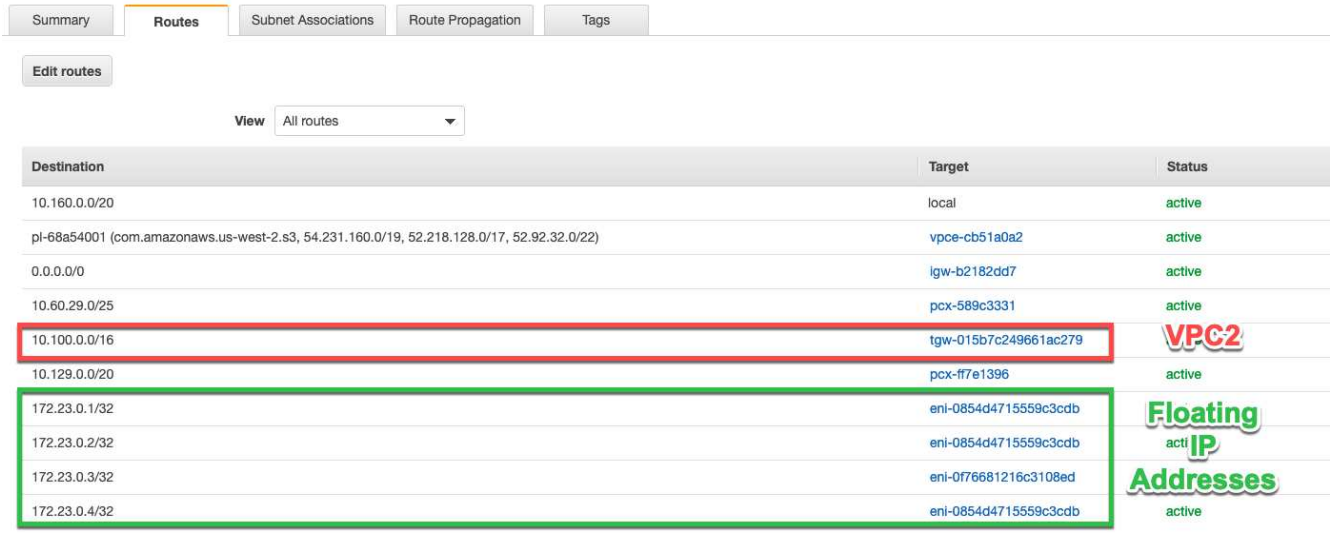
      Das folgende Beispielbild zeigt die Routingtabelle für VPC 2, die auch Routen zu VPC 1 und die fließenden IP-Adressen umfasst.



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.

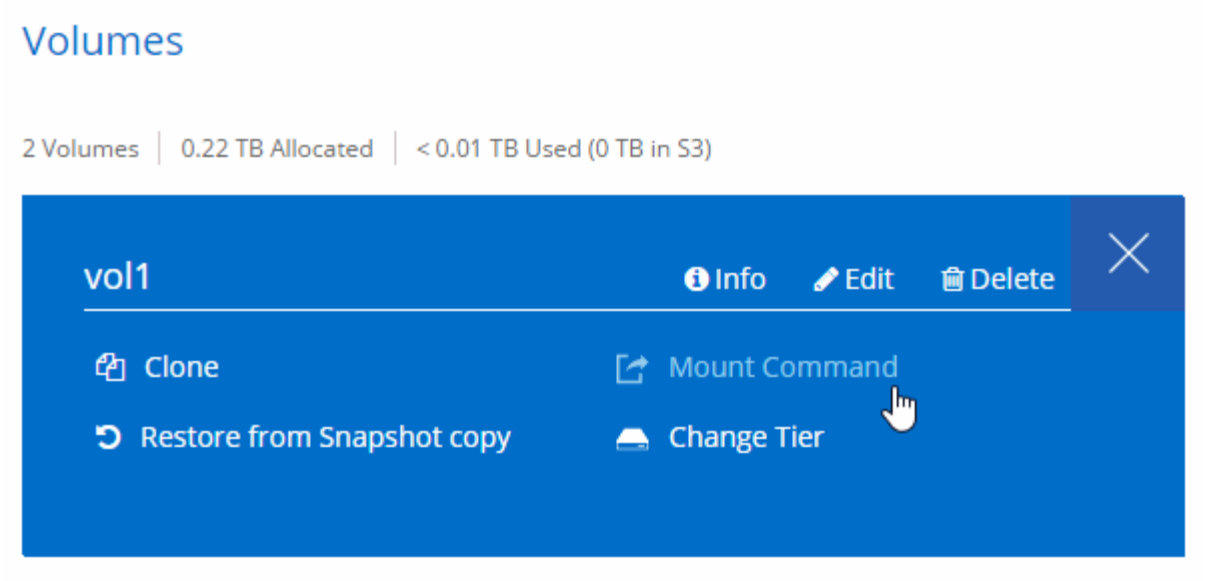
   Dieser Schritt ist wichtig, da er die Weiterleitung zwischen den VPCs abgeschlossen hat.

   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"

Netzwerkanforderungen für Cloud Volumes ONTAP in Azure

Richten Sie Ihr Azure Netzwerk ein, um Cloud Volumes ONTAP Systeme ordnungsgemäß funktionieren zu können.

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

Sicherheitsgruppen

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

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".

Netzwerkanforderungen für Cloud Volumes ONTAP in GCP

Richten Sie das Netzwerk Ihrer Google Cloud-Plattform ein, damit Cloud Volumes ONTAP-Systeme ordnungsgemäß funktionieren können.

Gemeinsame VPC

Cloud Manager und Cloud Volumes ONTAP werden in einer gemeinsamen Google Cloud Platform VPC 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 Cloud Manager und Cloud Volumes ONTAP Virtual Machines in einem *Service-Projekt* implementieren. "Google Cloud-Dokumentation: Gemeinsame VPC-Übersicht".

Die einzige Anforderung besteht in der Bereitstellung der folgenden Berechtigungen für das Cloud Manager-Servicekonto im Shared VPC-Hostprojekt:

compute.Firewalls.* compute.networks.* Compute.subnetzes.*

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

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 Ihr eigenes verwenden müssen, lesen Sie "Regeln für die GCP-Firewall".

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".

Zusätzliche Bereitstellungsoptionen

Anforderungen an den Cloud Manager Host

Wenn Sie Cloud Manager auf Ihrem eigenen Host installieren, müssen Sie die Unterstützung für Ihre Konfiguration überprüfen, die Betriebssystemanforderungen, Portanforderungen usw. umfasst.

Cloud Manager kann auf Ihrem eigenen Host in GCP installiert werden, nicht jedoch in Ihrem lokalen Netzwerk. Cloud Manager muss in GCP installiert sein, um Cloud Volumes ONTAP in GCP implementieren zu können.

Ein dedizierter Host ist erforderlich

Cloud Manager wird auf einem Host, der für andere Applikationen freigegeben ist, nicht unterstützt. Der Host muss ein dedizierter Host sein.

Unterstützte AWS EC2-Instanztypen

- t2.Mittel
- t3.Medium (empfohlen)
- m4.Large
- m5.xlarge
- M5.2xlarge
- M5.4xlarge
- M5.8xlarge

Unterstützte Azure VM-Größen

A2, D2 v2 oder D2 v3 (je nach Verfügbarkeit)

Unterstützte GCP-Maschinentypen

Einen Maschinentyp mit mindestens 2 vCPUs und 4 GB Speicher.

Unterstützte Betriebssysteme

- CentOS 7.2
- CentOS 7.3
- CentOS 7.4
- CentOS 7.5
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 7.5

  Das Red Hat Enterprise Linux System muss beim Red Hat Subscription Management registriert sein. Wenn sie nicht registriert ist, kann das System während der Cloud Manager-Installation nicht auf Repositorys zugreifen, um die erforderliche Software von Drittanbietern zu aktualisieren.

  Cloud Manager wird auf englischsprachigen Versionen dieser Betriebssysteme unterstützt.

Hypervisor

Ein Bare Metal- oder gehosteter Hypervisor, der für die Ausführung von CentOS oder Red hat Enterprise Linux zertifiziert isthttps://access.redhat.com/certified-hypervisors["Red hat Solution: Welche Hypervisoren sind für die Ausführung von Red hat Enterprise Linux zertifiziert?"^]

CPU

2,27 GHz oder höher mit zwei Cores

RAM

4 GB

Freier Speicherplatz

50 GB

Outbound-Internetzugang

Bei der Installation von Cloud Manager und bei der Implementierung von Cloud Volumes ONTAP ist ein Outbound-Internetzugang erforderlich. Eine Liste der Endpunkte finden Sie unter "Netzwerkanforderungen für Cloud Manager".

Ports

Folgende Ports müssen verfügbar sein:

- 80 für HTTP-Zugriff
- 443 für HTTPS-Zugriff
- 3306 für die Cloud Manager-Datenbank
- 8080 für den Cloud Manager-API-Proxy

Wenn andere Services diese Ports verwenden, schlägt die Installation von Cloud Manager fehl.

Es besteht ein potenzieller Konflikt mit Port 3306. Wenn eine andere Instanz von MySQL auf dem Host ausgeführt wird, verwendet es standardmäßig Port 3306. Sie müssen den Port ändern, den die vorhandene MySQL-Instanz verwendet.

Sie können die standardmäßigen HTTP- und HTTPS-Ports ändern, wenn Sie Cloud Manager installieren. Sie können den Standardport für die MySQL-Datenbank nicht ändern. Wenn Sie die HTTP- und HTTPS-Ports ändern, müssen Sie sicherstellen, dass Benutzer von einem Remote-Host aus auf die Cloud Manager-Webkonsole zugreifen können:

- Ändern Sie die Sicherheitsgruppe, um eingehende Verbindungen über die Ports zuzulassen.
- Geben Sie den Port an, wenn Sie die URL für die Cloud Manager-Webkonsole eingeben.

Installieren von Cloud Manager auf einem vorhandenen Linux-Host

Die geläufigste Methode für die Implementierung von Cloud Manager besteht aus Cloud Central oder aus dem Markt eines Cloud-Providers. Sie haben jedoch die Möglichkeit, die Cloud Manager-Software auf einem vorhandenen Linux-Host in Ihrem Netzwerk oder in der Cloud herunterzuladen und zu installieren.

Cloud Manager kann auf Ihrem eigenen Host in GCP installiert werden, nicht jedoch in Ihrem lokalen Netzwerk. Cloud Manager muss in GCP installiert sein, um Cloud Volumes ONTAP in GCP implementieren zu können.

Bevor Sie beginnen

- Ein Red Hat Enterprise Linux-System muss bei Red Hat Subscription Management registriert sein. Wenn sie nicht registriert ist, kann das System während der Cloud Manager-Installation nicht auf Repositorys zugreifen, um die erforderliche Software von Drittanbietern zu aktualisieren.
- Das Cloud Manager-Installationsprogramm greift während des Installationsvorgangs auf mehrere URLs zu. Sie müssen sicherstellen, dass ausgehende Internetzugriffe auf diese Endpunkte zulässig sind. Siehe "Netzwerkanforderungen für Cloud Manager".

Über diese Aufgabe

- Für die Installation von Cloud Manager sind keine Root-Berechtigungen erforderlich.
- Cloud Manager installiert die AWS-Befehlszeilentools (awscli), um Recovery-Verfahren vom NetApp

Support zu ermöglichen.

Wenn Sie eine Meldung erhalten, dass die Installation des awscli fehlgeschlagen ist, können Sie die Meldung ignorieren. Cloud Manager kann ohne die Tools erfolgreich arbeiten.

- Das Installationsprogramm, das auf der NetApp Support-Website verfügbar ist, kann möglicherweise eine frühere Version sein. Nach der Installation aktualisiert sich Cloud Manager automatisch, wenn eine neue Version verfügbar ist.

Schritte

1. Netzwerkanforderungen prüfen:
   - "Netzwerkanforderungen für Cloud Manager"
   - "Netzwerkanforderungen für Cloud Volumes ONTAP in AWS"
   - "Netzwerkanforderungen für Cloud Volumes ONTAP in Azure"
   - "Netzwerkanforderungen für Cloud Volumes ONTAP in GCP"
2. Prüfen "Anforderungen an den Cloud Manager Host".
3. Laden Sie die Software von herunter "NetApp Support Website", Und dann kopieren Sie es auf den Linux-Host.

   Informationen zum Verbinden und Kopieren der Datei auf eine EC2-Instanz in AWS finden Sie unter "AWS Documentation: Herstellen einer Verbindung zu Ihrer Linux-Instanz mithilfe von SSH".

4. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

   Beispiel

   ```
    chmod +x OnCommandCloudManager-V3.7.0.sh
   . Führen Sie das Installationsskript aus:
   ```

   ```
   ./OnCommandCloudManager-V3.7.0.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   Silent führt die Installation aus, ohne dass Sie zur Information aufgefordert werden.

   Proxy ist erforderlich, wenn sich der Cloud Manager-Host hinter einem Proxy-Server befindet.

   proxyport ist der Port für den Proxy-Server.

   Proxyuser ist der Benutzername für den Proxy-Server, wenn eine grundlegende Authentifizierung erforderlich ist.

   Proxypwd ist das Passwort für den von Ihnen angegebenen Benutzernamen.

5. Wenn Sie den Silent-Parameter nicht angegeben haben, geben Sie **Y** ein, um das Skript fortzusetzen, und geben Sie anschließend die HTTP- und HTTPS-Ports ein, wenn Sie dazu aufgefordert werden.

   Wenn Sie die HTTP- und HTTPS-Ports ändern, müssen Sie sicherstellen, dass Benutzer von einem Remote-Host aus auf die Cloud Manager-Webkonsole zugreifen können:

- Ändern Sie die Sicherheitsgruppe, um eingehende Verbindungen über die Ports zuzulassen.
- Geben Sie den Port an, wenn Sie die URL für die Cloud Manager-Webkonsole eingeben.

  Cloud Manager ist jetzt installiert. Nach Abschluss der Installation wird der Cloud Manager-Dienst (occm) zweimal neu gestartet, wenn Sie einen Proxyserver angegeben haben.

6. Öffnen Sie einen Webbrowser, und geben Sie die folgende URL ein:

   https://ipaddress:port

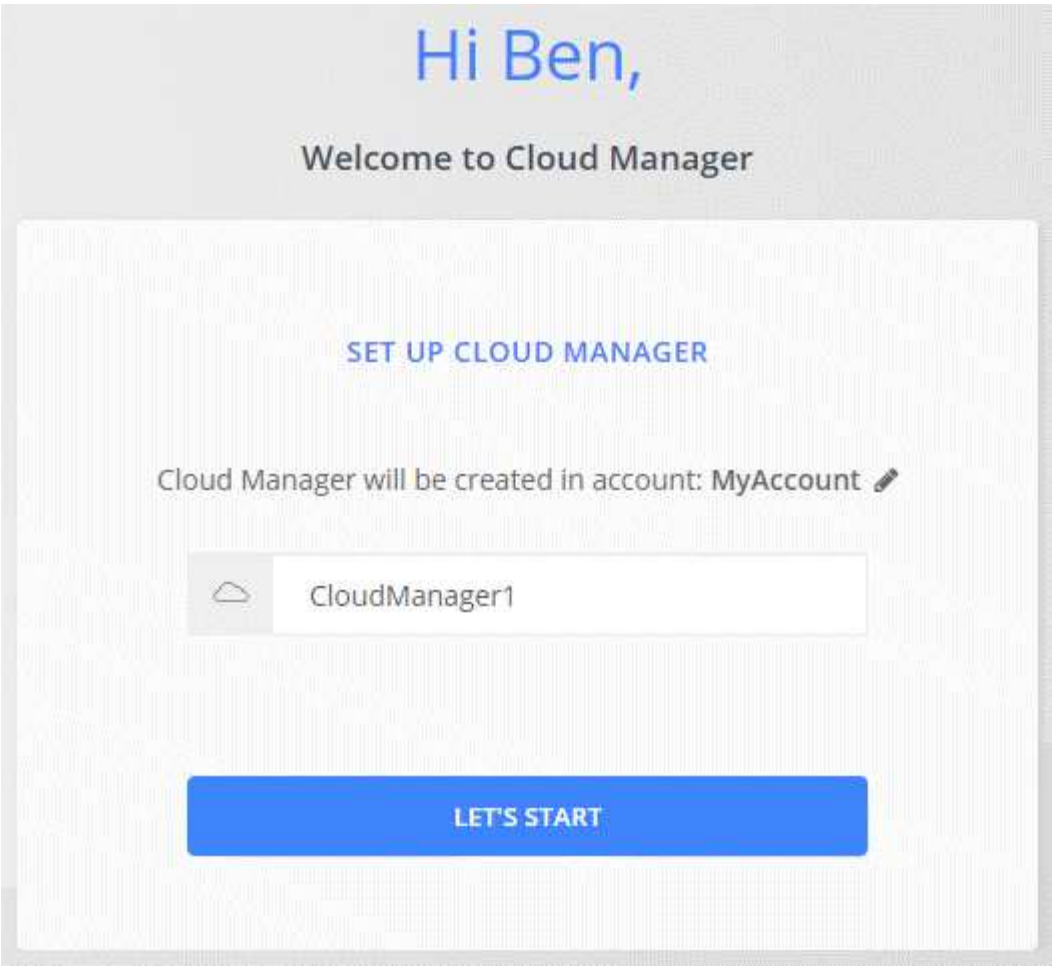
   Ipaddress kann abhängig von der Konfiguration des Cloud Manager-Hosts localhost, eine private IP-Adresse oder eine öffentliche IP-Adresse sein. Wenn sich Cloud Manager beispielsweise in der Public Cloud ohne öffentliche IP-Adresse befindet, müssen Sie eine private IP-Adresse von einem Host eingeben, der eine Verbindung zum Cloud Manager-Host hat.

   Port ist erforderlich, wenn Sie die Standard-HTTP (80)- oder HTTPS (443)-Ports geändert haben. Wenn beispielsweise der HTTPS-Port in 8443 geändert wurde, würden Sie eingeben https://ipaddress:8443

7. Melden Sie sich bei NetApp Cloud Central an oder melden Sie sich an.
8. Richten Sie Cloud Manager nach dem Einloggen ein:
   a. Geben Sie das Cloud Central-Konto an, das mit diesem Cloud Manager-System verknüpft werden soll.

      "Weitere Informationen zu Cloud Central Accounts".

   b. Geben Sie einen Namen für das System ein.



Nachdem Sie fertig sind

Einrichten von Berechtigungen, damit Cloud Manager Cloud Volumes ONTAP bei Ihrem Cloud-Provider implementieren kann:

- AWS, "AWS Konto einrichten und dann zu Cloud Manager hinzufügen".
- Azure: "Richten Sie ein Azure-Konto ein, und fügen Sie es anschließend zu Cloud Manager hinzu".
- GCP: Richten Sie ein Service-Konto ein, das über die Berechtigungen verfügt, die Cloud Manager für die Erstellung und das Management von Cloud Volumes ONTAP-Systemen in Projekten benötigt.
  a. "Rolle in GCP anlegen" Dazu gehören die im definierten Berechtigungen "Cloud Manager-Richtlinie für GCP".
  b. "Erstellen Sie ein GCP-Service-Konto und wenden Sie die benutzerdefinierte Rolle an, die Sie gerade erstellt haben".
  c. "Verknüpfen Sie dieses Servicekonto mit der Cloud Manager-VM".
  d. Wenn Sie Cloud Volumes ONTAP in anderen Projekten implementieren möchten, "Sie gewähren Zugriff, indem Sie dem Projekt das Service-Konto mit der Rolle Cloud Manager hinzufügen". Sie müssen diesen Schritt für jedes Projekt wiederholen.

Starten von Cloud Manager über den AWS Marketplace

Am besten sollte Cloud Manager in AWS gestartet werden, das verwendet wird "NetApp Cloud Central", Sie können diese jedoch bei Bedarf über den AWS Marketplace starten.

Wenn Sie Cloud Manager über den AWS Marketplace starten, ist Cloud Manager weiterhin in NetApp Cloud Central integriert. "Erfahren Sie mehr über die Integration".

Über diese Aufgabe

In den folgenden Schritten wird beschrieben, wie die Instanz von der EC2-Konsole aus gestartet wird, da Sie über die Konsole eine IAM-Rolle an die Cloud Manager-Instanz anhängen können. Dies ist mit der Aktion * von Website starten* nicht möglich.

Schritte

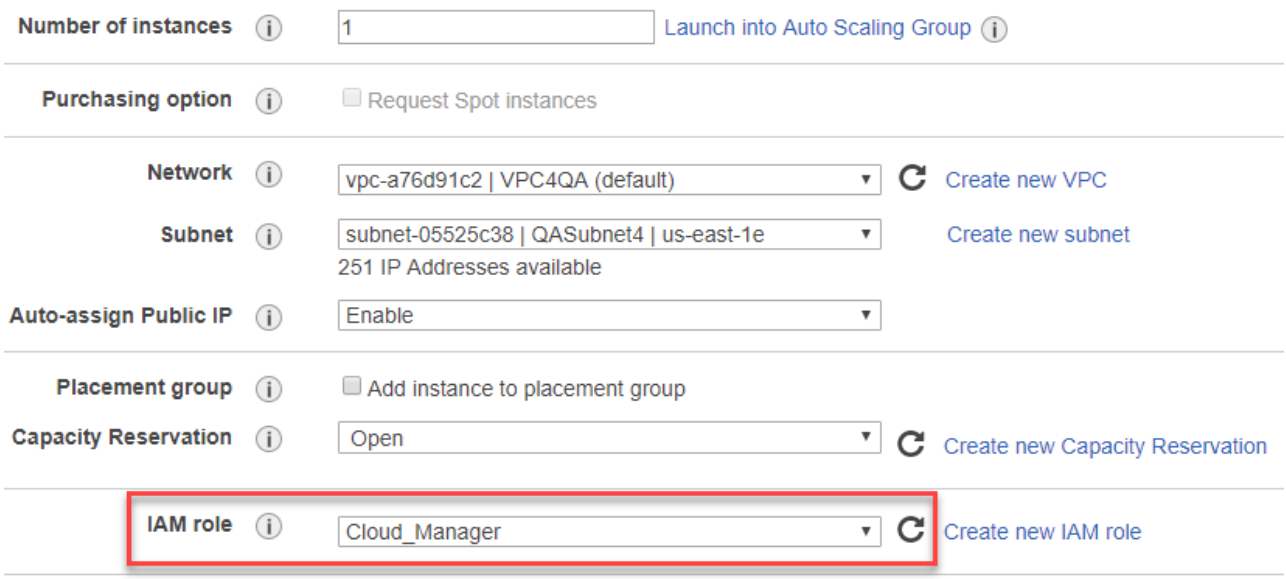
1. IAM-Richtlinie und -Rolle für die EC2-Instanz erstellen:
   a. Laden Sie die Cloud Manager IAM-Richtlinie von folgendem Speicherort herunter:

      "NetApp Cloud Manager: AWS, Azure und GCP-Richtlinien"

   b. Erstellen Sie über die IAM-Konsole Ihre eigene Richtlinie, indem Sie den Text aus der Cloud Manager IAM-Richtlinie kopieren und einfügen.
   c. Erstellen Sie eine IAM-Rolle mit dem Rollentyp Amazon EC2, und hängen Sie die im vorherigen Schritt erstellte Richtlinie an die Rolle an.
2. "Abonnieren Sie ihn im AWS Marketplace" Um sicherzustellen, dass es nach der kostenlosen Testversion von Cloud Volumes ONTAP keine Serviceunterbrechung gibt. 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.
3. Gehen Sie jetzt zum "Seite zu Cloud Manager im AWS Marketplace" Um Cloud Manager über eine AMI bereitzustellen.
4. Klicken Sie auf der Marketplace-Seite auf **Weiter zur Anmeldung** und dann auf **Weiter zur Konfiguration**.
5. Ändern Sie eine der Standardoptionen, und klicken Sie auf **Weiter zum Starten**.
6. Wählen Sie unter **Aktion auswählen über EC2 starten** und klicken Sie dann auf **Start**.
7. Befolgen Sie die Anweisungen zur Konfiguration und Bereitstellung der Instanz:
   - **Instanztyp wählen**: Wählen Sie je nach Verfügbarkeit der Region einen der unterstützten Instanztypen (t3.Medium wird empfohlen).

     "Überprüfen Sie die Liste der unterstützten Instanztypen".

   - **Instanz konfigurieren**: Wählen Sie eine VPC und ein Subnetz, die IAM-Rolle, die Sie in Schritt 1 erstellt haben, und andere Konfigurationsoptionen aus, die Ihren Anforderungen entsprechen.



- **Speicher hinzufügen**: Behalten Sie die Standard-Speicheroptionen.
- **Tags hinzufügen**: Geben Sie bei Bedarf Tags für die Instanz ein.
- **Sicherheitsgruppe konfigurieren**: Geben Sie die erforderlichen Verbindungsmethoden für die Cloud Manager-Instanz an: SSH, HTTP und HTTPS.
- **Review**: Überprüfen Sie Ihre Auswahl und klicken Sie auf **Start**.

  AWS startet die Software mit den angegebenen Einstellungen. Die Cloud Manager-Instanz und -Software sollten in etwa fünf Minuten ausgeführt werden.

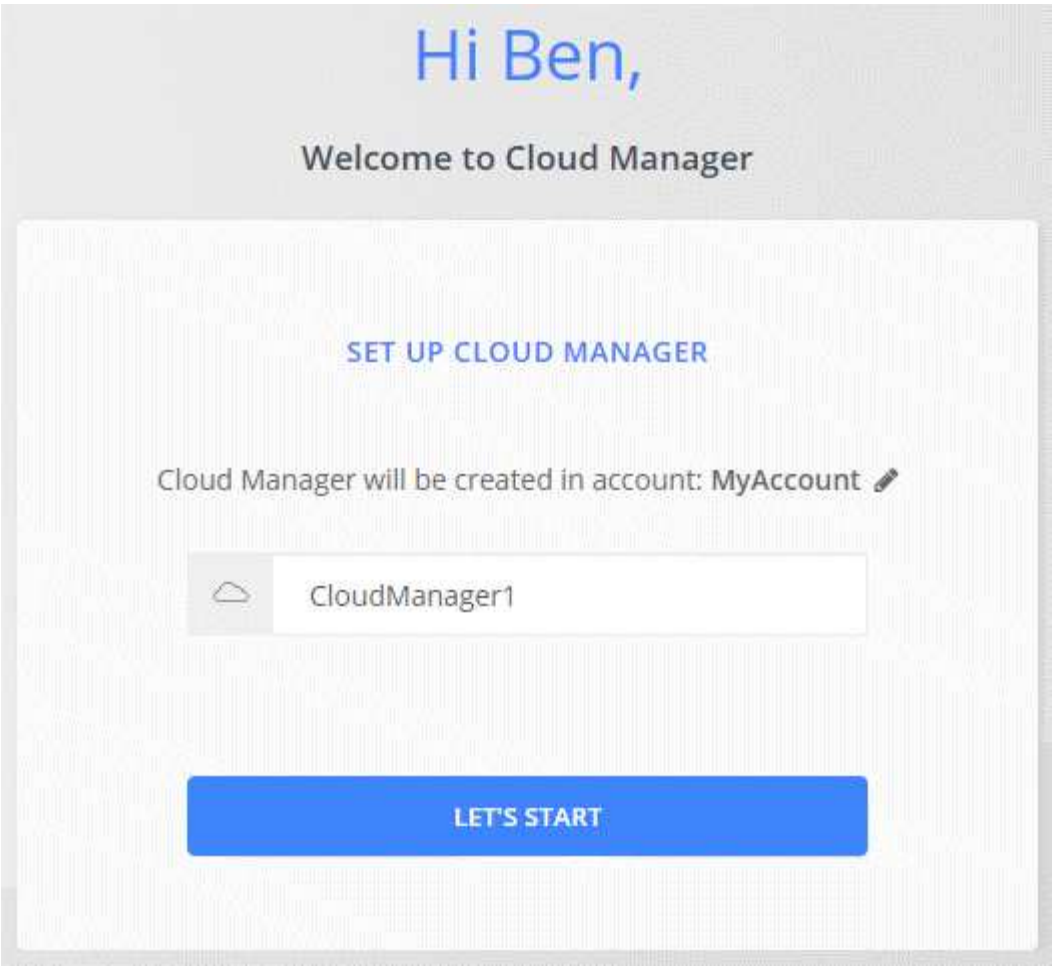
8. Öffnen Sie einen Webbrowser von einem Host aus, der eine Verbindung zur virtuellen Cloud Manager-Maschine hat, und geben Sie die folgende URL ein:

   http://ipaddress:80

9. Richten Sie Cloud Manager nach dem Einloggen ein:
   a. Geben Sie das Cloud Central-Konto an, das mit diesem Cloud Manager-System verknüpft werden soll.

      "Weitere Informationen zu Cloud Central Accounts".

   b. Geben Sie einen Namen für das System ein.



Ergebnis

Cloud Manager ist jetzt installiert und eingerichtet.

Bereitstellung von Cloud Manager über Azure Marketplace

Am besten implementieren Sie Cloud Manager in Azure "NetApp Cloud Central", Die Implementierung kann jedoch bei Bedarf im Azure Marketplace erfolgen.

Für die Implementierung von Cloud Manager in stehen separate Anweisungen zur Verfügung "Azure Regionen der US-Regierung" Und ein "Azure Deutschland Regionen".

Wenn Sie Cloud Manager über den Azure Marketplace implementieren, ist Cloud Manager weiterhin in NetApp Cloud Central integriert. "Erfahren Sie mehr über die Integration".

Bereitstellung von Cloud Manager in Azure

Sie müssen Cloud Manager installieren und einrichten, damit Sie Cloud Volumes ONTAP in Azure starten können.

Schritte

1. "Wechseln Sie zur Azure Marketplace-Seite für Cloud Manager".
2. Klicken Sie auf **Jetzt holen** und klicken Sie dann auf **Weiter**.

3. Klicken Sie im Azure-Portal auf **Erstellen** und befolgen Sie die Schritte zur Konfiguration der virtuellen Maschine.

   Beachten Sie beim Konfigurieren der VM Folgendes:

   - Cloud Manager kann mit HDD- oder SSD-Festplatten optimal arbeiten.
   - Wählen Sie eine der empfohlenen virtuellen Maschinengrößen: A2, D2 v2 oder D2 v3 (je nach Verfügbarkeit).
   - Für die Netzwerksicherheitsgruppe erfordert Cloud Manager eingehende Verbindungen unter Verwendung von SSH, HTTP und HTTPS.

     "Erfahren Sie mehr über die Regeln für Sicherheitsgruppen für Cloud Manager".

   - Aktivieren Sie unter **Management System zugewiesene verwaltete Identität** für Cloud Manager durch Auswahl von **ein**.

     Diese Einstellung ist wichtig, da eine gemanagte Identität es der Virtual Machine von Cloud Manager ermöglicht, sich in Azure Active Directory zu identifizieren, ohne Zugangsdaten angeben zu müssen. "Erfahren Sie mehr über Managed Identitäten für Azure Ressourcen".

4. Überprüfen Sie auf der Seite **Überprüfen + erstellen** Ihre Auswahl und klicken Sie auf **Erstellen**, um die Bereitstellung zu starten.

   Azure stellt die virtuelle Maschine mit den angegebenen Einstellungen bereit. Die virtuelle Maschine und die Cloud Manager-Software sollten in etwa fünf Minuten ausgeführt werden.

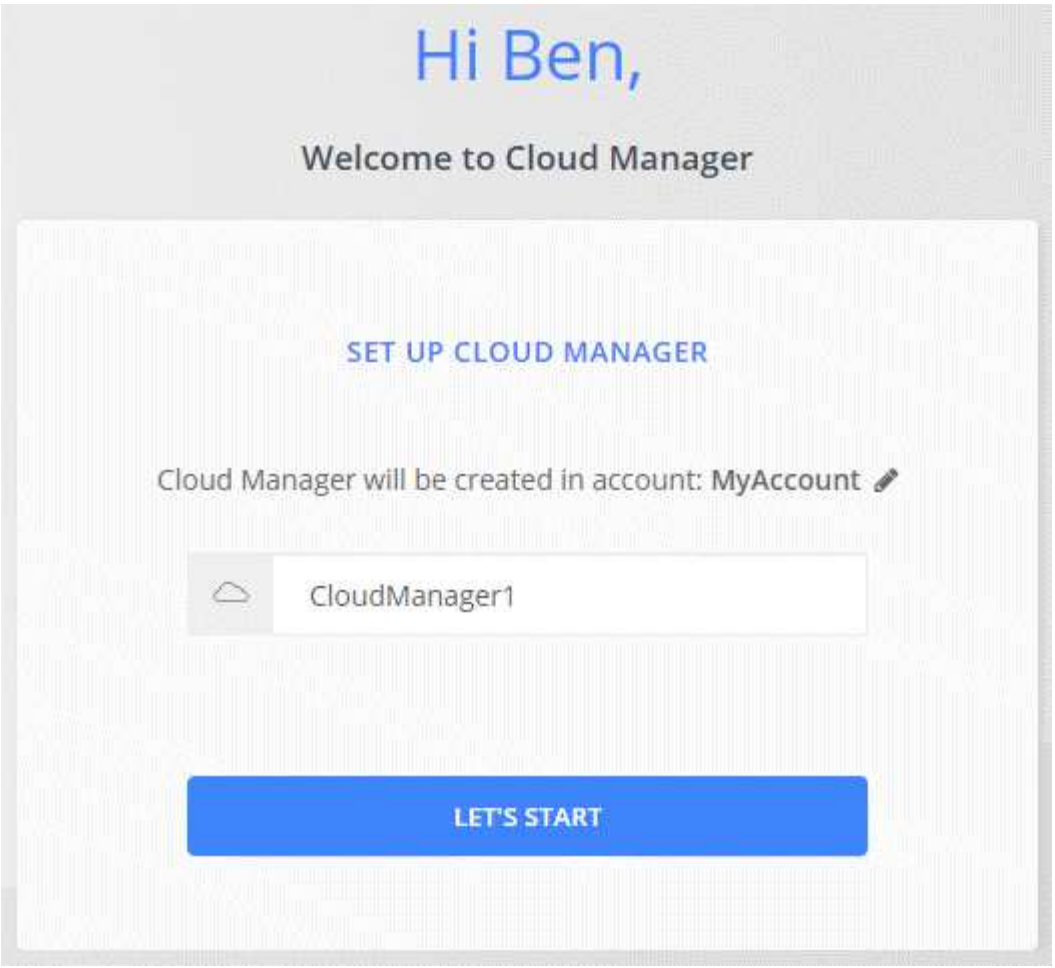
5. Öffnen Sie einen Webbrowser von einem Host aus, der eine Verbindung zur virtuellen Cloud Manager-Maschine hat, und geben Sie die folgende URL ein:

   http://ipaddress:80

6. Richten Sie Cloud Manager nach dem Einloggen ein:
   a. Geben Sie das Cloud Central-Konto an, das mit diesem Cloud Manager-System verknüpft werden soll.

      "Weitere Informationen zu Cloud Central Accounts".

   b. Geben Sie einen Namen für das System ein.



Ergebnis

Cloud Manager ist jetzt installiert und eingerichtet. Sie müssen Azure Berechtigungen erteilen, bevor Benutzer Cloud Volumes ONTAP in Azure bereitstellen können.

Azure Berechtigungen für Cloud Manager gewähren

Bei der Implementierung von Cloud Manager in Azure sollten Sie a aktiviert haben "Vom System zugewiesene verwaltete Identität". Sie müssen jetzt die erforderlichen Azure Berechtigungen erteilen, indem Sie eine benutzerdefinierte Rolle erstellen und dann die Rolle der virtuellen Cloud Manager-Maschine für eine oder mehrere Abonnements zuweisen.

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle mithilfe der Cloud Manager-Richtlinie:

   a. Laden Sie die herunter "Cloud Manager Azure-Richtlinie".

   b. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

      Sie sollten die ID für jedes Azure Abonnement hinzufügen, aus dem Benutzer Cloud Volumes ONTAP Systeme erstellen.

      Beispiel

      "AssignableScopes": ["/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzzzzzzzz", "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzzzz", "/subscriptions/398e471c-3b42-4zzae7-

9b59-zzz"

c. Verwenden Sie die JSON-Datei, um eine benutzerdefinierte Rolle in Azure zu erstellen.

   Im folgenden Beispiel wird gezeigt, wie eine benutzerdefinierte Rolle mithilfe der Azure CLI 2.0 erstellt wird:

   Az Rollendefinition erstellen --Role-Definition C:\Policy_for_Cloud_Manager_Azure_3.7.4.json

Sie sollten nun eine benutzerdefinierte Rolle namens OnCommand Cloud Manager Operator haben, die Sie der virtuellen Cloud Manager-Maschine zuweisen können.

2. Weisen Sie die Rolle der virtuellen Cloud Manager-Maschine für ein oder mehrere Abonnements zu:
   a. Öffnen Sie den Dienst **Abonnements** und wählen Sie dann das Abonnement aus, in dem Sie Cloud Volumes ONTAP-Systeme bereitstellen möchten.
   b. Klicken Sie auf **Access Control (IAM)**.
   c. Klicken Sie auf **Hinzufügen** > **Rollenzuordnung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:
      - Wählen Sie die Rolle **OnCommand Cloud Manager Operator** aus.

        OnCommand Cloud Manager Operator ist der im angegebene Standardname "Cloud Manager-Richtlinie". Wenn Sie einen anderen Namen für die Rolle ausgewählt haben, wählen Sie stattdessen diesen Namen aus.

      - Weisen Sie einer **virtuellen Maschine** Zugriff zu.
      - Wählen Sie das Abonnement aus, in dem die virtuelle Cloud Manager-Maschine erstellt wurde.
      - Wählen Sie die virtuelle Cloud Manager-Maschine aus.
      - Klicken Sie Auf **Speichern**.
   d. Wenn Sie Cloud Volumes ONTAP von zusätzlichen Abonnements aus implementieren möchten, wechseln Sie zu diesem Abonnement, und wiederholen Sie diese Schritte.

Ergebnis

Cloud Manager verfügt jetzt über die Berechtigungen, die es für die Bereitstellung und das Management von Cloud Volumes ONTAP in Azure benötigt.

Cloud Manager in einer Region der US-Regierung von Azure implementieren

Wenn Cloud Manager in einer Region der US-Regierung starten soll, implementieren Sie zunächst Cloud Manager über den Azure Government Marketplace. Stellen Sie dann die Berechtigungen bereit, die Cloud Manager für die Implementierung und das Management von Cloud Volumes ONTAP Systemen benötigt.

Eine Liste der unterstützten Regionen der US-Regierung in Azure finden Sie unter "Cloud Volumes Regionen Weltweit".

Cloud Manager über den Azure Marketplace für die US-Regierung bereitstellen

Cloud Manager ist als Bild im Azure US Government Marketplace erhältlich.

Schritte

1. Stellen Sie sicher, dass der Azure Government Marketplace in Ihrem Abonnement aktiviert ist:
   a. Melden Sie sich als Enterprise-Administrator beim Portal an.
   b. Navigieren Sie zu **Verwalten**.
   c. Klicken Sie unter **Anmeldedetails** auf das Bleistiftsymbol neben **Azure Marketplace**.
   d. Wählen Sie **Aktiviert**.
   e. Klicken Sie Auf **Speichern**.

      "Microsoft Azure-Dokumentation: Azure Government Marketplace"

2. Suchen Sie im Azure US Government Portal nach OnCommand Cloud Manager.
3. Klicken Sie auf **Erstellen** und befolgen Sie die Schritte zur Konfiguration der virtuellen Maschine.

   Beachten Sie beim Konfigurieren der virtuellen Maschine Folgendes:

   - Cloud Manager kann mit HDD- oder SSD-Festplatten optimal arbeiten.
   - Sie sollten eine der empfohlenen virtuellen Maschinengrößen wählen: A2, D2 v2 oder D2 v3 (je nach Verfügbarkeit).
   - Für die Netzwerksicherheitsgruppe empfiehlt es sich, **Erweitert** zu wählen.

     Mit der Option **Erweitert** wird eine neue Sicherheitsgruppe erstellt, die die erforderlichen eingehenden Regeln für Cloud Manager enthält. Wenn Sie „Basis“ wählen, lesen Sie unter "Regeln für Sicherheitsgruppen" Für die Liste der erforderlichen Regeln.

4. Überprüfen Sie auf der Übersichtsseite Ihre Auswahl und klicken Sie auf **Erstellen**, um die Bereitstellung zu starten.

   Azure stellt die virtuelle Maschine mit den angegebenen Einstellungen bereit. Die virtuelle Maschine und die Cloud Manager-Software sollten in etwa fünf Minuten ausgeführt werden.

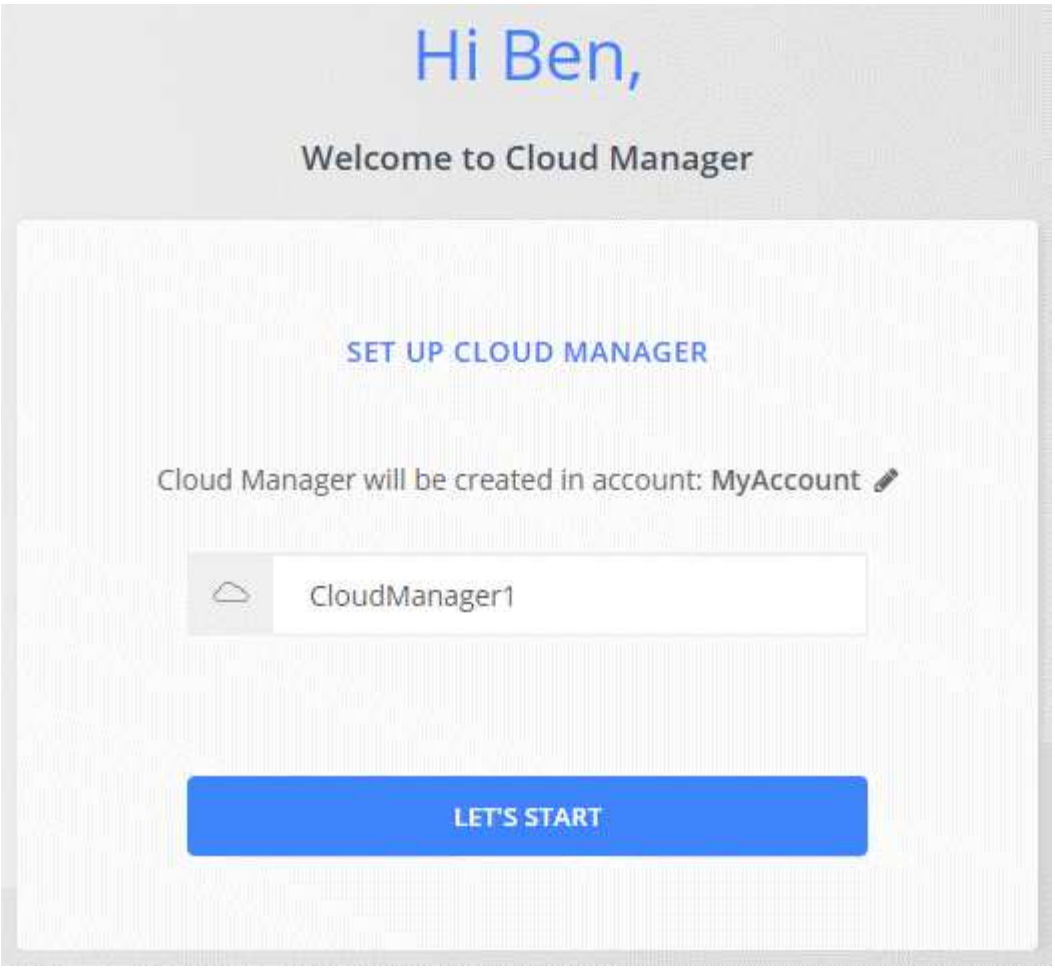
5. Öffnen Sie einen Webbrowser von einem Host aus, der eine Verbindung zur virtuellen Cloud Manager-Maschine hat, und geben Sie die folgende URL ein:

   http://ipaddress:80

6. Richten Sie Cloud Manager nach dem Einloggen ein:
   a. Geben Sie das Cloud Central-Konto an, das mit diesem Cloud Manager-System verknüpft werden soll.

      "Weitere Informationen zu Cloud Central Accounts".

   b. Geben Sie einen Namen für das System ein.



Ergebnis

Cloud Manager ist jetzt installiert und eingerichtet. Sie müssen Azure Berechtigungen erteilen, bevor Benutzer Cloud Volumes ONTAP in Azure bereitstellen können.

Zuweisen von Azure Berechtigungen für Cloud Manager unter Verwendung einer gemanagten Identität

Am einfachsten können Sie Berechtigungen bereitstellen, indem Sie ein aktivieren "Verwaltete Identität" Auf der virtuellen Cloud Manager-Maschine und dann durch Zuweisen der erforderlichen Berechtigungen zu der virtuellen Maschine. Falls gewünscht, ist eine alternative Methode "Azure-Berechtigungen über einen Service-Principal gewähren".

Schritte

1. Aktivieren einer verwalteten Identität auf der virtuellen Cloud Manager-Maschine:
   a. Navigieren Sie zu der virtuellen Cloud Manager-Maschine und wählen Sie **Identität**.
   b. Klicken Sie unter **System Assigned** auf **on** und dann auf **Speichern**.
2. Erstellen Sie eine benutzerdefinierte Rolle mithilfe der Cloud Manager-Richtlinie:
   a. Laden Sie die herunter "Cloud Manager Azure-Richtlinie".
   b. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

      Sie sollten die ID für jedes Azure Abonnement hinzufügen, aus dem Benutzer Cloud Volumes ONTAP Systeme erstellen.

Beispiel

"AssignableScopes": ["/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzzzzzzz", "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzzzz", "/subscriptions/398e471c-3b42-4zzae7-9b59-zzz"

c. Verwenden Sie die JSON-Datei, um eine benutzerdefinierte Rolle in Azure zu erstellen.

Im folgenden Beispiel wird gezeigt, wie eine benutzerdefinierte Rolle mithilfe der Azure CLI 2.0 erstellt wird:

Az Rollendefinition erstellen --Role-Definition C:\Policy_for_Cloud_Manager_Azure_3.7.4.json

Sie sollten nun eine benutzerdefinierte Rolle namens OnCommand Cloud Manager Operator haben, die Sie der virtuellen Cloud Manager-Maschine zuweisen können.

3. Weisen Sie die Rolle der virtuellen Cloud Manager-Maschine für ein oder mehrere Abonnements zu:
   a. Öffnen Sie den Dienst **Abonnements** und wählen Sie dann das Abonnement aus, in dem Sie Cloud Volumes ONTAP-Systeme bereitstellen möchten.
   b. Klicken Sie auf **Access Control (IAM)**.
   c. Klicken Sie auf **Hinzufügen**, klicken Sie auf **Rollenzuweisung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:
      - Wählen Sie die Rolle **OnCommand Cloud Manager Operator** aus.

        OnCommand Cloud Manager Operator ist der im angegebene Standardname "Cloud Manager-Richtlinie". Wenn Sie einen anderen Namen für die Rolle ausgewählt haben, wählen Sie stattdessen diesen Namen aus.

      - Weisen Sie einer **virtuellen Maschine** Zugriff zu.
      - Wählen Sie das Abonnement aus, in dem die virtuelle Cloud Manager-Maschine erstellt wurde.
      - Geben Sie den Namen der virtuellen Maschine ein, und wählen Sie sie aus.
      - Klicken Sie Auf **Speichern**.
   d. Wenn Sie Cloud Volumes ONTAP von zusätzlichen Abonnements aus implementieren möchten, wechseln Sie zu diesem Abonnement, und wiederholen Sie diese Schritte.

Ergebnis

Cloud Manager verfügt jetzt über die Berechtigungen, die es für die Bereitstellung und das Management von Cloud Volumes ONTAP in Azure benötigt.

Installieren von Cloud Manager in einer Azure Deutschland Region

Der Azure Marketplace ist in den Regionen von Azure Deutschland nicht verfügbar. Sie müssen daher das Cloud Manager-Installationsprogramm von der NetApp Support-Website herunterladen und auf einem vorhandenen Linux-Host in der Region installieren.

Schritte

1. "Netzwerkanforderungen für Azure prüfen".
2. "Host-Anforderungen für Cloud Manager prüfen".

3. "Laden Sie Cloud Manager herunter und installieren Sie es".
4. "Gewähren Sie Cloud Manager Azure Berechtigungen mit einem Service-Principal".

Nachdem Sie fertig sind

Cloud Manager ist jetzt bereit, Cloud Volumes ONTAP wie jede andere Region in Azure Deutschland zu implementieren. Möglicherweise möchten Sie jedoch zuerst ein zusätzliches Setup durchführen.

Unterbrechungsfreier Betrieb von Cloud Manager

Cloud Manager sollte stets verfügbar sein.

Cloud Manager ist eine Kernkomponente bei Systemzustand und Abrechnung von Cloud Volumes ONTAP. Wenn Cloud Manager heruntergefahren wird, werden Cloud Volumes ONTAP Systeme heruntergefahren, nachdem die Kommunikation mit Cloud Manager über mehr als 4 Tage lang unterbrochen wurde.

Implementieren Sie Cloud Volumes ONTAP

Bevor Sie Cloud Volumes ONTAP Systeme erstellen

Bevor Sie Cloud Manager zum Erstellen und Managen von Cloud Volumes ONTAP Systemen verwenden, sollte Ihr Cloud Manager Administrator das Netzwerk vorbereitet und Cloud Manager installiert und eingerichtet haben.

Vor der Implementierung von Cloud Volumes ONTAP sollten die folgenden Bedingungen erfüllt sein:

- Für Cloud Manager und Cloud Volumes ONTAP wurden die Netzwerkanforderungen erfüllt.
- Cloud Manager verfügt über die Berechtigungen, die Vorgänge bei dem gewählten Cloud-Provider durchzuführen.
- Für AWS haben Sie die entsprechende AWS Marketplace-Seite abonniert:
  - Wenn Sie ein PAYGO-System bereitstellen oder eine Add-on-Funktion aktivieren möchten: "Die Seite „Cloud Manager“ (für Cloud Volumes ONTAP".
  - Wenn Sie ein BYOL-System implementieren möchten: "Den einzelnen Node oder die HA-Seite im AWS Marketplace".
- Cloud Manager wurde installiert.

Weiterführende Links

- "Erste Schritte in AWS"
- "Erste Schritte in Azure"
- "Erste Schritte in GCP"
- "Einrichten von Cloud Manager"

Anmelden bei Cloud Manager

Sie können sich über einen beliebigen Webbrowser mit Verbindung zum Cloud Manager-System bei Cloud Manager anmelden. Sie sollten sich mit einem anmelden "NetApp Cloud Central" Benutzerkonto.

Schritte

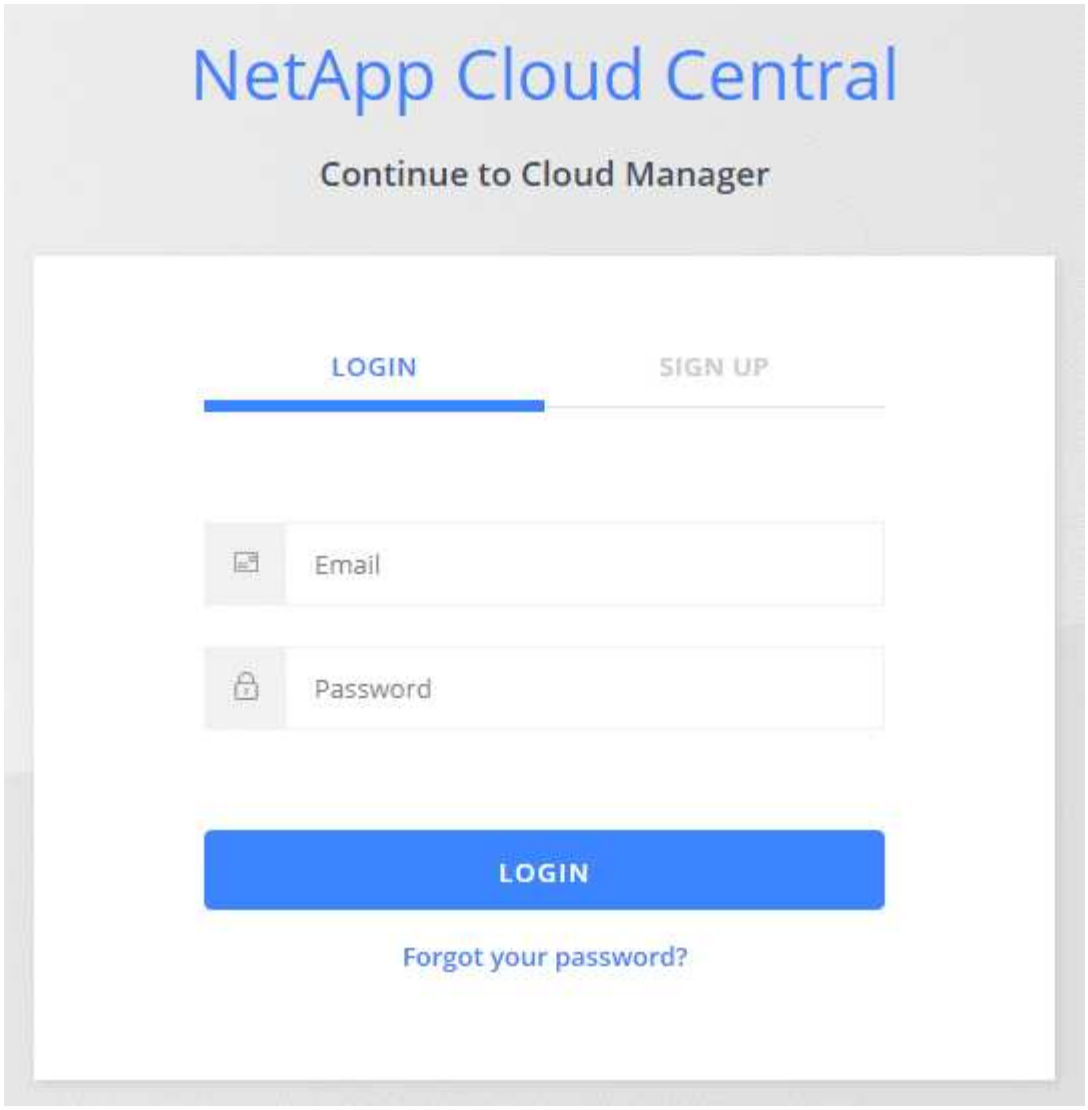
1. Öffnen Sie einen Webbrowser, und melden Sie sich bei an "NetApp Cloud Central".

   Dieser Schritt sollte Sie automatisch zur Fabric View leiten. Falls nicht, klicken Sie auf **Fabric View**.

2. Wählen Sie das Cloud Manager System aus, auf das Sie zugreifen möchten.

   Wenn keine Systeme aufgeführt sind, stellen Sie sicher, dass der Account Admin Sie zum Cloud Central Konto hinzugefügt hat, das mit dem Cloud Manager System verbunden ist.

3. Melden Sie sich mit Ihren NetApp Cloud Central Zugangsdaten bei Cloud Manager an.



Planung Ihrer Cloud Volumes ONTAP Konfiguration

Wenn Sie Cloud Volumes ONTAP implementieren, können Sie ein vorkonfiguriertes System auswählen, das Ihren Workload-Anforderungen entspricht, oder Sie können eine eigene Konfiguration erstellen. 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"
- "Unterstützte Konfigurationen für Cloud Volumes ONTAP 9.7 in Azure"
- "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-Limits für Cloud Volumes ONTAP 9.7 in AWS"
- "Storage-Höchstwerte für Cloud Volumes ONTAP 9.7 in Azure"
- "Storage-Grenzen für Cloud Volumes ONTAP 9.7 in GCP"

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.

AWS Planung

Planen Sie die Implementierung von Cloud Volumes ONTAP in AWS, indem Sie die Größe Ihres Systems dimensionieren und die erforderlichen Netzwerkinformationen überprüfen.

- Dimensionierung Ihres Systems in AWS
- Arbeitsblatt mit Informationen zum AWS-Netzwerk

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*

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	

AWS-Informationen	Ihr Wert
Unverankerte IP-Adresse für Daten auf Node 1	
Unverankerte IP-Adresse für Daten auf Node 2	
Routing-Tabellen für unverankerte IP-Adressen	

Azure Planung

Planen Sie die Implementierung von Cloud Volumes ONTAP in Azure, indem Sie die Größe Ihres Systems dimensionieren und die erforderlichen Netzwerkinformationen überprüfen.

- Dimensionierung Ihres Systems in Azure
- Azure Network Information Worksheet

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: Einführung in Microsoft Azure Storage".

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"

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)	

GCP-Planung

Planen Sie die Implementierung von Cloud Volumes ONTAP in der Google Cloud Platform, indem Sie die Größe Ihres Systems dimensionieren und die erforderlichen Netzwerkinformationen überprüfen.

- Dimensionierung Ihres Systems in GCP
- Informationarbeitsblatt für das GCP-Netzwerk

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	

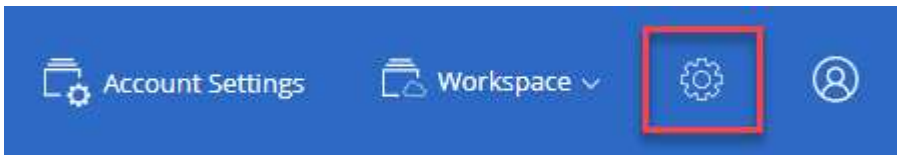
GCP-Informationen	Ihr Wert
Firewallrichtlinie (bei Nutzung eigener Richtlinien)	

Suchen der System-ID des Cloud Manager

Um Ihnen bei den ersten Schritten zu helfen, wird Sie möglicherweise von Ihrem NetApp Vertriebsmitarbeiter nach Ihrer Cloud Manager System-ID gefragt. Die ID wird in der Regel für Lizenzierungs- und Fehlerbehebungszwecke verwendet.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen.



2. Klicken Sie Auf **Support Dashboard**.

   Ihre System-ID wird oben rechts angezeigt.

   Beispiel

Aktivierung von Flash Cache für Cloud Volumes ONTAP

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.

Einschränkungen

- Um die Performance-Verbesserungen von Flash Cache nutzen zu können, muss die Komprimierung für alle Volumes deaktiviert sein.
- Cloud Volumes ONTAP unterstützt das Neustarten des Cache nicht, wenn ein Neustart nach einem Neustart erfolgen soll.

Aktivierung von Flash Cache für Cloud Volumes ONTAP in AWS

Flash Cache wird mit Cloud Volumes ONTAP Premium und BYOL in AWS unterstützt.

Schritte

1. Wählen Sie einen der folgenden EC2-Instanztypen mit einem neuen oder vorhandenen Cloud Volumes ONTAP Premium- oder BYOL-System aus:
   - C5d.4xlarge
   - C5d.9xlarge
   - R5d.2xlarge
2. Deaktivieren Sie die Komprimierung auf allen Volumes, um die Vorteile der Flash Cache Performance-Verbesserungen zu nutzen.

   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".

Aktivierung von Flash Cache auf Cloud Volumes ONTAP in Azure

Flash Cache wird mit Cloud Volumes ONTAP BYOL in Single-Node-Systemen unterstützt.

Schritte

1. Wählen Sie in Azure den VM-Typ Standard_L8S_v2 mit einem Cloud Volumes ONTAP BYOL-System mit einem einzelnen Node aus.
2. Deaktivieren Sie die Komprimierung auf allen Volumes, um die Vorteile der Flash Cache Performance-Verbesserungen zu nutzen.

   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".

Starten von Cloud Volumes ONTAP in AWS

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

Abonnieren im AWS Marketplace

Abonnieren Sie den AWS Marketplace, um für Cloud Volumes ONTAP nutzungsbasiert zu bezahlen, oder nutzen Sie die Möglichkeit zur Implementierung von Cloud Volumes ONTAP BYOL.

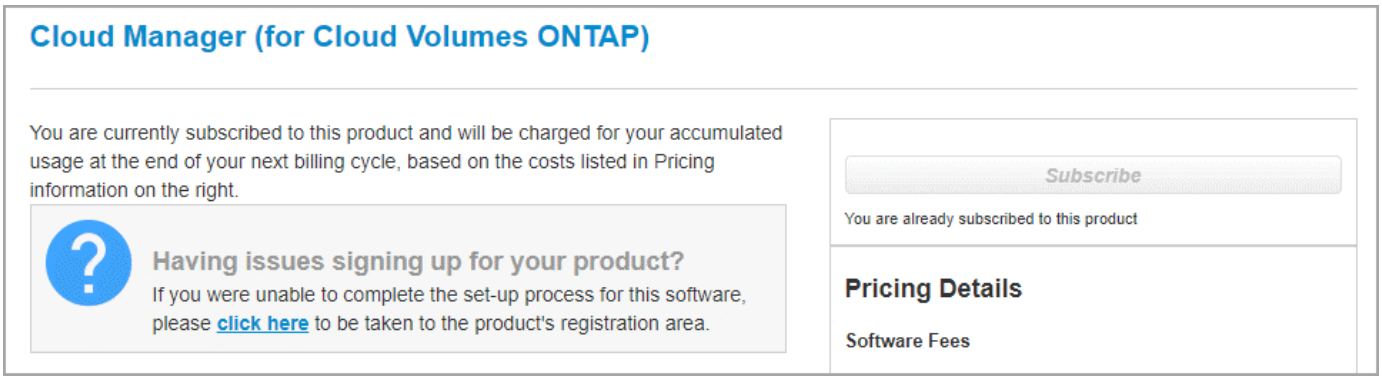
Abonnieren von PAYGO

"Abonnieren Sie ihn im AWS Marketplace" Um sicherzustellen, dass es nach der kostenlosen Testversion von Cloud Volumes ONTAP keine Serviceunterbrechung gibt. 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.

Das folgende Video zeigt den Abonnementprozess:

► https://docs.netapp.com/de-de/occm37//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, zeigt AWS den nachfolgenden Benutzern an, dass sie bereits abonniert sind, wie in der Abbildung unten dargestellt. Zwar besteht für das AWS Konto ein Abonnement, jeder IAM-Benutzer muss sich jedoch mit dem 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.



Abonnieren von BYOL

Wenn Sie Cloud Volumes ONTAP mit Ihrer eigenen Lizenz (BYOL) starten, "Anschließend müssen Sie das Angebot im AWS Marketplace abonnieren".

"Weitere Informationen zu den einzelnen AWS Marketplace finden Sie auf dieser Seite".

Einführung eines einzelnen Cloud Volumes ONTAP Systems 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 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

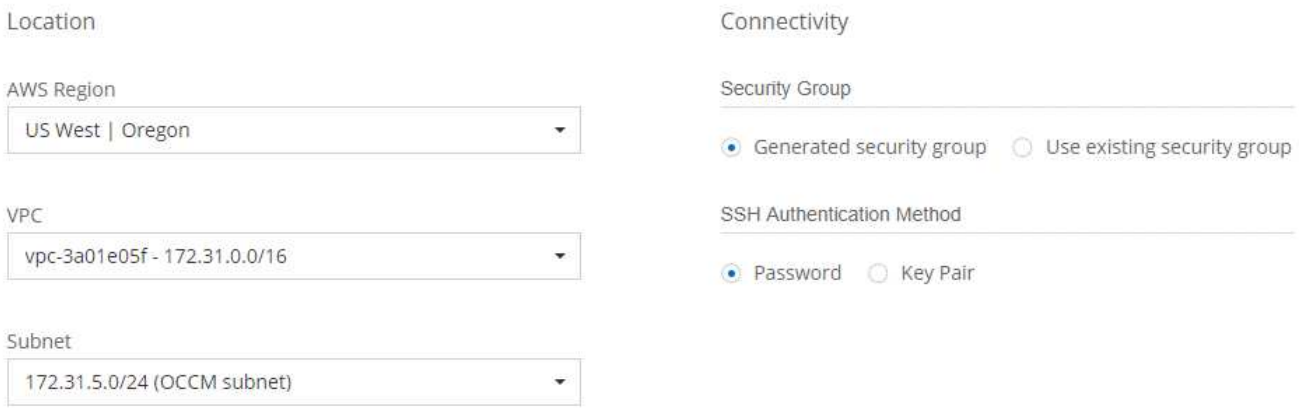
1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Cloud Volumes ONTAP erstellen** und befolgen Sie die Anweisungen.
2. **Definieren Sie Ihre Arbeitsumgebung**: Wählen Sie **Amazon Web Services** und **Cloud Volumes ONTAP**.
3. **Details und Anmeldeinformationen**: Optional können Sie das AWS-Konto und das Marketplace-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
Konto	Sie können ein anderes Konto wählen, wenn Sie "Zusätzliche AWS Konten zu Cloud Manager hinzugefügt".
Marketplace-Abonnement	Wählen Sie ein anderes Abonnement aus, wenn Sie das AWS Konto, von dem Sie belastet werden, ändern möchten. Um ein neues Abonnement hinzuzufügen, "Gehen Sie zum Angebot im AWS Marketplace".
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".
Anmeldedaten	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.

4. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie mit diesem Cloud Volumes ONTAP-System nicht verwenden möchten.
   - "Weitere Informationen zu Backup in S3".
   - "Erfahren Sie mehr über Cloud Compliance".
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 9.4 RC1 auswählen und 9.4 GA verfügbar ist. Das Update findet nicht von einer Version auf eine andere statt, z. B. von 9.3 auf 9.4.

11. **Zugrunde liegende Speicherressourcen**: Wählen Sie die Einstellungen für das anfängliche Aggregat: Einen Datenträgertyp, eine Größe für jede Platte, und ob S3 Tiering aktiviert werden soll.

    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".

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

    "Erfahren Sie mehr über Schreibgeschwindigkeit".

    "Erfahren Sie mehr über WORM Storage".

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

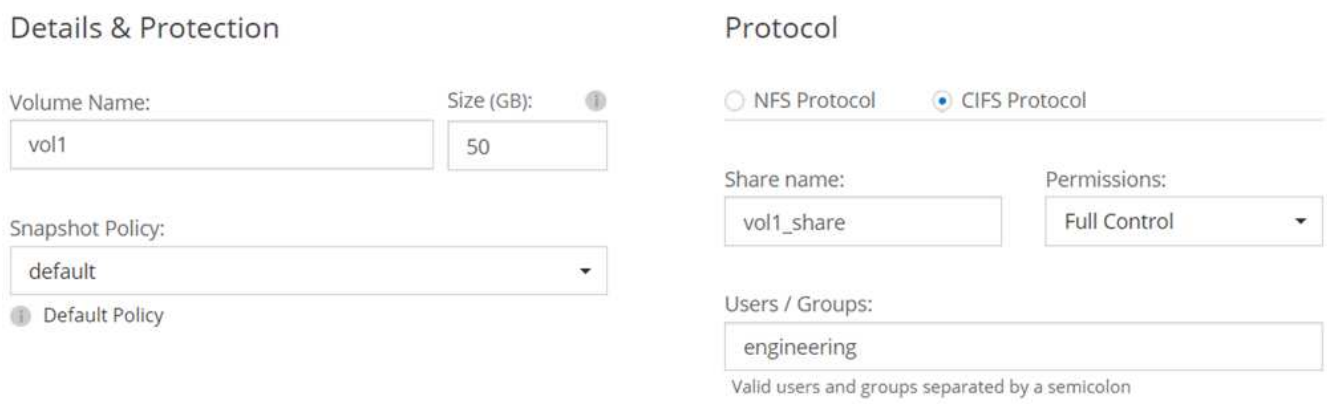
    Sie können diesen Schritt überspringen, wenn Sie ein Volume für iSCSI erstellen möchten. Cloud Manager richtet Volumes nur für NFS und CIFS ein.

    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.

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.

Feld	Beschreibung
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, ob Sie Funktionen zur Storage-Effizienz aktivieren und bei Bedarf die S3-Tiering-Richtlinie 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 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".

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 **Cloud Volumes ONTAP erstellen** und befolgen Sie die Anweisungen.
2. **Definieren Sie Ihre Arbeitsumgebung**: Wählen Sie **Amazon Web Services** und **Cloud Volumes ONTAP HA**.
3. **Details und Anmeldeinformationen**: Optional können Sie das AWS-Konto und das Marketplace-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
Konto	Sie können ein anderes Konto wählen, wenn Sie "Zusätzliche AWS Konten zu Cloud Manager hinzugefügt".
Marketplace-Abonnement	Wählen Sie ein anderes Abonnement aus, wenn Sie das AWS Konto, von dem Sie belastet werden, ändern möchten. Um ein neues Abonnement hinzuzufügen, "Gehen Sie zum Angebot im AWS Marketplace".
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".
Anmeldedaten	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.

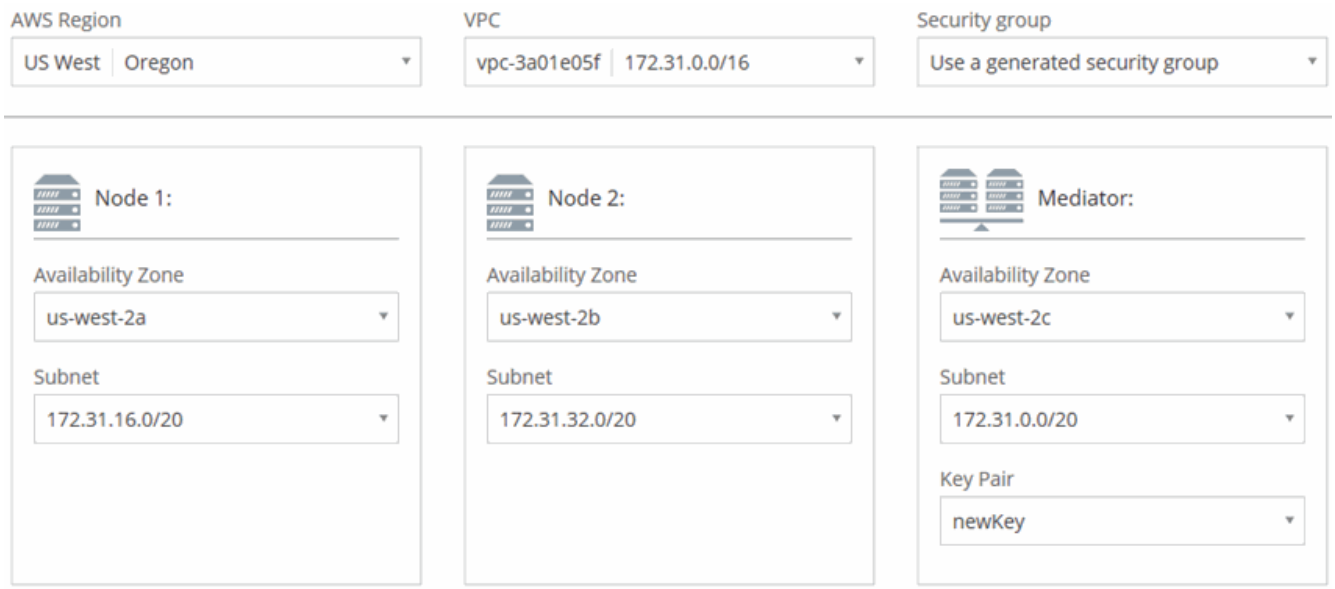
4. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie mit diesem Cloud Volumes ONTAP-System nicht verwenden möchten.
   - "Weitere Informationen zu Backup in S3".
   - "Erfahren Sie mehr über Cloud Compliance".

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 9.4 RC1 auswählen und 9.4 GA verfügbar ist. Das Update findet nicht von einer Version auf eine andere statt, z. B. von 9.3 auf 9.4.

15. **Zugrunde liegende Speicherressourcen**: Wählen Sie die Einstellungen für das anfängliche Aggregat: Einen Datenträgertyp, eine Größe für jede Platte, und ob S3 Tiering aktiviert werden soll.

    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".

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

    "Erfahren Sie mehr über WORM Storage".

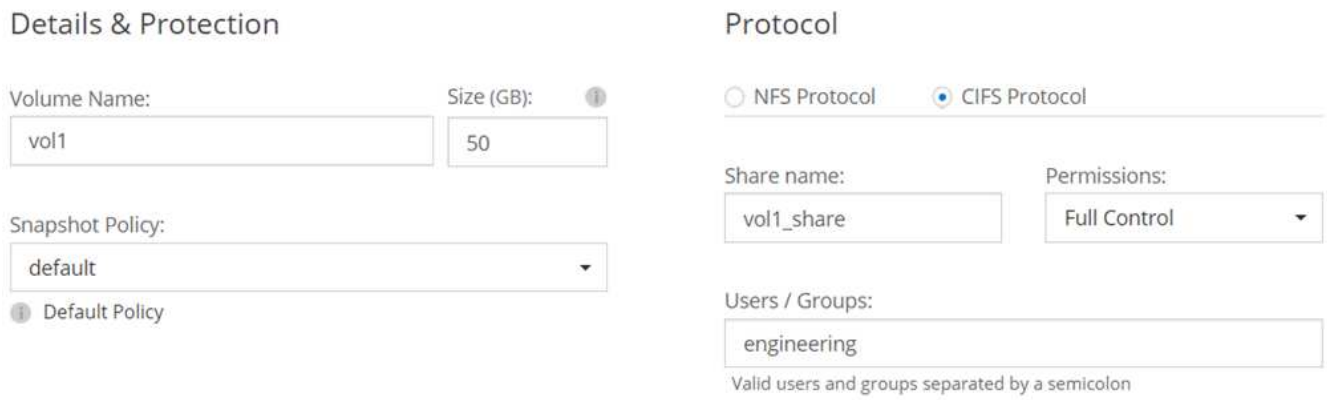
17. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

    Sie können diesen Schritt überspringen, wenn Sie ein Volume für iSCSI erstellen möchten. Cloud Manager richtet Volumes nur für NFS und CIFS ein.

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.

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.

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. 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, Festplattentyp und Tiering-Richtlinie**: Wählen Sie, ob Sie Funktionen zur Storage-Effizienz aktivieren und bei Bedarf die S3-Tiering-Richtlinie 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.

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

- Stellen Sie sicher, dass Ihr Azure Konto über die erforderlichen Berechtigungen verfügt, insbesondere dann, wenn Sie das Upgrade aus einer vorherigen Version durchgeführt und zum ersten Mal ein HA-System implementiert haben.

  Die neuesten Berechtigungen finden Sie im "NetApp Cloud Central-Richtlinie für Azure".

- 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.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Cloud Volumes ONTAP erstellen** und befolgen Sie die Anweisungen.
2. **Definieren Sie Ihre Arbeitsumgebung**: Wählen Sie **Microsoft Azure** und wählen Sie dann einen einzelnen Knoten oder ein HA-Paar.
3. **Details und Anmeldeinformationen**: Optional können Sie das Azure-Konto oder das Abonnement ändern, einen Cluster-Namen und einen Ressourcengruppennamen angeben, bei Bedarf Tags hinzufügen und dann Anmeldedaten angeben.

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

Feld	Beschreibung
Switch-Konto	Sie können ein anderes Konto oder Abonnement wählen, wenn Sie "Richten Sie sie ein und fügen sie zu Cloud Manager hinzu".
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.
Name der Ressourcengruppe	Wenn Sie **Standard verwenden** deaktivieren, können Sie den Namen einer neuen Ressourcengruppe eingeben. Wenn Sie eine vorhandene Ressourcengruppe verwenden möchten, müssen Sie die API verwenden.

Feld	Beschreibung
Tags	Tags sind Metadaten für Ihre Azure Ressourcen. Cloud Manager fügt die Tags dem Cloud Volumes ONTAP System und jeder Azure Ressource hinzu, die dem 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".
Anmeldedaten	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.

4. **Dienste**: Die Cloud-Konformität wird aktiviert oder deaktiviert, wenn Sie sie nicht mit diesem Cloud Volumes ONTAP-System verwenden möchten.

   "Erfahren Sie mehr über Cloud Compliance".

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 9.5 RC1 und 9.5 GA auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.4 bis 9.5.

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.

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".

11. **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".

   "Erfahren Sie mehr über WORM Storage".

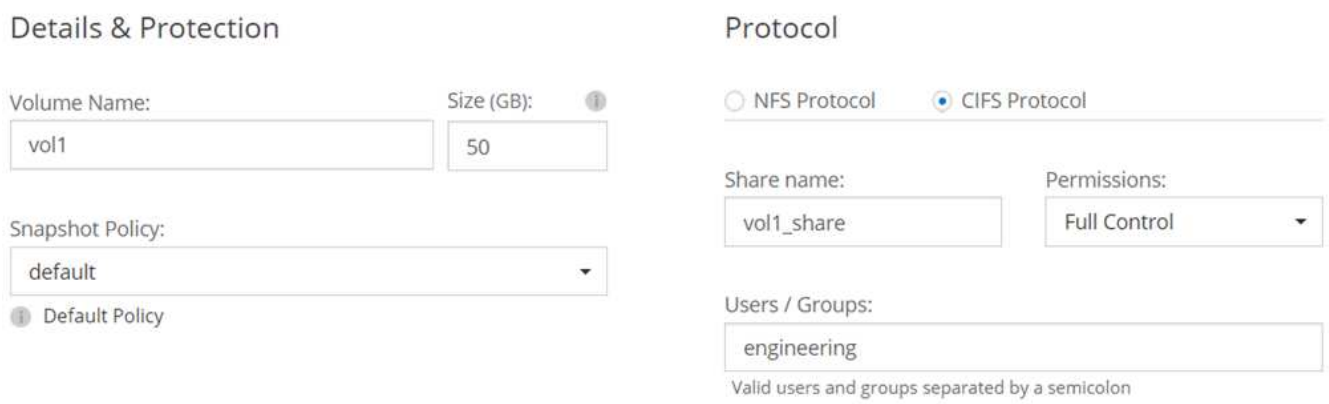
12. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

   Sie sollten diesen Schritt überspringen, wenn Sie iSCSI verwenden möchten. Mit Cloud Manager können Sie Volumes nur für NFS und CIFS erstellen.

   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.

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



13. **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. 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.

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

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

15. **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.

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.

Bevor Sie beginnen

- 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).

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebung auf **Cloud Volumes ONTAP erstellen** und folgen Sie den Anweisungen.
2. **Definieren Sie Ihre Arbeitsumgebung**: Klicken Sie Auf **Weiter**.
3. **Abonnieren Sie Cloud Volumes ONTAP**: Wenn Sie dazu aufgefordert werden, abonnieren Sie Cloud Volumes ONTAP im GCP Marketplace.

   Das folgende Video zeigt den Abonnementprozess:

   ► https://docs.netapp.com/de-de/occm37//media/video_subscribing_gcp.mp4 *(video)*

4. **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
Google Cloud Projekt	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 4b auf dieser Seite beschrieben".
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.
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".
Anmeldedaten	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.

5. **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".

6. **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".

7. **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.

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 9.5 RC1 und 9.5 GA auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.4 bis 9.5.

9. **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.

   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".

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

    "Erfahren Sie mehr über Schreibgeschwindigkeit".

    "Erfahren Sie mehr über WORM Storage".

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

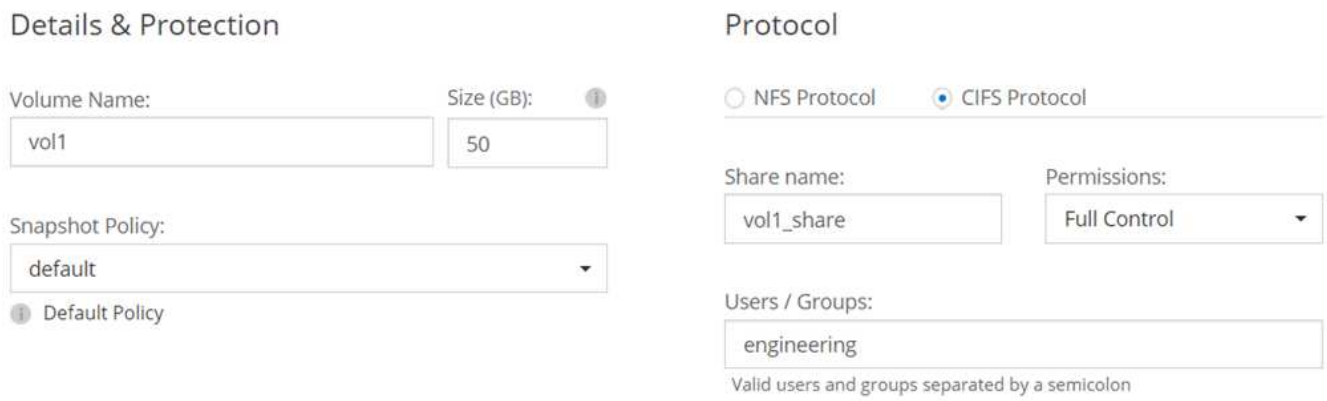
    Sie sollten diesen Schritt überspringen, wenn Sie iSCSI verwenden möchten. Mit Cloud Manager können Sie Volumes nur für NFS und CIFS erstellen.

    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.

Feld	Beschreibung
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.

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.
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.
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 Tiering-Richtlinie ändern möchten.

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

14. **Google Cloud Platform Account for Data Tiering**: Richten Sie Daten-Tiering durch Bereitstellung von interoperablen Speicherzugriffsschlüsseln für ein Google Cloud Platform Konto ein. Klicken Sie auf **Skip**, um das Daten-Tiering zu deaktivieren.

    Mithilfe der Schlüssel kann Cloud Manager einen Cloud Storage-Bucket für das Daten-Tiering einrichten. Weitere Informationen finden Sie unter "Einrichten und Hinzufügen von GCP-Konten zu Cloud Manager".

15. **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.

Registrieren von Pay-as-you-go-Systemen

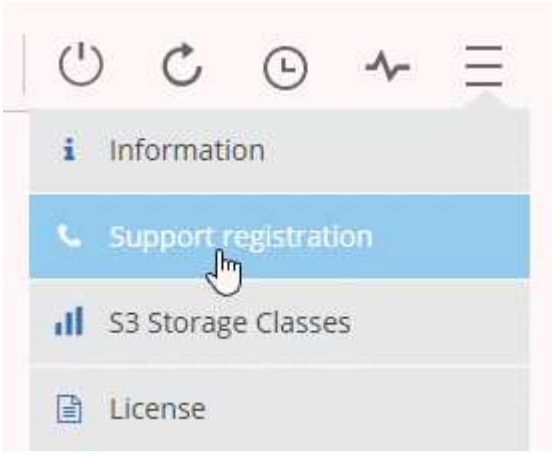
Cloud Volumes ONTAP Explore, Standard und Premium umfasst Support von NetApp. Sie müssen jedoch den Support erst aktivieren, wenn Sie die Systeme bei NetApp registrieren.

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**:



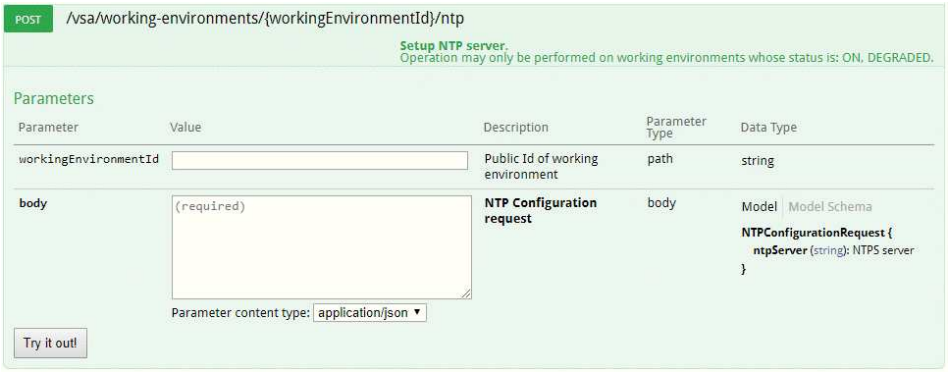
4. Wählen Sie ein NetApp Support Site Konto aus und klicken Sie auf **Registrieren**.

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: 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".

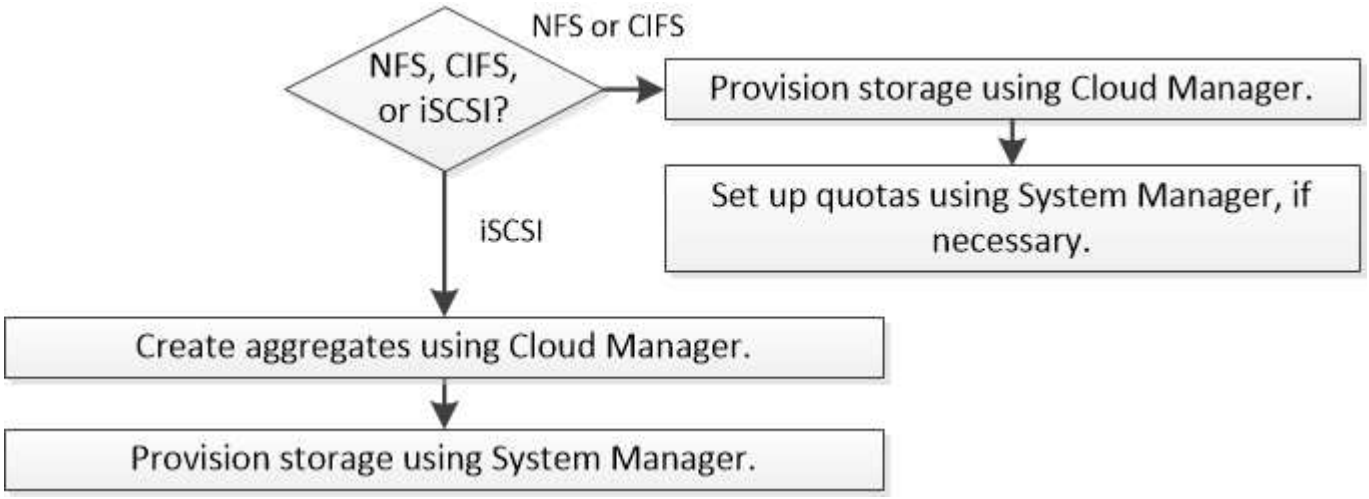
Aufgabe	Beschreibung
Optional: Erstellung einer SVM Management-Netzwerkschnittstelle (LIF) für HA-Systeme in mehreren AWS Verfügbarkeitszonen	Wenn Sie SnapCenter oder SnapDrive für Windows mit einem HA-Paar verwenden möchten, ist eine Storage Virtual Machine (SVM) Management Network Interface (LIF) erforderlich. 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 Cloud Manager-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".

Bereitstellung von Storage

Storage-Bereitstellung

Sie können zusätzlichen NFS- und CIFS-Storage für Ihre Cloud Volumes ONTAP Systeme über Cloud Manager bereitstellen, indem Sie Volumes und Aggregate managen. Wenn Sie iSCSI-Storage erstellen müssen, sollten Sie dies über System Manager tun.

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 Start eines Cloud Volumes ONTAP Systems mehr Storage benötigen, können Sie neue FlexVol Volumes für NFS oder CIFS über Cloud Manager 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**.

Aktion	Schritte
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.

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**.

Bereitstellung von iSCSI-LUNs

Wenn Sie iSCSI-LUNs erstellen möchten, müssen Sie dies über System Manager tun.

Bevor Sie beginnen

- Die Host-Dienstprogramme müssen auf den Hosts installiert und eingerichtet werden, die eine Verbindung zur LUN herstellen.
- Sie müssen den iSCSI-Initiatornamen vom Host aufgezeichnet haben. Sie müssen diesen Namen

angeben, wenn Sie eine igroup für die LUN erstellen.

- Bevor Sie Volumes in System Manager erstellen, müssen Sie sicherstellen, dass Sie über ein Aggregat mit ausreichend Speicherplatz verfügen. Sie müssen Aggregate in Cloud Manager erstellen. Weitere Informationen finden Sie unter "Aggregate werden erstellt".

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".
2. Klicken Sie auf **Storage > LUNs**.
3. Klicken Sie auf **Erstellen** und folgen Sie den Aufforderungen zur Erstellung der LUN.
4. Stellen Sie von Ihren Hosts eine Verbindung zur LUN her.

   Anweisungen hierzu finden Sie im "Host Utilities-Dokumentation" Für Ihr Betriebssystem.

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.

Tiering inaktiver Daten in kostengünstigen Objektspeicher

Sie können Storage-Kosten 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 einem GCP-Konto zum Cloud Manager hinzufügen und das Subnetz für privaten Google Access konfigurieren. 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

- Sie müssen einem Cloud Manager ein Google Cloud Platform Konto hinzufügen, indem Sie Storage-Zugriffschlüssel für ein Service-Konto eingeben. Mithilfe der Schlüssel kann Cloud Manager einen Cloud Storage-Bucket für das Daten-Tiering einrichten. Anweisungen hierzu finden Sie unter "Einrichten und Hinzufügen von GCP-Konten zu Cloud Manager".
- 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".

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

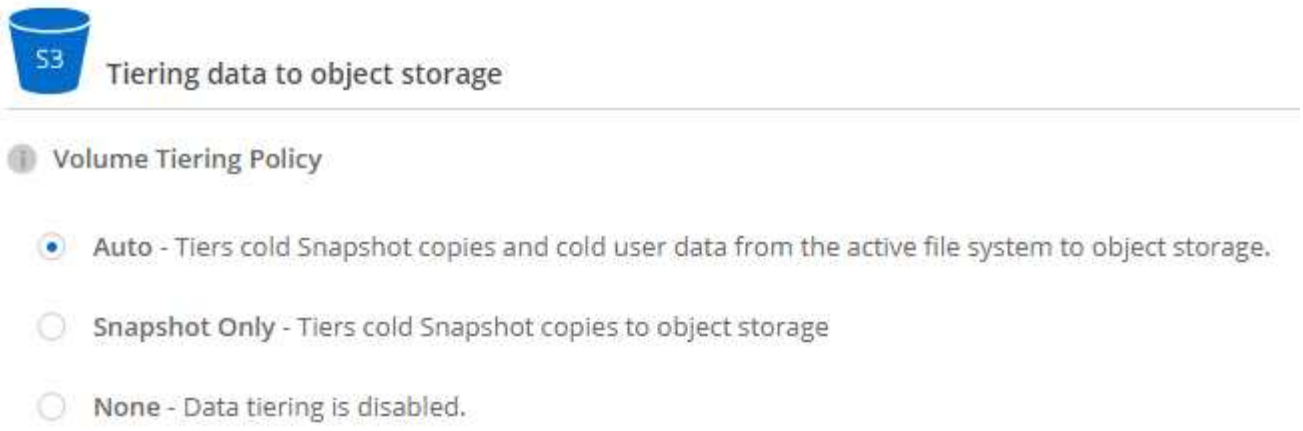
1. Erstellen Sie in der Arbeitsumgebung ein neues Volume, oder ändern Sie den Tier eines vorhandenen Volumes:

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 die Richtlinie "Nur Snapshot" oder die Richtlinie "Auto" 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.

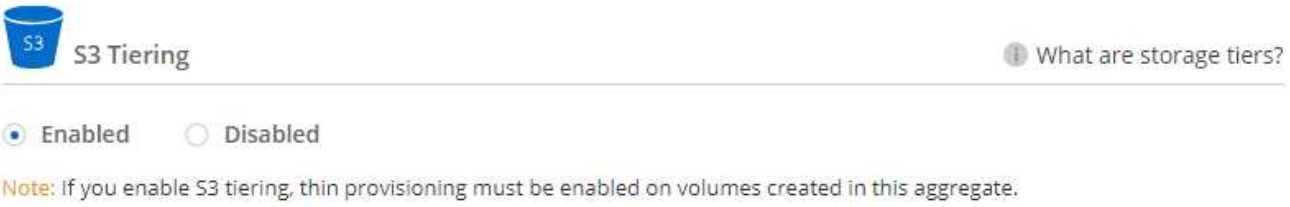
Tiering von Daten aus Datensicherungs-Volumes

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".

Ändern der Tiering-Ebene in AWS oder Azure

Wenn Sie das Daten-Tiering aktivieren, schichtet Cloud Volumes ONTAP inaktive Daten in AWS in die S3 *Standard* Storage-Klasse oder zum „*Hot* Storage Tier in Azure“. Nach der Implementierung von Cloud Volumes ONTAP können Sie Ihre Storage-Kosten senken, indem Sie die Tiering-Ebene für inaktive Daten ändern, auf die seit 30 Tagen nicht mehr zugegriffen wurde. Die Zugriffskosten sind höher, wenn Sie auf die Daten

zugreifen. Daher müssen Sie dies berücksichtigen, bevor Sie die Tiering Level ändern.

Sie können die Tiering-Stufe in GCP nicht ändern, da derzeit nur die *Regional* Storage-Klasse unterstützt wird.

Über diese Aufgabe

Die Tiering Level sind systemweit - sie sind nicht pro Volume.

In AWS können Sie die Tiering-Ebene ändern, sodass inaktive Daten nach 30 Tagen Inaktivität in eine der folgenden Storage-Klassen verschoben werden:

- Intelligentes Tiering
- Standardzugriff
- Ein einmaliger Zugriff

In Azure können Sie den Tiering-Level ändern, sodass inaktive Daten nach 30 Tagen Inaktivität in den Storage Tier „_cool_Storage“ verschoben werden.

Weitere Informationen zur Funktionsweise von Tiering-Ebenen finden Sie unter "Data Tiering - Übersicht".

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **S3 Storage Classes** oder **Blob Storage Tiering**.
2. Wählen Sie die Tiering-Ebene und klicken Sie dann auf **Speichern**.

Verwendung von ONTAP als persistenter Storage für Kubernetes

Cloud Manager kann die Implementierung von automatisieren "NetApp Trident" Auf Kubernetes-Clustern zur Verwendung von ONTAP als persistenten Storage für Container Dies funktioniert mit Cloud Volumes ONTAP und On-Premises-ONTAP-Clustern.

Bevor Sie diese Schritte ausführen, müssen Sie sie ausführen "Erstellen eines Cloud Volumes ONTAP Systems" Oder "Ermitteln eines lokalen ONTAP Clusters" Von Cloud Manager

Bei der Implementierung von Kubernetes-Clustern mit dem "NetApp Kubernetes Service", Cloud Manager kann die Cluster automatisch aus Ihrem NetApp Cloud Central Konto erkennen. Wenn das der Fall ist, überspringen Sie die ersten beiden Schritte und beginnen Sie mit Schritt 3.

Netzwerk-Konnektivität prüfen

1. Zwischen Cloud Manager und den Kubernetes-Clustern und den ONTAP-Clustern muss eine Netzwerkverbindung verfügbar sein.
2. Bei der 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/

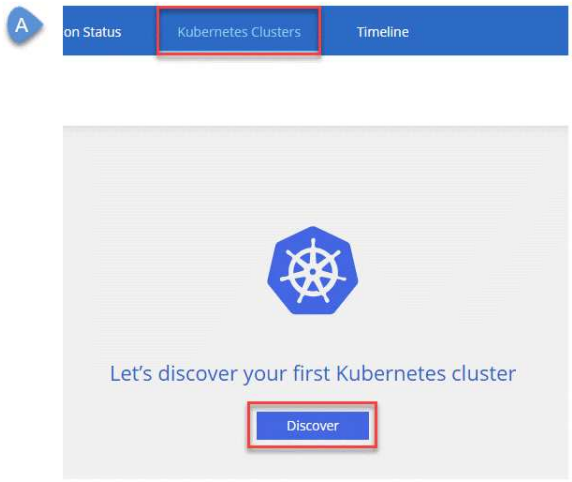
   Cloud Manager installiert Trident auf einem Kubernetes-Cluster, wenn Sie eine Arbeitsumgebung mit dem

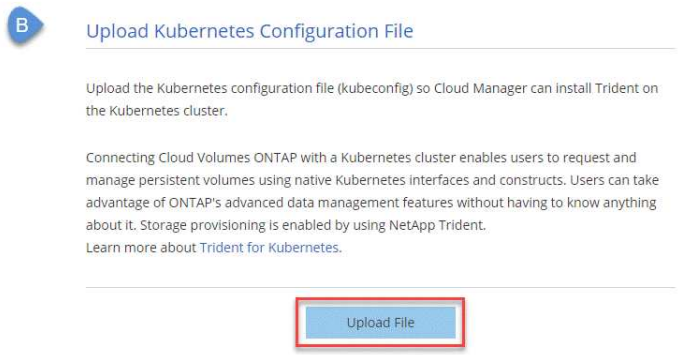
Cluster verbinden.

Kubernetes-Konfigurationsdateien in Cloud Manager hochladen

Der Account Admin muss für jeden Kubernetes eine Konfigurationsdatei (kubeconfig) im YAML-Format hochladen. Nach dem Hochladen der Datei überprüft Cloud Manager die Verbindung zum Cluster und speichert eine verschlüsselte Kopie der kubeconfig-Datei.

Klicken Sie auf **Kubernetes Clusters > Entdecken > Datei hochladen** und wählen Sie die kubeconfig-Datei aus.

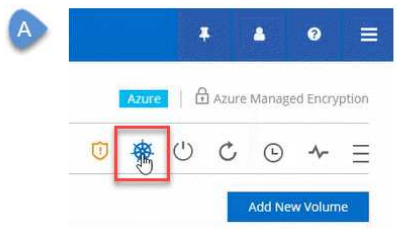


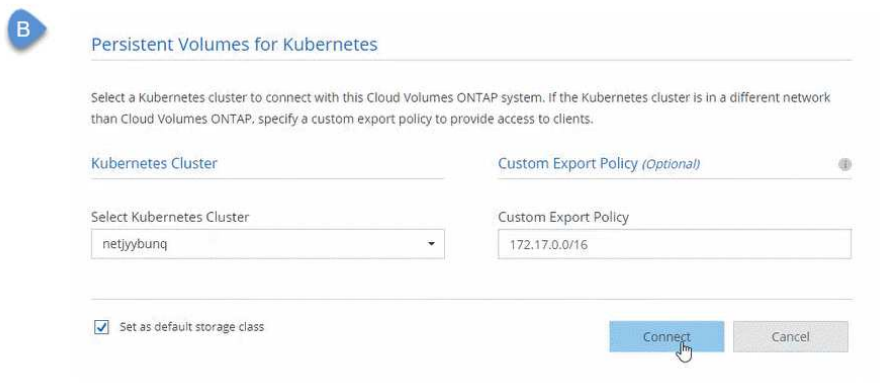


Verbinden Sie Ihre Arbeitsumgebungen mit Kubernetes-Clustern

Klicken Sie in der Arbeitsumgebung auf das Kubernetes-Symbol und folgen Sie den Aufforderungen. Sie können verschiedene Cluster mit verschiedenen ONTAP Systemen und mehreren Clustern mit demselben ONTAP System verbinden.

Sie haben die Möglichkeit, die NetApp Storage-Klasse als Standard-Storage-Klasse für den Kubernetes Cluster einzustellen. Wenn ein Benutzer ein persistentes Volume erstellt, kann der Kubernetes-Cluster standardmäßig verbundene ONTAP-Systeme als Back-End-Storage verwenden.





Starten Sie die Bereitstellung persistenter Volumes

Persistente Volumes können über native Kubernetes-Schnittstellen und -Konstrukte angefordert und gemanagt werden. Cloud Manager erstellt vier Kubernetes-Storage-Klassen, die bei der Provisionierung von persistenten Volumes genutzt werden können:

- **netapp-File**: Zur Anbindung persistenter Volumes an ONTAP-Systeme mit einem Node
- **netapp-File-san**: Zur Anbindung persistenter iSCSI-Volumes an Single-Node-ONTAP-Systeme
- **netapp-file-redundant**: Zur Anbindung persistenter Volumes an ONTAP HA-Paare
- **netapp-file-redundant-san**: Zur Anbindung persistenter iSCSI-Volumes an ONTAP HA-Paare

Cloud Manager konfiguriert Trident standardmäßig für die Verwendung folgender Bereitstellungsoptionen:

- Thin Volumes
- Die standardmäßige Snapshot-Richtlinie
- Verzeichnis für zugängliche Snapshots

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

Was sind die Dreizack_Trident Volumes?

Cloud Manager erstellt ein Volume auf dem ersten ONTAP System, das Sie mit einem Kubernetes-Cluster verbinden. Der Name des Volumes wird mit „_Trident_dreident_dreident“ angehängt. ONTAP verwendet dieses Volume, um die Verbindung zum Kubernetes-Cluster herzustellen. Diese Volumes sollten nicht gelöscht werden.

Was geschieht, wenn Sie ein Kubernetes Cluster trennen oder entfernen?

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

Nachdem Sie alle Systeme von einem Kubernetes-Cluster getrennt haben, können Sie auch die gesamte Kubernetes-Konfiguration aus Cloud Manager entfernen. Cloud Manager deinstalliert Trident nicht, wenn Sie den Cluster entfernen und keine persistenten Volumes gelöscht werden.

Beide Aktionen sind nur über APIs verfügbar. Wir planen, die Aktionen in einer zukünftigen Version der Schnittstelle hinzuzufügen."Klicken Sie hier, um weitere Informationen zu den APIs zu erhalten".

Verschlüsseln von Volumes mit 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.

Über diese Aufgabe

- 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.

- Derzeit unterstützt Cloud Volumes ONTAP NetApp Volume Encryption mit einem externen Verschlüsselungsmanagement Server. Ein Onboard Key Manager wird nicht unterstützt.
- Sie müssen NetApp Volume Encryption über die ONTAP CLI einrichten.

  Die Verschlüsselung für bestimmte Volumes kann dann entweder über die CLI oder mit System Manager aktiviert werden. Cloud Manager unterstützt NetApp Volume Encryption von seiner Benutzeroberfläche und seinen APIs nicht.

"Erfahren Sie mehr über unterstützte Verschlüsselungstechnologien".

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"

4. Erstellen Sie ein neues verschlüsseltes Volume oder konvertieren Sie ein vorhandenes unverschlüsseltes Volume mithilfe der CLI oder des System Manager.
   - CLI
     - Verwenden Sie für neue Volumes den Befehl **Volume create** mit dem Parameter -crypt.

       "ONTAP 9 NetApp Verschlüsselungs-Leitfaden: Verschlüsselung auf einem neuen Volume"

     - Verwenden Sie für vorhandene Volumes den Befehl **Volume Encryption Conversion Start**.

       "ONTAP 9 NetApp Verschlüsselungs-Power Guide: Aktivierung der Verschlüsselung auf einem vorhandenen Volume mit dem Befehl zur Konvertierung der Volume-Verschlüsselung"

   - System Manager:
     - Klicken Sie bei neuen Volumes auf **Speicherung > Volumes > Erstellen > FlexVol erstellen** und wählen Sie dann **verschlüsselt** aus.

       "ONTAP 9 Cluster Management mit System Manager: Erstellen von FlexVol Volumes"

     - Wählen Sie für vorhandene Volumes das Volume aus, klicken Sie auf **Bearbeiten** und wählen Sie dann **verschlüsselt**.

"ONTAP 9 Clustermanagement mit System Manager: Bearbeiten der Volume-Eigenschaften"

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**.
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-Zugriffssteuerungsliste 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**.

Aufgabe	Aktion
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**.
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.
Aktivieren oder deaktivieren Sie die Synchronisierung mit S3 für ein Volume	Wählen Sie ein Volume aus und klicken Sie dann auf **Synchronisierung zu S3** oder **Synchronisierungsbeziehung löschen**. Bevor Sie diese Optionen verwenden können, muss die Funktion zum Synchronisieren mit S3 aktiviert sein. Anweisungen hierzu finden Sie unter "Daten werden mit AWS S3 synchronisiert"
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**.
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.

Aufgabe	Aktion
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.

3. Klicken Sie Auf **Speichern**.

Ergebnis

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

Verschieben eines Volumes zur Vermeidung von Kapazitätsproblemen

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.

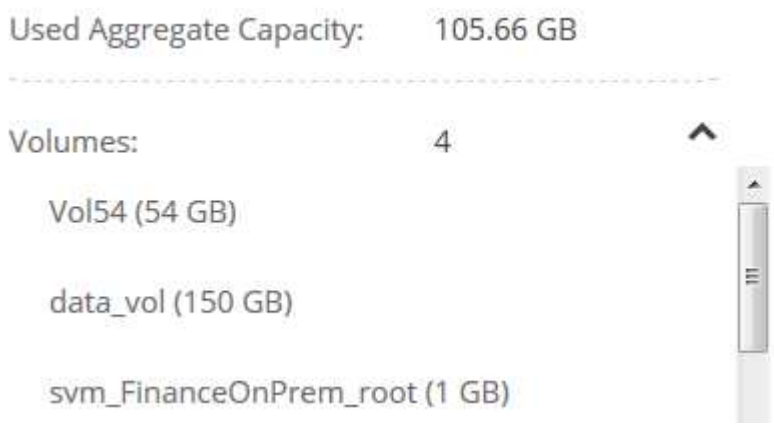
Schritte

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.

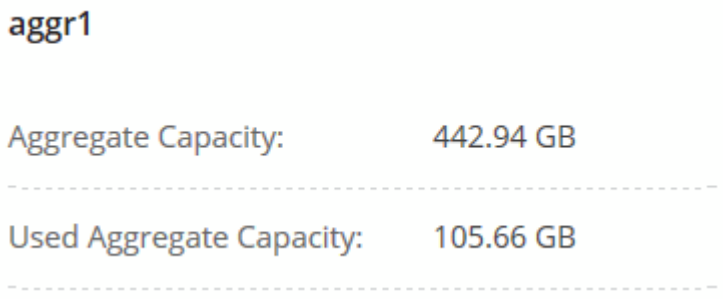
Über diese Aufgabe

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".

Replizierung und Sicherung von Daten

Erkennung und Management von ONTAP Clustern

Cloud Manager kann die ONTAP Cluster in Ihrer lokalen Umgebung, in einer NetApp Private Storage-Konfiguration und in der IBM Cloud erkennen. Durch die Erkennung dieser Cluster können Sie Daten einfach über Ihre Hybrid Cloud-Umgebung direkt über Cloud Manager replizieren.

Erkennung von ONTAP Clustern

Mit der Erkennung eines ONTAP Clusters in Cloud Manager können Sie Storage bereitstellen und Daten in Ihrer Hybrid Cloud replizieren.

Bevor Sie beginnen

Sie müssen über die Clusterverwaltungs-IP-Adresse und das Kennwort für das Administratorbenutzerkonto verfügen, um den Cluster zum Cloud Manager hinzuzufügen.

Cloud Manager erkennt ONTAP Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewall-Richtlinien verwenden, müssen diese die folgenden Anforderungen erfüllen:

- Der Cloud Manager-Host muss ausgehenden HTTPS-Zugriff über Port 443 zulassen.

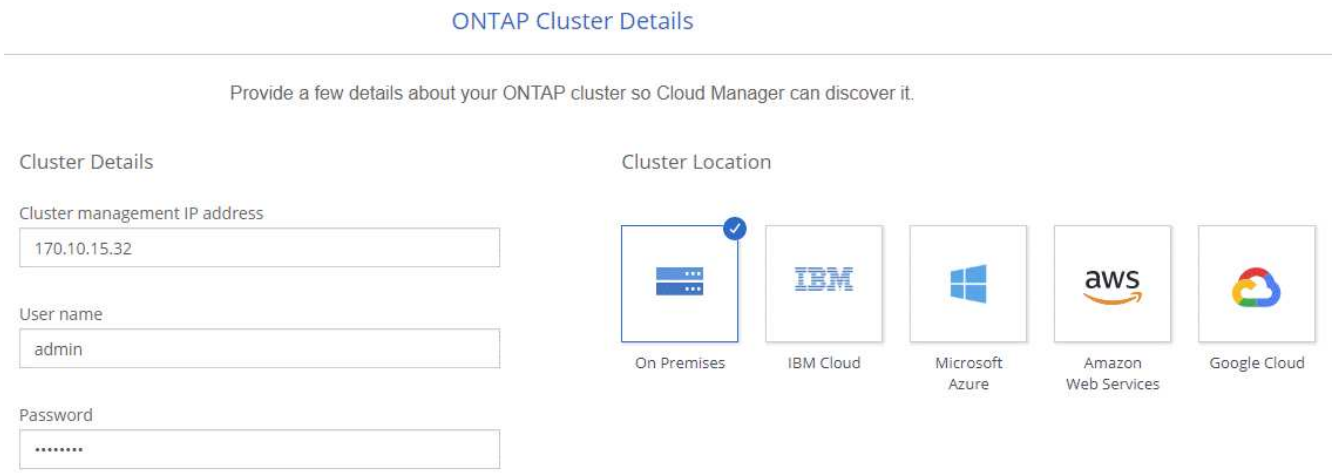
  Wenn sich Cloud Manager in AWS befindet, wird die gesamte ausgehende Kommunikation von der vordefinierten Sicherheitsgruppe zugelassen.

- Der ONTAP Cluster muss eingehenden HTTPS-Zugriff über Port 443 zulassen.

  Die standardmäßige "mgmt"-Firewall-Richtlinie ermöglicht eingehenden HTTPS-Zugriff von allen IP-Adressen. Wenn Sie diese Standardrichtlinie geändert haben oder eine eigene Firewall-Richtlinie erstellt haben, müssen Sie das HTTPS-Protokoll mit dieser Richtlinie verknüpfen und den Zugriff vom Cloud Manager-Host aus aktivieren.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Entdecken** und wählen Sie **ONTAP Cluster**.
2. Geben Sie auf der Seite **ONTAP-Cluster-Details** die Cluster-Management-IP-Adresse, das Passwort für das Admin-Benutzerkonto und den Standort des Clusters ein.



3. Geben Sie auf der Seite Details einen Namen und eine Beschreibung für die Arbeitsumgebung ein und klicken Sie dann auf **Go**.

Ergebnis

Cloud Manager erkennt das Cluster. Sie können jetzt Volumes erstellen, Daten auf und vom Cluster replizieren und OnCommand System Manager starten, um erweiterte Aufgaben auszuführen.

Bereitstellung von Volumes auf ONTAP Clustern

Mit Cloud Manager können Sie NFS- und CIFS-Volumes auf ONTAP Clustern bereitstellen.

Bevor Sie beginnen

NFS oder CIFS müssen auf dem Cluster eingerichtet sein. Sie können NFS und CIFS mit System Manager oder der CLI einrichten.

Über diese Aufgabe

Sie können Volumes auf vorhandenen Aggregaten erstellen. Sie können keine neuen Aggregate aus Cloud Manager erstellen.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf den Namen des ONTAP Clusters, auf dem Sie Volumes bereitstellen möchten.
2. Klicken Sie Auf **Neues Volume Hinzufügen**.
3. Geben Sie auf der Seite Neues Volume erstellen die Details für das Volume ein und klicken Sie dann auf **Erstellen**.

   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.
Nutzungsprofil	Mithilfe von Nutzungsprofilen werden die NetApp Storage-Effizienzfunktionen definiert, die für ein Volume aktiviert sind.

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.

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.

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 10000, 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

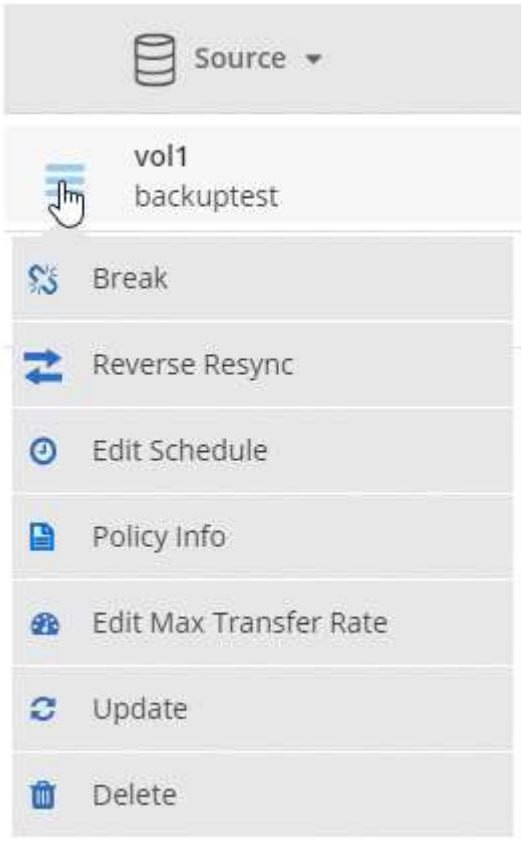
1. Zeigen Sie auf der Seite Arbeitsumgebungen den Replikationsstatus für alle Arbeitsumgebungen im Arbeitsbereich oder für eine bestimmte Arbeitsumgebung an:

Option	Aktion
Alle Arbeitsumgebungen im Arbeitsbereich	Klicken Sie oben im Cloud Manager auf **Replikationsstatus**.
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.
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".

Aktion	Beschreibung
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.

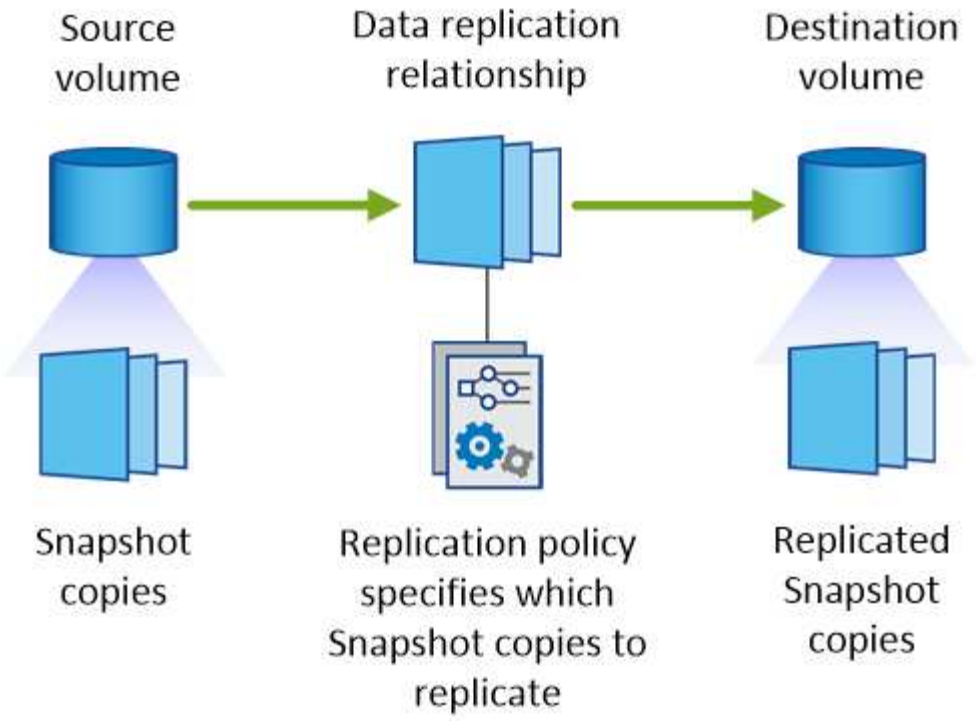
Was sind Replizierungsrichtlinien

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.

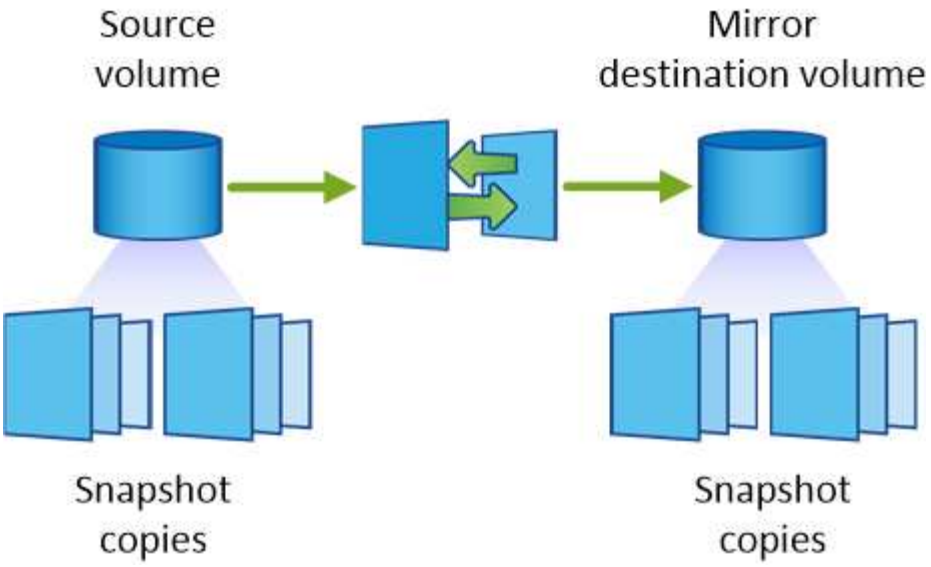
- Eine *Backup*-Richtlinie repliziert bestimmte Snapshot-Kopien zu einem Ziel-Volume und speichert diese in der Regel für einen längeren Zeitraum, als es auf dem Quell-Volume der Fall wäre.

  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.

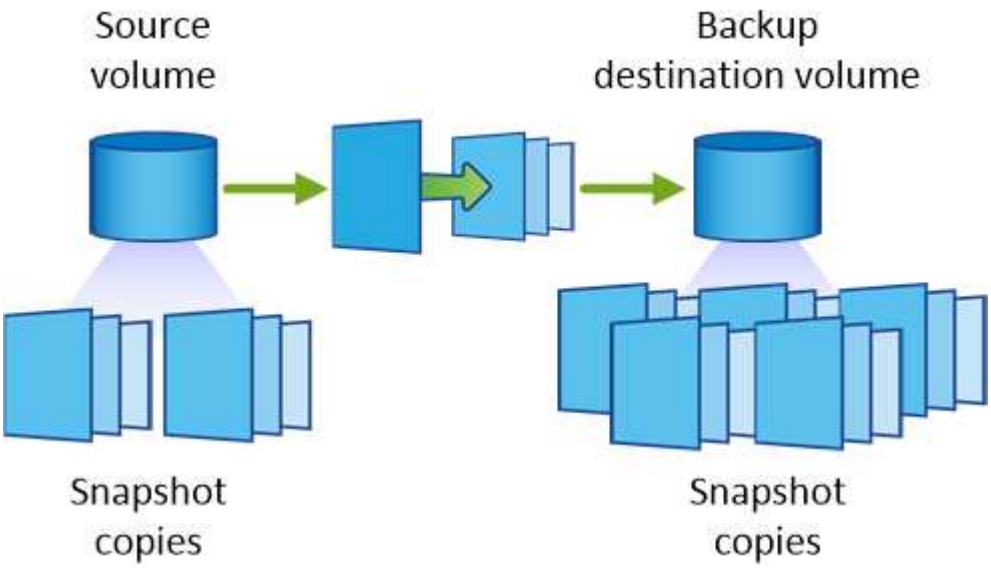
- Eine Richtlinie „ *Mirror und Backup*“ ermöglicht Disaster Recovery und langfristige Datenhaltung.

  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.

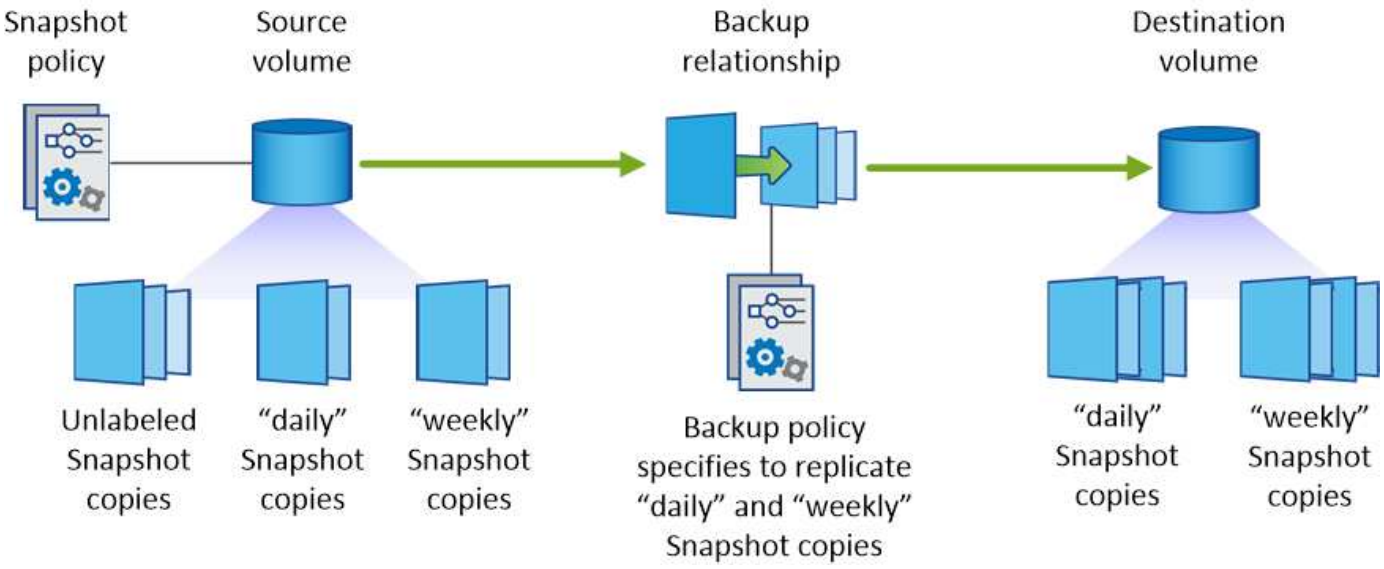
Verständnis der Beziehung zwischen Snapshot Copy Labels und Backup-Richtlinien

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.

Daten-Backups in Amazon S3 sichern

Backup in S3 ist ein Add-on-Feature für Cloud Volumes ONTAP, das Funktionen für vollumfängliches Backup und Restore in puncto Sicherung und Langzeitarchivierung Ihrer Cloud-Daten bereitstellt. Die Backups werden im S3-Objekt-Storage gespeichert, unabhängig von Volume-Snapshot-Kopien für die kurzfristige Wiederherstellung oder das Klonen.

Wenn Sie Backup in S3 aktivieren, führt der Service ein vollständiges Backup Ihrer Daten durch. Alle zusätzlichen Backups sind inkrementell, was bedeutet, dass nur geänderte Blöcke und neue Blöcke gesichert werden.

"Weitere Informationen zur Preisgestaltung finden Sie im NetApp Cloud Central".

Beachten Sie, dass Cloud Manager für alle Backup- und Restore-Vorgänge verwendet werden muss. Alle direkt von ONTAP oder von Amazon S3 aus ergriffenen Aktionen führen zu einer nicht unterstützten Konfiguration.

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

Überprüfen Sie Folgendes:

- Cloud Volumes ONTAP 9.4 oder höher läuft in einer unterstützten AWS-Region: N. Virginia, Oregon, Irland, Frankfurt oder Sydney
- Sie haben sich für das neue angemeldet "Cloud Manager Marketplace-Angebot"
- TCP-Port 5010 ist für ausgehenden Datenverkehr auf der Sicherheitsgruppe für Cloud Volumes ONTAP geöffnet (er ist standardmäßig geöffnet)
- TCP-Port 8088 ist für ausgehenden Datenverkehr auf der Sicherheitsgruppe für Cloud Manager geöffnet (er ist standardmäßig geöffnet)
- Auf den folgenden Endpunkt kann über Cloud Manager zugegriffen werden:

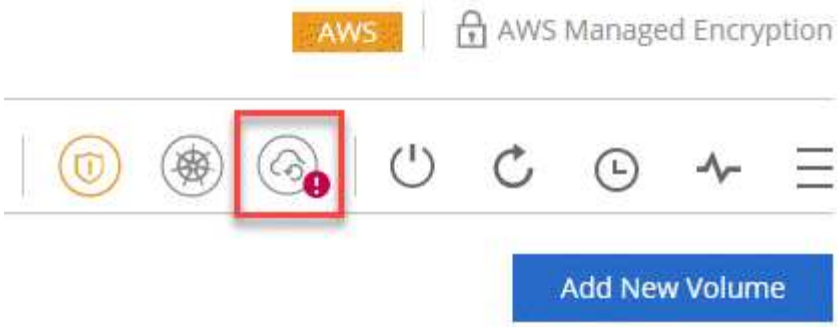
  https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

- Cloud Manager kann bis zu zwei VPC-Endpunkte in der VPC zuweisen (das AWS Limit pro VPC ist 20)
- Cloud Manager ist berechtigt, die in der neuesten Liste aufgeführten VPC-Endpunktberechtigungen zu verwenden "Cloud Manager-Richtlinie":

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

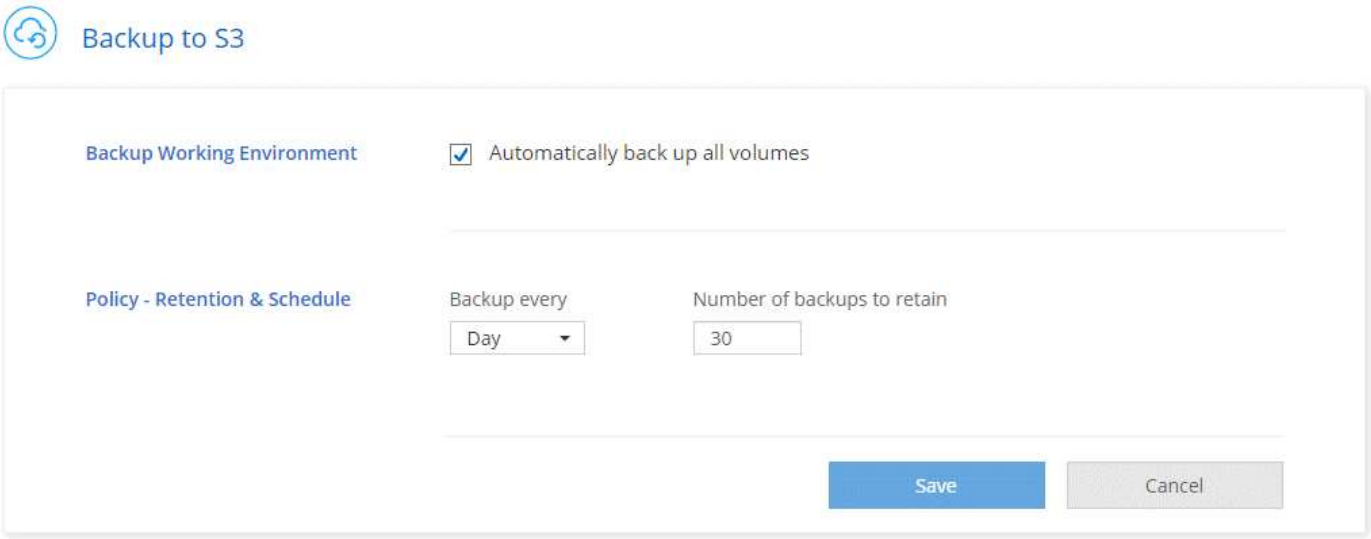
Aktivieren Sie Backup auf Ihrem neuen oder vorhandenen System in S3

- Neue Systeme: Die Funktion Backup to S3 ist standardmäßig im Assistenten für die Arbeitsumgebung aktiviert. Achten Sie darauf, dass die Option aktiviert bleibt.
- Bestehende Systeme: Öffnen Sie die Arbeitsumgebung, klicken Sie auf das Symbol für die Backup-Einstellungen und aktivieren Sie Backups.



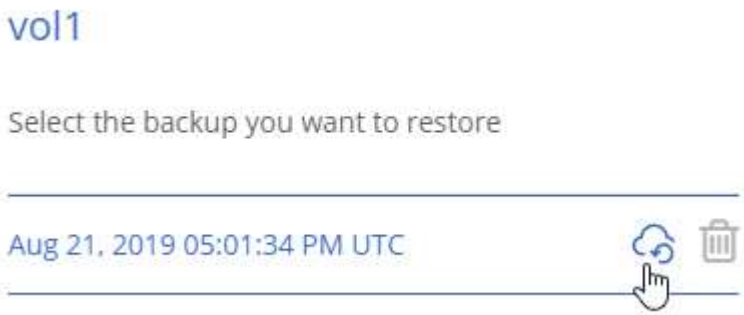
Ändern Sie bei Bedarf die Backup-Richtlinie

Die Standardrichtlinie sichert Volumes täglich und speichert 30 Backup-Kopien jedes Volumes. Bei Bedarf können Sie die Anzahl der zu behaltenden Backup-Kopien ändern.



Stellen Sie Ihre Daten nach Bedarf wieder her

Klicken Sie oben im Cloud Manager auf **Backup & Restore**, wählen Sie ein Volume aus, wählen Sie ein Backup aus und stellen Sie dann Daten aus dem Backup auf ein neues Volume wieder her.



Anforderungen

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie mit dem Backup von Volumes in S3 beginnen.

Unterstützte ONTAP-Versionen

Backup in S3 wird mit Cloud Volume ONTAP 9.4 und höher unterstützt.

Unterstützte AWS-Regionen

Backup in S3 wird mit Cloud Volumes ONTAP in den folgenden AWS Regionen unterstützt:

- US-Osten (N. Virginia)
- US West (Oregon)
- EU (Irland)
- EU (Frankfurt)
- Asien/Pazifik (Sydney)

AWS Berechtigungen erforderlich

Die IAM-Rolle, die Cloud Manager über Berechtigungen verfügt, muss Folgendes enthalten:

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

AWS Abonnement erforderlich

Ab Version 3.7.3 ist im AWS Marketplace ein neues Cloud Manager Abonnement verfügbar. Mit diesem Abonnement sind Implementierungen von Cloud Volumes ONTAP 9.6 und höher PAYGO Systemen und die Funktion Backup to S3 möglich. Sie müssen "Abonnieren Sie dieses neue Cloud Manager Abonnement" Bevor Sie Backup in S3 aktivieren. Über dieses Abonnement erfolgt die Abrechnung für die Funktion „Backup to S3“.

Port-Anforderungen

- TCP-Port 5010 muss für ausgehenden Datenverkehr von Cloud Volumes ONTAP zum Backup-Service offen sein.
- TCP-Port 8088 muss für Outbound-Datenverkehr auf der Sicherheitsgruppe für Cloud Manager offen sein.

  Diese Ports sind bereits geöffnet, wenn Sie die vordefinierten Sicherheitsgruppen verwenden. Aber wenn Sie Ihre eigenen verwendet haben, dann müssen Sie diese Ports öffnen.

Outbound-Internetzugang

Stellen Sie sicher, dass über Cloud Manager auf den folgenden Endpunkt zugegriffen werden kann: https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

Cloud Manager kontaktiert den Endpunkt, um Ihre AWS Konto-ID zur Liste der zugelassenen Benutzer für Backup in S3 hinzuzufügen.

VPC-Endpunkte Schnittstellen

Wenn Sie die Funktion Backup in S3 aktivieren, erstellt Cloud Manager einen VPC-Endpunkt in der VPC, an dem die Cloud Volumes ONTAP ausgeführt wird. Dieser *Backup-Endpunkt* stellt eine Verbindung zur NetApp VPC her, in der das Backup zu S3 ausgeführt wird. Wenn Sie ein Volume wiederherstellen, erstellt Cloud Manager einen zusätzlichen Schnittstellen-VPC-Endpunkt – den „*Restore-Endpunkt*“.

Weitere Cloud Volumes ONTAP Systeme in der VPC verwenden diese zwei VPC-Endpunkte.

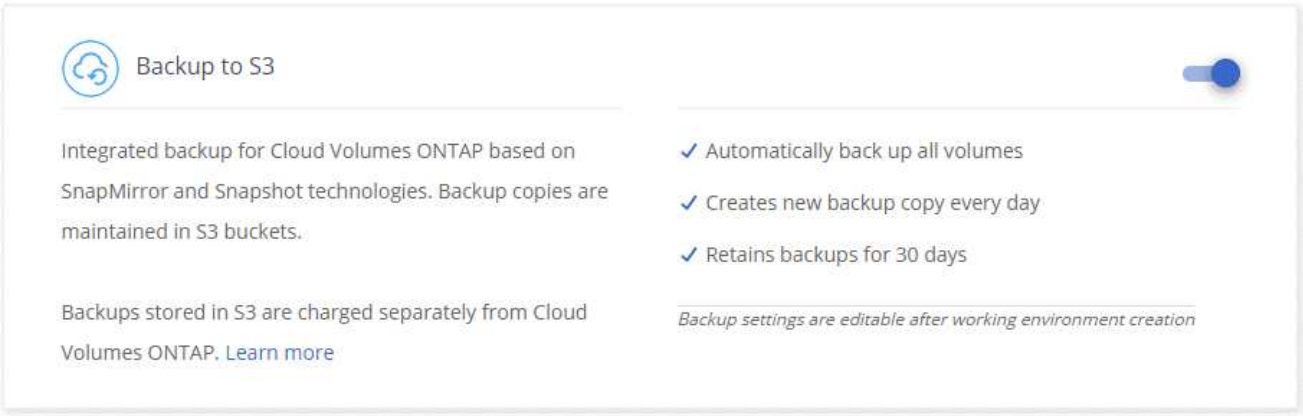
"Das Standardlimit für Interface-VPC-Endpunkte ist 20 pro VPC". Vergewissern Sie sich, dass die VPC nicht das Limit erreicht hat, bevor Sie die Funktion aktivieren.

Aktivieren von Backups in S3 auf einem neuen System

Die Funktion Backup in S3 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 Backup to S3 die Funktion aktiviert, und klicken Sie auf **Weiter**.



5. Führen Sie die Seiten im Assistenten aus, um das System bereitzustellen.

Ergebnis

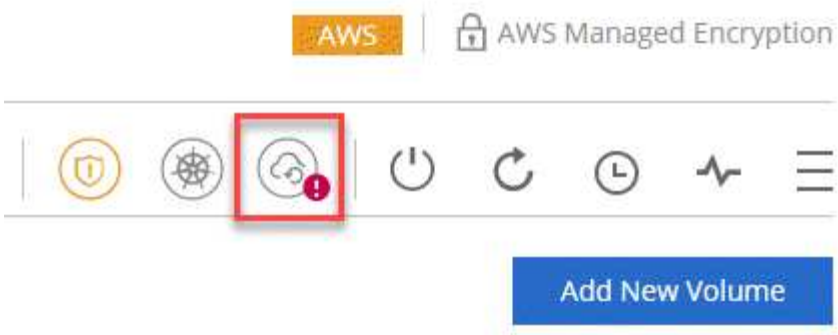
Die Funktion Backup auf S3 ist auf dem System aktiviert und sichert Volumes täglich und speichert 30 Backup-Kopien. Erfahren Sie, wie Sie die Backup-Aufbewahrung ändern können.

Aktivieren von Backups in S3 auf einem vorhandenen System

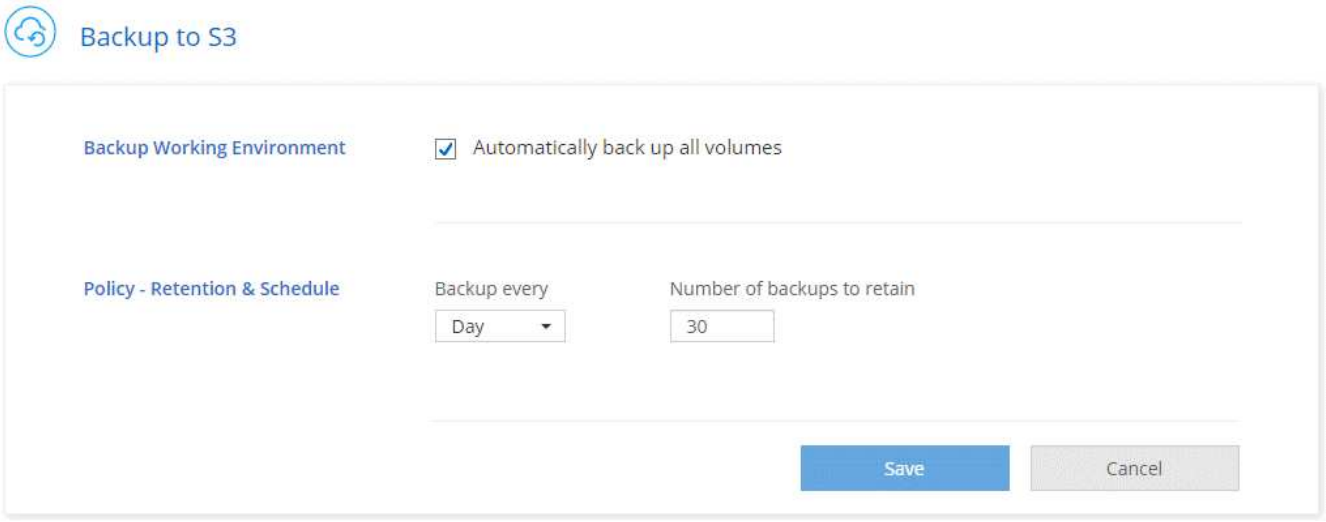
Sie können Backups in S3 auf einem vorhandenen Cloud Volumes ONTAP System aktivieren, solange Sie eine unterstützte Konfiguration ausführen. Weitere Informationen finden Sie unter Anforderungen.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Klicken Sie auf das Symbol Backup-Einstellungen.



3. Wählen Sie **Alle Volumes automatisch sichern**.
4. Wählen Sie Ihre Backup-Aufbewahrung und klicken Sie dann auf **Speichern**.



Ergebnis

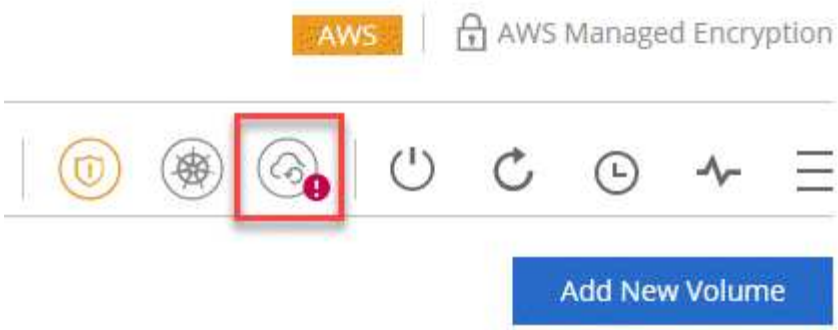
Die Funktion Backup in S3 beginnt mit den ersten Backups jedes Volumes.

Ändern der Backup-Aufbewahrung

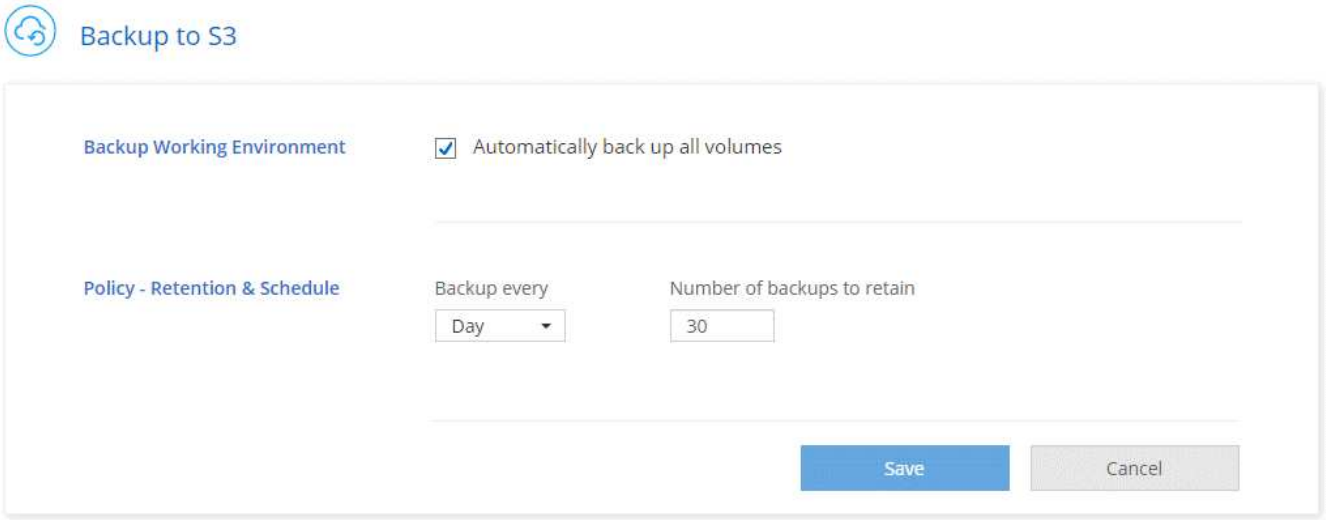
Die Standardrichtlinie sichert Volumes täglich und speichert 30 Backup-Kopien jedes Volumes. Sie können die Anzahl der beizubehaltenden Backup-Kopien ändern.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Klicken Sie auf das Symbol Backup-Einstellungen.



3. Ändern Sie die Backup-Aufbewahrung und klicken Sie dann auf **Speichern**.



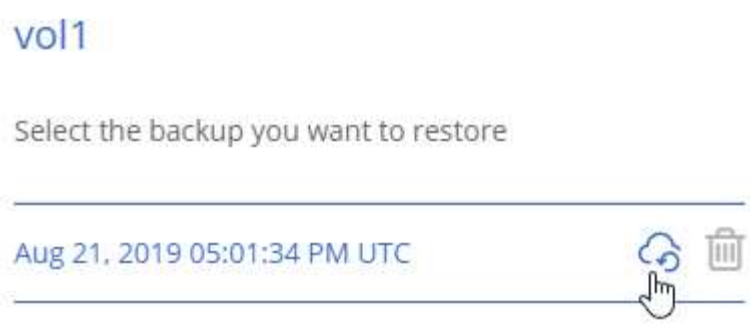
Wiederherstellen eines Volumes

Wenn Sie Daten aus einem Backup wiederherstellen, führt Cloud Manager eine vollständige Volume-Wiederherstellung in einem *neuen* Volume durch. Sie können die Daten in derselben Arbeitsumgebung oder in einer anderen Arbeitsumgebung wiederherstellen.

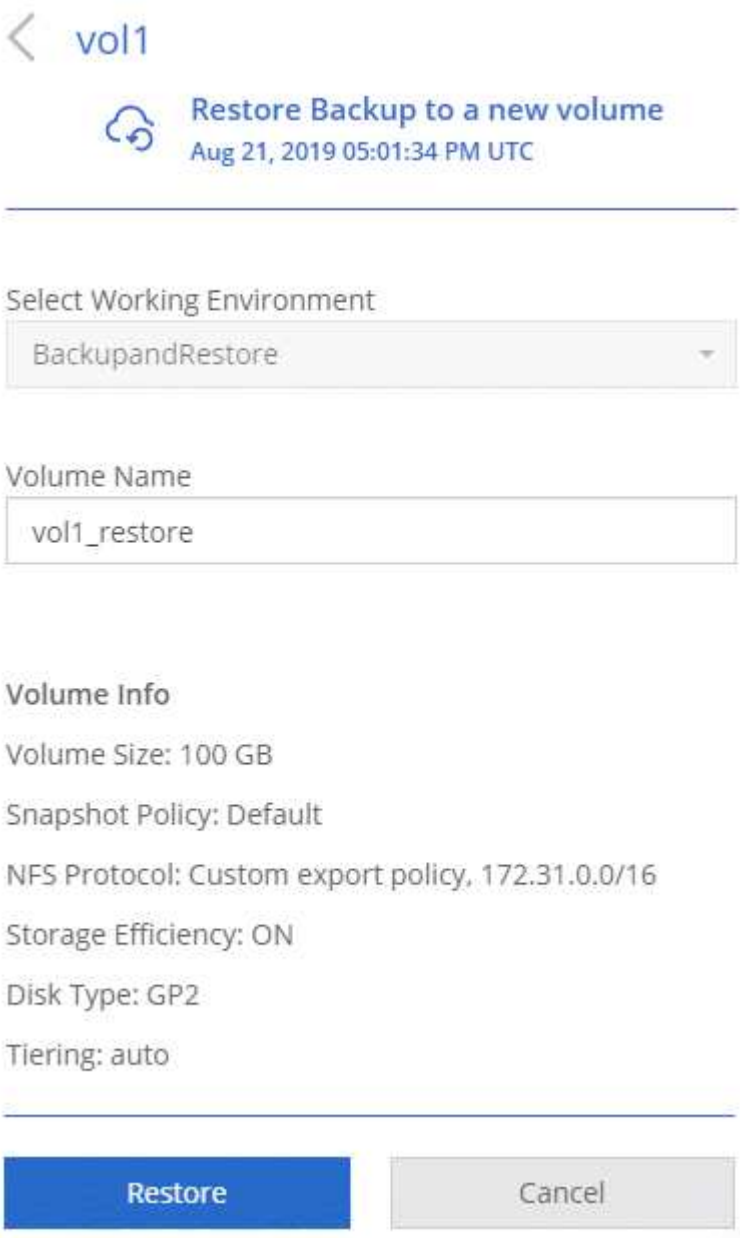
Schritte

1. Klicken Sie oben im Cloud Manager auf **Backup & Restore**.
2. Wählen Sie das Volume aus, das wiederhergestellt werden soll.

3. Suchen Sie das wiederherzustellende Backup, und klicken Sie auf das Wiederherstellungssymbol.



4. Wählen Sie die Arbeitsumgebung aus, in der Sie das Volume wiederherstellen möchten.
5. Geben Sie einen Namen für das Volume ein.
6. Klicken Sie Auf **Wiederherstellen**.

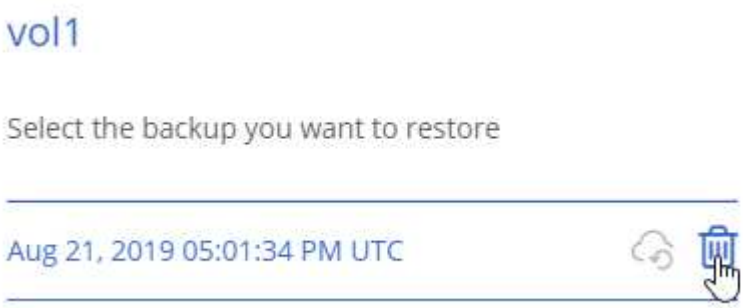


Backups werden gelöscht

Alle Backups werden in S3 aufbewahrt, bis Sie sie aus Cloud Manager löschen. Backups werden nicht gelöscht, wenn Sie ein Volume löschen oder das Cloud Volumes ONTAP-System löschen.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Backup & Restore**.
2. Wählen Sie ein Volume aus.
3. Suchen Sie das zu löschende Backup und klicken Sie auf das Löschsymbol.



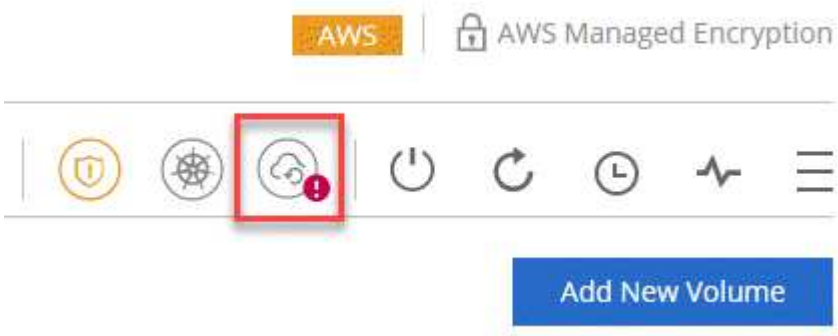
4. Bestätigen Sie, dass Sie das Backup löschen möchten.

Deaktivieren von Backups zu S3

Durch Deaktivieren von Backups an S3 werden Backups von jedem Volume im System deaktiviert. Vorhandene Backups werden nicht gelöscht.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Klicken Sie auf das Symbol Backup-Einstellungen.



3. Deaktivieren Sie **Sichern Sie automatisch alle Volumes** und klicken Sie dann auf **Speichern**.

So funktioniert Backup in S3

In den folgenden Abschnitten finden Sie weitere Informationen zur Funktion „Sichern in S3“.

Speicherort von Backups

Backup-Kopien werden in einem S3 Bucket von NetApp im Besitz von NetApp gespeichert, in derselben Region, in der sich das Cloud Volumes ONTAP System befindet.

Backups erfolgen inkrementell

Nach dem ersten vollständigen Backup Ihrer Daten sind alle weiteren Backups inkrementell, das heißt, dass nur geänderte Blöcke und neue Blöcke gesichert werden.

Backups werden um Mitternacht erstellt

Tägliche Backups beginnen jeden Tag kurz nach Mitternacht. Derzeit können Sie keine Backup-Vorgänge für einen vom Benutzer angegebenen Zeitpunkt planen.

Backup-Kopien sind mit Ihrem Cloud Central Konto verknüpft

Backup-Kopien sind dem zugewiesen "Cloud Central Konto" In der sich Cloud Manager befindet.

Wenn sich mehrere Cloud Manager Systeme im selben Cloud Central Konto befinden, zeigt jedes Cloud Manager System dieselbe Liste von Backups an. Dies schließt die Backups ein, die mit Cloud Volumes ONTAP Instanzen von anderen Cloud Manager Systemen verbunden sind.

Die Backup-Richtlinie gilt für das gesamte System

Die Anzahl der zu behaltenden Backups wird auf Systemebene festgelegt. Sie können keine andere Richtlinie für jedes Volume im System festlegen.

Sicherheit

Backup-Daten werden mit AES-256-Bit-Verschlüsselung im Ruhezustand und TLS 1.2 HTTPS-Verbindungen im Übertragungsprozess gesichert.

Die Daten werden über Direct-Connect-Links an den Service übertragen und im Ruhezustand mittels AES-256-Bit-Verschlüsselung geschützt. Die verschlüsselten Daten werden daraufhin mit HTTPS TLS 1.2-Verbindungen in die Cloud geschrieben. Die Daten werden auch über sichere VPC-Enpunktverbindungen zu Amazon S3 übertragen, sodass kein Traffic über das Internet gesendet wird.

Jedem Benutzer wird ein Mandantenschlüssel zugewiesen, zusätzlich zu einer allgemeinen Verschlüsselung des Service. Diese Anforderung ist vergleichbar mit der Notwendigkeit eines Schlüsselpaars, um einen Kunden sicher in einer Bank zu öffnen. Alle Schlüssel werden als Cloud-Anmeldedaten sicher durch den Service gespeichert und sind auf nur bestimmte NetApp Mitarbeiter beschränkt, die für die Wartung des Service verantwortlich sind.

Einschränkungen

- Wenn Sie einen der folgenden Instanztypen verwenden, kann ein Cloud Volumes ONTAP System maximal 20 Volumes in S3 sichern:
  - m4.xlarge
  - m5.xlarge
  - r4.xlarge
  - r5.xlarge

- Volumes, die außerhalb von Cloud Manager erstellt werden, werden nicht automatisch in S3 gesichert.

  Wenn Sie beispielsweise ein Volume aus der ONTAP CLI, der ONTAP API oder dem System Manager erstellen, wird das Volume nicht automatisch gesichert.

  Wenn Sie diese Volumes sichern möchten, müssen Sie Backup in S3 deaktivieren und dann erneut aktivieren.

- Wenn Sie Daten aus einem Backup wiederherstellen, führt Cloud Manager eine vollständige Volume-Wiederherstellung in einem *neuen* Volume durch. Dieses neue Volume wird nicht automatisch auf S3 gesichert.

  Wenn Sie Volumes sichern möchten, die aus einem Wiederherstellungsvorgang erstellt wurden, müssen Sie Backup in S3 deaktivieren und dann erneut aktivieren.

- Sie können Volumes mit einer Größe von maximal 50 TB sichern.
- Bei einem Backup auf S3 können bis zu 245 Backups eines Volumes insgesamt erstellt werden.
- WORM-Speicher wird auf einem Cloud Volumes ONTAP-System nicht unterstützt, wenn Backup in S3 aktiviert ist.

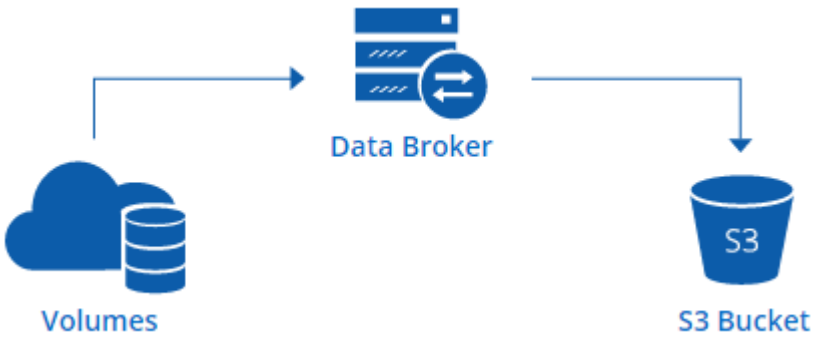
Datensynchronisierung mit Amazon S3

Daten von ONTAP Volumes können durch Integration einer Arbeitsumgebung mit in einen Amazon S3-Bucket synchronisiert werden "NetApp Cloud Sync". Sie können die synchronisierten Daten dann als sekundäre Kopie oder für die Datenverarbeitung mithilfe von AWS-Services wie EMR und Redshift verwenden.

Funktionsweise der Funktion "Sync to S3

Sie können jederzeit eine Arbeitsumgebung mit dem Cloud Sync Service integrieren. Wenn Sie eine Arbeitsumgebung integrieren, synchronisiert der Cloud Sync-Dienst Daten von den ausgewählten Volumes zu einem einzelnen S3-Bucket. Die Integration funktioniert mit Cloud Volumes ONTAP Arbeitsumgebungen sowie ONTAP Clustern, die vor Ort oder Teil einer NetApp Private Storage (NPS) Konfiguration sind.

Um die Daten zu synchronisieren, startet der Service eine Data Brokerinstanz in Ihrem VPC. Cloud Sync verwendet einen Daten-Broker pro Arbeitsumgebung, um Daten von Volumes mit einem S3-Bucket zu synchronisieren. Nach der ersten Synchronisierung synchronisiert der Service alle geänderten Daten einmal täglich um Mitternacht.



Wenn Sie erweiterte Cloud Sync-Aktionen durchführen möchten, rufen Sie den Cloud Sync-Dienst direkt auf.

Von dort aus können Sie Aktionen wie die Synchronisierung von S3 mit einem NFS-Server, die Auswahl verschiedener S3-Buckets für Volumes und das Ändern von Zeitplänen durchführen.

14-Tage-Testversion

Wenn Sie ein neuer Cloud Sync Benutzer sind, sind Ihre ersten 14 Tage kostenlos. Nach Ende der kostenlosen Testversion müssen Sie für jede *Sync-Beziehung* auf Stundenbasis oder durch den Kauf von Lizenzen bezahlen. Jedes Volume, das Sie mit einem S3-Bucket synchronisieren, gilt als Synchronisierungsbeziehung. Sie können beide Zahlungsoptionen direkt über Cloud Sync auf der Seite Lizenzeinstellungen einrichten.

So erhalten Sie Hilfe

Verwenden Sie die folgenden Optionen für jegliche Unterstützung im Zusammenhang mit der Cloud Manager Sync to S3-Funktion oder für Cloud Sync im Allgemeinen:

- Allgemeines Produkt-Feedback: Ng-cloudsync-contact@netapp.com
- Optionen für den technischen Support:
  - NetApp Cloud Sync Communitys
  - In-Product-Chat (unten rechts in Cloud Manager)

Integration einer Arbeitsumgebung in den Cloud Sync Service

Wenn Sie Volumes direkt aus Cloud Manager mit Amazon S3 synchronisieren möchten, müssen Sie die Arbeitsumgebung mit dem Cloud Sync Service integrieren.

[] | *https://img.youtube.com/vi/3hOtLs70_xE/maxresdefault.jpg*

Schritte

1. Öffnen Sie eine Arbeitsumgebung und klicken Sie auf **Sync to S3**.
2. Klicken Sie auf **Sync** und folgen Sie den Anweisungen, um Ihre Daten mit S3 zu synchronisieren.

> Datensicherungsvolumes können nicht mit S3 synchronisiert werden. Die Volumes müssen beschreibbar sein.

Verwalten von Volume-Sync-Beziehungen

Nachdem Sie eine Arbeitsumgebung mit dem Cloud Sync Service integriert haben, können Sie zusätzliche Volumes synchronisieren, die Synchronisierung eines Volumes beenden und die Integration mit Cloud Sync entfernen.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf die Arbeitsumgebung, in der Sie Synchronisierungsbeziehungen verwalten möchten.
2. Wenn Sie die Synchronisierung mit S3 für ein Volume aktivieren oder deaktivieren möchten, wählen Sie das Volume aus und klicken Sie dann auf **Synchronisierung mit S3** oder **Synchronisierungsbeziehung löschen**.
3. Wenn Sie alle Synchronisierungsbeziehungen für eine Arbeitsumgebung löschen möchten, klicken Sie auf die Registerkarte **Sync to S3** und dann auf **Sync löschen**.

   Durch diese Aktion werden synchronisierte Daten nicht aus dem S3-Bucket gelöscht. Wenn der Daten-

Broker nicht in anderen Synchronisierungsbeziehungen verwendet wird, löscht der Cloud Sync-Dienst den Daten-Broker.

Einblicke in den Datenschutz

Erfahren Sie mehr über Cloud Compliance

Cloud Compliance ist ein Datenschutz- und Compliance-Service für Cloud Volumes ONTAP in AWS und Azure. Mithilfe von künstlicher Intelligenz (KI) hilft Cloud Compliance Unternehmen dabei, den Datenkontext zu verstehen und sensible Daten in Cloud Volumes ONTAP Systemen zu ermitteln.

Cloud Compliance ist derzeit als Version für kontrollierte Verfügbarkeit verfügbar.

"Erfahren Sie mehr über Anwendungsfälle für Cloud Compliance".

Funktionen

Cloud Compliance bietet verschiedene Tools, die Sie bei Ihren Compliance-Strategien unterstützen. Cloud Compliance bietet Ihnen:

- Ermitteln von personenbezogenen Daten
- Vielzahl sensibler Daten, je nach DSGVO, CCPA, PCI und HIPAA-Datenschutzvorschriften, identifizieren
- Reagieren Sie auf DSAR (Data Subject Access Requests).

Kosten

Cloud Compliance ist ein Add-on-Service für Cloud Volumes ONTAP, der von NetApp ohne zusätzliche Kosten bereitgestellt wird. Zur Aktivierung von Cloud Compliance muss eine Cloud-Instanz implementiert werden, die von Ihrem Cloud-Provider in Rechnung gestellt wird. Für Datenein- oder -Ausgang sind keine Kosten anfallen, da die Daten nicht außerhalb des Netzwerks fließen.

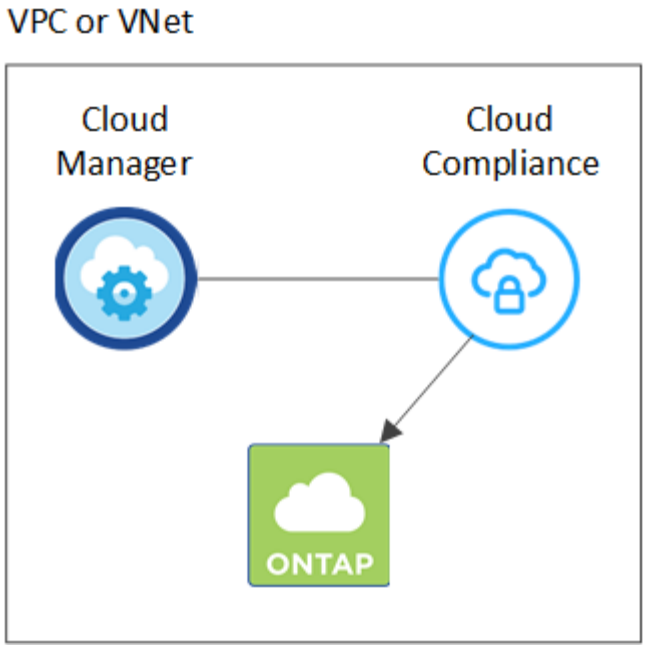
Funktionsweise von Cloud Compliance

Cloud Compliance funktioniert auf hohem Niveau wie folgt:

1. Sie aktivieren Cloud-Compliance auf einem oder mehreren Cloud Volumes ONTAP Systemen.
2. Cloud Compliance scannt die Daten mithilfe eines KI-Learning-Prozesses.
3. In Cloud Manager klicken Sie auf **Compliance** und verwenden Sie das bereitgestellte Dashboard und die Berichterstellungs-Tools, um Sie bei Ihren Compliance-Bemühungen zu unterstützen.

Die Instanz für Cloud Compliance

Wenn Sie Cloud-Compliance auf einem oder mehreren Cloud Volumes ONTAP Systemen aktivieren, implementiert Cloud Manager eine Cloud-Compliance-Instanz in derselben VPC oder vnet wie das erste Cloud Volumes ONTAP-System in der Anforderung.



Beachten Sie Folgendes über die Instanz:

- In Azure wird Cloud Compliance auf einer VM mit Standard_D16s_v3 mit einer Festplatte von 512 GB ausgeführt.
- In AWS wird Cloud-Compliance auf einer m5.4xlarge-Instanz mit einer 500-GB-io1-Festplatte ausgeführt.

  In Regionen, in denen m5.4xlarge nicht verfügbar ist, wird Cloud Compliance stattdessen auf einer m4.4xlarge-Instanz ausgeführt.

- Der Name der Instanz ist *CloudCompliance* mit einem generierten Hash (UUID), der verknüpft ist. Beispiel: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Pro Cloud Manager System wird nur eine Cloud-Compliance-Instanz bereitgestellt.
- Die Upgrades der Cloud Compliance-Software sind automatisiert – Sie müssen sich keine Gedanken darüber machen.

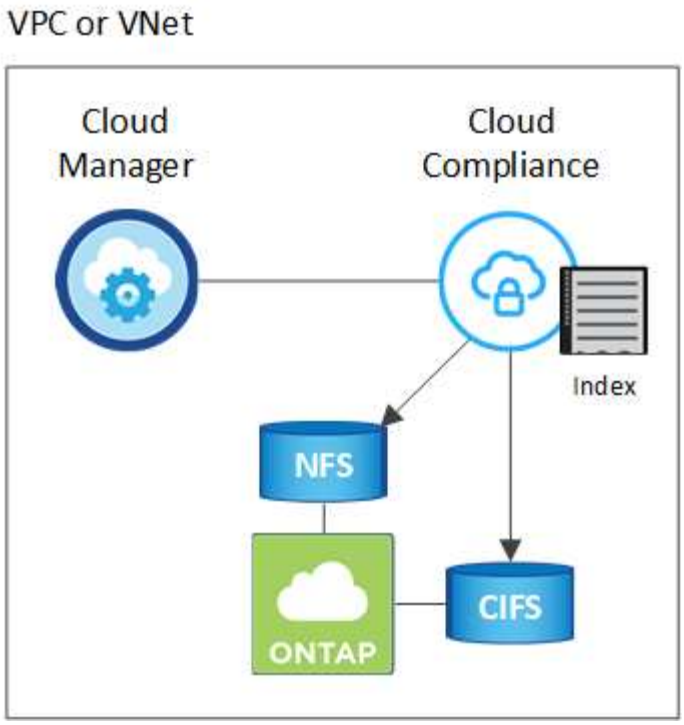
Die Instanz sollte jederzeit ausgeführt werden, da Cloud Compliance die Daten auf Cloud Volumes ONTAP Systemen kontinuierlich scannt.

Funktionsweise von Scans

Nach Aktivierung von Cloud Compliance beginnt die Überprüfung Ihrer Daten sofort, um persönliche und sensible Daten zu identifizieren.

Cloud Compliance stellt durch die Mounten von NFS- und CIFS-Volumes eine Verbindung zu Cloud Volumes ONTAP wie jedem anderen Client her. NFS Volumes werden automatisch als schreibgeschützt abgerufen und müssen zur Überprüfung von CIFS Volumes Active Directory Anmeldeinformationen bereitstellen.

Cloud Compliance scannt die unstrukturierten Daten auf jedem Volume auf eine Reihe von personenbezogenen Daten. Es ordnet Ihre Organisationsdaten zu, kategorisiert jede Datei und identifiziert und extrahiert Entitäten und vordefinierte Muster in den Daten. Das Ergebnis des Scans ist ein Index von persönlichen Daten, sensiblen persönlichen Daten und Datenkategorien.



Nach dem ersten Scan scannt Cloud Compliance jedes Volume kontinuierlich, um inkrementelle Änderungen zu erkennen (deshalb ist es wichtig, die Instanz weiterhin zu betreiben).

Sie können Scans auf der Ebene der Arbeitsumgebung ein- und ausschalten, aber nicht auf der Volumenebene. "Erfahren Sie, wie".

Information, die Cloud Compliance indiziert

Cloud Compliance erfasst, indiziert und weist Kategorien unstrukturierten Daten (Dateien) zu. Cloud Compliance umfasst folgende Daten:

Standard-Metadaten

Cloud Compliance sammelt Standard-Metadaten zu Dateien: Dateityp, Größe, Erstellung, Änderung usw.

Persönliche Daten

Personenbezogene Informationen wie E-Mail-Adressen, Identifikationsnummern oder Kreditkartennummern. "Weitere Informationen zu personenbezogenen Daten".

Sensible persönliche Daten

Besondere Arten sensibler Daten, wie etwa Gesundheitsdaten, ethnische Herkunft oder politische Ansichten, wie in der DSGVO und anderen Datenschutzvorschriften definiert "Erfahren Sie mehr über sensible persönliche Daten".

Kategorien

Bei Cloud Compliance werden die gescannten Daten in verschiedene Kategorien unterteilt. Kategorien sind Themen, die auf der KI-Analyse des Inhalts und der Metadaten jeder Datei basieren. "Weitere Informationen zu Kategorien".

Name der Entität Anerkennung

Cloud Compliance nutzt KI, um Namen natürlicher Personen aus Dokumenten zu extrahieren. "Informieren Sie sich über die Reaktion auf Zugriffsanfragen von Betroffenen".

Netzwerkübersicht

Cloud Manager implementiert die Cloud Compliance-Instanz mit einer privaten IP-Adresse und einer Sicherheitsgruppe, die eingehende HTTP-Verbindungen von Cloud Manager ermöglicht. Über diese Verbindung können Sie über die Cloud Manager-Schnittstelle auf das Cloud Compliance Dashboard zugreifen.

Ausgehende Regeln sind vollständig geöffnet. Die Instanz stellt über einen Proxy von Cloud Manager eine Verbindung zu Cloud Volumes ONTAP-Systemen und mit dem Internet her. Zum Upgrade der Cloud Compliance-Software und zum Senden von Nutzungsmetriken ist ein Internetzugang erforderlich.

Wenn Sie strenge Netzwerkanforderungen erfüllen, "Informationen zu den Endpunkten, die Cloud Compliance kontaktiert".

Die indizierten Daten verlassen niemals die Cloud Compliance-Instanz – die Daten werden nicht außerhalb Ihres virtuellen Netzwerks übertragen und werden nicht an Cloud Manager gesendet.

Zugriff des Benutzers auf Compliance-Informationen

Cloud Manager Administratoren können Compliance-Informationen für alle Arbeitsumgebungen anzeigen.

Workspace-Administratoren können Compliance-Informationen nur für Systeme anzeigen, auf die sie Zugriff haben. Wenn ein Workspace-Administrator nicht auf eine Arbeitsumgebung in Cloud Manager zugreifen kann, werden auf der Registerkarte Compliance keine Compliance-Informationen für die Arbeitsumgebung angezeigt.

"Erfahren Sie mehr über die Rollen von Cloud Manager".

Erste Schritte mit Cloud Compliance für Cloud Volumes ONTAP

Schritte für den Einstieg in Cloud Compliance for Cloud Volumes ONTAP in AWS oder Azure

Schnellstart

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

Vergewissern Sie sich, dass Ihre Konfiguration den Anforderungen entspricht

- Stellen Sie sicher, dass die Cloud-Compliance-Instanz über Outbound-Internetzugang verfügt.

  Cloud Manager implementiert die Instanz in derselben VPC oder vnet wie das erste Cloud Volumes ONTAP System in der Anforderung.

- Sicherstellen, dass Benutzer von einem Host mit direkter Verbindung zu AWS oder Azure auf die Cloud Manager Schnittstelle zugreifen können, oder von einem Host, der sich im gleichen Netzwerk befindet wie die Cloud Compliance Instanz (die Instanz hat eine private IP-Adresse).
- Stellen Sie sicher, dass die Cloud Compliance-Instanz ausgeführt wird.

Aktivierung von Cloud Compliance für Cloud Volumes ONTAP

- Neue Arbeitsumgebungen: Stellen Sie sicher, dass Cloud Compliance aktiviert ist, wenn Sie die Arbeitsumgebung erstellen (es ist standardmäßig aktiviert).
- Bestehende Arbeitsumgebungen: Klicken Sie auf **Compliance**, bearbeiten Sie optional die Liste der Arbeitsumgebungen und klicken Sie auf **Compliance Dashboard anzeigen**.

Zugriff auf Volumes sicherstellen

Jetzt, wo Cloud Compliance aktiviert ist, stellen Sie sicher, dass die IT auf Volumes zugreifen kann.

- Die Cloud Compliance Instanz benötigt eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP Subnetz.
- Sicherheitsgruppen für Cloud Volumes ONTAP müssen eingehende Verbindungen aus der Cloud-Compliance-Instanz zulassen.
- Die NFS Volume-Exportrichtlinien müssen den Zugriff aus der Cloud Compliance-Instanz zulassen.
- Cloud Compliance benötigt Active Directory-Anmeldeinformationen zum Scannen von CIFS Volumes.

  Klicken Sie auf **Compliance** > **CIFS-Scanstatus** > **CIFS-Anmeldeinformationen bearbeiten** und geben Sie die Anmeldeinformationen an. Die Anmeldedaten können schreibgeschützt sein. Durch Admin-Berechtigungen wird jedoch sichergestellt, dass Cloud Compliance Daten lesen kann, die erhöhte Berechtigungen erfordern.

Stellen Sie die Verbindung zwischen Cloud Manager und Cloud Compliance sicher

- Die Sicherheitsgruppe für Cloud Manager muss ein- und ausgehenden Traffic über Port 80 zu und von der Cloud Compliance-Instanz ermöglichen.
- Wenn Ihr AWS-Netzwerk keine NAT oder Proxy für den Internet-Zugriff verwendet, muss die Sicherheitsgruppe für Cloud Manager eingehenden Datenverkehr über TCP-Port 3128 von der Cloud-Compliance-Instanz zulassen.

Voraussetzungen prüfen

Die folgenden Voraussetzungen prüfen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie Cloud Compliance aktivieren. Nach Aktivierung von Cloud Compliance müssen Sie die Konnektivität zwischen Komponenten sicherstellen. Darauf sind wir unten eingegangen.

Aktivieren Sie den Outbound-Internetzugang

Cloud Compliance erfordert Outbound-Internetzugang. Wenn Ihr virtuelles Netzwerk einen Proxyserver für den Internetzugriff verwendet, stellen Sie sicher, dass die Cloud Compliance-Instanz über einen ausgehenden Internetzugriff verfügt, um die folgenden Endpunkte zu kontaktieren:

Endpunkte	Zweck
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://cloud-compliance-support-netapp.s3.us-west-1.amazonaws.com https://hub.docker.com	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Cloud Compliance ermöglicht es, auf Manifeste und Vorlagen zuzugreifen und diese herunterzuladen sowie Protokolle und Kennzahlen zu senden.

Überprüfen Sie die Verbindung des Webbrowsers zur Cloud-Compliance

Die Cloud Compliance Instanz verwendet eine private IP-Adresse, um sicherzustellen, dass die indizierten Daten nicht für das Internet verfügbar sind. Daher muss der Webbrowser, den Sie für den Zugriff auf Cloud Manager verwenden, über eine Verbindung zu dieser privaten IP-Adresse verfügen. Die Verbindung kann über eine direkte Verbindung zu AWS oder Azure (z. B. ein VPN) oder von einem Host im selben Netzwerk wie die Cloud-Compliance-Instanz hergestellt werden.

Wenn Sie Cloud Manager von einer öffentlichen IP-Adresse aus aufrufen, wird Ihr Webbrowser vermutlich nicht auf einem Host im Netzwerk ausgeführt.

Ausführung von Cloud-Compliance

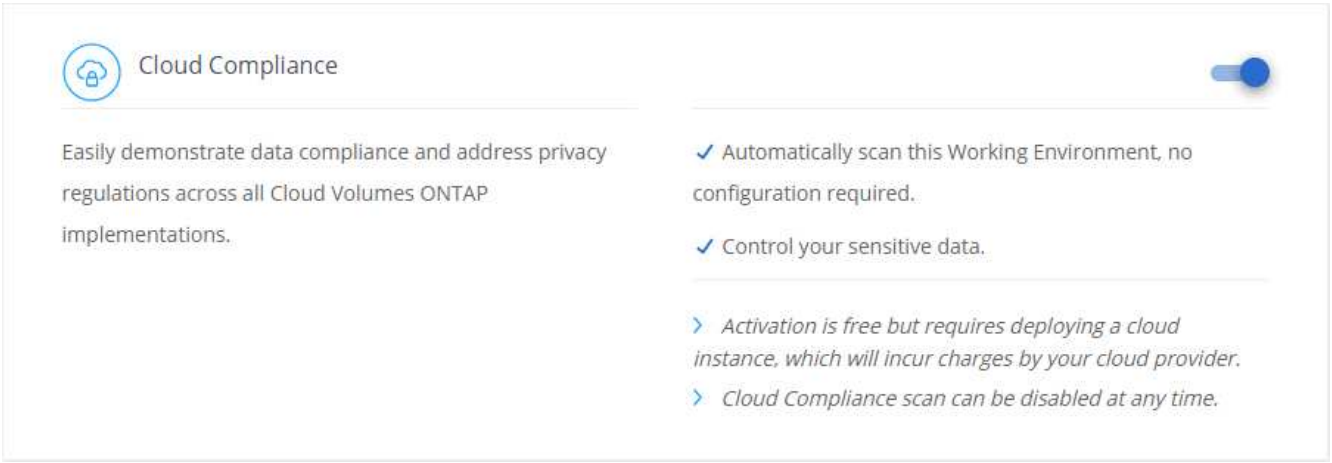
Die Cloud Compliance Instanz muss stets zum kontinuierlichen Scannen Ihrer Daten verfügbar sein.

Ermöglichung von Cloud-Compliance in einer neuen Arbeitsumgebung

Cloud Compliance ist im Assistenten für die Arbeitsumgebung standardmäßig aktiviert. Achten Sie darauf, dass die Option aktiviert bleibt.

Schritte

1. Klicken Sie auf **Cloud Volumes ONTAP erstellen**.
2. Wählen Sie Amazon Web Services oder Microsoft Azure 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 Services die Option Cloud Compliance aktiviert, und klicken Sie auf **Weiter**.



5. Führen Sie die Seiten im Assistenten aus, um das System bereitzustellen.

   Hilfe finden Sie unter "Starten von Cloud Volumes ONTAP in AWS" Und "Starten von Cloud Volumes ONTAP in Azure".

Ergebnis

Cloud Compliance ist auf dem Cloud Volumes ONTAP System aktiviert. Wenn Sie Cloud-Compliance zum ersten Mal aktiviert haben, implementiert Cloud Manager die Instanz zur Cloud-Compliance bei Ihrem Cloud-Provider. Sobald die Instanz verfügbar ist, beginnt sie mit dem Scannen der Daten, während sie auf jedes von Ihnen erstellte Volume geschrieben werden.

Aktivierung von Cloud Compliance für vorhandene Arbeitsumgebungen

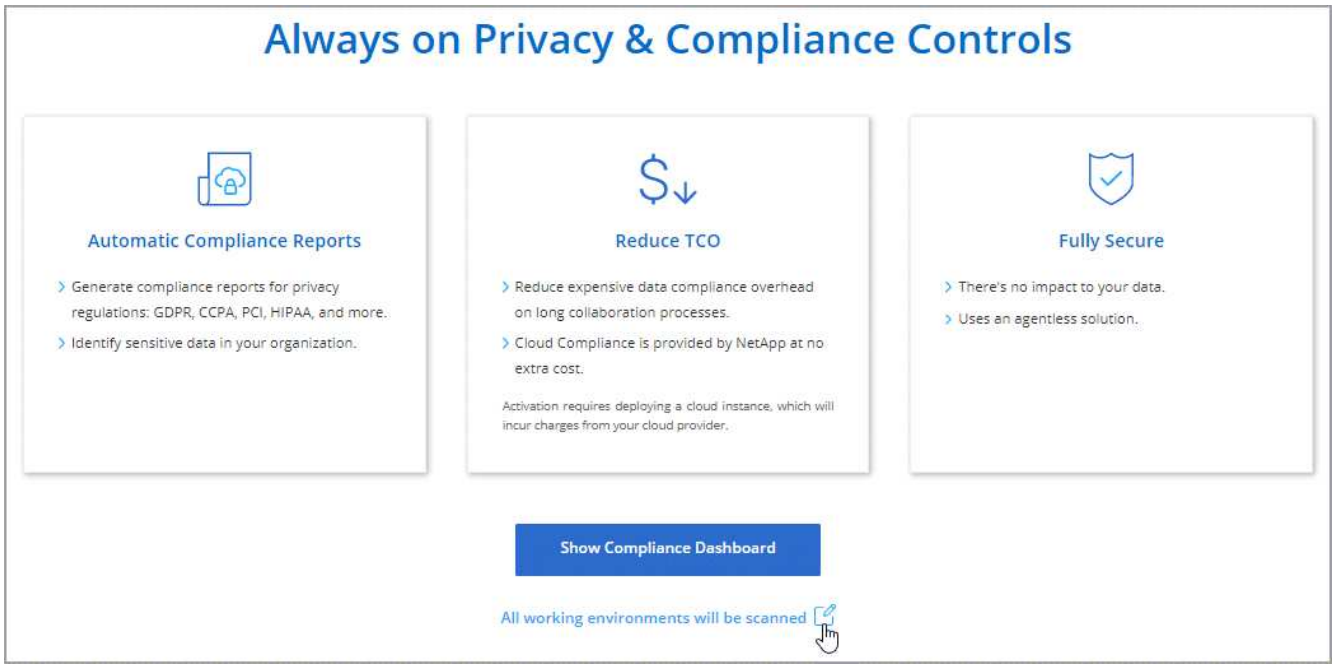
Aktivieren Sie Cloud-Compliance auf Ihren vorhandenen Cloud Volumes ONTAP Systemen über die Registerkarte **Compliance** in Cloud Manager.

Eine weitere Option ist die Aktivierung von Cloud Compliance auf der Registerkarte **Arbeitsumgebungen** durch die individuelle Auswahl der einzelnen Arbeitsumgebungen. Das dauert länger, bis Sie nur ein System haben.

Schritte für mehrere Arbeitsumgebungen

1. Klicken Sie oben im Cloud Manager auf **Compliance**.
2. Wenn Sie Cloud Compliance in bestimmten Arbeitsumgebungen aktivieren möchten, klicken Sie auf das Bearbeiten-Symbol.

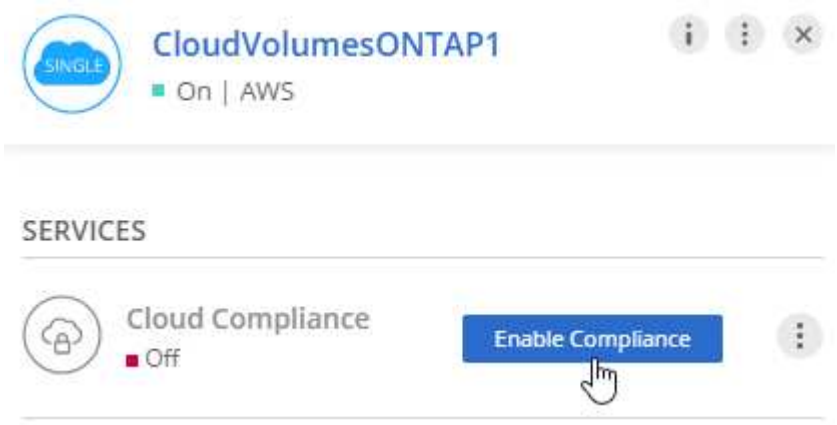
   Andernfalls ist Cloud Manager auf die Aktivierung von Cloud Compliance für alle Arbeitsumgebungen eingestellt, auf die Sie Zugriff haben.



3. Klicken Sie Auf **Compliance Dashboard Anzeigen**.

Schritte für eine einzelne Arbeitsumgebung

1. Klicken Sie oben im Cloud Manager auf **Arbeitsumgebungen**.
2. Wählen Sie eine Arbeitsumgebung aus.
3. Klicken Sie im rechten Fensterbereich auf **Compliance aktivieren**.



Ergebnis

Wenn Sie Cloud-Compliance zum ersten Mal aktiviert haben, implementiert Cloud Manager die Instanz zur Cloud-Compliance bei Ihrem Cloud-Provider.

Cloud Compliance beginnt mit der Überprüfung der Daten in den einzelnen Arbeitsumgebungen. Sobald Cloud Compliance die ersten Scans abgeschlossen hat, stehen die Daten im Compliance-Dashboard zur Verfügung. Die Dauer, die von der Datenmenge abhängt, kann ein paar Minuten oder Stunden betragen.

Es wird sichergestellt, dass Cloud Compliance Zugriff auf Volumes hat

Stellen Sie sicher, dass Cloud Compliance auf Volumes auf Cloud Volumes ONTAP zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen und Exportrichtlinien prüfen. Cloud Compliance muss über CIFS-

Anmeldedaten bereitgestellt werden, damit der Zugriff auf CIFS Volumes möglich ist.

Schritte

1. Stellen Sie sicher, dass eine Netzwerkverbindung zwischen der Cloud Compliance-Instanz und jedem Cloud Volumes ONTAP-Subnetz besteht.

   Cloud Manager implementiert die Cloud Compliance-Instanz in derselben VPC oder vnet wie das erste Cloud Volumes ONTAP-System der Anforderung. Dieser Schritt ist also wichtig, wenn sich einige Cloud Volumes ONTAP Systeme in unterschiedlichen Subnetzen oder virtuellen Netzwerken befinden.

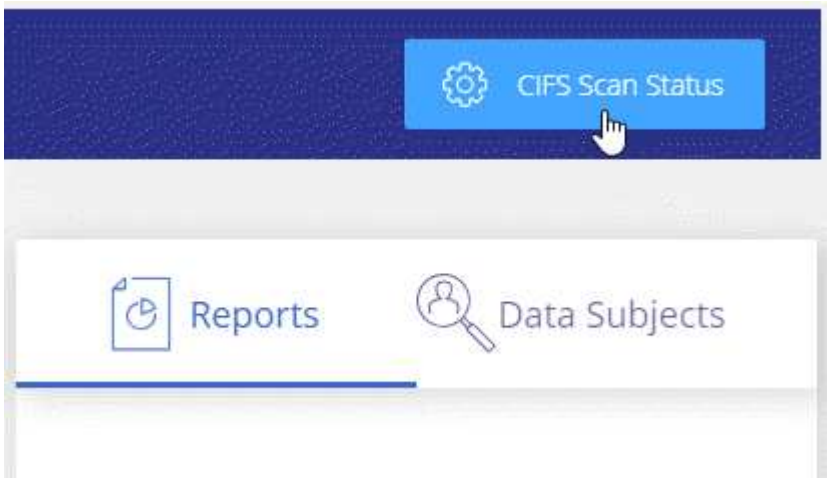
2. Stellen Sie sicher, dass die Sicherheitsgruppe für Cloud Volumes ONTAP eingehenden Datenverkehr aus der Cloud-Compliance-Instanz zulässt.

   Sie können entweder die Sicherheitsgruppe für den Datenverkehr von der IP-Adresse der Cloud Compliance-Instanz öffnen oder die Sicherheitsgruppe für den gesamten Datenverkehr im virtuellen Netzwerk öffnen.

3. Vergewissern Sie sich, dass die NFS-Volume-Exportrichtlinien die IP-Adresse der Cloud Compliance-Instanz enthalten, damit sie auf die Daten der einzelnen Volumes zugreifen können.
4. Wenn Sie CIFS verwenden, geben Sie Cloud Compliance mit Active Directory Anmeldedaten ein, damit CIFS Volumes gescannt werden können.

   a. Klicken Sie oben im Cloud Manager auf **Compliance**.

   b. Klicken Sie oben rechts auf **CIFS-Scanstatus**.



   c. Klicken Sie für jedes Cloud Volumes ONTAP-System auf **CIFS-Anmeldeinformationen bearbeiten** und geben Sie den Benutzernamen und das Kennwort ein, die Cloud-Compliance für den Zugriff auf CIFS-Volumes auf dem System benötigt.

      Die Anmeldedaten können schreibgeschützt sein. Durch Admin-Berechtigungen wird jedoch sichergestellt, dass Cloud Compliance Daten lesen kann, die erhöhte Berechtigungen benötigen. Die Anmeldedaten werden in der Instanz Cloud Compliance gespeichert.

      Nach Eingabe der Anmeldedaten sollte eine Meldung angezeigt werden, dass alle CIFS-Volumes erfolgreich authentifiziert wurden.

Sicherstellen, dass Cloud Manager auf Cloud Compliance zugreifen kann

Stellen Sie die Verbindung zwischen Cloud Manager und Cloud Compliance sicher, damit Sie die Compliance-Einblicke sehen können, die Sie in Cloud Compliance erhalten.

Schritte

1. Stellen Sie sicher, dass die Sicherheitsgruppe für Cloud Manager ein- und ausgehenden Datenverkehr über Port 80 zu und von der Cloud Compliance-Instanz ermöglicht.

   Über diese Verbindung können Sie Informationen auf der Registerkarte Compliance anzeigen.

2. Wenn Ihr AWS-Netzwerk keine NAT oder Proxy für den Internet-Zugriff verwendet, ändern Sie die Sicherheitsgruppe für Cloud Manager, um eingehenden Datenverkehr über TCP-Port 3128 von der Cloud Compliance-Instanz zu ermöglichen.

   Dies ist erforderlich, da die Cloud Compliance Instanz Cloud Manager als Proxy für den Zugriff auf das Internet verwendet.

   Dieser Port ist standardmäßig auf allen neuen Cloud Manager Instanzen geöffnet, beginnend mit Version 3.7.5. Für Cloud Manager Instanzen, die vor dieser Version erstellt wurden, ist dies nicht geöffnet.

Mehr Transparenz und Kontrolle über private Daten

Mehr Kontrolle über Ihre persönlichen Daten durch die Anzeige von Details zu den personenbezogenen Daten und vertraulichen personenbezogenen Daten in Ihrem Unternehmen. Auch die Kategorien und Dateitypen, die Cloud Compliance in Ihren Daten enthalten ist, können für Sie transparent dargestellt werden.

Persönliche Daten

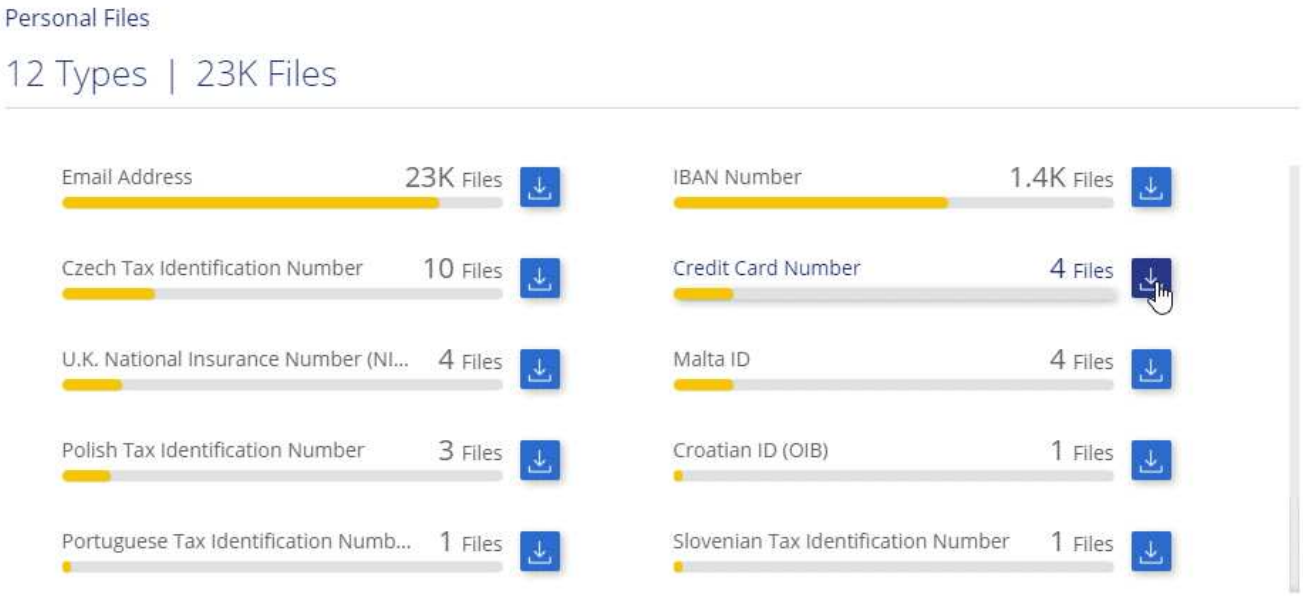
Cloud Compliance identifiziert automatisch bestimmte Wörter, Strings und Muster (Regex) in den Daten. Beispielsweise personenbezogene Daten (Personal Identification Information, PII), Kreditkartennummern, Sozialversicherungsnummern und Kontonummern. Die vollständige Liste finden Sie hier.

Für einige Arten von personenbezogenen Daten verwendet Cloud Compliance die *Proximity-Validierung*, um die Ergebnisse zu validieren. Die Validierung erfolgt, indem ein oder mehrere vordefinierte Schlüsselwörter in der Nähe der gefundenen personenbezogenen Daten gesucht werden. Cloud Compliance identifiziert z. B. eine US-amerikanische Sozialversicherungsnummer (SSN) als SSN, wenn sie neben ihr ein Näherungswort sieht - zum Beispiel *SSN* oder *Sozialversicherung*. Die Liste unten Zeigt an, wann Cloud Compliance die Näherungsüberprüfung verwendet.

Anzeigen von Dateien mit persönlichen Daten

Schritte

1. Klicken Sie oben im Cloud Manager auf **Compliance**.
2. Laden Sie die Details zu einem der beiden wichtigsten Dateitypen direkt vom Hauptbildschirm herunter, oder klicken Sie auf **Alle anzeigen** und laden Sie dann die Liste für alle gefundenen persönlichen Datentypen herunter.



Arten personenbezogener Daten

Die in Dateien gefundenen personenbezogenen Daten können allgemeine personenbezogene Daten oder nationale Kennungen sein. In der dritten Spalte wird angegeben, ob Cloud Compliance verwendet wird Prüfung der Nähe Zum Validieren seiner Ergebnisse für die Kennung.

Typ	Kennung	Näherungsvalidierung?
Allgemein	E-Mail-Adresse	Nein
	Kreditkartennummer	Nein
	IBAN-Nummer (International Bank Account Number)	Nein
	IP-Adresse	Ja.

Typ	Kennung	Näherungsvalidierung?
Nationale Kennungen	Belgischer Ausweis (Numero National)	Ja.
	Bulgarische ID (einheitliche Zivilnummer)	Ja.
	Zypern Steuernummer (TIC)	Ja.
	Dänische Steuernummer (HLW)	Ja.
	Estnische ID (Isikukood)	Ja.
	Finnische ID (Henkilötunnus)	Ja.
	Französische Steuernummer (SPI)	Ja.
	Steuernummer (Steuerliche Identifikationsnummer)	Ja.
	Ungarische Steuernummer (Adóazonosító jel)	Ja.
	Irish ID (PPS)	Ja.
	Israelische ID	Ja.
	Italienische ID (Codice Fisscale)	Ja.
	Lettische Steuernummer	Ja.
	Litauische ID (Asmens kodas)	Ja.
	Luxemburg-ID	Ja.
	Malta ID	Ja.
	Niederlande ID (BSN)	Ja.
	Polish Tax Identification Number	Ja.
	Portugiesische Steuernummer (NIF)	Ja.
	Rumänische Steuernummer	Ja.
	Slowakische Steuernummer	Ja.
	Slowenische Steuernummer	Ja.
	Südafrikanischer Ausweis	Ja.
	Spanische Steuernummer	Ja.
	Schwedische Steuernummer	Ja.
	GROSSBRITANNIEN Staatsversicherungsnummer (NINO)	Ja.
	USA Sozialversicherungsnummer (SSN)	Ja.

Sensible persönliche Daten

Cloud Compliance identifiziert automatisch spezielle Arten von sensiblen personenbezogenen Daten, wie sie in Datenschutzvorschriften wie z. B. definiert sind "Artikel 9 und 10 der DSGVO". Beispielsweise Informationen über die Gesundheit einer Person, ethnische Herkunft oder sexuelle Orientierung. Die vollständige Liste finden Sie hier.

Cloud Compliance verwendet künstliche Intelligenz (KI), NLP (Natural Language Processing), maschinelles

Lernen (ML) und Cognitive Computing (CC), um die Bedeutung des von ihm gescannten Inhalts zu verstehen, um Entitäten zu extrahieren und entsprechend zu kategorisieren.

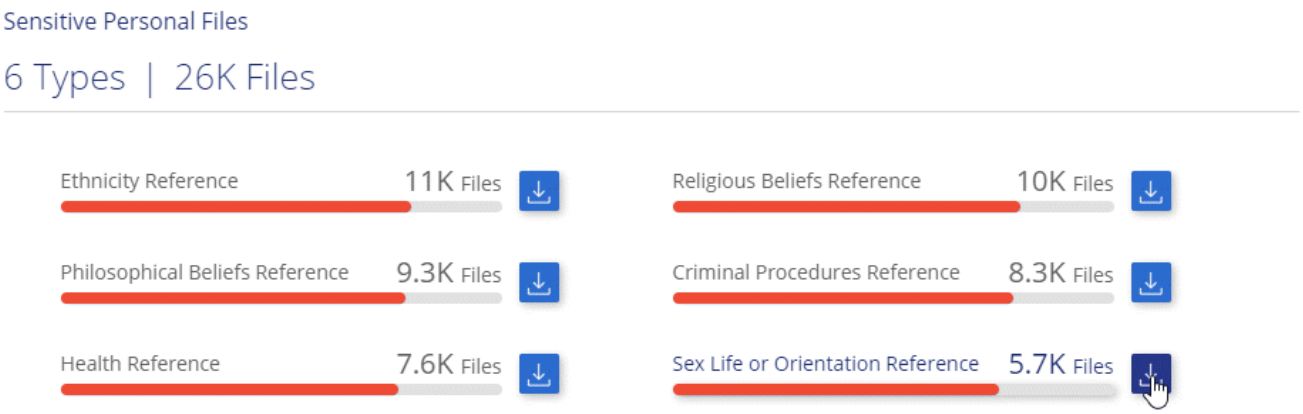
Beispielsweise ist eine sensitive DSGVO-Datenkategorie ethnisch Ursprungs. Aufgrund seiner NLP-Fähigkeiten kann Cloud Compliance den Unterschied zwischen einem Satz unterscheiden, der "George ist mexikanisch" (was auf sensible Daten wie in Artikel 9 der DSGVO angegeben), und "George isst mexikanisches Essen".

Nur Englisch wird beim Scannen sensibler personenbezogener Daten unterstützt. Support für weitere Sprachen wird später hinzugefügt.

Anzeigen von Dateien mit vertraulichen persönlichen Daten

Schritte

1. Klicken Sie oben im Cloud Manager auf **Compliance**.
2. Laden Sie die Details zu einem der beiden wichtigsten Dateitypen direkt vom Hauptbildschirm herunter, oder klicken Sie auf **Alle anzeigen** und laden Sie dann die Liste für alle gefundenen sensiblen personenbezogenen Datentypen herunter.



Arten sensibler personenbezogener Daten

Folgende sensible personenbezogene Daten, die Cloud Compliance in Dateien finden kann:

Referenz Für Kriminelle Verfahren
Daten zu strafrechtlichen Überzeugungen und Straftaten einer natürlichen Person.

Ethnische Referenz
Daten über die rassische oder ethnische Herkunft einer natürlichen Person.

Systemzustand
Daten über die Gesundheit einer natürlichen Person.

Philosophische Überzeugungen Referenz
Daten über die philosophischen Überzeugungen einer natürlichen Person.

Religiöse Überzeugungen Referenz
Daten über die religiösen Überzeugungen einer natürlichen Person.

Sexualleben oder Orientierung Referenz

Daten über das Sexualleben einer natürlichen Person oder die sexuelle Orientierung.

Kategorien

Bei Cloud Compliance werden die gescannten Daten in verschiedene Kategorien unterteilt. Kategorien sind Themen, die auf der KI-Analyse des Inhalts und der Metadaten jeder Datei basieren. Siehe die Liste der Kategorien.

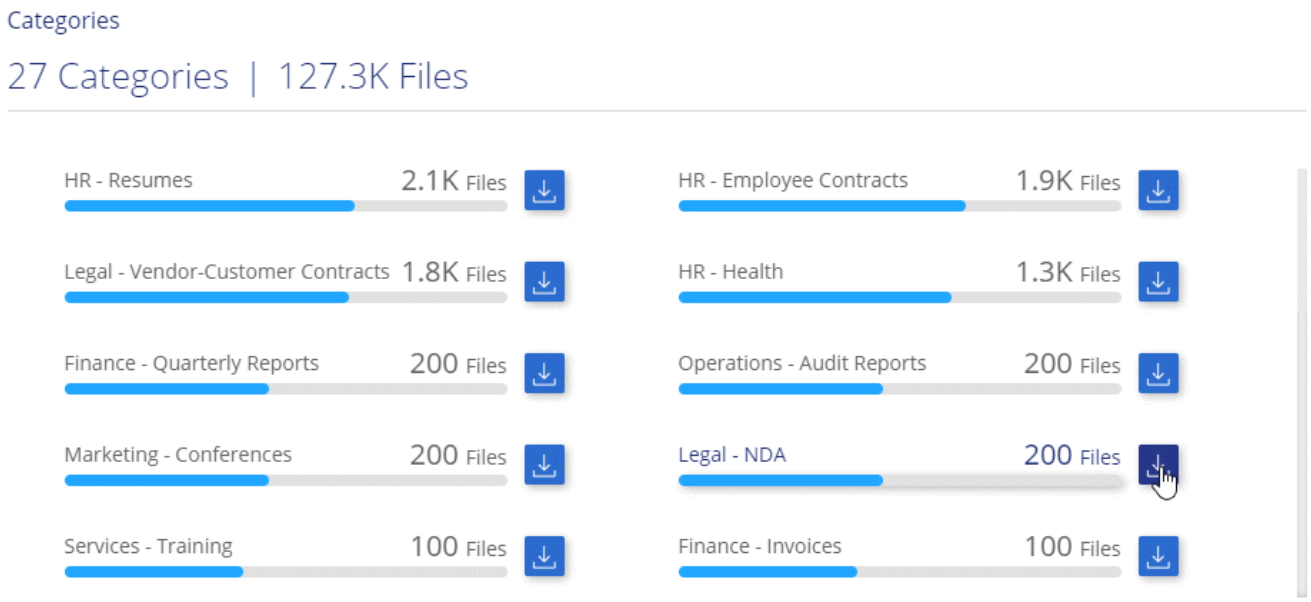
Kategorien können Ihnen dabei helfen zu verstehen, was mit Ihren Daten passiert, indem Sie die Art der Informationen anzeigen, die Sie haben. Beispielsweise kann eine Kategorie wie Lebensläufe oder Mitarbeiterverträge sensible Daten enthalten. Beim Herunterladen des CSV-Berichts können Sie feststellen, dass Mitarbeiterverträge an einem nicht sicheren Ort gespeichert sind. Sie können das Problem dann beheben.

Nur Englisch wird für Kategorien unterstützt. Support für weitere Sprachen wird später hinzugefügt.

Anzeigen von Dateien nach Kategorien

Schritte

1. Klicken Sie oben im Cloud Manager auf **Compliance**.
2. Laden Sie die Details für einen der 4 besten Dateitypen direkt vom Hauptbildschirm herunter, oder klicken Sie auf **Alle anzeigen** und laden Sie dann die Liste für eine der Kategorien herunter.



Arten von Kategorien

Cloud Compliance kategorisiert Ihre Daten wie folgt:

Finanzen

- Bilanz
- Bestellungen

- Rechnungen
- Vierteljährliche Berichte

HR

- Hintergrundprüfung
- Vergütungspläne
- Mitarbeiterverträge
- Mitarbeiterüberprüfung
- Systemzustand
- Wird Fortgesetzt

Legal

- NDA
- Verträge zwischen Anbietern und Kunden

Marketing

- Kampagnen
- Konferenzen

Betrieb

- Audit-Berichte

Vertrieb

- Aufträge

Services

- RFI
- AUSSCHREIBUNG
- Schulung

Unterstützung

- Reklamationen und Tickets

Andere

- Archivdateien
- Audio
- CAD-Dateien
- Codieren
- Ausführbare Dateien
- Bilder

Dateitypen

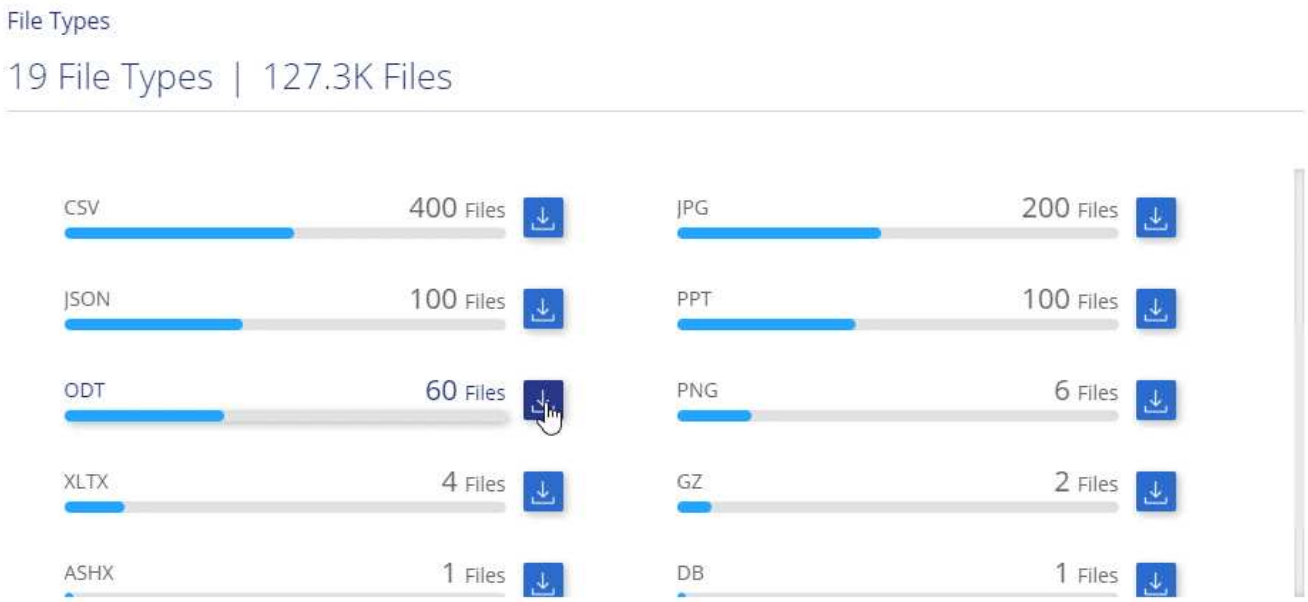
Cloud Compliance greift die gescannten Daten auf und legt sie nach Dateityp fest. Cloud Compliance kann alle Dateitypen anzeigen, die in den Scans gefunden werden.

Die Überprüfung Ihrer Dateitypen kann Ihnen helfen, Ihre sensiblen Daten zu kontrollieren, da Sie möglicherweise feststellen können, dass bestimmte Dateitypen nicht richtig gespeichert sind. Sie können beispielsweise CAD-Dateien speichern, die sehr sensible Informationen über Ihr Unternehmen enthalten. Wenn diese nicht gesichert sind, können Sie die Kontrolle über vertrauliche Daten übernehmen, indem Sie Berechtigungen beschränken oder Dateien an einen anderen Speicherort verschieben.

Anzeigen von Dateitypen

Schritte

1. Klicken Sie oben im Cloud Manager auf **Compliance**.
2. Laden Sie die Details für einen der 4 besten Dateitypen direkt vom Hauptbildschirm herunter, oder klicken Sie auf **Alle anzeigen** und laden Sie dann die Liste für einen beliebigen Dateityp herunter.



Genauigkeit der gefundenen Informationen

NetApp kann keine Garantie für 100 % Genauigkeit der persönlichen Daten und für sensible personenbezogene Daten, die Cloud Compliance identifiziert hat, geben. Überprüfen Sie die Informationen immer, indem Sie die Daten überprüfen.

Auf der Grundlage unserer Tests zeigt die folgende Tabelle die Richtigkeit der Informationen, die Cloud Compliance findet. Wir brechen es durch *Precision* und *Recall* ab:

Präzision

Die Wahrscheinlichkeit, dass das, was Cloud Compliance findet, korrekt identifiziert wurde. Beispielsweise bedeutet eine Datengenauigkeit von 90% für personenbezogene Daten, dass 9 von 10 Dateien, die als personenbezogene Daten identifiziert werden, tatsächlich personenbezogene Daten enthalten. 1 von 10 Dateien wäre falsch positiv.

Rückruf

Die Wahrscheinlichkeit, dass Cloud Compliance die entsprechenden Daten findet Beispielsweise bedeutet eine Rückrufquote von 70 % für personenbezogene Daten, dass Cloud Compliance 7 von 10 Dateien identifizieren kann, die tatsächlich personenbezogene Daten in Ihrem Unternehmen enthalten. Cloud Compliance würde 30% der Daten vermissen und wird nicht im Dashboard erscheinen.

Cloud Compliance gibt es in einer Version mit kontrollierter Verfügbarkeit und wir verbessern kontinuierlich die Genauigkeit unserer Ergebnisse. Diese Verbesserungen werden in zukünftigen Versionen der Cloud-Compliance automatisch verfügbar sein.

Typ	Präzision	Rückruf
Personenbezogene Daten - Allgemeines	90 % - 95 %	60 % - 80 %
Persönliche Daten – Länderkennungen	30 % - 60 %	40 % - 60 %
Sensible persönliche Daten	80 % - 95 %	20 % - 30 %
Kategorien	90 % - 97 %	60 % - 80 %

Was ist in jedem Datei Liste Bericht enthalten (CSV-Datei)

Über das Dashboard können Sie Dateilisten (im CSV-Format) mit Details zu den identifizierten Dateien herunterladen. Wenn es mehr als 10,000 Ergebnisse gibt, werden nur die 10,000 besten Ergebnisse in der Liste angezeigt (Unterstützung für weitere Ergebnisse wird später hinzugefügt).

Jede Dateiliste enthält die folgenden Informationen:

- Dateiname
- Positionstyp
- Standort
- Dateipfad
- Dateityp
- Kategorie
- Persönliche Angaben
- Sensible persönliche Daten
- Löscherkennung Datum

  Ein Löscherkennungsdatum gibt das Datum an, an dem die Datei gelöscht oder verschoben wurde. So können Sie feststellen, wann sensible Dateien verschoben wurden. Gelöschte Dateien sind nicht Teil der Dateinummernanzahl, die im Dashboard angezeigt wird. Die Dateien werden nur in den CSV-Berichten angezeigt.

Lesen des Datenschutzrisikobewertungsberichts

Der Datenschutzrisiko-Assessment-Bericht bietet einen Überblick über den Datenschutzrisikostatus Ihres Unternehmens, wie dies durch Datenschutzvorschriften wie DSGVO und CCPA erforderlich ist.

NetApp kann keine Garantie für 100 % Genauigkeit der persönlichen Daten und für sensible personenbezogene Daten, die Cloud Compliance identifiziert hat, geben. Überprüfen Sie die Informationen immer, indem Sie die Daten überprüfen.

Der Bericht enthält die folgenden Informationen:

Compliance-Status

Ein Wert für den Schweregrad (weitere Informationen finden Sie unten) und die Verteilung von Daten, unabhängig davon, ob es sich um nicht-sensible, persönliche oder sensible Daten handelt.

Assessment-Übersicht

Eine Aufschlüsselung der gefundenen Arten von personenbezogenen Daten sowie der Kategorien von Daten.

Betroffene in dieser Beurteilung

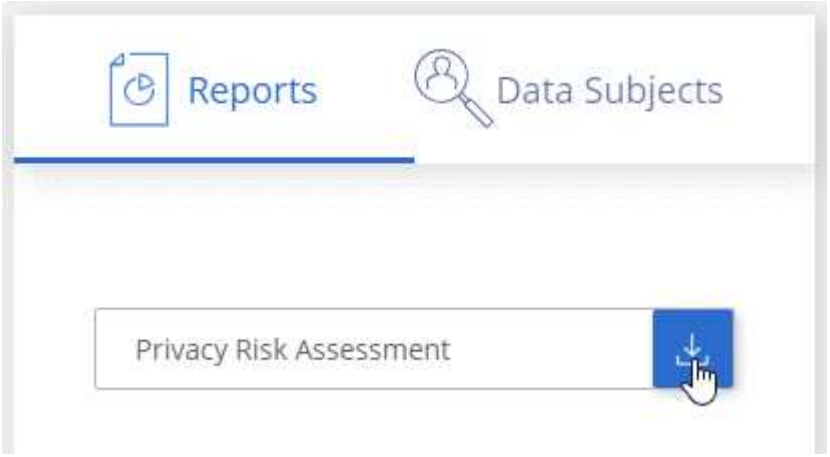
Die Anzahl der Personen nach Ort, für die nationale Kennungen gefunden wurden.

Generieren des Datenschutzrisikobewertungsberichts

Rufen Sie die Registerkarte Compliance auf, um den Bericht zu erstellen.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Compliance**.
2. Klicken Sie unter **Reports** auf das Download-Symbol neben **Privacy Risk Assessment**.



Ergebnis

Cloud Compliance generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

Schweregrad

Cloud Compliance berechnet den Schweregrad für den Privacy Risk Assessment-Bericht auf der Grundlage von drei Variablen:

- Der Prozentsatz der personenbezogenen Daten aus allen Daten.
- Der Prozentsatz sensibler personenbezogener Daten aus allen Daten.
- Der Prozentsatz der Dateien, die betroffene Daten enthalten, die durch nationale Kennungen wie nationale IDs, Sozialversicherungsnummern und Steuerkennzahlen bestimmt werden.

Die folgende Logik dient zur Ermittlung der Punktzahl:

Schweregrad	Logik
0	Alle drei Variablen sind genau 0%
1	Eine der Variablen ist größer als 0 %
2	Eine der Variablen ist größer als 3%
3	Zwei der Variablen sind größer als 3%
4	Drei der Variablen sind größer als 3 %
5	Eine der Variablen ist größer als 6%
6	Zwei der Variablen sind größer als 6%
7	Drei der Variablen sind größer als 6%
8	Eine der Variablen ist größer als 15%
9	Zwei der Variablen sind größer als 15%
10	Drei der Variablen sind größer als 15%

Reaktion auf eine Zugriffsanfrage für betroffene Person

Reagieren Sie auf eine DSAR (Data Subject Access Request), indem Sie nach dem vollständigen Namen oder der bekannten Kennung (z. B. einer E-Mail-Adresse) eines Studienteilnehmers suchen und dann einen Bericht herunterladen. Der Bericht soll Ihrem Unternehmen helfen, die Vorgaben der DSGVO oder ähnlicher Datenschutzgesetze einzuhalten.

NetApp kann keine Garantie für 100 % Genauigkeit der persönlichen Daten und für sensible personenbezogene Daten, die Cloud Compliance identifiziert hat, geben. Überprüfen Sie die Informationen immer, indem Sie die Daten überprüfen.

Was ist ein Antrag auf Zugang für betroffene Person?

Datenschutzvorschriften wie die Europäische DSGVO erteilen Betroffenen (wie Kunden oder Mitarbeitern) das Recht, auf ihre personenbezogenen Daten zuzugreifen. Wenn eine betroffene Person diese Informationen anfordert, wird dies als DSAR (Zugriffsanfrage für betroffene Person) bezeichnet. Unternehmen sind verpflichtet, auf diese Anfragen „ohne unzumutbare Verzögerung“ und spätestens innerhalb eines Monats nach Eingang zu reagieren.

Wie kann Cloud Compliance Ihnen helfen, auf einen DSAR zu reagieren?

Wenn Sie eine Suche des Betroffenen durchführen, findet Cloud Compliance alle Dateien, die den Namen oder die Kennung der betreffenden Person enthalten. Cloud Compliance prüft die neuesten vorindizierten Daten auf den Namen oder die Kennung. Es wird kein neuer Scan gestartet.

Nachdem die Suche abgeschlossen ist, können Sie die Liste der Dateien oder einen Bericht für die Anforderung von Datensubjekten herunterladen. Der Bericht sammelt Erkenntnisse aus den Daten und stellt die Daten zu rechtlichen Bedingungen bereit, die Sie an die Person zurücksenden können.

Suchen nach Betroffenen und Herunterladen von Berichten

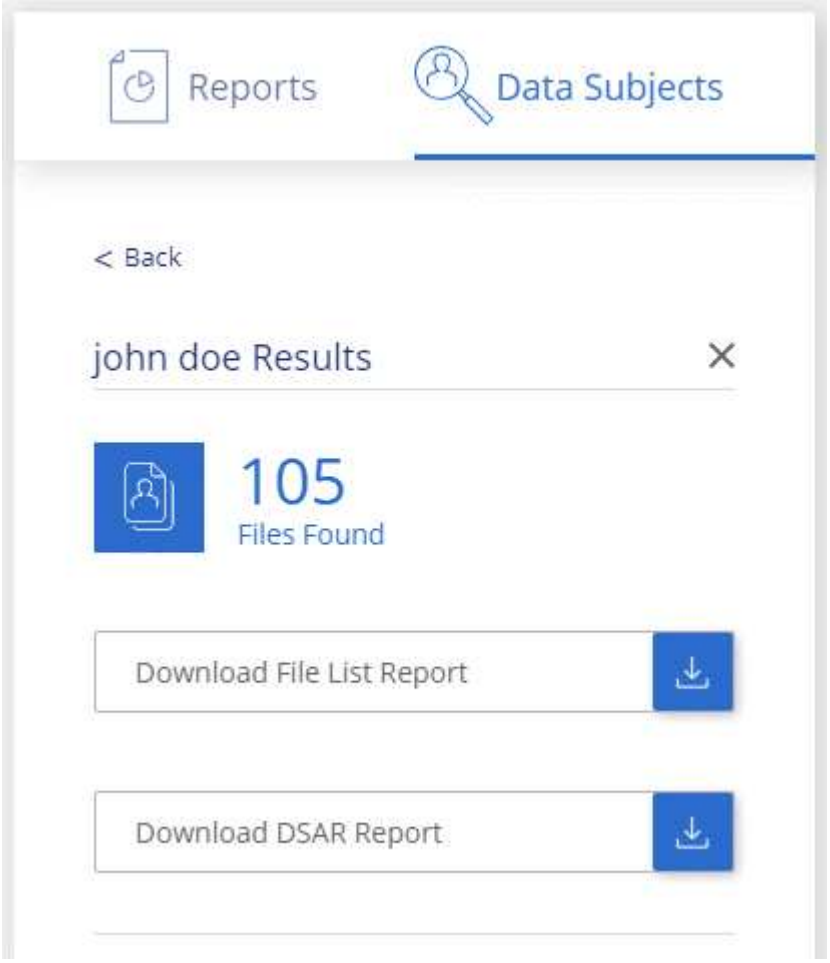
Suchen Sie nach dem vollständigen Namen oder der bekannten Kennung des Betroffenen, und laden Sie dann einen Dateilistenbericht oder einen DSAR-Bericht herunter. Suchen Sie nach "Alle persönlichen Informationstypen".

Nur Englisch wird bei der Suche nach den Namen von Betroffenen unterstützt. Support für weitere Sprachen wird später hinzugefügt.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Compliance**.
2. Klicken Sie Auf **Data Subjects**.
3. Suchen Sie nach dem vollständigen Namen oder der bekannten Kennung des Betroffenen.

   Hier ein Beispiel, das eine Suche nach dem Namen *john doe* zeigt:



4. Wählen Sie eine der folgenden Optionen:
   - **Bericht zur Dateiliste herunterladen**: Eine Liste der Dateien, die Informationen zur betroffenen Person enthalten.

     Wenn mehr als 10,000 Ergebnisse vorliegen, werden nur die 10,000 wichtigsten Ergebnisse im Bericht angezeigt (später wird die Unterstützung für weitere Ergebnisse hinzugefügt).

- **Download DSAR Report**: Eine formelle Antwort auf die Zugriffsanfrage, die Sie an den Betroffenen senden können. Dieser Bericht enthält automatisch generierte Informationen auf der Grundlage von Daten, die Cloud Compliance dem Betroffenen zur Verfügung stellte und für die Nutzung als Vorlage konzipiert wurde. Füllen Sie das Formular aus und überprüfen Sie es intern, bevor Sie es an den Betroffenen senden.

Deaktivieren Von Cloud Compliance

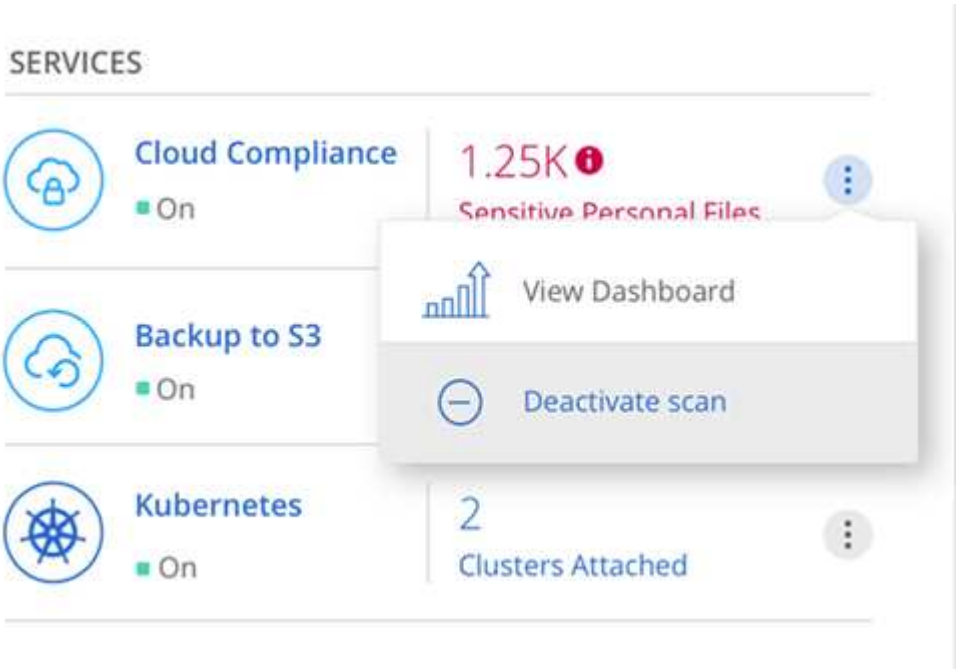
Wenn Sie dies benötigen, können Sie verhindern, dass Cloud Compliance eine oder mehrere Arbeitsumgebungen scannen kann. Sie können auch die Cloud Compliance-Instanz löschen, wenn Sie Cloud Compliance nicht mehr mit Ihren Cloud Volumes ONTAP Systemen verwenden möchten.

Deaktivieren von Compliance-Scans für eine Arbeitsumgebung

Wenn Scans deaktiviert werden, scannt Cloud Compliance die Daten auf dem System nicht mehr und entfernt die indizierten Compliance-Erkenntnisse aus der Cloud Compliance Instanz (die Daten aus der Arbeitsumgebung selbst werden nicht gelöscht).

Schritte

1. Klicken Sie oben im Cloud Manager auf **Arbeitsumgebungen**.
2. Wählen Sie die Arbeitsumgebung aus.
3. Klicken Sie im rechten Fensterbereich auf das Aktionssymbol für den Cloud-Compliance-Dienst und wählen Sie **Scan deaktivieren**.



Löschen der Cloud-Compliance-Instanz

Sie können die Cloud-Compliance-Instanz löschen, wenn Sie Cloud-Compliance mit Cloud Volumes ONTAP nicht mehr verwenden möchten. Durch das Löschen der Instanz werden auch die zugehörigen Festplatten gelöscht, auf denen sich die indizierten Daten befinden.

Schritt

1. Gehen Sie zur Konsole Ihres Cloud-Providers und löschen Sie die Instanz für Cloud Compliance.

   Der Name der Instanz ist *CloudCompliance* mit einem generierten Hash (UUID), der verknüpft ist. Beispiel: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

Häufig gestellte Fragen zur Cloud Compliance

Diese FAQ kann Ihnen helfen, wenn Sie nur eine schnelle Antwort auf eine Frage suchen.

Was ist Cloud Compliance?

Cloud Compliance ist ein neues Cloud-Angebot von NetApp. Mithilfe von künstlicher Intelligenz (KI) hilft Cloud Compliance Unternehmen dabei, den Datenkontext zu verstehen und sensible Daten über die in AWS oder Azure gehosteten Cloud Volumes ONTAP Systeme zu identifizieren.

Cloud Compliance stellt vordefinierte Parameter wie sensible Informationstypen und -Kategorien zur Verfügung, um neue Compliance-Vorschriften für Datenschutz und -Sensibilität wie DSGVO, CCPA usw. zu erfüllen.

Warum sollte ich Cloud-Compliance verwenden?

Cloud Compliance bietet Ihnen mehr Möglichkeiten für die Nutzung von Daten:

- Einhaltung von Daten-Compliance- und Datenschutzvorschriften
- Einhaltung von Richtlinien zur Datenaufbewahrung.
- Das Auffinden und Reporting von Daten zu bestimmten Daten als Antwort auf Betroffene kann auf einfache Weise entsprechend den Vorgaben von DSGVO, CCPA und anderen Datenschutzvorschriften erfolgen.

Was sind die gängigsten Anwendungsfälle für Cloud Compliance?

- Ermitteln von personenbezogenen Daten
- Identifizieren Sie einen breiten Umfang sensibler Daten, wie sie im Sinne der DSGVO- und CCPA-Datenschutzvorschriften erforderlich sind.
- Einhaltung neuer und anstehender Datenschutzvorschriften

"Erfahren Sie mehr über die Anwendungsfälle für Cloud Compliance".

Welche Datentypen können mit Cloud Compliance gescannt werden?

Cloud Compliance unterstützt die Überprüfung unstrukturierter Daten über NFS- und CIFS-Protokolle. Derzeit überprüft Cloud Compliance die von Cloud Volumes ONTAP gemanagten Daten.

"Lesen Sie, wie Scans funktionieren".

Welche Cloud-Provider werden unterstützt?

Cloud Compliance arbeitet als Teil von Cloud Manager und unterstützt derzeit AWS und Azure. Dadurch erhält Ihr Unternehmen Transparenz im Hinblick auf den Datenschutz bei verschiedenen Cloud-Providern.

Demnächst wird auch Support für die Google Cloud Platform (GCP) verfügbar sein.

Wie erhalte ich Zugriff auf Cloud Compliance?

Cloud Compliance wird über Cloud Manager betrieben und gemanagt. Sie können Cloud Compliance-Funktionen über die Registerkarte **Compliance** in Cloud Manager aufrufen.

Wie funktioniert Cloud Compliance?

Cloud Compliance implementiert gemeinsam mit Ihrem Cloud Manager System und Cloud Volumes ONTAP Instanzen eine weitere Schicht künstlicher Intelligenz. Anschließend scannt sie die Daten auf Cloud Volumes ONTAP und indiziert die gefundenen Dateneinblicke.

"Funktionsweise von Cloud Compliance".

Wie viel kostet Cloud Compliance?

Cloud-Compliance wird als Teil von Cloud Volumes ONTAP angeboten und erfordert keine zusätzlichen Kosten. Für kundenspezifische Funktionen können in Zukunft möglicherweise zusätzliche Kosten anfallen.

Cloud Compliance erfordert die Implementierung einer Instanz bei Ihrem Cloud-Provider, für die Sie durch Ihren Cloud-Provider in Rechnung gestellt werden.

Wie oft scannt Cloud Compliance meine Daten?

Da sich die Daten häufig ändern, scannt Cloud Compliance Ihre Daten kontinuierlich, ohne Auswirkungen auf Ihre Daten. Während der erste Scan Ihrer Daten länger dauern kann, scannen nachfolgende Scans nur die inkrementellen Änderungen, was die Dauer des Systemscans verkürzt.

"Lesen Sie, wie Scans funktionieren".

Bietet Cloud Compliance Berichte an?

Ja. Die von Cloud Compliance angebotenen Informationen können für andere Beteiligte in Ihrem Unternehmen relevant sein. So können Sie Berichte erstellen und Einblicke erhalten.

Für Cloud Compliance stehen folgende Berichte zur Verfügung:

Datenschutzrisiko-Assessment-Bericht

Bietet Einblicke in den Datenschutz und eine Bewertung des Datenschutzrisikos. "Weitere Informationen .".

Bericht für Anforderung von Datenfachzugriff

Ermöglicht Ihnen, einen Bericht aller Dateien zu extrahieren, die Informationen über den spezifischen Namen oder die persönliche Kennung eines Betroffenen enthalten. "Weitere Informationen .".

Berichte zu einem bestimmten Informationstyp

Es stehen Berichte zur Verfügung, die Details zu den identifizierten Dateien enthalten, die personenbezogene Daten und sensible personenbezogene Daten enthalten. Sie können auch Dateien nach Kategorie und Dateityp aufgeschlüsselt sehen. "Weitere Informationen .".

Welcher Instanztyp oder VM ist für Cloud Compliance erforderlich?

- In Azure wird Cloud Compliance auf einer VM mit Standard_D16s_v3 mit einer Festplatte von 512 GB ausgeführt.
- In AWS wird Cloud-Compliance auf einer m5.4xlarge-Instanz mit einer 500-GB-io1-Festplatte ausgeführt.

  In Regionen, in denen m5.4xlarge nicht verfügbar ist, wird Cloud Compliance stattdessen auf einer m4.4xlarge-Instanz ausgeführt.

"Funktionsweise von Cloud Compliance".

Ist die Scanleistung unterschiedlich?

Die Scan-Performance kann je nach Netzwerkbandbreite und durchschnittlicher Dateigröße in der Cloud-Umgebung variieren.

Wie kann ich Cloud-Compliance aktivieren?

Sie können Cloud-Compliance aktivieren, wenn Sie eine neue Arbeitsumgebung erstellen. Sie können es auf bestehenden Arbeitsumgebungen über die Registerkarte **Compliance** (nur bei der ersten Aktivierung) oder durch Auswahl einer bestimmten Arbeitsumgebung aktivieren.

"Erste Schritte".

Durch die Aktivierung von Cloud Compliance wird ein sofortiger anfänglicher Scan durchgeführt. Ergebnisse der Compliance werden kurz danach angezeigt.

Wie deaktiviere ich Cloud Compliance?

Sie können Cloud-Compliance auf der Seite Arbeitsumgebung deaktivieren, nachdem Sie eine individuelle Arbeitsumgebung ausgewählt haben.

"Weitere Informationen .".

Wenn Sie die Cloud Compliance-Instanz vollständig entfernen möchten, können Sie die Cloud Compliance-Instanz manuell aus dem Portal Ihres Cloud-Providers entfernen.

Was geschieht, wenn das Daten-Tiering auf Cloud Volumes ONTAP aktiviert ist?

Es ist sinnvoll, Cloud-Compliance auf einem Cloud Volumes ONTAP System zu aktivieren, das kalte Daten auf Objekt-Storage abschichtet. Wenn das Daten-Tiering aktiviert ist, scannt Cloud Compliance alle Daten auf Festplatten, die sich auf kalten Daten befinden, die in Objekt-Storage verschoben werden.

Der Compliance-Scan erhitzt die nicht kalten Daten – es bleibt kalt und führt zu Objekt-Storage.

Kann ich Cloud Compliance verwenden, um den lokalen ONTAP Storage zu scannen?

Nein Cloud Compliance ist derzeit Teil von Cloud Manager und unterstützt Cloud Volumes ONTAP. Wir planen, Cloud Compliance durch zusätzliche Cloud-Angebote wie Cloud Volumes Service und Azure NetApp Files zu unterstützen.

Kann Cloud Compliance Benachrichtigungen an mein Unternehmen senden?

Nein, aber Sie können Statusberichte herunterladen, die Sie intern in Ihrem Unternehmen teilen können.

Kann ich den Service an die Bedürfnisse meiner Organisation anpassen?

Cloud Compliance bietet sofortige Einblicke in Ihre Daten. Diese Erkenntnisse können extrahiert und für die Bedürfnisse Ihres Unternehmens verwendet werden.

Kann ich die Daten zur Cloud Compliance auf bestimmte Benutzer begrenzen?

Ja, Cloud Compliance ist vollständig in Cloud Manager integriert. Cloud Manager-Benutzer können nur Informationen für die Arbeitsumgebungen anzeigen, die sie entsprechend ihren Arbeitsbereichsberechtigungen anzeigen können.

"Weitere Informationen .".

Cloud Volumes ONTAP verwalten

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 OnCommand System Manager wird hergestellt

Möglicherweise müssen Sie einige Cloud Volumes ONTAP Aufgaben über OnCommand System Manager ausführen, ein browserbasiertes Management-Tool, 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.

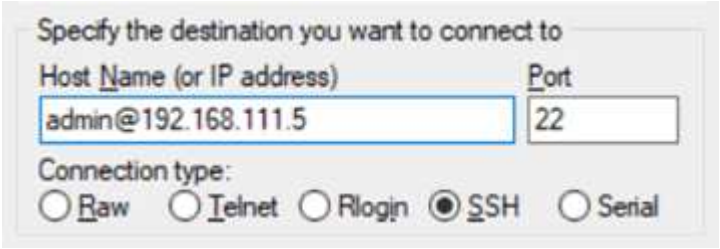
Wenn Cloud Volumes ONTAP HA in mehreren AZS implementiert wird, verwenden sie eine Floating-IP-Adresse für die Cluster-Management-Schnittstelle, was bedeutet, dass externes Routing nicht verfügbar ist. Sie müssen eine Verbindung von einem Host herstellen, der Teil derselben Routingdomäne ist.

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::>
```

Aktualisierung der Cloud Volumes ONTAP Software

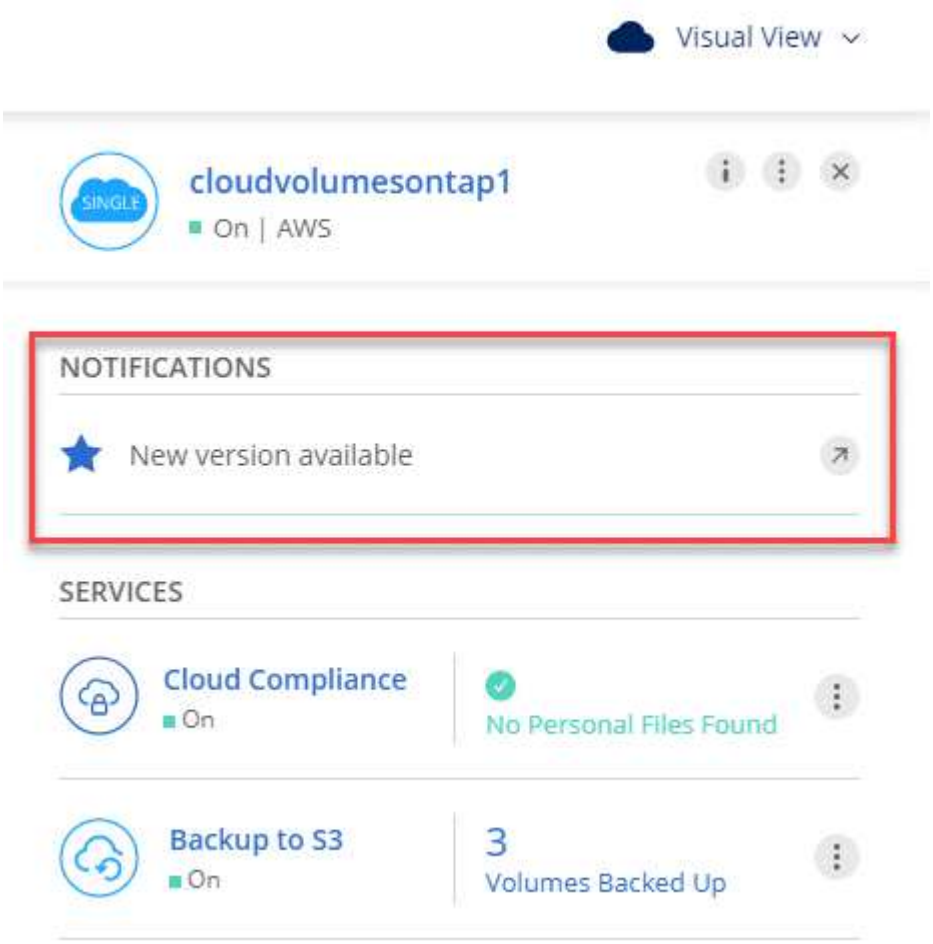
Cloud Manager umfasst mehrere Optionen, mit denen Sie auf die aktuelle Version von Cloud Volumes ONTAP aktualisieren oder Cloud Volumes ONTAP auf eine frühere Version herabstufen können. Sie sollten Cloud Volumes ONTAP Systeme vorbereiten, bevor Sie ein Upgrade oder Downgrade der Software durchführen.

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

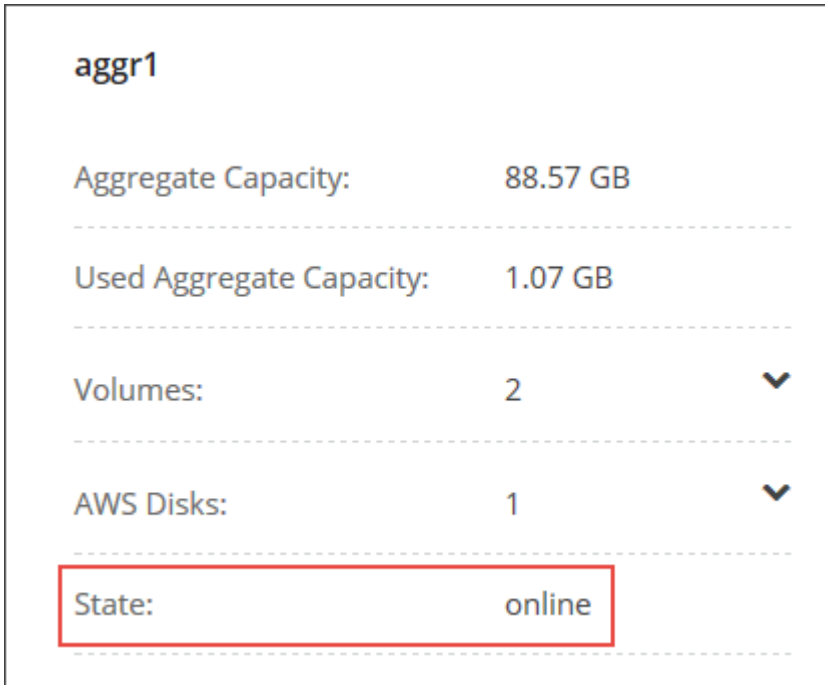
Aggregate für Cloud Volumes ONTAP muss online sein, bevor Sie die Software aktualisieren. Aggregate sollten in den meisten Konfigurationen online sein. Wenn dies nicht der Fall ist, sollten Sie sie jedoch online stellen.

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

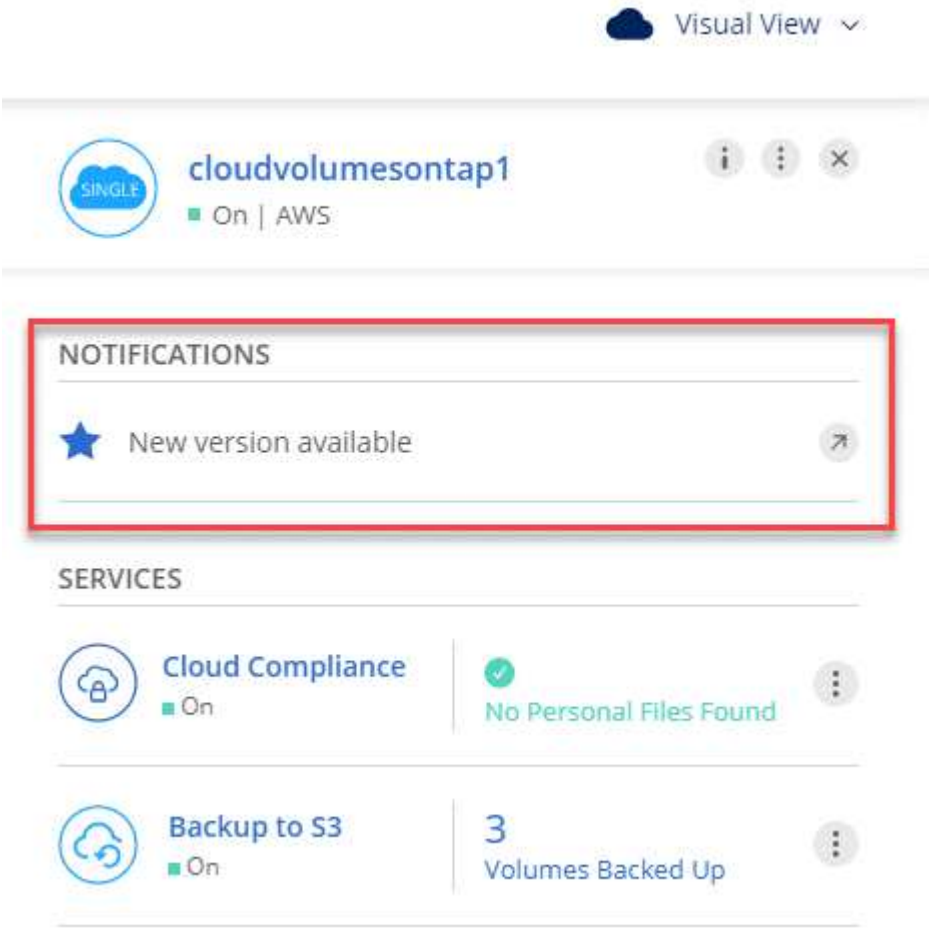
Cloud Manager-Vorgänge wie die Erstellung von Volumes oder Aggregaten dürfen für das Cloud Volumes

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 Instanzen ändern, wenn sich Ihre Storage-Anforderungen ändern. Sie können beispielsweise zwischen nutzungsbasierten Konfigurationen wechseln, die Instanz oder den VM-Typ ändern und zu einem alternativen Abonnement wechseln.

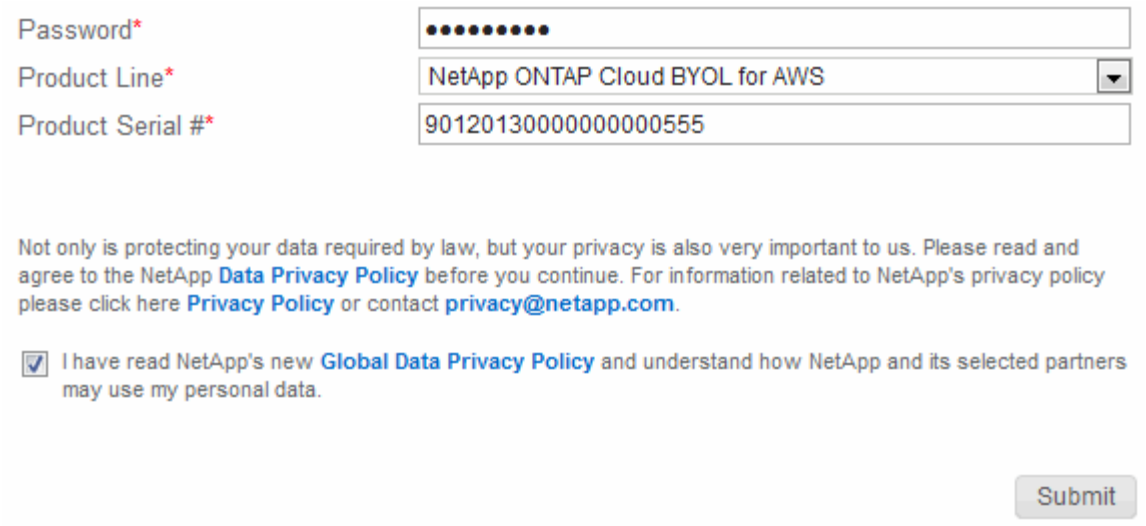
Installation von Lizenzdateien auf Cloud Volumes ONTAP Byol Systemen

Wenn Cloud Manager keine Byol Lizenzdatei von NetApp erhalten kann, können Sie die Datei selbst beziehen und die Datei dann manuell in Cloud Manager hochladen, damit die Lizenz auf dem Cloud Volumes ONTAP System installiert werden kann.

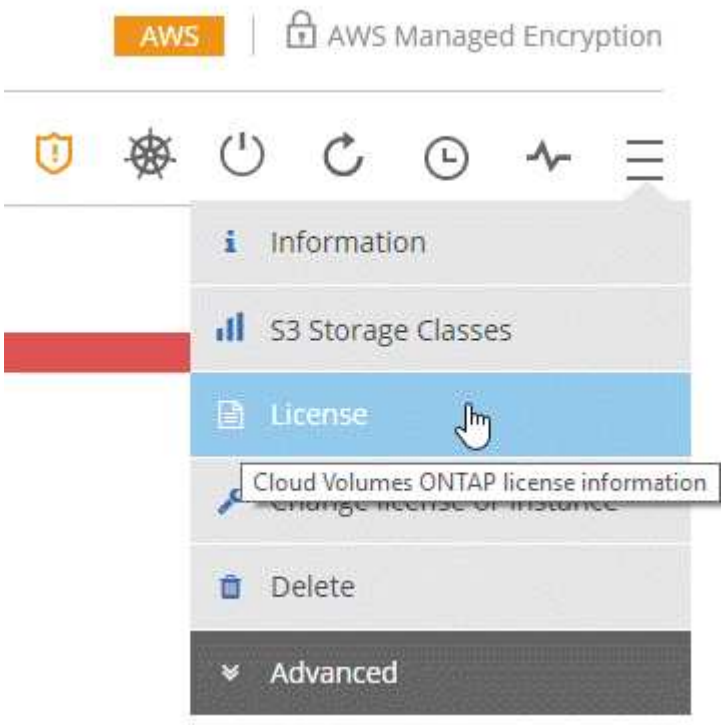
Schritte

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.
4. Öffnen Sie in Cloud Manager die BYOL-Arbeitsumgebung von Cloud Volumes ONTAP.
5. Klicken Sie auf das Menü-Symbol und dann auf **Lizenz**.



6. Klicken Sie Auf **Lizenzdatei Hochladen**.
7. Klicken Sie auf **Upload** und wählen Sie dann die Datei aus.

Ergebnis

Cloud Manager installiert die neue Lizenzdatei auf dem Cloud Volumes ONTAP System.

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"

- 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. 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 nutzungsbasierten Abonnement und einem Byol Abonnement oder zwischen einem einzelnen Cloud Volumes ONTAP System und einem HA-Paar wechseln möchten, können Sie ein neues System implementieren und dann Daten vom vorhandenen System auf 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 des AWS Marketplace Abonnements

Ändern Sie das AWS Marketplace Abonnement für Ihr Cloud Volumes ONTAP System, wenn Sie das AWS Konto, von dem Sie belastet werden, ändern möchten.

Schritte

1. Wenn Sie dies noch nicht getan haben, fügen Sie ein neues Abonnement von hinzu "Cloud Manager im AWS Marketplace".
2. Klicken Sie in der Arbeitsumgebung in Cloud Manager auf das Menü-Symbol und dann auf **Marketplace-Abonnement**.
3. Wählen Sie ein Abonnement aus der Dropdown-Liste aus.
4. Klicken Sie Auf **Speichern**.

Ändern der Schreibgeschwindigkeit auf „Normal“ oder „hoch“

Die standardmäßige Schreibgeschwindigkeit für Cloud Volumes ONTAP 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.

  Bei Systemen mit einem Node wird die I/O unterbrochen.

  Bei HA-Paaren ist die Änderung unterbrechungsfrei. Ha-Paare stellen weiterhin Daten bereit.

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.

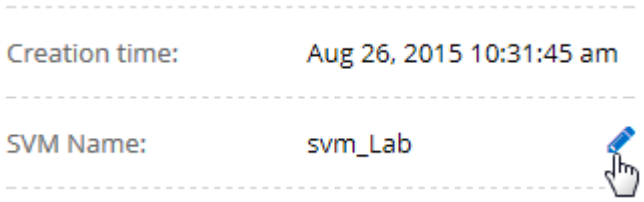
3. Klicken Sie auf **Speichern**, überprüfen Sie die Bestätigungsmeldung und klicken Sie dann auf **Weiter**.

Ändern des Namens der virtuellen Storage-Maschine

Cloud Manager benennt die Storage Virtual Machine (SVM) für Cloud Volumes ONTAP automatisch. Sie können den Namen der SVM ändern, wenn Sie strenge Benennungsstandards haben. Sie sollten beispielsweise festlegen, wie Sie die SVMs für Ihre ONTAP Cluster benennen.

Schritte

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



3. Ändern Sie im Dialogfeld SVM-Name ändern den SVM-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.

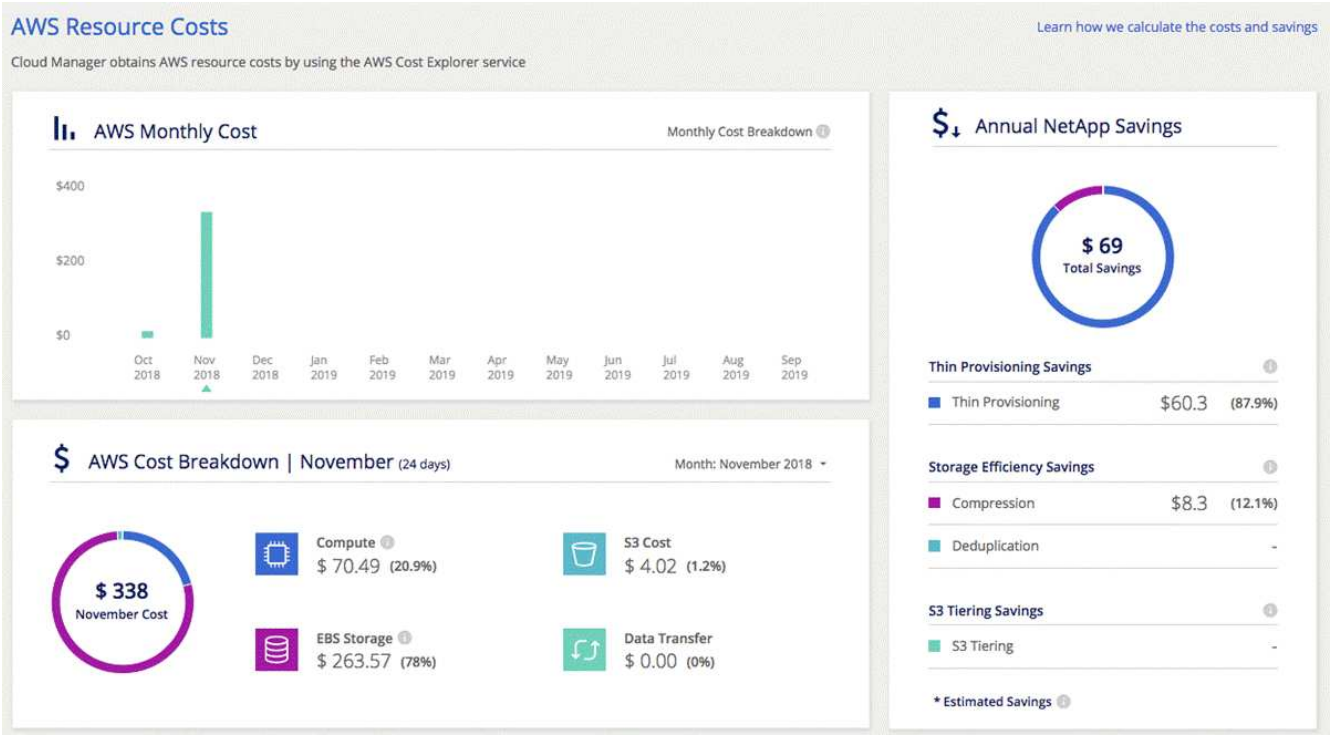
   b. "Aktivieren Sie das Tag **WorkingEnvironment ID**".

   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:

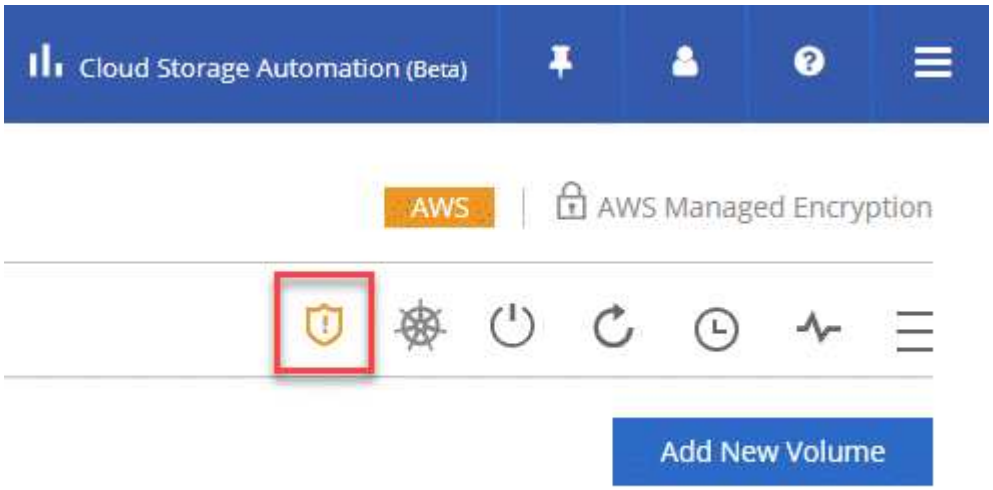


Besserer Schutz gegen Ransomware

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**.

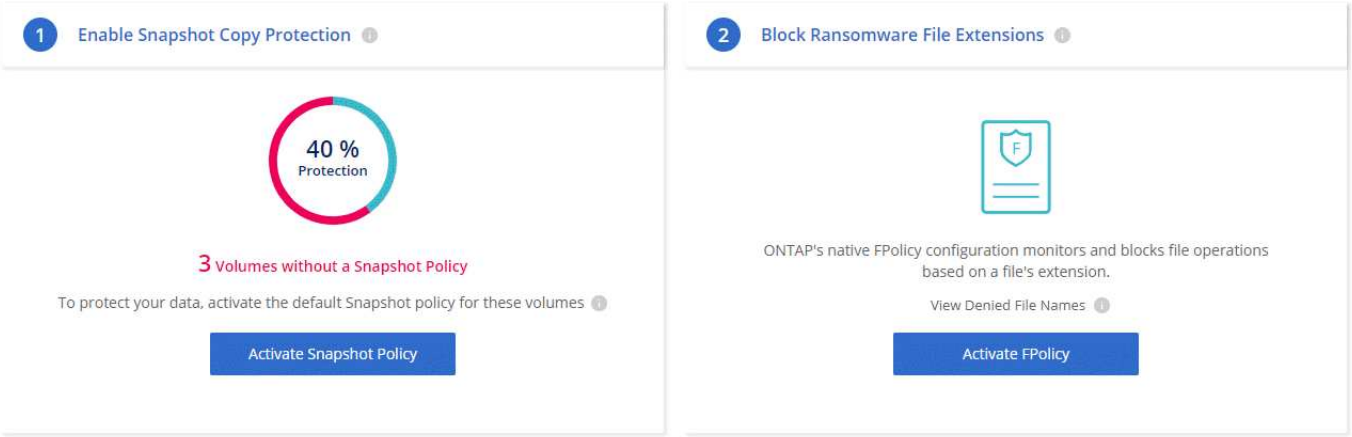


2. Implementierung der NetApp Lösung für Ransomware:
   a. Klicken Sie auf **Snapshot-Richtlinie aktivieren**, wenn Volumes ohne Snapshot-Richtlinie aktiviert sind.

      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.



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 **Entdecken** und wählen Sie **Cloud Volumes ONTAP**.
2. Wählen Sie den Cloud-Provider aus, in dem sich das System befindet.
3. Wählen Sie auf der Seite Region den Bereich aus, in dem die Instanzen ausgeführt werden, und wählen Sie dann die Instanzen aus.
4. 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.

Management Von Cloud Manager

Cloud Manager wird aktualisiert

Sie können Cloud Manager auf die neueste Version oder mit einem Patch aktualisieren, den Sie von NetApp Mitarbeitern erhalten haben.

Aktivieren automatischer Updates

Cloud Manager kann sich automatisch aktualisieren, wenn eine neue Version verfügbar ist. Dadurch wird sichergestellt, dass die neueste Version ausgeführt wird.

Über diese Aufgabe

Cloud Manager wird automatisch um 24:00 Uhr aktualisiert, wenn keine Vorgänge ausgeführt werden.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Cloud Manager-Einstellungen**.
2. Aktivieren Sie das Kontrollkästchen unter Automatische Cloud Manager-Updates und klicken Sie dann auf **Speichern**.

Aktualisierung von Cloud Manager auf die neueste Version

Sie sollten die automatischen Updates für Cloud Manager aktivieren, aber Sie können jederzeit eine manuelle Aktualisierung direkt über die Webkonsole durchführen. Cloud Manager bezieht das Software-Update von einem NetApp S3-Bucket in AWS.

Bevor Sie beginnen

Sie sollten die Prüfung durchgeführt haben "Neuerungen in dieser Version" Um neue Anforderungen und Änderungen im Support zu ermitteln.

Über diese Aufgabe

Das Softwareupdate dauert einige Minuten. Cloud Manager ist während des Updates nicht verfügbar.

Schritte

1. Prüfen Sie, ob eine neue Version verfügbar ist, indem Sie in der unteren rechten Ecke der Konsole nachsehen:

2. Wenn eine neue Version verfügbar ist, klicken Sie auf **Timeline**, um festzustellen, ob Aufgaben ausgeführt werden.

   Wenn Aufgaben ausgeführt werden, warten Sie, bis sie abgeschlossen sind, bevor Sie mit dem nächsten Schritt fortfahren.

3. Klicken Sie rechts unten auf der Konsole auf **Neue Version verfügbar**.
4. Klicken Sie auf der Seite Cloud Manager Software Update neben der gewünschten Version auf **Update**.

5. Füllen Sie das Bestätigungsdialogfeld aus und klicken Sie dann auf **OK**.

Ergebnis

Cloud Manager startet den Update-Prozess. Sie können sich nach einigen Minuten bei der Konsole anmelden.

Aktualisierung von Cloud Manager mit einem Patch

Wenn NetApp einen Patch gemeinsam mit Ihnen verwendet, können Sie Cloud Manager direkt über die Cloud Manager Webkonsole mit dem bereitgestellten Patch aktualisieren.

Über diese Aufgabe

Das Patch-Update dauert in der Regel einige Minuten. Cloud Manager ist während des Updates nicht verfügbar.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Software-Update**.

2. Klicken Sie auf den Link, um Cloud Manager mit dem bereitgestellten Patch zu aktualisieren.

3. Füllen Sie das Bestätigungsdialogfeld aus und klicken Sie dann auf **OK**.
4. Wählen Sie den bereitgestellten Patch aus.

Ergebnis

Cloud Manager wendet den Patch an. Sie können sich nach einigen Minuten bei der Konsole anmelden.

Managen von Workspaces und Benutzern im Cloud Central Konto

"Nach der ersten Einrichtung", Möglicherweise müssen Sie später Benutzer, Arbeitsbereiche und Service Connectors verwalten.

"Erfahren Sie mehr über die Funktionsweise von Cloud Central-Accounts".

Benutzer hinzufügen

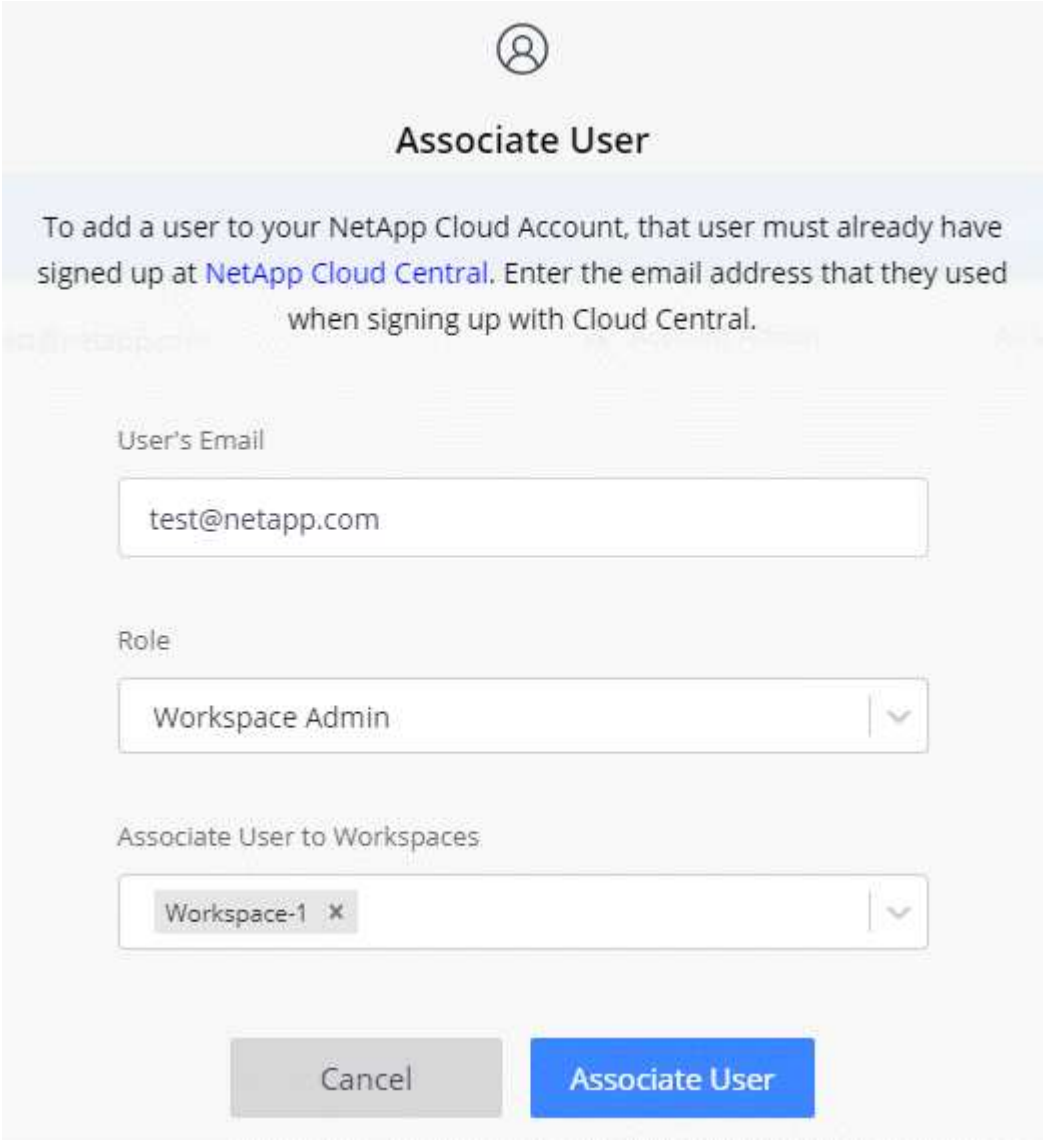
Cloud Central Benutzer werden mit dem Cloud Central Konto verknüpft, damit diese Arbeitsumgebungen in Cloud Manager erstellen und verwalten können.

Schritte

1. Wenn der Benutzer dies noch nicht getan hat, bitten Sie den Benutzer, zu wechseln "NetApp Cloud

Central" Und erstellen Sie ein Konto.

2. Klicken Sie in Cloud Manager auf **Kontoeinstellungen**.
3. Klicken Sie auf der Registerkarte Benutzer auf **Benutzer verknüpfen**.
4. Geben Sie die E-Mail-Adresse des Benutzers ein, und wählen Sie eine Rolle für den Benutzer aus:
   - **Account Admin**: Kann jede Aktion in Cloud Manager ausführen.
   - **Workspace Admin**: Kann Ressourcen in zugewiesenen Workspaces erstellen und verwalten.
5. Wenn Sie Workspace Admin ausgewählt haben, wählen Sie eine oder mehrere Arbeitsbereiche aus, die diesem Benutzer zugeordnet werden sollen.



6. Klicken Sie Auf * Benutzer Verknüpfen*.

Ergebnis

Der Benutzer sollte eine E-Mail von NetApp Cloud Central mit dem Titel „Account Association“ erhalten. Die E-Mail enthält die für den Zugriff auf Cloud Manager erforderlichen Informationen.

Ergebnis

Der Benutzer sollte eine E-Mail von NetApp Cloud Central mit dem Titel „Account Association“ erhalten. Die E-

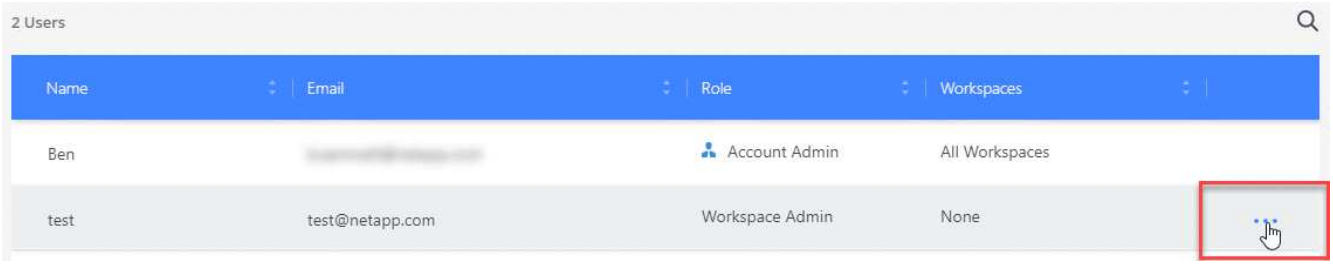
Mail enthält die für den Zugriff auf Cloud Manager erforderlichen Informationen.

Benutzer werden entfernt

Die Trennung der Verknüpfung eines Benutzers wird dadurch erschwert, dass er nicht mehr auf die Ressourcen eines Cloud Central Kontos zugreifen kann.

Schritte

1. Klicken Sie Auf **Kontoeinstellungen**.
2. Klicken Sie auf das Aktionsmenü in der Zeile, die dem Benutzer entspricht.



3. Klicken Sie zur Bestätigung auf **Benutzer entzuordnen** und klicken Sie zur Bestätigung auf **Mitarbeiter nicht zuordnen**.

Ergebnis

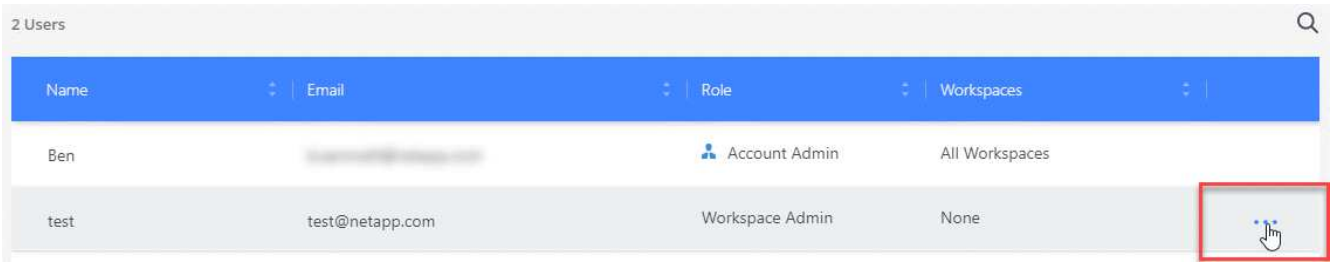
Der Benutzer kann nicht mehr auf die Ressourcen in diesem Cloud Central Konto zugreifen.

Arbeitsbereiche eines Arbeitsbereichs-Administrators verwalten

Sie können Workspace-Administratoren jederzeit mit Arbeitsbereichen verknüpfen und sie ablösen. Durch die Verknüpfung des Benutzers können die Arbeitsumgebungen in diesem Arbeitsbereich erstellt und angezeigt werden.

Schritte

1. Klicken Sie Auf **Kontoeinstellungen**.
2. Klicken Sie auf das Aktionsmenü in der Zeile, die dem Benutzer entspricht.



3. Klicken Sie Auf **Arbeitsbereiche Verwalten**.
4. Wählen Sie die Arbeitsbereiche aus, die dem Benutzer zugeordnet werden sollen, und klicken Sie auf **Anwenden**.

Ergebnis

Der Benutzer kann jetzt über Cloud Manager auf diese Arbeitsbereiche zugreifen, solange der Service Connector auch mit den Arbeitsbereichen verknüpft war.

Arbeitsbereiche verwalten

Verwalten Sie Ihre Arbeitsbereiche, indem Sie sie erstellen, umbenennen und löschen. Beachten Sie, dass Sie einen Arbeitsbereich nicht löschen können, wenn er Ressourcen enthält. Er muss leer sein.

Schritte

1. Klicken Sie Auf **Kontoeinstellungen**.
2. Klicken Sie Auf **Arbeitsbereiche**.
3. Wählen Sie eine der folgenden Optionen:
   - Klicken Sie auf **Neuen Arbeitsbereich hinzufügen**, um einen neuen Arbeitsbereich zu erstellen.
   - Klicken Sie auf **Umbenennen**, um den Arbeitsbereich umzubenennen.
   - Klicken Sie auf **Löschen**, um den Arbeitsbereich zu löschen.

Verwalten der Arbeitsbereiche eines Service Connectors

Sie müssen den Service Connector mit Arbeitsbereichen verknüpfen, damit Workspace-Administratoren über Cloud Manager auf diese Arbeitsbereiche zugreifen können.

Wenn Sie nur Kontoadministratoren haben, ist es nicht erforderlich, den Service Connector mit Arbeitsbereichen zu verknüpfen. Account-Administratoren haben standardmäßig die Möglichkeit, auf alle Workspaces in Cloud Manager zuzugreifen.

"Erfahren Sie mehr über Benutzer, Arbeitsbereiche und Serviceanschlüsse".

Schritte

1. Klicken Sie Auf **Kontoeinstellungen**.
2. Klicken Sie Auf **Service Connector**.
3. Klicken Sie auf **Arbeitsbereiche verwalten** für den Service-Anschluss, den Sie verknüpfen möchten.
4. Wählen Sie die Arbeitsbereiche aus, die mit dem Service Connector verknüpft werden sollen, und klicken Sie auf **Anwenden**.

Entfernen von Cloud Volumes ONTAP Arbeitsumgebungen

Der Kontoadministrator kann eine Cloud Volumes ONTAP Arbeitsumgebung entfernen, in der sie auf ein anderes System verschoben oder Fehler bei der Erkennung behoben werden.

Über diese Aufgabe

Durch das Entfernen einer Cloud Volumes ONTAP Arbeitsumgebung wird sie aus Cloud Manager entfernt. Das Cloud Volumes ONTAP System wird nicht gelöscht. Sie können die Arbeitsumgebung später neu entdecken.

Durch das Entfernen einer Arbeitsumgebung aus Cloud Manager können Sie Folgendes tun:

- In einem anderen Arbeitsbereich neu entdecken
- Entdecken Sie es von einem anderen Cloud Manager-System neu
- Entdecken Sie es erneut, wenn Sie während der ersten Erkennung Probleme hatten

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Tools**.

2. Klicken Sie auf der Seite Extras auf **Starten**.
3. Wählen Sie die Cloud Volumes ONTAP Arbeitsumgebung aus, die Sie entfernen möchten.
4. Klicken Sie auf der Seite „Prüfen und genehmigen“ auf **Los**.

Ergebnis

Cloud Manager entfernt die Arbeitsumgebung. Benutzer können diese Arbeitsumgebung jederzeit über die Seite Arbeitsumgebungen neu entdecken.

Konfigurieren von Cloud Manager für die Verwendung eines Proxyservers

Wenn Sie Cloud Manager zum ersten Mal implementieren, werden Sie aufgefordert, einen Proxyserver einzugeben, wenn das System nicht über einen Internetzugang verfügt. Sie können den Proxy auch manuell unter den Einstellungen von Cloud Manager eingeben und ändern.

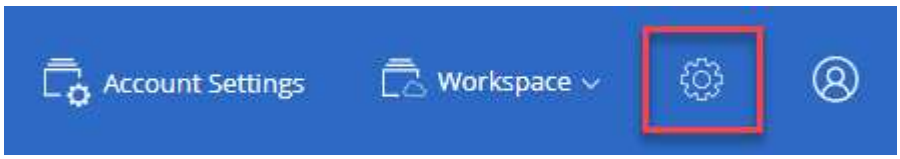
Über diese Aufgabe

Wenn Ihre Unternehmensrichtlinien vorschreiben, dass Sie einen Proxyserver für die gesamte HTTP-Kommunikation mit dem Internet verwenden, müssen Sie Cloud Manager so konfigurieren, dass dieser Proxyserver verwendet wird. Der Proxyserver kann sich in der Cloud oder im Netzwerk befinden.

Wenn Sie Cloud Manager für die Verwendung eines Proxy-Servers konfigurieren, verwenden Cloud Manager, Cloud Volumes ONTAP und der HA-Vermittler den Proxy-Server.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Cloud Manager-Einstellungen**.



2. Geben Sie unter HTTP Proxy den Server mithilfe der Syntax ein http://address:portGeben Sie einen Benutzernamen und ein Passwort an, wenn eine grundlegende Authentifizierung für den Server erforderlich ist, und klicken Sie dann auf Speichern.

Cloud Manager unterstützt keine Kennwörter, die das Zeichen @ enthalten.

Ergebnis

Nachdem Sie den Proxyserver angegeben haben, werden neue Cloud Volumes ONTAP Systeme automatisch so konfiguriert, dass sie den Proxyserver beim Senden von AutoSupport Nachrichten verwenden. Wenn Sie den Proxyserver nicht angeben, bevor Benutzer Cloud Volumes ONTAP Systeme erstellen, müssen sie den Proxyserver mithilfe von System Manager manuell in den AutoSupport-Optionen für jedes System festlegen.

Erneuerung des Cloud Manager HTTPS-Zertifikats

Sie sollten das HTTPS-Zertifikat von Cloud Manager vor dessen Ablauf erneuern, um einen sicheren Zugriff auf die Cloud Manager-Webkonsole zu gewährleisten. Wenn Sie das Zertifikat nicht vor Ablauf erneuern, wird eine Warnung angezeigt, wenn Benutzer über HTTPS auf die Webkonsole zugreifen.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **HTTPS-Setup**.

   Details zum Cloud Manager-Zertifikat werden angezeigt, einschließlich des Ablaufdatums.

2. Klicken Sie auf **HTTPS-Zertifikat erneuern** und befolgen Sie die Schritte, um eine CSR zu erstellen oder Ihr eigenes CA-signiertes Zertifikat zu installieren.

Ergebnis

Cloud Manager verwendet das neue CA-signierte Zertifikat, um sicheren HTTPS-Zugriff zu ermöglichen.

Cloud Manager Wird Wiederhergestellt

Ihr "NetApp Cloud Central Konto" Einfache Wiederherstellung einer Cloud Manager-Konfiguration Das Konto ist ein Dienst, der in Cloud Central ausgeführt wird, sodass die Benutzer, Arbeitsbereiche und Serviceanschlüsse, die Sie dem Konto zugeordnet haben, stets zugänglich sind. Auch wenn Ihr Cloud Manager System versehentlich gelöscht wurde.

Ab Version 3.7.1 unterstützt Cloud Manager nicht mehr das Herunterladen eines Backups und das Wiederherstellen der Konfiguration. Führen Sie diese Schritte aus, um Cloud Manager wiederherzustellen.

Schritte

1. Implementieren Sie ein neues Cloud Manager System in Ihrem bestehenden Cloud Central Konto.

   "Implementierungsoptionen"

2. Fügen Sie Ihre Cloud-Provider-Konten und NetApp Support Site Konten zu Cloud Manager hinzu.

   Mit diesem Schritt ist Cloud Manager einsatzbereit, und Sie können weitere Cloud Volumes ONTAP Systeme bei Ihrem Cloud-Provider erstellen.

   Um ein bestehendes Cloud Volumes ONTAP System zu implementieren, das in diesem neuen Cloud Manager System ermittelt werden soll, müssen Sie diesen Schritt unbedingt durchführen. Cloud Manager benötigt für die ordnungsgemäße Erkennung und das Management von Cloud Volumes ONTAP die AWS Schlüssel.

- "Hinzufügen von AWS Konten zu Cloud Manager"
- "Hinzufügen von Azure-Konten zu Cloud Manager"
- "Hinzufügen von NetApp Support Site Konten zu Cloud Manager"

3. Entdecken Sie Ihre Arbeitsumgebungen neu: Cloud Volumes ONTAP-Systeme, On-Premises-Cluster und NetApp Private Storage for Cloud-Konfigurationen.
   - "Hinzufügen vorhandener Cloud Volumes ONTAP Systeme zu Cloud Manager"
   - "Erkennung von ONTAP Clustern"

Ergebnis

Ihre Cloud Manager Konfiguration ist jetzt mit Ihren Accounts, Einstellungen und Arbeitsumgebungen wiederhergestellt.

Cloud Manager wird deinstalliert

Cloud Manager enthält ein Deinstallationsskript, mit dem Sie die Software deinstallieren können, um Probleme zu beheben oder die Software dauerhaft vom Host zu entfernen.

Schritte

1. Führen Sie auf dem Linux-Host das Deinstallationsskript aus:

   /opt/Application/netapp/cloudmanager/bin/uninstall.sh [Silent]

   Silent führt das Skript aus, ohne dass Sie zur Bestätigung aufgefordert werden.

Bereitstellung von Volumes für Fileservices

Management von Volumes für Azure NetApp Files

NFS-Volumes für anzeigen und erstellen "Azure NetApp Dateien" Direkt im Cloud Manager

Konfiguration einrichten

Ihre Konfiguration muss einige Anforderungen erfüllen, bevor Sie Volumes für Azure NetApp Files über Cloud Manager managen können.

1. Azure NetApp Files muss im Azure-Portal wie folgt eingerichtet werden:
   - "Für Azure NetApp Files anmelden"
   - "Erstellen Sie einen NetApp Account"
   - "Richten Sie einen Kapazitäts-Pool ein"
   - "Delegieren eines Subnetzes an Azure NetApp Files"
2. Cloud Manager muss wie folgt eingerichtet werden:
   - Cloud Manager muss in Azure ausgeführt werden – dem Konto, in dem Azure NetApp Files eingerichtet wurde.
   - Die virtuelle Maschine von Cloud Manager muss über ein Berechtigungen erhalten "Verwaltete Identität".

     Wenn Sie Cloud Manager über Cloud Central implementiert haben, sind alle Einstellungen eingerichtet. Cloud Central aktiviert automatisch eine vom System zugewiesene gemanagte Identität auf der virtuellen Maschine von Cloud Manager.

   Wenn Sie Cloud Manager über den Azure Marketplace implementiert haben, sollten Sie es gefolgt sein "Anweisungen zum Aktivieren einer verwalteten Identität".

   - Die Azure-Rolle, die der Virtual Machine Cloud Manager zugewiesen ist, muss die in der aktuellen Liste aufgeführten Berechtigungen enthalten "Cloud Manager-Richtlinie für Azure":

     ```
     "Microsoft.NetApp/netAppAccounts/read",
     "Microsoft.NetApp/netAppAccounts/capacityPools/read",
     "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
     "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
     "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete"
     ```

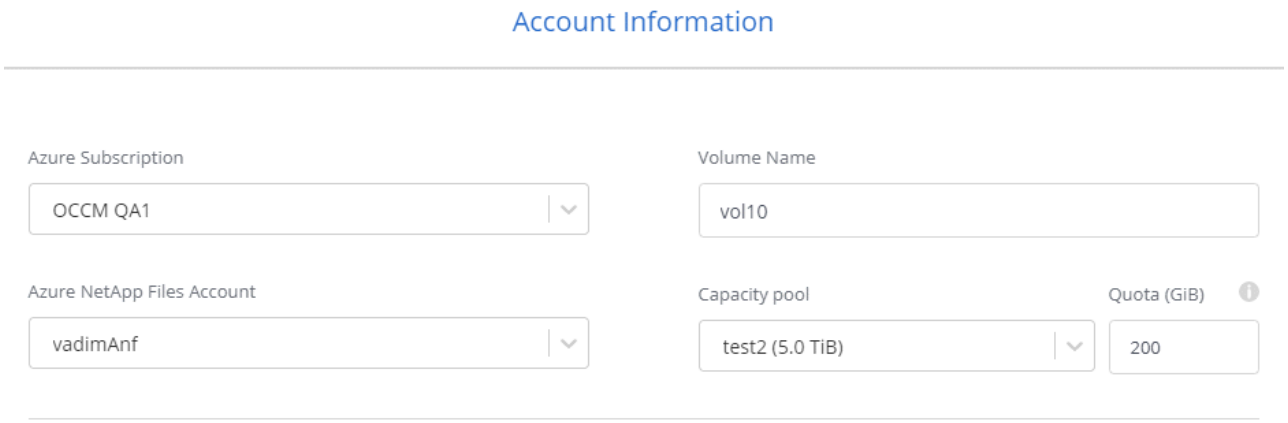
Wenn Ihre Konfiguration eingerichtet ist, zeigt Cloud Manager automatisch Azure NetApp Files auf der Seite Arbeitsumgebungen an:

Volumes werden erstellt

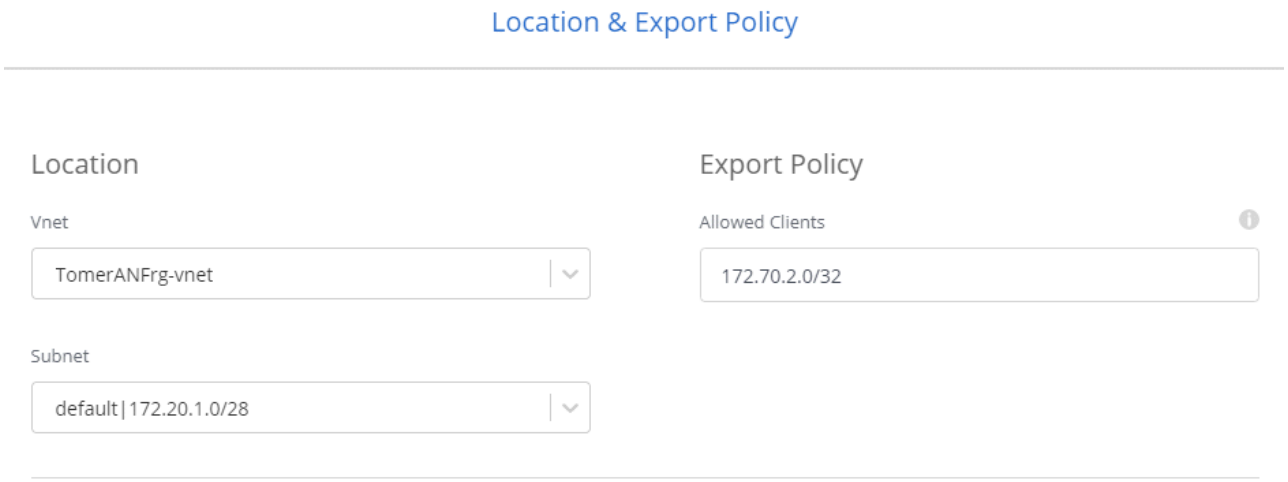
Cloud Manager ermöglicht Ihnen das Erstellen von NFSv3 Volumes für Azure NetApp Files.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Klicken Sie Auf **Neues Volume Hinzufügen**.
3. Geben Sie auf der Seite **Kontoinformationen** grundlegende Details zum Volume ein:
   a. Wählen Sie ein Azure Abonnement und ein Azure NetApp Files Konto aus.
   b. Geben Sie einen Namen für das Volume ein.
   c. Wählen Sie einen Kapazitätspool aus, und geben Sie ein Kontingent an, was der dem Volume zugewiesenen logischen Storage entspricht.



4. Füllen Sie die Seite **Location & Export Policy** aus:
   a. Wählen Sie ein vnet und ein Subnetz aus.
   b. Exportrichtlinie konfigurieren, um den Zugriff auf das Volume zu steuern



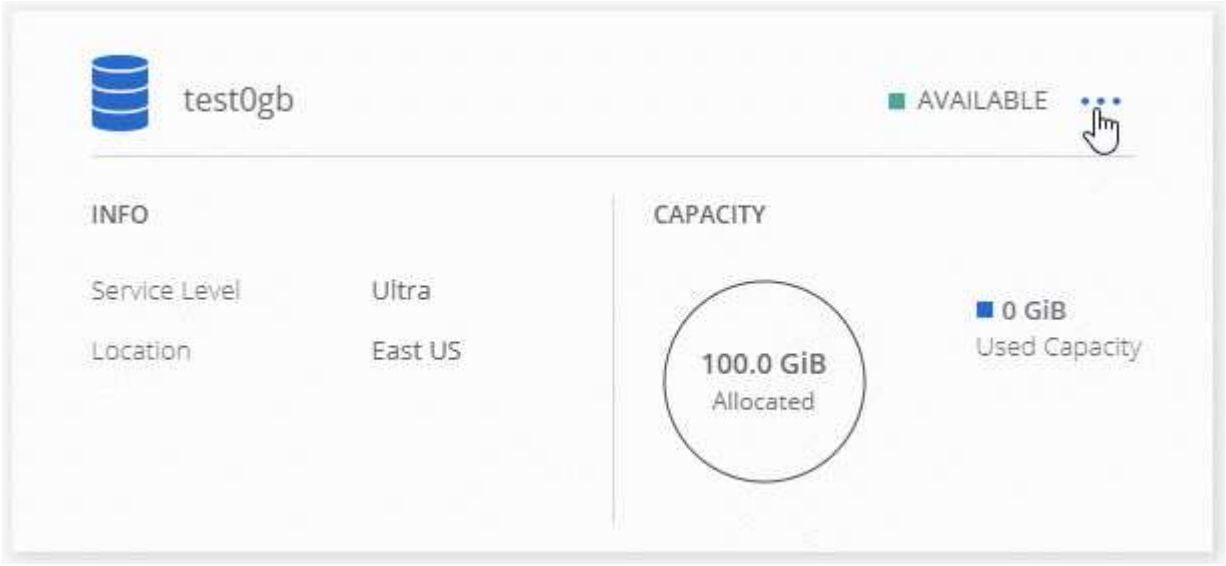
5. Klicken Sie Auf **Go**.

Abrufen des Bereitstellungspfads eines Volumes

Kopieren Sie den Mount-Pfad für ein Volume, damit Sie das Volume auf einem Linux-Rechner mounten können.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über die Lautstärke, und klicken Sie auf das Menü.



3. Klicken Sie Auf **Mount Command**.

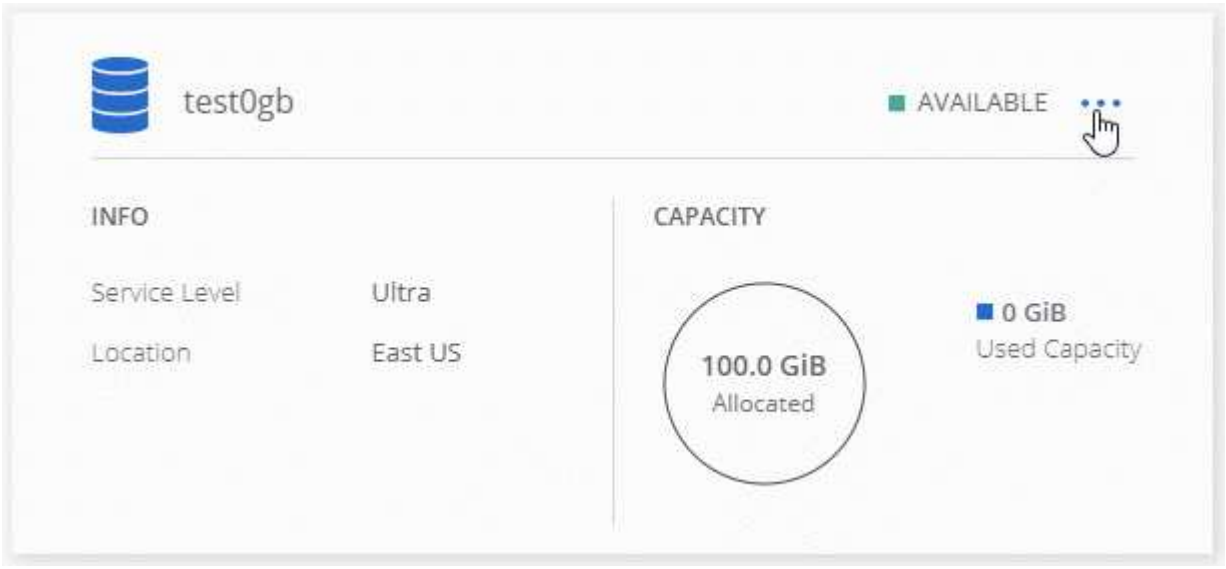
4. Kopieren Sie den Mount-Pfad, und verwenden Sie den kopierten Text, um das Volume auf einem Linux-Rechner zu mounten.

Volumes werden gelöscht

Löschen Sie die Volumes, die Sie nicht mehr benötigen.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über die Lautstärke, und klicken Sie auf das Menü.



3. Klicken Sie Auf **Löschen**.
4. Bestätigen Sie, dass Sie das Volume löschen möchten.

Hilfe wird abgerufen

Nutzen Sie den Cloud Manager Chat für allgemeine Servicefragen.

Bei Problemen mit dem technischen Support im Zusammenhang mit Azure NetApp Files können Sie im Azure-Portal eine Support-Anfrage an Microsoft protokollieren. Wählen Sie Ihr zugehöriges Microsoft-Abonnement aus, und wählen Sie den **Azure NetApp Files**-Dienstnamen unter **Speicherung.** aus. Geben Sie die verbleibenden Informationen an, die für die Erstellung Ihrer Microsoft-Supportanfrage erforderlich sind.

Cloud Manager bietet einen lokalen AutoSupport-Download unter der Menüoption **Support Dashboard**. Diese 7z-Datei enthält eine Azure-Debug-Datei, um ein- und ausgehende Kommunikation an Ihr Azure NetApp Files-Konto anzuzeigen.

Einschränkungen

- Cloud Manager unterstützt SMB Volumes nicht.
- Cloud Manager ermöglicht kein Management von Kapazitäts-Pools oder Volume Snapshots.
- Sie können Volumes mit einer Initialgröße und einer einzelnen Exportrichtlinie erstellen. Die Bearbeitung eines Volumes muss über die Azure NetApp Files Schnittstelle im Azure Portal erfolgen.
- Cloud Manager unterstützt keine Datenreplizierung von oder zu Azure NetApp Files.

Weiterführende Links

- "NetApp Cloud Central: Azure NetApp Files"
- "Azure NetApp Files-Dokumentation"

Management von Cloud Volumes Service für AWS

Cloud Manager ermöglicht es Ihnen, die NFS Cloud Volumes in Ihrer Erkennung zu erkennen "Cloud Volumes Service für AWS" Abonnement: Nach der Bestandsaufnahme können Sie zusätzliche NFS Cloud Volumes direkt aus Cloud Manager hinzufügen.

Cloud Manager unterstützt keine SMB- oder Dual-Protokoll-Volumes mit Cloud Volumes Service für AWS.

Bevor Sie beginnen

- Cloud Manager ermöglicht die Erkennung von vorhandenen_ Cloud Volumes Service für AWS Abonnements. Siehe "NetApp Cloud Volumes Service für AWS – Account Setup Guide" Wenn Sie Ihr Abonnement noch nicht eingerichtet haben.

  Sie müssen diesen Setup-Prozess für jede Region befolgen und Ihr erstes Volume über Cloud Volumes Service bereitstellen, bevor Sie die Region in Cloud Manager ermitteln können.

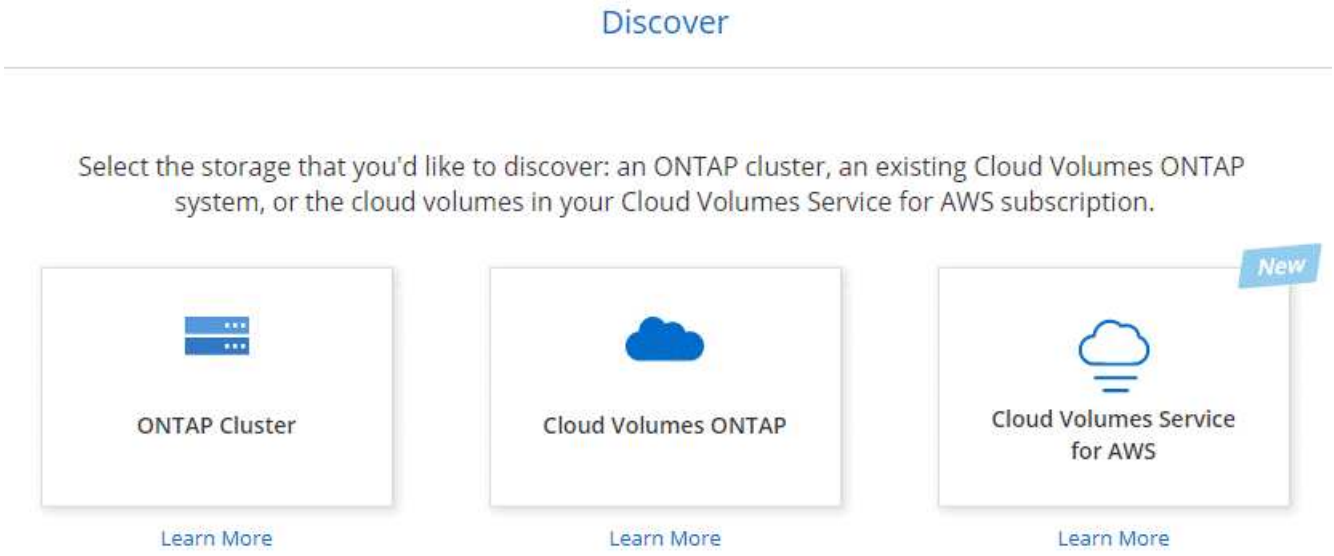
- Sie benötigen den API-Schlüssel und den geheimen Schlüssel von Cloud Volumes, damit Sie sie an Cloud Manager bereitstellen können. "Weitere Anweisungen finden Sie in der Dokumentation zu AWS in Cloud Volumes Service".

Abonnement von Cloud Volumes Service für AWS erkennen

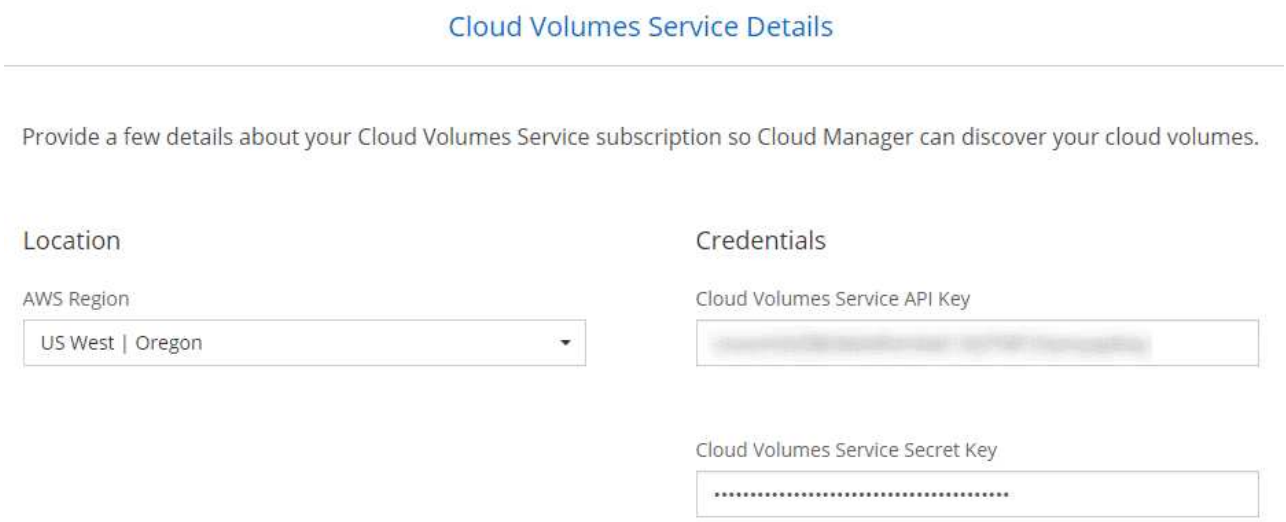
Zunächst müssen Sie die Cloud Volumes in einer AWS Region erkennen. Sie können später weitere Regionen entdecken.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Entdecken**.
2. Wählen Sie **Cloud Volumes Service für AWS** aus.



3. Stellen Sie Informationen zu Ihrem Cloud Volumes Service Abonnement bereit:
   a. Wählen Sie die Region von AWS aus, in der sich Ihre Cloud Volumes befinden.
   b. Geben Sie den API-Schlüssel und den geheimen Schlüssel von Cloud Volumes ein. "Weitere Anweisungen finden Sie in der Dokumentation zu AWS in Cloud Volumes Service".
   c. Klicken Sie Auf **Go**.



Ergebnis

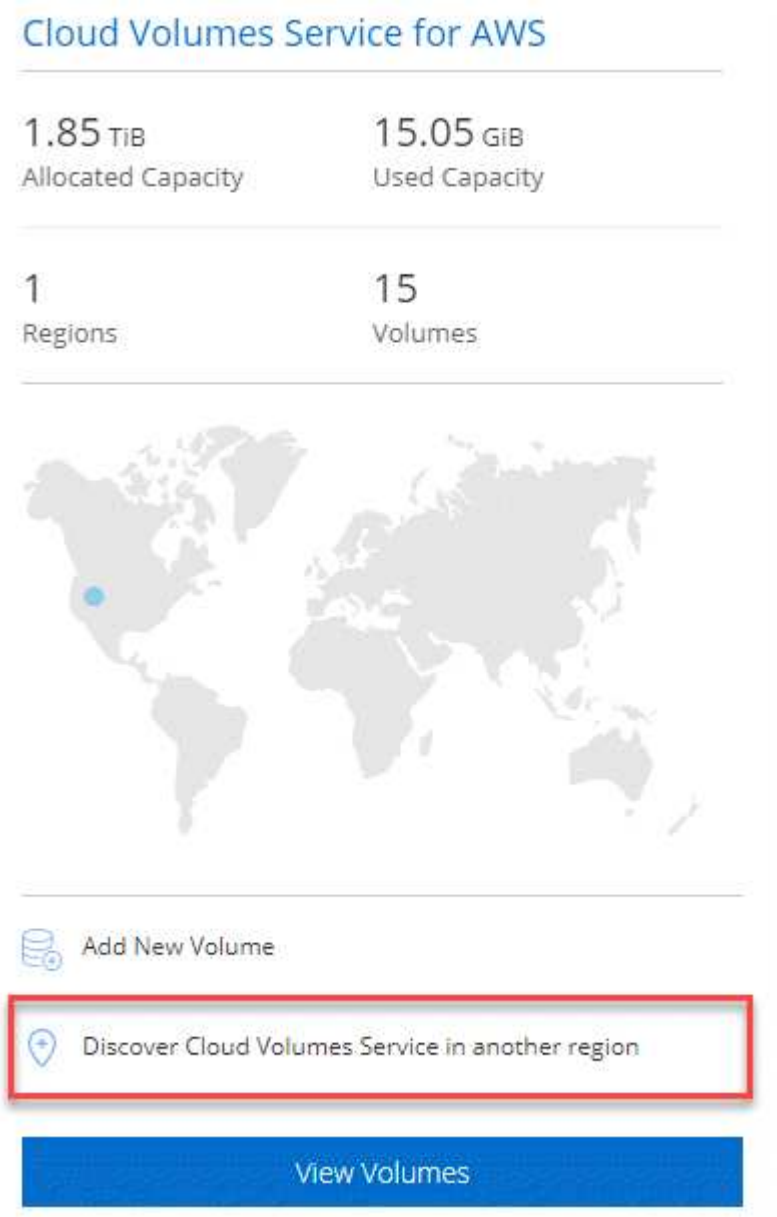
Cloud Manager sollte jetzt Ihre Cloud Volumes Service für AWS Konfiguration auf der Seite Arbeitsumgebungen anzeigen.

Entdecken weiterer Regionen

Wenn Cloud Volumes in zusätzlichen Regionen vorhanden sind, müssen Sie jede einzelne Region ermitteln.

Schritte

1. Wählen Sie auf der Seite Arbeitsumgebungen die Arbeitsumgebung aus (öffnen Sie sie jedoch nicht durch Doppelklicken).
2. Klicken Sie im rechten Fensterbereich auf **Cloud Volumes Service in einer anderen Region**.



3. Stellen Sie Informationen zu Ihrem Cloud Volumes Service Abonnement bereit:
   a. Wählen Sie die Region von AWS aus, in der sich Ihre Cloud Volumes befinden.
   b. Geben Sie den API-Schlüssel und den geheimen Schlüssel von Cloud Volumes ein. "Weitere Anweisungen finden Sie in der Dokumentation zu AWS in Cloud Volumes Service".
   c. Klicken Sie Auf **Go**.

Ergebnis

Cloud Manager ermittelt Informationen zu Cloud Volumes in der ausgewählten Region.

Erstellung von Cloud Volumes

Cloud Manager ermöglicht die Erstellung von NFSv3 Cloud Volumes. Cloud Volumes lassen sich nur mit einer Richtlinie für eine anfängliche Größe und einen einzelnen Export erstellen. Das Volume muss über die Benutzeroberfläche des Cloud Volume Service bearbeitet werden.

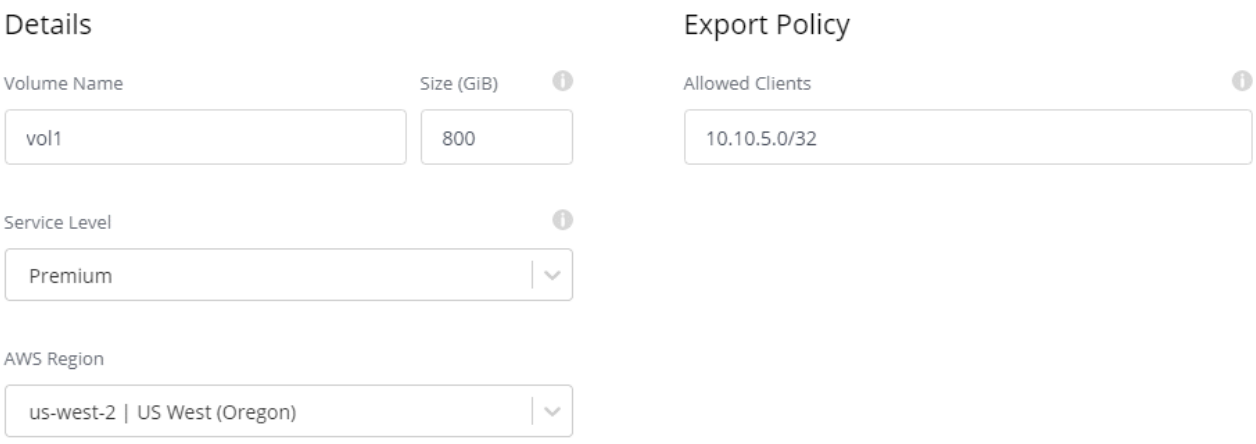
1. Öffnen Sie die Arbeitsumgebung.
2. Klicken Sie Auf **Neues Volume Hinzufügen**.
3. Geben Sie Details zum Volume ein:
   a. Geben Sie einen Namen für das Volume ein.
   b. Geben Sie eine Größe im Bereich von 100 gib bis 90,000 gib an (entspricht 88 TIBS).

      Cloud Manager zeigt Volumes in gib an, während auf der Cloud Volumes Service Volumes in GB angezeigt werden.

   c. Geben Sie ein Service-Level an: Standard, Premium oder Extreme.

      "Erfahren Sie mehr über diese Service Levels".

   d. Wählen Sie eine Region. Sie können das Volume in einer Region erstellen, die Cloud Manager erkannt hat.
   e. Beschränken Sie den Client-Zugriff, indem Sie eine IP-Adresse oder ein Classless Inter-Domain Routing (CIDR) angeben.



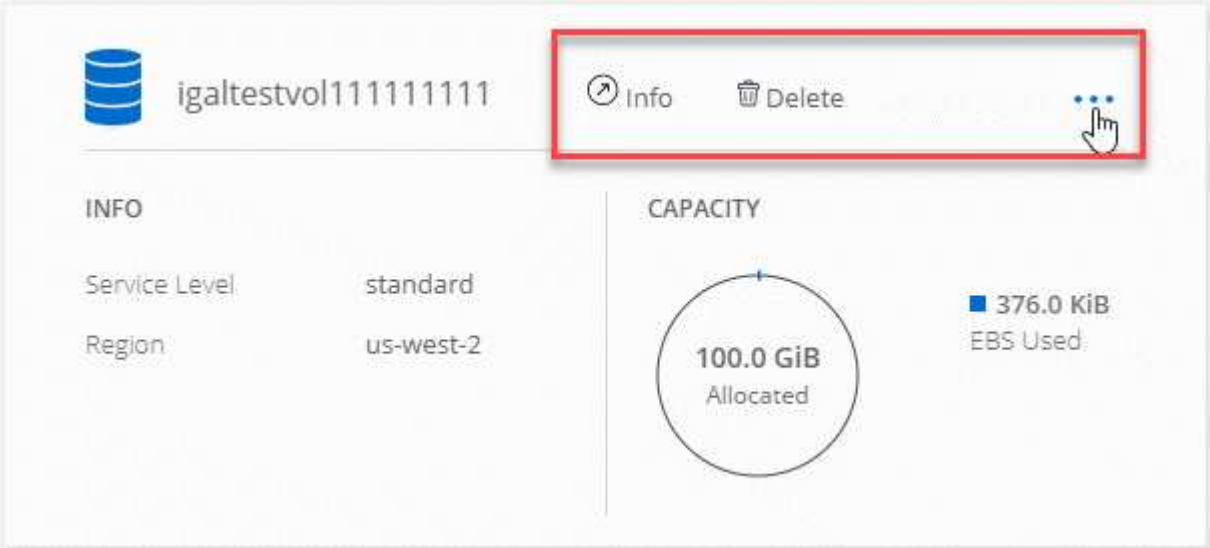
4. Klicken Sie Auf **Go**.

Cloud Volumes werden gelöscht

Löschen der nicht mehr benötigten Cloud-Volumes

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über die Lautstärke, und klicken Sie auf das Menü. Klicken Sie Auf **Löschen**.



3. Bestätigen Sie, dass Sie das Volume löschen möchten.

Hilfe wird abgerufen

Nutzen Sie den Cloud Manager Chat für allgemeine Servicefragen.

Bei technischen Support-Problemen im Zusammenhang mit Ihren Cloud Volumes verwenden Sie die 20-stellige Seriennummer „930“ auf der Registerkarte „Support“ der Cloud Volumes Service-Benutzeroberfläche. Verwenden Sie diese Support-ID, wenn Sie ein Web-Ticket öffnen oder Support-Anfrage stellen. Achten Sie darauf, Ihre Cloud Volumes Service Seriennummer für Support über die Cloud Volumes Service Benutzeroberfläche zu aktivieren. "Diese Schritte werden hier erläutert".

Einschränkungen

- Cloud Manager unterstützt SMB Volumes oder Dual-Protokoll-Volumes nicht.
- Cloud Volumes lassen sich nur mit einer Richtlinie für eine anfängliche Größe und einen einzelnen Export erstellen. Das Volume muss über die Benutzeroberfläche des Cloud Volume Service bearbeitet werden.
- Cloud Manager bietet keine Unterstützung für die Datenreplizierung von oder zu einem Cloud Volumes Service für AWS Abonnement.
- Das Entfernen des Cloud Volumes Service für AWS Abonnements aus Cloud Manager wird nicht unterstützt. Es sind keine Kosten für den Entdeckung einer Region von Cloud Manager anfallen.

Weiterführende Links

- "NetApp Cloud Central: Cloud Volumes Service für AWS"

- "NetApp Cloud Volumes Service für AWS – Dokumentation"

APIs und Automatisierung

Automatisierungsmuster für Infrastruktur als Code

Mithilfe der Ressourcen auf dieser Seite können Sie Hilfe bei der Integration von Cloud Manager und Cloud Volumes ONTAP in Ihr erhalten "Infrastruktur als Code".

DevOps-Teams verwenden diverse Tools zur Automatisierung des Setups neuer Umgebungen, mit denen sie Infrastruktur als Code behandeln können. Zwei solche Tools sind Ansible und Terraform. Wir haben Ansible und Terraform Proben entwickelt, die das DevOps-Team mit Cloud Manager verwenden kann, um Cloud Volumes ONTAP zu automatisieren und in Infrastruktur-als-Code zu integrieren.

"Sehen Sie sich die Beispiele für die Automatisierung an".

Sie können beispielsweise Beispiel-Playbooks mit Ansible verwenden, um Cloud Manager und Cloud Volumes ONTAP zu implementieren, ein Aggregat zu erstellen und ein Volume zu erstellen. Ändern Sie die Beispiele für Ihre Umgebung oder erstellen Sie anhand der Beispielbeispiele neue Playbooks.

Verwandte Links

- "NetApp Cloud Blog: Verwendung VON Cloud Manager REST-APIs mit Federated Access"
- "NetApp Cloud Blog: Cloud-Automatisierung mit Cloud Volumes ONTAP und REST"
- "NetApp Cloud Blog: Automatisiertes Klonen von Daten für Cloud-basierte Tests von Softwareapplikationen"
- "NetApp Blog: Von Infrastructure-as-Code (IAC) mit Ansible und NetApp beschleunigt"
- "NetApp thePub: Configuration Management Automation with Ansible"
- "NetApp thePub – Rollen für den Einsatz von Ansible-ONTAP"

Referenz

Häufig gestellte Fragen: Integration von Cloud Manager in NetApp Cloud Central

Beim Upgrade von Cloud Manager 3.4 oder einer älteren Version wählt NetApp bestimmte Cloud Manager Systeme aus, die sich in NetApp Cloud Central integrieren lassen, sofern sie nicht bereits integriert sind. In dieser FAQ können Sie Fragen zu diesem Prozess beantworten.

Was ist NetApp Cloud Central?

NetApp Cloud Central bietet einen zentralen Standort für den Zugriff auf und das Management von NetApp Cloud Data Services. 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.

Warum integriert NetApp mein Cloud Manager-System in Cloud Central?

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.

Was passiert während des Integrationsprozesses?

NetApp migriert alle lokalen Benutzerkonten in Ihrem Cloud Manager-System auf die zentralisierte Benutzerauthentifizierung, die in Cloud Central verfügbar ist.

Wie funktioniert die 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.

Muss ich mich für ein Cloud Central Benutzerkonto anmelden?

NetApp erstellt für Sie ein Cloud Central Benutzerkonto, wenn wir Ihr Cloud Manager System in Cloud Central integrieren. Sie müssen Ihr Passwort zurücksetzen, um die Registrierung abzuschließen.

Was passiert, wenn ich bereits ein Cloud Central Benutzerkonto habe?

Wenn die E-Mail-Adresse, mit der Sie sich bei Cloud Manager anmelden, mit der E-Mail-Adresse für ein Cloud Central-Benutzerkonto übereinstimmt, können Sie sich direkt bei Ihrem Cloud Manager-System anmelden.

Was ist, wenn mein Cloud Manager-System über mehrere Benutzerkonten verfügt?

NetApp migriert alle lokalen Benutzerkonten zu Cloud Central Benutzerkonten. Jeder Benutzer muss sein Passwort zurücksetzen.

Was passiert, wenn ich ein Benutzerkonto habe, das dieselbe E-Mail-Adresse in mehreren Cloud Manager-Systemen verwendet?

Sie müssen Ihr Kennwort nur einmal zurücksetzen. Anschließend können Sie sich über dasselbe Cloud Central-Benutzerkonto bei jedem Cloud Manager-System anmelden.

Was geschieht, wenn mein lokales Benutzerkonto eine ungültige E-Mail-Adresse verwendet?

Zum Zurücksetzen des Passworts ist eine gültige E-Mail-Adresse erforderlich. Kontaktieren Sie uns über das Chat-Symbol unten rechts in der Cloud Manager-Oberfläche.

Was ist, wenn ich Automatisierungsskripts für Cloud Manager-APIs habe?

Alle APIs sind abwärtskompatibel. Sie müssen Skripts aktualisieren, die Kennwörter verwenden, wenn Sie Ihr Kennwort ändern, wenn Sie es zurücksetzen.

Was ist, wenn mein Cloud Manager-System LDAP verwendet?

Wenn Ihr System LDAP verwendet, kann NetApp das System nicht automatisch in Cloud Central integrieren. Sie müssen die folgenden Schritte manuell ausführen:

1. Implementieren Sie ein neues Cloud Manager System von "NetApp Cloud Central".
2. "Richten Sie LDAP mit dem neuen System ein".
3. "Erkennung vorhandener Cloud Volumes ONTAP Systeme" Über das neue Cloud Manager System.
4. Löschen Sie das alte Cloud Manager-System.

Spielt es eine Rolle, wo ich mein Cloud Manager-System installiert habe?

Nein NetApp integriert Systeme in Cloud Central, unabhängig davon, wo sie sich befinden, ob AWS, Azure oder in Ihrem Unternehmen.

Die einzige Ausnahme bildet die AWS Commercial Cloud Services Environment.

Sicherheitsgruppenregeln für AWS

Cloud Manager erstellt AWS-Sicherheitsgruppen, die die ein- und ausgehenden Regeln enthalten, die Cloud Manager und Cloud Volumes ONTAP für einen erfolgreichen Betrieb benötigen. Sie können die Ports zu Testzwecken oder zur Verwendung eigener Sicherheitsgruppen verwenden.

Regeln für Cloud Manager

Für die Sicherheitsgruppe für Cloud Manager sind sowohl eingehende als auch ausgehende Regeln erforderlich.

Eingehende Regeln für Cloud Manager

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 Cloud Manager-Host
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern zur Cloud Manager Webkonsole und -Verbindungen über Cloud-Compliance
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die Cloud Manager-Webkonsole
TCP	3128	Bietet die Cloud Compliance-Instanz einen Internetzugang, wenn Ihr AWS-Netzwerk keine NAT oder Proxy verwendet

Outbound-Regeln für Cloud Manager

Die vordefinierte Sicherheitsgruppe für Cloud Manager 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 Manager 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 Cloud Manager erforderlich sind.

Die Quell-IP-Adresse ist der Cloud Manager-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
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

Regeln für Cloud Volumes ONTAP

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

Eingehende Regeln für Cloud Volumes ONTAP

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

Outbound-Regeln für Cloud Volumes ONTAP

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	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	Data LIF (NFS, CIFS)	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	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)
Backup auf S3	TCP	5010	Intercluster-LIF	Backup-Endpunkt oder Wiederherstellungsendpunkt	Backup- und Restore-Vorgänge für die Funktion „Backup in S3“

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

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	Ruhiger API-Zugriff über Cloud Manager

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	IP-Adresse von Cloud Manager	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

Sicherheitsgruppenregeln für Azure

Cloud Manager erstellt Azure Sicherheitsgruppen, die die ein- und ausgehenden Regeln enthalten, die Cloud Manager und Cloud Volumes ONTAP für einen erfolgreichen Betrieb benötigen. Sie können die Ports zu Testzwecken oder zur Verwendung eigener Sicherheitsgruppen verwenden.

Regeln für Cloud Manager

Für die Sicherheitsgruppe für Cloud Manager sind sowohl eingehende als auch ausgehende Regeln erforderlich.

Eingehende Regeln für Cloud Manager

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 Cloud Manager-Host
80	HTTP	Bietet HTTP-Zugriff von Client-Webbrowsern auf die Cloud Manager-Webkonsole
443	HTTPS	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die Cloud Manager-Webkonsole

Outbound-Regeln für Cloud Manager

Die vordefinierte Sicherheitsgruppe für Cloud Manager 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 Manager 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 Cloud Manager erforderlich sind.

Die Quell-IP-Adresse ist der Cloud Manager-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

Service	Port	Protokoll	Ziel	Zweck
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

Regeln für Cloud Volumes ONTAP

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
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

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
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
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

Outbound-Regeln für Cloud Volumes ONTAP

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	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	Data LIF (NFS, CIFS)	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	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
DHCPS	67	UDP	Node Management-LIF	DHCP	DHCP-Server

Service	Port	Protokoll	Quelle	Ziel	Zweck
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

Firewall-Regeln für GCP

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.

Regeln für Cloud Manager

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

Eingehende Regeln für Cloud Manager

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 Cloud Manager-Host

Protokoll	Port	Zweck
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die Cloud Manager-Webkonsole
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die Cloud Manager-Webkonsole

Outbound-Regeln für Cloud Manager

Die vordefinierten Firewall-Regeln für Cloud Manager 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 Cloud Manager umfassen die folgenden Outbound-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 Cloud Manager erforderlich sind.

Die Quell-IP-Adresse ist der Cloud Manager-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

Regeln für Cloud Volumes ONTAP

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

Eingehende Regeln für Cloud Volumes ONTAP

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

Outbound-Regeln für Cloud Volumes ONTAP

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	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	Data LIF (NFS, CIFS)	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	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

AWS Marketplace-Seiten für Cloud Manager und Cloud Volumes ONTAP

Im AWS Marketplace für Cloud Manager und Cloud Volumes ONTAP sind diverse

Angebote erhältlich. Wenn Sie sich nicht sicher sind, welche Seite Sie verwenden müssen, lesen Sie weiter unten. Wir leiten Sie entsprechend Ihrem Ziel auf die richtige Seite weiter.

Vergessen Sie in jedem Fall nicht, dass Sie Cloud Volumes ONTAP nicht über den AWS Marketplace in AWS starten können. Sie müssen es direkt über Cloud Manager starten.

Ziel	Zu verwendende AWS Marketplace Seite	Weitere Informationen
Implementierung von Cloud Volumes ONTAP PAYGO für Version 9.6 und höher ermöglichen	"Cloud Manager (für Cloud Volumes ONTAP)"	Auf dieser AWS Marketplace-Seite können Gebühren für die PAYGO-Version von Cloud Volumes ONTAP 9.6 und höher berechnet werden. Es ermöglicht außerdem das Aufladen von Cloud Volumes ONTAP-Zusatzfunktionen. Auf dieser Seite können Sie Cloud Manager in AWS nicht starten. Das sollte von geschehen "NetApp Cloud Central", Oder alternativ das AMI in Zeile 4 dieser Tabelle verwenden.
Add-on-Funktionen für Cloud Volumes ONTAP (PAYGO oder BYOL) aktivieren		
Implementierung von Cloud Volumes ONTAP mit einer Lizenz aktivieren, die ich von NetApp (BYOL) erworben habe	• "Cloud Volumes ONTAP für AWS (BYOL)" • "Cloud Volumes ONTAP für AWS – Hochverfügbarkeit (BYOL)"	Auf diesen AWS Marketplace-Seiten können Sie die Single Node- oder HA-Versionen von Cloud Volumes ONTAP BYOL abonnieren.
Implementieren Sie Cloud Manager über AWS Marketplace über ein AMI	"NetApp Cloud Manager (für NetApp Cloud Volumes ONTAP)"	Wir empfehlen Ihnen, Cloud Manager in AWS ab zu starten "NetApp Cloud Central", Aber Sie können es auf dieser AWS Marketplace Seite starten, wenn Sie es bevorzugen.
Implementierung von Cloud Volumes ONTAP PAYGO (9.5 oder früher) ermöglichen	• "Cloud Volumes ONTAP für AWS" • "Cloud Volumes ONTAP für AWS – Hochverfügbarkeit"	Auf diesen AWS Marketplace-Seiten können Sie für Version 9.5 und früher die Single Node- oder HA-Versionen von Cloud Volumes ONTAP PAYGO abonnieren. Ab Version 9.6 müssen Sie die Anmeldung über die in Zeile 1 dieser Tabelle aufgeführten AWS Marketplace-Seite für PAYGO-Implementierungen durchführen.

Wie Cloud Manager die Berechtigungen von Cloud-Providern nutzt

Für die Ausführung von Aktionen bei Ihrem Cloud-Provider sind für Cloud Manager

Berechtigungen erforderlich. Diese Berechtigungen sind in enthalten "Die von NetApp bereitgestellten Richtlinien". Sie möchten vielleicht wissen, was Cloud Manager mit diesen Berechtigungen macht.

Was Cloud Manager mit AWS-Berechtigungen macht

Cloud Manager verwendet ein AWS-Konto, um API-Aufrufe an mehrere AWS-Services durchzuführen, darunter EC2, S3, CloudFormation, IAM, den Security Token Service (STS) und den Key Management Service (KMS).

Aktionen	Zweck
„ec2:StartInstances“, „ec2:StopInstances“, „ec2:DescribeInstances“, „ec2:DescribeInstanceStatus“, „ec2:RunInstances“, „ec2:TerminateInstances“, „ec2:ModifyInstanceAttribut“,	Startet eine Cloud Volumes ONTAP Instanz und stoppt, startet und überwacht die Instanz.
"EC2:DescribeInstanceAttribute",	Überprüft, ob das erweiterte Netzwerk für unterstützte Instanztypen aktiviert ist.
„ec2:DescribeRouteTables“, „ec2:DescribeImages“,	Startet eine Cloud Volumes ONTAP HA-Konfiguration.
"EC2:CreateTags",	Kennzeichnet jede Ressource, die Cloud Manager erstellt, mit den Tags "workingenvironment" und "WorkingEnvironmentId". Cloud Manager verwendet diese Tags für Wartung und Kostenzuordnung.
„ec2:CreateVolume“, „ec2:DescribeVolumes“, „ec2:ModifyVolumeAttribute“, „ec2:AttachVolume“, „ec2:DeleteVolume“, „ec2:DetachVolume“,	Managt die EBS Volumes, die Cloud Volumes ONTAP als Back-End Storage verwendet.
„ec2:CreateSecurityGroup“, „ec2:DeleteSecurityGroup“, „ec2:DescribeSecurityGroups“, „ec2:RevokeSecurityGroupEgress“, „ec2:AuthoriseSecurityGroupEgress“, „ec2:AuthoriseSecurityGroupIngress“, „ec2:RevokeSecurityGroupIngress“,	Erstellt vordefinierte Sicherheitsgruppen für Cloud Volumes ONTAP.
„ec2:CreateNetworkInterface“, „ec2:DescribeNetworkInterfaces“, „ec2:DeleteNetworkInterface“, „ec2:ModifyNetworkInterface“,	Erstellt und managt Netzwerkschnittstellen für Cloud Volumes ONTAP im Ziel-Subnetz.
„ec2:DescribeSubnets“, „ec2:DescribeVpcs“,	Ruft die Liste der Zielsubnetze und Sicherheitsgruppen ab, die beim Erstellen einer neuen Arbeitsumgebung für Cloud Volumes ONTAP benötigt wird.
"EC2:DescribeDhcpOptions",	Bestimmt DNS-Server und den Standarddomänennamen beim Starten von Cloud Volumes ONTAP Instanzen.
„ec2:CreateSnapshot“, „ec2:DeleteSnapshot“, „ec2:DescribeSnapshots“,	Erstellt Snapshots von EBS Volumes während der Ersteinrichtung und bei jedem Anhalten einer Cloud Volumes ONTAP Instanz.

Aktionen	Zweck
"EC2:GetConsoleOutput",	Erfasst die Cloud Volumes ONTAP Konsole, die an AutoSupport Nachrichten angehängt ist.
"EC2:DescribeKeyPairs",	Ruft beim Starten von Instanzen die Liste der verfügbaren Schlüsselpaare ab.
"EC2:DescribeRegions",	Ruft eine Liste der verfügbaren AWS-Regionen ab.
„ec2:DeleteTags“, „ec2:DescribeTags“,	Managt Tags für Ressourcen, die mit Cloud Volumes ONTAP Instanzen verbunden sind.
„Cloudformation:CreateStack“, „Cloudformation:DeleteStack“, „Cloudformation:DescribeStacks“, „Cloudformation:DescribeStackEvents“, „Cloudformation:ValidateTemplate“,	Startet Cloud Volumes ONTAP Instanzen.
„iam:PassRollenole“, „iam:CreateRollenole“, „iam:DeleteRollenole“, „iam:PutRolePolicy“, „iam:CreateInstanceProfil“, „iam:DeleteRolePolicy“, „iam:AddRoleToInstanceProfile“, „iam:RemoveRoleFromInstanceProfile“, „iam:DeleteInstanceProfile“,	Startet eine Cloud Volumes ONTAP HA-Konfiguration.
„iam:ListInstanceProfiles“, „STS:DecodeAuthorisationMessage“, „ec2:AssociateIamInstanceProfil“, „ec2:DescribeIamInstanceProfilAssociations“, „ec2:DisassotionIamInstanceProfile“,	Managt Instanzprofile für Cloud Volumes ONTAP Instanzen.
„s3:GetBucketTagging“, „s3:GetBucketLocation“, „s3:ListAllMyBuckets“, „s3:ListBucket“	Informationen zu AWS S3-Buckets, damit Cloud Manager in den NetApp Data Fabric Cloud Sync Service integriert werden kann
„s3:CreateBucket“, „s3:DeleteBucket“, „s3:GetLifecycleConfiguration“, „s3:PutLifecycleConfiguration“, „s3:PutBucketTagging“, „s3:ListBucketVersions“,	Managt den S3-Bucket, den ein Cloud Volumes ONTAP System als Kapazitäts-Tier verwendet.
„Kms:Liste*“, „Kms:Beschreiben*“	Ruft Informationen zu Schlüsseln vom AWS Key Management Service ab.
„ce:GetReservationUtilisation“, „ce:GetDimensionValues“, „ce:GetCostAndUsage“, „ce:GetTags“	Abrufen von AWS-Kostendaten für Cloud Volumes ONTAP
„ec2:CreatePlacementGroup“, „ec2:DeletePlacementGroup“	Wenn Sie eine HA-Konfiguration in einer einzigen AWS Availability Zone implementieren, startet Cloud Manager die beiden HA-Nodes und den Mediator in einer AWS Spread-Placement-Gruppe.

Was Cloud Manager mit Azure-Berechtigungen tut

Die Cloud Manager Azure Policy enthält die Berechtigungen, die Cloud Manager für die Bereitstellung und das Management von Cloud Volumes ONTAP in Azure benötigt.

Aktionen	Zweck
„Microsoft.Compute/locations/operations/read", „Microsoft.Compute/locations/vmSizes/read", „Microsoft.Compute/operations/read", „Microsoft.Compute/virtualMachines/instanceView/read", „Microsoft.Compute/virtualMachines/powerOff/action", „Microsoft.Compute/virtualMachines/read", „Microsoft.Compute/virtualMachines/restart/action", „Microsoft.Compute/virtualMachines/start/action", „Microsoft.Compute/virtualMachines/deallocate/action", „Microsoft.Compute/virtualMachines/vmSizes/read", „Microsoft.Compute/virtualMachines/write",	Erstellt Cloud Volumes ONTAP und beendet, startet, löscht und erhält den Status des Systems.
„Microsoft.Compute/images/write", „Microsoft.Compute/images/read",	Ermöglicht die Implementierung von Cloud Volumes ONTAP über eine VHD.
„Microsoft.Compute/disks/delete", „Microsoft.Compute/disks/read", „Microsoft.Compute/disks/write", „Microsoft.Storage/ChecknameAvailability/read“, „Microsoft.Storage/Operations/read“, „Microsoft.Storage/StorageAccounts/Listkeys/Action“, „Microsoft.Storage/StorageAccounts/read“, „Microsoft.Storage/storageAccounts/Retgeneratekey/Action“, „Microsoft.Storage/storageAccounts/write“, „Microsoft.Storage/storageAccounts/delete“, „Microsoft.Storage/Nutzungs/Lesevorgang“,	Verwaltet Azure Storage-Konten und -Festplatten und hängt die Festplatten an Cloud Volumes ONTAP an.
„Microsoft.Network/networkInterfaces/read", „Microsoft.Network/networkInterfaces/write", „Microsoft.Network/networkInterfaces/join/action",	Erstellt und managt Netzwerkschnittstellen für Cloud Volumes ONTAP im Ziel-Subnetz.
„Microsoft.Network/networkSecurityGroups/read", „Microsoft.Network/networkSecurityGroups/write", „Microsoft.Network/networkSecurityGroups/join/action",	Erstellt vordefinierte Netzwerksicherheitsgruppen für Cloud Volumes ONTAP.
„Microsoft.Ressourcen/Abonnements/Standorte/gelesen“, „Microsoft.Network/locations/operationResults/read", „Microsoft.Network/locations/operations/read", „Microsoft.Network/virtualNetworks/read", „Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read", „Microsoft.Network/virtualNetworks/subnets/read", „Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", „Microsoft.Network/virtualNetworks/virtualMachines/read", „Microsoft.Network/virtualNetworks/subnets/join/action",	Ruft Netzwerkinformationen zu Regionen, dem Ziel-VNet und dem Subnetz ab und fügt Cloud Volumes ONTAP VNets hinzu.
„Microsoft.Network/virtualNetworks/subnets/write", „Microsoft.Network/routeTables/join/action",	Aktiviert VNet Service-Endpunkte für das Daten-Tiering.

Aktionen	Zweck
„Microsoft.Ressourcen/Implementierungen/Betrieb/Lesen“, „Microsoft.Resources/Deployments/read“, „Microsoft.Resources/Deployments/write“,	Implementierung von Cloud Volumes ONTAP anhand einer Vorlage
„Microsoft.Resources/Deployments/Operations/read“, „Microsoft.Resources/Deployments/read“, „Microsoft.Resources/Deployments/write“, „Microsoft.Resources/Resources/read“, „Microsoft.Resources/Subscriptions/Operationresults/read“, „Microsoft.Resources/subskriptions/resourceGroups/delete“, „Microsoft.Resources/Subskriptions/resourceGroups/read“, „Microsoft.Resources/subskriptions/resourcegruppen/Resources/read“, „Microsoft.Resources/subskriptions/resourceGroups/write“,	Erstellt und managt Ressourcengruppen für Cloud Volumes ONTAP.
„Microsoft.Compute/snapshots/write", „Microsoft.Compute/snapshots/read", „Microsoft.Compute/disks/beginGetAccess/action"	Erstellt und managt von Azure verwaltete Snapshots.
„Microsoft.Compute/availabilitySets/write", „Microsoft.Compute/availabilitySets/read",	Erstellt und managt Verfügbarkeitssätze für Cloud Volumes ONTAP.
„Microsoft.MarketplaceOrdering/offertypes/Publisher/offerers/Plans/Agreements/read“, „Microsoft.MarketplaceOrdering/offertypes/Publisher/Offerers/Plans/Agreements/write“	Ermöglicht programmatische Implementierungen über Azure Marketplace.
„Microsoft.Network/loadBalancers/read", „Microsoft.Network/loadBalancers/write", „Microsoft.Network/loadBalancers/delete", „Microsoft.Network/loadBalancers/backendAddressPools/read", „Microsoft.Network/loadBalancers/backendAddressPools/join/action", „Microsoft.Network/loadBalancers/frontendIPConfigurations/read", „Microsoft.Network/loadBalancers/loadBalancingRules/read", „Microsoft.Network/loadBalancers/probes/read", „Microsoft.Network/loadBalancers/probes/join/action",	Managt einen Azure Load Balancer für HA-Paare.
"Microsoft.Authorization/locks/*"	Ermöglicht das Management von Sperren auf Azure Festplatten.
„Microsoft.Authorization/roleDefinitions/write“, „Microsoft.Authorization/roleAssignments/write“, „Microsoft.Web/sites/*“	Managt Failover für HA-Paare

Was Cloud Manager mit GCP-Berechtigungen macht

Die Cloud Manager-Richtlinie für GCP beinhaltet die Berechtigungen, die Cloud Manager für die Implementierung und das Management von Cloud Volumes ONTAP benötigt.

Aktionen	Zweck
- Compute.Disks.create - Compute.Disks.createSnapshot - compute.disks.delete - Compute.Disks.get - Compute.Disks.list - compute.disks.setLabels - compute.disks.use	Zum Erstellen und Verwalten von Festplatten für Cloud Volumes ONTAP.
- Compute.Firewalls.create - compute.firewalls.delete - Compute.Firewalls.get - Compute.Firewalls.list	Um Firewall-Regeln für Cloud Volumes ONTAP zu erstellen.
- Compute.globalOperations.get	Um den Status von Vorgängen anzuzeigen.
- Compute.images.get - Compute.images.getFromFamily - Compute.images.list - compute.images.useReadOnly	Um Images für VM-Instanzen zu erhalten.
- compute.instances.attachDisk - compute.instances.detachDisk	Zum Verbinden und Trennen von Festplatten mit Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Um Cloud Volumes ONTAP VM-Instanzen zu erstellen und zu löschen.
- compute.instances.get	Um VM-Instanzen aufzulisten.
- compute.instances.getSerialPortOutput	Um Konsolenprotokolle zu erhalten.
- compute.instances.list	Um die Liste der Instanzen in einer Zone abzurufen.
- compute.instances.setDeletionProtection	So legen Sie den Löschschutz für die Instanz fest:
- compute.instances.setLabels	So fügen Sie Etiketten hinzu:
- compute.instances.setMachineType	So ändern Sie den Maschinentyp für Cloud Volumes ONTAP.
- compute.instances.setMetadata	Um Metadaten hinzuzufügen.
- compute.instances.setTags	Um Tags für Firewall-Regeln hinzuzufügen.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Um Cloud Volumes ONTAP zu starten und anzuhalten.
- Compute.machineTypes.get	Um die Anzahl der Kerne zu erhalten, um qouten zu überprüfen.
- compute.projects.get	Zur Unterstützung mehrerer Projekte.
- Compute.Snapshots.create - compute.snapshots.delete - Compute.Snapshots.get - Compute.Snapshots.list - compute.snapshots.setLabels	Um persistente Festplatten-Snapshots zu erstellen und zu managen.

Aktionen	Zweck
- compute.networks.get - compute.networks.list - Compute.Regions.get - Compute.Regions.list - Compute.subNetworks.get - Compute.subNetworks.list - Compute.zoneOperations.get - Compute.Zones.get - Compute.Zones.list	Um die Netzwerkinformationen zu erhalten, die für die Erstellung einer neuen Instanz einer Cloud Volumes ONTAP Virtual Machine erforderlich sind.
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - istmentmanager.Manifeste.get - istmentmanager.manifeste.list - istmentmanager.Operations.get - istmentmanager.Operations.list - bereitsmanager.Resources.get - bereitsmanager.Resources.list - Bereitstellungmanager.typeProviders.get - istmentmanager.tyArten.list	Um die Cloud Volumes ONTAP VM-Instanz mithilfe von Google Cloud Deployment Manager bereitzustellen.
- Logging.logEntries.list - Logging.privateLogEntries.list	Zum Abrufen von Stack-Protokolllaufwerken.
- resourcemanager.projects.get	Zur Unterstützung mehrerer Projekte.
- Storage.Buckets.create - storage.buckets.delete - Storage.Buckets.get - Storage.Buckets.list	Zur Erstellung und Verwaltung eines Google Cloud Storage Buckets für Daten-Tiering
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.kryptoKeys.get - cloudkms.kryptoKeys.list - cloudkms.Keyrings.list	Verwenden von vom Kunden gemanagten Verschlüsselungen aus dem Cloud-Verschlüsselungsmanagement-Service mit Cloud Volumes ONTAP.

Standardkonfigurationen

Details zur Konfiguration von Cloud Manager und Cloud Volumes ONTAP können Ihnen bei der Administration der Systeme helfen.

Standardkonfiguration für Cloud Manager unter Linux

Wenn Sie eine Fehlerbehebung für Cloud Manager oder Ihren Linux-Host durchführen müssen, kann dies dazu beitragen, die Konfiguration von Cloud Manager zu verstehen.

- Wenn Sie Cloud Manager von NetApp Cloud Central (oder direkt aus dem Marketplace eines Cloud-Providers) implementiert haben, beachten Sie Folgendes:
  - In AWS lautet der Benutzername für die EC2 Linux-Instanz ec2-user.
  - Das Betriebssystem für das Cloud Manager Image ist Red hat Enterprise Linux 7.4 (HVM).

    Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.

- Der Installationsordner von Cloud Manager befindet sich am folgenden Speicherort:

  /opt/application/netapp/cloudmanager

- Protokolldateien befinden sich im folgenden Ordner:

  /opt/application/netapp/cloudmanager/log

- Der Cloud Manager Service heißt occm.
- Der occm-Dienst ist vom MySQL-Dienst abhängig.

  Wenn der MySQL-Dienst nicht verfügbar ist, ist auch der occm-Dienst nicht verfügbar.

- Cloud Manager installiert die folgenden Pakete auf dem Linux-Host, sofern sie noch nicht installiert sind:
  - 7-Zip
  - AWSCLI
  - Java
  - Kubectl
  - MySQL
  - Tridentctl
  - Wget

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.

- 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 Data Serving SVM. Die Verwendung mehrerer Datenservice-SVMs wird nicht unterstützt.
- 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 Cloud Manager.

  Wenn Sie sich bei Cloud Manager anmelden, können Sie über die Backup-Daten darauf zugreifen https://ipaddress/occm/offboxconfig/

- 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 universell einsetzbare SSD-Festplatten:
  - Eine 140-GB-Festplatte für Stammdaten (eine pro Node)
  - 9.6 oder höher: Eine 86-GB-Festplatte für Boot-Daten (eine pro Node)
  - 9.5 und früher: Eine 45-GB-Festplatte für Boot-Daten (eine pro Node)
- 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)

- Zwei Premium-SSD-Festplatten:
  - Eine 90-GB-Festplatte für Boot-Daten
  - Eine 140-GB-Festplatte für Stammdaten
- Ein Azure Snapshot für jedes Boot- und Root-Laufwerk

Azure (HA-Paare)

- Zwei 90-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 128-GB-Standard-HDD-Festplatten zum Speichern der Cores (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.

Rollen

Die Rollen Kontoadministrator und Workspace-Administrator bieten Benutzern spezifische Berechtigungen.

Aufgabe	Kontoadministrator	Workspace-Verwaltung
Verwalten von Arbeitsumgebungen	Ja.	Ja, für die zugehörigen Arbeitsbereiche
Anzeigen des Status der Datenreplizierung	Ja.	Ja, für die zugehörigen Arbeitsbereiche
Zeitachse anzeigen	Ja.	Ja, für die zugehörigen Arbeitsbereiche
Arbeitsumgebungen löschen	Ja.	Nein
Kubernetes-Cluster mit Cloud Volumes ONTAP verbinden	Ja.	Nein
Cloud Volumes ONTAP Bericht erhalten	Ja.	Nein
Managen von Cloud Central Konten	Ja.	Nein
Konten von Cloud-Providern verwalten	Ja.	Nein
Ändern der Cloud Manager-Einstellungen	Ja.	Nein
Anzeigen und Verwalten des Support-Dashboards	Ja.	Nein
Entfernen Sie Arbeitsumgebungen aus Cloud Manager	Ja.	Nein
Aktualisieren Sie Cloud Manager	Ja.	Nein
Installieren Sie ein HTTPS-Zertifikat	Ja.	Nein
Einrichten von Active Directory	Ja.	Nein

Weiterführende Links

- "Einrichtung von Workspaces und Benutzern im Cloud Central Konto"
- "Managen von Workspaces und Benutzern im Cloud Central Konto"

Wo Sie Hilfe und weitere Informationen erhalten

Über verschiedene Ressourcen, darunter Videos, Foren und Support, erhalten Sie Hilfe und weitere Informationen zu Cloud Manager und Cloud Volumes ONTAP.

- "Videos für Cloud Manager und Cloud Volumes ONTAP"

  In diesem Video sehen Sie, wie Sie Cloud Volumes ONTAP implementieren und managen und wie Sie Daten in Ihrer gesamten Hybrid Cloud replizieren.

- "Richtlinien für Cloud Manager"

  Laden Sie JSON-Dateien herunter, die die Berechtigungen enthalten, die Cloud Manager für Aktionen in einem Cloud-Provider benötigt.

- "Cloud Manager API-Entwicklerleitfaden"

  Lesen Sie einen Überblick über die APIs, Beispiele für deren Verwendung und eine API-Referenz.

- Training für Cloud Volumes ONTAP
  - "Grundlagen von Cloud Volumes ONTAP"
  - "Implementierung und Management von Cloud Volumes ONTAP für Azure"
  - "Implementierung und Management von Cloud Volumes ONTAP für AWS"
- Technische Berichte
  - "NetApp Technical Report 4383: Performance Characterization of Cloud Volumes ONTAP in Amazon Web Services with Application Workloads"
  - "Technischer Bericht von NetApp 4671: Performance-Charakterisierung von Cloud Volumes ONTAP in Azure mit Applikations-Workloads"
- Disaster Recovery für SVM

  Bei der SVM Disaster Recovery wird die asynchrone Spiegelung von SVM-Daten und -Konfiguration von einer Quell-SVM zu einer Ziel-SVM erstellt. Sie können eine Ziel-SVM für den Datenzugriff schnell aktivieren, wenn die Quell-SVM nicht mehr verfügbar ist.

  - "Cloud Volumes ONTAP 9 SVM Disaster Recovery Preparation Express-Leitfaden"

    Beschreibt, wie eine Ziel-SVM zur Vorbereitung auf die Disaster Recovery schnell konfiguriert wird.

  - "Cloud Volumes ONTAP 9 SVM Disaster Recovery Express Guide"

    Beschreibt, wie Sie eine Ziel-SVM nach einem Notfall schnell aktivieren und dann die Quell-SVM erneut aktivieren.

- "FlexCache Volumes für schnelleren Datenzugriff – Power Guide"

  Beschreibt die Erstellung und Verwaltung von FlexCache Volumes im selben Cluster oder anderen Cluster wie das Ursprungs-Volume, um Daten zu beschleunigen access.es wie schnell eine Ziel-SVM nach einem Ausfall zu aktivieren und anschließend die Quell-SVM zu reaktivieren.

- "Sicherheitsratschläge"

  Bekannte Schwachstellen (CVEs) für NetApp Produkte, einschließlich ONTAP ermitteln Beachten Sie, dass Sie Sicherheitslücken bei Cloud Volumes ONTAP mithilfe der folgenden ONTAP Dokumentation beheben können.

- "ONTAP 9 Dokumentationszentrum"

Greifen Sie auf die Produktdokumentation für ONTAP zu, die Ihnen bei der Verwendung von Cloud Volumes ONTAP helfen kann.

- "NetApp Cloud Volumes ONTAP Support"

  Greifen Sie auf Support-Ressourcen zu, um Hilfe zu erhalten und Probleme mit Cloud Volumes ONTAP zu beheben.

- "NetApp Community: Cloud Data Services"

  Tauschen Sie sich mit Kollegen aus, stellen Sie Fragen, tauschen Sie Ideen aus, suchen Sie nach Ressourcen und tauschen Sie Best Practices aus.

- "NetApp Cloud Central"

  Hier finden Sie weitere Informationen zu NetApp Produkten und Lösungen für die Cloud.

- "NetApp Produktdokumentation"

  In der NetApp Produktdokumentation finden Sie Anleitungen, Ressourcen und Antworten.

Frühere Versionen der Cloud Manager-Dokumentation

Dokumentation für frühere Versionen von Cloud Manager ist verfügbar, falls Sie nicht die neueste Version ausführen.

"Cloud Manager 3.6"

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

http://www.netapp.com/us/legal/copyright.aspx

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/us/media/patents-page.pdf

Datenschutzrichtlinie

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

- "Hinweis zu Cloud Manager 3.7.4"
- "Hinweis zu Cloud Manager 3.7.1"
- "Hinweis zu Cloud Manager 3.7"
- "Hinweis zum Cloud Backup Service"