Cloud Manager und Cloud Volumes ONTAP Dokumentation

Cloud Manager 3.6

NetApp
June 27, 2025

This PDF was generated from https://docs.netapp.com/de-de/occm36/index.html on June 27, 2025.
Always check docs.netapp.com for the latest.

Inhalt

Cloud Manager und Cloud Volumes ONTAP Dokumentation . . . 1
- BlueXP . . . 1
- Entdecken Sie die Neuigkeiten . . . 1
- Los geht’s . . . 1
- Automatisierung mit APIs . . . 1
- Treten Sie mit Kollegen in Kontakt, holen Sie sich Hilfe und finden Sie weitere Informationen . . . 1

Versionshinweise . . . 2
- Cloud Manager . . . 2
  - Neues in Cloud Manager 3.6 . . . 2
  - Bekannte Probleme . . . 15
  - Bekannte Einschränkungen . . . 16

Konzepte . . . 17
- Überblick über Cloud Manager und Cloud Volumes ONTAP . . . 17
  - Cloud Manager . . . 17
  - Cloud Volumes ONTAP . . . 17
- NetApp Cloud Central . . . 18
- Konten und Berechtigungen für Cloud-Provider . . . 19
  - AWS Konten und Berechtigungen . . . 19
  - Azure-Konten und Berechtigungen . . . 21
- Storage . . . 23
  - Wie Cloud Volumes ONTAP Cloud Storage verwendet . . . 23
  - Data Tiering - Übersicht . . . 25
  - Storage-Management . . . 29
  - WORM-Storage . . . 36
- Hochverfügbarkeitspaare . . . 37
  - Hochverfügbarkeitspaare in AWS . . . 37
  - Hochverfügbarkeitspaare in Azure . . . 43
- Bewertung . . . 46
- Lizenzierung . . . 46
- Sicherheit . . . 47
  - Verschlüsselung von Daten im Ruhezustand . . . 47
  - ONTAP Virenscannen . . . 48
  - Schutz durch Ransomware . . . 48
- Leistung . . . 49

Erste Schritte . . . 50
- Implementierungsübersicht . . . 50
  - Installation von Cloud Manager . . . 50
  - Einrichtung von Cloud Manager . . . 50
  - Implementierung von Cloud Volumes ONTAP . . . 51
- Erste Schritte mit Cloud Volumes ONTAP in AWS . . . 51
- Erste Schritte mit Cloud Volumes ONTAP in Azure . . . 52
- Einrichten von Cloud Manager . . . 53
  - Cloud-Provider-Konten zu Cloud Manager hinzufügen . . . 53

Hinzufügen von NetApp Support Site Konten zu Cloud Manager . . . 63
Installieren eines HTTPS-Zertifikats für sicheren Zugriff . . . 64
Benutzer und Mandanten einrichten . . . 65
Einrichten des AWS KMS . . . 67
Netzwerkanforderungen . . . 70
Netzwerkanforderungen für Cloud Manager . . . 70
Netzwerkanforderungen für Cloud Volumes ONTAP in AWS . . . 73
Einrichten eines AWS-Transit-Gateways für HA-Paare in mehreren Verfügbarkeitszonen . . . 80
Netzwerkanforderungen für Cloud Volumes ONTAP in Azure . . . 84
Zusätzliche Bereitstellungsoptionen . . . 85
Anforderungen an den Cloud Manager Host . . . 85
Installieren von Cloud Manager auf einem vorhandenen Linux-Host . . . 86
Starten von Cloud Manager über den AWS Marketplace . . . 88
Bereitstellung von Cloud Manager über Azure Marketplace . . . 89
Cloud Manager in einer Region der US-Regierung von Azure implementieren . . . 92
Installieren von Cloud Manager in einer Azure Deutschland Region . . . 94
Implementierung von Cloud Volumes ONTAP . . . 95
Bevor Sie Cloud Volumes ONTAP Systeme erstellen . . . 95
Anmelden bei Cloud Manager . . . 95
Planung Ihrer Cloud Volumes ONTAP Konfiguration . . . 96
Auswahl eines Lizenztyps . . . 96
Storage-Grenzen kennen . . . 96
Dimensionierung Ihres Systems in AWS . . . 97
Dimensionierung Ihres Systems in Azure . . . 97
Auswählen einer Schreibgeschwindigkeit . . . 99
Auswählen eines Volume-Nutzungsprofils . . . 99
Arbeitsblatt mit Informationen zum AWS-Netzwerk . . . 100
Azure Network Information Worksheet . . . 101
Aktivierung von Flash Cache für Cloud Volumes ONTAP in AWS . . . 101
Starten von Cloud Volumes ONTAP in AWS . . . 101
Einführung eines einzelnen Cloud Volumes ONTAP Systems in AWS . . . 102
Starten eines Cloud Volumes ONTAP HA-Paars in AWS . . . 106
Starten von Cloud Volumes ONTAP in Azure . . . 112
Registrieren von Pay-as-you-go-Systemen . . . 116
Einrichten von Cloud Volumes ONTAP . . . 117
Storage-Bereitstellung . . . 119
Storage-Bereitstellung . . . 119
Bereitstellung von Volumes . . . 119
Bereitstellung von Volumes auf dem zweiten Node in einer HA-Konfiguration . . . 121
Aggregate werden erstellt . . . 122
Bereitstellung von iSCSI-LUNs . . . 122
Tiering inaktiver Daten in kostengünstigen Objektspeicher . . . 123
Konfigurationen, die Daten-Tiering unterstützen . . . 123
Anforderungen für Tiering von Daten in AWS . . . 123
Anforderungen für Tiering von Daten in Microsoft Azure . . . 124

Tiering von Daten auf Lese-/Schreib-Volumes . . . 124
Tiering von Daten auf Data-Protection-Volumes . . . 125
Ändern der Tiering Level . . . 125
Verwendung von Cloud Volumes ONTAP als persistenter Storage für Kubernetes . . . 126
Verschlüsseln von Volumes mit NetApp Volume Encryption . . . 128
Management von vorhandenem Storage . . . 129
Management vorhandener Volumes . . . 129
Management vorhandener Aggregate . . . 131
Ändern des CIFS-Servers . . . 132
Verschieben eines Volumes zur Vermeidung von Kapazitätsproblemen . . . 133
Bereitstellung von NFS-Volumes über die Volume-Ansicht . . . 136
Wechseln zur Volume-Ansicht . . . 136
Erstellen und Mounten von NFS-Volumes . . . 136
Managen von NFS-Volumes . . . 139
Datenmanagement in einer Hybrid Cloud . . . 142
Erkennung und Management von ONTAP Clustern . . . 142
Erkennung von ONTAP Clustern . . . 142
Bereitstellung von Volumes auf ONTAP Clustern . . . 143
Replizierung von Daten in die und aus der Cloud . . . 144
Auswählen einer Replizierungsrichtlinie . . . 144
Anforderungen an die Datenreplizierung . . . 147
Replizierung von Daten zwischen Systemen . . . 148
Managen von Plänen und Beziehungen zur Datenreplizierung . . . 149
Daten werden mit AWS S3 synchronisiert . . . 151
Funktionsweise der Funktion "Sync to S3 . . . 152
Integration einer Arbeitsumgebung in den Cloud Sync Service . . . 152
Verwalten von Volume-Sync-Beziehungen . . . 153
Administration von Cloud Volumes ONTAP . . . 154
Verbindung zu Cloud Volumes ONTAP . . . 154
Verbindung mit OnCommand System Manager wird hergestellt . . . 154
Herstellen einer Verbindung zur Cloud Volumes ONTAP CLI . . . 154
Aktualisierung der Cloud Volumes ONTAP Software . . . 155
Überblick . . . 155
Aktualisierung der Cloud Volumes ONTAP Software wird vorbereitet . . . 157
Upgrade von Cloud Volumes ONTAP auf die neueste Version . . . 158
Upgrade oder Downgrade von Cloud Volumes ONTAP mit einem HTTP- oder FTP-Server . . . 159
Downgrade von Cloud Volumes ONTAP mit einem lokalen Image . . . 160
Ändern von Cloud Volumes ONTAP Systemen . . . 161
Installation von Lizenzdateien auf Cloud Volumes ONTAP Byol Systemen . . . 161
Ändern der Instanz oder des Typs der virtuellen Maschine für Cloud Volumes ONTAP . . . 162
Wechsel zwischen nutzungsbasierten Konfigurationen . . . 163
Wechsel zu einer alternativen Cloud Volumes ONTAP Konfiguration . . . 163
Ändern des Namens der virtuellen Storage-Maschine . . . 164
Ändern des Passworts für Cloud Volumes ONTAP . . . 164
Ändern der Netzwerk-MTU für c4.4xlarge und c4.8xlarge Instanzen . . . 164

Ändern von Routingtabellen im Zusammenhang mit HA-Paaren in mehreren AWS AZS . . . 165
Managen des Status von Cloud Volumes ONTAP . . . 165
Planen automatischer Abschaltungen von Cloud Volumes ONTAP . . . 165
Beenden von Cloud Volumes ONTAP . . . 166
Überwachung der AWS-Ressourcenkosten . . . 166
Besserer Schutz gegen Ransomware . . . 168
Hinzufügen vorhandener Cloud Volumes ONTAP Systeme zu Cloud Manager . . . 169
Löschen einer Cloud Volumes ONTAP Arbeitsumgebung . . . 170
Administration von Cloud Manager . . . 171
Cloud Manager wird aktualisiert . . . 171
Aktivieren automatischer Updates . . . 171
Aktualisierung von Cloud Manager auf die neueste Version . . . 171
Aktualisierung von Cloud Manager mit einem Patch . . . 172
Backup und Wiederherstellung von Cloud Manager . . . 172
Backup von Cloud Manager . . . 172
Wiederherstellen von Cloud Manager aus einem Backup . . . 173
Entfernen von Cloud Volumes ONTAP Arbeitsumgebungen . . . 173
Bearbeiten von Benutzerkonten . . . 174
Konfigurieren von Cloud Manager für die Verwendung eines Proxyservers . . . 174
Erneuerung des Cloud Manager HTTPS-Zertifikats . . . 175
Cloud Manager wird deinstalliert . . . 175
APIs und Automatisierung . . . 177
Automatisierungsmuster für Infrastruktur als Code . . . 177
Referenz . . . 178
Häufig gestellte Fragen: Integration von Cloud Manager in NetApp Cloud Central . . . 178
Was ist NetApp Cloud Central? . . . 178
Warum integriert NetApp mein Cloud Manager-System in Cloud Central? . . . 178
Was passiert während des Integrationsprozesses? . . . 178
Wie funktioniert die zentralisierte Benutzerauthentifizierung? . . . 178
Muss ich mich für ein Cloud Central Benutzerkonto anmelden? . . . 178
Was passiert, wenn ich bereits ein Cloud Central Benutzerkonto habe? . . . 178
Was ist, wenn mein Cloud Manager-System über mehrere Benutzerkonten verfügt? . . . 178
Was passiert, wenn ich ein Benutzerkonto habe, das dieselbe E-Mail-Adresse in mehreren Cloud Manager-Systemen verwendet? . . . 179
Was geschieht, wenn mein lokales Benutzerkonto eine ungültige E-Mail-Adresse verwendet? . . . 179
Was ist, wenn ich Automatisierungsskripts für Cloud Manager-APIs habe? . . . 179
Was ist, wenn mein Cloud Manager-System LDAP verwendet? . . . 179
Spielt es eine Rolle, wo ich mein Cloud Manager-System installiert habe? . . . 179
Sicherheitsgruppenregeln für AWS . . . 179
Regeln für Cloud Manager . . . 179
Regeln für Cloud Volumes ONTAP . . . 181
Regeln für die externe Sicherheitsgruppe des HA Mediators . . . 185
Regeln für die interne Sicherheitsgruppe des HA-Vermittlers . . . 186
Sicherheitsgruppenregeln für Azure . . . 187
Regeln für Cloud Manager . . . 187

Regeln für Cloud Volumes ONTAP . . . 189
AWS- und Azure-Berechtigungen für Cloud Manager . . . 193
Was Cloud Manager mit AWS-Berechtigungen macht . . . 193
Was Cloud Manager mit Azure-Berechtigungen tut . . . 195
Standardkonfigurationen . . . 198
Standardkonfiguration für Cloud Manager unter Linux . . . 198
Standardkonfiguration für Cloud Volumes ONTAP . . . 198
Boot- und Root-Daten für Cloud Volumes ONTAP . . . 199
Benutzerrollen . . . 200
Wo Sie Hilfe und weitere Informationen erhalten . . . 201
Rechtliche Hinweise . . . 203
Urheberrecht . . . 203
Marken . . . 203
Patente . . . 203
Datenschutzrichtlinie . . . 203
Open Source . . . 203

Cloud Manager und Cloud Volumes ONTAP Dokumentation

Mit OnCommand Cloud Manager implementieren und managen Sie NetApp Cloud Volumes ONTAP – 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"
- "Suchen Sie nach unterstützten Konfigurationen für Cloud Volumes ONTAP"
- "Detaillierte Netzwerkanforderungen für Cloud Manager"
- "Detaillierte Netzwerkanforderungen für Cloud Volumes ONTAP für AWS"
- "Detaillierte Netzwerkanforderungen für Cloud Volumes ONTAP für Azure"
- "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 3.6

OnCommand Cloud Manager führt in der Regel jeden Monat eine neue Version ein, um Ihnen neue Funktionen, Verbesserungen und Bugfixes zu bieten.

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

Unterstützung für die AWS C2S-Umgebung (2. Mai 2019)

Cloud Volumes ONTAP 9.5 und Cloud Manager 3.6.4 stehen jetzt den USA zur Verfügung Intelligence Community (IC) über die AWS Commercial Cloud Services Umgebung (C2S) Sie können HA-Paare und Single-Node-Systeme in C2S implementieren.

"Quick Start Guide für die AWS Commercial Cloud Services-Umgebung"

Cloud Manager 3.6.6 (1. Mai 2019)

- Unterstützung von 6-TB-Festplatten in AWS
- Unterstützung neuer Festplattengrößen mit Single-Node-Systemen in Azure
- Unterstützung von Standard-SSDs mit Single-Node-Systemen in Azure
- die mit dem NetApp Kubernetes Service erstellt wurden
- Möglichkeit zum Konfigurieren eines NTP-Servers

Unterstützung von 6-TB-Festplatten in AWS

Sie können nun eine EBS-Festplattenkapazität von 6 TB mit Cloud Volumes ONTAP für AWS auswählen. Mit der kürzlich "Gesteigerte Performance von General Purpose SSDs", Eine 6-TB-Festplatte ist jetzt die beste Wahl für maximale Leistung.

Diese Änderung wird unterstützt durch Cloud Volumes ONTAP 9.5, 9.4 und 9.3.

Unterstützung neuer Festplattengrößen mit Single-Node-Systemen in Azure

In Azure können Sie nun 8-TB-, 16-TB- und 32-TB-Festplatten mit Single-Node-Systemen verwenden. Die höhere Festplattengröße ermöglicht bei Nutzung der Premium- oder BYOL-Lizenzen das Erreichen von bis zu 368 TB Systemkapazität ohne Festplatten.

Diese Änderung wird unterstützt durch Cloud Volumes ONTAP 9.5, 9.4 und 9.3.

Unterstützung von Standard-SSDs mit Single-Node-Systemen in Azure

Standard-SSD-gemanagte Festplatten werden jetzt von Single-Node-Systemen in Azure unterstützt. Diese Festplatten bieten eine Performance-Stufe zwischen Premium SSDs und Standard HDDs.

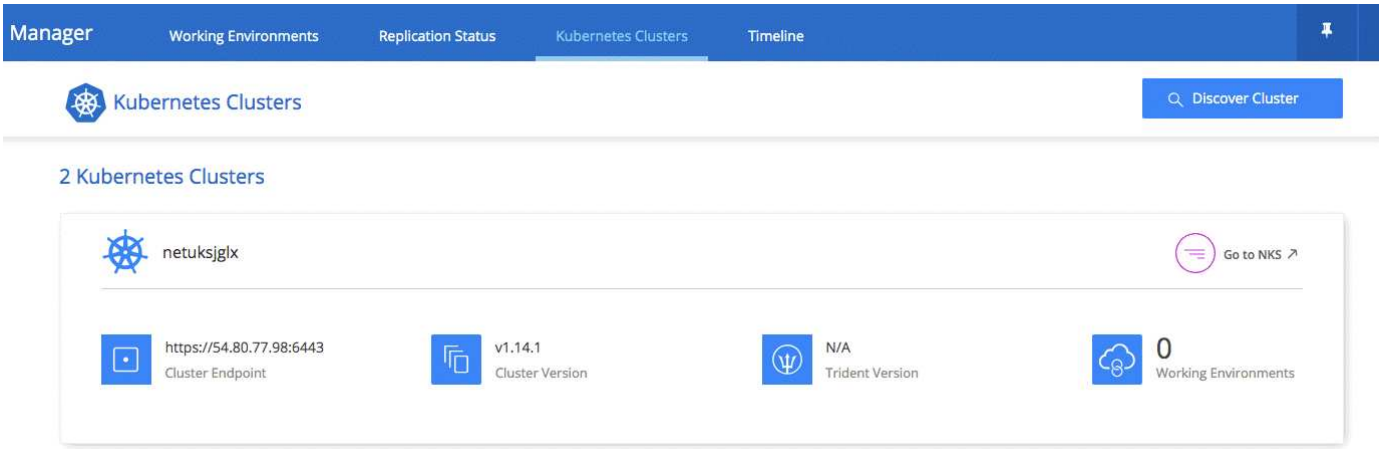
Diese Änderung wird unterstützt durch Cloud Volumes ONTAP 9.5, 9.4 und 9.3.

"Erfahren Sie mehr über Standard-SSDs".

Automatische Erkennung von Kubernetes-Clustern, die mit dem NetApp Kubernetes Service erstellt wurden

Cloud Manager erkennt jetzt automatisch die Kubernetes-Cluster, die Sie mit dem NetApp Kubernetes Service implementieren. Dadurch können Sie die Kubernetes-Cluster mit Ihren Cloud Volumes ONTAP-Systemen verbinden, sodass sie als persistenter Storage für Ihre Container verwendet werden können.

Das folgende Bild zeigt ein automatisch ermittelte Kubernetes-Cluster. Über den Link „Go to NKS“ gelangen Sie direkt zum NetApp Kubernetes Service.



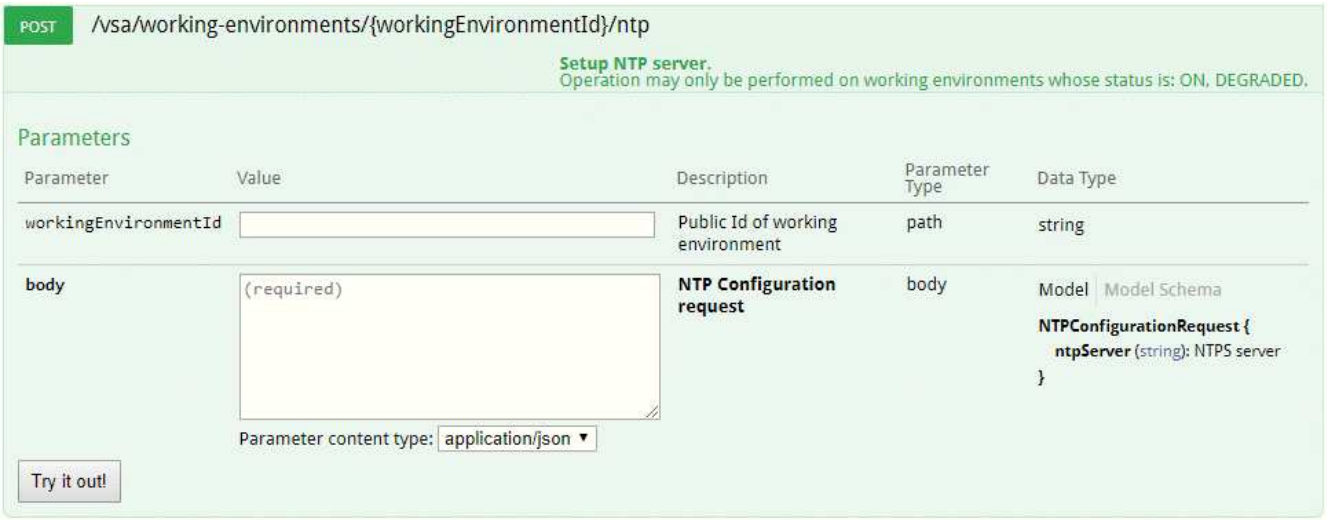
"Verbinden Sie Ihre Arbeitsumgebungen mit Kubernetes-Clustern".

Möglichkeit zum Konfigurieren eines NTP-Servers

Sie können Cloud Volumes ONTAP jetzt für die Verwendung eines NTP-Servers (Network Time Protocol) konfigurieren. Durch das Festlegen eines NTP-Servers wird die Zeit zwischen den Systemen im Netzwerk synchronisiert, wodurch Probleme aufgrund von Zeitunterschieden vermieden werden können.

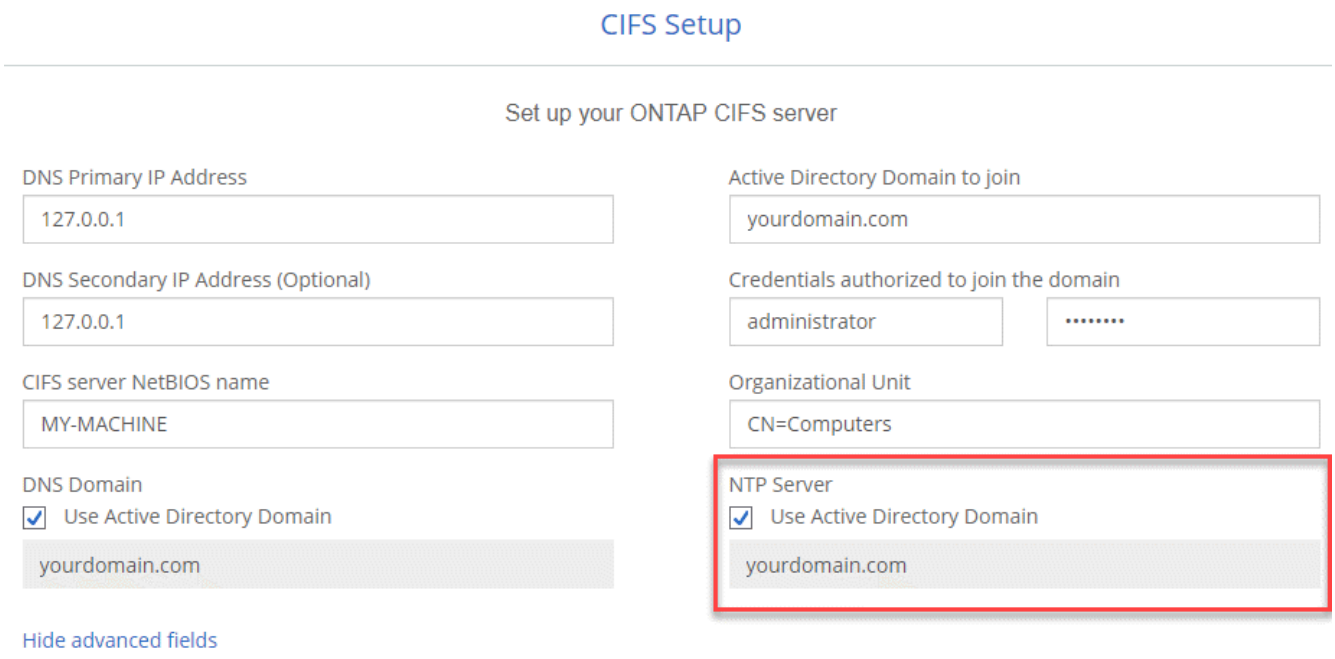
Geben Sie beim Einrichten eines CIFS-Servers einen NTP-Server mithilfe der Cloud Manager-API oder von der Benutzeroberfläche an:

- Der "Cloud Manager APIs" Aktivieren Sie, um eine beliebige Adresse für den NTP-Server anzugeben. Hier ist die API für ein Single-Node-System in AWS:



- Beim Konfigurieren eines CIFS-Servers können Sie über die Cloud Manager-Benutzeroberfläche einen NTP-Server angeben, der die Active Directory-Domäne verwendet. Wenn Sie eine andere Adresse verwenden müssen, sollten Sie die API verwenden.

  Das folgende Bild zeigt das NTP-Server-Feld, das beim Einrichten von CIFS verfügbar ist.



Cloud Manager 3.6.5 (2. April 2019)

Cloud Manager 3.6.5 umfasst die folgenden Verbesserungen:

- Kubernetes-Verbesserungen
- Konten der NetApp Support Site werden jetzt auf Systemebene verwaltet
- AWS Transit-Gateways können den Zugriff auf fließende IP-Adressen ermöglichen
- Azure-Ressourcengruppen sind jetzt gesperrt
- NFS 4 und NFS 4.1 sind nun standardmäßig aktiviert
- Eine neue API ermöglicht das Löschen von ONTAP Snapshot Kopien

Kubernetes-Verbesserungen

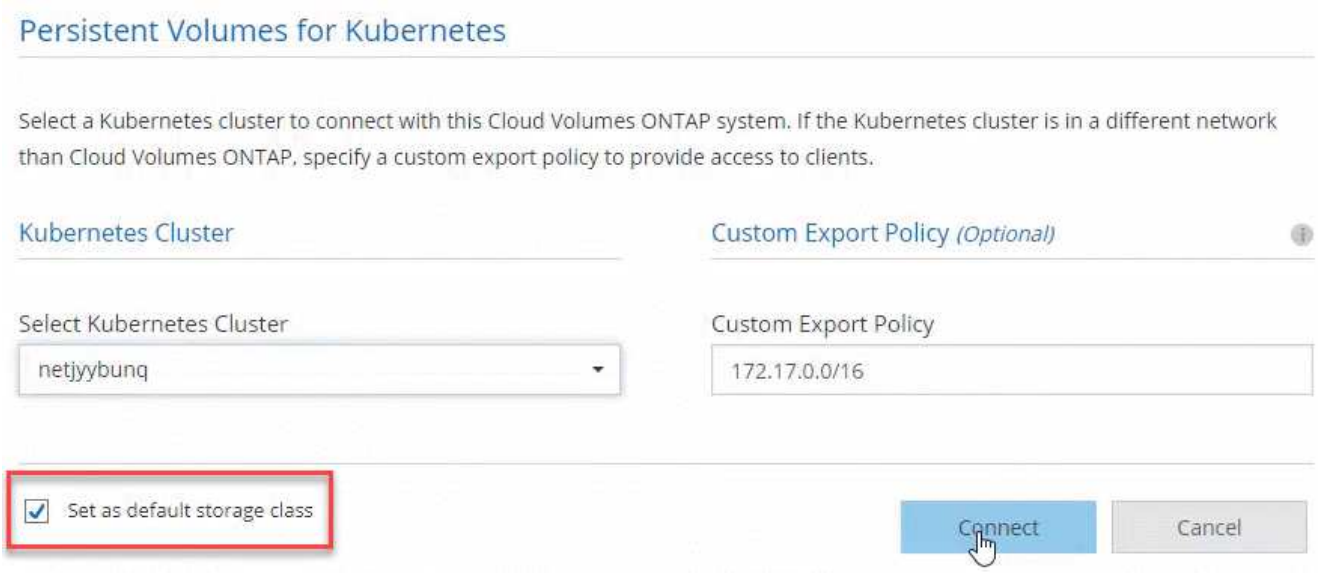
Wir haben einige Verbesserungen vorgenommen, die die Verwendung von Cloud Volumes ONTAP als persistenten Storage für Container vereinfachen:

- Sie können Cloud Manager nun mehrere Kubernetes-Cluster hinzufügen.

  So können Sie verschiedene Cluster mit verschiedenen Cloud Volumes ONTAP Systemen und mehreren Clustern mit demselben Cloud Volumes ONTAP System verbinden.

- Wenn Sie ein Cluster verbinden, können Sie nun Cloud Volumes ONTAP als Standard-Storage-Klasse für das Kubernetes Cluster festlegen.

  Wenn ein Benutzer ein persistentes Volume erstellt, kann der Kubernetes-Cluster Cloud Volumes ONTAP standardmäßig als Back-End-Storage verwenden:



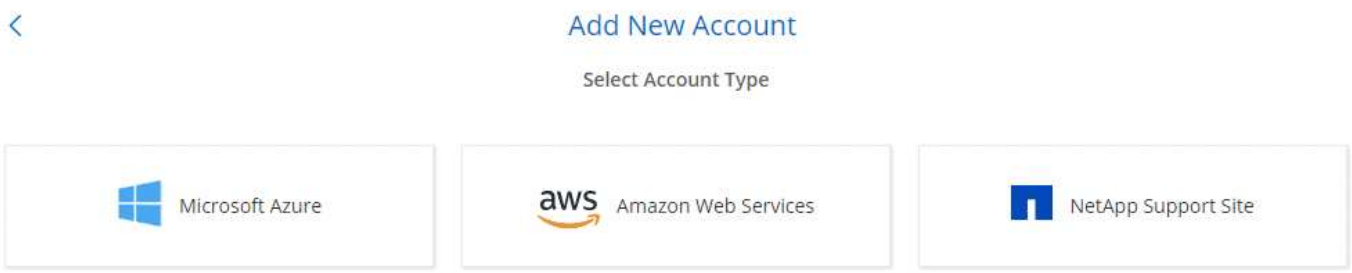
- Wir haben geändert, wie Cloud Manager die Kubernetes-Storage-Klassen benennt, um leichter erkennbar zu sein:
  - **netapp-File**: Zur Anbindung eines Persistent Volumes an ein Single-Node Cloud Volumes ONTAP System
  - **netapp-dateiredundant**: Zur Anbindung eines persistenten Volumes an ein Cloud Volumes ONTAP HA-Paar
- Die Version von NetApp Trident, die von Cloud Manager installiert wird, wurde auf die neueste Version aktualisiert.

"Lesen Sie, wie Sie Cloud Volumes ONTAP als persistenten Storage für Kubernetes verwenden".

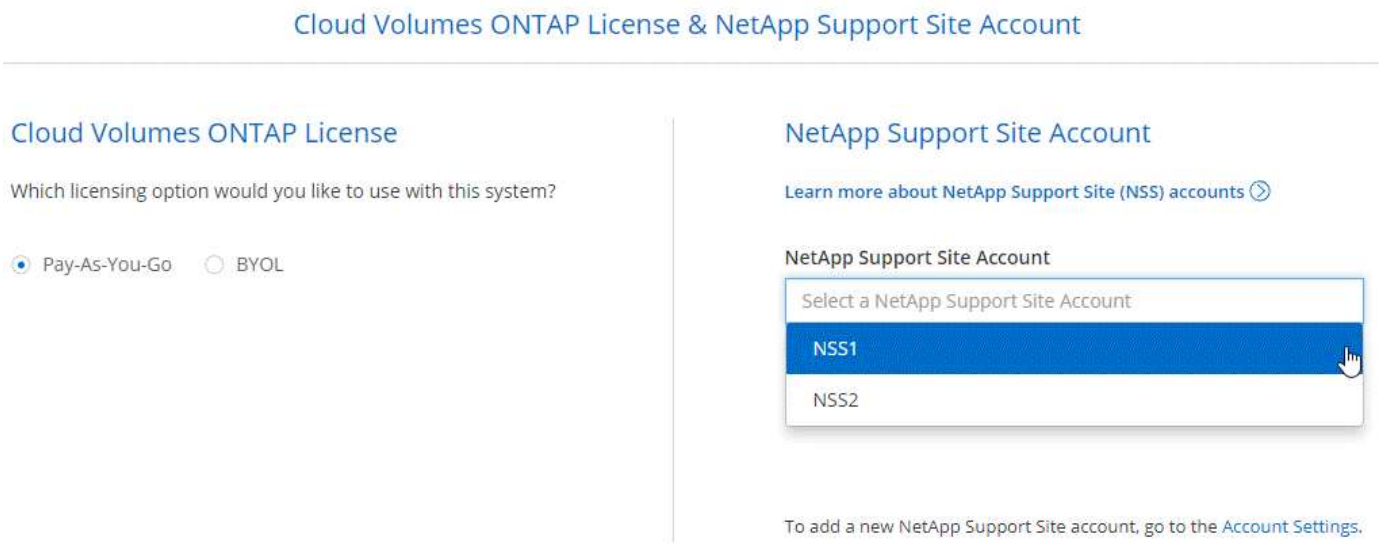
Konten der NetApp Support Site werden jetzt auf Systemebene verwaltet

Es ist jetzt einfacher, NetApp Support Site Konten in Cloud Manager zu managen.

In vorherigen Versionen mussten Sie ein NetApp Support Site Konto mit einem bestimmten Mandanten verknüpfen. Die Konten werden jetzt auf Systemebene wie bei Cloud Manager gemanagt, an derselben Stelle, an der Sie Cloud-Provider-Konten verwalten. Durch diese Änderung können Sie bei der Registrierung Ihrer Cloud Volumes ONTAP Systeme zwischen mehreren NetApp Support Site Accounts wählen.



Wenn Sie eine neue Arbeitsumgebung erstellen, wählen Sie einfach den NetApp Support Site Account aus, um das Cloud Volumes ONTAP System zu registrieren mit:



Wenn Cloud Manager auf 3.6 aktualisiert 5 wird, werden automatisch Konten der NetApp Support-Website für Sie hinzugefügt, wenn Sie zuvor Mandanten mit einem Konto verknüpft hatten.

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

AWS Transit-Gateways können den Zugriff auf fließende IP-Adressen ermöglichen

Ein HA-Paar in mehreren AWS Availability Zones verwendet *Floating IP-Adressen* für NAS-Datenzugriff und für Managementschnittstellen. Bis jetzt ist der Zugriff auf die fließenden IP-Adressen nicht über außerhalb der VPC möglich, wo sich das HA-Paar befindet.

Wir haben überprüft, dass Sie ein verwenden können "AWS Transit-Gateway" Um den Zugriff auf die unverankerten IP-Adressen von außerhalb der VPC zu ermöglichen. Das bedeutet, dass NetApp Management-Tools und NAS-Clients, die sich außerhalb der VPC befinden, auf die fließenden IPs zugreifen und von automatischem Failover profitieren können.

"Erfahren Sie, wie Sie ein AWS Transit-Gateway für HA-Paare in mehreren Verfügbarkeitszonen einrichten".

Azure-Ressourcengruppen sind jetzt gesperrt

Cloud Manager sperrt jetzt Cloud Volumes ONTAP-Ressourcengruppen in Azure, wenn sie erstellt werden. Durch das Sperren von Ressourcengruppen können Benutzer nicht versehentlich kritische Ressourcen löschen oder ändern.

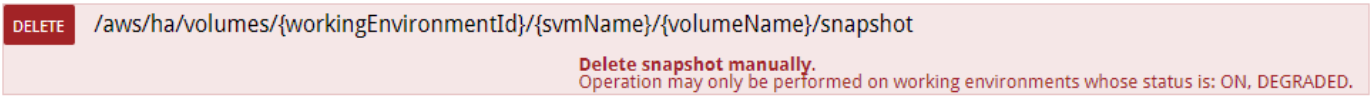
NFS 4 und NFS 4.1 sind nun standardmäßig aktiviert

Cloud Manager ermöglicht jetzt alle neu erstellten Cloud Volumes ONTAP Systeme die Protokolle NFS 4 und NFS 4.1. Diese Änderung spart Zeit, da Sie diese Protokolle nicht mehr manuell aktivieren müssen.

Eine neue API ermöglicht das Löschen von ONTAP Snapshot Kopien

Sie können jetzt Snapshot-Kopien von Lese-Schreib-Volumes mithilfe eines Cloud Manager-API-Aufrufs löschen.

Das folgende Beispiel zeigt die API-Aufruf für ein HA-System in AWS:



Ähnliche API-Aufrufe sind für Single-Node-Systeme in AWS sowie für Single-Node- und HA-Systeme in Azure verfügbar.

"OnCommand Cloud Manager API - Entwickler-Handbuch"

Update zu Cloud Manager 3.6.4 (18. März 2019)

Cloud Manager wurde aktualisiert und unterstützt so die Patch-Version 9.5 P1 für Cloud Volumes ONTAP. Mit diesem Patch-Release sind HA-Paare in Azure nun allgemein verfügbar (GA).

Siehe "Versionshinweise zu Cloud Volumes ONTAP 9.5" Weitere Details, einschließlich wichtiger Informationen zur Unterstützung von Azure Region für HA-Paare

Cloud Manager 3.6.4 (3. März 2019)

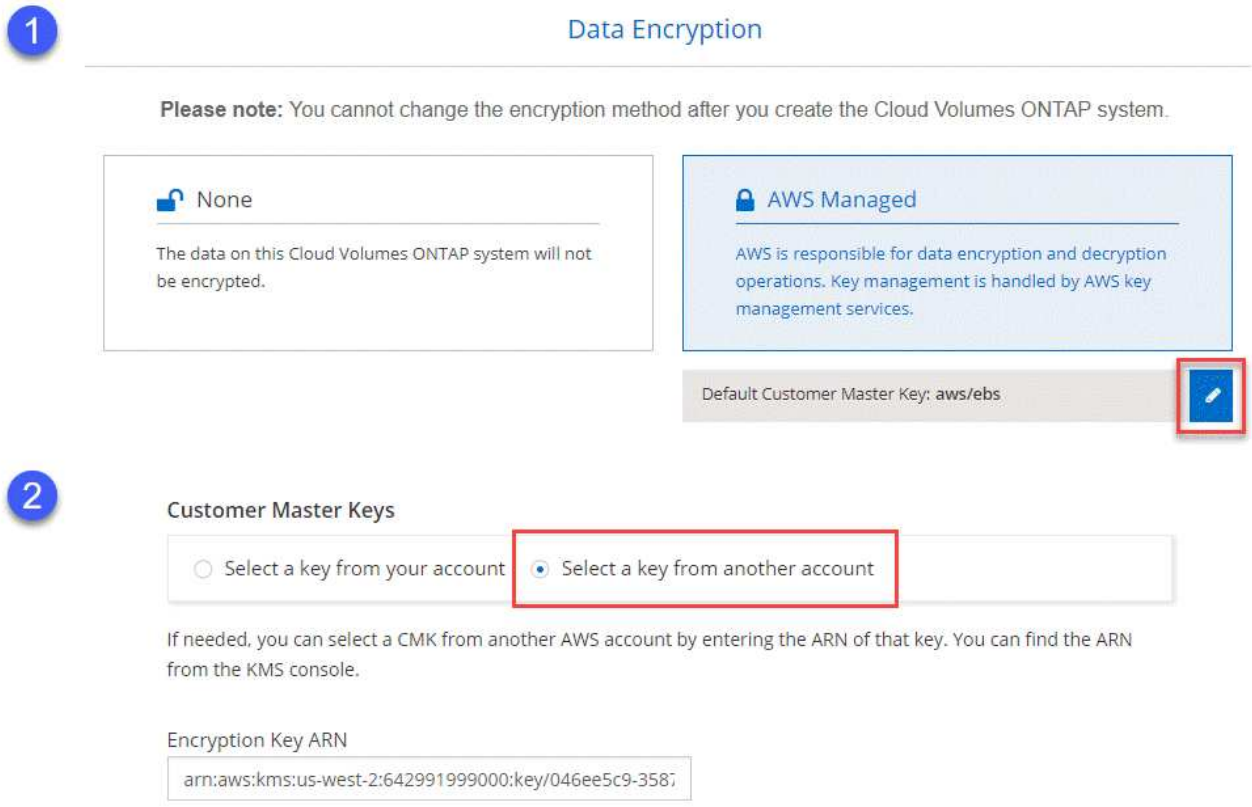
Cloud Manager 3.6.4 umfasst die folgenden Verbesserungen:

- Von AWS gemanagte Verschlüsselung mit einem Schlüssel von einem anderen Konto
- Wiederherstellung ausgefallener Festplatten
- wenn Daten-Tiering zu Blob Containern erfolgt

Von AWS gemanagte Verschlüsselung mit einem Schlüssel von einem anderen Konto

Wenn Sie ein Cloud Volumes ONTAP System in AWS starten, können Sie es jetzt aktivieren "Von AWS gemanagte Verschlüsselung" Verwenden eines Kunden-Master Key (CMK) von einem anderen AWS-Benutzerkonto.

Die folgenden Bilder zeigen, wie die Option beim Erstellen einer neuen Arbeitsumgebung ausgewählt wird:



"Erfahren Sie mehr über unterstützte Verschlüsselungstechnologien".

Wiederherstellung ausgefallener Festplatten

Cloud Manager versucht jetzt, ausgefallene Festplatten aus Cloud Volumes ONTAP Systemen wiederherzustellen. Erfolgreiche Versuche werden in E-Mail-Benachrichtigungsberichten festgehalten. Hier sehen Sie eine Beispielbenachrichtigung:

Sie können Benachrichtigungsberichte aktivieren, indem Sie Ihr Benutzerkonto bearbeiten.

Azure Storage-Konten für HTTPS aktiviert, wenn Daten-Tiering zu Blob Containern erfolgt

Wenn Sie ein Cloud Volumes ONTAP System für das Tiering inaktiver Daten zu einem Azure Blob Container einrichten, erstellt Cloud Manager ein Azure Storage-Konto für diesen Container. Ab diesem Release ermöglicht Cloud Manager jetzt neue Speicherkonten mit sicherem Transfer (HTTPS). Vorhandene Speicherkonten verwenden weiterhin HTTP.

Cloud Manager 3.6.3 (4. Februar 2019)

Cloud Manager 3.6.3 umfasst die folgenden Verbesserungen:

- Unterstützung für Cloud Volumes ONTAP 9.5 GA
- 368 TB Kapazitätsgrenze für alle Premium- und BYOL-Konfigurationen
- Unterstützung für neue AWS Regionen
- Unterstützung für intelligentes S3-Tiering
- Daten-Tiering auf dem ursprünglichen Aggregat zu deaktivieren
- Empfohlener EC2-Instanztyp jetzt t3.Medium für Cloud Manager
- Verschiebung geplanter Abschaltungen während der Datenübertragung

Unterstützung für Cloud Volumes ONTAP 9.5 GA

Cloud Manager unterstützt jetzt die allgemein verfügbare Version von Cloud Volumes ONTAP 9.5. Dies schließt auch die Unterstützung der M5- und R5-Instanzen in AWS ein. Weitere Informationen zur Version 9.5 finden Sie im "Versionshinweise zu Cloud Volumes ONTAP 9.5".

368 TB Kapazitätsgrenze für alle Premium- und BYOL-Konfigurationen

Die Systemkapazitätsgrenze für Cloud Volumes ONTAP Premium und BYOL beträgt jetzt 368 TB für alle Konfigurationen: Single Node und HA in AWS und Azure. Diese Änderung gilt für Cloud Volumes ONTAP 9.5, 9.4 und 9.3 (nur AWS mit 9.3).

Bei einigen Konfigurationen verhindern Festplattenlimits, dass Sie durch die Nutzung von Festplatten allein das Kapazitätslimit von 368 TB erreichen. In diesen Fällen erreichen Sie das Kapazitätslimit von 368 TB um "tiering inaktiver Daten in Objektspeicher". Ein Single-Node-System in Azure könnte beispielsweise eine festplattenbasierte Kapazität von 252 TB aufweisen, sodass bis zu 116 TB inaktiver Daten im Azure Blob Storage genutzt werden können.

Weitere Informationen zu Festplattenlimits finden Sie unter Storage-Limits im "Versionshinweise zu Cloud Volumes ONTAP".

Unterstützung für neue AWS Regionen

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

- Europa (Stockholm)

  Systeme mit einzelnen Nodes sind nur verfügbar. HA-Paare werden derzeit nicht unterstützt.

- GovCloud (Osten der USA)

  Dies wird zusätzlich zur Unterstützung für die Region AWS GovCloud (USA-West) angeboten.

"Eine vollständige Liste der unterstützten Regionen ist verfügbar".

Unterstützung für intelligentes S3-Tiering

Wenn Sie Daten-Tiering in AWS aktivieren, führt Cloud Volumes ONTAP standardmäßig inaktive Daten auf die S3 Standard-Storage-Klasse aus. Sie können nun die Tiering-Stufe in die Klasse *Intelligent Tiering* Storage ändern. Diese Storage-Klasse optimiert Storage-Kosten, indem Daten bei sich ändernden

Datenzugriffsmustern zwischen zwei Tiers verschoben werden. Eine Ebene ist für häufigen Zugriff und die andere für unregelmäßigen Zugriff.

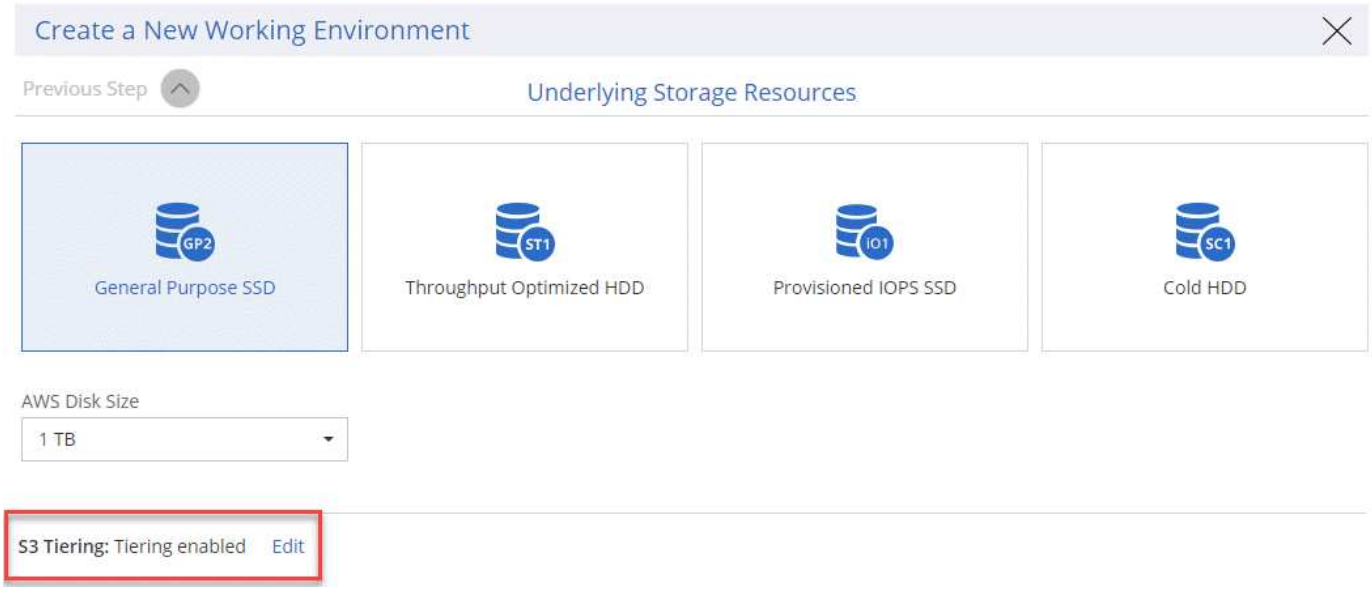
Wie in vorherigen Versionen können Sie auch die Standard-infrequent Access Tier und die one Zone-infrequent Access Tier verwenden.

"Weitere Informationen zum Daten-Tiering" Und "Erfahren Sie, wie Sie die Storage-Klasse ändern".

Möglichkeit, Daten-Tiering auf dem ursprünglichen Aggregat zu deaktivieren

In vorherigen Versionen aktivierte Cloud Manager das Daten-Tiering automatisch auf dem ersten Cloud Volumes ONTAP Aggregat. Sie können jetzt entscheiden, das Daten-Tiering auf diesem ersten Aggregat zu deaktivieren. (Sie können das Daten-Tiering auch bei nachfolgenden Aggregaten aktivieren oder deaktivieren.)

Diese neue Option ist bei der Auswahl der zugrunde liegenden Storage-Ressourcen verfügbar. Die folgende Abbildung zeigt ein Beispiel zum Starten eines Systems in AWS:



Empfohlener EC2-Instanztyp jetzt t3.Medium für Cloud Manager

Der Instanztyp für Cloud Manager ist jetzt t3.Medium, wenn Cloud Manager in AWS über NetApp Cloud Central bereitgestellt wird. Es ist auch der empfohlene Instanztyp in AWS Marketplace. Somit wird der Support in den neuesten AWS Regionen ermöglicht und die Instanzkosten sinken. Der empfohlene Instanztyp war vorher t2.Medium, der noch unterstützt wird.

Verschiebung geplanter Abschaltungen während der Datenübertragung

Wenn Sie ein automatisches Herunterfahren des Cloud Volumes ONTAP Systems geplant haben, verschiebt Cloud Manager jetzt das Herunterfahren, wenn ein aktiver Datentransfer stattfinden soll. Cloud Manager schaltet das System nach Abschluss der Übertragung aus.

Cloud Manager 3.6.2 (2. Jan. 2019)

Cloud Manager 3.6.2 umfasst neue Funktionen und Verbesserungen.

- AWS Spread Placement Group für Cloud Volumes ONTAP HA in einer einzelnen Verfügbarkeitszone
- Schutz durch Ransomware

- Neue Datenreplizierungsrichtlinien
- Volume-Zugriffssteuerung für Kubernetes

AWS Spread Placement Group für Cloud Volumes ONTAP HA in einer einzelnen Verfügbarkeitszone

Wenn Sie Cloud Volumes ONTAP HA in einer einzelnen AWS Verfügbarkeitszone implementieren, erstellt Cloud Manager jetzt 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.

Cloud Manager erfordert neue Berechtigungen für diese Funktion. Vergewissern Sie sich, dass die IAM-Richtlinie, die Cloud Manager über Berechtigungen verfügt, die folgenden Aktionen umfasst:

```
"ec2:CreatePlacementGroup",
"ec2:DeletePlacementGroup"
```

Die gesamte Liste der erforderlichen Berechtigungen finden Sie im "Aktuelle AWS Richtlinie für Cloud Manager".

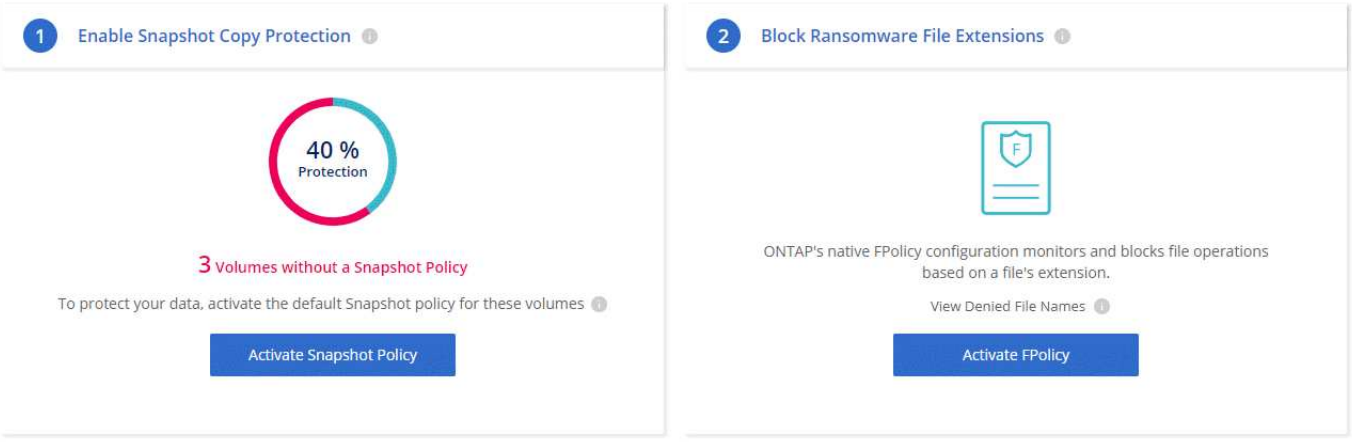
Schutz durch Ransomware

Ransomware-Angriffe können das Unternehmen Zeit, Ressourcen und Image-Schäden kosten. Cloud Manager ermöglicht Ihnen nun 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".

Neue Datenreplizierungsrichtlinien

Cloud Manager enthält fünf neue Datenreplizierungsrichtlinien für die Datensicherung.

Durch drei der Richtlinien wird die Disaster Recovery und die langfristige Aufbewahrung von Backups auf demselben Ziel-Volume konfiguriert. Jede Richtlinie bietet eine andere Aufbewahrungsdauer für Backups:

- Mirror und Backup (7-Jahres-Aufbewahrung)
- Spiegelung und Backup (7 Jahre Aufbewahrung mit mehr wöchentlichen Backups)
- Mirror und Backup (1 Jahr Aufbewahrung, monatlich)

Die verbleibenden Richtlinien bieten mehr Optionen für die langfristige Aufbewahrung von Backups:

- Backup (1-monatige Aufbewahrung)
- Backup (Aufbewahrung von 1 Woche)

Ziehen Sie einfach eine Arbeitsumgebung per Drag-and-Drop, um eine der neuen Richtlinien auszuwählen.

Volume-Zugriffssteuerung für Kubernetes

Die Exportrichtlinie für Kubernetes-persistente Volumes lässt sich nun konfigurieren. Die Exportrichtlinie kann den Zugriff auf Clients ermöglichen, wenn sich das Kubernetes-Cluster in einem anderen Netzwerk als das Cloud Volumes ONTAP System befindet.

Sie können die Exportrichtlinie konfigurieren, wenn Sie eine Arbeitsumgebung mit einem Kubernetes-Cluster verbinden und ein vorhandenes Volume bearbeiten.

Cloud Manager 3.6.1 (4. Dezember 2018)

Cloud Manager 3.6.1 umfasst neue Funktionen und Verbesserungen.

- Unterstützung von Cloud Volumes ONTAP 9.5 in Azure
- Accounts Von Cloud-Providern
- Verbesserungen am AWS Kostenbericht
- Unterstützung für neue Azure Regionen

Unterstützung von Cloud Volumes ONTAP 9.5 in Azure

Cloud Manager unterstützt jetzt die Version Cloud Volumes ONTAP 9.5 in Microsoft Azure, die eine Vorschau auf HA-Paare enthält. Sie können eine Vorschaulizenz für ein Azure HA-Paar anfordern. Senden Sie dazu eine eMail an ng-Cloud-Volume-ONTAP-preview@netapp.com.

Weitere Informationen zur Version 9.5 finden Sie im "Versionshinweise zu Cloud Volumes ONTAP 9.5".

Für Cloud Volumes ONTAP 9.5 sind neue Azure Berechtigungen erforderlich

Cloud Manager erfordert neue Azure Berechtigungen für die wichtigsten Funktionen von Cloud Volumes ONTAP 9.5. Um sicherzustellen, dass Cloud Manager Cloud Volumes ONTAP 9.5-Systeme implementieren und managen kann, sollten Sie Ihre Cloud Manager-Richtlinie aktualisieren, indem Sie die folgenden Berechtigungen hinzufügen:

```
"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",
"Microsoft.Network/routeTables/join/action"
"Microsoft.Authorization/roleDefinitions/write",
"Microsoft.Authorization/roleAssignments/write",
"Microsoft.Web/sites/*"
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/usages/read",
```

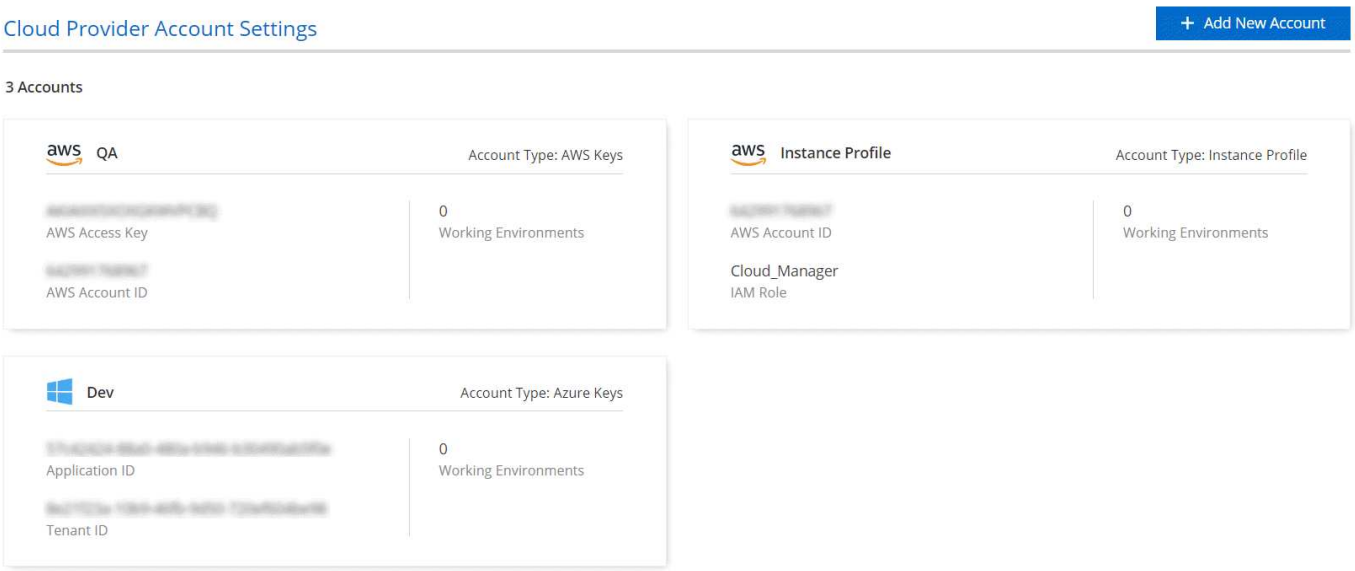
Die gesamte Liste der erforderlichen Berechtigungen finden Sie im "Aktuelle Azure-Richtlinie für Cloud Manager".

"So verwendet Cloud Manager diese Berechtigungen".

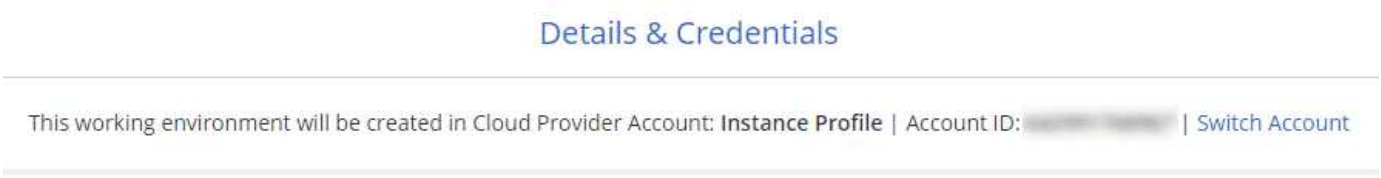
Accounts Von Cloud-Providern

Es ist jetzt einfacher, mehrere AWS und Azure Konten in Cloud Manager über Cloud-Provider-Konten zu managen.

In vorherigen Versionen mussten Sie für jedes Cloud Manager Benutzerkonto Berechtigungen für Cloud-Provider angeben. Die Berechtigungen werden jetzt auf Cloud Manager Systemebene über Cloud Provider Accounts verwaltet.



Wenn Sie eine neue Arbeitsumgebung erstellen, wählen Sie einfach das Konto aus, in dem Sie das Cloud Volumes ONTAP-System bereitstellen möchten:



Beim Upgrade auf 3.6 erstellt Cloud Manager basierend auf der aktuellen Konfiguration automatisch Cloud Provider-Konten für Sie. Wenn Sie Skripts haben, ist die Abwärtskompatibilität vorhanden, sodass nichts unterbrochen wird.

- "Funktionsweise von Cloud-Provider-Konten und -Berechtigungen"
- "Erfahren Sie, wie Sie Cloud Provider Accounts einrichten und zu Cloud Manager hinzufügen"

Verbesserungen am AWS Kostenbericht

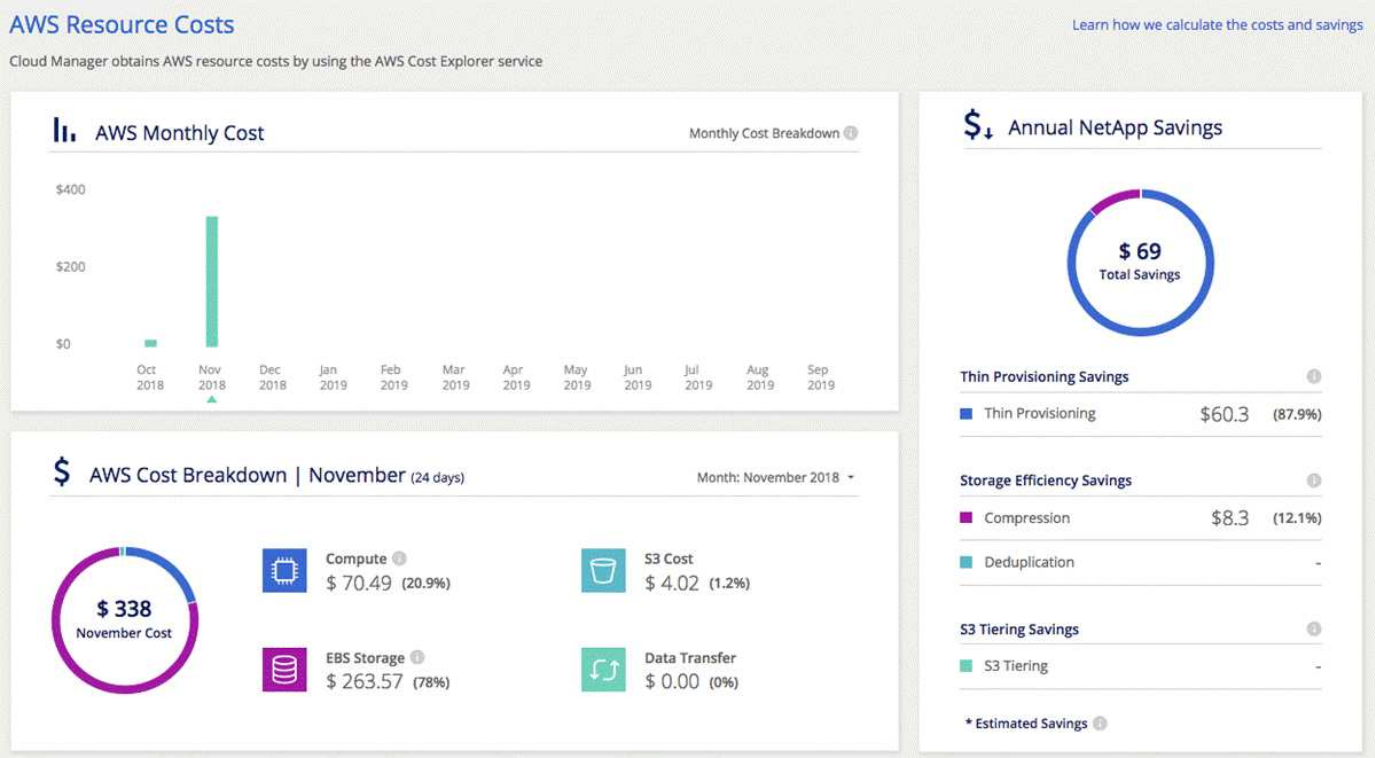
Der AWS Kostenbericht bietet jetzt mehr Informationen und lässt sich einfacher einrichten.

- Der Bericht unterteilt die monatlichen Ressourcenkosten, die für den Einsatz von Cloud Volumes ONTAP in AWS anfallen. Sie können die monatlichen Kosten für Computing, EBS Storage (einschließlich EBS Snapshots), S3 Storage und Datentransfers anzeigen.
- Der Bericht zeigt jetzt Kosteneinsparungen an, wenn Sie inaktive Daten nach S3 verschieben.
- Wir haben auch vereinfacht, wie Cloud Manager Kostendaten aus AWS holt.

  Cloud Manager benötigt keinen Zugriff mehr auf die Rechnungsberichte, die Sie in einem S3-Bucket speichern. Stattdessen verwendet Cloud Manager die Cost Explorer API. Sie müssen lediglich sicherstellen, dass die IAM-Richtlinie, die Cloud Manager über Berechtigungen verfügt, die folgenden Aktionen beinhaltet:

  ```
  "ce:GetReservationUtilization",
  "ce:GetDimensionValues",
  "ce:GetCostAndUsage",
  "ce:GetTags"
  ```

  Diese Aktionen sind in den letzten enthalten "Von NetApp bereitgestellte Richtlinie". Neue Systeme, die von NetApp Cloud Central implementiert werden, enthalten automatisch diese Berechtigungen.



Unterstützung für neue Azure Regionen

Sie können jetzt Cloud Manager und Cloud Volumes ONTAP in der Region Frankreich Central implementieren.

Cloud Manager 3.6 (4. November 2018)

Cloud Manager 3.6 enthält eine neue Funktion.

Verwendung von Cloud Volumes ONTAP als persistenter Storage für einen Kubernetes-Cluster

Cloud Manager kann die Implementierung von jetzt automatisieren "NetApp Trident" In einem einzelnen Kubernetes-Cluster können Sie Cloud Volumes ONTAP als persistenten Storage für Container verwenden. So können Benutzer persistente Volumes über native Kubernetes-Schnittstellen und -Konstrukte anfordern und managen und gleichzeitig die erweiterten Datenmanagement-Funktionen von ONTAP nutzen, ohne etwas darüber wissen zu müssen.

"Verbinden Sie Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster"

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 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.

Einschränkungen bei der Volume-Ansicht

- Die Volume-Ansicht wird in der AWS GovCloud (US)-Region, in der AWS Commercial Cloud Services-Umgebung und in Microsoft Azure nicht unterstützt.
- Mit der Volume-Ansicht können Sie nur NFS-Volumes erstellen.
- Cloud Manager startet Cloud Volumes ONTAP Byol Instanzen nicht in der Volume View.

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.

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

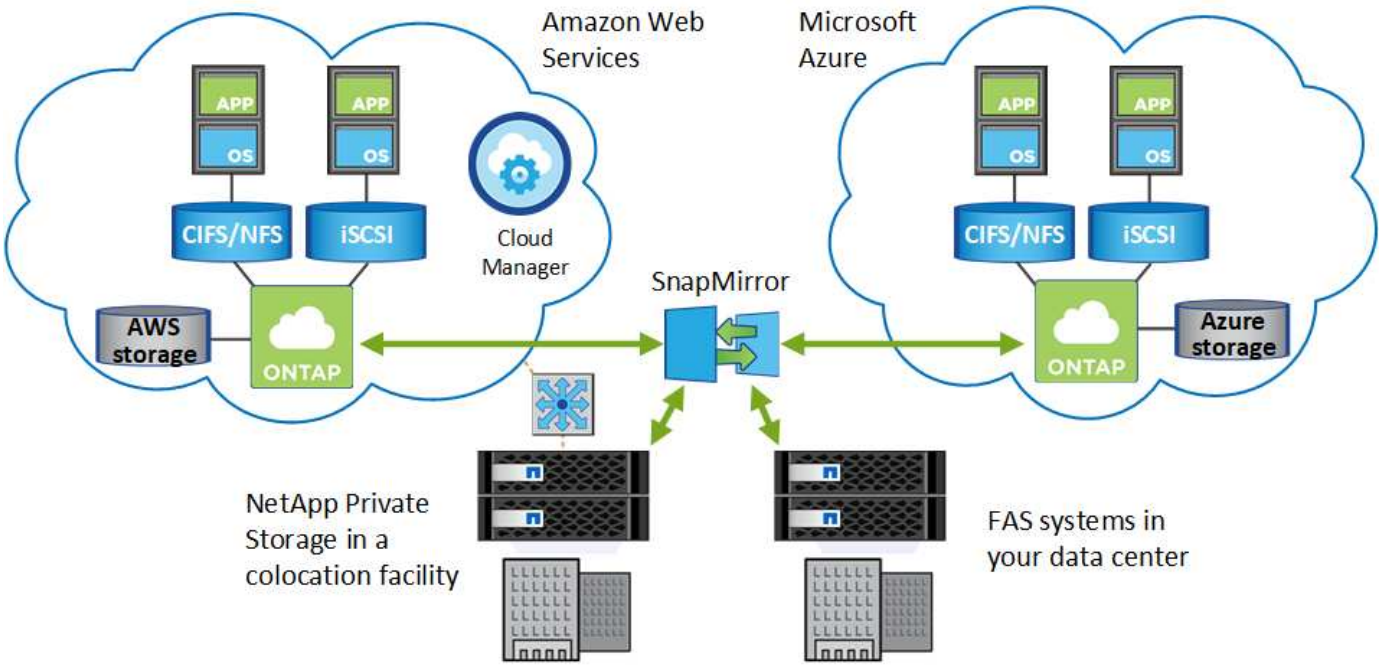
Mit OnCommand Cloud Manager können Sie Cloud Volumes ONTAP implementieren, das Funktionen der Enterprise-Klasse für Ihren Cloud-Storage bietet, und Daten einfach über Hybrid Clouds hinweg replizieren, die auf NetApp basieren.

Cloud Manager

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

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

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



"Erfahren Sie mehr über Cloud Manager"

Cloud Volumes ONTAP

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

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

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

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

"Anzeigen der unterstützten Cloud Volumes ONTAP Konfigurationen"

"Erfahren Sie mehr über Cloud Volumes ONTAP"

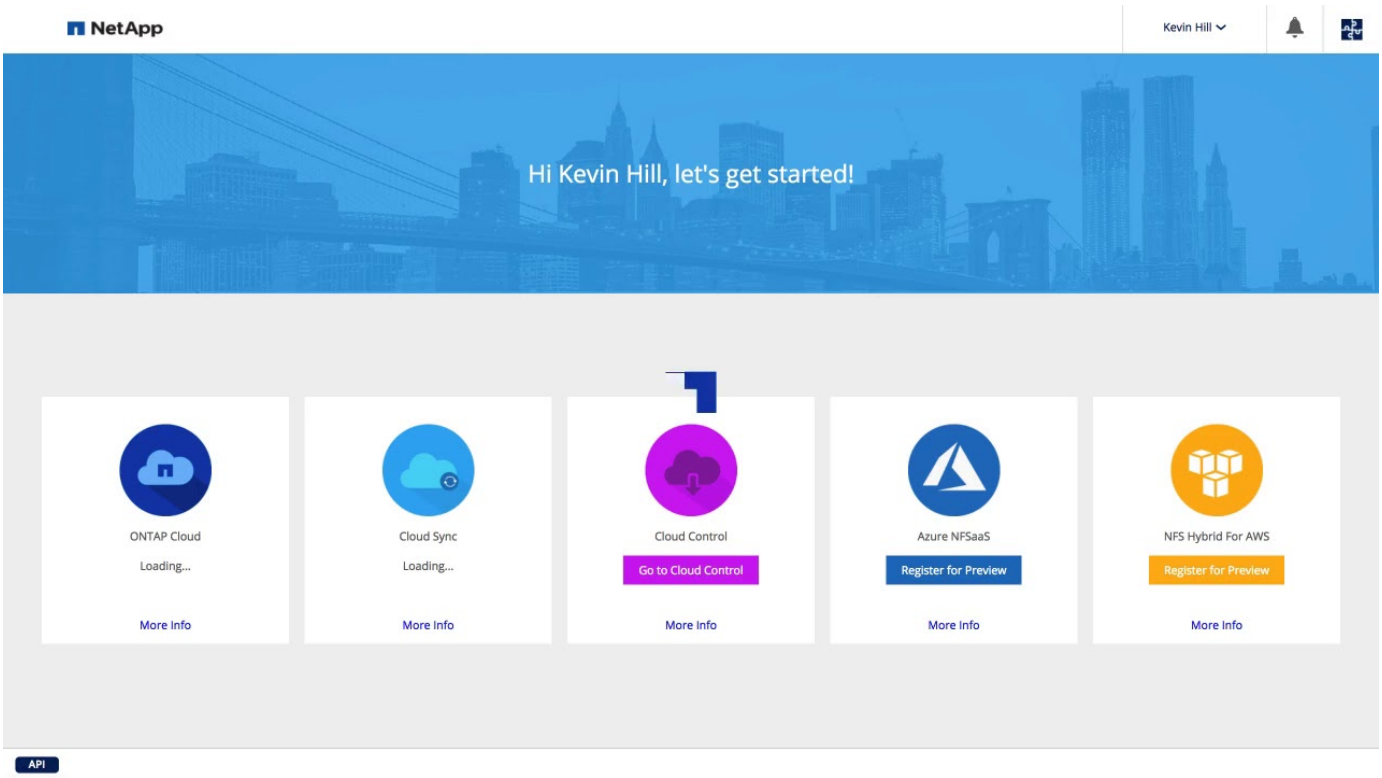
NetApp Cloud Central

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

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

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

Das folgende Video bietet einen Überblick über NetApp Cloud Central:



Konten und Berechtigungen für Cloud-Provider

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

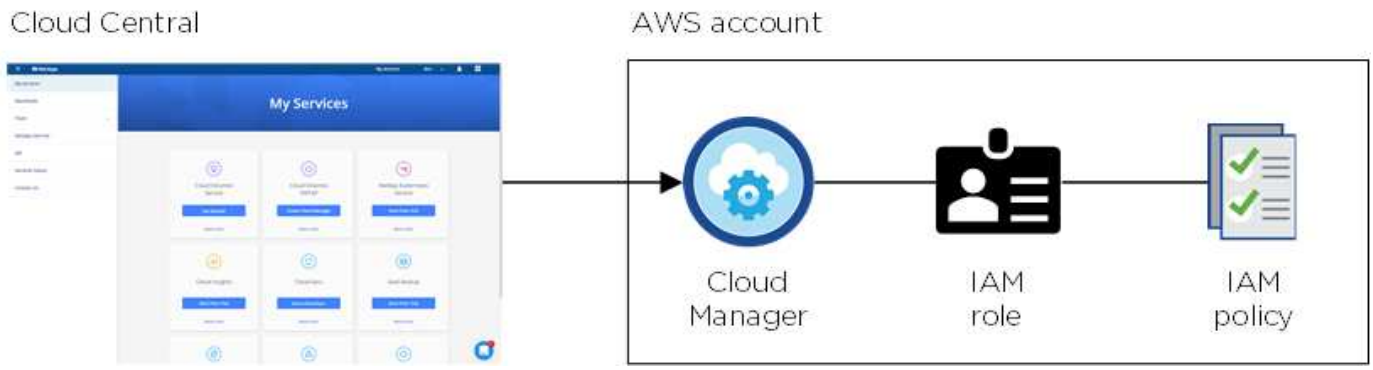
AWS Konten und Berechtigungen

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

Über das erste AWS Konto

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

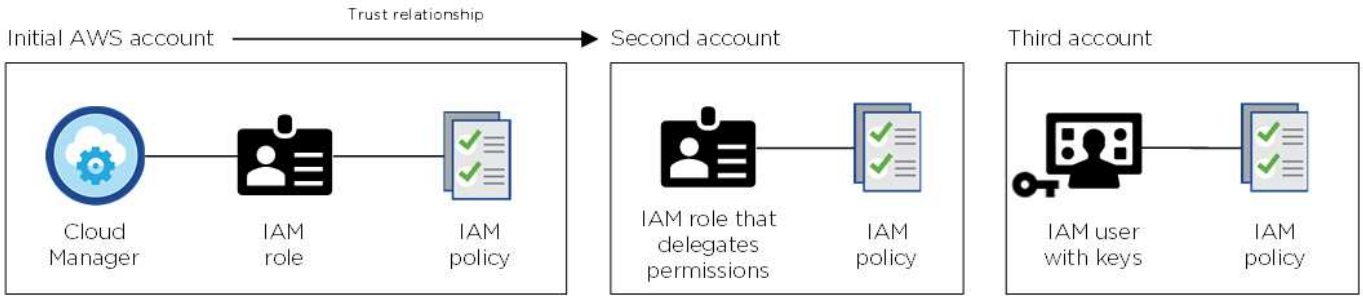
Wenn Cloud Central die Cloud Manager Instanz in AWS startet, wird eine IAM-Rolle und ein Instanzprofil für die Instanz erstellt. Zudem wird eine Richtlinie angehängt, die Cloud Manager Berechtigungen für die Implementierung und das Management von Cloud Volumes ONTAP in diesem AWS-Konto bereitstellt.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



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

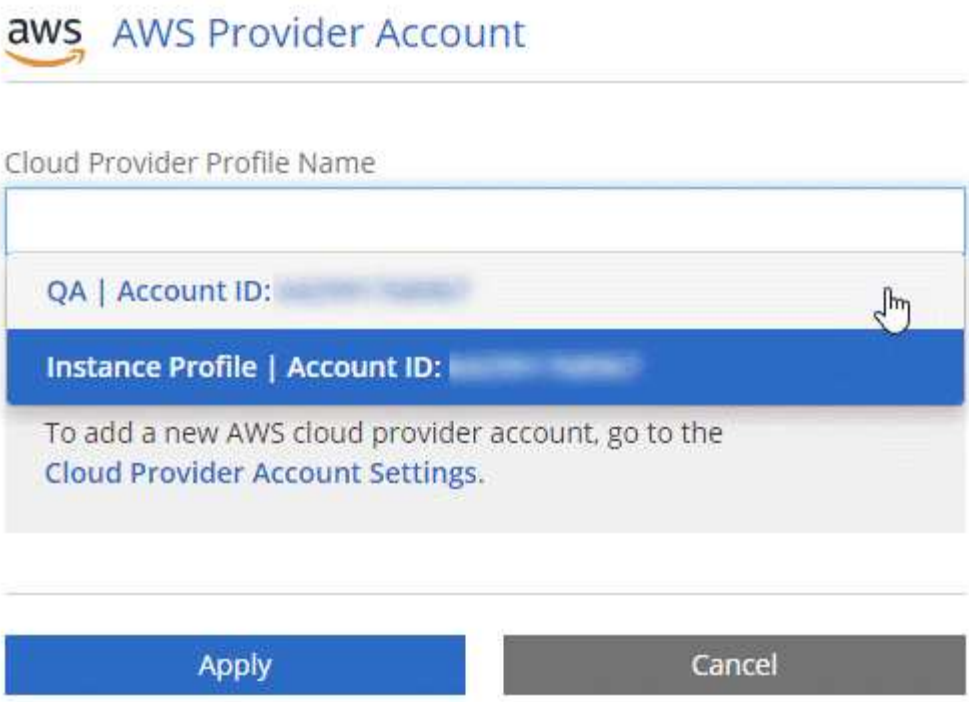
Weitere AWS Konten

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:



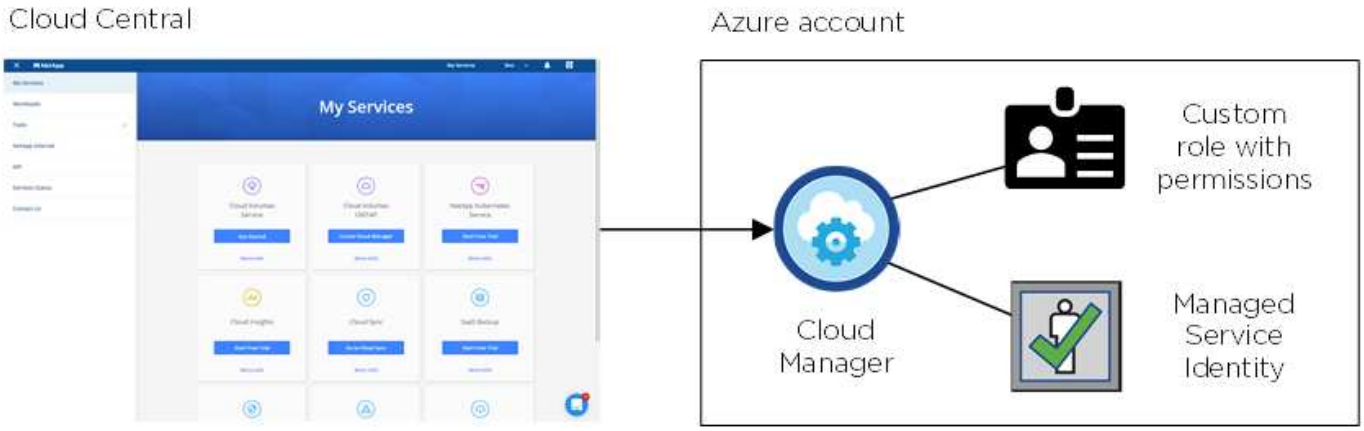
Azure-Konten und Berechtigungen

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

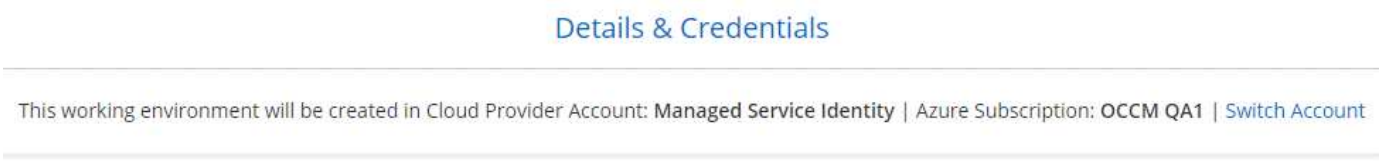
Zunächst das Azure-Konto

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

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



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

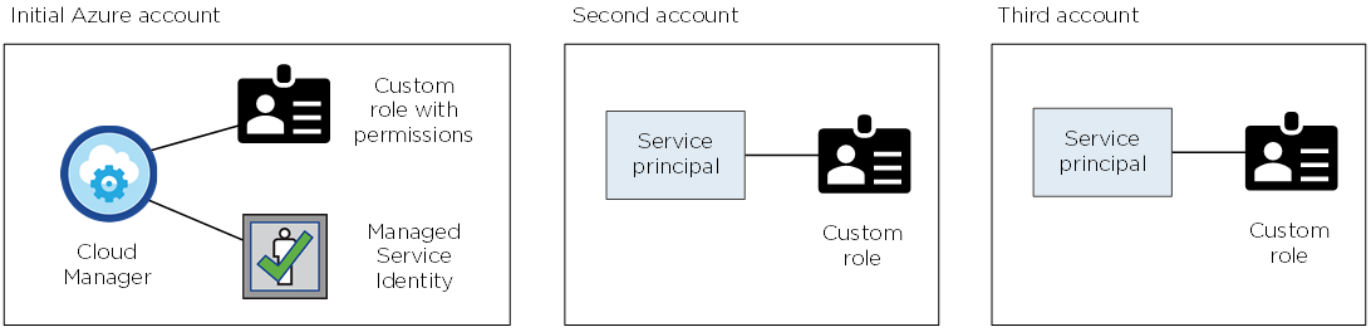


Zusätzliche Azure-Abonnements für das Erstkonto

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".

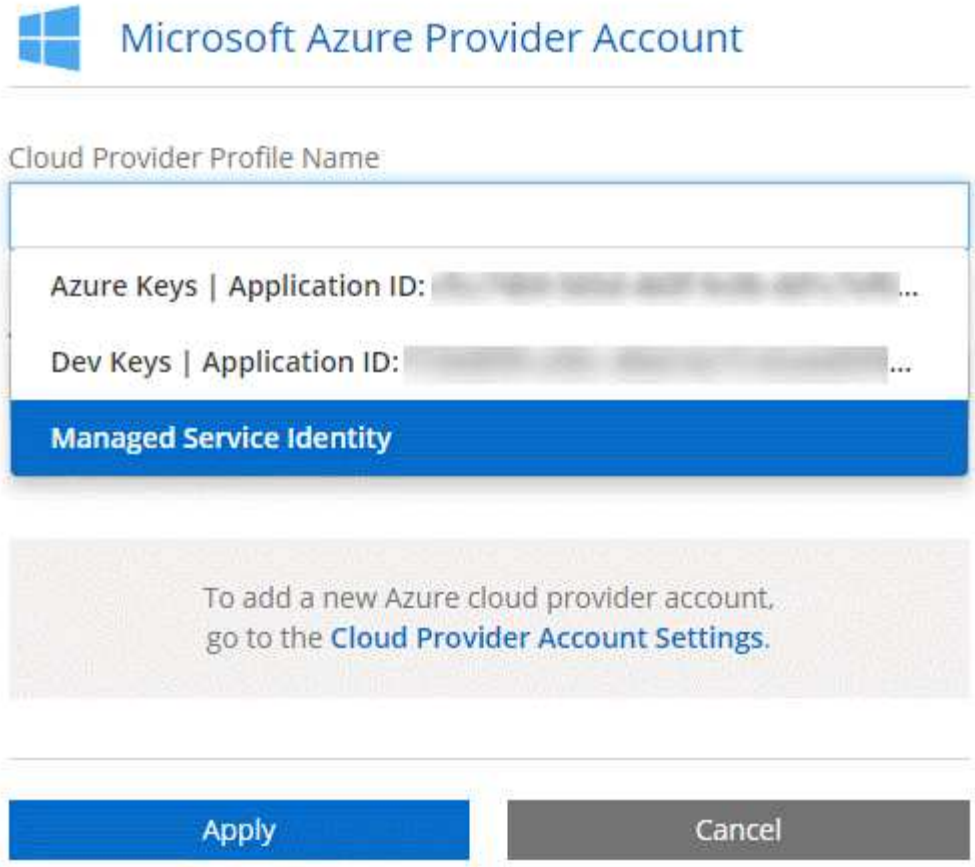
Zusätzliche Azure-Konten

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

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

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

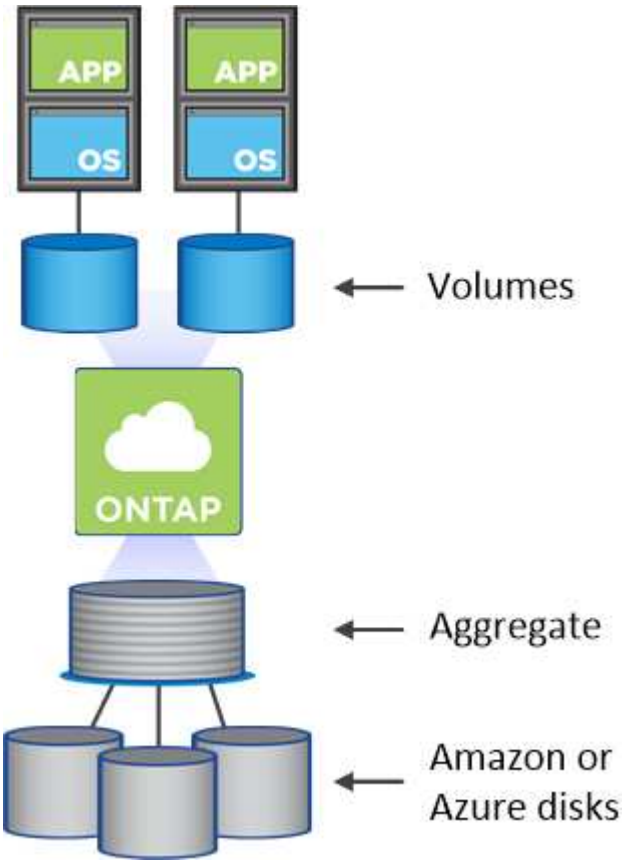
Storage

Wie Cloud Volumes ONTAP Cloud Storage verwendet

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

Überblick

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



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

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

AWS Storage

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

Der zugrunde liegende EBS-Festplattentyp kann entweder eine Universal-SSD, eine bereitgestellte IOPS-SSD, eine für den Durchsatz optimierte Festplatte oder eine kalte Festplatte sein. Es ist auch möglich, eine EBS-Festplatte für zu koppeln "Daten-Tiering".

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

- *Universal SSD* Festplatten balancieren Kosten und Performance für ein breites Spektrum an Workloads aus. Die Performance wird in Bezug auf IOPS definiert.
- *Bereitgestellte IOPS SSD*-Festplatten sind für kritische Applikationen geeignet, die höchste Performance

zu höheren Kosten erfordern.

- _Optimierte Festplatten mit hohem Durchsatz sind für häufig genutzte Workloads konzipiert, die einen schnellen und konsistenten Durchsatz zu einem niedrigeren Preis erfordern.
- *Cold HDD* Festplatten werden für Backups oder selten genutzte Daten gedacht, da die Performance nur sehr gering ist. Wie bei Festplatten mit Durchsatzoptimierung wird die Performance in Bezug auf den Durchsatz definiert.

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

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

"Lesen Sie, wie Sie Festplattentypen und Festplattengrößen für Ihre Systeme in AWS auswählen".

"Prüfen der Storage-Limits für Cloud Volumes ONTAP".

Azure Storage

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

Systeme mit einzelnen Nodes

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

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

  Jeder verwaltete Festplattentyp hat eine maximale Festplattengröße von 32 TB.

  Sie können eine gemanagte Festplatte mit Azure Blob Storage für kombinieren "Daten-Tiering".

HA-Paare

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

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

"Erfahren Sie, wie Sie Festplattentypen und Festplattengrößen für Ihre Systeme in Azure auswählen".

"Prüfen der Storage-Limits für Cloud Volumes ONTAP".

Data Tiering - Übersicht

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

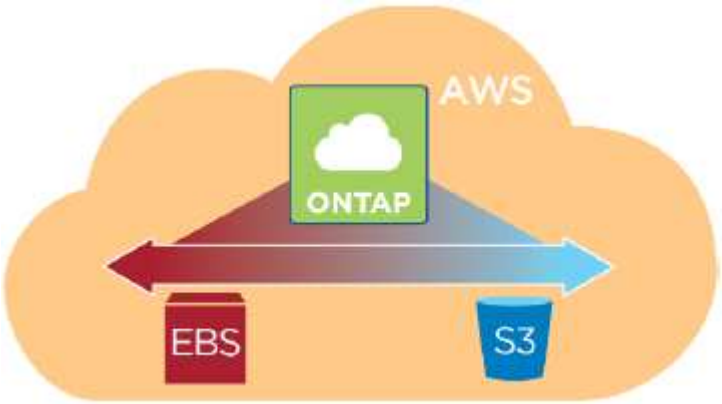
hochperformanten SSDs oder HDDs (dem Performance-Tier), während inaktive Daten auf kostengünstigen Objektspeicher (dem Kapazitäts-Tier) gestaffelt werden. Dadurch können Sie Speicherplatz auf Ihrem primären Storage zurückgewinnen und den sekundären Storage verkleinern.

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

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

Funktionsweise von Data Tiering in AWS

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



Performance Tier in AWS

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

Kapazitäts-Tier in AWS

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

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

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

Ein einmaliger Zugriff
: Für selten genutzte Daten, die in einer einzigen Verfügbarkeitszone gespeichert sind.

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

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

bevor Sie die Tiering Level ändern. Weitere Informationen zu S3-Speicherklassen finden Sie unter "AWS-Dokumentation".

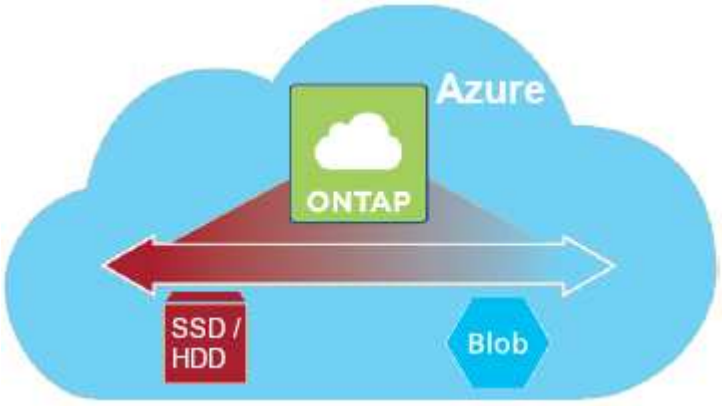
Wenn Sie die Tiering-Ebene ändern, werden inaktive Daten in der Klasse Standard-Speicher gestartet und in die von Ihnen ausgewählte Speicherklasse verschoben, sofern nach 30 Tagen kein Zugriff auf die Daten erfolgt. Weitere Informationen zum Ändern der Tiering-Ebene finden Sie unter "Tiering inaktiver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

Die Tiering-Ebene ist systemweit, nicht pro Volume.

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

Funktionsweise von Data Tiering in Microsoft Azure

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



Performance Tier in Azure

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

Kapazitäts-Tier in Azure

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

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

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

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

Die Tiering-Ebene ist systemweit, nicht pro Volume.

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

Auswirkungen von Data Tiering auf Kapazitätsgrenzen

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

Richtlinien für das Volume-Tiering

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

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

Cloud Volumes ONTAP unterstützt die folgenden Tiering Policies:

Nur Snapshot

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

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

Automatisch

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

Diese Richtlinie wird ab Cloud Volumes ONTAP 9.4 unterstützt.

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

Backup

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

Keine

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

Einrichten von Data Tiering

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

Storage-Management

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

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

Storage-Bereitstellung

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

Vereinfachte Bereitstellung

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

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

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

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

Der Cloud Manager Administrator kann die Schwellenwerte für freien Speicherplatz auf der Seite **Einstellungen** ändern.

Auswahl der Festplattengröße für Aggregate in AWS

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

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

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

Sie können die Festplattengröße selbst mithilfe der erweiterten Zuweisungsoption auswählen.

Erweiterte Zuweisung

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

Kapazitätsmanagement

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

Automatisches Kapazitätsmanagement

Wenn der Cloud Manager Administrator den Kapazitätsmanagement-Modus auf automatisch eingestellt hat, kauft Cloud Manager automatisch neue Festplatten für Cloud Volumes ONTAP-Instanzen, wenn mehr Kapazität benötigt wird, löscht nicht verwendete Festplatten-Sammlungen (Aggregate), verschiebt Volumes zwischen Aggregaten bei Bedarf und versucht, Festplatten nicht ordnungsgemäß wiederherzustellen.

Die folgenden Beispiele veranschaulichen die Funktionsweise dieses Modus:

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

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

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

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

Manuelles Kapazitätsmanagement

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

Storage-Isolierung mithilfe von Mandanten

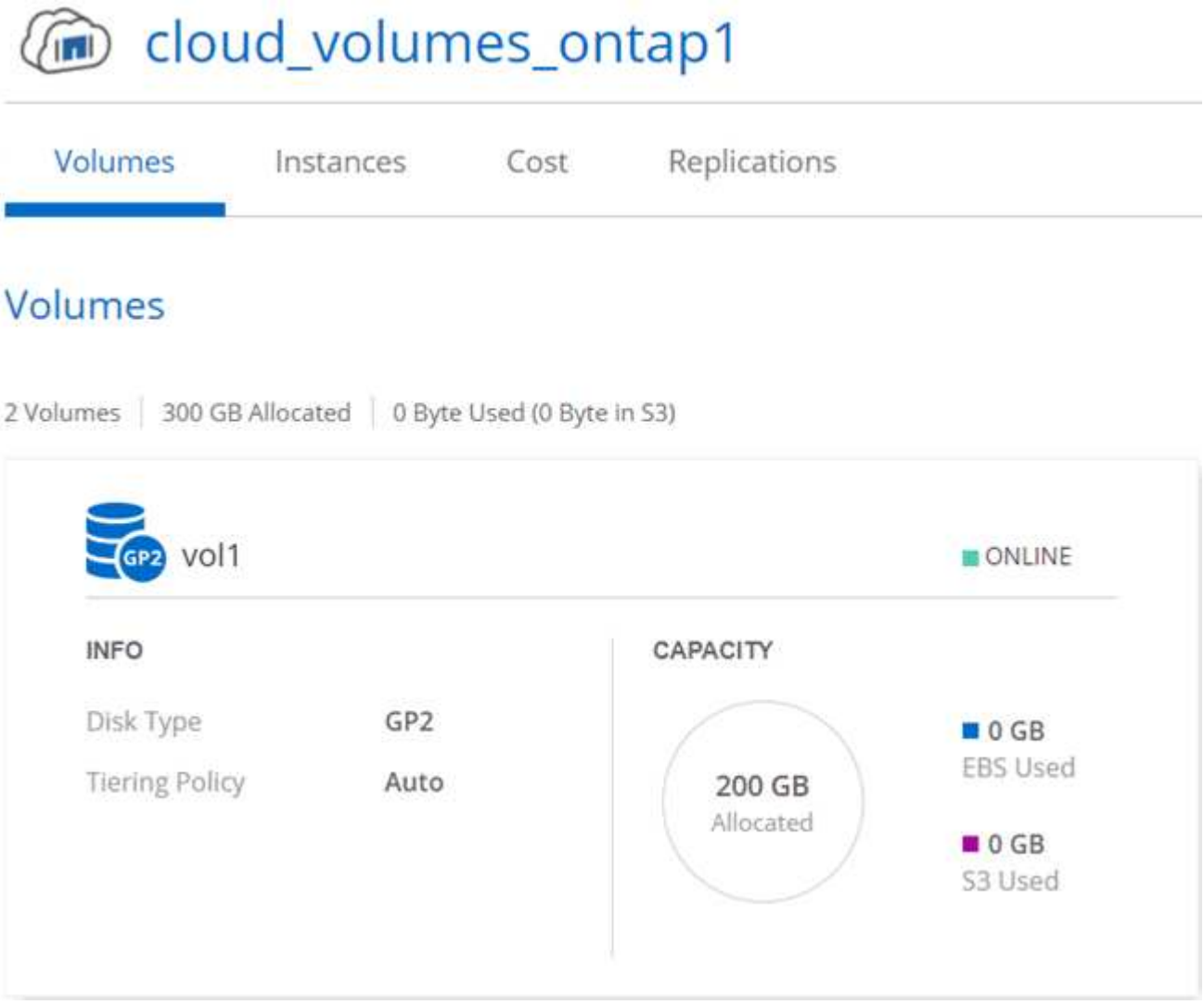
Mit Cloud Manager können Sie Storage in isolierten Gruppen, so genannten Mandanten, bereitstellen und managen. Sie müssen entscheiden, wie Cloud Manager-Benutzer und ihre Arbeitsumgebungen über Mandanten hinweg organisiert werden.

Arbeitsumgebungen

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

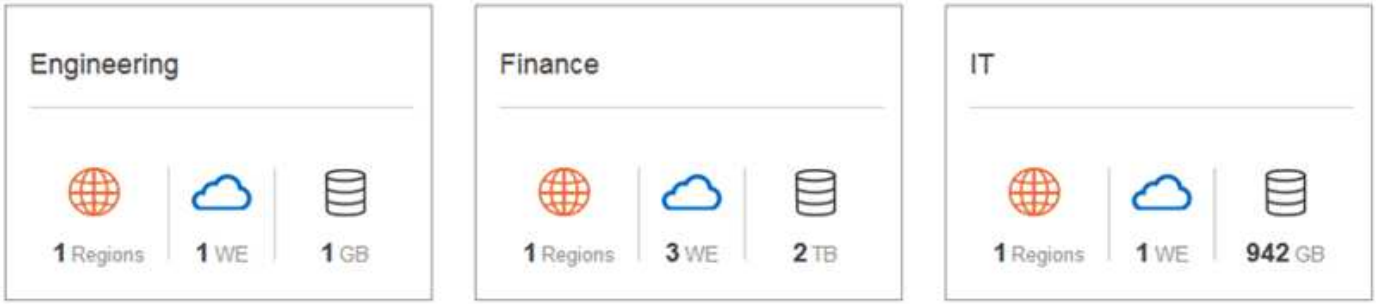
- Ein einzelnes Cloud Volumes ONTAP System oder ein HA-Paar
- Ein On-Premises ONTAP Cluster in Ihrem Netzwerk
- Ein ONTAP Cluster in einer NetApp Private Storage-Konfiguration

Das folgende Bild zeigt eine Cloud Volumes ONTAP Arbeitsumgebung:



Mandanten

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



Benutzerverwaltung von Mandanten und Arbeitsumgebungen

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

Cloud Manager Admin

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

Mandantenverwaltung

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

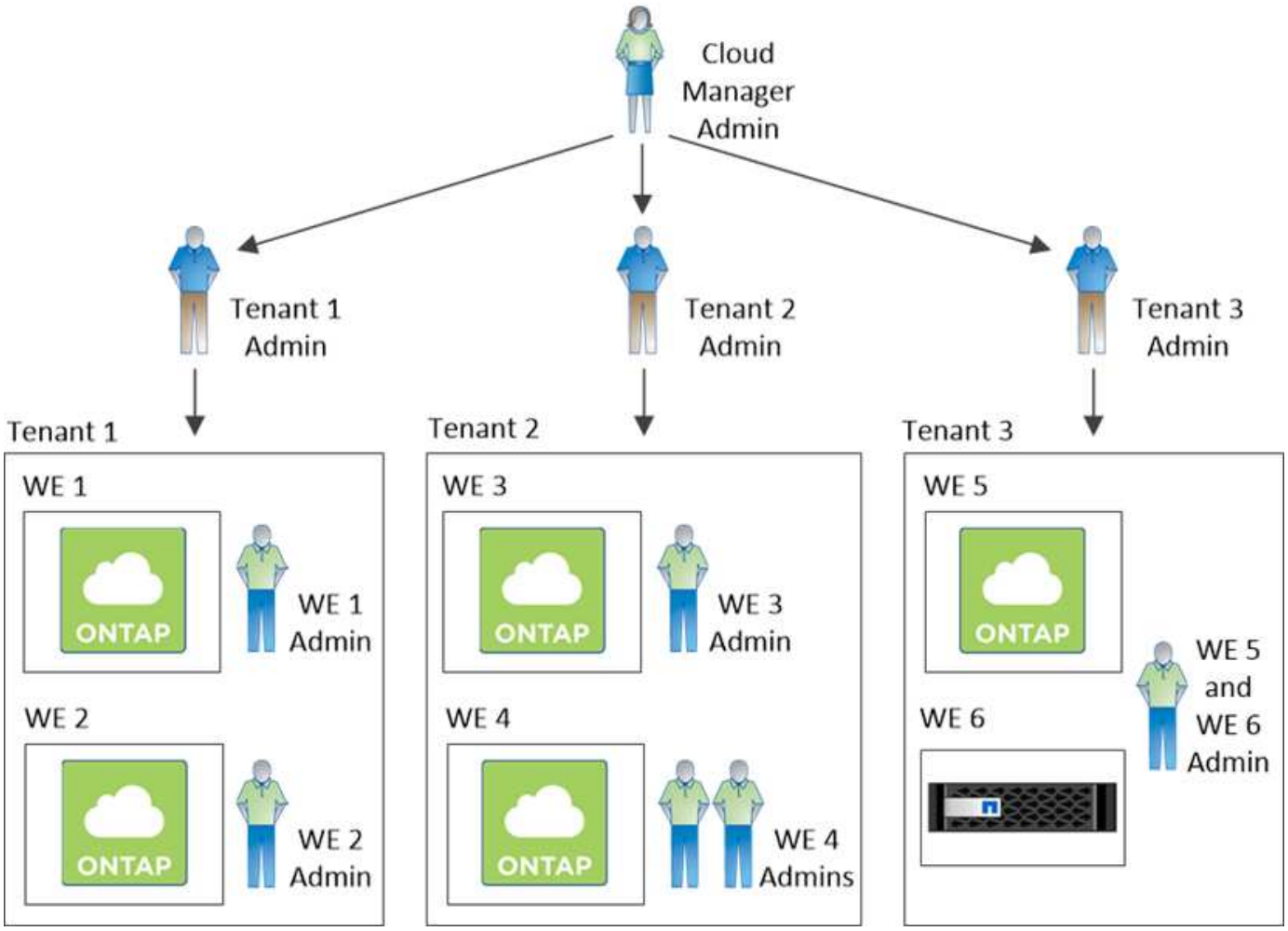
Administrator der Arbeitsumgebung

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

Beispiel für das Erstellen von Mandanten und Benutzern

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

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

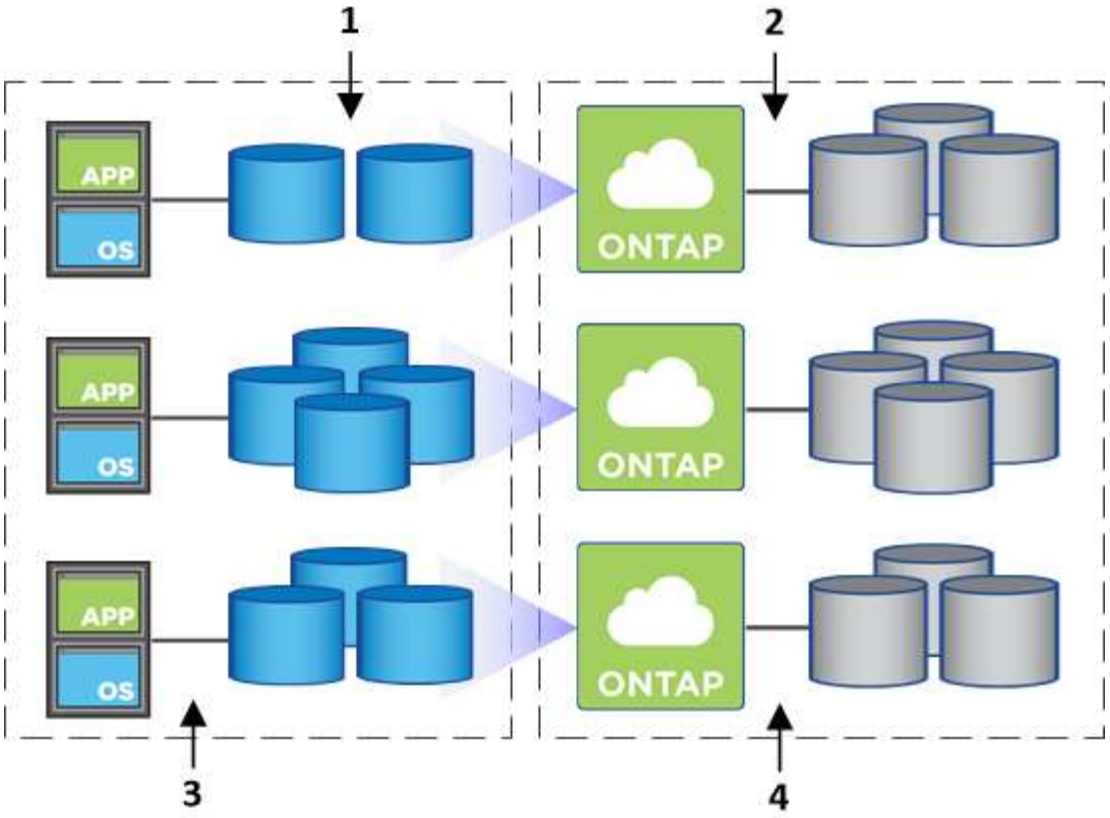


Vereinfachtes Storage-Management mit der Volume-Ansicht

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

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

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

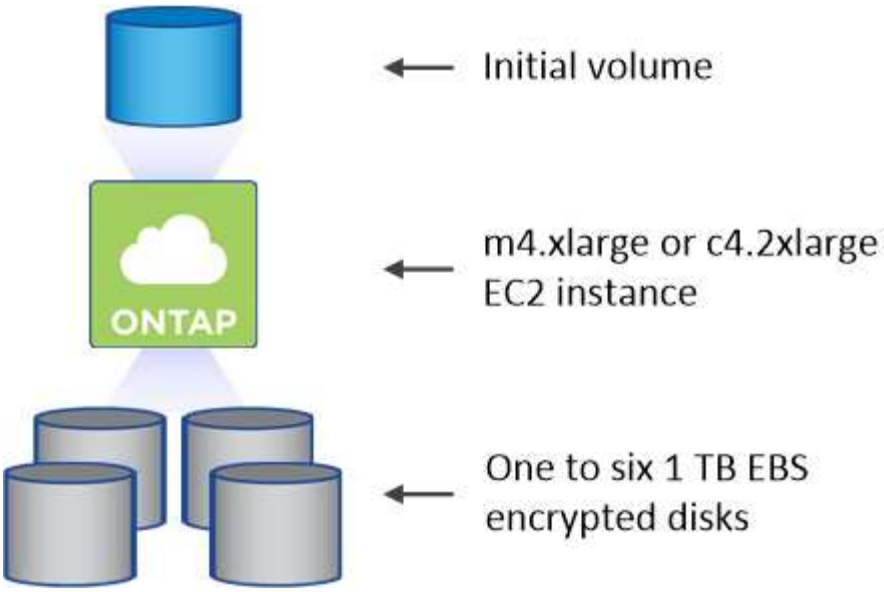


1. Sie erstellen NFS-Volumes.
2. Cloud Manager startet Cloud Volumes ONTAP Instanzen in AWS für neue Volumes oder erstellt Volumes auf vorhandenen Instanzen. Darüber hinaus wird physischer EBS Storage für die Volumes erworben.
3. Sie stellen die Volumes Ihren Hosts und Applikationen zur Verfügung.
4.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

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

Zuweisung von Cloud-Ressourcen für das anfängliche Volume

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



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

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

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

Zuweisung von Cloud-Ressourcen für zusätzliche Volumes

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

NetApp Storage-Effizienzfunktionen und Storage-Kosten

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

Entscheidungen zur Kapazitätszuweisung, die Cloud Manager automatisch übernimmt

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

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

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

WORM-Storage

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

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

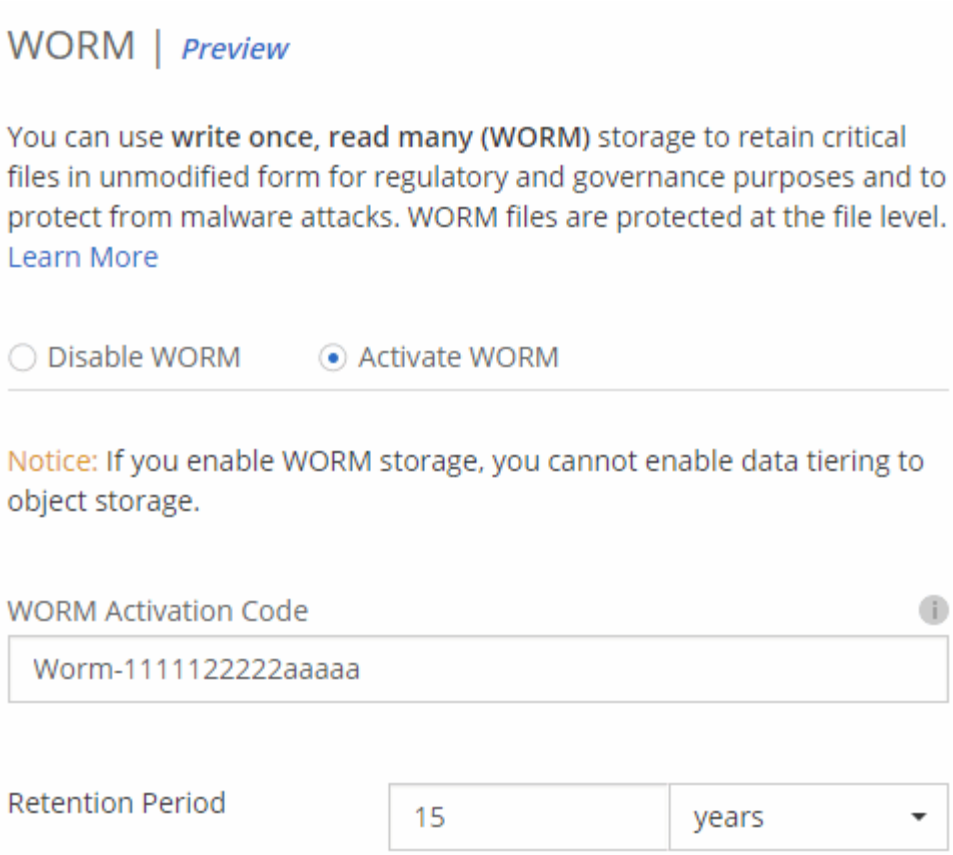
Nach Ablauf der Aufbewahrungsfrist sind Sie dafür verantwortlich, alle Dateien zu löschen, die Sie nicht mehr benötigen.

WORM-Storage wird aktiviert

Sie können WORM Storage auf einem Cloud Volumes ONTAP System aktivieren, wenn Sie eine neue Arbeitsumgebung erstellen. Dazu gehört die Angabe eines 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.

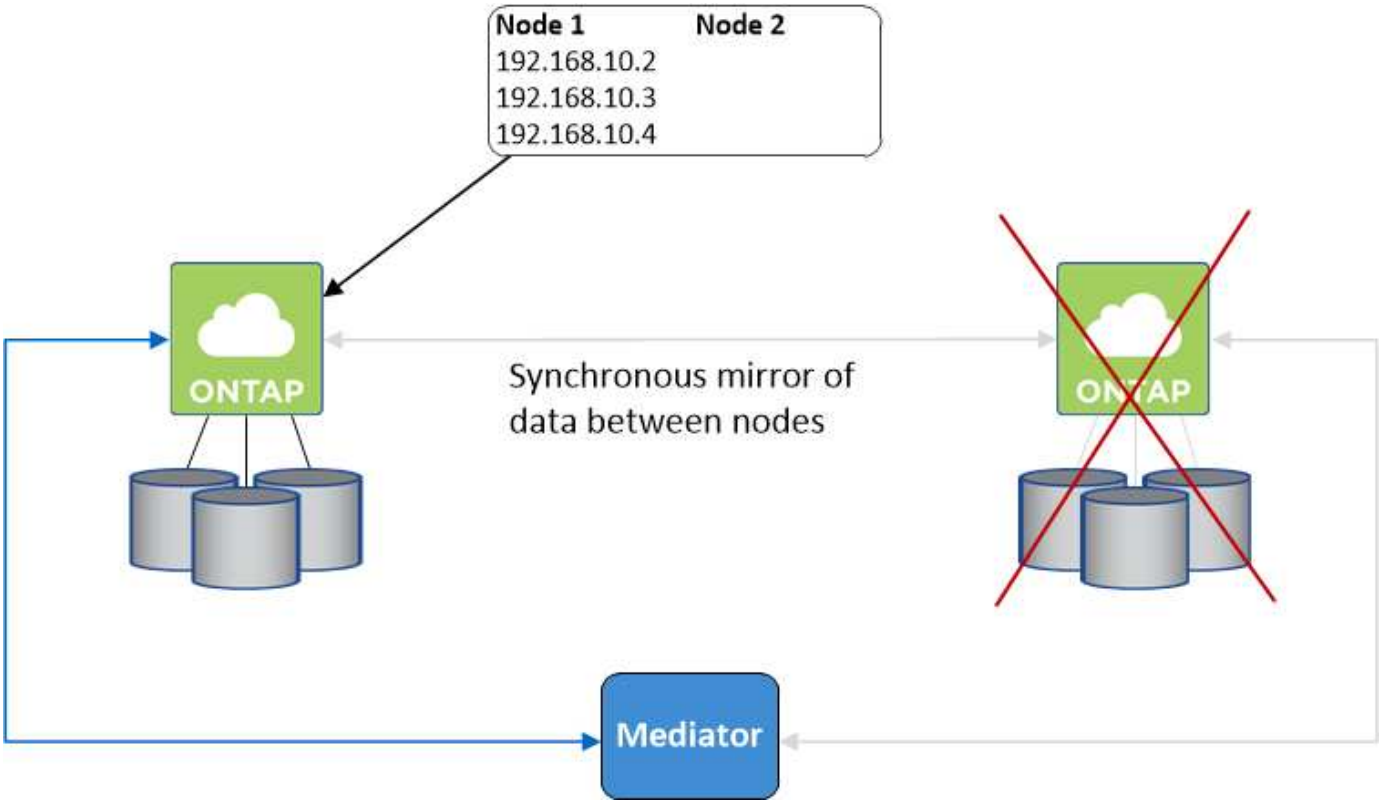
Storage-Übernahme und -Giveback für iSCSI

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

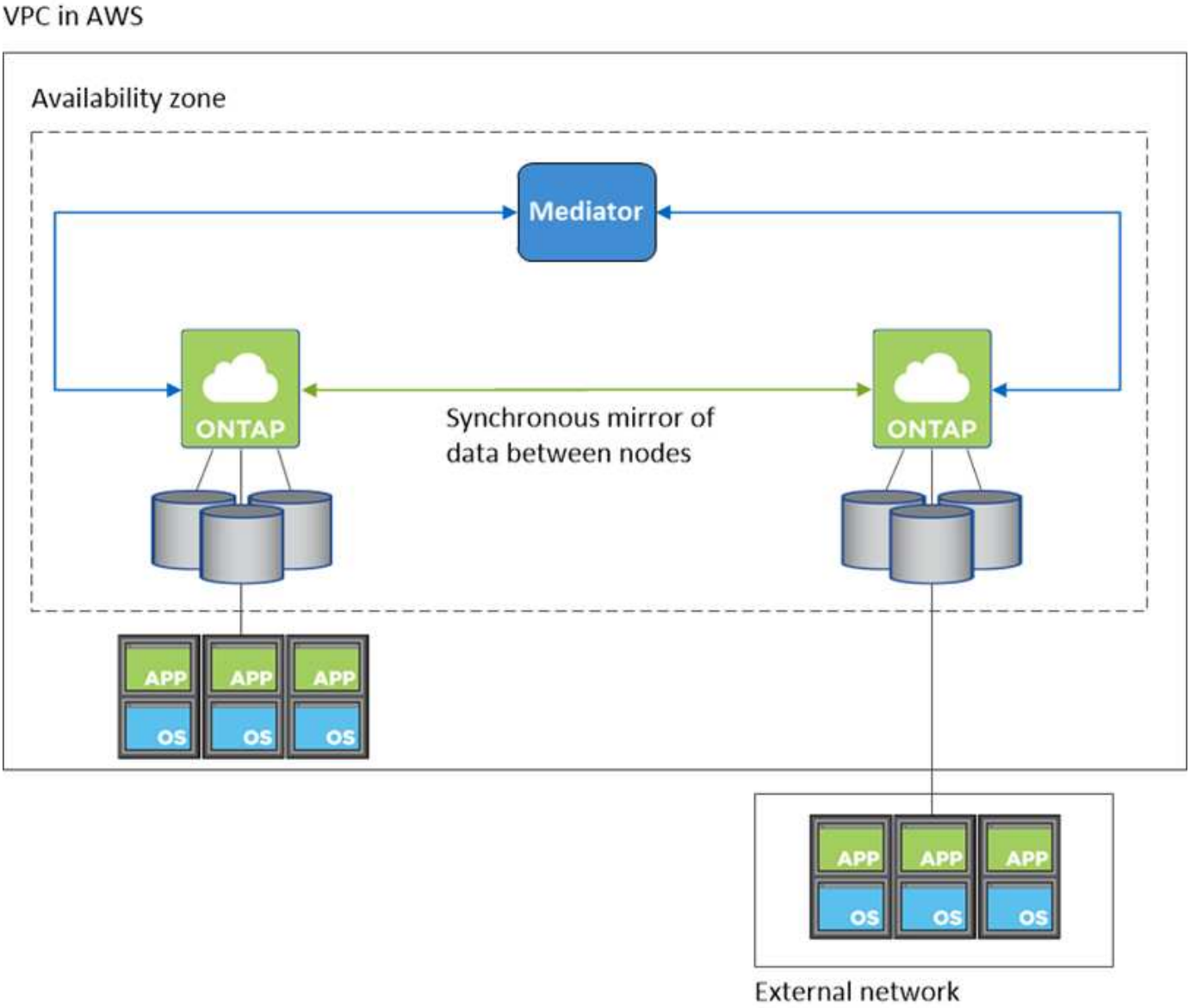
Durch die Implementierung einer HA-Konfiguration in einer einzelnen Verfügbarkeitszone (AZ) kann eine hohe Verfügbarkeit Ihrer Daten sichergestellt werden, wenn eine Instanz, auf der ein Cloud Volumes ONTAP Node ausgeführt wird, ausfällt. Alle Daten sind nativ von außerhalb des VPC zugänglich.

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.

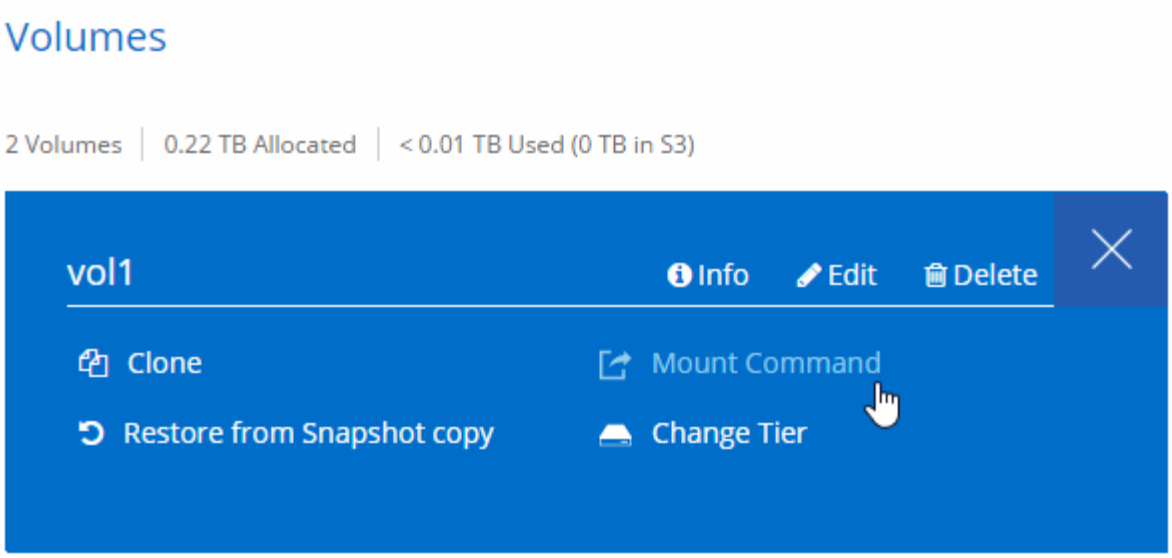
Weitere Informationen zur Performance von Cloud Volumes ONTAP finden Sie unter "Leistung".

Client-Zugriff auf Storage

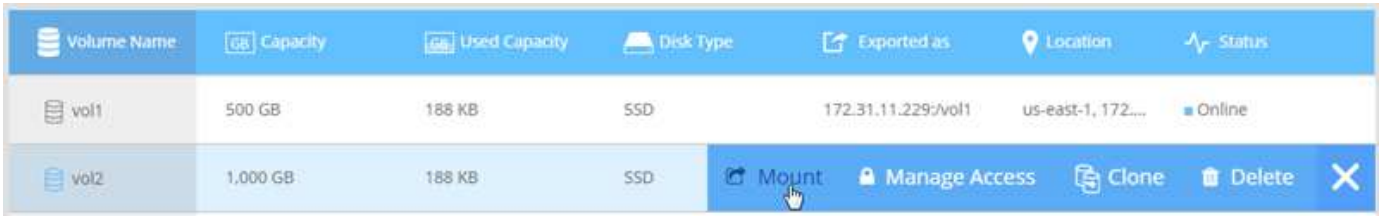
Clients sollten über die Daten-IP-Adresse des Node, auf dem sich das Volume befindet, auf NFS- und CIFS-Volumes zugreifen. Wenn NAS-Clients über die IP-Adresse des Partner-Node auf ein Volume zugreifen, wird der Datenverkehr zwischen beiden Nodes geleitet, wodurch die Performance verringert wird.

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.

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



Die folgende Abbildung zeigt die Volume-Ansicht:

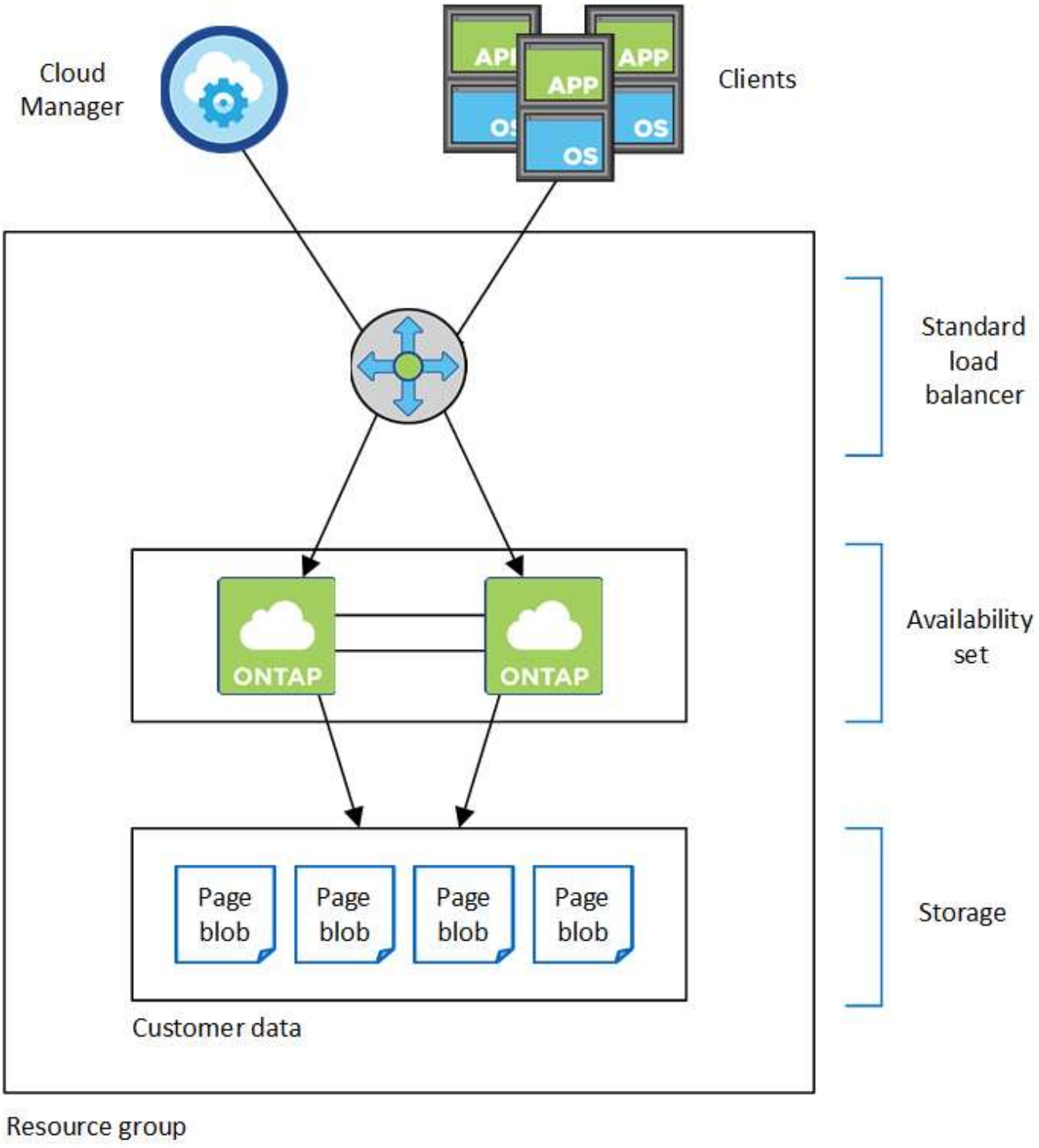


Hochverfügbarkeitspaare in Azure

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

HA-Komponenten

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



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

Azure Standard Load Balancer

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

Verfügbarkeitsgruppe

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

Storage

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

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

RPO und RTO

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

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

Storage-Übernahme und -Giveback

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

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

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

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

Storage-Konfigurationen

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

HA-Einschränkungen

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

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

  "Siehe die Liste der unterstützten Azure Regionen".

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

Bewertung

Vor der Zahlung für die Software können Sie Cloud Volumes ONTAP auswerten.

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

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

Lizenzierung

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

Lizenzmanagement für ein neues System

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

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

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

Ablauf der Lizenz

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

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

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

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

Lizenzerneuerung

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

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

Sicherheit

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

Verschlüsselung von Daten im Ruhezustand

Cloud Volumes ONTAP unterstützt die folgenden Verschlüsselungstechnologien:

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

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

NetApp Volume Encryption

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

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

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

AWS Key Management Service

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

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

Azure Storage Service Encryption

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

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

ONTAP 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".

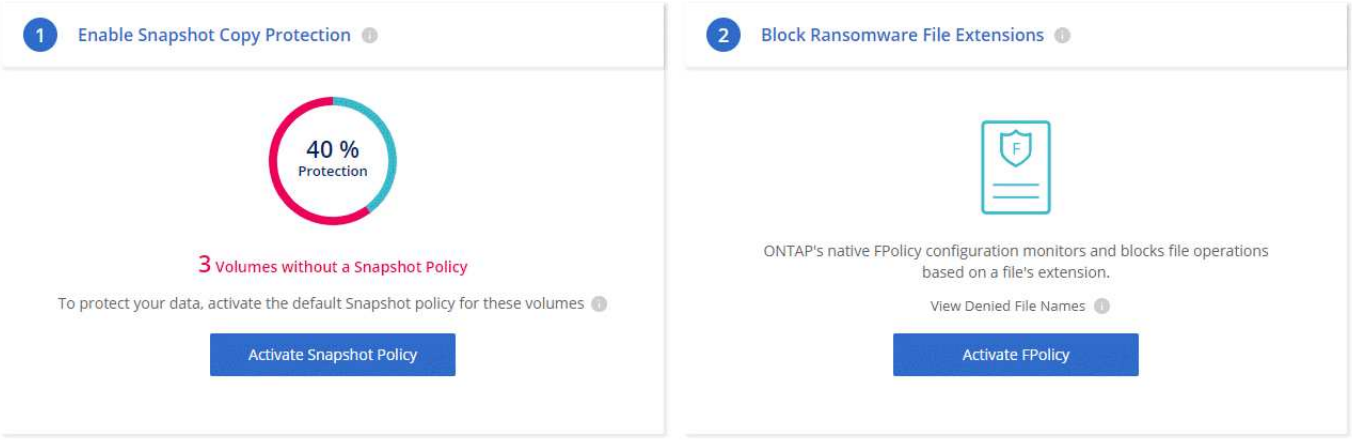
Schutz durch Ransomware

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".

Erste Schritte

Implementierungsübersicht

Bevor Sie beginnen, sollten Sie sich vielleicht besser mit Ihren Optionen für die Implementierung von OnCommand Cloud Manager und Cloud Volumes ONTAP vertraut machen.

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
- IBM Cloud
- In Ihrem eigenen Netzwerk

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

Standort	So implementieren Sie Cloud Manager
AWS	"Cloud Manager über NetApp Cloud Central implementieren"
AWS C2S	"Implementieren Sie Cloud Manager über den AWS Intelligence Community Marketplace"
Azure allgemein verfügbare Region	"Cloud Manager über NetApp Cloud Central implementieren"
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"
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.

- "Cloud Provider Accounts zu Cloud Manager hinzufügen"
- "Installieren eines HTTPS-Zertifikats"
- "Benutzer und Mandanten einrichten"
- "Einrichten des AWS KMS"

Implementierung von Cloud Volumes ONTAP

Nachdem Sie Cloud Manager in Betrieb genommen haben, können Sie mit der Implementierung von Cloud Volumes ONTAP in AWS und Microsoft Azure beginnen.

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

- "Unterstützte Konfigurationen für Cloud Volumes ONTAP 9.5"
- "Planung Ihrer Konfiguration"
- "Starten von Cloud Volumes ONTAP in AWS"
- "Starten von Cloud Volumes ONTAP in Azure"

Erste Schritte mit Cloud Volumes ONTAP in AWS

Die ersten Schritte mit Cloud Volumes ONTAP in AWS sind über NetApp Cloud Central möglich.

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 ausgehenden 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.

Abonnieren Sie Cloud Volumes ONTAP über den AWS Marketplace

Abonnieren von "AWS Marketplace" Ist zur Annahme der Softwarebedingungen erforderlich. Sie sollten sich nur über Marketplace anmelden. Starten von Cloud Volumes ONTAP von überall aus, Cloud Manager wird jedoch nicht unterstützt.

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.

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.

Weiterführende Links

- "Bewertung"
- "Netzwerkanforderungen für Cloud Manager"
- "Netzwerkanforderungen für Cloud Volumes ONTAP in AWS"
- "Sicherheitsgruppenregeln für AWS"
- "Cloud Provider Accounts zu Cloud Manager hinzufügen"
- "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

Erste Schritte mit Cloud Volumes ONTAP in Azure sind über NetApp Cloud Central möglich. 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"
- "Cloud Provider Accounts zu Cloud Manager hinzufügen"
- "Was Cloud Manager mit Azure-Berechtigungen tut"
- "Starten von Cloud Volumes ONTAP in Azure"
- "Cloud Manager über den Azure Marketplace starten"

Einrichten von Cloud Manager

Cloud-Provider-Konten zu Cloud Manager hinzufügen

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

Bei der Implementierung von Cloud Manager über Cloud Central fügt Cloud Manager automatisch einen hinzu "Konto eines Cloud-Providers" Für das Konto, in dem Sie Cloud Manager implementiert haben. Ein anfängliches Cloud-Provider-Konto wird nicht hinzugefügt, wenn Sie die Cloud Manager Software manuell auf einem vorhandenen System installieren.

Einrichten und Hinzufügen von AWS Konten zu Cloud Manager

Wenn Sie Cloud Volumes ONTAP in verschiedenen AWS Konten implementieren möchten, müssen Sie diese Konten die erforderlichen Berechtigungen erteilen und anschließend 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.

- Gewähren von Berechtigungen bei der Bereitstellung von AWS Schlüsseln
- Gewährung von Berechtigungen durch Annahme von IAM-Rollen in anderen Konten

Gewähren von Berechtigungen bei der 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

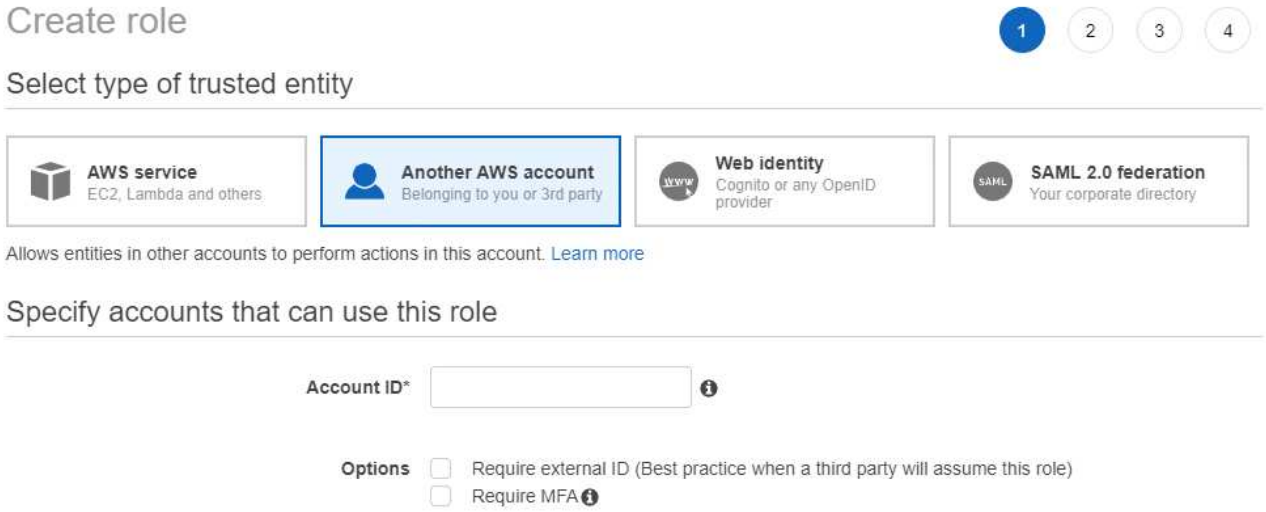
Sie können eine Vertrauensbeziehung zwischen dem Quell-AWS-Konto einrichten, in dem Sie die Cloud Manager-Instanz und anderen AWS-Konten mithilfe von IAM-Rollen bereitgestellt haben. Dann würden Sie Cloud Manager über die vertrauenswürdigen Konten mit dem ARN der IAM-Rollen versorgen.

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.

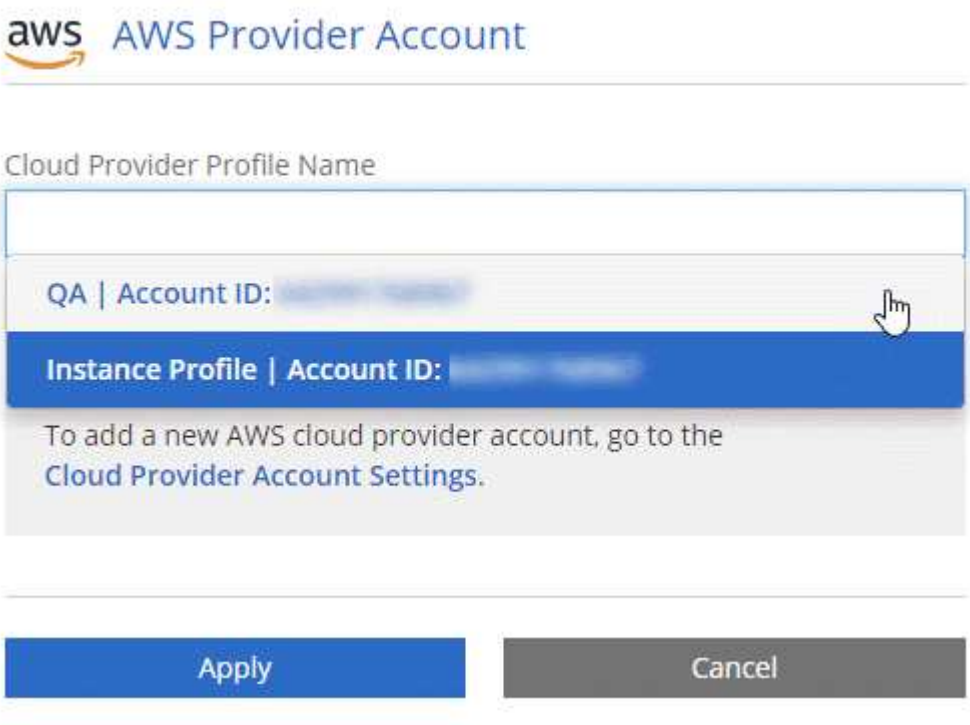
Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf die Dropdown-Liste Task und wählen Sie dann **Kontoeinstellungen** 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.

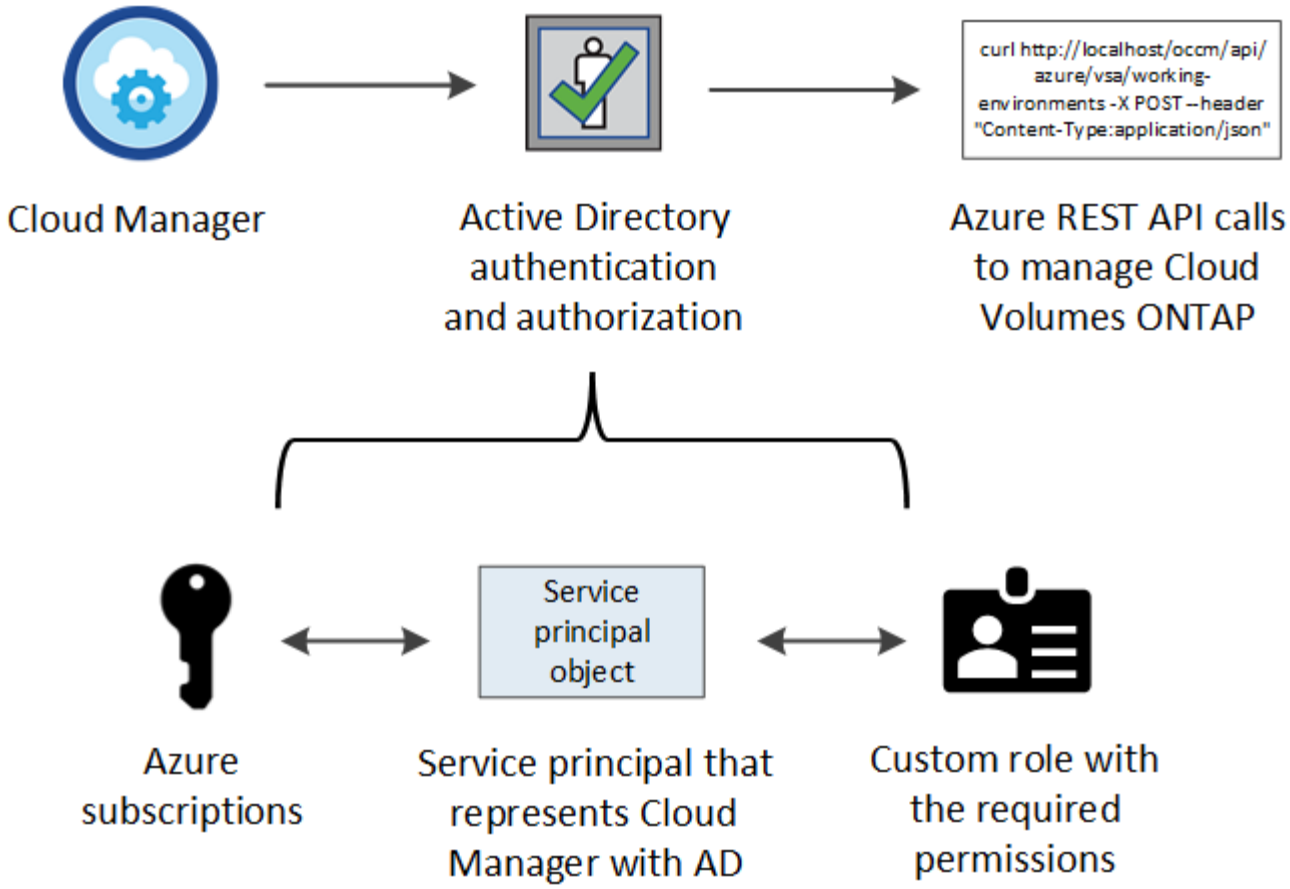
- Azure-Berechtigungen über einen Service-Principal gewähren
- Hinzufügen von Azure-Konten zu Cloud Manager

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.



Die folgenden Schritte verwenden das neue Azure Portal. Wenn Probleme auftreten, sollten Sie das klassische Azure Portal verwenden.

Schritte

1. Erstellen einer benutzerdefinierten Rolle mit den erforderlichen Cloud Manager-Berechtigungen.
2. Erstellen eines Active Directory-Dienstprinzipals.
3. Weisen Sie der Service-Principal die benutzerdefinierte Cloud Manager-Rolle zu.

Erstellen einer benutzerdefinierten Rolle mit den erforderlichen Cloud Manager-Berechtigungen

Eine benutzerdefinierte Rolle ist erforderlich, um Cloud Manager die Berechtigungen zu geben, die er zum Starten und Managen von Cloud Volumes ONTAP in Azure benötigt.

Schritte

1. Laden Sie die herunter "Cloud Manager Azure-Richtlinie".
2. 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"
```

3. 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_3.6.1.json

Ergebnis

Sie sollten nun eine benutzerdefinierte Rolle namens OnCommand Cloud Manager Operator haben.

Erstellen eines Active Directory-Dienstprinzipals

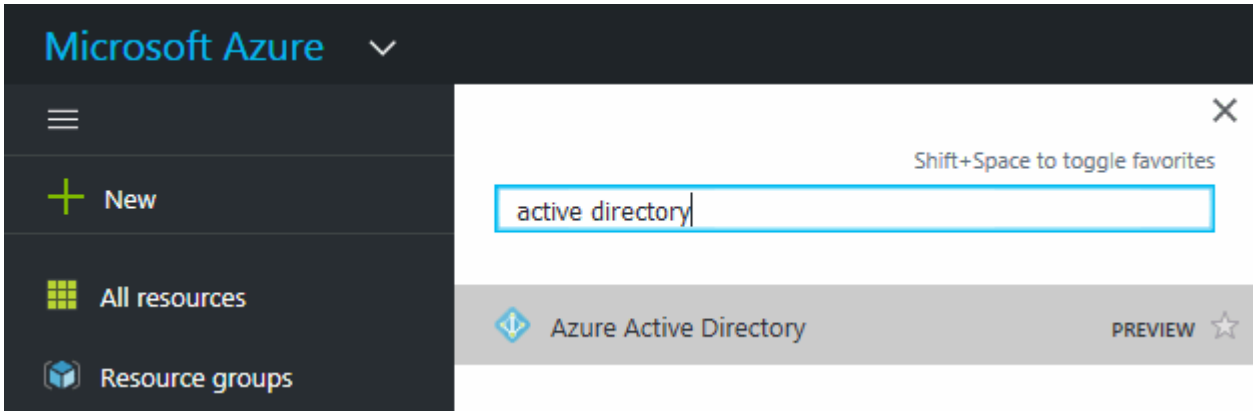
Sie müssen einen Active Directory-Dienstprinzipal erstellen, damit Cloud Manager sich mit Azure Active Directory authentifizieren kann.

Bevor Sie beginnen

Sie müssen über die entsprechenden 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: Erstellen Sie mithilfe eines Portals eine Active Directory-Applikation und einen Service-Principal, die auf Ressourcen zugreifen können".

Schritte

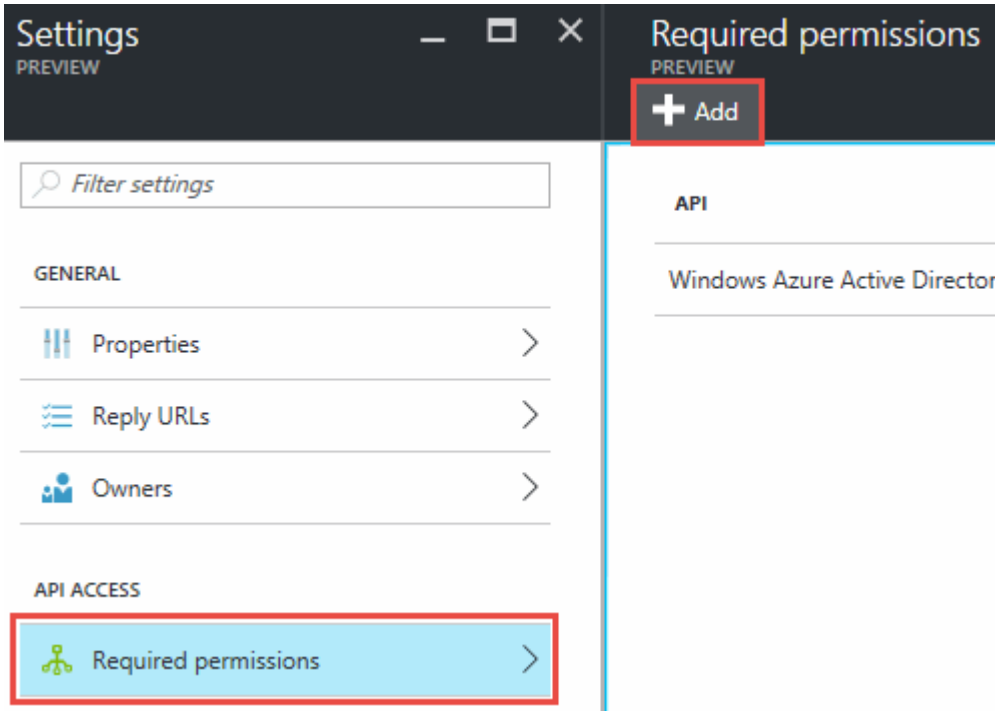
1. Öffnen Sie über das Azure-Portal den **Azure Active Directory**-Service.



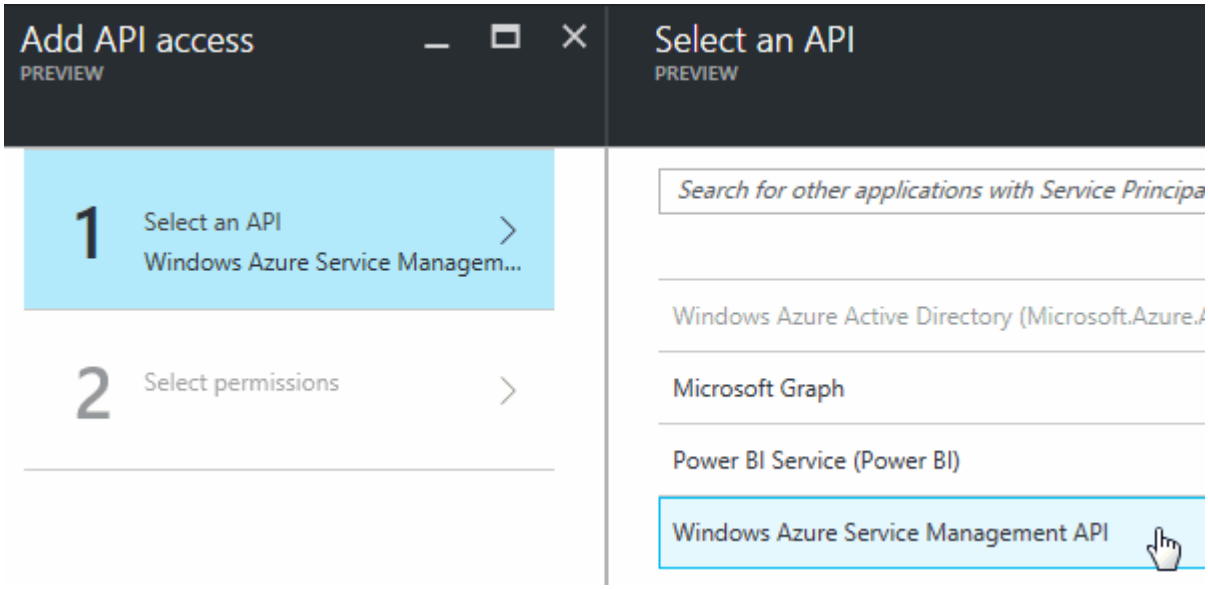
2. Klicken Sie im Menü auf **App-Registrierungen (Legacy)**.
3. Erstellen Sie den Service-Prinzipal:
   a. Klicken Sie auf **Registrierung neuer Anwendungen**.
   b. Geben Sie einen Namen für die Anwendung ein, lassen Sie **Web App / API** ausgewählt, und geben Sie dann eine beliebige URL ein, z. B. http://url
   c. Klicken Sie Auf **Erstellen**.
4. Ändern Sie die Anwendung, um die erforderlichen Berechtigungen hinzuzufügen:

a. Wählen Sie die erstellte Anwendung aus.

b. Klicken Sie unter Einstellungen auf **erforderliche Berechtigungen** und dann auf **Hinzufügen**.



c. Klicken Sie auf **Wählen Sie eine API**, wählen Sie **Windows Azure Service Management API** und klicken Sie dann auf **Auswählen**.



d. Klicken Sie auf **Zugriff auf Azure Service Management als Organisationsbenutzer**, klicken Sie auf **Auswählen** und dann auf **Fertig**.

5. Erstellen Sie einen Schlüssel für den Service Principal:

a. Klicken Sie unter Einstellungen auf **Schlüssel**.

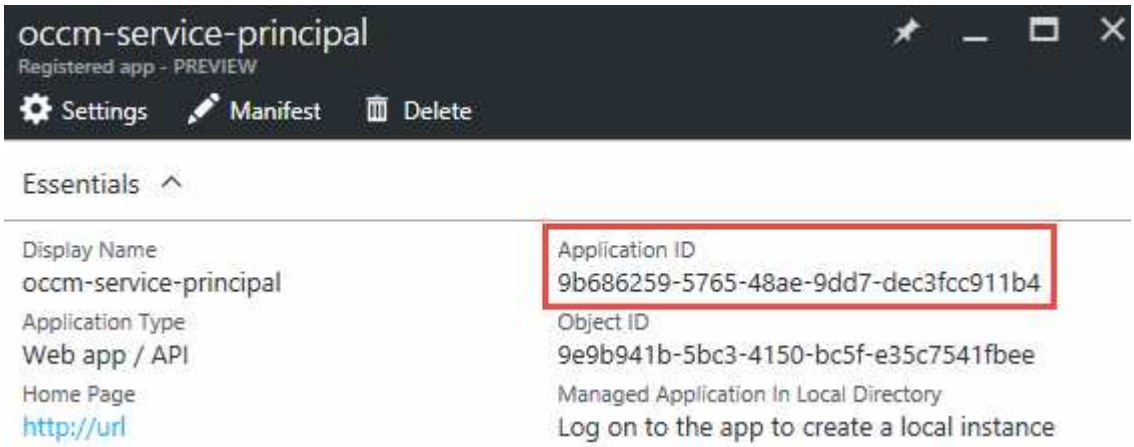
b. Geben Sie eine Beschreibung ein, wählen Sie eine Dauer aus und klicken Sie dann auf **Speichern**.

c. Kopieren Sie den Schlüsselwert.

Wenn Sie Cloud Manager einem Cloud-Provider-Konto hinzufügen, müssen Sie den Hauptwert eingeben.

d. Klicken Sie auf **Eigenschaften** und kopieren Sie dann die Anwendungs-ID für den Service-Principal.

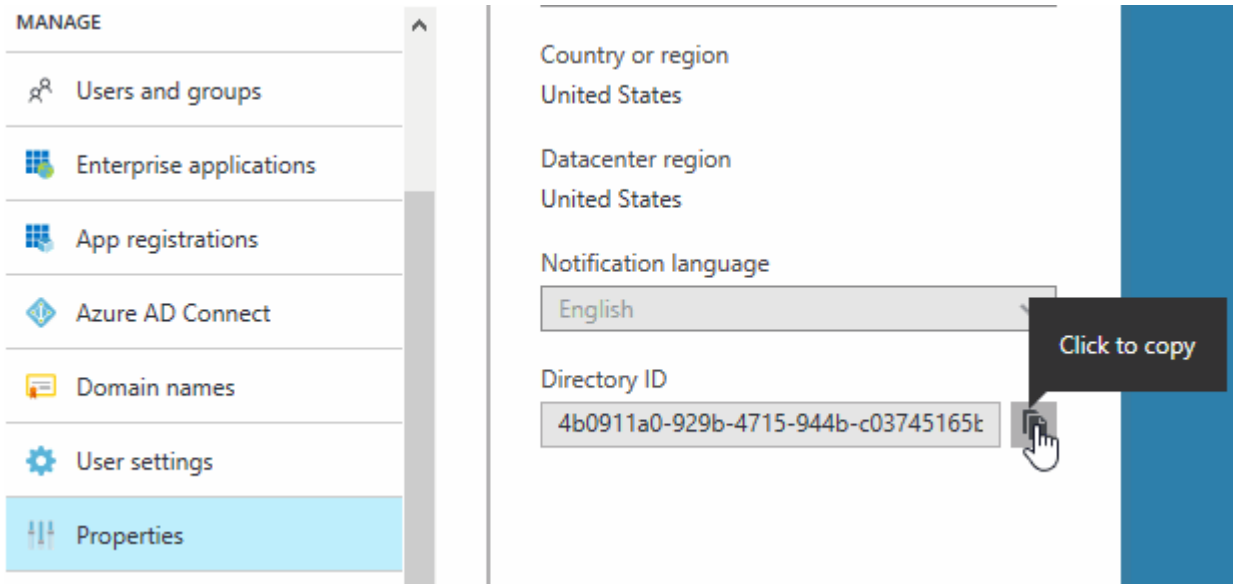
Ähnlich dem Schlüsselwert müssen Sie bei Cloud Manager ein Cloud-Provider-Konto hinzufügen, indem Sie die Anwendungs-ID in Cloud Manager eingeben.



6. Ermitteln Sie die Active Directory-Mandanten-ID für Ihr Unternehmen:

a. Klicken Sie im Menü Active Directory auf **Eigenschaften**.

b. Kopieren Sie die Verzeichnis-ID.



Genau wie die Anwendungs-ID und der Anwendungsschlüssel müssen Sie die Active Directory-Mandanten-ID eingeben, wenn Sie Cloud Manager ein Cloud-Provider-Konto hinzufügen.

Ergebnis

Sie sollten nun über einen Active Directory-Dienstprinzipal verfügen und die Anwendungs-ID, den Anwendungsschlüssel und die Active Directory-Mandanten-ID kopiert haben. Sie müssen diese Informationen in Cloud Manager eingeben, wenn Sie ein Cloud-Provider-Konto hinzufügen.

Zuweisen der Rolle "Cloud Manager Operator" zum Serviceprinzipal

Sie müssen den Dienstprinzipal an ein oder mehrere Azure Subscriptions binden und ihm die Rolle "Cloud Manager Operator" zuweisen, damit Cloud Manager über Berechtigungen in Azure verfügt.

Über diese Aufgabe

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.

Schritte

1. Wählen Sie im Azure-Portal im linken Bereich die Option **Abonnements** aus.
2. Wählen Sie das Abonnement aus.
3. Klicken Sie auf **Access Control (IAM)** und dann auf **Add**.
4. Wählen Sie die Rolle **OnCommand Cloud Manager Operator** aus.
5. Suchen Sie nach dem Namen der Anwendung (Sie können die Anwendung nicht in der Liste finden, indem Sie blättern).
6. Wählen Sie die Anwendung aus, klicken Sie auf **Auswählen** und dann auf **OK**.

Ergebnis

Der Dienstprinzipal für Cloud Manager verfügt jetzt über die erforderlichen Azure Berechtigungen.

Hinzufügen von Azure-Konten zu Cloud Manager

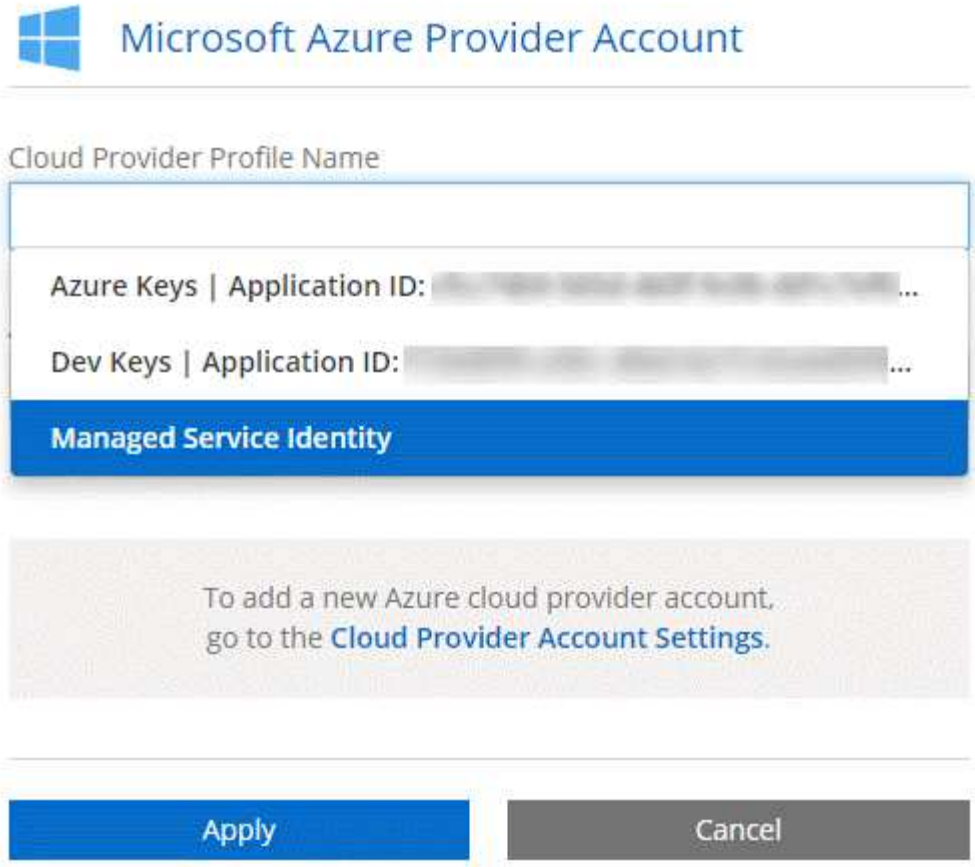
Nachdem Sie ein Azure Konto mit den erforderlichen Berechtigungen angegeben haben, können Sie das Konto zu Cloud Manager hinzufügen. Damit können Sie Cloud Volumes ONTAP Systeme in diesem Konto starten.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf die Dropdown-Liste Task und wählen Sie dann **Kontoeinstellungen** 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.
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 die erste "Konto eines Cloud-Providers" 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.

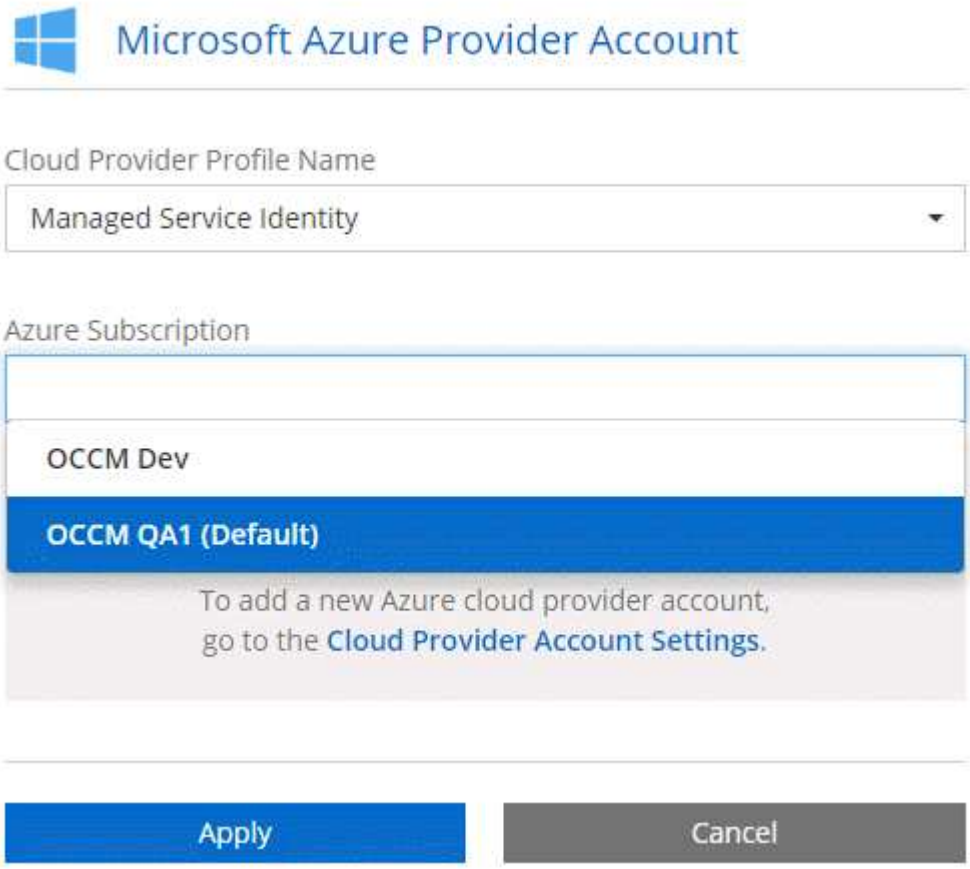
      OnCommand Cloud Manager Operator ist der im angegebene Standardname "Cloud Manager-Richtlinie". Wenn Sie einen anderen Namen für die Rolle ausgewählt haben, wählen Sie stattdessen diesen Namen aus.

- 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.



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 die Dropdown-Liste Task und wählen Sie dann **Kontoeinstellungen** 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.

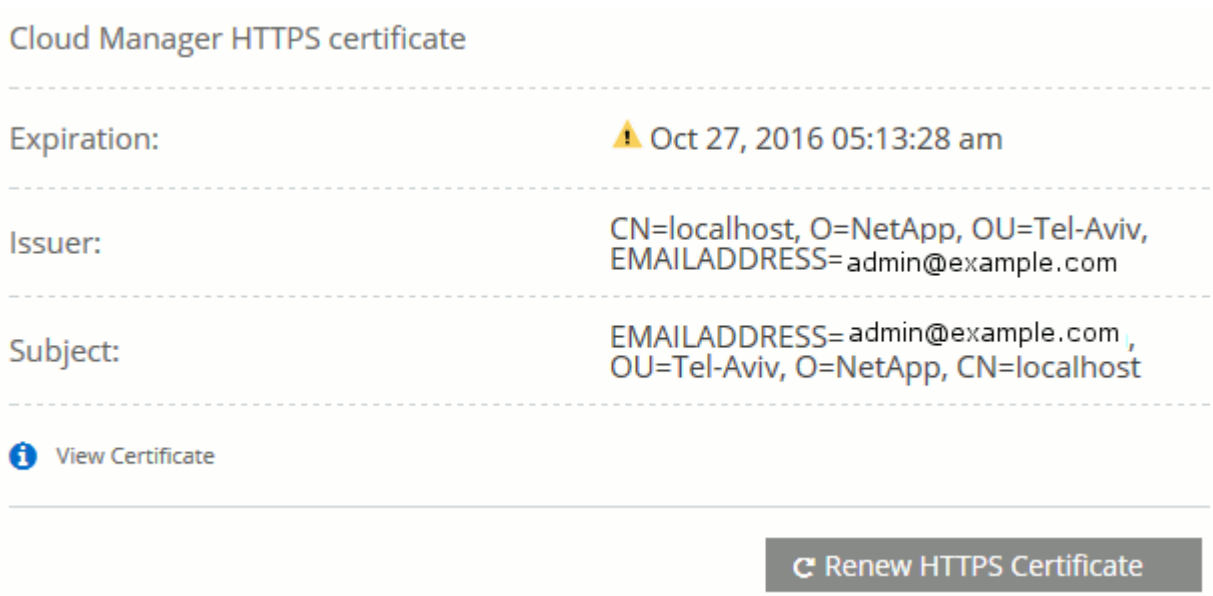
Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf die Dropdown-Liste Task, und wählen Sie dann **HTTPS-Setup** aus.
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:



Benutzer und Mandanten einrichten

Mit Cloud Manager können Sie Cloud Manager um weitere Cloud Central Benutzer erweitern und Arbeitsumgebungen durch die Verwendung von Mandanten isolieren.

Hinzufügen von Benutzern zu Cloud Manager

Wenn zusätzliche Benutzer Ihr Cloud Manager-System verwenden müssen, müssen sie sich bei NetApp Cloud Central registrieren. Sie können die Benutzer dann zu Cloud Manager hinzufügen.

Schritte

1. Wenn der Benutzer noch kein Konto in NetApp Cloud Central hat, senden Sie ihm einen Link zu Ihrem Cloud Manager-System, und lassen Sie ihn sich registrieren.

   Warten Sie, bis der Benutzer bestätigt, dass er sich für ein Konto angemeldet hat.

2. Klicken Sie in Cloud Manager auf das Benutzersymbol und dann auf **Benutzer anzeigen**.
3. Klicken Sie Auf **Neuer Benutzer**.
4. Geben Sie die dem Benutzerkonto zugeordnete E-Mail-Adresse ein, wählen Sie eine Rolle aus und klicken Sie auf **Hinzufügen**.

Was kommt als Nächstes?

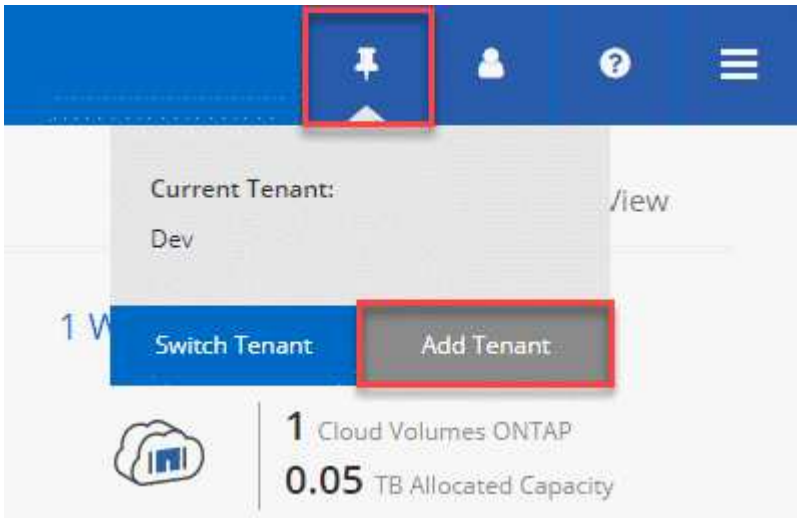
Informieren Sie den Benutzer, dass er sich jetzt beim Cloud Manager-System anmelden kann.

Erstellen von Mandanten

Mit Mandanten lassen sich Arbeitsumgebungen in separate Gruppen isolieren. Sie erstellen eine oder mehrere Arbeitsumgebungen innerhalb eines Mandanten. "Erfahren Sie mehr über Mandanten".

Schritte

1. Klicken Sie auf das Mietersymbol und dann auf **Mieter hinzufügen**.



2. Geben Sie ggf. einen Namen, eine Beschreibung und eine Kostenstelle ein.
3. Klicken Sie Auf **Speichern**.

Was kommt als Nächstes?

Sie können jetzt zu diesem neuen Mandanten wechseln und diesem Mandanten Mandantenadministratoren und Arbeitsumgebungsadministratoren hinzufügen.

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.

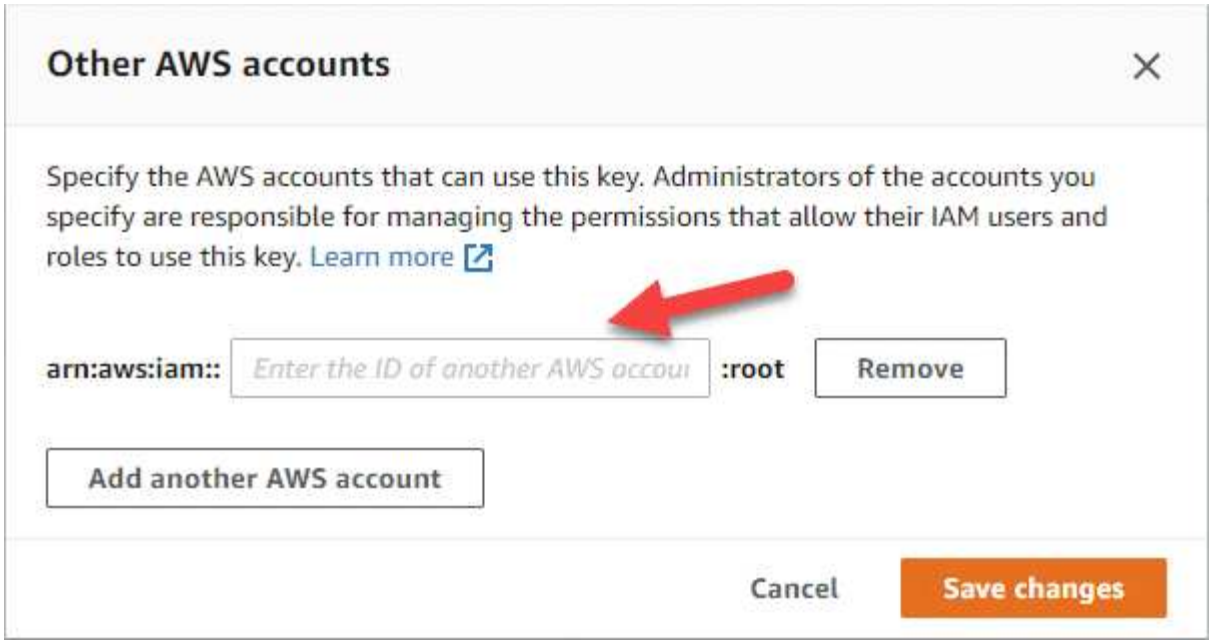
   b. Wählen Sie die Taste.

   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

Sie müssen Ihr Netzwerk so einrichten, dass Cloud Manager Cloud Volumes ONTAP Systeme in AWS oder in Microsoft Azure bereitstellen 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 erfordert eine Netzwerkverbindung zu den AWS VPCs und Azure VNets, in denen Sie Cloud Volumes ONTAP bereitstellen möchten.

Wenn Sie beispielsweise Cloud Manager in Ihrem Unternehmensnetzwerk installieren, müssen Sie eine VPN-Verbindung zum AWS VPC oder Azure VNet einrichten, in dem Sie Cloud Volumes ONTAP starten.

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.

Outbound-Internetzugang zum 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.
https://api.services.cloud.netapp.com:443	API-Anfragen an NetApp Cloud Central.

Endpunkte	Zweck
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://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 zur Lizenzierung und Support-Registrierung
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.

Outbound-Internetzugang 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.

Endpunkte	Zweck
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://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 zur Lizenzierung und Support-Registrierung
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.

Outbound-Internetzugang über Ihren Webbrowser

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.

Outbound-Internetzugang zur Installation 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"
- 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.

Suchen Sie nach der Liste der Endpunkte, auf die Cloud Manager Zugriff benötigt? Sie werden jetzt an einem einzigen Ort gepflegt. "Details finden Sie hier".

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)".

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".

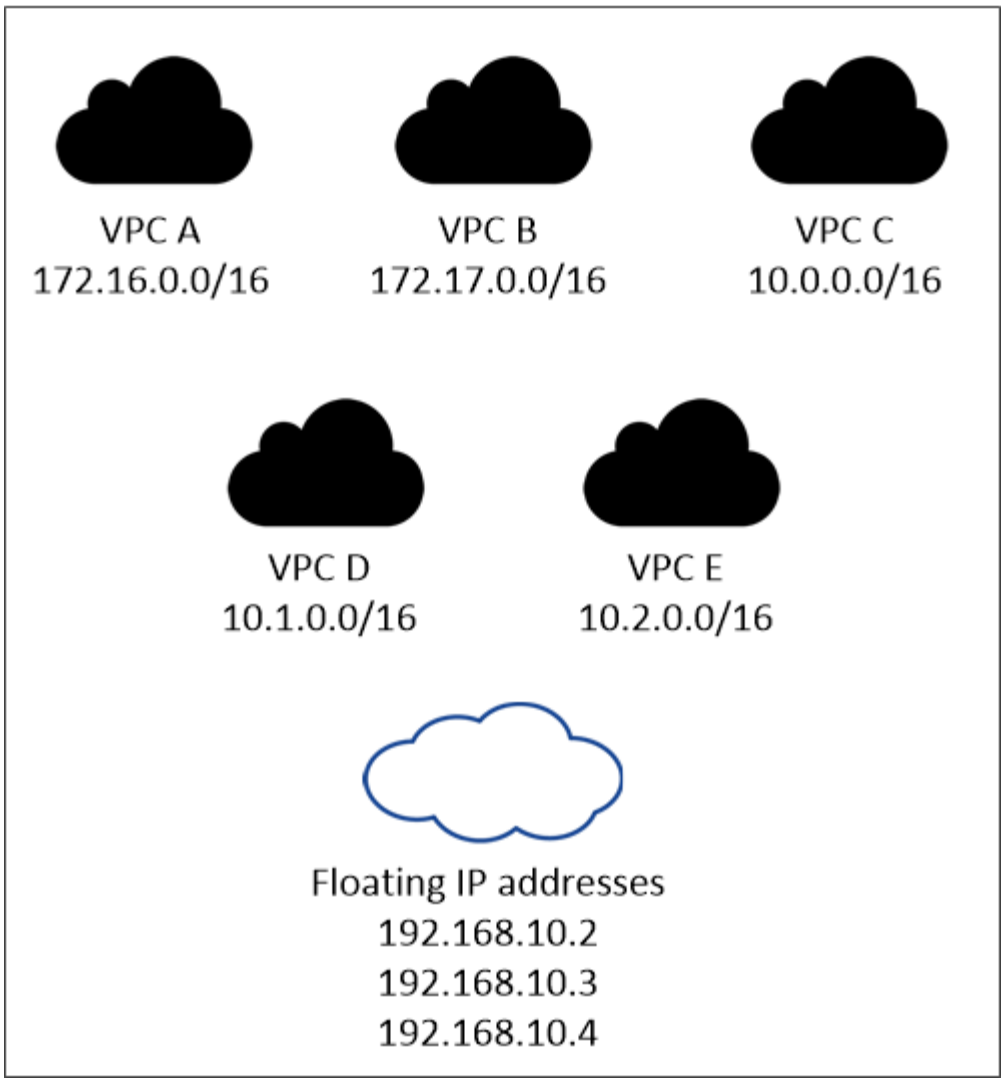
Eine Floating-IP-Adresse ist für das Cluster-Management, eine für NFS/CIFS-Daten auf Node 1 und eine für NFS/CIFS-Daten auf Node 2. Eine vierte Floating IP-Adresse für SVM-Management ist optional.

> 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".

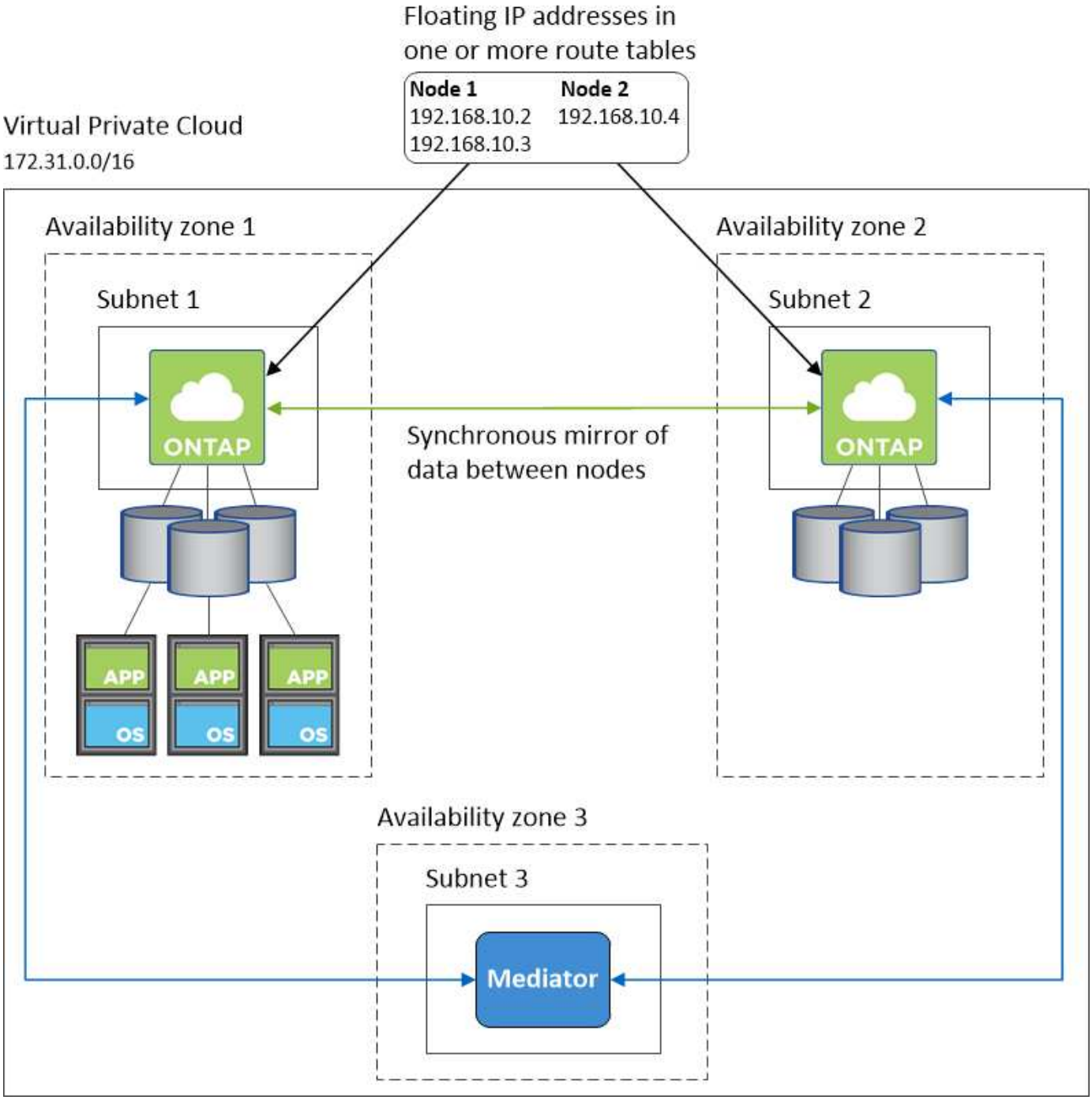
Anbindung an NetApp Management Tools

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

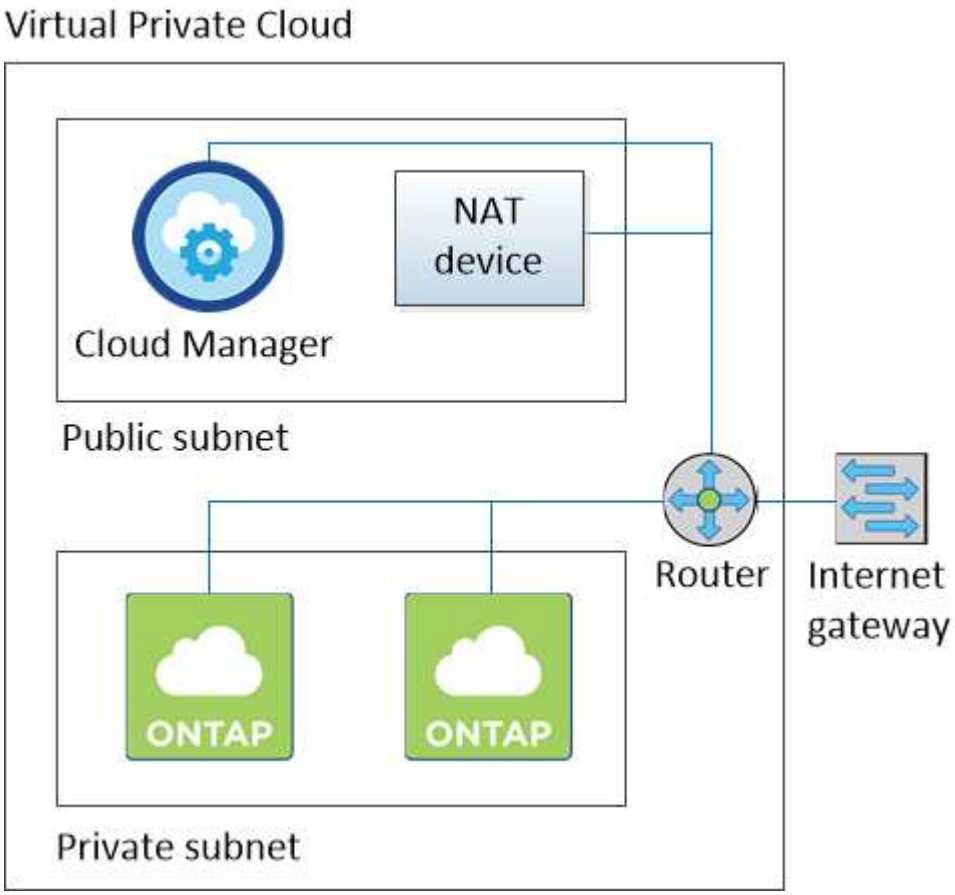
Diese VPC-Konfiguration umfasst öffentliche und private Subnetze, ein Internet-Gateway, das den VPC mit dem Internet verbindet, und ein NAT-Gateway oder eine NAT-Instanz im öffentlichen Subnetz, die

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.

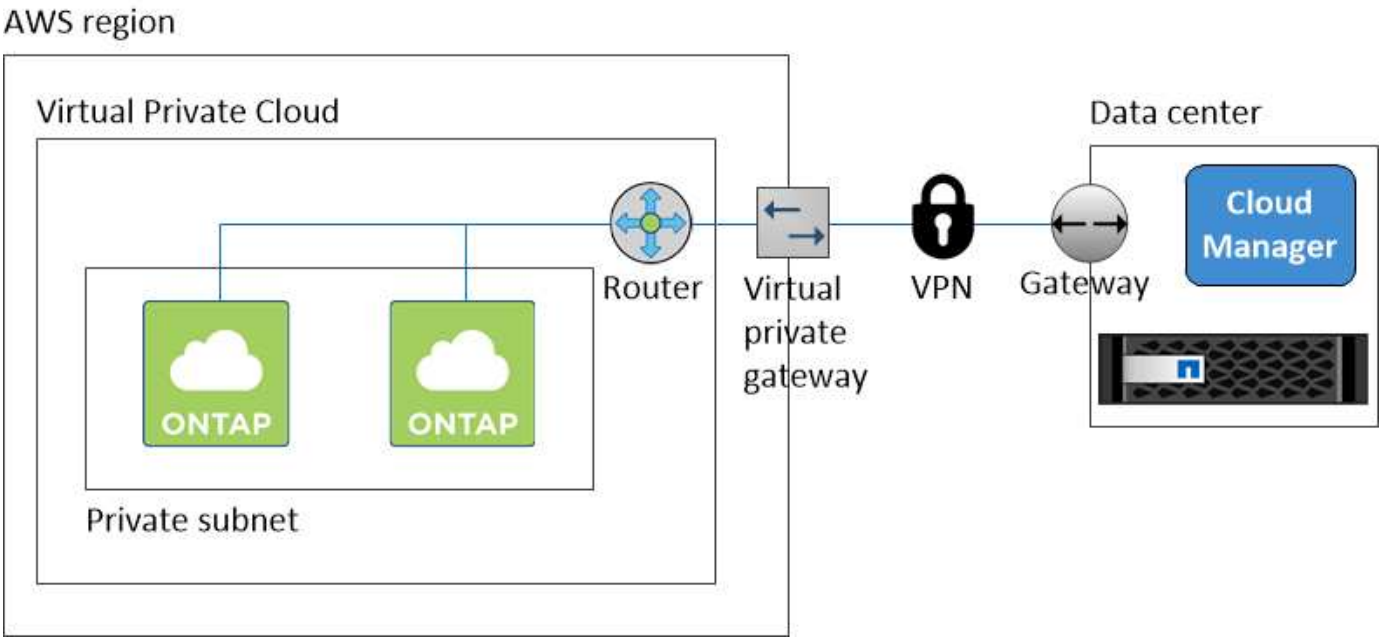
Sie können in dieser Konfiguration auch einen Proxyserver verwenden, um den Internetzugang zu ermöglichen. Der Proxy-Server kann sich in Ihrem Datacenter oder in AWS befinden.

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

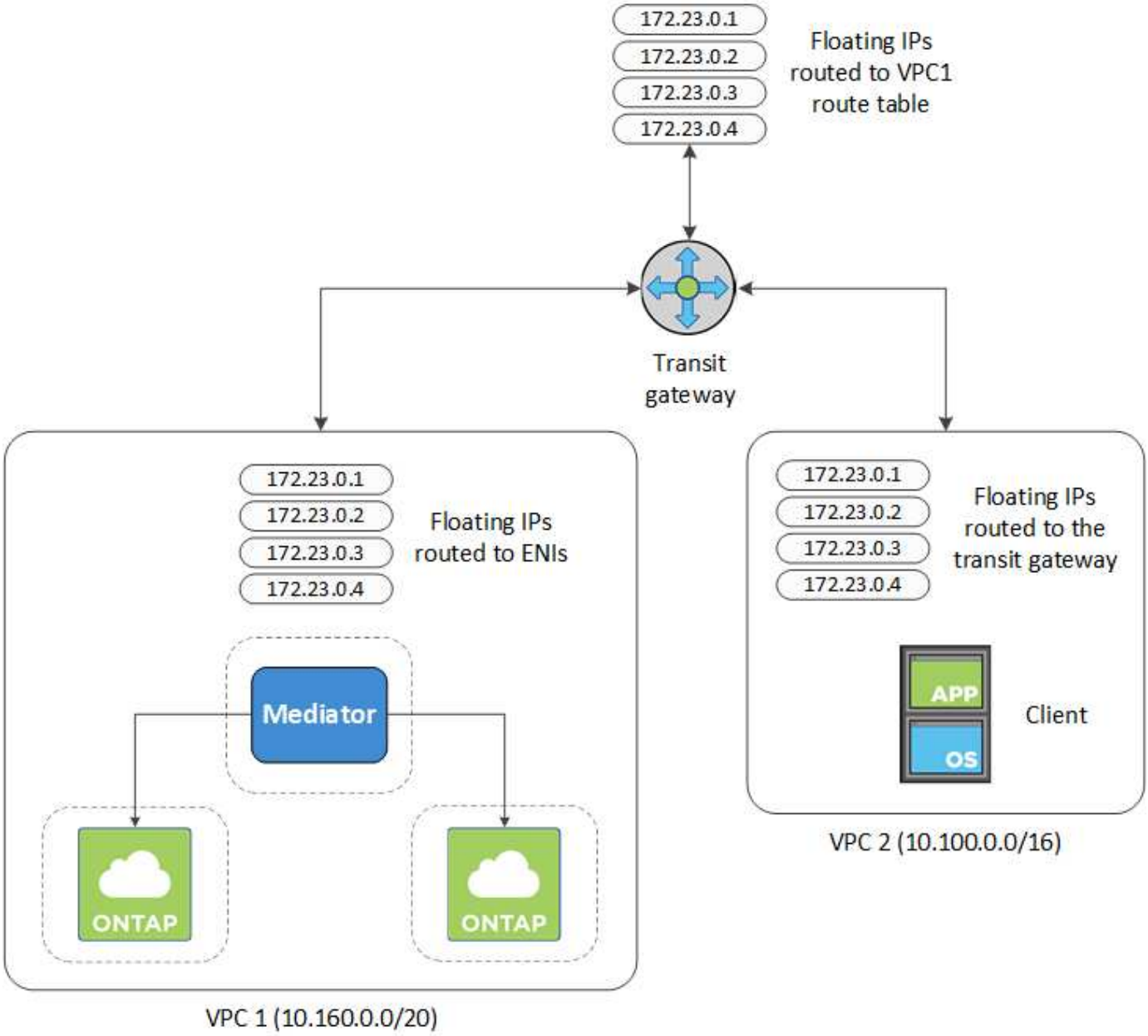
Einrichten eines AWS-Transit-Gateways für den Zugriff auf die unverankerten IP-Adressen eines HA-Paars von außerhalb der VPC aus, wo sich das HA-Paar befindet.

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.

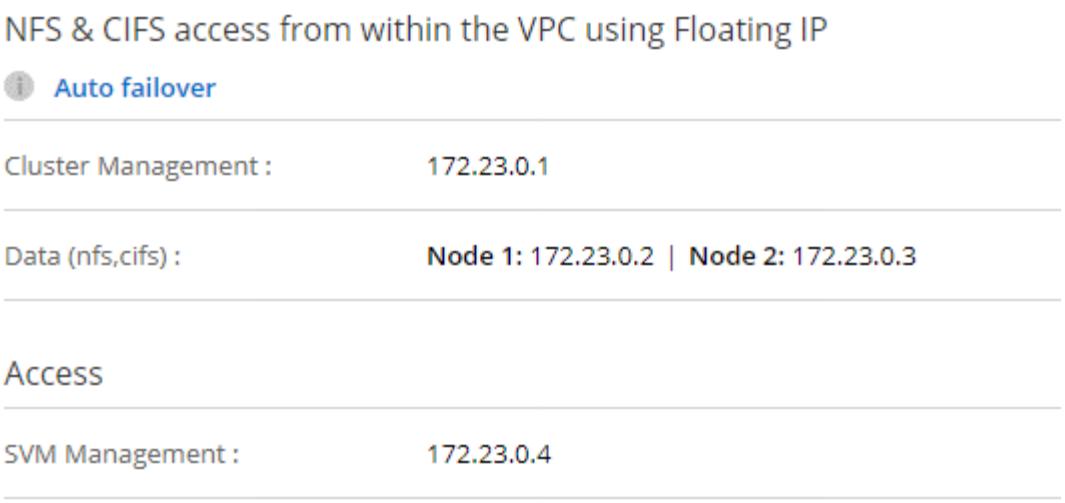


Die folgenden Schritte veranschaulichen die Einrichtung einer ähnlichen Konfiguration.

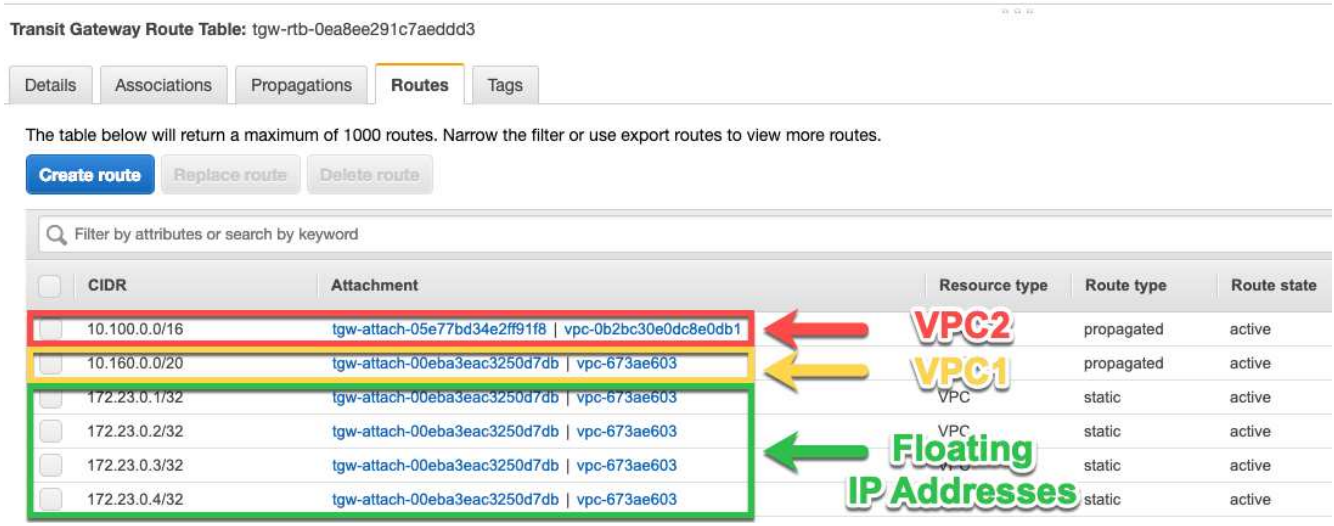
Schritte

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.

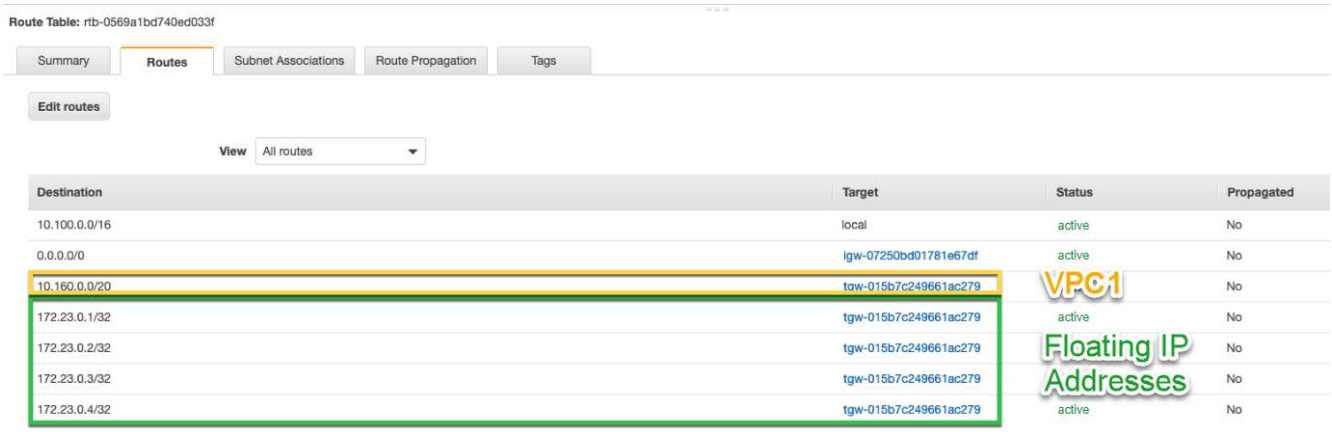


3. Ändern Sie die Routingtabelle von VPCs, die auf die fließenden IP-Adressen zugreifen müssen.

   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.

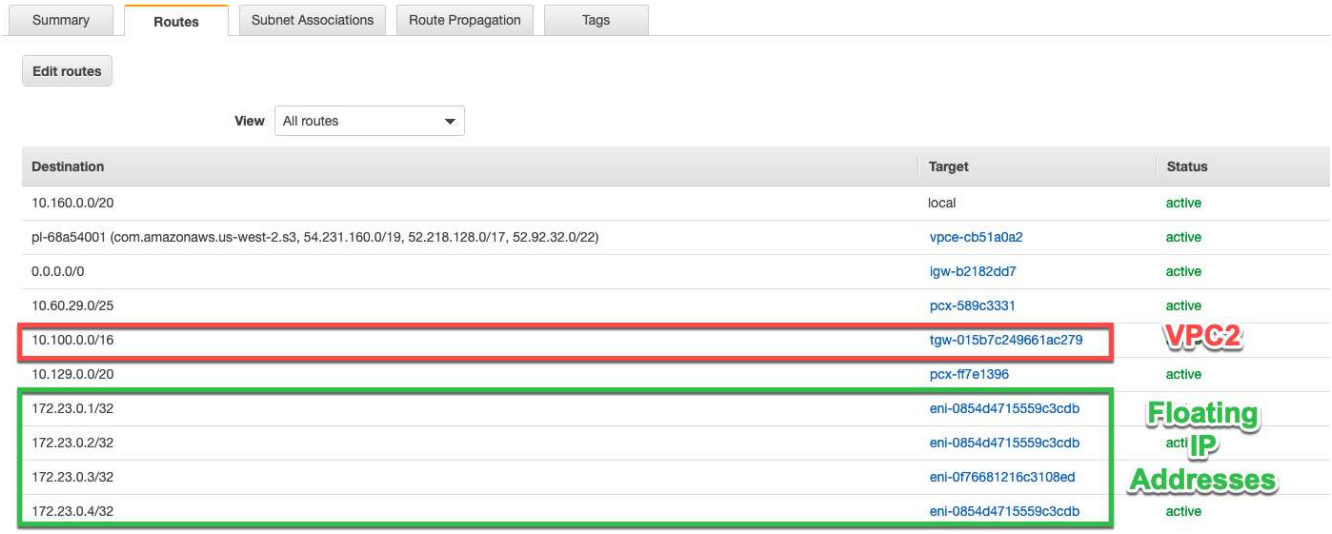
      Das folgende Beispielbild zeigt die Routingtabelle für VPC 2, die auch Routen zu VPC 1 und die fließenden IP-Adressen umfasst.



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.

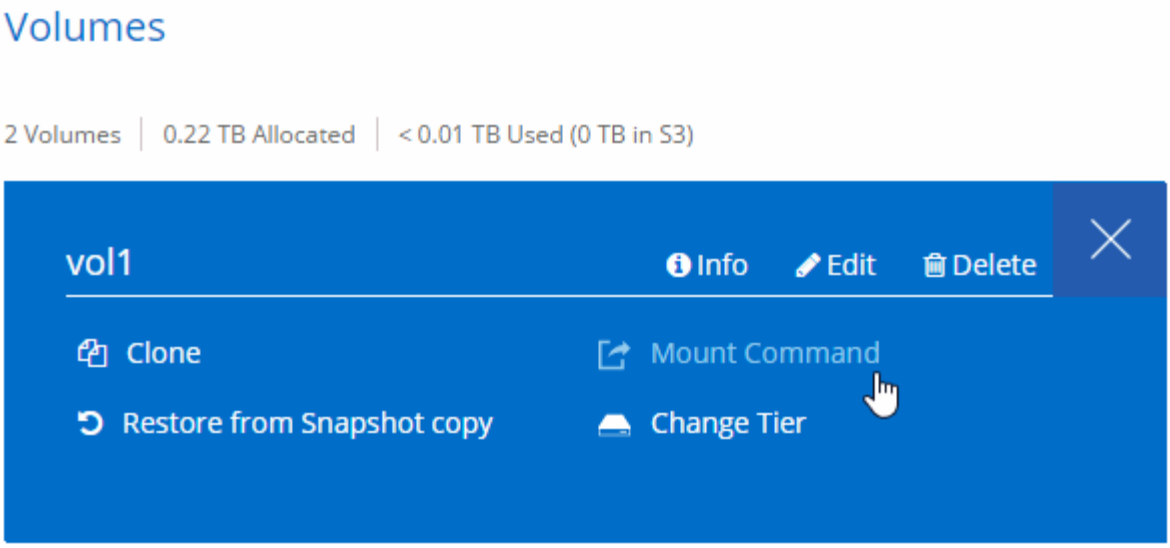
   Dieser Schritt ist wichtig, da er die Weiterleitung zwischen den VPCs abgeschlossen hat.

   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

Sie müssen Ihr Azure Networking so einrichten, dass Cloud Volumes ONTAP Systeme ordnungsgemäß funktionieren.

Suchen Sie nach der Liste der Endpunkte, auf die Cloud Manager Zugriff benötigt? Sie werden jetzt an einem einzigen Ort gepflegt. "Details finden Sie hier".

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 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

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 Azure Blob Storage für Data Tiering

Wenn Sie „kalte“ Daten für Azure Blob Storage Tiering möchten, müssen Sie keinen vnet Service-Endpunkt einrichten, wenn Cloud Manager über die erforderlichen 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".

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.

Unterstützte AWS EC2-Instanztypen

t3.Medium (empfohlen), t2.Medium und m4.Large

Unterstützte Azure VM-Größen

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

Unterstützte Betriebssysteme

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

  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.

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 für AWS"
   - "Netzwerkanforderungen für Cloud Volumes ONTAP für Azure"
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-V3.6.3.sh
   . Führen Sie das Installationsskript aus:
   ```

   ```
   ./OnCommandCloudManager-V3.6.3.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 für ein NetApp Cloud Central Konto an, oder melden Sie sich an, wenn Sie bereits über ein Konto verfügen.
8. Wenn Sie sich anmelden oder anmelden, fügt Cloud Manager Ihr Benutzerkonto automatisch als Administrator für dieses System hinzu.
9. Geben Sie nach der Anmeldung einen Namen für dieses Cloud Manager-System ein.

Nachdem Sie fertig sind

Richten Sie Berechtigungen für Ihre AWS und Azure Konten ein, damit Cloud Manager Cloud Volumes ONTAP implementieren kann:

- Wenn Sie Cloud Volumes ONTAP in AWS implementieren möchten, "AWS Konto einrichten und dann zu Cloud Manager hinzufügen".
- Wenn Sie Cloud Volumes ONTAP in Azure implementieren möchten, "Richten Sie ein Azure-Konto ein, und fügen Sie es anschließend zu Cloud Manager hinzu".

Starten von Cloud Manager über den AWS Marketplace

Am besten sollte Cloud Manager in AWS gestartet werden, indem 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 1-Klick-Option 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 OnCommand Cloud Manager: AWS- und Azure Policies"

   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. Wechseln Sie zum "Seite zu Cloud Manager im AWS Marketplace".
3. Klicken Sie Auf **Weiter**.
4. Klicken Sie auf der Registerkarte Benutzerdefinierter Start auf **mit EC2-Konsole** für Ihre Region starten, und wählen Sie dann Ihre Auswahl aus:
   a. Wählen Sie je nach Verfügbarkeit der Region den Instanztyp t3.Medium (empfohlen), t2.Medium oder m4.Large aus.
   b. Wählen Sie eine VPC, ein Subnetz, eine IAM-Rolle und andere Konfigurationsoptionen aus, die Ihren Anforderungen entsprechen.
   c. Behalten Sie die Standardspeicheroptionen bei.
   d. Geben Sie bei Bedarf Tags für die Instanz ein.
   e. Geben Sie die erforderlichen Verbindungsmethoden für die Cloud Manager-Instanz an: SSH, HTTP und HTTPS.
   f. Klicken Sie Auf **Start**.

Ergebnis

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

Nachdem Sie fertig sind

Melden Sie sich bei Cloud Manager an, indem Sie die öffentliche IP-Adresse oder die private IP-Adresse in einem Webbrowser eingeben und anschließend den Setup-Assistenten ausführen.

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

   Wenn Sie sich anmelden, fügt Cloud Manager Ihr Benutzerkonto automatisch als Administrator für dieses System hinzu.

6. Geben Sie nach der Anmeldung einen Namen für das Cloud Manager-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-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_3.6.1.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. Suchen Sie im Azure US Government Portal nach OnCommand Cloud Manager.
2. 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.

3. 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.

4. 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

   Wenn Sie sich anmelden, fügt Cloud Manager Ihr Benutzerkonto automatisch als Administrator für dieses System hinzu.

5. Geben Sie nach der Anmeldung einen Namen für das Cloud Manager-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_3.6.1.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.

Implementierung von 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.

Ihr Administrator sollte Anweisungen befolgt haben, um wieder in Betrieb zu gehen "In AWS statt" Oder "In Azure aus", Und optional "Cloud Manager einrichten".

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

- Die Netzwerkanforderungen von AWS und Azure wurden für Cloud Manager und Cloud Volumes ONTAP erfüllt.
- Cloud Manager verfügt über die Berechtigung, Vorgänge in AWS und Azure in Ihrem Namen auszuführen.
- Jedes Cloud Volumes ONTAP Produkt, das von Benutzern bereitgestellt wird, wurde über den AWS Marketplace abonniert.
- Cloud Manager wurde installiert.
- (Optional) Zusätzliche Mandanten wurden definiert.
- (Optional) Es wurden zusätzliche Benutzerkonten erstellt, die Mandanten- und Arbeitsumgebungsadministratoren umfassen können.

Anmelden bei Cloud Manager

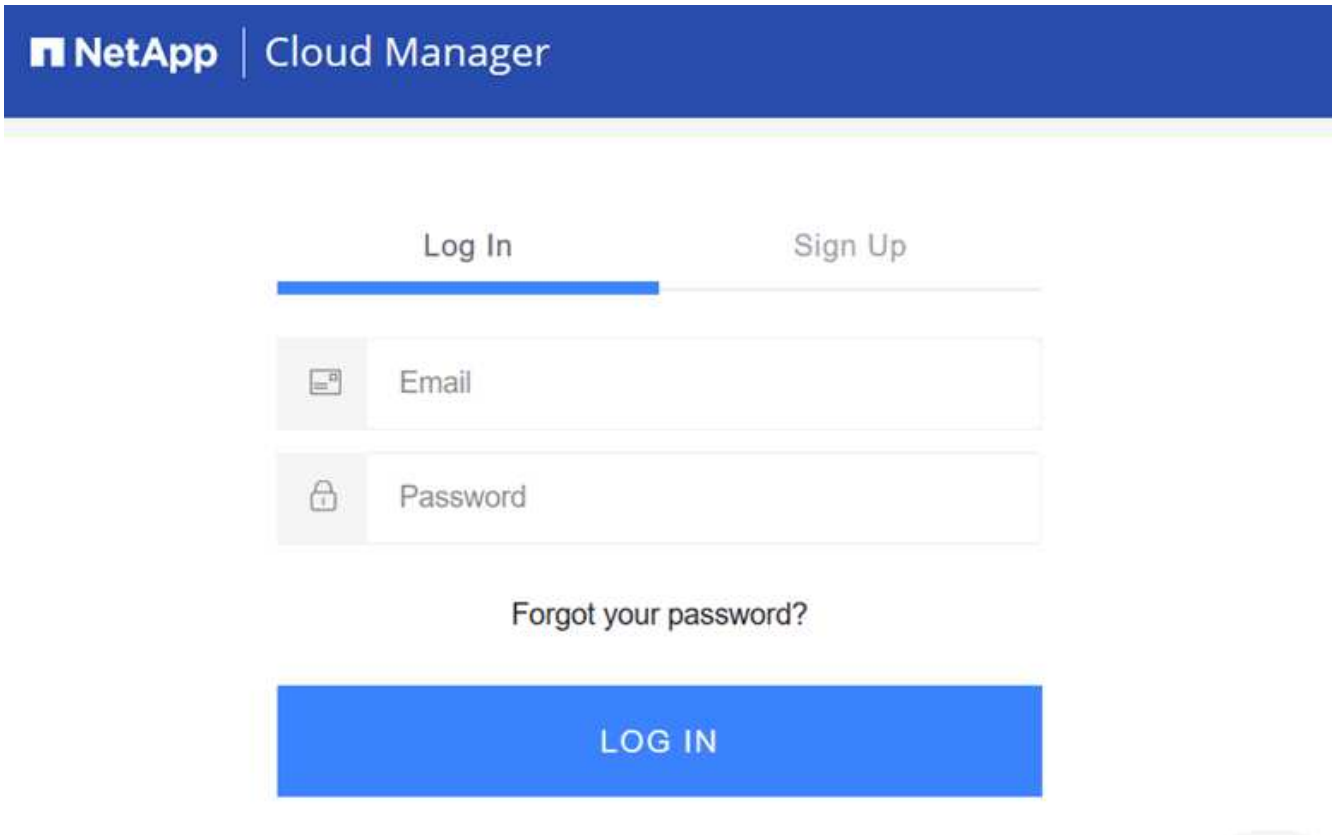
Sie können sich über einen beliebigen Webbrowser mit Verbindung zum Cloud Manager-System bei Cloud Manager anmelden. Sie sollten sich mit einem anmelden "NetApp Cloud Central" Benutzerkonto.

Schritte

1. Öffnen Sie einen Webbrowser, und melden Sie sich bei an "NetApp Cloud Central".
2. Klicken Sie auf **Gehe zu Cloud-Datenservices** und wählen Sie **Cloud Volumes ONTAP**.
3. Klicken Sie auf **Gehe zu Cloud Manager** für das Cloud Manager-System, auf das Sie zugreifen möchten.

Wenn keine Systeme aufgeführt sind, stellen Sie sicher, dass der Cloud Manager Administrator Ihr NetApp Cloud Central Konto zum System hinzugefügt hat.

4. Melden Sie sich mit Ihrem NetApp Cloud Central Account 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 AWS und Azure in zwei Preisoptionen verfügbar: "Pay-as-you-go" und "Bring Your Own License" (Byol). 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 9.5"
- "Unterstützte Konfigurationen für Cloud Volumes ONTAP 9.4"
- "Unterstützte Konfigurationen für ONTAP Cloud 9.3"

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.

- "Speicherplatzgrenzen für Cloud Volumes ONTAP 9.5"
- "Storage-Limits für Cloud Volumes ONTAP 9.4"

- "Storage-Limits für ONTAP Cloud 9.3"

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*

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"

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.

Arbeitsblatt mit Informationen zum AWS-Netzwerk

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

Netzwerkinformationen für Cloud Volumes ONTAP

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

Netzwerkinformationen für ein HA-Paar in mehreren AZS

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

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)	

Aktivierung von Flash Cache für Cloud Volumes ONTAP in AWS

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

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

Schritte

1. Wählen Sie einen der folgenden EC2-Instanztypen aus, die mit den Premium- und BYOL-Lizenzen erhältlich sind:
   - C5d.4xlarge
   - C5d.9xlarge
   - R5d.2xlarge
2. Deaktivieren Sie die Komprimierung für alle Volumes.

   Um die Performance-Verbesserungen von Flash Cache nutzen zu können, muss die Komprimierung für alle Volumes deaktiviert sein. Beim Erstellen eines Volumes aus Cloud Manager kann keine Storage-Effizienz gewählt werden. Alternativ können Sie ein Volume erstellen 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.

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 **Arbeitsumgebung hinzufügen**.
2. Wählen Sie unter Erstellen die Option **Cloud Volumes ONTAP** aus.
3. Ändern Sie auf der Seite Details und Anmeldeinformationen optional das AWS-Konto, geben Sie einen Namen für die Arbeitsumgebung ein, fügen Sie bei Bedarf Tags hinzu, und geben Sie dann ein Kennwort ein.

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

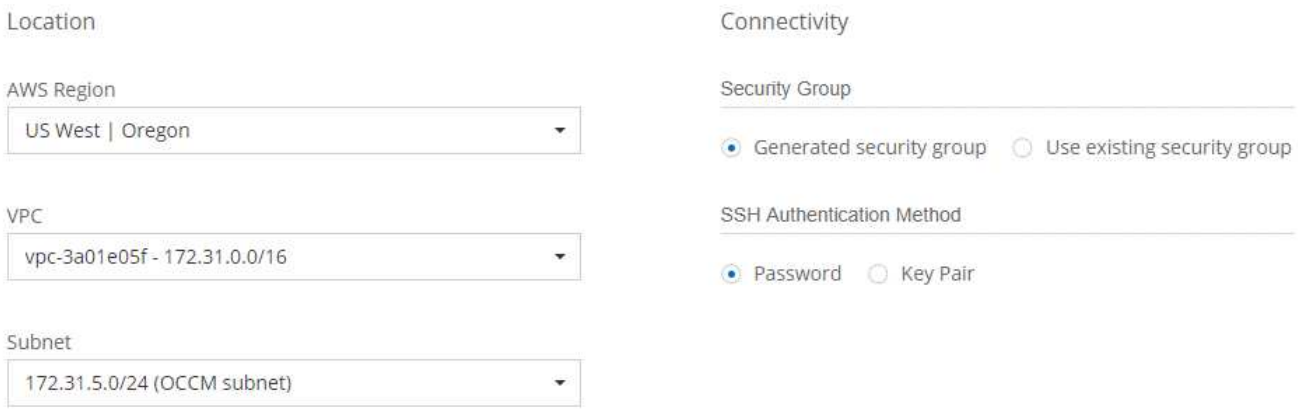
Feld	Beschreibung
Switch-Konto	Sie können ein anderes Konto auswählen, wenn Sie weitere Cloud Provider Accounts hinzufügen. Weitere Informationen finden Sie unter "Cloud Provider Accounts zu Cloud Manager hinzufügen".
Name der Arbeitsumgebung	Cloud Manager verwendet den Namen der Arbeitsumgebung, um 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".

Feld	Beschreibung
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.

Wenn AWS-Schlüssel nicht für Ihr Cloud Manager-Konto angegeben wurden, werden Sie nach dem Klicken auf "Fortfahren" zur Eingabe aufgefordert. Sie müssen sie eingeben, bevor Sie fortfahren können.

4. Geben Sie auf der Seite Location & Connectivity die Netzwerkinformationen ein, die Sie im AWS-Arbeitsblatt aufgezeichnet haben, und klicken Sie dann auf **Weiter**.

   Die folgende Abbildung zeigt die ausgefüllte Seite „Standort & Konnektivität“:



5. Wählen Sie auf der Seite Datenverschlüsselung keine Datenverschlüsselung oder AWS-verwaltete Verschlüsselung aus.

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

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

   "Erfahren Sie mehr über unterstützte Verschlüsselungstechnologien".

6. Geben Sie auf der Seite „Lizenz- und Support-Website-Konto“ an, ob Sie „Pay-as-you-go“ oder „BYOL“ verwenden möchten, und legen Sie anschließend 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. Wählen Sie auf der Seite vorkonfigurierte Pakete 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.

8. Auf der Seite IAM-Rolle sollten Sie die Standardoption beibehalten, damit Cloud Manager die Rolle für Sie

erstellt.

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

9. Ändern Sie auf der Seite Lizenzierung die Cloud Volumes ONTAP-Version nach Bedarf, wählen Sie eine Lizenz, einen Instanztyp, die Instanzenfähigkeit aus, und klicken Sie dann auf **Weiter**.

   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.

10. Wählen Sie auf der Seite „zugrunde liegende Storage-Ressourcen“ die Einstellungen für das anfängliche Aggregat aus: Einen Festplattentyp, eine Größe für jede Festplatte 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".

11. Wählen Sie auf der Seite Schreibgeschwindigkeit & WURM die Option **normale** oder **hohe** Schreibgeschwindigkeit und aktivieren Sie auf Wunsch den WORM-Speicher (Write Once, Read Many).

    "Erfahren Sie mehr über Schreibgeschwindigkeit".

    "Erfahren Sie mehr über WORM Storage".

12. Geben Sie auf der Seite „Create Volume“ Details für das neue Volume ein, und klicken Sie dann auf **Continue**.

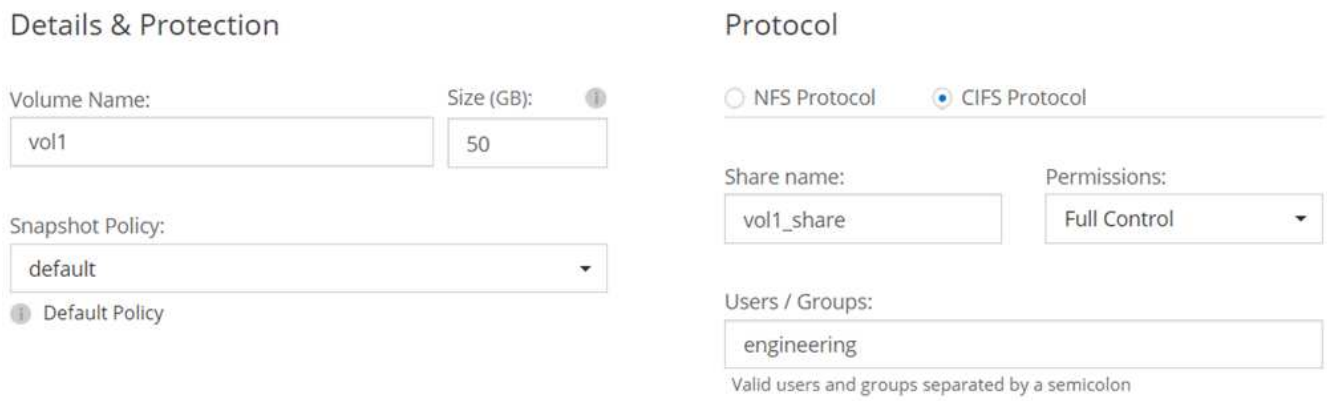
    Sie können diesen Schritt überspringen, wenn Sie ein Volume für iSCSI erstellen möchten. Cloud Manager richtet Volumes nur für NFS und CIFS ein.

    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.

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:



13. Wenn Sie das CIFS-Protokoll ausgewählt haben, richten Sie einen CIFS-Server auf der Seite CIFS-Setup 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.

14. Wählen Sie auf der Seite "Auslastungsprofil", "Festplattentyp" und "Tiering Policy" aus, ob Sie die Storage-Effizienzfunktionen aktivieren möchten, und bearbeiten Sie bei Bedarf die S3-Tiering Policy.

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

15. Überprüfen und bestätigen Sie Ihre Auswahl auf der Seite "Prüfen und genehmigen":
    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 **Arbeitsumgebung hinzufügen**.
2. Wählen Sie unter Erstellen **Cloud Volumes ONTAP HA** aus.
3. Ändern Sie auf der Seite Details und Anmeldeinformationen optional das AWS-Konto, geben Sie einen Namen für die Arbeitsumgebung ein, fügen Sie bei Bedarf Tags hinzu, und geben Sie dann ein Kennwort ein.

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

Feld	Beschreibung
Switch-Konto	Sie können ein anderes Konto auswählen, wenn Sie weitere Cloud Provider Accounts hinzufügen. Weitere Informationen finden Sie unter "Cloud Provider Accounts zu Cloud Manager hinzufügen".
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. 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.

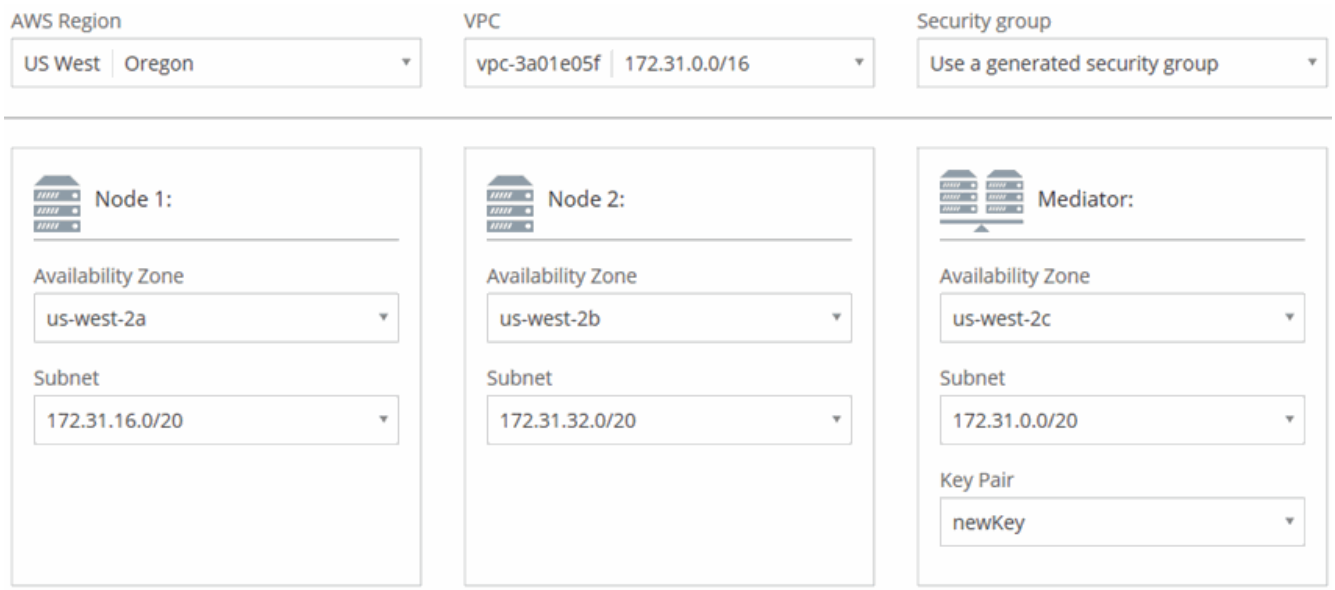
   Wenn AWS-Schlüssel nicht für Ihr Cloud Manager-Konto angegeben wurden, werden Sie nach dem Klicken auf "Fortfahren" zur Eingabe aufgefordert. Sie müssen die AWS-Tasten eingeben, bevor Sie fortfahren.

4. Wählen Sie auf der Seite HA Deployment Models eine HA-Konfiguration aus.

   Einen Überblick über die Implementierungsmodelle finden Sie unter "Cloud Volumes ONTAP HA für AWS".

5. Geben Sie auf der Seite Region & VPC die Netzwerkinformationen ein, die Sie im AWS-Arbeitsblatt aufgezeichnet haben, und klicken Sie dann auf **Weiter**.

   Die folgende Abbildung zeigt die Seite "Standort", die für eine mehrere AZ-Konfigurationen ausgefüllt wurde:



6. Wählen Sie auf der Seite Konnektivität und SSH-Authentifizierung Verbindungsmethoden für das HA-Paar und den Mediator aus.
7. Wenn Sie mehrere AZS ausgewählt haben, geben Sie die fließenden IP-Adressen an und klicken Sie dann auf **Weiter**.

   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".

8. Wenn Sie mehrere AZS ausgewählt haben, wählen Sie die Routentabellen aus, die Routen zu den schwimmenden IP-Adressen enthalten sollen, und klicken Sie dann auf **Weiter**.

   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".

9. Wählen Sie auf der Seite Datenverschlüsselung keine Datenverschlüsselung oder AWS-verwaltete Verschlüsselung aus.

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

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

   "Erfahren Sie mehr über unterstützte Verschlüsselungstechnologien".

10. Geben Sie auf der Seite „Lizenz- und Support-Website-Konto“ an, ob Sie „Pay-as-you-go“ oder „BYOL“ verwenden möchten, und legen Sie anschließend 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".

11. Wählen Sie auf der Seite vorkonfigurierte Pakete 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.

12. Auf der Seite IAM-Rolle sollten Sie die Standardoption beibehalten, damit Cloud Manager die Rollen für Sie erstellt.

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

13. Ändern Sie auf der Seite Lizenzierung die Cloud Volumes ONTAP-Version nach Bedarf, wählen Sie eine Lizenz, einen Instanztyp, die Instanzenfähigkeit aus, und klicken Sie dann auf **Weiter**.

    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.

14. Wählen Sie auf der Seite „zugrunde liegende Storage-Ressourcen“ die Einstellungen für das anfängliche Aggregat aus: Einen Festplattentyp, eine Größe für jede Festplatte 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".

15. Aktivieren Sie auf der WORM-Seite einmal beschreibbaren WORM-Storage (Read Many), falls gewünscht.

    "Erfahren Sie mehr über WORM Storage".

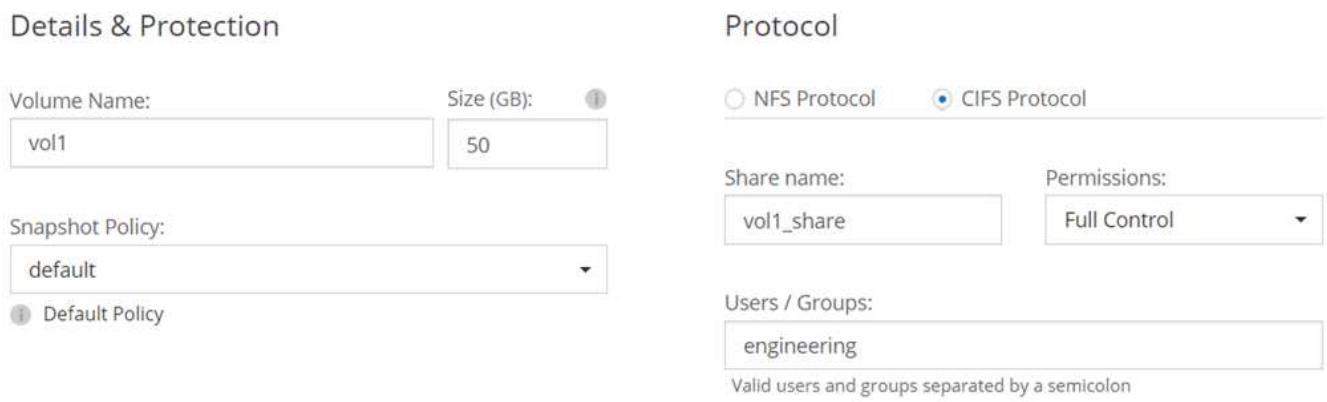
16. Geben Sie auf der Seite „Create Volume“ Details für das neue Volume ein, und klicken Sie dann auf **Continue**.

    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:



17. Wenn Sie das CIFS-Protokoll ausgewählt haben, richten Sie einen CIFS-Server auf der Seite CIFS-Setup 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.
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.

18. Wählen Sie auf der Seite "Auslastungsprofil", "Festplattentyp" und "Tiering Policy" aus, ob Sie die Storage-Effizienzfunktionen aktivieren möchten, und bearbeiten Sie bei Bedarf die S3-Tiering Policy.

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

19. Überprüfen und bestätigen Sie Ihre Auswahl auf der Seite "Prüfen und genehmigen":
    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.

  "Lesen Sie die neuen Berechtigungen, die für die Implementierung von HA-Systemen erforderlich sind".

- 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 **Arbeitsumgebung hinzufügen**
2. Wählen Sie unter Erstellen ein Single-Node-System in Azure oder ein HA-Paar in Azure aus.
3. Ändern Sie auf der Seite „Details and Credentials“ optional das Azure Konto oder das Azure Abonnement, geben Sie einen Cluster-Namen und Ressourcengruppennamen an, fügen Sie bei Bedarf Tags hinzu und geben Sie dann die Zugangsdaten an.

   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 "Zusätzliche Cloud Provider-Konten hinzugefügt".
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. Wählen Sie auf der Seite Standort einen Standort und eine Sicherheitsgruppe aus, aktivieren Sie das Kontrollkästchen, um die Netzwerkverbindung zu bestätigen, und klicken Sie dann auf **Weiter**.
5. Geben Sie auf der Seite „Lizenz- und Support-Website-Konto“ an, ob Sie „Pay-as-you-go“ oder „BYOL“ verwenden möchten, und legen Sie anschließend ein NetApp Support Site Konto fest.

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

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

6. Wählen Sie auf der Seite vorkonfigurierte Pakete eines der Pakete aus, um schnell ein Cloud Volumes ONTAP-System bereitzustellen, oder klicken Sie auf **eigene Konfiguration erstellen**.

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

7. Ändern Sie auf der Seite Lizenzierung die Cloud Volumes ONTAP-Version nach Bedarf, wählen Sie eine Lizenz und einen virtuellen Maschinentyp aus und klicken Sie dann auf **Weiter**.

   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.

8. Führen Sie auf der Seite Azure Marketplace die folgenden Schritte aus, wenn Cloud Manager die programmatische Implementierung von Cloud Volumes ONTAP nicht aktivieren konnte.
9. Wählen Sie auf der Seite „zugrunde liegende Storage-Ressourcen“ die Einstellungen für das anfängliche Aggregat aus: Einen Festplattentyp, eine Größe für jede Festplatte und ob das 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 Azure".

10. Wählen Sie auf der Seite Schreibgeschwindigkeit & WURM die Option **normale** oder **hohe** Schreibgeschwindigkeit und aktivieren Sie auf Wunsch den WORM-Speicher (Write Once, Read Many).

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

    "Erfahren Sie mehr über Schreibgeschwindigkeit".

    "Erfahren Sie mehr über WORM Storage".

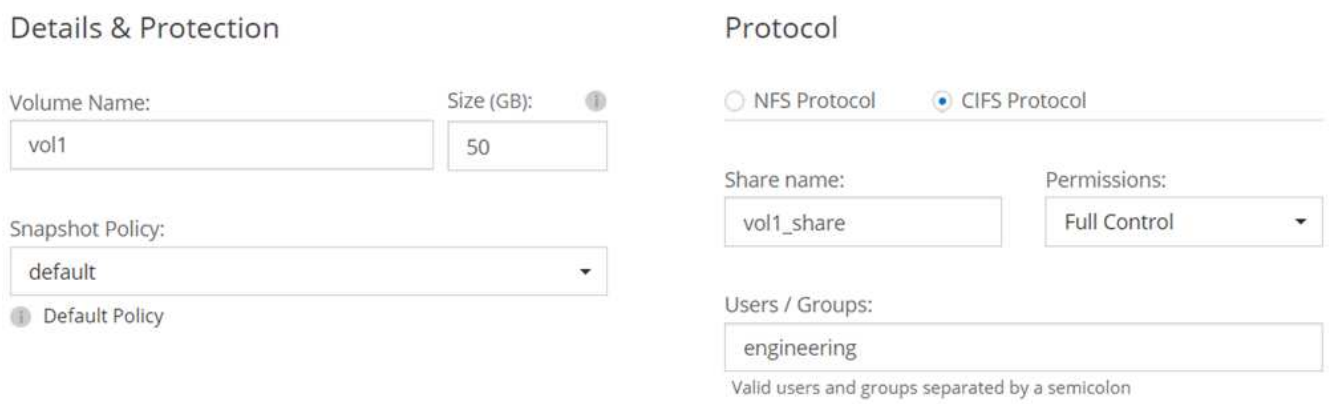
11. Geben Sie auf der Seite „Create Volume“ Details für das neue Volume ein, und klicken Sie dann auf **Continue**.

    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:



12. Wenn Sie das CIFS-Protokoll ausgewählt haben, richten Sie einen CIFS-Server auf der Seite CIFS-Setup 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.
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. Wählen Sie auf der Seite "Auslastungsprofil", "Festplattentyp" und "Tiering Policy" aus, ob Sie die Storage-Effizienzfunktionen aktivieren und die Tiering Policy bei Bedarf ändern möchten.

   Storage Tiering wird nur bei Single-Node-Systemen unterstützt.

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

14. Überprüfen und bestätigen Sie Ihre Auswahl auf der Seite "Prüfen und genehmigen":

   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.

Registrieren von Pay-as-you-go-Systemen

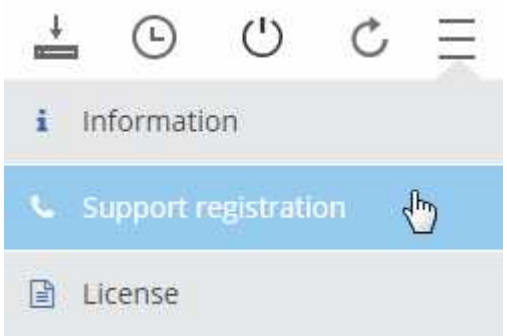
Cloud Volumes ONTAP Explore, Standard und Premium umfasst Support von NetApp. Sie müssen jedoch den Support erst aktivieren, wenn Sie die Systeme bei NetApp registrieren.

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**:



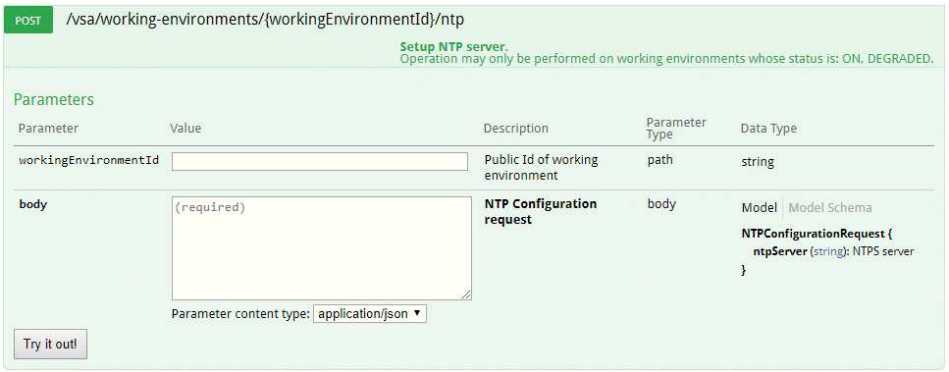
4. Wählen Sie ein NetApp Support Site Konto aus und klicken Sie auf **Registrieren**.

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 Cloud Manager Admin Cloud Manager vor dem Start der Instanz einen Proxyserver hinzugefügt hat, ist Cloud Volumes ONTAP so konfiguriert, dass dieser Proxyserver für AutoSupport Nachrichten verwendet wird. 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".

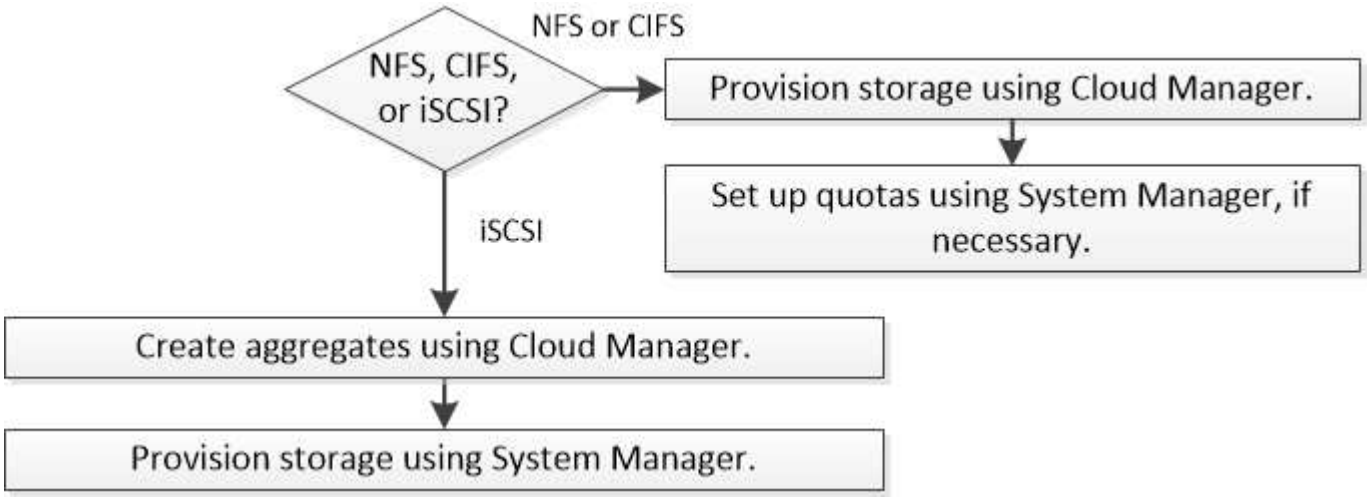
Aufgabe	Beschreibung
Optional: EMS konfigurieren	Das Event Management System (EMS) erfasst und zeigt Informationen zu Ereignissen an, die auf Cloud Volumes ONTAP Systemen auftreten. Um Ereignisbenachrichtigungen zu erhalten, können Sie Ereignisziele (E-Mail-Adressen, SNMP-Trap-Hosts oder Syslog-Server) 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".
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".

Storage-Bereitstellung

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.



Bereitstellung von Volumes

Wenn Sie nach dem Start eines Cloud Volumes ONTAP Systems mehr Storage benötigen, können Sie über Cloud Manager neue NFS- und CIFS-Volumes bereitstellen.

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 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.
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 "Auslastungsprofil", "Festplattentyp" und "Tiering Policy" aus, ob Sie Storage-Effizienzfunktionen aktivieren möchten, wählen Sie einen Festplattentyp aus und bearbeiten Sie bei Bedarf die S3-Tiering Policy.

   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.

Bereitstellung von 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".

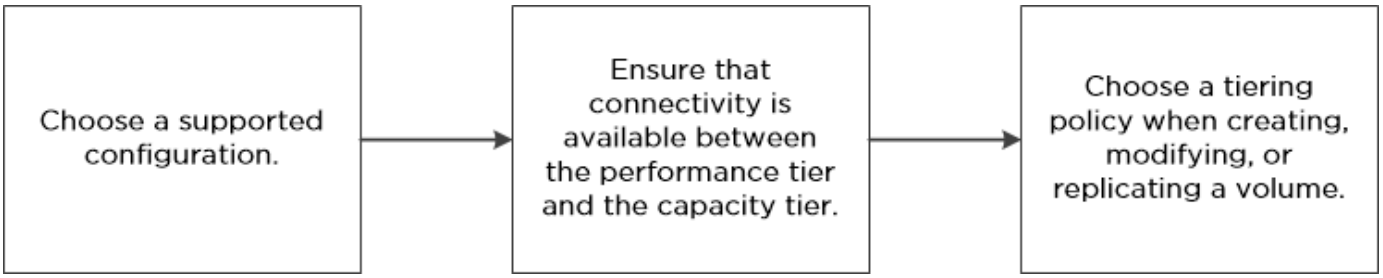
2. Klicken Sie auf **Storage > LUNs**.
3. Klicken Sie auf **Erstellen** und folgen Sie den Aufforderungen zur Erstellung der LUN.
4. Stellen Sie von Ihren Hosts eine Verbindung zur LUN her.

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

Tiering inaktiver Daten in kostengünstigen Objektspeicher

Durch die Kombination einer SSD- oder HDD-Performance-Tier für häufig abgerufene Daten mit einem Objekt-Storage-Kapazitäts-Tier für inaktive Daten können Storage-Kosten in AWS und Azure gesenkt werden. Eine allgemeine Übersicht finden Sie unter "Data Tiering - Übersicht".

Zum Einrichten von Data Tiering müssen Sie lediglich Folgendes tun:



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

- Sie müssen keine Funktionslizenz installieren, um Data Tiering zu aktivieren.
- Sie müssen die Kapazitätsstufe nicht erstellen (entweder ein S3-Bucket oder ein Azure Blob Container). Cloud Manager macht das für Sie.

Konfigurationen, die Daten-Tiering unterstützen

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

- Data Tiering wird mit Cloud Volumes ONTAP Standard, Premium und Byol unterstützt, beginnend mit Version 9.2 in AWS und Version 9.4 in Microsoft Azure.
  - Daten-Tiering wird nicht mit HA-Paaren in Microsoft Azure unterstützt.
  - 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.
- Daten-Tiering wird durch Verschlüsselungstechnologien unterstützt.
- Thin Provisioning muss auf Volumes aktiviert sein.

Anforderungen für Tiering von Daten in AWS

Sie müssen 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?".

Anforderungen für Tiering von Daten in Microsoft Azure

Sie müssen keine Verbindung zwischen der Performance-Ebene und der Kapazitätsebene herstellen, solange Cloud Manager über die erforderlichen Berechtigungen verfügt. Cloud Manager aktiviert einen VNet Service-Endpunkt für Sie, wenn die Cloud Manager-Richtlinie über die entsprechende Berechtigung verfügt:

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

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

Tiering von Daten auf Lese-/Schreib-Volumes

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

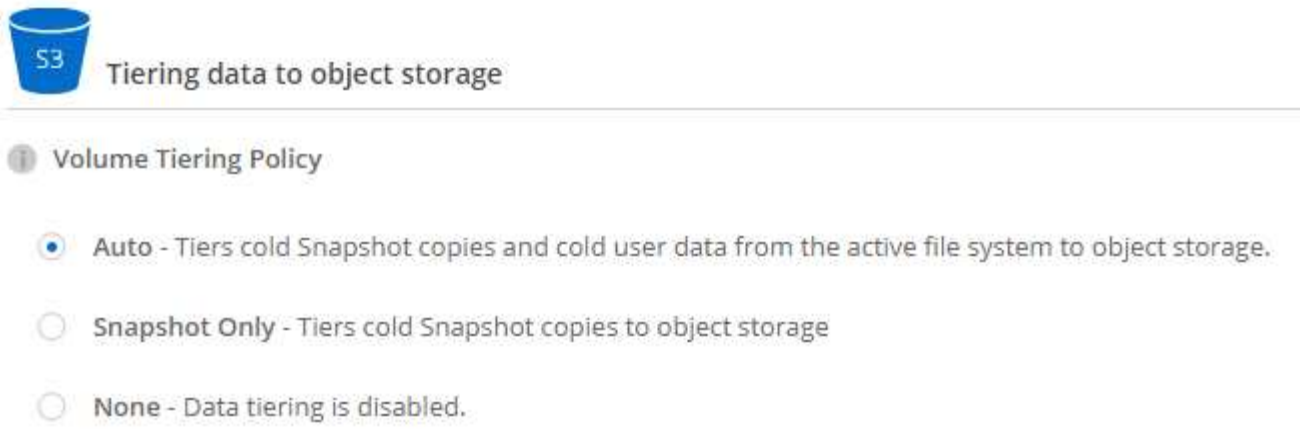
1. Erstellen Sie in der Arbeitsumgebung ein neues Volume, oder ändern Sie den Tier eines vorhandenen Volumes:

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.

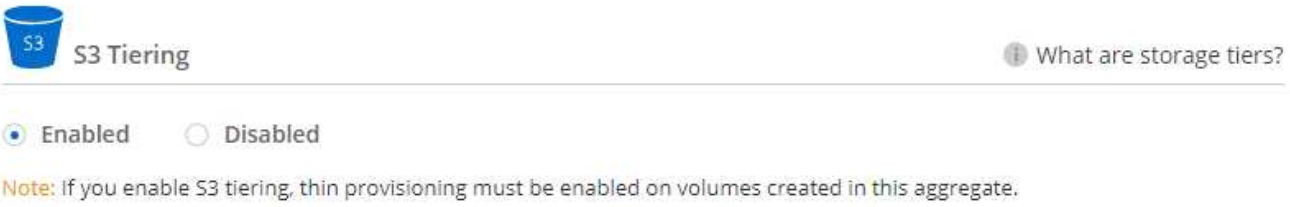
Tiering von Daten auf Data-Protection-Volumes

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 Level

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.

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 **Tiering Level**.
2. Wählen Sie die Tiering-Ebene und klicken Sie dann auf **Speichern**.

Verwendung von Cloud Volumes ONTAP als persistenter Storage für Kubernetes

Cloud Manager kann die Implementierung von automatisieren "NetApp Trident" Auf Kubernetes-Clustern zur Verwendung von Cloud Volumes ONTAP als persistenten Storage für Container Erste Schritte umfassen einige Schritte.

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 Cloud Volumes 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/

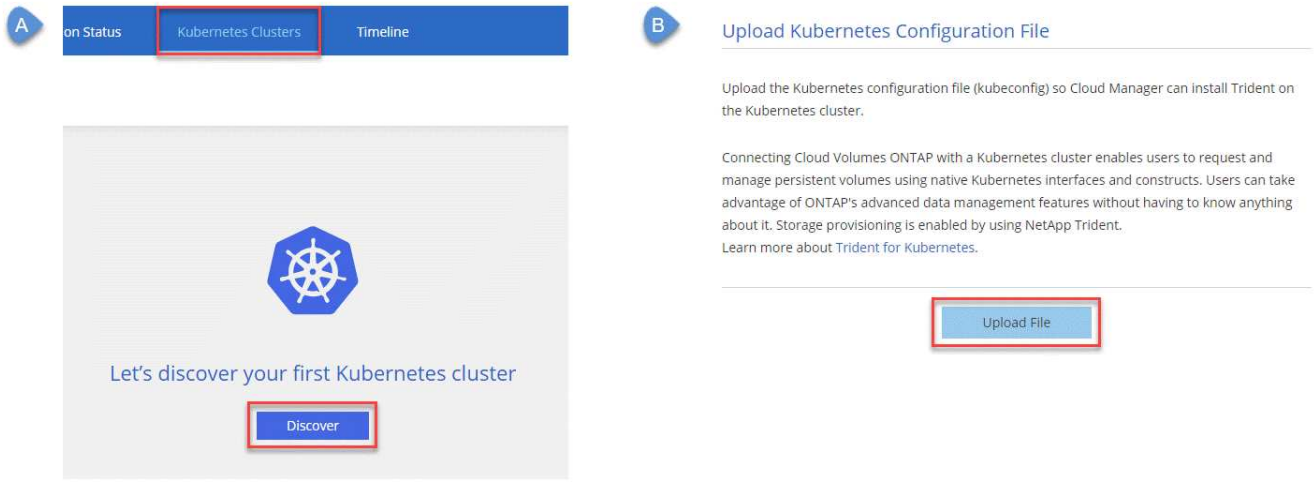
   Cloud Manager installiert Trident auf einem Kubernetes-Cluster, wenn Sie eine Arbeitsumgebung mit dem Cluster verbinden.

Kubernetes-Konfigurationsdateien in Cloud Manager hochladen

Für jeden Kubernetes-Cluster muss der Cloud Manager Administrator 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.

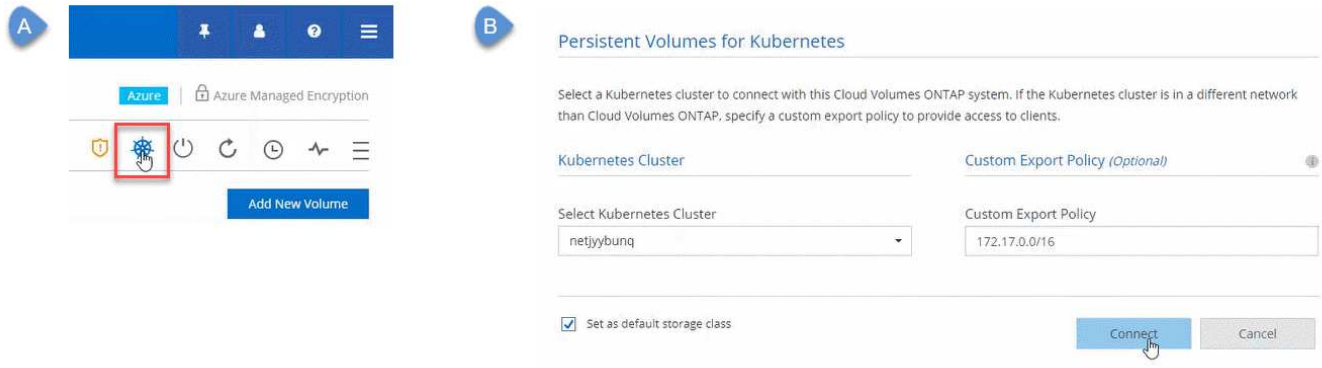
Klicken Sie auf **Kubernetes Clusters > Entdecken > Datei hochladen** und wählen Sie die kubeconfig-Datei aus.



3 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 Cloud Volumes ONTAP Systemen und mehreren Clustern mit demselben Cloud Volumes 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 Cloud Volumes ONTAP-Systeme als Back-End-Storage verwenden.



4 Starten Sie die Bereitstellung persistenter Volumes

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

- **netapp-File**: Zur Anbindung persistenter Volumes an Cloud Volumes ONTAP-Systeme mit einem Node
- **netapp-file-redundant**: Zur Anbindung persistenter Volumes an Cloud Volumes 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 Cloud Volumes ONTAP System, das Sie mit einem Kubernetes-Cluster verbinden. Der Name des Volumes wird mit „_Trident_dreident_dreident“ angehängt. Cloud Volumes ONTAP Systeme verwenden 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 Cloud Volumes ONTAP Systeme von einem Kubernetes Cluster trennen. Wenn Sie ein System trennen, können Sie dieses Cloud Volumes 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

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 einer Lizenz für NetApp Volume Encryption auf dem Cloud Volumes ONTAP System.

   "ONTAP 9 NetApp Verschlüsselungs-Anleitung: Installieren der Lizenz"

4. Installieren Sie SSL-Zertifikate und stellen Sie eine Verbindung zu den externen Schlüsselverwaltungsservern her.

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

5. 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**.
Klonen Sie ein Volume	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Clone**. b. Ändern Sie den Klonnamen nach Bedarf, und klicken Sie dann auf **Clone**. Bei diesem Prozess wird ein FlexClone Volume erstellt. Ein FlexClone Volume ist eine beschreibbare Point-in-Time-Kopie, die platzsparend ist, da es einen geringen Speicherplatz für Metadaten verbraucht und dann nur noch zusätzlichen Speicherplatz verbraucht, wenn Daten geändert oder hinzugefügt werden. Weitere Informationen zu FlexClone Volumes finden Sie im "ONTAP 9 Leitfaden für das Management von logischem Storage".
Wiederherstellen von Daten aus einer Snapshot Kopie auf einem neuen Volume	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Wiederherstellen aus Snapshot Kopie**. b. Wählen Sie eine Snapshot Kopie aus, geben Sie einen Namen für das neue Volume ein und klicken Sie dann auf **Wiederherstellen**.
Erstellen Sie bei Bedarf eine Snapshot Kopie	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Snapshot Kopie erstellen**. b. Ändern Sie ggf. den Namen und klicken Sie dann auf **Erstellen**.
Rufen Sie den NFS-Mount-Befehl ab	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Mount Command**. b. Klicken Sie Auf **Kopieren**.
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.

Aufgabe	Aktion
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**.

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

Ändern des CIFS-Servers

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

Schritte

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

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

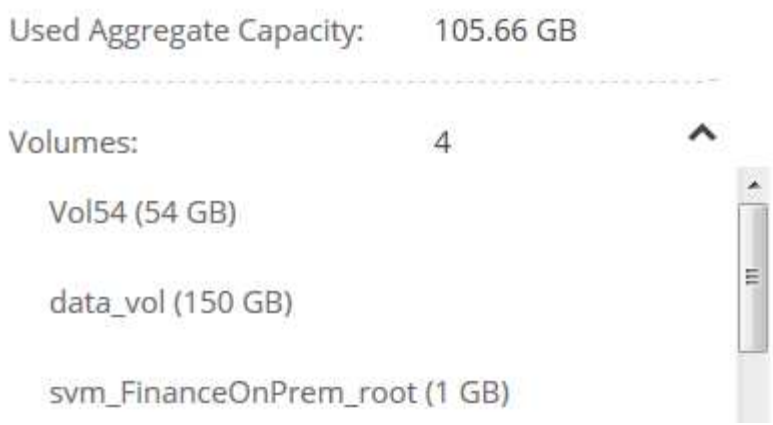
Wenn Cloud Manager keine Empfehlungen für das Verschieben eines Volumes zur Vermeidung von Kapazitätsproblemen geben kann, müssen Sie die Volumes identifizieren, die Sie verschieben müssen, und angeben, ob Sie sie in ein anderes Aggregat auf demselben System oder in ein anderes System verschieben sollten.

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.

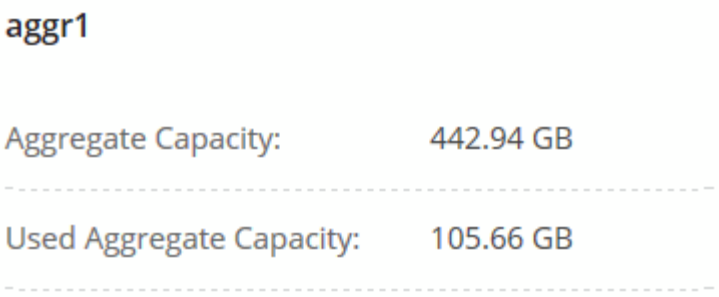
Über diese Aufgabe

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".

Bereitstellung von NFS-Volumes über die Volume-Ansicht

Wechseln zur Volume-Ansicht

Cloud Manager bietet zwei Managementansichten: Die Storage System View für das Management von Storage-Systemen in einer Hybrid Cloud und die Volume View für die Erstellung von Volumes in AWS, ohne Storage-Systeme managen zu müssen. Sie können zwischen diesen Ansichten wechseln. Diese Instanzen sollten jedoch selten vorkommen, da eine einzelne Ansicht Ihren Anforderungen entsprechen sollte.

Weitere Informationen zur Volume-Ansicht finden Sie unter "Vereinfachtes Storage-Management mit der Volume-Ansicht".

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Menü und dann auf **Auswahl anzeigen**.
2. Wählen Sie auf der Ansichtsseite Auswahl die Option **Speichersystemansicht** aus und klicken Sie dann auf **Switch**.

Ergebnis

Cloud Manager wechselt zur Volume-Ansicht.

Erstellen und Mounten von NFS-Volumes

Sie können Cloud Manager verwenden, um NFS-Volumes zu erstellen, die Funktionen der Enterprise-Klasse auf AWS Storage bieten.

Erstellen von NFS-Volumes

Sie können ein Volume erstellen, das mit einer einzelnen AWS-Instanz oder einer Instanz verbunden ist, die auf eine andere Instanz gespiegelt wird, um eine hohe Verfügbarkeit zu gewährleisten.

Schritte

1. Klicken Sie auf der Registerkarte Volumes auf **Neues Volume erstellen**.
2. Wählen Sie auf der Seite Neues Volume erstellen einen Volume-Typ aus:

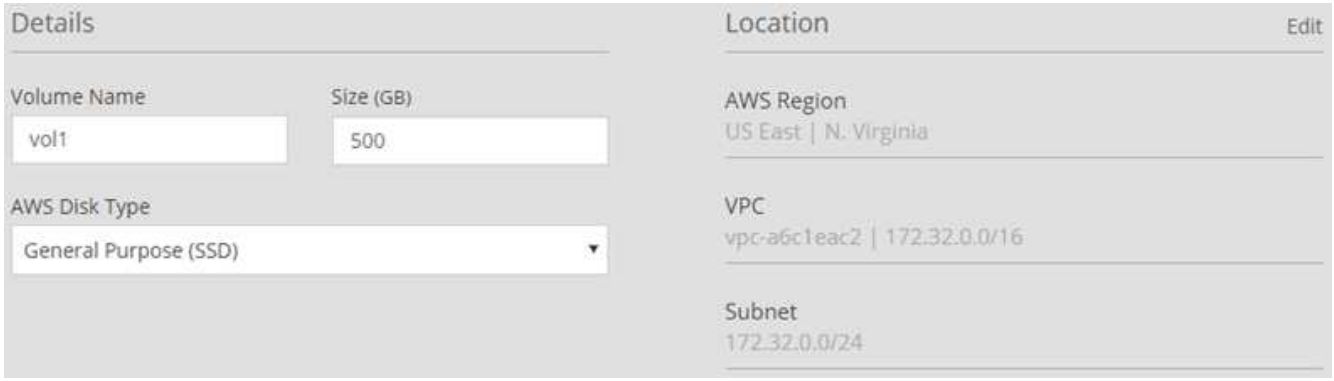
Option	Beschreibung
Volume erstellen	Erstellt ein Volume, das mit einer einzelnen AWS-Instanz verbunden ist.
Erstellen Sie ein HA-Volume	Erstellt ein Volume, das mit einer einzelnen AWS-Instanz verbunden und auf eine andere Instanz gespiegelt wird, um bei Ausfällen eine hohe Verfügbarkeit zu gewährleisten. Klicken Sie auf das Symbol Info, um weitere Details zu den für ein HA-Volume erforderlichen Instanzen anzuzeigen.

3. Wenn Sie „Volume erstellen“ ausgewählt haben, geben Sie die Details für Ihr erstes Volume an, und klicken Sie dann auf „Create*“.

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

Feld	Beschreibung
Größe	Die maximale Größe für das Volume hängt von der in vorhandenen Storage-Systemen verfügbaren Kapazität ab. Thin Provisioning wird automatisch auf dem Volume aktiviert, sodass Sie ein Volume erstellen können, das größer ist als der derzeit verfügbare physische Storage. Anstatt Speicherplatz vorab zuzuweisen, wird jedem Volume Speicherplatz zugewiesen, während Daten geschrieben werden.
AWS-Festplattentyp	Sie sollten die Festplatte auswählen, die Ihren Anforderungen hinsichtlich Performance und Kosten entspricht. • Universal SSD-Festplatten bieten ein ausgewogenes Verhältnis zwischen Kosten und Performance für eine breite Palette von Workloads. Die Performance wird in Bezug auf IOPS definiert. • Durchsatzoptimierte HDD-Festplatten eignen sich für Workloads, auf die häufig zugegriffen wird und die einen schnellen und konsistenten Durchsatz zu einem niedrigeren Preis erfordern. • Kalte Festplatten sind für Backups oder selten genutzte Daten gedacht, da die Performance sehr gering ist. Wie bei Festplatten mit Durchsatzoptimierung wird die Performance in Bezug auf den Durchsatz definiert. Weitere Informationen finden Sie unter "AWS Dokumentation: EBS Volume-Typen".

   Die folgende Abbildung zeigt die ausgefüllte Seite "Volume erstellen":

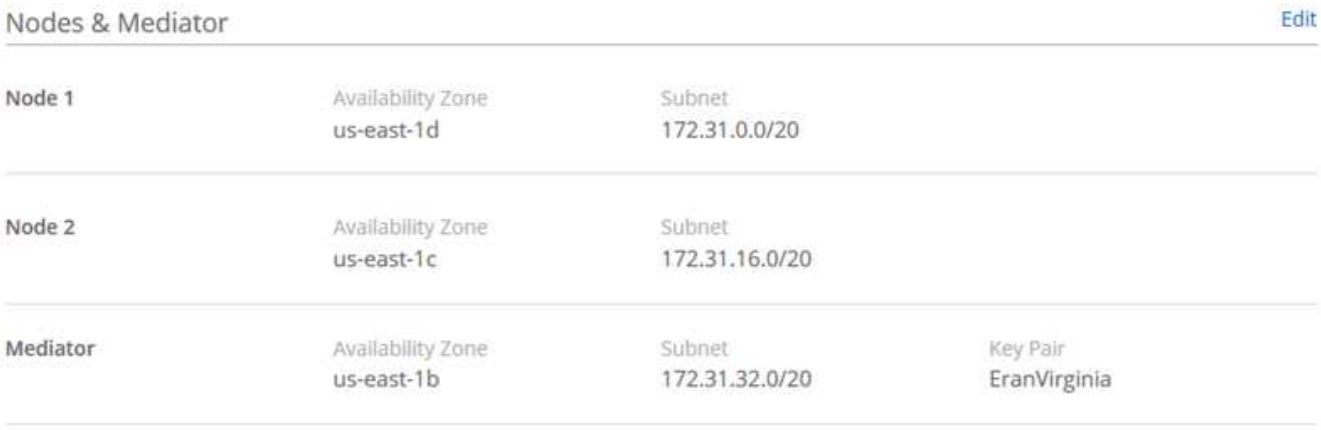


4. Wenn Sie „HA-Volumen erstellen“ ausgewählt haben, geben Sie die Details für das Volume an, und klicken Sie dann auf **Erstellen**.

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

Feld	Beschreibung
Größe	Die maximale Größe für das Volume hängt von der in vorhandenen Storage-Systemen verfügbaren Kapazität ab. Thin Provisioning wird automatisch auf dem Volume aktiviert, sodass Sie ein Volume erstellen können, das größer ist als der derzeit verfügbare physische Storage. Anstatt Speicherplatz vorab zuzuweisen, wird jedem Volume Speicherplatz zugewiesen, während Daten geschrieben werden.
AWS-Festplattentyp	Sie sollten die Festplatte auswählen, die Ihren Anforderungen hinsichtlich Performance und Kosten entspricht. • Universal SSD-Festplatten bieten ein ausgewogenes Verhältnis zwischen Kosten und Performance für eine breite Palette von Workloads. Die Performance wird in Bezug auf IOPS definiert. • Durchsatzoptimierte HDD-Festplatten eignen sich für Workloads, auf die häufig zugegriffen wird und die einen schnellen und konsistenten Durchsatz erfordern. Weitere Informationen finden Sie unter "AWS Dokumentation: EBS Volume-Typen".
Standort	Sie sollten einen VPC wählen, der drei Subnetze in drei separaten Verfügbarkeitszonen enthält.
Nodes und Mediator	Wenn möglich, wählt Cloud Manager für jede Instanz separate Verfügbarkeitszonen, da es sich um die unterstützte und optimale Konfiguration handelt.
Floating-IP	Die IP-Adressen müssen für alle VPCs in der Region außerhalb des CIDR-Blocks liegen.
Routentabelle	Wenn Sie mehr als eine Routentabelle haben, ist es sehr wichtig, die richtigen Routentabellen auszuwählen. Andernfalls haben einige Clients möglicherweise keinen Zugriff auf das HA-Paar. Weitere Informationen finden Sie unter "AWS Documentation: Routingtabellen".

   Die folgende Abbildung zeigt die Seite Nodes and Mediator. Jede Instanz befindet sich in einer separaten Verfügbarkeitszone.



Ergebnis

Cloud Manager erstellt das Volume auf einem vorhandenen System oder auf einem neuen System. Wenn ein neues System erforderlich ist, kann die Erstellung des Volumes ca. 25 Minuten dauern.

Mounten von Volumes auf Linux-Hosts

Nachdem Sie ein Volume erstellt haben, sollten Sie es auf Ihren Hosts mounten, damit diese auf das Volume zugreifen können.

Schritte

1. Legen Sie auf der Registerkarte Volumes den Mauszeiger über die Lautstärke, wählen Sie das Menüsymbol und klicken Sie dann auf **Mount**.
2. Klicken Sie Auf **Kopieren**.
3. Ändern Sie auf Ihren Linux-Hosts den kopierten Text, indem Sie das Zielverzeichnis ändern, und geben Sie dann den Befehl zum Mounten des Volumes ein.

Managen von NFS-Volumes

Sie können NFS-Volumes managen, indem Sie sie klonen, den Datenzugriff managen, den zugrunde liegenden Festplattentyp ändern und vieles mehr.

Klonen von Volumes

Wenn Sie eine sofortige Kopie Ihrer Daten benötigen, ohne viel Speicherplatz zu belegen, können Sie einen Klon eines vorhandenen Volumes erstellen.

Über diese Aufgabe

Das geklonte Volume ist eine beschreibbare Point-in-Time-Kopie, die platzsparend ist, da es einen geringen Speicherplatz für Metadaten verwendet und dann nur zusätzlichen Speicherplatz verbraucht, wenn Daten geändert oder hinzugefügt werden.

Schritte

1. Legen Sie auf der Registerkarte Volumes den Mauszeiger über die Lautstärke, wählen Sie das Menüsymbol und klicken Sie dann auf **Clone**.
2. Ändern Sie ggf. den Namen des geklonten Volumes und klicken Sie dann auf **Clone**.

Ergebnis

Cloud Manager erstellt ein neues Volume, das ein Klon eines vorhandenen Volumes ist.

Managen des Datenzugriffs auf Volumes

Wenn Sie ein Volume erstellen, stellt Cloud Manager das Volume allen EC2-Instanzen in dem VPC zur Verfügung, in dem das Volume erstellt wurde. Sie können diesen Standardwert ändern, wenn Sie den Datenzugriff auf das Volume einschränken müssen.

Schritte

1. Legen Sie auf der Registerkarte Volumes den Mauszeiger über die Lautstärke, wählen Sie das Menüsymbol und klicken Sie dann auf **Zugriff verwalten**.
2. Ändern Sie die Zugriffsliste für die Lautstärke, und klicken Sie dann auf **Speichern**.

Ändern der zugrunde liegenden AWS-Festplatte für ein Volume

Sie können die zugrunde liegende AWS-Festplatte ändern, die ein Volume zur Bereitstellung von Storage verwendet. Wenn beispielsweise eine höhere Performance erforderlich ist, können Sie von einer Throughput Optimized HDD zu einer General Purpose SSD wechseln.

Schritte

1. Legen Sie auf der Registerkarte Volumes den Mauszeiger über das Volumen, wählen Sie das Menüsymbol und klicken Sie dann auf **Datenträger ändern**.
2. Wählen Sie den AWS-Festplattentyp aus und klicken Sie auf **Ändern**.

Ergebnis

Cloud Manager verschiebt das Volume in ein vorhandenes Aggregat, das den ausgewählten Festplattentyp verwendet, oder erstellt ein neues Aggregat für das Volume.

Anzeigen und Ändern von AWS-Ressourcen

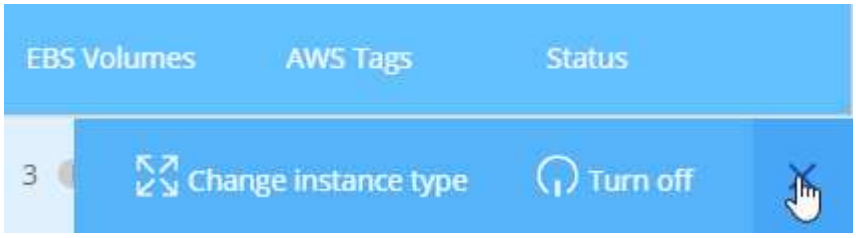
Wenn Sie ein neues Volume erstellen, weist Cloud Manager die für dieses Volume erforderlichen AWS-Instanzen und EBS-Speicher zu. Bei Bedarf können Sie Details zu AWS-Instanzen und EBS-Storage anzeigen, Instanztypen ändern und Instanzen aus- und wieder einschalten.

Schritte

1. Klicken Sie auf **AWS Ressourcen**.

   Die Liste der AWS-Instanzen wird angezeigt. Sie können Details wie Instanztyp, AWS-Speicherort und die an die Instanz angehängten Volumes anzeigen.

2. Wählen Sie bei Bedarf das Menüsymbol neben der Spalte Status aus, und wählen Sie dann eine der verfügbaren Aktionen aus:



Volumes werden gelöscht

Sie können Volumes löschen, die Sie nicht mehr benötigen.

Schritte

1. Legen Sie auf der Registerkarte Volumes den Mauszeiger über die Lautstärke, wählen Sie das Menüsymbol und klicken Sie dann auf **Löschen**.
2. Klicken Sie auf **Löschen**, um zu bestätigen, dass Sie das Volume löschen möchten.

Datenmanagement in einer Hybrid Cloud

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.

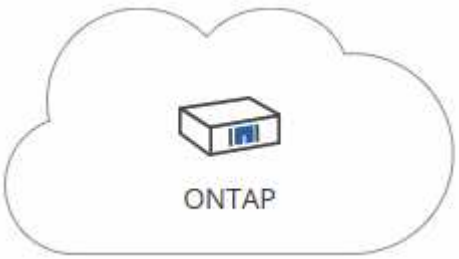
- Der ONTAP Cluster muss eingehenden HTTPS-Zugriff über Port 443 zulassen.

  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.

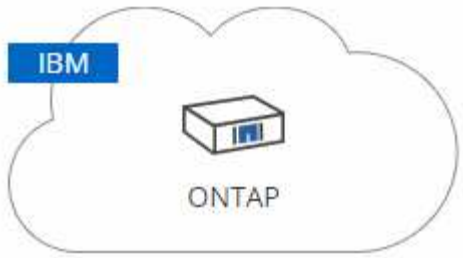
Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen**.
2. Wählen Sie unter **Discover** eines der Symbole, um einen ONTAP-Cluster zu entdecken.

   Mit dem folgenden Symbol können Sie ein lokales Cluster oder eine NetApp Private Storage-Konfiguration ermitteln:



   Mit dem folgenden Symbol können Sie ONTAP in der IBM Cloud erkennen:



3. Geben Sie auf der Seite **ONTAP-Cluster-Details** die Cluster-Management-IP-Adresse und das Passwort für das Admin-Benutzerkonto ein.

   Wenn Sie das erste Symbol ausgewählt haben, müssen Sie auch den Typ der Arbeitsumgebung auswählen: Entweder ein On-Premises-Cluster oder eine NetApp Private Storage-Konfiguration.

4. 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.

Feld	Beschreibung
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.
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 in die und aus der Cloud

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.

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.

Auswählen einer Replizierungsrichtlinie

Eine Replizierungsrichtlinie definiert, wie das Storage-System Daten von einem Quell-Volume auf ein Ziel-Volume repliziert. Sie müssen eine Replizierungsrichtlinie auswählen, wenn Sie die Datenreplizierung in Cloud Manager einrichten.

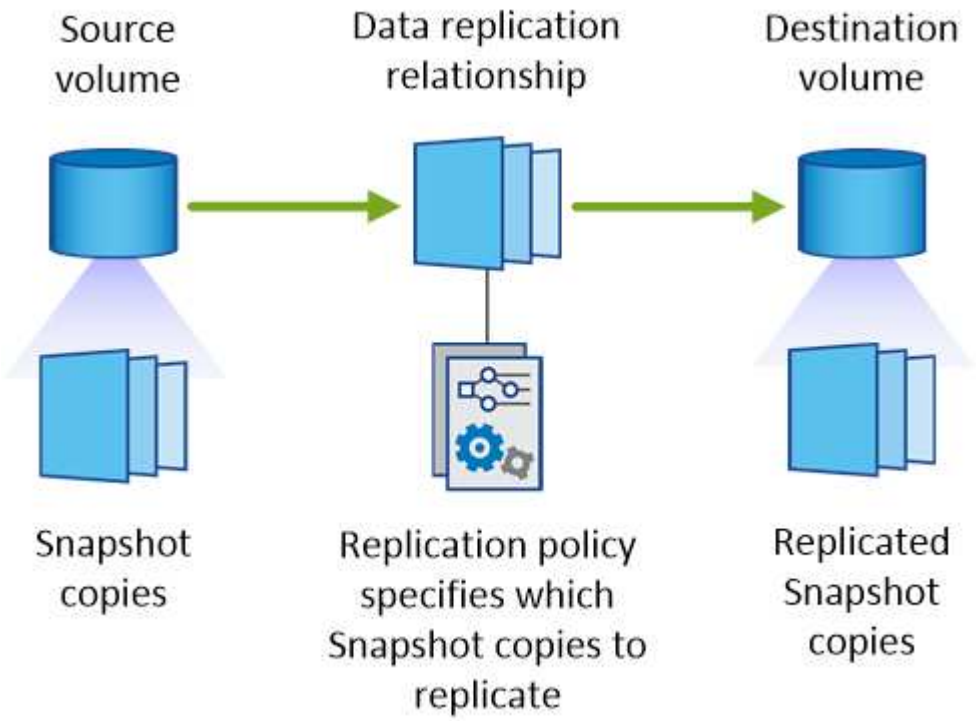
Was sind Replizierungsrichtlinien

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.

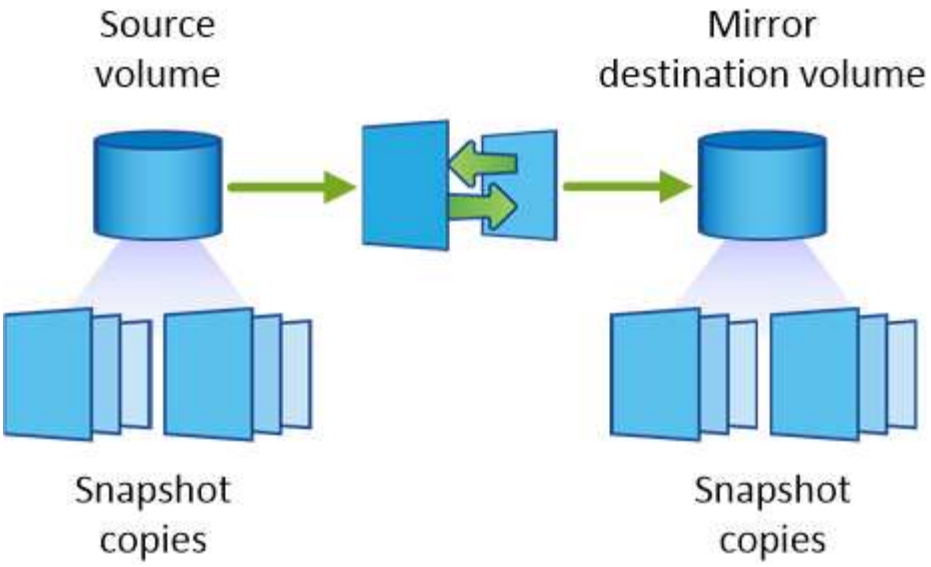
- Eine *Backup*-Richtlinie repliziert bestimmte Snapshot-Kopien zu einem Ziel-Volume und speichert diese in der Regel für einen längeren Zeitraum, als es auf dem Quell-Volume der Fall wäre.

  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.

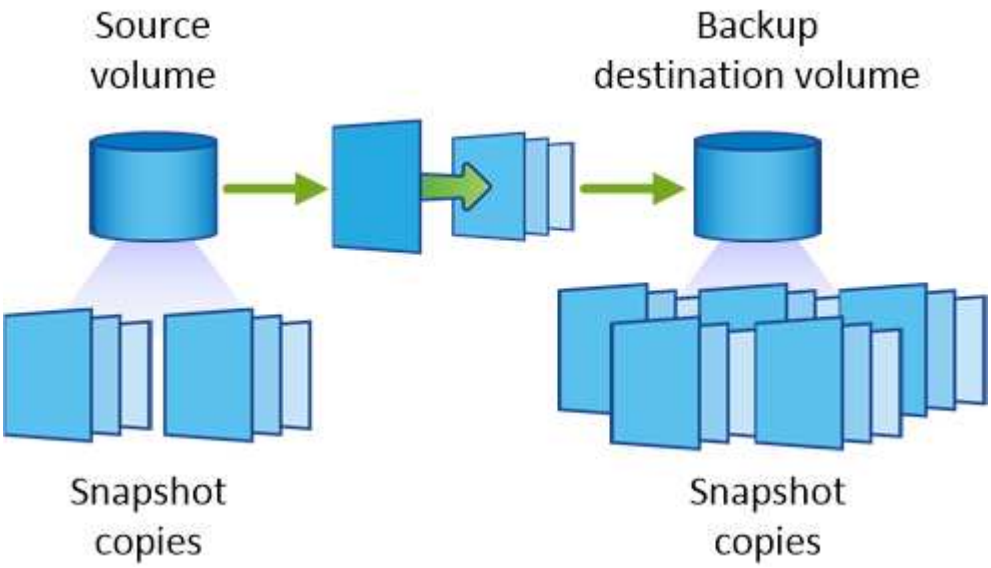
- Eine Richtlinie „ *Mirror und Backup*“ ermöglicht Disaster Recovery und langfristige Datenhaltung.

  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.

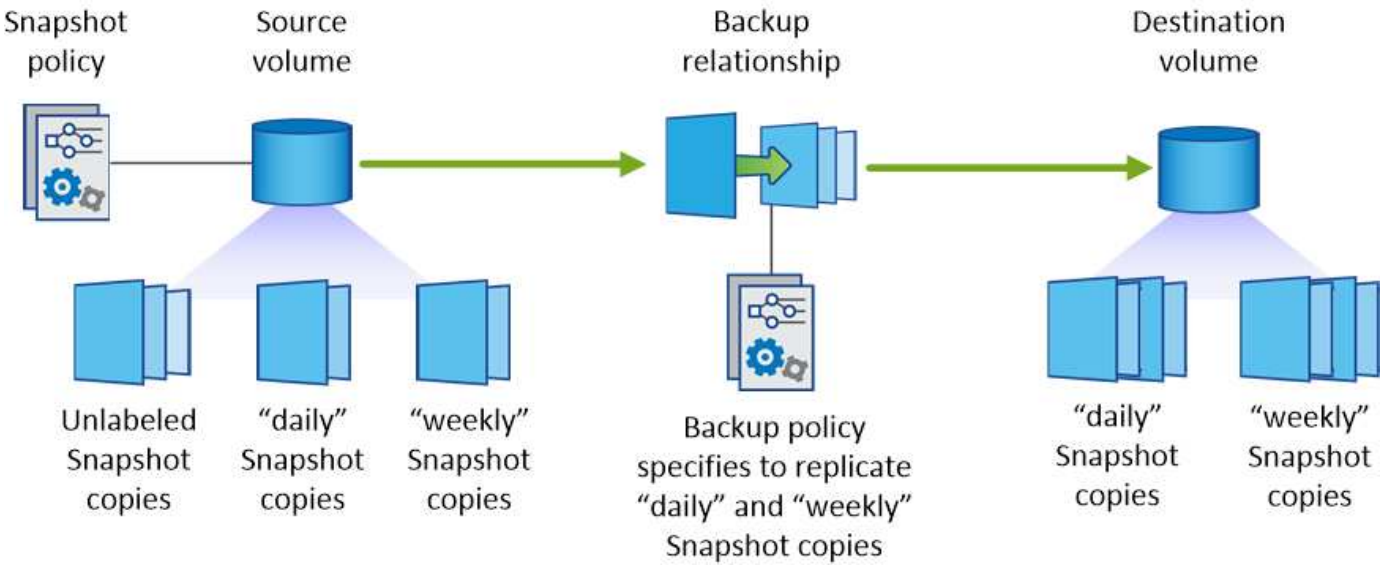
Verständnis der Beziehung zwischen Snapshot Copy Labels und Backup-Richtlinien

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.

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.

Replizierung von Daten zwischen Systemen

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.

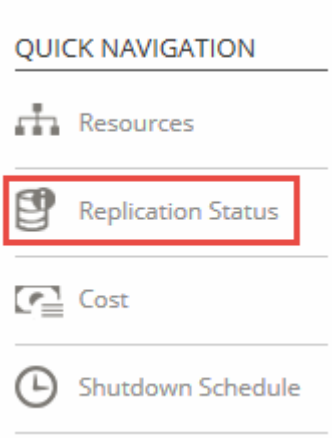
Managen von Plänen und Beziehungen zur Datenreplizierung

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 zugewiesenen Arbeitsumgebungen im Mandanten oder für eine bestimmte Arbeitsumgebung an:

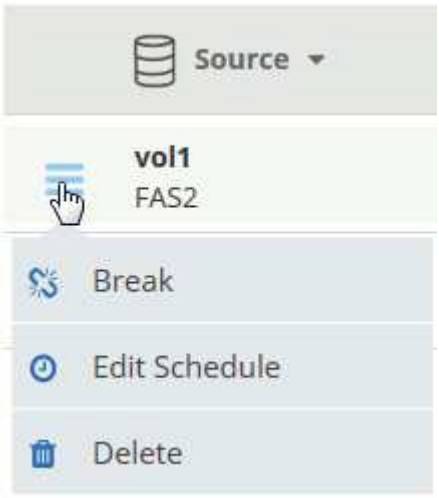
Option	Aktion
Alle zugewiesenen Arbeitsumgebungen im Mandanten	Klicken Sie in der Navigationsleiste auf Replikationsstatus.

Option	Aktion
Eine bestimmte Arbeitsumgebung	Wählen Sie die Arbeitsumgebung aus, und klicken Sie dann auf Replikationsstatus. 

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".
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.
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.

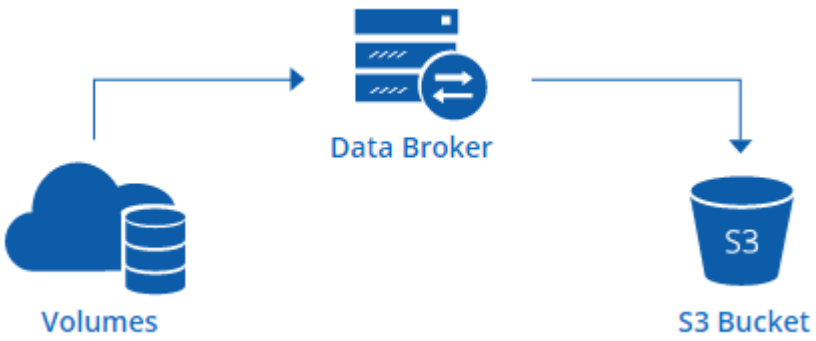
Daten werden mit AWS S3 synchronisiert

Daten von ONTAP Volumes können durch Integration einer Arbeitsumgebung mit in einen AWS 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.

Die Funktion zum Synchronisieren mit S3 ist nur für Cloud Manager Admins und Tenant Admins verfügbar.

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 über Cloud Manager mit AWS S3 synchronisieren möchten, müssen Sie die

Arbeitsumgebung in den 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.

Administration von Cloud Volumes ONTAP

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.

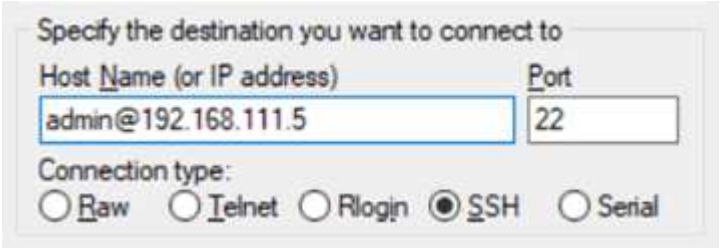
Wenn Cloud Volumes ONTAP HA in mehreren AZS implementiert wird, verwenden sie eine Floating-IP-Adresse für die Cluster-Management-Schnittstelle, was bedeutet, dass externes Routing nicht verfügbar ist. Sie müssen eine Verbindung von einem Host herstellen, der Teil derselben Routingdomäne ist.

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

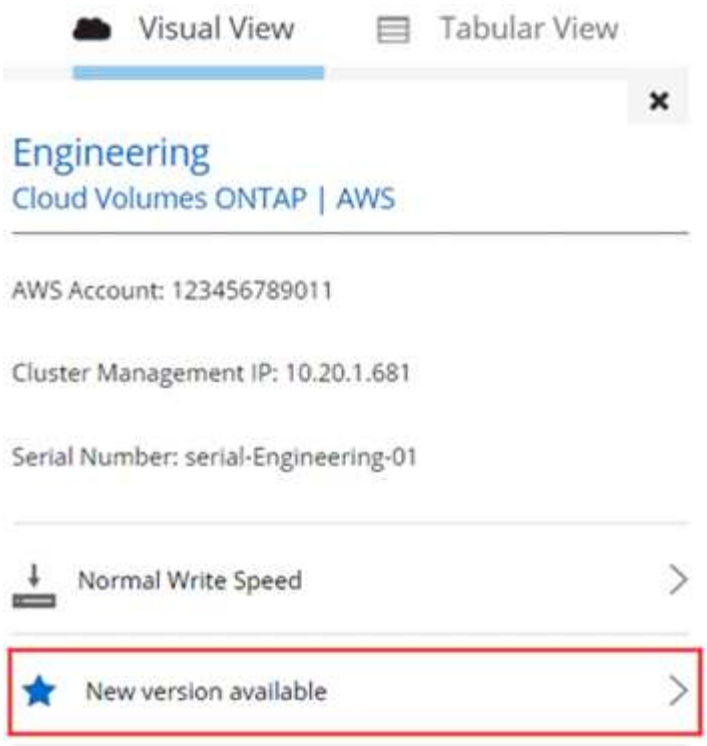
```
Password: ********
COT2::>
```

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.

Überblick

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 Upgrade von Cloud Volumes ONTAP auf die neueste Version.

Bei HA-Systemen 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
- 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.

Upgrades von HA-Paaren sind unterbrechungsfrei. Mit einem unterbrechungsfreien Upgrade werden beide Nodes in einem HA-Paar gleichzeitig aktualisiert, ohne dass der Service für die Clients aufrecht erhalten wird.

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".

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

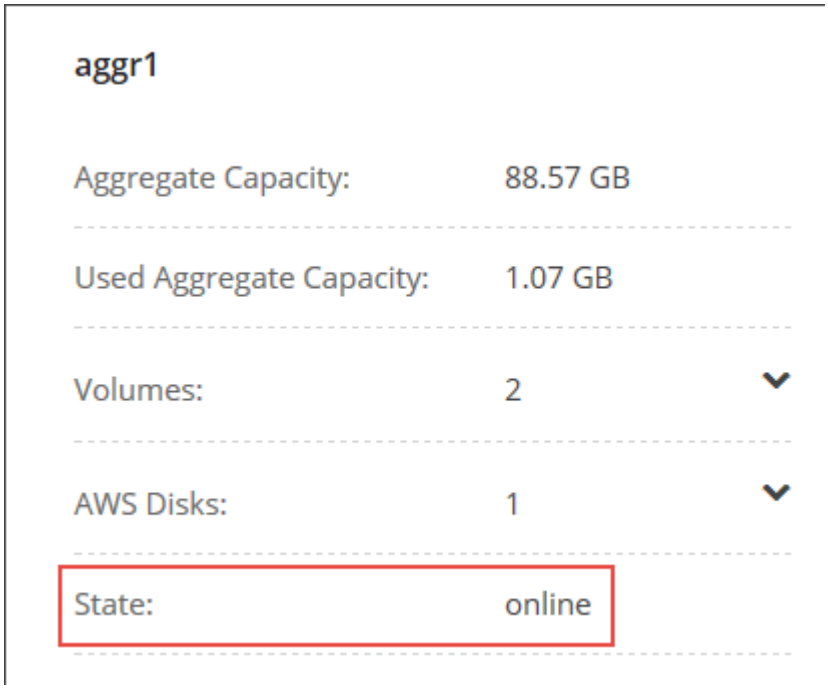
Aggregate für Cloud Volumes ONTAP muss online sein, bevor Sie die Software aktualisieren. Aggregate sollten in den meisten Konfigurationen online sein. Wenn dies nicht der Fall ist, sollten Sie sie jedoch online stellen.

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**.

Upgrade von Cloud Volumes ONTAP auf die neueste Version

Ein Upgrade auf die neueste Version von Cloud Volumes ONTAP ist direkt über Cloud Manager möglich. Cloud Manager benachrichtigt Sie, wenn eine neue Version verfügbar ist.

Bevor Sie beginnen

Cloud Manager-Vorgänge wie die Erstellung von Volumes oder Aggregaten dürfen für das Cloud Volumes ONTAP System nicht ausgeführt werden.

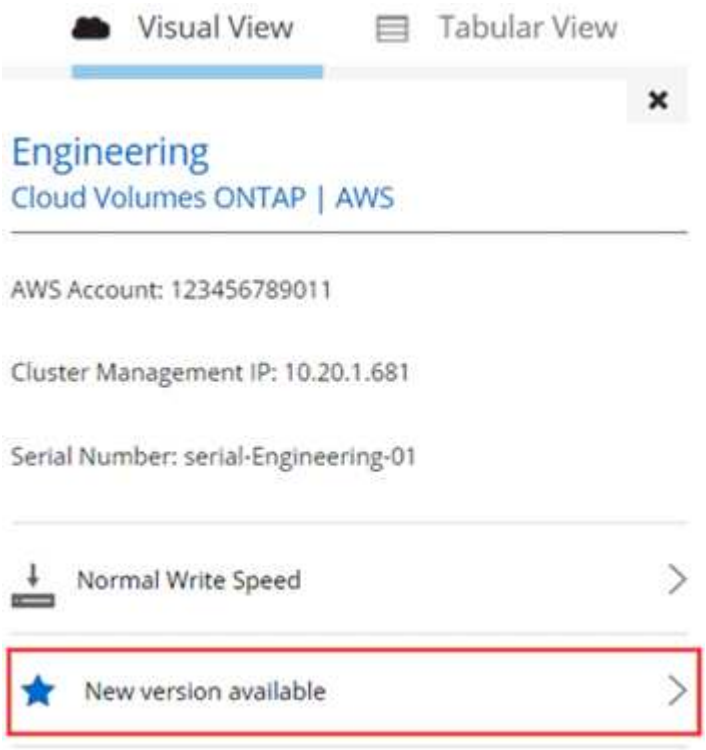
Über diese Aufgabe

- 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.
- Upgrades von HA-Paaren sind unterbrechungsfrei. Mit einem unterbrechungsfreien Upgrade werden beide Nodes in einem HA-Paar gleichzeitig aktualisiert, ohne dass der Service für die Clients aufrecht erhalten wird.

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.

Über diese Aufgabe

- 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.
- Upgrades von HA-Paaren sind unterbrechungsfrei. Mit einem unterbrechungsfreien Upgrade werden beide Nodes in einem HA-Paar gleichzeitig aktualisiert, ohne dass der Service für die Clients aufrecht erhalten

wird.

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 VPC 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 AWS ablegen.
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. Das Cloud Volumes ONTAP System ist bis zu 25 Minuten offline.

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.

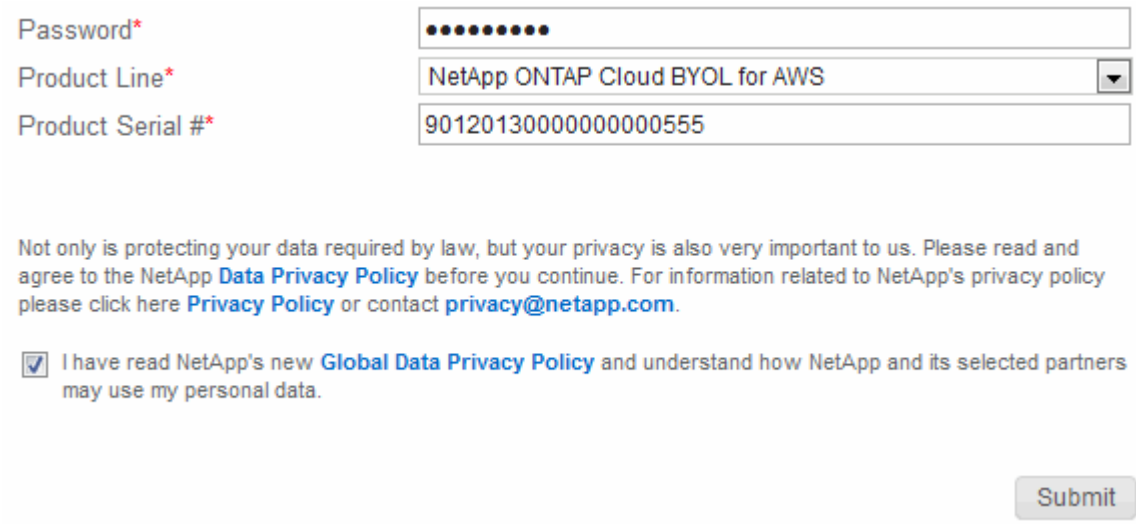
Installation von Lizenzdateien auf Cloud Volumes ONTAP Byol Systemen

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.

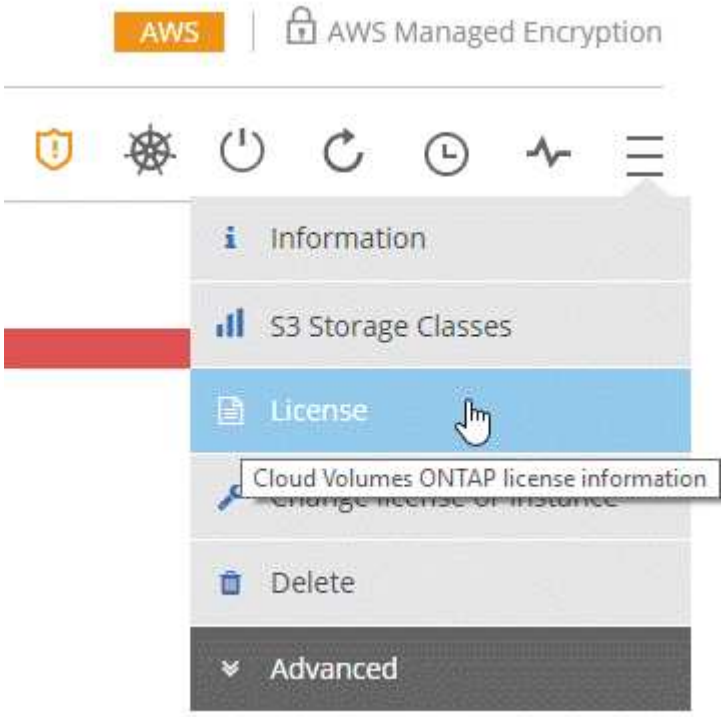
Schritte

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 (entweder **NetApp Cloud Volumes ONTAP BYOL für AWS**, **NetApp Cloud Volumes ONTAP BYOL für Azure** oder **NetApp Cloud Volumes ONTAP BYOL HA für AWS**), 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 der Instanz oder des Typs der virtuellen Maschine für Cloud Volumes ONTAP

Beim Start von Cloud Volumes ONTAP in AWS oder Azure können Sie zwischen verschiedenen Instanzen oder Virtual Machines wählen. Sie können die Instanz oder den Typ der virtuellen Maschine jederzeit ändern, wenn Sie feststellen, dass sie für Ihre Anforderungen zu klein oder zu groß ist.

Über diese Aufgabe

- 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.

- Das Ändern des Instanz- oder VM-Typs wirkt sich auf die Servicegebühren von AWS oder Azure aus.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Lizenz oder Instanz ändern** für AWS oder klicken Sie auf **Lizenz ändern oder VM** für Azure.

2. Wenn Sie eine nutzungsbasierte Konfiguration verwenden, können Sie optional eine andere Lizenz auswählen.
3. Wählen Sie einen Instanztyp oder einen virtuellen 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. Durch das Ändern der Lizenz wird die Rohkapazitätsgrenze erhöht oder verringert und Sie können zwischen verschiedenen EC2-Instanztypen oder Azure Virtual Machine-Typen 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.

- Das Ändern des Instanz- oder VM-Typs wirkt sich auf die Servicegebühren von AWS oder Azure aus.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Lizenz oder Instanz ändern** für AWS oder klicken Sie auf **Lizenz ändern oder VM** für Azure.
2. Wählen Sie einen Lizenztyp und einen Instanztyp oder einen virtuellen 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 startet neu mit der neuen Lizenz, dem Instanztyp oder dem Typ der virtuellen Maschine oder beides.

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"

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

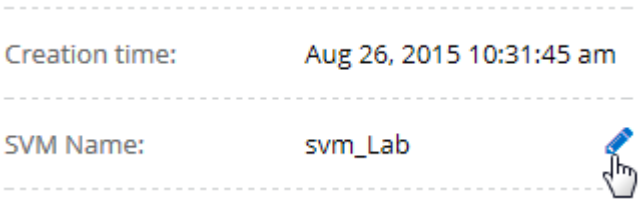
Arbeitsumgebung wird gelöscht".

Ändern des 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.

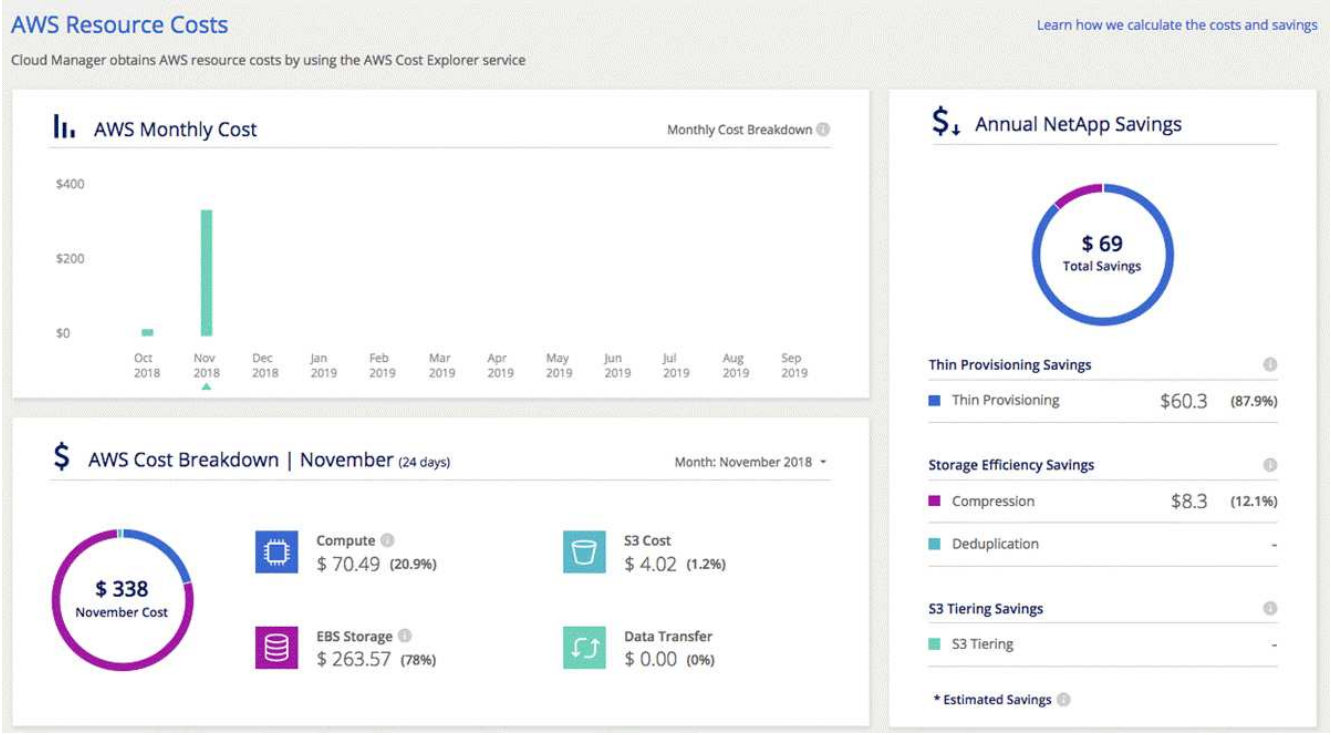
   b. "Aktivieren Sie das Tag **WorkingEnvironment ID**".

      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:

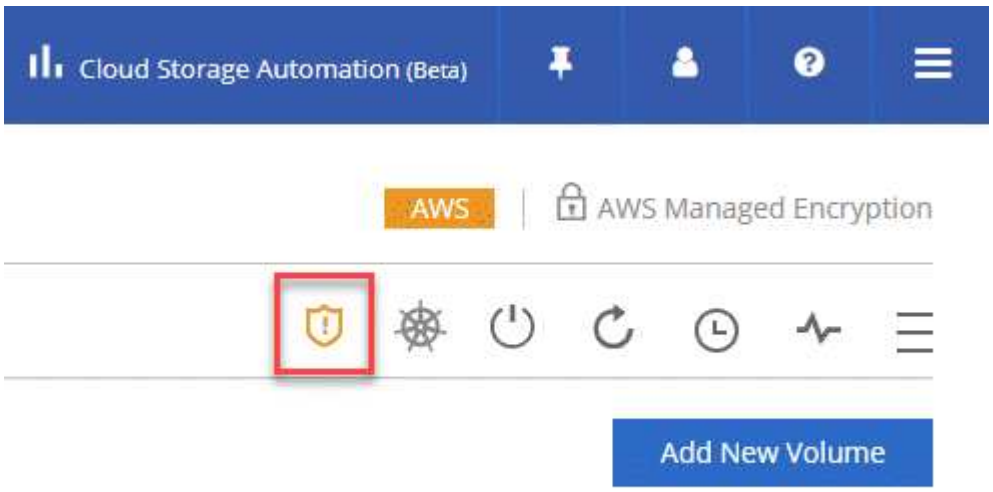


Besserer Schutz gegen Ransomware

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**.



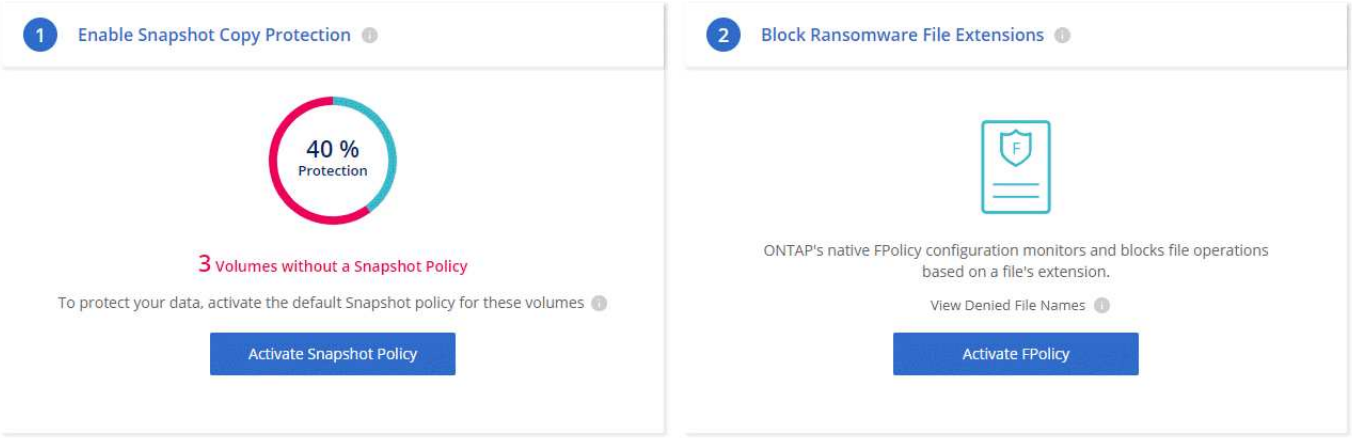
2. Implementierung der NetApp Lösung für Ransomware:
   a. Klicken Sie auf **Snapshot-Richtlinie aktivieren**, wenn Volumes ohne Snapshot-Richtlinie aktiviert

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. Dies könnte der Fall sein, wenn Ihr Cloud Manager-System unbrauchbar wurde und Sie ein neues System gestartet haben. Sie konnten jedoch nicht alle Cloud Volumes ONTAP Systeme aus einem kürzlich durchgeführten Cloud Manager Backup wiederherstellen.

Bevor Sie beginnen

Sie müssen das Kennwort für das Cloud Volumes ONTAP Admin-Benutzerkonto kennen.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen**.
2. Wählen Sie unter Entdecken **Cloud Volumes ONTAP** aus.

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 dem Mandanten die Cloud Volumes ONTAP Instanzen hinzu.

Löschen einer Cloud Volumes ONTAP Arbeitsumgebung

Am besten löschen Sie Cloud Volumes ONTAP Systeme aus Cloud Manager und nicht aus AWS oder Azure. Wenn Sie beispielsweise eine lizenzierte Cloud Volumes ONTAP Instanz von AWS beenden, können Sie den Lizenzschlüssel nicht für eine andere Instanz 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.

Administration 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 die Dropdown-Liste Task, und wählen Sie dann **Einstellungen** aus.
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

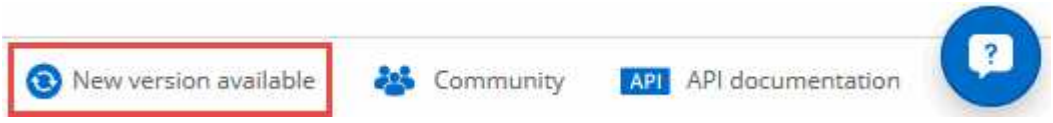
Sie sollten die Prüfung durchgeführt haben "Neuerungen in dieser Version" Um neue Anforderungen und Änderungen im Support zu ermitteln.

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**:
   a. Behalten Sie die Option zum Herunterladen eines Backups bei, da Sie es bei Bedarf zur Wiederherstellung Ihrer Cloud Manager-Konfiguration verwenden können.
   b. Lesen Sie die Geschäftsbedingungen und aktivieren Sie dann das Kontrollkästchen **Ich habe die Bedingungen gelesen und genehmigt (EULA)**.
6. Wenn Sie dazu aufgefordert werden, speichern Sie das Cloud Manager-Backup.

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 in der oberen rechten Ecke der Cloud Manager-Konsole auf die Dropdown-Liste Task und wählen Sie dann **Update** aus.
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**:
   a. Behalten Sie die Option zum Herunterladen eines Backups aktiviert bei, da Sie es bei Bedarf zur Wiederherstellung Ihrer Cloud Manager-Konfiguration verwenden können.
   b. Lesen Sie die Geschäftsbedingungen und aktivieren Sie dann das Kontrollkästchen **Ich habe die Bedingungen gelesen und genehmigt (EULA)**.
4. Wählen Sie den bereitgestellten Patch aus.
5. Wenn Sie dazu aufgefordert werden, speichern Sie das Cloud Manager-Backup.

Ergebnis

Cloud Manager wendet den Patch an. Sie können sich nach einigen Minuten bei der Konsole anmelden.

Backup und Wiederherstellung von Cloud Manager

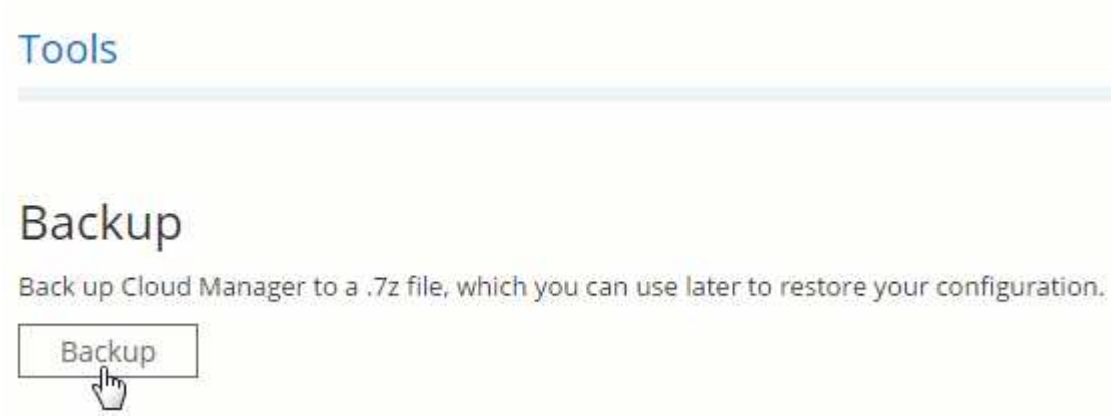
Mit Cloud Manager können Sie die Datenbank sichern und wiederherstellen, um Ihre Konfiguration zu schützen und Probleme zu beheben.

Backup von Cloud Manager

Es empfiehlt sich, die Cloud Manager-Datenbank regelmäßig zu sichern. Bei Problemen können Sie Cloud Manager aus einem früheren Backup wiederherstellen.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf die Dropdown-Liste Task, und wählen Sie dann **Tools** aus.
2. Klicken Sie Auf **Backup**.



3. Wenn Sie dazu aufgefordert werden, speichern Sie die Sicherungsdatei an einem sicheren Speicherort, damit Sie sie bei Bedarf abrufen können.

Wiederherstellen von Cloud Manager aus einem Backup

Durch die Wiederherstellung von Cloud Manager aus einem Backup werden vorhandene Daten durch die Daten aus dem Backup ersetzt.

Schritte

1. Klicken Sie in der oberen rechten Ecke der Cloud Manager-Konsole auf die Dropdown-Liste Task und wählen Sie dann **Tools** aus.
2. Klicken Sie Auf **Wiederherstellen**.
3. Klicken Sie zur Bestätigung auf **OK**.
4. Wählen Sie das Backup aus.

Ergebnis

Cloud Manager stellt die Datenbank aus der Sicherungsdatei wieder her.

Entfernen von Cloud Volumes ONTAP Arbeitsumgebungen

Der Cloud Manager Admin kann eine Cloud Volumes ONTAP Arbeitsumgebung entfernen, um sie auf ein anderes System zu verschieben oder Erkennungsprobleme zu beheben.

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:

- Entdecken Sie es in einem anderen Mandanten erneut

- 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 in der oberen rechten Ecke der Cloud Manager-Konsole auf die Dropdown-Liste Task und wählen Sie dann **Tools** aus.
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.

Bearbeiten von Benutzerkonten

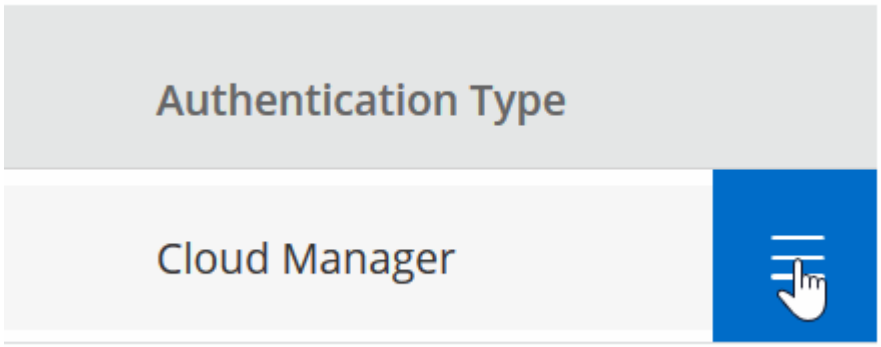
Sie können Benutzerkonten in Cloud Manager ändern, indem Sie den Benachrichtigungsbericht aktivieren und deaktivieren.

Über diese Aufgabe

Kennwort und Benutzerinformationen müssen in geändert werden "NetApp Cloud Central".

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Benutzersymbol und wählen Sie dann **Benutzer anzeigen** aus.
2. Wählen Sie das Menüsymbol am Ende der Zeile aus und klicken Sie auf **Benutzer bearbeiten**.



3. Ändern Sie auf der Seite Benutzereinstellungen das Benutzerkonto.

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 in der oberen rechten Ecke der Cloud Manager-Konsole auf die Dropdown-Liste Task, und wählen Sie dann **Einstellungen** aus.
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 die Dropdown-Liste Task, und wählen Sie dann **HTTPS-Setup** aus.

   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 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. Wenn Sie Cloud Manager neu installieren möchten, sichern Sie die Datenbank, bevor Sie die Software deinstallieren:
   a. Klicken Sie in der oberen rechten Ecke der Cloud Manager-Konsole auf die Dropdown-Liste Task und wählen Sie dann **Tools** aus.
   b. Klicken Sie auf **Backup** und speichern Sie die Sicherungsdatei auf Ihrem lokalen Rechner.
2. 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.

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

Bei einem Upgrade auf Cloud Manager 3.5 wählt NetApp bestimmte Cloud Manager-Systeme zur Integration in NetApp Cloud Central aus, sofern diese noch nicht 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 auf die Cloud Manager-Webkonsole
HTTPS	443	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.

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
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

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.

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Cloud Manager-Host
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 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
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 Single-Node-Systeme

Priorität	Name	Port	Protokoll	Quelle	Ziel	Aktion	Beschreibung
1000	Inbound_SSH	22	TCP	Alle	Alle	Zulassen	SSH-Zugriff auf die IP-Adresse der Cluster Management LIF oder einer Node Management LIF
1001	Eingehend_http	80	TCP	Alle	Alle	Zulassen	HTTP-Zugriff auf die System Manager Webkonsole mit der IP-Adresse der Cluster-Management-LIF
1002	Inbound_111_tcp	111	TCP	Alle	Alle	Zulassen	Remote-Prozeduraufruf für NFS
1003	Eingehend_111_udp	111	UDP	Alle	Alle	Zulassen	Remote-Prozeduraufruf für NFS
1004	Eingehend_139	139	TCP	Alle	Alle	Zulassen	NetBIOS-Servicesitzung für CIFS
1005	Inbound_161-162_tcp	161-162	TCP	Alle	Alle	Zulassen	Einfaches Netzwerkverwaltungsprotokoll
1006	Inbound_161-162_udp	161-162	UDP	Alle	Alle	Zulassen	Einfaches Netzwerkverwaltungsprotokoll
1007	Eingehend_443	443	TCP	Alle	Alle	Zulassen	HTTPS-Zugriff auf die System Manager-Webkonsole unter Verwendung der IP-Adresse der Cluster-Management-LIF
1008	Eingehend_445	445	TCP	Alle	Alle	Zulassen	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
1009	Inbound_635_tcp	635	TCP	Alle	Alle	Zulassen	NFS-Mount
1010	Eingehend_635_udp	635	TCP	Alle	Alle	Zulassen	NFS-Mount
1011	Eingehend_749	749	TCP	Alle	Alle	Zulassen	Kerberos
1012	Inbound_2049_tcp	2049	TCP	Alle	Alle	Zulassen	NFS-Server-Daemon
1013	Eingehend_2049_udp	2049	UDP	Alle	Alle	Zulassen	NFS-Server-Daemon

Priorität	Name	Port	Protokoll	Quelle	Ziel	Aktion	Beschreibung
1014	Eingehend_3260	3260	TCP	Alle	Alle	Zulassen	ISCSI-Zugriff über die iSCSI-Daten-LIF
1015	Inbound_4045-4046_tcp	4045-4046	TCP	Alle	Alle	Zulassen	NFS Lock Daemon und Network Status Monitor
1016	Inbound_4045-4046_udp	4045-4046	UDP	Alle	Alle	Zulassen	NFS Lock Daemon und Network Status Monitor
1017	Eingehend_10000	10.000	TCP	Alle	Alle	Zulassen	Backup mit NDMP
1018	Eingehend_11104-11105	11104-11105	TCP	Alle	Alle	Zulassen	SnapMirror Datenübertragung
3000	Inbound_Deny_all_tcp	Alle	TCP	Alle	Alle	Ablehnen	Blockieren Sie den gesamten anderen TCP-eingehenden Datenverkehr
3001	Inbound_Deny_all_udp	Alle	UDP	Alle	Alle	Ablehnen	Alle anderen UDP-eingehenden Datenverkehr blockieren
65000	AllowVnetInBound	Alle	Alle	VirtualNetwork	VirtualNetwork	Zulassen	Eingehender Verkehr aus dem vnet
65001	AllowAzureLoad BalancerInBound	Alle	Alle	AzureLoadBalancer	Alle	Zulassen	Datenverkehr vom Azure Standard Load Balancer
65500	DenyAllInBound	Alle	Alle	Alle	Alle	Ablehnen	Alle anderen eingehenden Datenverkehr blockieren

Eingehende Regeln für HA-Systeme

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	Name	Port	Protokoll	Quelle	Ziel	Aktion	Beschreibung
100	Eingehend_443	443	Alle	Alle	Alle	Zulassen	HTTPS-Zugriff auf die System Manager-Webkonsole unter Verwendung der IP-Adresse der Cluster-Management-LIF
101	Inbound_111_tcp	111	Alle	Alle	Alle	Zulassen	Remote-Prozeduraufruf für NFS
102	Inbound_2049_tcp	2049	Alle	Alle	Alle	Zulassen	NFS-Server-Daemon

Priorität	Name	Port	Protokoll	Quelle	Ziel	Aktion	Beschreibung
111	Inbound_SSH	22	Alle	Alle	Alle	Zulassen	SSH-Zugriff auf die IP-Adresse der Cluster Management LIF oder einer Node Management LIF
121	Eingehend_53	53	Alle	Alle	Alle	Zulassen	DNS und CIFS
65000	AllowVnetInBound	Alle	Alle	VirtualNetwork	VirtualNetwork	Zulassen	Eingehender Verkehr aus dem vnet
65001	AllowAzureLoad BalancerInBound	Alle	Alle	AzureLoadBalancer	Alle	Zulassen	Datenverkehr vom Azure Standard Load Balancer
65500	DenyAllInBound	Alle	Alle	Alle	Alle	Ablehnen	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.

Protokoll	Port	Zweck
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)
DHCP	UDP	68	Node Management-LIF	DHCP	DHCP-Client für die erstmalige Einrichtung
DHCPS	UDP	67	Node Management-LIF	DHCP	DHCP-Server

Service	Protokoll	Port	Quelle	Ziel	Zweck
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- und Azure-Berechtigungen für Cloud Manager

Cloud Manager benötigt Berechtigungen, um Aktionen in AWS und Azure in Ihrem Namen auszuführen. 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.
"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.

Aktionen	Zweck
„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

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 über NetApp Cloud Central (oder direkt über den AWS Marketplace oder Azure Marketplace) bereitgestellt haben, beachten Sie Folgendes:
  - In AWS lautet der Benutzername für die EC2 Linux-Instanz ec2-user.
  - Für AWS und Azure ist das Betriebssystem für das Cloud Manager-Image 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 und als HA-Paar in AWS und Azure verfügbar.

- Cloud Manager erstellt bei der Implementierung von Cloud Volumes ONTAP eine Data Serving SVM. Sie können zwar über System Manager oder die CLI eine weitere SVM mit Datenbereitstellung erstellen, jedoch wird die Verwendung mehrerer SVMs mit Datenbereitstellung nicht unterstützt.
- Standardmäßig werden mehrere Netzwerkschnittstellen erstellt:
  - Eine Cluster Management-LIF
  - Eine Intercluster-LIF
  - 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 Cloud Manager Admin 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

- Eine bereitgestellte IOPS SSD-Festplatte für Cloud Volumes ONTAP Boot-Daten, die ca. 45 GB und 1.250 Piops betragen
- Eine universelle SSD-Festplatte für Cloud Volumes ONTAP Root-Daten mit ca. 140 GB
- Ein EBS-Snapshot für jede Boot- und Root-Festplatte

In einem HA-Paar replizieren beide Cloud Volumes ONTAP Nodes ihre Root-Festplatte auf den Partner-Node.

Azure

- Eine Premium Storage SSD-Festplatte für Cloud Volumes ONTAP Bootdaten, die ca. 73 GB betragen
- Eine Premium Storage SSD-Festplatte für Cloud Volumes ONTAP Root-Daten, die ca. 140 GB betragen
- Ein Azure Snapshot für jedes Boot- und Root-Laufwerk

Wo sich die Festplatten befinden

Cloud Manager legt den Storage von AWS und Azure wie folgt fest:

- Startdaten befinden sich auf einer Festplatte, die mit der EC2-Instanz oder der Azure 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.

Benutzerrollen

Jedem Cloud Manager-Benutzerkonto wird eine Rolle zugewiesen, die Berechtigungen definiert.

Aufgabe	Cloud Manager Admin	Mandantenverwaltung	Administrator der Arbeitsumgebung
Verwalten von Mandanten	Ja.	Nein	Nein
Verwalten von Arbeitsumgebungen	Ja.	Ja, für den zugewiesenen Mandanten	Ja, für zugewiesene Arbeitsumgebungen
Integrieren Sie eine Arbeitsumgebung in Cloud Sync	Ja.	Ja.	Nein
Anzeigen des Status der Datenreplizierung	Ja.	Ja, für den zugewiesenen Mandanten	Ja, für zugewiesene Arbeitsumgebungen
Zeitachse anzeigen	Ja.	Ja.	Ja.
Erstellen und Löschen von Benutzerkonten	Ja.	Ja, für den zugewiesenen Mandanten	Nein

Aufgabe	Cloud Manager Admin	Mandantenverwaltung	Administrator der Arbeitsumgebung
Benutzerkonten ändern	Ja.	Ja, für den zugewiesenen Mandanten	Ja, für ihren eigenen Account
Kontoeinstellungen verwalten	Ja.	Nein	Nein
Einrichtung Von Kubernetes	Ja.	Nein	Nein
Wechseln Sie zwischen der Storage System View und der Volume View	Ja.	Nein	Nein
Einstellungen ändern	Ja.	Nein	Nein
Anzeigen und Verwalten des Support-Dashboards	Ja.	Nein	Nein
Backup und Wiederherstellung von Cloud Manager	Ja.	Nein	Nein
Entfernen Sie eine Arbeitsumgebung	Ja.	Nein	Nein
Aktualisieren Sie Cloud Manager	Ja.	Nein	Nein
Installieren Sie ein HTTPS-Zertifikat	Ja.	Nein	Nein
Einrichten von Active Directory	Ja.	Nein	Nein
Aktivieren Sie den Cloud Storage Automation Report	Ja.	Nein	Nein

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"

  Sehen Sie sich Videos an, die Ihnen zeigen, wie Sie Cloud Volumes ONTAP in AWS und Azure implementieren und managen und wie Sie Daten in Ihrer Hybrid Cloud replizieren können.

- "Richtlinien für Cloud Manager"

  Laden Sie JSON-Dateien herunter, die die Berechtigungen enthalten, die Cloud Manager zum Ausführen von Aktionen in AWS und Azure 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"
- 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"
- "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.
- "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.

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

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.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

- "Hinweis zu OnCommand Cloud Manager 3.6.6"
- "Hinweis zu OnCommand Cloud Manager 3.6.1"
- "Hinweis zu OnCommand Cloud Manager 3.6"

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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