Cloud Manager und Cloud Volumes ONTAP Dokumentation

Cloud Manager 3.8

NetApp
March 25, 2024

Inhalt

Cloud Manager und Cloud Volumes ONTAP Dokumentation

Cloud Manager ist IT-Experten und Cloud-Architekten in der Lage, ihre Hybrid-Multi-Cloud-Infrastruktur mithilfe der Cloud-Lösungen von NetApp zentral zu managen.

BlueXP

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

"Rufen Sie die BlueXP Dokumentation auf"

Entdecken Sie die Neuigkeiten

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

Los geht's

- "Cloud Manager"
- "Kontoeinstellungen"
- "Cloud Volumes ONTAP für AWS"
- "Cloud Volumes ONTAP für Azure"
- "Cloud Volumes ONTAP für Google Cloud"
- "Azure NetApp Dateien"
- "Cloud Volumes Service für AWS"
- "Cloud Volumes Service für Google Cloud"
- "Cloud-Compliance"
- "Globaler Datei-Cache"
- "Backup in die Cloud"
- "Einblicke in die Cloud"

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 3.8

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

Suchen Sie nach einer früheren Version?"Neuerungen in 3.7"
"Neuerungen in 3.6"
"Neuerungen in 3.5"

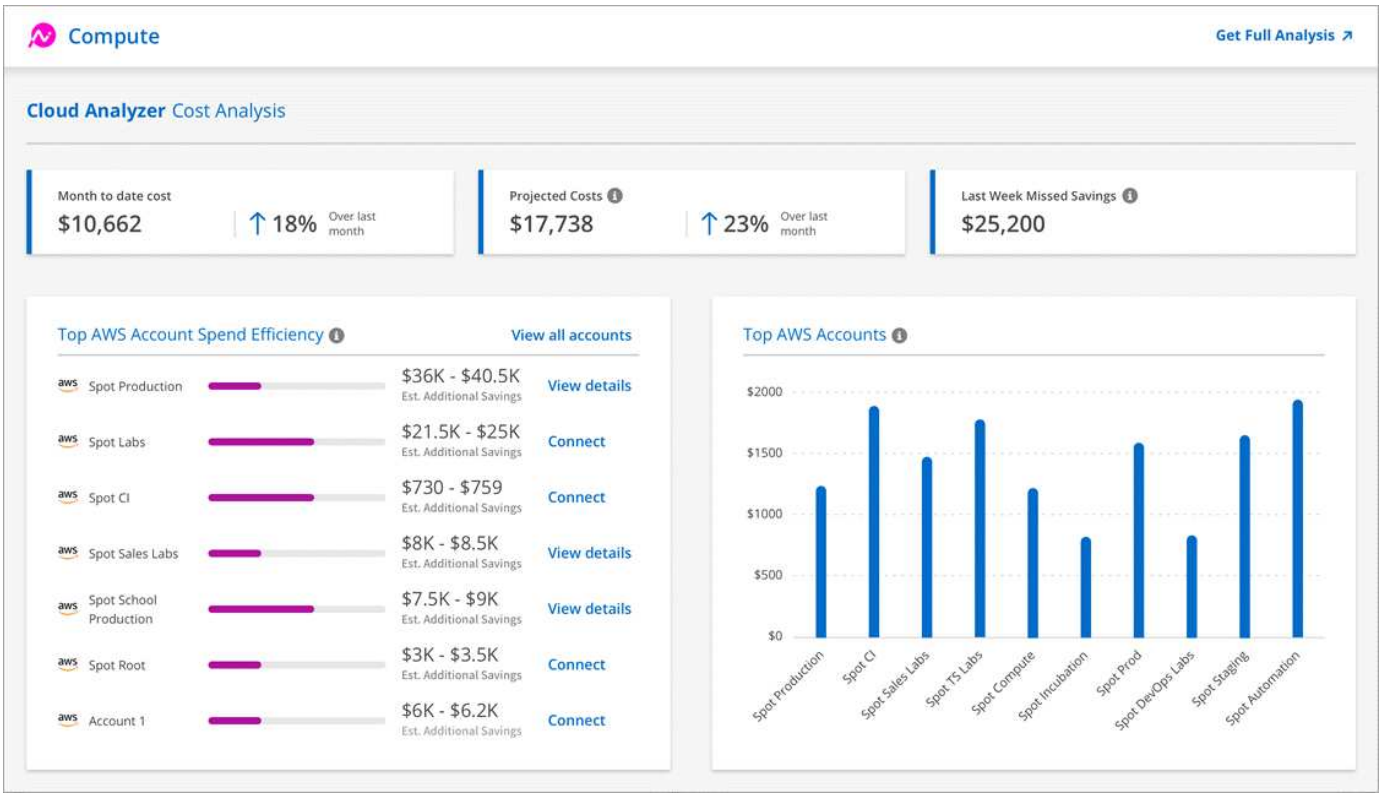
Neuer Terraform-Provider (19. Oktober 2020)

Wir haben einen neuen Terraform-Provider entwickelt, mit dem DevOps-Teams Cloud Volumes ONTAP mit Cloud Manager automatisieren und in Infrastruktur-als-Code integrieren können.

"Hier sehen Sie den netapp Cloud Manager Provider".

Update zu Cloud Manager 3.8.9 (18. Oktober 2020)

Durch den Einsatz "Spot's Cloud Analyzer", Cloud Manager bietet jetzt eine allgemeine Kostenanalyse Ihrer Cloud-Computing-Ausgaben und zeigt potenzielle Einsparungen auf. Diese Informationen erhalten Sie im **Compute** Service in Cloud Manager. "Weitere Informationen .".



Update zu Cloud Manager 3.8.9 (13. Oktober 2020)

Wir haben zwei Cloud Tiering Updates veröffentlicht:

- Lizenzierung für Cloud Tiering ist jetzt bei Cloud Manager erhältlich.

  Sie bezahlen für Daten-Tiering von einem ONTAP Cluster vor Ort in die Cloud über ein Pay-as-you-go-Abonnement, eine ONTAP-Tiering-Lizenz namens *FabricPool* oder eine Kombination beider Optionen.

- Der Standalone-Service Cloud Tiering wurde außer Betrieb genommen. Sie sollten jetzt direkt über Cloud Manager auf Cloud Tiering zugreifen, wo alle gleichen Funktionen verfügbar sind.

Cloud Manager 3.8.9 (4. Okt. 2020)

- Verbesserungen bei Cloud Compliance
- Verbesserungen von Cloud Volumes Service für AWS
- Cloud Sync Integration
- Verbesserungen beim Account-Management
- Änderungen für Regierungsregionen

Verbesserungen bei Cloud Compliance

- Eine neue **Cloud Compliance Viewer**-Rolle steht in Cloud Manager zur Verfügung.

  Benutzer, denen diese Rolle zugewiesen ist, können nur Compliance-Informationen anzeigen und Berichte für Arbeitsbereiche erstellen, auf die sie zugreifen können. Sie können Cloud Compliance-Einstellungen nicht managen und haben keinen Zugriff auf andere Funktionen und Services von Cloud Manager. Dies ist möglicherweise die perfekte Rolle für Ihre Rechtsabteilung, um die Ergebnisse von Cloud Compliance-Scans zu überwachen. Siehe "Benutzerrollen" Entsprechende Details.

- Unterstützung zum Scannen von MongoDB und PostgreSQL-Datenbankschemas hinzugefügt. Siehe "Datenbankschemas werden gescannt" Finden Sie weitere Informationen.
- Die Preise für Cloud-Compliance ändern sich ab dem 7. Oktober.

  Es sind die ersten 1 TB an Daten, die Cloud Compliance in einem Cloud Manager Workspace scannt, kostenlos. Dazu gehören Daten von Cloud Volumes ONTAP Volumes, Azure NetApp Files Volumes, Amazon S3 Buckets und Datenbank-Schemas. Um zusätzliche Daten nach Erreichen von 1 TB zu scannen, ist ein Abonnement erforderlich. Siehe "Preisgestaltung" Entsprechende Details.

Verbesserungen von Cloud Volumes Service für AWS

Wenn ein neues Volume erstellt wird, können Sie dieses Volume auf einer vorhandenen Snapshot-Kopie eines anderen Volume basieren.

Cloud Sync Integration

Der NetApp Cloud Sync Service ist jetzt über Cloud Manager verfügbar. Cloud Sync bietet eine einfache, sichere und automatisierte Möglichkeit, Ihre Daten von einem beliebigen Quellziel zu einem beliebigen Zielziel, in der Cloud oder vor Ort zu migrieren. "Weitere Informationen .".

Verbesserungen beim Account-Management

Wir haben weitere Möglichkeiten zur Verwaltung Ihres Kontos hinzugefügt.

- Eine Übersicht über die Ressourcen Ihres Accounts finden Sie jetzt.

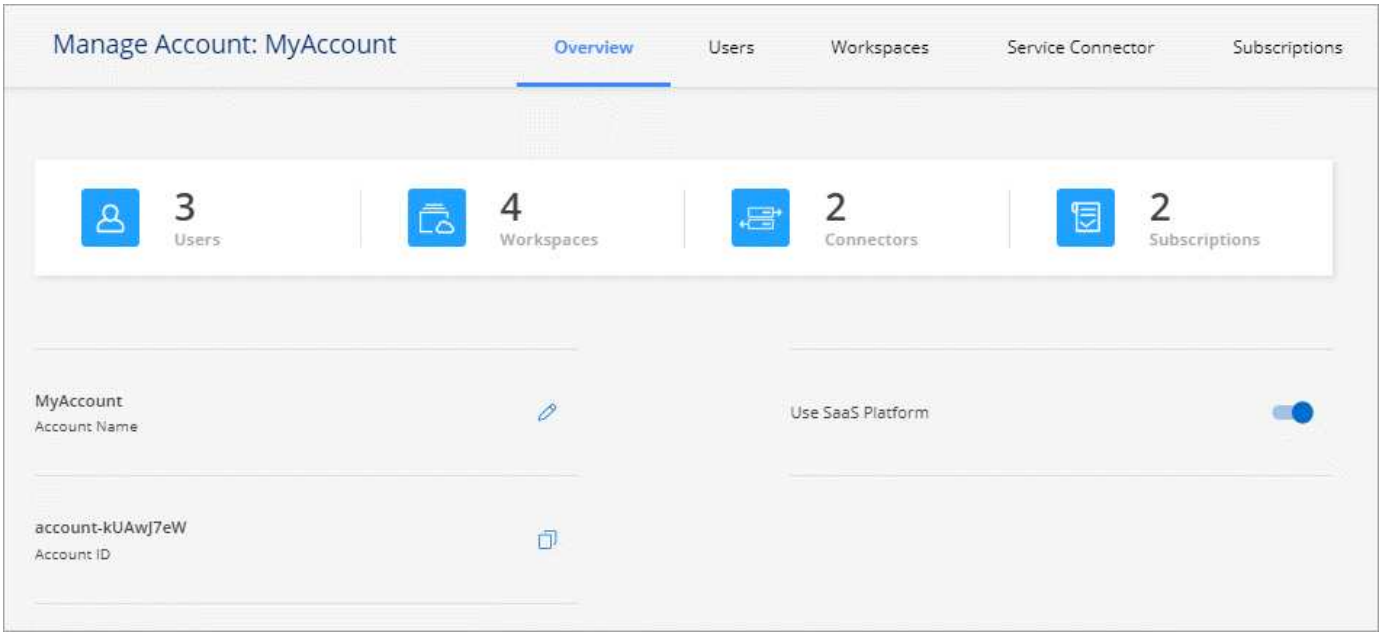
  Sie können schnell die Anzahl der Benutzer, Arbeitsbereiche, Anschlüsse und Abonnements in Ihrem Konto anzeigen.

- Sie können den Namen Ihres Kontos ändern.
- Sie können Ihre Konto-ID, die Workspace-ID oder die Konnektor-ID kopieren.

  Das Kopieren dieser IDs hilft bei den von uns geplanten Automatisierungsfunktionen.

- Sie können die Verwendung der SaaS-Plattform deaktivieren.

  Wir empfehlen, die SaaS-Plattform nur zu deaktivieren, wenn Sie zur Einhaltung der Sicherheitsrichtlinien Ihres Unternehmens erforderlich sind. Die Deaktivierung der SaaS-Plattform schränkt Ihre Möglichkeiten zur Nutzung der integrierten Cloud-Services von NetApp ein. "Weitere Informationen .".



Änderungen für Regierungsregionen

Wenn Sie einen Connector in einer AWS GovCloud Region, einer Azure Gov-Region oder einer Azure DoD-Region implementieren, steht der Zugriff auf Cloud Manager jetzt nur über die Host-IP-Adresse eines Connectors zur Verfügung. Der Zugriff auf die SaaS-Plattform ist für das gesamte Konto deaktiviert.

Das bedeutet, dass nur privilegierte Benutzer, die auf die interne VPC/vnet des Endbenutzers zugreifen können, die UI oder die API von Cloud Manager verwenden können.

"Erfahren Sie mehr über diese Einschränkung".

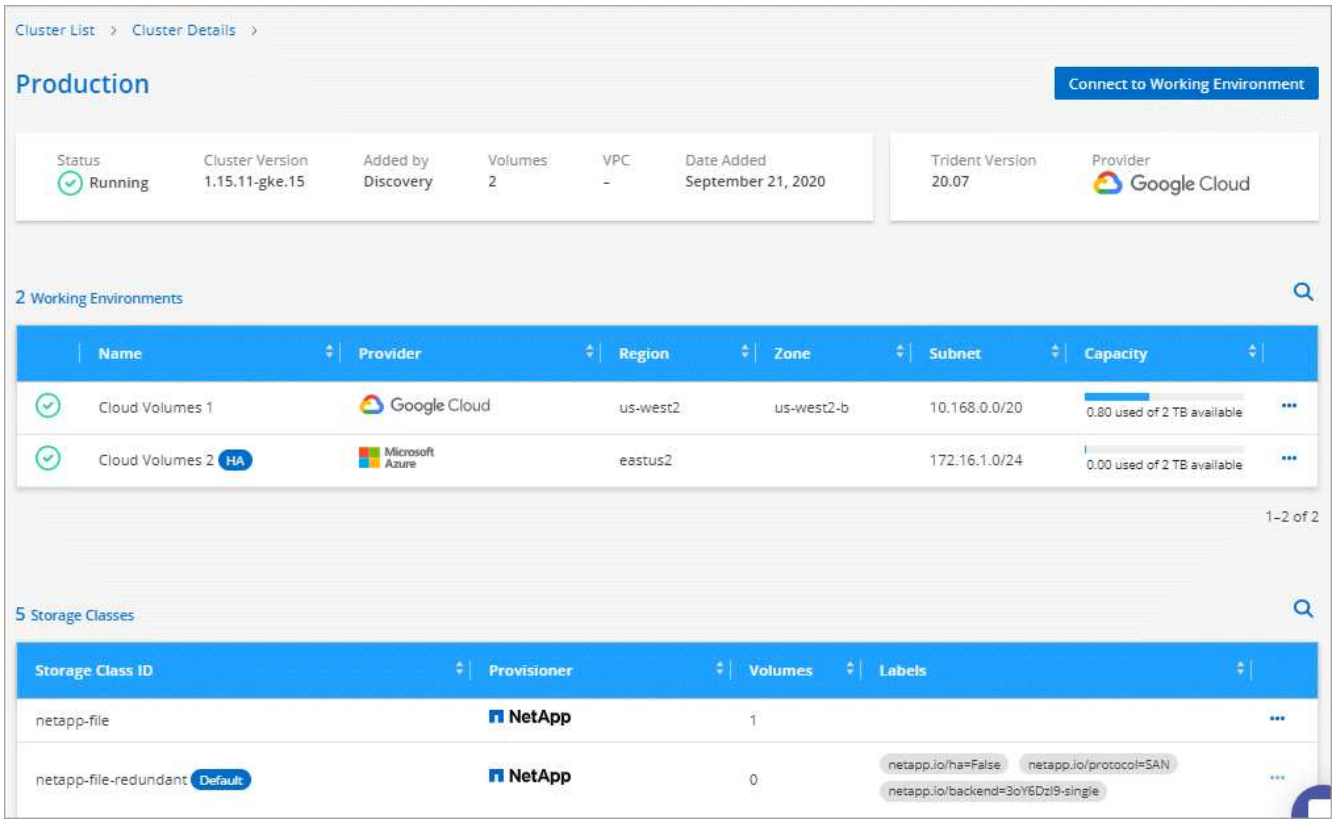
Update für Cloud Manager 3.8.8 (22. Sept. 2020)

Wir haben den Kubernetes-Service erweitert, um die Verwendung zu vereinfachen und zusätzliche Funktionen zur Verfügung zu stellen:

- Es ist einfacher, die Kubernetes-Cluster zu erkennen, die im Managed Kubernetes Service Ihres Cloud-Providers ausgeführt werden.

  Klicken Sie einfach auf **Discover Clusters** und Cloud Manager entdeckt Ihre verwalteten Cluster mit den von Ihnen bereits bereitgestellten Cloud-Provider-Berechtigungen.

- Sie können jetzt weitere Informationen zu einem erkannten Kubernetes Cluster anzeigen, einschließlich des Zustands, der Anzahl der Volumes, der Storage-Klassen und mehr.



- Wir haben eine Ressourcen- und Fehlerprüfung hinzugefügt, um sicherzustellen, dass die Kommunikation zwischen dem Cluster und dem Cloud Volumes ONTAP verfügbar ist. Falls nicht, lassen wir Sie es wissen.

"Erste Schritte".

Beachten Sie, dass das Service-Konto für einen Connector die folgenden Berechtigungen benötigt, um Kubernetes-Cluster zu ermitteln und zu managen, die in der Google Kubernetes Engine (GKE) ausgeführt werden:

```
- container.*
```

Update für Cloud Manager 3.8.8 (10. Sept. 2020)

Bei der Implementierung von Global File Cache über Cloud Manager sind die folgenden Verbesserungen verfügbar:

- Ein Cloud Volumes ONTAP HA Pair in AWS wird nun als Back-End Storage-Plattform für Ihren zentralen Storage unterstützt.

- Mehrere Global File Cache Core-Instanzen können in einem Design mit mehreren Load-Distributed-Dateien implementiert werden.

"Erfahren Sie mehr über Global File Cache".

Cloud Manager 3.8.8 (9. Sept. 2020)

- Unterstützung von Cloud Volumes Service für Google Cloud
- Backup in die Cloud unterstützt jetzt lokale ONTAP Cluster
- Backup in die Cloud
- Verbesserungen bei Cloud Compliance
- Navigation wurde aktualisiert
- Verbesserte Administration

Unterstützung von Cloud Volumes Service für Google Cloud

- Hinzufügen einer Arbeitsumgebung zum Management vorhandener Cloud Volumes Service für GCP Volumes und zur Erstellung neuer Volumes "Erfahren Sie, wie".
- Erstellen und managen Sie NFSv3 und NFSv4.1 Volumes für Linux- und UNIX-Clients sowie SMB 3.x Volumes für Windows-Clients.
- Erstellung, Löschung und Wiederherstellung von Volume Snapshots

Backup in die Cloud unterstützt jetzt lokale ONTAP Cluster

Sie erstellen Backups Ihrer Daten von On-Premises-ONTAP-Systemen in der Cloud. Backup in der Cloud in On-Premises-Arbeitsumgebungen für das Backup von Volumes auf Azure Blob Storage "Weitere Informationen .".

Backup in die Cloud

Die Benutzeroberfläche wurde für eine bessere Bedienbarkeit überarbeitet:

- Auf der Volume-Listenseite finden Sie ganz einfach die zu sichernden Volumes mit den verfügbaren Backups
- Backup-Einstellungen, um Backup-Einstellungen für jede Arbeitsumgebung anzuzeigen

Verbesserungen bei Cloud Compliance

- Möglichkeit zum Scannen von Daten aus Datenbanken

  Scannen Sie Ihre Datenbanken, um persönliche und sensible Daten in jedem Schema zu identifizieren. Zu den unterstützten Datenbanken gehören Oracle, SAP HANA und SQL Server (MSSQL). "Erfahren Sie mehr über das Scannen von Datenbanken".

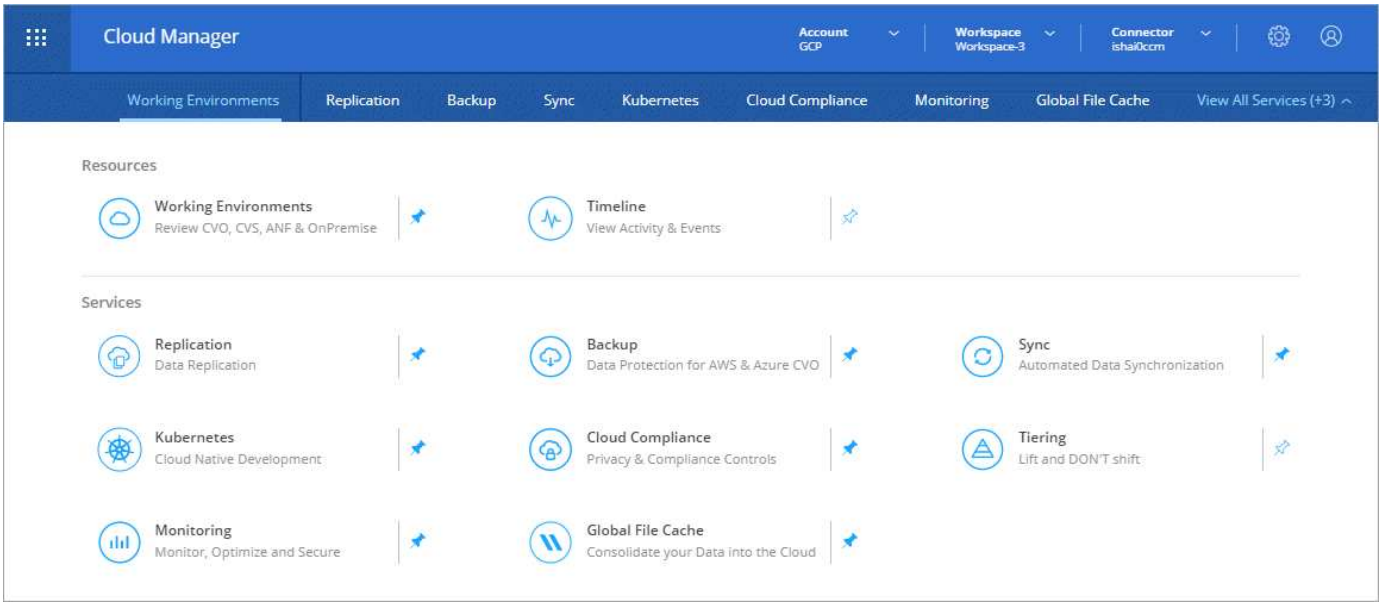
- Scannen von Datensicherungs-Volumes (DP)

  DP-Volumes sind Ziel-Volumes von SnapMirror Vorgängen in der Regel von On-Premises-ONTAP-Clustern. Sie können nun problemlos persönliche und sensible Daten in diesen On-Premises-Dateien ermitteln. "Erfahren Sie, wie".

Navigation wurde aktualisiert

Wir haben die Kopfzeile in Cloud Manager aktualisiert, um Ihnen die Navigation zwischen NetApp Cloud-Services zu erleichtern.

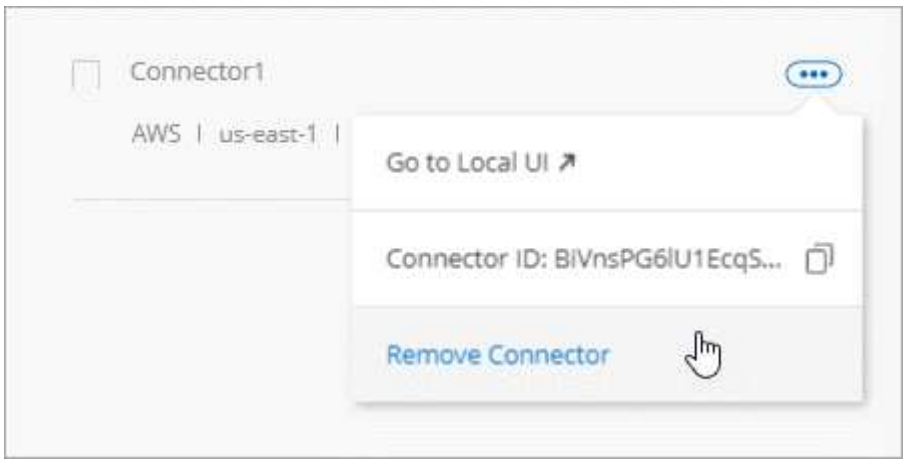
Klicken Sie auf **Alle Dienste anzeigen** und Sie können die Dienste, die Sie sehen möchten, in der Navigation anpinnen und lösen.



Wie Sie sehen, haben wir auch die Dropdown-Menüs Konto, Arbeitsbereich und Connector aktualisiert, sodass Sie Ihre aktuellen Einstellungen leichter anzeigen können.

Verbesserte Administration

- Sie können nun inaktive Verbindungen aus Cloud Manager entfernen. "Erfahren Sie, wie".



- Sie können jetzt das Marketplace-Abonnement ersetzen, das derzeit mit Ihren Zugangsdaten für Cloud-Provider verknüpft ist. Wenn Sie jemals die Abrechnung ändern müssen, können Sie mit dieser Änderung sicherstellen, dass Sie über das richtige Marketplace-Abonnement belastet werden.

  Erfahren Sie, wie "In AWS statt", "In Azure aus", und "In GCP ein".

Update zu erforderlichen Azure Berechtigungen (6. Aug. 2020)

Um Azure-Bereitstellungsausfälle zu vermeiden, stellen Sie sicher, dass Ihre Cloud Manager-Richtlinie in Azure die folgende Berechtigung enthält:

```
"Microsoft.Resources/deployments/operationStatuses/read"
```

Für Azure ist diese Berechtigung jetzt für einige Implementierungen von Virtual Machines erforderlich (es hängt von der zugrunde liegenden physischen Hardware ab, die während der Implementierung verwendet wird).

"Lesen Sie die aktuelle Cloud Manager-Richtlinie für Azure".

Cloud Manager 3.8.7 (3. August 2020)

- Neue Software-als-Service-Lösung
- Verbesserungen von Cloud Volumes ONTAP
- Verbesserungen von Azure NetApp Files
- Verbesserungen von Cloud Volumes Service für AWS
- Verbesserungen bei Cloud Compliance
- Backup in die Cloud
- Unterstützung für Global File Cache

Neue Software-als-Service-Lösung

Wir haben für Cloud Manager ein Software-als-Service-Erlebnis auf den Markt gebracht. Durch diese neue Erfahrung können Sie Cloud Manager einfacher nutzen. Wir stellen zusätzliche Funktionen zum Management Ihrer Hybrid-Cloud-Infrastruktur bereit.

Cloud Manager beinhaltet eine "SaaS-basierte Schnittstelle" Die Lösung ist in NetApp Cloud Central integriert und verfügt über Anschlüsse, über die Cloud Manager Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen kann. (Der Connector ist tatsächlich dieselbe wie die vorhandene Cloud Manager-Software, die Sie installiert haben.)

In den meisten Fällen ist ein Connector erforderlich, es ist jedoch nicht erforderlich, Azure NetApp Files, Cloud Volumes Service oder Cloud Sync von Cloud Manager zu verwenden.

Wie bereits in diesen Versionshinweisen erwähnt, müssen Sie den Maschinentyp für Ihre Connectors aktualisieren, um auf die neuen Funktionen zugreifen zu können, die wir anbieten. Cloud Manager fordert Sie zur Änderung des Maschinentyps auf. "Weitere Informationen .".

Verbesserungen von Cloud Volumes ONTAP

Für Cloud Volumes ONTAP sind zwei Verbesserungen verfügbar.

- **Mehrere Byol-Lizenzen zur Zuweisung zusätzlicher Kapazität**

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

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

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

"Erfahren Sie, wie Sie eine neue Systemlizenz hinzufügen".

- * Azure verwaltete Festplatten mit externen Schlüsseln verschlüsseln*

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

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

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

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

```
"Microsoft.Compute/diskEncryptionSets/read"
```

Verbesserungen von Azure NetApp Files

Diese Version enthält mehrere Verbesserungen zur Unterstützung von Azure NetApp Files.

- **Azure NetApp Files-Einrichtung**

  Azure NetApp Files kann jetzt direkt über den Cloud Manager eingerichtet und gemanagt werden. "Erfahren Sie, wie".

- **Neue Protokollunterstützung**

  Sie können jetzt NFSv4.1 Volumes und SMB Volumes erstellen.

- **Kapazitäts-Pool und Volumen Snapshot-Management**

  Cloud Manager ermöglicht das Erstellen, Löschen und Wiederherstellen von Volume Snapshots. Sie können auch neue Kapazitäts-Pools erstellen und deren Service Level angeben.

- **Fähigkeit zum Bearbeiten von Volumes**

  Sie können ein Volume bearbeiten, indem Sie seine Größe ändern und Tags verwalten.

Verbesserungen von Cloud Volumes Service für AWS

Im Cloud Manager wurden viele Verbesserungen zur Unterstützung von Cloud Volumes Service für AWS vorgenommen.

- **Neue Protokollunterstützung**

  Jetzt können Sie NFSv4.1 Volumes, SMB Volumes und Dual-Protokoll-Volumes erstellen. Zuvor konnten Sie NFSv3 Volumes nur in Cloud Manager erstellen und erkennen.

- **Snapshot-Unterstützung**

  Sie können Snapshot-Richtlinien erstellen, um die Erstellung von Volume Snapshots zu automatisieren, einen On-Demand-Snapshot zu erstellen, ein Volume aus einem Snapshot wiederherzustellen, ein neues Volume auf der Basis eines vorhandenen Snapshots zu erstellen und mehr. Siehe "Managen von Cloud Volumes Snapshots" Finden Sie weitere Informationen.

- **Erstellen Sie das Initialvolumen in einer Region aus Cloud Manager**

  Vor diesem Release musste das erste Volume in jeder Region auf der Schnittstelle Cloud Volumes Service für AWS erstellt werden. Jetzt können Sie sich anmelden "Eines der NetApp Cloud Volumes Service-Angebote im AWS Marketplace" Und dann das erste Volume aus Cloud Manager erstellen.

Verbesserungen bei Cloud Compliance

Die folgenden Verbesserungen sind jetzt für Cloud Compliance verfügbar.

- **Überarbeiteter Bereitstellungsprozess für Ihre Cloud Compliance-Instanz**

  Die Cloud Compliance-Instanz wird mit einem neuen Assistenten in Cloud Manager eingerichtet und bereitgestellt. Nach Abschluss der Bereitstellung aktivieren Sie den Service für jede zu scannenden Arbeitsumgebung.

- **Möglichkeit, die Volumes auszuwählen, die in einer Arbeitsumgebung gescannt werden sollen**

  Sie können nun die Suche nach einzelnen Volumes in einer Arbeitsumgebung von Cloud Volumes ONTAP oder Azure NetApp Files aktivieren und deaktivieren. Wenn Sie bestimmte Volumes nicht für Compliance scannen müssen, deaktivieren Sie sie.

  "Erfahren Sie mehr über das Deaktivieren des Scans nach Volumes."

- **Navigationskarten zum schnellen Sprung in Ihr Interessengebiet**

  Mit den neuen Registerkarten für Dashboard, Ermittlungen und Konfiguration können Sie diese Abschnitte einfacher erreichen.

- **HIPAA-Bericht**

  Ein neuer HIPAA-Bericht (Health Insurance Portability and Accountability Act) ist jetzt verfügbar. Dieser Bericht soll die Anforderung Ihres Unternehmens unterstützen, die HIPAA-Datenschutzgesetze einzuhalten.

  "Weitere Informationen zum HIPAA-Bericht."

- **Neuer sensibler personenbezogener Datentyp**

Cloud Compliance kann jetzt ICD-9-CM Medical Codes in Dateien finden.

- **Neuer personenbezogener Datentyp**

  Cloud Compliance kann jetzt zwei neue nationale Kennungen in Dateien finden: Kroatische ID (OIB) und griechische ID.

Backup in die Cloud

Die folgenden Verbesserungen sind jetzt für Backup in der Cloud verfügbar.

- **Bring your own License (BYOL) ist jetzt verfügbar**

  Backup in die Cloud war nur mit einer PAYGO-Lizenz (Pay as you Go) verfügbar. Mit einer BYOL-Lizenz können Sie bei NetApp eine Lizenz für die Nutzung von Backup in der Cloud für einen bestimmten Zeitraum und für einen maximalen Speicherplatz in Backup-Bereichen erwerben. Wenn eine der beiden Limits erreicht ist, müssen Sie die Lizenz erneuern.

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

- **Unterstützung für Data Protection (DP) Volumes**

  Datensicherungs-Volumes können jetzt gesichert und wiederhergestellt werden.

Unterstützung für Global File Cache

Mit NetApp Global File Cache können Sie Silos verteilter File Server zu einem zusammenhängenden globalen Storage-System in der Public Cloud konsolidieren. Dadurch wird ein global zugängliches File-System in der Cloud geschaffen, das alle verteilten Standorte so nutzen können, als ob sie lokal wären.

Ab dieser Version können die Global File Cache Management-Instanz und die Core-Instanz über Cloud Manager implementiert und gemanagt werden. Dadurch sparen Sie während des ersten Bereitstellungsprozesses viele Stunden und können über Cloud Manager eine zentrale Konsole für diese und andere implementierte Systeme bereitstellen. Instanzen von Global File Cache Edge werden weiterhin lokal an Ihren Remote-Standorten bereitgestellt.

Siehe "Übersicht über Global File Cache" Finden Sie weitere Informationen.

Die Erstkonfiguration, die mit Cloud Manager implementiert werden können, müssen die folgenden Anforderungen erfüllen. Andere Konfigurationen wie Cloud Volumes Service, Azure NetApp Files und Cloud Volumes Service für AWS und GCP werden weiterhin mithilfe der älteren Verfahren implementiert. "Weitere Informationen .".

- Die als zentraler Storage verwendete Back-End-Speicherplattform muss eine Arbeitsumgebung sein, in der Sie ein Cloud Volumes ONTAP HA-Paar in Azure implementiert haben.

  Andere Storage-Plattformen und andere Cloud-Provider werden derzeit nicht mit Cloud Manager unterstützt, können jedoch mit älteren Implementierungsverfahren implementiert werden.

- Der GFC Core kann nur als Standalone-Instanz eingesetzt werden.

  Wenn Sie ein verteiltes Load-Design verwenden möchten, das mehrere Kerninstanzen enthält, müssen Sie die älteren Verfahren verwenden.

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

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

Verbesserte Erfahrung erfordert stärkeren Maschinentyp (15. Juli 2020)

Mit einer verbesserten Nutzung von Cloud Manager müssen Sie Ihren Maschinentyp aktualisieren, um auf die neuen Funktionen zugreifen zu können, die wir anbieten werden. Die Verbesserungen beinhalten ein "Software-as-a-Service-Lösung für Cloud Manager" Und Integration neuer und verbesserter Cloud-Services.

Cloud Manager fordert Sie zur Änderung des Maschinentyps auf.

Hier sind einige Details:

1. Um sicherzustellen, dass für die ordnungsgemäße Funktion der neuen Funktionen in Cloud Manager ausreichend Ressourcen zur Verfügung stehen, haben wir die Standardinstanz, die VM und den Computertyp wie folgt geändert:
   - AWS: t3.xlarge
   - Azure: DS3 v2
   - GCP: n1-Standard-4

   Diese Standardgrößen werden als Minimum unterstützt "Basierend auf CPU- und RAM-Anforderungen".
2. Im Rahmen dieser Transition benötigt Cloud Manager Zugriff auf den folgenden Endpunkt, um Software-Images von Containerkomponenten für eine Docker Infrastruktur zu erhalten:

   https://cloudmanagerinfraprod.azurecr.io

   Stellen Sie sicher, dass Ihre Firewall über Cloud Manager den Zugriff auf diesen Endpunkt ermöglicht.

Cloud Manager 3.8.6 (6. Juli 2020)

- Unterstützung für iSCSI-Volumes
- Unterstützung für die All-Tiering-Richtlinie

Unterstützung für iSCSI-Volumes

Mit Cloud Manager können Sie jetzt iSCSI-Volumes für Cloud Volumes ONTAP und lokale ONTAP Cluster direkt über die Benutzeroberfläche erstellen.

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

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

Unterstützung für die All-Tiering-Richtlinie

Sie können nun die „Alle-Tiering“-Richtlinie auswählen, wenn Sie ein Volume für Cloud Volumes ONTAP erstellen oder ändern. Wenn Sie die All-Tiering-Richtlinie verwenden, werden Daten sofort als „kalt“ markiert und in den Objekt-Storage verschoben. "Weitere Informationen zum Daten-Tiering".

Cloud Manager Transition zu SaaS (22. Juni 2020)

Wir führen eine Software-als-Service-Erfahrung für Cloud Manager ein. Durch diese neue Erfahrung können Sie Cloud Manager einfacher nutzen. Wir stellen zusätzliche Funktionen zum Management Ihrer Hybrid-Cloud-Infrastruktur bereit. "Weitere Informationen .".

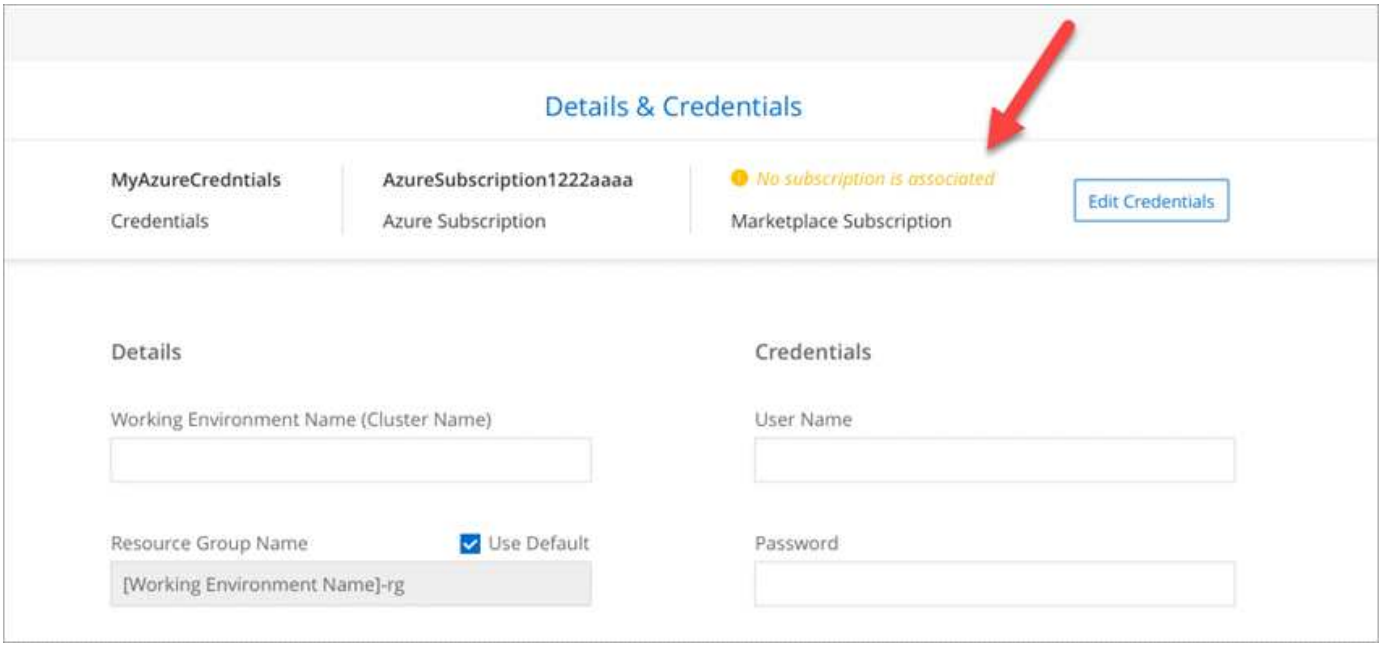
Cloud Manager 3.8.5 (31. Mai 2020)

- Im Azure Marketplace ist ein neues Abonnement erforderlich
- Backup in die Cloud
- Verbesserungen bei Cloud Compliance

Im Azure Marketplace ist ein neues Abonnement erforderlich

Ein neues Abonnement ist im Azure Marketplace erhältlich. Dieses einmalige Abonnement ist für die Implementierung von Cloud Volumes ONTAP 9.7 PAYGO erforderlich (außer für Ihr kostenloses 30-Tage-Testsystem). Mit dem Abonnement können wir auch Add-on-Funktionen für Cloud Volumes ONTAP PAYGO und BYOL anbieten. Sie erhalten für jedes von Ihnen erstellte Cloud Volumes ONTAP PAYGO-System und jedes von Ihnen aktiviert Add-on-Feature eine Gebühr in Höhe dieses Abonnements.

Cloud Manager fordert Sie auf, dieses Angebot bei der Implementierung eines neuen Cloud Volumes ONTAP Systems (9.7 P1 oder höher) zu abonnieren.



Backup in die Cloud

Die folgenden Verbesserungen sind jetzt für Backup in der Cloud verfügbar.

- In Azure können Sie jetzt eine neue Ressourcengruppe erstellen oder eine vorhandene Ressourcengruppe auswählen, anstatt eine von Cloud Manager erstellen zu müssen. Die Ressourcengruppe kann nicht geändert werden, nachdem Sie Backup in Cloud aktiviert haben.
- In AWS können Sie jetzt ein Backup von Cloud Volumes ONTAP Instanzen erstellen, die sich in einem anderen AWS Konto befinden als Ihr Cloud Manager AWS Konto.
- Bei der Auswahl des Backup-Zeitplans für Volumes stehen jetzt weitere Optionen zur Verfügung. Zusätzlich zu den täglichen, wöchentlichen und monatlichen Backup-Optionen steht nun eine der systemdefinierten Richtlinien zur Verfügung, die Kombinationsrichtlinien wie etwa 30 tägliche, 13 wöchentliche und 12 monatliche Backups enthalten.
- Nachdem Sie alle Backups für ein Volume gelöscht haben, können Sie jetzt wieder Backups für dieses Volume erstellen. Dies war eine bekannte Einschränkung in der vorherigen Version.

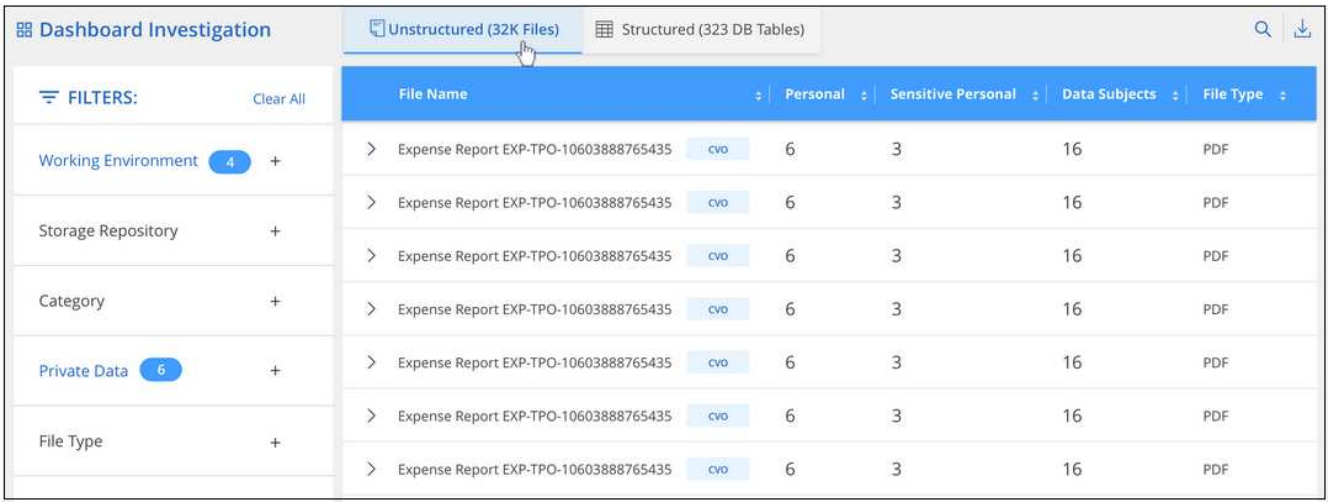
Verbesserungen bei Cloud Compliance

Folgende Verbesserungen sind für Cloud Compliance verfügbar:

- Sie können jetzt S3-Buckets scannen, die sich in unterschiedlichen AWS-Konten befinden als die Cloud-Compliance-Instanz. In diesem neuen Konto müssen Sie nur eine Rolle erstellen, damit die vorhandene Cloud Compliance-Instanz eine Verbindung zu diesen Buckets herstellen kann. "Weitere Informationen .".

  Wenn Sie Cloud-Compliance vor Version 3.8.5 konfiguriert haben, müssen Sie die vorhandene ändern "IAM-Rolle für die Cloud Compliance-Instanz" Um diese Funktion zu verwenden.

- Sie können jetzt den Inhalt der Untersuchungsseite filtern, um nur die Ergebnisse anzuzeigen, die Sie sehen möchten. Die Filter umfassen Arbeitsumgebung, Kategorie, private Daten, Dateityp, Datum der letzten Änderung, Und ob die Berechtigungen des S3-Objekts für den öffentlichen Zugriff zugänglich sind.



- Sie können Cloud Compliance jetzt direkt über die Registerkarte Cloud Compliance in einer Arbeitsumgebung aktivieren und deaktivieren.

Update zu Cloud Manager 3.8.4 (10. Mai 2020)

Wir haben eine Verbesserung für Cloud Manager 3.8.4 veröffentlicht.

Cloud Insights Integration

Durch den Einsatz des NetApp Cloud Insights-Service liefert Cloud Manager Einblicke in den Zustand und die Performance der Cloud Volumes ONTAP Instanzen und unterstützt Sie bei der Fehlerbehebung und Optimierung der Performance Ihrer Cloud-Storage-Umgebung. "Weitere Informationen .".

Cloud Manager 3.8.4 (3. Mai 2020)

In Cloud Manager 3.8.4 ist folgende Verbesserung enthalten:

Backup in die Cloud

Die folgenden Verbesserungen stehen jetzt für Backup in der Cloud zur Verfügung (ehemals *Backup zu S3* für AWS):

- * Backups auf Azure Blob Storage*

  Backup in der Cloud ist jetzt für Cloud Volumes ONTAP in Azure verfügbar. Backup in der Cloud bietet Backup- und Restore-Funktionen zum Schutz und zur langfristigen Archivierung Ihrer Cloud-Daten. "Weitere Informationen .".

- **Backups werden gelöscht**

  Alle Backups für ein bestimmtes Volume können nun direkt über die Benutzeroberfläche von Cloud Manager gelöscht werden. "Weitere Informationen .".

Cloud Manager 3.8.3 (5. April 2020)

- Integration von Cloud-Tiering
- Datenmigration auf Azure NetApp Files
- Verbesserungen bei Cloud Compliance

- Backup auf S3-Verbesserungen
- ISCSI-Volumes mit APIs

Integration von Cloud-Tiering

Der NetApp Cloud Tiering Service ist jetzt über Cloud Manager verfügbar. Mit Cloud-Tiering können Sie Daten von einem lokalen ONTAP Cluster zu kostengünstigerem Objekt-Storage in der Cloud verschieben. So wird im Cluster High-Performance-Speicherplatz für mehr Workloads frei.

"Weitere Informationen .".

Datenmigration auf Azure NetApp Files

NFS- oder SMB-Daten lassen sich nun direkt über Cloud Manager zu Azure NetApp Files migrieren. Die Synchronisierung von Daten wird durch den NetApp Cloud Sync Service unterstützt.

"Lesen Sie, wie Sie Daten zu Azure NetApp Files migrieren".

Verbesserungen bei Cloud Compliance

Die folgenden Verbesserungen sind jetzt für Cloud Compliance verfügbar.

- **30 Tage kostenlos testen mit Amazon S3**

  Zum Scannen von Amazon S3 Daten mit Cloud Compliance steht jetzt eine kostenlose 30-Tage-Testversion zur Verfügung. Wenn Sie zuvor Cloud-Compliance auf Amazon S3 aktiviert haben, ist Ihre kostenlose 30-Tage-Testversion ab heute aktiv (5. April 2020).

  Ein Abonnement des AWS Marketplace muss nach dem Ende der kostenlosen Testversion weiterhin Amazon S3 scannen. "Erfahren Sie, wie Sie abonniert werden können".

  "Weitere Informationen zu den Preisen zum Scannen von Amazon S3".

- **Neuer personenbezogener Datentyp**

  Cloud Compliance kann jetzt eine neue nationale Kennung in Dateien finden: Brasilianische ID (CPF).

  "Erfahren Sie mehr über personenbezogene Datentypen".

- **Unterstützung für weitere Metadaten Kategorien**

  In Cloud Compliance können Sie Ihre Daten jetzt in neun weitere Metadatenkategorien kategorisieren. "Weitere Informationen finden Sie in der vollständigen Liste der unterstützten Metadatenkategorien".

Backup auf S3-Verbesserungen

Die folgenden Verbesserungen sind jetzt für den Service Backup to S3 verfügbar.

- **S3 Lifecycle Policy für Backups**

  Backups beginnen in der Klasse *Standard* Storage und wechseln nach 30 Tagen zur Storage-Klasse *Standard-infrequent Access*.

- **Backups werden gelöscht**

Backups können jetzt über eine Cloud Manager API gelöscht werden. "Weitere Informationen .".

- * Öffentlichen Zugang blockieren*

  Cloud Manager ermöglicht das jetzt "Amazon S3 Block – Public Access-Funktion" Auf dem S3-Bucket, wo Backups gespeichert werden

ISCSI-Volumes mit APIs

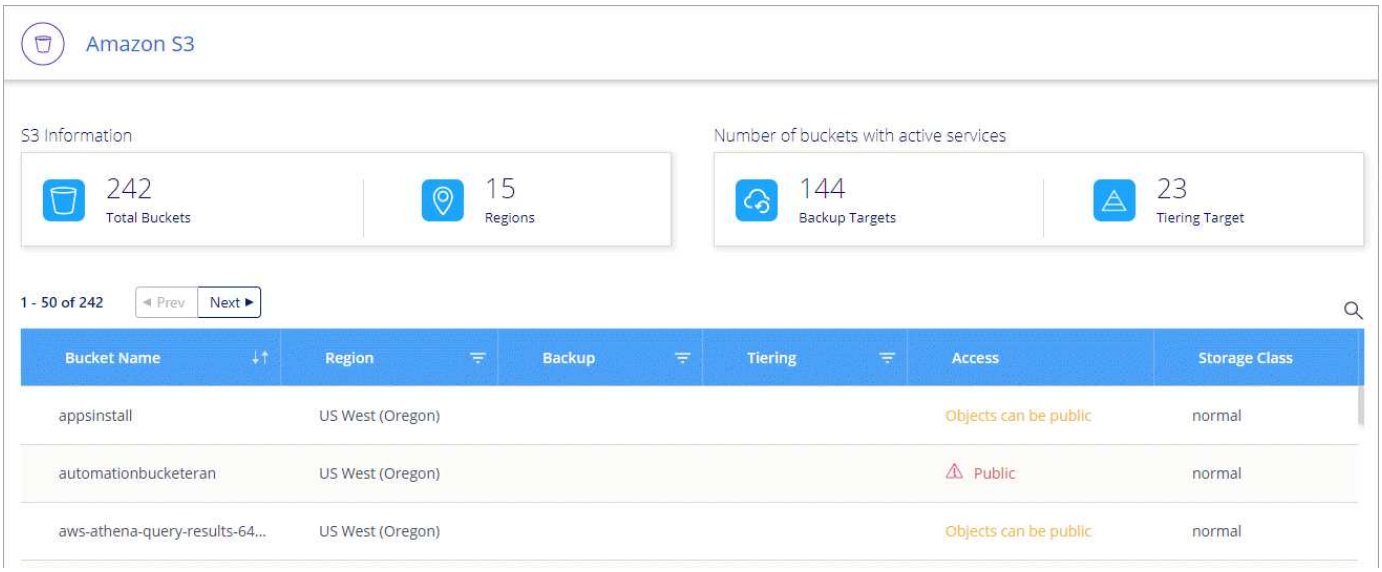
Mit den Cloud Manager APIs können Sie jetzt iSCSI Volumes erstellen. "Zeigen Sie hier ein Beispiel an".

Cloud Manager 3.8.2 (1. März 2020)

- Amazon S3-Arbeitsumgebungen
- Verbesserungen bei Cloud Compliance
- NFS-Version für Volumes
- Support für Azure US-Regionen

Amazon S3-Arbeitsumgebungen

Cloud Manager erkennt jetzt automatisch Informationen zu den Amazon S3 Buckets, die sich im AWS Konto befinden, wo sie installiert sind. Dadurch haben Sie problemlos Details zu Ihren S3 Buckets, einschließlich Region, Zugriffsebene, Storage-Klasse und darüber, ob der Bucket mit Cloud Volumes ONTAP für Backups oder Daten-Tiering verwendet wird. Zudem können Sie die S3-Buckets mithilfe von Cloud Compliance scannen, wie unten beschrieben.



Verbesserungen bei Cloud Compliance

Die folgenden Verbesserungen sind jetzt für Cloud Compliance verfügbar.

- **Unterstützung für Amazon S3**

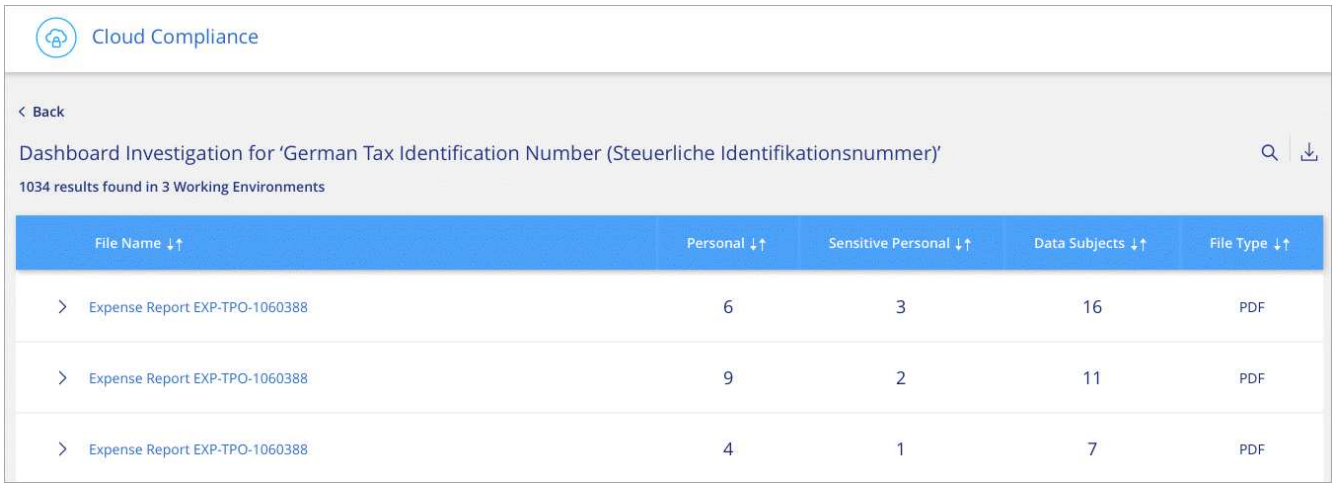
  Cloud Compliance kann jetzt Ihre Amazon S3 Buckets scannen, um die persönlichen und sensiblen Daten im S3 Objekt-Storage zu identifizieren. Cloud Compliance kann jeden Bucket auf dem Konto scannen, unabhängig davon, ob er für eine NetApp Lösung erstellt wurde.

"Erste Schritte".

- **Untersuchungsseite**

  Für jeden Typ von persönlichen Dateien, sensiblen persönlichen Dateien, Kategorien und Dateitypen steht jetzt eine neue Untersuchungsseite zur Verfügung. Die Seite zeigt Details zu den betroffenen Dateien an und ermöglicht die Sortierung nach Dateien, die die meisten personenbezogenen Daten, sensible personenbezogene Daten und Namen der betroffenen Personen enthalten. Diese Seite ersetzt den zuvor verfügbaren CSV-Bericht.

  Hier ein Beispiel:



  "Erfahren Sie mehr über die Untersuchungsseite".

- **PCI DSS Report**

  Ein neuer Payment Card Industry Data Security Standard (PCI DSS) Report ist jetzt verfügbar. Dieser Bericht kann Ihnen dabei helfen, die Verteilung von Kreditkarteninformationen auf Ihre Dateien zu identifizieren. Sie können sehen, wie viele Dateien Kreditkarteninformationen enthalten, ob die Arbeitsumgebungen durch Verschlüsselung, Ransomware-Schutz, Aufbewahrungsdetails und vieles mehr geschützt sind.

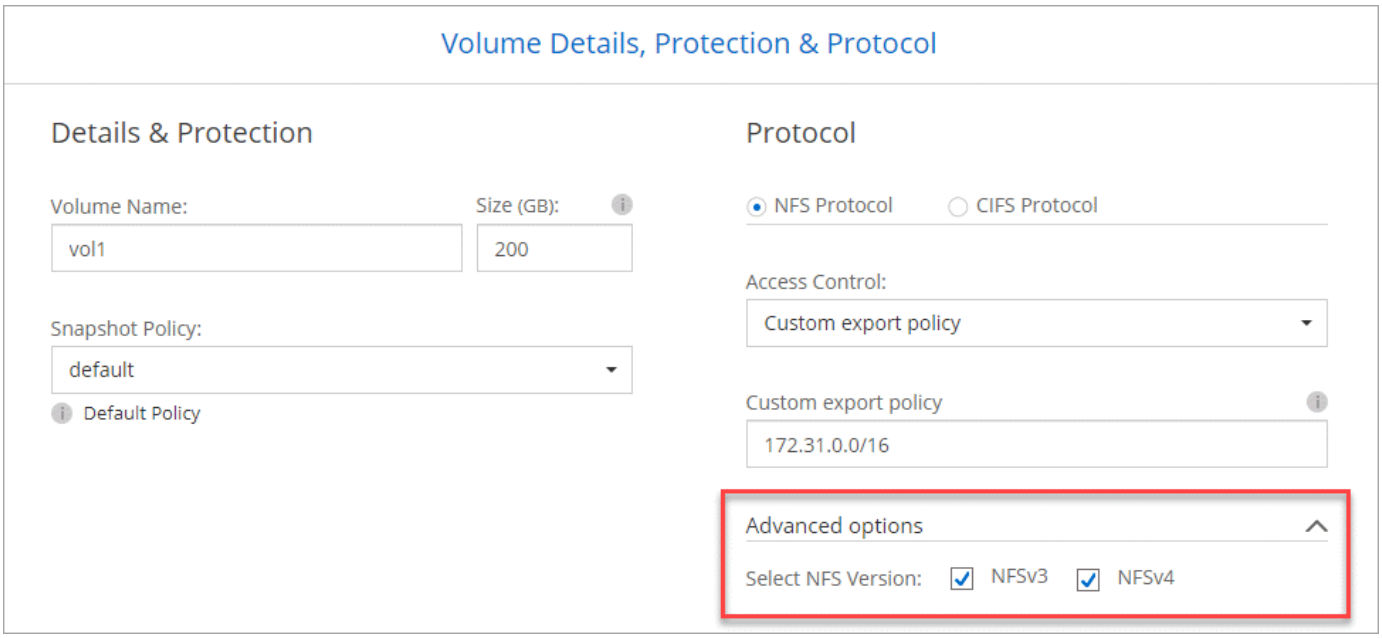
  "Erfahren Sie mehr über den PCI DSS-Bericht".

- **Neuer sensibler personenbezogener Datentyp**

  Cloud Compliance kann jetzt ICD-10-CM Medical Codes finden, die in der Medizin- und Gesundheitsbranche verwendet werden.

NFS-Version für Volumes

Sie können nun die NFS-Version auswählen, die auf einem Volume aktiviert werden soll, wenn Sie ein Volume für Cloud Volumes ONTAP erstellen oder bearbeiten.



Support für Azure US-Regionen

Cloud Volumes ONTAP HA-Paare werden jetzt in Azure US-Regionen unterstützt.

"Siehe die Liste der unterstützten Azure Regionen".

Update zu Cloud Manager 3.8.1 (16. Februar 2020)

Wir haben einige Verbesserungen an Cloud Manager 3.8 veröffentlicht.

Backup auf S3-Verbesserungen

- Backup-Kopien werden nun in einem S3-Bucket gespeichert, den Cloud Manager in Ihrem AWS-Konto erstellt, mit einem Bucket pro Cloud Volumes ONTAP-Arbeitsumgebung.
- Backup in S3 wird jetzt in allen AWS Regionen unterstützt "Wobei Cloud Volumes ONTAP unterstützt wird".
- Sie können den Backup-Zeitplan auf täglich, wöchentlich oder monatlich festlegen.
- Cloud Manager muss keine *privaten Links* zum Backup to S3 Service einrichten.

Für diese Verbesserungen sind zusätzliche S3 Berechtigungen erforderlich. Die IAM-Rolle, die Cloud Manager über Berechtigungen verfügt, muss Berechtigungen von der neuesten enthalten "Cloud Manager-Richtlinie".

"Weitere Informationen zu Backup in S3".

AWS Updates

Wir haben die Unterstützung für neue EC2 Instanzen eingeführt und eine Änderung der Anzahl der unterstützten Datenfestplatten für Cloud Volumes ONTAP 9.6 und 9.7. Sehen Sie sich die Änderungen in den Versionshinweisen zu Cloud Volumes ONTAP an.

- "Versionshinweise zu Cloud Volumes ONTAP 9.7"
- "Versionshinweise zu Cloud Volumes ONTAP 9.6"

Cloud Manager 3.8.1 (2. Februar 2020)

- Verbesserungen bei Cloud Compliance
- Erweiterungen für Konten und Abonnements
- Verbesserungen in der Zeitleiste

Verbesserungen bei Cloud Compliance

Die folgenden Verbesserungen sind jetzt für Cloud Compliance verfügbar.

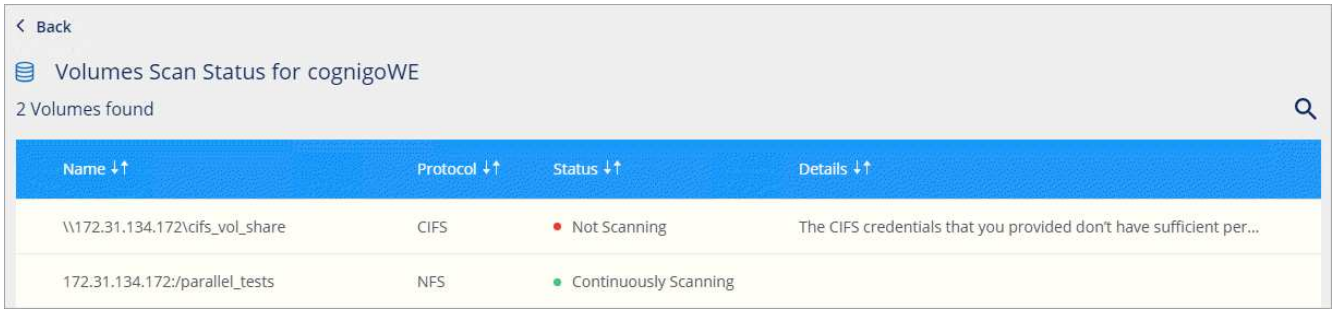
- **Unterstützung für Azure NetApp Files**

  Wir freuen uns, Ihnen bekannt geben zu können, dass Cloud Compliance Azure NetApp Files jetzt einscannen kann, um persönliche und sensible Daten auf Volumes zu identifizieren.

  "Erste Schritte".

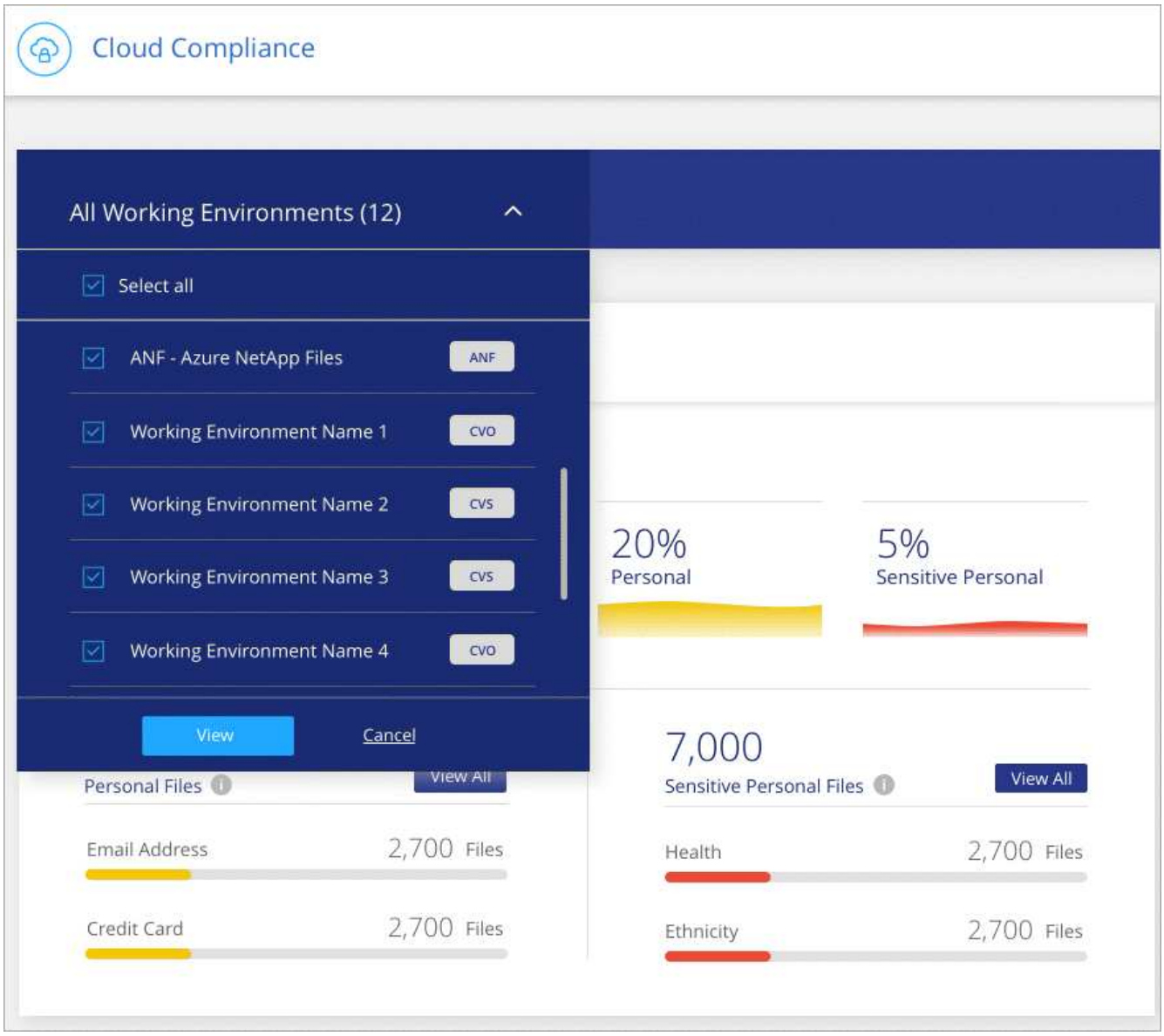
- **Scan-Status**

  Cloud Compliance zeigt Ihnen nun einen Scanstatus für jedes CIFS- und NFS-Volume, einschließlich Fehlermeldungen, mit denen Sie Probleme beheben können.



- **Dashboard nach Arbeitsumgebung filtern**

  Sie können den Inhalt des Cloud Compliance-Dashboards jetzt filtern, um Compliance-Daten für bestimmte Arbeitsumgebungen anzuzeigen.



- **Neuer personenbezogener Datentyp**

  Cloud Compliance kann jetzt beim Scannen von Daten die Lizenz eines kalifornischen Treibers ermitteln.

- **Unterstützung für weitere Kategorien**

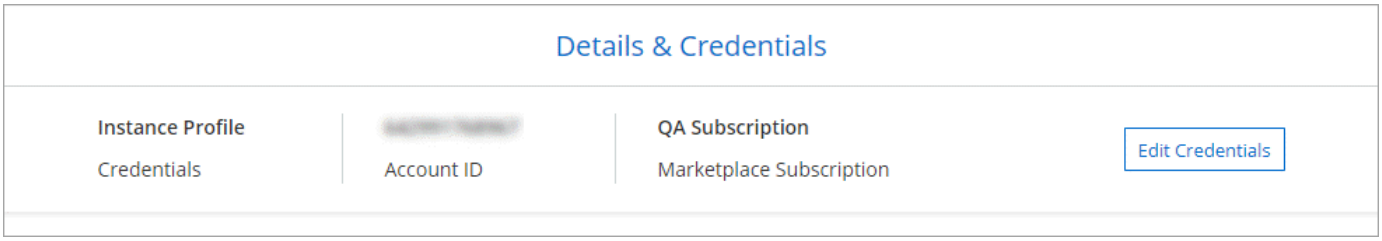
  Weitere drei Kategorien werden unterstützt: Anwendungsdaten, Protokolle sowie Datenbank- und Indexdateien.

  "Weitere Informationen zu Kategorien".

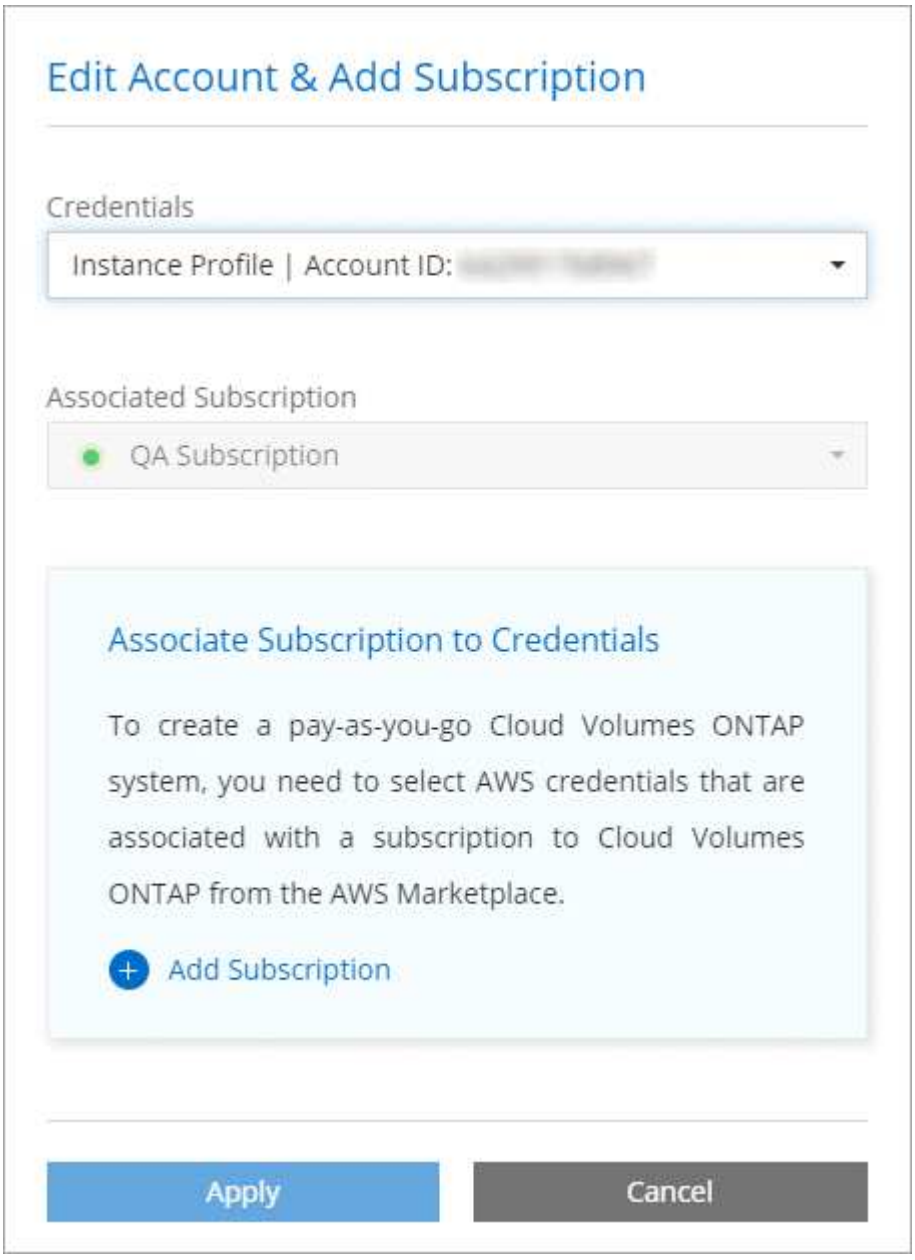
Erweiterungen für Konten und Abonnements

Die Auswahl eines AWS Accounts oder GCP-Projekts wird vereinfacht und es ist ein damit verbundener Marketplace-Abonnement für ein Pay-as-you-go-Cloud Volumes ONTAP-System erforderlich. Diese Verbesserungen sorgen dafür, dass Sie von Ihrem Konto oder Projekt aus zahlen.

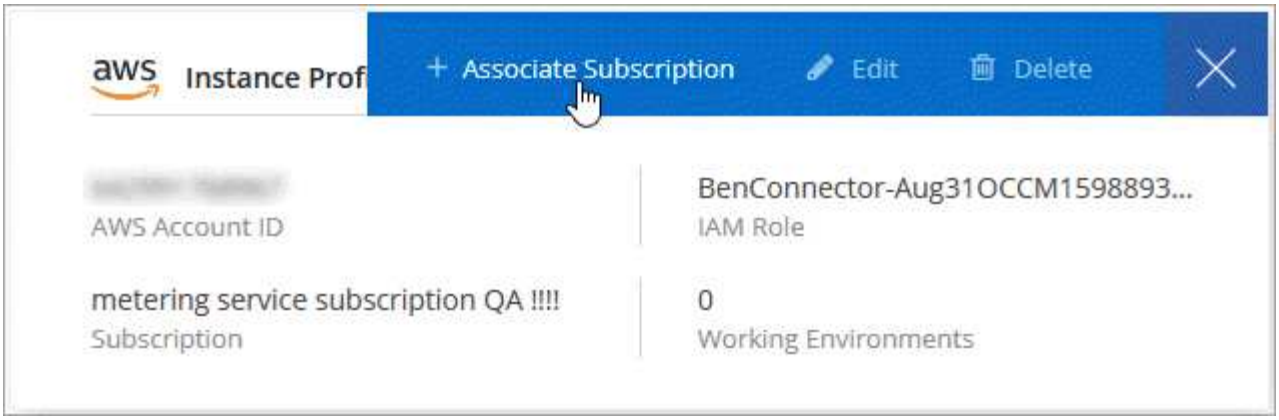
Wenn Sie beispielsweise ein System in AWS erstellen, klicken Sie auf **Anmeldedaten bearbeiten**, wenn Sie das Standardkonto und das Abonnement nicht verwenden möchten:



Dort können Sie die gewünschten Kontodaten sowie das zugehörige AWS Marketplace Abonnement auswählen. Sie können auch ein Abonnement für den Marktplatz hinzufügen, wenn Sie es benötigen.



Wenn Sie mehrere AWS-Abonnements verwalten, können Sie jedes davon verschiedenen AWS Zugangsdaten auf der Seite „Anmeldeinformationen“ in den Einstellungen zuweisen:

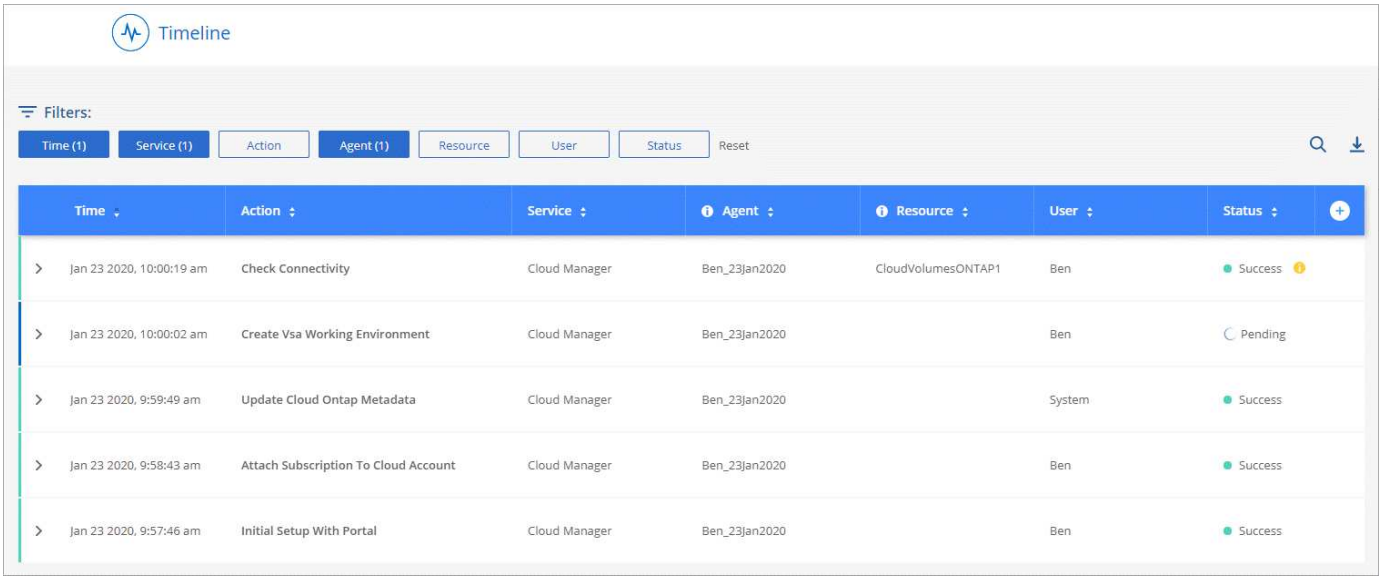


"Managen der AWS Zugangsdaten in Cloud Manager".

Verbesserungen in der Zeitleiste

In der Zeitleiste haben wir weitere Informationen zu den von Ihnen genutzten NetApp Cloud-Services erhalten.

- In der Zeitleiste werden nun Aktionen für alle Cloud Manager-Systeme im selben Cloud Central-Konto angezeigt
- Sie können jetzt einfacher Informationen finden, indem Sie Spalten filtern, suchen und hinzufügen und entfernen
- Sie können die Zeitachsendaten jetzt im CSV-Format herunterladen
- In der Zukunft werden in der Zeitleiste Aktionen für jeden von Ihnen verwendeten NetApp Cloud-Service angezeigt (die Informationen können jedoch nach unten auf einen einzelnen Service gefiltert werden).



Cloud Manager 3.8 (8. Januar 2020)

- HA-Verbesserungen in Azure
- Verbesserungen beim Daten-Tiering in GCP

HA-Verbesserungen in Azure

Die folgenden Verbesserungen sind jetzt für Cloud Volumes ONTAP HA-Paare in Azure verfügbar.

- **Überschreiben von CIFS-Locks für Cloud Volumes ONTAP HA in Azure**

  Sie können jetzt in Cloud Manager eine Einstellung aktivieren, die Probleme mit dem Cloud Volumes ONTAP Storage Failover bei Azure-Wartungsereignissen verhindert. Wenn Sie diese Einstellung aktivieren, sperrt Cloud Volumes ONTAP Vetoes CIFS und setzt aktive CIFS-Sitzungen zurück. "Weitere Informationen .".

- **HTTPS-Verbindung von Cloud Volumes ONTAP zu Speicherkonten**

  Sie können jetzt bei der Erstellung einer Arbeitsumgebung eine HTTPS-Verbindung von einem Cloud Volumes ONTAP 9.7 HA-Paar zu Azure Storage-Konten aktivieren. Beachten Sie, dass die Aktivierung dieser Option sich auf die Schreib-Performance auswirken kann. Sie können die Einstellung nicht ändern, nachdem Sie die Arbeitsumgebung erstellt haben.

- **Unterstützung für allgemeine Azure v2 Storage-Konten**

  Die Storage-Konten, die Cloud Manager für Cloud Volumes ONTAP 9.7 HA-Paare erstellt, sind jetzt allgemeine v2 Storage-Konten.

Verbesserungen beim Daten-Tiering in GCP

Die folgenden Verbesserungen sind für Cloud Volumes ONTAP Daten-Tiering in GCP verfügbar.

- **Google Cloud Speicherklassen für Daten-Tiering**

  Nun können Sie eine Storage-Klasse für Daten auswählen, die Cloud Volumes ONTAP in Google Cloud Storage Tiers verschieben:

  - Standard-Storage (Standard)
  - Nearline Storage
  - Coldline Storage

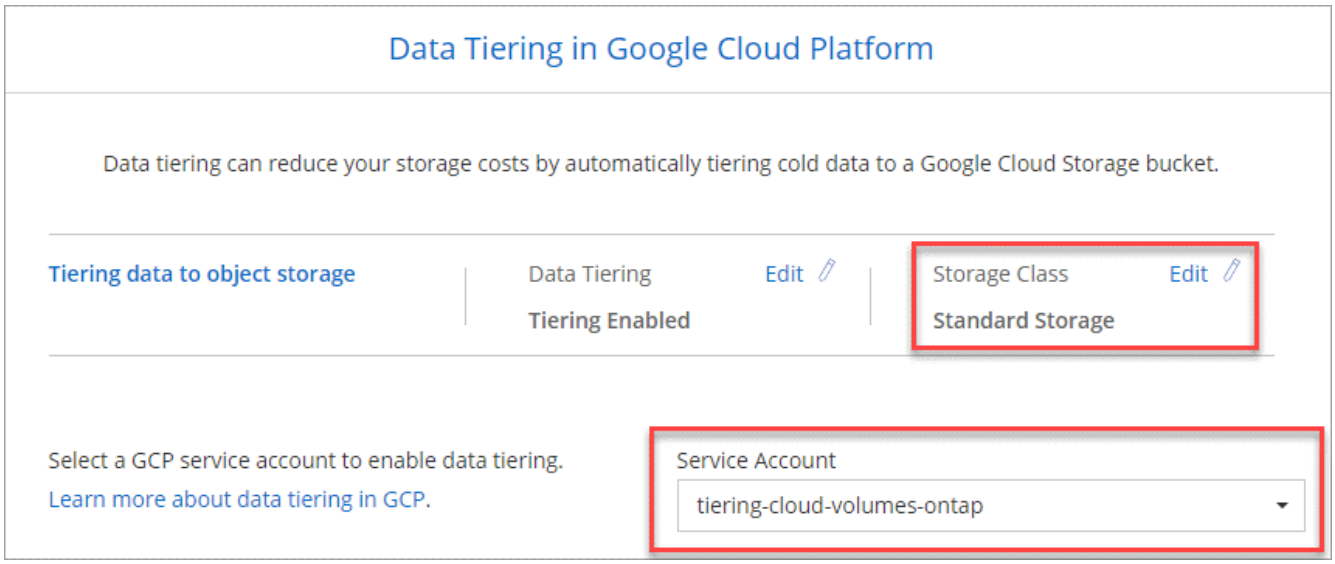
    "Erfahren Sie mehr über Google Cloud Storage Classes".

  "Erfahren Sie, wie Sie die Storage-Klasse für Cloud Volumes ONTAP ändern".

- **Daten-Tiering mit einem Service-Konto**

  Ab Version 9.7 legt Cloud Manager jetzt ein Service-Konto auf die Cloud Volumes ONTAP Instanz. Dieses Servicekonto bietet Berechtigungen für Daten-Tiering zu einem Google Cloud Storage Bucket. Diese Änderung sorgt für mehr Sicherheit und erfordert weniger Einrichtung. Für Schritt-für-Schritt-Anleitungen bei der Implementierung eines neuen Systems, "Siehe Schritt 4 auf dieser Seite".

  Das folgende Bild zeigt den Assistenten zur Arbeitsumgebung, in dem Sie eine Speicherklasse und ein Servicekonto auswählen können:



Für diese Verbesserungen ist für Cloud Manager die folgende GCP-Berechtigung erforderlich, wie in der aktuellen Version dargestellt "Cloud Manager-Richtlinie für GCP".

```
- storage.buckets.update
- compute.instances.setServiceAccount
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
```

Cloud Manager Transition zu SaaS

Wir haben für Cloud Manager eine Software-als-Service-Erfahrung auf den Markt gebracht. Durch diese neue Erfahrung können Sie Cloud Manager einfacher nutzen. Wir stellen zusätzliche Funktionen zum Management Ihrer Hybrid-Cloud-Infrastruktur bereit.

In der vorherigen Erfahrung mit Cloud Manager

Die Cloud Manager Software bestand zuvor aus einer Benutzeroberfläche und einer Managementebene, durch die Anfragen an Cloud-Provider gesendet wurden. Zunächst würden Sie Cloud Manager in Ihrem Cloud- oder On-Premises-Netzwerk implementieren und dann auf die Benutzeroberfläche zugreifen, die auf dieser Instanz ausgeführt wird.

Diese Erfahrung hat sich verändert.

Die neue SaaS-Erfahrung

Auf die Cloud Manager Schnittstelle kann jetzt über eine SaaS-basierte Benutzeroberfläche zugegriffen werden, die Sie sich von NetApp Cloud Central aus bei anmelden. Sie müssen nicht mehr von Software aus auf eine Benutzeroberfläche zugreifen, die im Netzwerk ausgeführt wird.

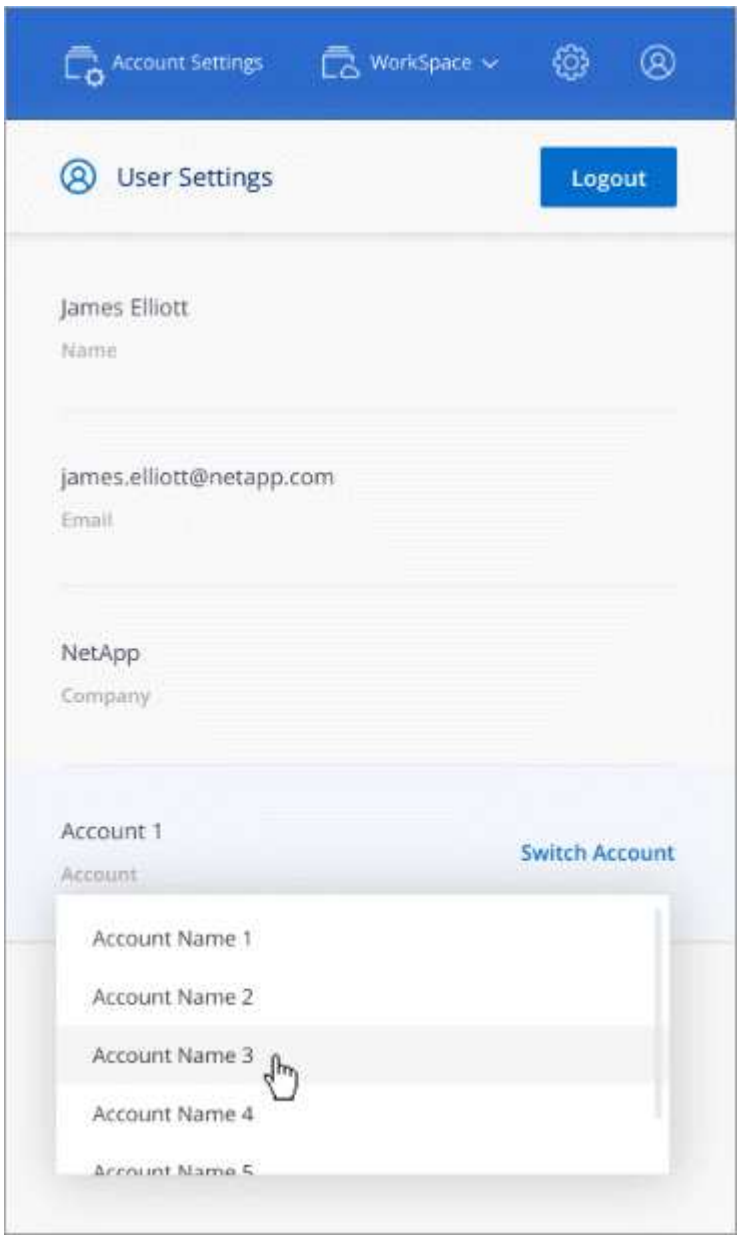
In den meisten Fällen muss ein Connector_ in Ihrer Cloud oder Ihrem On-Premises-Netzwerk implementiert werden. Der Connector ist eine Software, die für das Management von Cloud Volumes ONTAP und anderen Cloud-Datenservices benötigt wird. (Der Connector ist tatsächlich dieselbe wie die vorhandene Cloud Manager-Software, die Sie installiert haben.)

Vorteile

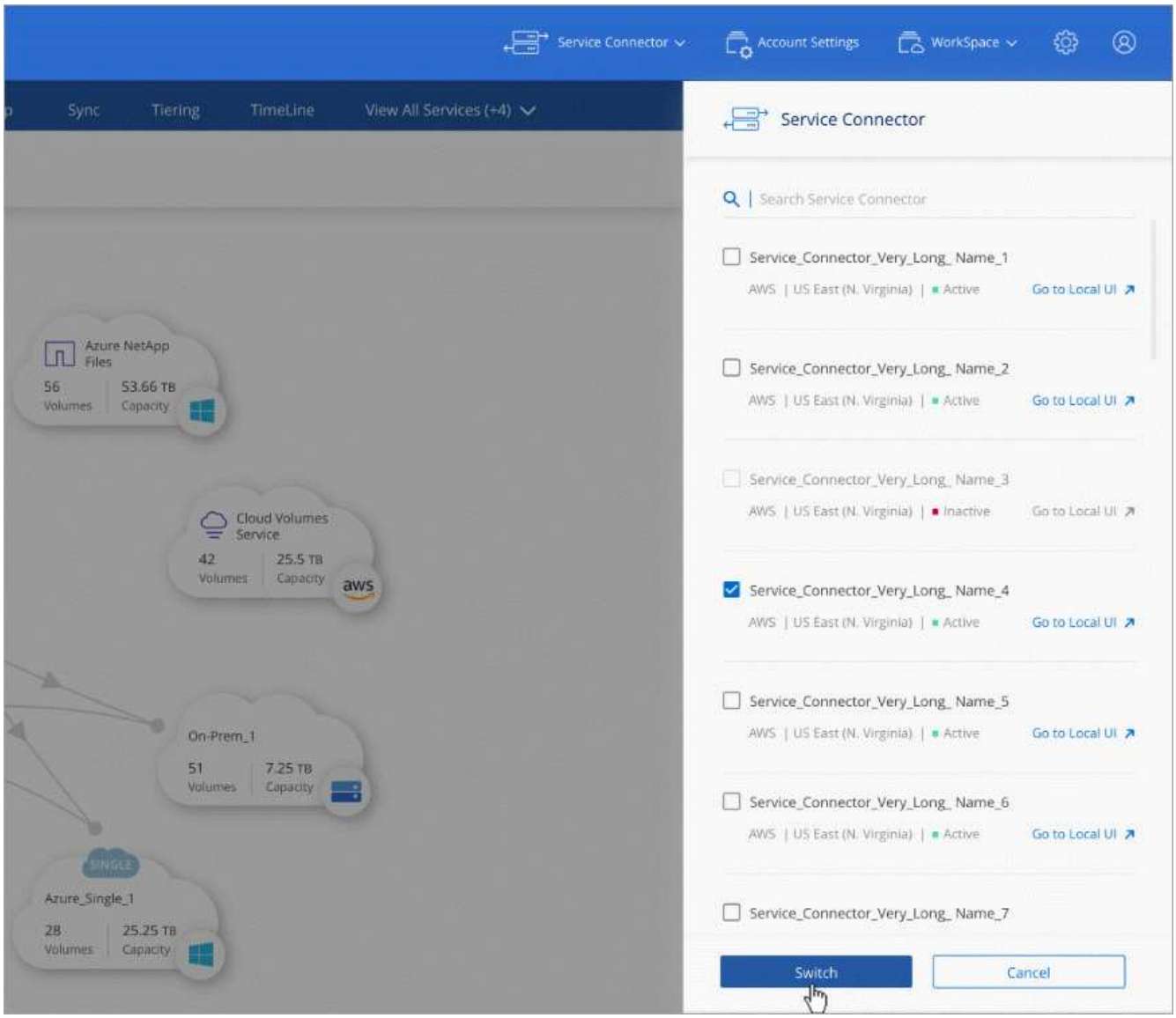
Dieser SaaS-basierte Ansatz bietet mehrere Vorteile:

- Wir können zusätzliche Management-Funktionen für Azure NetApp Files und Cloud Volumes Service bereitstellen, ohne dass eine Software in Ihrer Umgebung implementiert werden muss.
- Sie können einfach zwischen Ihren Cloud Central Accounts wechseln.

  Wenn ein Benutzer mit mehreren Cloud Central-Konten verknüpft ist, kann er jederzeit über das Menü „Benutzereinstellungen“ zu einem anderen Konto wechseln. Anschließend können sie die Anschlüsse und Arbeitsumgebungen sehen, die mit diesem Konto verknüpft sind.



- Sie können ganz einfach zwischen Connectors (was Sie heute als Cloud Manager-Software kennen) wechseln, die in verschiedenen Netzwerken oder verschiedenen Cloud-Providern installiert sind.

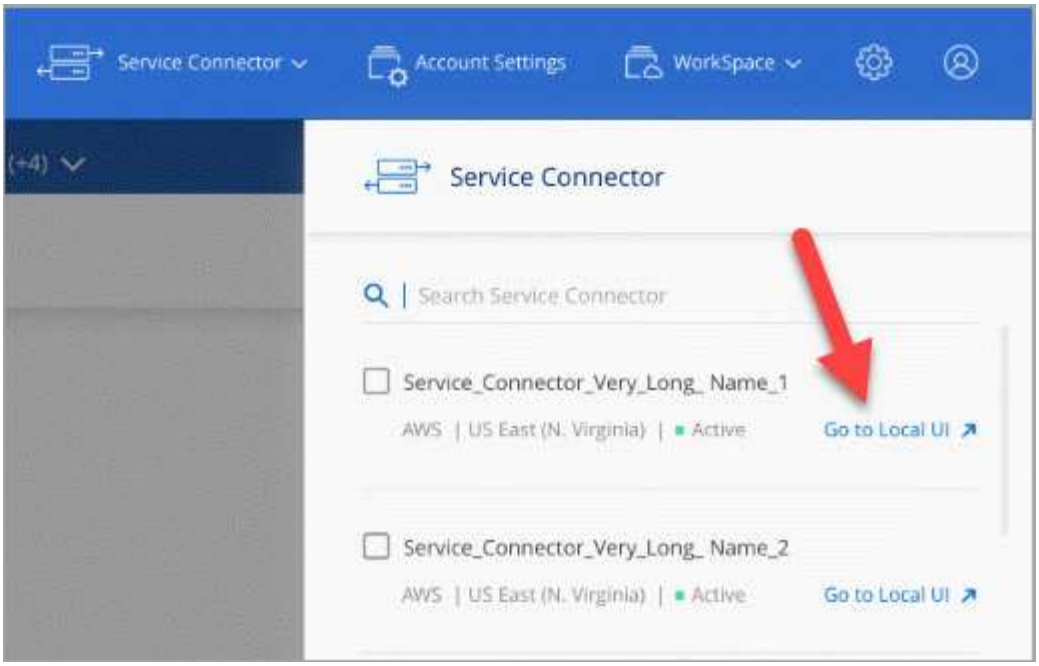


Die lokale Benutzeroberfläche

Während Sie fast alle Aufgaben über die SaaS-Benutzeroberfläche ausführen sollten, steht auf dem Connector weiterhin eine lokale Benutzeroberfläche zur Verfügung. Diese Schnittstelle wird für einige Aufgaben benötigt, die über den Connector selbst ausgeführt werden müssen:

- Festlegen eines Proxyservers
- Installieren eines Patches
- Herunterladen von AutoSupport Meldungen

Die lokale Benutzeroberfläche kann direkt über die SaaS-Benutzeroberfläche zugegriffen werden:



Änderungen am Instanztyp, der VM und am Computertyp

Um sicherzustellen, dass in Cloud Manager genügend Ressourcen für neue und neue Funktionen zur Verfügung stehen, haben wir das erforderliche Minimum an Instanz, VM und Maschinentyp wie folgt geändert:

- AWS: t3.xlarge
- Azure: DS3 v2
- GCP: n1-Standard-4

Wenn Sie einen Maschinentyp aktualisieren, erhalten Sie Zugriff auf Funktionen wie die neue Kubernetes Erfahrung, den globalen File Cache, das Monitoring usw.

Diese Standardgrößen werden als Minimum unterstützt "Basierend auf CPU- und RAM-Anforderungen".

Cloud Manager fordert Sie dazu auf, den Maschinentyp des Connectors zu ändern.

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.

Anschlüsse sollten weiterhin ausgeführt werden

Ein Steckverbinder sollte immer weiter laufen. Es ist wichtig für den fortwährenden Zustand und Betrieb der Services, die Sie ermöglichen.

Ein Connector ist beispielsweise eine wichtige Komponente im Zustand und Betrieb von Cloud Volumes ONTAP PAYGO-Systemen. Wenn ein Konnektor heruntergefahren wird, werden die Cloud Volumes ONTAP PAYGO-Systeme nach einem Verlust der Kommunikation mit einem Konnektor länger als 14 Tage heruntergefahren.

Die SaaS-Plattform ist für Regierungsregionen deaktiviert

Wenn Sie einen Connector in einer AWS GovCloud Region, einer Azure Gov-Region oder einer Azure DoD-Region implementieren, ist der Zugriff auf Cloud Manager nur über die Host-IP-Adresse eines Connectors verfügbar. Der Zugriff auf die SaaS-Plattform ist für das gesamte Konto deaktiviert.

Das bedeutet, dass nur privilegierte Benutzer, die auf die interne VPC/vnet des Endbenutzers zugreifen können, die UI oder die API von Cloud Manager verwenden können.

Das bedeutet auch, dass folgende Services bei Cloud Manager nicht verfügbar sind:

- Cloud-Compliance
- Kubernetes
- Cloud Tiering
- Globaler Datei-Cache
- Monitoring (Cloud Insights)

Zur Nutzung dieser Services ist die SaaS-Plattform erforderlich.

Freigegebene Linux-Hosts werden nicht unterstützt

Der Connector wird nicht auf einem Host unterstützt, der für andere Anwendungen freigegeben ist. Der Host muss ein dedizierter Host sein.

Cloud Manager unterstützt FlexGroup Volumes nicht

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

Wichtige Änderungen in Cloud Manager

Auf dieser Seite werden wichtige Änderungen im Cloud Manager vorgestellt, mit denen Sie den Service bei der Einführung neuer Verbesserungen nutzen können. Sie sollten weiterhin die lesen "Was ist neu" Seite an, um mehr über alle neuen Funktionen und Verbesserungen zu erfahren.

SaaS-Änderungen

Wir haben für Cloud Manager ein Software-als-Service-Erlebnis auf den Markt gebracht. Durch diese neue Erfahrung können Sie Cloud Manager einfacher nutzen. Wir stellen zusätzliche Funktionen zum Management Ihrer Hybrid-Cloud-Infrastruktur bereit.

- "Cloud Manager Transition zu SaaS"
- "Funktionsweise von Cloud Manager"

Maschinentyp ändert sich

Um sicherzustellen, dass in Cloud Manager genügend Ressourcen für neue und neue Funktionen zur Verfügung stehen, haben wir das erforderliche Minimum an Instanz, VM und Maschinentyp wie folgt geändert:

- AWS: t3.xlarge
- Azure: DS3 v2
- GCP: n1-Standard-4

Wenn Sie einen Maschinentyp aktualisieren, erhalten Sie Zugriff auf Funktionen wie die neue Kubernetes Erfahrung, den globalen File Cache, das Monitoring usw.

Diese Standardgrößen werden als Minimum unterstützt "Basierend auf CPU- und RAM-Anforderungen".

Cloud Manager fordert Sie dazu auf, den Maschinentyp des Connectors zu ändern.

Kontoeinstellungen

Wir haben Cloud Central-Konten eingeführt, um Mandantenfähigkeit zu bieten, um Benutzer und Ressourcen in isolierten Arbeitsbereichen zu organisieren und den Zugriff auf Connectors und Abonnements zu managen.

- "Weitere Informationen zu Cloud Central-Konten: Benutzer, Arbeitsbereiche, Steckverbinder und Abonnements"
- "Erste Schritte mit Ihrem Konto"
- "Erfahren Sie, wie Sie Ihr Konto verwalten, nachdem Sie es eingerichtet haben"

Neue Berechtigungen

Für Cloud Manager sind gelegentlich zusätzliche Berechtigungen für Cloud-Provider erforderlich, wenn wir neue Funktionen und Verbesserungen einführen. In diesem Abschnitt werden neue Berechtigungen aufgeführt, die jetzt erforderlich sind.

Die aktuelle Liste der Berechtigungen finden Sie auf der "Die Richtlinien von Cloud Manager".

AWS

Ab Version 3.8.1 sind für die Verwendung von Backup in Cloud mit Cloud Volumes ONTAP die folgenden Berechtigungen erforderlich. "Weitere Informationen .".

```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

Azure

- Um Azure-Bereitstellungsausfälle zu vermeiden, stellen Sie sicher, dass Ihre Cloud Manager-Richtlinie in Azure die folgende Berechtigung enthält:

  ```
  "Microsoft.Resources/deployments/operationStatuses/read"
  ```

- Ab Version 3.8.7 ist die folgende Berechtigung erforderlich, um von Azure verwaltete Festplatten auf Cloud Volumes ONTAP-Systemen mit einem einzelnen Node mit externen Schlüsseln aus einem anderen Konto zu verschlüsseln. "Weitere Informationen .".

  ```
  "Microsoft.Compute/diskEncryptionSets/read"
  ```

- Zur Aktivierung des globalen Dateicache auf Cloud Volumes ONTAP sind die folgenden Berechtigungen erforderlich. "Weitere Informationen .".

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

GCP

Neue Berechtigungen für Kubernetes Management

Ab Version 3.8.8 erfordert das Servicekonto für einen Connector die folgenden Berechtigungen, um Kubernetes-Cluster zu erkennen und zu managen, die in der Google Kubernetes Engine (GKE) ausgeführt werden:

```
- container.*
```

Neue Berechtigungen für Daten-Tiering

Ab Version 3.8 sind zur Verwendung eines Servicekontos für Daten-Tiering die folgenden Berechtigungen erforderlich. "Weitere Informationen .".

```
- storage.buckets.update
- compute.instances.setServiceAccount
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
```

Neue Endpunkte

Für den Connector ist ein abgehender Internetzugang erforderlich, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung zu managen. In diesem Abschnitt werden neue Endpunkte identifiziert, die jetzt erforderlich sind.

Sie finden die "Eine vollständige Liste der Endpunkte, auf die Sie über Ihren Webbrowser zugreifen können" Und das "Vollständige Liste der Endpunkte, auf die der Connector hier zugreifen kann".

- Benutzer müssen über einen Webbrowser auf Cloud Manager zugreifen, indem sie den folgenden Endpunkt kontaktieren:

  https://cloudmanager.netapp.com

- Für Konnektoren ist der Zugriff auf den folgenden Endpunkt erforderlich, um Software-Images von Container-Komponenten für eine Docker Infrastruktur zu erhalten:

  https://cloudmanagerinfraprod.azurecr.io

  Stellen Sie sicher, dass Ihre Firewall über den Connector den Zugriff auf diesen Endpunkt ermöglicht.

Erste Schritte mit Cloud Manager

Informationen zu Cloud Manager

Cloud Manager ist IT-Experten und Cloud-Architekten in der Lage, ihre Hybrid-Multi-Cloud-Infrastruktur mithilfe der Cloud-Lösungen von NetApp zentral zu managen.

Funktionen

Als SaaS-basierte Managementplattform der Enterprise-Klasse behalten Sie stets die Kontrolle über Ihre Daten – unabhängig vom Speicherort.

- Einrichtung und Verwendung "Cloud Volumes ONTAP" Für effizientes, Cloud-übergreifendes Multi-Protokoll-Datenmanagement
- Einrichten und Verwenden von File-Storage-Services: "Azure NetApp Dateien", "Cloud Volumes Service für AWS", und "Cloud Volumes Service für Google Cloud".
- Lokale ONTAP-Cluster erkennen und managen, indem sie Volumes erstellen, Backups in der Cloud erstellen, Daten in der gesamten Hybrid Cloud replizieren und selten genutzte Daten per Tiering in die Cloud verschieben.
- Ermöglichen Sie integrierte Cloud-Services und -Software wie "Cloud-Compliance", "Einblicke in die Cloud", "Cloud-Backup-Service", "Trident", Und vieles mehr.

"Erfahren Sie mehr über Cloud Manager".

Unterstützte Objekt-Storage-Provider

Cloud Manager ermöglicht Ihnen das Management von Cloud Storage und die Verwendung von Cloud-Services in Amazon Web Services, Microsoft Azure und Google Cloud.

Kosten

NetApp Cloud Manager ist kostenfrei.

Bei den meisten Aufgaben fordert Cloud Manager Sie zur Implementierung eines Connectors in Ihrem Cloud-Netzwerk auf. Dadurch werden von Ihrem Cloud-Provider Kosten für die Computing-Instanz und den zugehörigen Storage erhoben. Sie haben die Möglichkeit, die Connector-Software vor Ort auszuführen.

Funktionsweise von Cloud Manager

Cloud Manager umfasst eine SaaS-basierte Schnittstelle, die in NetApp Cloud Central integriert ist, sowie Connectors, die Cloud Volumes ONTAP und andere Cloud-Services managen.

Software-as-a-Service

Der Zugriff auf Cloud Manager ist über ein möglich "SaaS-basierte Benutzeroberfläche" Und APIs. Mit dieser SaaS-Erfahrung können Sie automatisch auf die neuesten Funktionen zugreifen, sobald sie veröffentlicht wurden, und Sie können einfach zwischen Ihren Cloud Central-Konten und -Connectors wechseln.

NetApp Cloud Central

"NetApp Cloud Central" Bietet einen zentralen Standort für den Zugriff und das Management "NetApp Cloud-Services". Durch die zentrale Benutzerauthentifizierung können Sie dieselben Anmeldedaten für den Zugriff auf Cloud Manager und andere Cloud-Services wie Cloud Insights verwenden.

Wenn Sie sich zum ersten Mal bei Cloud Manager anmelden, werden Sie aufgefordert, ein *Cloud Central Konto* zu erstellen. Dieses Konto bietet Mandantenfähigkeit und ermöglicht es Ihnen, Benutzer und Ressourcen in isolierten Arbeitsbereichen zu organisieren_.

Anschlüsse

In den meisten Fällen muss ein Account-Administrator einen *Connector* in Ihrer Cloud oder Ihrem On-Premises-Netzwerk bereitstellen. Mit dem Connector kann Cloud Manager Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen.

Ein Steckverbinder sollte immer weiter laufen. Es ist wichtig für den fortwährenden Zustand und Betrieb der Services, die Sie ermöglichen.

Ein Connector ist beispielsweise eine wichtige Komponente im Zustand und Betrieb von Cloud Volumes ONTAP PAYGO-Systemen. Wenn ein Konnektor heruntergefahren wird, werden die Cloud Volumes ONTAP PAYGO-Systeme nach einem Verlust der Kommunikation mit einem Konnektor länger als 14 Tage heruntergefahren.

"Erfahren Sie mehr darüber, wann Anschlüsse erforderlich sind und wie sie funktionieren".

Netzwerkübersicht

Bevor sich Benutzer bei Cloud Manager anmelden, müssen Sie sicherstellen, dass ihre Webbrowser auf bestimmte Endpunkte zugreifen können. Danach müssen Sie die Netzwerkanforderungen für die spezifische Arbeitsumgebung und Services überprüfen, die verwendet werden.

Endpunkte, auf die über Ihren Webbrowser zugegriffen wird

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

Endpunkte	Zweck
https://cloudmanager.cloud.netapp.com	Um eine Verbindung zur Cloud Manager SaaS-Schnittstelle herzustellen.
https://api.services.cloud.netapp.com	Für den Kontakt mit Cloud Central APIs.
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.

Index der Netzwerkanforderungen

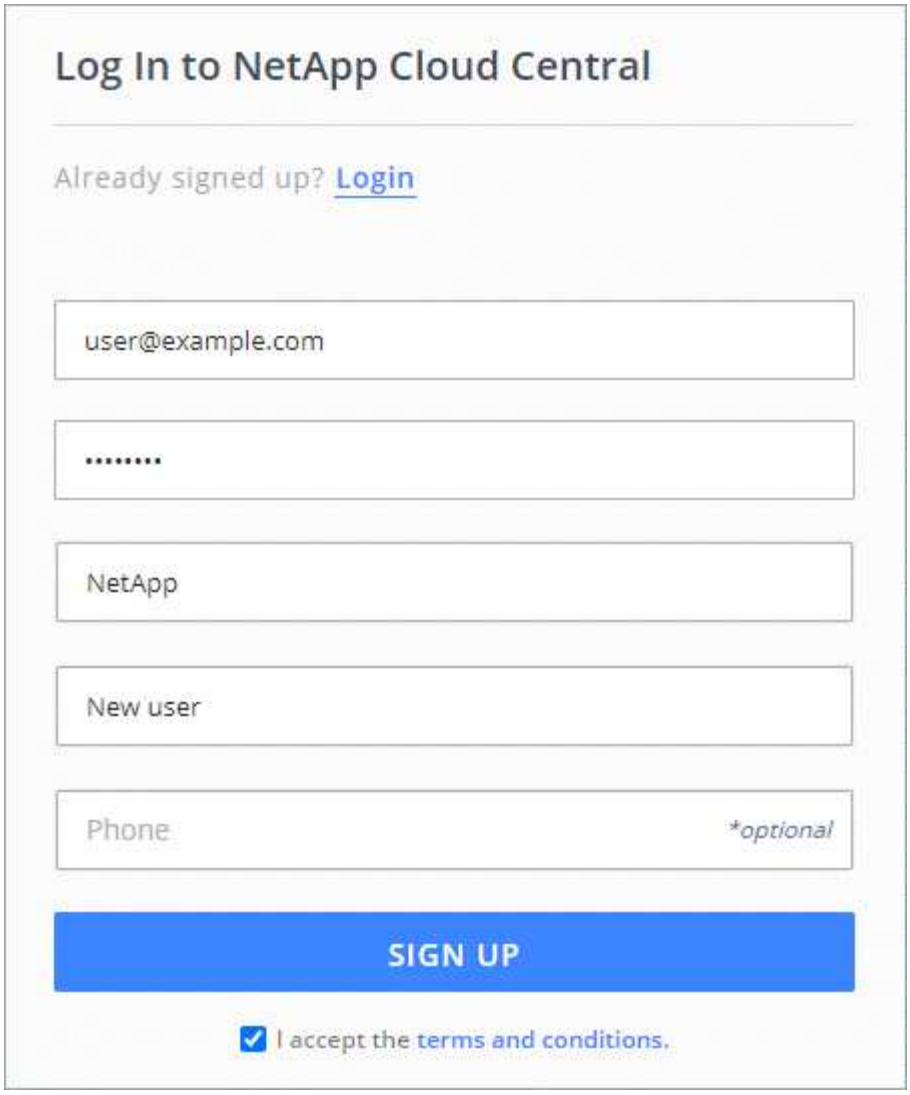
- "Anschlüsse"
- "Cloud Volumes ONTAP für AWS"
- "Cloud Volumes ONTAP für Azure"
- "Cloud Volumes ONTAP für GCP"
- "Datenreplizierung zwischen ONTAP Systemen"
- "Cloud Compliance für Cloud Volumes ONTAP oder Azure NetApp Files"
- "Cloud Compliance für Amazon S3"
- "ONTAP-Cluster vor Ort"
  - "Daten-Tiering von ONTAP Clustern zu Amazon S3"
  - "Daten-Tiering von ONTAP Clustern zu Azure Blob Storage"
  - "Daten-Tiering von ONTAP Clustern zu Google Cloud Storage"
  - "Daten-Tiering von ONTAP Clustern zu StorageGRID"

Anmeldung bei NetApp Cloud Central

Melden Sie sich bei NetApp Cloud Central an, um auf die Cloud-Services von NetApp zuzugreifen.

Schritte

1. Öffnen Sie einen Webbrowser, und gehen Sie zu "NetApp Cloud Central".
2. Klicken Sie Auf **Registrieren**.
3. Füllen Sie das Formular aus und klicken Sie auf **Registrieren**.



4. Warten Sie auf eine E-Mail von NetApp Cloud Central.
5. Klicken Sie auf den Link in der E-Mail, um Ihre E-Mail-Adresse zu überprüfen.

Ergebnis

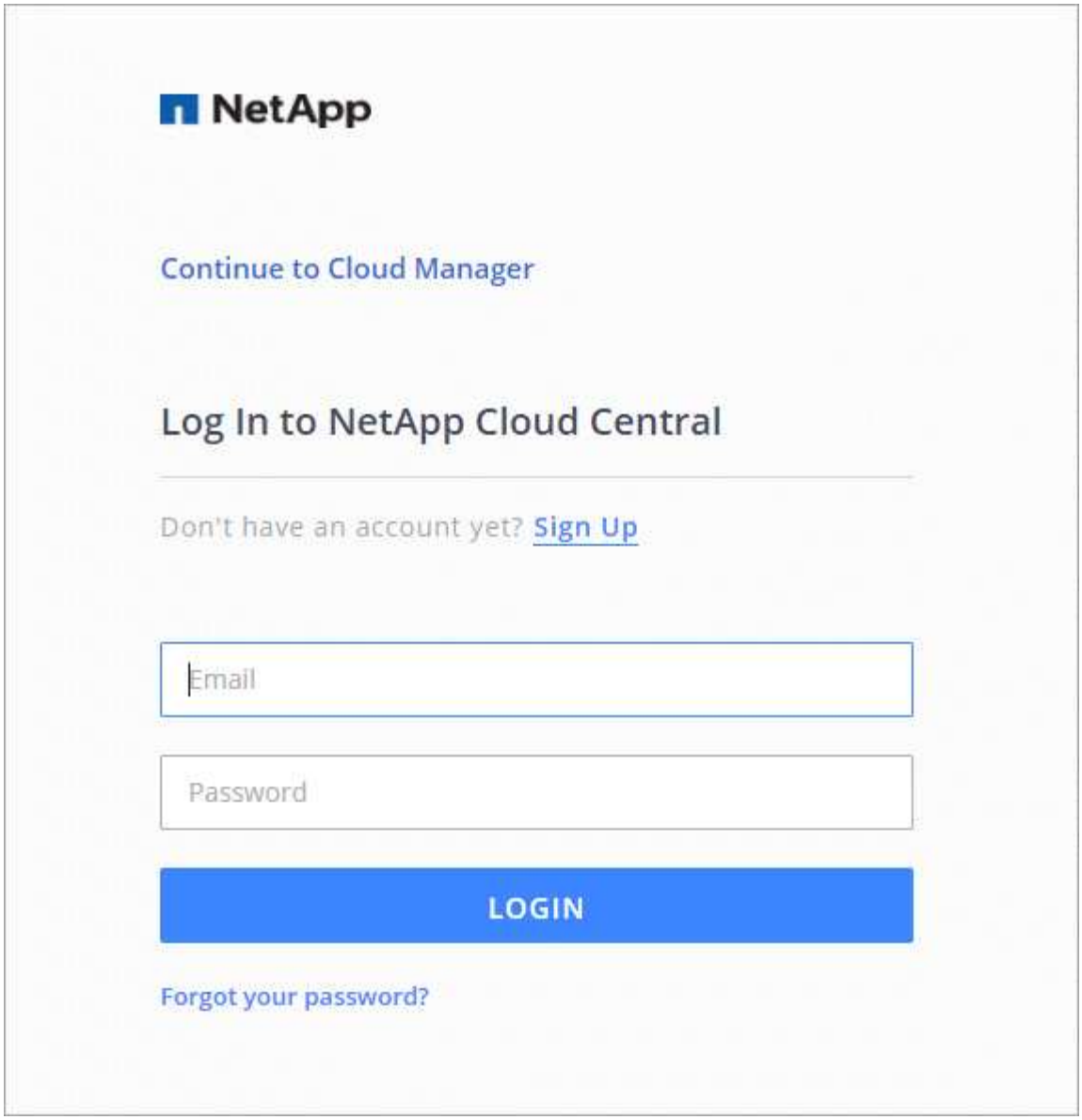
Sie haben jetzt eine aktive Cloud Central-Benutzeranmeldung.

Anmelden bei Cloud Manager

Der Zugriff auf die Cloud Manager-Schnittstelle ist über eine SaaS-basierte Benutzeroberfläche von unter bis möglich https://cloudmanager.netapp.com.

Schritte

1. Öffnen Sie einen Webbrowser, und gehen Sie zu https://cloudmanager.netapp.com.
2. Melden Sie sich mit Ihren NetApp Cloud Central Anmeldedaten an.



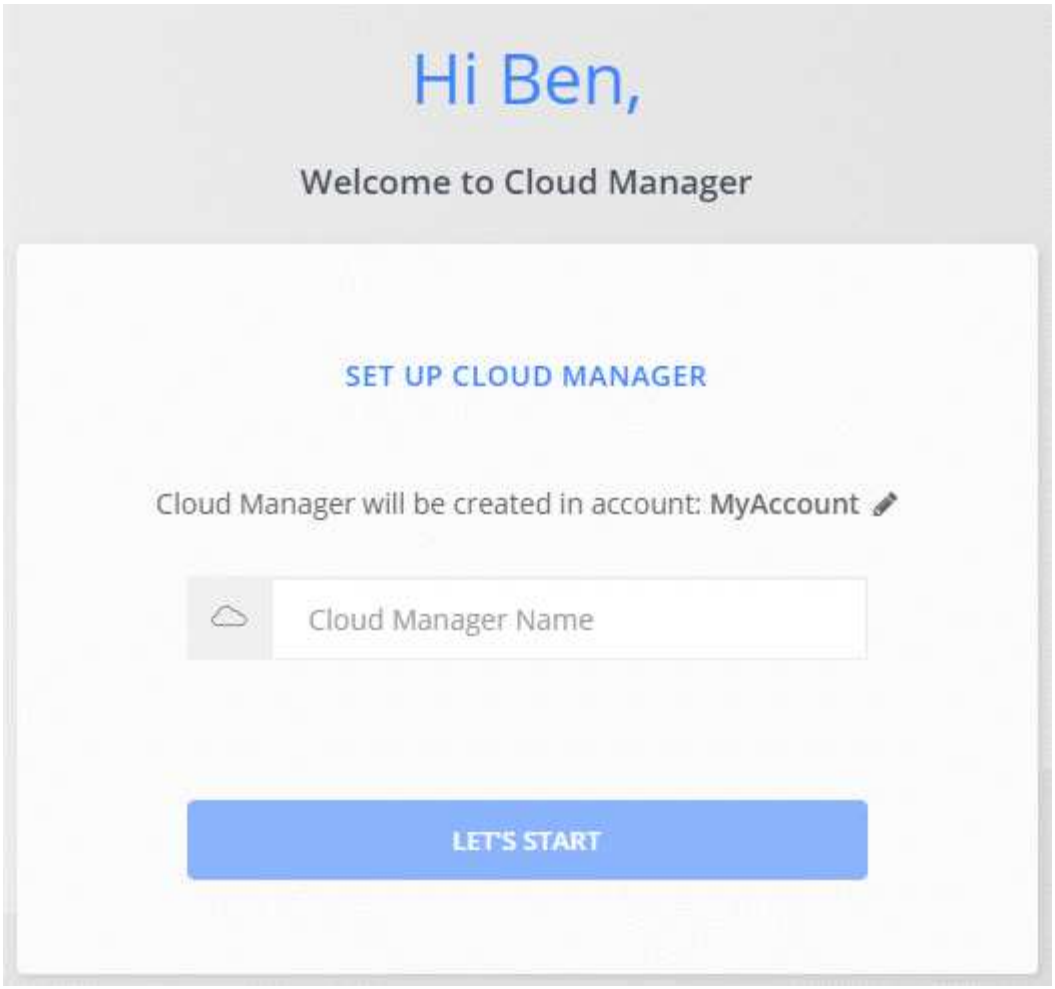
Richten Sie ein Cloud Central-Konto ein

Kontoeinstellungen: Benutzer, Arbeitsbereiche, Anschlüsse und Abonnements

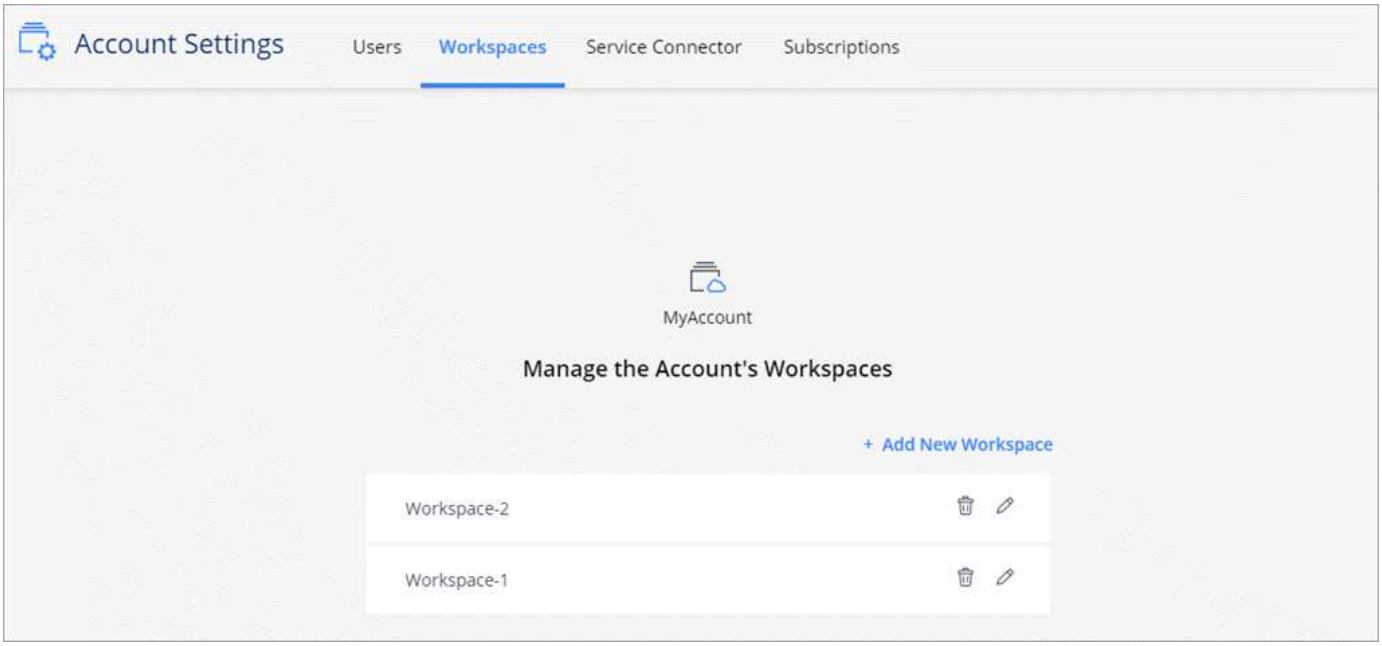
Ein *Cloud Central Konto* bietet Mandantenfähigkeit und ermöglicht die Organisation von Benutzern und Ressourcen in isolierten Arbeitsbereichen innerhalb von Cloud Manager.

So können beispielsweise mehrere Benutzer Cloud Volumes ONTAP Systeme in isolierten Umgebungen, sogenannte *Workspaces*, implementieren und managen. Diese Arbeitsbereiche sind für andere Benutzer unsichtbar, es sei denn, sie werden gemeinsam genutzt.

Wenn Sie zum ersten Mal auf Cloud Manager zugreifen, werden Sie aufgefordert, ein Cloud Central Konto auszuwählen oder zu erstellen:



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



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

Kontoeinstellungen

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

Benutzer

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

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

- *Account Admin*: Kann jede Aktion im Cloud Manager ausführen.
- *Workspace Admin*: Kann Ressourcen im zugewiesenen Arbeitsbereich erstellen und verwalten.
- *Cloud Compliance Viewer*: Kann Compliance-Informationen nur anzeigen und Berichte für Systeme generieren, auf die sie zugreifen können.

Arbeitsbereiche

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

Eine Arbeitsumgebung ist ein Speichersystem:

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

Anschlüsse

Ein Connector ermöglicht Cloud Manager das Managen von Ressourcen und Prozessen in Ihrer Public Cloud-Umgebung. Der Connector wird auf einer Virtual-Machine-Instanz ausgeführt, die Sie bei Ihrem Cloud-Provider implementieren, oder auf einem von Ihnen konfigurierten On-Premises-Host.

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

Abonnements

Im Widget „Account Settings“ werden die NetApp Abonnements für das ausgewählte Konto angezeigt.

Wenn Sie Cloud Manager über den Marktplatz eines Cloud-Providers abonnieren, werden Sie zu Cloud Central umgeleitet. Dort müssen Sie Ihr Abonnement speichern und einem bestimmten Konto zuordnen.

Nach der Anmeldung steht jedes Abonnement über das Widget „Kontoeinstellungen“ zur Verfügung. Sie sehen nur die Abonnements, die mit dem Konto verknüpft sind, das Sie derzeit anzeigen.

Sie haben die Möglichkeit, ein Abonnement umzubenennen und das Abonnement von einem oder mehreren Konten zu entfernen.

Nehmen wir zum Beispiel an, dass Sie zwei Konten haben und jedes über separate Abonnements abgerechnet wird. Sie können ein Abonnement von einem der Konten ablösen, so dass die Benutzer in diesem Konto nicht versehentlich das falsche Abonnement wählen, wenn Sie eine Cloud Volume ONTAP Arbeitsumgebung erstellen.

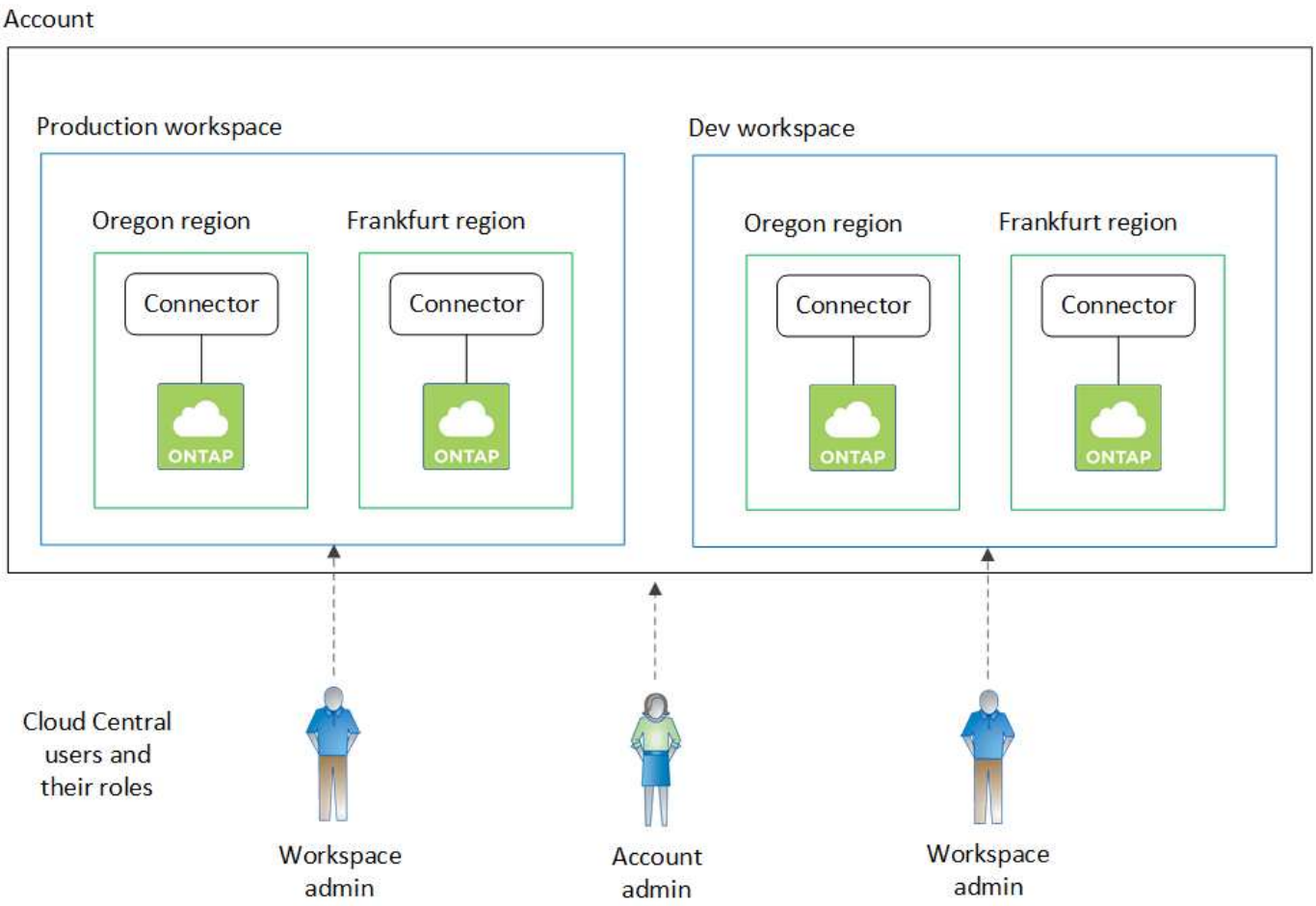
Beispiele

In den folgenden Beispielen wird veranschaulicht, wie Sie Ihre Konten einrichten könnten.

> In den folgenden Beispielabbildern sollten der Connector und die Cloud Volumes ONTAP Systeme nicht *in* dem NetApp Cloud Central Account residieren – sie laufen bei einem Cloud-Provider. Dies ist eine konzeptionelle Darstellung der Beziehung zwischen den einzelnen Komponenten.

Beispiel 1

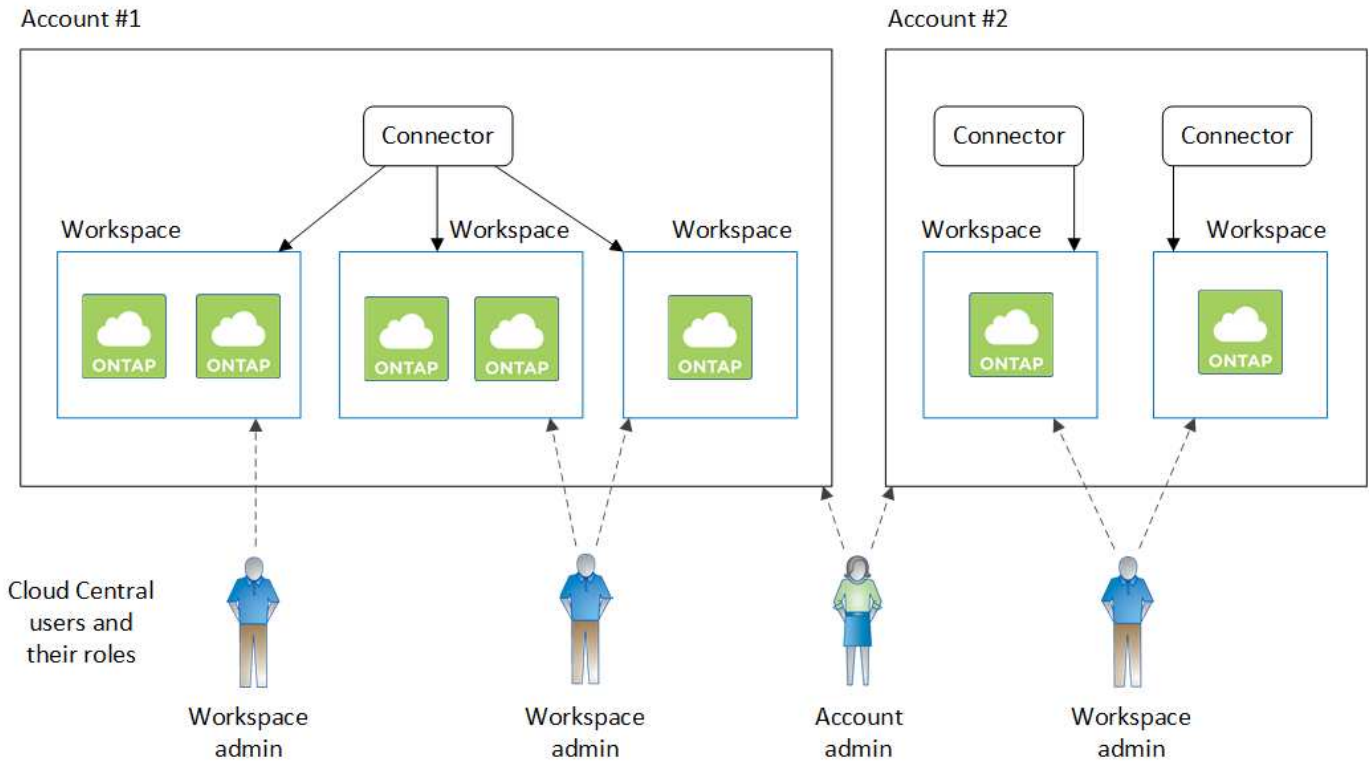
Das folgende Beispiel zeigt ein Konto, das zwei Arbeitsbereiche zum Erstellen isolierter Umgebungen verwendet. Der erste Arbeitsbereich ist für eine Produktionsumgebung und der zweite für eine Entwicklungsumgebung.



Beispiel 2

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

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



Einrichtung von Workspaces und Benutzern im Cloud Central Konto

Wenn Sie sich zum ersten Mal bei Cloud Manager anmelden, werden Sie aufgefordert, ein *NetApp Cloud Central Konto* zu erstellen. Dieses Konto bietet Mandantenfähigkeit und ermöglicht es Ihnen, Benutzer und Ressourcen in isolierten Arbeitsbereichen zu organisieren_.

"Erfahren Sie mehr über die Funktionsweise von Cloud Central-Accounts".

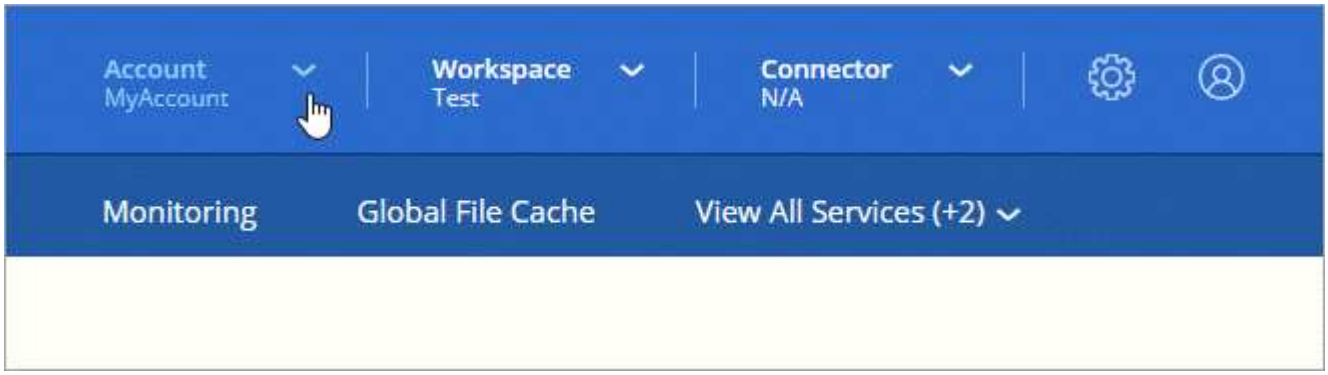
Richten Sie Ihr Cloud Central-Konto ein, damit Benutzer in einem Arbeitsbereich auf Cloud Manager zugreifen können. Fügen Sie einfach einen einzelnen Benutzer hinzu oder fügen Sie mehrere Benutzer und Arbeitsbereiche hinzu.

Arbeitsbereiche werden hinzugefügt

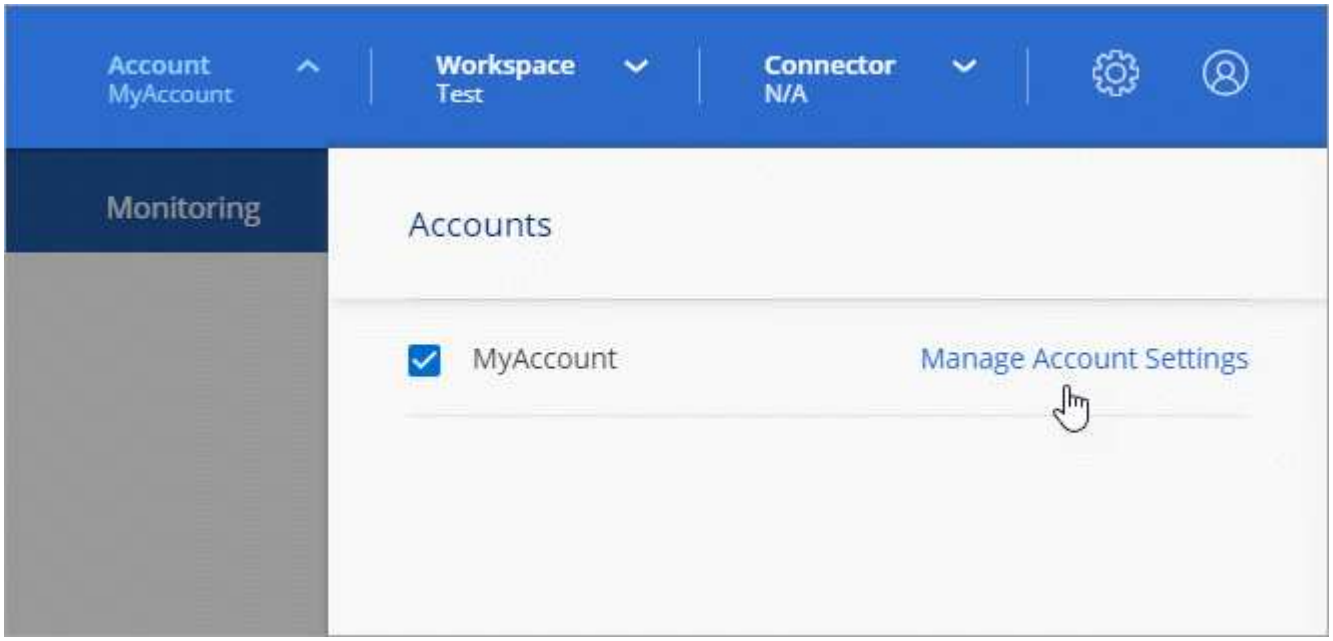
In Cloud Manager können Sie mithilfe von Workspaces eine Reihe von Arbeitsumgebungen von anderen Arbeitsumgebungen und anderen Benutzern isolieren. Sie können beispielsweise zwei Arbeitsbereiche erstellen und jedem Arbeitsbereich separate Benutzer zuordnen.

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto**.



2. Klicken Sie neben dem aktuell ausgewählten Konto auf **Konto verwalten**.



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

Nachdem Sie fertig sind

Wenn ein Workspace-Administrator Zugriff auf diesen Arbeitsbereich benötigt, müssen Sie den Benutzer zuordnen. Außerdem müssen Sie Connectors mit dem Arbeitsbereich verknüpfen, damit Arbeitsbereichsadministratoren diese Connectors verwenden können.

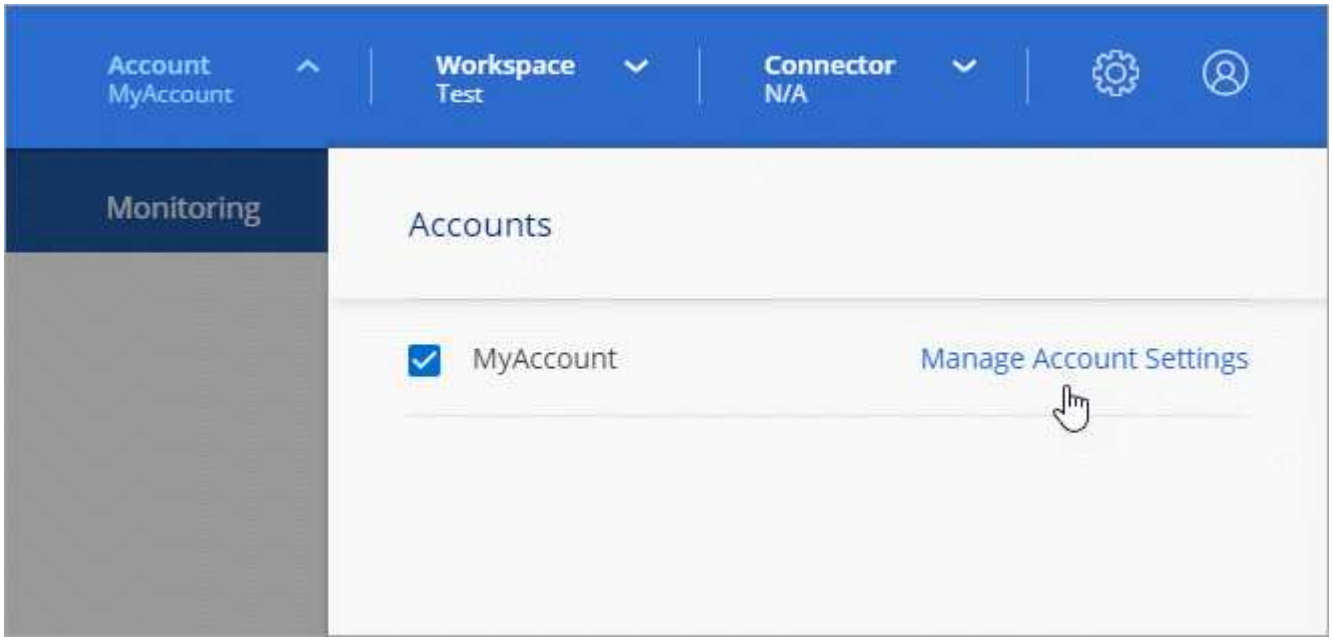
Benutzer hinzufügen

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

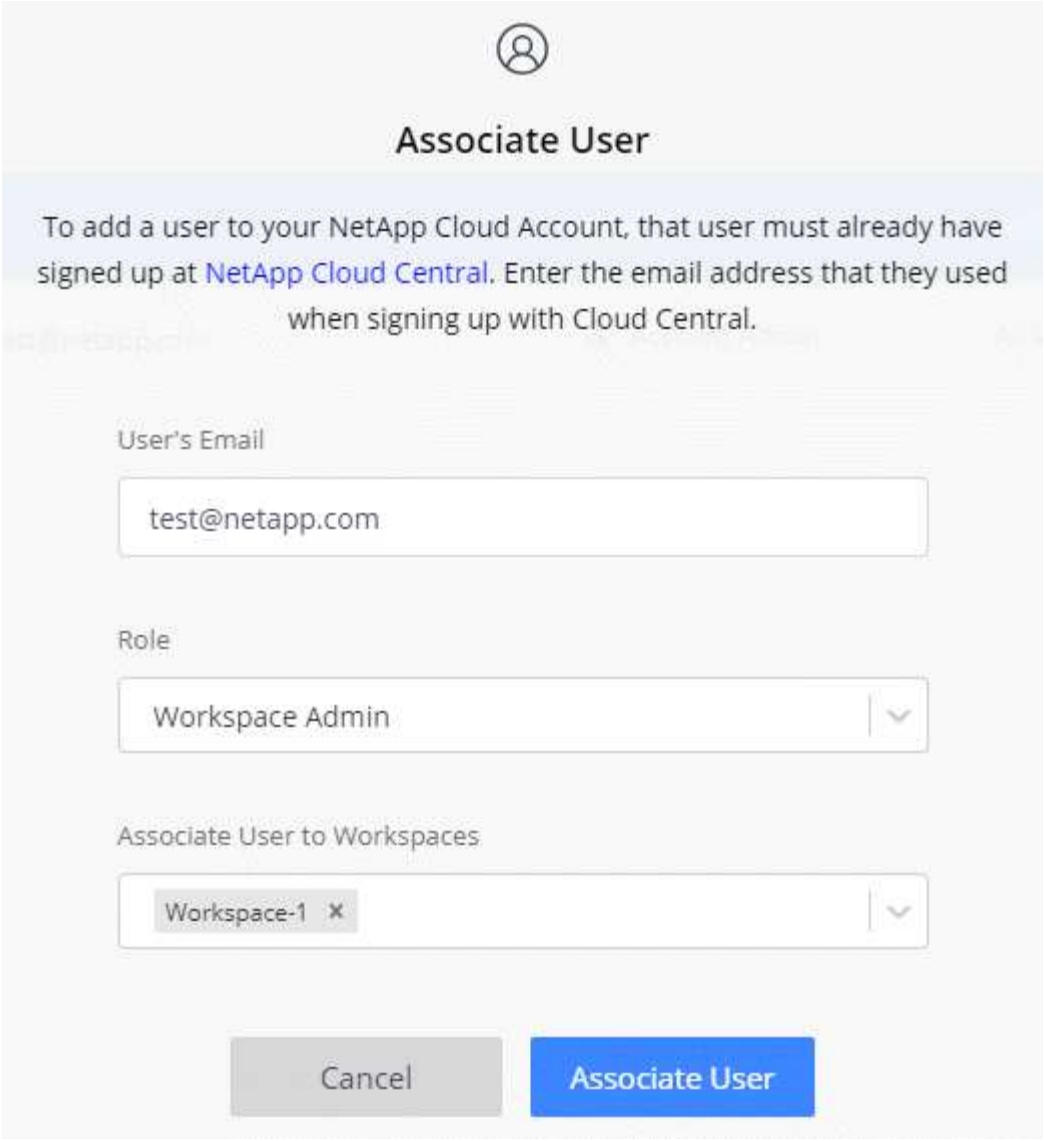
Schritte

1. Wenn der Benutzer dies noch nicht getan hat, bitten Sie den Benutzer, zu wechseln "NetApp Cloud Central" Und melden Sie sich an.

2. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.



3. Klicken Sie auf der Registerkarte Benutzer auf **Benutzer verknüpfen**.
4. Geben Sie die E-Mail-Adresse des Benutzers ein, und wählen Sie eine Rolle für den Benutzer aus:
   - **Account Admin**: Kann jede Aktion in Cloud Manager ausführen.
   - **Workspace Admin**: Kann Ressourcen in zugewiesenen Workspaces erstellen und verwalten.
   - **Compliance Viewer**: Kann nur Compliance-Informationen anzeigen und Berichte für Arbeitsbereiche erstellen, auf die sie zugreifen können.
5. Wenn Sie Workspace Admin oder Compliance Viewer ausgewählt haben, wählen Sie eine oder mehrere Arbeitsbereiche aus, die diesem Benutzer zugeordnet werden sollen.



6. Klicken Sie Auf * Benutzer Verknüpfen*.

Ergebnis

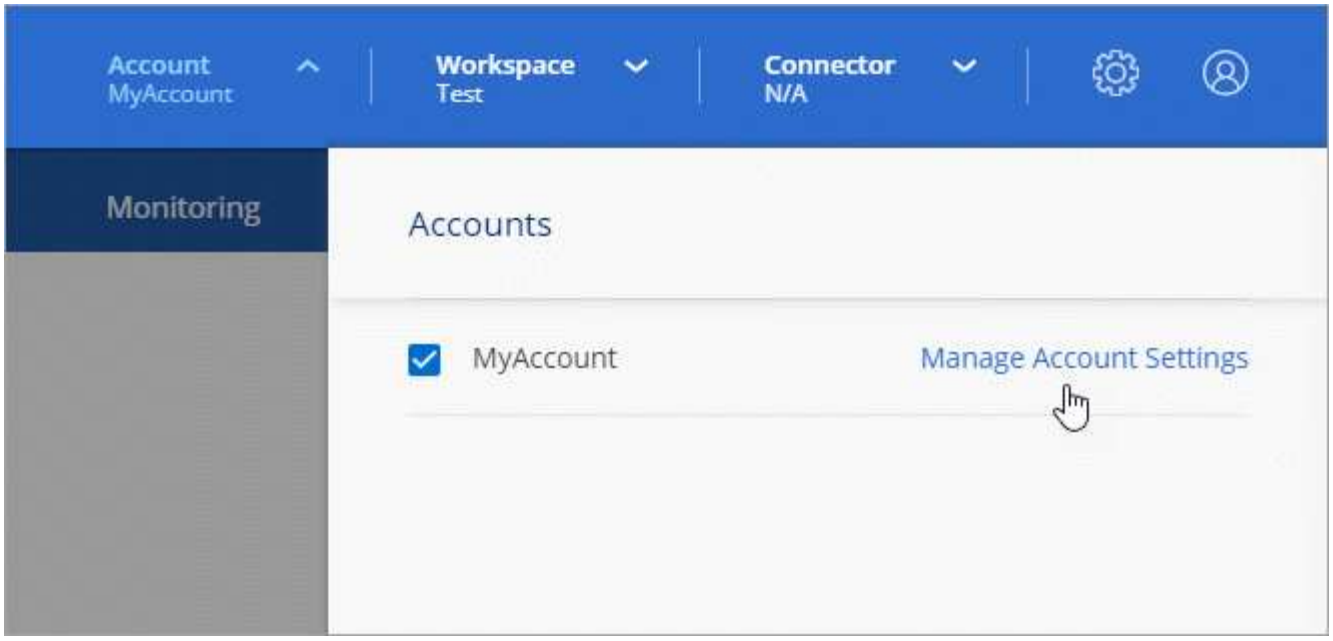
Der Benutzer sollte eine E-Mail von NetApp Cloud Central mit dem Titel „Account Association“ erhalten. Die E-Mail enthält die für den Zugriff auf Cloud Manager erforderlichen Informationen.

Verknüpfen von Workspace-Administratoren mit Arbeitsbereichen

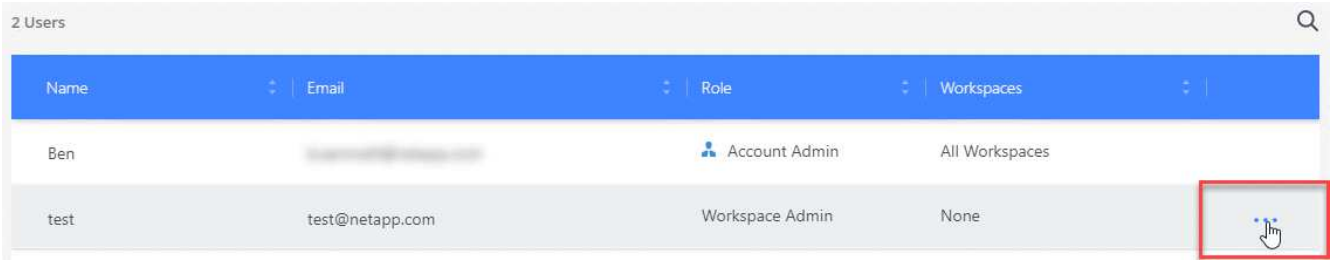
Sie können Workspace-Administratoren jederzeit mit zusätzlichen Arbeitsbereichen verknüpfen. Durch die Verknüpfung des Benutzers können die Arbeitsumgebungen in diesem Arbeitsbereich erstellt und angezeigt werden.

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.



2. Klicken Sie auf der Registerkarte Benutzer auf das Aktionsmenü in der Zeile, die dem Benutzer entspricht.



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

Ergebnis

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

Verknüpfen von Connectors mit Arbeitsbereichen

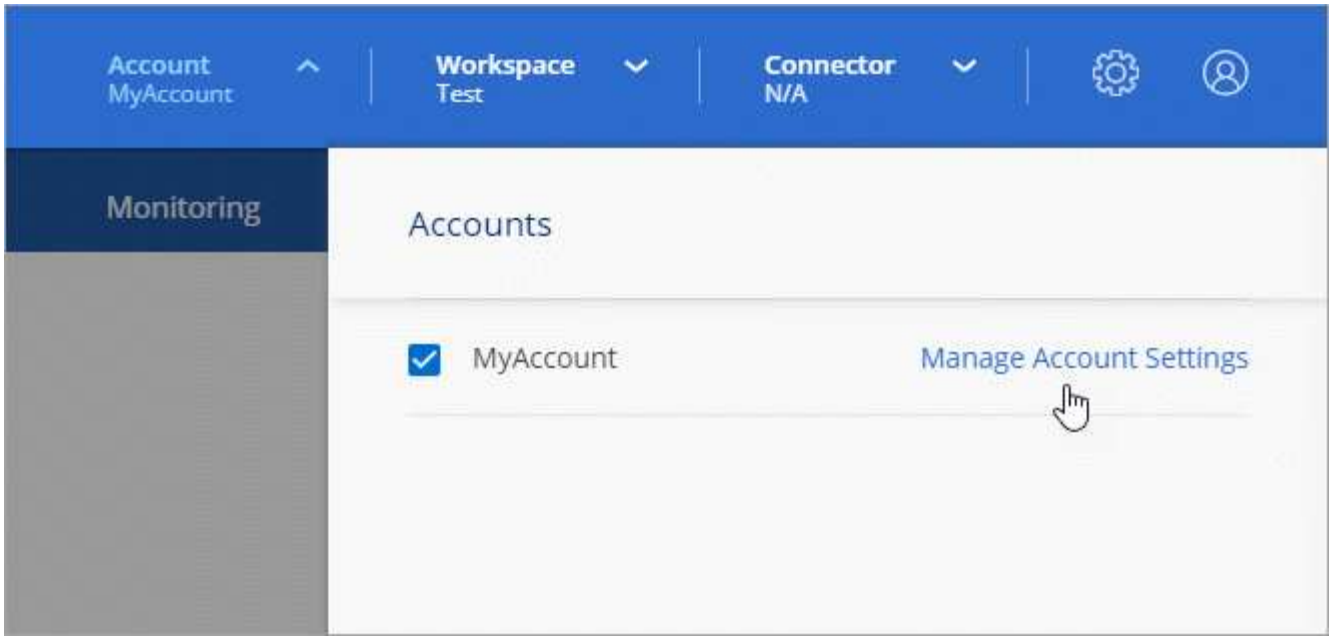
Sie müssen einen Connector mit Arbeitsbereichen verknüpfen, damit Arbeitsbereichsadministratoren diese Connectors zum Erstellen von Cloud Volumes ONTAP-Systemen verwenden können.

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

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

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.



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

Ergebnis

Workspace-Administratoren können diese Anschlüsse jetzt verwenden, um Cloud Volumes ONTAP-Systeme zu erstellen.

Was kommt als Nächstes?

Nachdem Sie Ihr Konto eingerichtet haben, können Sie es jederzeit verwalten, indem Sie Benutzer entfernen, Arbeitsbereiche, Connectors und Abonnements verwalten. "Weitere Informationen .".

Richten Sie einen Konnektor ein

Erfahren Sie mehr über Steckverbinder

In den meisten Fällen muss ein Account-Administrator einen *Connector* in Ihrer Cloud oder Ihrem On-Premises-Netzwerk bereitstellen. Mit dem Connector kann Cloud Manager Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen.

Wenn ein Stecker erforderlich ist

Für die Nutzung der folgenden Funktionen in Cloud Manager ist ein Connector erforderlich:

- Cloud Volumes ONTAP
- On-Premises ONTAP Cluster
- Cloud-Compliance
- Kubernetes
- Backup in die Cloud

- Monitoring
- Lokales Tiering
- Globaler Datei-Cache
- Amazon S3 Bucket-Erkennung

Für Azure NetApp Files, Cloud Volumes Service oder Cloud Sync ist ein Stecker *_Not_* erforderlich.

> Während kein Connector für die Einrichtung und das Management von Azure NetApp Files erforderlich ist, ist jedoch ein Connector erforderlich, wenn Sie Azure NetApp Files-Daten mithilfe von Cloud Compliance scannen möchten.

Unterstützte Standorte

Ein Connector wird an folgenden Stellen unterstützt:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- Vor Ort

> Wenn Sie ein Cloud Volumes ONTAP-System in Google Cloud erstellen möchten, dann müssen Sie einen Connector in Google Cloud laufen, sowie. Sie können keinen Konnektor verwenden, der an einem anderen Standort ausgeführt wird.

Anschlüsse sollten weiterhin ausgeführt werden

Ein Steckverbinder sollte immer weiter laufen. Es ist wichtig für den fortwährenden Zustand und Betrieb der Services, die Sie ermöglichen.

Ein Connector ist beispielsweise eine wichtige Komponente im Zustand und Betrieb von Cloud Volumes ONTAP PAYGO-Systemen. Wenn ein Konnektor heruntergefahren wird, werden die Cloud Volumes ONTAP PAYGO-Systeme nach einem Verlust der Kommunikation mit einem Konnektor länger als 14 Tage heruntergefahren.

So erstellen Sie einen Konnektor

Ein Kontoadministrator muss einen Konnektor erstellen, bevor ein Workspace-Administrator eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen und eine der anderen oben aufgeführten Funktionen verwenden kann.

Ein Kontoadministrator kann auf verschiedene Arten einen Connector erstellen:

- Direkt über Cloud Manager (empfohlen)
  - "In AWS erstellen"
  - "In Azure erstellen"
  - "In GCP erstellen"
- "Über AWS Marketplace"
- "Über den Azure Marketplace"

- "Durch Herunterladen und Installieren der Software auf einem vorhandenen Linux-Host"

Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von Cloud Manager aufgefordert, einen Connector zu erstellen, falls noch kein Connector vorhanden ist.

Berechtigungen

Zur Erstellung des Connectors sind spezielle Berechtigungen erforderlich, und für die Instanz des Connectors selbst sind weitere Berechtigungen erforderlich.

Berechtigungen zum Erstellen eines Connectors

Der Benutzer, der einen Connector aus Cloud Manager erstellt, benötigt spezielle Berechtigungen, um die Instanz bei Ihrem bevorzugten Cloud-Provider bereitzustellen. Cloud Manager erinnert Sie an die Berechtigungsanforderungen bei der Erstellung eines Connectors.

"Zeigen Sie Richtlinien für jeden Cloud-Provider an".

Berechtigungen für die Connector-Instanz

Für die Ausführung von Vorgängen in Ihrem Auftrag benötigt der Connector spezielle Cloud-Provider-Berechtigungen. Beispiel für die Implementierung und das Management von Cloud Volumes ONTAP.

Wenn Sie einen Connector direkt aus Cloud Manager erstellen, erstellt Cloud Manager den Connector mit den entsprechenden Berechtigungen. Es gibt nichts, was Sie tun müssen.

Wenn Sie den Connector selbst über AWS Marketplace, Azure Marketplace oder die Software manuell installieren, müssen Sie sicherstellen, dass die entsprechenden Berechtigungen vorhanden sind.

"Zeigen Sie Richtlinien für jeden Cloud-Provider an".

Wann werden mehrere Anschlüsse verwendet

In einigen Fällen benötigen Sie möglicherweise nur einen Connector, aber Sie benötigen möglicherweise zwei oder mehr Anschlüsse.

Hier nur ein paar Beispiele:

- Sie nutzen eine Multi-Cloud-Umgebung (AWS und Azure), d. h. einen Connector in AWS und einen anderen in Azure. Jedes managt die Cloud Volumes ONTAP Systeme, die in diesen Umgebungen ausgeführt werden.
- Ein Service-Provider nutzt möglicherweise ein Cloud Central Konto, um seinen Kunden Services bereitzustellen, und nutzt ein anderes Konto, um eine seiner Geschäftsbereiche Disaster Recovery zu bieten. Jedes Konto hätte separate Anschlüsse.

Wann muss zwischen den Anschlüssen gewechselt werden

Wenn Sie Ihren ersten Connector erstellen, verwendet Cloud Manager diesen Connector automatisch für jede von Ihnen erstellte zusätzliche Arbeitsumgebung. Wenn Sie einen zusätzlichen Connector erstellen, müssen Sie zwischen diesen wechseln, um die für jeden Connector spezifischen Arbeitsumgebungen zu sehen.

"Erfahren Sie, wie Sie zwischen den Anschlüssen wechseln".

Die lokale Benutzeroberfläche

Während Sie fast alle Aufgaben aus dem ausführen sollten "SaaS-Benutzeroberfläche", Eine lokale Benutzeroberfläche ist weiterhin auf dem Connector verfügbar. Diese Schnittstelle wird für einige Aufgaben benötigt, die über den Connector selbst ausgeführt werden müssen:

- "Festlegen eines Proxyservers"
- Installation eines Patches (Sie arbeiten in der Regel mit NetApp Mitarbeitern zusammen, um einen Patch zu installieren)
- Herunterladen von AutoSupport-Meldungen (normalerweise gerichtet von NetApp Mitarbeitern, wenn Sie Probleme haben)

"Erfahren Sie, wie Sie auf die lokale Benutzeroberfläche zugreifen".

Connector-Upgrades

Der Connector aktualisiert seine Software automatisch auf die neueste Version, solange er hat "Outbound-Internetzugang" Um das Softwareupdate zu erhalten.

Netzwerkanforderungen für den Connector

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

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

Verbindung zu Zielnetzwerken

Ein Connector erfordert eine Netzwerkverbindung zu der Art der Arbeitsumgebung, die Sie erstellen und die Dienste, die Sie planen zu ermöglichen.

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

Outbound-Internetzugang

Für den Connector ist ein abgehender Internetzugang erforderlich, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung zu managen. Der ausgehende Internetzugang ist auch erforderlich, wenn Sie den Connector manuell auf einem Linux-Host installieren oder auf die lokale UI zugreifen möchten, die auf dem Connector ausgeführt wird.

In den folgenden Abschnitten werden die spezifischen Endpunkte beschrieben.

Endpunkte zum Management von Ressourcen in AWS

Ein Connector kontaktiert die folgenden Endpunkte beim Management von Ressourcen in AWS:

Endpunkte	Zweck
AWS-Services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3) Der genaue Endpunkt hängt von der Region ab, in der Sie Cloud Volumes ONTAP implementieren. "Weitere Informationen finden Sie in der AWS-Dokumentation."	Ermöglicht die Implementierung und das Management von Cloud Volumes ONTAP in AWS mit dem Connector
https://api.services.cloud.netapp.com:443	API-Anfragen an NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://repo.cloud.support.netapp.com	Wird zum Herunterladen der Abhängigkeiten von Cloud Manager verwendet.
http://repo.mysql.com/	Zum Herunterladen von MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Ermöglicht dem Connector, auf Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images zuzugreifen und diese herunterzuladen.
https://cloudmanagerinfraprod.azurecr.io	Zugriff auf Software-Images von Container-Komponenten für eine Infrastruktur, die Docker ausführt und eine Lösung für die Service-Integration mit Cloud Manager bietet.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cloudmanager.cloud.netapp.com	Kommunikation mit dem Cloud Manager-Service, der Cloud Central-Konten einschließt
https://netapp-cloud-account.auth0.com	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Wird verwendet, um Ihre AWS Konto-ID der Liste der zugelassenen Benutzer für die Sicherung in S3 hinzuzufügen.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Kommunikation mit NetApp AutoSupport.

Endpunkte	Zweck
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Kommunikation mit NetApp bei Systemlizenzrechten und Support-Registrierung
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Er ermöglicht NetApp, Informationen zu sammeln, die für die Behebung von Support-Problemen erforderlich sind.
https://ipa-signer.cloudmanager.netapp.com	Ermöglicht Cloud Manager die Generierung von Lizenzen (beispielsweise eine FlexCache Lizenz für Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Erforderlich, um Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster zu verbinden Mit den Endpunkten ist die Installation von NetApp Trident möglich.
Verschiedene Standorte von Drittanbietern, z. B.: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com An Standorten von Drittanbietern können Änderungen vorgenommen werden.	Während Upgrades lädt Cloud Manager die neuesten Pakete für Abhängigkeiten von Drittanbietern herunter.

Endpunkte zum Managen von Ressourcen in Azure

Ein Connector kontaktiert folgende Endpunkte beim Managen von Ressourcen in Azure:

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den meisten Azure Regionen.
https://management.microsoftazure.de https://login.microsoftonline.de	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den Azure Germany Regionen.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den Azure US Gov Regionen.
https://api.services.cloud.netapp.com:443	API-Anfragen an NetApp Cloud Central.

Endpunkte	Zweck
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://repo.cloud.support.netapp.com	Wird zum Herunterladen der Abhängigkeiten von Cloud Manager verwendet.
http://repo.mysql.com/	Zum Herunterladen von MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Ermöglicht dem Connector, auf Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images zuzugreifen und diese herunterzuladen.
https://cloudmanagerinfraprod.azurecr.io	Zugriff auf Software-Images von Container-Komponenten für eine Infrastruktur, die Docker ausführt und eine Lösung für die Service-Integration mit Cloud Manager bietet.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cloudmanager.cloud.netapp.com	Kommunikation mit dem Cloud Manager-Service, der Cloud Central-Konten einschließt
https://netapp-cloud-account.auth0.com	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
https://mysupport.netapp.com	Kommunikation mit NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Kommunikation mit NetApp bei Systemlizenzrechten und Support-Registrierung
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Er ermöglicht NetApp, Informationen zu sammeln, die für die Behebung von Support-Problemen erforderlich sind.
https://ipa-signer.cloudmanager.netapp.com	Ermöglicht Cloud Manager die Generierung von Lizenzen (beispielsweise eine FlexCache Lizenz für Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Erforderlich, um Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster zu verbinden Mit den Endpunkten ist die Installation von NetApp Trident möglich.
*.blob.core.windows.net	Bei Verwendung eines Proxy erforderlich für HA-Paare

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

Endpunkte für das Management von Ressourcen in GCP

Ein Connector kontaktiert die folgenden Endpunkte beim Management von Ressourcen in GCP:

Endpunkte	Zweck
https://www.googleapis.com	Ermöglicht dem Connector den Kontakt zu Google APIs für die Bereitstellung und das Management von Cloud Volumes ONTAP in GCP.
https://api.services.cloud.netapp.com:443	API-Anfragen an NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://repo.cloud.support.netapp.com	Wird zum Herunterladen der Abhängigkeiten von Cloud Manager verwendet.
http://repo.mysql.com/	Zum Herunterladen von MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Ermöglicht dem Connector, auf Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images zuzugreifen und diese herunterzuladen.
https://cloudmanagerinfraprod.azurecr.io	Zugriff auf Software-Images von Container-Komponenten für eine Infrastruktur, die Docker ausführt und eine Lösung für die Service-Integration mit Cloud Manager bietet.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cloudmanager.cloud.netapp.com	Kommunikation mit dem Cloud Manager-Service, der Cloud Central-Konten einschließt
https://netapp-cloud-account.auth0.com	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
https://mysupport.netapp.com	Kommunikation mit NetApp AutoSupport.

Endpunkte	Zweck
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Kommunikation mit NetApp bei Systemlizenzrechten und Support-Registrierung
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Er ermöglicht NetApp, Informationen zu sammeln, die für die Behebung von Support-Problemen erforderlich sind.
https://ipa-signer.cloudmanager.netapp.com	Ermöglicht Cloud Manager die Generierung von Lizenzen (beispielsweise eine FlexCache Lizenz für Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Erforderlich, um Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster zu verbinden Mit den Endpunkten ist die Installation von NetApp Trident möglich.
Verschiedene Standorte von Drittanbietern, z. B.: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com An Standorten von Drittanbietern können Änderungen vorgenommen werden.	Während Upgrades lädt Cloud Manager die neuesten Pakete für Abhängigkeiten von Drittanbietern herunter.

Endpunkte zum Installieren des Connectors auf einem Linux-Host

Sie haben die Möglichkeit, die Connector-Software manuell auf Ihrem eigenen Linux-Host zu installieren. In diesem Fall muss das Installationsprogramm für den Connector 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

Der Host versucht möglicherweise, während der Installation Betriebssystempakete zu aktualisieren. Der Host kann verschiedene Spiegelungsstandorte für diese Betriebssystempakete kontaktieren.

Endpunkte, auf die Sie über Ihren Webbrowser zugreifen, wenn Sie die lokale Benutzeroberfläche verwenden

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

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

Ports und Sicherheitsgruppen

Es gibt keinen eingehenden Datenverkehr zum Konnektor, es sei denn, Sie initiieren ihn. HTTP und HTTPS bieten den Zugriff auf "Lokale Benutzeroberfläche", Die Sie in seltenen Fällen verwenden. SSH ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.

Regeln für den Connector in AWS

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

Regeln für eingehende Anrufe

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

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

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Konnektor öffnet den gesamten ausgehenden Datenverkehr. Wenn

dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

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

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

Erweiterte Outbound-Regeln

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

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

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

Service	Protokoll	Port	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe an AWS und ONTAP und Senden von AutoSupport Nachrichten an NetApp
API-Aufrufe	TCP	3000	ONTAP Cluster Management LIF	API-Aufrufe für ONTAP
	TCP	8088	Backup auf S3	API-Aufrufe zur Sicherung in S3
DNS	UDP	53	DNS	Wird für die DNS-Auflösung durch Cloud Manager verwendet
Cloud-Compliance	HTTP	80	Cloud Compliance Instanz	Cloud Compliance für Cloud Volumes ONTAP

Regeln für den Connector in Azure

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

Regeln für eingehende Anrufe

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

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

Regeln für ausgehende Anrufe

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

Grundlegende Regeln für ausgehende Anrufe

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

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

Erweiterte Outbound-Regeln

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

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

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

Service	Port	Protokoll	Ziel	Zweck
API-Aufrufe	3000	TCP	ONTAP Cluster Management LIF	API-Aufrufe für ONTAP
DNS	53	UDP	DNS	Wird für die DNS-Auflösung durch Cloud Manager verwendet

Regeln für den Connector in GCP

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

Regeln für eingehende Anrufe

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

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

Regeln für ausgehende Anrufe

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

Grundlegende Regeln für ausgehende Anrufe

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

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

Erweiterte Outbound-Regeln

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

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

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

Erstellen eines Connectors in AWS über Cloud Manager

Ein Kontoadministrator muss einen *Connector* bereitstellen, bevor Sie die meisten Funktionen von Cloud Manager nutzen können. "Informieren Sie sich, wann ein Anschluss erforderlich ist". Mit dem Connector kann Cloud Manager Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen.

Auf dieser Seite wird beschrieben, wie Sie einen Connector direkt aus Cloud Manager in AWS erstellen. Sie haben auch die Möglichkeit zu wählen "Erstellen Sie den Connector über den AWS Marketplace", Oder auf

"Laden Sie die Software herunter und installieren Sie sie auf Ihrem eigenen Host".

Diese Schritte müssen von einem Benutzer ausgeführt werden, der die Rolle „Account Admin“ hat. Ein Workspace-Administrator kann keinen Konnektor erstellen.

Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von Cloud Manager aufgefordert, einen Connector zu erstellen, falls noch kein Connector vorhanden ist.

Einrichtung von AWS Berechtigungen zum Erstellen eines Konnektors

Bevor Sie einen Connector von Cloud Manager implementieren können, müssen Sie sicherstellen, dass Ihr AWS-Konto die entsprechenden Berechtigungen hat.

Schritte

1. Laden Sie die IAM-Richtlinie für Connector von folgendem Speicherort herunter:

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

2. Erstellen Sie von der AWS IAM-Konsole aus Ihre eigene Richtlinie, indem Sie den Text aus der IAM-Richtlinie für Connector kopieren und einfügen.
3. Hängen Sie die Richtlinie, die Sie im vorherigen Schritt erstellt haben, dem IAM-Benutzer an, der den Connector aus Cloud Manager erstellt.

Ergebnis

Der AWS-Benutzer verfügt nun über die erforderlichen Berechtigungen, um den Connector aus Cloud Manager zu erstellen. Sie müssen für diesen Benutzer die AWS-Zugriffsschlüssel festlegen, wenn Sie von Cloud Manager aufgefordert werden.

Erstellen eines Konnektors in AWS

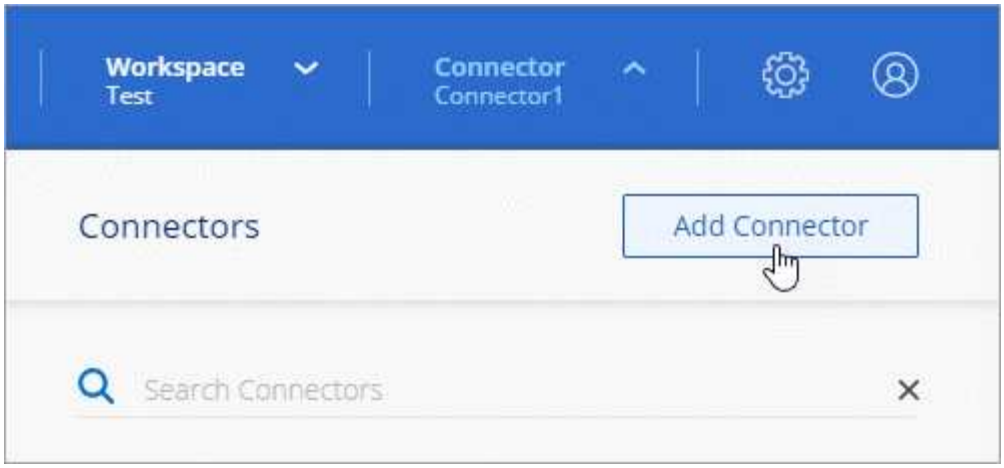
Mit Cloud Manager können Sie einen Connector in AWS direkt von der Benutzeroberfläche aus erstellen.

Was Sie benötigen

- Ein AWS-Zugriffsschlüssel und ein geheimer Schlüssel für einen IAM-Benutzer, der über den verfügt "Erforderliche Berechtigungen".
- Ein VPC, Subnetz und Schlüsselpairs in Ihrer bevorzugten AWS Region.

Schritte

1. Wenn Sie Ihre erste Arbeitsumgebung erstellen, klicken Sie auf **Arbeitsumgebung hinzufügen** und befolgen Sie die Anweisungen. Klicken Sie andernfalls auf das Dropdown-Menü **Connector** und wählen Sie **Connector hinzufügen** aus.



2. Klicken Sie auf **Let's Start**.
3. Wählen Sie als Cloud-Provider * Amazon Web Services* aus.

   Denken Sie daran, dass der Connector über eine Netzwerkverbindung mit der Art der Arbeitsumgebung, die Sie erstellen, und den Diensten, die Sie für die Aktivierung planen, verfügen muss.

   "Erfahren Sie mehr über die Netzwerkanforderungen für den Connector".

4. Überprüfen Sie, was Sie benötigen, und klicken Sie auf **Weiter**.
5. Geben Sie die erforderlichen Informationen ein:
   - **AWS Credentials**: Geben Sie einen Namen für die Instanz ein und geben Sie den AWS Zugriffsschlüssel und den geheimen Schlüssel an, der die Berechtigungsanforderungen erfüllt.
   - **Standort**: Geben Sie eine AWS Region, VPC und Subnetz für die Instanz an.
   - **Netzwerk**: Wählen Sie das Schlüsselpaar aus, das mit der Instanz verwendet werden soll, ob eine öffentliche IP-Adresse aktiviert werden soll, und geben Sie optional eine Proxy-Konfiguration an.
   - **Sicherheitsgruppe**: Wählen Sie aus, ob eine neue Sicherheitsgruppe erstellt werden soll oder ob eine vorhandene Sicherheitsgruppe ausgewählt werden soll, die einen eingehenden HTTP-, HTTPS- und SSH-Zugriff erlaubt.

   ⓘ Es gibt keinen eingehenden Datenverkehr zum Konnektor, es sei denn, Sie initiieren ihn. HTTP und HTTPS bieten den Zugriff auf "Lokale Benutzeroberfläche", Die Sie in seltenen Fällen verwenden. SSH ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.

6. Klicken Sie Auf **Erstellen**.

   Die Instanz sollte in ca. 7 Minuten fertig sein. Sie sollten auf der Seite bleiben, bis der Vorgang abgeschlossen ist.

Nachdem Sie fertig sind

Sie müssen einen Connector mit Arbeitsbereichen verknüpfen, damit Arbeitsbereichsadministratoren diese Connectors zum Erstellen von Cloud Volumes ONTAP-Systemen verwenden können. Wenn Sie nur Kontoadministratoren haben, ist es nicht erforderlich, den Connector mit Arbeitsbereichen zu verknüpfen. Account-Administratoren haben standardmäßig die Möglichkeit, auf alle Workspaces in Cloud Manager zuzugreifen. "Weitere Informationen .".

Erstellen eines Connectors in Azure über Cloud Manager

Ein Kontoadministrator muss einen *Connector* bereitstellen, bevor Sie die meisten Funktionen von Cloud Manager nutzen können. "Informieren Sie sich, wann ein Anschluss erforderlich ist". Mit dem Connector kann Cloud Manager Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen.

Auf dieser Seite wird beschrieben, wie Sie direkt aus Cloud Manager einen Connector in Azure erstellen. Sie haben auch die Möglichkeit zu wählen "Erstellen Sie den Connector aus dem Azure Marketplace", Oder auf "Laden Sie die Software herunter und installieren Sie sie auf Ihrem eigenen Host".

Diese Schritte müssen von einem Benutzer ausgeführt werden, der die Rolle „Account Admin“ hat. Ein Workspace-Administrator kann keinen Konnektor erstellen.

Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von Cloud Manager aufgefordert, einen Connector zu erstellen, falls noch kein Connector vorhanden ist.

Einrichten von Azure-Berechtigungen zum Erstellen eines Connectors

Bevor Sie einen Connector von Cloud Manager implementieren können, müssen Sie sicherstellen, dass Ihr Azure-Konto die entsprechenden Berechtigungen hat.

Schritte

1. Erstellen Sie mithilfe der Azure-Richtlinie für den Connector eine benutzerdefinierte Rolle:

   a. Laden Sie die herunter "Azure-Richtlinie für den Connector".

      Klicken Sie mit der rechten Maustaste auf den Link und klicken Sie auf **Link speichern unter…**, um die Datei herunterzuladen.

   b. Ändern Sie die JSON-Datei, indem Sie Ihre Azure Abonnement-ID dem zuweisbaren Umfang hinzufügen.

      Beispiel

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      ],
      ```

   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 role definition create --role-definition
      C:\Policy_for_Setup_As_Service_Azure.json
      ```

   Sie sollten jetzt eine benutzerdefinierte Rolle namens *Azure SetupAsService* haben.

2. Weisen Sie die Rolle dem Benutzer zu, der den Connector aus Cloud Manager bereitstellen soll:

a. Öffnen Sie den Dienst **Abonnements** und wählen Sie das Abonnement des Benutzers aus.

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 **Azure SetupAsService** aus.

> Azure SetupAsService ist der Standardname, der in angegeben wird "Connector-Implementierungsrichtlinie für Azure". Wenn Sie einen anderen Namen für die Rolle ausgewählt haben, wählen Sie stattdessen diesen Namen aus.

- Weisen Sie einem **Azure AD-Benutzer, einer Gruppe oder einer Anwendung** Zugriff zu.
- Wählen Sie das Benutzerkonto aus.
- Klicken Sie Auf **Speichern**.

Ergebnis

Der Azure-Benutzer verfügt nun über die erforderlichen Berechtigungen, um den Connector aus Cloud Manager zu implementieren.

Erstellen eines Connectors in Azure

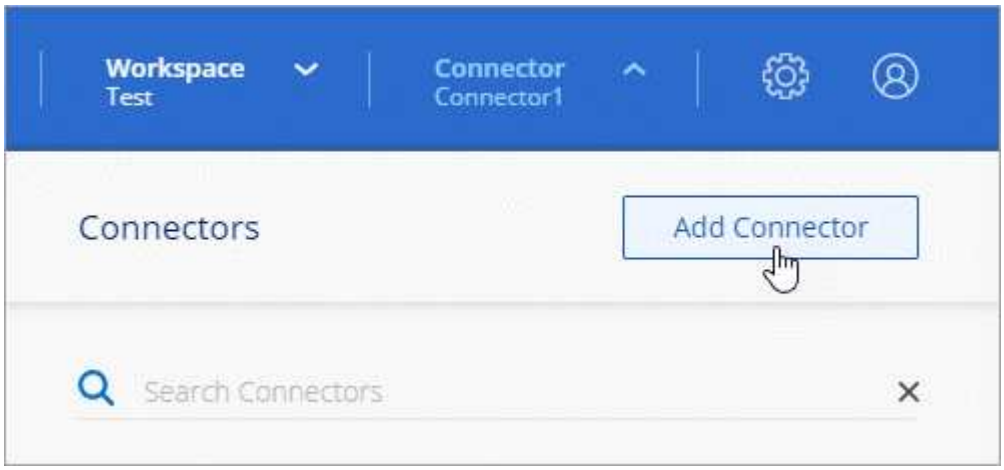
Mit Cloud Manager können Sie einen Connector in Azure direkt von der Benutzeroberfläche aus erstellen.

Was Sie benötigen

- Der "Erforderliche Berechtigungen" Für Ihr Azure Konto.
- Ein Azure Abonnement.
- Eine vnet und Subnetz in Ihrer bevorzugten Azure-Region.

Schritte

1. Wenn Sie Ihre erste Arbeitsumgebung erstellen, klicken Sie auf **Arbeitsumgebung hinzufügen** und befolgen Sie die Anweisungen. Klicken Sie andernfalls auf das Dropdown-Menü **Connector** und wählen Sie **Connector hinzufügen** aus.



2. Klicken Sie auf **Let's Start**.
3. Wählen Sie als Cloud-Provider * Microsoft Azure* aus.

Denken Sie daran, dass der Connector über eine Netzwerkverbindung mit der Art der Arbeitsumgebung, die Sie erstellen, und den Diensten, die Sie für die Aktivierung planen, verfügen muss.

"Erfahren Sie mehr über die Netzwerkanforderungen für den Connector".

4. Überprüfen Sie, was Sie benötigen, und klicken Sie auf **Weiter**.
5. Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem Microsoft-Konto an, das über die erforderlichen Berechtigungen zum Erstellen der virtuellen Maschine verfügt.

   Das Formular ist Eigentum von Microsoft und wird von Microsoft gehostet. Ihre Zugangsdaten werden nicht an NetApp bereitgestellt.

   Wenn Sie bereits bei einem Azure-Konto angemeldet sind, nutzt Cloud Manager das Konto automatisch. Wenn Sie über mehrere Konten verfügen, müssen Sie sich möglicherweise erst abmelden, um sicherzustellen, dass Sie das richtige Konto verwenden.

6. Geben Sie die erforderlichen Informationen ein:
   - **VM Authentication**: Geben Sie einen Namen für die virtuelle Maschine und einen Benutzernamen und ein Passwort oder einen öffentlichen Schlüssel ein.
   - **Grundeinstellungen**: Wählen Sie ein Azure-Abonnement, eine Azure-Region und ob Sie eine neue Ressourcengruppe erstellen oder eine vorhandene Ressourcengruppe verwenden möchten.
   - **Netzwerk**: Wählen Sie ein vnet und Subnetz, ob eine öffentliche IP-Adresse aktiviert werden soll, und geben Sie optional eine Proxy-Konfiguration an.
   - **Sicherheitsgruppe**: Wählen Sie aus, ob eine neue Sicherheitsgruppe erstellt werden soll oder ob eine vorhandene Sicherheitsgruppe ausgewählt werden soll, die einen eingehenden HTTP-, HTTPS- und SSH-Zugriff erlaubt.

   Es gibt keinen eingehenden Datenverkehr zum Konnektor, es sei denn, Sie initiieren ihn. HTTP und HTTPS bieten den Zugriff auf "Lokale Benutzeroberfläche", Die Sie in seltenen Fällen verwenden. SSH ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.

7. Klicken Sie Auf **Erstellen**.

   Die Virtual Machine sollte in ca. 7 Minuten einsatzbereit sein. Sie sollten auf der Seite bleiben, bis der Vorgang abgeschlossen ist.

Nachdem Sie fertig sind

Sie müssen einen Connector mit Arbeitsbereichen verknüpfen, damit Arbeitsbereichsadministratoren diese Connectors zum Erstellen von Cloud Volumes ONTAP-Systemen verwenden können. Wenn Sie nur Kontoadministratoren haben, ist es nicht erforderlich, den Connector mit Arbeitsbereichen zu verknüpfen. Account-Administratoren haben standardmäßig die Möglichkeit, auf alle Workspaces in Cloud Manager zuzugreifen. "Weitere Informationen .".

Erstellen eines Connectors in GCP über Cloud Manager

Ein Kontoadministrator muss einen *Connector* bereitstellen, bevor Sie die meisten Funktionen von Cloud Manager nutzen können. "Informieren Sie sich, wann ein Anschluss erforderlich ist". Mit dem Connector kann Cloud Manager Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen.

Auf dieser Seite wird beschrieben, wie ein Connector in GCP direkt aus Cloud Manager erstellt wird. Sie haben auch die Möglichkeit zu wählen "Laden Sie die Software herunter und installieren Sie sie auf Ihrem eigenen Host".

Diese Schritte müssen von einem Benutzer ausgeführt werden, der die Rolle „Account Admin“ hat. Ein Workspace-Administrator kann keinen Konnektor erstellen.

Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von Cloud Manager aufgefordert, einen Connector zu erstellen, falls noch kein Connector vorhanden ist.

Einrichten von GCP-Berechtigungen zum Erstellen eines Konnektors

Bevor Sie einen Connector von Cloud Manager bereitstellen können, müssen Sie sicherstellen, dass Ihr GCP-Konto die entsprechenden Berechtigungen hat und dass ein Servicekonto für die Connector-VM eingerichtet ist.

Schritte

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

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

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

   Dieses Servicekonto wird der Connector VM zugeordnet, wenn Sie es aus Cloud Manager erstellen.

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

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

   b. "Erstellen Sie ein GCP-Service-Konto und wenden Sie die benutzerdefinierte Rolle an, die Sie gerade erstellt haben".

   c. Wenn Sie Cloud Volumes ONTAP in anderen Projekten implementieren möchten, "Sie gewähren Zugriff, indem Sie dem Projekt das Service-Konto mit der Rolle Cloud Manager hinzufügen". Sie müssen diesen Schritt für jedes Projekt wiederholen.

Ergebnis

Der GCP-Benutzer verfügt jetzt über die erforderlichen Berechtigungen, um den Connector aus Cloud Manager zu erstellen, und das Servicekonto für die Connector-VM wird eingerichtet.

Aktivieren von Google Cloud APIs

Für die Bereitstellung des Connectors und der Cloud Volumes ONTAP sind mehrere APIs erforderlich.

Schritt

1. "Aktivieren Sie die folgenden Google Cloud APIs in Ihrem Projekt".
   - Cloud Deployment Manager V2-API
   - Cloud-ProtokollierungsAPI

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

Erstellen eines Konnektors in GCP

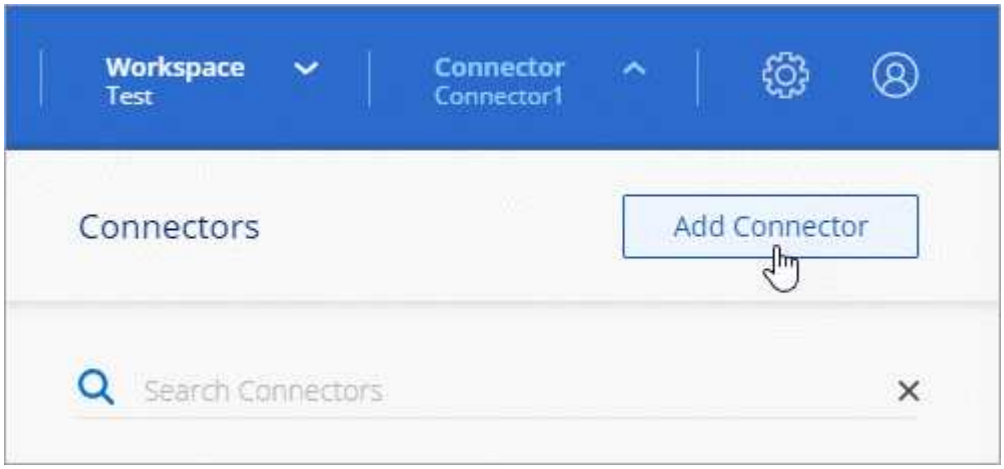
Mit Cloud Manager können Sie einen Connector in GCP direkt von der Benutzeroberfläche aus erstellen.

Was Sie benötigen

- Der "Erforderliche Berechtigungen" Für Ihren Google Cloud-Account.
- Ein Google Cloud-Projekt.
- Ein Servicekonto mit den erforderlichen Berechtigungen zum Erstellen und Verwalten von Cloud Volumes ONTAP.
- Ein VPC und Subnetz in Ihrer bevorzugten Google Cloud-Region.

Schritte

1. Wenn Sie Ihre erste Arbeitsumgebung erstellen, klicken Sie auf **Arbeitsumgebung hinzufügen** und befolgen Sie die Anweisungen. Klicken Sie andernfalls auf das Dropdown-Menü **Connector** und wählen Sie **Connector hinzufügen** aus.



2. Klicken Sie auf **Let's Start**.
3. Wählen Sie **Google Cloud Platform** als Cloud-Provider.

   Denken Sie daran, dass der Connector über eine Netzwerkverbindung mit der Art der Arbeitsumgebung, die Sie erstellen, und den Diensten, die Sie für die Aktivierung planen, verfügen muss.

   "Erfahren Sie mehr über die Netzwerkanforderungen für den Connector".

4. Überprüfen Sie, was Sie benötigen, und klicken Sie auf **Weiter**.
5. Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem Google-Konto an, das über die erforderlichen Berechtigungen zum Erstellen der virtuellen Maschineninstanz verfügen sollte.

   Das Formular ist Eigentum und wird von Google gehostet. Ihre Zugangsdaten werden nicht an NetApp bereitgestellt.

6. Geben Sie die erforderlichen Informationen ein:

- **Grundeinstellungen**: Geben Sie einen Namen für die virtuelle Maschineninstanz ein und geben Sie ein Projekt- und Servicekonto an, das über die erforderlichen Berechtigungen verfügt.
- **Ort**: Geben Sie eine Region, Zone, VPC und Subnetz für die Instanz an.
- **Netzwerk**: Wählen Sie, ob eine öffentliche IP-Adresse aktiviert werden soll und geben Sie optional eine Proxy-Konfiguration an.
- **Firewall-Richtlinie**: Wählen Sie, ob Sie eine neue Firewall-Richtlinie erstellen oder eine vorhandene Firewall-Richtlinie auswählen möchten, die einen eingehenden HTTP-, HTTPS- und SSH-Zugriff erlaubt.

Es gibt keinen eingehenden Datenverkehr zum Konnektor, es sei denn, Sie initiieren ihn. HTTP und HTTPS bieten den Zugriff auf "Lokale Benutzeroberfläche", Die Sie in seltenen Fällen verwenden. SSH ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.

7. Klicken Sie Auf **Erstellen**.

   Die Instanz sollte in ca. 7 Minuten fertig sein. Sie sollten auf der Seite bleiben, bis der Vorgang abgeschlossen ist.

Nachdem Sie fertig sind

Sie müssen einen Connector mit Arbeitsbereichen verknüpfen, damit Arbeitsbereichsadministratoren diese Connectors zum Erstellen von Cloud Volumes ONTAP-Systemen verwenden können. Wenn Sie nur Kontoadministratoren haben, ist es nicht erforderlich, den Connector mit Arbeitsbereichen zu verknüpfen. Account-Administratoren haben standardmäßig die Möglichkeit, auf alle Workspaces in Cloud Manager zuzugreifen. "Weitere Informationen .".

Weitere Schritte

Nachdem Sie sich jetzt angemeldet und Cloud Manager eingerichtet haben, können Benutzer jetzt mit dem Erstellen und Erkennen von Arbeitsumgebungen beginnen.

- "Erste Schritte mit Cloud Volumes ONTAP für AWS"
- "Erste Schritte mit Cloud Volumes ONTAP für Azure"
- "Erste Schritte mit Cloud Volumes ONTAP für Google Cloud"
- "Azure NetApp Files einrichten"
- "Cloud Volumes Service für AWS einrichten"
- "Ermitteln eines lokalen ONTAP Clusters"
- "Amazon S3 Buckets entdecken"

Als Administrator können Sie die Cloud Manager-Einstellungen verwalten, nachdem Sie den ersten Connector erstellt haben.

- "Erfahren Sie mehr über Steckverbinder"
- "Managen Sie ein HTTPS-Zertifikat für sicheren Zugriff"
- "Konfigurieren Sie Proxy-Einstellungen"

Managen Sie Cloud Volumes ONTAP

Know-How

Weitere Informationen zu Cloud Volumes ONTAP

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

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

- Storage-Effizienz

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

- Hochverfügbarkeit

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

- Datensicherung

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

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

- Daten-Tiering

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

- Applikationskonsistenz

  Konsistenz von NetApp Snapshot Kopien mit NetApp SnapCenter sicherstellen.

- Datensicherheit

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

- Kontrolloptionen für die Einhaltung des Datenschutzes

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

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

"Anzeigen der unterstützten Cloud Volumes ONTAP Konfigurationen"

"Erfahren Sie mehr über Cloud Volumes ONTAP"

Storage

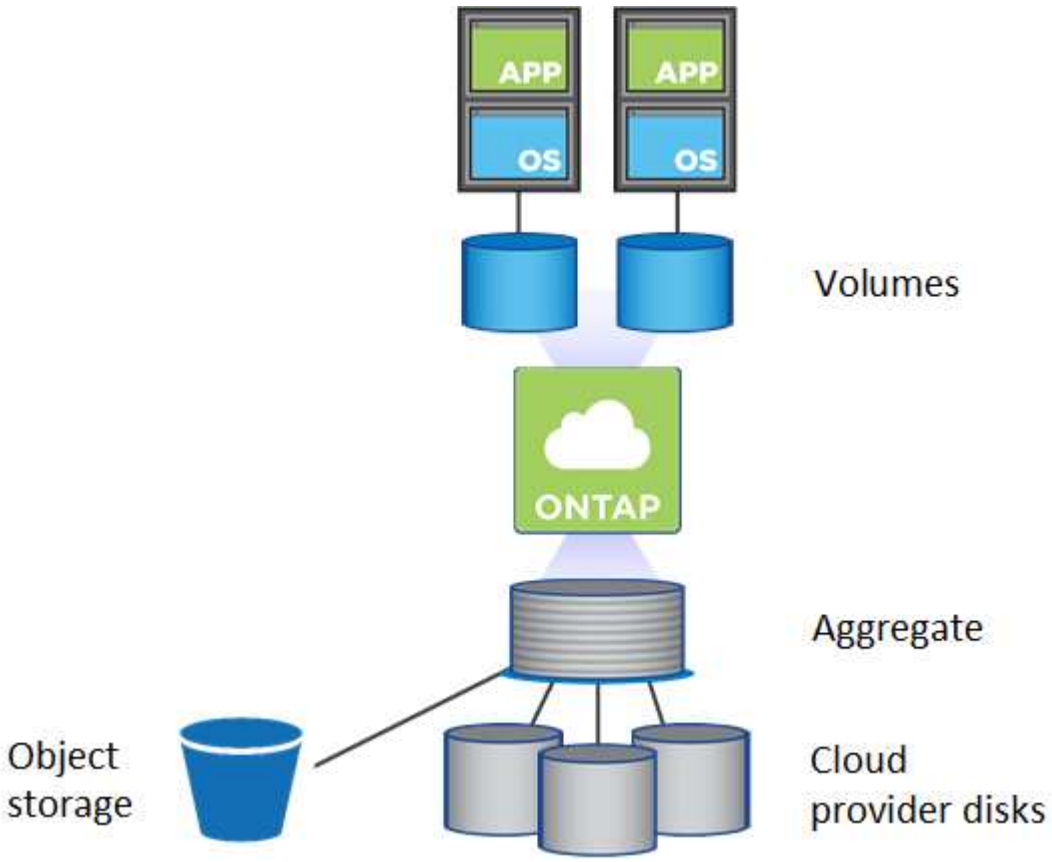
Festplatten und Aggregate

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

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

Überblick

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



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

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

AWS Storage

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

EBS Storage

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

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

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

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

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

Lokaler NVMe-Storage

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

Verwandte Links

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

Azure Storage

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

Systeme mit einzelnen Nodes

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

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

  Jeder verwaltete Festplattentyp hat eine maximale Festplattengröße von 32 TB.

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

HA-Paare

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

Verwandte Links

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

GCP-Storage

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

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

Verwandte Links

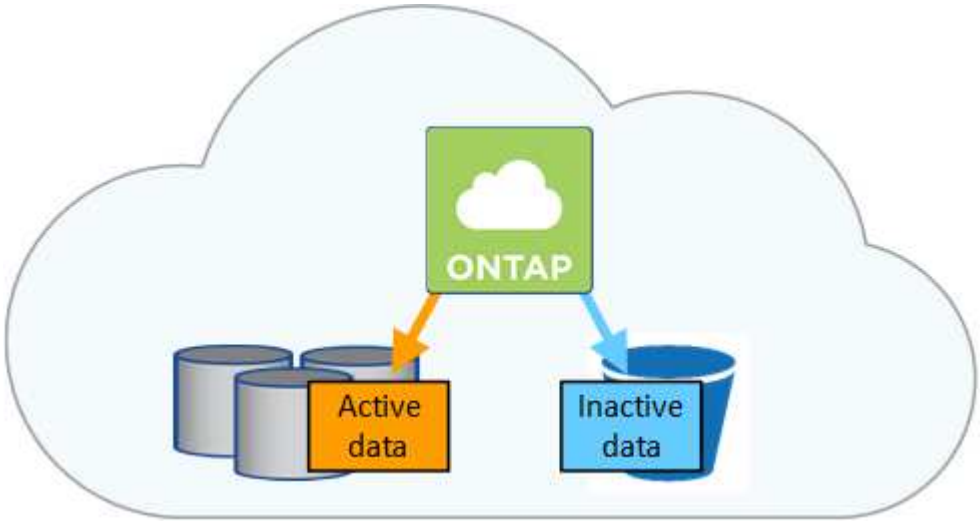
- "Dokumentation der Google Cloud Platform Storage Options"
- "Prüfen von Storage-Limits für Cloud Volumes ONTAP in GCP"

RAID-Typ

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

Data Tiering - Übersicht

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



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

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

Daten-Tiering in AWS

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

Performance-Tier

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

Kapazitäts-Tier

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

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

Speicherklassen

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

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

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

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

Daten-Tiering in Azure

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

Performance-Tier

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

Kapazitäts-Tier

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

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

Storage-Zugriffstufen

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

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

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

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

Daten-Tiering in GCP

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

Performance-Tier

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

Kapazitäts-Tier

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

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

Speicherklassen

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

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

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

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

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

Daten-Tiering und Kapazitätsgrenzen

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

Richtlinien für das Volume-Tiering

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

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

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

Nur Snapshot

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

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

Alle

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

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

Automatisch

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

Diese Richtlinie wird ab Cloud Volumes ONTAP 9.4 unterstützt.

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

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

Keine

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

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

Die Abschaltung von Cloud Volumes ONTAP beeinträchtigt die Kühlungszeit

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

- Auto: 31 Tage
- Nur Snapshot: 2 Tage

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

Einrichten von Data Tiering

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

Storage-Management

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

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

Storage-Bereitstellung

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

Vereinfachte Bereitstellung

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

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

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

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

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

Auswahl der Festplattengröße für Aggregate in AWS

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

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

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

Sie können die Festplattengröße selbst mithilfe der erweiterten Zuweisungsoption auswählen.

Erweiterte Zuweisung

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

Kapazitätsmanagement

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

Automatisches Kapazitätsmanagement

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

Die folgenden Beispiele veranschaulichen die Funktionsweise dieses Modus:

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

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

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

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

Verwaltung von LUNs mit automatischem Kapazitätsmanagement

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

Verwaltung von Inoden mit automatischem Kapazitätsmanagement

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

Manuelles Kapazitätsmanagement

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

Flash Cache

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

Was ist Flash Cache?

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

Unterstützte Instanzen in AWS

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

- C5d.4xlarge
- C5d.9xlarge

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

Unterstützter VM-Typ in Azure

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

Einschränkungen

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

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

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

WORM-Storage

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

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

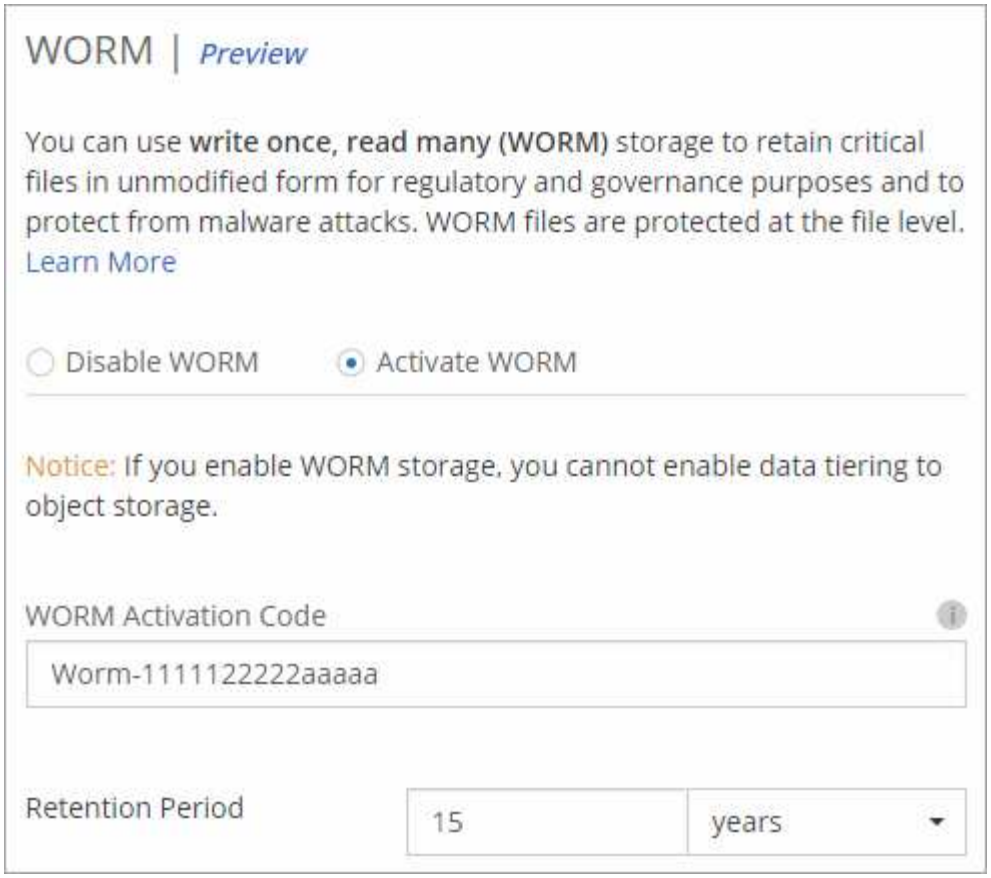
Nach Ablauf der Aufbewahrungsfrist sind Sie dafür verantwortlich, alle Dateien zu löschen, die Sie nicht mehr benötigen.

WORM-Storage wird aktiviert

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

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

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



Dateien werden in WORM gespeichert

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

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

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

Einschränkungen

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

Hochverfügbarkeitspaare

Hochverfügbarkeitspaare in AWS

Eine Cloud Volumes ONTAP Hochverfügbarkeitskonfiguration (HA) bietet unterbrechungsfreien Betrieb und Fehlertoleranz. In AWS werden die Daten zwischen

den beiden Nodes synchron gespiegelt.

Überblick

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

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

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

Storage-Übernahme und -Giveback

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

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

RPO und RTO

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

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

Ha-Bereitstellungsmodelle

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

Cloud Volumes ONTAP HA in mehreren Verfügbarkeitszonen

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

NFS- und CIFS-Datenzugriff

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

Wenn Sie kein Transit-Gateway einrichten können, sind private IP-Adressen für NAS-Clients außerhalb der

VPC verfügbar. Diese IP-Adressen sind jedoch statisch und können nicht zwischen Nodes ein Failover ausführen.

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

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

ISCSI-Datenzugriff

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

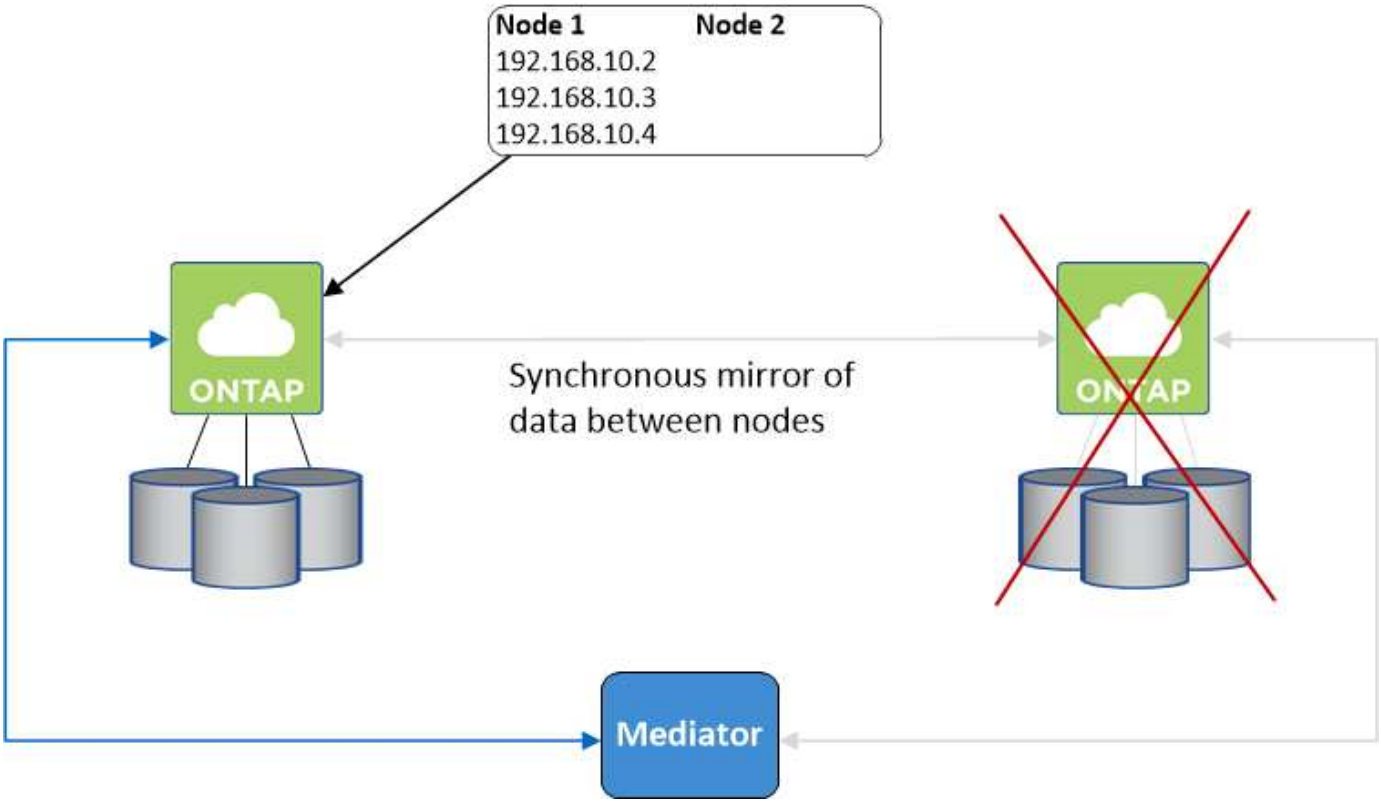
Storage-Übernahme und -Giveback für iSCSI

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

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

Storage-Übernahme und -Giveback für NAS

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



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

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

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

Cloud Volumes ONTAP HA in einer einzigen Verfügbarkeitszone

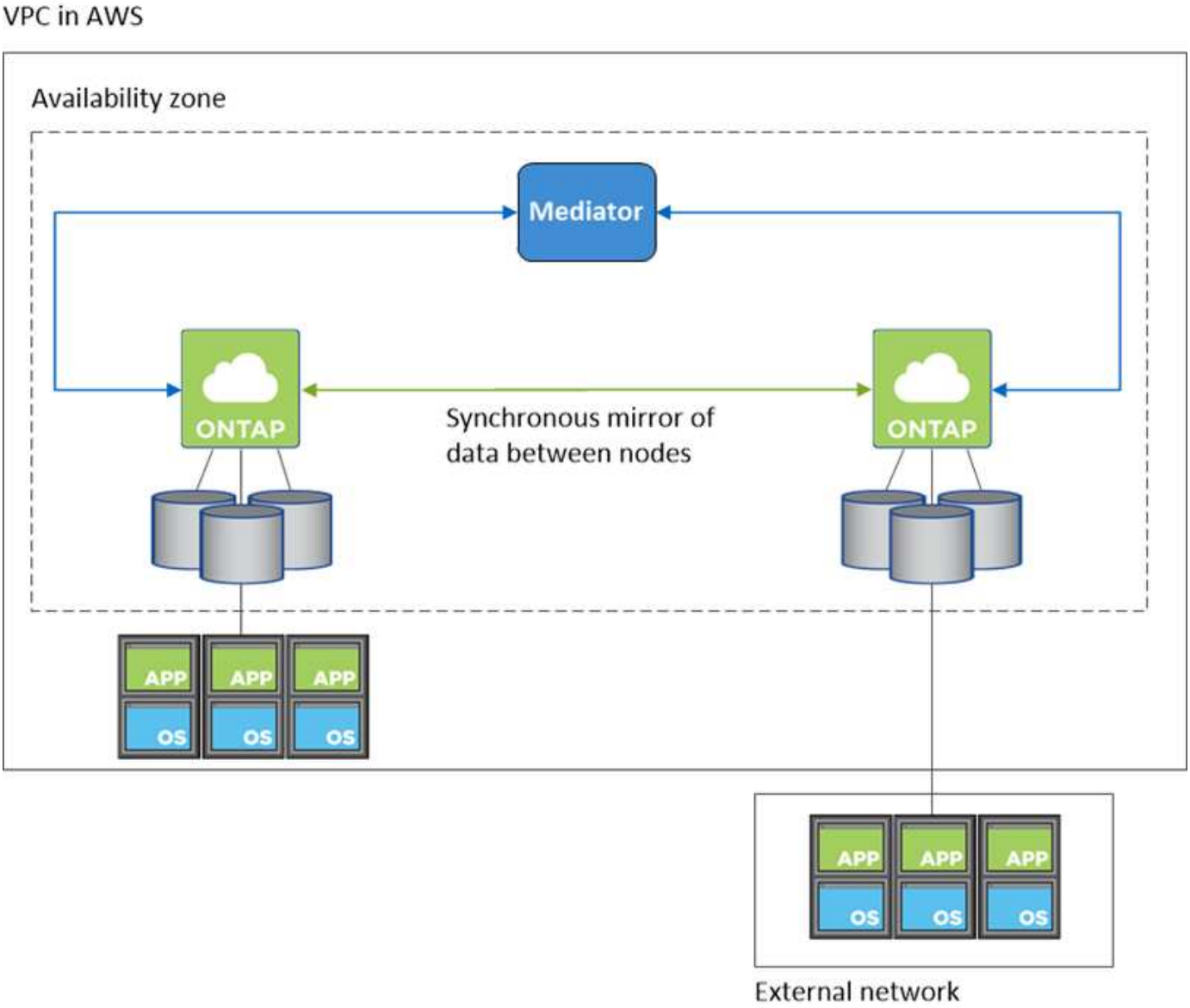
Durch die Implementierung einer HA-Konfiguration in einer einzelnen Verfügbarkeitszone (AZ) kann eine hohe Verfügbarkeit Ihrer Daten sichergestellt werden, wenn eine Instanz, auf der ein Cloud Volumes ONTAP Node ausgeführt wird, ausfällt. Alle Daten sind nativ von außerhalb des VPC zugänglich.

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

Datenzugriff

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

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



Storage-Übernahme und -Giveback

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

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

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

Funktionsweise von Storage in einem HA-Paar

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

Storage-Zuweisung

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

Storage-Konfigurationen

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

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

Performance-Erwartungen für eine HA-Konfiguration

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

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

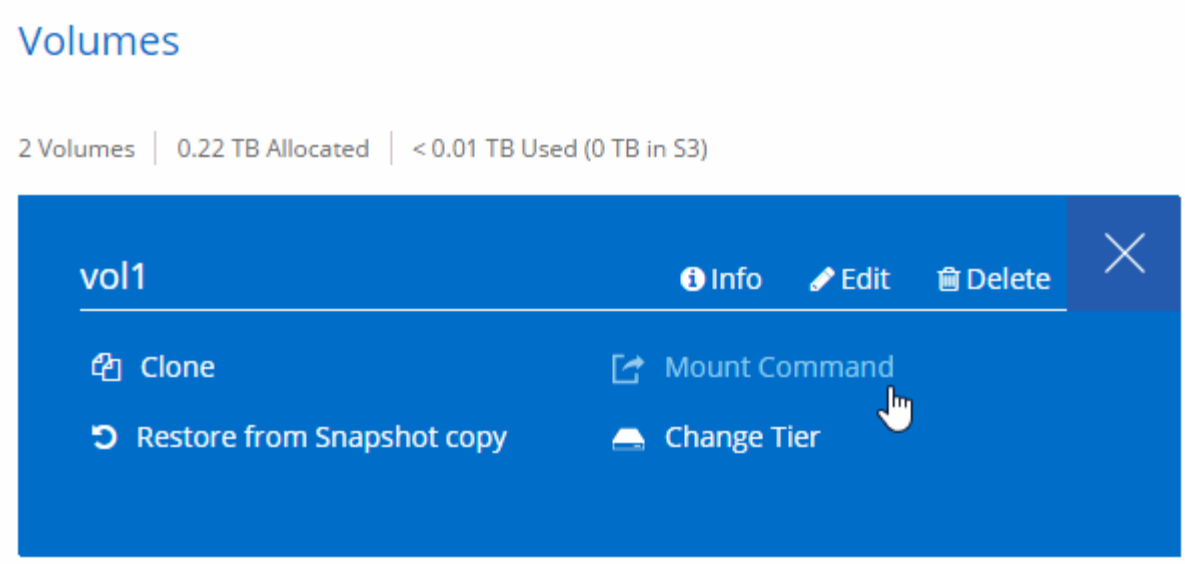
Weitere Informationen zur Performance von Cloud Volumes ONTAP finden Sie unter "Leistung".

Client-Zugriff auf Storage

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

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

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

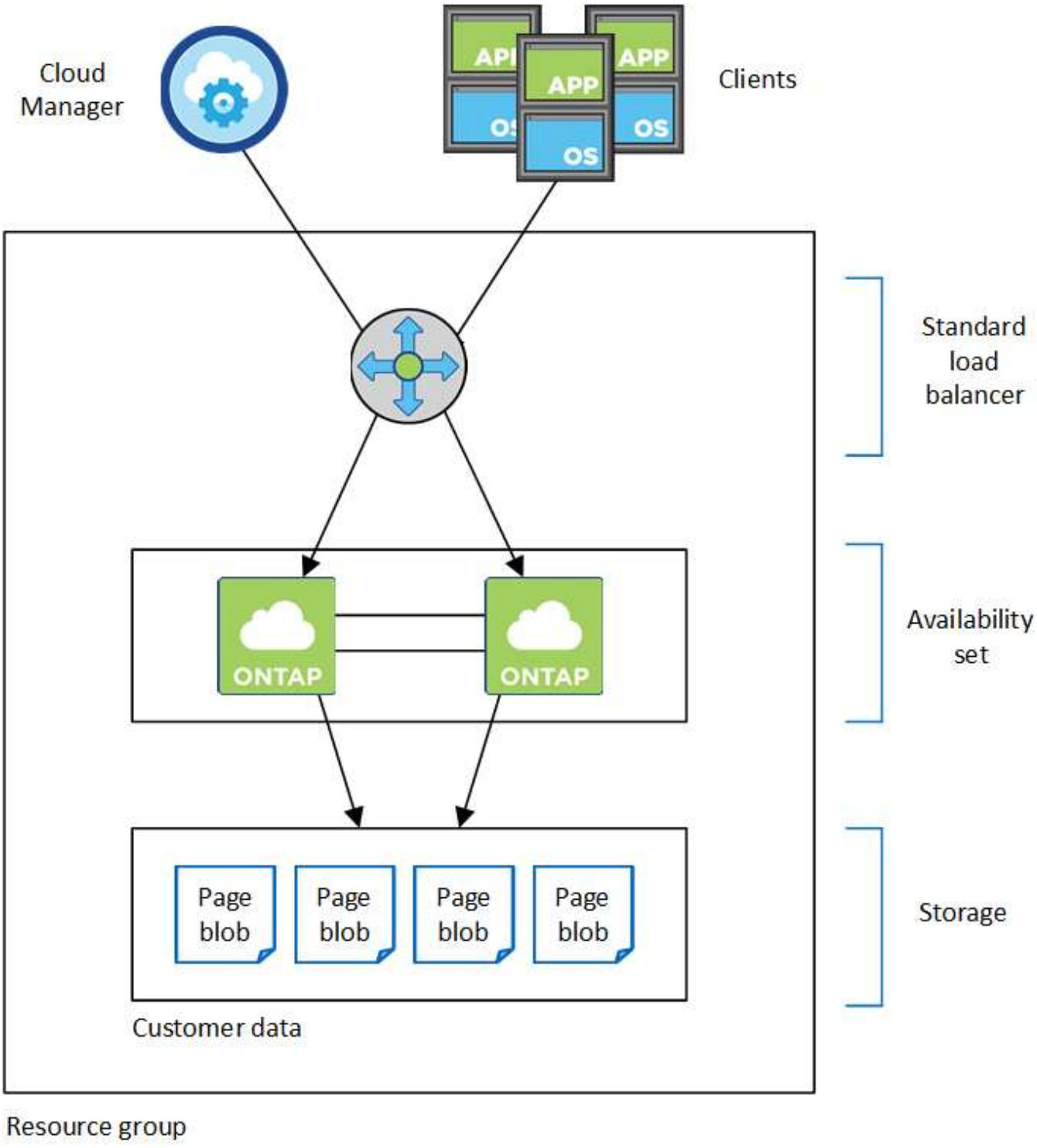


Hochverfügbarkeitspaare in Azure

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

HA-Komponenten

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



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

Azure Standard Load Balancer

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

Verfügbarkeitsgruppe

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

Festplatten

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

Konten mit Storage-Systemen

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

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

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

RPO und RTO

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

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

Storage-Übernahme und -Giveback

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

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

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

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

Storage-Konfigurationen

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

HA-Einschränkungen

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

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

  "Siehe die Liste der unterstützten Azure Regionen".

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

Bewertung

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

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

30-Tage-Testversionen für PAYGO

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

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

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

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

Evaluierungslizenzen für BYOL

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

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

Nach 30 Tagen werden tägliche Abschaltungen stattfinden, daher ist es am besten, im Voraus zu planen. Für ein in-Place-Upgrade kann eine neue BYOL-Lizenz auf die Evaluierungslizenz angewendet werden (hierfür ist ein Neustart einzelner Node-Systeme erforderlich). Ihre gehosteten Daten werden am Ende des Testzeitraums

nicht gelöscht.

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

Lizenzierung

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

Byol-Systemlizenzen

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

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

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

Lizenzmanagement für ein neues System

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

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

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

Warnung zum Ablauf der Lizenz

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

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

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

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

Lizenzerneuerung

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

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

Byol-Backup-Lizenzen

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

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

Sicherheit

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

Verschlüsselung von Daten im Ruhezustand

Cloud Volumes ONTAP unterstützt die folgenden Verschlüsselungstechnologien:

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

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

NetApp Verschlüsselungslösungen (NVE und NAE)

Cloud Volumes ONTAP unterstützt sowohl NetApp Volume Encryption (NVE) als auch NetApp Aggregate Encryption (NAE) mit einem externen Schlüsselmanager. NVE und NAE sind softwarebasierte Lösungen, mit denen die Verschlüsselung von Volumes im Ruhezustand (FIPS) 140-2-konform unterstützt wird.

- NVE verschlüsselt Daten im Ruhezustand nach einem Volume pro Zeit. Jedes Daten-Volume verfügt über

einen eigenen eindeutigen Verschlüsselungsschlüssel.

- NAE ist eine Erweiterung von NVE, denn es verschlüsselt Daten für jedes Volume, und die Volumes teilen sich einen Schlüssel im gesamten Aggregat. NAE ermöglicht außerdem die Deduplizierung allgemeiner Blöcke aller Volumes im Aggregat.

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

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

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

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

AWS Key Management Service

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

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

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

Azure Storage Service Encryption

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

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

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

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

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

Google Cloud Platform-Standardverschlüsselung

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

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

ONTAP Virenscannen

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

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

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

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

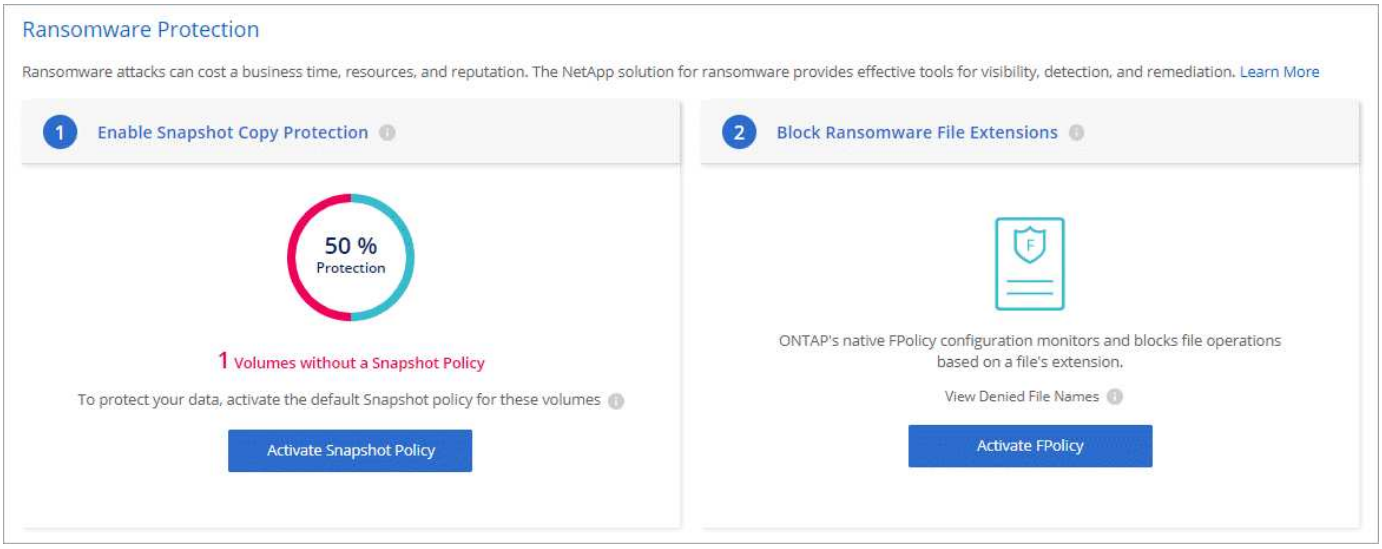
Schutz durch Ransomware

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

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

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

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



"So implementieren Sie die NetApp Lösung für Ransomware".

Leistung

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

- Cloud Volumes ONTAP für AWS

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

- Cloud Volumes ONTAP für Microsoft Azure

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

- Cloud Volumes ONTAP für Google Cloud

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

Standardkonfiguration für Cloud Volumes ONTAP

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

Standardwerte

- Cloud Volumes ONTAP ist als Single-Node-System in AWS, Azure und GCP verfügbar und als HA-Paar in AWS und Azure.
- Cloud Manager erstellt bei der Implementierung von Cloud Volumes ONTAP eine Storage-VM mit Datenservice. Einige Konfigurationen unterstützen zusätzliche Storage VMs. "Erfahren Sie mehr über das Management von Storage VMs".
- Cloud Manager installiert die folgenden ONTAP Funktionslizenzen automatisch auf Cloud Volumes ONTAP:
  - CIFS
  - FlexCache
  - FlexClone
  - ISCSI
  - NetApp Volume Encryption (nur für BYOL oder registrierte PAYGO Systeme)
  - NFS
  - SnapMirror
  - SnapRestore
  - SnapVault
- Standardmäßig werden mehrere Netzwerkschnittstellen erstellt:
  - Eine Cluster Management-LIF

- Eine Intercluster-LIF
- SVM-Management-LIF auf HA-Systemen in Azure, Single-Node-Systeme in AWS und optional auf HA-Systemen in mehreren AWS Availability Zones
- Eine Node Management-LIF
- Eine iSCSI-Daten-LIF
- Eine CIFS- und NFS-Daten-LIF

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

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

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

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

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

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

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

Boot- und Root-Daten für Cloud Volumes ONTAP

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

AWS

- Zwei Festplatten pro Node für Boot- und Root-Daten:

- 9.7: 160-GB-io1-Festplatte für Boot-Daten und eine 220-GB-gp2-Festplatte für Stammdaten
- 9.6: 93-GB-io1-Festplatte für Boot-Daten und eine 140-GB-gp2-Festplatte für Stammdaten
- 9.5: 45-GB-io1-Festplatte für Boot-Daten und eine 140-GB-gp2-Festplatte für Stammdaten

- Ein EBS-Snapshot für jede Boot- und Root-Festplatte
- Bei HA-Paaren ist ein EBS-Volume für die Mediator-Instanz, das ca. 8 GB beträgt

Azure (Single Node)

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

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

Azure (HA-Paare)

- Zwei 10-GB-Premium-SSD-Laufwerke für das Boot-Volume (eine pro Node)
- Zwei Blobs für 140 GB Premium-Storage für das Root-Volume (eine pro Node)
- Zwei 1024-GB-Standard-HDD-Festplatten zum Speichern der Cores (eine pro Node)
- Zwei 128-GB-Premium-SSD-Festplatten für NVRAM (eine pro Node)
- Ein Azure Snapshot für jedes Boot- und Root-Laufwerk

GCP

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

Wo sich die Festplatten befinden

Cloud Manager legt den Storage wie folgt vor:

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

  Diese Festplatte, die das Boot-Image enthält, steht Cloud Volumes ONTAP nicht zur Verfügung.
- Die Stammdaten, die die Systemkonfiguration und die Protokolle enthalten, befinden sich in aggr0.
- Das Root-Volume der Storage Virtual Machine (SVM) befindet sich in aggr1.
- Daten-Volumes befinden sich auch in aggr1.

Verschlüsselung

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

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

Erste Schritte in AWS

Erste Schritte mit Cloud Volumes ONTAP für AWS

Erste Schritte mit Cloud Volumes ONTAP für AWS

Einen Konnektor erstellen

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

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

Planen Sie Ihre Konfiguration

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

Richten Sie Ihr Netzwerk ein

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

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

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

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

"Erfahren Sie mehr über Netzwerkanforderungen".

AWS KMS einrichten

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

Starten Sie Cloud Volumes ONTAP mit Cloud Manager

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

Weiterführende Links

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

Cloud Volumes ONTAP-Konfiguration in AWS planen

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

Auswahl eines Lizenztyps

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

"Unterstützte Konfigurationen für Cloud Volumes ONTAP 9.7 in AWS"

Storage-Grenzen kennen

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

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

Dimensionierung Ihres Systems in AWS

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

Instanztyp

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

EBS-Festplattentyp

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

EBS-Festplattengröße

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

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

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

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

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

Auswahl einer Konfiguration, die Flash Cache unterstützt

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

Arbeitsblatt mit Informationen zum AWS-Netzwerk

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

Netzwerkinformationen für Cloud Volumes ONTAP

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

Netzwerkinformationen für ein HA-Paar in mehreren AZS

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

Auswählen einer Schreibgeschwindigkeit

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

Unterschied zwischen normaler Schreibgeschwindigkeit und hoher Schreibgeschwindigkeit

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

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

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

Wann wird hohe Schreibgeschwindigkeit verwendet

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

Empfehlungen bei hoher Schreibgeschwindigkeit

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

Auswählen eines Volume-Nutzungsprofils

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

NetApp Storage-Effizienzfunktionen bieten folgende Vorteile:

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

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

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

Richten Sie Ihr Netzwerk ein

Netzwerkanforderungen für Cloud Volumes ONTAP in AWS

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

Allgemeine Anforderungen für Cloud Volumes ONTAP

Die folgenden Anforderungen müssen in AWS erfüllt sein.

Outbound-Internetzugang für Cloud Volumes ONTAP Nodes

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

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

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

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

  "Erfahren Sie, wie AutoSupport konfiguriert wird".

Outbound-Internetzugang für den HA Mediator

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

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

Anzahl der IP-Adressen

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

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

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

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

Sicherheitsgruppen

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

Verbindung von Cloud Volumes ONTAP zu AWS S3 für Data Tiering

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

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

Cloud Volumes ONTAP keine Verbindung zum S3-Service herstellen.

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

Verbindungen zu ONTAP Systemen in anderen Netzwerken

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

DNS und Active Directory für CIFS

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

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

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

Anforderungen für HA-Paare in mehreren Verfügbarkeitszonen

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

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

Verfügbarkeitszonen

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

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

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

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

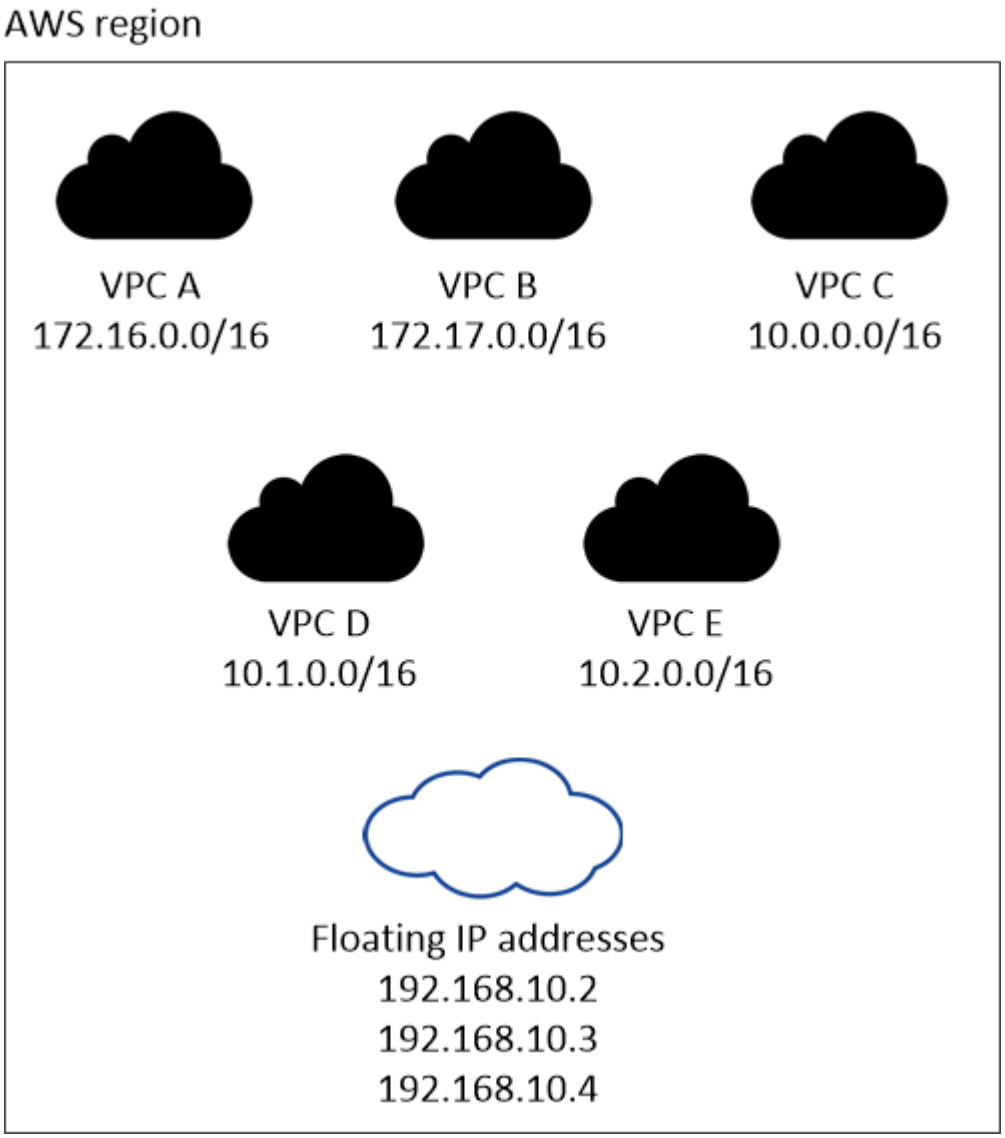
> Wenn Sie SnapDrive für Windows oder SnapCenter mit dem HA-Paar verwenden, ist eine unverankerte IP-Adresse für die SVM-Management-LIF erforderlich. Wenn Sie die IP-Adresse nicht angeben, wenn Sie das System implementieren, können Sie später die LIF erstellen. Weitere Informationen finden Sie unter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

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

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

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

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



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

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

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

Routentabellen

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

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

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

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

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

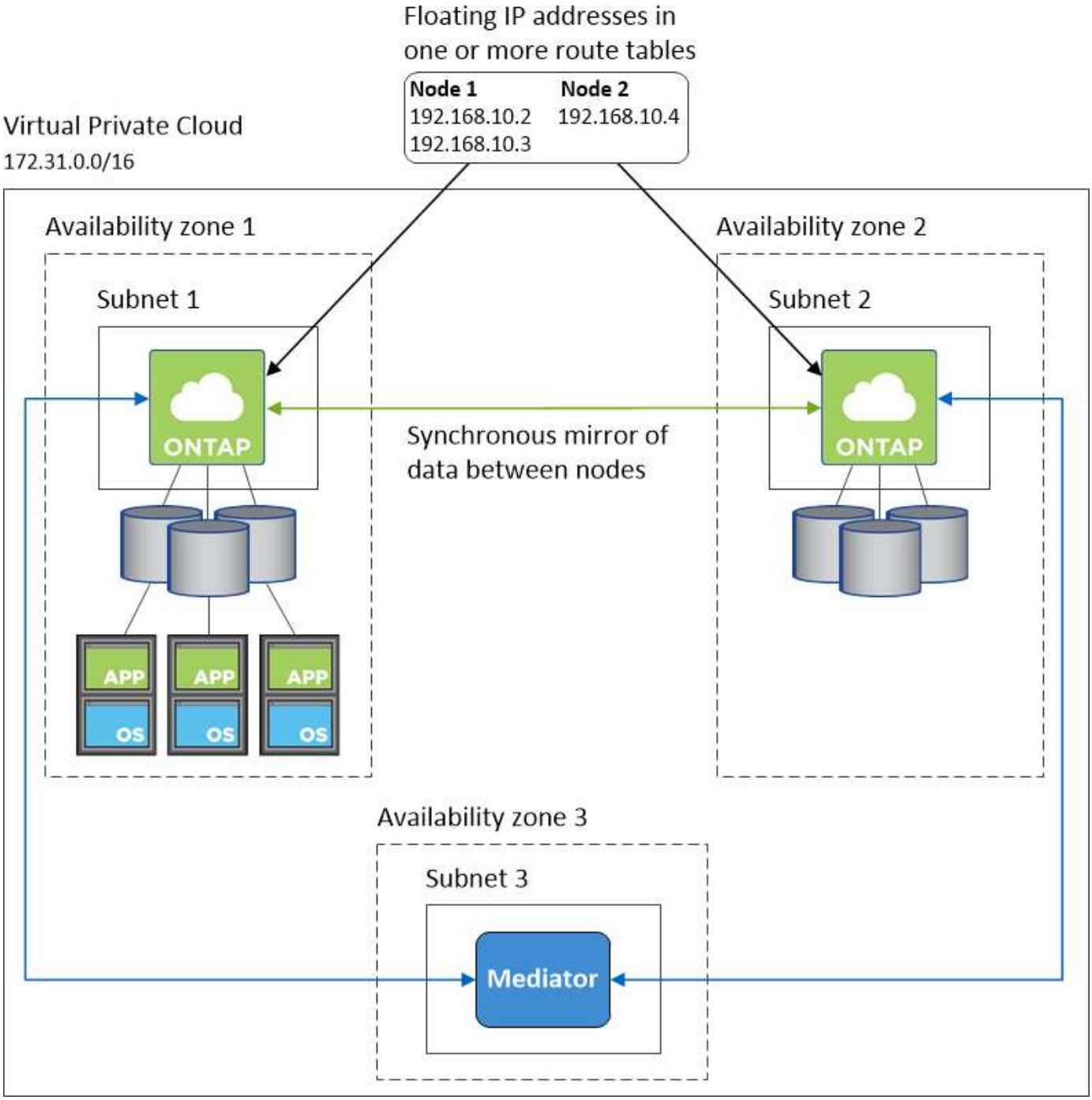
Anbindung an NetApp Management Tools

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

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

Beispiel für eine HA-Konfiguration

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



Anforderungen an den Steckverbinder

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

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

Verbindung zu Zielnetzwerken

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

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

Outbound-Internetzugang

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

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

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

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

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

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

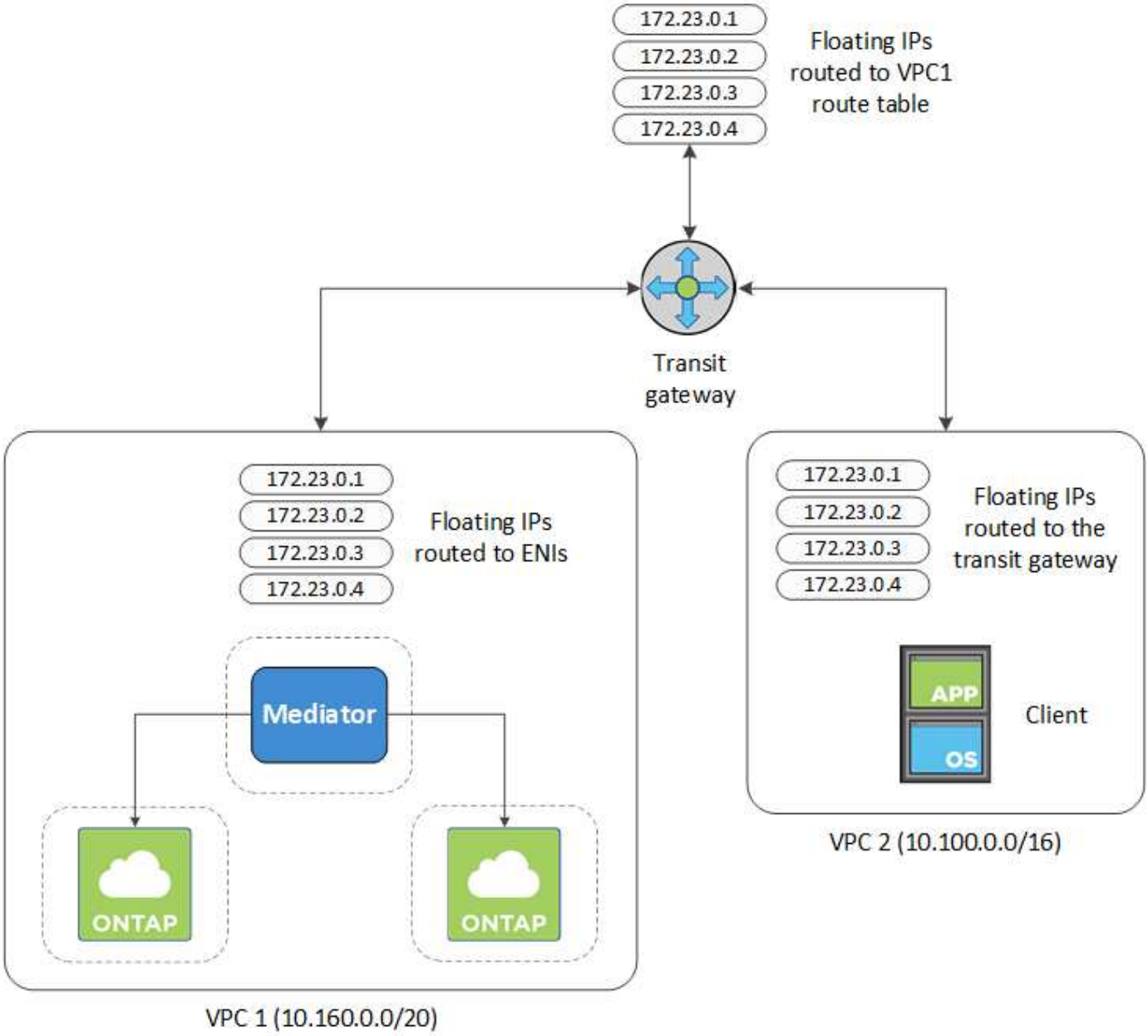
Einrichten eines AWS Transit-Gateways für den Zugriff auf HA-Paare "Floating-IP-Adressen" Von außerhalb der VPC, wo das HA-Paar residiert.

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

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

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

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

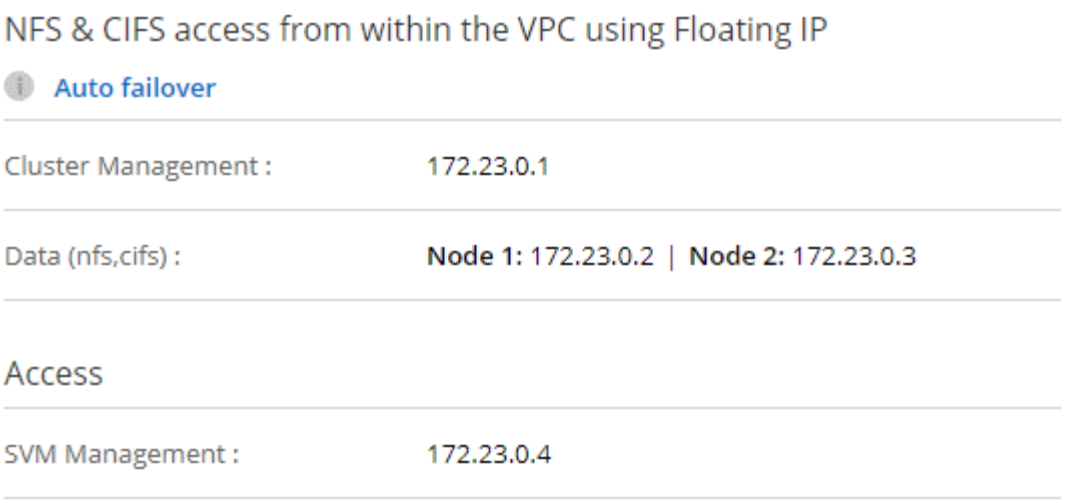


Die folgenden Schritte veranschaulichen die Einrichtung einer ähnlichen Konfiguration.

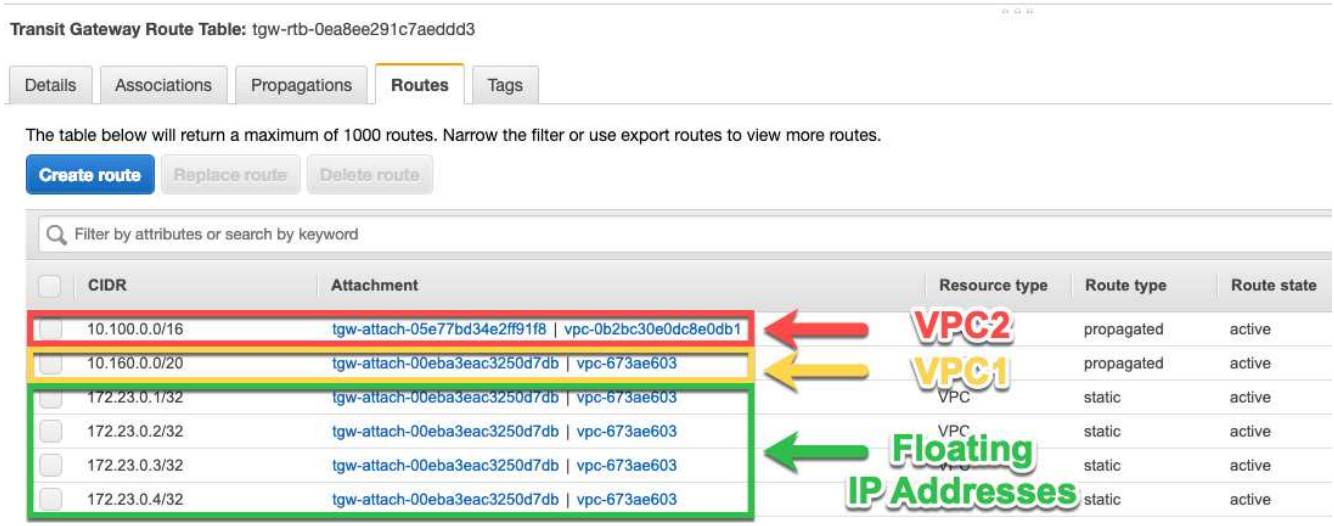
Schritte

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

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



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

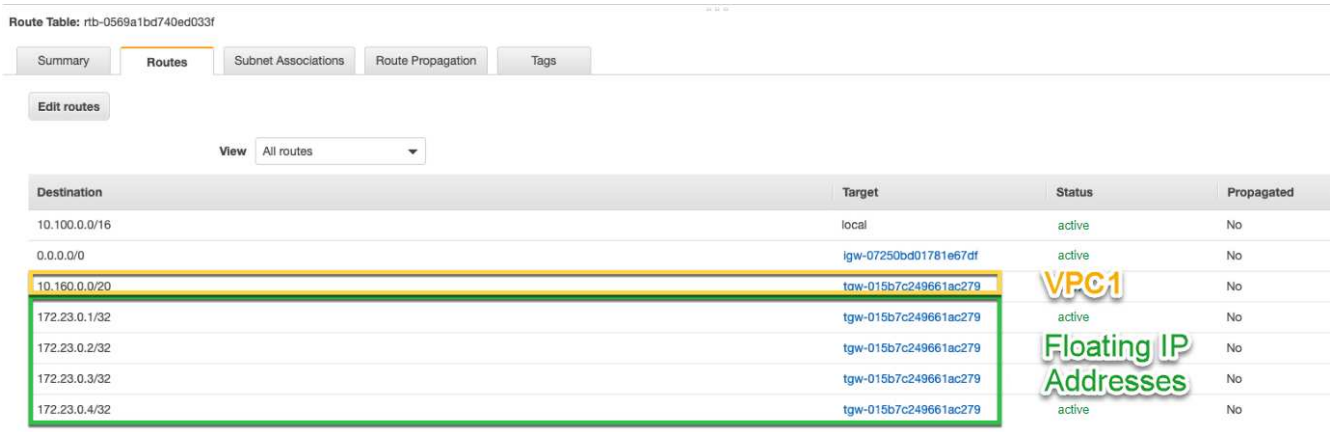


3. Ändern Sie die Routingtabelle von VPCs, die auf die fließenden IP-Adressen zugreifen müssen.

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

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

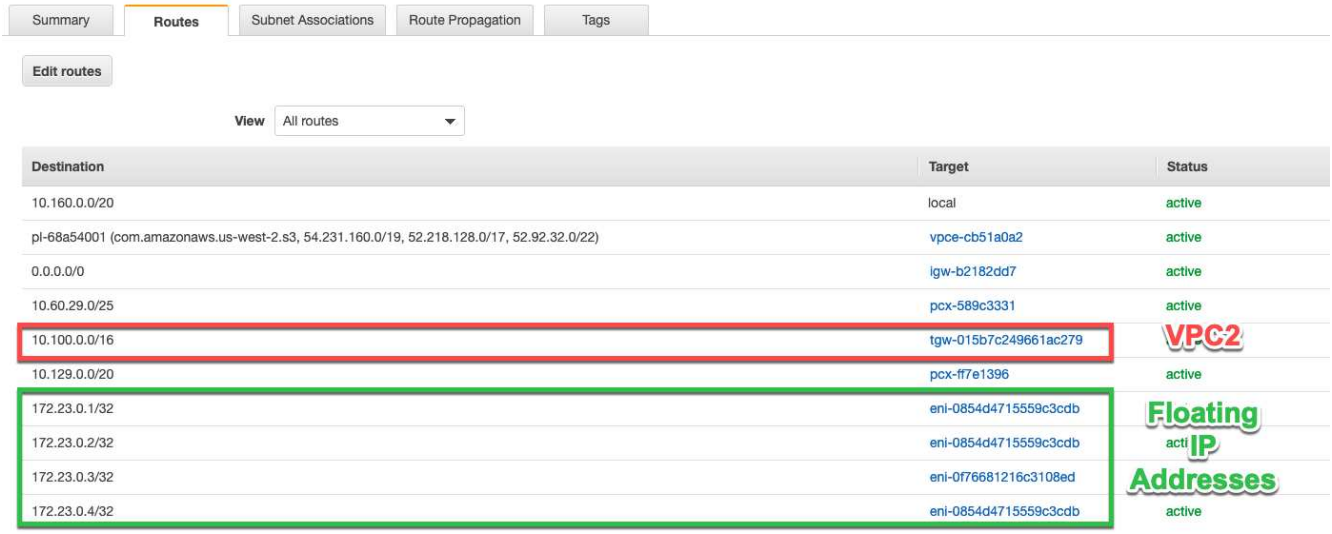
      Das folgende Beispielbild zeigt die Routingtabelle für VPC 2, die auch Routen zu VPC 1 und die fließenden IP-Adressen umfasst.



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

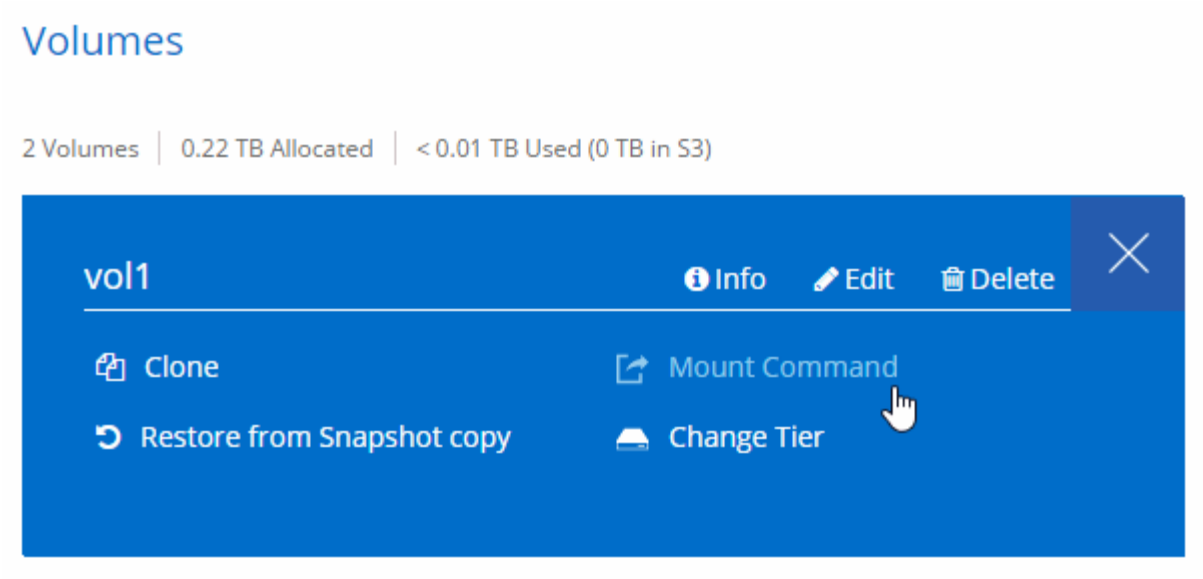
   Dieser Schritt ist wichtig, da er die Weiterleitung zwischen den VPCs abgeschlossen hat.

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



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

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



Verwandte Links

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

Sicherheitsgruppenregeln für AWS

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

Regeln für Cloud Volumes ONTAP

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

Regeln für eingehende Anrufe

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

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

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

Regeln für ausgehende Anrufe

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

Grundlegende Regeln für ausgehende Anrufe

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

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

Erweiterte Outbound-Regeln

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

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

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

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

Regeln für die externe Sicherheitsgruppe des HA Mediators

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

Regeln für eingehende Anrufe

Die Quelle für eingehende Regeln ist 0.0.0.0/0.

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

Regeln für ausgehende Anrufe

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

Grundlegende Regeln für ausgehende Anrufe

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

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

Erweiterte Outbound-Regeln

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

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

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

Regeln für die interne Sicherheitsgruppe des HA-Vermittlers

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

Regeln für eingehende Anrufe

Die vordefinierte Sicherheitsgruppe enthält die folgenden Regeln für eingehende Anrufe.

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

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe enthält die folgenden ausgehenden Regeln.

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

Regeln für den Konnektor

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

Regeln für eingehende Anrufe

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

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

Regeln für ausgehende Anrufe

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

Grundlegende Regeln für ausgehende Anrufe

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

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

Erweiterte Outbound-Regeln

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

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

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

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

Einrichten des AWS KMS

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

Schritte

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

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

   "AWS Dokumentation: Customer Master Keys (CMKs)"

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

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

   "AWS Dokumentation: Schlüssel bearbeiten"

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

   a. Wechseln Sie von dem Konto, in dem sich der CMK befindet, zur KMS-Konsole.

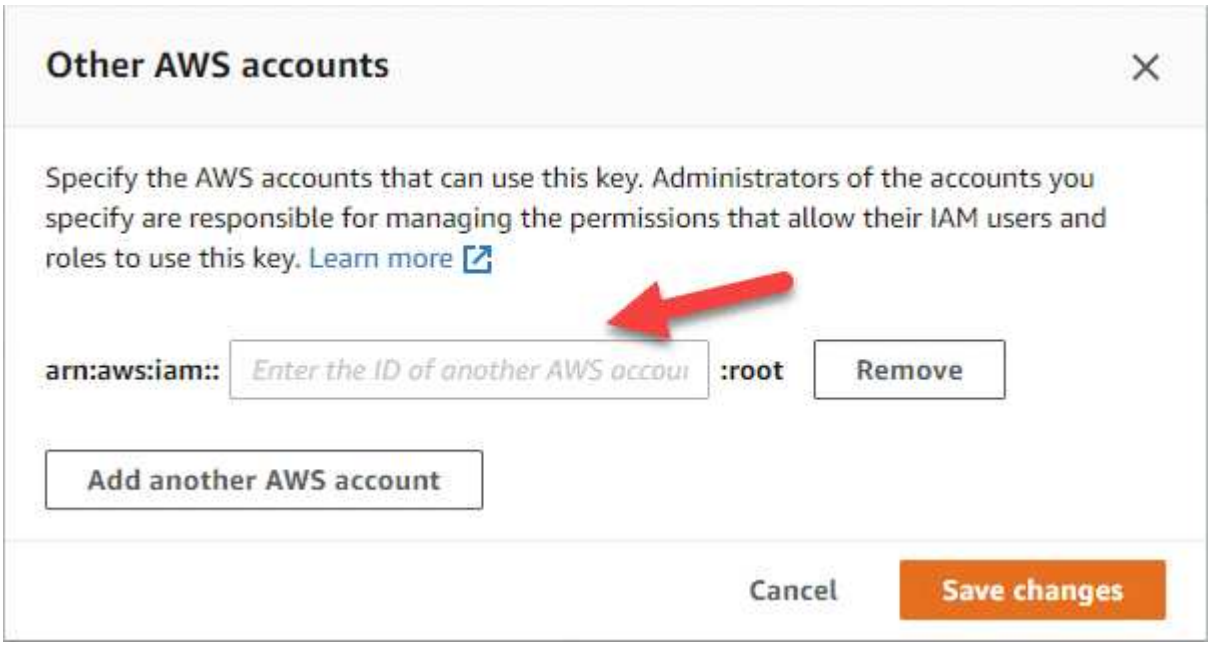
   b. Wählen Sie die Taste.

   c. Kopieren Sie im Fenster **Allgemeine Konfiguration** den ARN des Schlüssels.

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

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

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



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

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

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

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

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

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

Starten von Cloud Volumes ONTAP in AWS

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

Starten eines Cloud Volumes ONTAP Systems mit einem Node in AWS

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

Bevor Sie beginnen

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

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

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

Über diese Aufgabe

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

Schritte

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

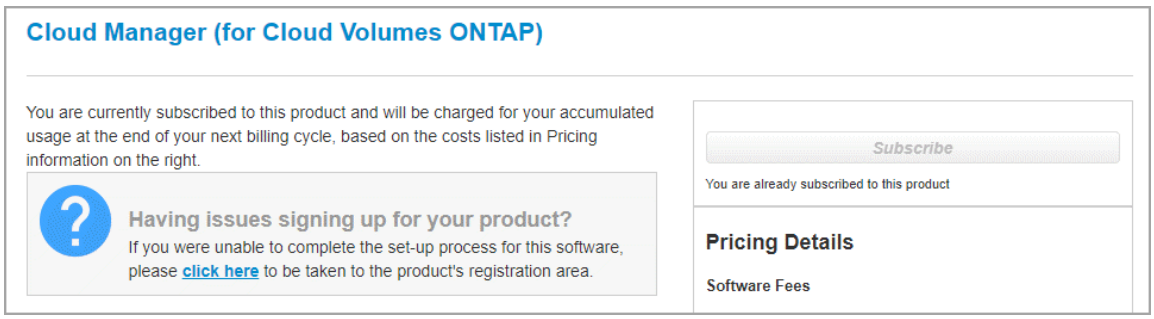
   Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

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

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

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

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



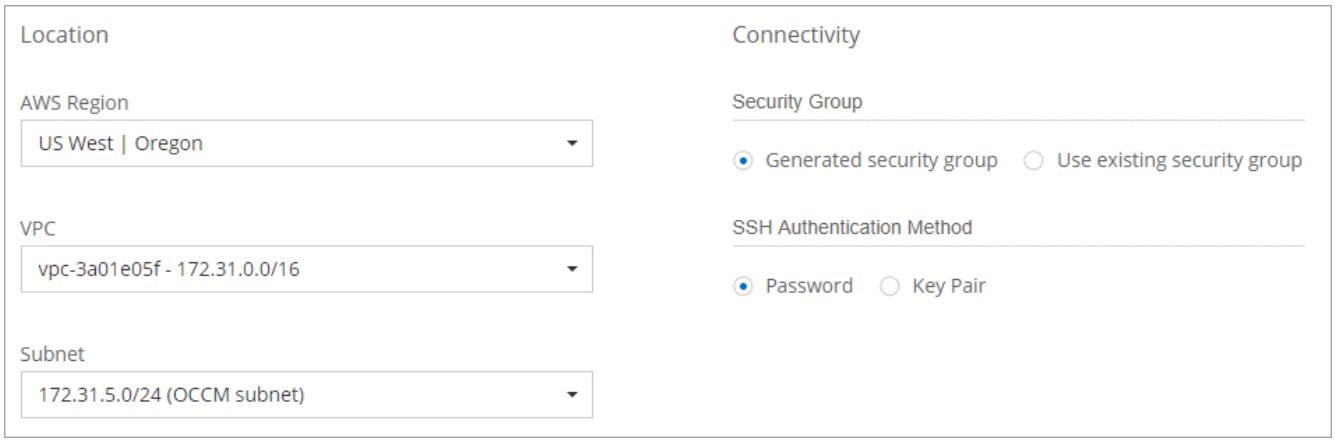
4. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie nicht mit

Cloud Volumes ONTAP verwenden möchten.

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

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

   Das folgende Bild zeigt die ausgefüllte Seite:



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

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

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

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

   "Erfahren Sie mehr über unterstützte Verschlüsselungstechnologien".

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

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

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

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

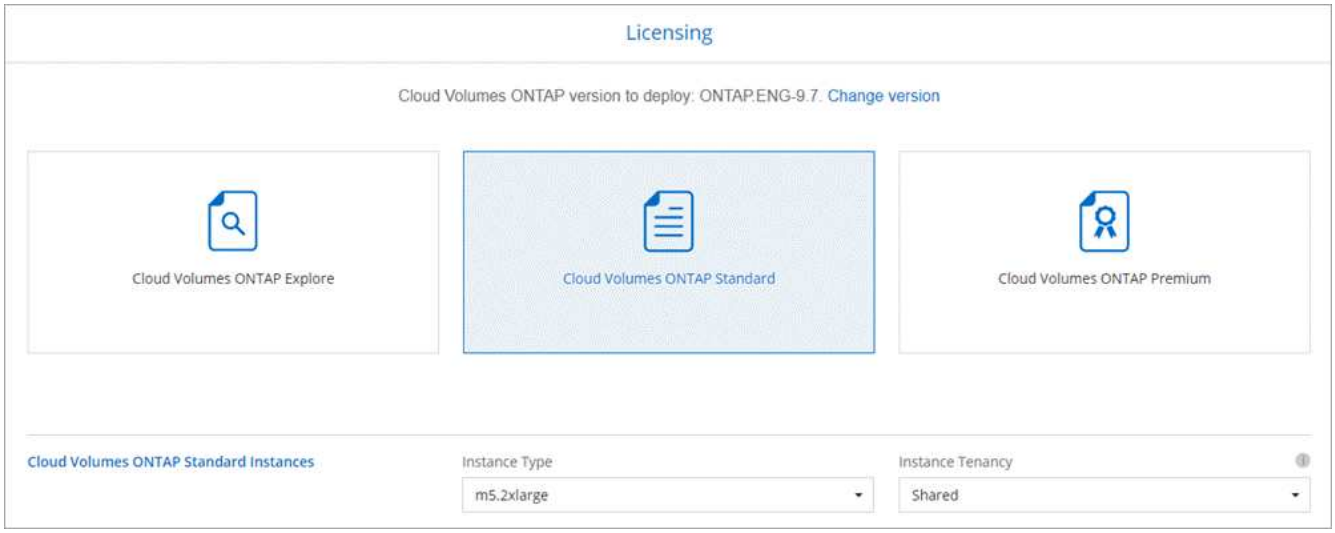
   Wenn Sie eines der Pakete auswählen, müssen Sie nur ein Volume angeben und dann die Konfiguration prüfen und genehmigen.

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

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

Cloud Volumes ONTAP-Nodes".

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



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

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

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

    Beachten Sie Folgendes:

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

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

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

      "So funktioniert Daten-Tiering".

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

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

"Erfahren Sie mehr über Schreibgeschwindigkeit".

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

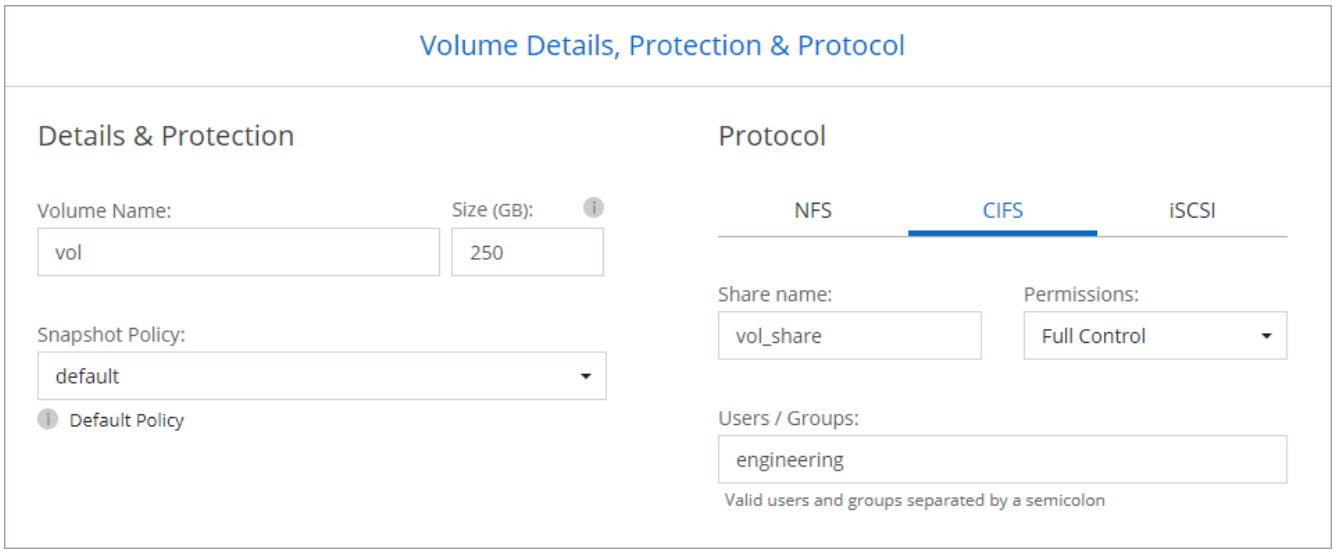
"Erfahren Sie mehr über WORM Storage".

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

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

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

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



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

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

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

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

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

a. Überprüfen Sie die Details zur Konfiguration.

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

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

d. Klicken Sie Auf **Go**.

Ergebnis

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

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

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

Nachdem Sie fertig sind

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

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

Starten eines Cloud Volumes ONTAP HA-Paars in AWS

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

Bevor Sie beginnen

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

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

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

Einschränkung

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

Über diese Aufgabe

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

Schritte

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

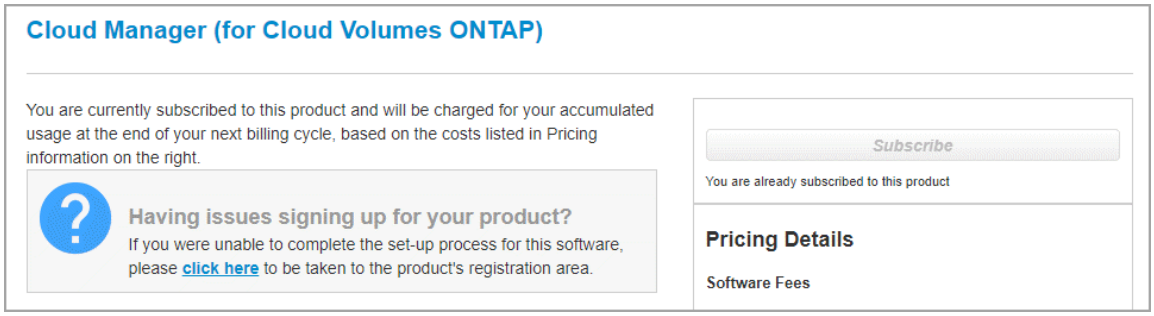
   Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

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

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

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

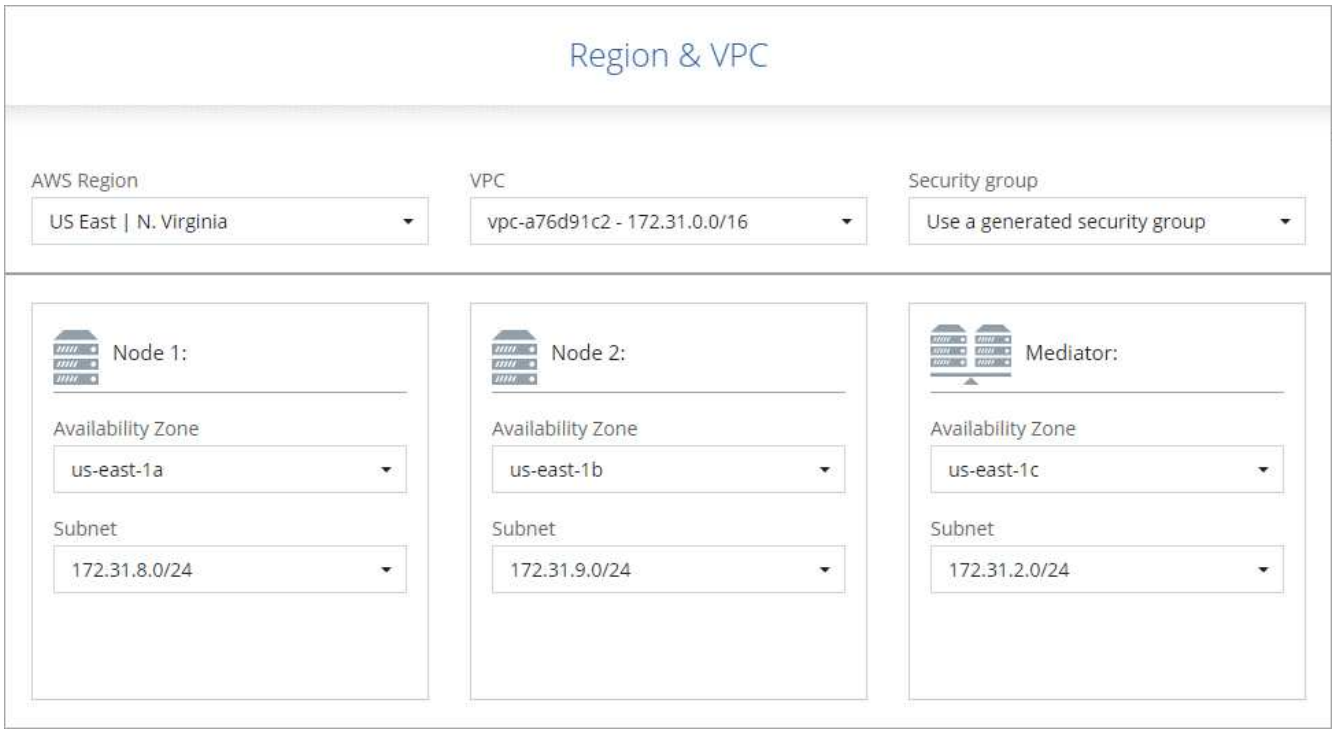
Wenn mehrere IAM-Benutzer im gleichen AWS-Konto arbeiten, muss jeder Benutzer sich anmelden. Wenn der erste Benutzer sich abonniert hat, informiert der AWS Marketplace die nachfolgenden Benutzer, dass sie bereits abonniert sind, wie in der Abbildung unten dargestellt. Während für das AWS *Account* ein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



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

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

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



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

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

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

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

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

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

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

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

    "Erfahren Sie mehr über unterstützte Verschlüsselungstechnologien".

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

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

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

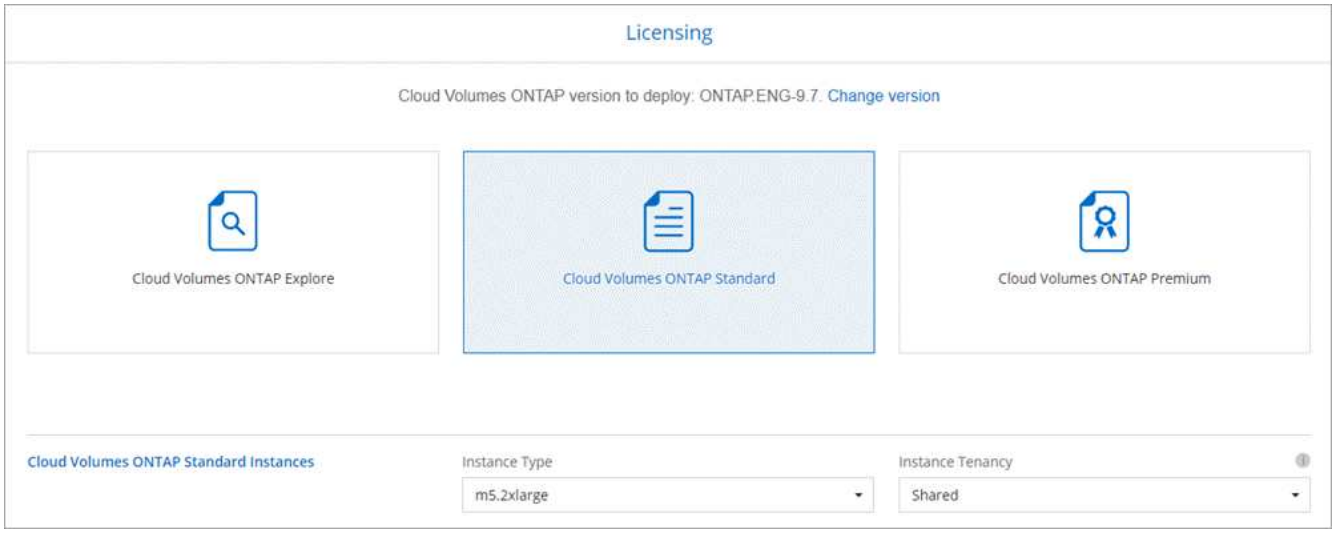
12. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete aus, um schnell ein Cloud Volumes ONTAP System zu starten, oder klicken Sie auf **eigene Konfiguration erstellen**.

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

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

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

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



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

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

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

    Beachten Sie Folgendes:

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

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

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

"So funktioniert Daten-Tiering".

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

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

    "Erfahren Sie mehr über WORM Storage".

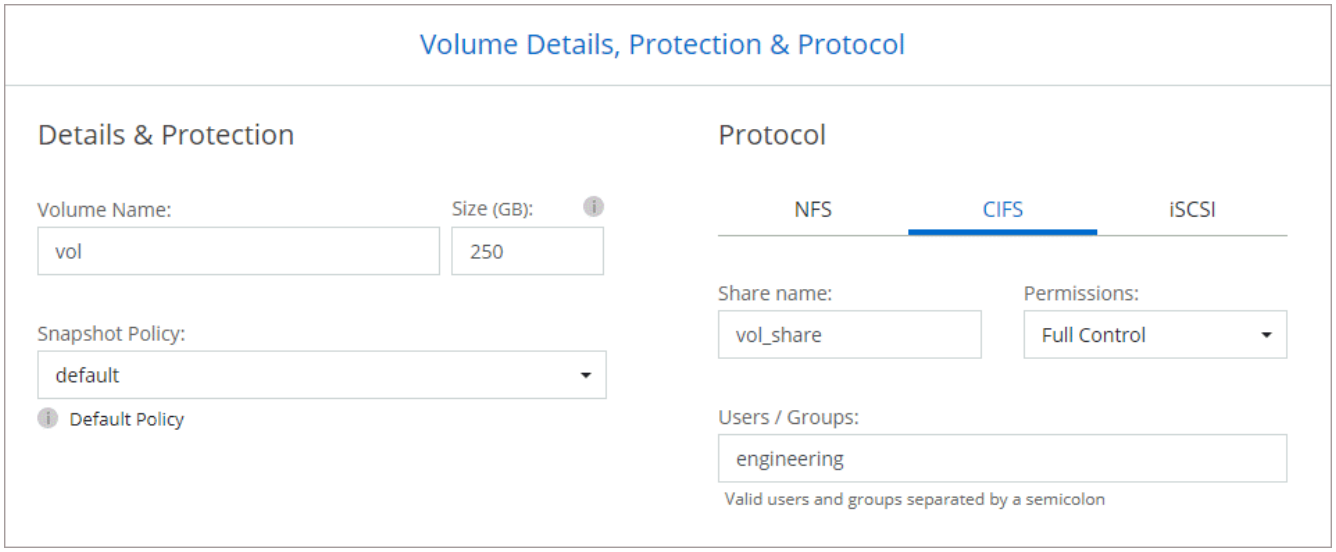
17. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

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

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

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

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



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

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

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

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

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

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

Ergebnis

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

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

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

Nachdem Sie fertig sind

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

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

Erste Schritte in Azure

Erste Schritte mit Cloud Volumes ONTAP für Azure

Erste Schritte mit Cloud Volumes ONTAP für Azure

Einen Konnektor erstellen

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

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

Planen Sie Ihre Konfiguration

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

Richten Sie Ihr Netzwerk ein

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

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

"Erfahren Sie mehr über Netzwerkanforderungen".

Starten Sie Cloud Volumes ONTAP mit Cloud Manager

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

Weiterführende Links

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

Planen Ihrer Cloud Volumes ONTAP-Konfiguration in Azure

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

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

Auswahl eines Lizenztyps

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

"Unterstützte Konfigurationen für Cloud Volumes ONTAP 9.7 in Azure"

Storage-Grenzen kennen

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

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

Dimensionierung Ihres Systems in Azure

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

Typ der virtuellen Maschine

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

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

Azure-Festplattentyp

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

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

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

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

Festplattengröße Azure

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

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

Alle Festplatten in einem Aggregat müssen dieselbe Größe haben.

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

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

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

Unter Azure finden Sie IOPS und Durchsatz nach Festplattengröße:

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

Auswahl einer Konfiguration, die Flash Cache unterstützt

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

Azure Network Information Worksheet

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

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

Auswählen einer Schreibgeschwindigkeit

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

Unterschied zwischen normaler Schreibgeschwindigkeit und hoher Schreibgeschwindigkeit

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

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

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

Wann wird hohe Schreibgeschwindigkeit verwendet

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

Empfehlungen bei hoher Schreibgeschwindigkeit

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

Auswählen eines Volume-Nutzungsprofils

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

NetApp Storage-Effizienzfunktionen bieten folgende Vorteile:

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

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

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

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

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

Anforderungen für Cloud Volumes ONTAP

Die folgenden Netzwerkanforderungen müssen in Azure erfüllt werden.

Outbound-Internetzugang für Cloud Volumes ONTAP

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

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

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

"Erfahren Sie, wie AutoSupport konfiguriert wird".

Sicherheitsgruppen

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

Anzahl der IP-Adressen

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

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

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

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

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

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

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

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

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

Verbindungen zu ONTAP Systemen in anderen Netzwerken

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

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

Anforderungen an den Steckverbinder

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

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

Verbindungen zu Zielnetzwerken

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

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

Outbound-Internetzugang

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

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

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

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

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

Regeln für Sicherheitsgruppen für Cloud Volumes ONTAP

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

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

Eingehende Regeln für Single-Node-Systeme

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

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

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

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

Eingehende Regeln für HA-Systeme

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

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

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

Regeln für ausgehende Anrufe

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

Grundlegende Regeln für ausgehende Anrufe

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

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

Erweiterte Outbound-Regeln

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

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

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

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

Sicherheitsgruppenregeln für den Konnektor

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

Regeln für eingehende Anrufe

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

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

Regeln für ausgehende Anrufe

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

Grundlegende Regeln für ausgehende Anrufe

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

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

Erweiterte Outbound-Regeln

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

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

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

Starten von Cloud Volumes ONTAP in Azure

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

Bevor Sie beginnen

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

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

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

Über diese Aufgabe

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

Risiko von Datenverlusten

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

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

Schritte

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

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

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

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

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

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

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

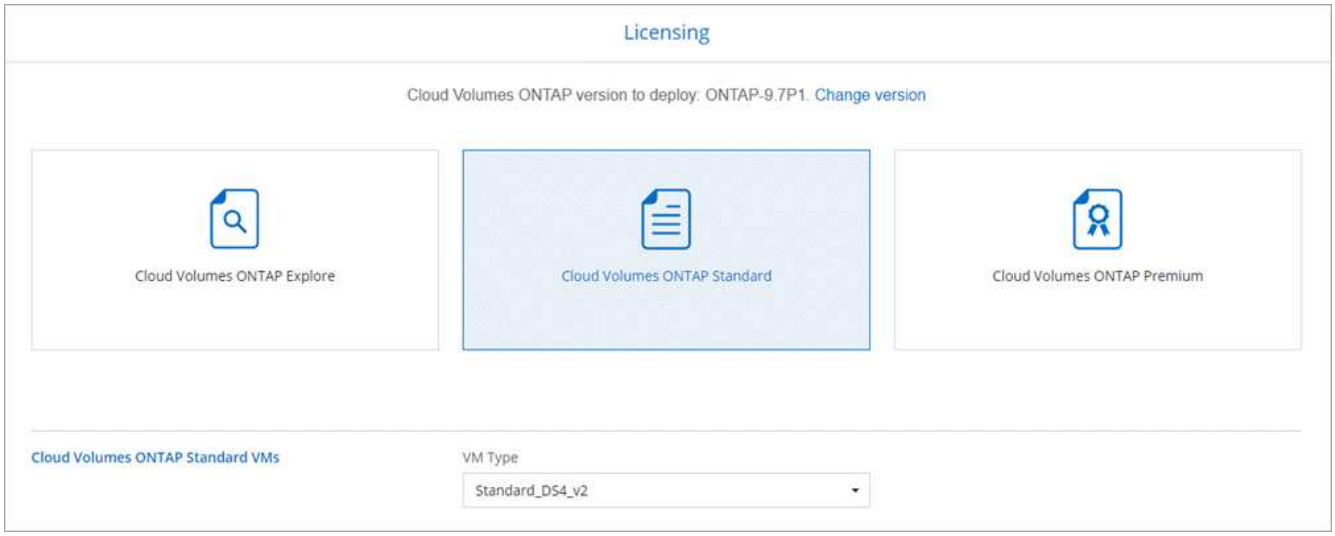
   Informationen zur Funktionsweise von Lizenzen finden Sie unter "Lizenzierung".

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

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

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

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



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

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

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

    Beachten Sie Folgendes:

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

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

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

"Weitere Informationen zum Daten-Tiering".

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

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

    "Erfahren Sie mehr über Schreibgeschwindigkeit".

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

    "Erfahren Sie mehr über WORM Storage".

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

    Die HTTPS-Verbindung besteht aus einem Cloud Volumes ONTAP 9.7 HA-Paar zu Azure Storage-Konten. Beachten Sie, dass die Aktivierung dieser Option sich auf die Schreib-Performance auswirken kann. Sie können die Einstellung nicht ändern, nachdem Sie die Arbeitsumgebung erstellt haben.

    "Erfahren Sie mehr über WORM Storage".

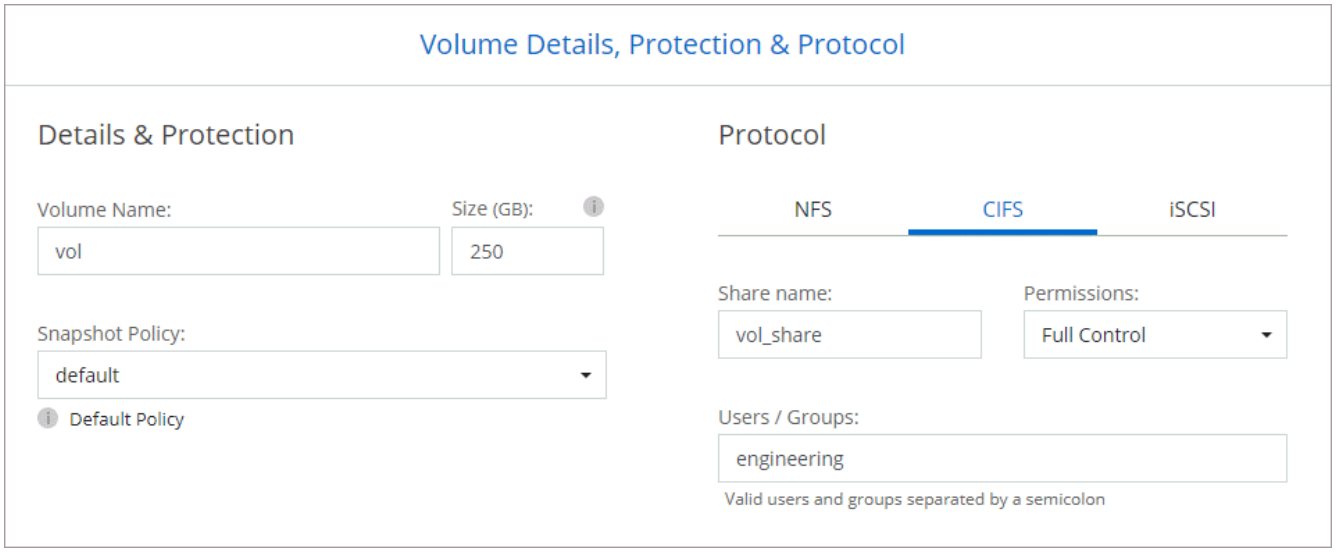
13. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

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

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

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

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



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

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

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

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

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

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

Ergebnis

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

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

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

Nachdem Sie fertig sind

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

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

Erste Schritte in GCP

Erste Schritte mit Cloud Volumes ONTAP für Google Cloud

Erste Schritte mit Cloud Volumes ONTAP für GCP

Einen Konnektor erstellen

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

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

Planen Sie Ihre Konfiguration

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

Richten Sie Ihr Netzwerk ein

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

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

"Erfahren Sie mehr über Netzwerkanforderungen".

GCP für Daten-Tiering einrichten

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

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

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

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

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

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

Aktivieren Sie Google Cloud-APIs

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

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

Starten Sie Cloud Volumes ONTAP mit Cloud Manager

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

Weiterführende Links

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

Cloud Volumes ONTAP-Konfiguration in Google Cloud planen

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

Auswahl eines Lizenztyps

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

"Unterstützte Konfigurationen für Cloud Volumes ONTAP 9.7 in GCP"

Storage-Grenzen kennen

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

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

Dimensionierung Ihres Systems in GCP

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

Maschinentyp

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

Weitere Informationen finden Sie im Folgenden:

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

GCP-Festplattentyp

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

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

GCP-Festplattengröße

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

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

  Weitere Informationen finden Sie im Folgenden:

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

Informationarbeitsblatt für das GCP-Netzwerk

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

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

Auswählen einer Schreibgeschwindigkeit

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

Unterschied zwischen normaler Schreibgeschwindigkeit und hoher Schreibgeschwindigkeit

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

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

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

Wann wird hohe Schreibgeschwindigkeit verwendet

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

Empfehlungen bei hoher Schreibgeschwindigkeit

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

Auswählen eines Volume-Nutzungsprofils

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

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

NetApp Storage-Effizienzfunktionen bieten folgende Vorteile:

Thin Provisioning

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

Deduplizierung

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

Komprimierung

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

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

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

Anforderungen für Cloud Volumes ONTAP

Die folgenden Anforderungen müssen in GCP erfüllt sein.

Virtuelle Private Cloud

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

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

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

Outbound-Internetzugang für Cloud Volumes ONTAP

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

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

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

"Erfahren Sie, wie AutoSupport konfiguriert wird".

Anzahl der IP-Adressen

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

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

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

Firewall-Regeln

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

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

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

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

Verbindungen zu ONTAP Systemen in anderen Netzwerken

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

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

Anforderungen an den Steckverbinder

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

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

Verbindung zu Zielnetzwerken

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

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

Outbound-Internetzugang

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

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

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

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

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

Firewall-Regeln für Cloud Volumes ONTAP

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

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

Regeln für eingehende Anrufe

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

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

Regeln für ausgehende Anrufe

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

Grundlegende Regeln für ausgehende Anrufe

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

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

Erweiterte Outbound-Regeln

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

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

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

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

Firewall-Regeln für den Connector

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

Regeln für eingehende Anrufe

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

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

Regeln für ausgehende Anrufe

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

Grundlegende Regeln für ausgehende Anrufe

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

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

Erweiterte Outbound-Regeln

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

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

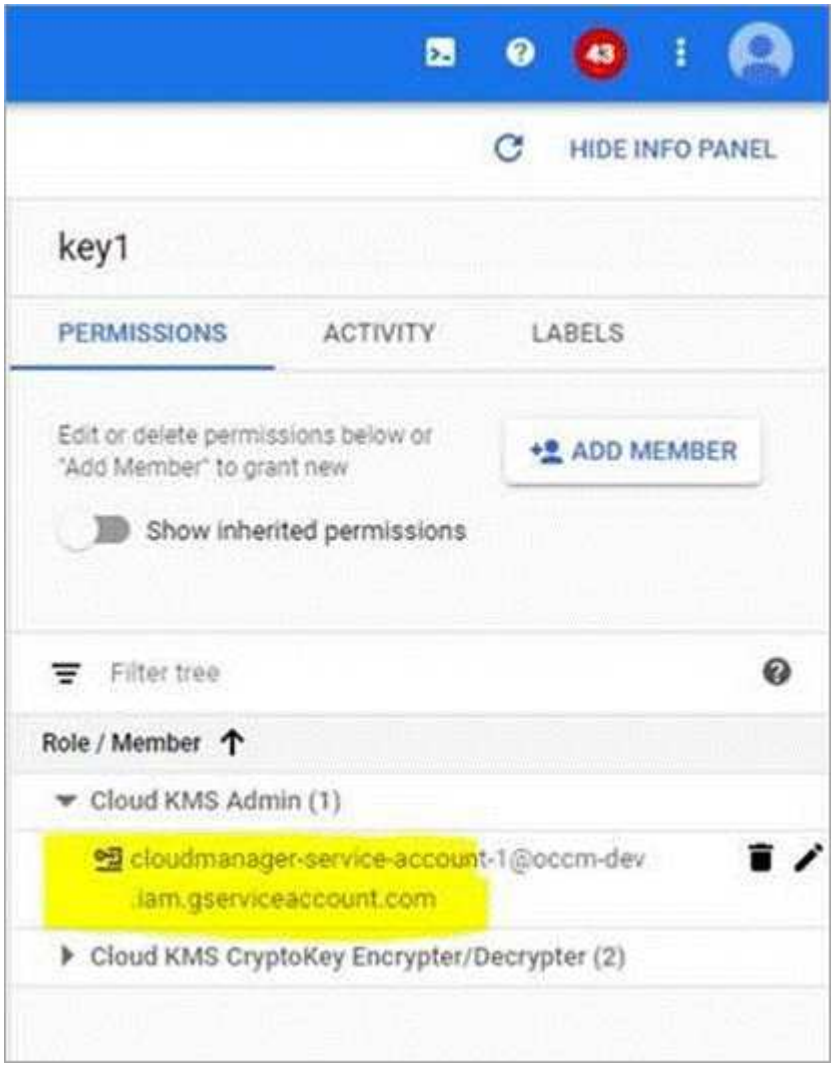
Service	Protokoll	Port	Ziel	Zweck
Active Directory	TCP	88	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	TCP	139	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP	389	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über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

Nutzung von vom Kunden gemanagten Schlüsseln mit Cloud Volumes ONTAP

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

Schritte

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



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

   Beispiel

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

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

Einführung von Cloud Volumes ONTAP in GCP

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

Was Sie benötigen

- Sie sollten ein haben "Anschluss, der Ihrem Arbeitsbereich zugeordnet ist".

> Sie müssen ein Kontoadministrator sein, um einen Konnektor zu erstellen. Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, fordert Cloud Manager Sie auf, einen Connector zu erstellen, wenn Sie noch keinen haben.

- "Sie sollten darauf vorbereitet sein, den Konnektor jederzeit in Betrieb zu nehmen".
- Sie sollten eine Konfiguration auswählen und GCP-Netzwerkinformationen von Ihrem Administrator erhalten haben. Weitere Informationen finden Sie unter "Planung Ihrer Cloud Volumes ONTAP Konfiguration".
- Für die Implementierung eines BYOL-Systems benötigen Sie für jeden Node die 20-stellige Seriennummer (Lizenzschlüssel).
- Die folgenden Google Cloud APIs sollten sein "In Ihrem Projekt aktiviert":
  - Cloud Deployment Manager V2-API
  - Cloud-ProtokollierungsAPI
  - Cloud Resource Manager API
  - Compute Engine-API
  - IAM-API (Identitäts- und Zugriffsmanagement

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.
2. **Wählen Sie einen Standort**: Wählen Sie **Google Cloud** und **Cloud Volumes ONTAP**.
3. **Details & Anmeldeinformationen**: Wählen Sie ein Projekt aus, geben Sie einen Clusternamen an, fügen Sie optional Labels hinzu und geben Sie dann Anmeldeinformationen an.

   In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Name der Arbeitsumgebung	Cloud Manager verwendet den Namen der Arbeitsumgebung, um sowohl das Cloud Volumes ONTAP System als auch die GCP VM-Instanz zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.

Feld	Beschreibung
Etiketten Hinzufügen	Beschriftungen sind Metadaten für Ihre GCP-Ressourcen. Cloud Manager fügt die Bezeichnungen dem Cloud Volumes ONTAP System und den GCP-Ressourcen hinzu, die dem System zugeordnet sind. Sie können bis zu vier Etiketten von der Benutzeroberfläche hinzufügen, wenn Sie eine Arbeitsumgebung erstellen, und dann können Sie weitere hinzufügen, nachdem sie erstellt wurde. Beachten Sie, dass Sie durch die API beim Erstellen einer Arbeitsumgebung nicht auf vier Labels beschränkt werden. Informationen zu Etiketten finden Sie unter "Google Cloud-Dokumentation: Ressourcen Zur Kennzeichnung".
Benutzername und Passwort	Dies sind die Anmeldedaten für das Cloud Volumes ONTAP Cluster-Administratorkonto. Sie können diese Anmeldedaten für die Verbindung mit Cloud Volumes ONTAP über System Manager oder dessen CLI verwenden.
Projekt Bearbeiten	Wählen Sie das Projekt aus, in dem Cloud Volumes ONTAP gespeichert werden soll. Das Standardprojekt ist das Projekt, in dem Cloud Manager residiert. Wenn in der Dropdown-Liste keine weiteren Projekte angezeigt werden, ist das Cloud Manager-Servicekonto noch nicht mit anderen Projekten verbunden. Rufen Sie die Google Cloud-Konsole auf, öffnen Sie den IAM-Service und wählen Sie das Projekt aus. Fügen Sie dem Projekt das Service-Konto mit der Rolle Cloud Manager hinzu. Sie müssen diesen Schritt für jedes Projekt wiederholen. Dies ist das Service-Konto, das Sie für Cloud Manager eingerichtet haben. "Wie in Schritt 2b auf dieser Seite beschrieben". Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen einem Abonnement zuzuordnen. Zum Erstellen eines nutzungsbasierten Cloud Volumes ONTAP Systems müssen Sie über GCP Marketplace ein GCP-Projekt für ein Cloud Volumes ONTAP Abonnement auswählen.

Das folgende Video zeigt, wie Sie ein Pay-as-you-go Marketplace Abonnement für Ihr GCP-Projekt verknüpfen:

► https://docs.netapp.com/de-de/occm38//media/video_subscribing_gcp.mp4 *(video)*

4. **Standort & Konnektivität**: Wählen Sie einen Speicherort, wählen Sie eine Firewall-Richtlinie und aktivieren Sie das Kontrollkästchen, um die Netzwerkverbindung zu Google Cloud Storage für Daten-Tiering zu bestätigen.

   Wenn „kalte“ Daten in einen Google Cloud Storage Bucket verschoben werden sollen, muss das Subnetz, in dem Cloud Volumes ONTAP residiert, für privaten Google Zugriff konfiguriert sein. Anweisungen finden Sie unter "Google Cloud Documentation: Configuring Private Google Access".

5. **Lizenz & Support Site Account**: Geben Sie an, ob Sie Pay-as-you-go oder BYOL verwenden möchten, und legen Sie dann ein NetApp Support Site Konto fest.

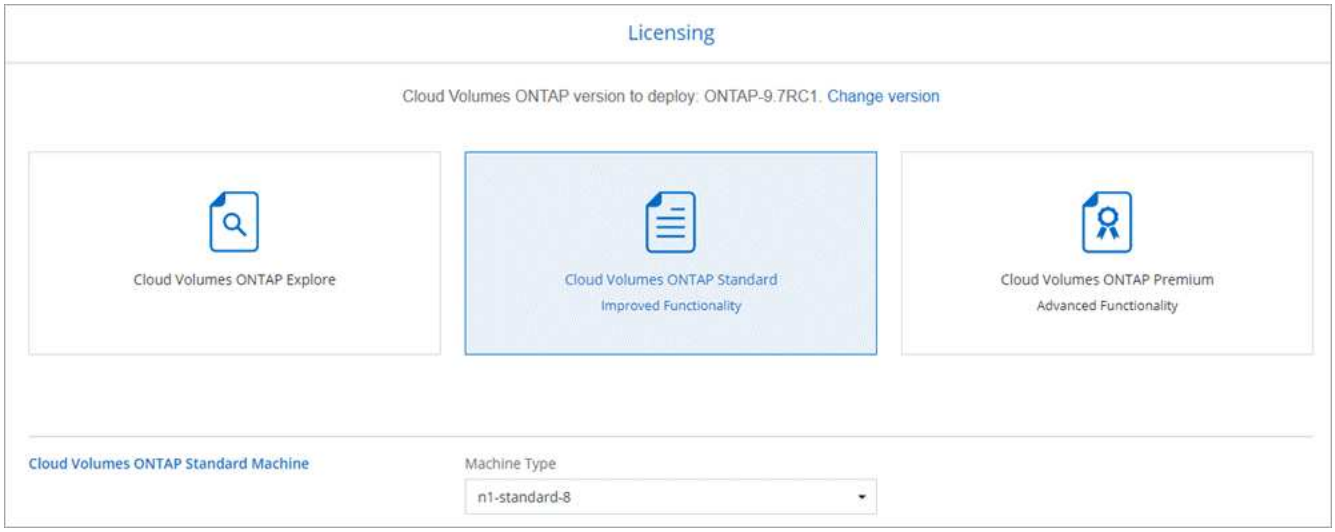
Informationen zur Funktionsweise von Lizenzen finden Sie unter "Lizenzierung".

Ein NetApp Support Site Konto ist optional für „Pay-as-you-go“-Systeme erhältlich, wird aber für BYOL-Systeme benötigt. "Erfahren Sie, wie Sie Konten der NetApp Support Site hinzufügen".

6. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete, um schnell ein Cloud Volumes ONTAP System bereitzustellen, oder klicken Sie auf **eigene Konfiguration erstellen**.

   Wenn Sie eines der Pakete auswählen, müssen Sie nur ein Volume angeben und dann die Konfiguration prüfen und genehmigen.

7. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP-Version nach Bedarf, wählen Sie eine Lizenz und wählen Sie einen virtuellen Maschinentyp.



   Wenn sich Ihre Anforderungen nach dem Start des Systems ändern, können Sie die Lizenz oder den Typ der virtuellen Maschine später ändern.

   Wenn für die ausgewählte Version ein neuer Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert Cloud Manager das System beim Erstellen der Arbeitsumgebung auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.6 RC1 und 9.6 GA auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.6 bis 9.7.

8. **Zugrunde liegende Speicherressourcen**: Wählen Sie die Einstellungen für das anfängliche Aggregat: Einen Datenträgertyp und die Größe für jede Platte.

   Der Festplattentyp ist für das anfängliche Volume. Sie können einen anderen Festplattentyp für nachfolgende Volumes auswählen.

   Die Festplattengröße gilt für alle Festplatten im ursprünglichen Aggregat und für alle zusätzlichen Aggregate, die Cloud Manager erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuweisungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

   Hilfe bei der Auswahl von Festplattentyp und -Größe finden Sie unter "Dimensionierung Ihres Systems in GCP".

9. **Schreibgeschwindigkeit & WURM**: Wählen Sie **Normal** oder **hohe** Schreibgeschwindigkeit, und

aktivieren Sie auf Wunsch den Schreib-Speicher, den WORM-Speicher.

Auswahl einer Schreibgeschwindigkeit wird nur bei Single-Node-Systemen unterstützt.

"Erfahren Sie mehr über Schreibgeschwindigkeit".

WORM kann nicht aktiviert werden, wenn Daten-Tiering aktiviert wurde.

"Erfahren Sie mehr über WORM Storage".

10. **Daten-Tiering in der Google Cloud Platform**: Wählen Sie, ob Daten-Tiering auf dem ursprünglichen Aggregat aktiviert werden soll, wählen Sie eine Storage-Klasse für die Tiered Daten, und wählen Sie dann entweder ein Service-Konto mit der vordefinierten Storage-Administratorrolle (erforderlich für Cloud Volumes ONTAP 9.7) oder wählen Sie ein GCP-Konto (erforderlich für Cloud Volumes ONTAP 9.6).

    Beachten Sie Folgendes:

    - Cloud Manager legt das Service-Konto auf der Cloud Volumes ONTAP Instanz fest. Dieses Servicekonto bietet Berechtigungen für Daten-Tiering zu einem Google Cloud Storage Bucket. Stellen Sie sicher, dass Sie das Cloud Manager-Servicekonto als Benutzer des Tiering-Dienstkontos hinzufügen, andernfalls können Sie es nicht aus Cloud Manager auswählen.
    - Hilfe zum Hinzufügen eines GCP-Kontos finden Sie unter "Einrichten und Hinzufügen von GCP-Konten für Daten-Tiering mit 9.6".
    - Sie können eine bestimmte Volume-Tiering-Richtlinie auswählen, wenn Sie ein Volume erstellen oder bearbeiten.
    - Wenn Sie das Daten-Tiering deaktivieren, können Sie es auf nachfolgenden Aggregaten aktivieren, jedoch müssen Sie das System deaktivieren und ein Service-Konto über die GCP-Konsole hinzufügen.

      "Weitere Informationen zum Daten-Tiering".

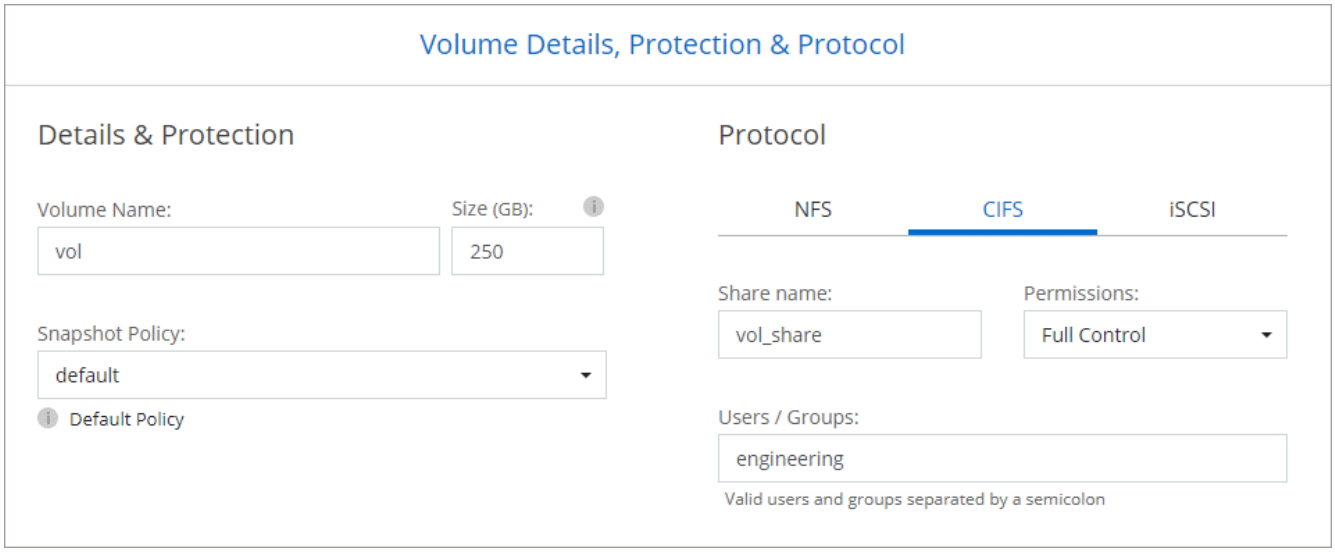
11. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

    Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren, wodurch Sie ein Volume erstellen können, das größer ist als der derzeit verfügbare physische Storage.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt Cloud Manager einen Wert ein, der Zugriff auf alle Instanzen im Subnetz ermöglicht.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch Zugriffssteuerungslisten oder ACLs genannt). Sie können lokale oder domänenbasierte Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Domain-Windows-Benutzernamen angeben, müssen Sie die Domäne des Benutzers mit dem Format Domain\Benutzername einschließen.

Feld	Beschreibung
Snapshot-Richtlinie	Eine Snapshot Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot Kopien an. Bei einer NetApp Snapshot Kopie handelt es sich um ein zeitpunktgenaues Filesystem Image, das keine Performance-Einbußen aufweist und minimalen Storage erfordert. Sie können die Standardrichtlinie oder keine auswählen. Sie können keine für transiente Daten auswählen, z. B. tempdb für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume: Entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt Cloud Manager automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Nachdem Sie das Volume erstellt haben, "Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen".

Die folgende Abbildung zeigt die für das CIFS-Protokoll ausgefüllte Volume-Seite:



12. **CIFS Setup**: Wenn Sie das CIFS-Protokoll wählen, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.

Feld	Beschreibung
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers.
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden** aus, um einen NTP-Server mit Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Siehe "Cloud Manager API-Entwicklerleitfaden" Entsprechende Details.

13. **Nutzungsprofil, Festplattentyp und Tiering-Richtlinie**: Wählen Sie aus, ob Sie Funktionen für die Storage-Effizienz aktivieren und gegebenenfalls die Volume Tiering-Richtlinie ändern möchten.

    Weitere Informationen finden Sie unter "Allgemeines zu Volume-Nutzungsprofilen" Und "Data Tiering - Übersicht".

14. **Überprüfen & Genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um weitere Informationen zum Support und zu den von Cloud Manager erworbenen GCP-Ressourcen zu erhalten.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie Auf **Go**.

Ergebnis

Cloud Manager implementiert das Cloud Volumes ONTAP System. Sie können den Fortschritt in der Timeline verfolgen.

Wenn Sie Probleme bei der Implementierung des Cloud Volumes ONTAP Systems haben, lesen Sie die Fehlermeldung. Sie können auch die Arbeitsumgebung auswählen und auf **Umgebung neu erstellen** klicken.

Weitere Hilfe finden Sie unter "NetApp Cloud Volumes ONTAP Support".

Nachdem Sie fertig sind

- Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner, und überprüfen Sie, ob diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.
- Wenn Sie Kontingente auf Volumes anwenden möchten, verwenden Sie System Manager oder die CLI.

  Mithilfe von Quotas können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder qtree verwendeten Dateien einschränken oder nachverfolgen.

Provisionierung und Management von Storage

Storage-Bereitstellung

Durch das Managen von Volumes und Aggregaten kann zusätzlicher Storage für die Cloud Volumes ONTAP Systeme vom Cloud Manager bereitgestellt werden.

> Alle Festplatten und Aggregate müssen direkt aus Cloud Manager erstellt und gelöscht werden. Sie sollten diese Aktionen nicht über ein anderes Management-Tool ausführen. Dies kann sich auf die Systemstabilität auswirken, die Fähigkeit zum Hinzufügen von Festplatten in der Zukunft beeinträchtigen und möglicherweise Kosten für redundante Cloud-Provider verursachen.

FlexVol Volumes werden erstellt

Wenn Sie nach dem Starten eines Cloud Volumes ONTAP Systems mehr Storage benötigen, können Sie aus Cloud Manager neue FlexVol Volumes für NFS, CIFS oder iSCSI erstellen.

Über diese Aufgabe

Wenn Sie ein iSCSI-Volume erstellen, erstellt Cloud Manager automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Nachdem Sie das Volume erstellt haben, Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen.

> Sie können weitere LUNs aus System Manager oder der CLI erstellen.

Bevor Sie beginnen

Wenn Sie CIFS in AWS verwenden möchten, müssen Sie DNS und Active Directory eingerichtet haben. Weitere Informationen finden Sie unter "Netzwerkanforderungen für Cloud Volumes ONTAP für AWS".

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf den Namen des Cloud Volumes ONTAP Systems, auf dem Sie FlexVol Volumes bereitstellen möchten.
2. Erstellen Sie ein neues Volume in einem beliebigen Aggregat oder in einem bestimmten Aggregat:

Aktion	Schritte
Erstellen Sie ein neues Volume, und lassen Sie Cloud Manager das enthaltende Aggregat auswählen	Klicken Sie Auf **Neues Volume Hinzufügen**.
Erstellen Sie ein neues Volume auf einem bestimmten Aggregat	a. Klicken Sie auf das Menüsymbol und dann auf **Erweitert > Erweiterte Zuweisung**. b. Klicken Sie auf das Menü für ein Aggregat. c. Klicken Sie auf **Create Volume**.

3. Geben Sie die Details für den neuen Volume ein, und klicken Sie dann auf **Weiter**.

   Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren, wodurch Sie ein Volume erstellen können, das größer ist als der derzeit verfügbare physische Storage.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt Cloud Manager einen Wert ein, der Zugriff auf alle Instanzen im Subnetz ermöglicht.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch Zugriffssteuerungslisten oder ACLs genannt). Sie können lokale oder domänenbasierte Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Domain-Windows-Benutzernamen angeben, müssen Sie die Domäne des Benutzers mit dem Format Domain\Benutzername einschließen.
Snapshot-Richtlinie	Eine Snapshot Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot Kopien an. Bei einer NetApp Snapshot Kopie handelt es sich um ein zeitpunktgenaues Filesystem Image, das keine Performance-Einbußen aufweist und minimalen Storage erfordert. Sie können die Standardrichtlinie oder keine auswählen. Sie können keine für transiente Daten auswählen, z. B. tempdb für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume: Entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt Cloud Manager automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Nachdem Sie das Volume erstellt haben, "Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen".

4. Wenn Sie das CIFS-Protokoll ausgewählt haben und der CIFS-Server noch nicht eingerichtet wurde, geben Sie im Dialogfeld Create a CIFS Server die Details für den Server an und klicken Sie dann auf **Save and Continue**:

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.

Feld	Beschreibung
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. • Um von AWS verwaltete Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, müssen Sie in diesem Feld **OU=Computers,OU=corp** eingeben. • Um Azure AD-Domänendienste als AD-Server für Cloud Volumes ONTAP zu konfigurieren, müssen Sie in diesem Feld **OU=AADDC-Computer** oder **OU=AADDC-Benutzer** eingeben.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure-Dokumentation: Erstellen Sie eine Organisationseinheit (Organisationseinheit, OU) in einer von Azure AD-Domänendiensten gemanagten Domäne"^]
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden** aus, um einen NTP-Server mit Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Siehe "Cloud Manager API-Entwicklerleitfaden" Entsprechende Details.

5. Wählen Sie auf der Seite Nutzungsprofil, Festplattentyp und Tiering-Richtlinie aus, ob Sie Funktionen der Storage-Effizienz aktivieren möchten, wählen Sie einen Festplattentyp aus und bearbeiten Sie die Tiering-Richtlinie falls erforderlich.

   Weitere Informationen finden Sie unter:

   - "Allgemeines zu Volume-Nutzungsprofilen"
   - "Dimensionierung Ihres Systems in AWS"
   - "Dimensionierung Ihres Systems in Azure"
   - "Data Tiering - Übersicht"

6. Klicken Sie Auf **Go**.

Ergebnis

Cloud Volumes ONTAP stellt das Volume bereit.

Nachdem Sie fertig sind

Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner, und überprüfen Sie, ob diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.

Wenn Sie Kontingente auf Volumes anwenden möchten, müssen Sie System Manager oder die CLI verwenden. Mithilfe von Quotas können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer

Gruppe oder qtree verwendeten Dateien einschränken oder nachverfolgen.

Erstellen von FlexVol Volumes auf dem zweiten Node in einer HA-Konfiguration

Standardmäßig erstellt Cloud Manager Volumes auf dem ersten Node in einer HA-Konfiguration. Wenn Sie eine Aktiv/Aktiv-Konfiguration benötigen, in der beide Nodes Daten für Clients bereitstellen, müssen Sie Aggregate und Volumes auf dem zweiten Node erstellen.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf den Namen der Cloud Volumes ONTAP Arbeitsumgebung, in der Sie Aggregate managen möchten.
2. Klicken Sie auf das Menü-Symbol und dann auf **Erweitert > Erweiterte Zuweisung**.
3. Klicken Sie auf **Aggregat hinzufügen** und erstellen Sie dann das Aggregat.
4. Wählen Sie für Home Node den zweiten Node im HA-Paar aus.
5. Nachdem Cloud Manager das Aggregat erstellt hat, wählen Sie es aus und klicken Sie dann auf **Create Volume**.
6. Geben Sie Details für den neuen Volume ein und klicken Sie dann auf **Erstellen**.

Nachdem Sie fertig sind

Sie können bei Bedarf weitere Volumes auf diesem Aggregat erstellen.

> Bei HA-Paaren, die in mehreren AWS Availability Zones implementiert sind, müssen Sie das Volume mithilfe der Floating-IP-Adresse des Node, auf dem sich das Volume befindet, an Clients mounten.

Aggregate werden erstellt

Sie können Aggregate selbst erstellen oder Cloud Manager bei der Erstellung von Volumes verwenden lassen. Der Vorteil der Erstellung von Aggregaten besteht darin, dass Sie die zugrunde liegende Festplattengröße wählen können, um das Aggregat an die Kapazität und Performance zu dimensionieren, die Sie benötigen.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf den Namen der Cloud Volumes ONTAP Instanz, auf der Sie Aggregate managen möchten.
2. Klicken Sie auf das Menüsymbol und dann auf **Erweitert > Erweiterte Zuweisung**.
3. Klicken Sie auf **Add Aggregate** und geben Sie dann Details für das Aggregat an.

   Hilfe zu Festplattentyp und Festplattengröße finden Sie unter "Planung Ihrer Konfiguration".

4. Klicken Sie auf **Go** und dann auf **Genehmigen und Kaufen**.

Verbinden einer LUN mit einem Host

Wenn Sie ein iSCSI-Volume erstellen, erstellt Cloud Manager automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Verwenden Sie nach dem Erstellen des Volumes den IQN, um von den Hosts eine Verbindung zur LUN herzustellen.

Beachten Sie Folgendes:

1. Das automatische Kapazitätsmanagement von Cloud Manager gilt nicht für LUNs. Wenn Cloud Manager eine LUN erstellt, wird die Autogrow Funktion deaktiviert.
2. Sie können weitere LUNs aus System Manager oder der CLI erstellen.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf die Arbeitsumgebung Cloud Volumes ONTAP, in der Sie Volumes managen möchten.
2. Wählen Sie ein Volume aus, und klicken Sie dann auf **Ziel-IQN**.
3. Klicken Sie auf **Kopieren**, um den IQN-Namen zu kopieren.
4. Richten Sie eine iSCSI-Verbindung vom Host zur LUN ein.
   - "ONTAP 9 iSCSI Express-Konfiguration für Red hat Enterprise Linux: Starten der iSCSI-Sitzungen mit dem Ziel"
   - "ONTAP 9 iSCSI Express-Konfiguration für Windows: Starten von iSCSI-Sitzungen mit dem Ziel"

Beschleunigen Sie den Datenzugriff mit FlexCache Volumes

Ein FlexCache Volume ist ein Storage Volume, das NFS-gelesene Daten aus einem Ursprungs-Volume (oder Quell-Volume) zwischenspeichert. Nachfolgende Lesezugriffe auf die zwischengespeicherten Daten führen zu einem schnelleren Zugriff auf diese Daten.

FlexCache Volumes beschleunigen den Zugriff auf Daten oder verlagern den Datenverkehr von Volumes, auf die stark zugegriffen wird. FlexCache Volumes tragen zu einer besseren Performance bei, insbesondere wenn Clients wiederholt auf dieselben Daten zugreifen müssen, da die Daten direkt ohne Zugriff auf das Ursprungs-Volume bereitgestellt werden können. FlexCache Volumes eignen sich gut für leseintensive System-Workloads.

Cloud Manager bietet derzeit kein Management von FlexCache Volumes, aber ONTAP CLI oder ONTAP System Manager ermöglicht die Erstellung und das Management von FlexCache Volumes:

- "FlexCache Volumes für schnelleren Datenzugriff – Power Guide"
- "FlexCache Volumes werden in System Manager erstellt"

Ab Version 3.7.2 generiert Cloud Manager eine FlexCache Lizenz für alle neuen Cloud Volumes ONTAP Systeme. Die Lizenz beinhaltet ein Nutzungslimit von 500 GB.

Zum Generieren der Lizenz muss Cloud Manager auf https://ipa-signer.cloudmanager.netapp.com zugreifen. Stellen Sie sicher, dass diese URL von Ihrer Firewall aus zugänglich ist.

Management von vorhandenem Storage

Mit Cloud Manager können Sie Volumes, Aggregate und CIFS-Server managen. Außerdem werden Sie aufgefordert, Volumes zu verschieben, um Kapazitätsprobleme zu vermeiden.

Management vorhandener Volumes

Sie können vorhandene Volumes managen, wenn sich Ihre Storage-Anforderungen ändern. Sie können Volumes anzeigen, bearbeiten, klonen, wiederherstellen und löschen.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf die Arbeitsumgebung Cloud Volumes ONTAP, in der Sie Volumes managen möchten.
2. Managen Sie Ihre Volumes:

Aufgabe	Aktion
Anzeigen von Informationen zu einem Volume	Wählen Sie ein Volume aus, und klicken Sie dann auf **Info**.

Aufgabe	Aktion
Bearbeiten eines Volumes (nur Volumes mit Lese-/Schreibzugriff)	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Bearbeiten**. b. Ändern Sie die Snapshot-Richtlinie des Volumes, die NFS-Protokollversion, die NFS-Zugriffskontrollliste oder die Freigabeberechtigungen und klicken Sie dann auf **Update**. Wenn Sie benutzerdefinierte Snapshot-Richtlinien benötigen, können Sie diese mit System Manager erstellen.
Klonen Sie ein Volume	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Clone**. b. Ändern Sie den Klonnamen nach Bedarf, und klicken Sie dann auf **Clone**. Bei diesem Prozess wird ein FlexClone Volume erstellt. Ein FlexClone Volume ist eine beschreibbare Point-in-Time-Kopie, die platzsparend ist, da es einen geringen Speicherplatz für Metadaten verbraucht und dann nur noch zusätzlichen Speicherplatz verbraucht, wenn Daten geändert oder hinzugefügt werden. Weitere Informationen zu FlexClone Volumes finden Sie im "ONTAP 9 Leitfaden für das Management von logischem Storage".
Wiederherstellen von Daten aus einer Snapshot Kopie auf einem neuen Volume	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Wiederherstellen aus Snapshot Kopie**. b. Wählen Sie eine Snapshot Kopie aus, geben Sie einen Namen für das neue Volume ein und klicken Sie dann auf **Wiederherstellen**.
Erstellen Sie bei Bedarf eine Snapshot Kopie	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Snapshot Kopie erstellen**. b. Ändern Sie ggf. den Namen und klicken Sie dann auf **Erstellen**.
Rufen Sie den NFS-Mount-Befehl ab	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Mount Command**. b. Klicken Sie Auf **Kopieren**.
Zeigen Sie die Ziel-IQN für ein iSCSI-Volume an	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Ziel-IQN**. b. Klicken Sie Auf **Kopieren**. c. "Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen".

Aufgabe	Aktion
Ändern Sie den zugrunde liegenden Festplattentyp	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Festplattentyp und Tiering Policy**. b. Wählen Sie den Laufwerkstyp aus und klicken Sie dann auf **Ändern**. Cloud Manager verschiebt das Volume in ein vorhandenes Aggregat, das den ausgewählten Festplattentyp verwendet, oder erstellt ein neues Aggregat für das Volume.
Ändern Sie die Tiering Policy	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Festplattentyp und Tiering Policy**. b. Klicken Sie Auf **Richtlinie Bearbeiten**. c. Wählen Sie eine andere Richtlinie aus und klicken Sie auf **Ändern**. Cloud Manager verschiebt das Volume in ein vorhandenes Aggregat, das den ausgewählten Festplattentyp mit Tiering verwendet, oder erstellt ein neues Aggregat für das Volume.
Löschen Sie ein Volume	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Löschen**. b. Klicken Sie zur Bestätigung erneut auf **Löschen**.

Management vorhandener Aggregate

Managen Sie Aggregate selbst, indem Sie Festplatten hinzufügen, Informationen über die Aggregate anzeigen und sie löschen.

Bevor Sie beginnen

Wenn Sie ein Aggregat löschen möchten, müssen Sie zunächst die Volumes im Aggregat gelöscht haben.

Über diese Aufgabe

Wenn einem Aggregat nicht mehr genügend Speicherplatz zur Verfügung steht, können Sie Volumes mithilfe von OnCommand System Manager in ein anderes Aggregat verschieben.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf die Arbeitsumgebung Cloud Volumes ONTAP, in der Sie Aggregate managen möchten.
2. Klicken Sie auf das Menü-Symbol und dann auf **Erweitert > Erweiterte Zuweisung**.
3. Verwalten Sie Ihre Aggregate:

Aufgabe	Aktion
Anzeigen von Informationen zu einem Aggregat	Wählen Sie ein Aggregat aus und klicken Sie auf **Info**.

Aufgabe	Aktion
Erstellen Sie ein Volume auf einem bestimmten Aggregat	Wählen Sie ein Aggregat aus und klicken Sie auf **Create Volume**.
Hinzufügen von Festplatten zu einem Aggregat	a. Wählen Sie ein Aggregat aus und klicken Sie auf **AWS-Festplatten hinzufügen** oder **Azure-Festplatten hinzufügen**. b. Wählen Sie die Anzahl der Festplatten aus, die Sie hinzufügen möchten, und klicken Sie auf **Hinzufügen**. Alle Festplatten in einem Aggregat müssen dieselbe Größe haben.
Löschen Sie ein Aggregat	a. Wählen Sie ein Aggregat aus, das keine Volumes enthält, und klicken Sie auf **Löschen**. b. Klicken Sie zur Bestätigung erneut auf **Löschen**.

Ändern des CIFS-Servers

Wenn Sie Ihre DNS-Server oder Active Directory-Domain ändern, müssen Sie den CIFS-Server in Cloud Volumes ONTAP ändern, damit er weiterhin Storage für Clients bereitstellen kann.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Erweitert > CIFS-Setup**.
2. Geben Sie die Einstellungen für den CIFS-Server an:

Aufgabe	Aktion
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. Wenn Sie von AWS verwaltete Microsoft AD als AD-Server für Cloud Volumes ONTAP konfigurieren, sollten Sie in diesem Feld **OU=Computers,OU=corp** eingeben.
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.

Aufgabe	Aktion
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden** aus, um einen NTP-Server mit Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Siehe "Cloud Manager API-Entwicklerleitfaden" Entsprechende Details.

3. Klicken Sie Auf **Speichern**.

Ergebnis

Cloud Volumes ONTAP aktualisiert den CIFS-Server mit den Änderungen.

Verschieben eines Volumes

Verschieben Sie Volumes, um die Kapazitätsauslastung, die Performance zu verbessern und Service Level Agreements zu erfüllen.

Sie können ein Volume in System Manager verschieben, indem Sie ein Volume und das Zielaggregat auswählen, den Vorgang zur Volume-Verschiebung starten und optional den Auftrag zur Volume-Verschiebung überwachen. Bei Nutzung von System Manager wird die Verschiebung eines Volumes automatisch abgeschlossen.

Schritte

1. Verwenden Sie System Manager oder die CLI, um die Volumes in das Aggregat zu verschieben.

   In den meisten Fällen können Sie mit System Manager Volumes verschieben.

   Anweisungen hierzu finden Sie im "ONTAP 9 Volume Move Express Guide".

Durch das Verschieben eines Volumes, wenn Cloud Manager eine Meldung über die erforderliche Aktion angezeigt wird

Cloud Manager zeigt möglicherweise eine Meldung "Aktion erforderlich" an, die besagt, dass das Verschieben eines Volumes erforderlich ist, um Kapazitätsprobleme zu vermeiden, aber keine Empfehlungen zur Behebung des Problems geben kann. In diesem Fall müssen Sie herausfinden, wie das Problem behoben werden kann, und dann ein oder mehrere Volumes verschieben.

Schritte

1. wie Kapazitätsprobleme behoben werden,Identifizieren, wie das Problem behoben werden kann.
2. Verschieben Sie Volumes basierend auf Ihrer Analyse, um Kapazitätsprobleme zu vermeiden:
   - um Kapazitätsprobleme zu vermeiden,Volumes werden in ein anderes System verschoben.
   - um Kapazitätsprobleme zu vermeiden,Verschieben Sie Volumes zu einem anderen Aggregat auf demselben System.

Identifizieren, wie Kapazitätsprobleme behoben werden

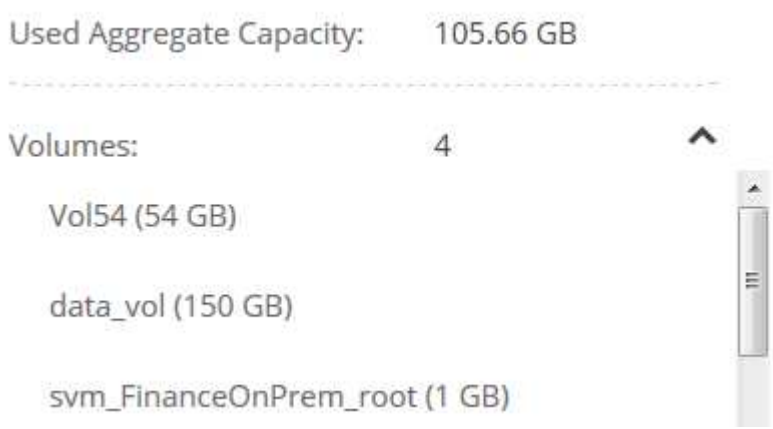
Wenn Cloud Manager keine Empfehlungen für das Verschieben eines Volumes zur Vermeidung von Kapazitätsproblemen geben kann, müssen Sie die Volumes identifizieren, die Sie verschieben müssen, und angeben, ob Sie sie in ein anderes Aggregat auf demselben System oder in ein anderes System verschieben sollten.

Schritte

1. Zeigen Sie die erweiterten Informationen in der Meldung Aktion erforderlich an, um das Aggregat zu identifizieren, das seine Kapazitätsgrenze erreicht hat.

   Die erweiterten Informationen sollten beispielsweise Folgendes enthalten: Aggregat aggr1 hat seine Kapazitätsgrenze erreicht.

2. Identifizieren Sie ein oder mehrere Volumes, die aus dem Aggregat verschoben werden sollen:
   a. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Erweiterte Zuweisung**.
   b. Wählen Sie das Aggregat aus und klicken Sie dann auf **Info**.
   c. Erweitern Sie die Liste der Volumes.



   d. Überprüfen Sie die Größe jedes Volumes, und wählen Sie ein oder mehrere Volumes aus, die aus dem Aggregat verschoben werden sollen.

      Sie sollten Volumes auswählen, die groß genug sind, um Speicherplatz im Aggregat freizugeben, damit Sie in Zukunft zusätzliche Kapazitätsprobleme vermeiden können.

3. Wenn das System die Festplattengrenze nicht erreicht hat, sollten Sie die Volumes in ein vorhandenes Aggregat oder ein neues Aggregat auf demselben System verschieben.

   Weitere Informationen finden Sie unter "Verschieben von Volumes in ein anderes Aggregat, um Kapazitätsprobleme zu vermeiden".

4. Wenn das System die Festplattengrenze erreicht hat, führen Sie einen der folgenden Schritte aus:
   a. Löschen Sie nicht verwendete Volumes.
   b. Ordnen Sie Volumes neu an, um Speicherplatz auf einem Aggregat freizugeben.

      Weitere Informationen finden Sie unter "Verschieben von Volumes in ein anderes Aggregat, um Kapazitätsprobleme zu vermeiden".

   c. Verschieben Sie zwei oder mehr Volumes auf ein anderes System mit Speicherplatz.

      Weitere Informationen finden Sie unter "Verschieben von Volumes auf ein anderes System, um Kapazitätsprobleme zu vermeiden".

Verschieben von Volumes auf ein anderes System, um Kapazitätsprobleme zu vermeiden

Sie können ein oder mehrere Volumes in ein anderes Cloud Volumes ONTAP System verschieben, um Kapazitätsprobleme zu vermeiden. Dies kann erforderlich sein, wenn das System die Festplattengrenze erreicht hat.

Über diese Aufgabe

Sie können die folgenden Schritte in dieser Aufgabe ausführen, um die folgende Meldung "Aktion erforderlich" zu korrigieren:

```
 Moving a volume is necessary to avoid capacity issues; however, Cloud
Manager cannot perform this action for you because the system has reached
the disk limit.
.Schritte
. Identifizieren Sie ein Cloud Volumes ONTAP System mit verfügbarer
Kapazität, oder implementieren Sie ein neues System.
. Ziehen Sie die Quellarbeitsumgebung per Drag & Drop in die
Zielarbeitsumgebung, um eine einmalige Datenreplizierung des Volumes
durchzuführen.
```

+
Weitere Informationen finden Sie unter "Replizierung von Daten zwischen Systemen".

1. Wechseln Sie zur Seite "Replication Status", und brechen Sie die SnapMirror Beziehung ab, um das replizierte Volume von einem Datensicherungsvolume in ein Lese-/Schreibvolume zu konvertieren.

   Weitere Informationen finden Sie unter "Managen von Plänen und Beziehungen zur Datenreplizierung".

2. Konfigurieren Sie das Volume für den Datenzugriff.

   Informationen über die Konfiguration eines Ziel-Volume für den Datenzugriff finden Sie unter "ONTAP 9 Express Guide für die Disaster Recovery von Volumes".

3. Löschen Sie das ursprüngliche Volume.

   Weitere Informationen finden Sie unter "Management vorhandener Volumes".

Verschieben von Volumes in ein anderes Aggregat, um Kapazitätsprobleme zu vermeiden

Sie können ein oder mehrere Volumes in ein anderes Aggregat verschieben, um Kapazitätsprobleme zu vermeiden.

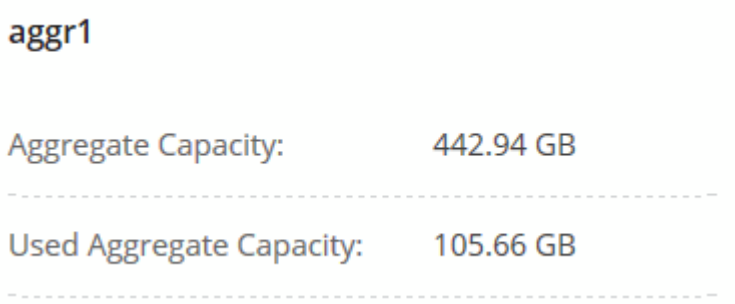
Über diese Aufgabe

Sie können die folgenden Schritte in dieser Aufgabe ausführen, um die folgende Meldung "Aktion erforderlich" zu korrigieren:

```
 Moving two or more volumes is necessary to avoid capacity issues;
however, Cloud Manager cannot perform this action for you.
.Schritte
. Überprüfen Sie, ob ein vorhandenes Aggregat über die verfügbare
Kapazität für die Volumes verfügt, die Sie verschieben müssen:
```

+
.. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Erweiterte Zuweisung**.
.. Wählen Sie jedes Aggregat aus, klicken Sie auf **Info** und sehen Sie dann die verfügbare Kapazität (Aggregatskapazität minus genutzte Aggregatskapazität).

+



1. Fügen Sie bei Bedarf Festplatten zu einem vorhandenen Aggregat hinzu:
   a. Wählen Sie das Aggregat aus und klicken Sie dann auf **Add Disks**.
   b. Wählen Sie die Anzahl der hinzuzufügenden Festplatten aus, und klicken Sie dann auf **Hinzufügen**.
2. Wenn keine Aggregate über verfügbare Kapazität verfügen, erstellen Sie ein neues Aggregat.

   Weitere Informationen finden Sie unter "Aggregate werden erstellt".
3. Verwenden Sie System Manager oder die CLI, um die Volumes in das Aggregat zu verschieben.
4. In den meisten Fällen können Sie mit System Manager Volumes verschieben.

   Anweisungen hierzu finden Sie im "ONTAP 9 Volume Move Express Guide".

Gründe, warum eine Volume-Verschiebung langsam durchführen könnte

Das Verschieben eines Volumes dauert möglicherweise länger, als erwartet wird, wenn eine der folgenden Bedingungen für Cloud Volumes ONTAP zutrifft:

- Das Volume ist ein Klon.
- Das Volume ist ein übergeordnetes Objekt eines Klons.
- Das Quell- oder Zielaggregat verfügt über eine einzige durchsatzoptimierte Festplatte (st1).
- Das Cloud Volumes ONTAP System befindet sich in AWS und ein Aggregat verwendet ein älteres Benennungsschema für Objekte. Beide Aggregate müssen das gleiche Namenformat verwenden.

  Ein älteres Benennungsschema wird verwendet, wenn das Daten-Tiering auf einem Aggregat in Version 9.4 oder früher aktiviert wurde.

- Die Verschlüsselungseinstellungen stimmen nicht mit den Quell- und Zielaggregaten überein. Zudem wird ein Rekey ausgeführt.
- Die Option *-Tiering-Richtlinie* wurde bei der Verschiebung des Volumes angegeben, um die Tiering-Richtlinie zu ändern.
- Die Option *-Generate-Destination-key* wurde für die Verschiebung des Volumes angegeben.

Tiering inaktiver Daten in kostengünstigen Objektspeicher

Sie können die Storage-Kosten für Cloud Volumes ONTAP senken, indem Sie eine SSD- oder HDD-Performance-Tier für häufig abgerufene Daten mit einem Objekt-Storage-Kapazitäts-Tier für inaktive Daten kombinieren. Eine allgemeine Übersicht finden Sie unter "Data Tiering - Übersicht".

Zum Einrichten von Data Tiering müssen Sie lediglich Folgendes tun:

Wählen Sie eine unterstützte Konfiguration aus

Die meisten Konfigurationen werden unterstützt. Wenn Sie über ein Cloud Volumes ONTAP Standard-, Premium- oder BYOL-System mit der aktuellsten Version verfügen, sollten Sie sich dafür entscheiden. "Weitere Informationen .".

Stellen Sie die Konnektivität zwischen Cloud Volumes ONTAP und Objekt-Storage sicher

- Für AWS ist ein VPC Endpunkt zu S3 erforderlich. Weitere Informationen ..
- Bei Azure sind keine Vorgänge mehr notwendig, solange Cloud Manager über die erforderlichen Berechtigungen verfügt. Weitere Informationen ..
- Für GCP müssen Sie das Subnetz für privaten Google Access konfigurieren und ein Service-Konto einrichten. Weitere Informationen ..

Wählen Sie eine Tiering-Richtlinie beim Erstellen, Ändern oder Replizieren eines Volume

Cloud Manager fordert Sie auf, beim Erstellen, Ändern oder Replizieren eines Volume eine Tiering-Richtlinie auszuwählen.

- "Tiering von Daten auf Lese-/Schreib-Volumes"
- "Tiering von Daten auf Data-Protection-Volumes"

Welche und#8217;s sind für das Daten-Tiering nicht erforderlich

- Für die Aktivierung von Daten-Tiering müssen Sie keine Funktionslizenz installieren.
- Es ist nicht erforderlich, die Kapazitäts-Tier (ein S3-Bucket, Azure Blob-Container oder GCP-Bucket) zu erstellen. Cloud Manager macht das für Sie.

Konfigurationen, die Daten-Tiering unterstützen

Sie können das Daten-Tiering aktivieren, wenn Sie bestimmte Konfigurationen und Funktionen verwenden:

- Das Daten-Tiering wird mit Cloud Volumes ONTAP Standard, Premium und BYOL unterstützt. Es beginnt mit den folgenden Versionen:
  - Version 9.2 in AWS
  - Version 9.4 in Azure mit Single-Node-Systemen
  - Version 9.6 in Azure mit HA-Paaren
  - Version 9.6 in GCP

  Data Tiering wird in Azure mit dem virtuellen Maschinentyp DS3_v2 nicht unterstützt.

- In AWS kann es sich um allgemeine SSDs, bereitgestellte IOPS SSDs oder Throughput Optimized HDDs handeln.
- In Azure kann die Performance-Tier Premium-Festplatten mit SSD-Management, von Standard-SSDs gemanagte Festplatten oder von Standard-HDDs gemanagte Festplatten sein.
- In der GCP kann die Performance-Tier entweder SSDs oder HDDs (Standard-Festplatten) sein.
- Daten-Tiering wird durch Verschlüsselungstechnologien unterstützt.
- Thin Provisioning muss auf Volumes aktiviert sein.

Anforderungen für das Tiering selten genutzter Daten in AWS S3

Stellen Sie sicher, dass Cloud Volumes ONTAP eine Verbindung zu S3 hat. Die beste Möglichkeit, diese Verbindung bereitzustellen, besteht darin, einen VPC-Endpunkt für den S3-Dienst zu erstellen. Anweisungen hierzu finden Sie unter "AWS Dokumentation: Erstellen eines Gateway-Endpunkts".

Wenn Sie den VPC-Endpunkt erstellen, wählen Sie die Region, den VPC und die Routing-Tabelle aus, die der Cloud Volumes ONTAP Instanz entspricht. Sie müssen auch die Sicherheitsgruppe ändern, um eine ausgehende HTTPS-Regel hinzuzufügen, die Datenverkehr zum S3-Endpunkt ermöglicht. Andernfalls kann Cloud Volumes ONTAP keine Verbindung zum S3-Service herstellen.

Informationen zu Problemen finden Sie unter "AWS Support Knowledge Center: Warum kann ich mich nicht über einen Gateway VPC Endpunkt mit einem S3-Bucket verbinden?".

Tiering selten genutzter Daten auf Azure Blob Storage

Es muss keine Verbindung zwischen der Performance-Tier und der Kapazitäts-Tier eingerichtet werden, sofern Cloud Manager über die erforderlichen Berechtigungen verfügt. Cloud Manager unterstützt ein vnet-Service-Endpunkt für Sie, wenn die Cloud Manager-Richtlinie über die folgenden Berechtigungen verfügt:

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Die Berechtigungen sind in der letzten enthalten "Cloud Manager-Richtlinie".

Anforderungen für das Tiering selten genutzter Daten in einen Google Cloud Storage Bucket

- Das Subnetz, in dem Cloud Volumes ONTAP residiert, muss für privaten Google-Zugriff konfiguriert werden. Anweisungen finden Sie unter "Google Cloud Documentation: Configuring Private Google Access".
- Sie benötigen ein Servicekonto mit der vordefinierten Storage-Administratorrolle. Wählen Sie dieses Servicekonto aus, wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen.

  "Richten Sie dieses Tiering-Dienstkonto wie folgt ein":

  a. Weisen Sie dem Tiering-Service-Konto die vordefinierte Rolle „*Storage Admin*“ zu.

  b. Fügen Sie das Connector-Dienstkonto als *Service-Konto-Benutzer* zum Tiering-Dienstkonto hinzu.

     Sie können die Benutzerrolle angeben "In Schritt 3 des Assistenten, wenn Sie das Tiering Service-Konto erstellen", Oder "Geben Sie die Rolle nach der Erstellung des Dienstkontos ein".

     Sie müssen das Tiering Service-Konto später auswählen, wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen.

  Wenn Sie kein Daten-Tiering aktivieren und bei der Erstellung des Cloud Volumes ONTAP-Systems ein Service-Konto auswählen, müssen Sie das System deaktivieren und das Service-Konto über die GCP-Konsole zu Cloud Volumes ONTAP hinzufügen.

Tiering von Daten aus Volumes mit Lese- und Schreibvorgängen

Cloud Volumes ONTAP kann inaktive Daten auf Volumes mit Lese- und Schreibvorgängen auf kostengünstigen Objekt-Storage verschieben und so den Performance-Tier für häufig abgerufene Daten freisetzen.

Schritte

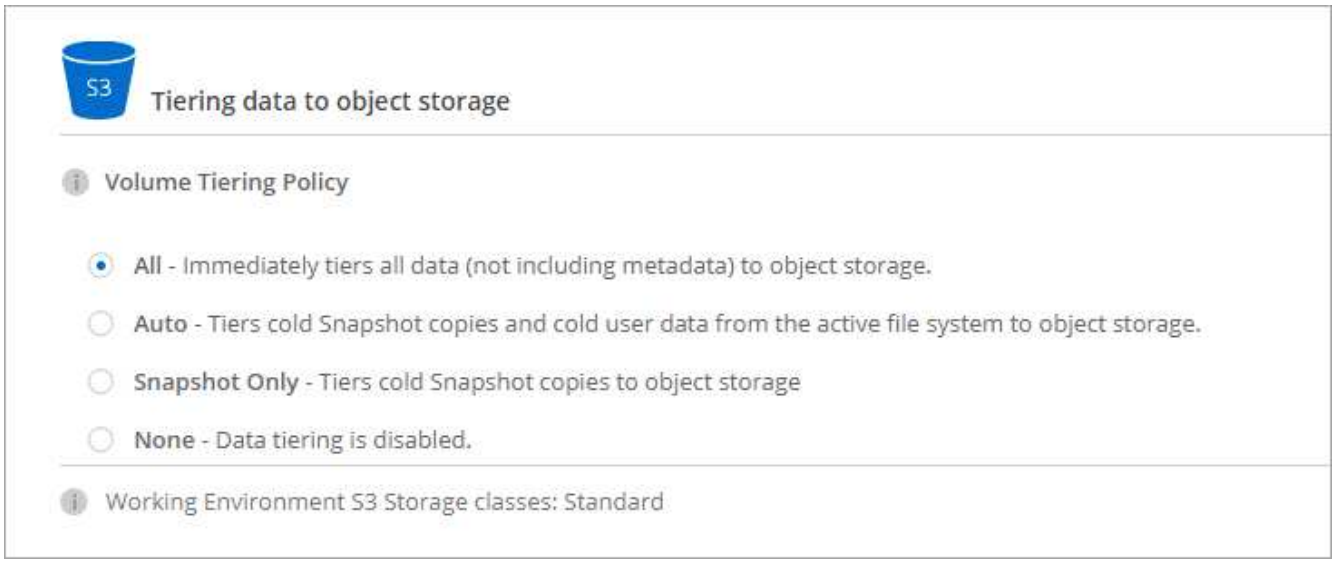
1. Erstellen Sie in der Arbeitsumgebung ein neues Volume, oder ändern Sie den Tier eines vorhandenen Volumes:

Aufgabe	Aktion
Erstellen Sie ein neues Volume	Klicken Sie Auf **Neues Volume Hinzufügen**.
Ändern Sie ein vorhandenes Volume	Wählen Sie das Volume aus und klicken Sie auf **Disk Type & Tiering Policy**.

2. Wählen Sie eine Tiering-Richtlinie aus.

   Eine Beschreibung dieser Richtlinien finden Sie unter "Data Tiering - Übersicht".

   Beispiel



Cloud Manager erstellt ein neues Aggregat für das Volume, wenn noch kein Daten Tiering-aktiviertes Aggregat vorhanden ist.

Wenn Sie Aggregate selbst erstellen möchten, können Sie beim Erstellen von Aggregaten das Daten-Tiering aktivieren.

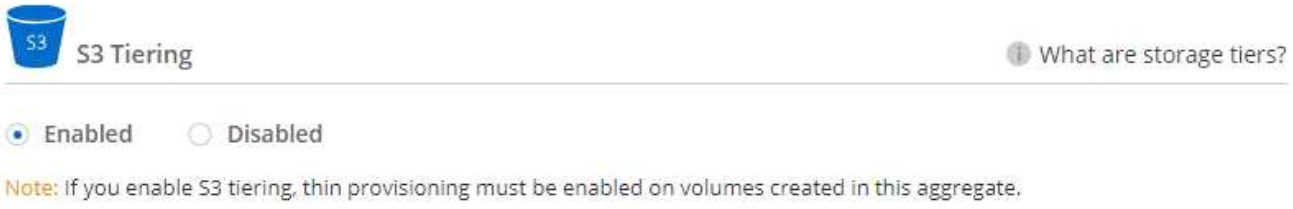
Tiering von Daten aus Datensicherungs-Volumes

Cloud Volumes ONTAP kann Daten von einem Daten-Protection-Volume auf eine Kapazitäts-Tier einstufen. Wenn Sie das Ziel-Volume aktivieren, werden die Daten beim Lesen schrittweise auf die Performance-Ebene verschoben.

Schritte

1. Wählen Sie auf der Seite Arbeitsumgebungen die Arbeitsumgebung aus, die das Quell-Volume enthält, und ziehen Sie es in die Arbeitsumgebung, in die Sie das Volume replizieren möchten.
2. Folgen Sie den Anweisungen, bis Sie die Seite Tiering aufrufen und Data Tiering für Objektspeicher aktivieren.

Beispiel



Unterstützung bei der Datenreplizierung finden Sie unter "Replizierung von Daten in die und aus der Cloud".

Änderung der Storage-Klasse für Tiered Daten

Nachdem Sie Cloud Volumes ONTAP implementiert haben, können Sie Ihre Storage-Kosten senken, indem Sie die Storage-Klasse für inaktive Daten ändern, auf die seit 30 Tagen nicht mehr zugegriffen wurde. Die

Zugriffskosten sind höher, wenn der Zugriff auf die Daten erfolgt. Berücksichtigen Sie diese also vor einem Wechsel der Storage-Klasse.

Die Storage-Klasse für Tiered Daten beträgt im gesamten System – nicht It pro Volume.

Informationen zu unterstützten Speicherklassen finden Sie unter "Data Tiering - Übersicht".

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Speicherklassen** oder **Blob Storage Tiering**.
2. Wählen Sie eine Speicherklasse aus und klicken Sie dann auf **Speichern**.

Kann ich Daten-Tiering auf einem vorhandenen Aggregat aktivieren?

Nein, Sie können das Daten-Tiering nicht auf einem vorhandenen Aggregat aktivieren. Sie können Daten-Tiering nur auf neuen Aggregaten aktivieren.

Sie können auch Daten-Tiering auf einem neuen Aggregat aktivieren "Indem Sie ein Aggregat selbst erstellen" Oder Indem ein neues Volume mit aktiviertem Daten-Tiering erstellt wird. Cloud Manager würde dann ein neues Aggregat für das Volume erstellen, wenn es bereits ein Daten-Tiering-fähiges Aggregat gibt.

Managen von Storage-VMs

Eine Storage VM ist eine Virtual Machine, die in ONTAP ausgeführt wird und Ihren Kunden Storage und Datenservices zur Verfügung stellt. Vielleicht wissen Sie das als *SVM* oder *vServer*. Cloud Volumes ONTAP ist standardmäßig mit einer Storage-VM konfiguriert, aber einige Konfigurationen unterstützen zusätzliche Storage-VMs.

Unterstützte Anzahl von Storage-VMs

Cloud Volumes ONTAP 9.7 unterstützt mehrere Storage-VMs in AWS mit bestimmten Konfigurationen und einer Add-on-Lizenz. "Anzeige der Anzahl der unterstützten Storage-VMs in AWS". Wenden Sie sich an Ihr Account-Team, um eine SVM-Add-on-Lizenz zu erhalten.

Alle anderen Cloud Volumes ONTAP Konfigurationen unterstützen eine Storage-VM mit Datenbereitstellung und eine Ziel-Storage-VM für die Disaster Recovery. Sie können die Ziel-Storage-VM für den Datenzugriff aktivieren, wenn es einen Ausfall auf der Quell-Storage-VM gibt.

Eine Storage-VM umfasst das gesamte Cloud Volumes ONTAP System (HA-Paar oder Single Node).

Erstellen von zusätzlichen Storage-VMs

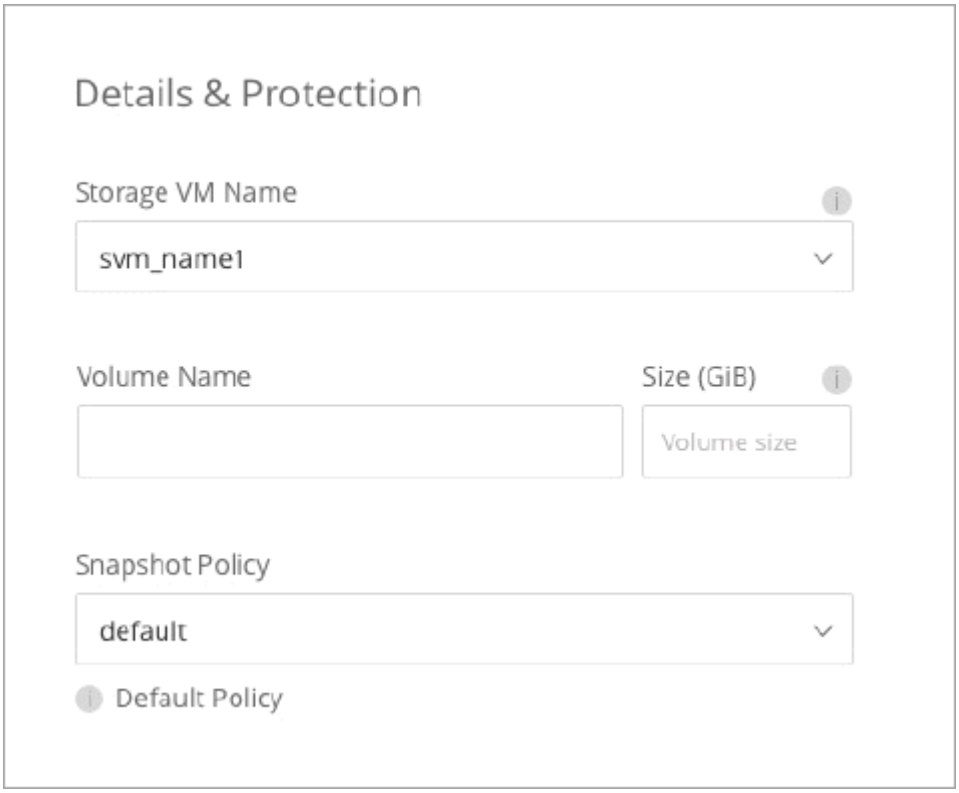
Wenn diese von Ihrer Konfiguration unterstützt werden, können Sie mit zusätzliche Storage-VMs erstellen "System Manager oder die CLI".

- "Erstellen einer SVM für SMB-Zugriff"
- "Erstellen einer SVM für NFS-Zugriff"
- "Erstellen einer SVM für iSCSI-Zugriff"
- "Erstellung einer Ziel-SVM für Disaster Recovery"

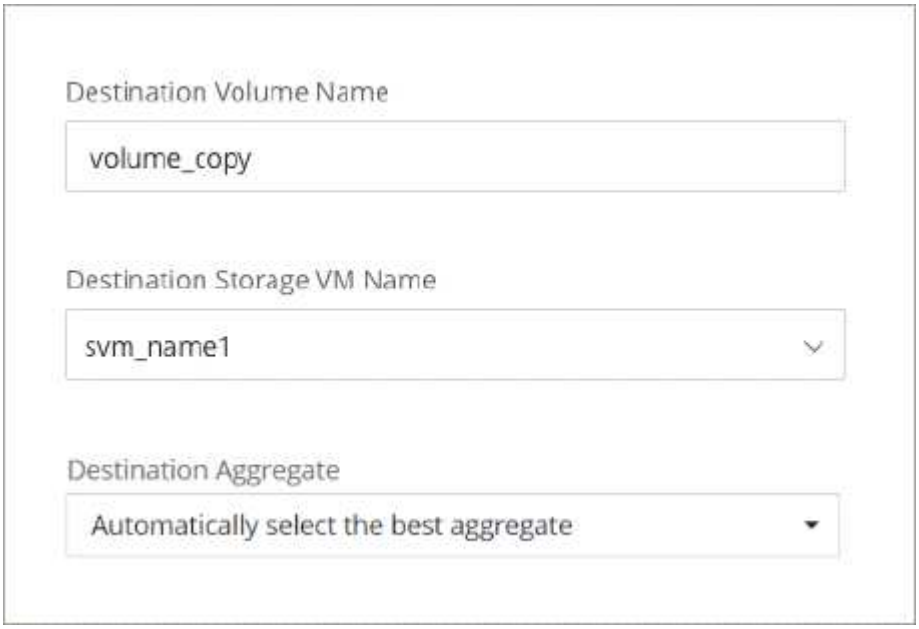
Arbeiten mit mehreren Storage VMs in Cloud Manager

Cloud Manager unterstützt alle zusätzlichen Storage-VMs, die Sie über System Manager oder die CLI erstellen.

Das folgende Bild zeigt beispielsweise, wie Sie beim Erstellen eines Volumes eine Storage-VM auswählen können.



Das folgende Bild zeigt, wie Sie bei der Replizierung eines Volumes in ein anderes System eine Storage VM auswählen können.



Management der Disaster Recovery für Storage VMs

Cloud Manager bietet keine Unterstützung für die Einrichtung oder Orchestrierung von Storage VM Disaster Recovery. Sie müssen System Manager oder die CLI verwenden.

- "Express Guide zur Vorbereitung des SVM-Disaster Recovery"
- "SVM Disaster Recovery Express Guide"

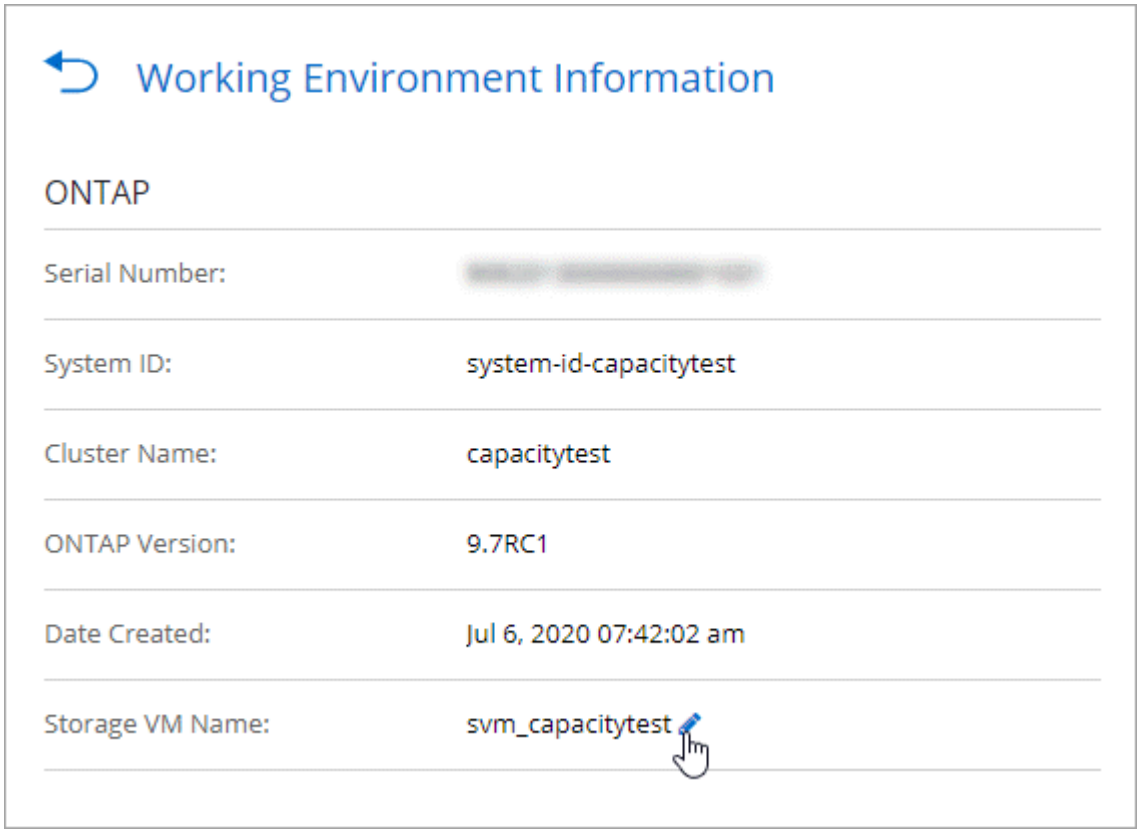
Ändern des Namens der Storage-VM

Cloud Manager benennt automatisch die einzelne Storage-VM, die sie für Cloud Volumes ONTAP erstellt. Sie können den Namen der Storage VM ändern, wenn Sie strenge Namensstandards haben. Beispielsweise möchte der Name Ihnen entsprechen, wie Sie die Storage-VMs für Ihre ONTAP Cluster benennen.

Wenn Sie zusätzliche Storage VMs für Cloud Volumes ONTAP erstellt haben, können Sie die Storage-VMs nicht aus Cloud Manager umbenennen. Sie müssen dies direkt von Cloud Volumes ONTAP mit System Manager oder der CLI ausführen.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Information**.
2. Klicken Sie rechts neben dem Namen der Storage-VM auf das Bearbeiten-Symbol.



3. Ändern Sie im Dialogfeld SVM-Name ändern den Namen und klicken Sie dann auf **Speichern**.

Verwendung von Cloud Volumes ONTAP als persistenter Storage für Kubernetes

Cloud Manager kann die Implementierung von NetApp Trident auf Kubernetes-Clustern automatisieren, sodass Sie Cloud Volumes ONTAP als persistenten Storage für

Container verwenden können.

Trident ist ein vollständig von NetApp unterstütztes Open-Source-Projekt. Trident lässt sich nativ mit Kubernetes und dessen Persistent Volume Framework integrieren und ermöglicht das nahtlose Bereitstellen und Managen von Volumes auf Systemen, die auf beliebigen Kombinationen von NetApp Storage-Plattformen ausgeführt werden. "Weitere Informationen zu Trident".

Die Kubernetes-Funktion wird nicht durch lokale ONTAP-Cluster unterstützt. Es wird nur mit Cloud Volumes ONTAP unterstützt.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

Voraussetzungen prüfen

Stellen Sie sicher, dass Ihre Umgebung die Voraussetzungen erfüllt, einschließlich Konnektivität zwischen Kubernetes-Clustern und Cloud Volumes ONTAP, Konnektivität zwischen Kubernetes-Clustern und einem Connector, mindestens Kubernetes-Version von 1.14, mindestens einen Worker-Node in einem Cluster und mehr. Eine vollständige Liste finden Sie hier.

Fügen Sie Ihre Kubernetes Cluster zu Cloud Manager hinzu

Klicken Sie in Cloud Manager auf **Kubernetes**, um Cluster direkt aus dem Managed Service Ihres Cloud-Providers zu ermitteln, oder importieren Sie einen Cluster, indem Sie eine kubeconfig-Datei bereitstellen.

Verbinden Sie die Cluster mit Cloud Volumes ONTAP

Klicken Sie nach dem Hinzufügen eines Kubernetes-Clusters auf **Verbinden mit der Arbeitsumgebung**, um den Cluster mit einem oder mehreren Cloud Volumes ONTAP-Systemen zu verbinden.

Starten Sie die Bereitstellung persistenter Volumes

Persistente Volumes können über native Kubernetes-Schnittstellen und -Konstrukte angefordert und gemanagt werden. Cloud Manager erstellt NFS- und iSCSI-Storage-Klassen, die bei der Bereitstellung persistenter Volumes genutzt werden können.

"Erfahren Sie mehr über die Bereitstellung Ihres ersten Volumes mit Trident für Kubernetes".

Voraussetzungen prüfen

Bevor Sie beginnen, stellen Sie sicher, dass die Kubernetes-Cluster und der Connector bestimmte Anforderungen erfüllen.

Kubernetes-Cluster-Anforderungen

- Zwischen einem Kubernetes Cluster und dem Connector sowie zwischen einem Kubernetes Cluster und Cloud Volumes ONTAP ist eine Netzwerkverbindung erforderlich.

  Sowohl der Connector als auch der Cloud Volumes ONTAP benötigen eine Verbindung zum Kubernetes API Endpunkt:

  - Legen Sie für gemanagte Cluster eine Route zwischen der VPC eines Clusters und der VPC fest, an der sich der Connector und die Cloud Volumes ONTAP befinden.
  - Bei anderen Clustern muss die IP-Adresse des Hauptknotens oder des Load Balancer (wie in der kubeconfig-Datei angegeben) über den Connector und den Cloud Volumes ONTAP erreichbar sein, und es muss ein gültiges TLS-Zertifikat vorhanden sein.
- Ein Kubernetes-Cluster kann sich an jedem Ort befinden, an dem die oben aufgeführte Netzwerkverbindung vorhanden ist.
- Ein Kubernetes Cluster muss mindestens Version 1.14 ausführen.

  Die Version mit der maximalen Anzahl wird von Trident definiert. "Klicken Sie hier, um die maximal unterstützte Kubernetes-Version anzuzeigen".
- Ein Kubernetes-Cluster muss mindestens einen Worker-Node aufweisen.
- Für Cluster, die im Amazon Elastic Kubernetes Service (Amazon EKS) ausgeführt werden, benötigt jedes Cluster eine IAM-Rolle, um einen Berechtigungsfehler zu beheben. Nachdem Sie das Cluster hinzugefügt haben, werden Sie von Cloud Manager mit dem exact eksctl-Befehl aufgefordert, der den Fehler auflöst.

  "Erfahren Sie mehr über die Grenzen der IAM-Berechtigungen".
- Für Cluster, die im Azure Kubernetes Service (AKS) ausgeführt werden, müssen diesen Clustern die Rolle „*Azure Kubernetes Service RBAC für Cluster Admin*“ zugewiesen werden. Dies ist nötig, damit Cloud Manager Trident installieren und Storage-Klassen auf dem Cluster konfigurieren kann.
- Bei Clustern, die in der Google Kubernetes Engine (GKE) ausgeführt werden, dürfen diese Cluster nicht das standardmäßige für Container optimierte Betriebssystem verwenden. Sie sollten sie wechseln, um Ubuntu zu verwenden.

  GKE verwendet standardmäßig Google "Für Container optimiertes Image", Welches nicht über die Dienstprogramme verfügt, die Trident zum Mounten von Volumes benötigt.

Anforderungen an Steckverbinder

Stellen Sie sicher, dass die folgenden Netzwerk- und Berechtigungen für den Connector vorhanden sind.

Netzwerkbetrieb

- Für die Installation von Trident ist eine ausgehende Internetverbindung erforderlich, um auf die folgenden Endpunkte zuzugreifen:

  https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/

  Cloud Manager installiert Trident auf einem Kubernetes-Cluster, wenn Sie eine Arbeitsumgebung mit dem Cluster verbinden.

Erforderliche Berechtigungen zum ermitteln und Verwalten von EKS-Clustern

Für die Erkennung und das Management von Kubernetes-Clustern in Amazon Elastic Kubernetes Service (EKS) benötigt der Connector Administratorberechtigungen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "eks:*",
            "Resource": "*"
        }
    ]
}
```

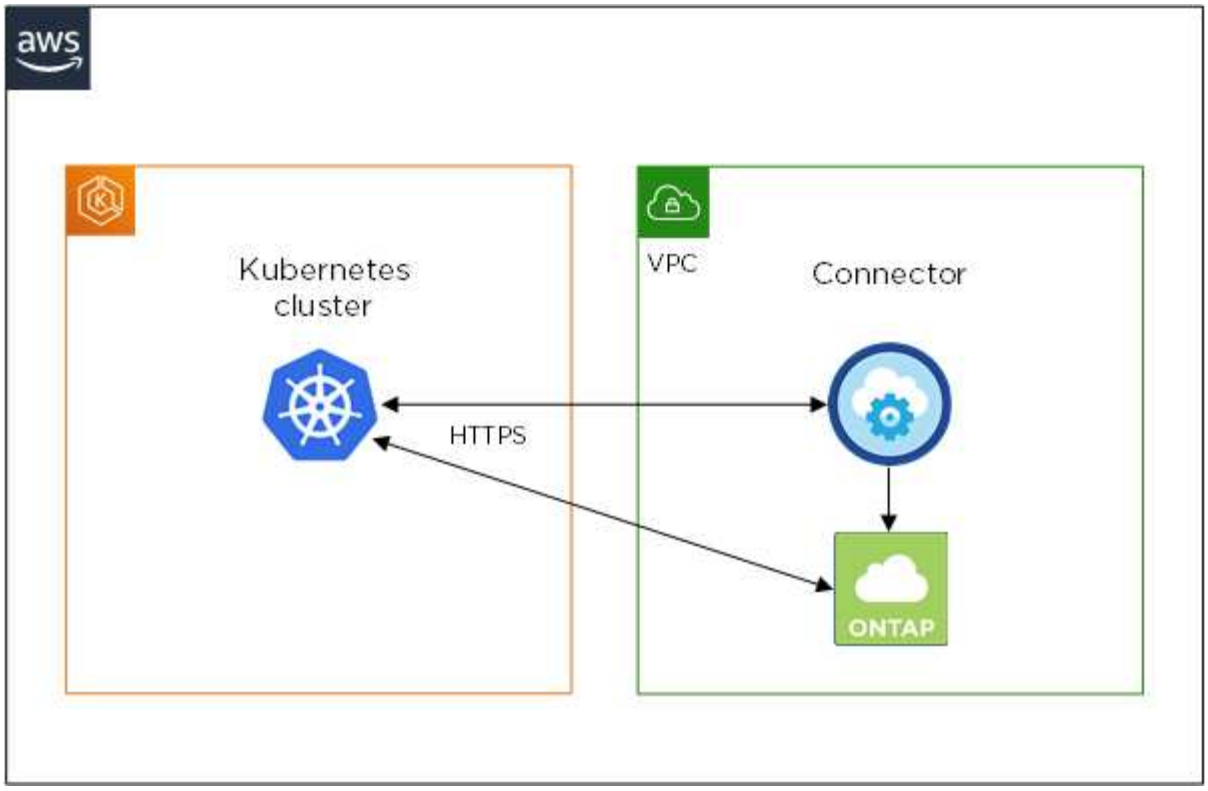
Erforderliche Berechtigungen zum ermitteln und Verwalten von GKE-Clustern

Für die Erkennung und das Management von Kubernetes-Clustern in der Google Kubernetes Engine (GKE) benötigt der Connector folgende Berechtigungen:

```
container.*
```

Beispiel für die Einrichtung

Das folgende Bild zeigt ein Beispiel für einen Kubernetes-Cluster mit Amazon Elastic Kubernetes Service (Amazon EKS) und dessen Verbindungen zum Connector und Cloud Volumes ONTAP.



Hinzufügen von Kubernetes Clustern

Fügen Sie Kubernetes-Cluster zu Cloud Manager hinzu, indem Sie die Cluster ermitteln, die im Managed Kubernetes Service des Cloud-Providers ausgeführt werden, oder indem Sie die kubeconfig-Datei eines Clusters importieren.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Kubernetes**.
2. Klicken Sie Auf **Cluster Hinzufügen**.
3. Wählen Sie eine der folgenden Optionen:
   - Klicken Sie auf **Cluster ermitteln**, um die verwalteten Cluster zu ermitteln, auf die Cloud Manager Zugriff hat, basierend auf den Berechtigungen, die Sie dem Connector bereitgestellt haben.

     Wenn Ihr Connector beispielsweise in Google Cloud ausgeführt wird, verwendet Cloud Manager die Berechtigungen aus dem Dienstkonto des Connectors, um Cluster zu ermitteln, die in der Google Kubernetes Engine (GKE) ausgeführt werden.

   - Klicken Sie auf **Cluster importieren**, um einen Cluster mit einer kubeconfig-Datei zu importieren.

     Nach dem Hochladen der Datei überprüft Cloud Manager die Verbindung zum Cluster und speichert eine verschlüsselte Kopie der kubeconfig-Datei.

Ergebnis

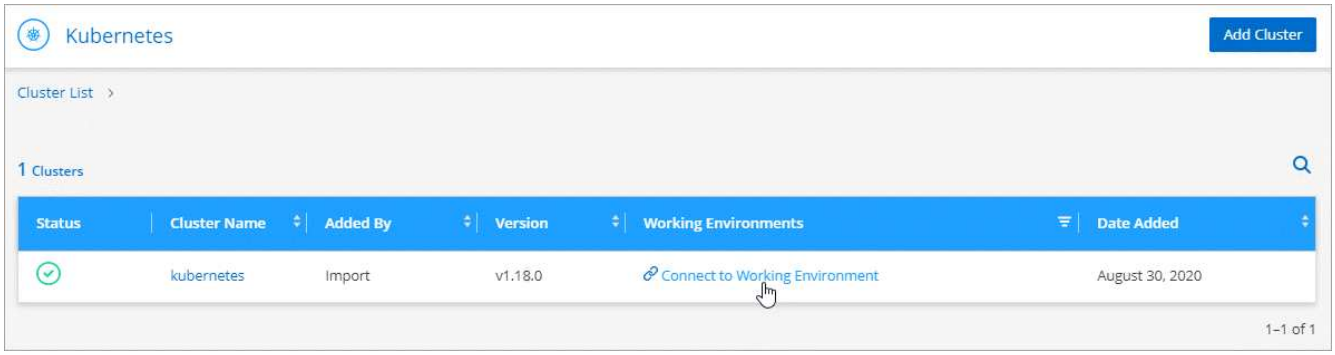
Cloud Manager fügt den Kubernetes-Cluster hinzu. Sie können das Cluster jetzt mit Cloud Volumes ONTAP verbinden.

Verbinden eines Clusters mit Cloud Volumes ONTAP

Verbinden Sie ein Kubernetes Cluster mit Cloud Volumes ONTAP, damit Sie Cloud Volumes ONTAP als persistenten Storage für Container verwenden können.

Schritte

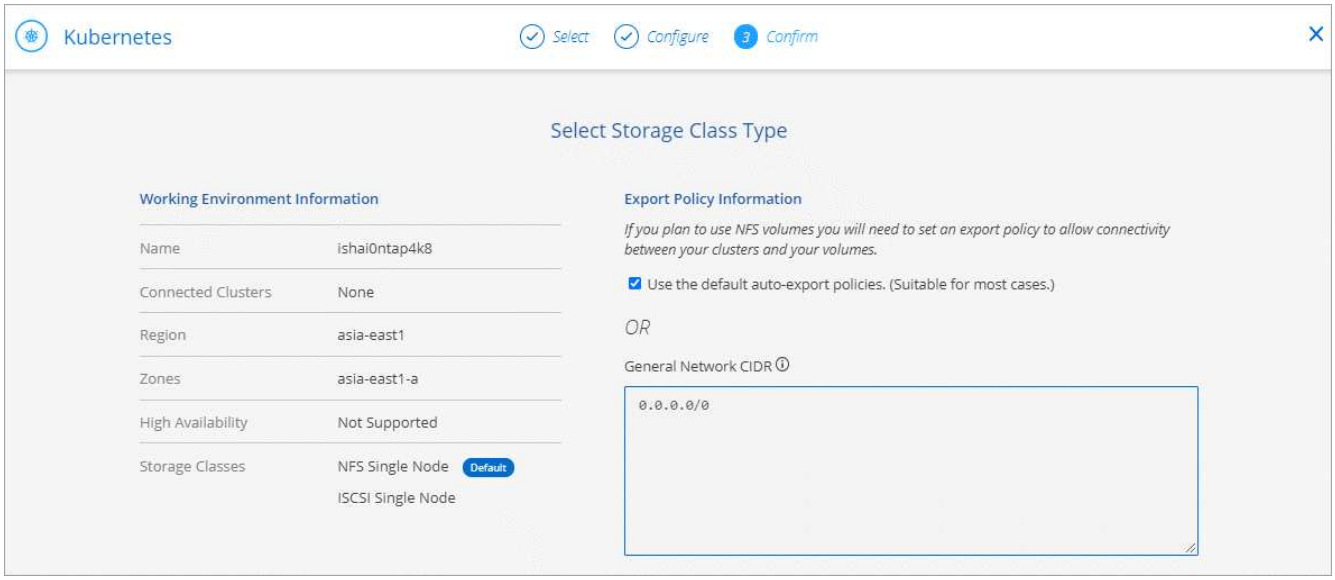
1. Klicken Sie oben im Cloud Manager auf **Kubernetes**.
2. Klicken Sie für den Cluster, den Sie gerade hinzugefügt haben, auf **mit der Arbeitsumgebung verbinden**.



3. Wählen Sie eine Arbeitsumgebung aus und klicken Sie auf **Weiter**.
4. Wählen Sie die NetApp Storage-Klasse als Standard-Storage-Klasse für den Kubernetes Cluster und klicken Sie auf **Weiter**.

   Wenn ein Benutzer ein persistentes Volume erstellt, kann der Kubernetes-Cluster diese Storage-Klasse standardmäßig als Back-End-Storage verwenden.

5. Wählen Sie, ob Sie die Standard-Richtlinien für den automatischen Export verwenden oder einen benutzerdefinierten CIDR-Block hinzufügen möchten.



6. Klicken Sie Auf **Arbeitsumgebung Hinzufügen**.

Ergebnis

Cloud Manager verbindet die Arbeitsumgebung mit dem Cluster, was bis zu 15 Minuten dauert.

Verwalten von Clustern

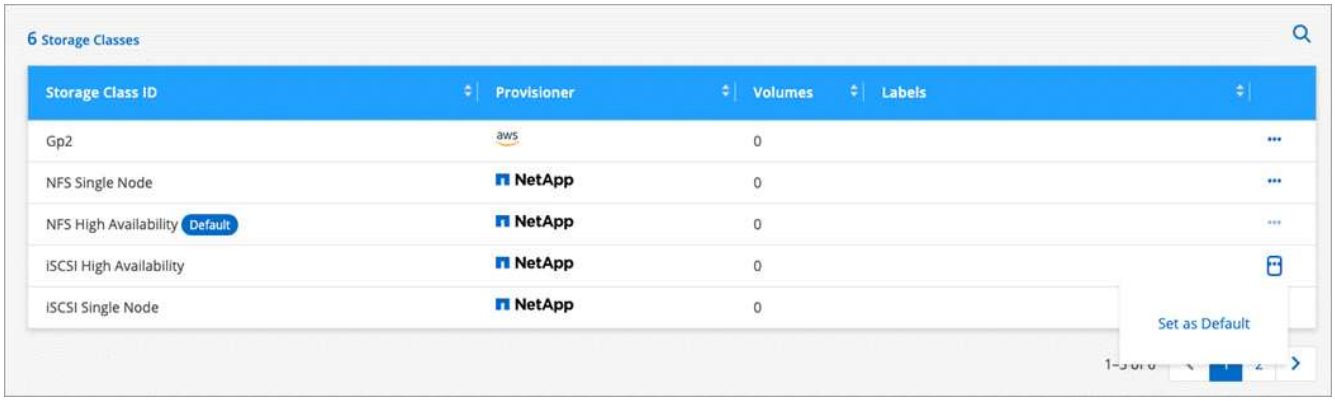
Mit Cloud Manager können Sie Ihre Kubernetes-Cluster managen, indem Sie die Standard-Storage-Klasse ändern, Trident aktualisieren und vieles mehr.

Ändern der Standard-Storage-Klasse

Stellen Sie sicher, dass Sie eine Cloud Volumes ONTAP Storage-Klasse als Standard-Storage-Klasse eingestellt haben, sodass Cluster Cloud Volumes ONTAP als Back-End Storage verwenden.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Kubernetes**.
2. Klicken Sie auf den Namen des Kubernetes-Clusters.
3. Klicken Sie in der Tabelle **Speicherklassen** ganz rechts auf das Menü Aktionen für die Speicherklasse, die Sie als Standard festlegen möchten.



4. Klicken Sie auf **als Standard festlegen**.

Upgrade Von Trident

Sie können Trident von Cloud Manager aktualisieren, wenn eine neue Version von Trident verfügbar ist.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Kubernetes**.
2. Klicken Sie auf den Namen des Kubernetes-Clusters.
3. Wenn eine neue Version verfügbar ist, klicken Sie neben der Trident-Version auf **Upgrade**.

Die kubeconfig-Datei wird aktualisiert

Wenn Sie den Cluster zum Cloud Manager hinzugefügt haben, indem Sie die kubeconfig-Datei importieren, können Sie die neueste kubeconfig-Datei jederzeit in Cloud Manager hochladen. Dies ist möglich, wenn Sie die Anmeldeinformationen aktualisiert haben, Benutzer oder Rollen geändert haben oder wenn sich etwas

geändert hat, das das Cluster, Benutzer, Namespaces oder die Authentifizierung betrifft.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Kubernetes**.
2. Klicken Sie auf den Namen des Kubernetes-Clusters.
3. Klicken Sie Auf **Kubeconfeigent Aktualisieren**.
4. Wenn Sie durch Ihren Webbrowser aufgefordert werden, wählen Sie die aktualisierte kubeconfg-Datei aus und klicken Sie auf **Öffnen**.

Ergebnis

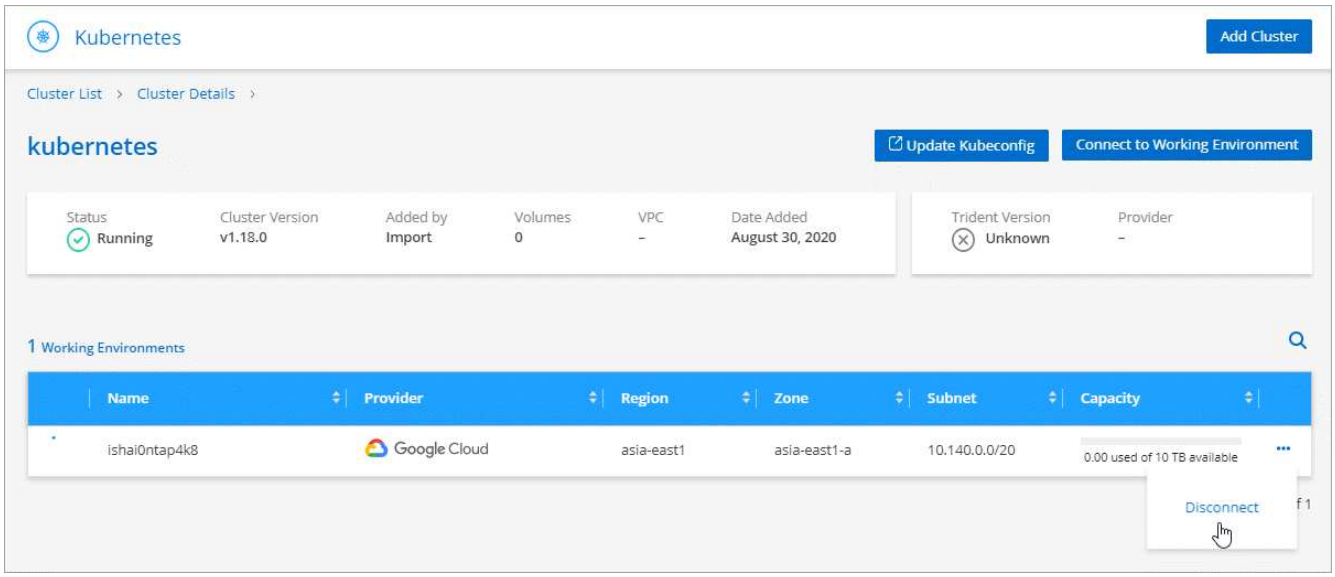
Cloud Manager aktualisiert die Informationen zum Kubernetes-Cluster auf der Grundlage der neuesten kubeconfig Datei.

Trennen eines Clusters

Wenn Sie ein Cluster von Cloud Volumes ONTAP trennen, können Sie dieses Cloud Volumes ONTAP System nicht mehr als persistenten Storage für Container verwenden. Vorhandene persistente Volumes werden nicht gelöscht.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Kubernetes**.
2. Klicken Sie auf den Namen des Kubernetes-Clusters.
3. Klicken Sie in der Tabelle **Arbeitsumgebungen** auf das Menü Aktionen ganz rechts für die Arbeitsumgebung, die Sie trennen möchten.



4. Klicken Sie Auf **Trennen**.

Ergebnis

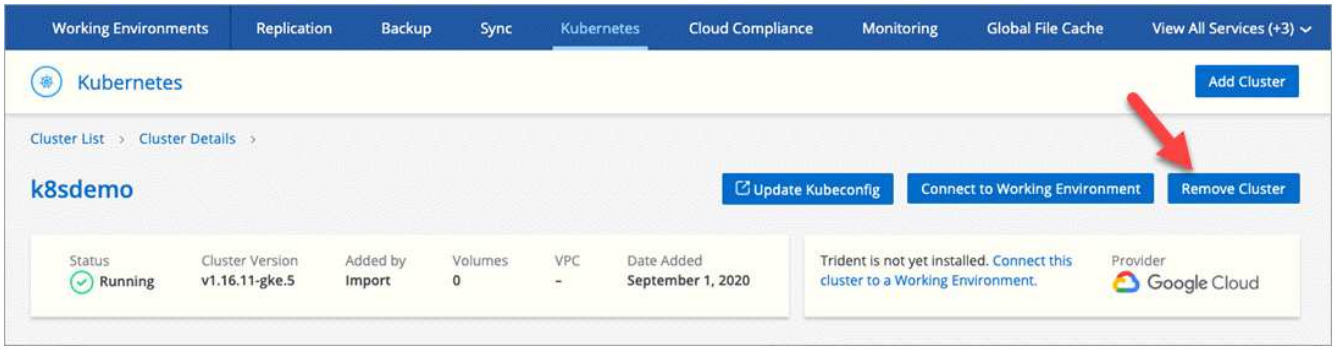
Cloud Manager trennt die Verbindung des Clusters vom Cloud Volumes ONTAP System.

Entfernen eines Clusters

Entfernen Sie stillgelegte Cluster aus dem Cloud Manager, nachdem Sie alle Arbeitsumgebungen vom Cluster getrennt haben.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Kubernetes**.
2. Klicken Sie auf den Namen des Kubernetes-Clusters.
3. Klicken Sie Auf **Cluster Entfernen**.



Verschlüsseln von Volumes mit NetApp Verschlüsselungslösungen

Cloud Volumes ONTAP unterstützt sowohl NetApp Volume Encryption (NVE) als auch NetApp Aggregate Encryption (NAE) mit einem externen Schlüsselmanager. NVE und NAE sind softwarebasierte Lösungen, mit denen die Verschlüsselung von Volumes im Ruhezustand (FIPS) 140-2-konform unterstützt wird. "Weitere Informationen zu diesen Verschlüsselungslösungen".

Ab Cloud Volumes ONTAP 9.7 werden neue Aggregate standardmäßig NAE aktiviert haben, nachdem Sie einen externen Schlüsselmanager eingerichtet haben. Für neue Volumes, die nicht Teil eines NAE-Aggregats sind, ist NVE standardmäßig aktiviert (bei vorhandenen Aggregaten, die vor dem Einrichten eines externen Schlüsselmanagers erstellt wurden).

Cloud Volumes ONTAP unterstützt kein Onboard-Verschlüsselungsmanagement.

Was Sie benötigen

Ihr Cloud Volumes ONTAP System sollte beim NetApp Support registriert sein. Ab Cloud Manager 3.7 wird auf jedem Cloud Volumes ONTAP System, das beim NetApp Support registriert ist, automatisch eine NetApp Volume Encryption Lizenz installiert.

- "Hinzufügen von NetApp Support Site Konten zu Cloud Manager"
- "Registrieren von Pay-as-you-go-Systemen"

Cloud Manager installiert die NVE-Lizenz nicht auf Systemen, die sich in der Region China befinden.

Schritte

1. Überprüfen Sie die Liste der unterstützten Schlüsselmanager im "NetApp Interoperabilitäts-Matrix-Tool".

   Suchen Sie nach der **Key Manager**-Lösung.

2. "Stellen Sie eine Verbindung zur Cloud Volumes ONTAP-CLI her".
3. Installieren Sie SSL-Zertifikate und stellen Sie eine Verbindung zu den externen

Schlüsselverwaltungsservern her.

"ONTAP 9 NetApp Verschlüsselungs-Leitfaden: Konfiguration externer Verschlüsselungsmanagement"

Replizierung von Daten zwischen Systemen

Sie können Daten zwischen Arbeitsumgebungen replizieren, indem Sie eine einmalige Datenreplizierung für die Datenübertragung oder einen wiederkehrenden Zeitplan für Disaster Recovery oder langfristige Aufbewahrung wählen. Sie können beispielsweise die Datenreplizierung eines lokalen ONTAP-Systems auf Cloud Volumes ONTAP für Disaster Recovery einrichten.

Cloud Manager vereinfacht die Datenreplizierung zwischen Volumes auf separaten Systemen mithilfe von SnapMirror und SnapVault Technologien. Sie müssen lediglich das Quell-Volume und das Ziel-Volume identifizieren und dann eine Replizierungsrichtlinie und einen Zeitplan auswählen. Cloud Manager erwirbt die erforderlichen Festplatten, konfiguriert Beziehungen, wendet die Replizierungsrichtlinie an und initiiert dann den Basistransfer zwischen Volumes.

Die Basisplanübertragung enthält eine vollständige Kopie der Quelldaten. Nachfolgende Übertragungen enthalten differenzielle Kopien der Quelldaten.

Cloud Manager ermöglicht Datenreplizierung zwischen den folgenden Arbeitsumgebungen:

- Von einem Cloud Volumes ONTAP System zu einem anderen Cloud Volumes ONTAP System
- Zwischen einem Cloud Volumes ONTAP System und einem ONTAP-Cluster vor Ort
- Von einem ONTAP-Cluster vor Ort zu einem anderen ONTAP-Cluster vor Ort

Anforderungen an die Datenreplizierung

Bevor Sie Daten replizieren können, sollten Sie sicherstellen, dass sowohl für Cloud Volumes ONTAP Systeme als auch für ONTAP Cluster spezifische Anforderungen erfüllt sind.

Versionsanforderungen

Sie sollten überprüfen, ob die Quell- und Ziel-Volumes kompatible ONTAP Versionen ausführen, bevor Sie Daten replizieren. Weitere Informationen finden Sie im "Data Protection Power Guide".

Spezifische Anforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen ein- und ausgehenden Regeln enthalten: Speziell Regeln für ICMP und die Ports 11104 und 11105.

  Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.

- Um Daten zwischen zwei Cloud Volumes ONTAP Systemen in verschiedenen Subnetzen zu replizieren, müssen die Subnetze gemeinsam geroutet werden (dies ist die Standardeinstellung).
- Um Daten zwischen einem Cloud Volumes ONTAP System in AWS und einem System in Azure zu replizieren, müssen Sie über eine VPN-Verbindung zwischen AWS VPC und Azure VNet verfügen.

Spezifische Anforderungen für ONTAP Cluster

- Eine aktive SnapMirror Lizenz muss installiert sein.

- Wenn sich das Cluster in Ihrem Betrieb befindet, sollten Sie eine Verbindung von Ihrem Unternehmensnetzwerk zu AWS oder Azure haben, bei der es sich in der Regel um eine VPN-Verbindung handelt.
- ONTAP Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Cluster-Anforderungen erfüllen.

  Weitere Informationen finden Sie im Cluster and SVM Peering Express Guide für Ihre Version von ONTAP.

Datenreplikation zwischen Systemen einrichten

Sie können Daten zwischen Cloud Volumes ONTAP Systemen und ONTAP Clustern replizieren, indem Sie sich für eine einmalige Datenreplizierung entscheiden, mit der Sie Daten in die und aus der Cloud verschieben können, oder für einen wiederkehrenden Zeitplan, der zur Disaster Recovery oder langfristigen Aufbewahrung beitragen kann.

Über diese Aufgabe

Cloud Manager unterstützt einfache, fanout- und kaskadierende Datensicherungskonfigurationen:

- In einer einfachen Konfiguration erfolgt die Replizierung von Volume A auf Volume B.
- In einer Fanout-Konfiguration erfolgt die Replizierung von Volume A zu mehreren Zielen.
- Bei einer kaskadierten Konfiguration erfolgt die Replizierung von Volume A auf Volume B und von Volume B auf Volume C.

Sie können Fanout- und Kaskadenkonfigurationen in Cloud Manager konfigurieren, indem Sie mehrere Datenreplizierungen zwischen Systemen einrichten. Zum Beispiel durch Replizierung eines Volumes von System A auf System B und anschließendes Replizieren desselben Volumes von System B auf System C.

Schritte

1. Wählen Sie auf der Seite Arbeitsumgebungen die Arbeitsumgebung aus, die das Quell-Volume enthält, und ziehen Sie es in die Arbeitsumgebung, in die Sie das Volume replizieren möchten:

2. Wenn die Setup-Seiten für Quell- und Zielpeering angezeigt werden, wählen Sie alle Intercluster-LIFs für die Cluster-Peer-Beziehung aus.

   Das Cluster-übergreifende Netzwerk sollte so konfiguriert werden, dass Cluster-Peers *paarweise vollständige Mesh-Konnektivität* haben. Das bedeutet, dass jedes Cluster-Paar in einer Cluster-Peer-Beziehung über Konnektivität zwischen allen Intercluster LIFs verfügt.

   Diese Seiten werden angezeigt, wenn ein ONTAP Cluster mit mehreren LIFs Quelle oder Ziel ist.

3. Wählen Sie auf der Seite Quellvolumenauswahl das Volume aus, das Sie replizieren möchten.

4. Geben Sie auf der Seite Name und Tiering des Zieldatenträgers den Namen des Zieldatenträgers an, wählen Sie einen zugrunde liegenden Laufwerkstyp aus, ändern Sie eine der erweiterten Optionen, und klicken Sie dann auf **Weiter**.

   Wenn das Ziel ein ONTAP Cluster ist, müssen Sie auch das Ziel-SVM und das Aggregat angeben.

5. Geben Sie auf der Seite Max. Übertragungsrate die maximale Rate (in Megabyte pro Sekunde) an, mit der Daten übertragen werden können.
6. Wählen Sie auf der Seite Replikationsrichtlinie eine der Standardrichtlinien aus, oder klicken Sie auf **zusätzliche Richtlinien**, und wählen Sie dann eine der erweiterten Richtlinien aus.

   Hilfe finden Sie unter "Auswählen einer Replizierungsrichtlinie".

   Wenn Sie eine benutzerdefinierte Backup- (SnapVault-) Policy wählen, müssen die mit der Policy verknüpften Labels mit den Labels der Snapshot Kopien auf dem Quell-Volume übereinstimmen. Weitere Informationen finden Sie unter "Funktionsweise von Backup-Richtlinien".

7. Wählen Sie auf der Seite Zeitplan eine einmalige Kopie oder einen wiederkehrenden Zeitplan aus.

   Es stehen mehrere Standardzeitpläne zur Verfügung. Wenn Sie einen anderen Zeitplan möchten, müssen Sie mithilfe von System Manager einen neuen Zeitplan auf dem Cluster *Destination* erstellen.

8. Überprüfen Sie auf der Seite „Prüfen“ Ihre Auswahl und klicken Sie dann auf **Los**.

Ergebnis

Cloud Manager startet den Datenreplizierungsprozess. Details zur Replikation können Sie auf der Seite "Replication Status" anzeigen.

Managen von Plänen und Beziehungen zur Datenreplizierung

Nachdem Sie die Datenreplizierung zwischen zwei Systemen eingerichtet haben, können Sie den Zeitplan und die Beziehung für die Datenreplizierung über Cloud Manager managen.

Schritte

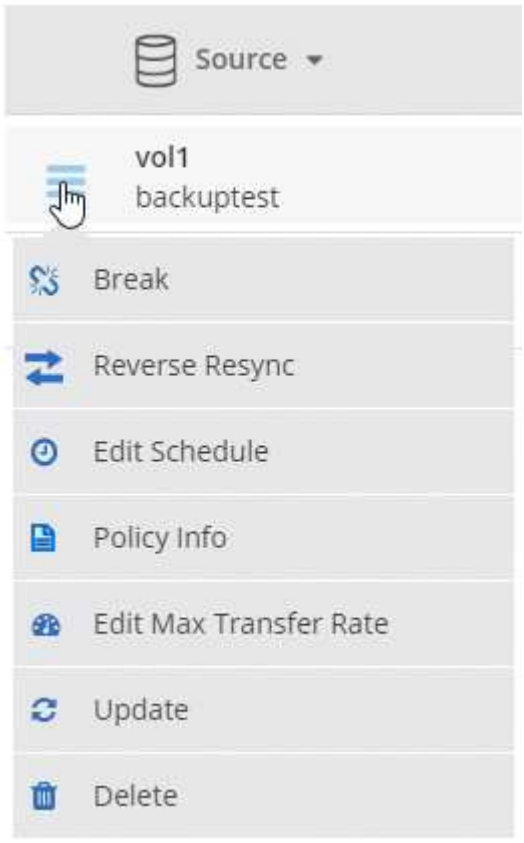
1. Zeigen Sie auf der Seite Arbeitsumgebungen den Replikationsstatus für alle Arbeitsumgebungen im Arbeitsbereich oder für eine bestimmte Arbeitsumgebung an:

Option	Aktion
Alle Arbeitsumgebungen im Arbeitsbereich	Klicken Sie oben im Cloud Manager auf **Replikation**.
Eine bestimmte Arbeitsumgebung	Öffnen Sie die Arbeitsumgebung und klicken Sie auf **Replikationen**.

2. Überprüfen Sie den Status der Datenreplizierungsbeziehungen, um sicherzustellen, dass sie in Ordnung sind.

Wenn der Status einer Beziehung inaktiv ist und der Spiegelungsstatus nicht initialisiert ist, müssen Sie die Beziehung vom Zielsystem initialisieren, damit die Datenreplizierung gemäß dem definierten Zeitplan ausgeführt werden kann. Sie können die Beziehung mit System Manager oder der Befehlszeilenschnittstelle (CLI) initialisieren. Diese Zustände können angezeigt werden, wenn das Zielsystem ausfällt und dann wieder online geht.

3. Wählen Sie das Menüsymbol neben dem Quellvolume und anschließend eine der verfügbaren Aktionen aus.



Die folgende Tabelle beschreibt die verfügbaren Aktionen:

Aktion	Beschreibung
Pause	Bricht die Beziehung zwischen Quell- und Ziel-Volumes und aktiviert das Ziel-Volume für den Datenzugriff. Diese Option wird in der Regel verwendet, wenn das Quell-Volume aufgrund von Ereignissen wie Datenbeschädigung, versehentlichem Löschen oder einem Offline-Status keine Daten bereitstellen kann. Informationen zum Konfigurieren eines Ziel-Volumes für den Datenzugriff und zur Reaktivierung eines Quell-Volumes finden Sie im ONTAP 9 Volume Disaster Recovery Express Guide.

Aktion	Beschreibung
Neu synchronisieren	Stellt eine unterbrochene Beziehung zwischen Volumes wieder her und setzt die Datenreplizierung gemäß dem definierten Zeitplan fort. Wenn Sie die Volumes erneut synchronisieren, werden die Inhalte auf dem Ziel-Volume durch die Inhalte auf dem Quell-Volume überschrieben. Informationen zur Neusynchronisierung, die die Daten vom Ziel-Volume zum Quell-Volume neu synchronisiert, finden Sie im "ONTAP 9 Express Guide für die Disaster Recovery von Volumes".
Reverse Resync	Kehrt die Rollen der Quell- und Ziel-Volumes um. Der Inhalt des ursprünglichen Quell-Volumes wird durch den Inhalt des Ziel-Volumes überschrieben. Dies ist hilfreich, wenn Sie ein Quell-Volume, das offline gegangen ist, reaktivieren möchten. Alle Daten, die zwischen der letzten Datenreplizierung und dem Zeitpunkt, zu dem das Quell-Volume deaktiviert wurde, auf das ursprüngliche Quell-Volume geschrieben wurden, bleiben nicht erhalten.
Zeitplan bearbeiten	Ermöglicht die Auswahl eines anderen Zeitplans für die Datenreplizierung.
Richtlinieninformationen	Zeigt die der Datenreplizierungsbeziehung zugewiesene Schutzrichtlinie an.
Max. Übertragungsrate bearbeiten	Hier können Sie die maximale Rate (in Kilobyte pro Sekunde) bearbeiten, mit der Daten übertragen werden können.
Aktualisierung	Startet einen inkrementellen Transfer, um das Zielvolume zu aktualisieren.
Löschen	Löscht die Data-Protection-Beziehung zwischen Quell- und Ziel-Volumes, d. H., die Datenreplizierung findet nicht mehr zwischen den Volumes statt. Durch diese Aktion wird das Ziel-Volume nicht für den Datenzugriff aktiviert. Durch diese Aktion werden auch die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung (Storage Virtual Machine) gelöscht, wenn keine anderen Data-Protection-Beziehungen zwischen den Systemen bestehen.

Ergebnis

Nachdem Sie eine Aktion ausgewählt haben, aktualisiert Cloud Manager die Beziehung oder den Zeitplan.

Auswählen einer Replizierungsrichtlinie

Möglicherweise benötigen Sie Hilfe bei der Auswahl einer Replizierungsrichtlinie, wenn Sie die Datenreplizierung in Cloud Manager einrichten. Eine Replizierungsrichtlinie definiert, wie das Storage-System Daten von einem Quell-Volume auf ein Ziel-Volume repliziert.

Was sind Replizierungsrichtlinien

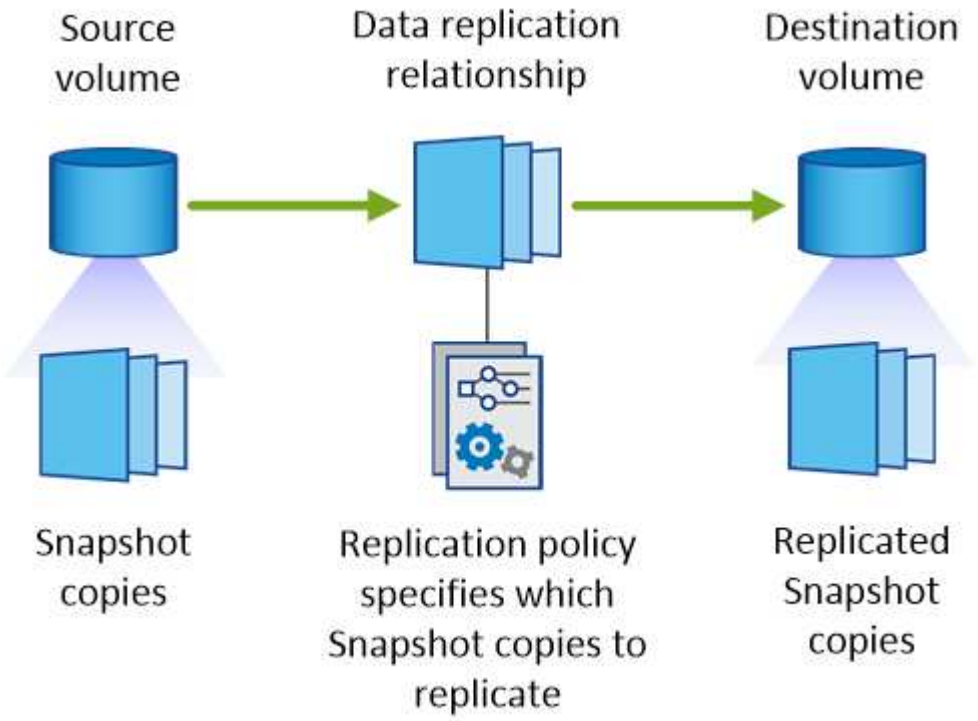
Das Betriebssystem ONTAP erstellt automatisch Backups mit dem Namen Snapshot Kopien. Eine Snapshot Kopie ist ein schreibgeschütztes Image eines Volumes, das den Status des Dateisystems zu einem bestimmten Zeitpunkt erfasst.

Wenn Sie Daten zwischen Systemen replizieren, replizieren Sie Snapshot Kopien von einem Quell-Volume zu einem Ziel-Volume. Eine Replizierungsrichtlinie gibt an, welche Snapshot Kopien vom Quell-Volume auf das

Ziel-Volume repliziert werden sollen.

Replizierungsrichtlinien werden auch als *Protection* -Richtlinien bezeichnet, da sie durch SnapMirror und SnapVault Technologien unterstützt werden, die Disaster Recovery-Schutz und Disk-to-Disk Backup und Recovery bieten.

Die folgende Abbildung zeigt die Beziehung zwischen Snapshot Kopien und Replizierungsrichtlinien:



Arten von Replizierungsrichtlinien

Es gibt drei Arten von Replizierungsrichtlinien:

- Eine *Mirror* Richtlinie repliziert neu erstellte Snapshot Kopien zu einem Ziel-Volume.

  Sie können diese Snapshot Kopien verwenden, um das Quell-Volume als Vorbereitung für die Disaster Recovery oder für die einmalige Datenreplizierung zu schützen. Sie können das Ziel-Volume jederzeit für den Datenzugriff aktivieren.

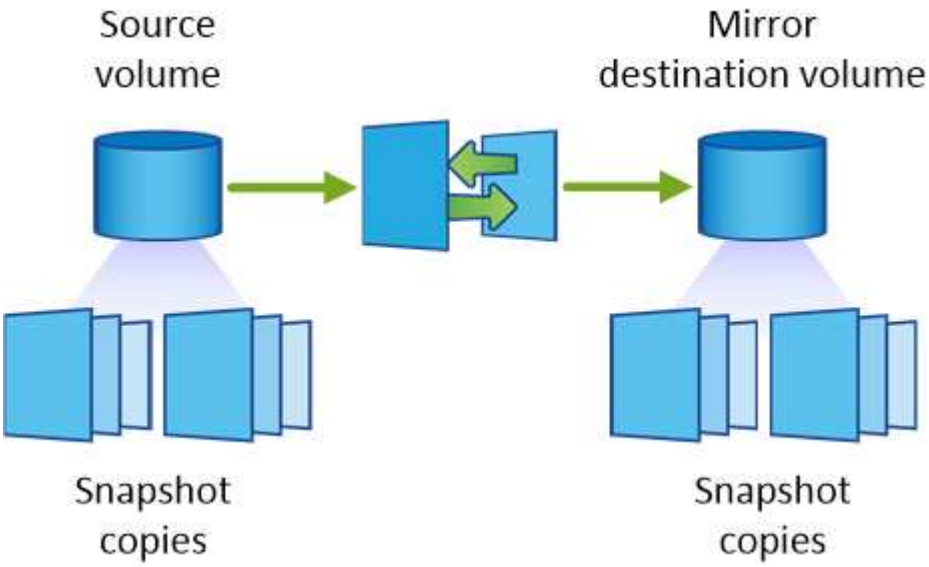
- Eine *Backup*-Richtlinie repliziert bestimmte Snapshot-Kopien zu einem Ziel-Volume und speichert diese in der Regel für einen längeren Zeitraum, als es auf dem Quell-Volume der Fall wäre.

  Sie können Daten aus diesen Snapshot Kopien wiederherstellen, wenn Daten beschädigt oder verloren gehen, und sie zur Einhaltung von Standards und zu anderen Governance-Zwecken aufbewahren.

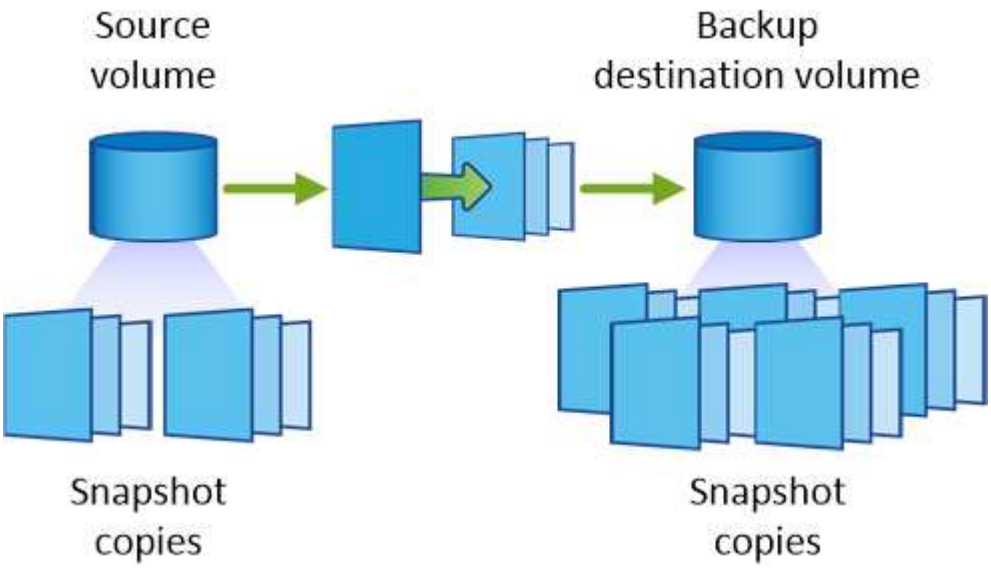
- Eine Richtlinie „ *Mirror und Backup*“ ermöglicht Disaster Recovery und langfristige Datenhaltung.

  Jedes System verfügt über eine standardmäßige Mirror- und Backup-Policy, die in vielen Situationen gut funktioniert. Wenn Sie benutzerdefinierte Richtlinien benötigen, können Sie mit System Manager eigene Richtlinien erstellen.

Die folgenden Abbildungen zeigen den Unterschied zwischen den Richtlinien für Spiegelung und Sicherung. Eine Spiegelungsrichtlinie spiegelt die auf dem Quell-Volume verfügbaren Snapshot Kopien wider.



Eine Backup-Policy behält Snapshot-Kopien in der Regel länger bei, als sie auf dem Quell-Volume aufbewahrt werden:



Funktionsweise von Backup-Richtlinien

Im Gegensatz zu Spiegelungsrichtlinien replizieren Backup-Richtlinien (SnapVault) bestimmte Snapshot Kopien auf ein Ziel-Volume. Es ist wichtig zu verstehen, wie Backup-Richtlinien funktionieren, wenn Sie Ihre eigenen Richtlinien anstelle der Standardrichtlinien verwenden möchten.

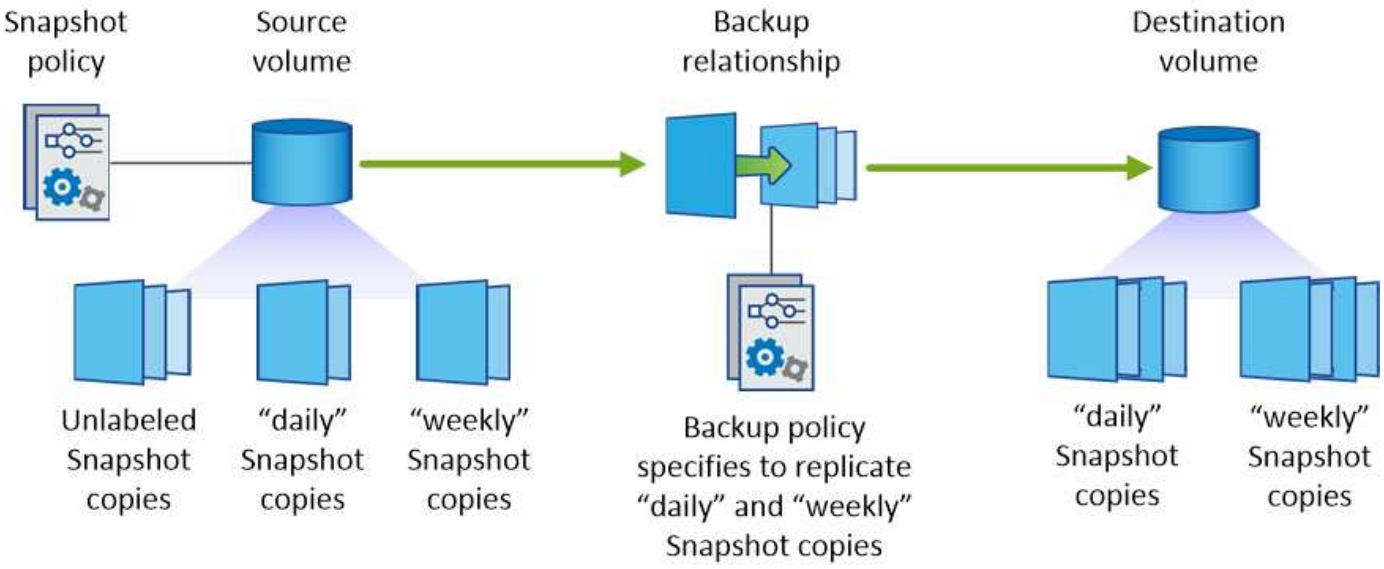
Verständnis der Beziehung zwischen Snapshot Copy Labels und Backup-Richtlinien

Eine Snapshot-Richtlinie definiert, wie das System Snapshot-Kopien von Volumes erstellt. Die Richtlinie gibt an, wann die Snapshot Kopien erstellt werden sollen, wie viele Kopien aufbewahrt werden sollen und wie sie beschriften werden. Ein System erstellt beispielsweise jeden Tag um 12:10 Uhr eine Snapshot Kopie, behält die beiden neuesten Kopien bei und kennzeichnet sie "täglich".

Eine Backup-Richtlinie enthält Regeln, die festlegen, welche benannten Snapshot Kopien auf ein Ziel-Volume repliziert werden sollen und wie viele Kopien aufbewahrt werden sollen. Die in einer Backup-Richtlinie definierten Bezeichnungen müssen mit einer oder mehreren Bezeichnungen übereinstimmen, die in einer

Snapshot-Richtlinie definiert sind. Andernfalls kann das System keine Snapshot Kopien replizieren.

Eine Backup-Policy, die beispielsweise die Bezeichnungen "täglich" und "wöchentlich" enthält, führt zur Replizierung von Snapshot Kopien, die nur diese Bezeichnungen enthalten. Es werden keine anderen Snapshot Kopien repliziert, wie im folgenden Bild dargestellt:



Standardrichtlinien und benutzerdefinierte Richtlinien

Die Standard-Snapshot-Richtlinie erstellt stündlich, täglich und wöchentlich Snapshot Kopien, wobei sechs Stunden, zwei Tage und zwei wöchentliche Snapshot Kopien aufbewahrt werden.

Sie können problemlos eine Standard-Backup-Richtlinie mit der Standard-Snapshot-Richtlinie verwenden. Die Standard-Backup-Richtlinien replizieren tägliche und wöchentliche Snapshot Kopien, wobei sieben tägliche und 52 wöchentliche Snapshot Kopien aufbewahrt werden.

Wenn Sie benutzerdefinierte Richtlinien erstellen, müssen die durch diese Richtlinien definierten Bezeichnungen übereinstimmen. Sie können benutzerdefinierte Richtlinien mit System Manager erstellen.

Datenreplizierung von NetApp HCI auf Cloud Volumes ONTAP

Wenn Sie versuchen, Daten von NetApp HCI zu Cloud Volumes ONTAP zu replizieren, können Sie dies auf einem NetApp HCI System tun, auf dem NetApp Element Software mit SnapMirror läuft. Alternativ können Sie Daten auf Volumes replizieren, die auf einem ONTAP Select System erstellt wurden, das als virtueller Gast in einer NetApp HCI Lösung ausgeführt wird, auf Cloud Volumes ONTAP.

Details finden Sie in den folgenden technischen Berichten:

- "Technischer Bericht 4641: NetApp HCI Datensicherung"
- "Technischer Bericht 4651: NetApp SolidFire SnapMirror Architektur und Konfiguration"

Monitoring der Performance

Erfahren Sie mehr über den Monitoring-Service

Durch die Nutzung der "NetApp Cloud Insights Service", Cloud Manager liefert Einblicke

in den Zustand und die Performance Ihrer Cloud Volumes ONTAP Instanzen und unterstützt Sie bei der Fehlerbehebung und Optimierung der Performance Ihrer Cloud-Storage-Umgebung.

Funktionen

- Automatische Überwachung aller Volumes
- Anzeige von Volume-Performance-Daten in Bezug auf IOPS, Durchsatz und Latenz
- Identifizieren von Performance-Problemen, um die Auswirkungen auf Benutzer und Applikationen zu minimieren

Unterstützte Cloud-Provider

Der Monitoring-Service wird mit Cloud Volumes ONTAP für AWS unterstützt.

Kosten

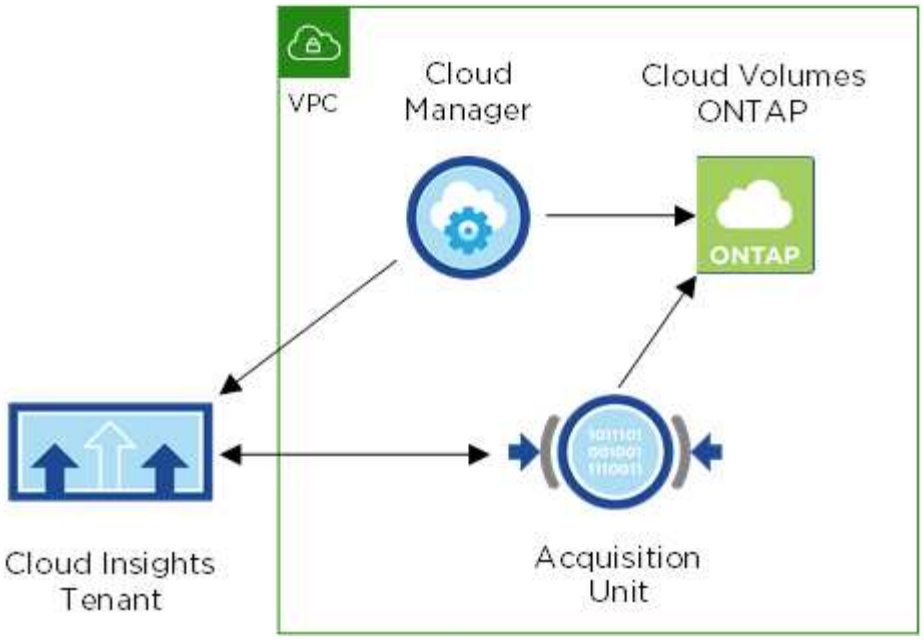
Die Überwachung ist derzeit als Vorschau verfügbar. Die Aktivierung ist zwar kostenlos, aber Cloud Manager startet eine Virtual Machine in der VPC, um die Überwachung zu erleichtern. Diese VM verursacht Gebühren von Ihrem Cloud-Provider.

Funktionsweise von Cloud Insights mit Cloud Manager

Die Cloud Insights Integration auf höherer Ebene in Cloud Manager funktioniert folgendermaßen:

1. Sie aktivieren den Überwachungsdienst auf Cloud Volumes ONTAP.
2. Cloud Manager konfiguriert Ihre Umgebung. Er führt folgende Maßnahmen durch:
    a. Erstellt einen Cloud Insights-Mandanten (auch „*Environment*“ genannt) und ordnet alle Benutzer in Ihrem Cloud Central-Konto dem Mandanten zu.
    b. Cloud Insights: 30 Tage kostenlos testen
    c. Implementiert eine Virtual Machine in der VPC, der als „Acquisition Unit“ bezeichnet wird, die das Monitoring von Volumes erleichtert (dies ist die VM, die im Abschnitt „Kosten“ oben erwähnt ist).
    d. Verbindet die Akquisitionseinheit mit Cloud Volumes ONTAP und mit dem Cloud Insights-Mandanten.
3. In Cloud Manager klicken Sie auf Monitoring und verwenden die Performance-Daten, um Fehler zu beheben und die Performance zu optimieren.

Die Beziehung zwischen diesen Komponenten wird in der folgenden Abbildung dargestellt:



Die Akquisitionseinheit

Wenn Sie Monitoring aktivieren, implementiert Cloud Manager eine Erfassungseinheit im selben Subnetz wie der Connector.

Eine *Acquisition Unit* sammelt Performancedaten von Cloud Volumes ONTAP und sendet sie an den Cloud Insights-Mandanten. Cloud Manager fragt diese Daten ab und stellt sie Ihnen zur Verfügung.

Beachten Sie Folgendes über die Instanz der Erfassungseinheit:

- Die Erfassungseinheit wird auf einer instanz mit t3.xlarge mit einem GP2-Volumen von 100 GB ausgeführt.
- Die Instanz heißt *AcquitionUnit* mit einem generierten Hash (UUID), der mit ihm verknüpft ist. Beispiel: *AcquitionUnit-FAN7FqeH*
- Pro Connector wird nur eine Akquisitionseinheit bereitgestellt.
- Die Instanz muss ausgeführt werden, um auf Leistungsinformationen auf der Registerkarte Überwachung zuzugreifen.

Cloud Insights-Mandant

Cloud Manager richtet bei der Aktivierung von Monitoring einen *Tenant* ein. Ein Cloud Insights-Mandant ermöglicht Ihnen den Zugriff auf die Leistungsdaten, die die Acquisition Unit sammelt. Der Mandant ist eine sichere Datenpartition innerhalb des NetApp Cloud Insights Service.

Cloud Insights Webschnittstelle

Die Registerkarte „Monitoring“ in Cloud Manager bietet grundlegende Performance-Daten für die Volumes. Über die Cloud Insights Weboberfläche können Sie in Ihrem Browser eine detailliertere Überwachung durchführen und Warnmeldungen für Ihre Cloud Volumes ONTAP Systeme konfigurieren.

Kostenlose Testversion und Abonnement

Cloud Manager ermöglicht eine kostenlose 30-Tage-Testversion von Cloud Insights zur Bereitstellung von Performance-Daten innerhalb von Cloud Manager. Sie können sich mit den Funktionen der Cloud Insights Standard Edition beschäftigen.

Sie müssen sich bis zum Ende der kostenlosen Testversion anmelden, anderenfalls wird Ihr Cloud Insights Mandant endgültig gelöscht. Sie können die Basic-, Standard- oder Premium-Edition abonnieren, um die Monitoring-Funktion in Cloud Manager fortzusetzen.

"Erfahren Sie, wie Sie Cloud Insights abonnieren".

Monitoring von Cloud Volumes ONTAP in AWS

Führen Sie einige Schritte durch, um mit der Überwachung der Cloud Volumes ONTAP-Performance zu beginnen.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

Überprüfen Sie die Unterstützung Ihrer Konfiguration

Sie benötigen eine Neuinstallation von Cloud Manager 3.8.4 oder höher in AWS, Cloud Volumes ONTAP in AWS und als neuer Cloud Insights Kunde.

Aktivieren Sie die Überwachung auf Ihrem neuen oder vorhandenen System

- Neue Arbeitsumgebungen: Achten Sie darauf, Monitoring aktiviert zu halten, wenn Sie die Arbeitsumgebung erstellen (es ist standardmäßig aktiviert).
- Bestehende Arbeitsumgebungen: Wählen Sie eine Arbeitsumgebung und klicken Sie auf **Monitoring starten**.

Anzeigen von Performance-Daten

Klicken Sie auf **Monitoring** und zeigen Sie Leistungsdaten für Ihre Volumes an.

Abonnieren Sie Cloud Insights

Wenn Sie sich für eine kostenlose 30-Tage-Testversion anmelden, werden auch weiterhin Performance-Daten in Cloud Manager und Cloud Insights gespeichert. "Erfahren Sie, wie Sie abonniert werden können".

Anforderungen

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen.

Unterstützte Cloud Manager Versionen

Sie benötigen eine neue Installation von Cloud Manager 3.8.4 oder höher. Es ist eine neue Installation erforderlich, weil für den Monitoring-Service eine neue Infrastruktur erforderlich ist. Die Infrastruktur ist bei Neuinstallationen von Cloud Manager 3.8 verfügbar 4.

Unterstützte Cloud Volumes ONTAP-Versionen

Jede Version von Cloud Volumes ONTAP in AWS.

Cloud Insights-Anforderungen

Sie müssen ein neuer Cloud Insights Kunde sein. Die Überwachung wird nicht unterstützt, wenn Sie bereits über einen Cloud Insights-Mandanten verfügen.

E-Mail-Adresse für Cloud Central

Die E-Mail-Adresse für Ihr Cloud Central-Benutzerkonto sollte Ihre geschäftliche E-Mail-Adresse sein. Kostenlose E-Mail-Domains wie gmail und Hotmail werden bei der Erstellung eines Cloud Insights-Mandanten nicht unterstützt.

Netzwerk für die Akquisitionseinheit

Die Akquisitionseinheit verwendet eine 2-Wege-/gegenseitige Authentifizierung, um eine Verbindung zum Cloud Insights-Server herzustellen. Das Clientzertifikat muss an den Cloud Insights-Server zur Authentifizierung übergeben werden. Dazu muss der Proxy eingerichtet werden, um die HTTP-Anforderung an den Cloud Insights-Server weiterzuleiten, ohne die Daten zu entschlüsseln.

Die Erfassungseinheit verwendet die folgenden beiden Endpunkte, um mit Cloud Insights zu kommunizieren. Wenn Sie eine Firewall zwischen dem Erfassungs- und dem Cloud Insights-Server besitzen, benötigen Sie diese Endpunkte, wenn Sie Firewall-Regeln konfigurieren:

```
https://aulogin.<Cloud Insights Domain>
https://<your-tenant-ID>.<Cloud Insights Domain>
```

Beispiel:

```
https://aulogin.c01.cloudinsights.netapp.com
https://cg0c586a-ee05-45rb-a5ac-
333b5ae7718d7.c01.cloudinsights.netapp.com
```

Kontaktieren Sie uns über den Chat in Product, wenn Sie Hilfe bei der Identifizierung Ihrer Cloud Insights-Domain und Mandanten-ID benötigen.

Vernetzung für den Connector

Ähnlich wie die Erfassungseinheit muss der Connector über eine ausgehende Verbindung zum Cloud Insights-Mandanten verfügen. Aber der Endpunkt, den der Connector kontaktiert, ist etwas anders. Die Mandantenhost-URL wird über die verkürzte Mandanten-ID kontaktiert:

```
 https://<your-short-tenant-ID>.<Cloud Insights Domain>
Beispiel:
```

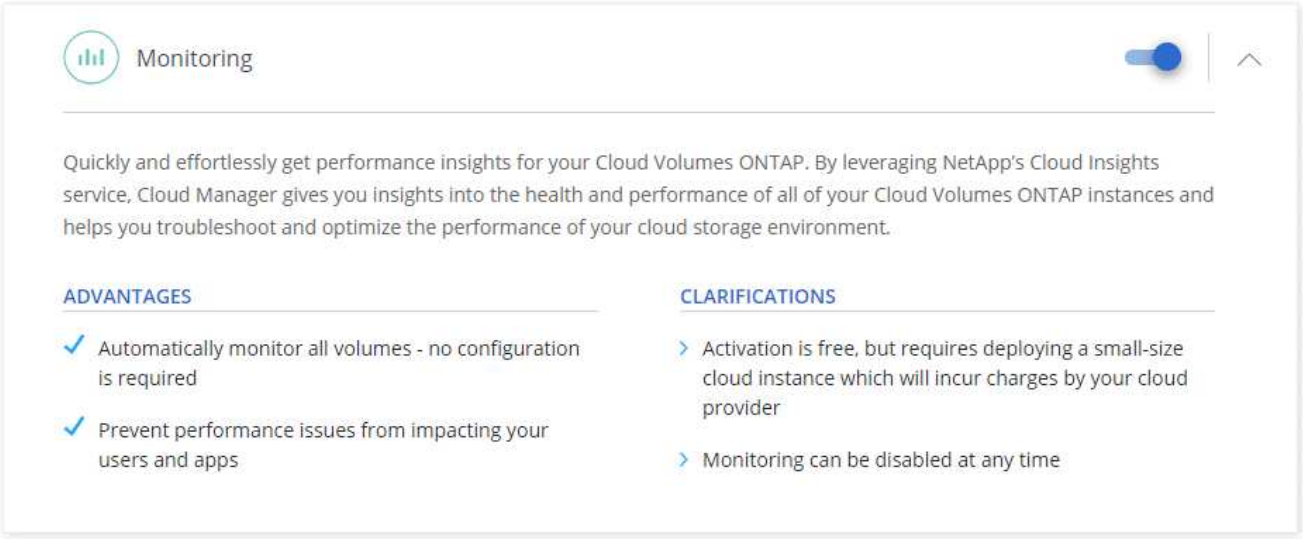
```
 https://abcd12345.c01.cloudinsights.netapp.com
Auch hier können Sie uns über den Produkt-Chat kontaktieren, wenn Sie
Hilfe bei der Ermittlung der Mandanten-Host-URL benötigen.
```

Aktivieren der Überwachung auf einem neuen System

Der Überwachungsdienst ist standardmäßig im Assistenten für die Arbeitsumgebung aktiviert. Achten Sie darauf, dass die Option aktiviert bleibt.

Schritte

1. Klicken Sie auf **Cloud Volumes ONTAP erstellen**.
2. Wählen Sie Amazon Web Services als Cloud-Provider und wählen Sie dann einen einzelnen Node oder ein HA-System.
3. Füllen Sie die Seite „Details & Credentials“ aus.
4. Lassen Sie auf der Seite Dienste den Dienst aktiviert, und klicken Sie auf **Weiter**.

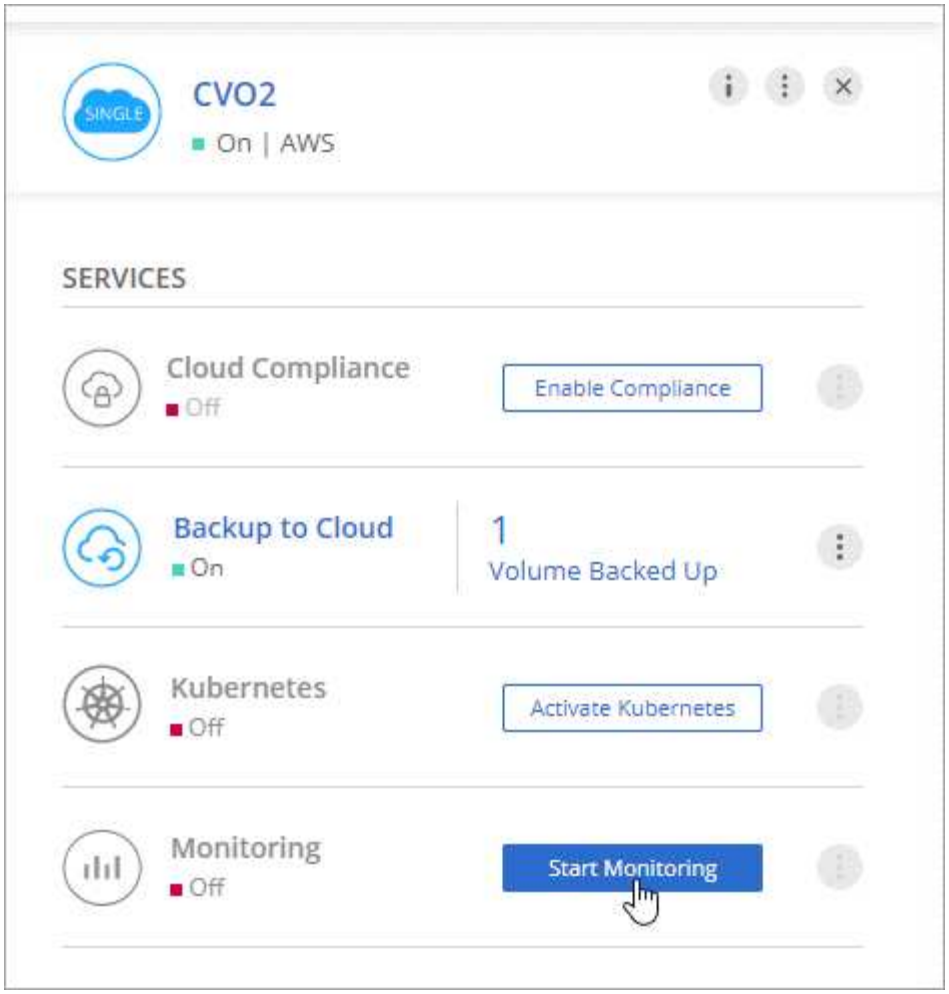


Aktivieren der Überwachung auf einem vorhandenen System

Ermöglichen Sie jederzeit die Überwachung aus der Arbeitsumgebung.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Arbeitsumgebungen**.
2. Wählen Sie eine Arbeitsumgebung aus.
3. Klicken Sie im rechten Fensterbereich auf **Überwachung starten**.



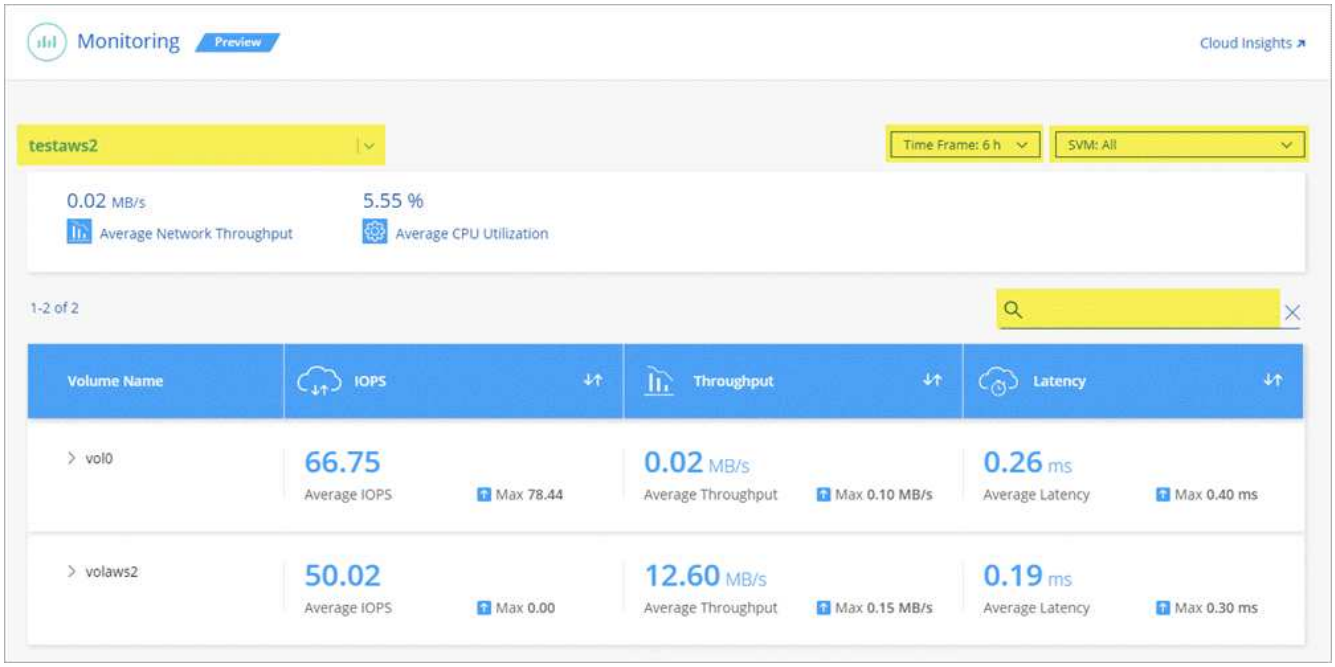
Monitoring Ihrer Volumes

Monitoring der Performance durch IOPS, Durchsatz und Latenz für jedes der Volumes

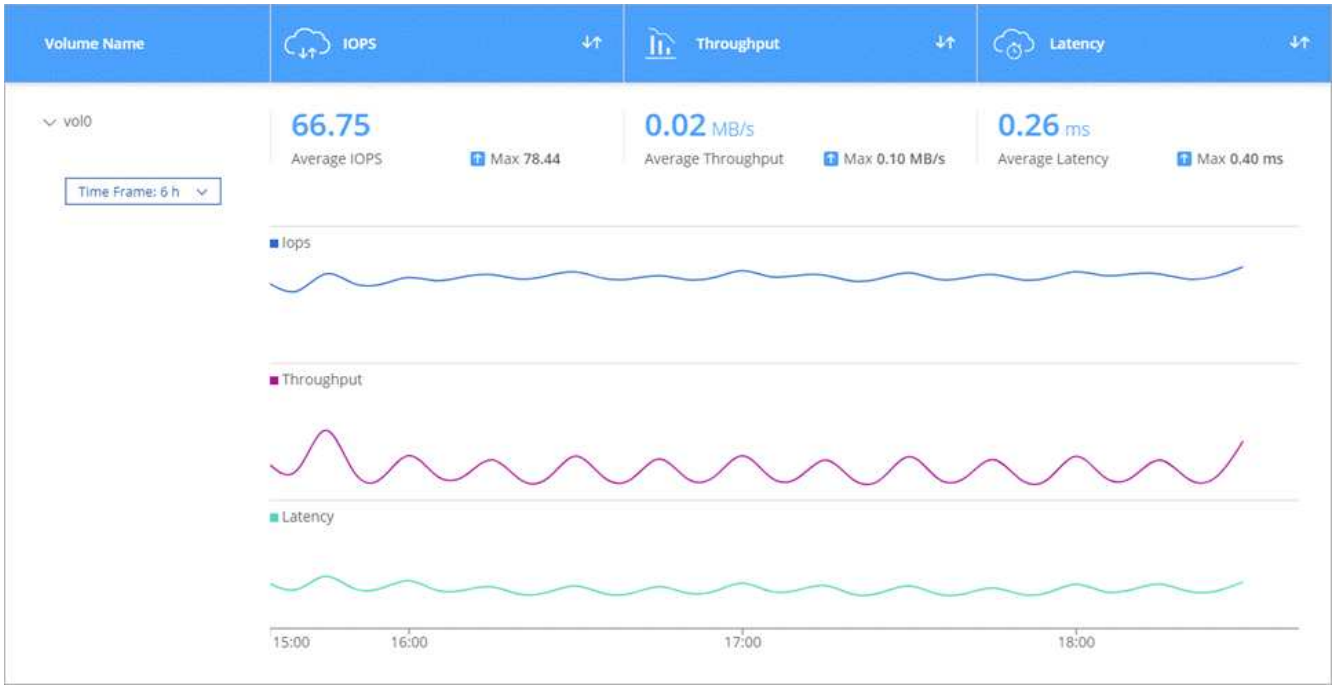
Schritte

1. Klicken Sie oben im Cloud Manager auf **Überwachung**.
2. Filtern Sie den Inhalt des Dashboards, um die gewünschten Informationen abzurufen.
    - Wählen Sie eine bestimmte Arbeitsumgebung aus.
    - Wählen Sie einen anderen Zeitrahmen aus.
    - Wählen Sie eine bestimmte SVM aus.
    - Suchen Sie nach einem bestimmten Volume.

    Die folgende Abbildung zeigt jede dieser Optionen:



3. Klicken Sie in der Tabelle auf ein Volume, um die Zeile zu erweitern und einen Zeitplan für IOPS, Durchsatz und Latenz anzuzeigen.



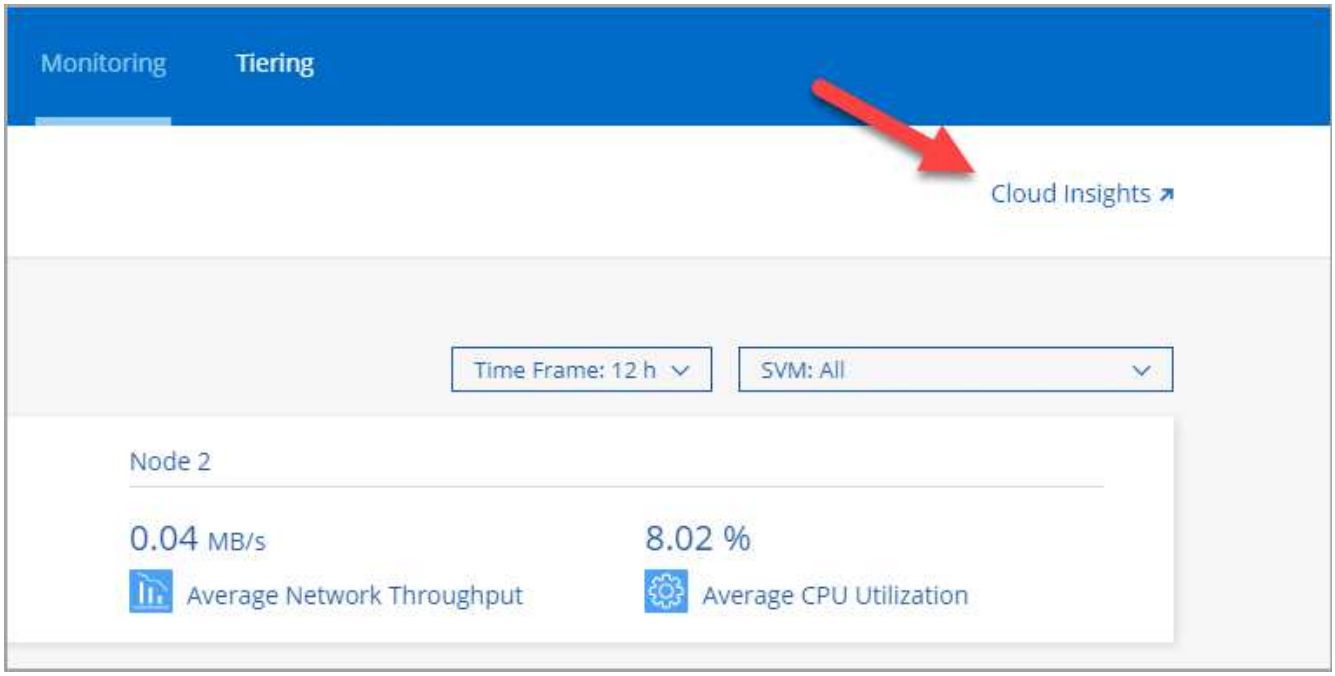
4. Ermitteln Sie mithilfe der Daten Performance-Probleme, um die Auswirkungen auf Benutzer und Applikationen zu minimieren.

Weitere Informationen von Cloud Insights

Die Registerkarte „Monitoring“ in Cloud Manager bietet grundlegende Performance-Daten für die Volumes. Über die Cloud Insights Weboberfläche können Sie in Ihrem Browser eine detailliertere Überwachung durchführen und Warnmeldungen für Ihre Cloud Volumes ONTAP Systeme konfigurieren.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Überwachung**.
2. Klicken Sie auf den Link **Cloud Insights**.



Ergebnis

Cloud Insights in einer neuen Browser-Registerkarte öffnen. Wenn Sie Hilfe benötigen, lesen Sie den "Cloud Insights-Dokumentation".

Überwachung wird deaktiviert

Wenn Sie Cloud Volumes ONTAP nicht mehr überwachen möchten, können Sie den Dienst jederzeit deaktivieren.

Wenn Sie das Monitoring in jeder Ihrer Arbeitsumgebungen deaktivieren, müssen Sie die EC2-Instanz selbst löschen. Die Instanz heißt *AcquitionUnit* mit einem generierten Hash (UUID), der mit ihm verknüpft ist. Beispiel: *AcquitionUnit-FAN7FqeH*

Schritte

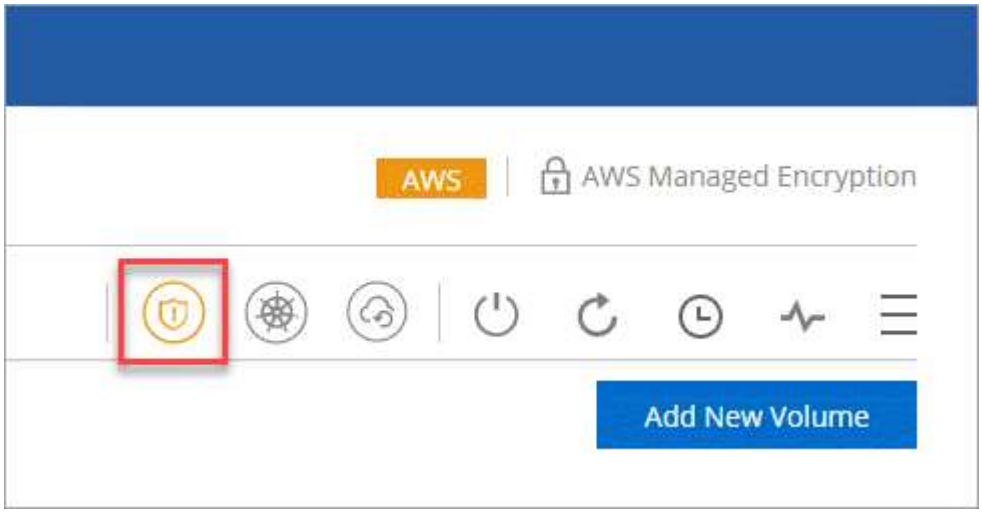
1. Klicken Sie oben im Cloud Manager auf **Arbeitsumgebungen**.
2. Wählen Sie eine Arbeitsumgebung aus.
3. Klicken Sie im rechten Fensterbereich auf das Symbol und wählen Sie **Scan deaktivieren**.

Besserer Schutz gegen Ransomware

Ransomware-Angriffe können das Unternehmen Zeit, Ressourcen und Image-Schäden kosten. Cloud Manager ermöglicht die Implementierung der NetApp Lösung für Ransomware, die mit effektiven Tools für Transparenz, Erkennung und Korrektur ausgestattet ist.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Symbol **Ransomware**.

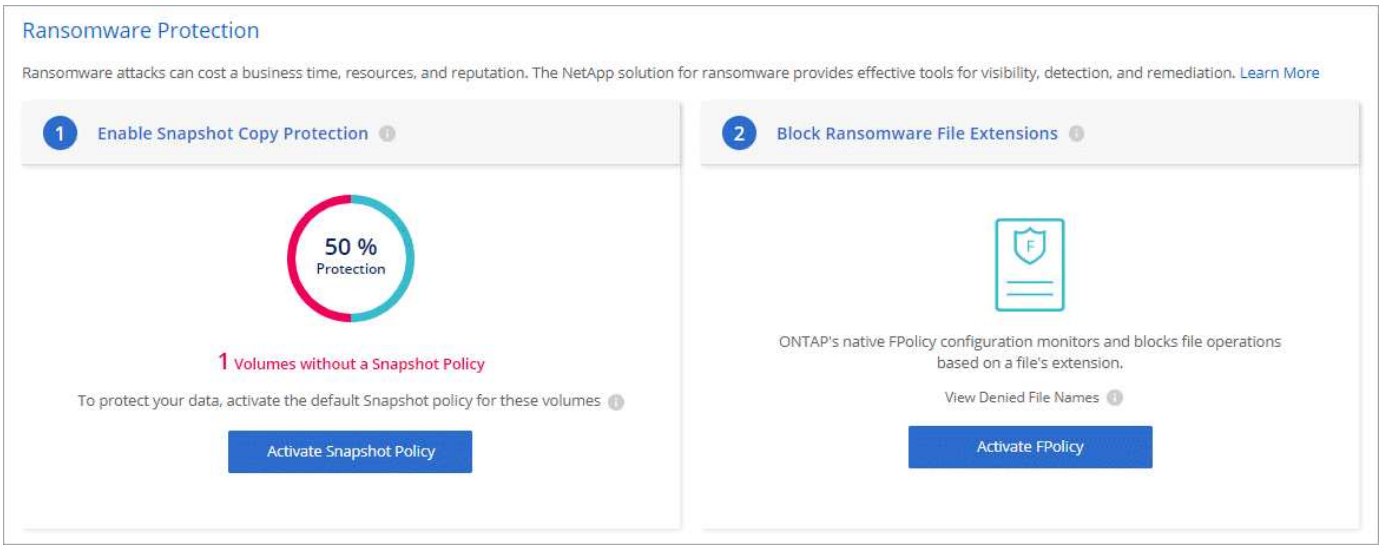


2. Implementierung der NetApp Lösung für Ransomware:
   a. Klicken Sie auf **Snapshot-Richtlinie aktivieren**, wenn Volumes ohne Snapshot-Richtlinie aktiviert sind.

      Die NetApp Snapshot-Technologie bietet die branchenweit beste Lösung zur Behebung von Ransomware. Der Schlüssel zu einer erfolgreichen Recovery liegt im Restore aus einem nicht infizierten Backup. Snapshot Kopien sind schreibgeschützt, der Ransomware-Beschädigungen verhindert. Sie können außerdem die Granularität nutzen, um Images einer einzelnen Dateikopie oder einer kompletten Disaster-Recovery-Lösung zu erstellen.

   b. Klicken Sie auf **FPolicy** aktivieren, um die FPolicy Lösung von ONTAP zu aktivieren, die Dateivorgänge auf Basis der Dateierweiterung blockieren kann.

      Diese präventive Lösung verbessert den Schutz vor Ransomware-Angriffen, indem sie gängige Ransomware-Dateitypen blockiert.



Verwaltung

Registrieren von Pay-as-you-go-Systemen

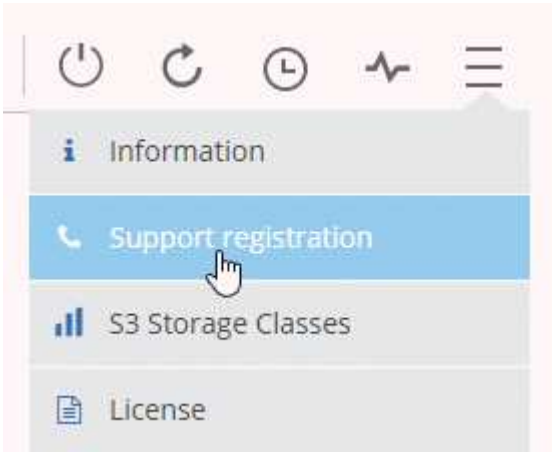
Cloud Volumes ONTAP Explore, Standard und Premium umfasst Support von NetApp. Sie müssen jedoch den Support erst aktivieren, wenn Sie die Systeme bei NetApp registrieren.

Schritte

1. Wenn Sie noch kein NetApp Support Site Konto zu Cloud Manager hinzugefügt haben, gehen Sie zu **Account Settings** und fügen Sie es jetzt hinzu.

   "Erfahren Sie, wie Sie Konten der NetApp Support Site hinzufügen".

2. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf den Namen des Systems, das Sie registrieren möchten.
3. Klicken Sie auf das Menü-Symbol und dann auf **Support-Registrierung**:



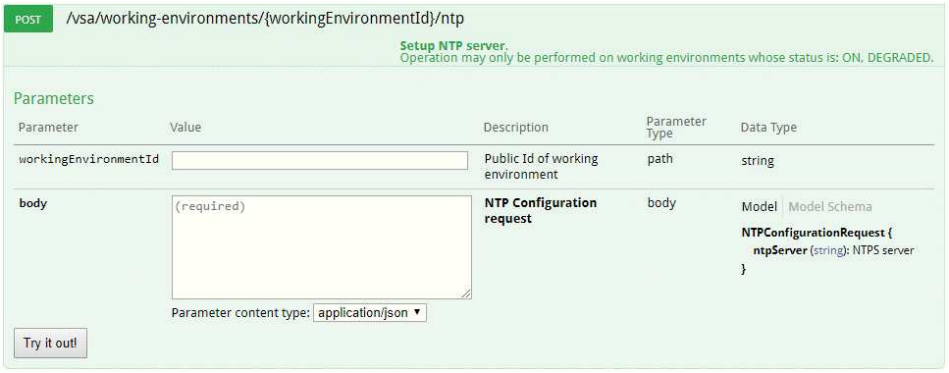
4. Wählen Sie ein NetApp Support Site Konto aus und klicken Sie auf **Registrieren**.

Ergebnis

Cloud Manager registriert das System bei NetApp.

Einrichten von Cloud Volumes ONTAP

Nachdem Sie Cloud Volumes ONTAP implementiert haben, können Sie diese einrichten, indem Sie die Systemzeit mithilfe von NTP synchronisieren und einige optionale Aufgaben entweder über den System Manager oder die CLI ausführen.

Aufgabe	Beschreibung
Synchronisieren Sie die Systemzeit mit NTP	Durch das Festlegen eines NTP-Servers wird die Zeit zwischen den Systemen im Netzwerk synchronisiert, wodurch Probleme aufgrund von Zeitunterschieden vermieden werden können. Geben Sie beim Einrichten eines CIFS-Servers einen NTP-Server mithilfe der Cloud Manager-API oder von der Benutzeroberfläche an. • "Ändern des CIFS-Servers" • "Cloud Manager API-Entwicklerleitfaden" Hier ist zum Beispiel die API für ein Single-Node-System in AWS: 
Optional: AutoSupport konfigurieren	AutoSupport überwacht proaktiv den Systemzustand und sendet standardmäßig automatisch Meldungen an den technischen Support von NetApp. Wenn der Kontoadministrator dem Cloud-Manager einen Proxyserver hinzugefügt hat, bevor Sie Ihre Instanz gestartet haben, ist Cloud Volumes ONTAP so konfiguriert, dass er diesen Proxyserver für AutoSupport-Nachrichten verwendet. Sie sollten AutoSupport testen, um sicherzustellen, dass Nachrichten gesendet werden können. Anweisungen hierzu finden Sie in der Hilfe zum System Manager oder in der "ONTAP 9 – Systemadministrationshandbuch".
Optional: Konfigurieren Sie Cloud-Manager als AutoSupport-Proxy	Wenn in Ihrer Umgebung ein Proxyserver zum Senden von AutoSupport Meldungen benötigt wird, können Sie Cloud Manager so konfigurieren, dass er als Proxy verwendet wird. Für Cloud Manager ist keine Konfiguration erforderlich – abgesehen vom Internet-Zugriff. Sie müssen einfach zur CLI für Cloud Volumes ONTAP gehen und den folgenden Befehl ausführen: `system node autosupport modify -proxy-url <cloud-manager-ip-address>`
Optional: EMS konfigurieren	Das Event Management System (EMS) erfasst und zeigt Informationen zu Ereignissen an, die auf Cloud Volumes ONTAP Systemen auftreten. Um Ereignisbenachrichtigungen zu erhalten, können Sie Ereignisziele (E-Mail-Adressen, SNMP-Trap-Hosts oder Syslog-Server) und Ereignisrouten für einen bestimmten Ereignisschweregrad festlegen. Sie können EMS über die CLI konfigurieren. Anweisungen hierzu finden Sie im "ONTAP 9 EMS Configuration Express Guide".

Aufgabe	Beschreibung
Optional: Erstellung einer SVM Management-Netzwerkschnittstelle (LIF) für HA-Systeme in mehreren AWS Verfügbarkeitszonen	Wenn Sie SnapCenter oder SnapDrive für Windows mit einem HA-Paar verwenden möchten, ist eine Storage Virtual Machine (SVM) Management Network Interface (LIF) erforderlich. Die SVM-Management-LIF muss bei Verwendung eines HA-Paars über mehrere AWS Availability Zones eine „*Floating* IP-Adresse“ verwenden. Cloud Manager fordert Sie auf, die unverankerte IP-Adresse anzugeben, wenn Sie das HA-Paar starten. Wenn Sie die IP-Adresse nicht angegeben haben, können Sie die SVM Management-LIF selbst über den System Manager oder die CLI erstellen. Das folgende Beispiel zeigt, wie Sie die LIF über die CLI erstellen: `network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home-port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall -policy mgmt`
Optional: Ändern Sie den Speicherort der Konfigurationsdateien	Cloud Volumes ONTAP erstellt automatisch Backup-Dateien für die Konfiguration, die Informationen zu den konfigurierbaren Optionen enthalten, die für einen ordnungsgemäßen Betrieb erforderlich sind. Standardmäßig sichert Cloud Volumes ONTAP die Dateien alle acht Stunden auf dem Connector-Host. Wenn Sie die Backups an einen anderen Speicherort senden möchten, können Sie den Speicherort auf einen FTP- oder HTTP-Server in Ihrem Datacenter oder in AWS ändern. Sie verfügen beispielsweise bereits über einen Backup-Speicherort für Ihre FAS Storage-Systeme. Sie können den Backup-Speicherort über die CLI ändern. Siehe "ONTAP 9 – Systemadministrationshandbuch".

Byol-Lizenzen für Cloud Volumes ONTAP verwalten

Fügen Sie eine Cloud Volumes ONTAP-BYOL-Systemlizenz hinzu, um zusätzliche Kapazität hinzuzufügen, eine vorhandene Systemlizenz zu aktualisieren und BYOL-Lizenzen für Backup in der Cloud zu managen.

Verwalten von Systemlizenzen

Sie können mehrere Lizenzen für ein Cloud Volumes ONTAP BYOL-System erwerben und so mehr als 368 TB Kapazität zuweisen. Beispielsweise können Sie zwei Lizenzen erwerben, um Cloud Volumes ONTAP bis zu 736 TB Kapazität zuzuweisen. Alternativ können Sie vier Lizenzen erwerben, um bis zu 1.4 PB zu erhalten.

Die Anzahl der Lizenzen, die Sie für ein Single Node-System oder ein HA-Paar erwerben können, ist unbegrenzt.

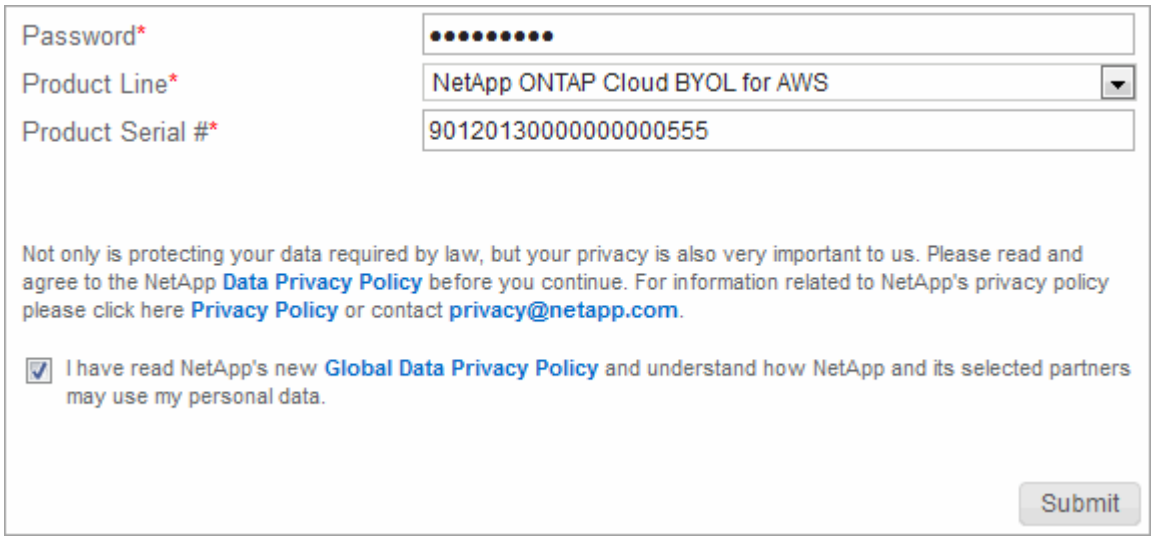
Abrufen einer Systemlizenzdatei

In den meisten Fällen kann Cloud Manager Ihre Lizenzdatei automatisch über Ihren NetApp Support Site Account beziehen. Aber wenn es nicht kann, dann müssen Sie die Lizenzdatei manuell hochladen. Wenn Sie die Lizenzdatei nicht haben, können Sie sie von netapp.com beziehen.

Schritte

1. Wechseln Sie zum "NetApp Lizenzdatei-Generator" Und loggen Sie sich mit Ihren Anmeldedaten für die NetApp Support Site ein.
2. Geben Sie Ihr Passwort ein, wählen Sie Ihr Produkt aus, geben Sie die Seriennummer ein, bestätigen Sie, dass Sie die Datenschutzrichtlinie gelesen und akzeptiert haben, und klicken Sie dann auf **Absenden**.

   Beispiel



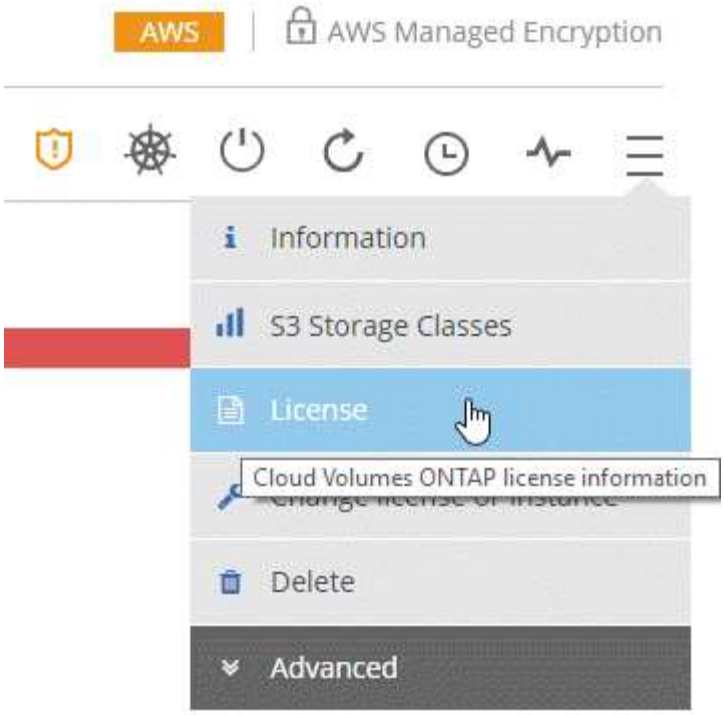
3. Wählen Sie aus, ob Sie die Datei serialnumber.NLF JSON per E-Mail oder direkt herunterladen möchten.

Hinzufügen einer neuen Systemlizenz

Fügen Sie jederzeit eine neue BYOL-Systemlizenz hinzu, um Ihrem Cloud Volumes ONTAP BYOL-System weitere 368 TB zusätzlicher Kapazität zuzuweisen.

Schritte

1. Öffnen Sie in Cloud Manager die BYOL-Arbeitsumgebung von Cloud Volumes ONTAP.
2. Klicken Sie auf das Menü-Symbol und dann auf **Lizenz**.



3. Klicken Sie auf **CVO-Systemlizenz hinzufügen**.

4. Geben Sie die Seriennummer ein oder laden Sie die Lizenzdatei hoch.
5. Klicken Sie Auf **Lizenz Hinzufügen**.

Ergebnis

Cloud Manager installiert die neue Lizenzdatei auf dem Cloud Volumes ONTAP System.

Aktualisieren einer Systemlizenz

Wenn Sie ein Byol Abonnement erneuern, indem Sie sich an einen NetApp Vertreter wenden, erhält Cloud Manager automatisch die neue Lizenz von NetApp und installiert sie auf dem Cloud Volumes ONTAP System.

Wenn Cloud Manager über die sichere Internetverbindung nicht auf die Lizenzdatei zugreifen kann, können Sie die Datei selbst beziehen und die Datei anschließend manuell auf Cloud Manager hochladen.

Schritte

1. Öffnen Sie in Cloud Manager die BYOL-Arbeitsumgebung von Cloud Volumes ONTAP.
2. Klicken Sie auf das Menü-Symbol und dann auf **Lizenz**.
3. Klicken Sie auf **Aktualisieren der CVO-Systemlizenz**.

4. Klicken Sie auf **Datei hochladen** und wählen Sie die Lizenzdatei aus.
5. Klicken Sie Auf **Lizenz Aktualisieren**.

Ergebnis

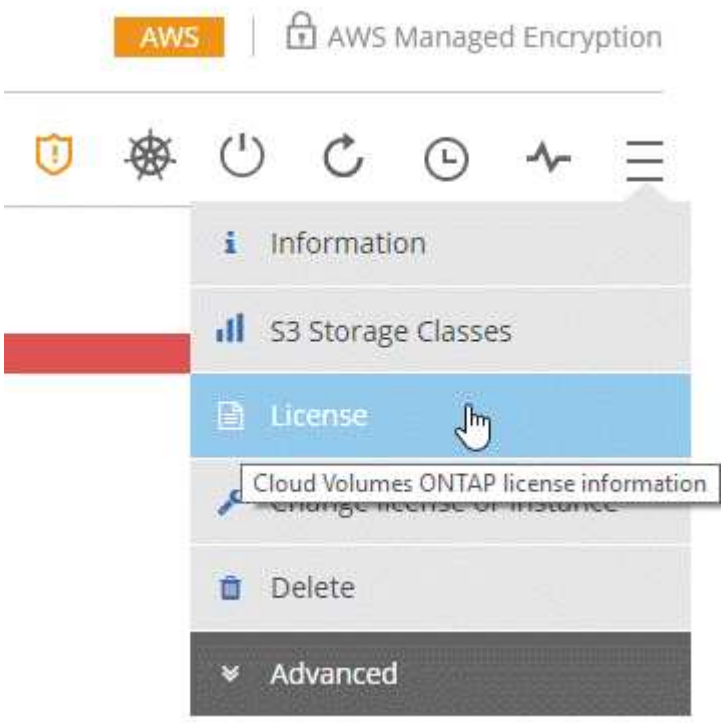
Cloud Manager aktualisiert die Lizenz auf dem Cloud Volumes ONTAP System.

Hinzufügen und Aktualisieren der Backup-BYOL-Lizenz

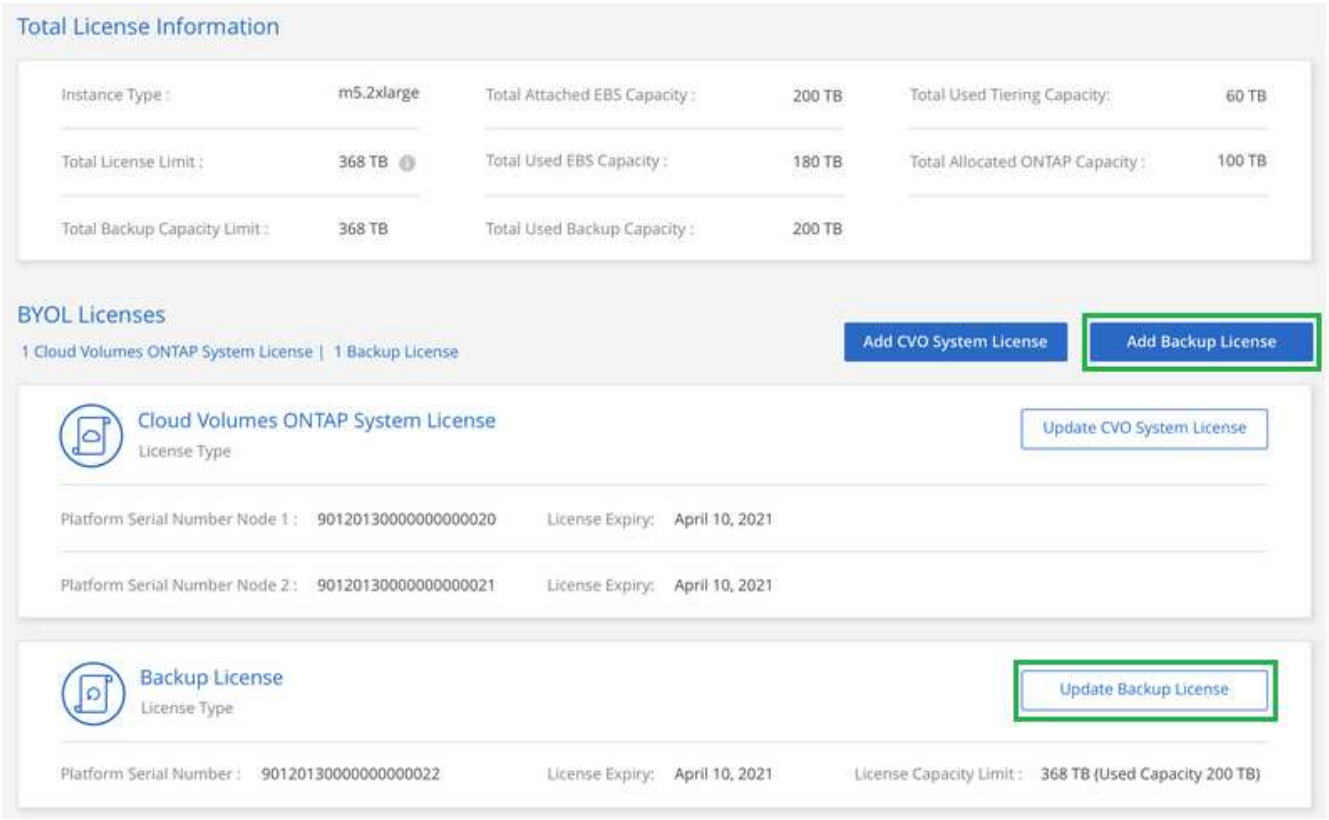
Auf der Seite „Byol Licenses“ können Sie Ihre BYOL-Lizenz für Backups hinzufügen oder aktualisieren.

Schritte

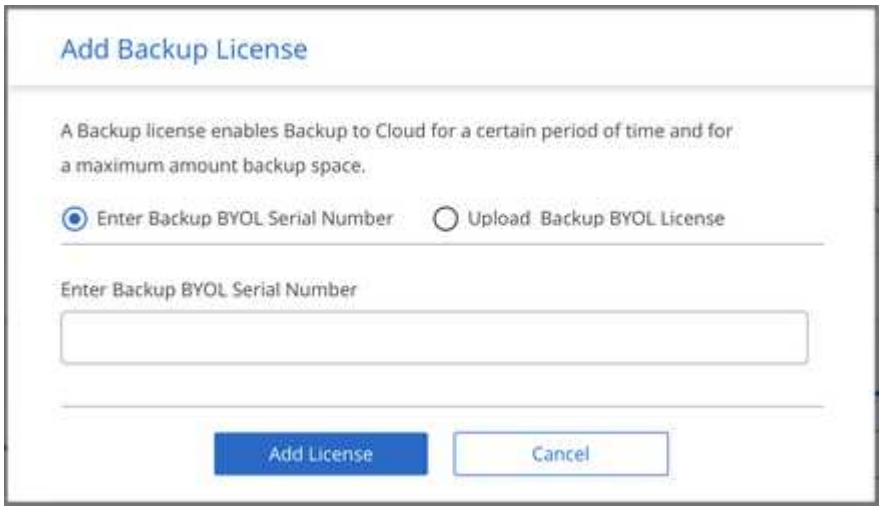
1. Öffnen Sie in Cloud Manager die BYOL-Arbeitsumgebung von Cloud Volumes ONTAP.
2. Klicken Sie auf das Menü-Symbol und dann auf **Lizenz**.



3. Klicken Sie abhängig davon, ob Sie eine neue Lizenz hinzufügen oder eine vorhandene Lizenz aktualisieren möchten, auf **Backup License** oder auf **Update Backup License**.



4. Geben Sie die Lizenzinformationen ein und klicken Sie auf **Lizenz hinzufügen**:
   - Wenn Sie die Seriennummer haben, wählen Sie die Option **Byol-Seriennummer eingeben** und geben Sie die Seriennummer ein.
   - Wenn Sie über die Backup-Lizenzdatei verfügen, wählen Sie die Option **BYOL-Lizenz hochladen** aus, und folgen Sie den Anweisungen, um die Datei anzuhängen.



Ergebnis

Cloud Manager fügt die Lizenz hinzu oder aktualisiert sie, sodass Ihr Cloud-Service für Backup aktiv ist.

Aktualisierung der Cloud Volumes ONTAP Software

Cloud Manager umfasst mehrere Optionen, mit denen Sie auf die aktuelle Version von

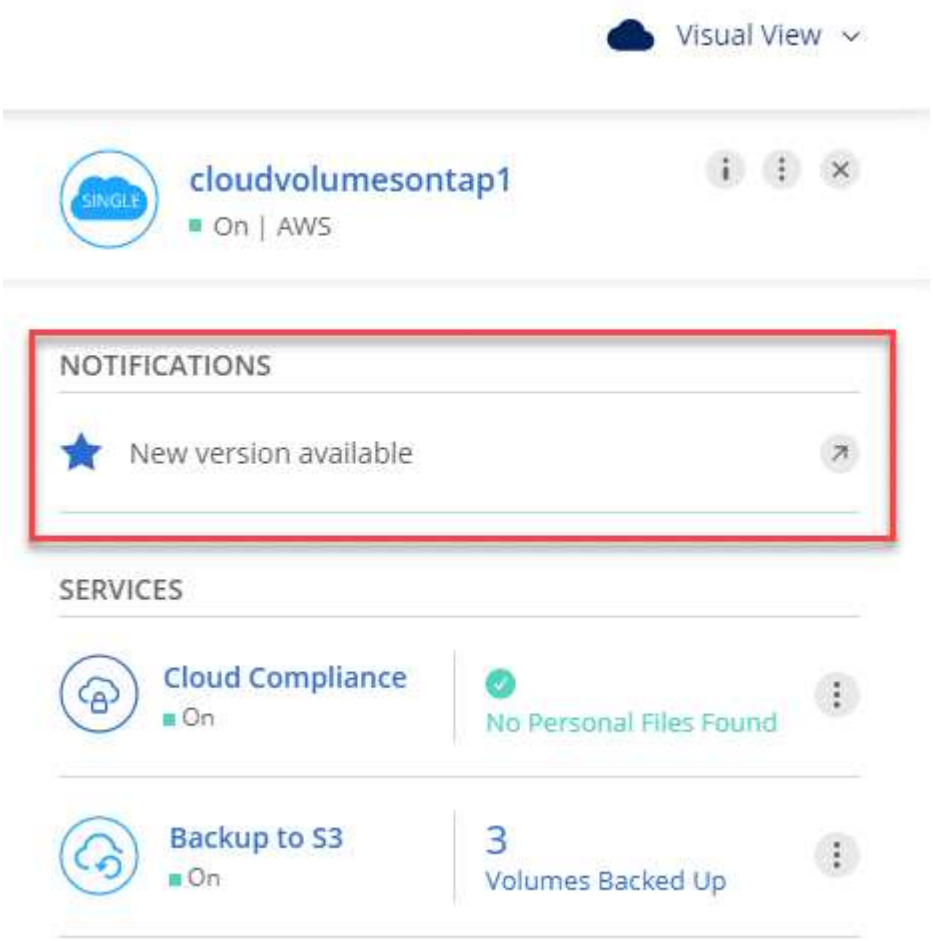
Cloud Volumes ONTAP aktualisieren oder Cloud Volumes ONTAP auf eine frühere Version herabstufen können. Sie sollten Cloud Volumes ONTAP Systeme vorbereiten, bevor Sie ein Upgrade oder Downgrade der Software durchführen.

Software-Updates müssen von Cloud Manager abgeschlossen werden

Upgrades von Cloud Volumes ONTAP müssen von Cloud Manager abgeschlossen werden. Sie sollten kein Cloud Volumes ONTAP-Upgrade mit System Manager oder der CLI durchführen. Dies kann die Stabilität des Systems beeinträchtigen.

Möglichkeiten zum Aktualisieren von Cloud Volumes ONTAP

Cloud Manager zeigt eine Benachrichtigung in den Arbeitsumgebungen von Cloud Volumes ONTAP an, wenn eine neue Version von Cloud Volumes ONTAP verfügbar ist:



Sie können den Upgrade-Prozess von dieser Benachrichtigung aus starten, die den Prozess automatisiert, indem Sie das Software-Image aus einem S3-Bucket beziehen, das Image installieren und das System dann neu starten. Weitere Informationen finden Sie unter Aktualisieren von Cloud Volumes ONTAP über Cloud Manager Benachrichtigungen.

Bei HA-Systemen in AWS kann Cloud Manager im Rahmen des Upgrades den HA-Mediator aktualisieren.

Erweiterte Optionen für Software-Updates

Cloud Manager bietet außerdem die folgenden erweiterten Optionen für die Aktualisierung der Cloud Volumes ONTAP Software:

- Software-Updates mit einem Bild auf einer externen URL

  Diese Option ist hilfreich, wenn Cloud Manager nicht auf den S3-Bucket zugreifen kann, um die Software zu aktualisieren, wenn Ihnen ein Patch zur Verfügung steht oder wenn Sie die Software auf eine bestimmte Version herunterstufen möchten.

  Weitere Informationen finden Sie unter Upgrade oder Downgrade von Cloud Volumes ONTAP mit einem HTTP- oder FTP-Server.

- Software-Updates mit dem alternativen Image auf dem System

  Mit dieser Option können Sie auf die vorherige Version zurückstufen, indem Sie das alternative Software-Image zum Standardbild machen. Diese Option ist für HA-Paare nicht verfügbar.

  Weitere Informationen finden Sie unter Downgrade von Cloud Volumes ONTAP mit einem lokalen Image.

Aktualisierung der Cloud Volumes ONTAP Software wird vorbereitet

Bevor Sie ein Upgrade oder Downgrade durchführen, müssen Sie sicherstellen, dass Ihre Systeme bereit sind, und alle erforderlichen Konfigurationsänderungen vornehmen.

- Planung von Ausfallzeiten
- Überprüfen der Versionsanforderungen
- dass das automatische Giveback weiterhin aktiviert ist
- SnapMirror Übertragungen werden ausgesetzt
- ob Aggregate online sind

Planung von Ausfallzeiten

Wenn Sie ein Single-Node-System aktualisieren, stellt der Upgrade-Prozess das System für bis zu 25 Minuten offline, während dieser I/O-Unterbrechung ausgeführt wird.

Das Upgrade eines HA-Paars erfolgt unterbrechungsfrei und die I/O wird unterbrochen. Während dieses unterbrechungsfreien Upgrade-Prozesses wird jeder Node entsprechend aktualisiert, um den I/O-Datenverkehr für die Clients weiterhin bereitzustellen.

Überprüfen der Versionsanforderungen

Die ONTAP Version, auf die Sie aktualisieren oder herunterstufen können, variiert abhängig von der Version von ONTAP, die derzeit auf Ihrem System ausgeführt wird.

Informationen zu Versionsanforderungen finden Sie unter "ONTAP 9 Dokumentation: Anforderungen für Cluster-Updates".

Es wird sichergestellt, dass das automatische Giveback weiterhin aktiviert ist

Automatisches Giveback muss auf einem Cloud Volumes ONTAP HA-Paar aktiviert sein (dies ist die Standardeinstellung). Wenn nicht, schlägt der Vorgang fehl.

"ONTAP 9 Dokumentation: Befehle zur Konfiguration von automatischem Giveback"

SnapMirror Übertragungen werden ausgesetzt

Wenn ein Cloud Volumes ONTAP System über aktive SnapMirror Beziehungen verfügt, sollten Sie die Übertragungen am besten unterbrechen, bevor Sie die Cloud Volumes ONTAP Software aktualisieren. Das Anhalten der Übertragungen verhindert SnapMirror Ausfälle. Sie müssen die Übertragungen vom Zielsystem anhalten.

Über diese Aufgabe

In diesen Schritten wird die Verwendung von System Manager für Version 9.3 und höher beschrieben.

Schritte

1. "Melden Sie sich bei System Manager an" Von dem Zielsystem stammen.
2. Klicken Sie Auf **Schutz > Beziehungen**.
3. Wählen Sie die Beziehung aus, und klicken Sie auf **Operationen > Quiesce**.

Überprüfen, ob Aggregate online sind

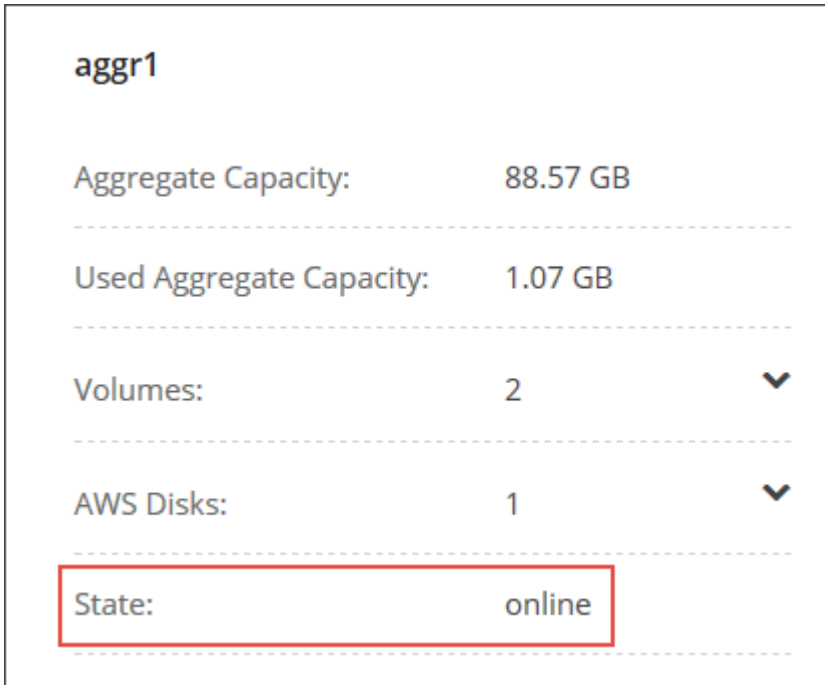
Aggregate für Cloud Volumes ONTAP muss online sein, bevor Sie die Software aktualisieren. Aggregate sollten in den meisten Konfigurationen online sein. Wenn dies nicht der Fall ist, sollten Sie sie jedoch online stellen.

Über diese Aufgabe

In diesen Schritten wird die Verwendung von System Manager für Version 9.3 und höher beschrieben.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Erweiterte Zuweisung**.
2. Wählen Sie ein Aggregat aus, klicken Sie auf **Info** und überprüfen Sie dann, ob der Status online ist.



3. Wenn das Aggregat offline ist, verwenden Sie System Manager, um das Aggregat online zu schalten:
   a. "Melden Sie sich bei System Manager an".
   b. Klicken Sie Auf **Storage > Aggregate & Disks > Aggregate**.
   c. Wählen Sie das Aggregat aus und klicken Sie dann auf **Weitere Aktionen > Status > Online**.

Aktualisieren von Cloud Volumes ONTAP über Cloud Manager Benachrichtigungen

Cloud Manager benachrichtigt Sie, wenn eine neue Version von Cloud Volumes ONTAP verfügbar ist. Klicken Sie auf die Benachrichtigung, um den Aktualisierungsprozess zu starten.

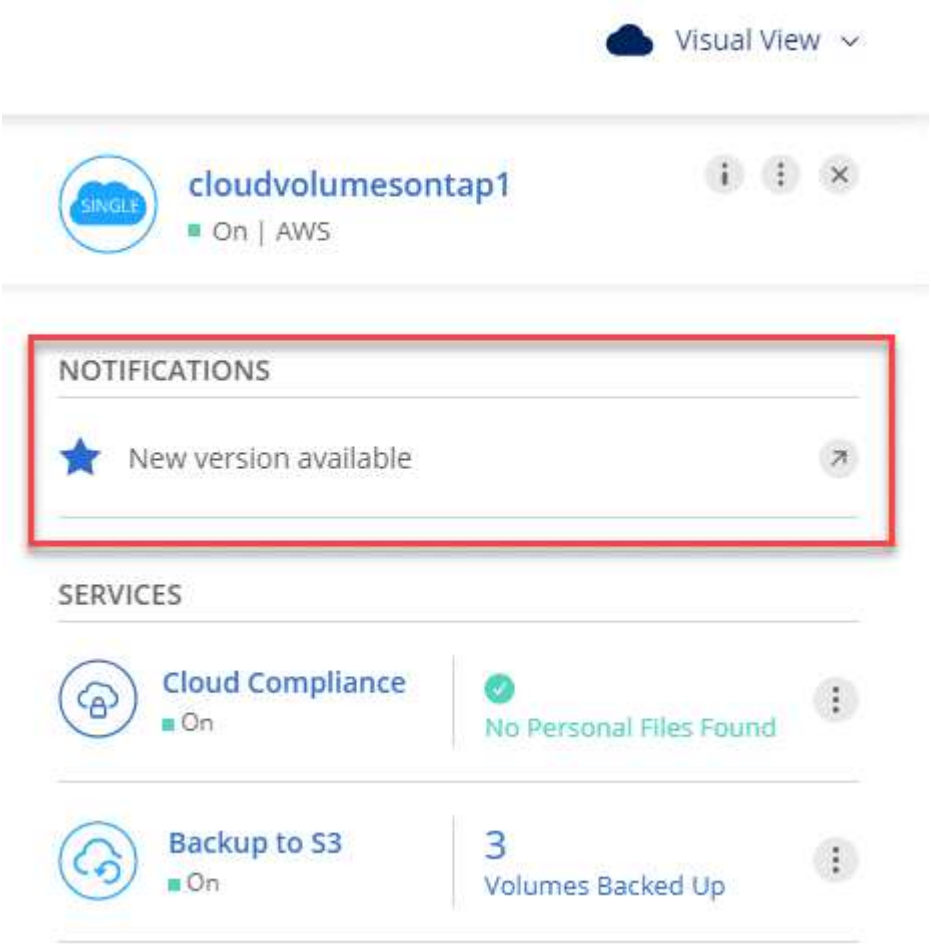
Bevor Sie beginnen

Cloud Manager-Vorgänge wie die Erstellung von Volumes oder Aggregaten dürfen für das Cloud Volumes ONTAP System nicht ausgeführt werden.

Schritte

1. Klicken Sie Auf **Arbeitsumgebungen**.
2. Wählen Sie eine Arbeitsumgebung aus.

   Im rechten Fensterbereich wird eine Benachrichtigung angezeigt, wenn eine neue Version verfügbar ist:



3. Wenn eine neue Version verfügbar ist, klicken Sie auf **Upgrade**.

4. Klicken Sie auf der Seite Release Information auf den Link, um die Versionshinweise für die angegebene Version zu lesen, und aktivieren Sie dann das Kontrollkästchen **Ich habe gelesen…**.
5. Lesen Sie auf der Seite Endbenutzer-Lizenzvereinbarung (EULA) die EULA, und wählen Sie dann **Ich habe die EULA gelesen und genehmigt**.
6. Lesen Sie auf der Seite Prüfen und genehmigen die wichtigen Hinweise, wählen Sie **Ich verstehe…** und klicken Sie dann auf **Go**.

Ergebnis

Cloud Manager startet das Software-Upgrade. Nach Abschluss der Softwareaktualisierung können Sie in der Arbeitsumgebung Aktionen ausführen.

Nachdem Sie fertig sind

Wenn Sie SnapMirror Transfers ausgesetzt haben, setzen Sie die Transfers mit System Manager fort.

Upgrade oder Downgrade von Cloud Volumes ONTAP mit einem HTTP- oder FTP-Server

Sie können das Cloud Volumes ONTAP Software-Image auf einem HTTP- oder FTP-Server platzieren und dann das Software-Update über Cloud Manager starten. Sie können diese Option verwenden, wenn Cloud Manager nicht auf den S3-Bucket zugreifen kann, um die Software zu aktualisieren, oder wenn Sie ein Downgrade der Software durchführen möchten.

Schritte

1. Richten Sie einen HTTP-Server oder FTP-Server ein, der das Cloud Volumes ONTAP Software-Image hosten kann.
2. Wenn Sie eine VPN-Verbindung zum virtuellen Netzwerk haben, können Sie das Cloud Volumes ONTAP Software-Image auf einem HTTP-Server oder FTP-Server in Ihrem eigenen Netzwerk platzieren. Andernfalls müssen Sie die Datei auf einem HTTP-Server oder FTP-Server in der Cloud platzieren.
3. Wenn Sie Ihre eigene Sicherheitsgruppe für Cloud Volumes ONTAP verwenden, stellen Sie sicher, dass die Outbound-Regeln HTTP- oder FTP-Verbindungen zulassen, damit Cloud Volumes ONTAP auf das Software-Image zugreifen kann.

   Die vordefinierte Sicherheitsgruppe Cloud Volumes ONTAP ermöglicht standardmäßig ausgehende HTTP- und FTP-Verbindungen.

4. Beziehen Sie das Software-Image von "Die NetApp Support Site".
5. Kopieren Sie das Software-Image in das Verzeichnis auf dem HTTP- oder FTP-Server, von dem die Datei bereitgestellt wird.
6. Klicken Sie in der Arbeitsumgebung des Cloud Managers auf das Menü-Symbol und dann auf **Erweitert > Cloud Volumes ONTAP aktualisieren**.
7. Wählen Sie auf der Seite Aktualisierungssoftware **Wählen Sie ein Bild aus einer URL** aus, geben Sie die URL ein und klicken Sie dann auf **Bild ändern**.
8. Klicken Sie zur Bestätigung auf **Weiter**.

Ergebnis

Cloud Manager startet das Softwareupdate. Nach Abschluss der Softwareaktualisierung können Sie in der Arbeitsumgebung Aktionen ausführen.

Nachdem Sie fertig sind

Wenn Sie SnapMirror Transfers ausgesetzt haben, setzen Sie die Transfers mit System Manager fort.

Downgrade von Cloud Volumes ONTAP mit einem lokalen Image

Der Wechsel von Cloud Volumes ONTAP auf eine frühere Version derselben Versionsfamilie (beispielsweise 9.5 bis 9.4) wird als Downgrade bezeichnet. Sie können ein Downgrade ohne Unterstützung durchführen, wenn Sie neue Cluster oder Testcluster herunterstufen möchten. Wenden Sie sich jedoch an den technischen Support, wenn Sie ein Downgrade eines Produktionsclusters durchführen möchten.

Jedes Cloud Volumes ONTAP System kann zwei Software-Images enthalten: Das aktuelle Image, das ausgeführt wird, und ein alternatives Image, das Sie booten können. Cloud Manager kann das alternative Bild als Standardbild ändern. Mit dieser Option können Sie auf die vorherige Version von Cloud Volumes ONTAP zurückstufen, wenn Probleme mit dem aktuellen Image auftreten.

Über diese Aufgabe

Dieser Downgrade-Prozess ist nur für einzelne Cloud Volumes ONTAP Systeme verfügbar. Es ist nicht für HA-Paare verfügbar.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Cloud Volumes ONTAP aktualisieren**.
2. Wählen Sie auf der Seite Aktualisierungssoftware das alternative Bild aus und klicken Sie dann auf **Bild ändern**.
3. Klicken Sie zur Bestätigung auf **Weiter**.

Ergebnis

Cloud Manager startet das Softwareupdate. Nach Abschluss der Softwareaktualisierung können Sie in der Arbeitsumgebung Aktionen ausführen.

Nachdem Sie fertig sind

Wenn Sie SnapMirror Transfers ausgesetzt haben, setzen Sie die Transfers mit System Manager fort.

Ändern von Cloud Volumes ONTAP Systemen

Möglicherweise müssen Sie die Konfiguration von Cloud Volumes ONTAP-Systemen ändern, wenn sich Ihre Storage-Anforderungen ändern. Sie können beispielsweise zwischen nutzungsbasierten Konfigurationen wechseln, den Instanz- oder VM-Typ ändern und vieles mehr.

Ändern des Instanz- oder Maschinentyps für Cloud Volumes ONTAP

Bei der Einführung von Cloud Volumes ONTAP in AWS, Azure oder GCP können Sie zwischen verschiedenen Instanzen oder Maschinentypen wählen. Sie können den Instanz- oder Maschinentyp jederzeit ändern, wenn Sie feststellen, dass er für Ihre Anforderungen unterdimensioniert oder überdimensioniert ist.

Über diese Aufgabe

- Automatisches Giveback muss auf einem Cloud Volumes ONTAP HA-Paar aktiviert sein (dies ist die Standardeinstellung). Wenn nicht, schlägt der Vorgang fehl.

  "ONTAP 9 Dokumentation: Befehle zur Konfiguration von automatischem Giveback"

- Eine Änderung des Instanz- oder Maschinentyps wirkt sich auf die Servicegebühren von Cloud-Providern aus.

- Der Vorgang startet Cloud Volumes ONTAP neu.

  Bei Systemen mit einem Node wird die I/O unterbrochen.

  Bei HA-Paaren ist die Änderung unterbrechungsfrei. Ha-Paare stellen weiterhin Daten bereit.

Cloud Manager ändert den Node nach dem anderen ordnungsgemäß, indem es Takeover und Warten auf Giveback initiiert. Das QA-Team von NetApp testete während dieses Prozesses sowohl das Schreiben als auch das Lesen der Dateien und sah keine Probleme auf Kundenseite. Wenn sich die Verbindungen änderten, wurden Wiederholungen auf I/O-Ebene gesehen, aber die Applikationsebene übergab diese kurze „Re-Wire“ der NFS/CIFS-Verbindungen.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Lizenz oder Instanz ändern** für AWS, **Lizenz ändern oder VM** für Azure oder **Lizenz oder Rechner ändern** für GCP.
2. Wenn Sie eine nutzungsbasierte Konfiguration verwenden, können Sie optional eine andere Lizenz auswählen.
3. Wählen Sie eine Instanz oder einen Maschinentyp aus, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Auswirkungen der Änderung verstehen, und klicken Sie dann auf **OK**.

Ergebnis

Cloud Volumes ONTAP wird mit der neuen Konfiguration neu gestartet.

Wechsel zwischen nutzungsbasierten Konfigurationen

Nachdem Sie Pay-as-you-go Cloud Volumes ONTAP Systeme gestartet haben, können Sie jederzeit zwischen den Konfigurationen Explore, Standard und Premium wechseln, indem Sie die Lizenz ändern. Das Ändern der Lizenz erhöht oder verringert die Obergrenze für die Rohkapazität und ermöglicht die Auswahl aus verschiedenen AWS Instanztypen oder Azure Virtual Machine-Typen.

In GCP ist für jede Pay-as-you-go-Konfiguration ein einziger Maschinentyp verfügbar. Sie können nicht zwischen verschiedenen Maschinentypen wählen.

Über diese Aufgabe

Beachten Sie Folgendes, um zwischen nutzungsbasierten Lizenzen zu wechseln:

- Der Vorgang startet Cloud Volumes ONTAP neu.

  Bei Systemen mit einem Node wird die I/O unterbrochen.

  Bei HA-Paaren ist die Änderung unterbrechungsfrei. Ha-Paare stellen weiterhin Daten bereit.

- Eine Änderung des Instanz- oder Maschinentyps wirkt sich auf die Servicegebühren von Cloud-Providern aus.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Lizenz oder Instanz ändern** für AWS, **Lizenz ändern oder VM** für Azure oder **Lizenz oder Rechner ändern** für GCP.
2. Wählen Sie einen Lizenztyp und einen Instanztyp oder Maschinentyp aus, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Auswirkungen der Änderung verstehen, und klicken Sie

dann auf **OK**.

Ergebnis

Cloud Volumes ONTAP wird mit der neuen Lizenz, dem Instanztyp oder dem Maschinentyp oder beides neu gebootet.

Wechsel zu einer alternativen Cloud Volumes ONTAP Konfiguration

Wenn Sie zwischen einem Pay-as-you-go-Abonnement und einem BYOL-Abonnement oder zwischen einem einzelnen Cloud Volumes ONTAP System und einem HA-Paar wechseln möchten, müssen Sie ein neues System implementieren und anschließend Daten aus dem vorhandenen System in das neue System replizieren.

Schritte

1. Erstellen Sie eine neue Cloud Volumes ONTAP Arbeitsumgebung.

   "Starten von Cloud Volumes ONTAP in AWS"
   "Starten von Cloud Volumes ONTAP in Azure"
   "Einführung von Cloud Volumes ONTAP in GCP"

2. "Einmalige Datenreplizierung einrichten" Zwischen den Systemen für jedes zu replizierende Volume wechseln.
3. Beenden Sie das Cloud Volumes ONTAP System, das Sie von nicht mehr benötigen "Die ursprüngliche Arbeitsumgebung wird gelöscht".

Ändern der Schreibgeschwindigkeit auf „Normal“ oder „hoch“

Mit Cloud Manager können Sie eine Einstellung für die Schreibgeschwindigkeit für Cloud Volumes ONTAP Systeme mit einem Node wählen. Die standardmäßige Schreibgeschwindigkeit ist normal. Wenn für Ihren Workload eine hohe Schreib-Performance erforderlich ist, kann die hohe Schreibgeschwindigkeit geändert werden. Bevor Sie die Schreibgeschwindigkeit ändern, sollten Sie dies tun "Die Unterschiede zwischen den normalen und den hohen Einstellungen verstehen".

Über diese Aufgabe

- Stellen Sie sicher, dass Vorgänge wie die Volume- oder Aggregaterstellung nicht ausgeführt werden.
- Beachten Sie, dass durch diese Änderung Cloud Volumes ONTAP neu gestartet wird, was bedeutet, dass I/O unterbrochen wird.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Schreibgeschwindigkeit**.
2. Wählen Sie **normal** oder **hoch**.

   Wenn Sie „hoch“ wählen, müssen Sie die „Ich verstehe…“-Aussage lesen und bestätigen, indem Sie das Kästchen aktivieren.

3. Klicken Sie auf **Speichern**, überprüfen Sie die Bestätigungsmeldung und klicken Sie dann auf **Weiter**.

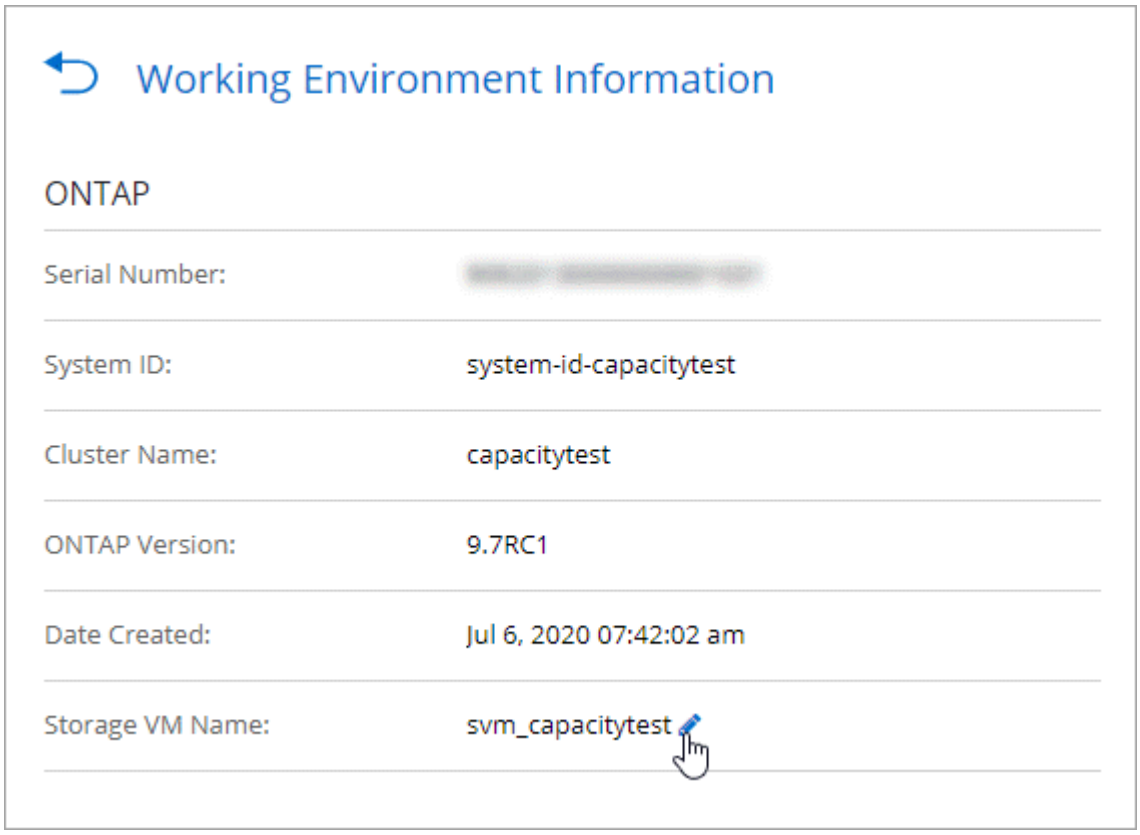
Ändern des Namens der Storage-VM

Cloud Manager benennt automatisch die einzelne Storage-VM (SVM), die für Cloud Volumes ONTAP erstellt wird. Sie können den Namen der SVM ändern, wenn Sie strenge Benennungsstandards haben. Beispielsweise sollte der Name Ihnen entsprechen, wie Sie die SVMs für Ihre ONTAP Cluster benennen.

Wenn Sie aber zusätzliche SVMs für Cloud Volumes ONTAP erstellen, können Sie die SVMs nicht aus Cloud Manager umbenennen. Sie müssen dies direkt von Cloud Volumes ONTAP mit System Manager oder der CLI ausführen.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Information**.
2. Klicken Sie rechts neben dem Namen der Storage-VM auf das Bearbeiten-Symbol.



3. Ändern Sie im Dialogfeld SVM-Name ändern den Namen und klicken Sie dann auf **Speichern**.

Ändern des Passworts für Cloud Volumes ONTAP

Cloud Volumes ONTAP enthält ein Cluster-Administratorkonto. Sie können das Kennwort für dieses Konto bei Bedarf über Cloud Manager ändern.

Sie sollten das Kennwort für das Administratorkonto nicht über System Manager oder die CLI ändern. Das Kennwort wird nicht in Cloud Manager angezeigt. Daher kann Cloud Manager die Instanz nicht ordnungsgemäß überwachen.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Passwort festlegen**.
2. Geben Sie das neue Passwort zweimal ein und klicken Sie dann auf **Speichern**.

   Das neue Kennwort muss sich von einem der letzten sechs Kennwörter unterscheiden.

Ändern der Netzwerk-MTU für c4.4xlarge und c4.8xlarge Instanzen

Standardmäßig ist Cloud Volumes ONTAP so konfiguriert, dass 9.000 MTU (auch Jumbo Frames genannt) verwendet werden, wenn Sie die c4.4xlarge Instanz oder die c4.8xlarge Instanz in AWS auswählen. Sie können die Netzwerk-MTU auf 1.500 Byte ändern, wenn dies für Ihre Netzwerkkonfiguration besser geeignet ist.

Über diese Aufgabe

Eine maximale Netzwerkübertragungseinheit (Maximum Transmission Unit, MTU) von 9.000 Byte bietet den höchstmöglichen Netzwerkdurchsatz für bestimmte Konfigurationen.

9.000 MTU ist eine gute Wahl, wenn Clients in demselben VPC mit dem Cloud Volumes ONTAP System kommunizieren und einige oder alle dieser Clients ebenfalls 9.000 MTU unterstützen. Wenn der Datenverkehr den VPC verlässt, kann es zu einer Paketfragmentierung kommen, die die Performance beeinträchtigt.

Eine Netzwerk-MTU von 1.500 Byte ist eine gute Wahl, wenn Clients oder Systeme außerhalb des VPC mit dem Cloud Volumes ONTAP System kommunizieren.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Netzwerknutzung**.
2. Wählen Sie **Standard** oder **Jumbo Frames**.
3. Klicken Sie Auf **Ändern**.

Ändern von Routingtabellen im Zusammenhang mit HA-Paaren in mehreren AWS AZS

Sie können die AWS-Routing-Tabellen mit Routen zu den unverankerten IP-Adressen für ein HA-Paar ändern. Vielleicht möchten Sie dies tun, wenn neue NFS- oder CIFS-Clients auf ein HA-Paar in AWS zugreifen müssen.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Information**.
2. Klicken Sie Auf **Routentabellen**.
3. Ändern Sie die Liste der ausgewählten Routentabellen und klicken Sie dann auf **Speichern**.

Ergebnis

Cloud Manager sendet eine AWS-Anforderung zum Ändern der Routentabellen.

Managen des Status von Cloud Volumes ONTAP

Sie können Cloud Volumes ONTAP über Cloud Manager anhalten und starten, um Ihre Cloud-Computing-Kosten zu managen.

Planen automatischer Abschaltungen von Cloud Volumes ONTAP

Sie sollten Cloud Volumes ONTAP in bestimmten Zeitintervallen herunterfahren, um Ihre Computing-Kosten zu senken. Statt dies manuell zu tun, können Sie Cloud Manager so konfigurieren, dass Systeme automatisch heruntergefahren und dann zu bestimmten Zeiten neu gestartet werden.

Über diese Aufgabe

Wenn Sie einen automatischen Shutdown des Cloud Volumes ONTAP Systems planen, verschiebt Cloud Manager das Herunterfahren vor, wenn ein aktiver Datentransfer stattfinden soll. Cloud Manager schaltet das

System nach Abschluss der Übertragung aus.

Diese Aufgabe plant das automatische Herunterfahren beider Nodes in einem HA-Paar.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Uhrsymbol:

2. Geben Sie den Zeitplan für das Herunterfahren an:

   a. Wählen Sie aus, ob Sie das System täglich, jeden Werktag, jedes Wochenende oder eine beliebige Kombination der drei Optionen herunterfahren möchten.

   b. Geben Sie an, wann und wie lange das System ausgeschaltet werden soll.

      Beispiel

      Die folgende Abbildung zeigt einen Zeitplan, in dem Cloud Manager angewiesen wird, das System jeden Samstag um 24:00 Uhr auszuschalten Für 48 Stunden. Cloud Manager startet das System jeden Montag um 12:00 Uhr neu

3. Klicken Sie Auf **Speichern**.

Ergebnis

Cloud Manager speichert den Zeitplan. Das Uhrensymbol ändert sich, um anzuzeigen, dass ein Zeitplan festgelegt wurde: 

Beenden von Cloud Volumes ONTAP

Stoppen von Cloud Volumes ONTAP erspart Ihnen das Ansteigen von Computing-Kosten und erstellt Snapshots der Root- und Boot-Festplatten, was bei der Fehlerbehebung hilfreich sein kann.

Über diese Aufgabe

Wenn Sie ein HA-Paar anhalten, fährt Cloud Manager beide Nodes herunter.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Symbol **Ausschalten**.

2. Behalten Sie die Option zum Erstellen von Snapshots aktiviert bei, da die Snapshots die System-Recovery ermöglichen können.
3. Klicken Sie Auf **Ausschalten**.

   Es kann bis zu einigen Minuten dauern, bis das System gestoppt wird. Sie können Systeme zu einem späteren Zeitpunkt von der Seite "Arbeitsumgebung" aus neu starten.

Überwachung der AWS-Ressourcenkosten

Mit Cloud Manager können Sie die Ressourcenkosten anzeigen, die mit der Ausführung von Cloud Volumes ONTAP in AWS verbunden sind. Außerdem erfahren Sie, wie viel Geld Sie durch den Einsatz von NetApp Funktionen zur Senkung der Storage-Kosten gespart haben.

Über diese Aufgabe

Cloud Manager aktualisiert die Kosten bei Aktualisierung der Seite. Die endgültigen Kostendetails finden Sie in AWS.

Schritt

1. Stellen Sie sicher, dass Cloud Manager Kosteninformationen von AWS beziehen kann:
   a. Vergewissern Sie sich, dass die IAM-Richtlinie, die Cloud Manager über Berechtigungen verfügt, die folgenden Aktionen umfasst:

      ```
      "ce:GetReservationUtilization",
      "ce:GetDimensionValues",
      "ce:GetCostAndUsage",
      "ce:GetTags"
      ```

      Diese Aktionen sind in den letzten enthalten "Cloud Manager-Richtlinie". Neue Systeme, die von NetApp Cloud Central implementiert werden, enthalten automatisch diese Berechtigungen.

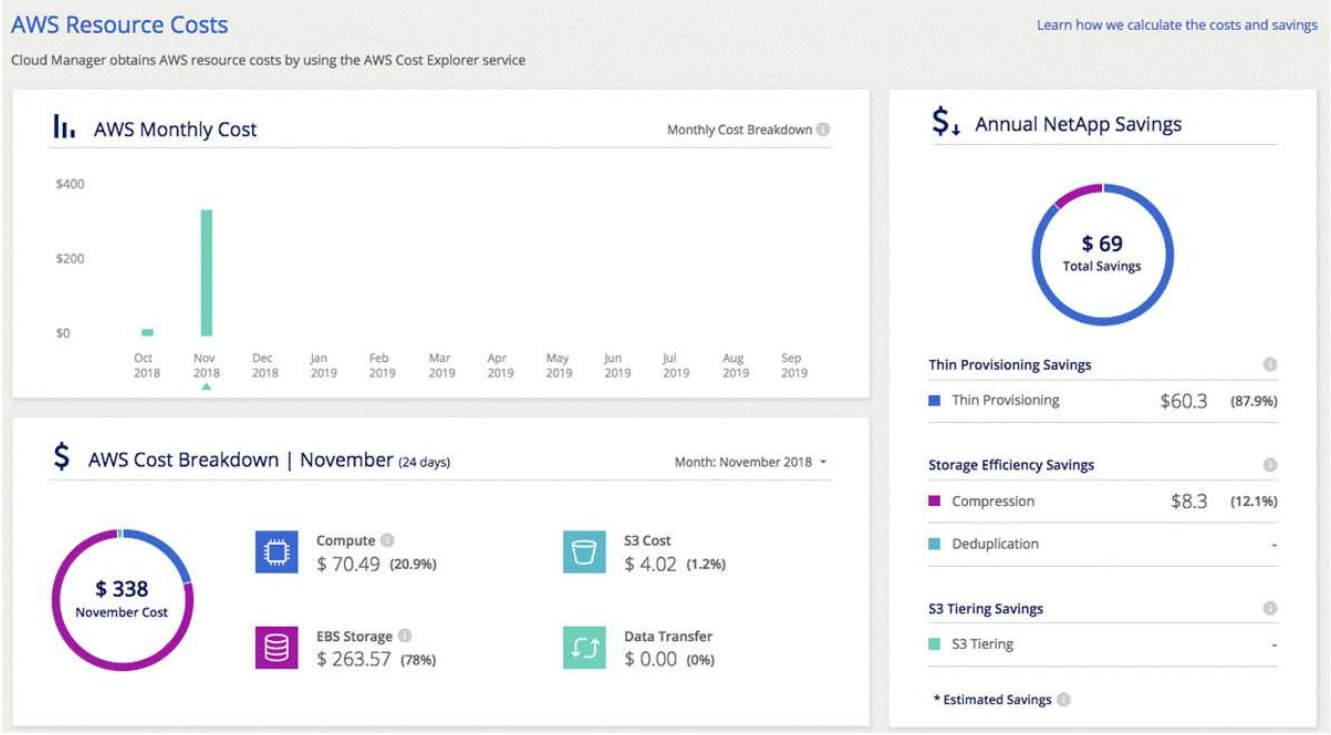
   b. "Aktivieren Sie das Tag **WorkingEnvironment ID**".

      Um die AWS-Kosten zu verfolgen, weist Cloud Manager Cloud Volumes ONTAP Instanzen ein Tag der Kostenzuteilung zu. Nachdem Sie Ihre erste Arbeitsumgebung erstellt haben, aktivieren Sie das Tag **WorkingEnvironment ID**. Benutzerdefinierte Tags werden erst in den AWS Abrechnungsberichten angezeigt, wenn Sie sie in der Konsole „Rechnungsstellung“ und „Kostenmanagement“ aktivieren.

2. Wählen Sie auf der Seite Arbeitsumgebungen eine Cloud Volumes ONTAP Arbeitsumgebung aus und klicken Sie dann auf **Kosten**.

   Auf der Kostenseite werden die Kosten für die aktuelle und die vorherigen Monate angezeigt sowie Ihre jährlichen NetApp Einsparungen angezeigt, wenn Sie die kostensparenden Funktionen von NetApp auf den Volumes aktiviert haben.

   Das folgende Bild zeigt eine Beispiel-Kostenseite:



Verbindung zu Cloud Volumes ONTAP

Wenn Sie ein erweitertes Management von Cloud Volumes ONTAP durchführen müssen, können Sie dies mit OnCommand System Manager oder der Befehlszeilenoberfläche tun.

Verbindung mit System Manager wird hergestellt

Möglicherweise müssen Sie einige Cloud Volumes ONTAP-Aufgaben aus System Manager ausführen. Hierbei handelt es sich um ein Browser-basiertes Managementtool, das auf dem Cloud Volumes ONTAP System ausgeführt wird. Sie müssen beispielsweise System Manager verwenden, wenn Sie LUNs erstellen möchten.

Bevor Sie beginnen

Der Computer, von dem aus Sie auf Cloud Manager zugreifen, muss über eine Netzwerkverbindung zu Cloud Volumes ONTAP verfügen. Sie müssen sich beispielsweise von einem Jump Host in AWS oder Azure bei Cloud Manager anmelden.

> Bei der Implementierung in mehreren AWS Availability Zones verwenden Cloud Volumes ONTAP HA-Konfigurationen eine Floating-IP-Adresse für die Cluster-Management-Schnittstelle, was bedeutet, dass externes Routing nicht verfügbar ist. Sie müssen eine Verbindung von einem Host herstellen, der Teil derselben Routingdomäne ist.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsumgebungen auf das Cloud Volumes ONTAP System, das Sie mit System Manager managen möchten.
2. Klicken Sie auf das Menüsymbol und dann auf **Erweitert > System Manager**.
3. Klicken Sie Auf **Start**.

   System Manager wird in eine neue Browser-Registerkarte geladen.

4. Geben Sie im Anmeldebildschirm im Feld Benutzername * das Passwort ein, das Sie beim Erstellen der Arbeitsumgebung angegeben haben, und klicken Sie dann auf **Anmelden**.

Ergebnis

Die System Manager-Konsole wird geladen. Sie können es jetzt zum Managen von Cloud Volumes ONTAP verwenden.

Herstellen einer Verbindung zur Cloud Volumes ONTAP CLI

Die Cloud Volumes ONTAP CLI ermöglicht Ihnen die Ausführung aller administrativen Befehle und ist eine gute Wahl für erweiterte Aufgaben oder wenn Sie sich mit der CLI besser vertraut machen. Sie können über Secure Shell (SSH) eine Verbindung zur CLI herstellen.

Bevor Sie beginnen

Der Host, von dem aus Sie SSH für die Verbindung zu Cloud Volumes ONTAP verwenden, muss über eine Netzwerkverbindung zu Cloud Volumes ONTAP verfügen. Sie müssen beispielsweise SSH von einem Jump Host in AWS oder Azure verwenden.

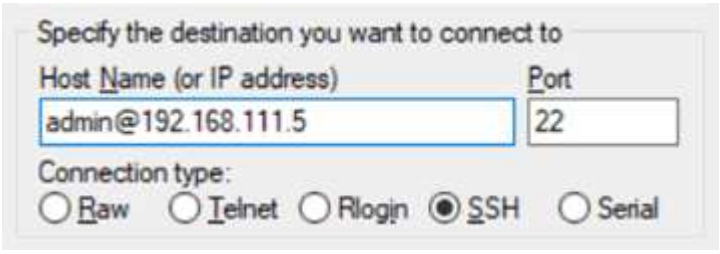
Wenn Cloud Volumes ONTAP HA in mehreren AZS implementiert wird, verwenden sie eine Floating-IP-Adresse für die Cluster-Management-Schnittstelle, was bedeutet, dass externes Routing nicht verfügbar ist. Sie müssen eine Verbindung von einem Host herstellen, der Teil derselben Routingdomäne ist.

Schritte

1. Identifizieren Sie in Cloud Manager die IP-Adresse der Cluster-Management-Schnittstelle:
   a. Wählen Sie auf der Seite Arbeitsumgebungen das Cloud Volumes ONTAP System aus.
   b. Kopieren Sie die IP-Adresse der Clusterverwaltung, die im rechten Fensterbereich angezeigt wird.
2. Verwenden Sie SSH, um über das Administratorkonto eine Verbindung zur IP-Adresse der Cluster-Managementschnittstelle herzustellen.

   Beispiel

   Das folgende Bild zeigt ein Beispiel mit PuTTY:



3. Geben Sie an der Anmeldeaufforderung das Kennwort für das Administratorkonto ein.

   Beispiel

```
Password: ********
COT2::>
```

Hinzufügen vorhandener Cloud Volumes ONTAP Systeme zu Cloud Manager

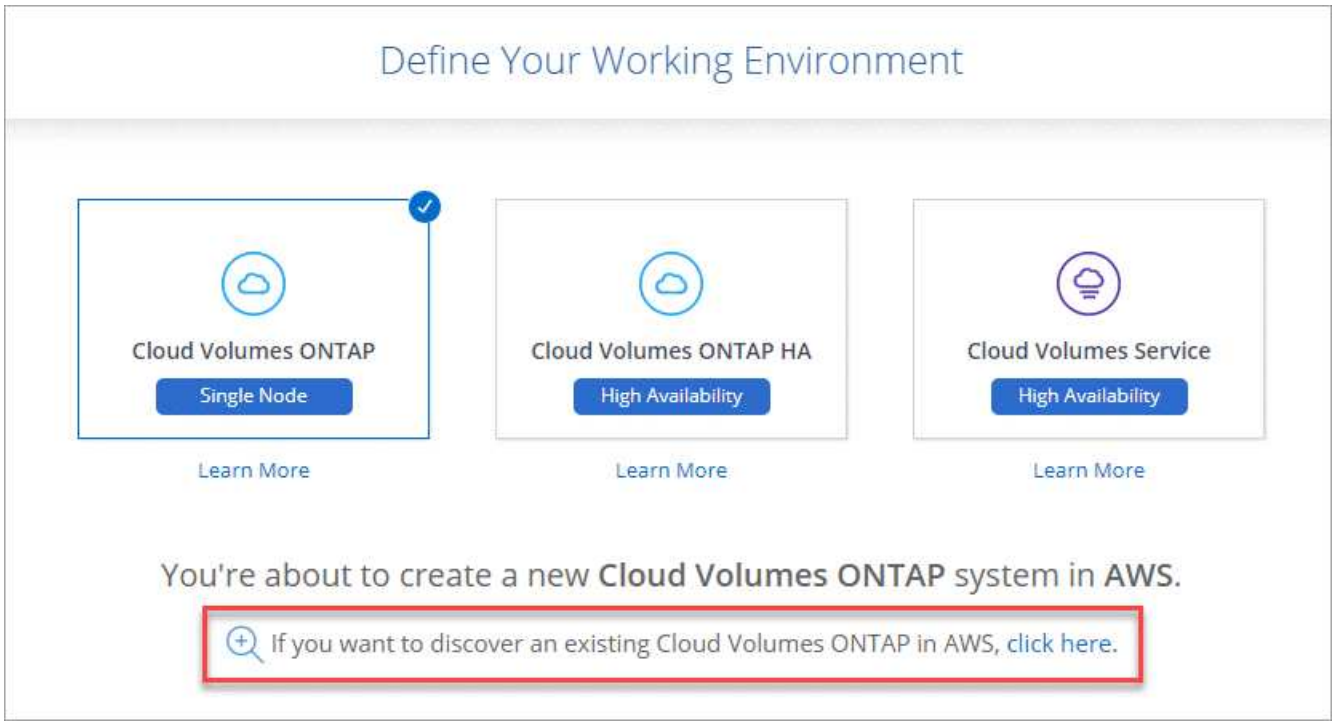
Sie können vorhandene Cloud Volumes ONTAP Systeme erkennen und zu Cloud Manager hinzufügen. Das könnte Sie erreichen, wenn Sie ein neues Cloud Manager System implementieren.

Bevor Sie beginnen

Sie müssen das Kennwort für das Cloud Volumes ONTAP Admin-Benutzerkonto kennen.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen**.
2. Wählen Sie den Cloud-Provider aus, in dem sich das System befindet.
3. Wählen Sie den Typ des Cloud Volumes ONTAP Systems aus.
4. Klicken Sie auf den Link, um ein vorhandenes System zu ermitteln.



5. Wählen Sie auf der Seite Region den Bereich aus, in dem die Instanzen ausgeführt werden, und wählen Sie dann die Instanzen aus.
6. Geben Sie auf der Seite Anmeldeinformationen das Kennwort für den Cloud Volumes ONTAP-Admin-Benutzer ein, und klicken Sie dann auf **Los**.

Ergebnis

Cloud Manager fügt den Arbeitsbereich die Cloud Volumes ONTAP-Instanzen hinzu.

Löschen einer Cloud Volumes ONTAP Arbeitsumgebung

Am besten löschen Sie die Cloud Volumes ONTAP Systeme aus dem Cloud Manager, nicht jedoch von der Konsole Ihres Cloud-Providers. Wenn Sie beispielsweise eine lizenzierte Cloud Volumes ONTAP-Instanz von AWS beenden, können Sie den

Lizenzschlüssel für eine andere Instanz nicht verwenden. Sie müssen die Arbeitsumgebung aus Cloud Manager löschen, um die Lizenz freizugeben.

Über diese Aufgabe

Wenn Sie eine Arbeitsumgebung löschen, beendet Cloud Manager Instanzen, löscht Festplatten und Snapshots.

> Cloud Volumes ONTAP Instanzen verfügen über einen aktivierten Kündigungsschutz, um eine versehentliche Beendigung von AWS zu verhindern. Wenn Sie jedoch eine Cloud Volumes ONTAP Instanz von AWS beenden, müssen Sie zur Konsole AWS CloudFormation wechseln und den Stack der Instanz löschen. Der Stack-Name ist der Name der Arbeitsumgebung.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Löschen**.
2. Geben Sie den Namen der Arbeitsumgebung ein und klicken Sie dann auf **Löschen**.

   Das Löschen der Arbeitsumgebung kann bis zu 5 Minuten dauern.

Stellen Sie Volumes über einen Fileservice bereit

Azure NetApp Dateien

Weitere Informationen zu Azure NetApp Files

Mit Azure NetApp Files können Unternehmen ihre Performance-intensiven und latenzkritischen Core-Applikationen in Azure migrieren und ausführen, ohne für die Cloud einen Refactoring durchführen zu müssen.

Funktionen

- Da mehrere Protokolle unterstützt werden, kann das „Lift and Shift“ von Linux- und Windows-Applikationen nahtlos in Azure ausgeführt werden.
- Mehrere Performance-Tiers ermöglichen eine enge Ausrichtung an den Workload-Performance-Anforderungen.
- Führende Zertifizierungen wie SAP HANA, DSGVO und HIPPA ermöglichen die Migration der anspruchsvollsten Workloads zu Azure.

Zusätzliche Funktionen in Cloud Manager

- Migrieren Sie NFS- oder SMB-Daten direkt aus Cloud Manager zu Azure NetApp Files. Datenmigrationen sind durch den NetApp Cloud Sync Service möglich. "Weitere Informationen .".
- Mithilfe von künstlicher Intelligenz (KI) hilft Cloud Compliance Ihnen dabei, den Datenkontext zu verstehen und sensible Daten in Ihren Azure NetApp Files-Konten zu identifizieren. "Weitere Informationen .".

Kosten

"Informieren Sie sich über die Preise für Azure NetApp Files".

Beachten Sie, dass das Abonnement und die Abrechnung über den Azure NetApp Files Service erfolgen und nicht durch Cloud Manager.

Unterstützte Regionen

"Unterstützte Azure Regionen anzeigen".

Zugriff wird angefordert

Sie müssen von Zugriff auf Azure NetApp Files erhalten "Einreichung einer Online-Anfrage". Sie müssen das Azure NetApp Files-Team erst dann auf die Genehmigung warten, bevor Sie fortfahren können.

Hilfe wird abgerufen

Bei Problemen mit dem technischen Support im Zusammenhang mit Azure NetApp Files können Sie im Azure-Portal eine Support-Anfrage an Microsoft protokollieren. Wählen Sie Ihr zugehöriges Microsoft-Abonnement aus, und wählen Sie den **Azure NetApp Files**-Dienstnamen unter **Speicherung** aus. Geben Sie die verbleibenden Informationen an, die für die Erstellung Ihrer Microsoft Support-Anfrage erforderlich sind.

Bei Problemen mit Cloud Sync und Azure NetApp Files können Sie mit NetApp direkt über den Cloud Sync Service mit Ihrer Cloud Sync Seriennummer beginnen. Sie müssen über den Link in Cloud Manager auf den

Cloud Sync Service zugreifen. "Prozess zum Aktivieren des Cloud Sync Supports anzeigen".

Weiterführende Links

- "NetApp Cloud Central: Azure NetApp Files"
- "Azure NetApp Files-Dokumentation"
- "Cloud Sync-Dokumentation"

Einrichtung von Azure NetApp Files

Azure NetApp Files-Arbeitsumgebung in Cloud Manager erstellen und managen – NetApp Kunden, Kapazitätspools, Volumes und Snapshots

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

Zugriff anfordern

"Online-Anforderung einreichen" Zugriff auf Azure NetApp Files zu erhalten.

Richten Sie eine Azure AD-Applikation ein

Von Azure erteilen Sie Berechtigungen für eine Azure AD-Applikation und kopieren Sie die Anwendungs-ID (Client), die Verzeichnis- (Mandanten-)ID und den Wert eines Clientgeheimnisses.

Schaffung einer Azure NetApp Files-Arbeitsumgebung

Klicken Sie im Cloud Manager auf **Arbeitsumgebung hinzufügen** > **Microsoft Azure** > **Azure NetApp Files** und geben Sie dann Details zur AD-Anwendung an.

Zugriff wird angefordert

Sie müssen von Zugriff auf Azure NetApp Files erhalten "Einreichung einer Online-Anfrage". Sie müssen das Azure NetApp Files-Team erst dann auf die Genehmigung warten, bevor Sie fortfahren können.

Einrichten einer Azure AD-Applikation

Cloud Manager benötigt Berechtigungen für die Einrichtung und das Management von Azure NetApp Files. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie eine Azure AD-Applikation erstellen und einrichten, und die von Cloud Manager benötigten Azure Zugangsdaten erhalten.

Erstellen der AD-Anwendung

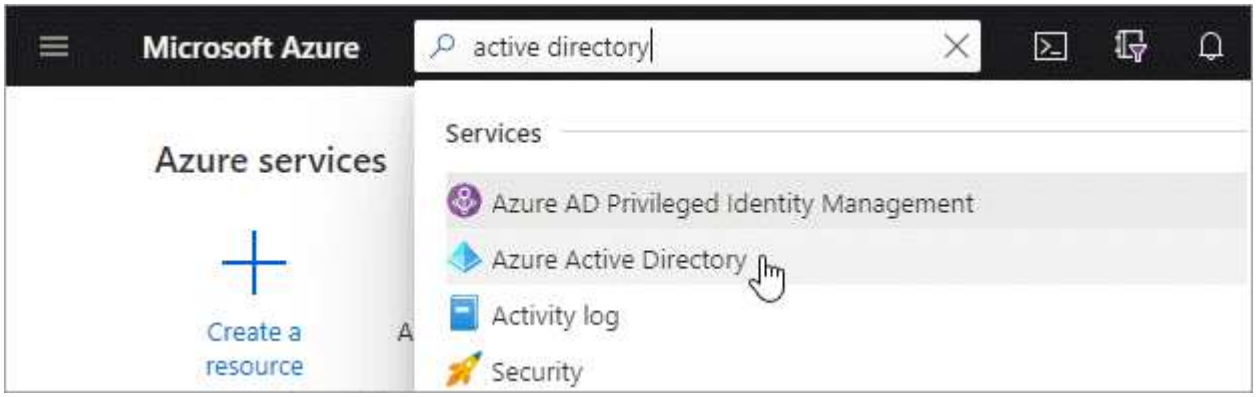
Erstellen einer Azure Active Directory (AD)-Applikation und eines Service-Principal, den Cloud Manager für die rollenbasierte Zugriffssteuerung nutzen kann

Bevor Sie beginnen

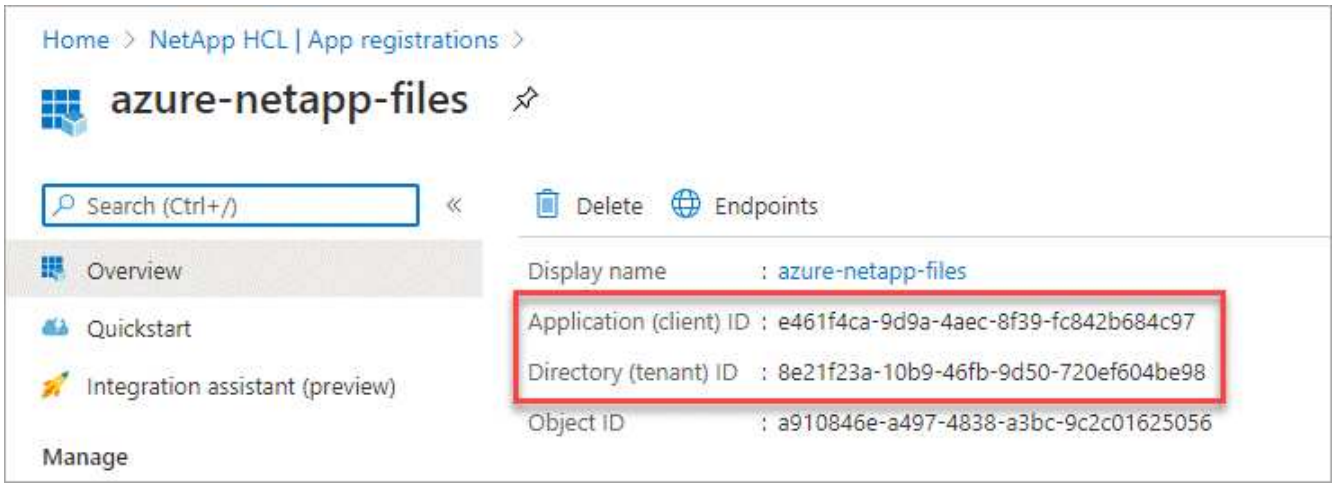
Sie müssen über die richtigen Berechtigungen in Azure verfügen, um eine Active Directory-Anwendung zu erstellen und die Anwendung einer Rolle zuzuweisen. Weitere Informationen finden Sie unter "Microsoft Azure-Dokumentation: Erforderliche Berechtigungen".

Schritte

1. Öffnen Sie über das Azure-Portal den **Azure Active Directory**-Service.



2. Klicken Sie im Menü auf **App-Registrierungen**.
3. Anwendung erstellen:
   a. Klicken Sie auf **Neue Registrierung**.
   b. Geben Sie Details zur Anwendung an:
      - **Name**: Geben Sie einen Namen für die Anwendung ein.
      - **Kontotyp**: Wählen Sie einen Kontotyp aus (jeder funktioniert mit Cloud Manager).
      - **Redirect URI**: Sie können diesen leer lassen.
   c. Klicken Sie Auf **Registrieren**.
4. Kopieren Sie die **Application (Client) ID** und die **Directory (Tenant) ID**.



Wenn Sie die Azure NetApp Files Arbeitsumgebung in Cloud Manager erstellen, müssen Sie die Applikations- (Client)-ID und die Verzeichnis- (Mandanten-)ID für die Applikation angeben. Cloud Manager verwendet die IDs, um sich programmatisch anzumelden.

5. Erstellen eines Client-Geheimnisses für die Applikation, damit Cloud Manager sie zur Authentifizierung mit

Azure AD verwenden kann:

a. Klicken Sie auf **Zertifikate & Geheimnisse > Neuer Client Secret**.

b. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.

c. Klicken Sie Auf **Hinzufügen**.

d. Kopieren Sie den Wert des Clientgeheimnisses.

Ergebnis

Ihre AD-Anwendung ist jetzt eingerichtet und Sie sollten die Anwendungs-ID (Client), die Verzeichnis- (Mandanten-) ID und den Wert des Clientgeheimnisses kopiert haben. Sie müssen diese Informationen in Cloud Manager eingeben, wenn Sie eine Azure NetApp Files Arbeitsumgebung hinzufügen.

Anwendung einer Rolle zuweisen

Sie müssen den Service-Principal an Ihr Azure-Abonnement binden und ihm eine benutzerdefinierte Rolle zuweisen, die über die erforderlichen Berechtigungen verfügt.

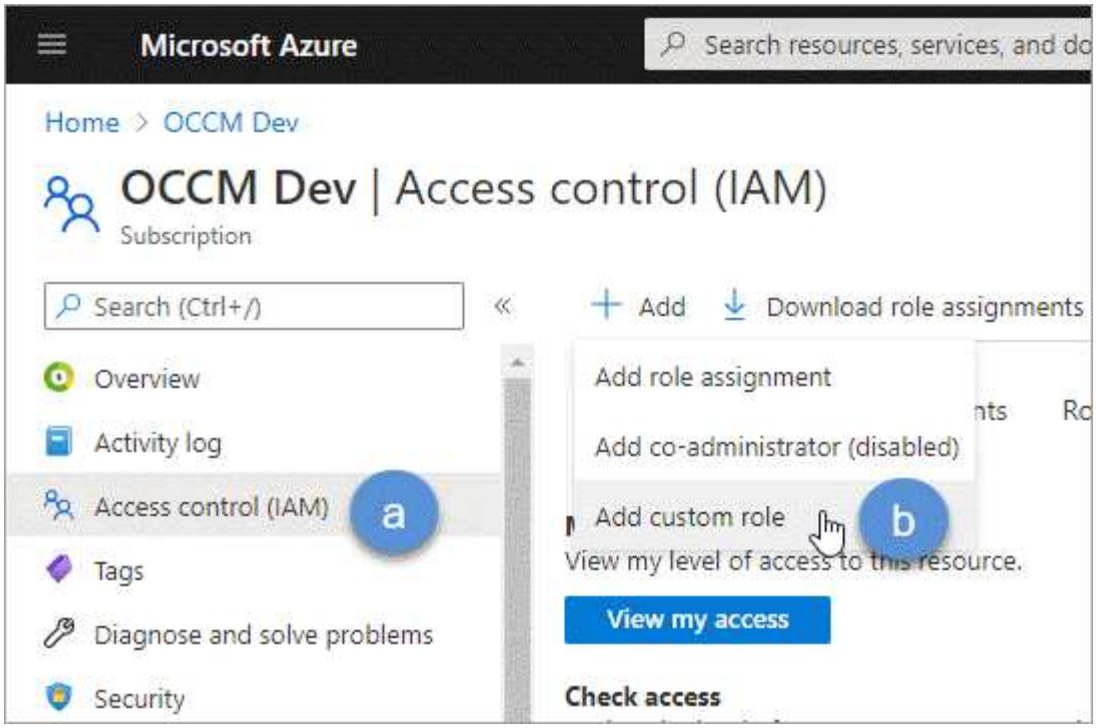
Schritte

1. "Erstellen einer benutzerdefinierten Rolle in Azure".

   In den folgenden Schritten wird beschrieben, wie die Rolle aus dem Azure-Portal erstellt wird.

   a. Öffnen Sie das Abonnement und klicken Sie auf **Access Control (IAM)**.

   b. Klicken Sie auf **Hinzufügen > Benutzerdefinierte Rolle hinzufügen**.



c. Geben Sie auf der Registerkarte **Grundlagen** einen Namen und eine Beschreibung für die Rolle ein.

d. Klicken Sie auf **JSON** und klicken Sie auf **Bearbeiten**, das oben rechts im JSON-Format angezeigt wird.

e. Fügen Sie unter *Actions* die folgenden Berechtigungen hinzu:

```
"actions": [
    "Microsoft.NetApp/*",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Insights/Metrics/Read"
    ],
```

f. Klicken Sie auf **Speichern**, klicken Sie auf **Weiter** und dann auf **Erstellen**.

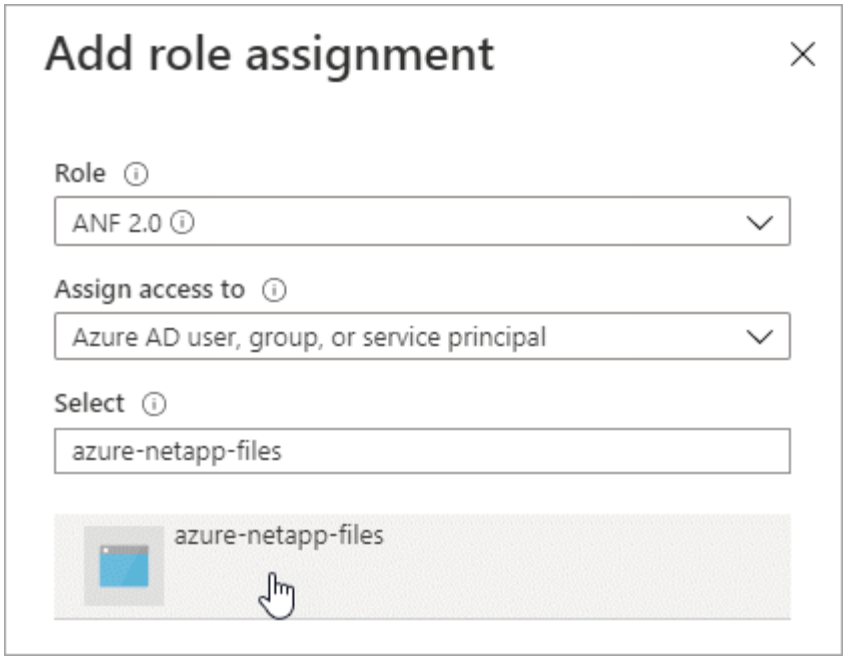
2. Weisen Sie nun die Anwendung der gerade erstellten Rolle zu:

a. Öffnen Sie im Azure-Portal das Abonnement und klicken Sie auf **Access Control (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.

b. Wählen Sie die benutzerdefinierte Rolle aus, die Sie erstellt haben.

c. * Azure AD Benutzer, Gruppe oder Serviceprincipal* ausgewählt lassen.

d. Suchen Sie nach dem Namen der Anwendung (Sie finden sie nicht in der Liste durch Scrollen).



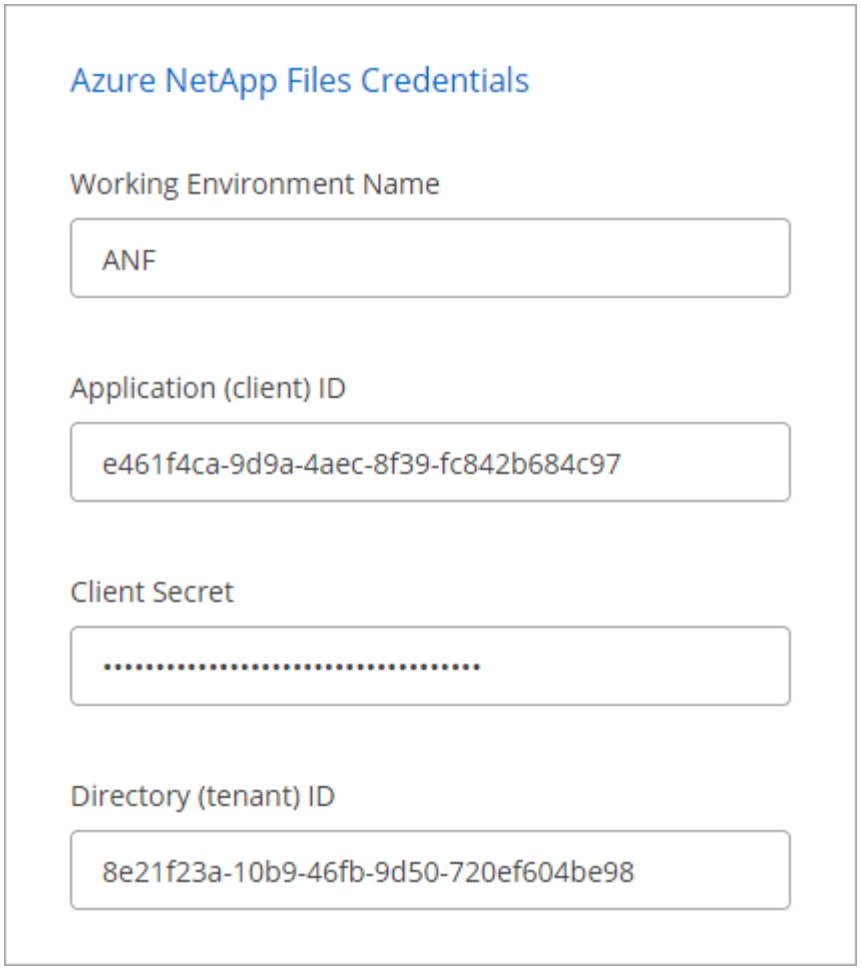
e. Wählen Sie die Anwendung aus und klicken Sie auf **Speichern**.

   Der Service Principal für den Cloud Manager verfügt jetzt über die erforderlichen Azure Berechtigungen für das Abonnement.

Erstellen einer Azure NetApp Files-Arbeitsumgebung

Richten Sie in Cloud Manager eine Azure NetApp Files-Arbeitsumgebung ein, in der Sie Volumes erstellen können.

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen**.
2. Wählen Sie **Microsoft Azure** und dann **Azure NetApp Files**.
3. Stellen Sie Details zur AD-Anwendung bereit, die Sie zuvor eingerichtet haben.



4. Klicken Sie Auf **Hinzufügen**.

Ergebnis

Sie sollten nun über eine Azure NetApp Files-Arbeitsumgebung verfügen.

Was kommt als Nächstes?

"Beginnen Sie mit dem Erstellen und Managen von Volumes".

Erstellen und Verwalten von Volumes für Azure NetApp Files

Nach der Einrichtung der Arbeitsumgebung können Azure NetApp Files Konten, Kapazitäts-Pools, Volumes und Snapshots erstellt und gemanagt werden.

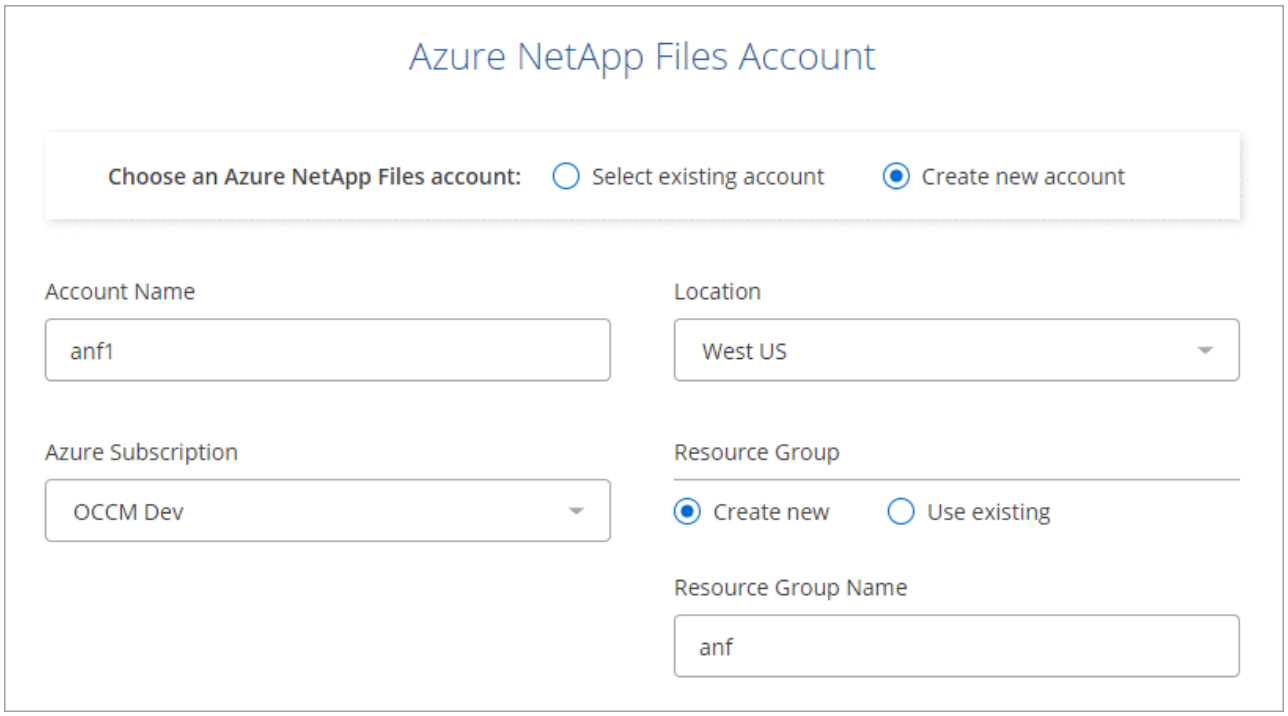
Volumes werden erstellt

NFS- oder SMB-Volumes können in einem neuen oder vorhandenen Azure NetApp Files-Konto erstellt werden.

Schritte

1. Öffnen Sie die Azure NetApp Files-Arbeitsumgebung.
2. Klicken Sie Auf **Neues Volume Hinzufügen**.
3. Geben Sie die erforderlichen Informationen auf den einzelnen Seiten an:

   - **Azure NetApp Files-Konto**: Wählen Sie ein bestehendes Azure NetApp Files-Konto oder erstellen Sie ein neues Konto.



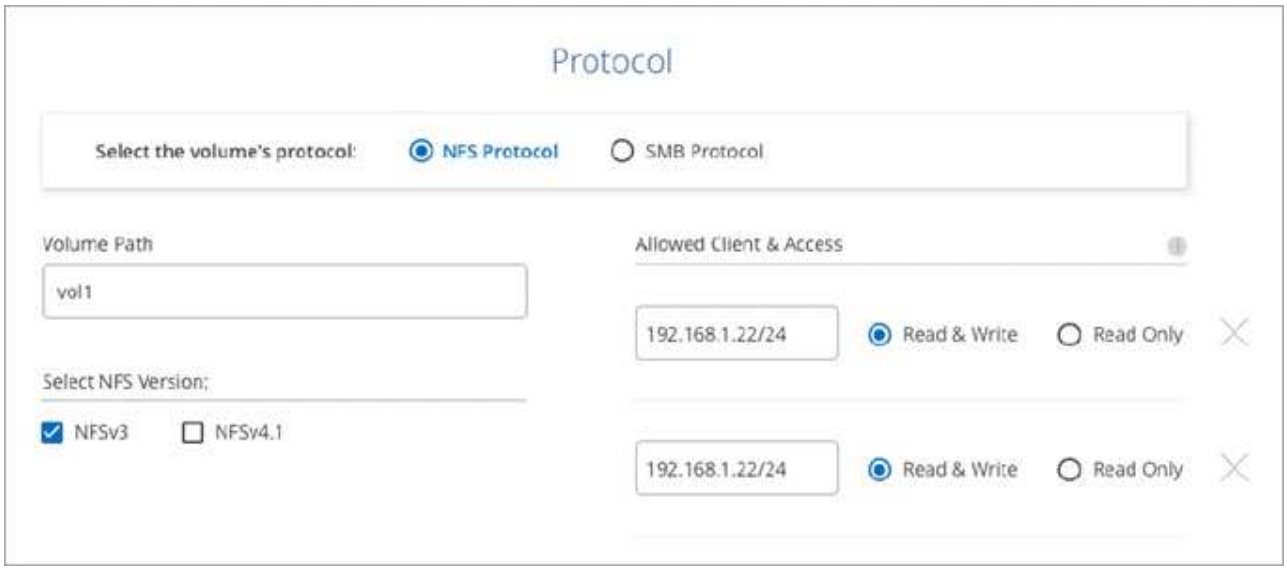
   - **Kapazitäts-Pool**: Wählen Sie einen vorhandenen Kapazitäts-Pool aus oder erstellen Sie einen neuen Kapazitäts-Pool.

     Wenn Sie einen neuen Kapazitätspool erstellen, müssen Sie eine Größe angeben und ein auswählen "Service-Level".

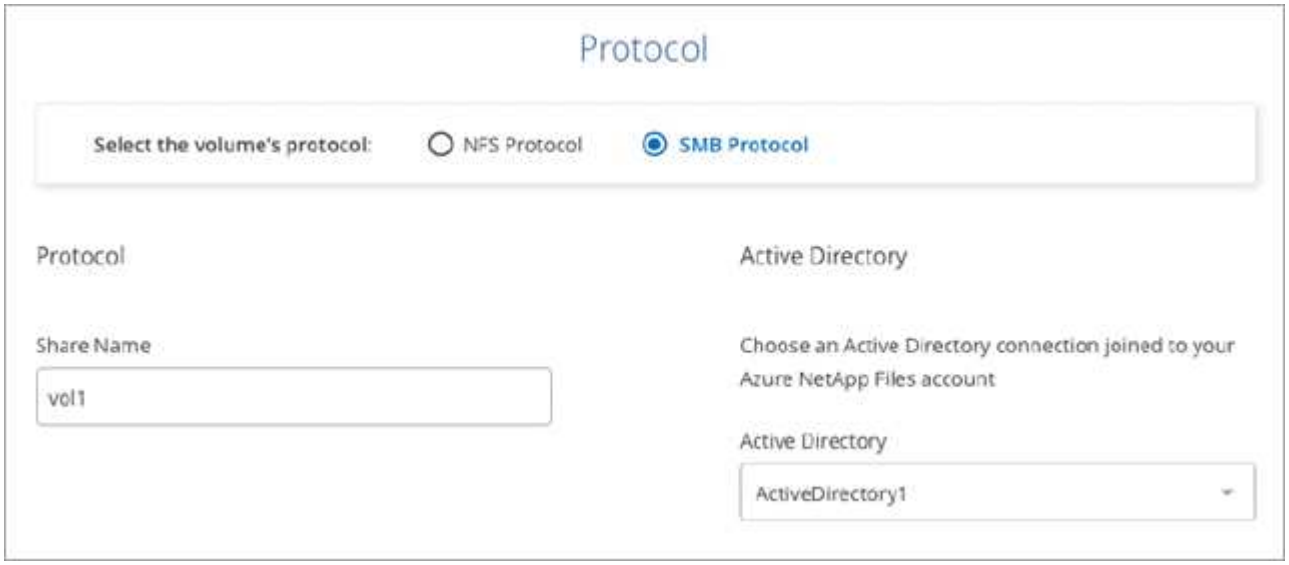
     Die Mindestgröße für den Kapazitäts-Pool beträgt 4 TB. Sie können eine Größe in einem Vielfachen von 4 TB angeben.

   - **Details & Tags**: Geben Sie einen Namen und Größe des Datenträgers, vnet und Subnetz ein, in dem sich das Volume befinden soll, und geben Sie optional Tags für das Volume an.
   - **Protokoll**: Wählen Sie das NFS- oder SMB-Protokoll und geben Sie die erforderlichen Informationen ein.

     Dies ist ein Beispiel für die Details für NFS.



Dies ist ein Beispiel für Details für SMB. Sie müssen Active Directory-Informationen bereitstellen, wenn Sie Ihr erstes SMB-Volume einrichten.



4. Klicken Sie Auf **Volumen Hinzufügen**.

Montage der Volumen

Sie können das Volume in einem Cloud Manager mounten und auf einem Host zugreifen, indem Sie die Anweisungen im Anschluss nehmen.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über die Lautstärke, und wählen Sie **Mounten Sie die Lautstärke**.

3. Befolgen Sie die Anweisungen zum Montieren des Volumens.

Größe und Tags eines Volumes werden bearbeitet

Nachdem Sie ein Volume erstellt haben, können Sie dessen Größe und Tags jederzeit ändern.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über die Lautstärke und wählen Sie **Bearbeiten**.
3. Ändern Sie die Größe und die Tags nach Bedarf.
4. Klicken Sie Auf **Anwenden**.

Verwalten von Snapshot Kopien

Snapshot Kopien erstellen eine zeitpunktgenaue Kopie des Volume. Erstellen Sie Snapshot Kopien, stellen Sie die Daten in einem neuen Volume wieder her und löschen Sie Snapshot Kopien.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über das Volume und wählen Sie eine der verfügbaren Optionen zum Managen von Snapshot Kopien aus:
   - **Erstellen Sie eine Snapshot Kopie**
   - **Wiederherstellen auf einem neuen Volume**
   - **Löschen einer Snapshot Kopie**
3. Befolgen Sie die Anweisungen, um die ausgewählte Aktion abzuschließen.

Volumes werden gelöscht

Löschen Sie die Volumes, die Sie nicht mehr benötigen.

Schritte

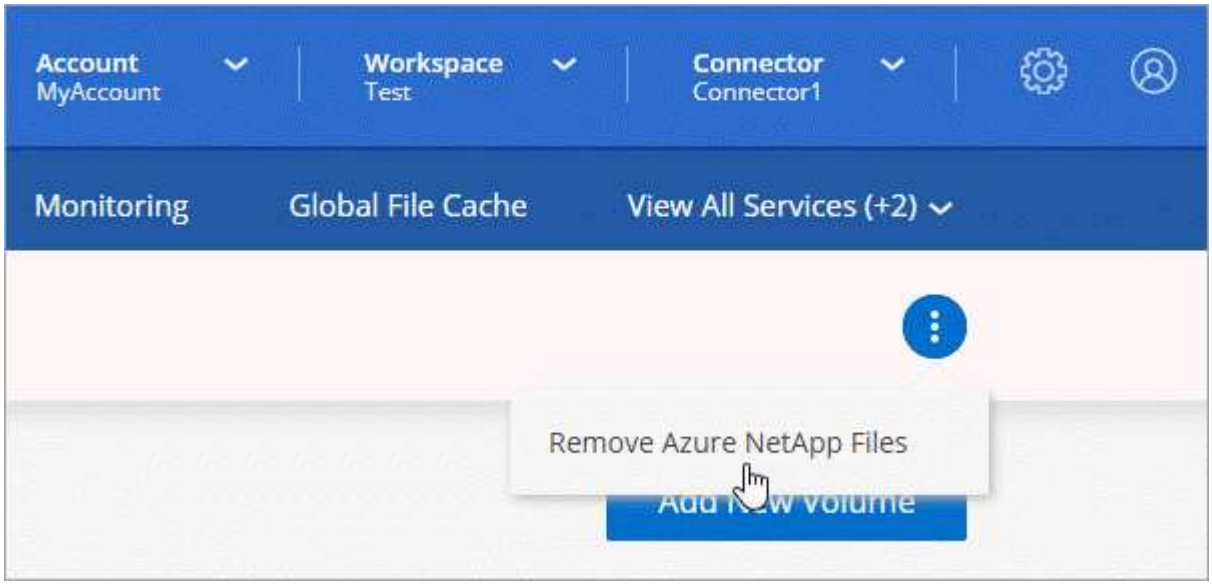
1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über die Lautstärke und klicken Sie auf **Löschen**.
3. Bestätigen Sie, dass Sie das Volume löschen möchten.

Azure NetApp Files wird entfernt

Durch diese Aktion wird Azure NetApp Files aus Cloud Manager entfernt. Ihr Azure NetApp Files-Konto oder Ihre Volumes werden nicht gelöscht. Sie können Azure NetApp Files jederzeit wieder zu Cloud Manager hinzufügen.

Schritte

1. Öffnen Sie die Azure NetApp Files-Arbeitsumgebung.
2. Wählen Sie oben rechts auf der Seite das Menü Aktionen aus und klicken Sie auf **Azure NetApp Files entfernen**.



3. Klicken Sie zur Bestätigung auf **Entfernen**.

Cloud Volumes Service für AWS

Weitere Informationen zu Cloud Volumes Service für AWS

NetApp Cloud Volumes Service für AWS ist ein Cloud-nativer Fileservice, der NAS-Volumes über NFS und SMB mit All-Flash-Performance bereitstellt. Dieser Service ermöglicht die Ausführung aller Workloads, auch älterer Applikationen, in der AWS Cloud.

Vorteile der Nutzung von Cloud Volumes Service für AWS

Cloud Volumes Service für AWS bietet folgende Vorteile:

- Vollständig gemanagter Service – Sie müssen daher keine Storage-Geräte konfigurieren oder managen
- Unterstützung für die NAS-Protokolle NFSv3 und NFSv4.1 sowie SMB 3.0 und 3.1.1
- Sicherer Zugriff auf Linux- und Windows Elastic Container Service (ECS)-Instanzen mit Unterstützung wie:
  - Amazon Linux 2, Red hat Enterprise Linux 7.5, SLES 12 SP3 und Ubuntu 16.04 LTS
  - Windows Server 2008 R2, Windows Server 2012 R2 und Windows Server 2016
- Optionen für Pakete und Pay-as-you-go-Preise

Kosten

Von der Cloud Volumes Service für AWS erstellte Volumes werden auf Grundlage Ihres Abonnements für den Service und nicht über Cloud Manager berechnet.

Es sind keine Kosten für die Entdeckung einer Region oder eines Volumens von Cloud Volumes Service für AWS durch Cloud Manager anfallen.

Bevor Sie beginnen

- Cloud Manager kann vorhandene Cloud Volumes Service für AWS Abonnements und Volumes erkennen. Siehe "NetApp Cloud Volumes Service für AWS – Account Setup Guide" Wenn Sie Ihr Abonnement noch nicht eingerichtet haben. Dieser Einrichtungsvorgang ist für jede Region erforderlich, bevor Sie die AWS-Abonnements und -Volumes in Cloud Manager hinzufügen können.
- Sie benötigen den API-Schlüssel und den geheimen Schlüssel von Cloud Volumes, damit Sie sie an Cloud Manager bereitstellen können. "Weitere Anweisungen finden Sie in der Dokumentation zu AWS in Cloud Volumes Service".

Schnellstart

Führen Sie die Schritte schnell durch, oder rufen Sie den nächsten Abschnitt auf, um weitere Einzelheiten zu erfahren.

Überprüfen Sie die Unterstützung Ihrer Konfiguration

Sie haben AWS für Cloud Volumes Service eingerichtet und müssen einen der abonniert haben "NetApp Cloud Volumes Service-Angebote im AWS Marketplace".

Fügen Sie Ihr Abonnement für Cloud Volumes Service für AWS hinzu

Sie müssen eine Arbeitsumgebung für Volumes erstellen, die auf Ihrem Cloud Volumes Service für AWS Abonnement basiert.

Cloud Volumes erstellen

Cloud Volumes, die bereits für dieses Abonnement vorhanden sind, werden in der neuen Arbeitsumgebung angezeigt. Andernfalls erstellen Sie neue Volumes aus Cloud Manager.

Cloud Volume mounten

Binden Sie neue Cloud Volumes in Ihre AWS Instanz ein, damit Benutzer den Storage verwenden können.

Hilfe wird abgerufen

Nutzen Sie den Cloud Manager Chat für allgemeine Servicefragen.

Bei technischen Support-Problemen im Zusammenhang mit Ihren Cloud Volumes verwenden Sie die 20-stellige Seriennummer „930“ auf der Registerkarte „Support“ der Cloud Volumes Service-Benutzeroberfläche.

Verwenden Sie diese Support-ID, wenn Sie ein Web-Ticket öffnen oder Support-Anfrage stellen. Achten Sie darauf, Ihre Cloud Volumes Service Seriennummer für Support über die Cloud Volumes Service Benutzeroberfläche zu aktivieren. "Diese Schritte werden hier erläutert".

Einschränkungen

- Cloud Manager unterstützt bei der Verwendung von Cloud Volumes Service Volumes keine Datenreplizierung zwischen Arbeitsumgebungen.
- Das Entfernen des Cloud Volumes Service für AWS Abonnements aus Cloud Manager wird nicht unterstützt. Dies ist nur über die Schnittstelle Cloud Volumes Service für AWS möglich.

Weiterführende Links

- "NetApp Cloud Central: Cloud Volumes Service für AWS"
- "NetApp Cloud Volumes Service für AWS – Dokumentation"

Management von Cloud Volumes Service für AWS

Mit Cloud Manager können Sie Cloud Volumes auf Basis Ihres erstellen "Cloud Volumes Service für AWS" Abonnement: Sie können auch Cloud Volumes erkennen, die Sie bereits über die Cloud Volumes Service-Schnittstelle erstellt haben, und sie einer Arbeitsumgebung hinzufügen.

Fügen Sie Ihr Abonnement für Cloud Volumes Service für AWS hinzu

Unabhängig davon, ob Sie bereits Volumes über die Benutzeroberfläche von Cloud Volumes Service erstellt haben oder ob Sie sich gerade für Cloud Volumes Service für AWS angemeldet haben und noch keine Volumes haben, müssen Sie im ersten Schritt eine Arbeitsumgebung für die Volumes erstellen, die auf Ihrem AWS Abonnement basiert.

Wenn bereits Cloud Volumes für dieses Abonnement vorhanden sind, werden die Volumes automatisch zur neuen Arbeitsumgebung hinzugefügt. Wenn Sie noch keine Cloud Volumes für das AWS Abonnement hinzugefügt haben, gehen Sie nach der Erstellung der neuen Arbeitsumgebung vor.

Wenn Sie über Abonnements und Volumes in mehreren AWS Regionen verfügen, müssen Sie diese Aufgabe für jede Region ausführen.

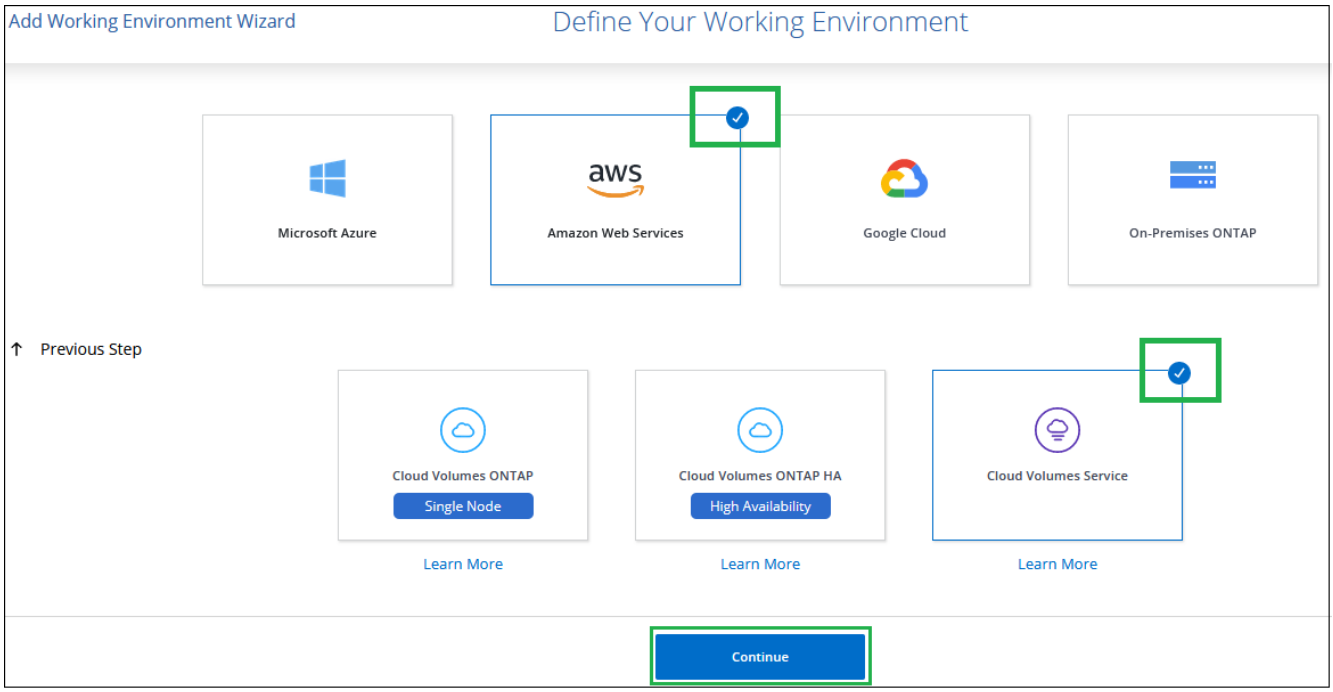
Bevor Sie beginnen

Wenn Sie in jeder Region ein Abonnement hinzufügen, müssen Sie über die folgenden Informationen verfügen:

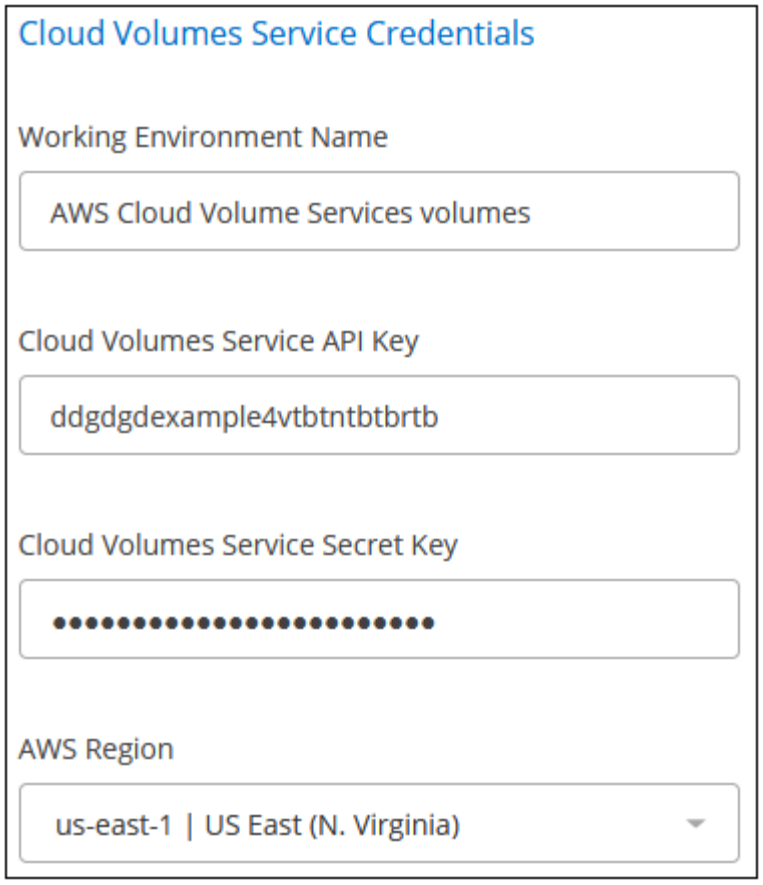
- Cloud Volumes API-Schlüssel und geheimer Schlüssel: "In der Dokumentation zu Cloud Volumes Service für AWS erhalten Sie diese Informationen".
- Der Region AWS, in der das Abonnement erstellt wurde.

Schritte

1. Fügen Sie in Cloud Manager eine neue Arbeitsumgebung hinzu, wählen Sie den Standort **Amazon Web Services** und klicken Sie auf **Weiter**.
2. Wählen Sie **Cloud Volumes Service** und klicken Sie auf **Weiter**.

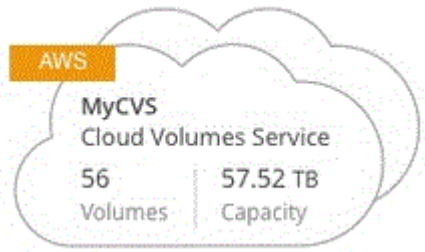


3. Stellen Sie Informationen zu Ihrem Cloud Volumes Service Abonnement bereit:
   a. Geben Sie den Namen der Arbeitsumgebung ein, den Sie verwenden möchten.
   b. Geben Sie den Cloud Volumes Service-API-Schlüssel und den geheimen Schlüssel ein.
   c. Wählen Sie die Region von AWS aus, in der sich Ihre Cloud Volumes befinden oder wo sie implementiert werden sollen.
   d. Klicken Sie Auf **Hinzufügen**.



Ergebnis

In Cloud Manager wird die Konfiguration von Cloud Volumes Service für AWS auf der Seite Arbeitsumgebungen angezeigt.



Wenn Cloud Volumes bereits für dieses Abonnement vorhanden sind, werden die Volumes automatisch der neuen Arbeitsumgebung hinzugefügt, wie im Screenshot dargestellt. Sie können weitere Cloud Volumes über Cloud Manager hinzufügen.

Wenn für dieses Abonnement keine Cloud Volumes vorhanden sind, können Sie sie jetzt erstellen.

Cloud Volumes erstellen

Für Konfigurationen, bei denen Volumes bereits in der Cloud Volumes Service-Arbeitsumgebung vorhanden sind, können Sie mit diesen Schritten neue Volumes hinzufügen.

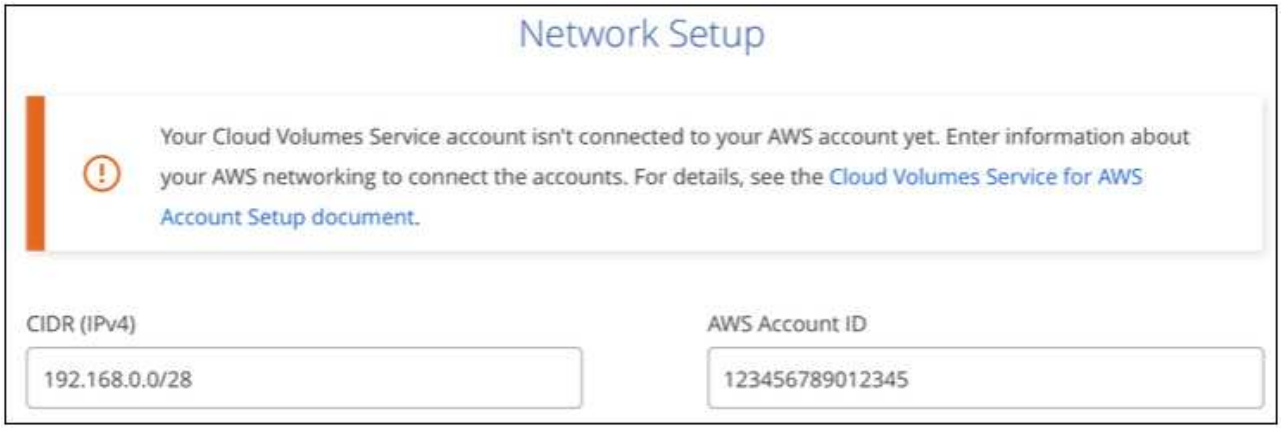
Wenn keine Volumes vorhanden sind, können Sie das erste Volume direkt aus Cloud Manager erstellen, nachdem Sie das Cloud Volumes Service für AWS Abonnement eingerichtet haben. In der Vergangenheit musste das erste Volume direkt in der Benutzeroberfläche von Cloud Volumes Service erstellt werden.

Bevor Sie beginnen

- Wenn Sie SMB in AWS verwenden möchten, müssen Sie DNS und Active Directory einrichten.
- Wenn Sie planen, ein SMB-Volume zu erstellen, müssen Sie über einen Windows Active Directory-Server verfügen, mit dem Sie eine Verbindung herstellen können. Sie geben diese Informationen bei der Erstellung des Volumes ein. Stellen Sie außerdem sicher, dass der Admin-Benutzer in der Lage ist, ein Maschinenkonto im angegebenen Organisationseinheit-Pfad (OU) zu erstellen.
- Sie benötigen diese Informationen, wenn Sie das erste Volume in einer neuen Region/Arbeitsumgebung erstellen:
  - AWS Konto-ID: Eine 12-stellige Amazon-Account-ID ohne Bindestriche. Informationen zur Suche nach Ihrer Konto-ID finden Sie in dieser "AWS Thema".
  - Classless Inter-Domain Routing (CIDR) Block: Ein nicht verwendeter IPv4-CIDR-Block. Das Netzwerkpräfix muss zwischen /16 und /28 liegen und muss auch innerhalb der Bereiche liegen, die für private Netzwerke reserviert sind (RFC 1918). Wählen Sie kein Netzwerk aus, das Ihre VPC-CIDR-Zuweisungen überschneidet.

Schritte

1. Wählen Sie die neue Arbeitsumgebung aus und klicken Sie auf **Neues Volume hinzufügen**.
2. Wenn Sie das erste Volume zur Arbeitsumgebung in der Region hinzufügen, müssen Sie AWS Netzwerkinformationen hinzufügen.
   a. Geben Sie den IPv4-Bereich (CIDR) für die Region ein.
   b. Geben Sie die 12-stellige AWS-Konto-ID (ohne Bindestriche) ein, um Ihr Cloud Volumes Konto mit Ihrem AWS Konto zu verbinden.
   c. Klicken Sie Auf **Weiter**.



3. Auf der Seite Virtuelle Schnittstellen akzeptieren werden einige Schritte beschrieben, die Sie nach dem Hinzufügen des Volumes durchführen müssen, damit Sie bereit sind, diesen Schritt abzuschließen. Klicken Sie einfach wieder auf **Weiter**.
4. Geben Sie auf der Seite Details & Tags Einzelheiten zum Volume ein:
   a. Geben Sie einen Namen für das Volume ein.
   b. Geben Sie eine Größe im Bereich von 100 gib bis 90,000 gib an (entspricht 88 TIBS).

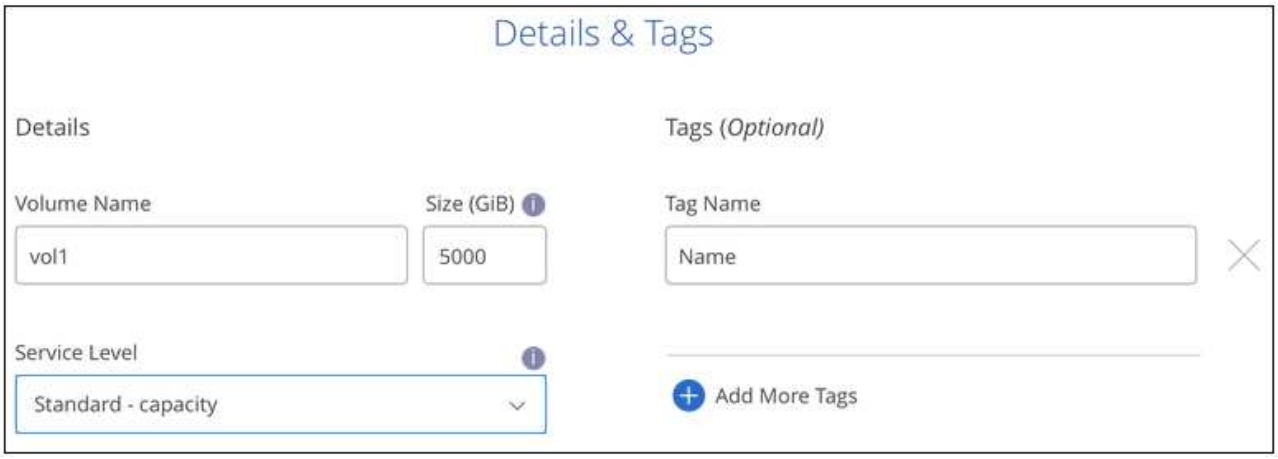
      "Hier erhalten Sie weitere Informationen über zugewiesene Kapazität".

   c. Geben Sie ein Service-Level an: Standard, Premium oder Extreme.

      "Erfahren Sie mehr über Service-Level".

d. Geben Sie einen oder mehrere Tag-Namen ein, um das Volume zu kategorisieren, falls Sie möchten.

e. Klicken Sie Auf **Weiter**.

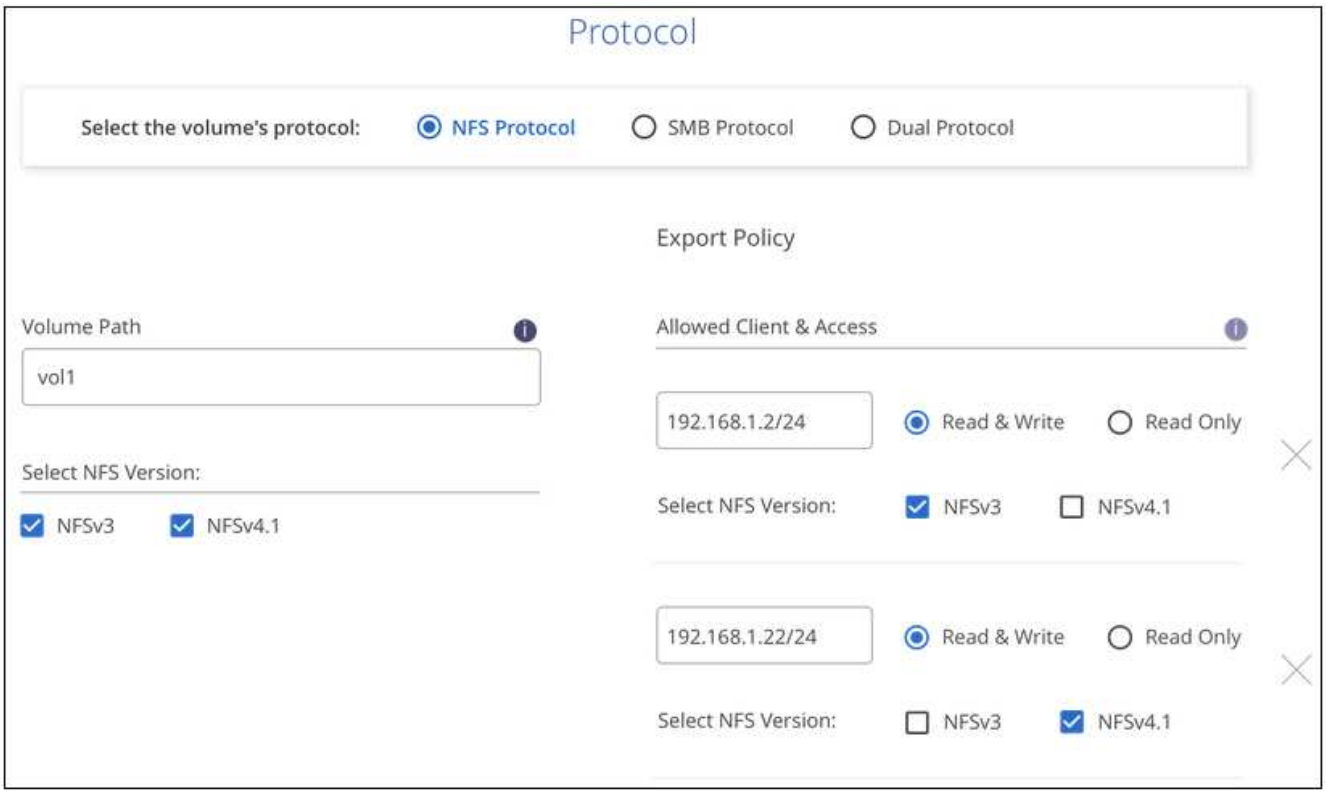


5. Wählen Sie auf der Seite Protokoll NFS, SMB oder Dual Protocol aus und definieren Sie die Details. Erforderliche Einträge für NFS und SMB sind in separaten Abschnitten unten dargestellt.
6. Geben Sie im Feld Volume Path den Namen des Volume-Exports an, den Sie beim Mounten des Volumes sehen werden.
7. Wenn Sie Dual-Protocol auswählen, können Sie den Sicherheitsstil durch Auswahl von NTFS oder UNIX auswählen. Sicherheitsstile beeinflussen den verwendeten Berechtigungstyp und die Art der Änderung der Berechtigungen.
   - UNIX verwendet Bits im NFSv3 Modus, und nur NFS-Clients können Berechtigungen ändern.
   - NTFS verwendet NTFS ACLs. Nur SMB-Clients können Berechtigungen ändern.
8. Für NFS:

   a. Wählen Sie im Feld NFS-Version NFSv3, NFSv4.1 oder beides, je nach Ihren Anforderungen.

   b. Optional können Sie eine Exportrichtlinie erstellen, um die Clients zu identifizieren, die auf das Volume zugreifen können. Geben Sie Folgendes an:
      - Zulässige Clients unter Verwendung einer IP-Adresse oder eines Classless Inter-Domain Routing (CIDR).
      - Zugriffsrechte als Lese- und Schreibgeschützt.
      - Zugriffsprotokoll (oder Protokolle, wenn das Volume sowohl NFSv3 als auch NFSv4.1 Zugriff ermöglicht) für Benutzer verwendet.
      - Klicken Sie auf **+ Add Export Policy Rule**, wenn Sie zusätzliche Exportrichtlinien-Regeln definieren möchten.

        Das folgende Bild zeigt die für das NFS-Protokoll ausgefüllte Volume-Seite:



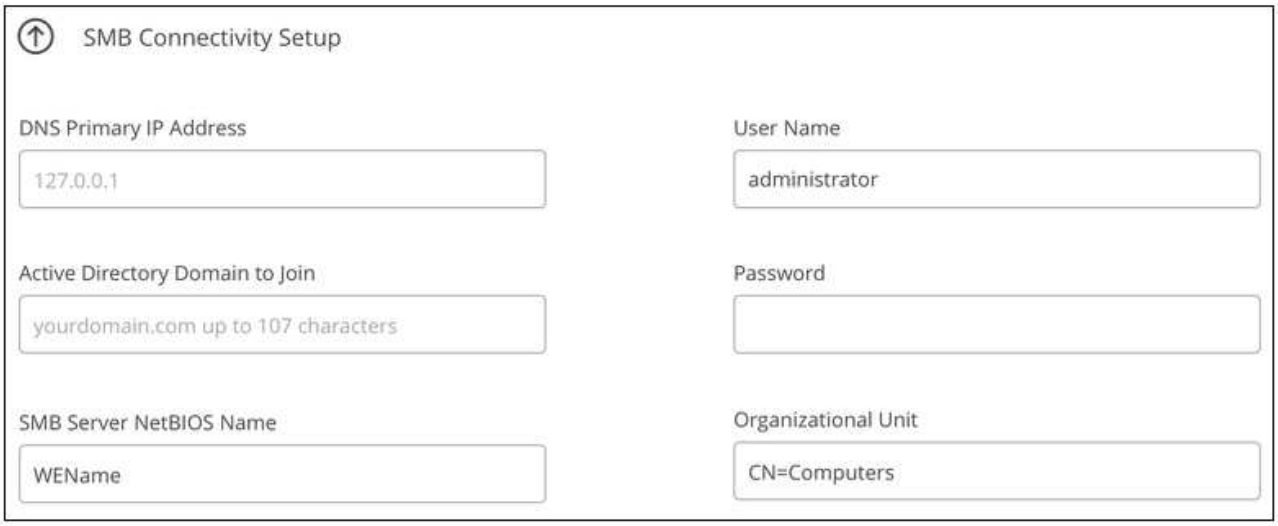
9. Für SMB:

   a. Aktivieren Sie die SMB-Sitzungsverschlüsselung, indem Sie das Kontrollkästchen für SMB-Protokollverschlüsselung aktivieren.

   b. Sie können das Volume in einen vorhandenen Windows Active Directory-Server integrieren, indem Sie die Felder im Abschnitt Active Directory ausfüllen:

Feld	Beschreibung
Primäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die eine Namensauflösung für den SMB-Server angeben. Verwenden Sie ein Komma, um die IP-Adressen zu trennen, wenn Sie auf mehrere Server verweisen, z. B. 172.31.25.223, 172.31.2.74.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domäne, der der SMB-Server beitreten soll. Verwenden Sie bei Verwendung von AWS Managed Microsoft AD den Wert aus dem Feld „Directory DNS Name“.
SMB Server NetBIOS-Name	Ein NetBIOS-Name für den zu erstellenden SMB-Server.
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.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domäne, die mit dem SMB-Server verknüpft werden soll. Die Standardeinstellung ist CN=Computer für Verbindungen zu Ihrem eigenen Windows Active Directory Server. Wenn Sie von AWS verwaltete Microsoft AD als AD-Server für die Cloud Volumes Service konfigurieren, sollten Sie in diesem Feld **OU=Computers,OU=corp** eingeben.

Das folgende Bild zeigt die für das SMB-Protokoll ausgefüllte Volume-Seite:



Sie sollten die Anleitung zu den AWS-Sicherheitseinstellungen befolgen, um die korrekte Integration von Cloud Volumes in Windows Active Directory-Server zu ermöglichen. Siehe "Einstellungen der AWS Sicherheitsgruppen für Windows AD Server" Finden Sie weitere Informationen.

10. Wenn Sie auf der Seite „Volume from Snapshot“ möchten, dass dieses Volume auf Grundlage eines Snapshots eines vorhandenen Volumes erstellt werden soll, wählen Sie den Snapshot aus der Dropdown-Liste „Snapshot Name“ aus.
11. Sie können auf der Seite Snapshot-Richtlinie Cloud Volumes Service aktivieren, um auf Grundlage eines Zeitplans Snapshot-Kopien Ihrer Volumes zu erstellen. Sie können dies jetzt tun oder das Volume zu einem späteren Zeitpunkt bearbeiten, um die Snapshot-Richtlinie zu definieren.

    Siehe "Erstellen einer Snapshot-Richtlinie" Weitere Informationen zur Snapshot-Funktionalität.

12. Klicken Sie Auf **Volumen Hinzufügen**.

Das neue Volumen wird der Arbeitsumgebung hinzugefügt.

Nachdem Sie fertig sind

Wenn dies das erste Volume ist, das in diesem AWS-Abonnement erstellt wurde, müssen Sie die AWS Management Console starten, damit Sie die beiden virtuellen Schnittstellen akzeptieren können, die in dieser AWS Region zum Verbinden aller Cloud Volumes verwendet werden. Siehe "NetApp Cloud Volumes Service für AWS – Account Setup Guide" Entsprechende Details.

Sie müssen die Schnittstellen innerhalb von 10 Minuten akzeptieren, nachdem Sie auf die Schaltfläche **Add Volume** geklickt haben, oder das System hat möglicherweise eine Auszeit. Sollte dies passieren, senden Sie eine E-Mail an cvs-support@netapp.com mit Ihrer AWS Kunden-ID und der NetApp Seriennummer. Der Support behebt das Problem, und Sie können den Onboarding-Prozess neu starten.

Fahren Sie dann mit fort "Montieren des Cloud Volumes".

Montieren Sie das Cloud Volume

Ein Cloud-Volume kann in Ihre AWS Instanz eingebunden werden. Cloud Volumes unterstützen derzeit NFSv3 und NFSv4.1 für Linux- und UNIX-Clients sowie SMB 3.0 und 3.1.1 für Windows-Clients.

Hinweis: Bitte verwenden Sie das hervorgehobene Protokoll/Dialekt, das von Ihrem Kunden unterstützt wird.

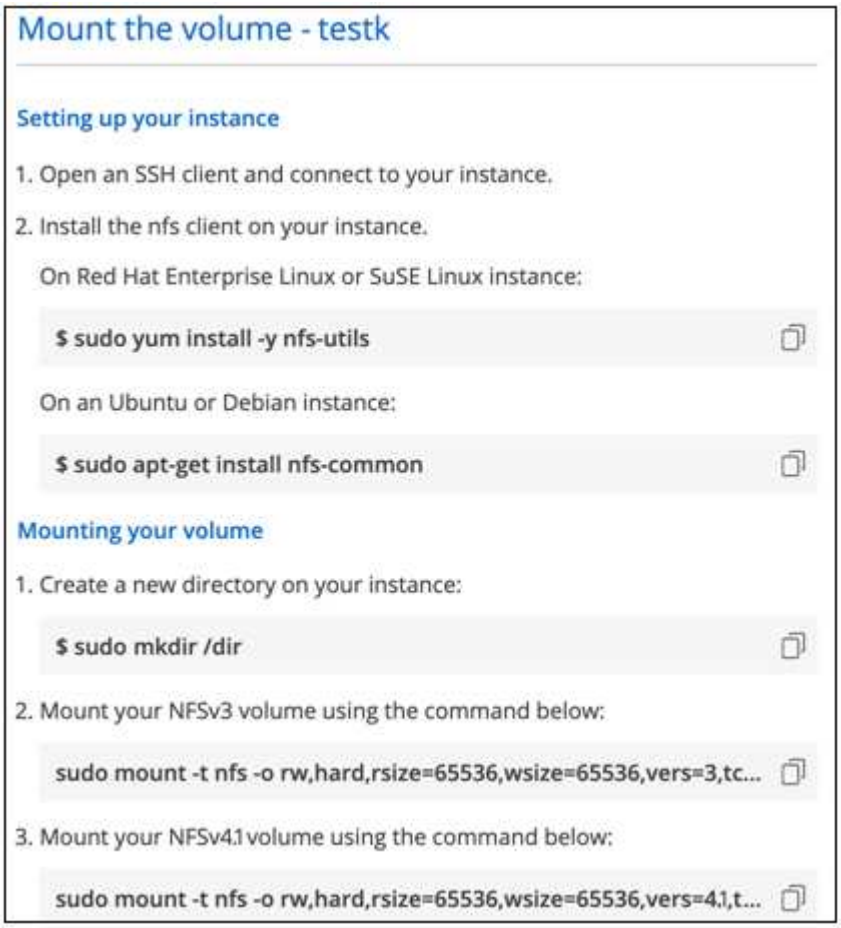
Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über die Lautstärke und klicken Sie auf **Mounten Sie die Lautstärke**.

   Auf NFS- und SMB-Volumes werden Mount-Anweisungen für dieses Protokoll angezeigt. Dual-Protokoll-Volumes bieten beide Befehlssets.

3. Bewegen Sie den Mauszeiger über die Befehle und kopieren Sie sie in die Zwischenablage, um diesen Prozess zu vereinfachen. Fügen Sie einfach das Zielverzeichnis / den Bereitstellungspunkt am Ende des Befehls hinzu.

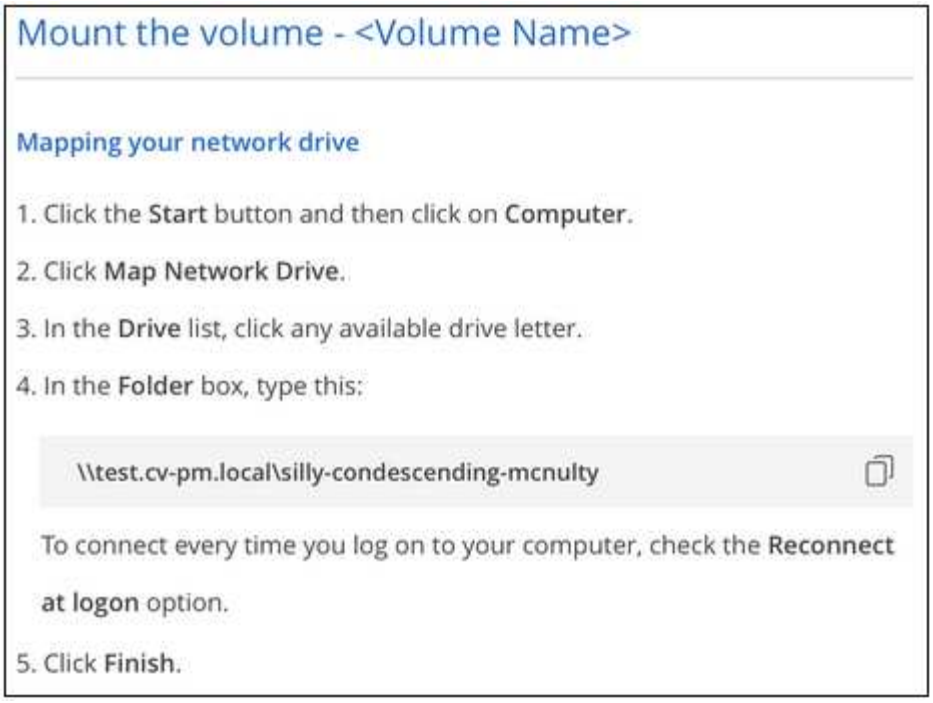
   NFS-Beispiel:



   Die von definierte maximale I/O-Größe `rsize` Und `wsize` Optionen sind 1048576, allerdings wird für die meisten Anwendungsfälle der empfohlene Standardwert von 65536 verwendet.

   Beachten Sie, dass Linux-Clients standardmäßig auf NFSv4.1 gesetzt werden, es sei denn, die Version wird mit dem angegeben `vers=<nfs_version>` Option.

   SMB-Beispiel:



4. Stellen Sie über eine SSH oder RDP-Client eine Verbindung zu Ihrer Amazon Elastic Compute Cloud (EC2) Instanz her, und befolgen Sie dann die Mount-Anweisungen für Ihre Instanz.

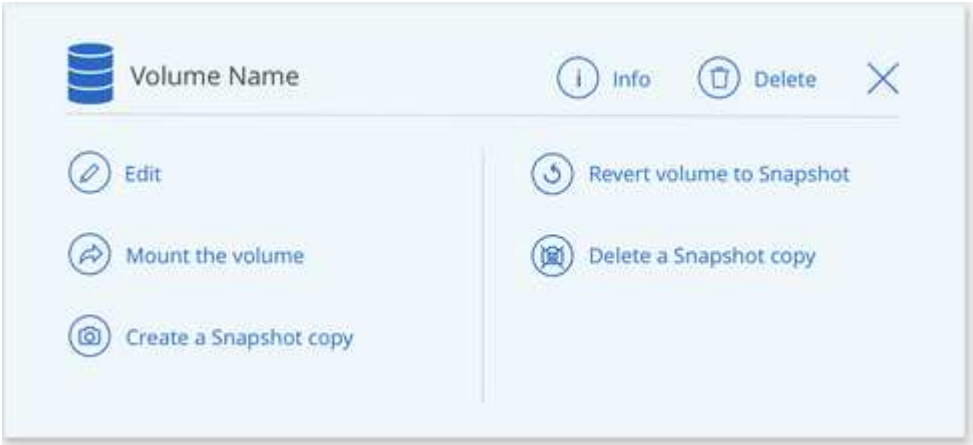
   Nach Abschluss der Schritte in der Mount-Anleitung haben Sie das Cloud-Volume erfolgreich in die AWS-Instanz eingebunden.

Management vorhandener Volumes

Sie können vorhandene Volumes managen, wenn sich Ihre Storage-Anforderungen ändern. Sie können Volumes anzeigen, bearbeiten, wiederherstellen und löschen.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Zeigen Sie den Mauszeiger auf das Volume.



3. Managen Sie Ihre Volumes:

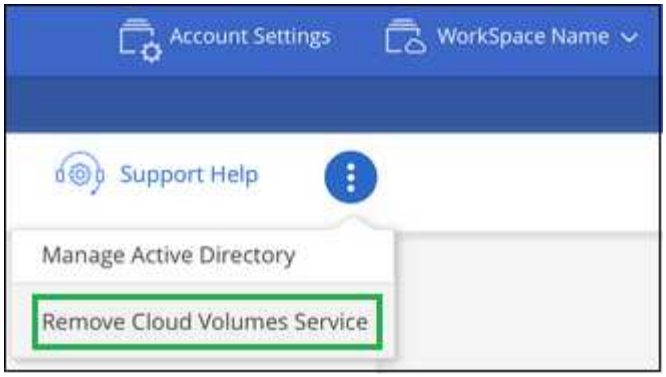
Aufgabe	Aktion
Anzeigen von Informationen zu einem Volume	Wählen Sie ein Volume aus, und klicken Sie dann auf **Info**.
Bearbeiten eines Volumes (einschließlich Snapshot-Richtlinie)	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Bearbeiten**. b. Ändern Sie die Eigenschaften des Volumes und klicken Sie dann auf **Update**.
Holen Sie den NFS- oder SMB-Mount-Befehl	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Mounten Sie das Volume**. b. Klicken Sie auf **Kopieren**, um den Befehl(en) zu kopieren.
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 Snapshot-Namen und klicken Sie dann auf **Erstellen**.
Ersetzen Sie das Volume durch den Inhalt einer Snapshot Kopie	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Volume in Snapshot zurücksetzen**. b. Wählen Sie eine Snapshot Kopie aus und klicken Sie auf **Zurücksetzen**.
Löschen einer Snapshot Kopie	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Löschen einer Snapshot Kopie**. b. Wählen Sie die Snapshot Kopie aus, die Sie löschen möchten, und klicken Sie auf **Löschen**. c. Klicken Sie zur Bestätigung erneut auf **Löschen**.
Löschen Sie ein Volume	a. Heben Sie die Bereitstellung des Volumes von allen Clients ab: ◦ Verwenden Sie unter Linux-Clients das `umount` Befehl. ◦ Klicken Sie unter Windows-Clients auf **Netzlaufwerk trennen**. b. Wählen Sie ein Volume aus, und klicken Sie dann auf **Löschen**. c. Klicken Sie zur Bestätigung erneut auf **Löschen**.

Entfernen Sie Cloud Volumes Service aus Cloud Manager

Sie können ein Cloud Volumes Service für AWS Abonnement und alle vorhandenen Volumes aus Cloud Manager entfernen. Die Volumes werden nicht gelöscht, sie werden einfach aus der Cloud Manager Schnittstelle entfernt.

Schritte

1. Öffnen Sie die Arbeitsumgebung.



2. Klicken Sie auf das Klicken Sie oben auf der Seite auf **Cloud Volumes Service entfernen**.
3. Klicken Sie im Bestätigungsdialogfeld auf **Entfernen**.

Active Directory-Konfiguration verwalten

Wenn Sie Ihre DNS-Server oder Active Directory-Domäne ändern, müssen Sie den SMB-Server in Cloud Volumes Services ändern, damit dieser weiterhin Storage für Clients bereitstellen kann.

Sie können den Link zu einem Active Directory auch löschen, wenn Sie ihn nicht mehr benötigen.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Klicken Sie auf das Klicken Sie oben auf der Seite auf **Active Directory verwalten**.
3. Wenn kein Active Directory konfiguriert ist, können Sie jetzt ein Verzeichnis hinzufügen. Wenn eine konfiguriert ist, können Sie die Einstellungen ändern oder mit dem löschen Schaltfläche.
4. Legen Sie die Einstellungen für das Active Directory fest, dem Sie beitreten möchten:

Feld	Beschreibung
Primäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die eine Namensauflösung für den SMB-Server angeben. Verwenden Sie ein Komma, um die IP-Adressen zu trennen, wenn Sie auf mehrere Server verweisen, z. B. 172.31.25.223, 172.31.2.74.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domäne, der der SMB-Server beitreten soll. Verwenden Sie bei Verwendung von AWS Managed Microsoft AD den Wert aus dem Feld „Directory DNS Name“.
SMB Server NetBIOS-Name	Ein NetBIOS-Name für den zu erstellenden SMB-Server.
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.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domäne, die mit dem SMB-Server verknüpft werden soll. Die Standardeinstellung ist CN=Computer für Verbindungen zu Ihrem eigenen Windows Active Directory Server. Wenn Sie von AWS verwaltete Microsoft AD als AD-Server für die Cloud Volumes Service konfigurieren, sollten Sie in diesem Feld **OU=Computers,OU=corp** eingeben.

5. Klicken Sie auf **Speichern**, um Ihre Einstellungen zu speichern.

Managen von Cloud Volumes Snapshots

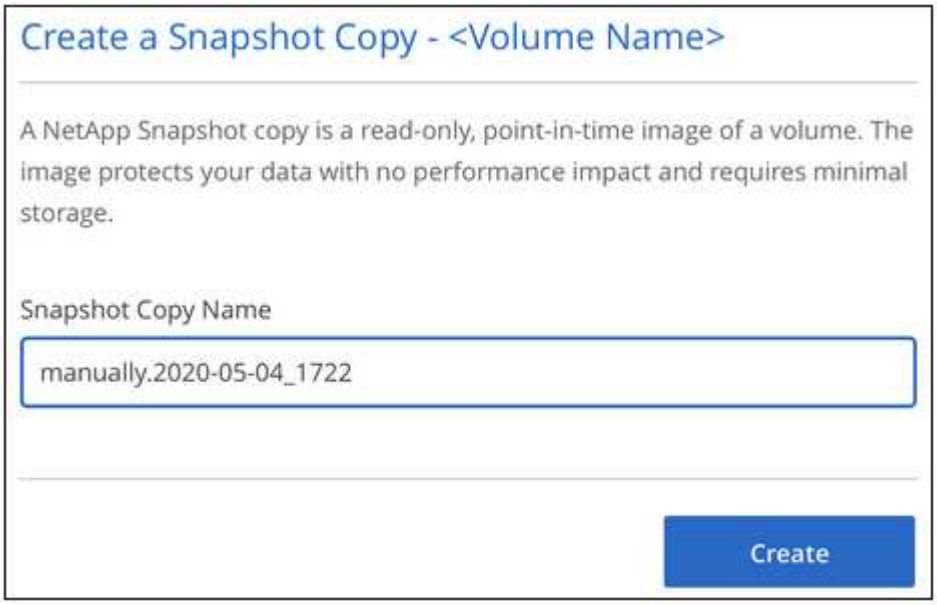
Sie können für jedes Volume eine Snapshot-Richtlinie erstellen, sodass Sie den gesamten Inhalt eines Volumes von einer früheren Zeit wiederherstellen können. Bei Bedarf können Sie auch einen On-Demand Snapshot eines Cloud Volumes erstellen.

Erstellen Sie einen On-Demand Snapshot

Sie können einen On-Demand-Snapshot eines Cloud Volumes erstellen, wenn Sie einen Snapshot im aktuellen Volume-Zustand erstellen möchten.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über den Datenträger und klicken Sie auf **Erstellen Sie eine Snapshot Kopie**.
3. Geben Sie einen Namen für den Snapshot ein, oder verwenden Sie den automatisch generierten Namen, und klicken Sie auf **Erstellen**.



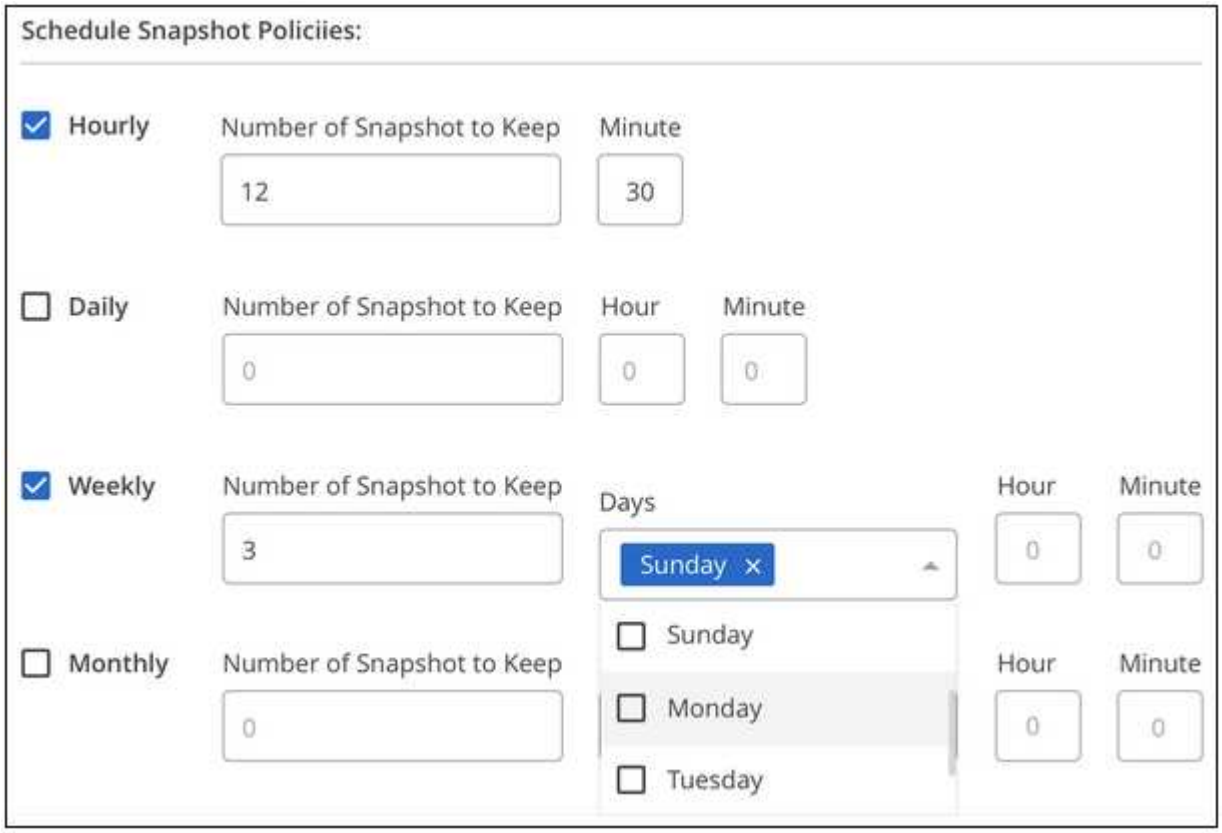
Erstellen oder Ändern einer Snapshot-Richtlinie

Sie können je nach Bedarf eine Snapshot-Richtlinie für ein Cloud-Volume erstellen oder ändern. Sie definieren die Snapshot-Richtlinie auf der Registerkarte „*Snapshot Policy*“ entweder beim Erstellen eines Volumes oder beim Bearbeiten eines Volumes.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über die Lautstärke und klicken Sie auf **Bearbeiten**.
3. Verschieben Sie auf der Registerkarte „*Snapshot Policy*“ den Schieberegler zum Aktivieren der Snapshots nach rechts.

4. Legen Sie den Zeitplan für Snapshots fest:
   a. Wählen Sie die Häufigkeit aus: **Stündlich**, **täglich**, **wöchentlich** oder **monatlich**
   b. Wählen Sie die Anzahl der Schnappschüsse aus, die beibehalten werden sollen.
   c. Wählen Sie den Tag, die Stunde und die Minute aus, an dem der Snapshot erstellt werden soll.



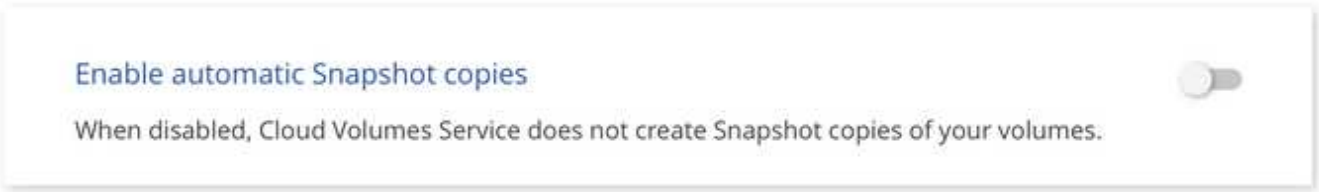
5. Klicken Sie auf **Add Volume** oder **Update Volume**, um Ihre Richtlinieneinstellungen zu speichern.

Deaktivieren einer Snapshot-Richtlinie

Sie können eine Snapshot-Richtlinie deaktivieren, um die Erstellung von Snapshots für einen kurzen Zeitraum zu verhindern, während Ihre Snapshot-Richtlinieneinstellungen beibehalten werden.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über die Lautstärke und klicken Sie auf **Bearbeiten**.
3. Verschieben Sie auf der Registerkarte „*Snapshot Policy*“ den Schieberegler „Snapshots aktivieren“ nach links.



4. Klicken Sie auf **Lautstärke aktualisieren**.

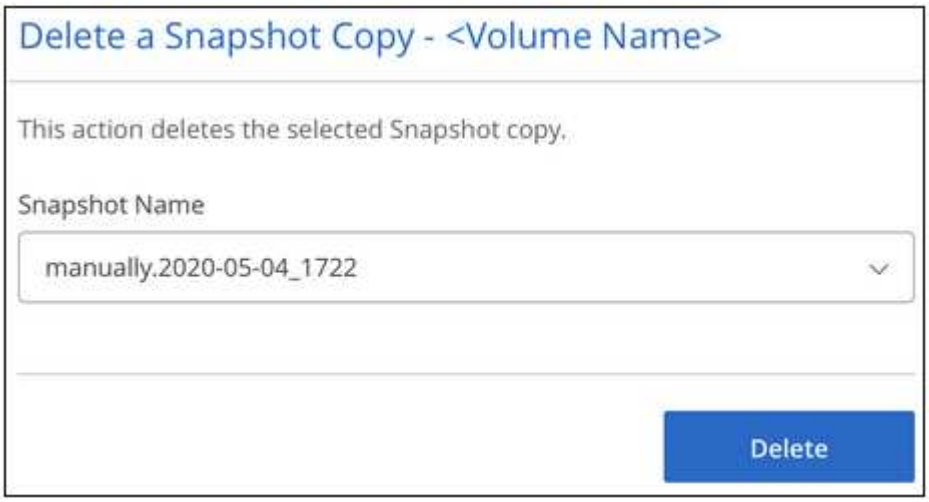
Wenn Sie die Snapshot-Richtlinie wieder aktivieren möchten, verschieben Sie den Schieberegler Snapshots aktivieren nach rechts und klicken Sie auf **Datenträger aktualisieren**.

Löschen Sie einen Snapshot

Sie können einen Snapshot von der Seite Volumes löschen.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über das Volume und klicken Sie auf **Löschen einer Snapshot Kopie**.
3. Wählen Sie den Snapshot aus der Dropdown-Liste aus und klicken Sie auf **Löschen**.



4. Klicken Sie im Bestätigungsdialogfeld auf **Löschen**.

Zurücksetzen eines Volumes aus einem Snapshot

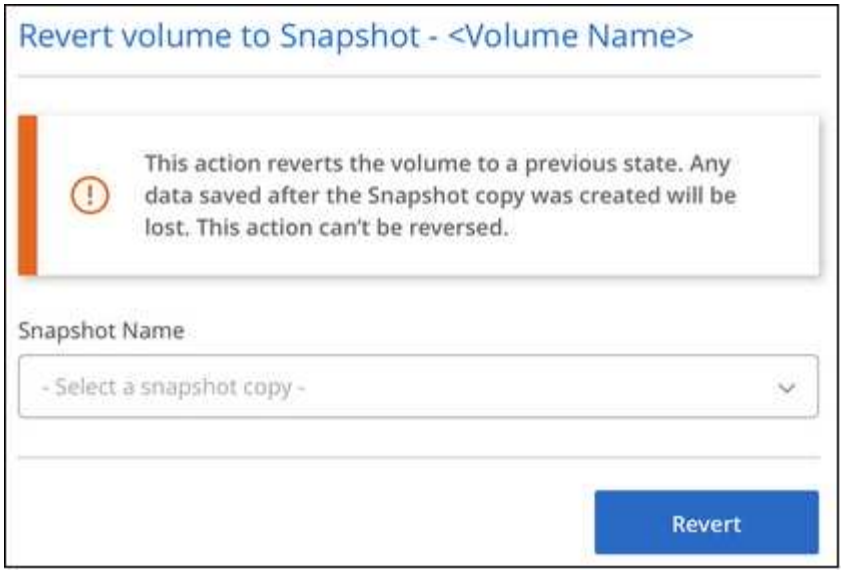
Sie können ein Volume von einem vorhandenen Snapshot auf einen früheren Zeitpunkt zurücksetzen.

Wenn Sie ein Volume zurücksetzen, überschreibt der Inhalt des Snapshots die vorhandene Volume-Konfiguration. Alle Änderungen an den Daten auf dem Volume nach der Erstellung des Snapshots gehen verloren.

Beachten Sie, dass Clients das Volume nach der Umrüstung nicht neu mounten müssen.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über das Volume und klicken Sie auf **Volume zum Snapshot zurücksetzen**.
3. Wählen Sie den Snapshot aus der Dropdown-Liste aus, den Sie verwenden möchten, um das vorhandene Volume wiederherzustellen, und klicken Sie auf **revert**.



Referenz

Service Level und zugewiesene Kapazität

Die Kosten für Cloud Volumes Service für AWS basieren auf dem *Service Level* und der von Ihnen ausgewählten *zugewiesenen Kapazität*. Durch die Auswahl des geeigneten Service Levels und der Kapazität erfüllen Sie Ihre Storage-Anforderungen zu den niedrigsten Kosten.

Überlegungen

Storage-Anforderungen beinhalten zwei grundlegende Aspekte:

- Storage_Capacity_ für das Speichern von Daten
- Storage *Bandbreite* für die Interaktion mit Daten

Wenn Sie mehr Speicherplatz verbrauchen als die für das Volume ausgewählte Kapazität, gelten die folgenden Überlegungen:

- Sie werden die zusätzliche Storage-Kapazität, die Sie verbrauchen, zu dem von Ihrem Service Level definierten Preis in Rechnung gestellt.
- Die für das Volume verfügbare Storage-Bandbreite wächst erst, wenn Sie die zugewiesene Kapazitätsgröße erhöhen oder den Service Level ändern.

Service-Leveln

Cloud Volumes Service für AWS unterstützt drei Service-Level. Sie geben Ihren Service-Level an, wenn Sie das Volume erstellen oder ändern.

Die Service Levels werden auf unterschiedliche Storage-Kapazitäts- und Storage-Anforderungen abgestimmt:

- **Standard** (Kapazität)

  Wenn Sie Kapazität zu den niedrigsten Kosten benötigen und Ihre Bandbreitenanforderungen begrenzt sind, eignen sich die standardmäßigen Service-Levels möglicherweise am besten für Sie. Ein Beispiel

hierfür ist die Nutzung des Volumes als Backup-Ziel.

    - Bandbreite: 16 KB Bandbreite pro bereitgestelltem GB Kapazität

- **Premium** (ein ausgewogenes Verhältnis von Kapazität und Performance)

  Wenn Ihre Applikation einen ausgewogenen Bedarf an Storage-Kapazität und Bandbreite hat, ist das Premium Service Level möglicherweise am besten für Sie geeignet. Dieses Level ist pro MB/s günstiger als das Standard-Service-Level und ist zudem pro GB günstiger als das Extreme Service Level.

    - Bandbreite: 64 KB Bandbreite pro bereitgestelltem GB Kapazität

- **Extreme** (Leistung)

  Das extrem hohe Service-Level ist hinsichtlich der Storage-Bandbreite am kostengünstigsten. Wenn Ihre Applikation eine Storage-Bandbreite ohne die damit verbundene Nachfrage nach viel Storage-Kapazität benötigt, ist das Extreme Service Level wahrscheinlich das richtige für Sie.

    - Bandbreite: 128 KB Bandbreite pro bereitgestelltem GB Kapazität

Zugewiesene Kapazität

Beim Erstellen oder Ändern des Volume wird die zugewiesene Kapazität für das Volume angegeben.

Wählen Sie Ihr Service Level zwar basierend auf Ihren allgemeinen und allgemeinen geschäftlichen Anforderungen aus, Sie sollten jedoch Ihre zugewiesene Kapazitätsgröße entsprechend den spezifischen Anforderungen von Applikationen auswählen, zum Beispiel:

- Wie viel Speicherplatz benötigen die Applikationen
- Wie viel Storage-Bandbreite pro Sekunde benötigen die Applikationen oder Benutzer

Die zugewiesene Kapazität wird in GB angegeben. Die zugewiesene Kapazität eines Volumes kann im Bereich von 100 GB bis 100,000 GB (entspricht 100 TB) eingestellt werden.

Anzahl Inodes

Volumes kleiner als oder gleich 1 TB können bis zu 20 Millionen Inodes belegen. Die Zahl der Inodes steigt um 20 Millionen pro TB, die Sie zuweisen, bis zu einem Maximum von 100 Millionen Inodes.

- <= 1 TB = 20 Millionen Inodes
- >1 TB bis 2 TB = 40 Millionen Inodes
- >2 TB bis 3 TB = 60 Millionen Inodes
- >3 TB bis 4 TB = 80 Millionen Inodes
- >4 TB bis 100 TB = 100 Millionen Inodes

Bandbreite

Die Kombination aus Service Level und der ausgewählten Kapazität bestimmt die maximale Bandbreite für das Volume.

Wenn Ihre Applikationen oder Benutzer mehr Bandbreite benötigen als Ihre Auswahl, können Sie den Service Level ändern oder die zugewiesene Kapazität erhöhen. Die Änderungen unterbrechen den Datenzugriff nicht.

Auswählen des Service-Levels und der zugewiesenen Kapazität

Um das für Ihren Bedarf am besten geeignete Service-Level und die zugewiesene Kapazität auszuwählen, müssen Sie wissen, wie viel Kapazität und Bandbreite Sie zu Spitzenzeiten oder am Edge-Bereich benötigen.

Liste der Service Level und der zugewiesenen Kapazität

Die Spalte links zeigt die Kapazität an, und die anderen Spalten definieren die verfügbaren MB/s an jedem Kapazitätspunkt basierend auf dem Service Level.

Siehe "Abonnementpreise für Verträge" Und "Metered-Abonnementpreise" Für vollständige Details zum Preis.

Kapazität (TB)	Standard (MB/s)	Premium (MB/s)	Extrem (MB/s)
0.1 (100 GB)	1.6	6.4	12.8
1	16	64	128
2	32	128	256
3	48	192	384
4	64	256	512
5	80	320	640
6	96	384	768
7	112	448	896
8	128	512	1,024
9	144	576	1,152
10	160	640	1,280
11	176	704	1,408
12	192	768	1,536
13	208	832	1,664
14	224	896	1,792
15	240	960	1,920
16	256	1,024	2,048
17	272	1,088	2,176
18	288	1,152	2,304
19	304	1,216	2,432
20	320	1,280	2,560
21	336	1,344	2,688
22	352	1,408	2,816
23	368	1,472	2,944
24	384	1,536	3,072
25	400	1,600	3,200

Kapazität (TB)	Standard (MB/s)	Premium (MB/s)	Extrem (MB/s)
26	416	1,664	3,328
27	432	1,728	3,456
28	448	1,792	3,584
29	464	1,856	3,712
30	480	1,920	3,840
31	496	1,984	3,968
32	512	2,048	4,096
33	528	2,112	4,224
34	544	2,176	4,352
35	560	2,240	4,480
36	576	2,304	4,500
37	592	2,368	4,500
38	608	2,432	4,500
39	624	2,496	4,500
40	640	2,560	4,500
41	656	2,624	4,500
42	672	2,688	4,500
43	688	2,752	4,500
44	704	2,816	4,500
45	720	2,880	4,500
46	736	2,944	4,500
47	752	3,008	4,500
48	768	3,072	4,500
49	784	3,136	4,500
50	800	3,200	4,500
51	816	3,264	4,500
52	832	3,328	4,500
53	848	3,392	4,500
54	864	3,456	4,500
55	880	3,520	4,500
56	896	3,584	4,500
57	912	3,648	4,500
58	928	3,712	4,500

Kapazität (TB)	Standard (MB/s)	Premium (MB/s)	Extrem (MB/s)
59	944	3,776	4,500
60	960	3,840	4,500
61	976	3,904	4,500
62	992	3,968	4,500
63	1,008	4,032	4,500
64	1,024	4,096	4,500
65	1,040	4,160	4,500
66	1,056	4,224	4,500
67	1,072	4,288	4,500
68	1,088	4,352	4,500
69	1,104	4,416	4,500
70	1,120	4,480	4,500
71	1,136	4,500	4,500
72	1,152	4,500	4,500
73	1,168	4,500	4,500
74	1,184	4,500	4,500
75	1,200	4,500	4,500
76	1,216	4,500	4,500
77	1,232	4,500	4,500
78	1,248	4,500	4,500
79	1,264	4,500	4,500
80	1,280	4,500	4,500
81	1,296	4,500	4,500
82	1,312	4,500	4,500
83	1,328	4,500	4,500
84	1,344	4,500	4,500
85	1,360	4,500	4,500
86	1,376	4,500	4,500
87	1,392	4,500	4,500
88	1,408	4,500	4,500
89	1,424	4,500	4,500
90	1,440	4,500	4,500
91	1,456	4,500	4,500

Kapazität (TB)	Standard (MB/s)	Premium (MB/s)	Extrem (MB/s)
92	1,472	4,500	4,500
93	1,488	4,500	4,500
94	1,504	4,500	4,500
95	1,520	4,500	4,500
96	1,536	4,500	4,500
97	1,552	4,500	4,500
98	1,568	4,500	4,500
99	1,584	4,500	4,500
100	1,600	4,500	4,500

Beispiel 1

Beispielsweise benötigt Ihre Applikation 25 TB Kapazität und 100 MB/s Bandbreite. Bei einer Kapazität von 25 TB würde das Standard Service Level 400 MB/s Bandbreite zu einem Preis von 2,500 US-Dollar bereitstellen (Schätzung: Siehe aktuelle Preise). Damit ist Standard in diesem Fall das am besten geeignete Servicelevel.

	Standard		Premium		Extreme	
capacity	Bandwidth		Bandwidth		Bandwidth	
TB	MB/s	Cost	MB/s	Cost	MB/s	Cost
24	384	$2,400	1,536	$4,800	3,072	$7,200
25	400	$2,500	1,600	$5,000	3,200	$7,500
26	416	$2,600	1,664	$5,200	3,328	$7,800

Beispiel 2

Beispielsweise benötigt Ihre Applikation 12 TB Kapazität und eine Spitzenbandbreite von 800 MB/s. Obwohl das extreme Service-Level die Anforderungen der Applikation an die 12-TB-Marke erfüllen kann, ist es kostengünstiger (Schätzung: Siehe aktueller Preis), 13 TB auf dem Premium-Service-Level auszuwählen.

	Standard		Premium		Extreme	
capacity	Bandwidth		Bandwidth		Bandwidth	
TB	MB/s	Cost	MB/s	Cost	MB/s	Cost
12	192	$1,200	768	$2,400	1,536	$3,600
13	208	$1,300	832	$2,600	1,664	$3,900
14	224	$1,400	896	$2,800	1,792	$4,200

Einstellungen der AWS Sicherheitsgruppen für Windows AD Server

Wenn Sie Windows Active Directory (AD)-Server mit Cloud Volumes verwenden, sollten Sie sich mit den Anleitungen zu den Einstellungen der AWS-Sicherheitsgruppen vertraut machen. Die Einstellungen ermöglichen die korrekte Integration von Cloud Volumes mit AD.

Standardmäßig enthält die AWS-Sicherheitsgruppe, die auf eine EC2 Windows-Instanz angewendet wird, keine eingehenden Regeln für ein Protokoll außer RDP. Sie müssen den Sicherheitsgruppen, die an jede Windows AD-Instanz angehängt sind, Regeln hinzufügen, um eingehende Kommunikation von Cloud Volumes Service zu aktivieren. Folgende Ports sind erforderlich:

Service	Port	Protokoll
AD Web Services	9389	TCP
DNS	53	TCP
DNS	53	UDP
ICMPv4	K. A.	Echo Antwort
Kerberos	464	TCP
Kerberos	464	UDP
Kerberos	88	TCP
Kerberos	88	UDP
LDAP	389	TCP
LDAP	389	UDP
LDAP	3268	TCP
NetBIOS-Name	138	UDP
SAM/LSA	445	TCP
SAM/LSA	445	UDP
Sicheres LDAP	636	TCP
Sicheres LDAP	3269	TCP
W32mal	123	UDP

Wenn Sie Ihre AD-Installations-Domain-Controller und Mitgliedsserver auf einer AWS EC2-Instanz implementieren und managen, benötigen Sie mehrere Sicherheitsgruppenregeln, um den Datenverkehr für die Cloud Volumes Service zuzulassen. Im Folgenden finden Sie ein Beispiel zur Implementierung dieser Regeln für AD-Applikationen im Rahmen der AWS CloudFormation-Vorlage.

```
{
    "AWSTemplateFormatVersion" : "2010-09-09",
    "Description" : "Security Group for AD",
    "Parameters" :
    {
        "VPC" :
        {
            "Type" : "AWS::EC2::VPC::Id",
            "Description" : "VPC where the Security Group will belong:"
        },
        "Name" :
        {
```

```
            "Type" : "String",
            "Description" : "Name Tag of the Security Group:"
        },
        "Description" :
        {
            "Type" : "String",
            "Description" : "Description Tag of the Security Group:",
            "Default" : "Security Group for Active Directory for CVS "
        },
        "CIDRrangeforTCPandUDP" :
        {
            "Type" : "String",
            "Description" : "CIDR Range for the UDP ports
445,138,464,389,53,123 and for the TCP ports
464,339,3389,3268,88,636,9389,445 and 0-65535: *CIDR range format:
10.0.0.0/24"
        }
    },
    "Resources" :
    {
        "ADSGWest" :
        {
            "Type" : "AWS::EC2::SecurityGroup",
            "Properties" :
            {
                "GroupDescription" : {"Ref" : "Description"},
                "VpcId" : { "Ref" : "VPC" },
                "SecurityGroupIngress" : [
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "445",
                        "ToPort" : "445"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "138",
                        "ToPort" : "138"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "464",
                        "ToPort" : "464"
                    },
```

```
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "464",
                        "ToPort" : "464"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "389",
                        "ToPort" : "389"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "53",
                        "ToPort" : "53"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "339",
                        "ToPort" : "339"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "123",
                        "ToPort" : "123"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "3389",
                        "ToPort" : "3389"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "3268",
                        "ToPort" : "3268"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "88",
```

```
                    "ToPort" : "88"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "636",
                    "ToPort" : "636"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "3269",
                    "ToPort" : "3269"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "53",
                    "ToPort" : "53"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "0",
                    "ToPort" : "65535"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "9389",
                    "ToPort" : "9389"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "445",
                    "ToPort" : "445"
                }
            ]
        }
    }
},
"Outputs" :
{
    "SecurityGroupID" :
    {
```

```
            "Description" : "Security Group ID",
            "Value" : { "Ref" : "ADSGWest" }
        }
    }
}
```

Cloud Volumes Service für GCP

Erfahren Sie mehr über Cloud Volumes Service für Google Cloud

Mit NetApp Cloud Volumes Service für Google Cloud können Sie im Handumdrehen Multi-Protokoll-Workloads hinzufügen und sowohl Windows-basierte als auch UNIX-basierte Applikationen erstellen und implementieren.

Zentrale Punkte:

- Migrieren von Daten zwischen On-Premises-Systemen und Google Cloud
- Stellen Sie Volumes von 1 bis 100 tib in Sekundenschnelle bereit.
- Multi-Protokoll-Unterstützung (ein NFS- oder SMB-Volume kann erstellt werden)
- Sichern Sie Ihre Daten mit automatisierten, effizienten Snapshots.
- Beschleunigte Applikationsentwicklung durch schnelles Klonen

Kosten

Volumes, die im Cloud Volumes Service für Google Cloud erstellt wurden, stellen für Ihr Abonnement des Services statt über Cloud Manager eine Gebühr in Rechnung.

"Preise anzeigen"

Es fallen keine Kosten an, eine Region oder ein Volumen von Cloud Volumes Service für Google Cloud von Cloud Manager zu entdecken.

Unterstützte Regionen

"Unterstützte Google-Cloud-Regionen anzeigen."

Bevor Sie beginnen

Cloud Manager kann vorhandene Cloud Volumes Service für GCP-Abonnements und Volumes ermitteln. Siehe "NetApp Cloud Volumes Service für Google Cloud - Dokumentation" Wenn Sie Ihr Abonnement noch nicht eingerichtet haben.

Hilfe wird abgerufen

Verwenden Sie den Chat von Cloud Manager für allgemeine Fragen zum Cloud Volumes Service Betrieb in Cloud Manager.

Für allgemeine Fragen zu Cloud Volumes Service für Google Cloud senden Sie eine E-Mail an das Google Cloud Team von NetApp unter gcinfo@netapp.com.

Bei technischen Problemen in Verbindung mit Ihren Cloud Volumes können Sie über die Google Cloud Console einen technischen Support-Case erstellen. Siehe "Support erhalten" Entsprechende Details.

Einschränkungen

- Cloud Manager unterstützt bei der Verwendung von Cloud Volumes Service Volumes keine Datenreplizierung zwischen Arbeitsumgebungen.
- Das Löschen Ihres Cloud Volumes Service für Google Cloud Abonnements aus Cloud Manager wird nicht unterstützt. Dies ist nur über die Google Cloud Console möglich.

Weiterführende Links

- "NetApp Cloud Central: Cloud Volumes Service für Google Cloud"
- "NetApp Cloud Volumes Service für Google Cloud - Dokumentation"

Einrichtung von Cloud Volumes Service für Google Cloud

Erstellung und Management von Volumes und Snapshots in Cloud Manager einer Cloud Volumes Service für Google Cloud-Arbeitsumgebung

Schnellstart

Führen Sie die Schritte schnell durch, oder rufen Sie den nächsten Abschnitt auf, um weitere Einzelheiten zu erfahren.

Aktivieren Sie die Cloud Volumes Service-API

Aktivieren Sie von Google die Cloud Volumes Service für GCP-API, damit Cloud Manager die Abonnement- und Cloud-Volumes managen kann.

Erstellen eines GCP-Service-Kontos und Zugangsdaten für den Download

Erstellen Sie in Google ein GCP-Servicekonto und eine Rolle, damit Cloud Manager auf Ihr Cloud Volumes Service für GCP-Konto zugreifen kann.

Einrichtung einer Cloud Volumes Service für GCP-Arbeitsumgebung

Klicken Sie im Cloud Manager auf **Arbeitsumgebung hinzufügen** > **Google Cloud** > **Cloud Volumes Service** und geben Sie dann Details zum Servicekonto und dem Google Cloud Projekt an.

Aktivieren Sie die Cloud Volumes Service-API

Führen Sie in Google Cloud Shell den folgenden Befehl aus, um die Cloud Volumes Service-API zu aktivieren:

```
gcloud --project=<my-cvs-project> services enable cloudvolumesgcp-api.netapp.com
```

Cloud Manager Zugriff auf das Cloud Volumes Service für GCP-Konto gewähren

Führen Sie die folgenden Aufgaben aus, damit Cloud Manager auf Ihr Google Cloud-Projekt zugreifen kann:

- Erstellen Sie ein neues Dienstkonto
- Fügen Sie das neue Servicekontomitglied zu Ihrem Projekt hinzu und weisen Sie ihm spezifische Rollen (Berechtigungen) zu.
- Erstellen und Herunterladen eines Schlüsselpaares für das Dienstkonto, das zur Authentifizierung bei Google verwendet wird

Schritte

1. Gehen Sie in der Google Cloud Console zur Seite **Servicekonten**.
2. Klicken Sie auf **Wählen Sie ein Projekt**, wählen Sie Ihr Projekt aus und klicken Sie auf **Öffnen**.
3. Klicken Sie auf **Dienstkonto erstellen**, geben Sie den Namen des Dienstkontos (Anzeigename) und die Beschreibung ein und klicken Sie auf **Erstellen**.
4. Klicken Sie auf der Seite *IAM* auf **Hinzufügen** und füllen Sie die Felder auf der Seite *Mitglieder hinzufügen* aus:
   a. Geben Sie im Feld Neue Mitglieder die vollständige Dienstkontokennung ein, z. B. user1-service-account-cvs@project1.iam.gserviceaccount.com.
   b. Fügen Sie die folgenden Rollen hinzu:
      - *NetApp Cloud Volumes Admin*
      - Netzwerk-Viewer Berechnen_
      - *Ordneranzeige*
   c. Klicken Sie Auf **Speichern**.
5. Klicken Sie auf der Seite *Service Account Details* auf **Add key > Create New key**.
6. Wählen Sie als Schlüsseltyp **JSON** aus und klicken Sie auf **Erstellen**.

   Durch Klicken auf **Erstellen** wird Ihr neues Public/Private Key-Paar generiert und auf Ihr System heruntergeladen. Es dient als einzige Kopie des privaten Schlüssels. Speichern Sie diese Datei sicher, da sie zur Authentifizierung als Dienstkonto verwendet werden kann.

Ausführliche Schritte finden Sie in den Google Cloud-Themen "Erstellen und Verwalten von Servicekonten", "Gewähren, Ändern und Entzug des Zugriffs auf Ressourcen", und "Erstellen und Verwalten von Service-Kontokasten".

Einrichtung einer Cloud Volumes Service für GCP-Arbeitsumgebung

Einrichtung einer Cloud Volumes Service für GCP-Arbeitsumgebung in Cloud Manager für die Erstellung von Volumes

Unabhängig davon, ob Sie bereits Volumes über die Google Cloud Console erstellt haben, oder ob Sie sich einfach nur für Cloud Volumes Service für GCP angemeldet haben und noch keine Volumes haben, sollten Sie als Erstes eine Arbeitsumgebung für Volumes erstellen, die auf Ihrem GCP-Abonnement basiert.

Wenn bereits Cloud Volumes für dieses Abonnement vorhanden sind, werden die Volumes in der neuen Arbeitsumgebung angezeigt. Wenn Sie noch keine Cloud Volumes für das GCP Abonnement hinzugefügt haben, gehen Sie nach dem Erstellen der neuen Arbeitsumgebung vor.

Wenn in mehreren GCP-Projekten Abonnements und Volumes vorhanden sind, müssen Sie diese Aufgabe für jedes Projekt ausführen.

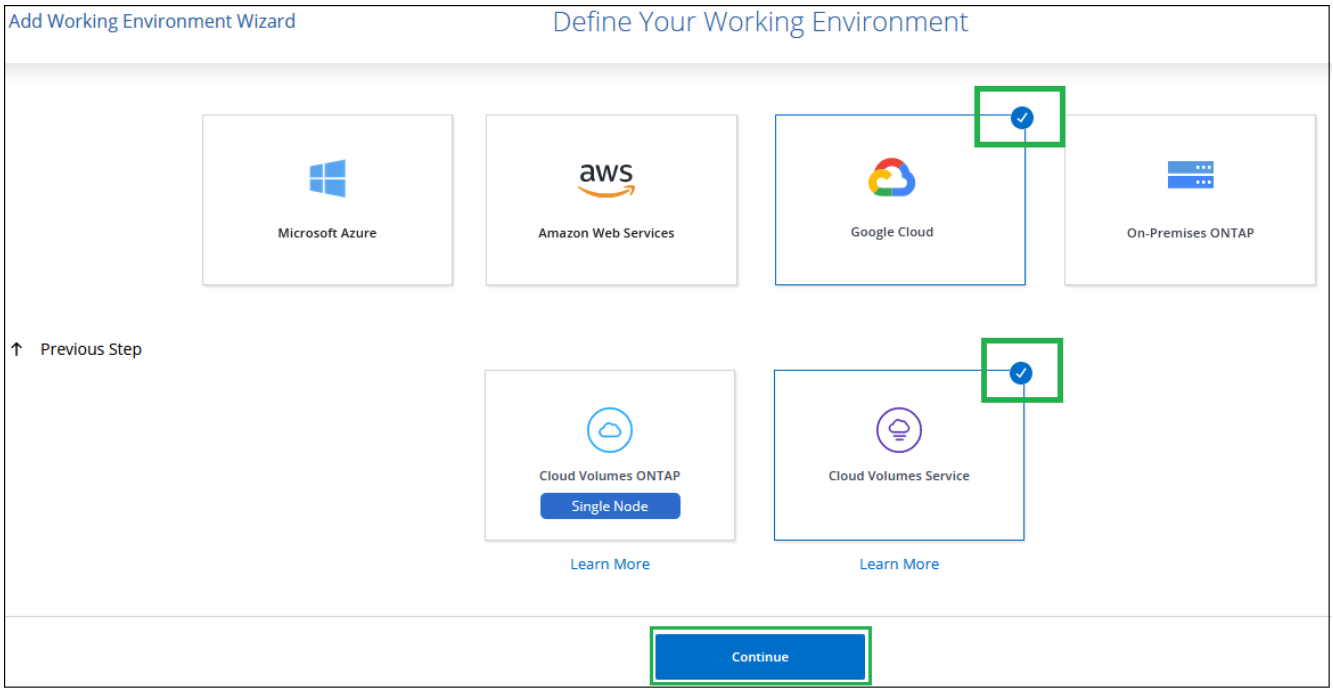
Bevor Sie beginnen

Beim Hinzufügen eines Abonnements für jedes Projekt müssen Sie über die folgenden Informationen verfügen:

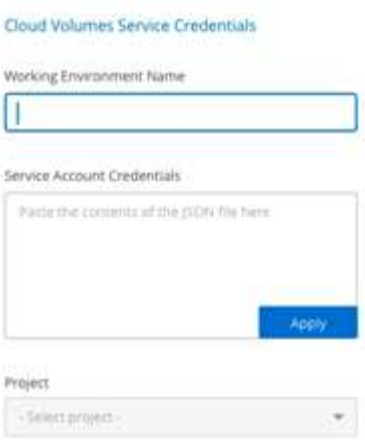
- Zugangsdaten für ein Servicekonto (JSON-privater Schlüssel, den Sie heruntergeladen haben)
- Projektname

Schritte

1. Fügen Sie in Cloud Manager eine neue Arbeitsumgebung hinzu, wählen Sie den Standort **Google Cloud** und klicken Sie auf **Weiter**.
2. Wählen Sie **Cloud Volumes Service** und klicken Sie auf **Weiter**.



3. Stellen Sie Informationen zu Ihrem Cloud Volumes Service Abonnement bereit:
   a. Geben Sie den Namen der Arbeitsumgebung ein, den Sie verwenden möchten.
   b. Kopieren Sie den JSON-privaten Schlüssel, den Sie in den vorherigen Schritten heruntergeladen haben, und fügen Sie ihn ein.
   c. Wählen Sie den Namen Ihres Google Cloud-Projekts aus.
   d. Klicken Sie Auf **Hinzufügen**.



Ergebnis

Cloud Manager zeigt Ihre Arbeitsumgebung „Cloud Volumes Service for Google Cloud“ an.

Wenn bereits Cloud Volumes für dieses Abonnement vorhanden sind, werden die Volumes in der neuen Arbeitsumgebung angezeigt, wie im Screenshot dargestellt. Sie können weitere Cloud Volumes über Cloud Manager hinzufügen.

Wenn für dieses Abonnement keine Cloud Volumes vorhanden sind, erstellen Sie sie jetzt.

Was kommt als Nächstes?

"Beginnen Sie mit dem Erstellen und Managen von Volumes".

Erstellung und Management von Volumes für Cloud Volumes Service für Google Cloud

Mit Cloud Manager können Sie Cloud Volumes auf Basis Ihres erstellen "Cloud Volumes Service für Google Cloud" Abonnement: Sie können auch bestimmte Attribute eines Volumes bearbeiten, die entsprechenden Mount-Befehle abrufen, Snapshot-Kopien erstellen und Cloud-Volumes löschen.

Cloud Volumes erstellen

NFS- oder SMB-Volumes werden in einem neuen oder vorhandenen Cloud Volumes Service für Google Cloud Konto erstellt. Cloud Volumes unterstützen derzeit NFSv3 und NFSv4.1 für Linux- und UNIX-Clients und SMB 3.x für Windows-Clients.

Bevor Sie beginnen

- Wenn Sie SMB in GCP verwenden möchten, müssen Sie DNS und Active Directory einrichten.

- Wenn Sie planen, ein SMB-Volume zu erstellen, müssen Sie über einen Windows Active Directory-Server verfügen, mit dem Sie eine Verbindung herstellen können. Sie geben diese Informationen bei der Erstellung des Volumes ein. Stellen Sie außerdem sicher, dass der Admin-Benutzer in der Lage ist, ein Maschinenkonto im angegebenen Organisationseinheit-Pfad (OU) zu erstellen.

Schritte

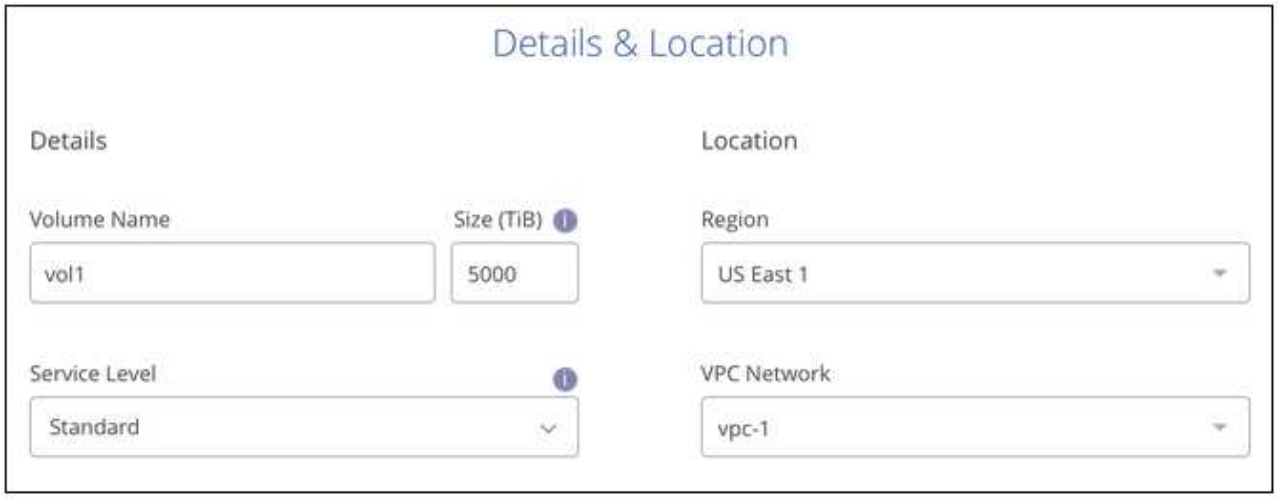
1. Wählen Sie die Arbeitsumgebung aus und klicken Sie auf **Neues Volume hinzufügen**.
2. Geben Sie auf der Seite Details & Location Details zum Volume ein:
   a. Geben Sie einen Namen für das Volume ein.
   b. Geben Sie eine Größe im Bereich von 1 tib (1024 gib) bis 100 tib an.

      "Hier erhalten Sie weitere Informationen über zugewiesene Kapazität".

   c. Geben Sie ein Service-Level an: Standard, Premium oder Extreme.

      "Erfahren Sie mehr über Service-Level".

   d. Wählen Sie die Google Cloud-Region aus.
   e. Wählen Sie das VPC-Netzwerk aus, auf das das Volume zugegriffen werden soll. Beachten Sie, dass die VPC nicht mehr geändert oder bearbeitet werden kann, nachdem das Volume erstellt wurde.
   f. Klicken Sie Auf **Weiter**.

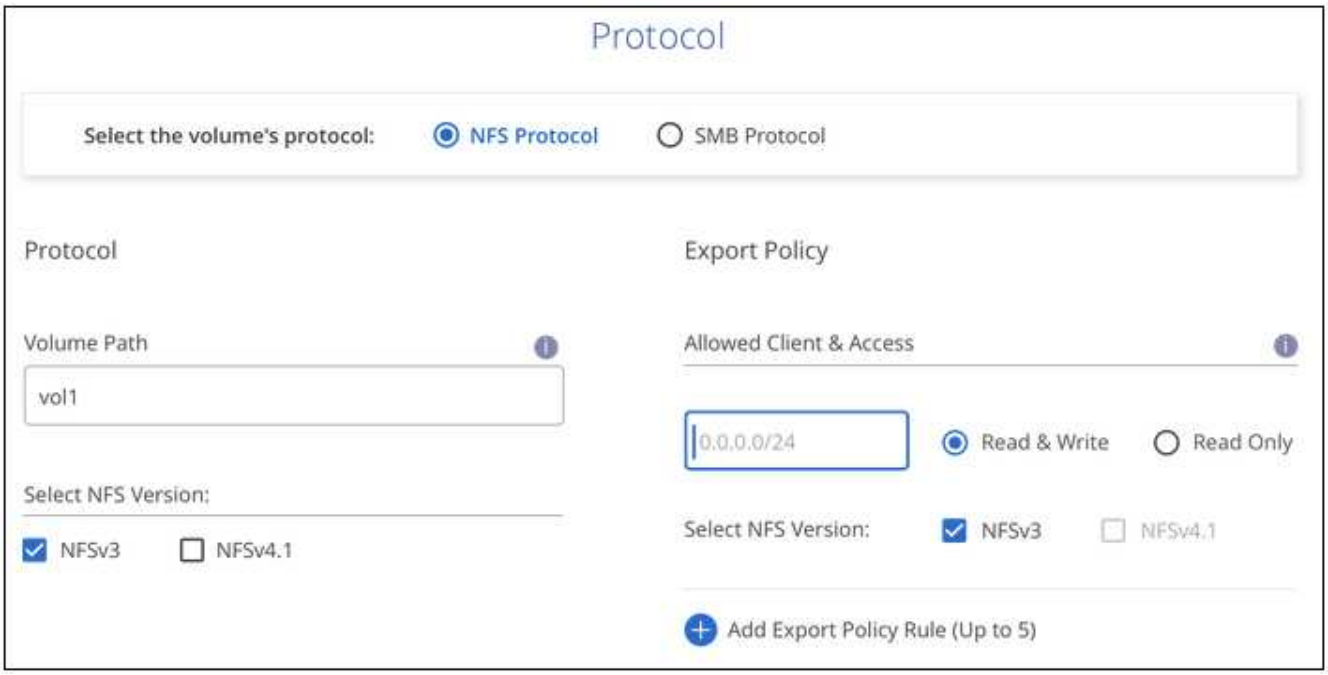


3. Wählen Sie auf der Seite Protokoll NFS oder SMB aus und definieren Sie die Details. Erforderliche Einträge für NFS und SMB sind in separaten Abschnitten unten dargestellt.
4. Für NFS:

   a. Geben Sie im Feld Volume Path den Namen des Volume-Exports an, den Sie beim Mounten des Volumes sehen werden.
   b. Wählen Sie NFSv3, NFSv4.1 oder beides nach Ihren Anforderungen aus.
   c. Optional können Sie eine Exportrichtlinie erstellen, um die Clients zu identifizieren, die auf das Volume zugreifen können. Geben Sie Folgendes an:
      - Zulässige Clients unter Verwendung einer IP-Adresse oder eines Classless Inter-Domain Routing (CIDR).
      - Zugriffsrechte als Lese- und Schreibgeschützt.

- Zugriffsprotokoll (oder Protokolle, wenn das Volume sowohl NFSv3 als auch NFSv4.1 Zugriff ermöglicht) für Benutzer verwendet.
- Klicken Sie auf **+ Add Export Policy Rule**, wenn Sie zusätzliche Exportrichtlinien-Regeln definieren möchten.

  Das folgende Bild zeigt die für das NFS-Protokoll ausgefüllte Volume-Seite:



5. Für SMB:

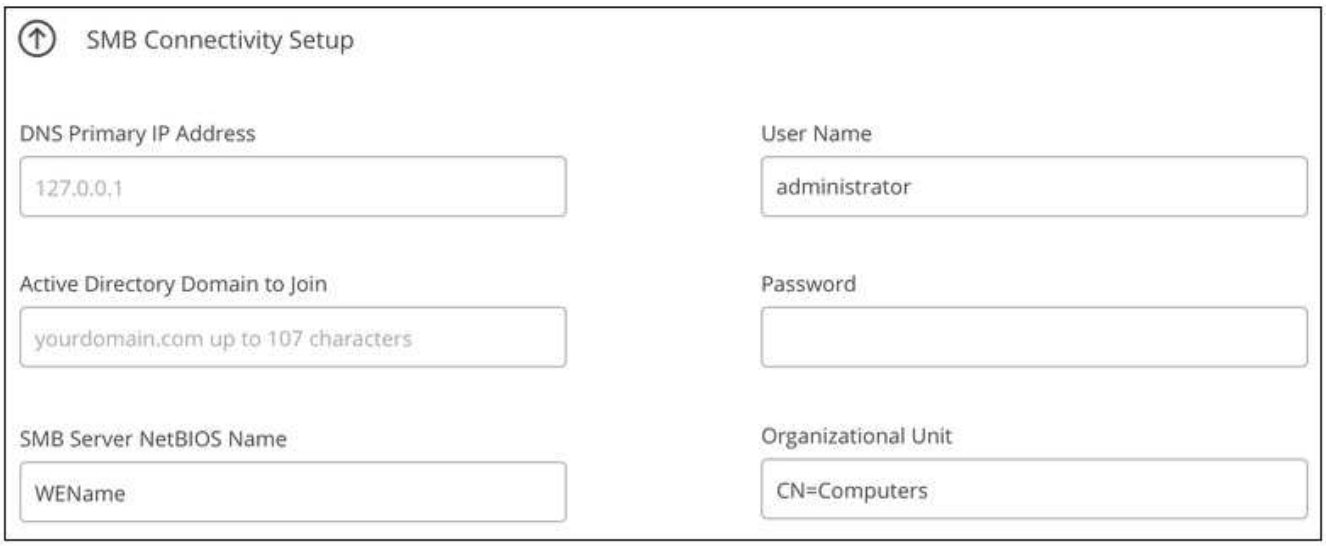
   a. Geben Sie im Feld Volume Path den Namen des Volume-Exports an, der beim Mounten des Volumes angezeigt wird, und klicken Sie auf **Continue**.

   b. Wenn Active Directory eingerichtet wurde, wird die Konfiguration angezeigt. Wenn es sich um das erste Volume handelt, das eingerichtet wurde und kein Active Directory eingerichtet wurde, können Sie die SMB-Sitzungsverschlüsselung auf der Seite SMB Connectivity Setup aktivieren:

Feld	Beschreibung
Primäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die eine Namensauflösung für den SMB-Server angeben. Verwenden Sie ein Komma, um die IP-Adressen zu trennen, wenn Sie auf mehrere Server verweisen, z. B. 172.31.25.223, 172.31.2.74.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domäne, der der SMB-Server beitreten soll.
SMB Server NetBIOS-Name	Ein NetBIOS-Name für den zu erstellenden SMB-Server.
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.

Feld	Beschreibung
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domäne, die mit dem SMB-Server verknüpft werden soll. Die Standardeinstellung ist CN=Computer für Verbindungen zu Ihrem eigenen Windows Active Directory Server.

Das folgende Bild zeigt die für das SMB-Protokoll ausgefüllte Volume-Seite:



6. Klicken Sie Auf **Weiter**.
7. Wenn Sie das Volume auf Grundlage eines Snapshots eines vorhandenen Volumes erstellen möchten, wählen Sie den Snapshot aus der Dropdown-Liste Snapshot Name aus. Ansonsten klicken Sie einfach auf **Weiter**.
8. Sie können auf der Seite Snapshot-Richtlinie Cloud Volumes Service aktivieren, um auf Grundlage eines Zeitplans Snapshot-Kopien Ihrer Volumes zu erstellen. Sie können dies jetzt tun, indem Sie den Wahlschalter nach rechts verschieben oder das Volume später bearbeiten, um die Snapshot-Richtlinie zu definieren.

   Siehe "Erstellen einer Snapshot-Richtlinie" Weitere Informationen zur Snapshot-Funktionalität.

9. Klicken Sie Auf **Volumen Hinzufügen**.

Das neue Volumen wird der Arbeitsumgebung hinzugefügt.

Weiter mit "Montieren des Cloud Volumes".

Und Cloud Volumes mounten

Sie können das Volume in einem Cloud Manager mounten und auf einem Host zugreifen, indem Sie die Anweisungen im Anschluss nehmen.

Hinweis: Bitte verwenden Sie das hervorgehobene Protokoll/Dialekt, das von Ihrem Kunden unterstützt wird.

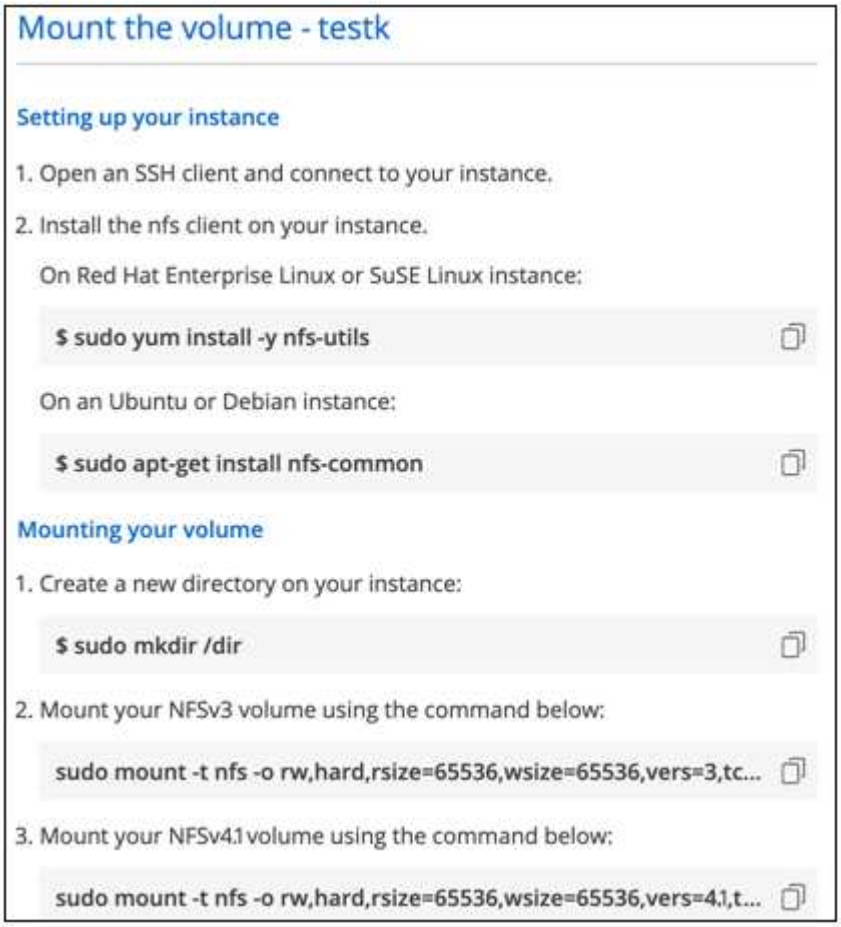
Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über die Lautstärke und klicken Sie auf **Mounten Sie die Lautstärke**.

Auf NFS- und SMB-Volumes werden Mount-Anweisungen für dieses Protokoll angezeigt.

3. Bewegen Sie den Mauszeiger über die Befehle und kopieren Sie sie in die Zwischenablage, um diesen Prozess zu vereinfachen. Fügen Sie einfach das Zielverzeichnis / den Bereitstellungspunkt am Ende des Befehls hinzu.

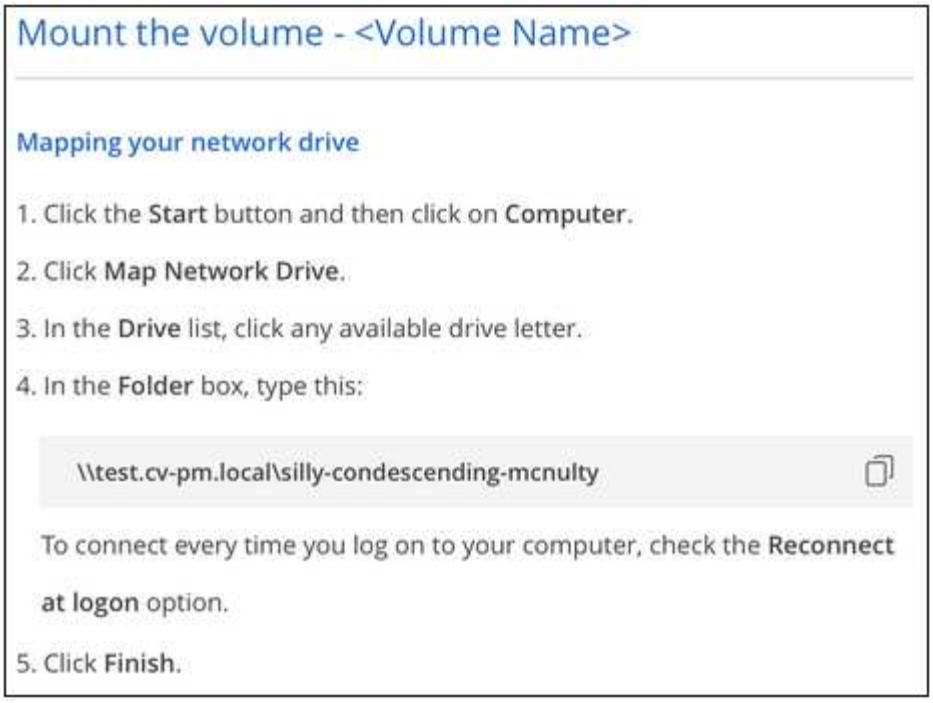
   NFS-Beispiel:



   Die von definierte maximale I/O-Größe `rsize` Und `wsize` Optionen sind 1048576, allerdings wird für die meisten Anwendungsfälle der empfohlene Standardwert von 65536 verwendet.

   Beachten Sie, dass Linux-Clients standardmäßig auf NFSv4.1 gesetzt werden, es sei denn, die Version wird mit dem angegeben `vers=<nfs_version>` Option.

   SMB-Beispiel:



4. Ordnen Sie Ihr Netzlaufwerk zu, indem Sie den Mount-Anweisungen für Ihre Instanz folgen.

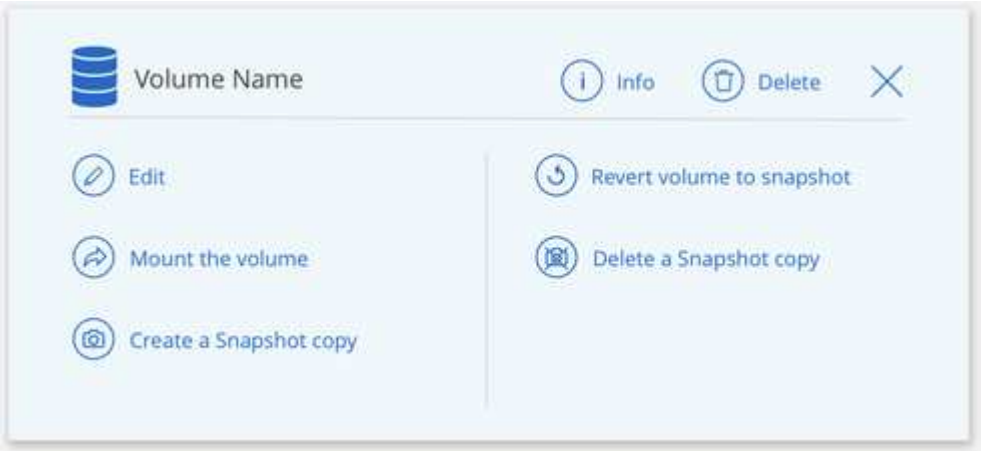
   Nach Abschluss der Schritte in der Mount-Anleitung ist das Cloud-Volume erfolgreich in die GCP-Instanz eingebunden.

Management vorhandener Volumes

Sie können vorhandene Volumes managen, wenn sich Ihre Storage-Anforderungen ändern. Sie können Volumes anzeigen, bearbeiten, wiederherstellen und löschen.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Zeigen Sie den Mauszeiger auf das Volume.



3. Managen Sie Ihre Volumes:

Aufgabe	Aktion
Anzeigen von Informationen zu einem Volume	Klicken Sie Auf **Info**.
Bearbeiten eines Volumes (einschließlich Snapshot-Richtlinie)	a. Klicken Sie Auf **Bearbeiten**. b. Ändern Sie die Eigenschaften des Volumes und klicken Sie dann auf **Update**.
Holen Sie den NFS- oder SMB-Mount-Befehl	a. Klicken Sie auf **Montierung des Volumens**. b. Klicken Sie auf **Kopieren**, um den Befehl(en) zu kopieren.
Erstellen Sie bei Bedarf eine Snapshot Kopie	a. Klicken Sie auf **Snapshot Kopie erstellen**. b. Ändern Sie ggf. den Namen und klicken Sie dann auf **Erstellen**.
Ersetzen Sie das Volume durch den Inhalt einer Snapshot Kopie	a. Klicken Sie auf **Volume auf Snapshot zurücksetzen**. b. Wählen Sie eine Snapshot Kopie aus und klicken Sie auf **Wiederherstellen**.
Löschen einer Snapshot Kopie	a. Klicken Sie auf **Snapshot Kopie löschen**. b. Wählen Sie den Snapshot aus und klicken Sie auf **Löschen**. c. Klicken Sie erneut auf **Löschen**, wenn Sie zur Bestätigung aufgefordert werden.
Löschen Sie ein Volume	a. Heben Sie die Bereitstellung des Volumes von allen Clients ab: ◦ Verwenden Sie unter Linux-Clients das `umount` Befehl. ◦ Klicken Sie unter Windows-Clients auf **Netzlaufwerk trennen**. b. Wählen Sie ein Volume aus, und klicken Sie dann auf **Löschen**. c. Klicken Sie zur Bestätigung erneut auf **Löschen**.

Entfernen Sie Cloud Volumes Service aus Cloud Manager

Sie können ein Cloud Volumes Service für Google Cloud Abonnement und alle vorhandenen Volumes aus Cloud Manager entfernen. Die Volumes werden nicht gelöscht, sie werden einfach aus der Cloud Manager Schnittstelle entfernt.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Klicken Sie auf das Klicken Sie oben auf der Seite auf **Cloud Volumes Service entfernen**.
3. Klicken Sie im Bestätigungsdialogfeld auf **Entfernen**.

Active Directory-Konfiguration verwalten

Wenn Sie Ihre DNS-Server oder Active Directory-Domäne ändern, müssen Sie den SMB-Server in Cloud Volumes Services ändern, damit dieser weiterhin Storage für Clients bereitstellen kann.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Klicken Sie auf das Klicken Sie oben auf der Seite auf **Active Directory verwalten**. Wenn kein Active Directory konfiguriert ist, können Sie jetzt ein Verzeichnis hinzufügen. Wenn eine konfiguriert ist, können Sie die Einstellungen mit dem ändern oder löschen Schaltfläche.
3. Legen Sie die Einstellungen für den SMB-Server fest:

Feld	Beschreibung
Primäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die eine Namensauflösung für den SMB-Server angeben. Verwenden Sie ein Komma, um die IP-Adressen zu trennen, wenn Sie auf mehrere Server verweisen, z. B. 172.31.25.223, 172.31.2.74.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domäne, der der SMB-Server beitreten soll.
SMB Server NetBIOS-Name	Ein NetBIOS-Name für den zu erstellenden SMB-Server.
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.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domäne, die mit dem SMB-Server verknüpft werden soll. Die Standardeinstellung ist CN=Computer für Verbindungen zu Ihrem eigenen Windows Active Directory Server.

4. Klicken Sie auf **Speichern**, um Ihre Einstellungen zu speichern.

Managen von Cloud Volumes Snapshots

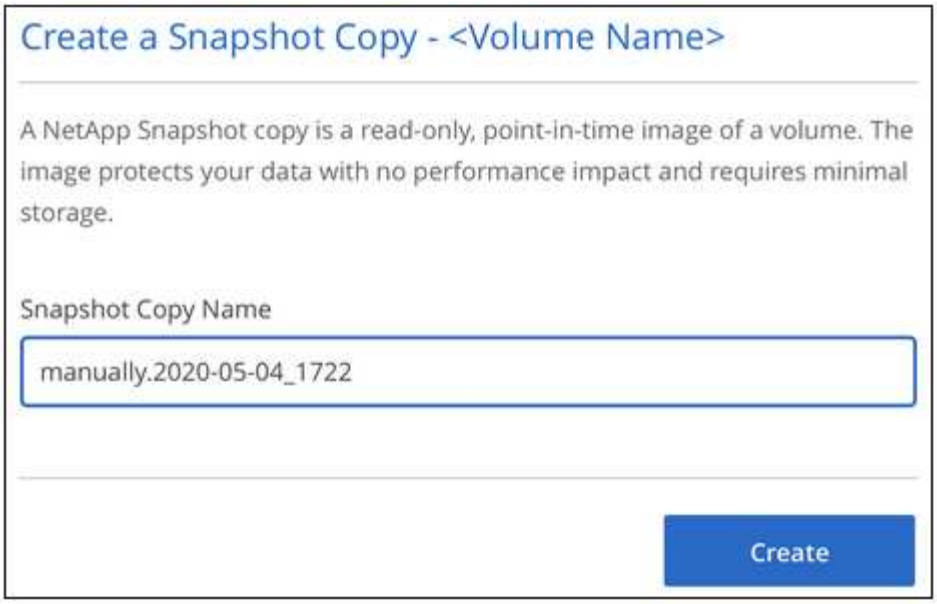
Sie können für jedes Volume eine Snapshot-Richtlinie erstellen, sodass Sie den gesamten Inhalt eines Volumes von einer früheren Zeit wiederherstellen können. Bei Bedarf können Sie auch einen On-Demand Snapshot eines Cloud Volumes erstellen.

Erstellen Sie einen On-Demand Snapshot

Sie können einen On-Demand-Snapshot eines Cloud Volumes erstellen, wenn Sie einen Snapshot im aktuellen Volume-Zustand erstellen möchten.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über den Datenträger und klicken Sie auf **Erstellen Sie eine Snapshot Kopie**.
3. Geben Sie einen Namen für den Snapshot ein, oder verwenden Sie den automatisch generierten Namen, und klicken Sie auf **Erstellen**.



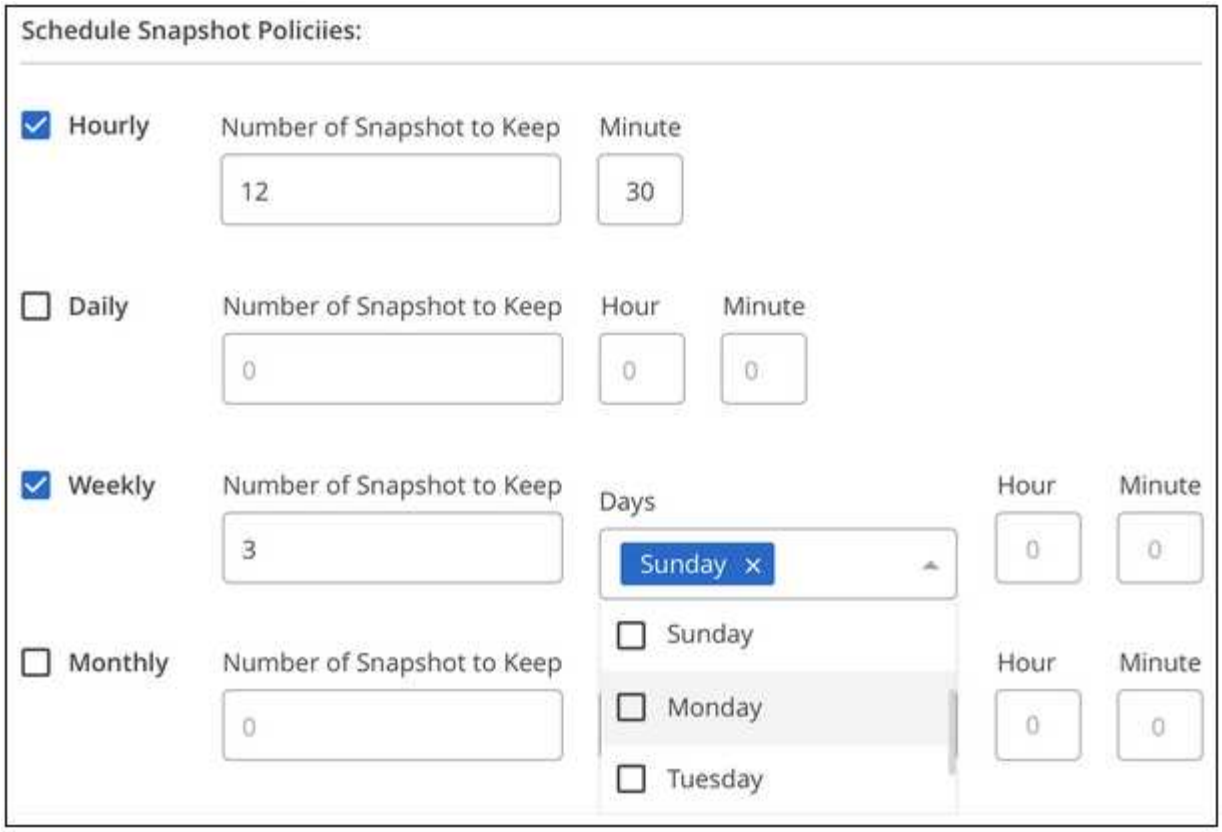
Der Snapshot wird erstellt.

Erstellen oder Ändern einer Snapshot-Richtlinie

Sie können je nach Bedarf eine Snapshot-Richtlinie für ein Cloud-Volume erstellen oder ändern. Sie definieren die Snapshot-Richtlinie auf der Registerkarte „*Snapshot Policy*“ entweder beim Erstellen eines Volumes oder beim Bearbeiten eines Volumes.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über die Lautstärke und klicken Sie auf **Bearbeiten**.
3. Verschieben Sie auf der Registerkarte „*Snapshot Policy*“ den Schieberegler zum Aktivieren der Snapshots nach rechts.
4. Legen Sie den Zeitplan für Snapshots fest:
   a. Wählen Sie die Häufigkeit aus: **Stündlich**, **täglich**, **wöchentlich** oder **monatlich**
   b. Wählen Sie die Anzahl der Schnappschüsse aus, die beibehalten werden sollen.
   c. Wählen Sie den Tag, die Stunde und die Minute aus, an dem der Snapshot erstellt werden soll.



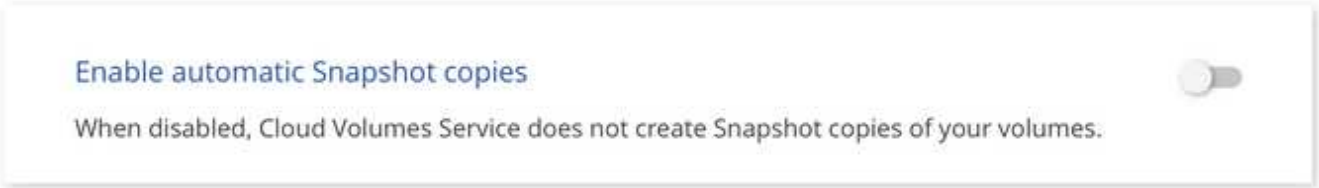
5. Klicken Sie auf **Add Volume** oder **Update Volume**, um Ihre Richtlinieneinstellungen zu speichern.

Deaktivieren einer Snapshot-Richtlinie

Sie können eine Snapshot-Richtlinie deaktivieren, um die Erstellung von Snapshots für einen kurzen Zeitraum zu verhindern, während Ihre Snapshot-Richtlinieneinstellungen beibehalten werden.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über die Lautstärke und klicken Sie auf **Bearbeiten**.
3. Verschieben Sie auf der Registerkarte „*Snapshot Policy*“ den Schieberegler „Snapshots aktivieren“ nach links.



4. Klicken Sie auf **Lautstärke aktualisieren**.

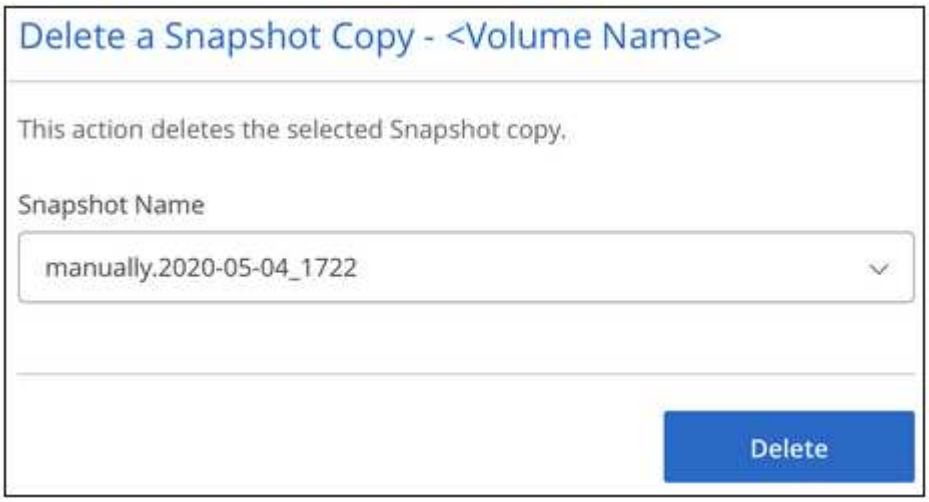
Wenn Sie die Snapshot-Richtlinie wieder aktivieren möchten, verschieben Sie den Schieberegler Snapshots aktivieren nach rechts und klicken Sie auf **Datenträger aktualisieren**.

Löschen Sie einen Snapshot

Sie können einen Snapshot löschen, wenn er nicht mehr benötigt wird.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über das Volume und klicken Sie auf **Löschen einer Snapshot Kopie**.
3. Wählen Sie den Snapshot aus der Dropdown-Liste aus und klicken Sie auf **Löschen**.



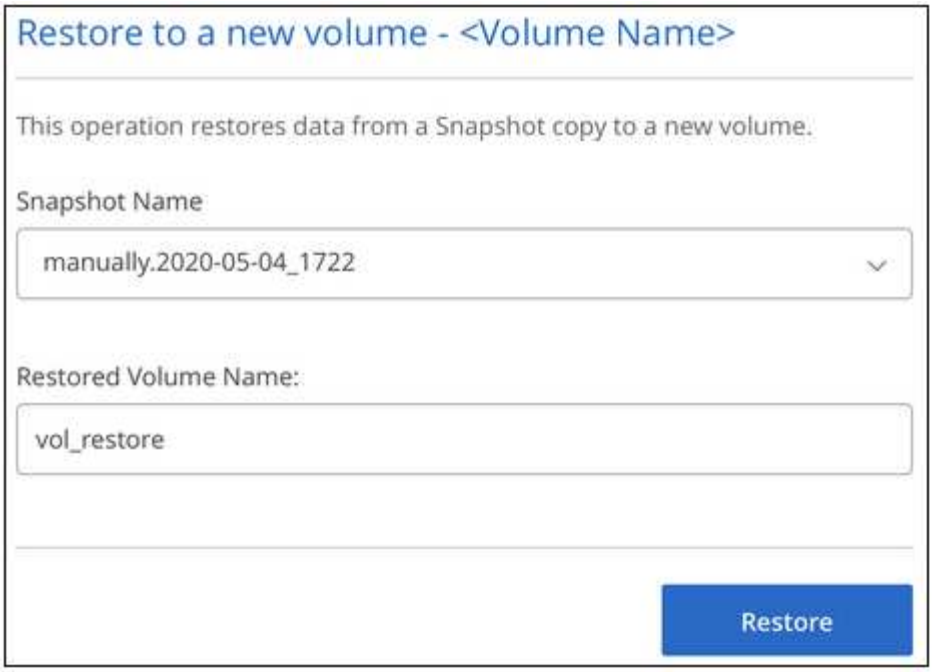
4. Klicken Sie im Bestätigungsdialogfeld auf **Löschen**.

Wiederherstellung eines Snapshots auf einem neuen Volume

Sie können bei Bedarf einen Snapshot auf einem neuen Volume wiederherstellen.

Schritte

1. Öffnen Sie die Arbeitsumgebung.
2. Bewegen Sie den Mauszeiger über das Volume und klicken Sie auf **auf ein neues Volume wiederherstellen**.
3. Wählen Sie den Snapshot aus der Dropdown-Liste aus, den Sie zum Erstellen des neuen Volumes verwenden möchten.
4. Geben Sie einen Namen für das neue Volume ein und klicken Sie auf **Wiederherstellen**.



Das Volume wird in der Arbeitsumgebung erstellt.

5. Falls Sie eines der Volume-Attribute wie Volume-Pfad oder Service Level ändern müssen:
   a. Bewegen Sie den Mauszeiger über die Lautstärke und klicken Sie auf **Bearbeiten**.
   b. Nehmen Sie Ihre Änderungen vor und klicken Sie auf **Lautstärke aktualisieren**.

Nachdem Sie fertig sind

Weiter mit "Montieren des Cloud Volumes".

Verwalten Sie ONTAP Cluster

Erkennung 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. Die Entdeckung eines ONTAP Clusters ermöglicht die Provisionierung von Storage, Replizierung von Daten, Backup von Daten und das Tiering selten genutzter Daten aus einem lokalen Cluster in die Cloud.

Was Sie benötigen

- Ein Connector, der bei einem Cloud-Provider oder vor Ort installiert ist.

  Wenn kalte Daten in die Cloud verschoben werden sollen, sollten Sie die Anforderungen für den Connector prüfen, je nachdem, wo Sie kalte Daten Tiering möchten.

  - "Erfahren Sie mehr über Steckverbinder"
  - "Wechseln zwischen den Anschlüssen"
  - "Erfahren Sie mehr über Cloud Tiering"

- Die Cluster-Management-IP-Adresse und das Passwort für das Admin-Benutzerkonto, um das Cluster zu Cloud Manager hinzuzufügen.

  Cloud Manager erkennt ONTAP Cluster mithilfe von HTTPS. Wenn Sie benutzerdefinierte Firewall-Richtlinien verwenden, müssen diese die folgenden Anforderungen erfüllen:

  - Der Connector-Host muss ausgehenden HTTPS-Zugriff über Port 443 ermöglichen.

    Wenn sich der Connector in der Cloud befindet, ist die gesamte ausgehende Kommunikation durch die vordefinierte Sicherheitsgruppe zulässig.

  - Der ONTAP Cluster muss eingehenden HTTPS-Zugriff über Port 443 zulassen.

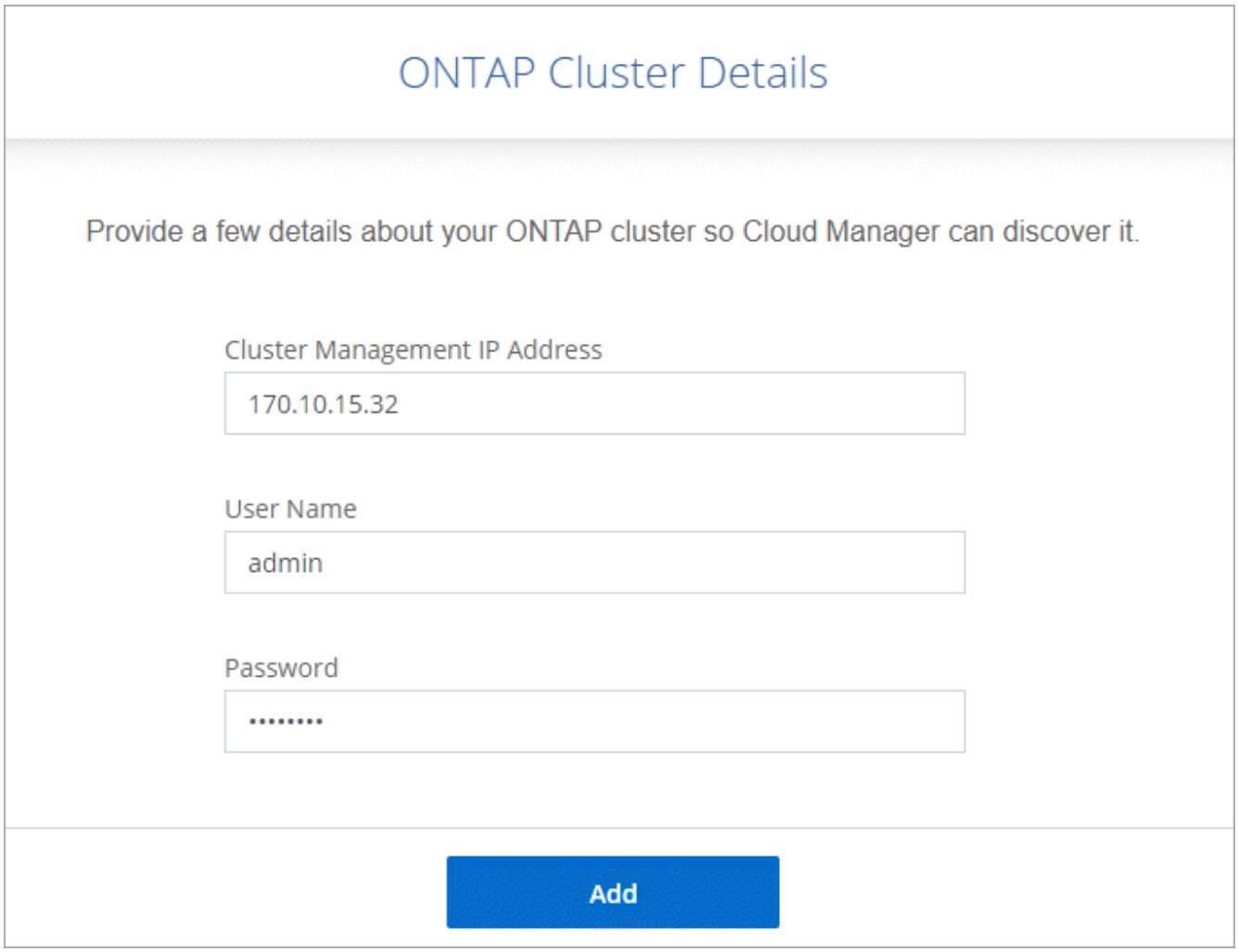
    Die standardmäßige "mgmt"-Firewall-Richtlinie ermöglicht eingehenden HTTPS-Zugriff von allen IP-Adressen. Wenn Sie diese Standardrichtlinie geändert haben oder wenn Sie eine eigene Firewall-Richtlinie erstellt haben, müssen Sie das HTTPS-Protokoll mit dieser Richtlinie verknüpfen und den Zugriff über den Connector-Host aktivieren.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen** und wählen Sie **On-Premise ONTAP**.
2. Wenn Sie dazu aufgefordert werden, erstellen Sie einen Konnektor.

   Weitere Informationen erhalten Sie über die obigen Links.

3. Geben Sie auf der Seite **ONTAP-Cluster-Details** die Cluster-Management-IP-Adresse, das Passwort für das Admin-Benutzerkonto und den Standort des Clusters ein.



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 in den und aus dem Cluster replizieren, Daten-Tiering in die Cloud einrichten, Volumes in der Cloud sichern und System Manager starten, um erweiterte Aufgaben auszuführen.

Managen von Storage für ONTAP-Cluster

Nachdem Sie den ONTAP Cluster von Cloud Manager entdeckt haben, können Sie die Arbeitsumgebung für das Bereitstellen und Managen von Storage öffnen.

Erstellen von Volumes für ONTAP Cluster

Cloud Manager ermöglicht die Bereitstellung von NFS-, CIFS- und iSCSI-Volumes auf ONTAP Clustern.

Bevor Sie beginnen

Die Datenprotokolle müssen über System Manager oder die CLI auf dem Cluster eingerichtet werden.

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.
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.
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.
Initiatorgruppe und IQN (nur für iSCSI)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt Cloud Manager automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Nachdem Sie das Volume erstellt haben, wählen Sie es aus, klicken Sie auf Ziel-IQN, und verwenden Sie dann den IQN, um eine Verbindung zur LUN von Ihren Hosts herzustellen.
Nutzungsprofil	Mithilfe von Nutzungsprofilen werden die NetApp Storage-Effizienzfunktionen definiert, die für ein Volume aktiviert sind.

Datenreplizierung

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.

"Klicken Sie hier, um weitere Informationen zu erhalten".

Daten werden gesichert

Über den Cloud Manager Backup to Cloud Service können Sie Daten-Backups von Ihrem lokalen ONTAP System auf kostengünstigen Objekt-Storage in der Cloud erstellen. Dieser Service bietet Backup- und Restore-Funktionen zum Schutz und zum langfristigen Archiv Ihrer Cloud-Daten.

"Klicken Sie hier, um weitere Informationen zu erhalten".

Daten-Tiering in die Cloud

Erweitern Sie Ihr Datacenter in die Cloud durch das automatische Tiering inaktiver Daten von ONTAP Clustern in Objekt-Storage.

"Klicken Sie hier, um weitere Informationen zu erhalten".

Backup in die Cloud

Erfahren Sie mehr über Backup in der Cloud

Der Add-on-Service für Cloud Volumes ONTAP und ONTAP Cluster vor Ort bietet Backup- und Restore-Funktionen zur Sicherung und zum langfristigen Archiv Ihrer Cloud-Daten. Backups werden in einem Objektspeicher in Ihrem Cloud-Konto gespeichert, unabhängig von Volume Snapshot Kopien für die kurzfristige Wiederherstellung oder das Klonen.

Backup in der Cloud wird von dem unterstützt "Cloud-Backup-Service".

Alle Backup- und Restore-Vorgänge müssen mit Cloud Manager durchgeführt werden. Alle Maßnahmen, die direkt von ONTAP oder Ihrem Cloud-Provider ausgeführt werden, führen zu einer nicht unterstützten Konfiguration.

Funktionen

- Erstellen Sie unabhängige Kopien Ihrer Datenvolumen in der Cloud auf kostengünstigen Objekt-Storage.
- Backup-Daten werden mit AES-256-Bit-Verschlüsselung im Ruhezustand und TLS 1.2 HTTPS-Verbindungen im Übertragungsprozess gesichert.
- Backup von der Cloud in die Cloud und von lokalen ONTAP Systemen in die Cloud.
- Unterstützung für bis zu 1,019 Backups eines einzelnen Volumes.
- Wiederherstellung von Daten aus einem bestimmten Zeitpunkt
- Stellen Sie die Daten auf einem Volume im Quellsystem oder einem anderen System wieder her.

Unterstützte Arbeitsumgebungen und Objekt-Storage-Anbieter

Backup in der Cloud wird mit den folgenden Arbeitsumgebungen unterstützt:

- Cloud Volumes ONTAP in AWS
- Cloud Volumes ONTAP in Azure
- On-Premises ONTAP Cluster

Kosten

Backup in der Cloud ist in zwei Preisoptionen erhältlich: Bring Your Own License (BYOL) und Pay as you Go (PAYGO).

Bei BYOL bezahlen Sie NetApp für den Service für einen Zeitraum von 6 Monaten und für eine maximale Backup-Kapazität von 10 GB (vor der Storage-Effizienz). Sie müssen dann Ihren Cloud-Provider für Objekt-Storage-Kosten bezahlen. Sie erhalten eine Seriennummer, die Sie auf der Seite „Cloud Manager Licensing“ eingeben, um den Service zu aktivieren. Wenn eine der beiden Limits erreicht ist, müssen Sie die Lizenz erneuern. Siehe "Hinzufügen und Aktualisieren der Backup-BYOL-Lizenz". Die BYOL-Lizenz für Backup gilt für alle mit dem verbundenen Cloud Volumes ONTAP-Systeme "Cloud Central Konto".

Bei PAYGO müssen Sie Ihren Cloud-Provider für Objekt-Storage-Kosten und NetApp für Backup-Lizenzkosten bezahlen. Die Lizenzkosten basieren auf der genutzten Kapazität (vor der Nutzung von Storage-Effizienz):

- AWS, "Weitere Informationen zu den Preisen finden Sie im Cloud Manager Marketplace Angebot".
- Azure: "Weitere Informationen zu den Preisen finden Sie im Cloud Manager Marketplace Angebot".

Kostenlose Testversion

Eine kostenlose 30-Tage-Testversion ist erhältlich. Wenn Sie die Testversion verwenden, werden Sie über die Anzahl der noch freien Testtage informiert. Am Ende Ihrer kostenlosen Testversion werden Backups nicht mehr erstellt. Sie müssen den Service abonnieren oder eine Lizenz erwerben, um den Service weiterhin nutzen zu können.

Die Sicherung wird nicht gelöscht, wenn der Dienst deaktiviert ist. Cloud-Provider stellen weiterhin die Kosten für Objekt-Storage für die von Ihren Backups verwendete Kapazität in Rechnung, es sei denn, die Backups werden gelöscht.

So funktioniert Backup in der Cloud

Wenn Sie das Backup in der Cloud auf einem Cloud Volumes ONTAP- oder lokalen ONTAP-System aktivieren, führt der Service ein vollständiges Backup Ihrer Daten durch. Volume Snapshots werden nicht im Backup-Image berücksichtigt. Nach dem ersten Backup sind alle weiteren Backups inkrementell, das heißt, dass nur geänderte Blöcke und neue Blöcke gesichert werden.

Speicherort von Backups

Backup-Kopien werden in einem S3-Bucket oder Azure Blob-Container gespeichert, den Cloud Manager in Ihrem Cloud-Konto erstellt. Bei Cloud Volumes ONTAP Systemen wird der Objektspeicher in derselben Region erstellt, in der sich das Cloud Volumes ONTAP System befindet. Bei ONTAP-Systemen vor Ort identifizieren Sie die Region, wenn Sie den Service aktivieren.

Ein Objektspeicher pro Cloud Volumes ONTAP oder ein On-Premises ONTAP System steht zur Verfügung. Cloud Manager benennt den Objektspeicher wie folgt: netapp-Backup-*clusterUUID*

Stellen Sie sicher, dass Sie diesen Objektspeicher nicht löschen.

Hinweise:

- In AWS ermöglicht Cloud Manager das "Amazon S3 Block – Public Access-Funktion" Auf dem S3-Bucket.
- In Azure verwendet Cloud Manager eine neue oder vorhandene Ressourcengruppe mit einem Storage-Konto für den Blob-Container.

Unterstützte S3-Storage-Klassen

In Amazon S3 beginnen Backups in der Klasse „ *Standard* Storage“ und wechseln nach 30 Tagen zur Storage-Klasse „ *Standard-infrequent Access*“.

Unterstützte Azure Blob-Zugriffsebenen

In Azure ist jedes Backup der „*Cold* Access Tier“ zugeordnet.

Backup-Einstellungen sind systemweit

Wenn Sie Backup in der Cloud aktivieren, werden alle Volumes, die Sie im System identifizieren, in der Cloud gesichert.

Der Zeitplan und die Anzahl der zu behaltenden Backups werden auf Systemebene festgelegt. Die Backup-

Einstellungen wirken sich auf alle Volumes im System aus.

Der Zeitplan ist täglich, wöchentlich, monatlich oder eine Kombination

Sie können tägliche, wöchentliche oder monatliche Backups aller Volumes auswählen. Sie haben außerdem die Wahl zwischen einer der systemdefinierten Richtlinien, die 3 Monate, 1 Jahr und 7 Jahre Backups und Aufbewahrung bieten. Im Folgenden werden die Richtlinien aufgeführt:

Name Der Richtlinie	Backups pro Intervall…			Maximale Backups
	* Daily*	Wöchentlich	Monatlich	
Netapp3MonatDatenhaltung	30	13	3	46
Netapp1YearRetention	30	13	12	55
Netapp7YearsRetention	30	53	84	167

Sobald Sie die maximale Anzahl von Backups für eine Kategorie oder ein Intervall erreicht haben, werden ältere Backups entfernt, sodass Sie immer über die aktuellsten Backups verfügen.

Beachten Sie, dass die Aufbewahrungsdauer für Backups von Datensicherungs-Volumes identisch ist mit der in der SnapMirror Quell-Beziehung definierten Aufbewahrungsdauer. Sie können dies gegebenenfalls mithilfe der API ändern.

Backups werden um Mitternacht erstellt

- Tägliche Backups beginnen jeden Tag kurz nach Mitternacht.
- Wöchentliche Backups beginnen direkt nach Mitternacht am Sonntagmorgen.
- Monatliche Backups beginnen knapp nach Mitternacht am ersten jedes Monats.

Zu diesem Zeitpunkt können Sie keine Backup-Operationen zu einem vom Benutzer bestimmten Zeitpunkt planen.

Backup-Kopien sind mit Ihrem Cloud Central Konto verknüpft

Backup-Kopien sind dem zugewiesen "Cloud Central Konto" In der sich Cloud Manager befindet.

Wenn sich mehrere Cloud Manager Systeme im selben Cloud Central Konto befinden, zeigt jedes Cloud Manager System dieselbe Liste von Backups an. Dazu gehören auch die Backups, die mit Cloud Volumes ONTAP und lokalen ONTAP Instanzen aus anderen Cloud Manager Systemen verbunden sind.

Überlegungen zu BYOL-Lizenzen

Bei Verwendung einer BYOL-Lizenz für Backup in der Cloud benachrichtigt Sie Cloud Manager, wenn sich Backups dem Kapazitätslimit nähern oder sich dem Ablaufdatum der Lizenz nähern. Sie erhalten folgende Benachrichtigungen:

- Wenn Backups 80 % der lizenzierten Kapazität erreicht haben, und noch einmal, wenn Sie die Obergrenze erreicht haben
- 30 Tage, bevor eine Lizenz abläuft, und wieder, wenn die Lizenz abläuft

Verwenden Sie das Chat-Symbol rechts unten in der Cloud Manager-Schnittstelle, um Ihre Lizenz zu verlängern, wenn Sie diese Benachrichtigungen erhalten.

Zwei Dinge können passieren, wenn Ihre Lizenz abläuft:

- Wenn das Konto, das Sie für Ihre ONTAP-Systeme nutzen, über ein Marketplace-Konto verfügt, läuft der Backup-Service weiter, wird jedoch von einem PAYGO-Lizenzmodell übernommen. Sie zahlen durch Ihren Cloud-Provider für Objekt-Storage-Kosten und durch NetApp für Backup-Lizenzkosten für die Kapazität, die Ihre Backups verwenden.
- Wenn das Konto, das Sie für Ihre ONTAP Systeme verwenden, kein Marketplace-Konto hat, läuft der Backup-Service weiter, Sie erhalten jedoch weiterhin die Ablaufdatum.

Nach der Erneuerung des BYOL-Abonnements erhält Cloud Manager automatisch die neue Lizenz von NetApp und installiert sie. Wenn Cloud Manager nicht über die sichere Internetverbindung auf die Lizenzdatei zugreifen kann, können Sie die Datei selbst beziehen und sie manuell in Cloud Manager hochladen. Anweisungen hierzu finden Sie unter "Hinzufügen und Aktualisieren der Backup-BYOL-Lizenz".

Systeme, die auf eine PAYGO-Lizenz verschoben wurden, werden automatisch an die BYOL-Lizenz zurückgegeben. Systeme, die ohne Lizenz ausgeführt wurden, erhalten die Warnmeldung nicht mehr und werden für Backups belastet, die während des Lizenzzeitraums aufgetreten sind.

Unterstützte Volumes

Backup in der Cloud unterstützt Volumes mit Lese- und Schreibvorgängen sowie Datensicherungs-Volumes (DP).

FlexGroup Volumes werden derzeit nicht unterstützt.

Einschränkungen

- WORM Storage (SnapLock) wird nicht auf einem Cloud Volumes ONTAP oder On-Premises-System unterstützt, wenn Backup in der Cloud aktiviert ist.
- Einschränkungen bei Backups von lokalen ONTAP-Systemen in die Cloud:
  - Der On-Prem-Cluster muss ONTAP 9.7P5 oder höher ausführen.
  - Cloud Manager muss auf Azure implementiert werden. Für lokale Cloud Manager Implementierungen wird keine Unterstützung geboten.
  - Der Zielspeicherort für Backups ist nur Objekt-Storage auf Azure.
  - Backups können nur auf in Azure implementierten Cloud Volumes ONTAP Systemen wiederhergestellt werden. Das Backup kann nicht auf einem lokalen ONTAP System oder auf einem Cloud Volumes ONTAP System mit einem anderen Cloud-Provider wiederhergestellt werden.
- Bei der Sicherung von Datensicherungs-Volumes (DP) muss die für die SnapMirror-Richtlinie definierte Regel auf dem Quell-Volume ein Etikett verwenden, das mit den zulässigen Backup in Cloud-Richtlinien * Daily*, **Weekly** oder **monthly** übereinstimmt. Ansonsten wird der Backup für das DP-Volume fehlschlagen.
- Wenn Sie in Azure Backup in Cloud aktivieren, wenn Cloud Volumes ONTAP bereitgestellt wird, erstellt Cloud Manager die Ressourcengruppe für Sie, und Sie können sie nicht ändern. Wenn Sie Ihre eigene Ressourcengruppe auswählen möchten, wenn Sie Backup in Cloud aktivieren, **deaktivieren** Backup in Cloud bei der Bereitstellung von Cloud Volumes ONTAP und aktivieren dann Backup in Cloud und wählen Sie die Ressourcengruppe aus der Seite Backup in Cloud Einstellungen.
- Beim Backup von Volumes aus Cloud Volumes ONTAP Systemen werden die außerhalb von Cloud Manager erstellten Volumes nicht automatisch gesichert.

  Wenn Sie beispielsweise ein Volume aus der ONTAP CLI, der ONTAP API oder dem System Manager erstellen, wird das Volume nicht automatisch gesichert.

Wenn Sie diese Volumes sichern möchten, müssen Sie Backup in Cloud deaktivieren und dann erneut aktivieren.

Los geht's

Daten-Backups in Amazon S3 sichern

Führen Sie einige Schritte aus, um mit dem Backup von Daten von Cloud Volumes ONTAP in Amazon S3 zu beginnen.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

Überprüfen Sie die Unterstützung Ihrer Konfiguration

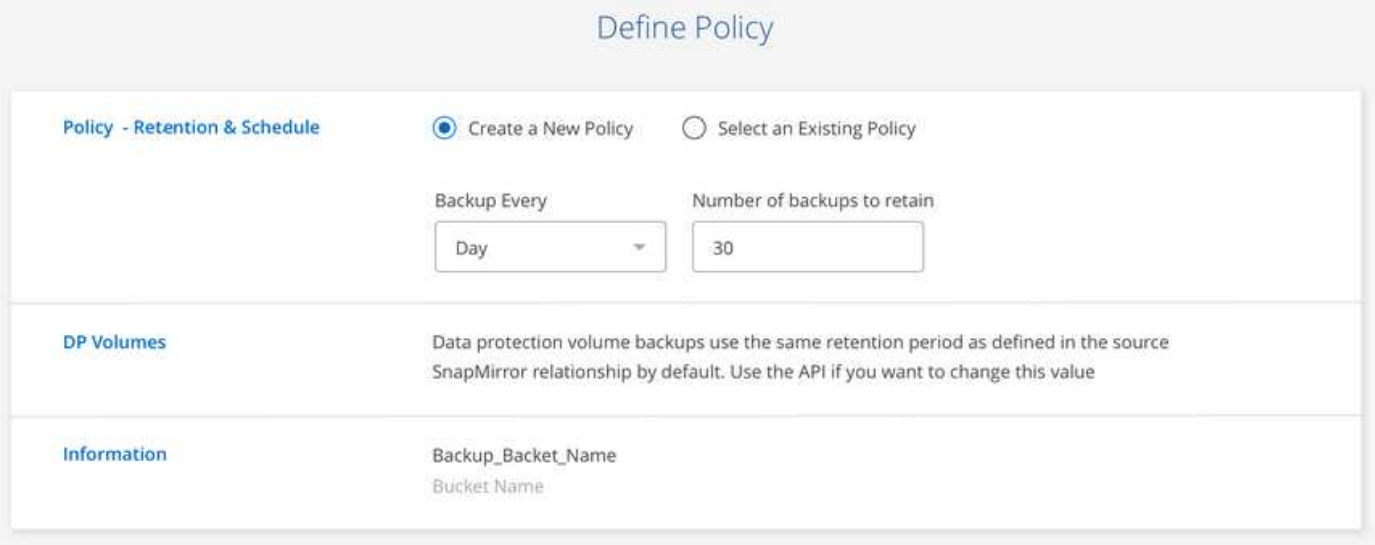
- Cloud Volumes ONTAP 9.6 oder höher wird in AWS ausgeführt.
- Sie haben sich für das angemeldet "Cloud Manager Marketplace Backup-Angebot", Oder Sie haben gekauft "Und aktiviert" Eine BYOL-Lizenz für Backup in der Cloud von NetApp
- Die IAM-Rolle, die Cloud Manager Berechtigungen bereitstellt, umfasst die neuesten S3-Berechtigungen "Cloud Manager-Richtlinie".

Aktivieren Sie Backup in der Cloud auf Ihrem neuen oder vorhandenen System

- Neue Systeme: Backup in der Cloud ist standardmäßig im Assistenten für die Arbeitsumgebung aktiviert. Achten Sie darauf, dass die Option aktiviert bleibt.
- Bestehende Systeme: Wählen Sie die Arbeitsumgebung aus und klicken Sie auf **Aktivieren** neben dem Dienst Backup to Cloud im rechten Fenster, und folgen Sie dann dem Setup-Assistenten.

Definieren der Backup-Richtlinie

Die Standardrichtlinie sichert Volumes täglich und speichert die letzten 30 Backup-Kopien jedes Volumes. Ändern Sie zu wöchentlichen oder monatlichen Backups oder wählen Sie eine der systemdefinierten Richtlinien mit mehr Optionen aus. Sie können auch die Anzahl der beizubehaltenden Backup-Kopien ändern.

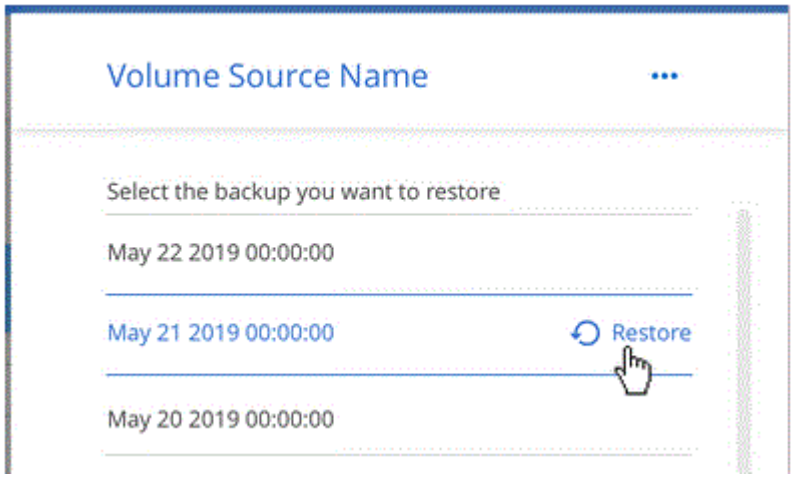


4 Wählen Sie die Volumes aus, die Sie sichern möchten

Legen Sie fest, welche Volumes Sie in der Seite Volumes auswählen sichern möchten.

5 Stellen Sie Ihre Daten nach Bedarf wieder her

Wählen Sie in der Sicherungsliste ein Volume aus, wählen Sie ein Backup aus und stellen Sie dann Daten aus dem Backup auf ein neues Volume wieder her.



Anforderungen

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie mit dem Backup von Volumes in S3 beginnen.

Unterstützte ONTAP-Versionen

Cloud Volumes ONTAP 9.6 und höher

Unterstützte AWS-Regionen

Backup in die Cloud wird in allen AWS Regionen unterstützt "Wobei Cloud Volumes ONTAP unterstützt wird".

Lizenzanforderungen

Bei der Lizenzierung von Backup in die Cloud-PAYGO ist im AWS Marketplace ein Cloud Manager-Abonnement verfügbar, das Implementierungen von Cloud Volumes ONTAP 9.6 und höher (PAYGO) und Backup in der Cloud ermöglicht. Sie müssen "Abonnieren Sie dieses Cloud Manager Abonnement" Vor Aktivierung von Backup in der Cloud. Die Abrechnung für Backup in der Cloud erfolgt über dieses Abonnement.

Für die BYOL-Lizenzierung von Backup in der Cloud benötigen Sie kein AWS Backup in der Cloud Abonnement. Sie benötigen die Seriennummer von NetApp, mit der Sie den Service für die Dauer und die Kapazität der Lizenz nutzen können. Siehe "Hinzufügen und Aktualisieren der Backup-BYOL-Lizenz".

Darüber hinaus müssen Sie über ein AWS Abonnement für den Speicherplatz verfügen, auf dem sich Ihre Backups befinden.

AWS Berechtigungen erforderlich

Die IAM-Rolle, die Cloud Manager über Berechtigungen verfügt, muss die neuesten S3-Berechtigungen enthalten "Cloud Manager-Richtlinie".

Hier sind die spezifischen Berechtigungen aus der Richtlinie:

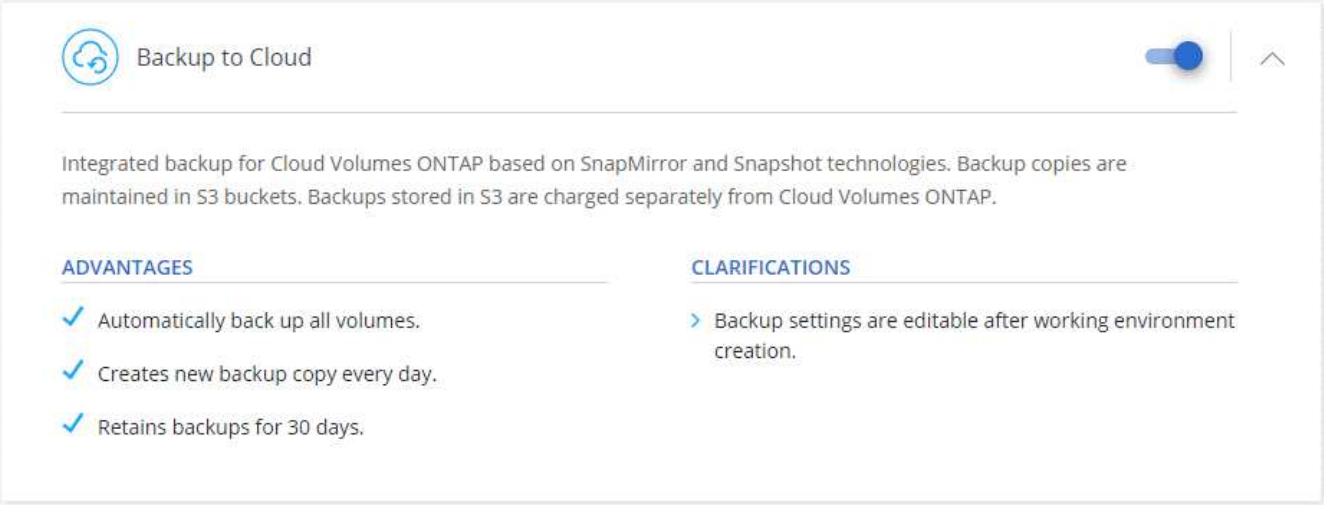
```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

Aktivieren von Backup in der Cloud auf einem neuen System

Backup in der Cloud ist standardmäßig im Assistenten für die Arbeitsumgebung aktiviert. Achten Sie darauf, dass die Option aktiviert bleibt.

Schritte

1. Klicken Sie auf **Cloud Volumes ONTAP erstellen**.
2. Wählen Sie Amazon Web Services als Cloud-Provider und wählen Sie dann einen einzelnen Node oder ein HA-System.
3. Füllen Sie die Seite „Details & Credentials“ aus.
4. Lassen Sie auf der Seite Dienste den Dienst aktiviert, und klicken Sie auf **Weiter**.



5. Führen Sie die Seiten im Assistenten aus, um das System bereitzustellen.

Ergebnis

Backup in der Cloud ist auf dem System aktiviert und sichert Volumes täglich und speichert die letzten 30 Backup-Kopien.

Was kommt als Nächstes?

"Sie können Backups managen, indem Sie den Backup-Zeitplan ändern, Volumes wiederherstellen und mehr".

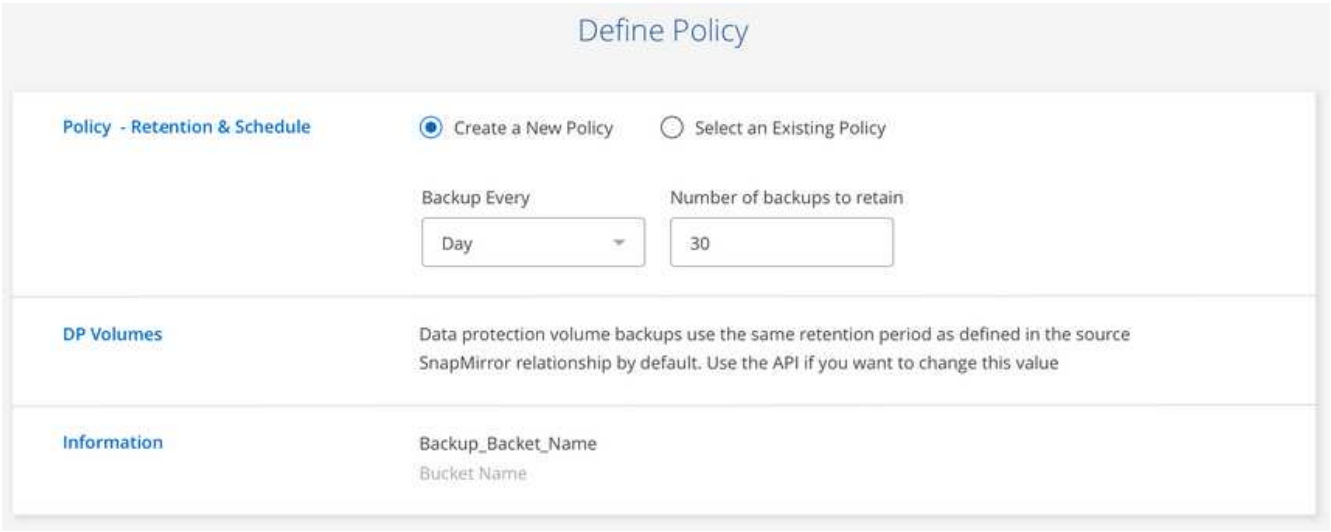
Aktivieren von Backup in der Cloud auf einem vorhandenen System

Sie können Backup in die Cloud jederzeit direkt aus der Arbeitsumgebung aktivieren.

Schritte

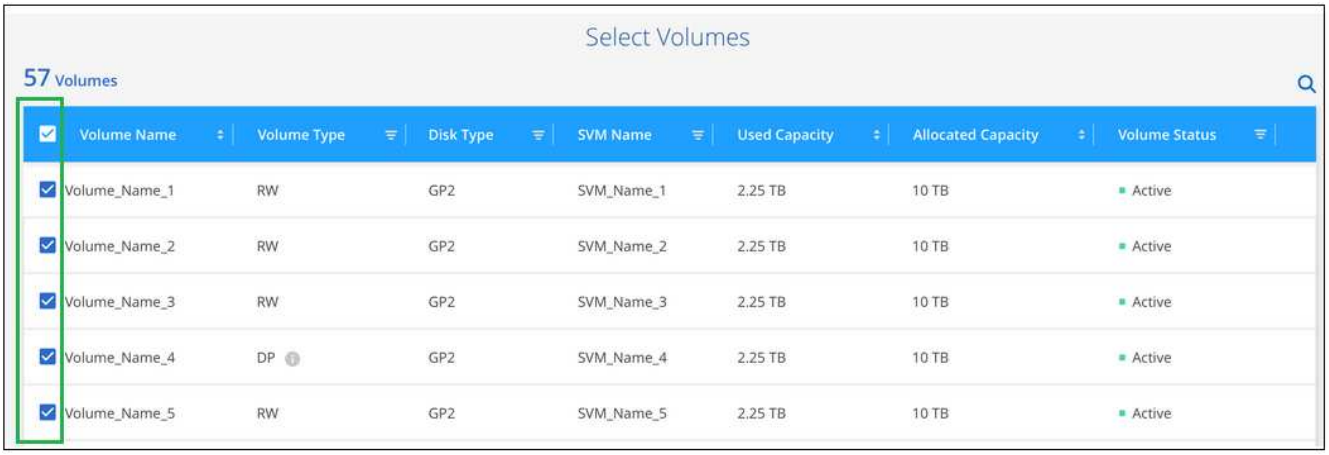
1. Wählen Sie die Arbeitsumgebung aus und klicken Sie im rechten Fenster neben dem Dienst Backup to Cloud auf **Aktivieren**.

2. Legen Sie den Backup-Zeitplan und den Aufbewahrungswert fest und klicken Sie auf **Weiter**.



Siehe "Die Liste der vorhandenen Richtlinien".

3. Wählen Sie die Volumes aus, die Sie sichern möchten, und klicken Sie auf **Aktivieren**.



Ergebnis

Backup in der Cloud beginnt die ersten Backups jedes ausgewählten Volumes.

Was kommt als Nächstes?

"Sie können Backups managen, indem Sie den Backup-Zeitplan ändern, Volumes wiederherstellen und mehr".

Daten werden auf Azure Blob Storage gesichert

Führen Sie einige Schritte aus, um die Datensicherung von Cloud Volumes ONTAP auf Azure Blob Storage zu starten.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

Überprüfen Sie die Unterstützung Ihrer Konfiguration

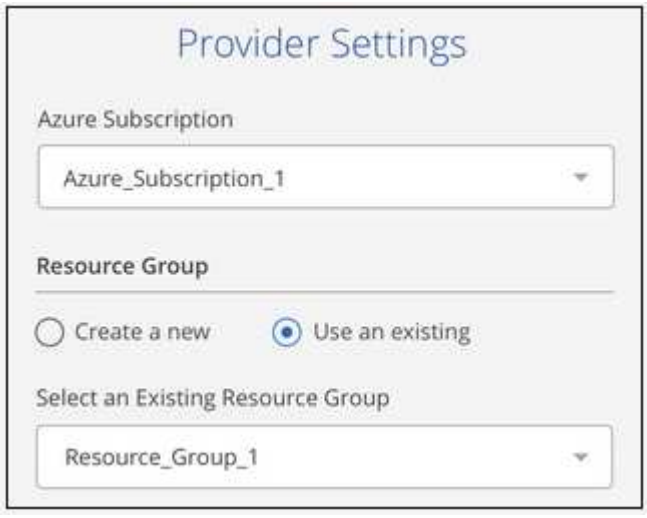
- Cloud Volumes ONTAP 9.7 oder höher wird in Azure ausgeführt.
- Sie verfügen über ein gültiges Cloud-Provider-Abonnement für den Speicherplatz, auf dem sich Ihre Backups befinden.
- Sie haben sich für das angemeldet "Cloud Manager Marketplace Backup-Angebot", Oder Sie haben gekauft "Und aktiviert" Eine BYOL-Lizenz für Backup in der Cloud von NetApp

Aktivieren Sie Backup in der Cloud auf Ihrem neuen oder vorhandenen System

- Neue Systeme: Backup in der Cloud ist standardmäßig im Assistenten für die Arbeitsumgebung aktiviert. Achten Sie darauf, dass die Option aktiviert bleibt.
- Bestehende Systeme: Wählen Sie die Arbeitsumgebung aus und klicken Sie auf **Aktivieren** neben dem Dienst Backup to Cloud im rechten Fenster, und folgen Sie dann dem Setup-Assistenten.

Geben Sie die Anbieterdetails ein

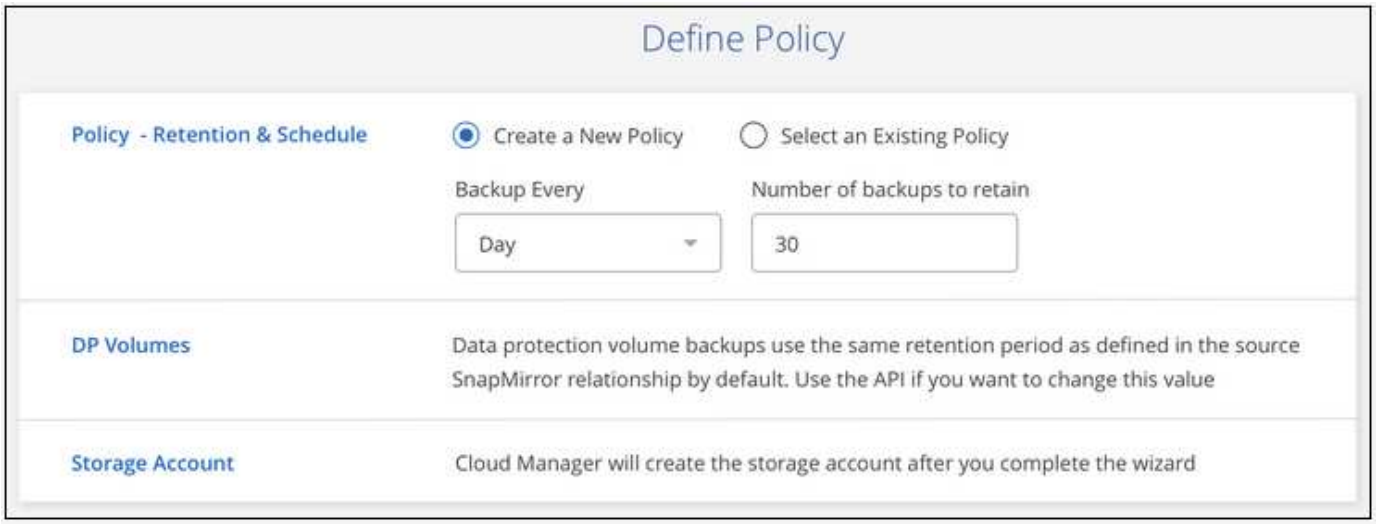
Wählen Sie das Provider-Abonnement aus, und legen Sie fest, ob Sie eine neue Ressourcengruppe erstellen oder eine bereits vorhandene Ressourcengruppe verwenden möchten.



Definieren der Backup-Richtlinie

Die Standardrichtlinie sichert Volumes täglich und speichert die letzten 30 Backup-Kopien jedes Volumes. Ändern Sie zu wöchentlichen oder monatlichen Backups oder wählen Sie eine der systemdefinierten

Richtlinien mit mehr Optionen aus.

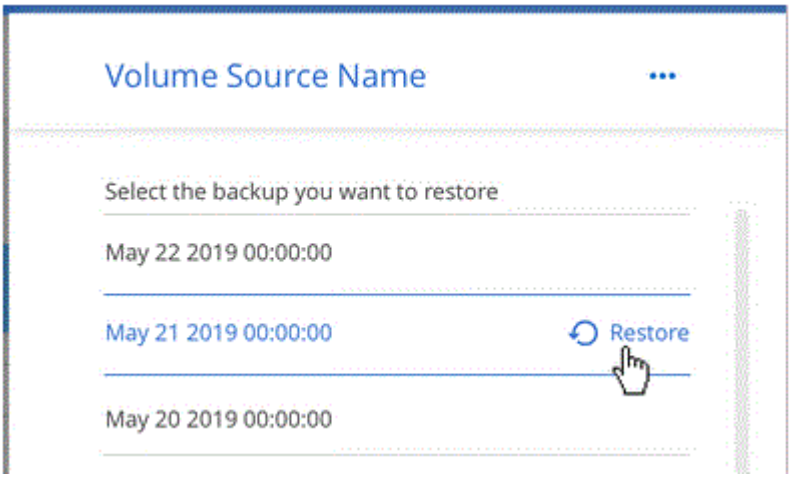


5 Wählen Sie die Volumes aus, die Sie sichern möchten

Legen Sie fest, welche Volumes Sie in der Seite Volumes auswählen sichern möchten.

6 Stellen Sie Ihre Daten nach Bedarf wieder her

Wählen Sie in der Sicherungsliste ein Volume aus, wählen Sie ein Backup aus und stellen Sie dann Daten aus dem Backup auf ein neues Volume wieder her.



Anforderungen

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie mit dem Backup von Volumes in Azure Blob Storage beginnen.

Unterstützte ONTAP-Versionen

Cloud Volumes ONTAP 9.7 und höher

Unterstützte Azure Regionen

Backup in die Cloud wird in allen Azure Regionen unterstützt "Wobei Cloud Volumes ONTAP unterstützt wird".

Lizenzanforderungen

Bei einer PAYGO-Lizenzierung von Backup in der Cloud ist ein Abonnement über den Azure Marketplace erforderlich, bevor Sie Backup in der Cloud aktivieren. Die Abrechnung für Backup in der Cloud erfolgt über dieses Abonnement. "Sie können sich auf der Seite Details Credentials des Assistenten für die Arbeitsumgebung anmelden".

Für die BYOL-Lizenzierung von Backup in der Cloud benötigen Sie die Seriennummer von NetApp, mit der Sie den Service für die Dauer und die Kapazität der Lizenz nutzen können. Siehe "Hinzufügen und Aktualisieren der Backup-BYOL-Lizenz".

Darüber hinaus benötigen Sie ein Microsoft Azure-Abonnement für den Speicherplatz, auf dem sich Ihre Backups befinden.

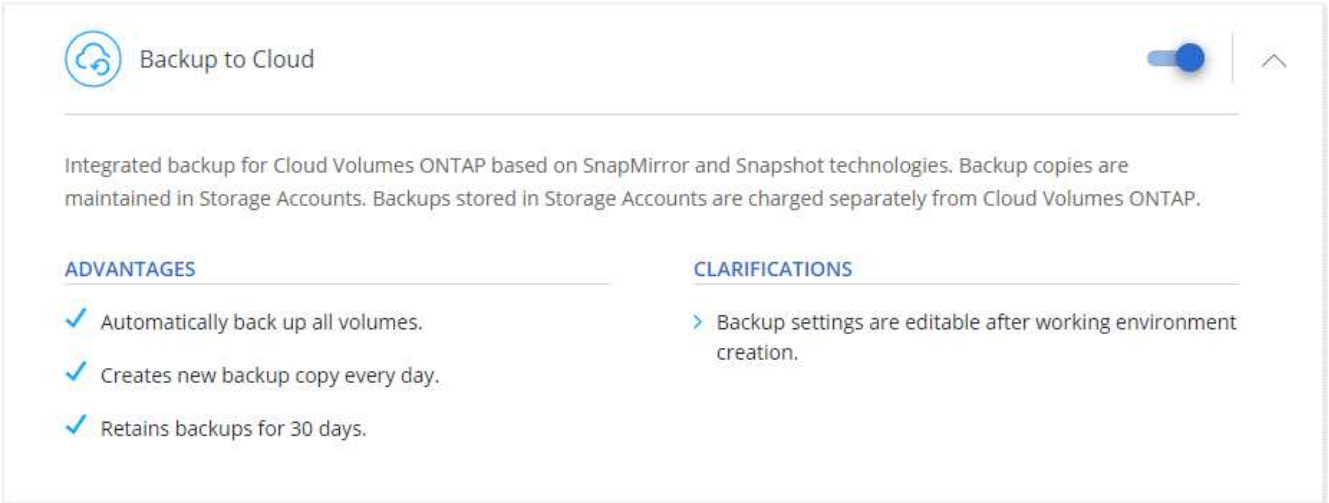
Aktivieren von Backup in der Cloud auf einem neuen System

Backup in der Cloud ist standardmäßig im Assistenten für die Arbeitsumgebung aktiviert. Achten Sie darauf, dass die Option aktiviert bleibt.

Wenn Sie den Namen der Ressourcengruppe auswählen möchten, deaktivieren Sie bei der Bereitstellung von Cloud Volumes ONTAP * Sicherung in der Cloud. Befolgen Sie die Schritte für Backup in der Cloud auf einem vorhandenen System Aktivieren von Backup in Cloud und Auswahl der Ressourcengruppe.

Schritte

1. Klicken Sie auf **Cloud Volumes ONTAP erstellen**.
2. Wählen Sie Microsoft Azure als Cloud-Provider und wählen Sie anschließend einen einzelnen Node oder ein HA-System.
3. Füllen Sie die Seite „Details & Credentials“ aus und stellen Sie sicher, dass ein Azure Marketplace Abonnement besteht.
4. Lassen Sie auf der Seite Dienste den Dienst aktiviert, und klicken Sie auf **Weiter**.



5. Führen Sie die Seiten im Assistenten aus, um das System bereitzustellen.

Ergebnis

Backup in der Cloud ist auf dem System aktiviert und sichert Volumes täglich und speichert die letzten 30 Backup-Kopien.

Was kommt als Nächstes?

"Sie können Backups managen, indem Sie den Backup-Zeitplan ändern, Volumes wiederherstellen und mehr".

Aktivieren von Backup in der Cloud auf einem vorhandenen System

Sie können Backup in die Cloud jederzeit direkt aus der Arbeitsumgebung aktivieren.

Schritte

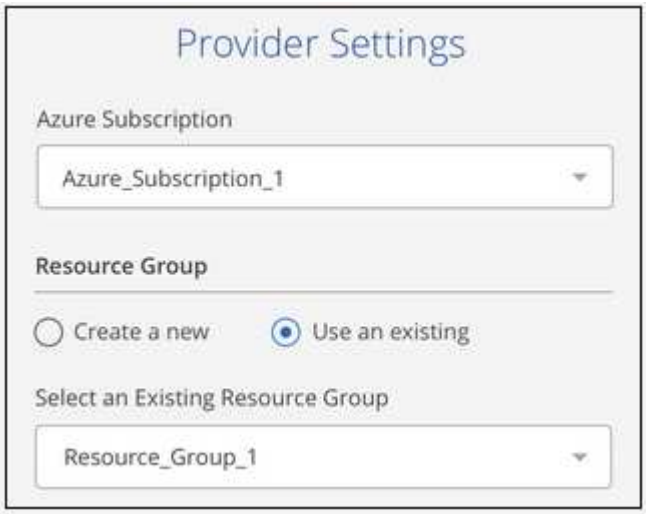
1. Wählen Sie die Arbeitsumgebung aus und klicken Sie im rechten Fenster neben dem Dienst Backup to Cloud auf **Aktivieren**.

2. Wählen Sie die Anbieterdetails aus:

   a. Das Azure-Abonnement zum Speichern der Backups.

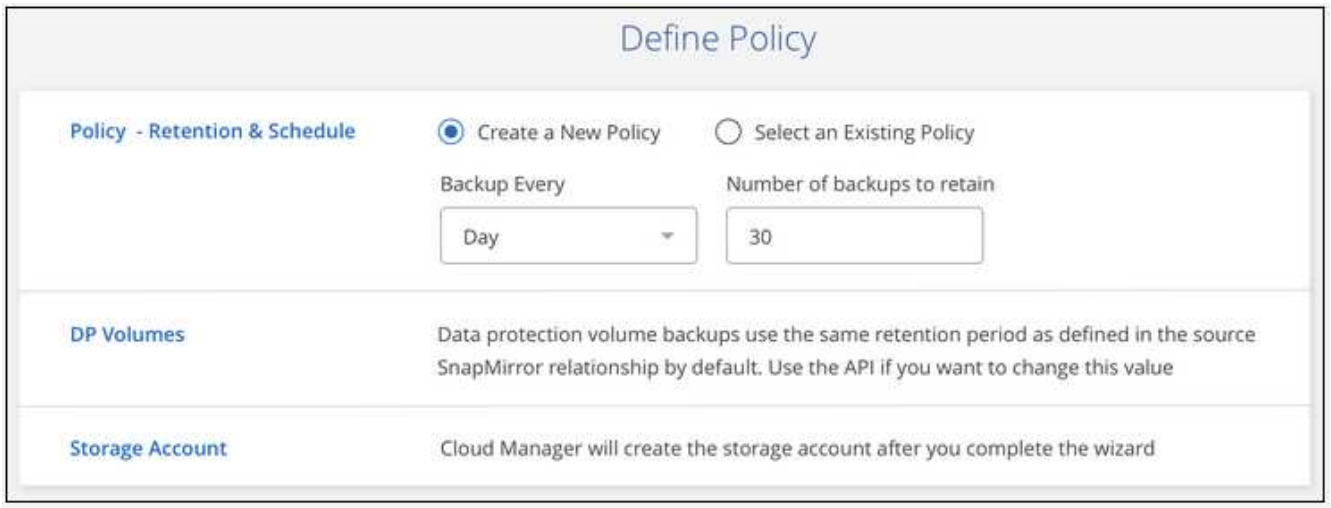
   b. Ressourcengruppe: Sie können eine neue Ressourcengruppe erstellen oder eine vorhandene Ressourcengruppe auswählen.

   c. Und klicken Sie dann auf **Weiter**.



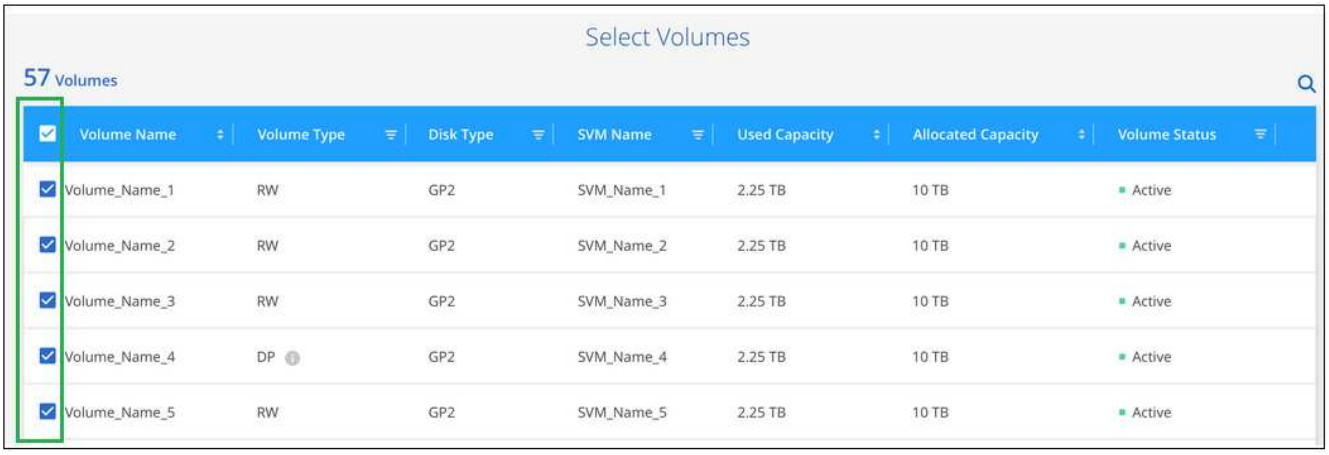
   Beachten Sie, dass Sie das Abonnement oder die Ressourcengruppe nach dem Start der Services nicht ändern können.

3. Wählen Sie auf der Seite *Policy* definieren den Backup-Zeitplan und den Aufbewahrungswert aus und klicken Sie auf **Weiter**.



Siehe "Die Liste der vorhandenen Richtlinien".

4. Wählen Sie die Volumes aus, die Sie sichern möchten, und klicken Sie auf **Aktivieren**.



Ergebnis

Backup in der Cloud beginnt die ersten Backups jedes ausgewählten Volumes.

Was kommt als Nächstes?

"Sie können Backups managen, indem Sie den Backup-Zeitplan ändern, Volumes wiederherstellen und mehr".

Daten werden von einem lokalen ONTAP System in der Cloud gesichert

Unternehmen Sie einige Schritte, um den Backup von Daten von Ihrem lokalen ONTAP System auf kostengünstigem Objekt-Storage in der Cloud zu starten.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

Überprüfen Sie die Unterstützung Ihrer Konfiguration

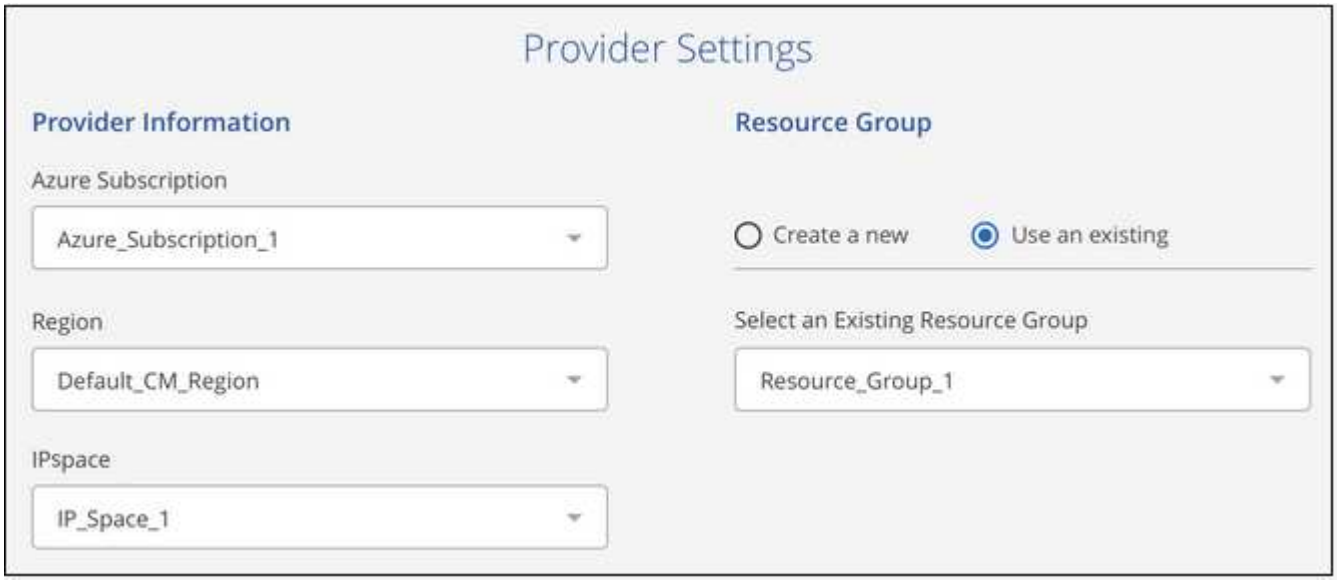
- Sie haben das On-Premises-Cluster erkannt und einer Arbeitsumgebung in Cloud Manager hinzugefügt. Siehe "Erkennung von ONTAP Clustern" Entsprechende Details.
- Sie verwenden ONTAP 9.7P5 oder höher auf dem Cluster.
- Sie verfügen über ein gültiges Cloud-Provider-Abonnement für den Speicherplatz, auf dem sich Ihre Backups befinden.
- Sie haben sich für das angemeldet "Cloud Manager Marketplace Backup-Angebot", Oder Sie haben gekauft "Und aktiviert" Eine BYOL-Lizenz für Backup in der Cloud von NetApp

Aktivieren Sie Backup in Cloud auf dem System

Wählen Sie die Arbeitsumgebung aus und klicken Sie im rechten Fenster neben dem Dienst Backup to Cloud auf **Aktivieren** und folgen Sie dann dem Setup-Assistenten.

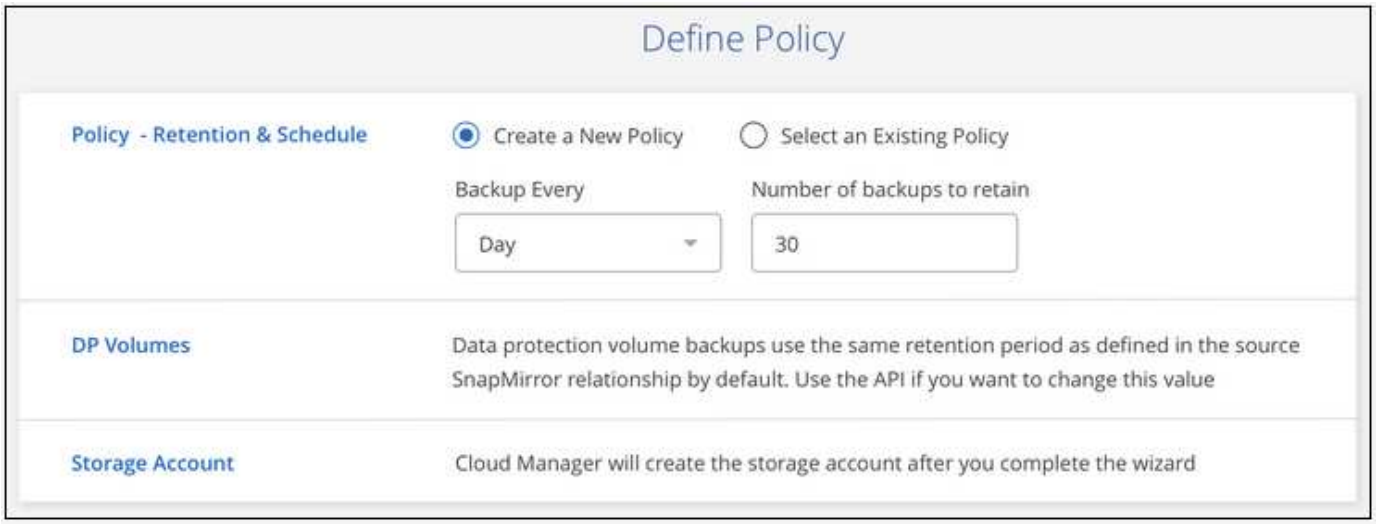
Wählen Sie den Cloud-Provider aus und geben Sie die Anbieterdetails ein

Wählen Sie den Provider aus, und wählen Sie dann das Provider-Abonnement, die Region und die Ressourcengruppe aus. Sie müssen außerdem den IPspace im ONTAP Cluster angeben, auf dem sich die Volumes befinden.



Definieren der Backup-Richtlinie

Die Standardrichtlinie sichert Volumes täglich und speichert die letzten 30 Backup-Kopien jedes Volumes. Ändern Sie zu wöchentlichen oder monatlichen Backups oder wählen Sie eine der systemdefinierten Richtlinien mit mehr Optionen aus.

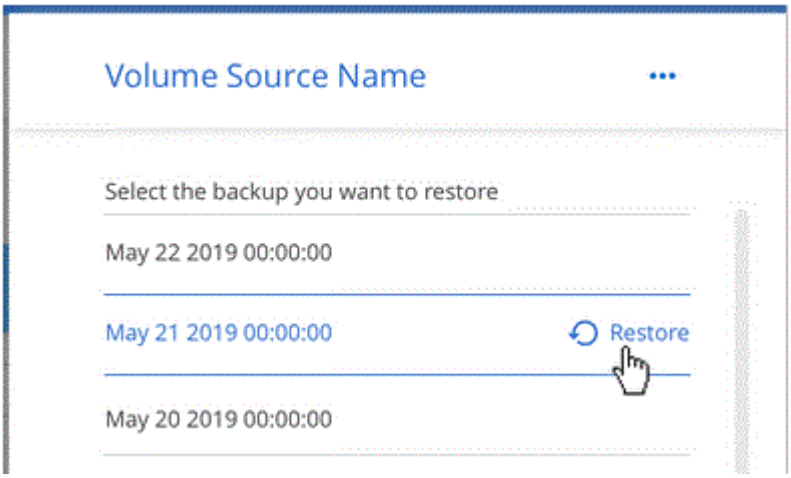


Wählen Sie die Volumes aus, die Sie sichern möchten

Ermitteln Sie, welche Volumes vom Cluster aus gesichert werden sollen.

Stellen Sie Ihre Daten nach Bedarf wieder her

Wählen Sie aus der Liste der Backups ein Volume aus, wählen Sie ein Backup aus und stellen Sie dann die Daten aus dem Backup auf ein neues Volume in einem Cloud Volumes ONTAP System wieder her, das denselben Cloud-Provider verwendet.



Anforderungen

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie mit dem Backup von Volumes in Azure Blob Storage beginnen.

Unterstützte ONTAP-Versionen

ONTAP 9.7P5 und höher.

Netzwerkanforderungen für Cluster

Auf jedem ONTAP Node ist eine Intercluster-LIF erforderlich, die die Volumes hostet, die Sie sichern möchten. Die LIF muss dem *IPspace* zugewiesen sein, den ONTAP zur Verbindung mit Objekt-Storage verwenden sollte. Die Admin-SVM muss sich im IPspace befinden. "Erfahren Sie mehr über IPspaces".

Wenn Sie Backup in der Cloud einrichten, werden Sie aufgefordert, den IPspace zu verwenden. Sie sollten den IPspace auswählen, dem jede LIF zugeordnet ist. Dies kann der „Standard"-IPspace oder ein benutzerdefinierter IPspace sein, den Sie erstellt haben.

Unterstützte Azure Regionen

Backup in die Cloud wird in allen Azure Regionen unterstützt "Wobei Cloud Volumes unterstützt werden".

Lizenzanforderungen

Für Backup in der Cloud-PAYGO-Lizenzierung, ein Abonnement beim "Azure Marketplace Cloud Manager Backup-Angebot" Ist erforderlich, bevor Sie Backup in der Cloud aktivieren. Die Abrechnung für Backup in der Cloud erfolgt über dieses Abonnement.

Für die BYOL-Lizenzierung von Backup in der Cloud benötigen Sie die Seriennummer von NetApp, mit der Sie den Service für die Dauer und die Kapazität der Lizenz nutzen können. Siehe "Hinzufügen und Aktualisieren der Backup-BYOL-Lizenz".

Darüber hinaus benötigen Sie ein Microsoft Azure-Abonnement für den Speicherplatz, auf dem sich Ihre Backups befinden.

Aktivieren von Backup in der Cloud

Sie können Backup in die Cloud jederzeit direkt aus der Arbeitsumgebung aktivieren.

Schritte

1. Wählen Sie die Arbeitsumgebung aus und klicken Sie im rechten Fenster neben dem Dienst Backup to Cloud auf **Aktivieren**.

2. Wählen Sie den Anbieter aus, und geben Sie dann die Provider-Details ein:

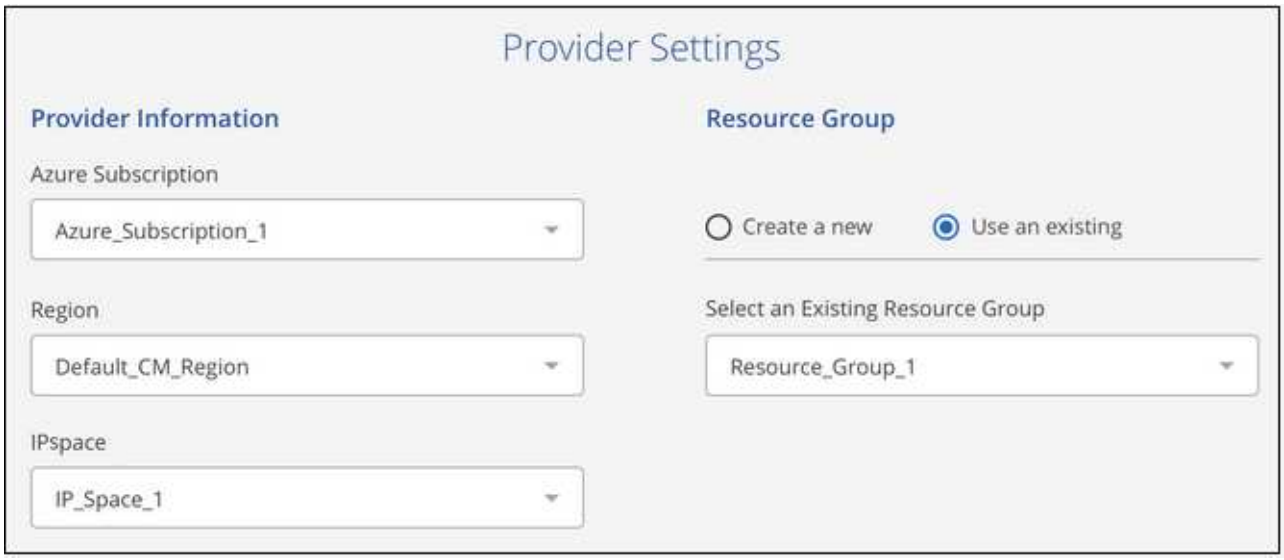
   a. Das Azure-Abonnement zum Speichern der Backups.

   b. Die Region Azure.

   c. Ressourcengruppe: Sie können eine neue Ressourcengruppe erstellen oder eine vorhandene Ressourcengruppe auswählen.

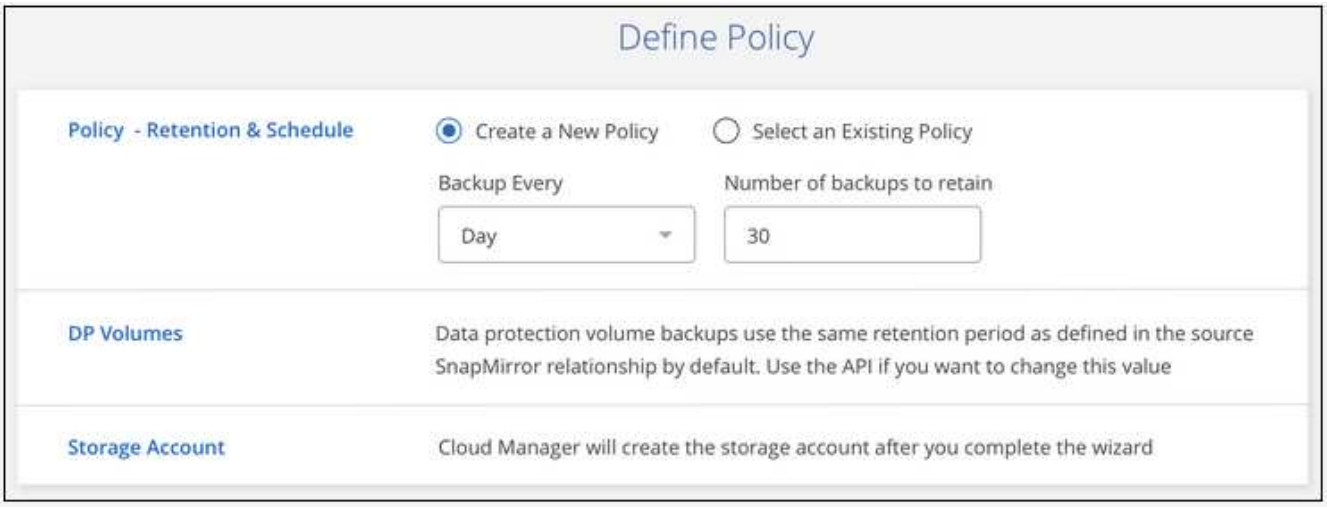
d. Der IPspace im ONTAP Cluster, in dem sich die Volumes, die Sie sichern möchten, befinden.

e. Und klicken Sie dann auf **Weiter**.



Beachten Sie, dass Sie das Abonnement oder die Ressourcengruppe nach dem Start der Services nicht ändern können.

3. Wählen Sie auf der Seite *Policy* definieren den Backup-Zeitplan und den Aufbewahrungswert aus und klicken Sie auf **Weiter**.



Siehe "Die Liste der vorhandenen Richtlinien".

4. Wählen Sie die Volumes aus, die Sie sichern möchten, und klicken Sie auf **Aktivieren**.

Ergebnis

Backup in der Cloud beginnt die ersten Backups jedes ausgewählten Volumes.

Was kommt als Nächstes?

"Sie können Backups managen, indem Sie den Backup-Zeitplan ändern, Volumes wiederherstellen und mehr".

Management von Backups für Cloud Volumes ONTAP und lokale ONTAP Systeme

Ändern Sie den Backup-Zeitplan, die Wiederherstellung von Volumes, das Löschen von Backups usw. und verwalten Sie Backups für Cloud Volumes ONTAP und ONTAP Systeme vor Ort.

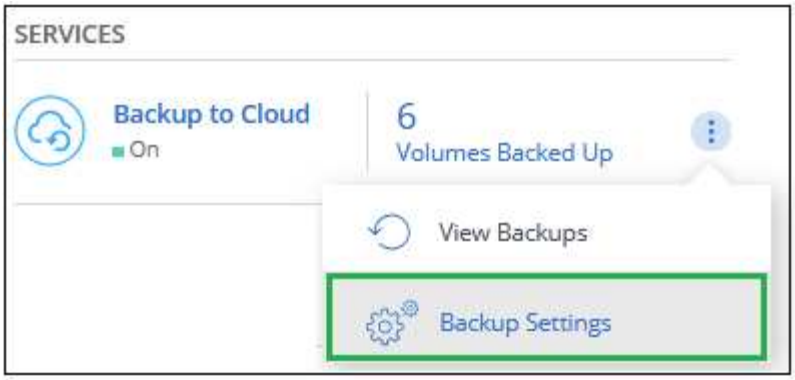
Ändern des Zeitplans und der Backup-Aufbewahrung

Die Standardrichtlinie sichert Volumes täglich und speichert die letzten 30 Backup-Kopien jedes Volumes. Sie können zu wöchentlichen oder monatlichen Backups wechseln und die Anzahl der beizubehaltenden Backup-Kopien ändern. Sie können auch eine der systemdefinierten Richtlinien auswählen, die geplante Backups für 3 Monate, 1 Jahr und 7 Jahre bereitstellen.

Das Ändern der Backup-Richtlinie betrifft nur neue Volumes, die nach der Änderung des Zeitplans erstellt wurden. Er hat keine Auswirkung auf den Zeitplan für vorhandene Volumes.

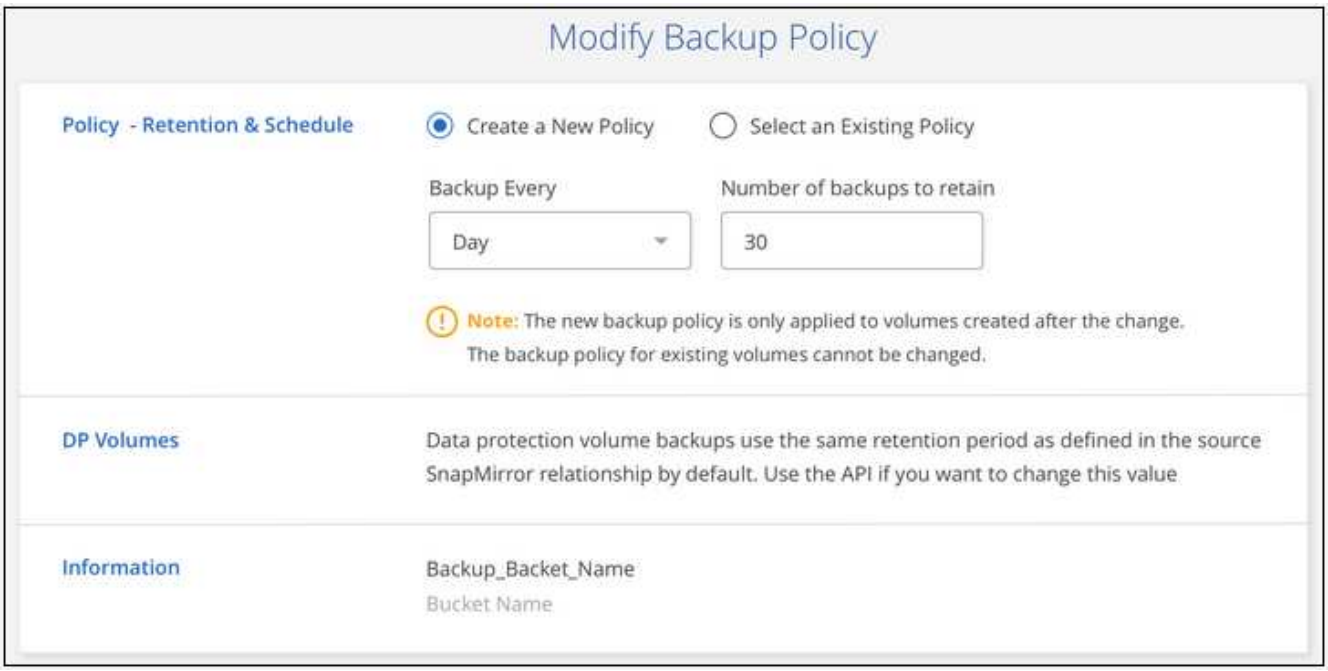
Schritte

1. Wählen Sie die Arbeitsumgebung aus.
2. Klicken Sie Auf Und wählen Sie **Backup-Einstellungen**.



3. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Wählen Sie für die Arbeitsumgebung **Backup Policy ändern**.

4. Ändern Sie auf der Seite *Backup Policy* den Zeitplan und die Backup-Aufbewahrung und klicken Sie dann auf **Speichern**.

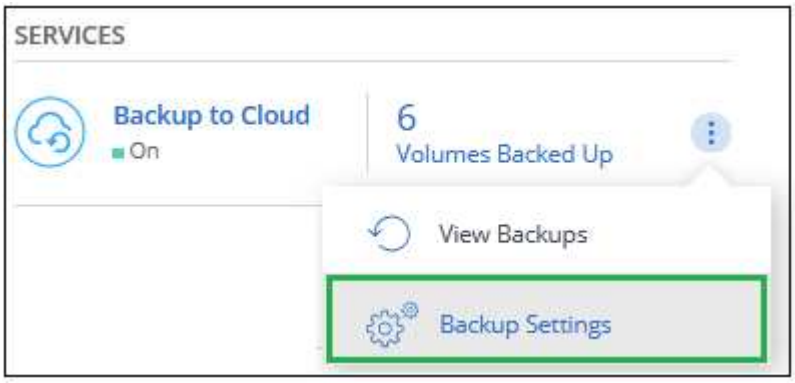


Starten und Stoppen von Backups der Volumes

Sie können die Sicherung eines Volumes anhalten, wenn Sie keine Backup-Kopien dieses Volumes benötigen und nicht für die Kosten für die Speicherung der Backups bezahlen möchten. Sie können auch ein neues Volume zur Backup-Liste hinzufügen, wenn das Volume derzeit nicht gesichert wird.

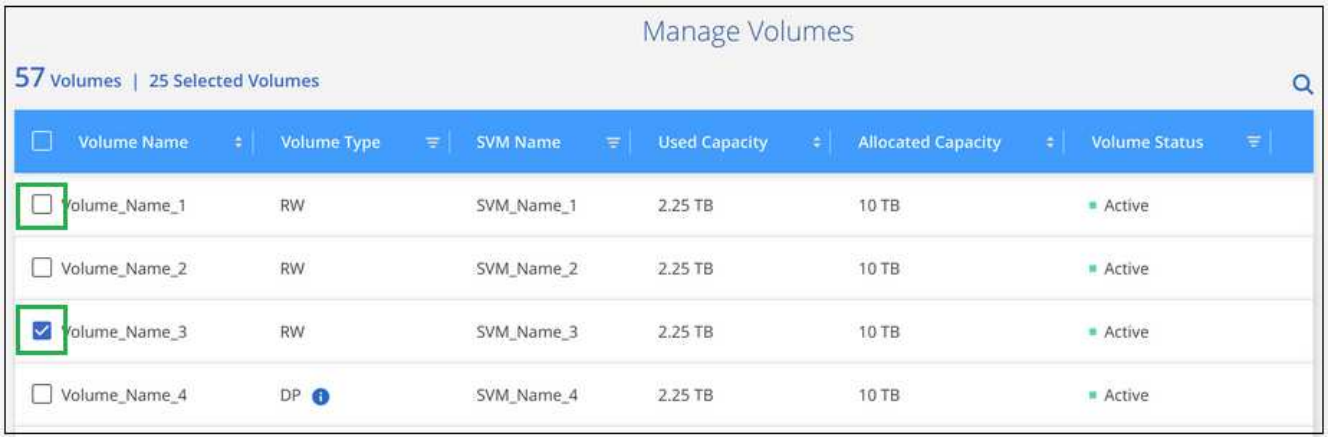
Schritte

1. Wählen Sie die Arbeitsumgebung aus.
2. Klicken Sie Auf ⋮ Und wählen Sie **Backup-Einstellungen**.



3. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Wählen Sie für die Arbeitsumgebung **Volumes verwalten** aus.

4. Aktivieren Sie das Kontrollkästchen für Volumes, die mit dem Backup beginnen sollen, und deaktivieren Sie das Kontrollkästchen für Volumes, die nicht mehr gesichert werden sollen.



Hinweis: Wenn ein Volume nicht gesichert werden soll, werden Sie Ihrem Cloud Provider weiterhin die Kosten für die Objektspeicherung für die Kapazität in Rechnung gestellt, die die Backups nutzen, es sei denn, Sie Löschen Sie die Backups.

Wiederherstellen eines Volumes aus einem Backup

Wenn Sie Daten aus einem Backup wiederherstellen, erstellt Cloud Manager mithilfe der Daten aus dem

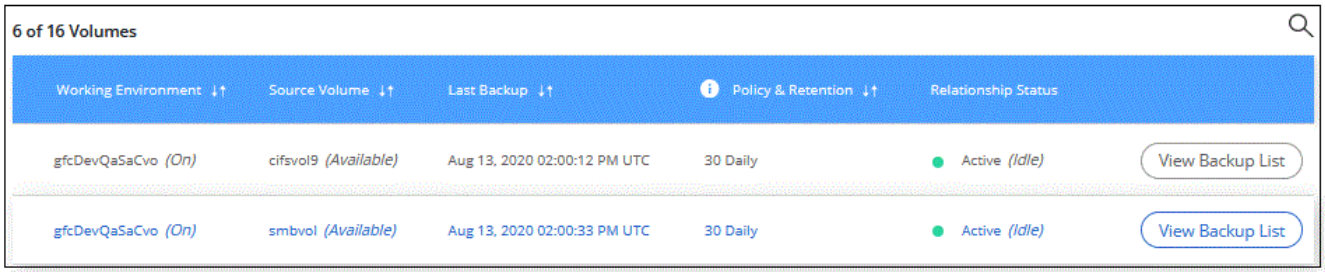
Backup ein *neues* Volume. Sie können die Daten auf einem Volume in derselben Arbeitsumgebung oder in einer anderen Arbeitsumgebung wiederherstellen, die sich in demselben Cloud-Konto wie die Arbeitsquelle befindet. Da das Backup keine Snapshots enthält, tut auch das neu wiederhergestellte Volume nicht.

Backups, die aus lokalen ONTAP Systemen erstellt wurden, können nur auf Cloud Volumes ONTAP Systemen wiederhergestellt werden, die denselben Cloud-Provider verwenden wie der Speicherort des Backups.

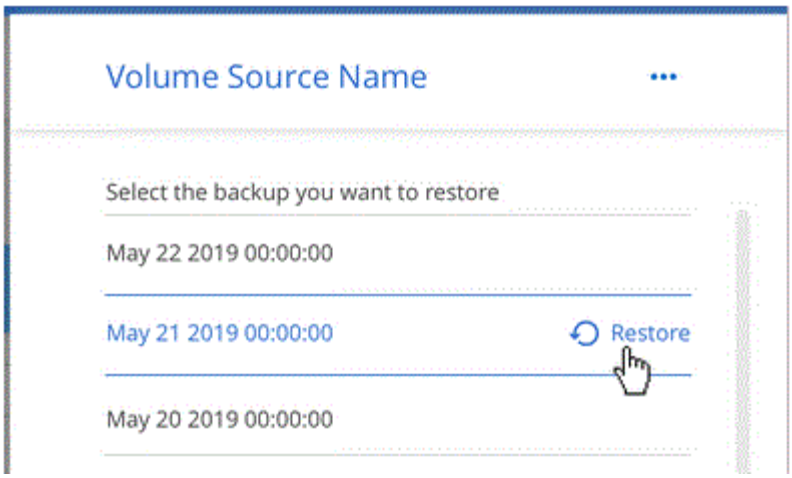
Schritte

1. Wählen Sie die Arbeitsumgebung aus.
2. Klicken Sie Auf Und wählen Sie **Backups anzeigen**.

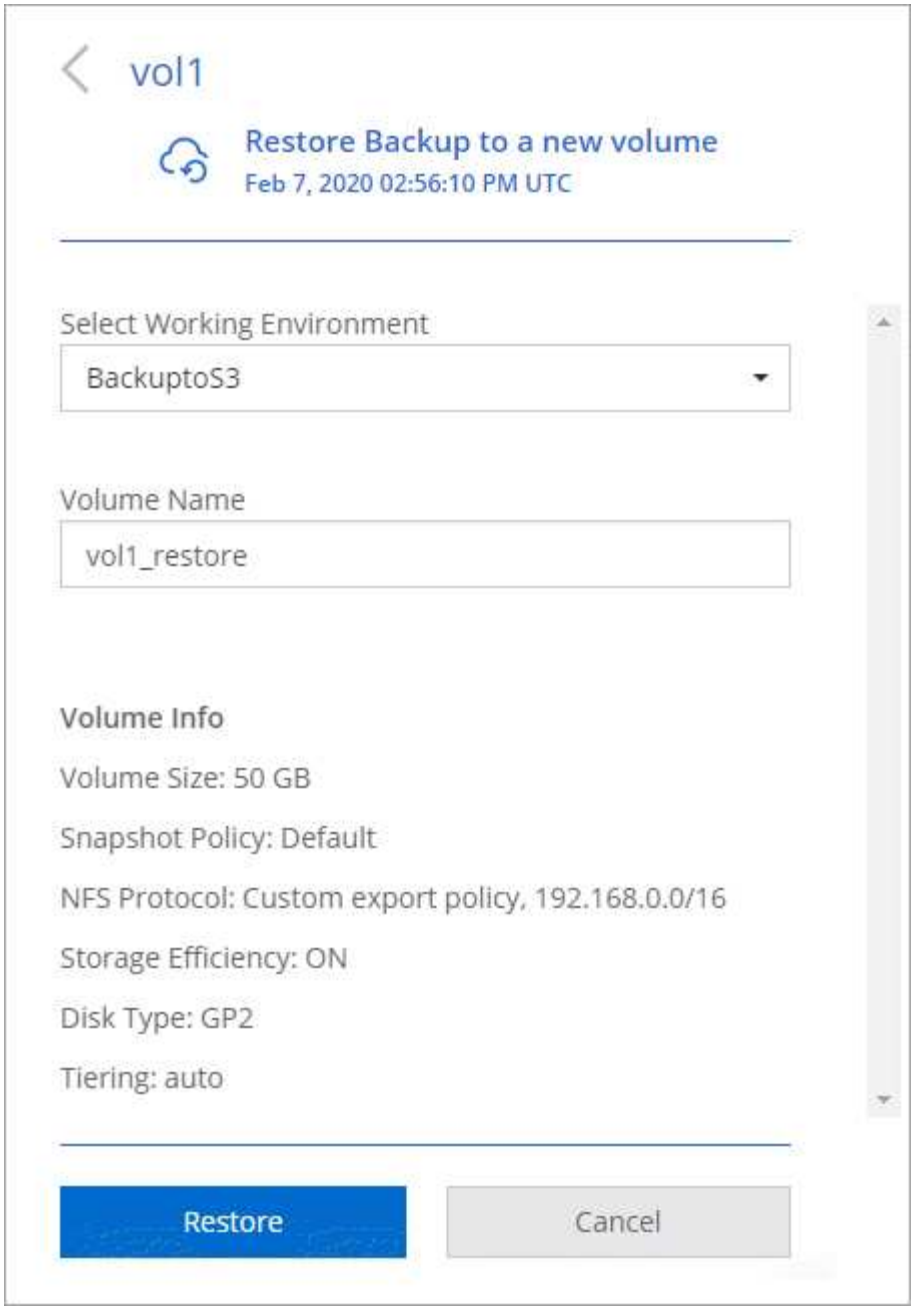
3. Wählen Sie die Zeile für den Datenträger aus, den Sie wiederherstellen möchten, und klicken Sie auf **Backup-Liste anzeigen**.



4. Suchen Sie das Backup, das Sie wiederherstellen möchten, und klicken Sie auf das Symbol **Wiederherstellen**.



5. Füllen Sie die Seite „ Sicherung auf neues Volume wiederherstellen “ aus:
   a. Wählen Sie die Arbeitsumgebung aus, in der Sie das Volume wiederherstellen möchten.
   b. Geben Sie einen Namen für das Volume ein.
   c. Klicken Sie Auf **Wiederherstellen**.



Ergebnis

Cloud Manager erstellt auf Basis des ausgewählten Backups ein neues Volume. Das können Sie "Verwalten Sie dieses neue Volume" Nach Bedarf.

Backups werden gelöscht

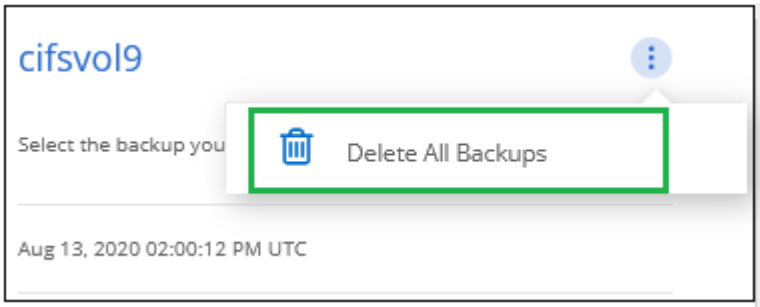
Backup in der Cloud ermöglicht Ihnen das Löschen aller Backups eines bestimmten Volumes. Sie können keine *einzelnen* Backups löschen.

Dies ist möglicherweise der Fall, wenn Sie die Backups nicht mehr benötigen oder das Quell-Volume gelöscht haben und alle Backups entfernen möchten.

Wenn Sie planen, ein Cloud Volumes ONTAP- oder On-Premise-ONTAP-System mit Backups zu löschen, müssen Sie die Backups *löschen, bevor Sie das System löschen. Backup to Cloud nicht automatisch löschen Backups, wenn Sie ein System löschen, und es gibt keine aktuelle Unterstützung in der UI, die Backups zu löschen, nachdem das System gelöscht wurde.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Backup**.
2. Suchen Sie in der Liste des Volumes nach dem Datenträger und klicken Sie auf **Backup-Liste anzeigen**.
3. Klicken Sie Auf ••• Und wählen Sie **Alle Backups löschen**.



4. Klicken Sie im Bestätigungsdialogfeld auf **Löschen**.

Deaktivieren von Backup in der Cloud

Durch das Deaktivieren von Backup in der Cloud für eine funktionierende Umgebung werden Backups von jedem Volume im System deaktiviert, außerdem wird die Möglichkeit zur Wiederherstellung eines Volumes deaktiviert. Vorhandene Backups werden nicht gelöscht.

Beachten Sie, dass Ihr Cloud-Provider Ihnen weiterhin die Kosten für Objekt-Storage für die Kapazität berechnet, die Ihre Backups verwenden, es sei denn, Sie löschen die Backups.

Schritte

1. Wählen Sie die Arbeitsumgebung aus.
2. Klicken Sie Auf ⋮ Und wählen Sie **Backup-Einstellungen**.

3. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Wählen Sie für die Arbeitsumgebung **Sichern in Cloud** deaktivieren.

4. Klicken Sie im Bestätigungsdialogfeld auf **Deaktivieren**.

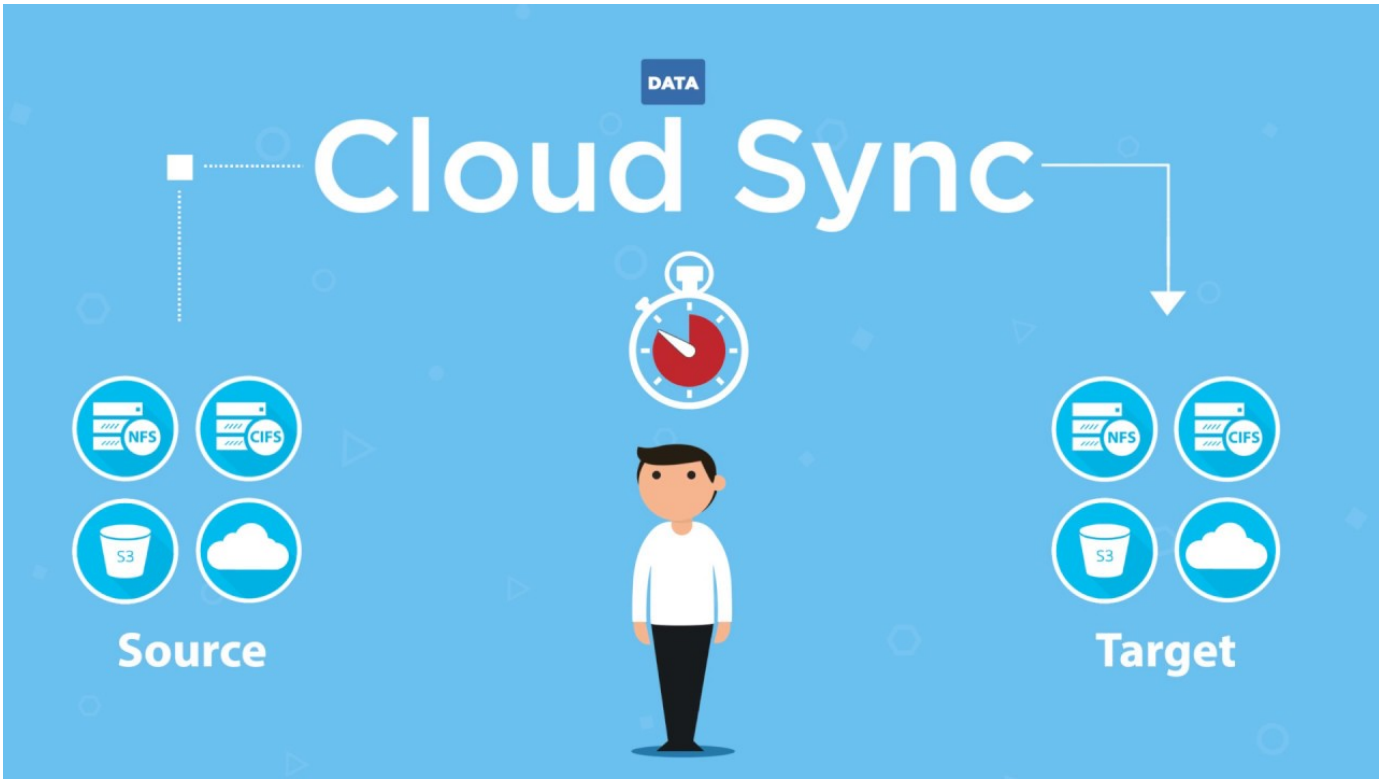
Daten kopieren und synchronisieren

Übersicht über Cloud Sync

Der NetApp Cloud Sync Service bietet eine einfache, sichere und automatisierte Möglichkeit zur Migration Ihrer Daten auf beliebige Ziele, in der Cloud oder vor Ort. Ob es sich um einen dateibasierten NAS-Datensatz (NFS oder SMB), um ein S3-Objektformat (Amazon Simple Storage Service), eine NetApp StorageGRID Appliance oder einen anderen Cloud-Provider-Objektspeicher handelt: Cloud Sync kann diesen für Sie konvertieren und verschieben.

Funktionen

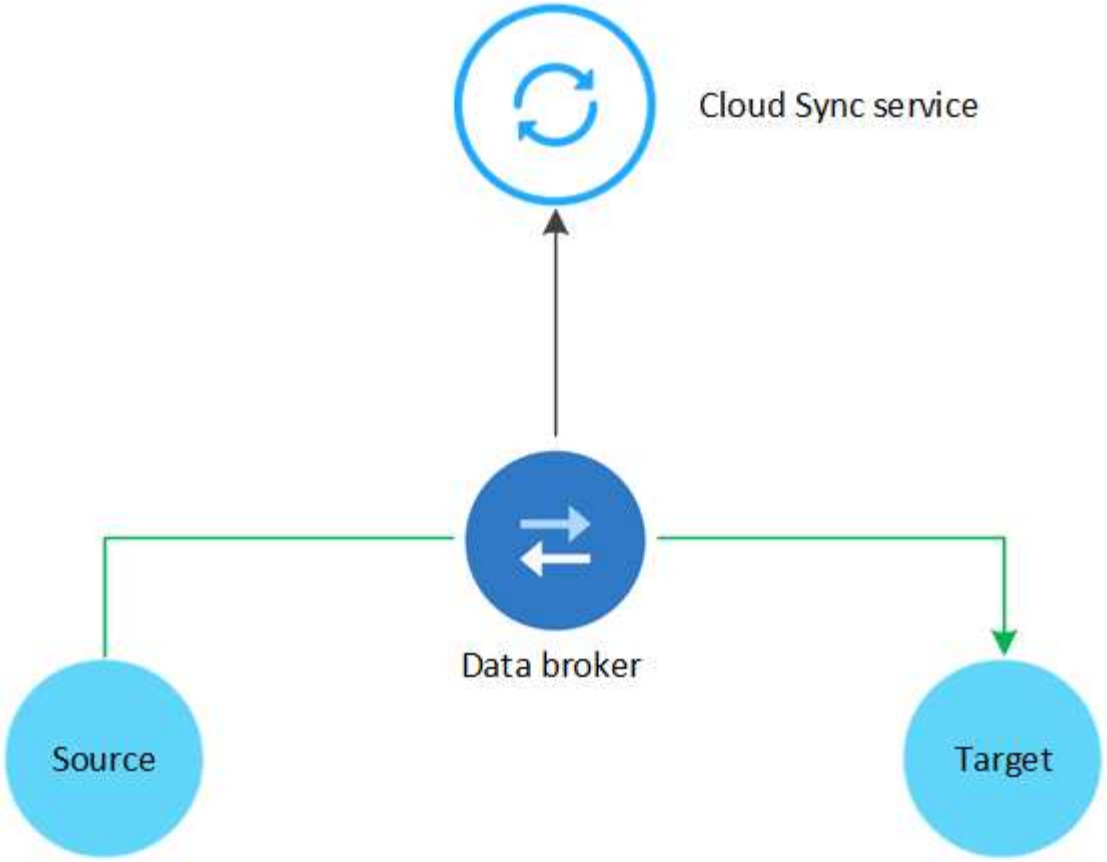
Sehen Sie sich das folgende Video an, um einen Überblick über Cloud Sync zu erhalten:



Funktionsweise von Cloud Sync

Cloud Sync ist eine SaaS-Plattform (Software-as-a-Service), die aus einem Datenmanager, einer Cloud-basierten Schnittstelle, die über Cloud Manager verfügbar ist, sowie aus einer Quelle und einem Ziel besteht.

Die folgende Abbildung zeigt die Beziehung zwischen Cloud Sync-Komponenten:



Die NetApp Daten-Broker Software synchronisiert Daten von einer Quelle zu einem Ziel (dies wird als „*Sync Relationship*“ bezeichnet). Sie können den Data Broker in AWS, Azure, Google Cloud Platform oder vor Ort ausführen. Der Daten-Broker benötigt eine ausgehende Internetverbindung über Port 443, damit er mit dem Cloud Sync-Dienst kommunizieren und sich mit einigen anderen Diensten und Repositorys in Verbindung setzen kann. "Zeigen Sie die Liste der Endpunkte an".

Nach der ersten Kopie synchronisiert der Service alle geänderten Daten auf der Grundlage des von Ihnen festgelegten Zeitplans.

Unterstützte Speichertypen

Cloud Sync unterstützt folgende Speichertypen:

- Beliebiger NFS-Server
- Alle SMB-Server
- AWS EFS
- AWS S3
- Azure Blob
- Azure NetApp Dateien
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Google Cloud Storage
- IBM Cloud Objekt-Storage

- On-Premises-ONTAP-Cluster
- ONTAP S3 Storage
- StorageGRID

"Unterstützte Synchronisierungsbeziehungen prüfen".

Kosten

Mit der Nutzung von Cloud Sync sind zwei Arten von Kosten verbunden: Ressourcengebühren und Servicegebühren.

Ressourcenkosten

Ressourcengebühren beziehen sich auf die Computing- und Storage-Kosten für den Betrieb des Daten-Brokers in der Cloud.

Servicegebühren

Es gibt zwei Möglichkeiten, für Synchronisierungsbeziehungen zu bezahlen, nachdem die 14-tägige kostenlose Testversion abgelaufen ist. Als erste Option können Sie AWS oder Azure abonnieren, wodurch Sie stündlich oder jährlich bezahlen können. Die zweite Option besteht darin, Lizenzen direkt von NetApp zu erwerben. Lesen Sie die folgenden Abschnitte, um weitere Details zu erhalten.

Marketplace-Abonnement

Wenn Sie den Cloud Sync Service von AWS oder Azure abonnieren, können Sie die Kosten pro Stunde oder pro Jahr zahlen. "Sie können sich für die Anmeldung über AWS oder Azure anmelden", Je nachdem, wo Sie abgerechnet werden möchten.

Stündliche Abonnements

Bei einem nutzungsbasierten Abonnement auf Stundenbasis berechnet der Cloud Sync Service jede Stunde, basierend auf der Anzahl der erstellten Synchronisierungsbeziehungen.

- "Preise in Azure anzeigen"
- "Pay-as-you-go-Preise in AWS anzeigen"

Jahresabonnements

Ein Jahresabonnement bietet eine Lizenz für 20 Synchronisierungsbeziehungen, die Sie vorab bezahlen. Wenn Sie über 20 synchrone Beziehungen verfügen und über Azure angemeldet sind, zahlen Sie für die zusätzlichen Beziehungen pro Stunde.

"Jährliche Preise in AWS anzeigen"

Lizenzen von NetApp

Eine weitere Möglichkeit, für Synchronisierungsbeziehungen vorab zu bezahlen, besteht darin, Lizenzen direkt von NetApp zu erwerben. Mit jeder Lizenz können Sie bis zu 20 Synchronisierungsbeziehungen erstellen.

Sie können diese Lizenzen mit einem AWS- oder Azure-Abonnement verwenden. Wenn Sie beispielsweise 25 Synchronisierungsbeziehungen haben, können Sie die ersten 20 Synchronisierungsbeziehungen mit einer Lizenz bezahlen und dann mit den restlichen 5 Synchronisierungsbeziehungen von AWS oder Azure bezahlen.

"Erfahren Sie, wie Sie Lizenzen erwerben und zu Cloud Sync hinzufügen".

Lizenzbestimmungen

Kunden, die eine Bring Your Own License (Byol) für den Cloud Sync Service erwerben, sollten sich der Einschränkungen im Zusammenhang mit der Lizenzberechtigung bewusst sein.

- Der Kunde ist berechtigt, die Byol-Lizenz für einen Zeitraum von höchstens einem Jahr ab Lieferdatum zu nutzen.
- Kunden haben das Recht, die Byol-Lizenz zu nutzen, um insgesamt 20 einzelne Verbindungen zwischen einer Quelle und einem Ziel (jeweils eine "Sync-Beziehung") herzustellen und nicht zu überschreiten.
- Die Berechtigung eines Kunden erlischt mit Ablauf der einjährigen Lizenzlaufzeit, unabhängig davon, ob der Kunde die 20-Sync-Beziehungs-Limitierung erreicht hat.
- Falls der Kunde seine Lizenz erneuern möchte, werden nicht verwendete Synchronisierungsbeziehungen, die mit der vorherigen Lizenzgewährung verknüpft waren, NICHT auf die Lizenzverlängerung übertragen.

Datenschutz

NetApp hat keinen Zugriff auf Ihre Zugangsdaten, die Sie während der Nutzung des Cloud Sync-Dienstes zur Verfügung stellen. Die Anmeldeinformationen werden direkt auf dem Data Broker-Computer in Ihrem Netzwerk gespeichert.

Abhängig von der ausgewählten Konfiguration werden Sie möglicherweise von Cloud Sync aufgefordert, Anmeldeinformationen einzugeben, wenn Sie eine neue Beziehung erstellen. Wenn Sie beispielsweise eine Beziehung einrichten, die einen SMB-Server umfasst, oder den Daten-Broker in AWS bereitstellen.

Diese Zugangsdaten werden immer direkt beim Data Broker selbst gespeichert. Der Daten-Broker befindet sich auf einem Rechner im Netzwerk, unabhängig davon, ob er sich vor Ort oder in Ihrem Cloud-Konto befindet. Die Zugangsdaten werden NetApp nie zur Verfügung gestellt.

Die Anmeldedaten werden mithilfe von HashiCorp Vault lokal auf dem Daten-Broker-Rechner verschlüsselt.

Einschränkungen

- Cloud Sync wird in China nicht unterstützt.
- Neben China wird der Cloud Sync Data Broker in den folgenden Regionen nicht unterstützt:
  - AWS GovCloud (USA)
  - Azure US Gov
  - Azure US DoD

Los geht’s

Schnellstart für Cloud Sync

Die ersten Schritte mit dem Cloud Sync Service umfassen einige Schritte.

Bereiten Sie Ihre Quelle und Ihr Ziel vor

Stellen Sie sicher, dass Ihre Quelle und Ihr Ziel unterstützt und eingerichtet werden. Die wichtigste Anforderung besteht darin, die Konnektivität zwischen dem Daten-Broker und dem Quell- und Zielstandort zu überprüfen. "Weitere Informationen .".

Bereiten Sie einen Standort für den NetApp Data Broker vor

Die NetApp Daten-Broker Software synchronisiert Daten von einer Quelle zu einem Ziel (dies wird als „*Sync Relationship*“ bezeichnet). Sie können den Data Broker in AWS, Azure, Google Cloud Platform oder vor Ort ausführen. Der Daten-Broker benötigt eine ausgehende Internetverbindung über Port 443, damit er mit dem Cloud Sync-Dienst kommunizieren und sich mit einigen anderen Diensten und Repositorys in Verbindung setzen kann. "Zeigen Sie die Liste der Endpunkte an".

Cloud Sync führt Sie durch den Installationsprozess, wenn Sie eine Synchronisierungsbeziehung erstellen. An diesem Punkt können Sie den Daten-Broker in der Cloud bereitstellen oder ein Installationsskript für Ihren eigenen Linux-Host herunterladen.

- "Überprüfen Sie die AWS-Installation"
- "Überprüfen Sie die Azure Installation"
- "Überprüfen Sie die GCP-Installation"
- "Überprüfen Sie die Installation des Linux-Hosts"

Erstellen Sie Ihre erste Synchronisierungsbeziehung

Melden Sie sich bei an "Cloud Manager"Klicken Sie auf **Sync** und ziehen Sie dann die Auswahl für die Quelle und das Ziel und legen Sie sie ab. Befolgen Sie die Anweisungen, um die Einrichtung abzuschließen. "Weitere Informationen .".

Bezahlen Sie Ihre Synchronisierungsbeziehungen, nachdem die kostenlose Testversion abgelaufen ist

Abonnieren Sie AWS oder Azure, um nutzungsbasiert zu bezahlen oder jährlich zu zahlen. Oder erwerben Sie Lizenzen direkt von NetApp. Rufen Sie einfach die Seite Lizenzeinstellungen in Cloud Sync auf, um sie einzurichten. "Weitere Informationen .".

Quelle und Ziel werden vorbereitet

Bereiten Sie die Synchronisierung von Daten vor, indem Sie überprüfen, ob Quelle und Ziel unterstützt werden und einrichten.

Unterstützte Synchronisierungsbeziehungen

Mit Cloud Sync können Sie Daten von einer Quelle zu einem Ziel synchronisieren (dies wird als „*Sync Relationship*“ bezeichnet). Sie sollten die unterstützten Beziehungen verstehen, bevor Sie beginnen.

Quellspeicherort	Unterstützte Zielstandorte
AWS EFS	• AWS EFS • AWS S3 • Azure Blob • Azure NetApp Dateien (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Objekt-Storage • Google Cloud Storage • NFS-Server • On-Premises-ONTAP-Cluster • StorageGRID
AWS S3	• AWS EFS • AWS S3 • Azure Blob • Azure NetApp Dateien • Cloud Volumes ONTAP • Cloud Volumes Service • IBM Cloud Objekt-Storage • Google Cloud Storage • NFS-Server • On-Premises-ONTAP-Cluster • SMB Server • StorageGRID

Quellspeicherort	Unterstützte Zielstandorte
Azure Blob	• AWS EFS • AWS S3 • Azure Blob • Azure NetApp Dateien • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Objekt-Storage • NFS-Server • On-Premises-ONTAP-Cluster • SMB Server • StorageGRID
Azure NetApp Dateien (NFS)	• AWS EFS • AWS S3 • Azure Blob • Azure NetApp Dateien (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Objekt-Storage • Google Cloud Storage • NFS-Server • On-Premises-ONTAP-Cluster • StorageGRID
Azure NetApp Files (SMB)	• AWS S3 • Azure Blob • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • IBM Cloud Objekt-Storage • On-Premises-ONTAP-Cluster • SMB Server • StorageGRID

Quellspeicherort	Unterstützte Zielstandorte
Cloud Volumes ONTAP (NFS)	• AWS EFS • AWS S3 • Azure Blob • Azure NetApp Dateien (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Objekt-Storage • Google Cloud Storage • NFS-Server • On-Premises-ONTAP-Cluster • StorageGRID
Cloud Volumes ONTAP (SMB)	• AWS S3 • Azure Blob • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • IBM Cloud Objekt-Storage • On-Premises-ONTAP-Cluster • SMB Server • StorageGRID
Cloud Volumes Service (NFS)	• AWS EFS • AWS S3 • Azure Blob • Azure NetApp Dateien (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Objekt-Storage • Google Cloud Storage • NFS-Server • On-Premises-ONTAP-Cluster • StorageGRID

Quellspeicherort	Unterstützte Zielstandorte
Cloud Volumes Service (SMB)	• AWS S3 • Azure Blob • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • IBM Cloud Objekt-Storage • On-Premises-ONTAP-Cluster • SMB Server • StorageGRID
Google Cloud Storage	• AWS EFS • AWS S3 • Azure Blob • Azure NetApp Dateien • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Objekt-Storage • NFS-Server • On-Premises-ONTAP-Cluster • SMB Server • StorageGRID
IBM Cloud Objekt-Storage	• AWS EFS • AWS S3 • Azure Blob • Azure NetApp Dateien • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Objekt-Storage • NFS-Server • On-Premises-ONTAP-Cluster • SMB Server • StorageGRID

Quellspeicherort	Unterstützte Zielstandorte
NFS-Server	• AWS EFS • AWS S3 • Azure Blob • Azure NetApp Dateien (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Objekt-Storage • Google Cloud Storage • NFS-Server • On-Premises-ONTAP-Cluster • StorageGRID
ONTAP-Cluster vor Ort (NFS)	• AWS EFS • AWS S3 • Azure Blob • Azure NetApp Dateien (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Objekt-Storage • Google Cloud Storage • NFS-Server • On-Premises-ONTAP-Cluster • StorageGRID
ONTAP-Cluster vor Ort (SMB)	• AWS S3 • Azure Blob • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • IBM Cloud Objekt-Storage • On-Premises-ONTAP-Cluster • SMB Server • StorageGRID
ONTAP S3 Storage	• StorageGRID

Quellspeicherort	Unterstützte Zielstandorte
SMB Server	• AWS S3 • Azure Blob • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • IBM Cloud Objekt-Storage • Google Cloud Storage • On-Premises-ONTAP-Cluster • SMB Server • StorageGRID
StorageGRID	• AWS EFS • AWS S3 • Azure Blob • Azure NetApp Dateien • Cloud Volumes ONTAP • Cloud Volumes Service • IBM Cloud Objekt-Storage • Google Cloud Storage • NFS-Server • On-Premises-ONTAP-Cluster • ONTAP S3 Storage • SMB Server • StorageGRID

Hinweise:

1. Sie können eine bestimmte Azure Blob Storage Tier auswählen, wenn ein Blob Container das Ziel ist:
    - Hot-Storage
    - Kühl lagern
2.]Sie können eine bestimmte S3-Storage-Klasse auswählen, wenn AWS S3 Ziel ist:
    - Standard (dies ist die Standardklasse)
    - Intelligent-Tiering
    - Standardzugriff
    - Ein einmaliger Zugriff
    - Glacier
    - Glacier Deep Archive

Networking für Quelle und Ziel

- Quelle und Ziel müssen über eine Netzwerkverbindung zum Daten-Broker verfügen.

  Wenn sich beispielsweise ein NFS-Server in Ihrem Datacenter befindet und der Data Broker in AWS ist, benötigen Sie eine Netzwerkverbindung (VPN oder Direct Connect) von Ihrem Netzwerk zum VPC.

- NetApp empfiehlt die Konfiguration des Quell-, Ziel- und Daten-Brokers für die Verwendung eines NTP-Services (Network Time Protocol). Die Zeitdifferenz zwischen den drei Komponenten darf 5 Minuten nicht überschreiten.

Quell- und Zielanforderungen

Stellen Sie sicher, dass Ihre Quelle und Ihre Ziele die folgenden Anforderungen erfüllen.

AWS S3-Bucket-Anforderungen

Stellen Sie sicher, dass Ihr AWS S3-Bucket die folgenden Anforderungen erfüllt.

Unterstützte Data Broker-Standorte für AWS S3

Für die Synchronisierung von Beziehungen, die S3-Storage beinhalten, ist ein Daten-Broker erforderlich, der in AWS oder in Ihrem Unternehmen implementiert ist. In beiden Fällen werden Sie von Cloud Sync aufgefordert, den Daten-Broker während der Installation mit einem AWS-Konto zu verknüpfen.

- "Erfahren Sie, wie Sie den AWS Data Broker implementieren"
- "Erfahren Sie, wie Sie den Data Broker auf einem Linux-Host installieren"

Unterstützte AWS-Regionen

Alle Regionen werden unterstützt, mit Ausnahme der Regionen China und GovCloud (USA).

Berechtigungen für S3-Buckets in anderen AWS-Konten erforderlich

Beim Einrichten einer Synchronisierungsbeziehung kann ein S3-Bucket angegeben werden, der sich in einem AWS-Konto befindet, das nicht mit dem Daten-Broker verbunden ist.

"Die in dieser JSON-Datei enthaltenen Berechtigungen" Muss auf diesen S3-Bucket angewendet werden, damit der Daten-Broker auf ihn zugreifen kann. Mit diesen Berechtigungen kann der Daten-Broker Daten in den und aus dem Bucket kopieren und die Objekte im Bucket auflisten.

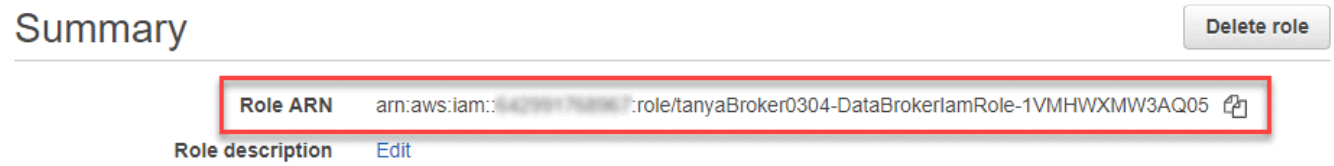
Beachten Sie Folgendes zu den in der JSON-Datei enthaltenen Berechtigungen:

1. *<BucketName>* ist der Name des Buckets, der sich im AWS-Konto befindet und nicht mit dem Daten-Broker verknüpft ist.
2. *<RoleARN>* sollte durch eine der folgenden Komponenten ersetzt werden:

   - Wenn der Datenvermittler manuell auf einem Linux-Host installiert wurde, sollte *RoleARN* der ARN des AWS-Benutzers sein, für den Sie bei der Bereitstellung des Datenmakers AWS Zugangsdaten angegeben haben.
   - Wenn der Datenvermittler mithilfe der CloudFormation-Vorlage in AWS implementiert wurde, sollte *RoleARN* der ARN der von der Vorlage erstellten IAM-Rolle sein.

     Sie finden die Role ARN, indem Sie die EC2-Konsole aufrufen, die Data Broker-Instanz auswählen und

auf der Registerkarte Beschreibung auf die IAM-Rolle klicken. Anschließend sollte die Seite Zusammenfassung in der IAM-Konsole angezeigt werden, die die Role ARN enthält.



Azure Blob Storage-Anforderungen

Stellen Sie sicher, dass Ihr Azure Blob Storage die folgenden Anforderungen erfüllt.

Unterstützte Data Broker-Standorte für Azure Blob

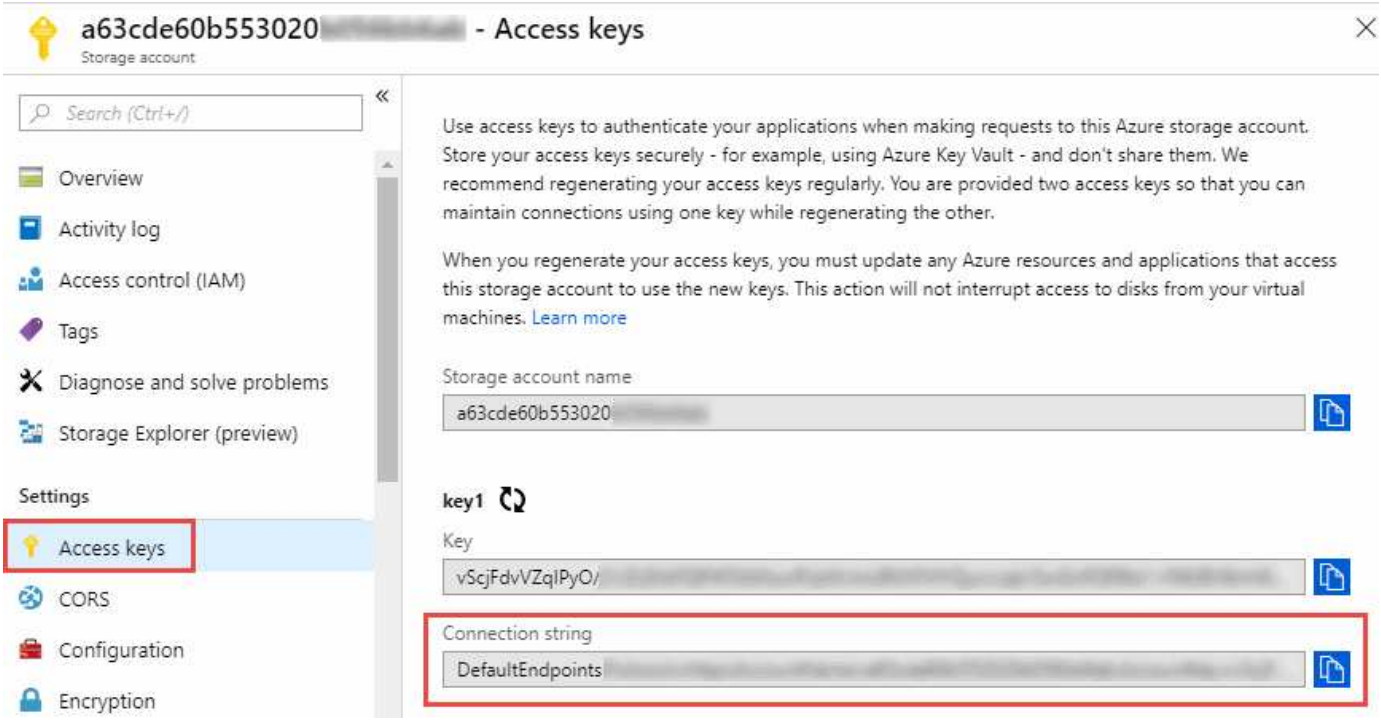
Der Data Broker kann sich an jedem beliebigen Speicherort befinden, wenn eine Synchronisierungsbeziehung Azure Blob Storage umfasst.

Unterstützte Azure Regionen

Alle Regionen werden unterstützt, mit Ausnahme der Regionen China, US Gov und US DoD.

Verbindungszeichenfolge wird für Beziehungen benötigt, die Azure Blob und NFS/SMB umfassen

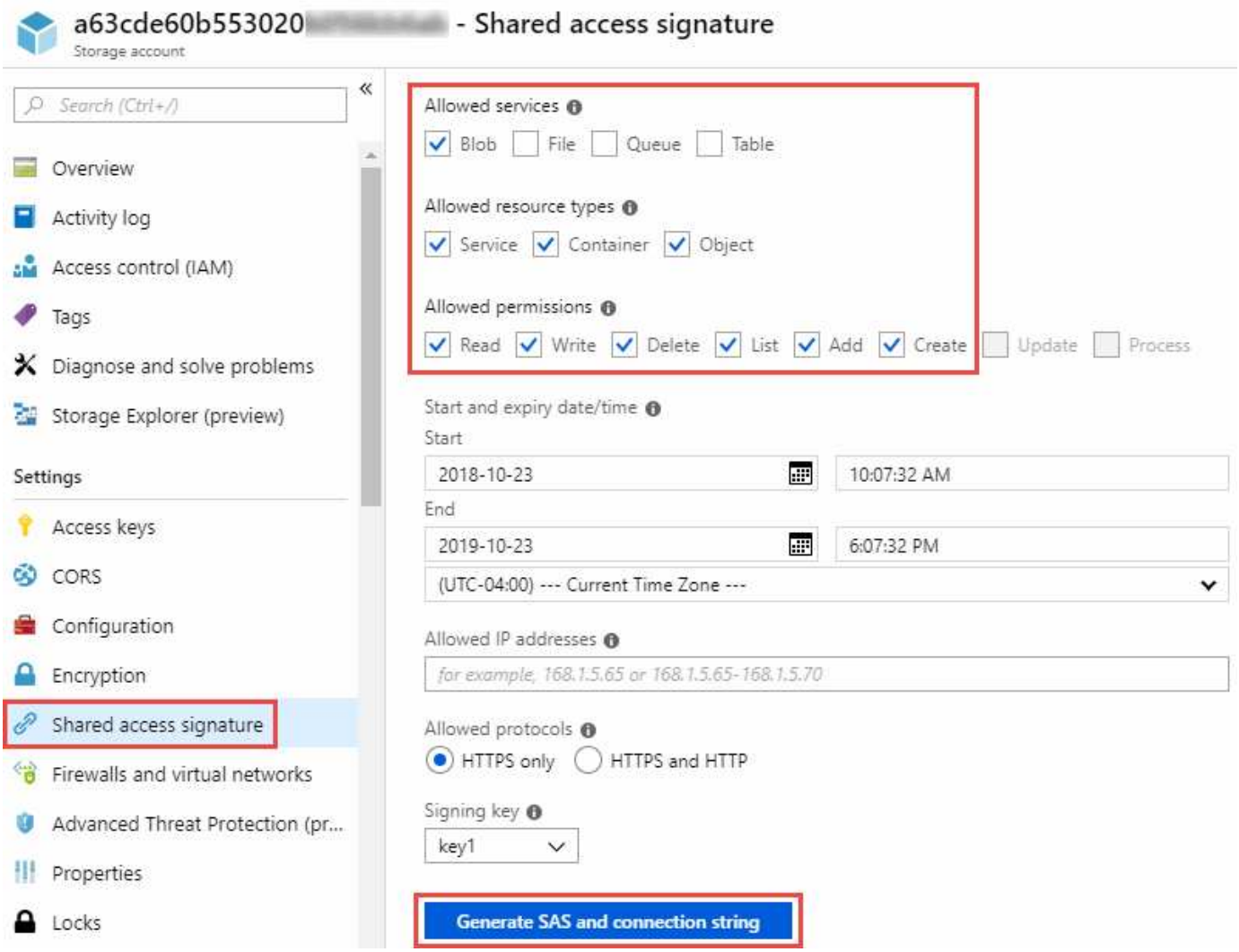
Wenn eine Synchronisierungsbeziehung zwischen einem Azure Blob Container und einem NFS- oder SMB-Server erstellt wird, muss Cloud Sync den Storage-Konto-Verbindungsstring bereitstellen:



Wenn Sie Daten zwischen zwei Azure Blob Containern synchronisieren möchten, muss die Verbindungszeichenfolge eine enthalten "Signatur für gemeinsamen Zugriff" (SAS). Außerdem haben Sie die Möglichkeit, eine SAS bei der Synchronisierung zwischen einem Blob Container und einem NFS- oder SMB-Server zu verwenden.

Der SAS muss den Zugriff auf den Blob Service und alle Ressourcentypen (Service, Container und Objekt) zulassen. Der SAS muss außerdem die folgenden Berechtigungen enthalten:

- Für den Blob Quellcontainer: Lesen und auflisten
- Für den Blob Zielcontainer: Lesen, Schreiben, Liste, Hinzufügen und Erstellen



Azure NetApp Files-Anforderungen

Verwenden Sie den Premium- oder Ultra-Service-Level, wenn Sie Daten mit oder von Azure NetApp Files synchronisieren. Im Falle eines standardmäßigen Festplatten-Service-Levels können Ausfälle und Performance-Probleme auftreten.

Wenden Sie sich an einen Solution Architect, wenn Sie Hilfe bei der Ermittlung des richtigen Service Levels benötigen. Die Volume-Größe und die Volume-Ebene bestimmen den zu ererzielen Durchsatz.

"Erfahren Sie mehr über Azure NetApp Files Service-Level und Durchsatz".

Anforderungen an Google Cloud Storage Bucket

Stellen Sie sicher, dass Ihr Google Cloud Storage Bucket die folgenden Anforderungen erfüllt.

Unterstützte Data Broker-Standorte für Google Cloud Storage

Für die Synchronisierung von Beziehungen, die Google Cloud Storage beinhalten, ist ein Daten-Broker erforderlich, der in GCP oder in Ihrem Unternehmen implementiert ist. Cloud Sync führt Sie beim Erstellen einer Synchronisierungsbeziehung durch den Installationsvorgang für Data Broker.

- "Erfahren Sie, wie Sie den GCP Data Broker implementieren"
- "Erfahren Sie, wie Sie den Data Broker auf einem Linux-Host installieren"

Unterstützte GCP-Regionen

Alle Regionen werden unterstützt.

NFS-Serveranforderungen

- Bei dem NFS-Server kann es sich um ein NetApp System oder ein System eines anderen Anbieters handeln.
- Der Dateiserver muss dem Data Broker-Host den Zugriff auf die Exporte ermöglichen.
- NFS-Versionen 3, 4.0, 4.1 und 4.2 werden unterstützt.

  Die gewünschte Version muss auf dem Server aktiviert sein.

- Wenn Sie NFS-Daten von einem ONTAP System synchronisieren möchten, stellen Sie sicher, dass der Zugriff auf die NFS-Exportliste für eine SVM aktiviert ist (vserver nfs modify -vServer *svm_Name* -showmount aktiviert).

  Die Standardeinstellung für showmount ist *enabled* ab ONTAP 9.2.

ONTAP-S3-Storage-Anforderungen

ONTAP 9.7 unterstützt Amazon Simple Storage Service (Amazon S3) als öffentliche Vorschau. "Weitere Informationen zur ONTAP Unterstützung für Amazon S3".

Wenn Sie eine Synchronisierungsbeziehung mit ONTAP S3 Storage einrichten, müssen Sie Folgendes angeben:

- Die IP-Adresse der mit ONTAP S3 verbundenen LIF
- Der Zugriffsschlüssel und der Geheimschlüssel, den ONTAP für die Verwendung konfiguriert ist

Anforderungen an SMB-Server

- Beim SMB Server kann es sich um ein NetApp System oder ein System eines anderen Herstellern beziehen.
- Der Dateiserver muss dem Data Broker-Host den Zugriff auf die Exporte ermöglichen.
- SMB-Versionen 1.0, 2.0, 2.1, 3.0 und 3.11 werden unterstützt.
- Gewähren Sie der Gruppe „Administratoren“ die Berechtigung „vollständige Kontrolle“ für die Quell- und Zielordner.

  Wenn Sie diese Berechtigung nicht erteilen, dann hat der Datenvermittler möglicherweise nicht genügend Berechtigungen, um die ACLs in einer Datei oder einem Verzeichnis zu erhalten. In diesem Fall erhalten Sie den folgenden Fehler: "Getxattr error 95"

SMB-Einschränkung für versteckte Verzeichnisse und Dateien

Eine SMB-Einschränkung betrifft versteckte Verzeichnisse und Dateien bei der Synchronisierung von Daten zwischen SMB-Servern. Wenn Verzeichnisse oder Dateien auf dem SMB-Quellserver durch Windows ausgeblendet wurden, wird das verborgene Attribut nicht auf den SMB-Zielserver kopiert.

Verhalten bei SMB-Synchronisierung aufgrund von Beschränkungen bei der Groß-/Kleinschreibung

Die Groß-/Kleinschreibung des SMB-Protokolls wird nicht berücksichtigt, sodass Groß- und Kleinbuchstaben als identisch behandelt werden. Dieses Verhalten kann zu Fehlern beim Überschreiben von Dateien und Verzeichniskopie führen, wenn eine Synchronisierungsbeziehung einen SMB-Server umfasst und bereits Daten auf dem Ziel vorhanden sind.

Nehmen wir zum Beispiel an, dass eine Datei namens „A“ auf der Quelle und eine Datei mit dem Namen „A“ auf dem Ziel vorhanden sind. Wenn Cloud Sync die Datei namens „A“ in das Ziel kopiert, wird Datei „A“ von der Quelle mit Datei „A“ überschrieben.

Im Falle von Verzeichnissen, sagen wir, dass es ein Verzeichnis namens "b" auf der Quelle und ein Verzeichnis namens "B" auf dem Ziel. Wenn Cloud Sync versucht, das Verzeichnis namens „b“ auf das Ziel zu kopieren, erhält Cloud Sync eine Fehlermeldung, dass das Verzeichnis bereits vorhanden ist. Infolgedessen kann Cloud Sync das Verzeichnis „b“ immer nicht kopieren.

Der beste Weg, um diese Einschränkung zu vermeiden, ist sicherzustellen, dass Sie Daten in einem leeren Verzeichnis synchronisieren.

Berechtigungen für ein SnapMirror Ziel

Wenn die Quelle für eine Sync-Beziehung ein SnapMirror-Ziel ist (schreibgeschützt), reichen die „Lese-/Listenberechtigungen“ aus, um die Daten aus der Quelle auf ein Ziel zu synchronisieren.

Netzwerkübersicht für Cloud Sync

Networking for Cloud Sync umfasst die Konnektivität zwischen dem Daten-Broker und den Quell- und Zielstandorten sowie eine ausgehende Internetverbindung vom Daten-Broker über Port 443.

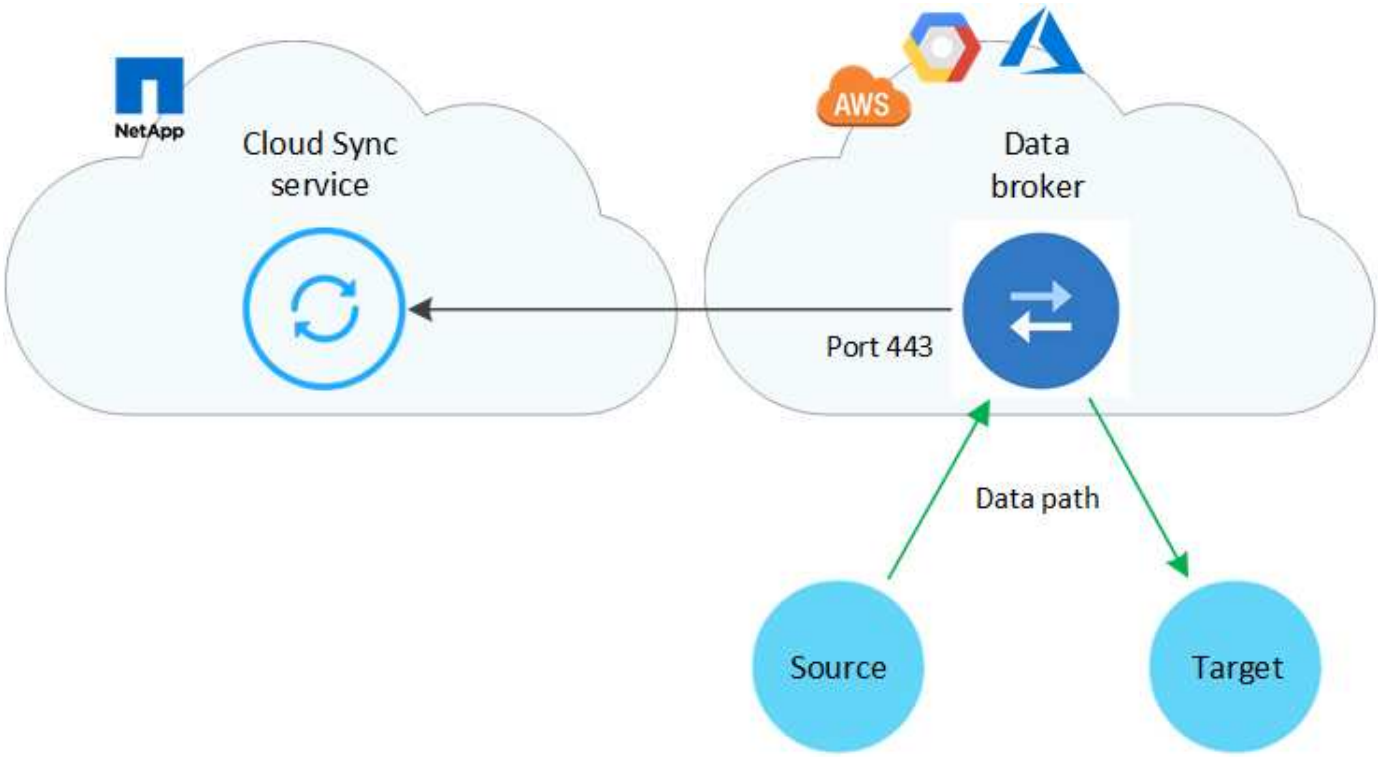
Speicherort für Daten-Broker

Installieren Sie den Daten-Broker in der Cloud oder vor Ort.

Data Broker in der Cloud

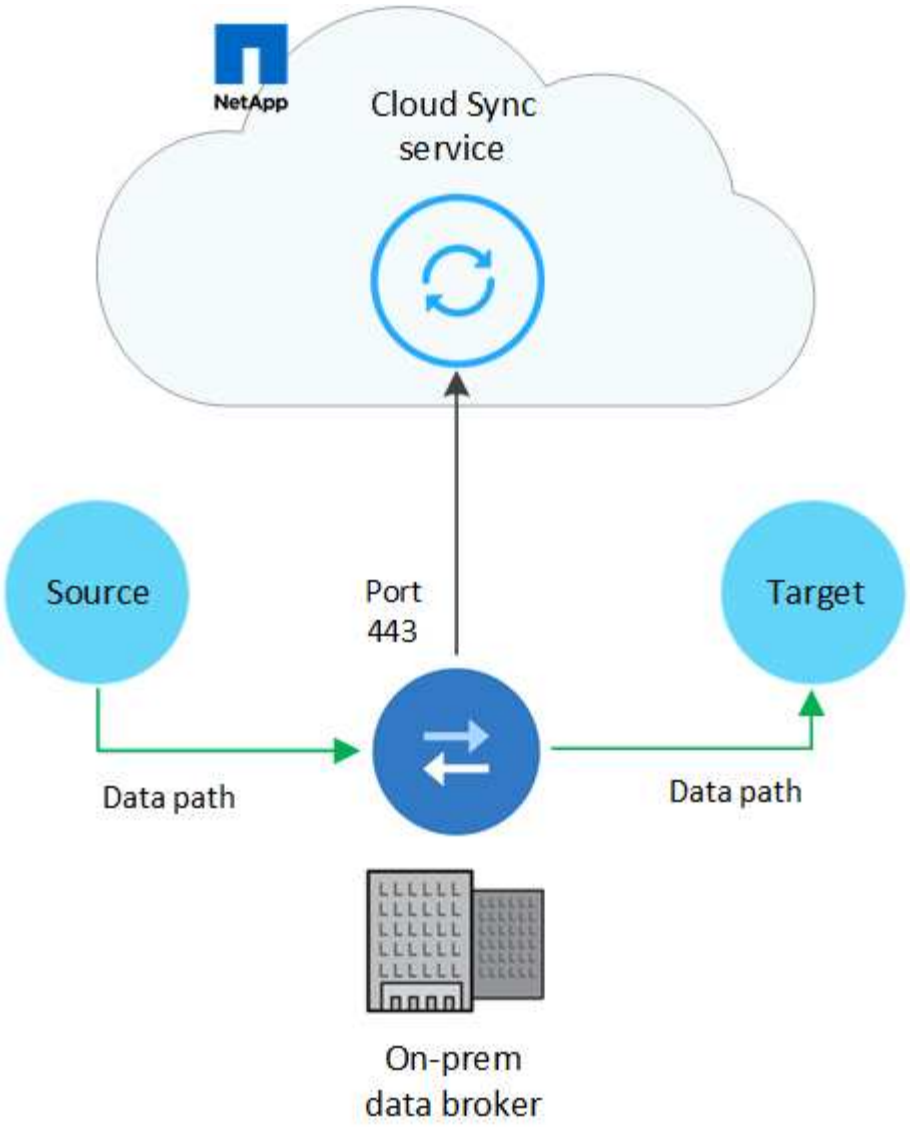
Die folgende Abbildung zeigt den Daten-Broker, der in der Cloud ausgeführt wird, entweder in AWS, GCP oder Azure. Quelle und Ziel können sich an jedem beliebigen Standort befinden, solange eine Verbindung zum Daten-Broker besteht. Sie haben beispielsweise eine VPN-Verbindung zwischen Ihrem Datacenter und Ihrem Cloud-Provider.

Wenn Cloud Sync den Data Broker in AWS, Azure oder GCP implementiert, erstellt es eine Sicherheitsgruppe, die die erforderliche ausgehende Kommunikation ermöglicht.



Data Broker vor Ort

Die folgende Abbildung zeigt den Data Broker, der in einem Datacenter auf dem Prem ausgeführt wird. Quelle und Ziel können sich an jedem beliebigen Standort befinden, solange die Verbindung zum Daten-Broker besteht.



Netzwerkanforderungen

- Quelle und Ziel müssen über eine Netzwerkverbindung zum Daten-Broker verfügen.

  Wenn sich beispielsweise ein NFS-Server in Ihrem Datacenter befindet und der Data Broker in AWS ist, benötigen Sie eine Netzwerkverbindung (VPN oder Direct Connect) von Ihrem Netzwerk zum VPC.

- Der Daten-Broker benötigt eine ausgehende Internetverbindung, damit er den Cloud Sync Service für Aufgaben über Port 443 abfragen kann.
- NetApp empfiehlt die Konfiguration des Quell-, Ziel- und Daten-Brokers für die Verwendung eines NTP-Services (Network Time Protocol). Die Zeitdifferenz zwischen den drei Komponenten darf 5 Minuten nicht überschreiten.

Netzwerkendpunkte

Der NetApp Data Broker benötigt ausgehenden Internetzugang über Port 443, um mit dem Cloud Sync Service zu kommunizieren und einige andere Services und Repositorys zu kontaktieren. Darüber hinaus erfordert Ihr lokaler Webbrowser für bestimmte Aktionen Zugriff auf Endpunkte. Wenn Sie die ausgehende Konnektivität beschränken müssen, lesen Sie die folgende Liste der Endpunkte, wenn Sie Ihre Firewall für ausgehenden Datenverkehr konfigurieren.

Data Broker-Endpunkte

Der Daten-Broker kontaktiert die folgenden Endpunkte:

Endpunkte	Zweck
Olcentgbl.trafficmanager.net:443	Um ein Repository für die Aktualisierung von CentOS-Paketen für den Data Broker-Host zu kontaktieren. Dieser Endpunkt wird nur kontaktiert, wenn Sie den Data Broker manuell auf einem CentOS Host installieren.
Rpm.nodesource.com:443 registry.npmjs.org/:443 nodejs.org/:443	Um Repositorys für die Aktualisierung von Node.js, NPM und anderen Drittanbieter-Paketen zu kontaktieren, die in der Entwicklung verwendet werden.
Tgz.pm2.io:443	Zugriff auf ein Repository zur Aktualisierung von PM2, einem Drittanbieter-Paket zur Überwachung von Cloud Sync.
Sqs.us-east-1.amazonaws.com:443 kinesis.us-east-1.amazonaws.com:443	Um die AWS-Services zu kontaktieren, die Cloud Sync für den Betrieb verwendet (Dateien in Warteschlange stellen, Aktionen registrieren und Aktualisierungen an den Daten-Broker senden).
s3.*region*.amazonaws.com:443 Beispiel: s3.us-east-2.amazonaws.com:443https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region["Eine Liste der S3-Endpunkte finden Sie in der AWS Dokumentation"^]	Um Amazon S3 zu kontaktieren, wenn eine Synchronisierungsbeziehung einen S3-Bucket enthält.
Cf.cloudsync.netapp.com:443 repo.cloudsync.netapp.com:443	Um den Cloud Sync Service zu kontaktieren.
Support.netapp.com:443	Um den NetApp Support zu kontaktieren, wenn eine Byol Lizenz für Synchronisierungsbeziehungen verwendet wird.
fedoraproject.org:443	Installation von 7 z auf der virtuellen Maschine des Datenmakers während der Installation und Aktualisierungen 7z ist erforderlich, um AutoSupport Meldungen an den technischen Support von NetApp zu senden.

Webbrowser-Endpunkte

Ihr Webbrowser benötigt Zugriff auf den folgenden Endpunkt, um Protokolle zur Fehlerbehebung herunterzuladen:

logs.cloudsync.netapp.com:443

Installieren eines Daten-Brokers

Installation des Data Brokers in AWS

Wenn Sie eine Synchronisierungsbeziehung erstellen, wählen Sie die Option AWS Data Broker, um die Data Broker-Software auf einer neuen EC2-Instanz in einem VPC bereitzustellen. Cloud Sync führt Sie durch den Installationsprozess, aber die Anforderungen und Schritte werden auf dieser Seite wiederholt, um Sie bei der

Vorbereitung auf die Installation zu unterstützen.

Sie haben auch die Möglichkeit, den Data Broker auf einem vorhandenen Linux-Host in der Cloud oder vor Ort zu installieren. "Weitere Informationen .".

Unterstützte AWS-Regionen

Alle Regionen werden unterstützt, mit Ausnahme der Regionen China und GovCloud (USA).

Netzwerkanforderungen

- Der Daten-Broker benötigt eine ausgehende Internetverbindung, damit er den Cloud Sync Service für Aufgaben über Port 443 abfragen kann.

  Wenn Cloud Sync den Datenbroker in AWS implementiert, wird eine Sicherheitsgruppe erstellt, die die erforderliche ausgehende Kommunikation ermöglicht. Beachten Sie, dass Sie den Data Broker so konfigurieren können, dass er während des Installationsvorgangs einen Proxyserver verwendet.

  Wenn Sie die ausgehende Verbindung begrenzen müssen, lesen Sie "Die Liste der Endpunkte, die der Datenmanager kontaktiert".

- NetApp empfiehlt die Konfiguration des Quell-, Ziel- und Daten-Brokers für die Verwendung eines NTP-Services (Network Time Protocol). Die Zeitdifferenz zwischen den drei Komponenten darf 5 Minuten nicht überschreiten.

Erforderliche Berechtigungen für die Bereitstellung des Data Brokers in AWS

Das AWS Benutzerkonto, das Sie für die Bereitstellung des Daten-Brokers verwenden, muss über die Berechtigungen in verfügen "Von NetApp bereitgestellt".

] Anforderungen, Ihre eigene IAM-Rolle mit dem AWS Daten-Broker zu nutzen

Wenn Cloud Sync den Data Broker bereitstellt, erstellt es eine IAM-Rolle für die Data Brokerinstanz. Sie können den Data Broker auf Wunsch mit Ihrer eigenen IAM-Rolle bereitstellen. Sie können diese Option verwenden, wenn Ihr Unternehmen über strenge Sicherheitsrichtlinien verfügt.

Die IAM-Rolle muss die folgenden Anforderungen erfüllen:

- Der EC2-Dienst muss die IAM-Rolle als vertrauenswürdige Einheit übernehmen können.
- "Die in dieser JSON-Datei definierten Berechtigungen" Muss mit der IAM-Rolle verbunden sein, damit der Daten-Broker ordnungsgemäß funktionieren kann.

Befolgen Sie die folgenden Schritte, um die IAM-Rolle beim Bereitstellen des Daten-Brokers anzugeben.

Installation des Data Brokers

Sie können einen Daten-Broker in AWS installieren, wenn Sie eine Synchronisierungsbeziehung erstellen.

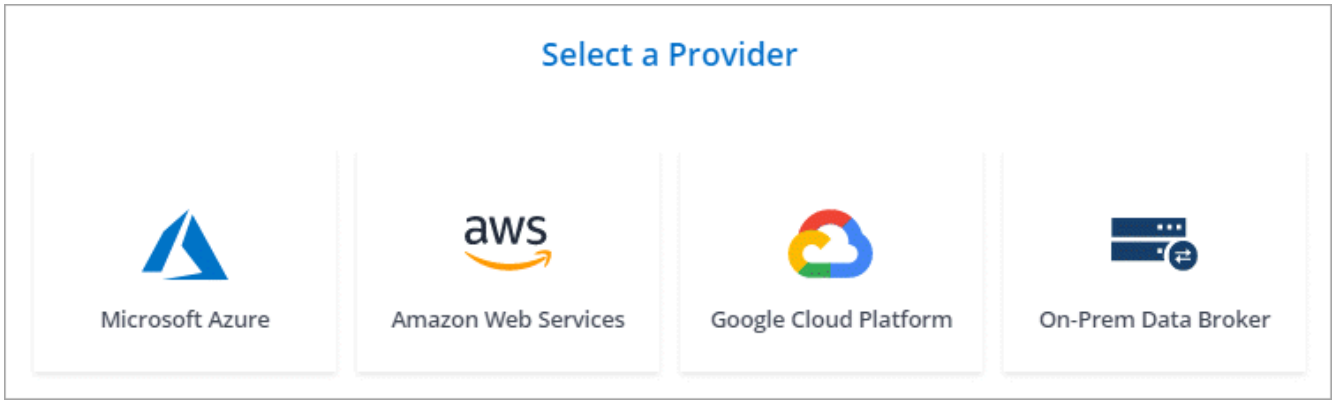
Schritte

1. Klicken Sie Auf **Neuen Sync Erstellen**.
2. Wählen Sie auf der Seite **Synchronisierungsbeziehung definieren** eine Quelle und ein Ziel aus und klicken Sie auf **Weiter**.

   Führen Sie die Schritte aus, bis Sie zur Seite **Data Broker** gelangen.

3. Klicken Sie auf der Seite **Data Broker** auf **Daten Broker erstellen** und wählen Sie dann **Amazon Web Services** aus.

   Wenn Sie bereits einen Daten-Broker haben, müssen Sie auf klicken + Symbol zuerst.



4. Geben Sie einen Namen für den Daten-Broker ein und klicken Sie auf **Weiter**.
5. Geben Sie einen AWS-Zugriffsschlüssel ein, damit Cloud Sync in Ihrem Auftrag den Daten-Broker in AWS erstellen kann.

   Die Tasten werden nicht gespeichert oder für andere Zwecke verwendet.

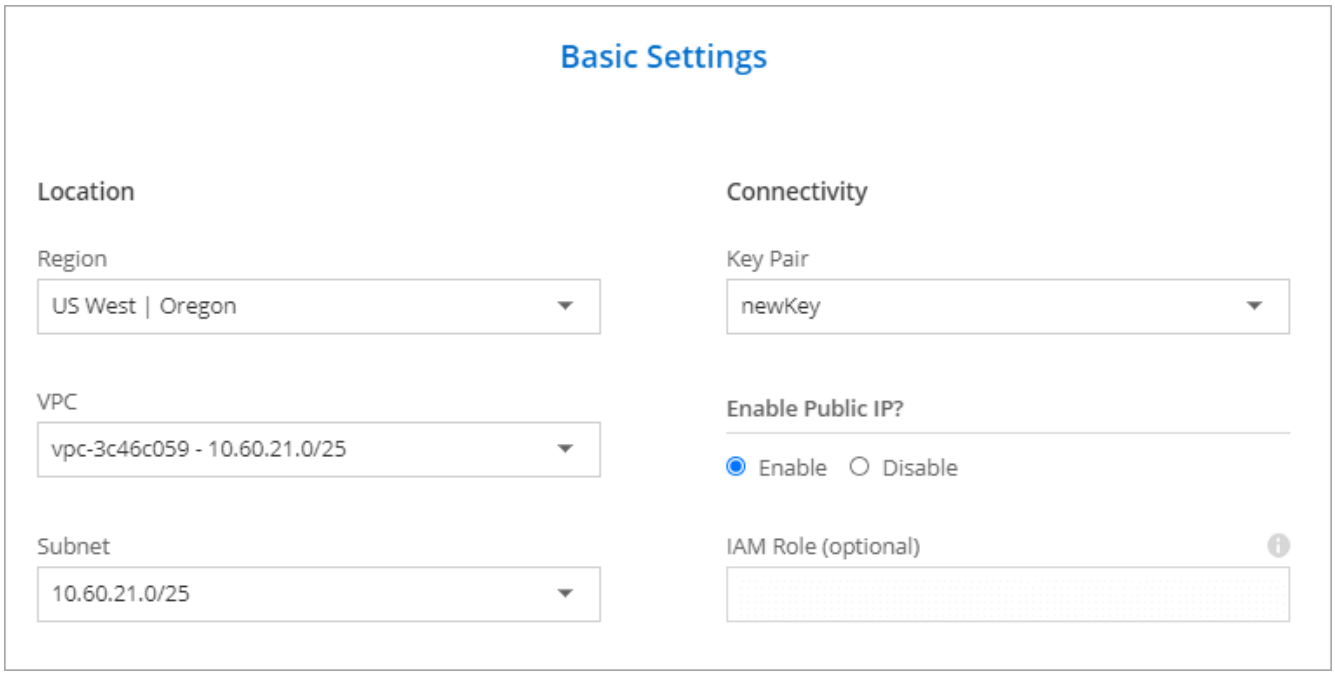
   Falls Sie keine Zugriffsschlüssel angeben möchten, klicken Sie auf den Link unten auf der Seite, um stattdessen eine CloudFormation-Vorlage zu verwenden. Wenn Sie diese Option verwenden, müssen Sie keine Anmeldedaten angeben, da Sie sich direkt bei AWS anmelden.

   das folgende Video zeigt, wie die Instanz des Datenmakers mithilfe einer CloudFormation-Vorlage gestartet wird:

   ► https://docs.netapp.com/de-de/occm38//media/video_cloud_sync.mp4 *(video)*

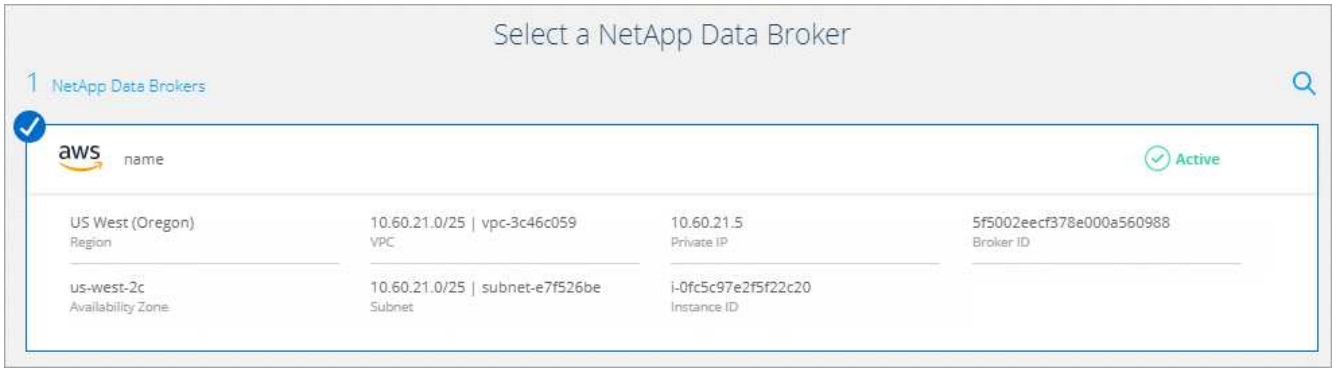
6. Wenn Sie einen AWS-Zugriffsschlüssel eingegeben haben, wählen Sie einen Speicherort für die Instanz aus, wählen Sie ein Schlüsselpaar aus, wählen Sie aus, ob eine öffentliche IP-Adresse aktiviert werden soll, und wählen Sie dann eine vorhandene IAM-Rolle aus. Lassen Sie das Feld leer, sodass Cloud Sync die Rolle für Sie erstellt.

   Wenn Sie Ihre eigene IAM-Rolle wählen, Sie müssen die erforderlichen Berechtigungen angeben.



7. Klicken Sie nach Verfügbarkeit des Datenmakers in Cloud Sync auf **Weiter**.

   Das folgende Bild zeigt eine erfolgreich implementierte Instanz in AWS:



8. Füllen Sie die Seiten im Assistenten aus, um die neue Synchronisierungsbeziehung zu erstellen.

Ergebnis

Sie haben einen Daten-Broker in AWS implementiert und eine neue Synchronisierungsbeziehung erstellt. Sie können diesen Daten-Broker mit zusätzlichen Synchronisierungsbeziehungen verwenden.

Installieren des Data Brokers in Azure

Wenn Sie eine Synchronisierungsbeziehung erstellen, wählen Sie die Option Azure Data Broker, um die Data Broker-Software auf einer neuen virtuellen Maschine in einem VNet bereitzustellen. Cloud Sync führt Sie durch den Installationsprozess, aber die Anforderungen und Schritte werden auf dieser Seite wiederholt, um Sie bei der Vorbereitung auf die Installation zu unterstützen.

Sie haben auch die Möglichkeit, den Data Broker auf einem vorhandenen Linux-Host in der Cloud oder vor Ort zu installieren. "Weitere Informationen .".

Unterstützte Azure Regionen

Alle Regionen werden unterstützt, mit Ausnahme der Regionen China, US Gov und US DoD.

Netzwerkanforderungen

- Der Daten-Broker benötigt eine ausgehende Internetverbindung, damit er den Cloud Sync Service für Aufgaben über Port 443 abfragen kann.

  Wenn Cloud Sync den Data Broker in Azure bereitstellt, erstellt es eine Sicherheitsgruppe, die die erforderliche ausgehende Kommunikation ermöglicht.

  Wenn Sie die ausgehende Verbindung begrenzen müssen, lesen Sie "Die Liste der Endpunkte, die der Datenmanager kontaktiert".

- NetApp empfiehlt die Konfiguration des Quell-, Ziel- und Daten-Brokers für die Verwendung eines NTP-Services (Network Time Protocol). Die Zeitdifferenz zwischen den drei Komponenten darf 5 Minuten nicht überschreiten.

Authentifizierungsmethode

Bei der Bereitstellung des Daten-Brokers müssen Sie eine Authentifizierungsmethode wählen: Ein Passwort oder ein SSH Public-Private Key Pair.

Hilfe zum Erstellen eines Schlüsselpaares finden Sie unter "Azure Dokumentation: Erstellen und Verwenden eines öffentlichen SSH-privaten Schlüsselpaares für Linux VMs in Azure".

Installation des Data Brokers

Sie können einen Data Broker in Azure installieren, wenn Sie eine Synchronisierungsbeziehung erstellen.

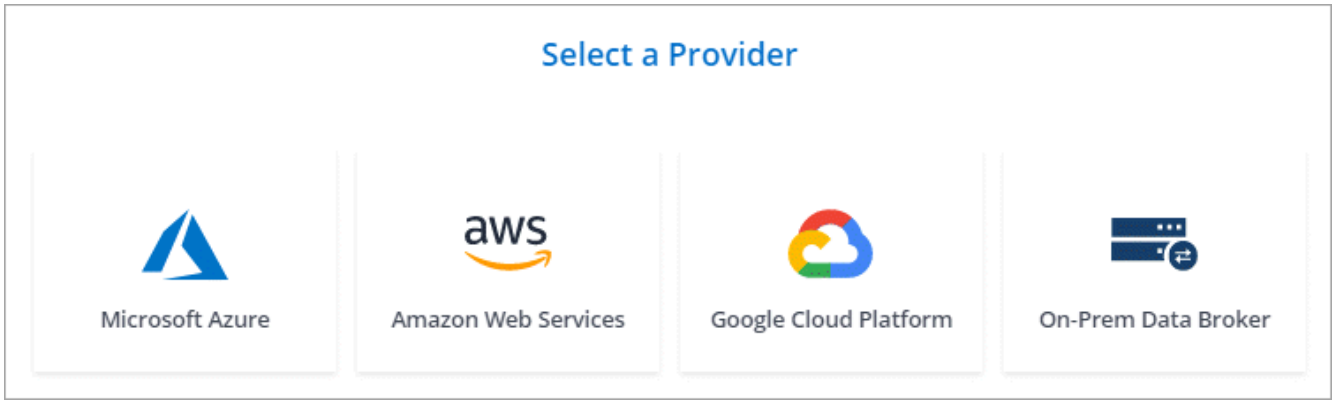
Schritte

1. Klicken Sie Auf **Neuen Sync Erstellen**.
2. Wählen Sie auf der Seite **Synchronisierungsbeziehung definieren** eine Quelle und ein Ziel aus und klicken Sie auf **Weiter**.

   Füllen Sie die Seiten aus, bis Sie zur Seite **Data Broker** gelangen.

3. Klicken Sie auf der Seite **Data Broker** auf **Daten Broker erstellen** und wählen Sie dann **Microsoft Azure** aus.

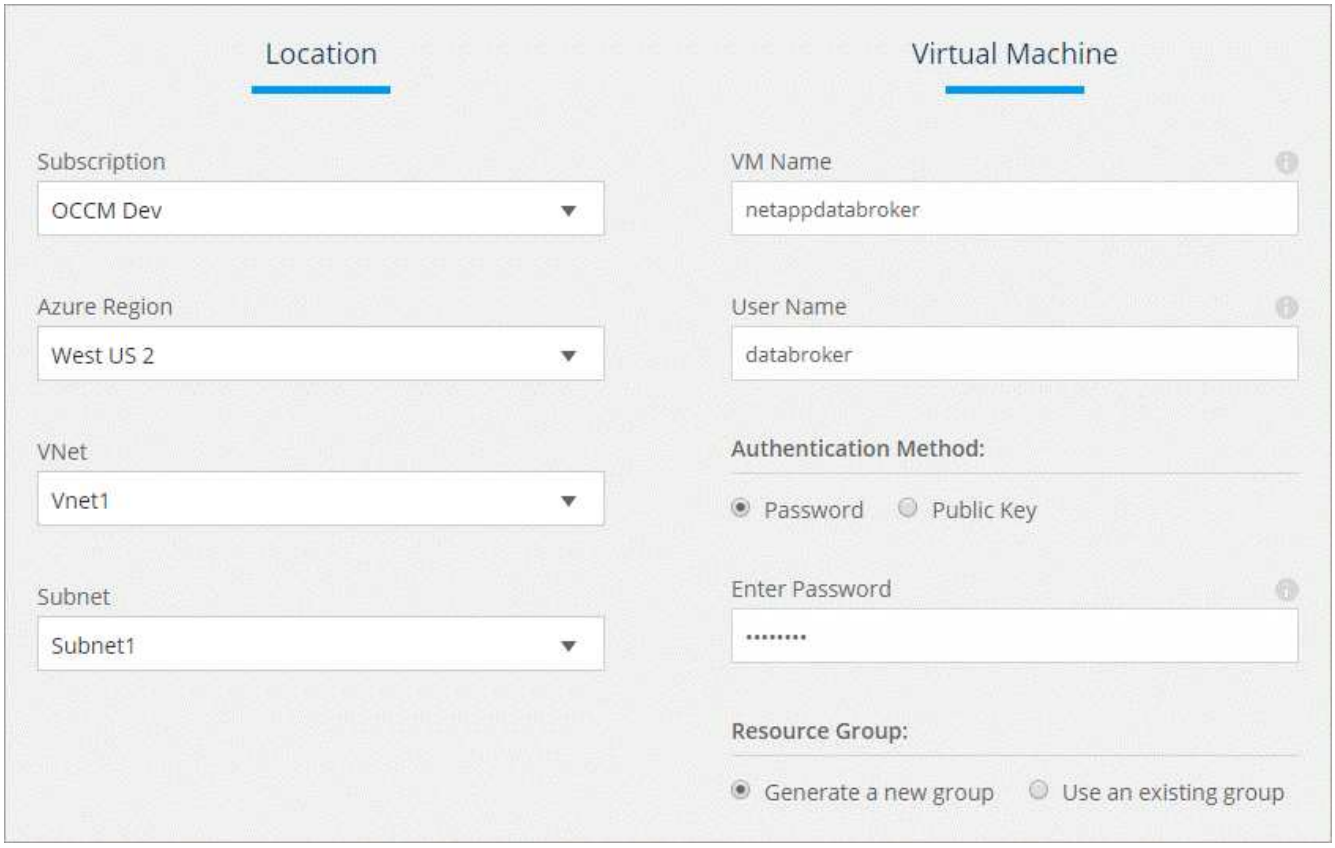
   Wenn Sie bereits einen Daten-Broker haben, müssen Sie auf klicken  Symbol zuerst.



4. Geben Sie einen Namen für den Daten-Broker ein und klicken Sie auf **Weiter**.
5. Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem Microsoft-Konto an. Wenn Sie nicht aufgefordert werden, klicken Sie auf **in Azure** anmelden.

   Das Formular ist Eigentum von Microsoft und wird von Microsoft gehostet. Ihre Zugangsdaten werden nicht an NetApp bereitgestellt.

6. Wählen Sie einen Speicherort für den Daten-Broker aus, und geben Sie grundlegende Details zur virtuellen Maschine ein.



7. Klicken Sie auf **Weiter** und lassen Sie die Seite offen, bis die Bereitstellung abgeschlossen ist.

   Dieser Vorgang kann bis zu 7 Minuten dauern.

8. Klicken Sie in Cloud Sync auf **Weiter**, sobald der Datenvermittler verfügbar ist.
9. Füllen Sie die Seiten im Assistenten aus, um die neue Synchronisierungsbeziehung zu erstellen.

Ergebnis

Sie haben einen Data Broker in Azure bereitgestellt und eine neue Synchronisierungsbeziehung erstellt. Sie können diesen Daten-Broker mit zusätzlichen Synchronisierungsbeziehungen verwenden.

Möchten Sie eine Nachricht über die Notwendigkeit einer Administratorerklärung erhalten?

Wenn Microsoft Sie benachrichtigt, dass eine Administratorgenehmigung erforderlich ist, da Cloud Sync die Berechtigung für den Zugriff auf Ressourcen in Ihrem Unternehmen benötigt, stehen Ihnen zwei Optionen zur Verfügung:

1. Bitten Sie Ihren AD-Administrator, Ihnen die folgende Berechtigung zu erteilen:

   In Azure gehen Sie zu **Admin Center > Azure AD > Users and Groups > User Settings** und aktivieren Sie **Benutzer können den Zugriff von Apps auf Unternehmensdaten für sie zustimmen**.

2. Bitten Sie Ihren AD-Administrator um Zustimmung für **CloudSync-AzureDataBrokerCreator** unter Verwendung der folgenden URL (dies ist der Admin-Einwilligungsendpunkt):

   https://login.microsoftonline.com/{FILL HIER IHRE MANDANTEN-ID}/v2.0/adminZustimmung?Client_id=8ee4ca3a-bafa-4831-97cc-5a38923c85&redirect_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read

   Wie in der URL dargestellt, ist unsere App-URL https://cloudsync.netapp.com und die Application-Client-ID 8ee4ca3a-bafa-4831-97cc-5a38923cab85.

Installation des Daten-Brokers in Google Cloud Platform

Wenn Sie eine Synchronisierungsbeziehung erstellen, wählen Sie die Option GCP Data Broker, um die Data Broker-Software auf einer neuen virtuellen Maschineninstanz in einem VPC bereitzustellen. Cloud Sync führt Sie durch den Installationsprozess, aber die Anforderungen und Schritte werden auf dieser Seite wiederholt, um Sie bei der Vorbereitung auf die Installation zu unterstützen.

Sie haben auch die Möglichkeit, den Data Broker auf einem vorhandenen Linux-Host in der Cloud oder vor Ort zu installieren. "Weitere Informationen .".

Unterstützte GCP-Regionen

Alle Regionen werden unterstützt.

Netzwerkanforderungen

- Der Daten-Broker benötigt eine ausgehende Internetverbindung, damit er den Cloud Sync Service für Aufgaben über Port 443 abfragen kann.

  Wenn Cloud Sync den Data Broker in GCP implementiert, erstellt es eine Sicherheitsgruppe, die die erforderliche ausgehende Kommunikation ermöglicht.

Wenn Sie die ausgehende Verbindung begrenzen müssen, lesen Sie "Die Liste der Endpunkte, die der Datenmanager kontaktiert".

- NetApp empfiehlt die Konfiguration des Quell-, Ziel- und Daten-Brokers für die Verwendung eines NTP-Services (Network Time Protocol). Die Zeitdifferenz zwischen den drei Komponenten darf 5 Minuten nicht überschreiten.

Erforderliche Berechtigungen zum Bereitstellen des Data Brokers in GCP

Stellen Sie sicher, dass der GCP-Benutzer, der den Daten-Broker bereitstellt, folgende Berechtigungen hat:

```
- compute.networks.list
- compute.regions.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.operations.get
- iam.serviceAccounts.list
```

Für das Servicekonto erforderliche Berechtigungen

Wenn Sie den Datenvermittler bereitstellen, müssen Sie ein Servicekonto mit den folgenden Berechtigungen auswählen:

```
- logging.logEntries.create
- resourcemanager.projects.get
- storage.buckets.get
- storage.buckets.list
- storage.objects.*
```

Installation des Data Brokers

Sie können einen Daten-Broker in GCP installieren, wenn Sie eine Synchronisierungsbeziehung erstellen.

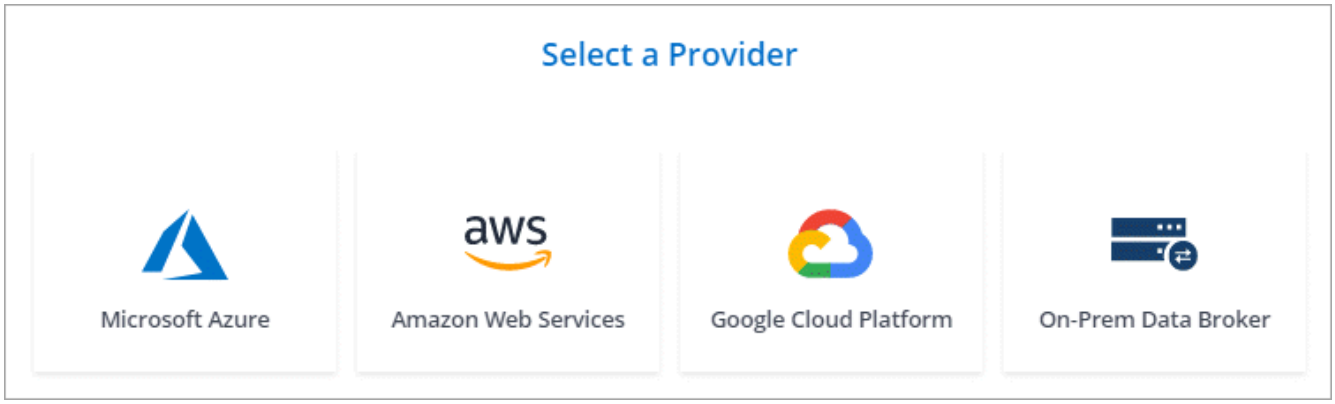
Schritte

1. Klicken Sie Auf **Neuen Sync Erstellen**.
2. Wählen Sie auf der Seite **Synchronisierungsbeziehung definieren** eine Quelle und ein Ziel aus und klicken Sie auf **Weiter**.

   Führen Sie die Schritte aus, bis Sie zur Seite **Data Broker** gelangen.

3. Klicken Sie auf der Seite **Data Broker** auf **Daten Broker erstellen** und wählen Sie dann **Google Cloud Platform** aus.

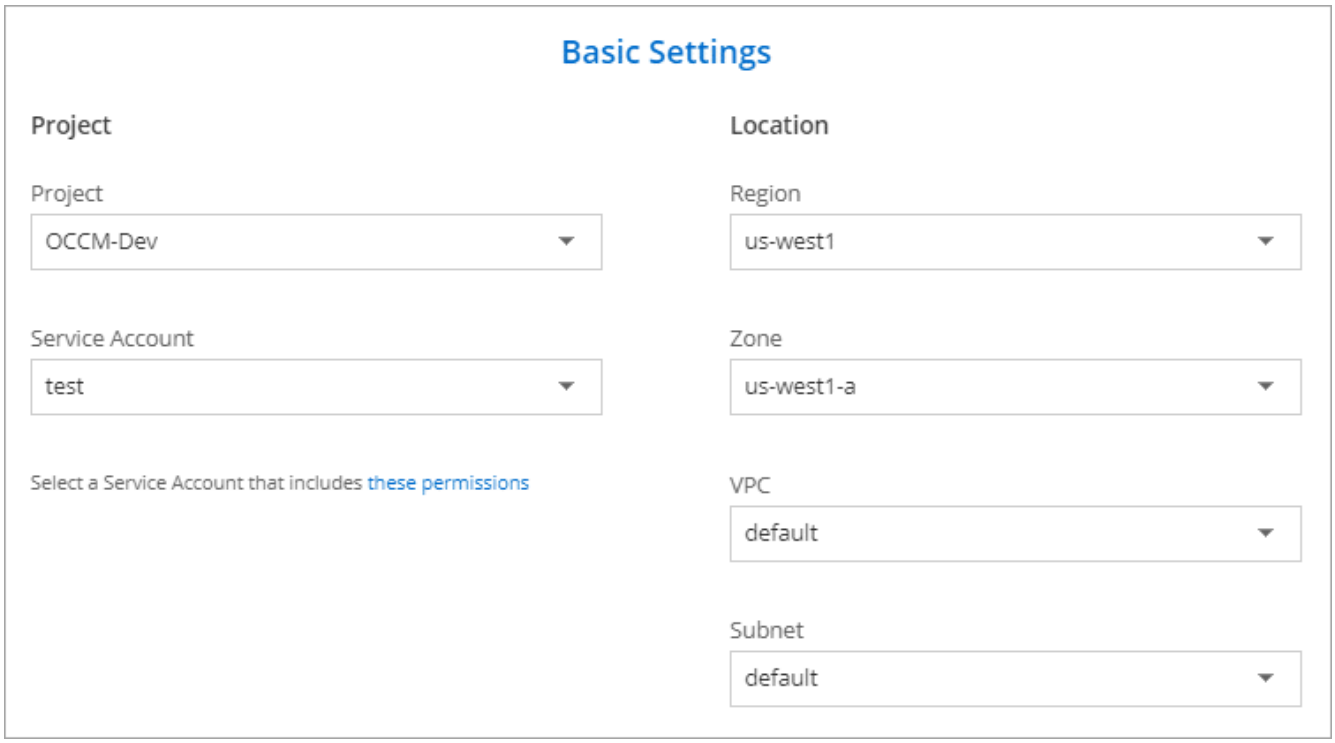
   Wenn Sie bereits einen Daten-Broker haben, müssen Sie auf klicken  Symbol zuerst.



4. Geben Sie einen Namen für den Daten-Broker ein und klicken Sie auf **Weiter**.
5. Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem Google-Konto an.

   Das Formular ist Eigentum und wird von Google gehostet. Ihre Zugangsdaten werden nicht an NetApp bereitgestellt.

6. Wählen Sie ein Projekt- und ein Servicekonto aus, und wählen Sie dann einen Speicherort für den Datenvermittler aus.



7. Sobald der Datenvermittler verfügbar ist, klicken Sie in Cloud Sync auf **Weiter**.

   Die Bereitstellung der Instanz dauert etwa 5 bis 10 Minuten. Sie können den Fortschritt des Cloud Sync-Dienstes überwachen, der automatisch aktualisiert wird, wenn die Instanz verfügbar ist.

8. Füllen Sie die Seiten im Assistenten aus, um die neue Synchronisierungsbeziehung zu erstellen.

Ergebnis

Sie haben einen Datenvermittler in GCP implementiert und eine neue Synchronisierungsbeziehung erstellt. Sie können diesen Daten-Broker mit zusätzlichen Synchronisierungsbeziehungen verwenden.

Installation des Data Brokers auf einem Linux-Host

Wenn Sie eine Synchronisierungsbeziehung erstellen, wählen Sie die Option On-Prem Data Broker, um die Data Broker-Software auf einem lokalen Linux-Host oder auf einem vorhandenen Linux-Host in der Cloud zu installieren. Cloud Sync führt Sie durch den Installationsprozess, aber die Anforderungen und Schritte werden auf dieser Seite wiederholt, um Sie bei der Vorbereitung auf die Installation zu unterstützen.

Anforderungen an Linux-Hosts

- **Betriebssystem**:
  - CentOS 7.0, 7.7 und 8.0
  - Red hat Enterprise Linux 7.7 und 8.0
  - Ubuntu Server 18.04 LTS
  - SUSE Linux Enterprise Server 15 SP1

    Der Befehl `yum update all` Muss auf dem Host ausgeführt werden, bevor Sie den Daten-Broker installieren.

  Ein Red Hat Enterprise Linux-System muss bei Red Hat Subscription Management registriert sein. Wenn sie nicht registriert ist, kann das System während der Installation nicht auf Repositorys zugreifen, um die erforderliche Software von Drittanbietern zu aktualisieren.

- **RAM**: 16 GB
- **CPU**: 4 Kerne
- **Freier Speicherplatz**: 10 GB
- **SELinux**: Wir empfehlen Ihnen zu deaktivieren "SELinux" Auf dem Host.

  SELinux setzt eine Richtlinie durch, die Softwareupdates für den Datentmanager blockiert und den Datenmanager davon absperrt, Endpunkte zu kontaktieren, die für den normalen Betrieb erforderlich sind.

- **OpenSSL**: OpenSSL muss auf dem Linux-Host installiert sein.

Netzwerkanforderungen

- Der Linux-Host muss eine Verbindung mit der Quelle und dem Ziel haben.
- Der Dateiserver muss es dem Linux-Host ermöglichen, auf die Exporte zuzugreifen.
- Port 443 muss auf dem Linux-Host für Outbound-Datenverkehr zu AWS offen sein (der Daten-Broker kommuniziert fortwährend mit dem Amazon SQS Service).
- NetApp empfiehlt die Konfiguration des Quell-, Ziel- und Daten-Brokers für die Verwendung eines NTP-Services (Network Time Protocol). Die Zeitdifferenz zwischen den drei Komponenten darf 5 Minuten nicht überschreiten.

Zugriff auf AWS wird ermöglicht

Wenn Sie den Daten-Broker mit einer Synchronisierungsbeziehung mit einem S3-Bucket verwenden möchten, sollten Sie den Linux-Host für den AWS-Zugriff vorbereiten. Nach der Installation des Daten-Brokers müssen Sie AWS Schlüssel für einen AWS-Benutzer bereitstellen, der programmatischen Zugriff und bestimmte Berechtigungen hat.

Schritte

1. Erstellen Sie eine IAM-Richtlinie mit "Von NetApp bereitgestellt". "AWS-Anweisungen anzeigen".
2. Erstellen Sie einen IAM-Benutzer mit programmatischem Zugriff. "AWS-Anweisungen anzeigen".

   Achten Sie darauf, die AWS-Schlüssel zu kopieren, da Sie sie bei der Installation der Data Broker-Software angeben müssen.

Zugriff auf Google Cloud wird ermöglicht

Wenn Sie den Daten-Broker mit einer Synchronisierung verwenden möchten, die einen Google Cloud Storage Bucket enthält, sollten Sie den Linux-Host für GCP-Zugriff vorbereiten. Nach der Installation des Daten-Brokers müssen Sie einen Schlüssel für ein Servicekonto mit spezifischen Berechtigungen bereitstellen.

Schritte

1. Erstellen Sie ein GCP-Servicekonto mit Storage Admin-Berechtigungen, wenn Sie noch nicht über eines verfügen.
2. Erstellen Sie einen im JSON-Format gespeicherten Dienstkontenschlüssel. "GCP-Anweisungen anzeigen".

   Die Datei sollte mindestens die folgenden Eigenschaften enthalten: „Project_id“, „Private_Key“ und „Client_email“

   Wenn Sie einen Schlüssel erstellen, wird die Datei generiert und auf Ihren Computer heruntergeladen.

3. Speichern Sie die JSON-Datei auf dem Linux-Host.

Zugriff auf Microsoft Azure wird ermöglicht

Der Zugriff auf Azure wird pro Beziehung definiert. Dazu wird ein Storage-Konto und eine Verbindungszeichenfolge im Assistenten für synchrone Beziehungen bereitgestellt.

Installation des Data Brokers

Sie können einen Data Broker auf einem Linux-Host installieren, wenn Sie eine Synchronisierungsbeziehung erstellen.

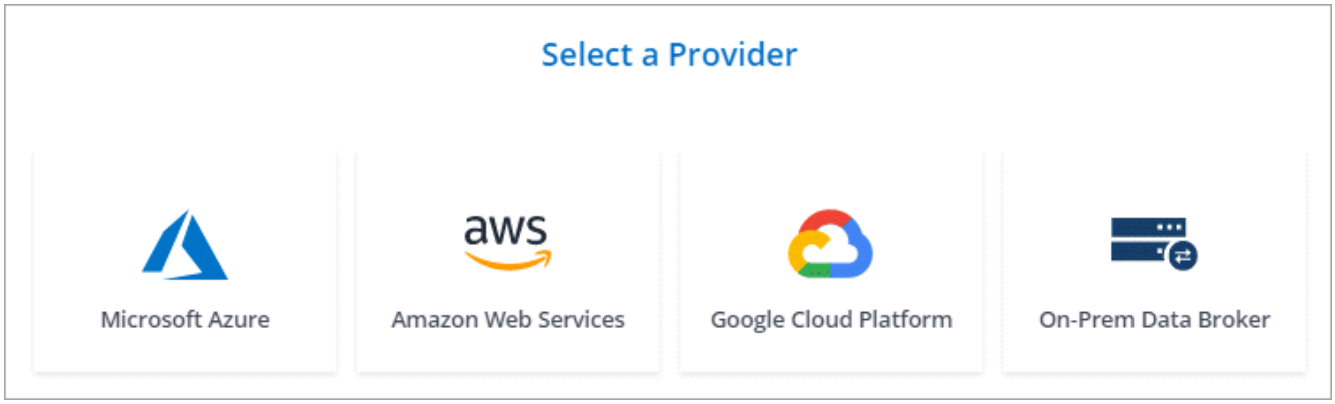
Schritte

1. Klicken Sie Auf **Neuen Sync Erstellen**.
2. Wählen Sie auf der Seite **Synchronisierungsbeziehung definieren** eine Quelle und ein Ziel aus und klicken Sie auf **Weiter**.

   Führen Sie die Schritte aus, bis Sie zur Seite **Data Broker** gelangen.

3. Klicken Sie auf der Seite **Data Broker** auf **Daten Broker erstellen** und wählen Sie dann **On-Prem Data Broker** aus.

   Wenn Sie bereits einen Daten-Broker haben, müssen Sie auf klicken + Symbol zuerst.



Obwohl die Option mit ***On-Prem*** **Data Broker** gekennzeichnet ist, gilt sie für einen Linux-Host vor Ort oder in der Cloud.

4. Geben Sie einen Namen für den Daten-Broker ein und klicken Sie auf **Weiter**.

   Die Seite mit den Anweisungen wird in Kürze geladen. Sie müssen diese Anweisungen befolgen - sie enthalten einen eindeutigen Link, um das Installationsprogramm herunterzuladen.

5. Auf der Seite mit den Anweisungen:
   a. Wählen Sie aus, ob der Zugriff auf **AWS**, **Google Cloud** oder beides aktiviert werden soll.
   b. Wählen Sie eine Installationsoption aus: **Kein Proxy**, **Proxy-Server verwenden** oder **Proxy-Server mit Authentifizierung verwenden**.
   c. Verwenden Sie die Befehle, um den Daten-Broker herunterzuladen und zu installieren.

      Die folgenden Schritte enthalten Details zu den einzelnen möglichen Installationsoption. Folgen Sie der Seite mit den Anweisungen, um den genauen Befehl basierend auf Ihrer Installationsoption anzuzeigen.

   d. Laden Sie das Installationsprogramm herunter:
      - Kein Proxy:

        ```
        curl <URI> -o data_broker_installer.sh
        ```

      - Proxy-Server verwenden:

        ```
        curl <URI> -o data_broker_installer.sh -x <proxy_host>:<proxy_port>
        ```

      - Proxy-Server mit Authentifizierung verwenden:

        ```
        curl <URI> -o data_broker_installer.sh -x
        <proxy_username>:<proxy_password>@<proxy_host>:<proxy_port>
        ```

        URI

        Cloud Sync zeigt die URI der Installationsdatei auf der Seite mit den Anweisungen an, die beim Befolgen der Anweisungen zur Bereitstellung des On-Prem-Datenmakers geladen wird. Dieser URI wird hier nicht wiederholt, weil der Link dynamisch erzeugt wird und nur einmal verwendet werden kann. Führen Sie diese Schritte aus, um den URI aus Cloud Sync zu erhalten.

   e. Wechseln Sie zu Superuser, machen Sie das Installationsprogramm ausführbar und installieren Sie die Software:

Jeder der unten aufgeführten Befehle enthält Parameter für AWS-Zugriff und GCP-Zugriff. Folgen Sie der Seite mit den Anweisungen, um den genauen Befehl basierend auf Ihrer Installationsoption anzuzeigen.

- Keine Proxy-Konfiguration:

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file>
```

- Proxy-Konfiguration:

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port>
```

- Proxy-Konfiguration mit Authentifizierung:

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port> -u
<proxy_username> -w <proxy_password>
```

AWS-Schlüssel

Dies sind die Tasten für den Benutzer, die Sie vorbereitet haben sollten Befolgen Sie diese Schritte. Die AWS Schlüssel werden im Daten-Broker gespeichert, der in Ihrem lokalen oder Cloud-Netzwerk ausgeführt wird. NetApp verwendet die Schlüssel nicht außerhalb des Datenmaklers.

JSON-Datei

Dies ist die JSON-Datei, die einen Service-Account-Schlüssel enthält, den Sie vorbereitet haben sollten Befolgen Sie diese Schritte.

6. Sobald der Datenvermittler verfügbar ist, klicken Sie in Cloud Sync auf **Weiter**.
7. Füllen Sie die Seiten im Assistenten aus, um die neue Synchronisierungsbeziehung zu erstellen.

Erstellen einer Synchronisierungsbeziehung

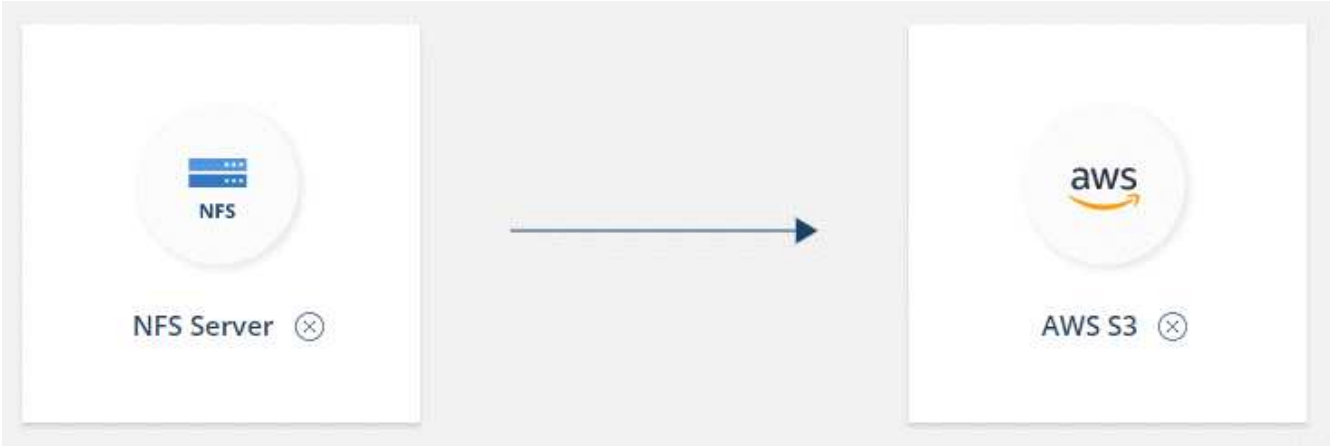
Wenn Sie eine Synchronisierungsbeziehung erstellen, kopiert der Cloud Sync-Dienst Dateien von der Quelle zum Ziel. Nach der ersten Kopie synchronisiert der Service alle 24 Stunden alle geänderten Daten.

Die folgenden Schritte zeigen ein Beispiel, wie eine Synchronisierungsbeziehung von einem NFS-Server zu einem S3-Bucket eingerichtet wird.

Schritte

1. Klicken Sie in Cloud Manager auf **Sync**.
2. Wählen Sie auf der Seite * Synchronisierungsbeziehung definieren* eine Quelle und ein Ziel aus.

Die folgenden Schritte zeigen ein Beispiel für das Erstellen einer Synchronisierungsbeziehung von einem NFS-Server zu einem S3-Bucket.

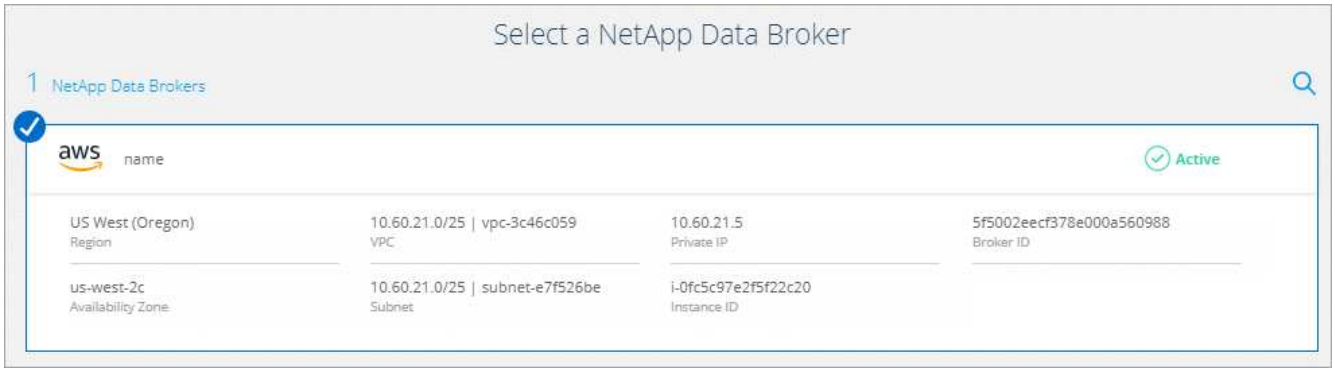


3. Geben Sie auf der Seite **NFS Server** die IP-Adresse oder den vollqualifizierten Domänennamen des NFS-Servers ein, den Sie mit AWS synchronisieren möchten.
4. Folgen Sie auf der Seite **Data Broker** den Aufforderungen zur Erstellung einer virtuellen Maschine für den Datenvermittler in AWS, Azure oder Google Cloud Platform oder zur Installation der Datenvermittler-Software auf einem vorhandenen Linux-Host.

   Weitere Informationen finden Sie auf den folgenden Seiten:

   - "Installation des Data Brokers in AWS"
   - "Installieren des Data Brokers in Azure"
   - "Installation des Data Brokers im GCP"
   - "Installation des Data Brokers auf einem Linux-Host"
5. Klicken Sie nach der Installation des Datenmaklers auf **Weiter**.

   Das folgende Bild zeigt einen erfolgreich implementierten Data Broker in AWS:

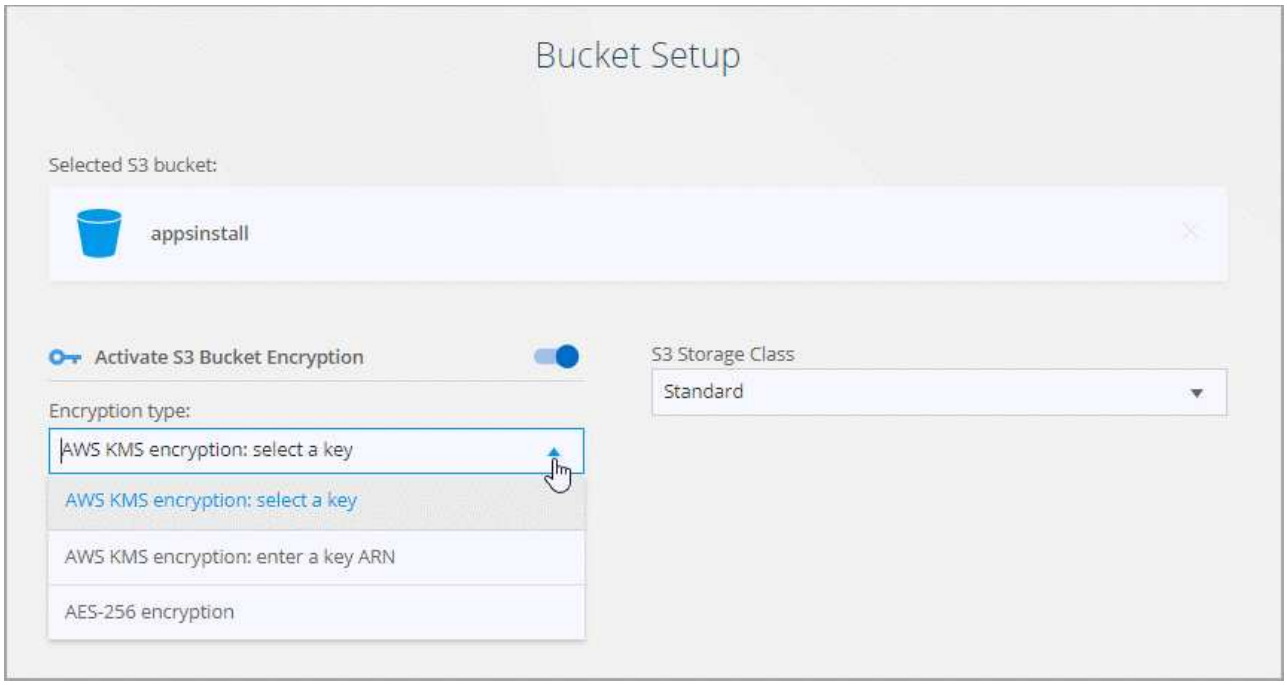


6. Wählen Sie auf der Seite **Directories** ein Verzeichnis oder Unterverzeichnis auf oberster Ebene aus.

   Wenn Cloud Sync die Exporte nicht abrufen kann, klicken Sie auf **Export manuell hinzufügen** und geben Sie den Namen eines NFS-Exports ein.

   Wenn Sie mehr als ein Verzeichnis auf dem NFS-Server synchronisieren möchten, müssen Sie nach Abschluss der Synchronisierung weitere Synchronisierungsbeziehungen erstellen.

7. Wählen Sie auf der Seite **AWS S3 Bucket** einen Bucket aus:
   - Drill-down zum Auswählen eines vorhandenen Ordners innerhalb des Buckets oder zum Auswählen eines neuen Ordners, den Sie innerhalb des Buckets erstellen.
   - Klicken Sie auf **zur Liste hinzufügen**, um einen S3-Bucket auszuwählen, der nicht mit Ihrem AWS-Konto verknüpft ist. "Spezifische Berechtigungen müssen auf den S3-Bucket angewendet werden".
8. Richten Sie auf der Seite **Bucket Setup** den Bucket ein:
   - Legen Sie fest, ob die S3-Bucket-Verschlüsselung aktiviert und dann einen AWS KMS-Schlüssel ausgewählt werden soll, den ARN eines KMS-Schlüssels eingeben oder die AES-256-Verschlüsselung auswählen soll.
   - Wählen Sie eine S3-Storage-Klasse aus. "Zeigen Sie die unterstützten Speicherklassen an".



9. Legen Sie auf der Seite **Einstellungen** fest, wie Quelldateien und Ordner am Zielspeicherort synchronisiert und verwaltet werden:

Zeitplan

Wählen Sie einen wiederkehrenden Zeitplan für zukünftige Synchronisierungen aus oder deaktivieren Sie den Synchronisationsplan. Sie können eine Beziehung planen, um Daten bis zu alle 1 Minute zu synchronisieren.

Wiederholungen

Legen Sie fest, wie oft Cloud Sync versuchen soll, eine Datei zu synchronisieren, bevor Sie sie überspringen.

Kürzlich geänderte Dateien

Wählen Sie diese Option aus, um Dateien auszuschließen, die vor der geplanten Synchronisierung zuletzt geändert wurden.

Dateien auf Quelle löschen

Wählen Sie diese Option aus, um Dateien vom Quellspeicherort zu löschen, nachdem Cloud Sync die Dateien auf den Zielspeicherort kopiert hat. Diese Option schließt das Risiko eines Datenverlusts ein, da die Quelldateien nach dem Kopieren gelöscht werden.

Wenn Sie diese Option aktivieren, müssen Sie auch einen Parameter in der Datei local.json im Datenvermittler ändern. Öffnen Sie die Datei und ändern Sie den Parameter *workers.transferrer.delete-on-source* in **true**.

Dateien auf Ziel löschen

Wählen Sie diese Option aus, um Dateien vom Zielspeicherort zu löschen, wenn sie aus der Quelle gelöscht wurden. Standardmäßig werden Dateien nie vom Zielspeicherort gelöscht.

Objekt-Tagging

Wenn AWS S3 das Ziel in einer Synchronisierungsbeziehung ist, markiert Cloud Sync S3-Objekte mit für den Synchronisierungsvorgang relevanten Metadaten. Sie können das Tagging von S3-Objekten deaktivieren, wenn es in Ihrer Umgebung nicht gewünscht ist. Cloud Sync hat keine Auswirkungen, wenn Sie Tagging deaktivieren – Cloud Sync speichert einfach die Sync-Metadaten auf andere Weise.

Dateitypen

Definieren Sie die Dateitypen, die in jede Synchronisierung einbezogen werden sollen: Dateien, Verzeichnisse und symbolische Links.

Dateierweiterungen ausschließen

Geben Sie Dateierweiterungen an, die vom Sync ausgeschlossen werden sollen, indem Sie die Dateierweiterung eingeben und **Enter** drücken. Geben Sie beispielsweise *log* oder *.log* ein, um *.log-Dateien auszuschließen. Für mehrere Erweiterungen ist kein Trennzeichen erforderlich. Das folgende Video enthält eine kurze Demo:

► https://docs.netapp.com/de-de/occm38//media/video_file_extensions.mp4 *(video)*

Dateigröße

Wählen Sie, ob alle Dateien unabhängig von ihrer Größe oder nur Dateien in einem bestimmten Größenbereich synchronisiert werden sollen.

Änderungsdatum

Wählen Sie alle Dateien unabhängig vom letzten Änderungsdatum aus, Dateien, die nach einem bestimmten Datum, vor einem bestimmten Datum oder zwischen einem bestimmten Zeitraum geändert wurden.

10. Geben Sie auf der Seite **Relationship Tags** bis zu 9 Beziehungs-Tags ein und klicken Sie dann auf **Weiter**.

    Der Cloud Sync-Dienst weist die Tags jedem Objekt zu, das er mit dem S3-Bucket synchronisiert.

11. Überprüfen Sie die Details der Synchronisierungsbeziehung und klicken Sie dann auf **Beziehung erstellen**.

Ergebnis

Cloud Sync beginnt mit der Synchronisierung von Daten zwischen Quelle und Ziel.

Bezahlen für Synchronisierungsbeziehungen, sobald die kostenlose Testversion endet

Es gibt zwei Möglichkeiten, für Synchronisierungsbeziehungen zu bezahlen, nachdem die 14-tägige kostenlose Testversion abgelaufen ist. Die erste Option besteht darin, AWS oder Azure zu abonnieren, um nutzungsbasiert zu bezahlen oder jährlich zu zahlen. Die zweite Option besteht darin, Lizenzen direkt von

NetApp zu erwerben.

Sie können Lizenzen von NetApp mit einem AWS- oder Azure-Abonnement verwenden. Wenn Sie beispielsweise 25 Synchronisierungsbeziehungen haben, können Sie die ersten 20 Synchronisierungsbeziehungen mit einer Lizenz bezahlen und dann mit den restlichen 5 Synchronisierungsbeziehungen von AWS oder Azure bezahlen.

"Erfahren Sie mehr über die Funktionsweise von Lizenzen".

Was ist, wenn ich nicht und#8217;t sofort zahlen, nachdem meine kostenlose Testversion endet?

Sie werden keine weiteren Beziehungen erstellen können. Bestehende Beziehungen werden nicht gelöscht, Sie können jedoch erst dann Änderungen an ihnen vornehmen, wenn Sie eine Lizenz abonnieren oder eingeben.

abonnieren von AWS

AWS ermöglicht Ihnen, nutzungsbasiert zu zahlen oder jährlich zu zahlen.

Schritte zum nutzungsbasierten Bezahlen

1. Klicken Sie Auf **Sync > Licensing**.
2. Wählen Sie **AWS** aus
3. Klicken Sie auf **Abonnieren** und dann auf **Weiter**.
4. Melden Sie sich über den AWS Marketplace an, und melden Sie sich dann wieder beim Cloud Sync Service an, um die Registrierung abzuschließen.

   Das folgende Video zeigt den Prozess:

   ► https://docs.netapp.com/de-de/occm38//media/video_cloud_sync_registering.mp4 *(video)*

Jährliche Zahlung

1. "Rufen Sie die AWS Marketplace Seite auf".
2. Klicken Sie auf **Weiter zur Anmeldung**.
3. Wählen Sie Ihre Vertragsoptionen aus und klicken Sie auf **Vertrag erstellen**.

abonnieren von Azure

Azure ermöglicht Ihnen, nutzungsbasiert zu zahlen oder jährlich zu zahlen.

Was Sie benötigen

Ein Azure Benutzerkonto, das Mitarbeiter- oder Eigentümerberechtigungen für das entsprechende Abonnement besitzt.

Schritte

1. Klicken Sie Auf **Sync > Licensing**.
2. Wählen Sie **Azure**.
3. Klicken Sie auf **Abonnieren** und dann auf **Weiter**.

4. Klicken Sie im Azure-Portal auf **Erstellen**, wählen Sie Ihre Optionen aus und klicken Sie auf **Abonnieren**.

   Wählen Sie * monatlich*, um auf Stundenbasis zu bezahlen, oder **jährlich**, um für ein Jahr im Voraus zu bezahlen.

5. Wenn die Bereitstellung abgeschlossen ist, klicken Sie im Benachrichtigungs-Popup auf den Namen der SaaS-Ressource.
6. Klicken Sie auf **Konto konfigurieren**, um zu Cloud Sync zurückzukehren.

   Das folgende Video zeigt den Prozess:

   ► https://docs.netapp.com/de-de/occm38//media/video_cloud_sync_registering_azure.mp4 *(video)*

Lizenzen von NetApp erwerben und zu Cloud Sync hinzufügen

Um Ihre Synchronisierungsbeziehungen vorab zu bezahlen, müssen Sie eine oder mehrere Lizenzen erwerben und sie dem Cloud Sync Service hinzufügen.

Schritte

1. Erwerben Sie eine Lizenz per Kontakt mit NetApp.
2. Klicken Sie in Cloud Manager auf **Sync > Licensing**.
3. Klicken Sie auf **Lizenz hinzufügen** und fügen Sie die Lizenz hinzu.

Lernprogramme

Kopieren von ACLs zwischen SMB-Freigaben

Cloud Sync kann Zugriffssteuerungslisten (ACLs) zwischen einer SMB-Quell-Freigabe und einer SMB-Zielfreigabe kopieren. Bei Bedarf können Sie die ACLs manuell mithilfe von robocopy beibehalten.

Wahlmöglichkeiten

- um ACLs zwischen SMB-Servern zu kopieren,Richten Sie Cloud Sync so ein, dass ACLs automatisch kopiert werden
- Kopieren Sie die ACLs manuell

Cloud Sync einrichten, um ACLs zwischen SMB-Servern zu kopieren

Kopieren Sie ACLs zwischen SMB-Servern, indem Sie eine Einstellung aktivieren, wenn Sie eine Beziehung erstellen oder nachdem Sie eine Beziehung erstellt haben.

Beachten Sie, dass diese Funktion für neue Synchronisierungsbeziehungen verfügbar ist, die nach der Version vom 23. Februar 2020 erstellt wurden. Wenn Sie möchten, um dieses Feature mit bestehenden Beziehungen vor diesem Datum erstellt verwenden, dann müssen Sie die Beziehung neu erstellen.

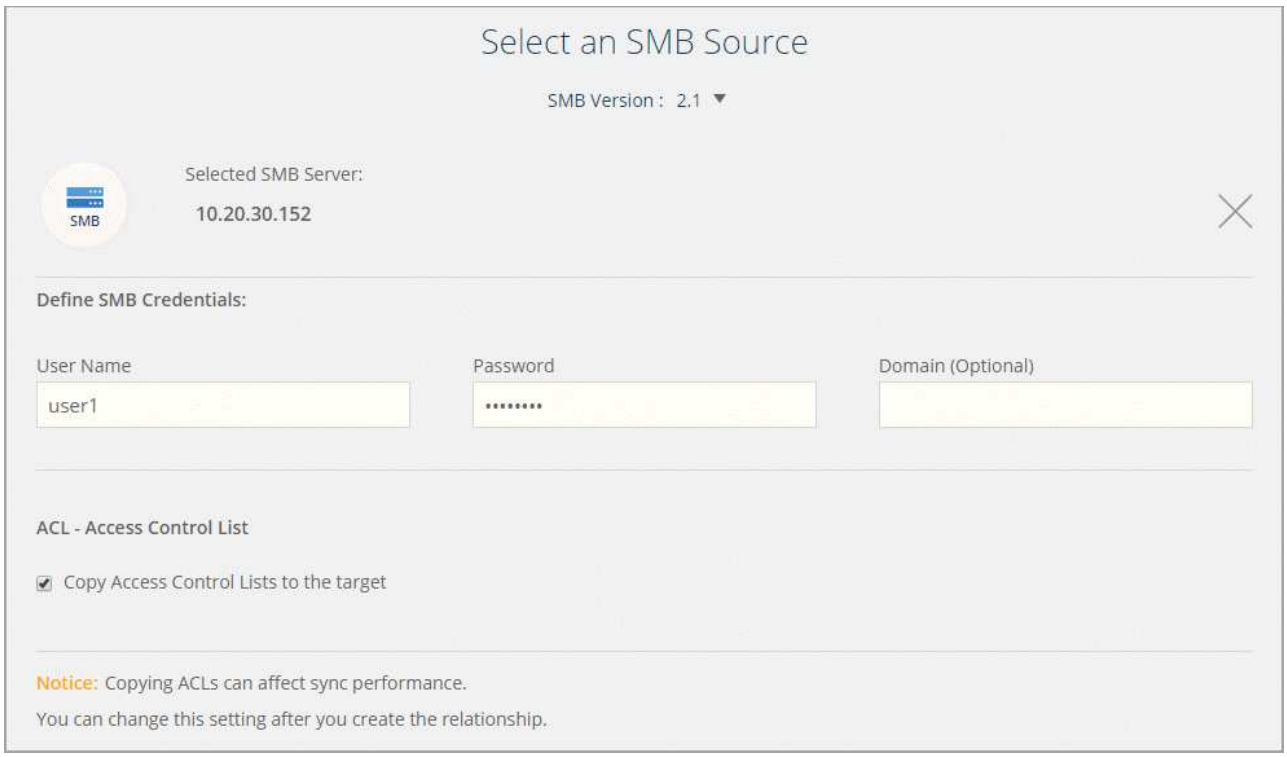
Was Sie benötigen

- Eine neue Sync-Beziehung oder eine bestehende Sync-Beziehung, die nach dem Release des 23. Februar 2020 erstellt wurde.
- Jeder Typ von Daten-Broker.

Diese Funktion arbeitet mit jedem Datentyp Broker zusammen – AWS, Azure, Google Cloud Platform oder On-Premises-Daten-Broker. Der On-Premises-Daten-Broker kann ausgeführt werden "Alle unterstützten Betriebssysteme".

Schritte für eine neue Beziehung

1. Klicken Sie in Cloud Sync auf **Neuen Sync erstellen**.
2. Ziehen Sie **SMB Server** an die Quelle und das Ziel und klicken Sie auf **Weiter**.
3. Auf der Seite **SMB Server**:
   a. Geben Sie einen neuen SMB-Server ein oder wählen Sie einen vorhandenen Server aus und klicken Sie auf **Weiter**.
   b. Geben Sie die Anmeldedaten für den SMB-Server ein.
   c. Wählen Sie **Zugriffssteuerungslisten zum Ziel kopieren** und klicken Sie auf **Weiter**.



4. Befolgen Sie die übrigen Anweisungen, um die Synchronisierungsbeziehung zu erstellen.

Schritte für eine bestehende Beziehung

1. Zeigen Sie mit der Maus auf die Synchronisierungsbeziehung, und klicken Sie auf das Aktionsmenü.
2. Klicken Sie Auf **Einstellungen**.
3. Wählen Sie **Zugriffssteuerungslisten zum Ziel kopieren** aus.
4. Klicken Sie Auf **Einstellungen Speichern**.

Ergebnis

Beim Synchronisieren von Daten behält Cloud Sync die ACLs zwischen den Quell- und Ziel-SMB-Freigaben vor.

Manuelles Kopieren von ACLs

Sie können ACLs manuell zwischen SMB-Freigaben beibehalten, indem Sie den Befehl Windows robocopy verwenden.

Schritte

1. Identifizieren Sie einen Windows-Host mit vollem Zugriff auf beide SMB-Freigaben.
2. Wenn einer der Endpunkte eine Authentifizierung erfordert, verwenden Sie den Befehl **net use**, um eine Verbindung zu den Endpunkten vom Windows-Host herzustellen.

   Sie müssen diesen Schritt ausführen, bevor Sie Robocopy verwenden.

3. Von Cloud Sync aus: Erstellen Sie eine neue Beziehung zwischen Quell- und Ziel-SMB-Freigaben, oder synchronisieren Sie eine vorhandene Beziehung.
4. Führen Sie nach Abschluss der Datensynchronisierung den folgenden Befehl vom Windows-Host aus aus, um die ACLs und Besitzrechte zu synchronisieren:

   ```
   robocopy /E /COPY:SOU /secfix [source] [target] /w:0 /r:0 /XD ~snapshots
   /UNILOG:”[logfilepath]
   ```

   Es sollten sowohl *Source* als auch *Target* mit dem UNC-Format angegeben werden. Beispiel: \\<Server>\<Freigabe>\<Pfad>

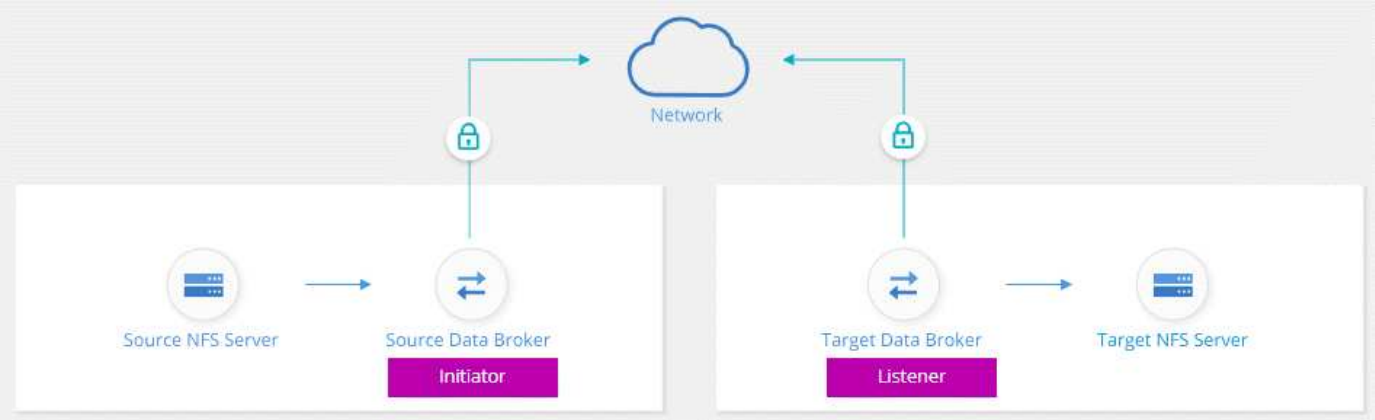
Synchronisierung von NFS-Daten mithilfe von Verschlüsselung bei der Übertragung

Verfügt Ihr Unternehmen über strenge Sicherheitsrichtlinien, können Sie NFS-Daten mithilfe von Verschlüsselung der aktiven Daten synchronisieren. Diese Funktion wird von einem NFS-Server zu einem anderen NFS-Server und von Azure NetApp Files zu Azure NetApp Files unterstützt.

So könnten Sie beispielsweise Daten zwischen zwei NFS Servern synchronisieren, die sich in verschiedenen Netzwerken befinden. Alternativ müssen Daten über Azure NetApp Files sicher über Subnetze und Regionen hinweg übertragen werden.

Funktionsweise der Datenverschlüsselung während des Flugs

Verschlüsselung von übertragenen Daten verschlüsselt NFS-Daten, wenn sie zwischen zwei Datenmaklern über das Netzwerk gesendet werden. Das folgende Bild zeigt eine Beziehung zwischen zwei NFS-Servern und zwei Datenmaklern:



Ein Datenvermittler fungiert als *Initiator*. Wenn es Zeit ist, Daten zu synchronisieren, sendet es eine Verbindungsanforderung an den anderen Daten-Broker, der *Listener* ist. Der Datenmanager wartet auf Anfragen am Port 443. Sie können bei Bedarf einen anderen Port verwenden, überprüfen jedoch, ob der Port nicht von einem anderen Dienst verwendet wird.

Wenn Sie beispielsweise Daten von einem lokalen NFS-Server mit einem Cloud-basierten NFS-Server synchronisieren, können Sie auswählen, welcher Daten-Broker die Verbindungsanforderungen abhört und welche sendet.

Funktionsweise der Verschlüsselung auf der Übertragungsstrecke:

1. Nachdem Sie die Synchronisierungsbeziehung erstellt haben, startet der Initiator eine verschlüsselte Verbindung mit dem anderen Daten-Broker.
2. Der Quell-Datenvermittler verschlüsselt Daten aus der Quelle mithilfe von TLS 1.3.
3. Die Daten werden dann über das Netzwerk an den Ziel-Data-Broker gesendet.
4. Der Zieldatenbroker entschlüsselt die Daten, bevor sie an das Ziel gesendet werden.
5. Nach der ersten Kopie synchronisiert der Service alle 24 Stunden alle geänderten Daten. Wenn Daten zu synchronisieren sind, beginnt der Prozess mit dem Öffnen einer verschlüsselten Verbindung mit dem anderen Daten-Broker durch den Initiator.

   Falls Sie Daten häufiger synchronisieren möchten, "Sie können den Zeitplan nach dem Erstellen der Beziehung ändern".

Unterstützte NFS-Versionen

- Bei NFS-Servern wird die Verschlüsselung der aktiven Daten mit NFS Version 3, 4.0, 4.1 und 4.2 unterstützt.
- Für Azure NetApp Files wird die Verschlüsselung von aktiven Daten mit NFS Version 3 und 4.1 unterstützt.

Was Sie benötigen, um zu beginnen

Stellen Sie sicher, dass Sie über Folgendes verfügen:

- Zwei NFS-Server, die erfüllen "Quell- und Zielanforderungen" Oder Azure NetApp Files in zwei Subnetzen oder Regionen.
- Die IP-Adressen oder vollqualifizierte Domain-Namen der Server.
- Netzwerkstandorte für zwei Datenvermittler.

Sie können einen vorhandenen Daten-Broker auswählen, der jedoch als Initiator fungieren muss. Der Listener-Daten-Broker muss ein *New* Daten-Broker sein.

Wenn Sie noch keinen Data Broker implementiert haben, überprüfen Sie die Anforderungen des Data Brokers. Da Sie über strenge Sicherheitsrichtlinien verfügen, überprüfen Sie unbedingt die Netzwerkanforderungen, einschließlich des ausgehenden Datenverkehrs von Port 443 und dem "internetendpunkte" Dass sich der Daten-Broker mit diesen in Verbindung setzt.

- "Überprüfen Sie die AWS-Installation"
- "Überprüfen Sie die Azure Installation"
- "Überprüfen Sie die GCP-Installation"
- "Überprüfen Sie die Installation des Linux-Hosts"

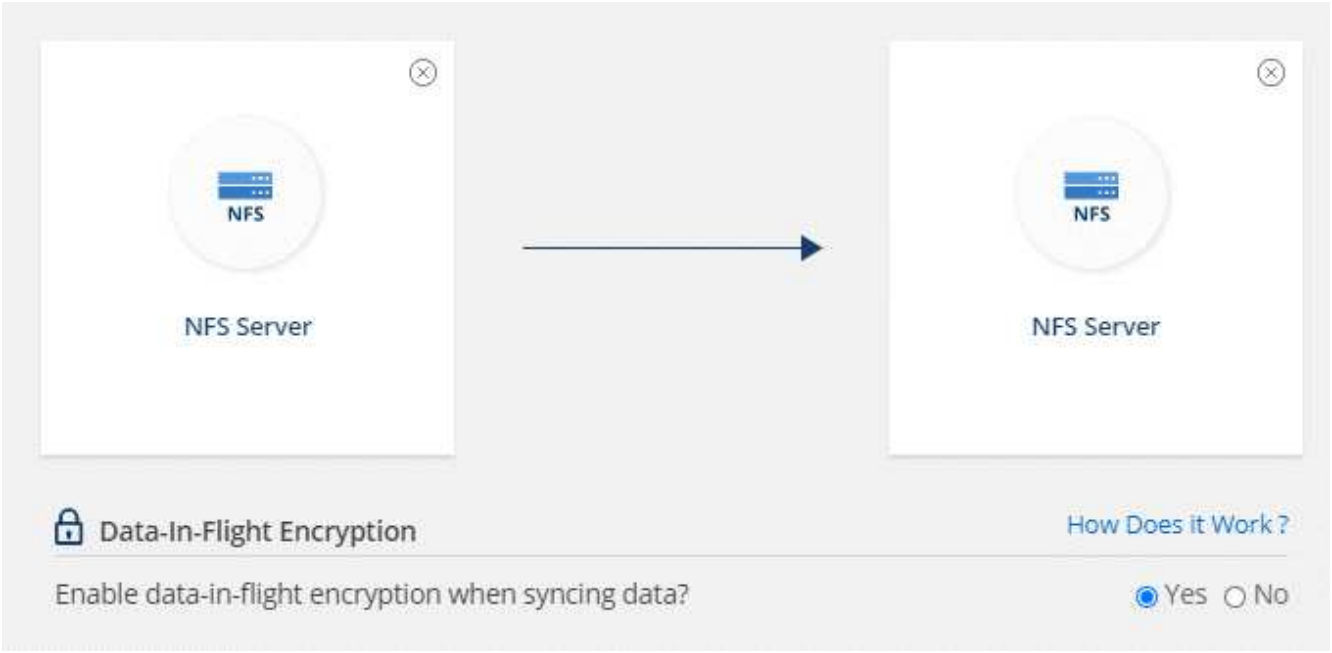
Synchronisierung von NFS-Daten mithilfe von Verschlüsselung bei der Übertragung

Erstellen Sie eine neue Synchronisierungsbeziehung zwischen zwei NFS-Servern oder zwischen Azure NetApp Files, aktivieren Sie die Option für die Verschlüsselung während des Fluges, und befolgen Sie die Anweisungen.

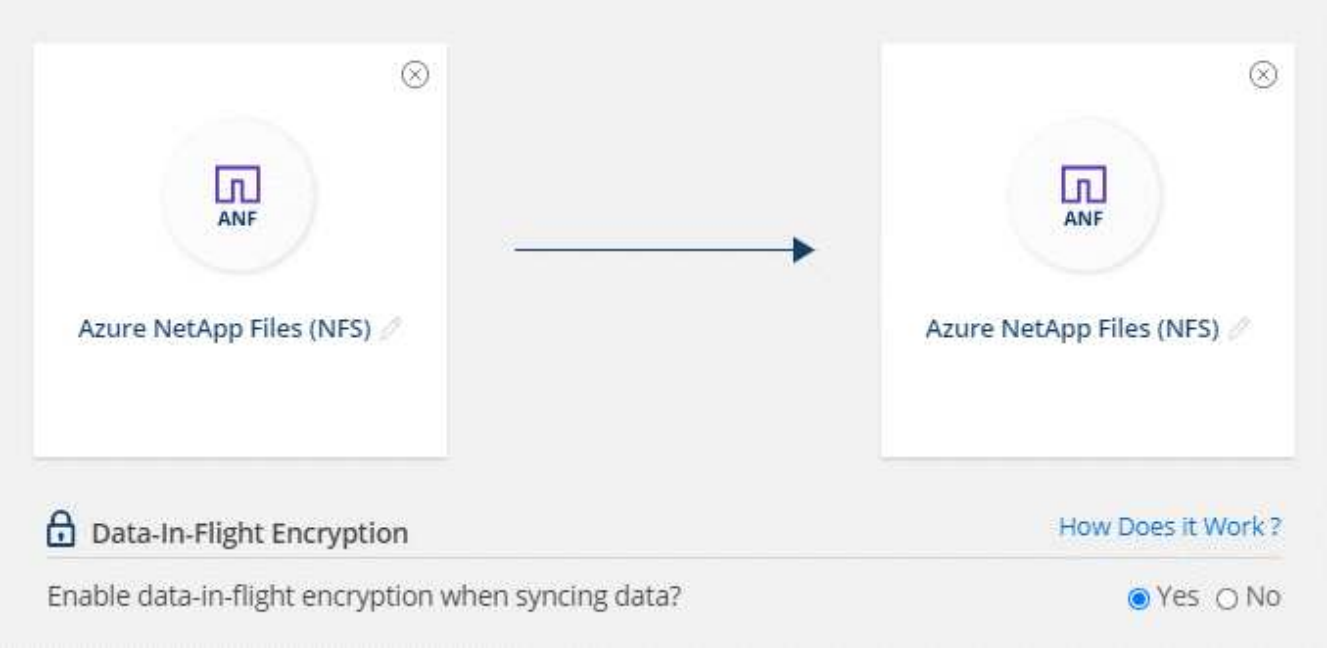
Schritte

1. Klicken Sie Auf **Neuen Sync Erstellen**.
2. Ziehen Sie **NFS-Server** an den Quell- und Zielspeicherort oder **Azure NetApp Files** an den Quell- und Zielstandorten und wählen Sie **Ja** aus, um die Verschlüsselung von Daten während der Übertragung zu aktivieren.

   Das folgende Bild zeigt, was Sie für die Synchronisierung von Daten zwischen zwei NFS-Servern auswählen würden:



   Das folgende Bild zeigt, was Sie für die Synchronisierung von Daten zwischen Azure NetApp Files auswählen würden:



3. Folgen Sie den Anweisungen, um die Beziehung zu erstellen:

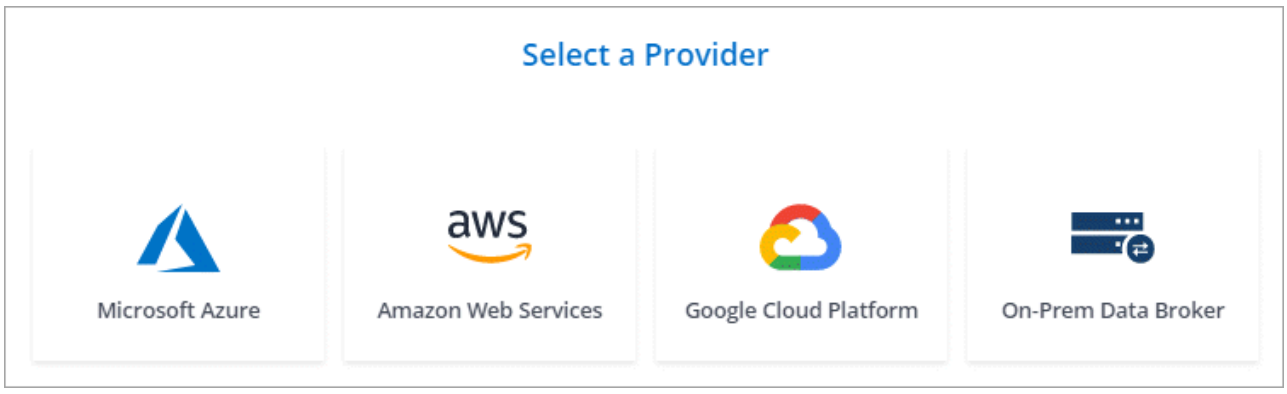
   a. **NFS Server/Azure NetApp Files**: Wählen Sie die NFS-Version und geben Sie dann eine neue NFS-Quelle an oder wählen Sie einen bestehenden Server aus.

   b. **Definieren der Data Broker-Funktionalität**: Legen Sie fest, welcher Datenbroker *hört* nach Verbindungsanfragen an einem Port ab und welcher die Verbindung initiiert. Treffen Sie Ihre Wahl auf der Grundlage Ihrer Netzwerkanforderungen.

   c. **Data Broker**: Folgen Sie den Aufforderungen, um einen neuen Quell-Daten-Broker hinzuzufügen oder einen vorhandenen Datenmakler auszuwählen.

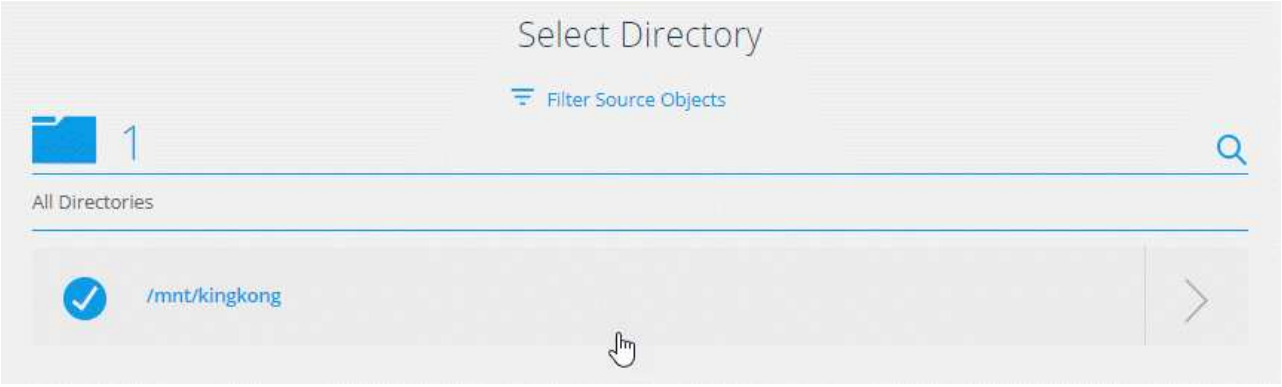
      Wenn der Quelldaten-Broker als Listener fungiert, muss er ein neuer Daten-Broker sein.

      Wenn Sie einen neuen Daten-Broker benötigen, werden Sie von Cloud Sync aufgefordert, die Installationsanweisungen einzugeben. Sie können den Data Broker in der Cloud bereitstellen oder ein Installationsskript für Ihren eigenen Linux-Host herunterladen.

   d. **Directories**: Wählen Sie die Verzeichnisse aus, die Sie synchronisieren möchten, indem Sie alle Verzeichnisse auswählen oder indem Sie nach unten bohren und ein Unterverzeichnis auswählen.

      Klicken Sie auf **Quellobjekte filtern**, um Einstellungen zu ändern, die festlegen, wie Quelldateien und Ordner synchronisiert und am Zielspeicherort verwaltet werden.

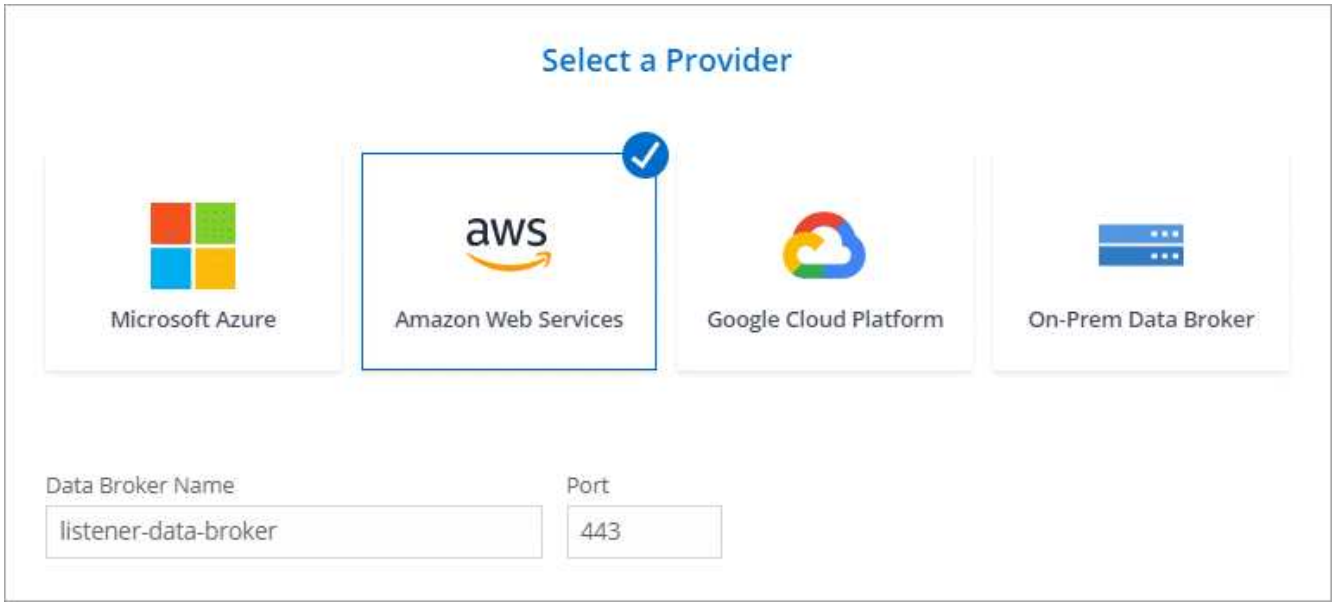


e. **Ziel-NFS-Server/Ziel-Azure NetApp Files**: Wählen Sie die NFS-Version und geben Sie dann ein neues NFS-Ziel ein oder wählen Sie einen vorhandenen Server aus.

f. **Target Data Broker**: Befolgen Sie die Aufforderungen, um einen neuen Quell-Daten-Broker hinzuzufügen oder einen vorhandenen Daten-Broker auszuwählen.

   Wenn der Ziel-Data-Broker als Listener fungiert, muss er ein neuer Daten-Broker sein.

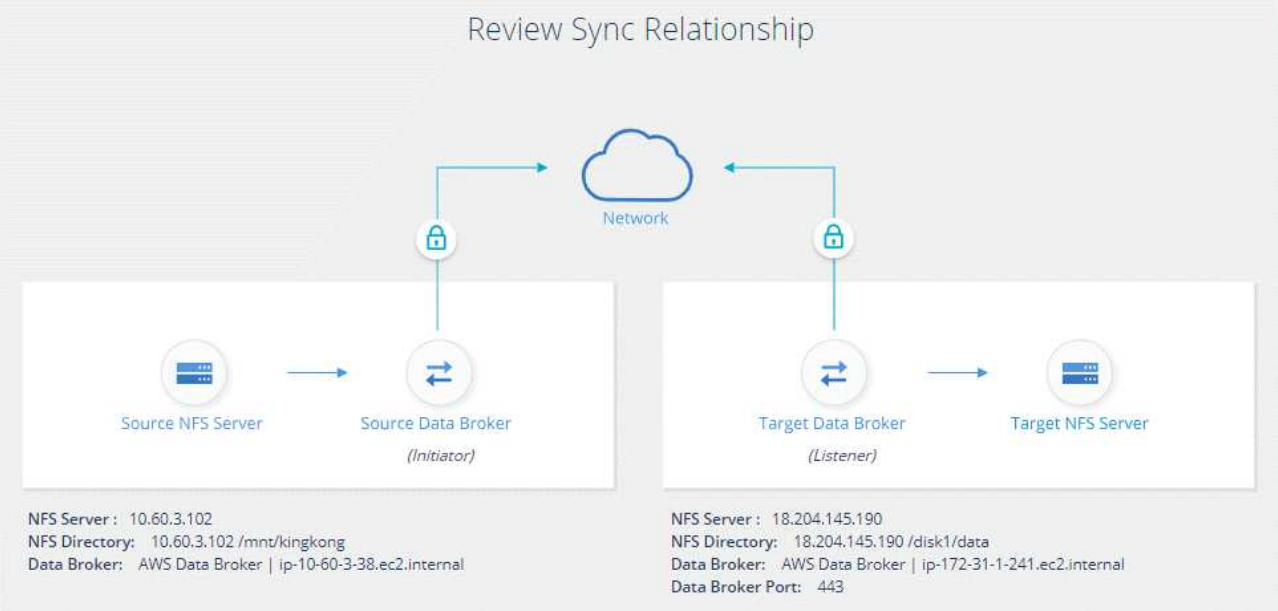
   Dies ist ein Beispiel für die Eingabeaufforderung, wenn der Zieldatenbroker als Listener fungiert. Beachten Sie die Option zur Angabe des Ports.



a. **Zielverzeichnisse**: Wählen Sie ein Verzeichnis der obersten Ebene aus, oder gehen Sie nach unten, um ein vorhandenes Unterverzeichnis auszuwählen oder einen neuen Ordner in einem Export zu erstellen.

b. **Einstellungen**: Legen Sie fest, wie Quelldateien und Ordner im Zielverzeichnis synchronisiert und verwaltet werden.

c. **Review**: Überprüfen Sie die Details der Synchronisierungsbeziehung und klicken Sie dann auf **Beziehung erstellen**.



Ergebnis

Cloud Sync beginnt mit der Erstellung der neuen Synchronisierungsbeziehung. Klicken Sie anschließend auf **Anzeigen in Dashboard**, um Details zur neuen Beziehung anzuzeigen.

Verwalten von Synchronisierungsbeziehungen

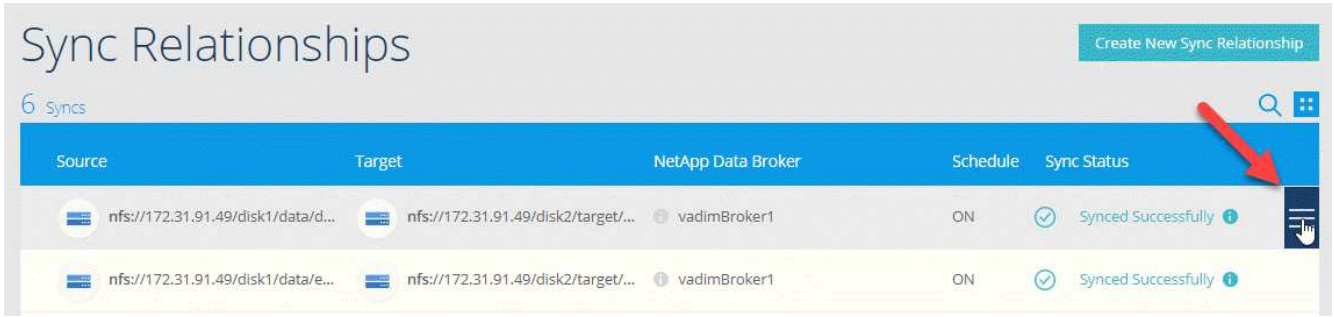
Sie können Synchronisierungsbeziehungen jederzeit verwalten, indem Sie Daten sofort synchronisieren, Zeitpläne ändern und vieles mehr.

Durchführen einer sofortigen Datensynchronisierung

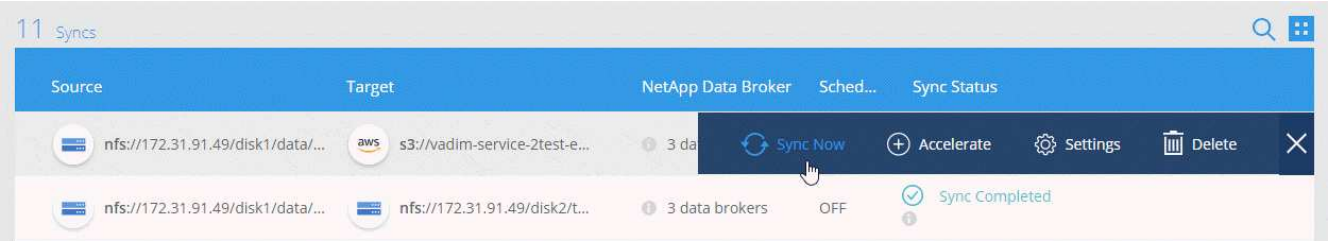
Anstatt auf die nächste geplante Synchronisierung zu warten, können Sie eine Taste drücken, um Daten sofort zwischen Quelle und Ziel zu synchronisieren.

Schritte

1. Bewegen Sie im **Sync Dashboard** den Mauszeiger über die Synchronisierungsbeziehung und klicken Sie auf das Aktivitätsmenü.



2. Klicken Sie auf **Jetzt synchronisieren** und dann auf **Sync**, um zu bestätigen.



Ergebnis

Cloud Sync startet den Datensynchronisierungsprozess für die Beziehung.

Beschleunigung der Sync-Performance

Beschleunigen Sie die Performance einer Synchronisierungsbeziehung, indem Sie der Beziehung einen zusätzlichen Daten-Broker hinzufügen. Der zusätzliche Daten-Broker muss ein *neuer* Daten-Broker sein.

So funktioniert das

Wenn die vorhandenen Datenvermittler in der Beziehung in anderen Synchronisierungsbeziehungen verwendet werden, fügt Cloud Sync diesen Beziehungen automatisch auch den neuen Datenvermittler hinzu.

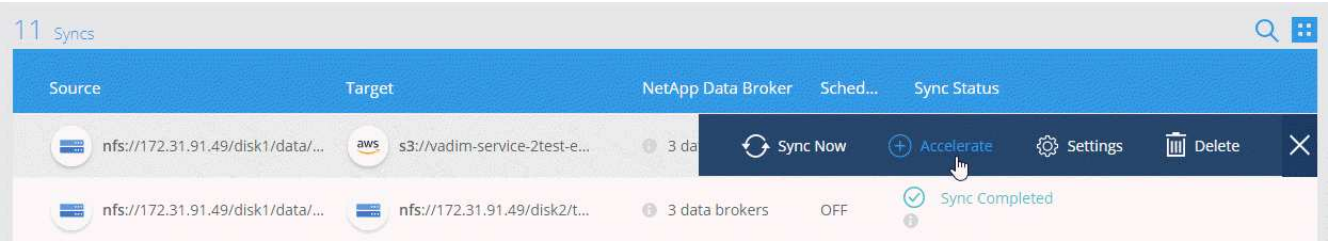
Nehmen wir zum Beispiel an, Sie haben drei Beziehungen:

- Beziehung 1 verwendet Datenbroker A
- Beziehung 2 verwendet Datenbroker B.
- Beziehung 3 verwendet Datenbroker A

Sie möchten die Performance von Beziehung 1 beschleunigen, sodass Sie dieser Beziehung einen neuen Daten-Broker hinzufügen (Daten-Broker C). Da Data Broker A auch in Beziehung 3 verwendet wird, wird der neue Data Broker automatisch auch zu Beziehung 3 hinzugefügt.

Schritte

1. Stellen Sie sicher, dass mindestens einer der vorhandenen Datenvermittler in der Beziehung online ist.
2. Zeigen Sie mit der Maus auf die Synchronisierungsbeziehung, und klicken Sie auf das Aktionsmenü.
3. Klicken Sie Auf **Beschleunigen**.



4. Folgen Sie den Anweisungen, um einen neuen Daten-Broker zu erstellen.

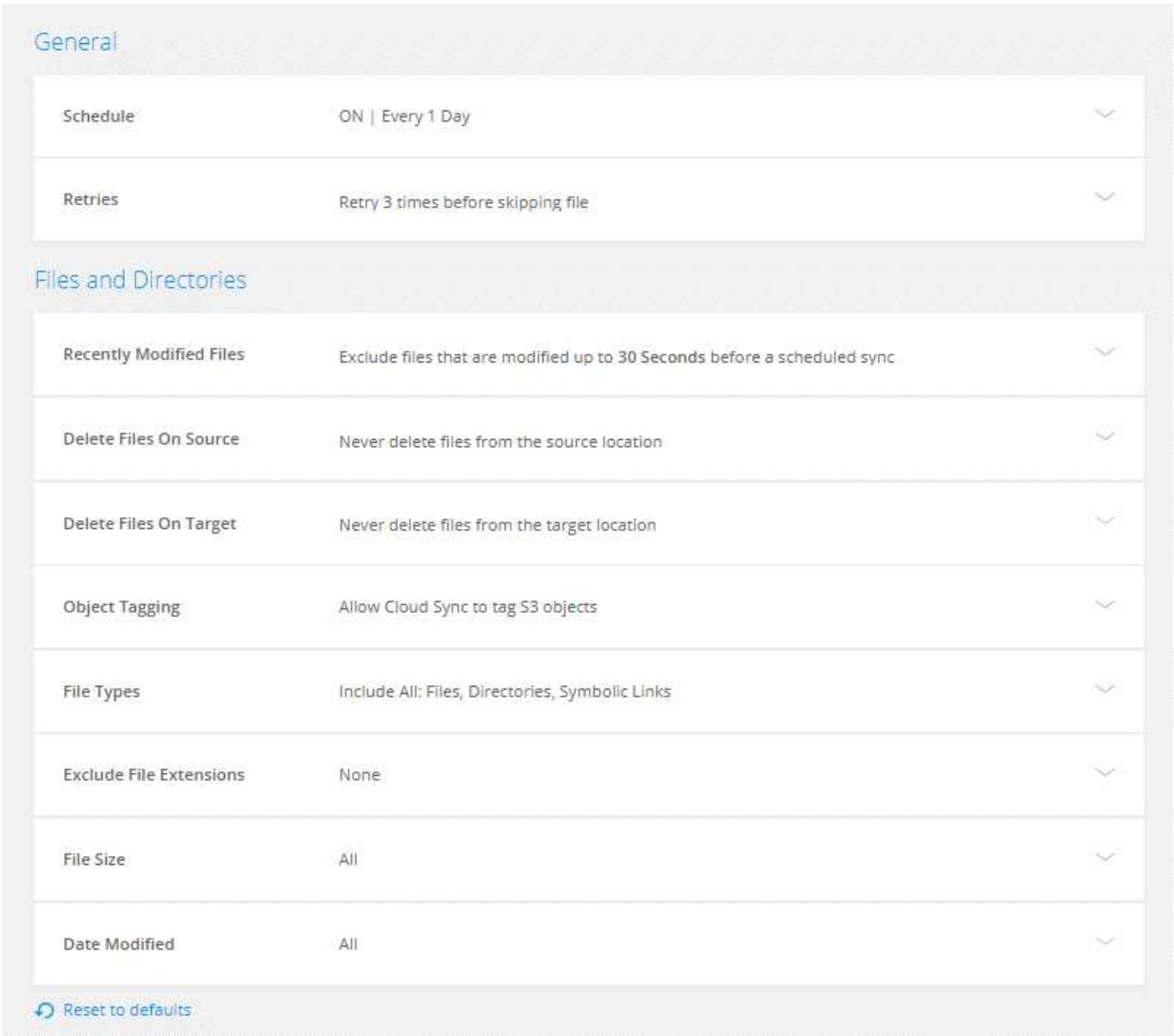
Ergebnis

Cloud Sync fügt den neuen Daten-Broker zu den Synchronisierungsbeziehungen hinzu. Die Performance der nächsten Datensynchronisierung sollte beschleunigt werden.

Ändern der Einstellungen für eine Synchronisierungsbeziehung

Ändern Sie Einstellungen, mit denen festgelegt wird, wie Quelldateien und Ordner synchronisiert und am Zielspeicherort verwaltet werden.

1. Zeigen Sie mit der Maus auf die Synchronisierungsbeziehung, und klicken Sie auf das Aktionsmenü.
2. Klicken Sie Auf **Einstellungen**.
3. Ändern Sie alle Einstellungen.



[[deleteonsource] Hier eine kurze Beschreibung der einzelnen Einstellungen:

Zeitplan

Wählen Sie einen wiederkehrenden Zeitplan für zukünftige Synchronisierungen aus oder deaktivieren Sie den Synchronisationsplan. Sie können eine Beziehung planen, um Daten bis zu alle 1 Minute zu synchronisieren.

Wiederholungen

Legen Sie fest, wie oft Cloud Sync versuchen soll, eine Datei zu synchronisieren, bevor Sie sie überspringen.

Kürzlich geänderte Dateien

Wählen Sie diese Option aus, um Dateien auszuschließen, die vor der geplanten Synchronisierung zuletzt geändert wurden.

Dateien auf Quelle löschen

Wählen Sie diese Option aus, um Dateien vom Quellspeicherort zu löschen, nachdem Cloud Sync die Dateien auf den Zielspeicherort kopiert hat. Diese Option schließt das Risiko eines Datenverlusts ein, da die Quelldateien nach dem Kopieren gelöscht werden.

Wenn Sie diese Option aktivieren, müssen Sie auch einen Parameter in der Datei local.json im Datenvermittler ändern. Öffnen Sie die Datei und ändern Sie den Parameter *workers.transferrer.delete-on-source* in **true**.

Dateien auf Ziel löschen

Wählen Sie diese Option aus, um Dateien vom Zielspeicherort zu löschen, wenn sie aus der Quelle gelöscht wurden. Standardmäßig werden Dateien nie vom Zielspeicherort gelöscht.

Objekt-Tagging

Wenn AWS S3 das Ziel in einer Synchronisierungsbeziehung ist, markiert Cloud Sync S3-Objekte mit für den Synchronisierungsvorgang relevanten Metadaten. Sie können das Tagging von S3-Objekten deaktivieren, wenn es in Ihrer Umgebung nicht gewünscht ist. Cloud Sync hat keine Auswirkungen, wenn Sie Tagging deaktivieren – Cloud Sync speichert einfach die Sync-Metadaten auf andere Weise.

Dateitypen

Definieren Sie die Dateitypen, die in jede Synchronisierung einbezogen werden sollen: Dateien, Verzeichnisse und symbolische Links.

Dateierweiterungen ausschließen

Geben Sie Dateierweiterungen an, die vom Sync ausgeschlossen werden sollen, indem Sie die Dateierweiterung eingeben und **Enter** drücken. Geben Sie beispielsweise *log* oder *.log* ein, um *.log-Dateien auszuschließen. Für mehrere Erweiterungen ist kein Trennzeichen erforderlich. Das folgende Video enthält eine kurze Demo:

► https://docs.netapp.com/de-de/occm38//media/video_file_extensions.mp4 *(video)*

Dateigröße

Wählen Sie, ob alle Dateien unabhängig von ihrer Größe oder nur Dateien in einem bestimmten Größenbereich synchronisiert werden sollen.

Änderungsdatum

Wählen Sie alle Dateien unabhängig vom letzten Änderungsdatum aus, Dateien, die nach einem bestimmten Datum, vor einem bestimmten Datum oder zwischen einem bestimmten Zeitraum geändert wurden.

Zugriffskontrolllisten auf das Ziel kopieren

Sie können Zugriffssteuerungslisten (ACLs) zwischen SMB-Quell-Freigaben und SMB-Ziel-Freigaben kopieren. Beachten Sie, dass diese Option nur für Synchronisierungsbeziehungen verfügbar ist, die nach der Version vom 23. Februar 2020 erstellt wurden.

4. Klicken Sie Auf **Einstellungen Speichern**.

Ergebnis

Cloud Sync ändert die Synchronisierungsbeziehung mit den neuen Einstellungen.

Löschen von Beziehungen

Sie können eine Synchronisierungsbeziehung löschen, wenn Sie keine Daten mehr zwischen Quelle und Ziel synchronisieren müssen. Diese Aktion löscht die Data Brokerinstanz nicht und löscht keine Daten vom Ziel.

Schritte

1. Zeigen Sie mit der Maus auf die Synchronisierungsbeziehung, und klicken Sie auf das Aktionsmenü.
2. Klicken Sie auf **Löschen** und dann erneut auf **Löschen**, um zu bestätigen.

Ergebnis

Cloud Sync löscht die Synchronisierungsbeziehung.

Cloud Sync-APIs

Die Cloud Sync-Funktionen, die über die Webbenutzeroberfläche verfügbar sind, sind auch über RESTful APIs verfügbar.

Erste Schritte

Für den Einstieg in die Cloud Sync APIs müssen Sie ein Benutzer-Token und Ihre Cloud Central Account-ID erhalten. Bei API-Aufrufen müssen Sie das Token und die Konto-ID der Autorisierungs-Kopfzeile hinzufügen.

Schritte

1. Holen Sie sich ein Benutzer-Token von NetApp Cloud Central.

```
POST https://netapp-cloud-account.auth0.com/oauth/token
Header: Content-Type: application/json
Body:
{
                "username": "<user_email>",
                "scope": "profile",
                "audience": "https://api.cloud.netapp.com",
                "client_id": "UaVhOIXMWQs5i1WdDxauXe5Mqkb34NJQ",
                "grant_type": "password",
                "password": "<user_password>"
}
```

2. Beschaffen der ID Ihres Cloud Central-Kontos

```
GET https://cloudsync.netapp.com/api/accounts
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
```

Diese API gibt eine Antwort wie die folgende zurück:

```
[
  {
    "accountId": "account-JeL97Ry3",
    "name": "Test"
  }
]
```

3. Fügen Sie bei jedem API-Aufruf das Benutzer-Token und die Konto-ID in die Autorisierungskopfzeile ein.

   Beispiel

   Das folgende Beispiel zeigt einen API-Aufruf zum Erstellen eines Data Brokers in Microsoft Azure. Sie ersetzen einfach <user_Token> und <AccountID> durch das Token und die ID, die Sie in den vorherigen Schritten erhalten haben.

```
POST https://cloudsync.netapp.com/api/data-brokers
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
Body: { "name": "databroker1", "type": "AZURE" }
```

Was kann ich tun, wenn das Token abläuft?

Das Benutzer-Token von NetApp Cloud Central hat ein Ablaufdatum. Um das Token zu aktualisieren, müssen Sie die API von Schritt 1 erneut aufrufen.

Die API-Antwort enthält ein Feld "expires_in", das angibt, wann das Token abläuft.

API-Referenz

Die Dokumentation für jede Cloud Sync-API finden Sie unter "NetApp Cloud Central".

Verwenden von Listen-APIs

Liste-APIs sind asynchrone APIs, sodass das Ergebnis nicht sofort zurückgegeben wird (z. B.: `GET /data-brokers/{id}/list-nfs-export-folders` Und `GET /data-brokers/{id}/list-s3-buckets`). Die einzige Antwort des Servers lautet HTTP-Status 202. Um das tatsächliche Ergebnis zu erhalten, müssen Sie den verwenden `GET /messages/client` API:

Schritte

1. Rufen Sie die Liste-API auf, die Sie verwenden möchten.
2. Verwenden Sie die `GET /messages/client` API zum Anzeigen des Ergebnisses des Vorgangs.
3. Verwenden Sie dieselbe API, indem Sie sie mit der ID anhängen, die Sie gerade erhalten haben: `GET http://cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>`

   Beachten Sie, dass sich die ID jedes Mal ändert, wenn Sie das anrufen `GET /messages/client` API:

Beispiel

Wenn Sie den anrufen `list-s3-buckets` API, ein Ergebnis wird nicht sofort zurückgegeben:

```
GET http://cloudsync.netapp.com/api/data-brokers/<data-broker-id>/list-s3-buckets
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

Das Ergebnis ist der HTTP-Statuscode 202, d. H. Die Nachricht wurde akzeptiert, aber noch nicht verarbeitet.

Um das Ergebnis des Vorgangs zu erhalten, müssen Sie die folgende API verwenden:

```
GET http://cloudsync.netapp.com/api/messages/client
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

Das Ergebnis ist ein Array mit einem Objekt, das ein ID-Feld enthält. Das ID-Feld stellt die letzte Nachricht dar, die der Server gesendet hat. Beispiel:

```
[
    {
        "header": {
            "requestId": "init",
            "clientId": "init",
            "agentId": "init"
        },
        "payload": {
            "init": {}
        },
        "id": "5801"
    }
]
```

Sie würden nun den folgenden API-Aufruf mit der ID durchführen, die Sie gerade erhalten haben:

```
GET http://cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

Das Ergebnis ist ein Array von Meldungen. In jeder Nachricht befindet sich ein Nutzlastobjekt, das aus dem Namen der Operation (als Schlüssel) und ihrem Ergebnis (als Wert) besteht. Beispiel:


```
[
    {
        "payload": {
            "list-s3-buckets": [
                {
                    "tags": [
                        {
                            "Value": "100$",
                            "Key": "price"
                        }
                    ],
                    "region": {
                        "displayName": "US West (Oregon)",
                        "name": "us-west-2"
                    },
                    "name": "small"
                }
            ]
        },
        "header": {
            "requestId": "f687ac55-2f0c-40e3-9fa6-57fb8c4094a3",
            "clientId": "5beb032f548e6e35f4ed1ba9",
            "agentId": "5bed61f4489fb04e34a9aac6"
        },
        "id": "5802"
    }
]
```


Cloud Sync – technische FAQ

Diese FAQ kann Ihnen helfen, wenn Sie nur eine schnelle Antwort auf eine Frage suchen.

Erste Schritte

Die folgenden Fragen beziehen sich auf die ersten Schritte mit Cloud Sync.

Wie funktioniert Cloud Sync?

Cloud Sync synchronisiert mithilfe der Datenmanager-Software von NetApp Daten von einer Quelle zu einem Ziel (dies wird als „*Sync Relationship*“ bezeichnet).

Der Daten-Broker steuert die Synchronisierungsbeziehungen zwischen Ihren Quellen und Zielen. Nachdem Sie eine Synchronisierungsbeziehung eingerichtet haben, analysiert Cloud Sync Ihr Quellsystem und unterteilt es in mehrere Replizierungsstreams, um die ausgewählten Zieldaten per Push zu übertragen.

Nach der ersten Kopie synchronisiert der Service alle geänderten Daten auf der Grundlage des von Ihnen festgelegten Zeitplans.

Wie funktioniert die 14-tägige kostenlose Testversion?

Die 14-tägige kostenlose Testversion beginnt, wenn Sie sich für den Cloud Sync Service anmelden. Sie unterliegen keinen NetApp Kosten für Cloud Sync-Beziehungen, die Sie 14 Tage lang erstellen. Alle Ressourcengebühren für jeden Daten-Broker, den Sie bereitstellen, gelten jedoch weiterhin.

Wie viel kostet Cloud Sync?

Bei der Verwendung von Cloud Sync fallen zwei Kostenarten an: Servicegebühren und Ressourcengebühren.

Servicegebühren

Bei nutzungsbasierten Preisen fallen die Servicegebühren für Cloud Sync stündlich an, basierend auf der Anzahl der von Ihnen erstellten Synchronisierungsbeziehungen.

- "Pay-as-you-go-Preise in AWS anzeigen"
- "Jährliche Preise in AWS anzeigen"
- "Preise in Azure anzeigen"

Cloud Sync Lizenzen sind auch über Ihren NetApp Ansprechpartner erhältlich. Jede Lizenz ermöglicht 20 Synchronisierungsbeziehungen für 12 Monate.

"Weitere Informationen zu Lizenzen".

Ressourcengebühren

Die Ressourcenkosten beziehen sich auf die Computing- und Storage-Kosten für die Ausführung des Data Brokers in der Cloud.

Wie wird Cloud Sync abgerechnet?

Es gibt zwei Möglichkeiten, für Synchronisierungsbeziehungen zu bezahlen, nachdem die 14-tägige kostenlose Testversion abgelaufen ist. Die erste Möglichkeit besteht darin, AWS oder Azure zu abonnieren, sodass Sie nutzungsbasiert oder jährlich zahlen können. Die zweite Option besteht darin, Lizenzen direkt von NetApp zu erwerben.

Kann ich Cloud Sync auch außerhalb der Cloud verwenden?

Ja, Sie können Cloud Sync in einer Architektur verwenden, die nicht in der Cloud liegt. Die Quelle und das Ziel können sich vor Ort befinden, so dass der Daten-Broker.

Beachten Sie die folgenden wichtigen Punkte zur Verwendung von Cloud Sync außerhalb der Cloud:

- Für die lokale Synchronisierung ist ein privater Amazon S3-Bucket über NetApp StorageGRID verfügbar.
- Der Daten-Broker benötigt eine Internetverbindung, um mit dem Cloud Sync Service zu kommunizieren.
- Wenn Sie keine Lizenz direkt von NetApp erwerben, benötigen Sie ein AWS oder Azure Konto für die Abrechnung des PAYGO Cloud Sync Service.

Wie greife ich auf Cloud Sync zu?

Cloud Sync ist im Cloud Manager auf der Registerkarte **Sync** verfügbar.

Unterstützte Quellen und Ziele

Die folgenden Fragen beziehen sich auf die Quelle und die Ziele, die in einer Synchronisierungsbeziehung unterstützt werden.

Welche Quellen und Ziele unterstützt Cloud Sync?

Cloud Sync unterstützt viele verschiedene Arten von Synchronisierungsbeziehungen. "Die gesamte Liste anzeigen".

Welche Versionen von NFS und SMB werden von Cloud Sync unterstützt?

Cloud Sync unterstützt NFS Version 3 und höher sowie SMB Version 1 und höher.

"Erfahren Sie mehr über Synchronisierungsanforderungen".

Wenn Amazon S3 das Ziel ist, können die Daten auf eine bestimmte S3-Storage-Klasse gestaffelt werden?

Ja, Sie können eine bestimmte S3-Storage-Klasse auswählen, wenn AWS S3 das Ziel ist:

- Standard (dies ist die Standardklasse)
- Intelligent-Tiering
- Standardzugriff
- Ein einmaliger Zugriff
- Glacier
- Glacier Deep Archive

Was ist mit Storage Tiers für Azure Blob Storage?

Sie können eine bestimmte Azure Blob Storage Tier auswählen, wenn ein Blob Container das Ziel ist:

- Hot-Storage
- Kühl lagern

Netzwerkbetrieb

Die folgenden Fragen beziehen sich auf die Netzwerkanforderungen für Cloud Sync.

Welche Netzwerkanforderungen gelten für Cloud Sync?

Die Cloud Sync-Umgebung erfordert, dass der Daten-Broker über das ausgewählte Protokoll (NFS, SMB, EFS) oder die Objektspeicher-API (Amazon S3, Azure Blob, IBM Cloud Object Storage) mit der Quelle und dem Ziel verbunden ist.

Darüber hinaus benötigt der Daten-Broker eine ausgehende Internetverbindung über Port 443, damit er mit dem Cloud Sync-Dienst kommunizieren und mit einigen anderen Diensten und Repositorys Kontakt aufnehmen kann.

Weitere Informationen "Netzwerkanforderungen prüfen".

Gibt es Netzwerkeinschränkungen im Zusammenhang mit der Konnektivität von Data Brokern?

Datenvermittler benötigen einen Internetzugang. Wir unterstützen keinen Proxy-Server wenn wir den Daten-Broker in Azure oder in Google Cloud Platform bereitstellen.

Datensynchronisierung

Die folgenden Fragen beziehen sich auf die Funktionsweise der Datensynchronisierung.

Wie oft erfolgt die Synchronisierung?

Der Standardzeitplan ist für die tägliche Synchronisierung festgelegt. Nach der ersten Synchronisierung können Sie:

- Ändern Sie den Synchronisierungszeitplan auf die gewünschte Anzahl von Tagen, Stunden oder Minuten
- Deaktivieren Sie den Synchronisierungszeitplan
- Synchronisierungszeitplan löschen (keine Daten verloren; nur die Synchronisierungsbeziehung wird entfernt)

Wie ist der Mindestsynchronisierungszeitplan?

Sie können eine Beziehung planen, um Daten bis zu alle 1 Minute zu synchronisieren.

Versucht der Daten-Broker erneut, wenn eine Datei nicht synchronisiert werden kann? Oder wird das Zeitlimit überschritten?

Der Datenvermittler hat kein Timeout, wenn eine einzelne Datei nicht übertragen werden kann. Stattdessen versucht der Daten-Broker dreimal, bevor die Datei übersprungen wird. Der Wiederholungswert kann in den Einstellungen für eine Synchronisierungsbeziehung konfiguriert werden.

"Hier erfahren Sie, wie Sie die Einstellungen für eine Synchronisierungsbeziehung ändern".

Was ist, wenn ich einen sehr großen Datensatz habe?

Wenn ein einzelnes Verzeichnis 600,000 oder mehr Dateien enthält, kontaktieren Sie uns, damit wir Ihnen helfen können, den Datenvermittler so zu konfigurieren, dass die Nutzlast behandelt wird. Möglicherweise müssen wir dem Data Broker-Computer zusätzlichen Speicher hinzufügen.

Sicherheit

Die folgenden Fragen zur Sicherheit.

Ist Cloud Sync sicher?

Ja. Alle Netzwerkkonnektivität zum Cloud Sync-Service wird mittels ausgeführt "Amazon Simple Queue Service (SQS)".

Die gesamte Kommunikation zwischen dem Daten-Broker und Amazon S3, Azure Blob, Google Cloud Storage und IBM Cloud Object Storage erfolgt über das HTTPS-Protokoll.

Wenn Sie Cloud Sync mit On-Premises-Systemen (Quelle oder Ziel) verwenden, sind hier einige empfohlene Konnektivitätsoptionen:

- Eine AWS Direct Connect-, Azure ExpressRoute- oder Google Cloud Interconnect-Verbindung, die nicht über das Internet geroutet wird (und nur mit den von Ihnen angegebenen Cloud-Netzwerken kommunizieren kann)
- Eine VPN-Verbindung zwischen Ihrem lokalen Gateway-Gerät und Ihren Cloud-Netzwerken
- Für eine besonders sichere Datenübertragung mit S3-Buckets, Azure Blob Storage oder Google Cloud Storage kann ein Amazon Private S3 Endpoint, Azure Virtual Network Service-Endpunkte oder Private Google Access eingerichtet werden.

Jede dieser Methoden stellt eine sichere Verbindung zwischen Ihren lokalen NAS-Servern und einem Cloud Sync Datenbroker her.

Werden Daten mit Cloud Sync verschlüsselt?

- Cloud Sync unterstützt die Verschlüsselung von Daten während des Flugs zwischen Quell- und Ziel-NFS-Servern. "Weitere Informationen .".
- Verschlüsselung wird von SMB nicht unterstützt.
- Wenn ein Amazon S3-Bucket in einer Synchronisierungsbeziehung das Ziel ist, hat der Kunde die Wahl, ob die Datenverschlüsselung mittels AWS KMS-Verschlüsselung oder AES-256-Verschlüsselung aktiviert werden soll.

Berechtigungen

Die folgenden Fragen beziehen sich auf Datenberechtigungen.

Werden SMB-Datenberechtigungen mit dem Zielspeicherort synchronisiert?

Sie können Cloud Sync so einrichten, dass Zugriffssteuerungslisten (ACLs) zwischen einer Quell-SMB-Freigabe und einer Ziel-SMB-Freigabe beibehalten werden. Sie können die ACLs auch manuell kopieren. "Lesen Sie, wie Sie ACLs zwischen SMB-Freigaben kopieren".

Werden NFS-Datenberechtigungen mit dem Zielspeicherort synchronisiert?

Cloud Sync kopiert NFS-Berechtigungen automatisch wie folgt zwischen NFS-Servern:

- NFS Version 3: Cloud Sync kopiert die Berechtigungen und den Besitzer der Benutzergruppe.
- NFS Version 4: Cloud Sync kopiert die ACLs.

Leistung

Die folgenden Fragen beziehen sich auf die Cloud Sync-Performance.

Was stellt die Fortschrittsanzeige für eine Synchronisierungsbeziehung dar?

Die Synchronisierungsbeziehung zeigt den Durchsatz des Netzwerkadapters des Datenbrokers. Wenn Sie die Synchronisierungsleistung durch die Verwendung mehrerer Datenmakler beschleunigen, ist der Durchsatz die Summe des gesamten Datenverkehrs. Dieser Durchsatz wird alle 20 Sekunden aktualisiert.

Ich habe Performance-Probleme. Können wir die Anzahl der gleichzeitigen Übertragungen begrenzen?

Der Daten-Broker kann 4 Dateien gleichzeitig synchronisieren. Wenn Sie über sehr große Dateien verfügen (jeweils mehrere TB), kann es sehr lange dauern, bis der Übertragungsprozess abgeschlossen ist, und die Performance kann beeinträchtigt werden.

Die Begrenzung der Anzahl gleichzeitiger Übertragungen kann hilfreich sein. Mailto:ng-cloudsync-support@netapp.com[Hilfe anfordern].

Warum ist die Performance mit Azure NetApp Files niedrig?

Wenn Sie Daten mit oder von Azure NetApp Files synchronisieren, können Ausfälle und Performance-Probleme auftreten, sobald das Service-Level der Festplatte Standard ist.

Ändern Sie den Service-Level auf Premium oder Ultra, um die Synchronisationsperformance zu verbessern.

"Erfahren Sie mehr über Azure NetApp Files Service-Level und Durchsatz".

Warum erhalte ich mit Cloud Volumes Service für AWS eine geringe Performance?

Wenn Sie Daten mit einem oder von einem Cloud-Volume synchronisieren, treten möglicherweise Fehler und Performance-Probleme auf, wenn die Performance für das Cloud-Volume Standard ist.

Ändern Sie den Service-Level in "Premium" oder "Extreme", um die Synchronisierungsleistung zu erhöhen.

Wie viele Daten-Broker sind erforderlich?

Wenn Sie eine neue Beziehung erstellen, beginnen Sie mit einem einzelnen Daten-Broker (es sei denn, Sie haben einen vorhandenen Daten-Broker ausgewählt, der zu einer beschleunigten Synchronisierungsbeziehung gehört). In vielen Fällen kann ein einzelner Daten-Broker die Performance-Anforderungen für eine Synchronisierungsbeziehung erfüllen. Ist dies nicht der Fall, können Sie die Sync Performance durch das Hinzufügen weiterer Datenmanager beschleunigen. Sie sollten jedoch zunächst andere Faktoren prüfen, die sich auf die Synchronisierungsleistung auswirken können.

Mehrere Faktoren können die Datenübertragungsleistung beeinflussen. Die Gesamt-Sync-Performance kann durch Netzwerkbandbreite, Latenz und Netzwerktopologie sowie die VM-Spezifikationen des Data Brokers und die Performance des Storage-Systems beeinträchtigt werden. Ein einzelner Daten-Broker in einer Synchronisierungsbeziehung kann beispielsweise 100 MB/s erreichen, während der Festplattendurchsatz auf dem Ziel möglicherweise nur 64 MB/s zulässt. Folglich versucht der Daten-Broker, die Daten zu kopieren, doch das Ziel kann die Performance des Daten-Brokers nicht erreichen.

Überprüfen Sie also die Performance Ihres Netzwerks und den Festplattendurchsatz auf dem Ziel.

Dann können Sie die Sync-Performance beschleunigen, indem Sie einen zusätzlichen Daten-Broker hinzufügen, um die Last dieser Beziehung gemeinsam zu nutzen. "Erfahren Sie, wie Sie die synchrone

Performance beschleunigen".

Dinge löschen

Die folgenden Fragen beziehen sich auf das Löschen von Synchronisierungsbeziehungen und -daten aus Quellen und Zielen.

Was passiert, wenn ich meine Cloud Sync-Beziehung lösche?

Durch das Löschen einer Beziehung werden alle zukünftigen Daten synchronisiert und die Zahlung wird beendet. Alle Daten, die mit dem Ziel synchronisiert wurden, bleiben unverändert.

Was passiert, wenn ich etwas von meinem Quellserver lösche? Wird sie auch aus dem Ziel entfernt?

Wenn Sie eine aktive Synchronisierungsbeziehung haben, wird das auf dem Quellserver gelöschte Element bei der nächsten Synchronisierung standardmäßig nicht vom Ziel gelöscht. In den Synchronisierungseinstellungen für jede Beziehung gibt es jedoch eine Option, mit der Sie festlegen können, dass Cloud Sync Dateien im Zielspeicherort löscht, wenn sie aus der Quelle gelöscht wurden.

"Hier erfahren Sie, wie Sie die Einstellungen für eine Synchronisierungsbeziehung ändern".

Was passiert, wenn ich etwas von meinem Ziel lösche? Wird es auch aus meiner Quelle entfernt?

Wenn ein Element aus dem Ziel gelöscht wird, wird es nicht aus der Quelle entfernt. Die Beziehung verläuft von der Quelle zum Ziel. Beim nächsten Synchronisierungszyklus vergleicht Cloud Sync die Quelle mit dem Ziel, erkennt, dass das Element fehlt, und Cloud Sync kopiert es erneut von der Quelle zum Ziel.

Fehlerbehebung

"NetApp Knowledgebase: FAQ zu Cloud Sync: Support und Fehlerbehebung"

Data Broker - tief greifend

Die folgende Frage bezieht sich auf den Data Broker.

Können Sie die Architektur des Data Brokers erläutern?

Sicher. Hier die wichtigsten Punkte:

- Der Data Broker ist eine Node.js-Anwendung, die auf einem Linux-Host ausgeführt wird.
- Cloud Sync stellt den Daten-Broker wie folgt bereit:
  - AWS: Aus einer AWS CloudFormation Vorlage
  - Azure: Von Azure Resource Manager
  - Google: Von Google Cloud Deployment Manager
  - Wenn Sie Ihren eigenen Linux-Host verwenden, müssen Sie die Software manuell installieren
- Die Data Broker-Software aktualisiert sich automatisch auf die neueste Version.
- Der Data Broker nutzt AWS SQS als zuverlässigen und sicheren Kommunikationskanal sowie zur Steuerung und Überwachung. SQS bietet auch eine Persistenzschicht.
- Sie können einer Beziehung zusätzliche Datenvermittler hinzufügen, um die Übertragungsgeschwindigkeit zu erhöhen und eine hohe Verfügbarkeit hinzuzufügen. Bei Ausfall eines Data Brokers besteht Service-

Ausfallsicherheit.

Einblicke in den Datenschutz

Erfahren Sie mehr über Cloud Compliance

Cloud Compliance ist ein Datenschutz- und Compliance-Service für Cloud Manager, der Ihre Volumes, Amazon S3 Buckets und Datenbanken scannt, um die persönlichen und sensiblen Daten zu ermitteln, die sich in diesen Dateien befinden. Mithilfe von künstlicher Intelligenz (KI) hilft Cloud Compliance Unternehmen dabei, den Datenkontext zu verstehen und sensible Daten zu ermitteln.

"Erfahren Sie mehr über Anwendungsfälle für Cloud Compliance".

Funktionen

Cloud Compliance bietet verschiedene Tools, die Sie bei Ihren Compliance-Strategien unterstützen. Cloud Compliance bietet Ihnen:

- Ermitteln von personenbezogenen Daten
- Vielzahl sensibler Daten, je nach DSGVO, CCPA, PCI und HIPAA-Datenschutzvorschriften, identifizieren
- Reagieren Sie auf DSAR (Data Subject Access Requests).

Unterstützte Arbeitsumgebungen und Datenquellen

Cloud Compliance kann Daten aus folgenden Datenquellen scannen:

- Cloud Volumes ONTAP in AWS
- Cloud Volumes ONTAP in Azure
- Azure NetApp Dateien
- Amazon S3
- Datenbanken, die sich überall befinden (die Datenbank muss sich nicht in einer Arbeitsumgebung befinden)

Hinweis: für Azure NetApp Files kann Cloud Compliance alle Volumes scannen, die sich in derselben Region wie Cloud Manager befinden.

Kosten

- Die Kosten für die Verwendung von Cloud Compliance hängen von der Datenmenge ab, die Sie scannen. Zum 7. Oktober 2020 werden die ersten 1 TB der Daten, die Cloud Compliance in einem Cloud Manager-Arbeitsbereich scannt, kostenlos bereitgestellt. Dazu gehören Daten von Cloud Volumes ONTAP Volumes, Azure NetApp Files Volumes, Amazon S3 Buckets und Datenbank-Schemas. Danach ist ein Abonnement für AWS oder Azure Marketplace erforderlich, um mit dem Scannen der Daten fortzufahren. Siehe "Preisgestaltung" Entsprechende Details.

  "Erfahren Sie, wie Sie abonniert werden können".

- Für die Installation von Cloud Compliance ist die Implementierung einer Cloud-Instanz erforderlich, was für den Cloud-Provider, bei dem sie implementiert wird, Gebühren anfallen. Siehe Der für jeden Cloud-Provider implementierte Instanztyp

- Cloud Compliance erfordert die Implementierung eines Konnektors. Aufgrund anderer Storage-Systeme und Services, die Sie in Cloud Manager verwenden, haben Sie häufig bereits einen Connector. Die Connector-Instanz verursacht Gebühren bei dem Cloud-Provider, wo sie implementiert wird. Siehe "Für jeden Cloud-Provider implementierte Instanztyp".

Datentransferkosten

Die Datentransferkosten hängen von Ihrer Einrichtung ab. Wenn sich die Cloud Compliance-Instanz und die Datenquelle in derselben Verfügbarkeitszone und Region befinden, entstehen keine Datentransferkosten. Wenn sich die Datenquelle, beispielsweise ein Cloud Volumes ONTAP-Cluster oder S3-Bucket, jedoch in einer *verschiedenen* Verfügbarkeitszone oder -Region befindet, wird Ihr Cloud-Provider für Datentransferkosten berechnet. Weitere Informationen finden Sie unter diesen Links:

- "AWS: Amazon EC2-Preisgestaltung"
- "Microsoft Azure: Preisangaben Für Die Bandbreite"

Funktionsweise von Cloud Compliance

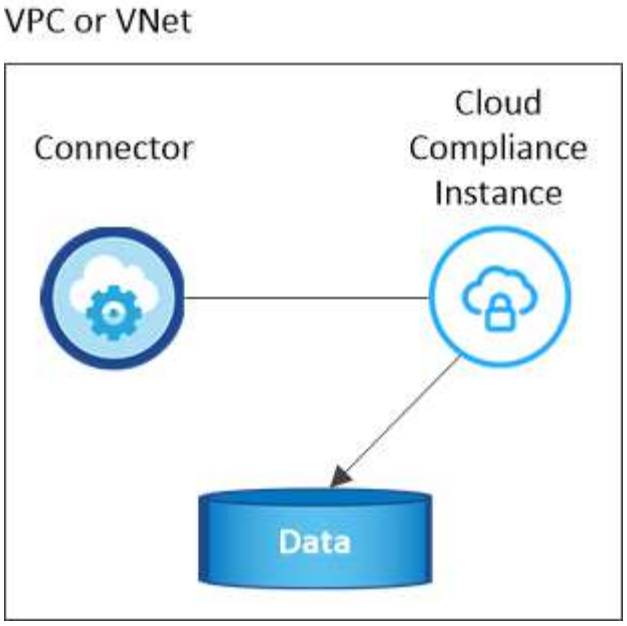
Cloud Compliance funktioniert auf hohem Niveau wie folgt:

1. Sie implementieren eine Instanz von Cloud Compliance in Cloud Manager.
2. Sie ermöglichen es in einer oder mehreren Arbeitsumgebungen oder in Ihren Datenbanken.
3. Cloud Compliance scannt die Daten mithilfe eines KI-Learning-Prozesses.
4. In Cloud Manager klicken Sie auf **Compliance** und verwenden Sie das bereitgestellte Dashboard und die Berichterstellungs-Tools, um Ihre Compliance-Bemühungen zu unterstützen.

Die Instanz für Cloud Compliance

Wenn Sie Cloud Compliance aktivieren, implementiert Cloud Manager eine Cloud Compliance-Instanz im selben Subnetz wie der Connector. "Erfahren Sie mehr über Steckverbinder."

Falls der Connector lokal installiert wird, implementiert er die Cloud Compliance-Instanz in derselben VPC oder vnet wie das erste Cloud Volumes ONTAP-System in der Anfrage.



Beachten Sie Folgendes über die Instanz:

- In Azure wird Cloud Compliance auf einer VM mit Standard_D16s_v3 mit einer Festplatte von 512 GB ausgeführt.
- In AWS wird Cloud-Compliance auf einer m5.4xlarge-Instanz mit einer 500-GB-GP2-Festplatte ausgeführt.

  In Regionen, in denen m5.4xlarge nicht verfügbar ist, wird Cloud Compliance stattdessen auf einer m4.4xlarge-Instanz ausgeführt.

  Das Ändern oder Ändern der Größe des Instanz-/VM-Typs wird nicht unterstützt. Sie müssen die angegebene Größe verwenden.

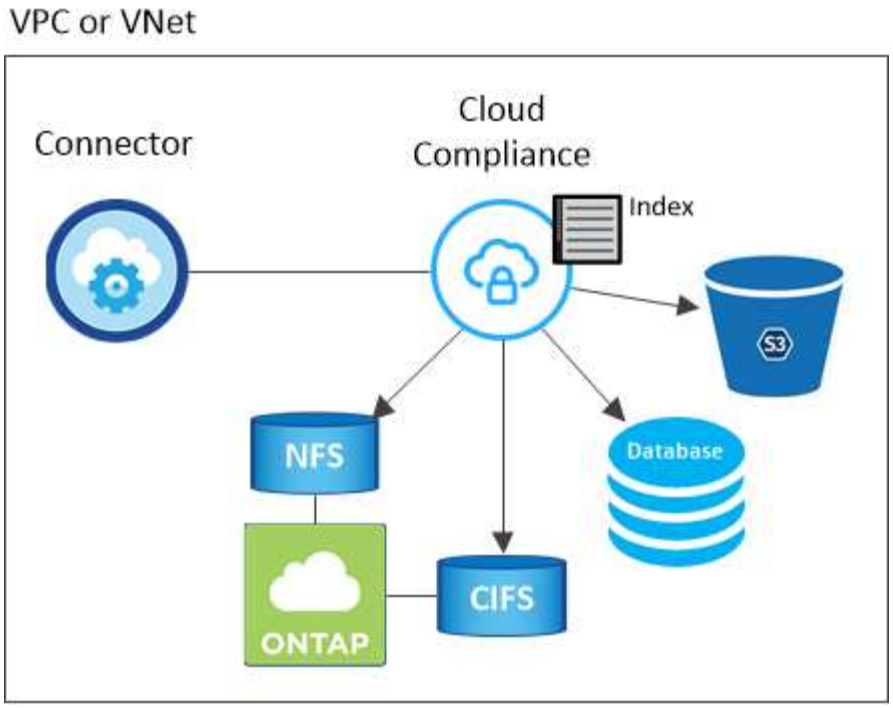
- Der Name der Instanz ist *CloudCompliance* mit einem generierten Hash (UUID), der verknüpft ist. Beispiel: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Pro Connector wird nur eine Cloud-Compliance-Instanz bereitgestellt.
- Die Upgrades der Cloud Compliance-Software sind automatisiert – Sie müssen sich keine Gedanken darüber machen.

Die Instanz sollte jederzeit ausgeführt werden, da Cloud Compliance die Daten kontinuierlich scannt.

Funktionsweise von Scans

Nachdem Sie Cloud Compliance aktiviert und die Volumes, Buckets oder Datenbankschemata ausgewählt haben, die Sie scannen möchten, wird sofort mit dem Scannen der Daten begonnen, um persönliche und sensible Daten zu identifizieren. Es ordnet Ihre Organisationsdaten zu, kategorisiert jede Datei und identifiziert und extrahiert Entitäten und vordefinierte Muster in den Daten. Das Ergebnis des Scans ist ein Index von persönlichen Daten, sensiblen persönlichen Daten und Datenkategorien.

Cloud Compliance stellt durch das Mounten von NFS- und CIFS-Volumes eine Verbindung zu den Daten wie jedem anderen Client her. NFS Volumes werden automatisch als schreibgeschützt abgerufen und müssen zur Überprüfung von CIFS Volumes Active Directory Anmeldeinformationen bereitstellen.



Nach dem ersten Scan scannt Cloud Compliance jedes Volume kontinuierlich, um inkrementelle Änderungen zu erkennen (deshalb ist es wichtig, die Instanz weiterhin zu betreiben).

Sie können Scans im aktivieren und deaktivieren "Volume-Ebene", Am "Bucket-Ebene", Und am "Datenbankschemenebene".

Information, die Cloud Compliance indiziert

Cloud Compliance erfasst, indiziert und weist Kategorien unstrukturierten Daten (Dateien) zu. Cloud Compliance umfasst folgende Daten:

Standard-Metadaten

Cloud Compliance sammelt Standard-Metadaten zu Dateien: Dateityp, Größe, Erstellung, Änderung usw.

Persönliche Daten

Personenbezogene Informationen wie E-Mail-Adressen, Identifikationsnummern oder Kreditkartennummern. "Weitere Informationen zu personenbezogenen Daten".

Sensible persönliche Daten

Besondere Arten sensibler Daten, wie etwa Gesundheitsdaten, ethnische Herkunft oder politische Ansichten, wie in der DSGVO und anderen Datenschutzvorschriften definiert "Erfahren Sie mehr über sensible persönliche Daten".

Kategorien

Bei Cloud Compliance werden die gescannten Daten in verschiedene Kategorien unterteilt. Kategorien sind Themen, die auf der KI-Analyse des Inhalts und der Metadaten jeder Datei basieren. "Weitere Informationen zu Kategorien".

Name der Entität Anerkennung

Cloud Compliance nutzt KI, um Namen natürlicher Personen aus Dokumenten zu extrahieren. "Informieren Sie sich über die Reaktion auf Zugriffsanfragen von Betroffenen".

Netzwerkübersicht

Cloud Manager implementiert die Cloud Compliance-Instanz mit einer Sicherheitsgruppe, die eingehende HTTP-Verbindungen von der Connector-Instanz ermöglicht.

Bei der Verwendung von Cloud Manager im SaaS-Modus, wird die Verbindung zu Cloud Manager über HTTPS bedient, und die privaten Daten, die zwischen Ihrem Browser und der Cloud Compliance-Instanz gesendet werden, sind mit End-to-End-Verschlüsselung gesichert, was bedeutet, dass NetApp und Dritte nicht lesen können.

Wenn Sie aus irgendeinem Grund die lokale Benutzeroberfläche anstelle der SaaS-Benutzeroberfläche verwenden müssen, können Sie immer noch "Greifen Sie auf die lokale UI zu".

Ausgehende Regeln sind vollständig geöffnet. Zum Installieren und Aktualisieren der Cloud Compliance-Software und zum Senden von Nutzungsmetriken ist Internetzugang erforderlich.

Wenn Sie strenge Netzwerkanforderungen erfüllen, "Informationen zu den Endpunkten, die Cloud Compliance kontaktiert".

Zugriff des Benutzers auf Compliance-Informationen

Jeder Benutzer verfügt über verschiedene Funktionen innerhalb von Cloud Manager und innerhalb von Cloud Compliance:

- **Kontoadministratoren** können Compliance-Einstellungen verwalten und Compliance-Informationen für alle Arbeitsumgebungen anzeigen.
- **Workspace-Administratoren** können Compliance-Einstellungen verwalten und Compliance-Informationen nur für Systeme anzeigen, auf die sie Zugriff haben. Wenn ein Workspace-Administrator nicht auf eine Arbeitsumgebung in Cloud Manager zugreifen kann, werden auf der Registerkarte Compliance keine Compliance-Informationen für die Arbeitsumgebung angezeigt.
- Benutzer mit der Rolle **Cloud Compliance Viewer** können Compliance-Informationen nur anzeigen und Berichte für Systeme erstellen, auf die sie zugreifen können. Diese Benutzer können das Scannen von Volumes, Buckets oder Datenbankschemata nicht aktivieren/deaktivieren.

"Erfahren Sie mehr über die Rollen von Cloud Manager" Und wie "Benutzer mit bestimmten Rollen hinzufügen".

Los geht’s

Implementierung Von Cloud Compliance

Führen Sie einige Schritte durch, um die Cloud Compliance-Instanz in Ihrem Cloud Manager Workspace zu implementieren.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

Einen Konnektor erstellen

Falls Sie noch keinen Connector haben, erstellen Sie in Azure oder AWS einen Connector. Siehe "Erstellen eines Konnektors in AWS" Oder "Erstellen eines Connectors in Azure".

Voraussetzungen prüfen

Stellen Sie sicher, dass Ihre Cloud-Umgebung die Voraussetzungen erfüllt, die 16 vCPUs für die Cloud Compliance Instanz, Outbound-Internetzugang zur Instanz, Konnektivität zwischen Connector und Cloud Compliance über Port 80 umfassen kann. Eine vollständige Liste finden Sie hier.

Implementierung Von Cloud Compliance

Starten Sie den Installationsassistenten, um die Cloud Compliance-Instanz in Cloud Manager zu implementieren.

Abonnieren Sie den Cloud Compliance Service

Die ersten 1 TB an Daten, die Cloud Compliance in Cloud Manager scannt, sind kostenlos. Danach ist ein Abonnement für AWS oder Azure Marketplace erforderlich, um mit dem Scannen der Daten fortzufahren.

Erstellen eines Connectors

Falls Sie noch keinen Connector haben, erstellen Sie in Azure oder AWS einen Connector. Siehe "Erstellen eines Konnektors in AWS" Oder "Erstellen eines Connectors in Azure". In den meisten Fällen haben Sie wahrscheinlich einen Connector eingerichtet, bevor Sie Cloud Compliance aktivieren, da die meisten davon "Für die Funktionen von Cloud Manager ist ein Connector erforderlich", Aber es gibt Fälle, wenn Sie eine Einrichtung jetzt.

Es gibt einige Szenarien, in denen ein Connector in AWS oder Azure für Cloud Compliance verwendet werden muss.

- Beim Scannen von Daten in Cloud Volumes ONTAP in AWS oder in AWS S3 Buckets verwenden Sie einen Connector in AWS.
- Beim Scannen von Daten in Cloud Volumes ONTAP in Azure oder in Azure NetApp Files verwenden Sie einen Konnektor in Azure.
- Datenbanken können über einen der beiden Connectors gescannt werden.

Wie Sie sehen können, gibt es einige Situationen, in denen Sie verwenden müssen "Mehrere Anschlüsse".

Wenn Sie Azure NetApp Files scannen möchten, müssen Sie sicherstellen, dass Sie in derselben Region wie die Volumes bereitstellen, die Sie scannen möchten.

Voraussetzungen prüfen

Prüfen Sie die folgenden Voraussetzungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie Cloud Compliance bereitstellen.

Aktivieren Sie den Outbound-Internetzugang

Cloud Compliance erfordert Outbound-Internetzugang. Wenn Ihr virtuelles Netzwerk einen Proxyserver für den Internetzugriff verwendet, stellen Sie sicher, dass die Cloud Compliance-Instanz über einen ausgehenden Internetzugriff verfügt, um die folgenden Endpunkte zu kontaktieren. Beachten Sie, dass Cloud Manager die Cloud Compliance-Instanz im selben Subnetz wie der Connector bereitstellt.

Endpunkte	Zweck
https://cloudmanager.cloud.netapp.com	Kommunikation mit dem Cloud Manager-Service, der Cloud Central-Konten einschließt
https://netapp-cloud-account.auth0.com https://auth0.com	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Cloud Compliance ermöglicht es, auf Manifeste und Vorlagen zuzugreifen und diese herunterzuladen sowie Protokolle und Kennzahlen zu senden.

Stellen Sie sicher, dass Cloud Manager über die erforderlichen Berechtigungen verfügt

Stellen Sie sicher, dass Cloud Manager über die Berechtigungen zum Implementieren von Ressourcen verfügt und Sicherheitsgruppen für die Instanz Cloud Compliance erstellen kann. Die neuesten Berechtigungen von Cloud Manager finden Sie in "Die von NetApp bereitgestellten Richtlinien".

Überprüfen Sie Ihre vCPU-Limits

Stellen Sie sicher, dass das vCPU-Limit Ihres Cloud-Providers die Bereitstellung einer Instanz mit 16 Cores ermöglicht. Sie müssen das vCPU-Limit für die entsprechende Instanzfamilie in der Region, in der Cloud Manager ausgeführt wird, überprüfen.

In AWS lautet die Instanzfamilie *On-Demand Standard-Instanzen*. In Azure ist die Instanzfamilie *Standard DSv3 Family*.

Weitere Informationen zu vCPU-Limits finden Sie im folgenden Dokument:

- "AWS Dokumentation: Amazon EC2 Service Limits"
- "Azure Dokumentation: VCPU Kontingente von Virtual Machines"

Stellen Sie sicher, dass Cloud Manager auf Cloud Compliance zugreifen kann

Stellen Sie die Verbindung zwischen dem Connector und der Cloud Compliance-Instanz sicher. Die Sicherheitsgruppe für den Connector muss ein- und ausgehenden Datenverkehr über Port 80 zu und von der Cloud Compliance-Instanz ermöglichen.

Diese Verbindung ermöglicht die Bereitstellung der Cloud Compliance-Instanz sowie die Anzeige von Informationen auf der Registerkarte Compliance.

Einrichten der Erkennung von Azure NetApp Files

Bevor Sie Volumes für Azure NetApp Files scannen können, "Cloud Manager muss eingerichtet sein, um die Konfiguration zu ermitteln".

Stellen Sie sicher, dass Cloud-Compliance weiterhin verfügbar ist

Die Cloud Compliance Instanz muss stets zum kontinuierlichen Scannen Ihrer Daten verfügbar sein.

Stellen Sie die Verbindung zwischen Webbrowser und Cloud Compliance sicher

Stellen Sie nach Aktivierung von Cloud Compliance sicher, dass Benutzer von einem Host, der über eine Verbindung zur Cloud Compliance-Instanz verfügt, auf die Cloud Manager-Schnittstelle zugreifen.

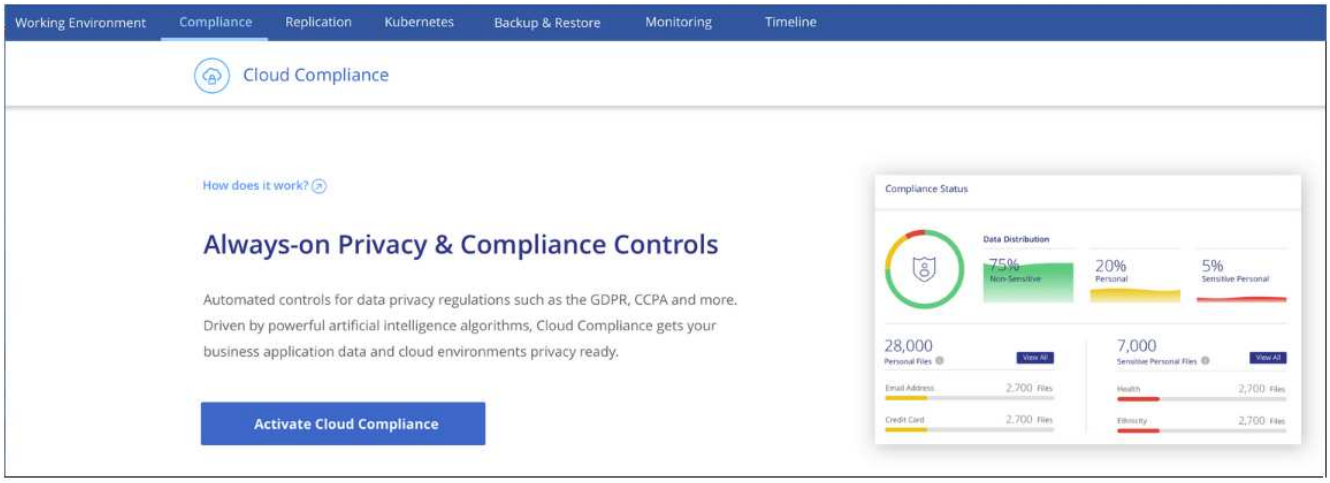
Die Cloud Compliance Instanz verwendet eine private IP-Adresse, um sicherzustellen, dass die indizierten Daten nicht für das Internet verfügbar sind. Daher muss der Webbrowser, den Sie für den Zugriff auf Cloud Manager verwenden, über eine Verbindung zu dieser privaten IP-Adresse verfügen. Die Verbindung kann über eine direkte Verbindung zu AWS oder Azure (z. B. ein VPN) oder von einem Host im selben Netzwerk wie die Cloud-Compliance-Instanz hergestellt werden.

Bereitstellen der Instanz für Cloud-Compliance

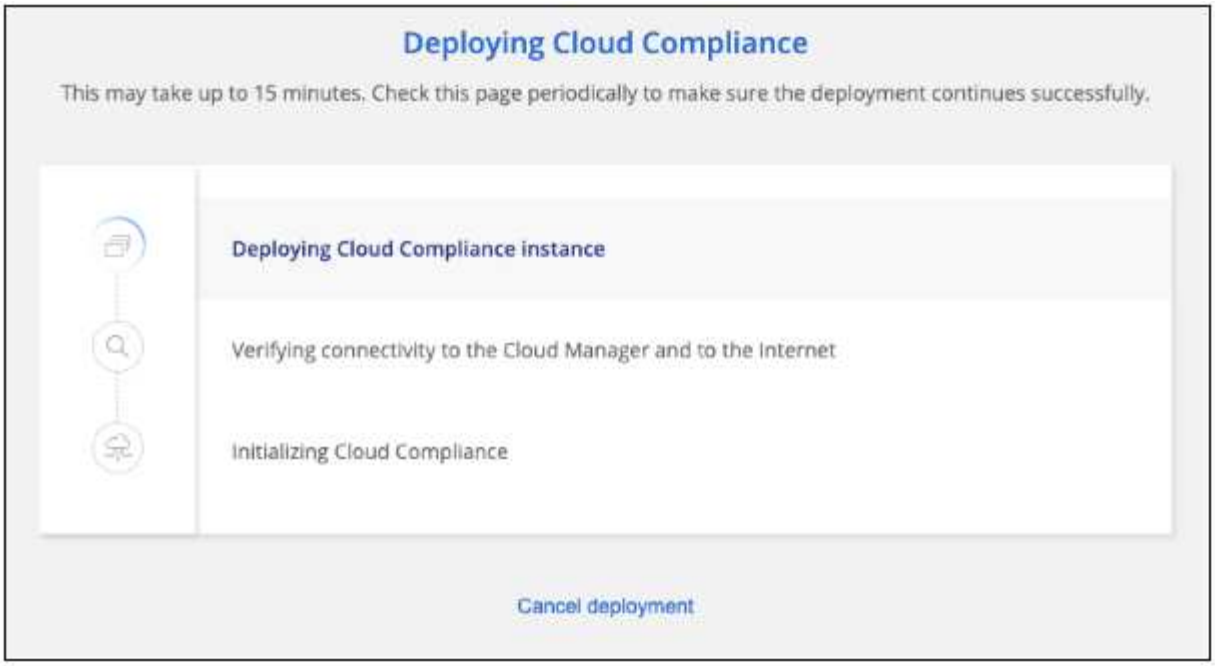
Sie implementieren für jede Cloud Manager Instanz eine Instanz von Cloud Compliance.

Schritte

1. Klicken Sie in Cloud Manager auf **Cloud Compliance**.
2. Klicken Sie auf **Cloud Compliance aktivieren**, um den Bereitstellungsassistenten zu starten.



3. Der Assistent zeigt den Fortschritt während der Bereitstellungsschritte an. Er wird angehalten und um Informationen gebeten, wenn es zu Problemen kommt.



4. Wenn die Instanz bereitgestellt wird, klicken Sie auf **Weiter zur Konfiguration**, um zur Seite *Scan Configuration* zu gelangen.

Ergebnis

Cloud Manager implementiert die Cloud Compliance-Instanz bei Ihrem Cloud-Provider.

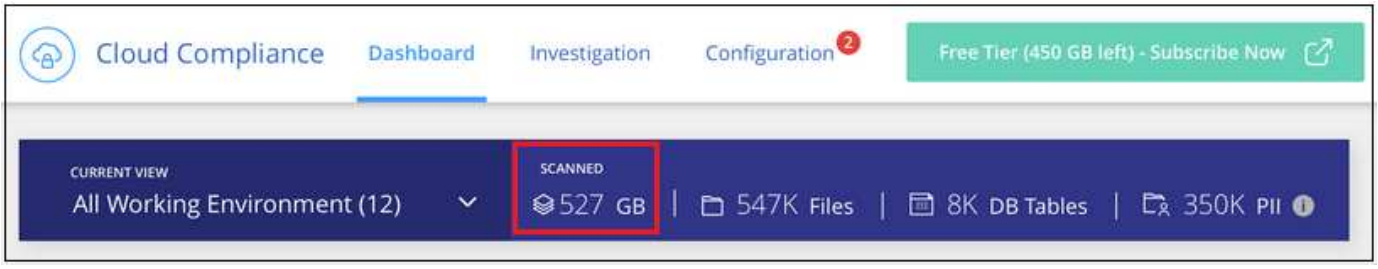
Nächste Schritte

Auf der Seite Scankonfiguration können Sie die Arbeitsumgebungen, Volumes und Buckets auswählen, die Sie auf Compliance überprüfen möchten. Sie können auch eine Verbindung zu einem Datenbankserver herstellen, um bestimmte Datenbankschemas zu scannen. Aktivieren Sie Cloud Compliance für eine dieser Datenquellen.

Abonnieren des Cloud Compliance Service

Es sind die ersten 1 TB an Daten, die Cloud Compliance in einem Cloud Manager Workspace scannt, kostenlos. Danach ist ein Abonnement für AWS oder Azure Marketplace erforderlich, um mit dem Scannen der Daten fortzufahren.

Sie können sich jederzeit für eine Anmeldung anmelden. Die Abrechnung erfolgt erst, wenn die Datenmenge mehr als 1 TB beträgt. Über das Cloud Compliance Dashboard sehen Sie immer die Gesamtdatenmenge an, die gescannt wird. Und die Schaltfläche *Jetzt abonnieren* erleichtert die Anmeldung, wenn Sie bereit sind.

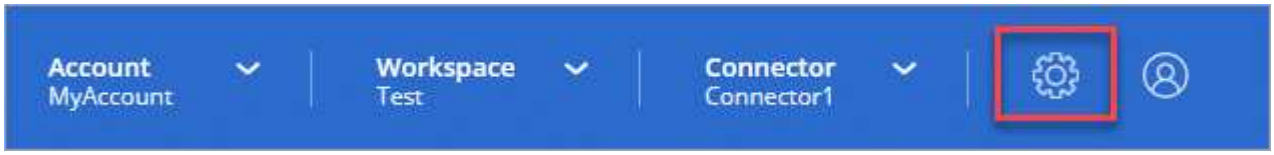


Hinweis: Wenn Sie von Cloud Compliance aufgefordert werden, sich zu abonnieren, aber Sie bereits über ein Azure-Abonnement verfügen, verwenden Sie wahrscheinlich das alte **Cloud Manager**-Abonnement und müssen in das neue **NetApp Cloud Manager**-Abonnement wechseln. SieheÄnderung im neuen NetApp Cloud Manager Plan in Azure Entsprechende Details.

Schritte

Diese Schritte müssen von einem Benutzer ausgeführt werden, der über die Rolle *Account Admin* verfügt.

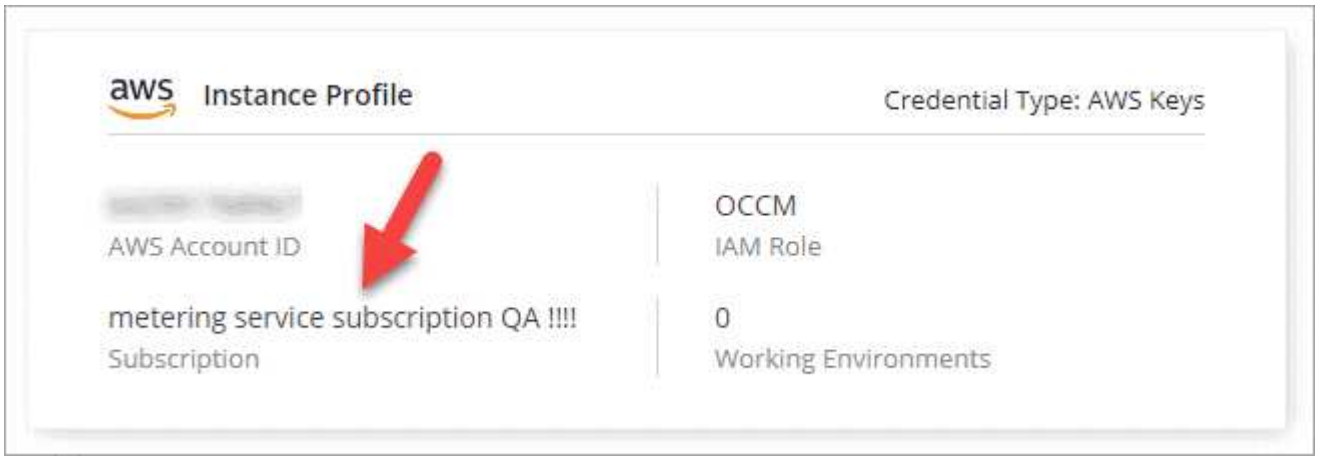
1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.



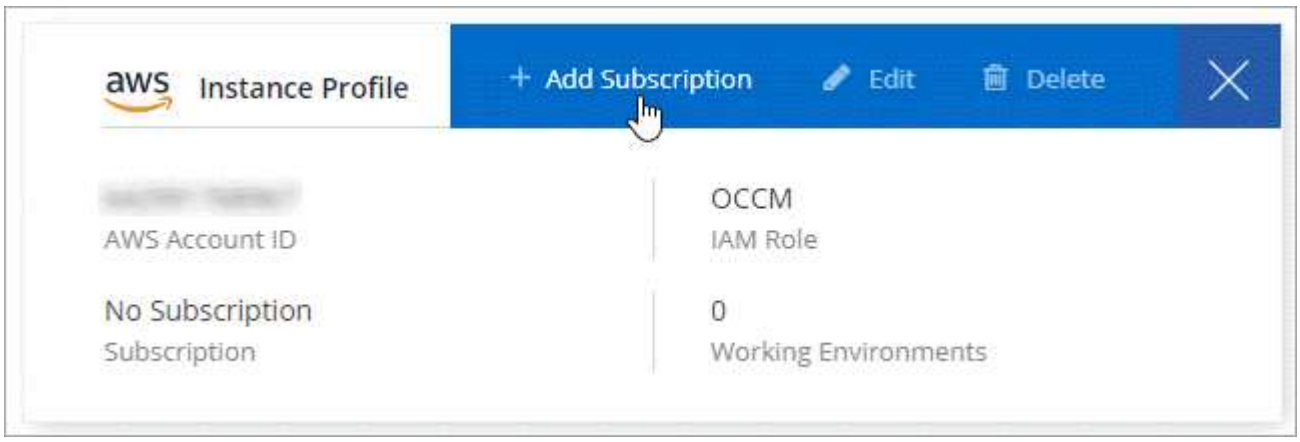
2. Suchen Sie die Zugangsdaten für das AWS Instance Profile oder die Azure Managed Service Identity.

   Das Abonnement muss dem Instanzprofil oder der Managed Service Identity hinzugefügt werden. Das Laden funktioniert nicht anders.

   Wenn Sie bereits ein Abonnement haben, sind Sie alle eingerichtet – es gibt nichts anderes, was Sie tun müssen.



3. Wenn Sie noch kein Abonnement haben, bewegen Sie den Mauszeiger über die Anmeldeinformationen und klicken Sie auf das Aktionsmenü.
4. Klicken Sie Auf **Abonnement Hinzufügen**.



5. Klicken Sie auf **Abonnement hinzufügen**, klicken Sie auf **Weiter** und befolgen Sie die Schritte.

   Im folgenden Video wird gezeigt, wie Sie ein Marketplace-Abonnement zu einem AWS Abonnement

verknüpfen:

► https://docs.netapp.com/de-de/occm38//media/video_subscribing_aws.mp4 *(video)*

Im folgenden Video wird gezeigt, wie Sie ein Marketplace-Abonnement zu einem Azure-Abonnement verknüpfen:

► https://docs.netapp.com/de-de/occm38//media/video_subscribing_azure.mp4 *(video)*

Änderung beim neuen Cloud Manager Plan in Azure

Cloud Compliance wurde zum Azure Marketplace Abonnement mit dem Namen **NetApp Cloud Manager** zum 7. Oktober 2020 hinzugefügt. Wenn Sie bereits über das ursprüngliche Azure **Cloud Manager**-Abonnement verfügen, können Sie Cloud Compliance nicht nutzen.

Sie müssen diese Schritte ausführen und das neue **NetApp Cloud Manager** Abonnement auswählen und dann das alte **Cloud Manager** Abonnement entfernen.

> Wenn Ihr Abonnement auf einem speziellen privaten Angebot ausgestellt wurde, müssen Sie sich an NetApp wenden, damit wir ein neues privates Angebot mit Compliance inbegriffen anbieten können.

Schritte

Diese Schritte ähneln dem Hinzufügen eines neuen Abonnements wie oben beschrieben, variieren jedoch an einigen Stellen.

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Suchen Sie die Anmeldeinformationen für die Azure Managed Service Identity, für die Sie das Abonnement ändern möchten, und zeigen Sie mit dem Mauszeiger über die Anmeldeinformationen, und klicken Sie auf **Associate Subscription**.

   Die Details zu Ihrem aktuellen Marketplace-Abonnement werden angezeigt.
3. Klicken Sie auf **Abonnement hinzufügen**, klicken Sie auf **Weiter** und befolgen Sie die Schritte. Sie werden auf das Azure Portal umgeleitet, um das neue Abonnement zu erstellen.
4. Stellen Sie sicher, dass Sie den Plan **NetApp Cloud Manager** für den Zugriff auf Cloud Compliance und nicht **Cloud Manager** wählen.
5. Gehen Sie die Schritte im Video durch, um ein Marketplace-Abonnement für ein Azure-Abonnement zuzuordnen:

   ► https://docs.netapp.com/de-de/occm38//media/video_subscribing_azure.mp4 *(video)*
6. Kehren Sie zu Cloud Manager zurück, wählen Sie das neue Abonnement aus und klicken Sie auf **Associate**.
7. Um zu überprüfen, ob sich Ihr Abonnement geändert hat, bewegen Sie den Mauszeiger über das „i“-Abonnement in der Anmeldeinformationen-Karte.

   Jetzt können Sie Ihr altes Abonnement vom Azure Portal abbestellen.
8. Gehen Sie im Azure-Portal zu Software as a Service (SaaS), wählen Sie das Abonnement aus und klicken Sie auf **Abmelden**.

Aktivieren Sie das Scannen Ihrer Datenquellen

Erste Schritte mit Cloud Compliance für Cloud Volumes ONTAP und Azure NetApp Files

Erste Schritte mit Cloud Compliance für Cloud Volumes ONTAP oder Azure NetApp Files

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

Implementieren der Cloud Compliance-Instanz

"Cloud Compliance in Cloud Manager implementieren" Falls noch keine Instanz implementiert wurde.

Cloud Compliance in Ihren Arbeitsumgebungen

Klicken Sie auf **Cloud Compliance**, wählen Sie die Registerkarte **Konfiguration** und aktivieren Sie Compliance-Scans für bestimmte Arbeitsumgebungen.

Zugriff auf Volumes sicherstellen

Jetzt, wo Cloud Compliance aktiviert ist, stellen Sie sicher, dass die IT auf Volumes zugreifen kann.

- Die Cloud Compliance Instanz benötigt eine Netzwerkverbindung zu jedem Cloud Volumes ONTAP- oder Azure NetApp Files-Subnetz.
- Sicherheitsgruppen für Cloud Volumes ONTAP müssen eingehende Verbindungen aus der Cloud-Compliance-Instanz zulassen.
- Die NFS-Volume-Exportrichtlinien müssen den Zugriff aus der Cloud Compliance-Instanz zulassen.
- Cloud Compliance benötigt Active Directory-Anmeldeinformationen zum Scannen von CIFS Volumes.

  Klicken Sie auf **Cloud Compliance** > **Scan-Konfiguration** > **CIFS-Anmeldeinformationen bearbeiten** und geben Sie die Anmeldeinformationen an. Die Anmeldedaten können schreibgeschützt sein. Durch Admin-Berechtigungen wird jedoch sichergestellt, dass Cloud Compliance Daten lesen kann, die erhöhte Berechtigungen erfordern.

Konfigurieren Sie die Volumes für das Scannen

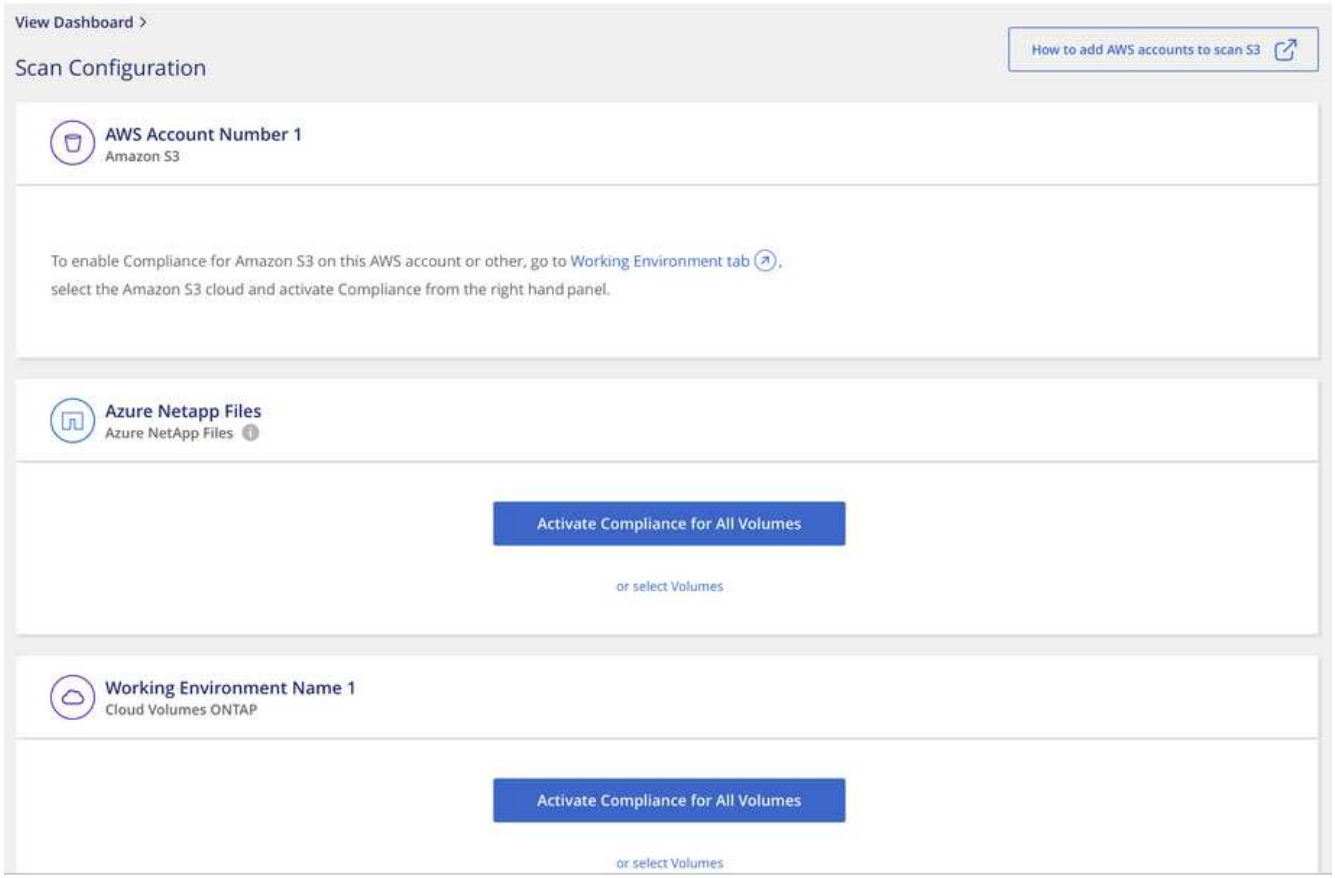
Wählen Sie die Volumes aus, die Sie scannen möchten, und Cloud Compliance beginnt, sie zu scannen.

Bereitstellen der Instanz für Cloud-Compliance

"Cloud Compliance in Cloud Manager implementieren" Falls noch keine Instanz implementiert wurde.

Cloud Compliance in Ihren Arbeitsumgebungen

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance** und wählen Sie dann die Registerkarte **Konfiguration** aus.



2. Um alle Volumes in einer Arbeitsumgebung zu scannen, klicken Sie auf **Compliance für alle Volumes aktivieren**.

   Um nur bestimmte Volumes in einer Arbeitsumgebung zu scannen, klicken Sie auf **oder wählen Sie Volumes** und wählen Sie dann die Volumes aus, die Sie scannen möchten.

Siehe Aktivieren und Deaktivieren von Compliance-Scans auf Volumes Entsprechende Details.

Ergebnis

Cloud Compliance beginnt mit der Überprüfung der Daten in den einzelnen Arbeitsumgebungen. Die Ergebnisse werden im Compliance-Dashboard verfügbar sein, sobald Cloud Compliance die ersten Scans abgeschlossen hat. Die Dauer, die von der Datenmenge abhängt, kann ein paar Minuten oder Stunden betragen.

Es wird sichergestellt, dass Cloud Compliance Zugriff auf Volumes hat

Stellen Sie sicher, dass Cloud Compliance auf Volumes zugreifen kann, indem Sie Ihre Netzwerk-, Sicherheitsgruppen- und Exportrichtlinien prüfen. Cloud Compliance muss über CIFS-Anmeldedaten bereitgestellt werden, damit der Zugriff auf CIFS Volumes möglich ist.

Schritte

1. Vergewissern Sie sich, dass eine Netzwerkverbindung zwischen Cloud Compliance-Instanz und jedem Netzwerk besteht, das Volumes für Cloud Volumes ONTAP oder Azure NetApp Files umfasst.

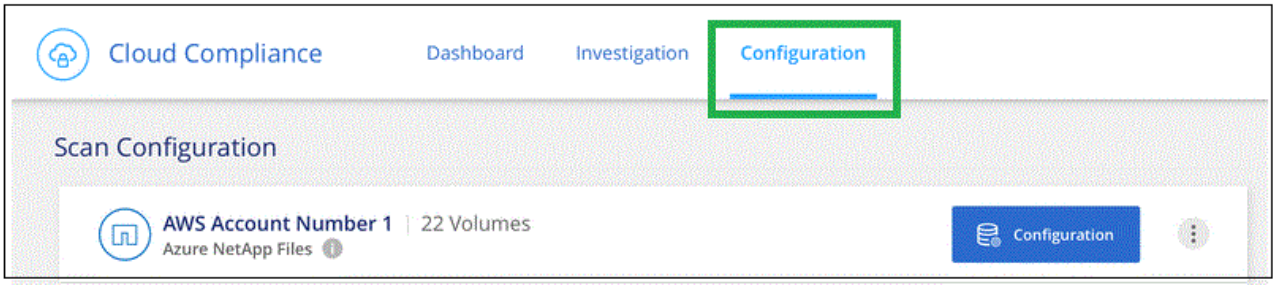
Bei Azure NetApp Files kann Cloud Compliance Volumes nur in derselben Region wie Cloud Manager überprüfen.

2. Stellen Sie sicher, dass die Sicherheitsgruppe für Cloud Volumes ONTAP eingehenden Datenverkehr aus der Cloud-Compliance-Instanz zulässt.

   Sie können entweder die Sicherheitsgruppe für den Datenverkehr von der IP-Adresse der Cloud Compliance-Instanz öffnen oder die Sicherheitsgruppe für den gesamten Datenverkehr im virtuellen Netzwerk öffnen.

3. Vergewissern Sie sich, dass die NFS-Volume-Exportrichtlinien die IP-Adresse der Cloud Compliance-Instanz enthalten, damit sie auf die Daten der einzelnen Volumes zugreifen können.
4. Wenn Sie CIFS verwenden, geben Sie Cloud Compliance mit Active Directory Anmeldedaten ein, damit CIFS Volumes gescannt werden können.

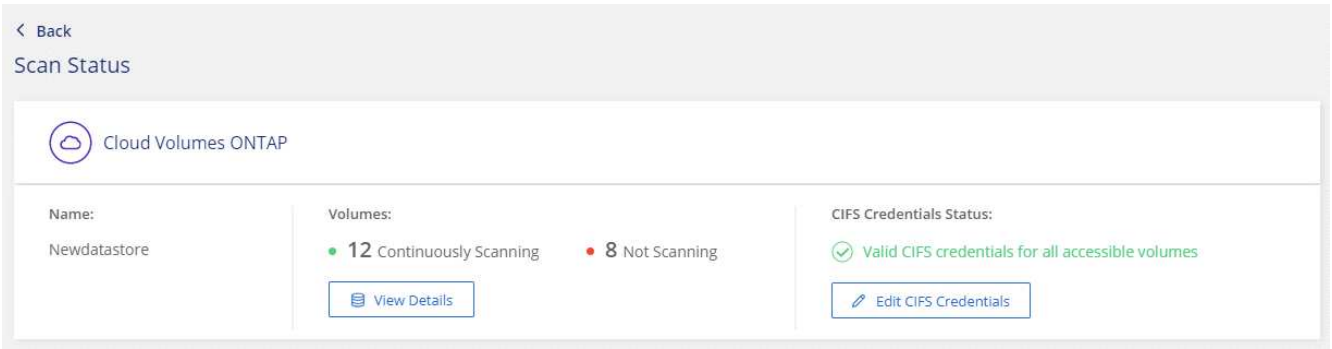
   a. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
   b. Klicken Sie auf die Registerkarte **Konfiguration**.



   c. Klicken Sie für jede Arbeitsumgebung auf **CIFS-Anmeldeinformationen bearbeiten** und geben Sie den Benutzernamen und das Passwort ein, die Cloud Compliance für den Zugriff auf CIFS-Volumes auf dem System benötigt.

      Die Anmeldedaten können schreibgeschützt sein. Durch Admin-Berechtigungen wird jedoch sichergestellt, dass Cloud Compliance Daten lesen kann, die erhöhte Berechtigungen benötigen. Die Anmeldedaten werden in der Instanz Cloud Compliance gespeichert.

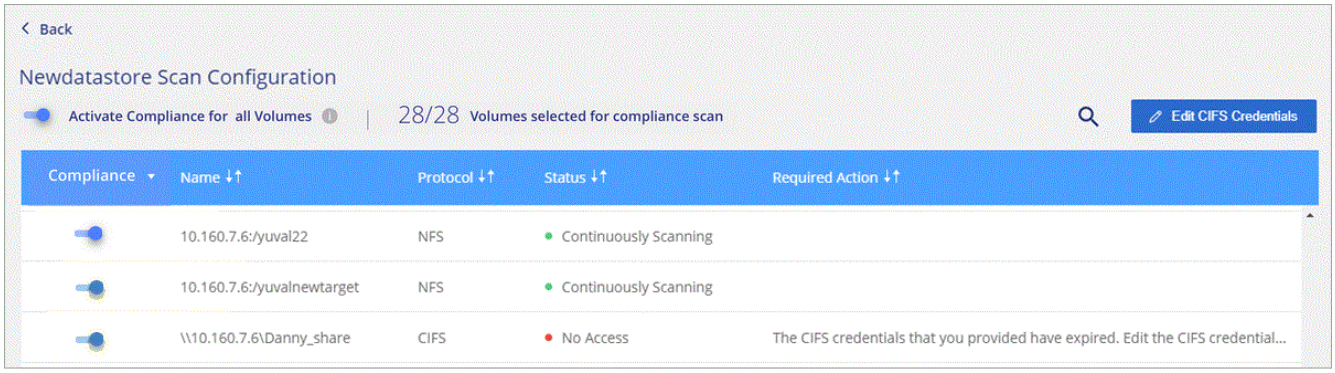
      Nach Eingabe der Anmeldedaten sollte eine Meldung angezeigt werden, dass alle CIFS-Volumes erfolgreich authentifiziert wurden.



5. Klicken Sie auf der Seite *Scan Configuration* auf **Details anzeigen**, um den Status für jedes CIFS- und NFS-Volume zu überprüfen und eventuelle Fehler zu beheben.

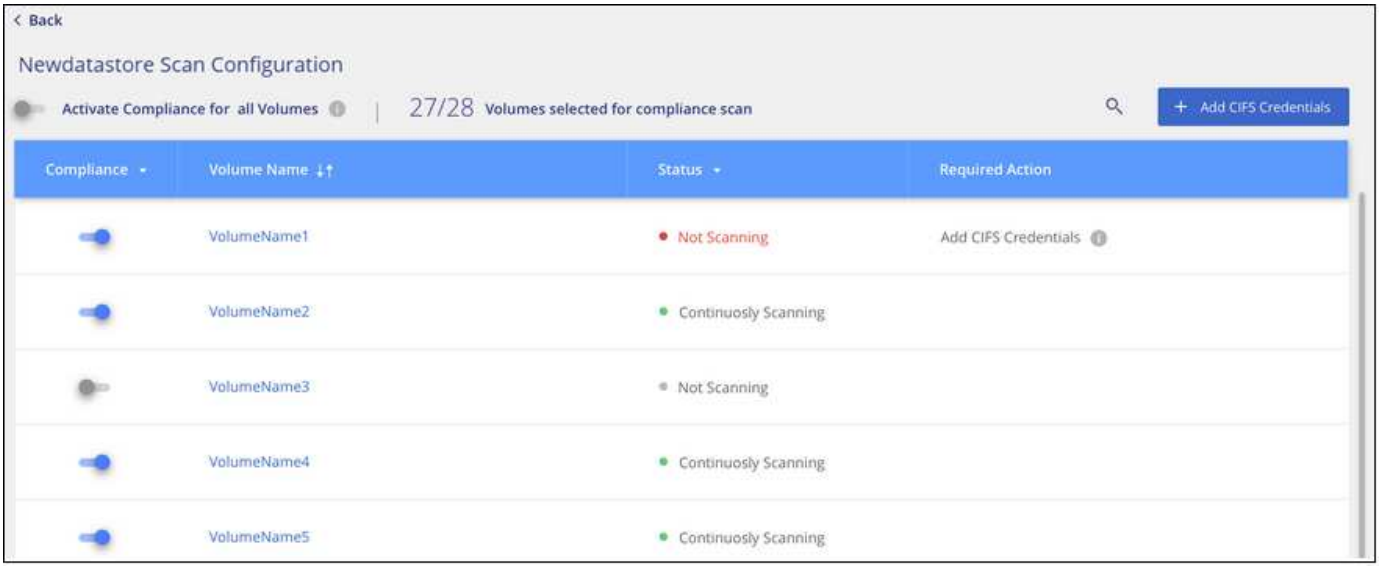
   Das folgende Bild zeigt beispielsweise drei Volumes, von denen Cloud Compliance aufgrund von

Netzwerkverbindungsproblemen zwischen der Cloud-Compliance-Instanz und dem Volume nicht scannen kann.



Aktivieren und Deaktivieren von Compliance-Scans auf Volumes

Sie können das Scannen von Volumes in einer Arbeitsumgebung jederzeit über die Seite Scankonfiguration anhalten oder starten. Wir empfehlen, alle Volumen zu scannen.



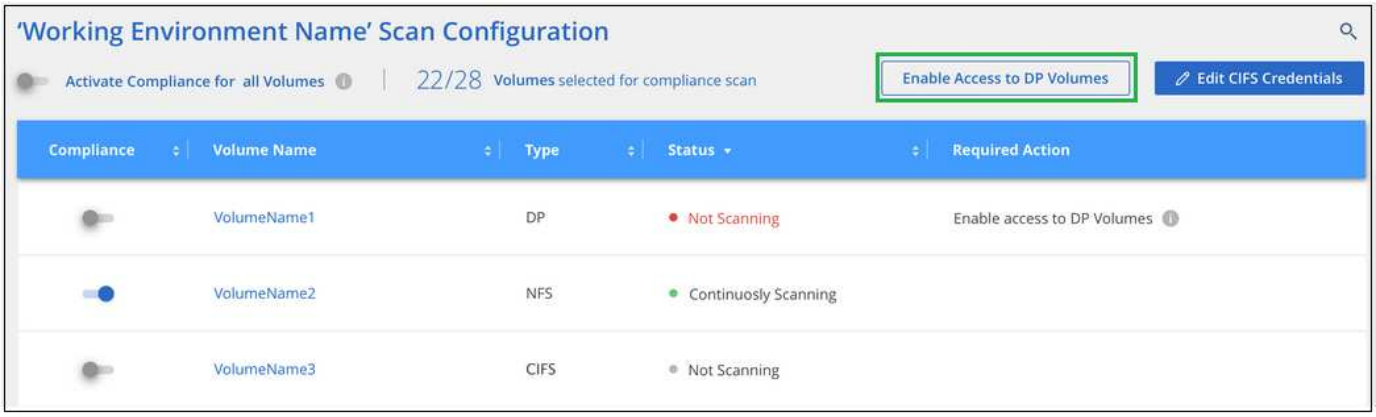
An:	Tun Sie dies:
Deaktivieren Sie das Scannen nach einem Volume	Bewegen Sie den Lautstärkeregler nach links
Deaktivieren Sie das Scannen für alle Volumes	Bewegen Sie den Schieberegler **Compliance für alle Volumes** nach links
Aktivieren Sie das Scannen nach einem Volume	Bewegen Sie den Lautstärkeregler nach rechts
Aktivieren Sie das Scannen für alle Volumes	Bewegen Sie den Schieberegler **Compliance für alle Volumes** nach rechts

Neue Volumes, die der Arbeitsumgebung hinzugefügt werden, werden nur dann automatisch gescannt, wenn die Einstellung **Compliance für alle Volumes** aktivieren aktiviert ist. Wenn diese Einstellung deaktiviert ist, müssen Sie das Scannen für jedes neue Volumen aktivieren, das Sie in der Arbeitsumgebung erstellen.

Scannen von Datensicherungs-Volumes

Standardmäßig werden Datensicherungs-Volumes nicht gescannt, weil sie nicht extern zugänglich sind und Cloud Compliance nicht darauf zugreifen kann. Diese Volumes sind normalerweise Ziel-Volumes für SnapMirror Vorgänge über ein ONTAP-Cluster vor Ort.

Zunächst erkennt die Liste der Cloud-Compliance-Volumes diese Volumes als *Type* **DP** mit dem *Status* **Not Scanning** und dem *required Action* **Enable Access to DP Volumes**.



Schritte

Wenn Sie diese Datensicherungs-Volumes scannen möchten:

1. Klicken Sie oben auf der Seite auf die Schaltfläche **Zugriff auf DP-Volumes aktivieren**.
2. Aktivieren Sie jedes DP-Volume, das Sie scannen möchten, oder verwenden Sie die Kontrolle **Compliance für alle Volumes aktivieren**, um alle Volumes, einschließlich aller DP-Volumes, zu aktivieren.

Sobald Cloud Compliance aktiviert ist, erstellt jedes DP Volume eine NFS-Freigabe, die für Compliance aktiviert wurde, sodass sie gescannt werden kann. Die Richtlinien für den Share-Export erlauben nur den Zugriff aus der Cloud Compliance-Instanz.

> In der Liste der Volumes werden nur Volumes angezeigt, die anfangs als NFS-Volumes im Quell-ONTAP-System erstellt wurden. Quell-Volumes, die zunächst als CIFS erstellt wurden, werden derzeit nicht in Cloud Compliance angezeigt.

Erste Schritte mit Cloud Compliance für Amazon S3

Cloud Compliance kann Ihre Amazon S3 Buckets scannen, um die persönlichen und sensiblen Daten zu identifizieren, die sich im S3 Objekt-Storage befinden. Cloud Compliance kann jeden Bucket auf dem Konto scannen, unabhängig davon, ob er für eine NetApp Lösung erstellt wurde.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

S3-Anforderungen in Ihrer Cloud-Umgebung einrichten

Stellen Sie sicher, dass Ihre Cloud-Umgebung die Anforderungen für Cloud Compliance erfüllen kann, einschließlich der Vorbereitung einer IAM-Rolle und der Einrichtung der Konnektivität von Cloud Compliance bis S3. Eine vollständige Liste finden Sie hier.

Implementieren der Cloud Compliance-Instanz

"Cloud Compliance in Cloud Manager implementieren" Falls noch keine Instanz implementiert wurde.

Aktivieren Sie Compliance in Ihrer S3-Arbeitsumgebung

Wählen Sie die Amazon S3-Arbeitsumgebung aus, klicken Sie auf **Compliance aktivieren** und wählen Sie eine IAM-Rolle aus, die die erforderlichen Berechtigungen enthält.

Wählen Sie die zu scannenden Buckets aus

Wählen Sie die Buckets aus, die Sie scannen möchten, und Cloud Compliance beginnt mit dem Scannen.

Überprüfen der S3-Voraussetzungen

Die folgenden Anforderungen gelten insbesondere für das Scannen von S3-Buckets.

Einrichten einer IAM-Rolle für die Cloud Compliance-Instanz

Cloud Compliance benötigt Berechtigungen, um sich mit den S3-Buckets Ihres Kontos zu verbinden und zu scannen. Richten Sie eine IAM-Rolle ein, die die unten aufgeführten Berechtigungen enthält. Cloud Manager fordert Sie auf, eine IAM-Rolle auszuwählen, wenn Sie Cloud Compliance in der Amazon S3-Arbeitsumgebung aktivieren.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:HeadBucket"
          ],
          "Resource": "*"
      },
      {
          "Effect": "Allow",
          "Action": [
              "iam:GetPolicyVersion",
              "iam:GetPolicy",
              "iam:ListAttachedRolePolicies"
          ],
          "Resource": [
              "arn:aws:iam::*:policy/*",
              "arn:aws:iam::*:role/*"
          ]
      }
  ]
}
```

Bereitstellung der Konnektivität von Cloud Compliance zu Amazon S3

Cloud Compliance benötigt eine Verbindung zu Amazon S3. Die beste Möglichkeit, eine solche Verbindung bereitzustellen, ist über einen VPC Endpunkt zum S3-Service. Anweisungen hierzu finden Sie unter "AWS Dokumentation: Erstellen eines Gateway-Endpunkts".

Wenn Sie den VPC-Endpunkt erstellen, sollten Sie die Region, die VPC und die Routing-Tabelle auswählen, die der Cloud Compliance-Instanz entspricht. Sie müssen auch die Sicherheitsgruppe ändern, um eine ausgehende HTTPS-Regel hinzuzufügen, die Datenverkehr zum S3-Endpunkt ermöglicht. Andernfalls kann Cloud Compliance 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?"

Eine Alternative besteht darin, die Verbindung über ein NAT Gateway bereitzustellen.

Sie können keinen Proxy verwenden, um über das Internet nach S3 zu gelangen.

Bereitstellen der Instanz für Cloud-Compliance

"Cloud Compliance in Cloud Manager implementieren" Falls noch keine Instanz implementiert wurde.

Sie müssen die Instanz in einem AWS Connector implementieren, damit Cloud Manager die S3-Buckets in diesem AWS-Konto automatisch erkennt und in einer Amazon S3-Arbeitsumgebung angezeigt wird.

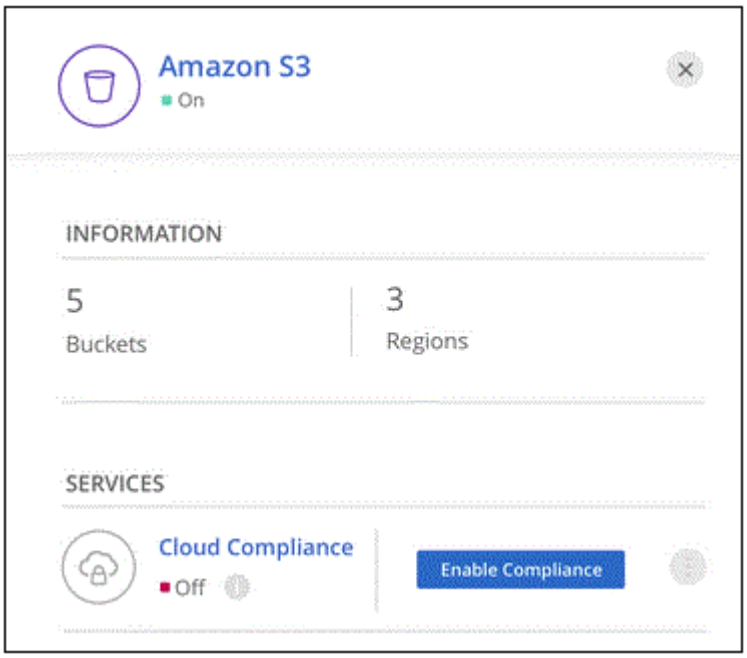
Aktivierung von Compliance in Ihrer S3-Arbeitsumgebung

Aktivieren Sie Cloud-Compliance auf Amazon S3, nachdem Sie die Voraussetzungen überprüft haben.

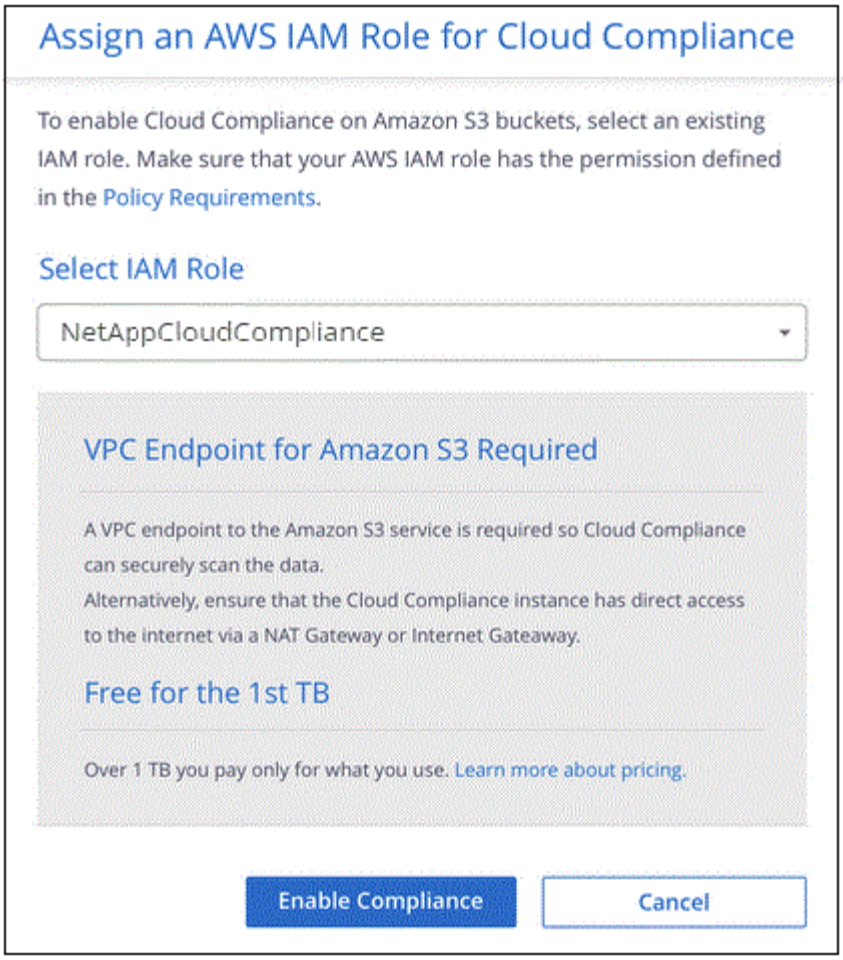
Schritte

1. Klicken Sie oben im Cloud Manager auf **Arbeitsumgebungen**.
2. Wählen Sie die Amazon S3-Arbeitsumgebung aus.

3. Klicken Sie im rechten Fensterbereich auf **Compliance aktivieren**.



4. Weisen Sie bei der entsprechenden Aufforderung der Cloud Compliance-Instanz eine IAM-Rolle zu Die erforderlichen Berechtigungen.



5. Klicken Sie Auf **Compliance Aktivieren**.

Sie können Compliance-Scans für eine Arbeitsumgebung auch über die Seite Scankonfiguration aktivieren, indem Sie auf die klicken Und wählen Sie **Compliance aktivieren**.

Ergebnis

Cloud Manager weist der Instanz die IAM-Rolle zu.

Aktivieren und Deaktivieren von Compliance-Scans auf S3-Buckets

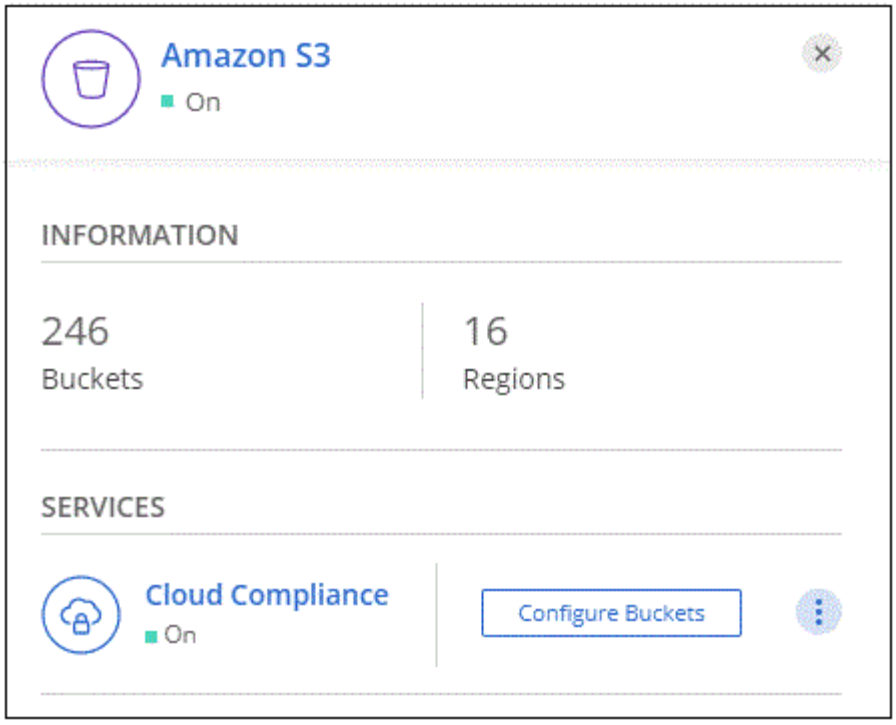
Nachdem Cloud Manager Cloud Compliance in Amazon S3 aktiviert hat, müssen die Buckets konfiguriert werden, die überprüft werden sollen.

Wenn Cloud Manager im AWS Konto ausgeführt wird, das über die S3-Buckets verfügt, die Sie scannen möchten, erkennt es diese Buckets und zeigt sie in einer Amazon S3-Arbeitsumgebung an.

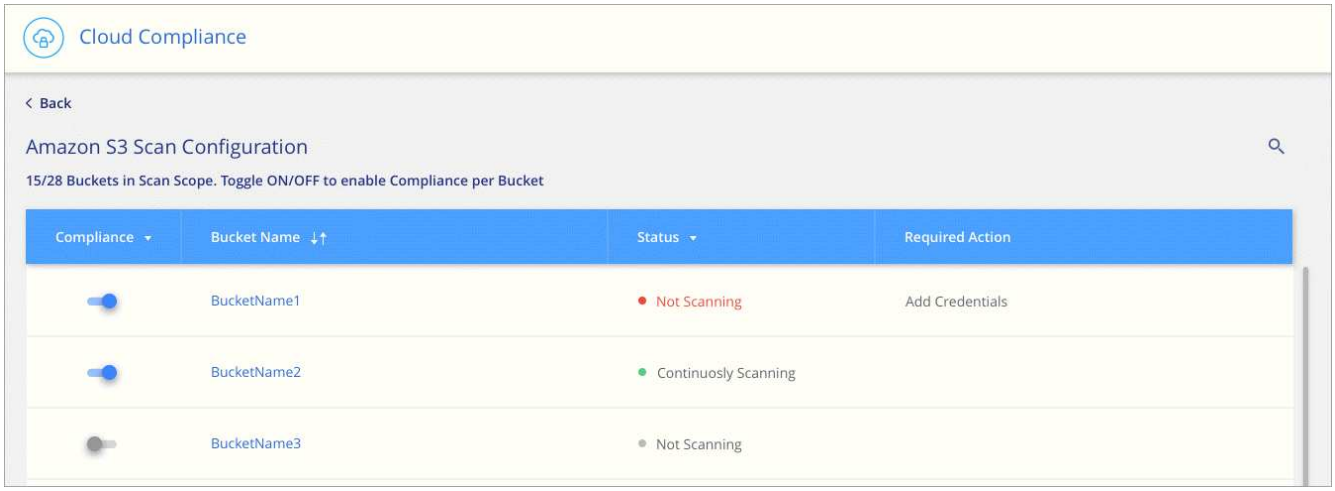
Auch Cloud Compliance kann Scannen von S3-Buckets, die in unterschiedlichen AWS Konten vorhanden sind.

Schritte

1. Wählen Sie die Amazon S3-Arbeitsumgebung aus.
2. Klicken Sie im rechten Fensterbereich auf **Eimer konfigurieren**.



3. Aktivieren Sie Compliance in den Buckets, die Sie scannen möchten.



Ergebnis

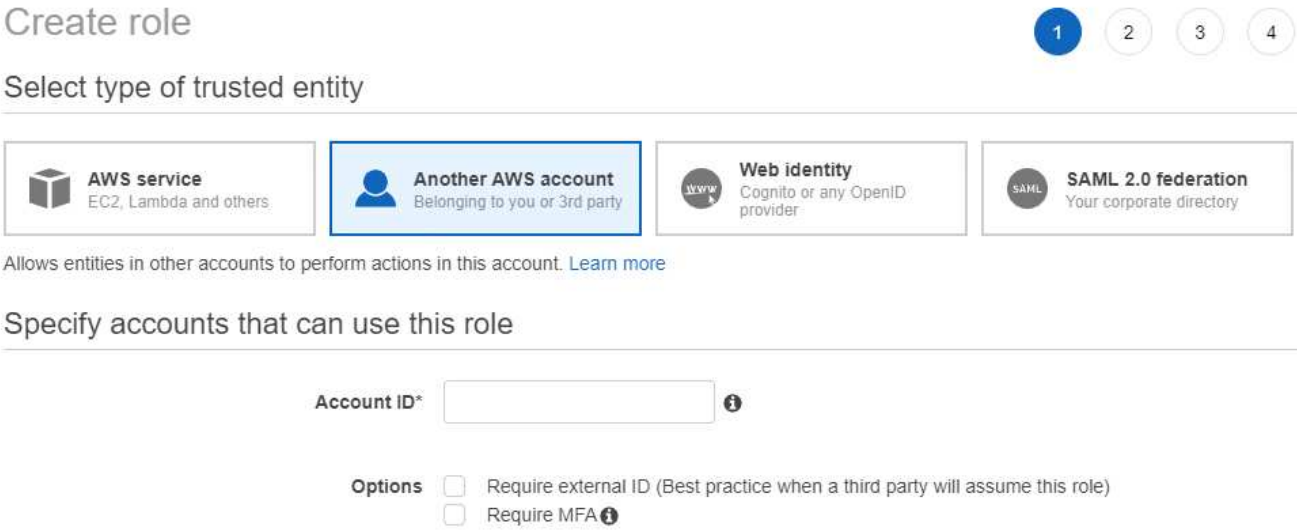
Cloud Compliance beginnt mit dem Scannen der aktivierten S3-Buckets. Wenn Fehler auftreten, werden sie neben der erforderlichen Aktion zur Behebung des Fehlers in der Spalte Status angezeigt.

Scannen von Buckets für weitere AWS Konten

Sie können S3-Buckets scannen, die sich unter einem anderen AWS-Konto befinden, indem Sie von diesem Konto eine Rolle zuweisen, um auf die vorhandene Cloud-Compliance-Instanz zuzugreifen.

Schritte

1. Gehen Sie zum AWS Ziel-Konto, in dem Sie S3 Buckets scannen 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-Compliance-Instanz befindet.
- Ändern Sie die maximale CLI/API-Sitzungsdauer* von 1 Stunde auf 12 Stunden und speichern Sie diese Änderung.
- Hängen Sie die Cloud Compliance IAM-Richtlinie an. Stellen Sie sicher, dass es über die erforderlichen Berechtigungen verfügt.

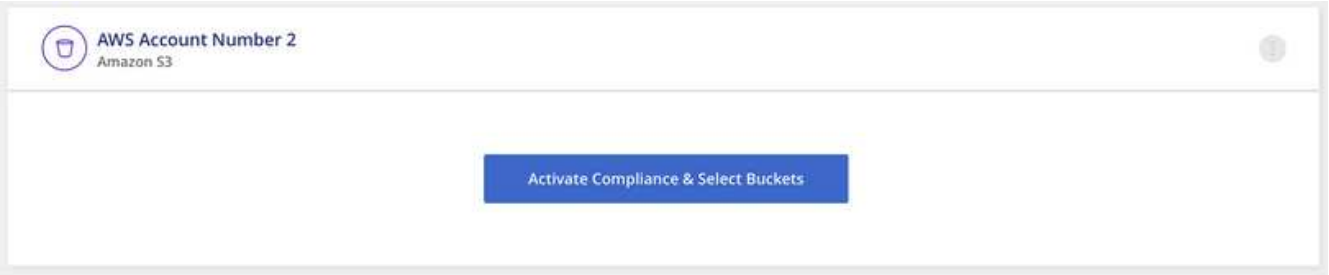
```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:HeadBucket"
          ],
          "Resource": "*"
      },
  ]
}
```

2. Wechseln Sie zum AWS Quellkonto, in dem sich die Cloud Compliance Instanz befindet, und wählen Sie die IAM-Rolle aus, die mit der Instanz verbunden ist.
   a. Ändern Sie die maximale CLI/API-Sitzungsdauer* von 1 Stunde auf 12 Stunden und speichern Sie diese Änderung.
   b. Klicken Sie auf **Richtlinien anhängen** und dann auf **Richtlinien erstellen**.
   c. Erstellen Sie eine Richtlinie, die die Aktion „STS:AssumeRole“ und den ARN der Rolle umfasst, die Sie im Zielkonto erstellt haben.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-
ID>:role/<ADDITIONAL_ROLE_NAME>"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/*",
                "arn:aws:iam::*:role/*"
            ]
        }
    ]
}
```

Das Instanzprofil für Cloud Compliance hat nun Zugriff auf das zusätzliche AWS Konto.

3. Gehen Sie auf die Seite **Amazon S3 Scan Configuration** und das neue AWS-Konto wird angezeigt. Beachten Sie, dass es einige Minuten dauern kann, bis Cloud Compliance die Arbeitsumgebung des neuen Kontos synchronisiert und diese Informationen anzeigt.



4. Klicken Sie auf **Compliance aktivieren & Buckets auswählen** und wählen Sie die Eimer aus, die Sie scannen möchten.

Ergebnis

Cloud Compliance beginnt mit dem Scannen der neuen aktivierten S3-Buckets.

Datenbankschemas werden gescannt

Führen Sie einige Schritte durch, um den Scan des Datenbankschemas mit Cloud

Compliance zu beginnen.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

Datenbankvoraussetzungen prüfen

Stellen Sie sicher, dass Ihre Datenbank unterstützt wird und dass Sie über die erforderlichen Informationen verfügen, um eine Verbindung zur Datenbank herzustellen.

Implementieren der Cloud Compliance-Instanz

"Cloud Compliance in Cloud Manager implementieren" Falls noch keine Instanz implementiert wurde.

Fügen Sie den Datenbankserver hinzu

Fügen Sie den Datenbankserver hinzu, auf den Sie zugreifen möchten.

Wählen Sie die Schemas aus

Wählen Sie die Schemata aus, die Sie scannen möchten.

Voraussetzungen prüfen

Die folgenden Voraussetzungen prüfen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie Cloud Compliance aktivieren.

Unterstützte Datenbanken

Cloud Compliance kann Schemen aus den folgenden Datenbanken scannen:

- MongoDB
- Oracle
- PostgreSQL
- SAP HANA
- SQL Server (MSSQL)

Die Statistik-Sammelfunktion *muss in der Datenbank aktiviert sein.

Datenbankanforderungen erfüllt

Jede Datenbank mit Anbindung an die Cloud Compliance-Instanz kann unabhängig vom gehosteten Speicherort gescannt werden. Sie benötigen lediglich die folgenden Informationen, um eine Verbindung zur Datenbank herzustellen:

- IP-Adresse oder Hostname
- Port
- Dienstname (nur für den Zugriff auf Oracle-Datenbanken)
- Anmeldeinformationen, die einen Lesezugriff auf die Schemas ermöglichen

  Bei der Auswahl eines Benutzernamens und Kennworts ist es wichtig, einen zu wählen, der volle Lese-Berechtigungen für alle Schemas und Tabellen, die Sie scannen möchten. Es wird empfohlen, einen dedizierten Benutzer für das Cloud Compliance-System mit allen erforderlichen Berechtigungen zu erstellen.

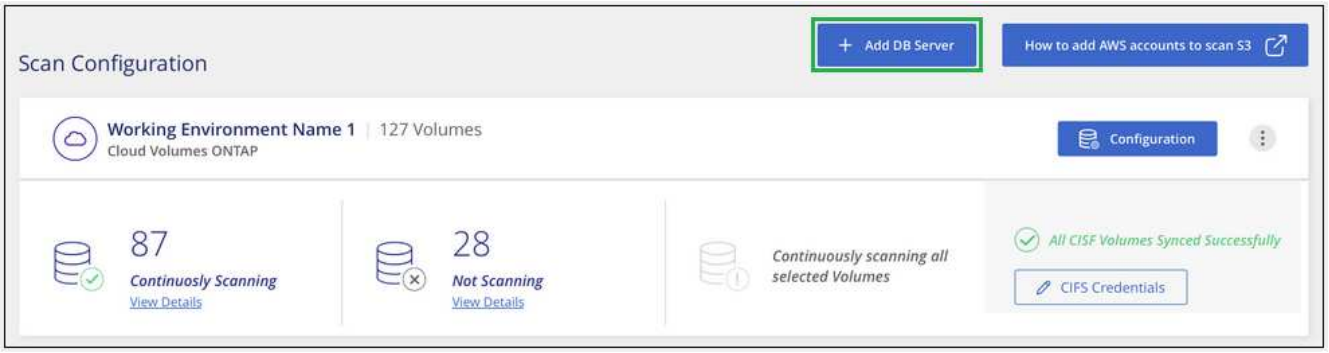
Hinweis: für MongoDB ist eine schreibgeschützte Administratorrolle erforderlich.

Hinzufügen des Datenbankservers

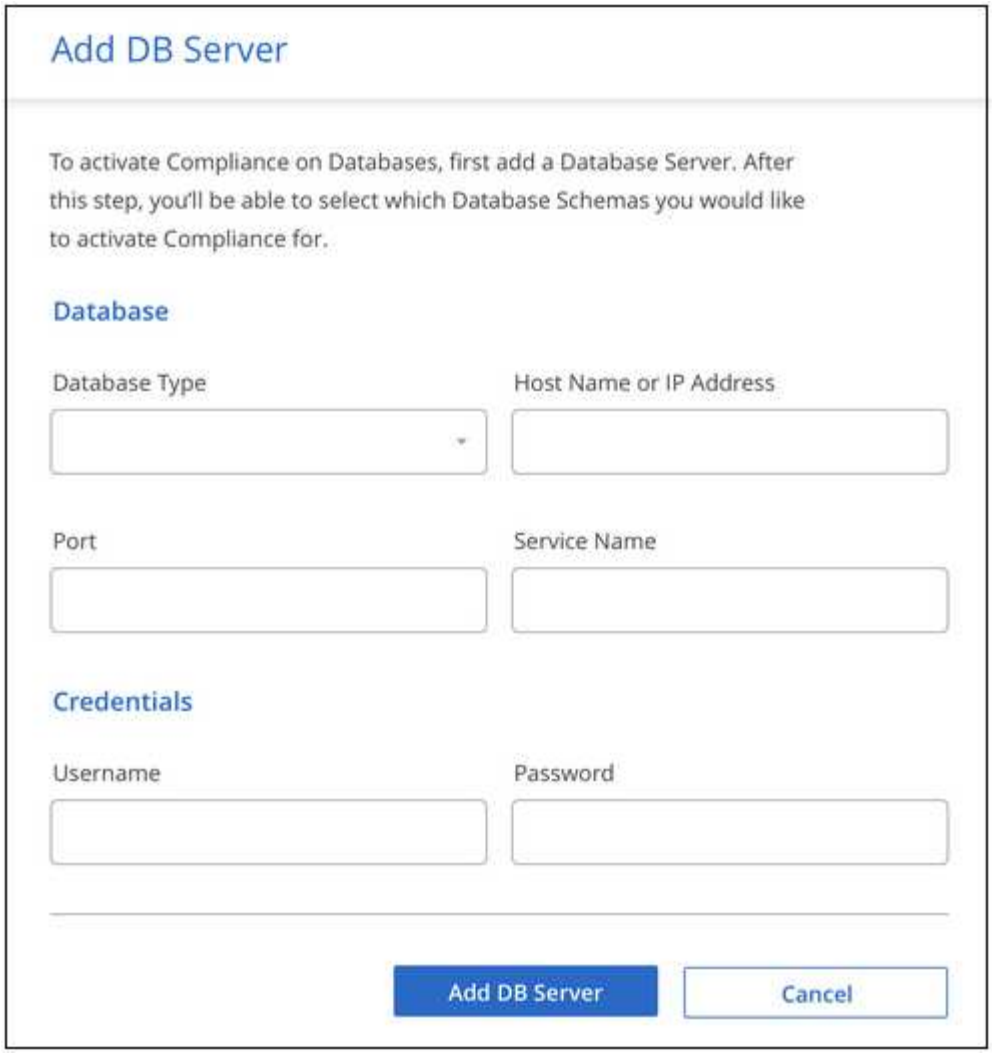
Dieser muss unbedingt vorhanden sein "Bereits eine Instanz von Cloud Compliance in Cloud Manager implementiert".

Fügen Sie den Datenbankserver dort hinzu, wo sich die Schemas befinden.

1. Klicken Sie auf der Seite *Scan Configuration* auf die Schaltfläche **DB Server hinzufügen**.



2. Geben Sie die erforderlichen Informationen ein, um den Datenbankserver zu identifizieren.
   a. Wählen Sie den Datenbanktyp aus.
   b. Geben Sie den Port und den Hostnamen oder die IP-Adresse ein, um eine Verbindung zur Datenbank herzustellen.
   c. Geben Sie für Oracle-Datenbanken den Dienstnamen ein.
   d. Geben Sie die Anmeldeinformationen ein, damit Cloud Compliance auf den Server zugreifen kann.
   e. Klicken Sie auf **DB-Server hinzufügen**.



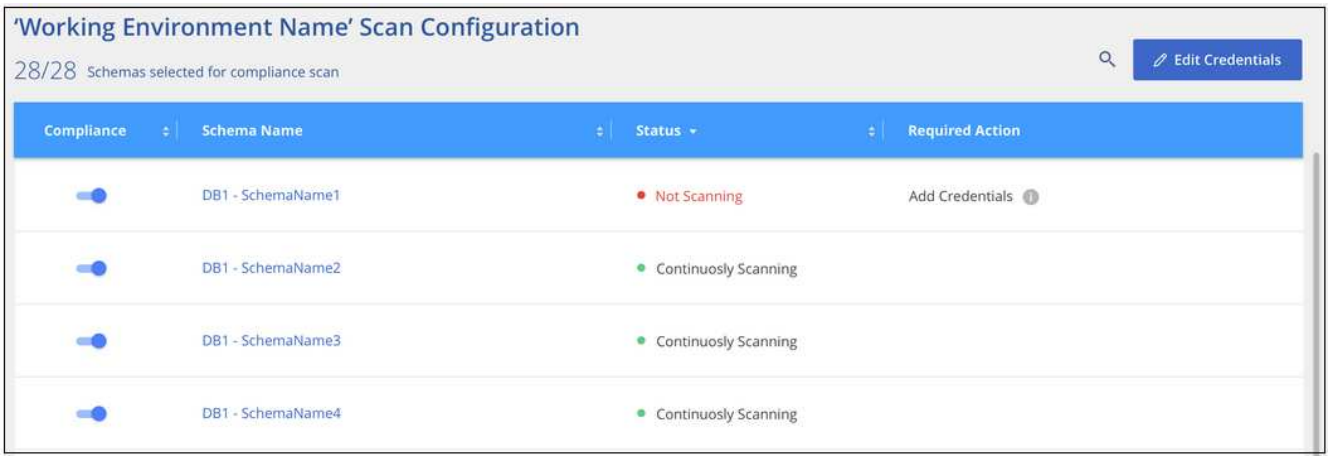
Die Datenbank wird der Liste der Arbeitsverzeichnisse hinzugefügt.

Aktivieren und Deaktivieren von Compliance-Scans auf Datenbankschemas

Sie können die Scanschemata jederzeit anhalten oder starten.

1. Klicken Sie auf der Seite *Scan Configuration* auf die Schaltfläche **Konfiguration** für die zu konfigurierende Datenbank.

2. Wählen Sie die Schemata aus, die Sie scannen möchten, indem Sie den Schieberegler nach rechts bewegen.



Ergebnis

Cloud Compliance beginnt mit dem Scannen der von Ihnen aktivierten Datenbankschemata. Wenn Fehler auftreten, werden sie in der Spalte Status angezeigt, neben der erforderlichen Aktion, um den Fehler zu beheben.

Entfernen einer Datenbank aus Cloud Manager

Wenn Sie eine bestimmte Datenbank nicht mehr scannen möchten, können Sie sie über die Cloud Manager Schnittstelle löschen und alle Scans anhalten.

Klicken Sie auf der Seite *Scan Configuration* auf Klicken Sie in der Zeile der Datenbank auf **DB Server entfernen**.

Scannen lokaler ONTAP Daten mit Cloud-Compliance mit SnapMirror

Sie können Ihre lokalen ONTAP-Daten mit Cloud-Compliance scannen, indem Sie die On-Premises-NFS- oder CIFS-Daten in eine Cloud Volumes ONTAP Arbeitsumgebung replizieren und damit Compliance sicherstellen. Das Scannen der Daten direkt aus einer lokalen ONTAP-Arbeitsumgebung wird nicht unterstützt.

Dieser muss unbedingt vorhanden sein "Bereits eine Instanz von Cloud Compliance in Cloud Manager implementiert".

Schritte

1. Erstellen Sie in Cloud Manager eine SnapMirror Beziehung zwischen dem lokalen ONTAP Cluster und Cloud Volumes ONTAP.

a. "Ermitteln des On-Premises-Clusters in Cloud Manager".

b. "Erstellen einer SnapMirror Replizierung zwischen dem lokalen ONTAP Cluster und Cloud Volumes ONTAP aus Cloud Manager".

2. Konfigurieren Sie bei DP-Volumes, die aus SMB-Quell-Volumes erstellt wurden, über die Befehlszeilenschnittstelle von ONTAP die SMB-Ziel-Volumes für den Datenzugriff. (Dies ist für NFS-Volumes nicht erforderlich, da der Datenzugriff automatisch über Cloud-Compliance aktiviert wird.)

   a. "SMB-Freigabe auf dem Ziel-Volume erstellen".

   b. "Wenden Sie die entsprechenden ACLs auf die SMB-Freigabe am Ziel-Volume an".

3. Aktivieren Sie über Cloud Manager Cloud Compliance in der Cloud Volumes ONTAP Arbeitsumgebung, die die SnapMirror Daten enthält:

   a. Klicken Sie Auf **Arbeitsumgebungen**.

   b. Wählen Sie die Arbeitsumgebung aus, die die SnapMirror Daten enthält, und klicken Sie auf **Compliance aktivieren**.

      "Klicken Sie hier, wenn Sie Hilfe bei der Aktivierung von Cloud-Compliance auf einem Cloud Volumes ONTAP System benötigen".

   c. Klicken Sie oben auf der Seite *Scan Configuration* auf die Schaltfläche **Zugriff auf DP-Volumes** aktivieren.

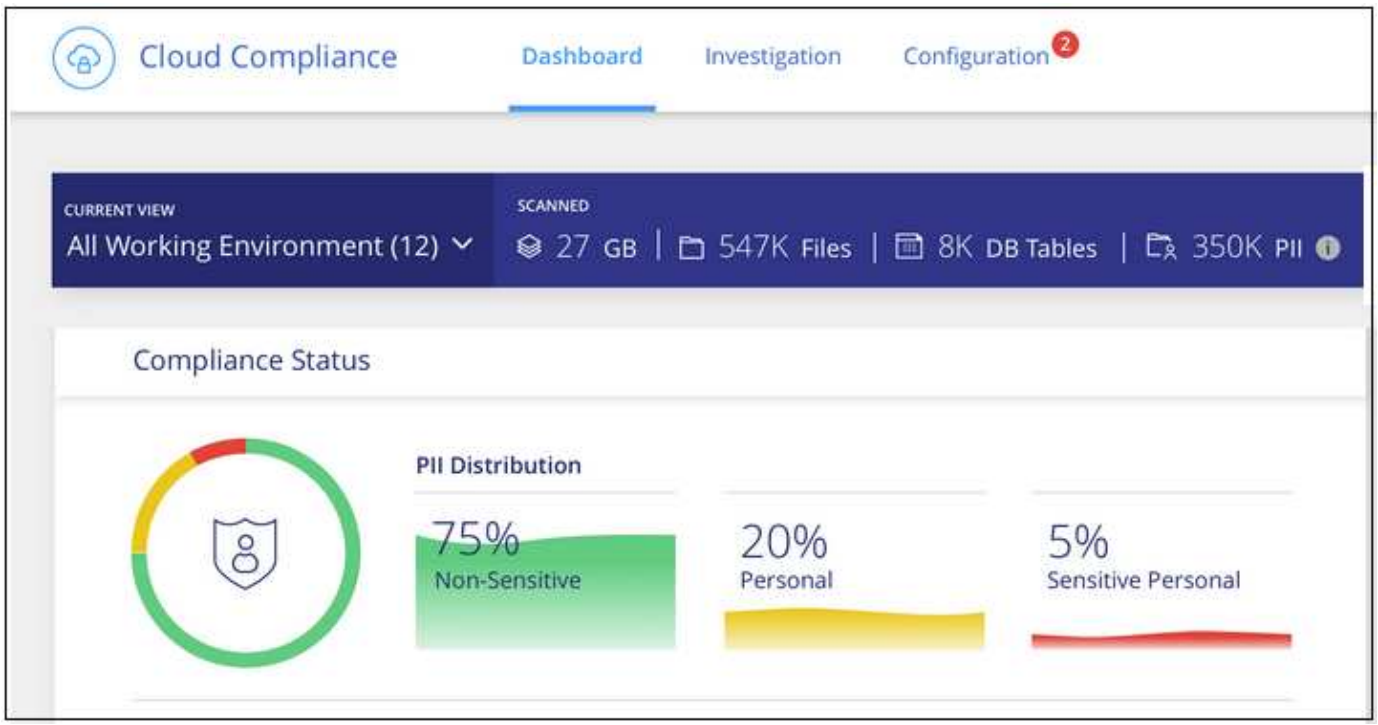
   d. Aktivieren Sie jedes DP-Volume, das Sie scannen möchten, oder verwenden Sie die Kontrolle **Compliance für alle Volumes aktivieren**, um alle Volumes, einschließlich aller DP-Volumes, zu aktivieren.

Siehe "Scannen von Datensicherungs-Volumes" Weitere Informationen zum Scannen von DP-Volumes.

Mehr Transparenz und Kontrolle über private Daten

Mehr Kontrolle über Ihre persönlichen Daten durch die Anzeige von Details zu den personenbezogenen Daten und vertraulichen personenbezogenen Daten in Ihrem Unternehmen. Auch die Kategorien und Dateitypen, die Cloud Compliance in Ihren Daten enthalten ist, können für Sie transparent dargestellt werden.

Standardmäßig werden auf dem Cloud Compliance-Dashboard Compliance-Daten für alle Arbeitsumgebungen und Datenbanken angezeigt.



Wenn Sie Daten nur für einige der Arbeitsumgebungen sehen möchten, Wählen Sie diese Arbeitsumgebungen aus.

Persönliche Daten

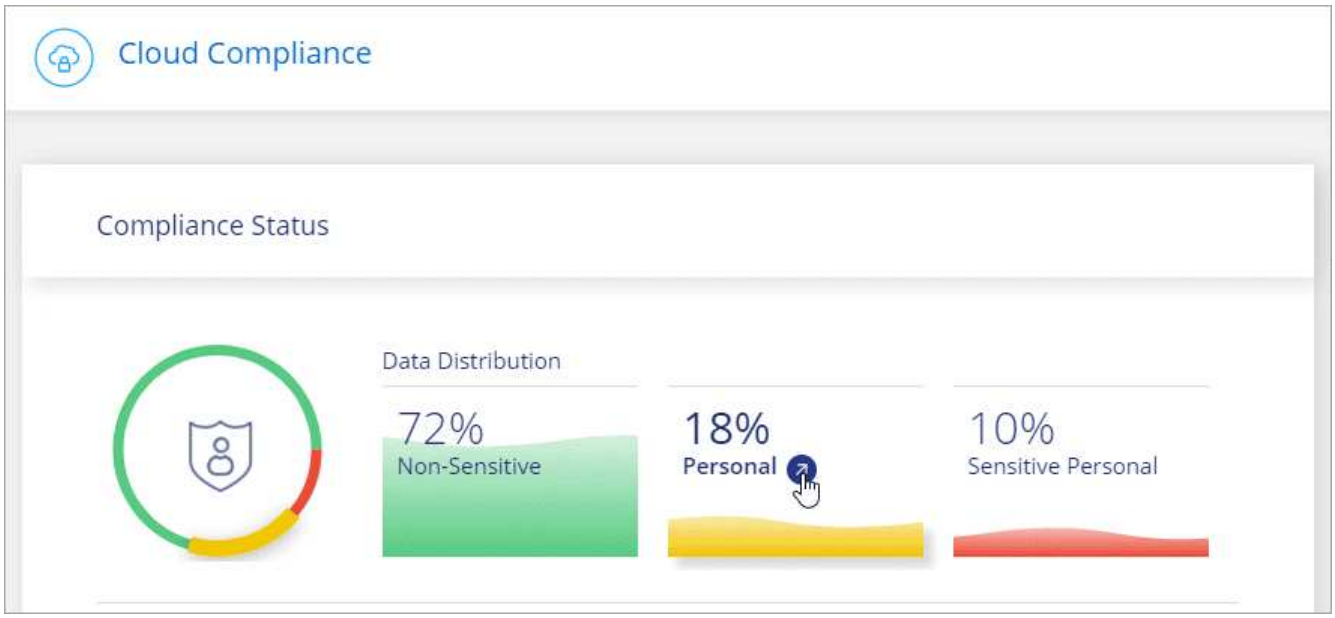
Cloud Compliance identifiziert automatisch bestimmte Wörter, Strings und Muster (Regex) in den Daten. Beispielsweise personenbezogene Daten (Personal Identification Information, PII), Kreditkartennummern, Sozialversicherungsnummern und Kontonummern. Die vollständige Liste finden Sie hier.

Für einige Arten von personenbezogenen Daten verwendet Cloud Compliance die *Proximity-Validierung*, um die Ergebnisse zu validieren. Die Validierung erfolgt, indem ein oder mehrere vordefinierte Schlüsselwörter in der Nähe der gefundenen personenbezogenen Daten gesucht werden. Cloud Compliance identifiziert z. B. eine US-amerikanische Sozialversicherungsnummer (SSN) als SSN, wenn sie neben ihr ein Näherungswort sieht - zum Beispiel *SSN* oder *Sozialversicherung*. Die Liste unten Zeigt an, wann Cloud Compliance die Näherungsüberprüfung verwendet.

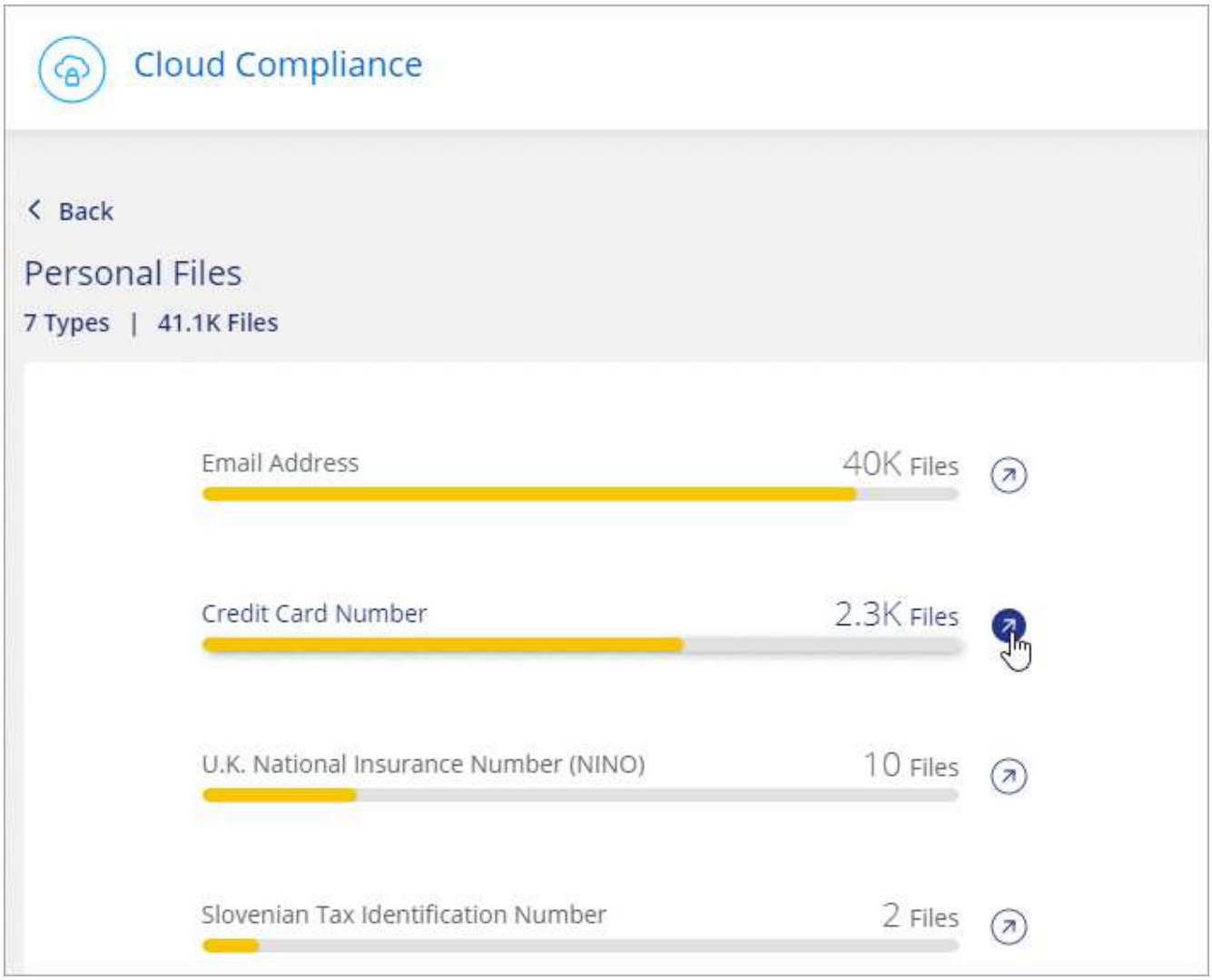
Anzeigen von Dateien mit persönlichen Daten

Schritte

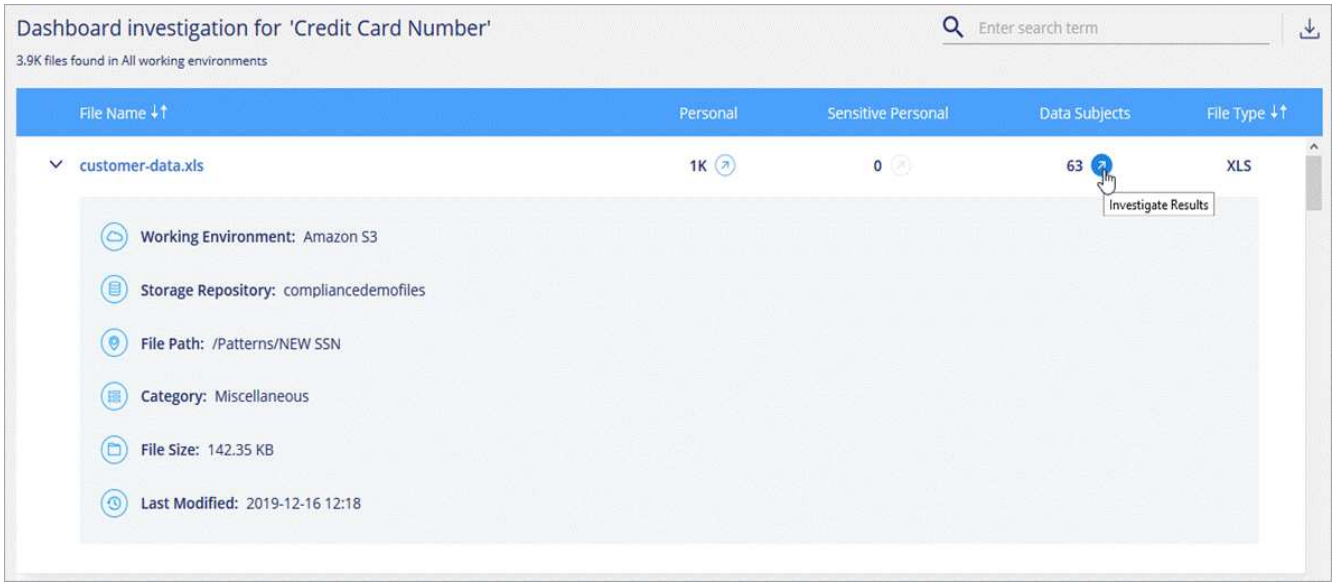
1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance** und klicken Sie auf die Registerkarte **Dashboard**.
2. Um die Angaben zu allen personenbezogenen Daten zu untersuchen, klicken Sie auf das Symbol neben dem Prozentsatz der persönlichen Daten.



3. Um die Daten für eine bestimmte Art von personenbezogenen Daten zu untersuchen, klicken Sie auf **Alle anzeigen** und dann auf das Symbol **Ergebnisse untersuchen** für einen bestimmten Typ von personenbezogenen Daten.

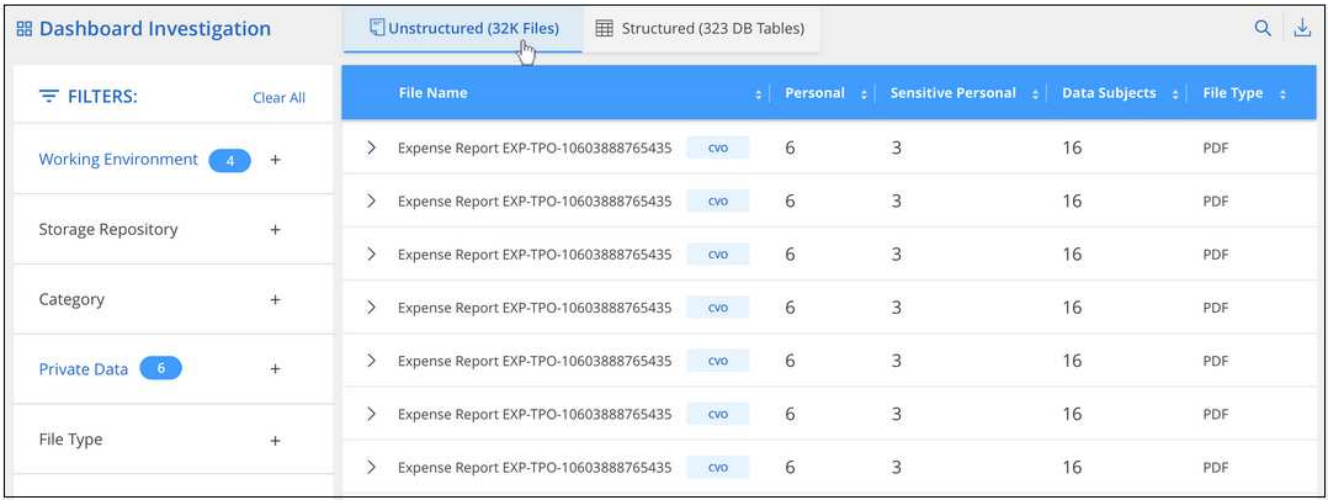


4. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die Dateiliste herunter.



5. Sie können den Inhalt der Untersuchungsseite auch so filtern, dass nur die Ergebnisse angezeigt werden, die angezeigt werden sollen. Auf den Registerkarten der obersten Ebene können Sie Daten aus Dateien (unstrukturierte Daten) oder aus Datenbanken (strukturierte Daten) anzeigen.

   Dann haben Sie Filter für die Arbeitsumgebung, das Storage-Repository, die Kategorie, die privaten Daten, den Dateityp, Datum der letzten Änderung und ob die Berechtigungen des S3-Objekts für den öffentlichen Zugriff zugänglich sind.



Arten personenbezogener Daten

Die in Dateien gefundenen personenbezogenen Daten können allgemeine personenbezogene Daten oder nationale Kennungen sein. In der dritten Spalte wird angegeben, ob Cloud Compliance verwendet wird Prüfung der Nähe Zum Validieren seiner Ergebnisse für die Kennung.

Typ	Kennung	Näherungsvalidierung?
Allgemein	E-Mail-Adresse	Nein
	Kreditkartennummer	Nein
	IBAN-Nummer (International Bank Account Number)	Nein

Typ	Kennung	Näherungsvalidierung?
Nationale Kennungen	Belgischer Ausweis (Numero National)	Ja.
	Brasilianischer Ausweis (CPF)	Ja.
	Bulgarische ID (UCN)	Ja.
	California Driver's License	Ja.
	Kroatische ID (OIB)	Ja.
	Zypern Steuernummer (TIC)	Ja.
	Tschechische/Slowakische Ausweisnummer	Ja.
	Dänische ID (HLW)	Ja.
	Niederländische ID (BSN)	Ja.
	Estnische ID	Ja.
	Finnische ID (HETU)	Ja.
	Französische Steuernummer (SPI)	Ja.
	Steuernummer (Steuerliche Identifikationsnummer)	Ja.
	Griechische ID	Ja.
	Ungarische Steuernummer	Ja.
	Irish ID (PPS)	Ja.
	Israelische ID	Ja.
	Italienische Steuernummer	Ja.
	Lettischer Ausweis	Ja.
	Litauische ID	Ja.
	Luxemburg-ID	Ja.
	Maltesische ID	Ja.
	Polish ID (PESEL)	Ja.
	Portugiesische Steuernummer (NIF)	Ja.
	Rumänische ID (CNP)	Ja.
	Slowenische ID (EMSO)	Ja.
	Südafrikanischer Ausweis	Ja.
	Spanische Steuernummer	Ja.
	Schwedische ID	Ja.
	GROSSBRITANNIEN ID (NINO)	Ja.
	USA Sozialversicherungsnummer (SSN)	Ja.

Sensible persönliche Daten

Cloud Compliance identifiziert automatisch spezielle Arten von sensiblen personenbezogenen Daten, wie sie in Datenschutzvorschriften wie z. B. definiert sind "Artikel 9 und 10 der DSGVO". Beispielsweise Informationen über die Gesundheit einer Person, ethnische Herkunft oder sexuelle Orientierung. Die vollständige Liste finden Sie hier.

Cloud Compliance verwendet künstliche Intelligenz (KI), NLP (Natural Language Processing), maschinelles Lernen (ML) und Cognitive Computing (CC), um die Bedeutung des von ihm gescannten Inhalts zu verstehen, um Entitäten zu extrahieren und entsprechend zu kategorisieren.

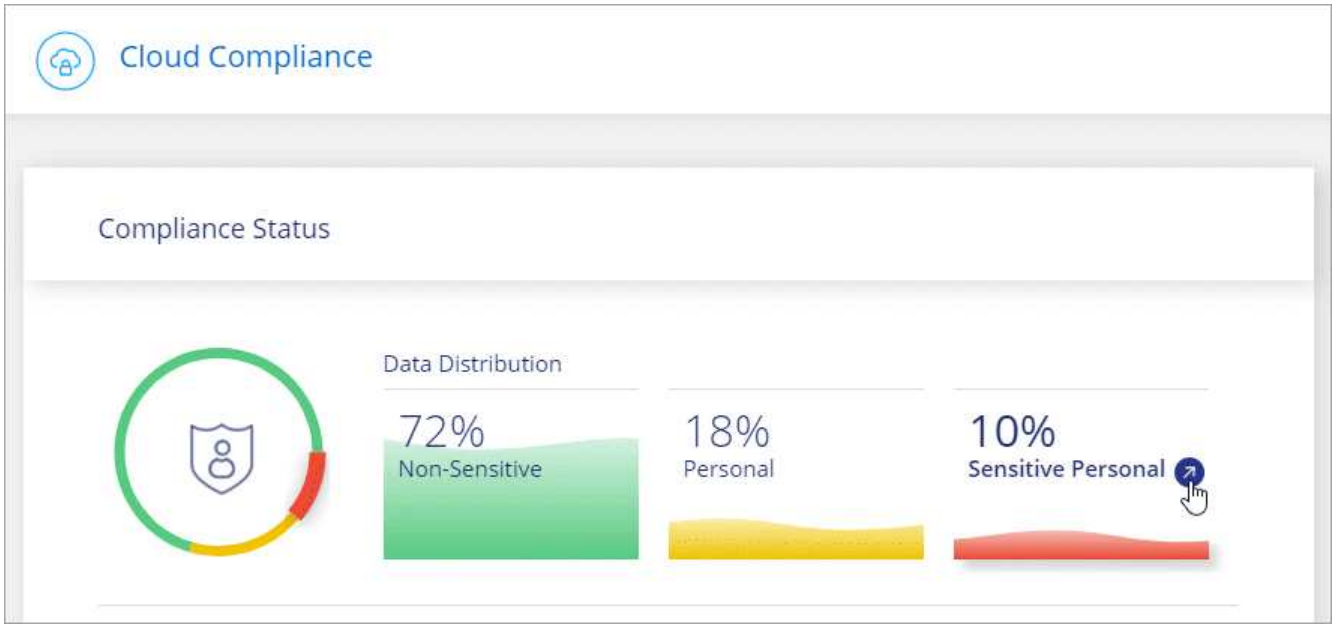
Beispielsweise ist eine sensitive DSGVO-Datenkategorie ethnisch Ursprungs. Aufgrund seiner NLP-Fähigkeiten kann Cloud Compliance den Unterschied zwischen einem Satz unterscheiden, der "George ist mexikanisch" (was auf sensible Daten wie in Artikel 9 der DSGVO angegeben), und "George isst mexikanisches Essen".

Nur Englisch wird beim Scannen sensibler personenbezogener Daten unterstützt. Support für weitere Sprachen wird später hinzugefügt.

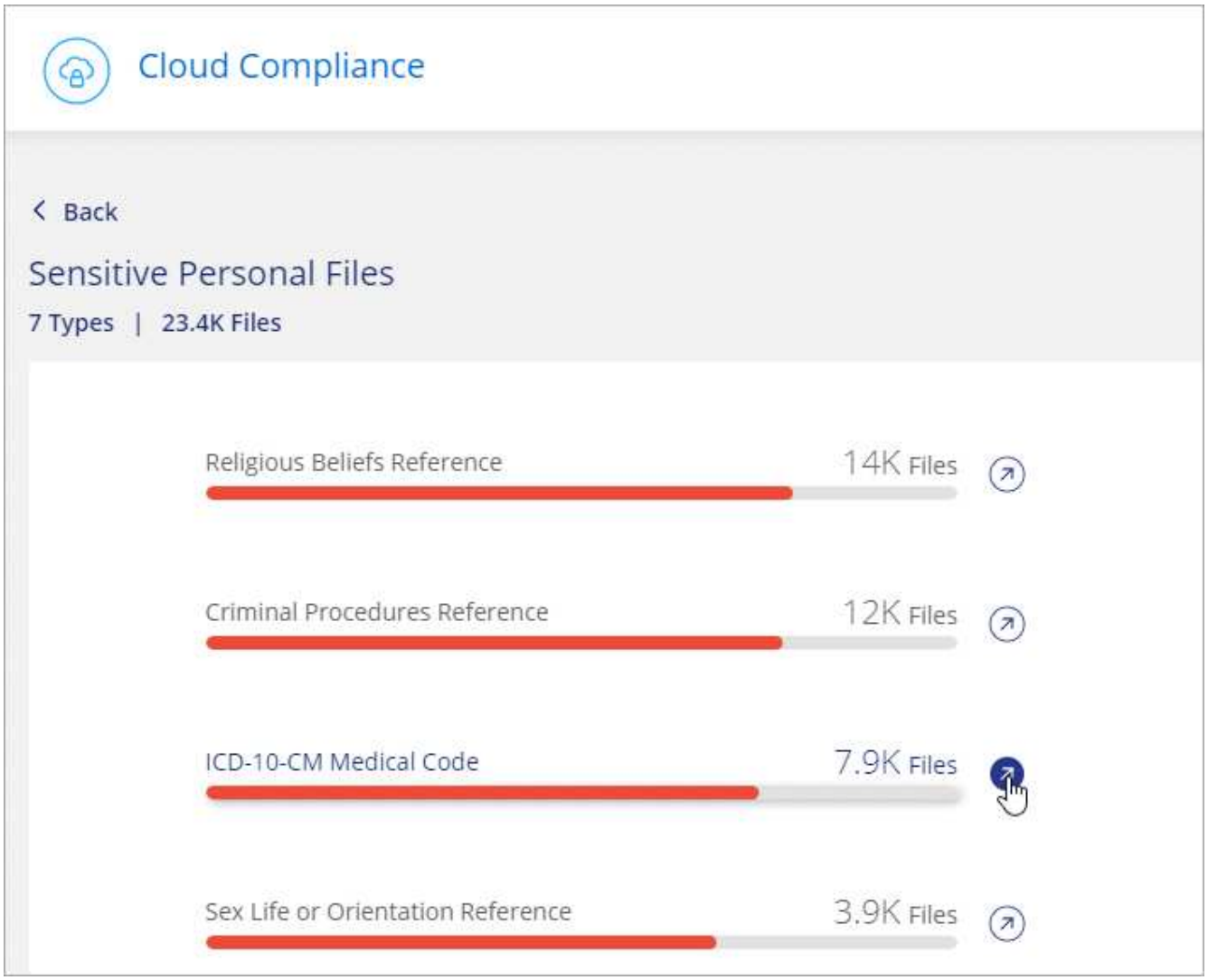
Anzeigen von Dateien mit vertraulichen persönlichen Daten

Schritte

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
2. Um die Details für alle sensiblen persönlichen Daten zu untersuchen, klicken Sie auf das Symbol neben dem Prozentsatz sensibler personenbezogener Daten.



3. Um die Details für eine bestimmte Art sensibler personenbezogener Daten zu untersuchen, klicken Sie auf **Alle anzeigen** und klicken Sie dann auf das Symbol **Ergebnisse untersuchen** für einen bestimmten Typ sensibler personenbezogener Daten.



4. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die Dateiliste herunter.

Arten sensibler personenbezogener Daten

Folgende sensible personenbezogene Daten, die Cloud Compliance in Dateien finden kann:

Referenz Für Kriminelle Verfahren
Daten zu strafrechtlichen Überzeugungen und Straftaten einer natürlichen Person.

Ethnische Referenz
Daten über die rassische oder ethnische Herkunft einer natürlichen Person.

Systemzustand
Daten über die Gesundheit einer natürlichen Person.

ICD-9-CM-Ärztliche Codes
Codes, die in der Medizin- und Gesundheitsbranche verwendet werden.

ICD-10-CM-Ärztliche Codes

Codes, die in der Medizin- und Gesundheitsbranche verwendet werden.

Philosophische Überzeugungen Referenz

Daten über die philosophischen Überzeugungen einer natürlichen Person.

Religiöse Überzeugungen Referenz

Daten über die religiösen Überzeugungen einer natürlichen Person.

Sexualleben oder Orientierung Referenz

Daten über das Sexualleben einer natürlichen Person oder die sexuelle Orientierung.

Kategorien

Bei Cloud Compliance werden die gescannten Daten in verschiedene Kategorien unterteilt. Kategorien sind Themen, die auf der KI-Analyse des Inhalts und der Metadaten jeder Datei basieren. Siehe die Liste der Kategorien.

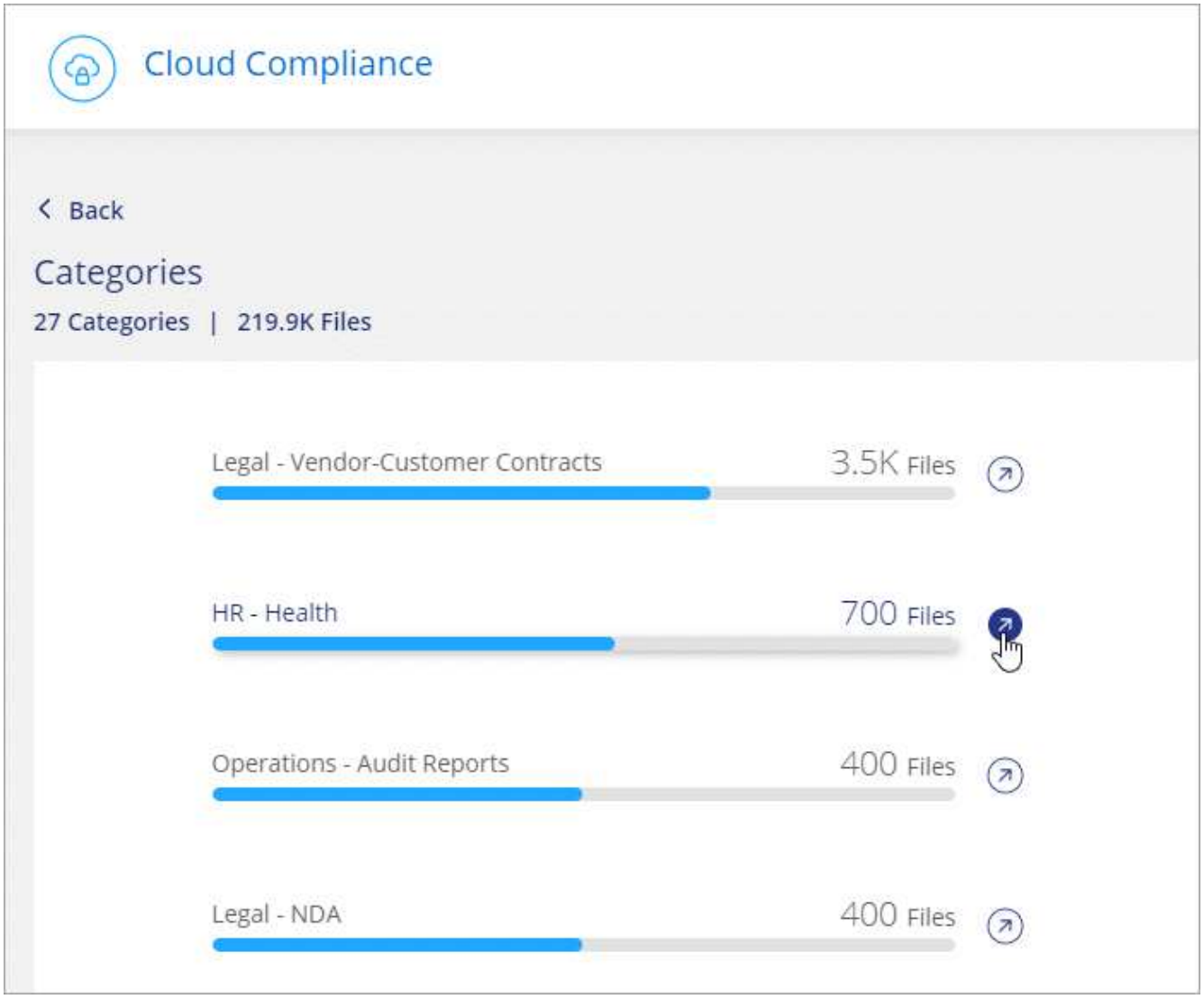
Kategorien können Ihnen dabei helfen zu verstehen, was mit Ihren Daten passiert, indem Sie die Arten von Informationen anzeigen, die Sie haben. Beispielsweise kann eine Kategorie wie Lebensläufe oder Mitarbeiterverträge sensible Daten enthalten. Wenn Sie die Ergebnisse untersuchen, können Sie feststellen, dass Mitarbeiterverträge an einem unsicheren Ort gespeichert sind. Sie können das Problem dann beheben.

Nur Englisch wird für Kategorien unterstützt. Support für weitere Sprachen wird später hinzugefügt.

Anzeigen von Dateien nach Kategorien

Schritte

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
2. Klicken Sie auf das Symbol **Ergebnisse untersuchen** für eine der 4 Top-Kategorien direkt im Hauptbildschirm oder klicken Sie auf **Alle anzeigen** und dann auf das Symbol für eine der Kategorien.



3. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die Dateiliste herunter.

Arten von Kategorien

Cloud Compliance kategorisiert Ihre Daten wie folgt:

Finanzen

- Bilanz
- Bestellungen
- Rechnungen
- Vierteljährliche Berichte

HR

- Background-Checks
- Vergütungspläne
- Mitarbeiterverträge

- Mitarbeiterbewertung
- Systemzustand
- Wird Fortgesetzt

Legal
- NDAs
- Verträge zwischen Anbietern und Kunden

Marketing
- Kampagnen
- Konferenzen

Betrieb
- Audit-Berichte

Vertrieb
- Aufträge

Services
- RFI
- AUSSCHREIBUNG
- SOW
- Schulung

Unterstützung
- Reklamationen und Tickets

Metadatenkategorien
- Applikationsdaten
- Archivdateien
- Audio
- Daten Von Business-Applikationen
- CAD-Dateien
- Codieren
- Datenbank- und Indexdateien
- Design-Dateien
- E-Mail-Anwendungsdaten
- Ausführbare Dateien
- Daten Aus Finanzapplikationen
- Daten Der Integritätsanwendungen
- Bilder
- Protokolle
- Verschiedene Dokumente

- Diverse Präsentationen
- Verschiedene Tabellenkalkulationen
- Videos

Dateitypen

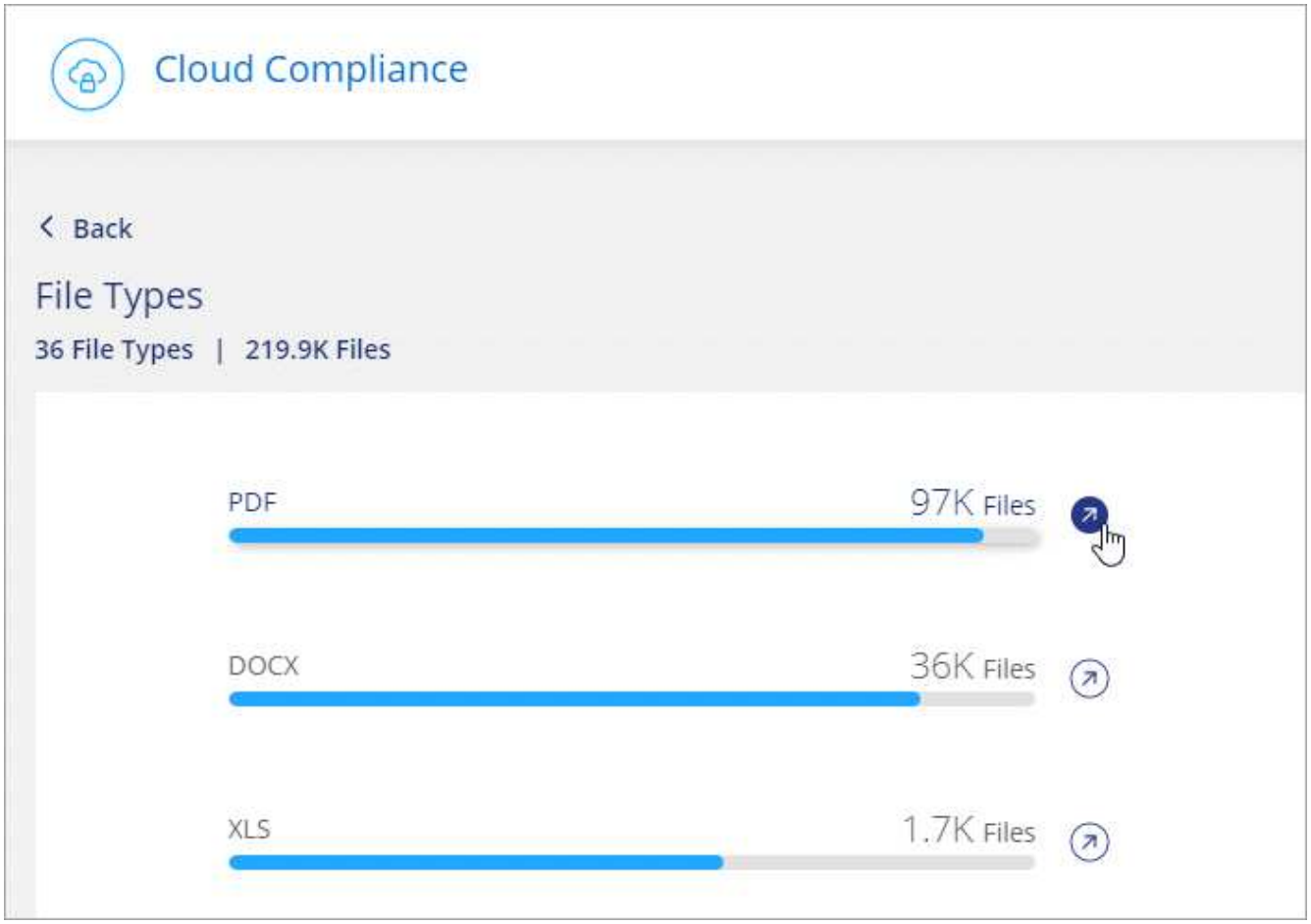
Cloud Compliance greift die gescannten Daten auf und legt sie nach Dateityp fest. Die Überprüfung Ihrer Dateitypen kann Ihnen helfen, Ihre sensiblen Daten zu kontrollieren, da Sie möglicherweise feststellen können, dass bestimmte Dateitypen nicht richtig gespeichert sind. Siehe die Liste der Dateitypen.

Sie können beispielsweise CAD-Dateien speichern, die sehr sensible Informationen über Ihr Unternehmen enthalten. Wenn diese nicht gesichert sind, können Sie die Kontrolle über vertrauliche Daten übernehmen, indem Sie Berechtigungen beschränken oder Dateien an einen anderen Speicherort verschieben.

Anzeigen von Dateitypen

Schritte

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
2. Klicken Sie auf das Symbol **Ergebnisse untersuchen** für einen der 4 wichtigsten Dateitypen direkt vom Hauptbildschirm aus, oder klicken Sie auf **Alle anzeigen** und dann auf das Symbol für einen der Dateitypen.



3. Untersuchen Sie die Daten, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern, auf **Ergebnisse untersuchen** klicken, um maskierte Informationen anzuzeigen, oder laden Sie die

Dateiliste herunter.

Dateitypen

Cloud Compliance scannt alle Dateien nach Informationen zu Kategorien und Metadaten und zeigt alle Dateitypen im Abschnitt Dateitypen im Dashboard an.

Wenn aber Cloud Compliance personenbezogene Daten (PII) erkennt oder eine DSAR-Suche durchführt, werden nur die folgenden Dateiformate unterstützt: .PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF UND .JSON.

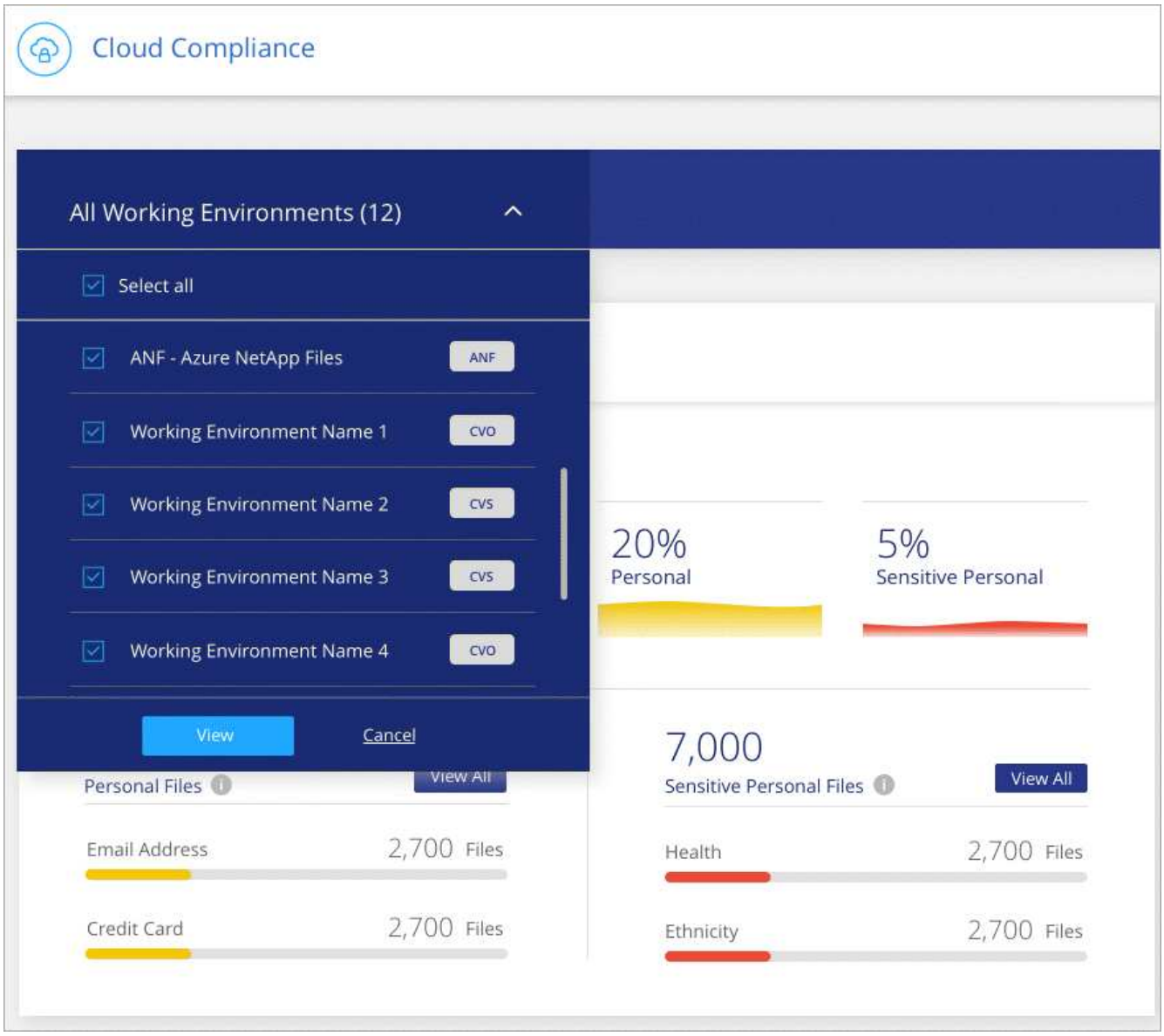
Anzeigen von Daten aus bestimmten Arbeitsumgebungen

Sie können die Inhalte des Cloud Compliance Dashboards filtern, um Compliance-Daten für alle Arbeitsumgebungen und Datenbanken oder nur für bestimmte Arbeitsumgebungen anzuzeigen.

Wenn Sie das Dashboard filtern, wird durch Cloud Compliance die Compliance-Daten und -Berichte genau den von Ihnen ausgewählten Arbeitsumgebungen beschrieben.

Schritte

1. Klicken Sie auf das Dropdown-Menü Filter, wählen Sie die Arbeitsumgebungen aus, für die Sie Daten anzeigen möchten, und klicken Sie auf **Ansicht**.



Genauigkeit der gefundenen Informationen

NetApp kann keine Garantie für 100 % Genauigkeit der persönlichen Daten und für sensible personenbezogene Daten, die Cloud Compliance identifiziert hat, geben. Überprüfen Sie die Informationen immer, indem Sie die Daten überprüfen.

Auf der Grundlage unserer Tests zeigt die folgende Tabelle die Richtigkeit der Informationen, die Cloud Compliance findet. Wir brechen es durch *Precision* und *Recall* ab:

Präzision

Die Wahrscheinlichkeit, dass das, was Cloud Compliance findet, korrekt identifiziert wurde. Beispielsweise bedeutet eine Datengenauigkeit von 90% für personenbezogene Daten, dass 9 von 10 Dateien, die als personenbezogene Daten identifiziert werden, tatsächlich personenbezogene Daten enthalten. 1 von 10 Dateien wäre falsch positiv.

Rückruf

Die Wahrscheinlichkeit, dass Cloud Compliance die entsprechenden Daten findet Beispielsweise bedeutet eine Rückrufquote von 70 % für personenbezogene Daten, dass Cloud Compliance 7 von 10 Dateien

identifizieren kann, die tatsächlich personenbezogene Daten in Ihrem Unternehmen enthalten. Cloud Compliance würde 30% der Daten vermissen und wird nicht im Dashboard erscheinen.

Cloud Compliance gibt es in einer Version mit kontrollierter Verfügbarkeit und wir verbessern kontinuierlich die Genauigkeit unserer Ergebnisse. Diese Verbesserungen werden in zukünftigen Versionen der Cloud-Compliance automatisch verfügbar sein.

Typ	Präzision	Rückruf
Personenbezogene Daten - Allgemeines	90 % - 95 %	60 % - 80 %
Persönliche Daten – Länderkennungen	30 % - 60 %	40 % - 60 %
Sensible persönliche Daten	80 % - 95 %	20 % - 30 %
Kategorien	90 % - 97 %	60 % - 80 %

Was ist in jedem Datei Liste Bericht enthalten (CSV-Datei)

Auf jeder Untersuchungsseite können Sie Dateilisten (im CSV-Format) mit Details zu den identifizierten Dateien herunterladen. Wenn es mehr als 10,000 Ergebnisse gibt, werden nur die Top 10,000 in der Liste angezeigt.

Jede Dateiliste enthält die folgenden Informationen:

- Dateiname
- Positionstyp
- Arbeitsumgebung
- Storage Repository
- Protokoll
- Dateipfad
- Dateityp
- Kategorie
- Persönliche Angaben
- Sensible persönliche Daten
- Löscherkennung Datum

  Ein Löscherkennungsdatum gibt das Datum an, an dem die Datei gelöscht oder verschoben wurde. So können Sie feststellen, wann sensible Dateien verschoben wurden. Gelöschte Dateien sind nicht Teil der Anzahl der Dateinummern, die im Dashboard oder auf der Untersuchungsseite angezeigt wird. Die Dateien werden nur in den CSV-Berichten angezeigt.

Anzeigen von Compliance-Berichten

Cloud Compliance stellt Berichte bereit, anhand deren Sie den Status des Datenschutzprogramms Ihres Unternehmens besser verstehen können.

Standardmäßig werden auf dem Cloud Compliance-Dashboard Compliance-Daten für alle Arbeitsumgebungen und Datenbanken angezeigt. Wenn Sie Berichte anzeigen möchten, die Daten nur für einige Arbeitsumgebungen enthalten, Wählen Sie diese Arbeitsumgebungen aus.

NetApp kann keine Garantie für 100 % Genauigkeit der persönlichen Daten und für sensible personenbezogene Daten, die Cloud Compliance identifiziert hat, geben. Überprüfen Sie die Informationen immer, indem Sie die Daten überprüfen.

Datenschutzrisiko-Assessment-Bericht

Der Datenschutzrisiko-Assessment-Bericht bietet einen Überblick über den Datenschutzrisikostatus Ihres Unternehmens, wie dies durch Datenschutzvorschriften wie DSGVO und CCPA erforderlich ist. Der Bericht enthält die folgenden Informationen:

Compliance-Status

A Schweregrad Und die Verteilung von Daten, ganz gleich, ob es sich um unempfindliche, personenbezogene oder sensible Daten handelt.

Assessment-Übersicht

Eine Aufschlüsselung der gefundenen Arten von personenbezogenen Daten sowie der Kategorien von Daten.

Betroffene in dieser Beurteilung

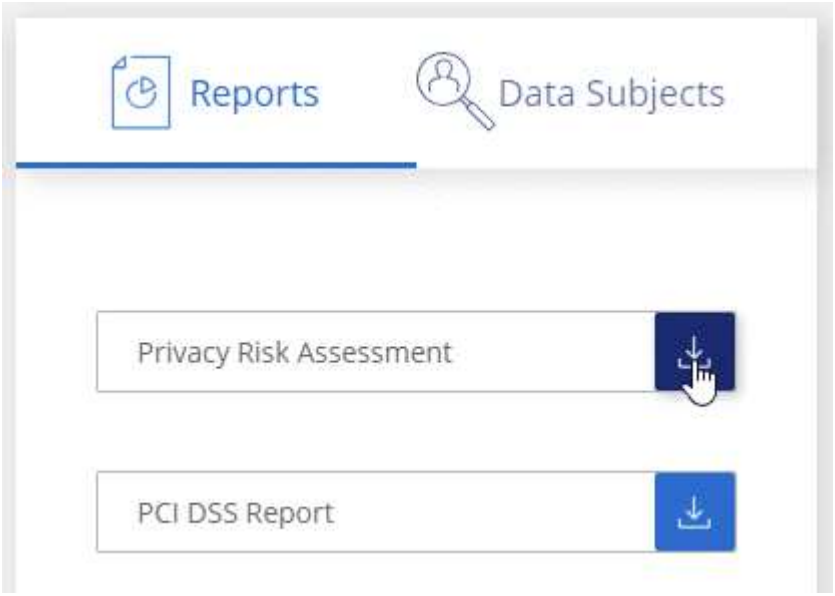
Die Anzahl der Personen, nach Ort, für die nationale Kennungen gefunden wurden.

Generieren des Datenschutzrisikobewertungsberichts

Rufen Sie die Registerkarte Compliance auf, um den Bericht zu erstellen.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
2. Klicken Sie unter **Reports** auf das Download-Symbol neben **Privacy Risk Assessment**.



Ergebnis

Cloud Compliance generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

Schweregrad

Cloud Compliance berechnet den Schweregrad für den Privacy Risk Assessment-Bericht auf der Grundlage von drei Variablen:

- Der Prozentsatz der personenbezogenen Daten aus allen Daten.
- Der Prozentsatz sensibler personenbezogener Daten aus allen Daten.
- Der Prozentsatz der Dateien, die betroffene Daten enthalten, die durch nationale Kennungen wie nationale IDs, Sozialversicherungsnummern und Steuerkennzahlen bestimmt werden.

Die folgende Logik dient zur Ermittlung der Punktzahl:

Schweregrad	Logik
0	Alle drei Variablen sind genau 0%
1	Eine der Variablen ist größer als 0 %
2	Eine der Variablen ist größer als 3%
3	Zwei der Variablen sind größer als 3%
4	Drei der Variablen sind größer als 3 %
5	Eine der Variablen ist größer als 6%
6	Zwei der Variablen sind größer als 6%
7	Drei der Variablen sind größer als 6 %
8	Eine der Variablen ist größer als 15%
9	Zwei der Variablen sind größer als 15%
10	Drei der Variablen sind größer als 15 %

PCI DSS-Bericht

Der PCI DSS-Bericht (Payment Card Industry Data Security Standard) hilft Ihnen bei der Identifizierung der Verteilung von Kreditkarteninformationen über Ihre Dateien hinweg. Der Bericht enthält die folgenden Informationen:

Überblick

Wie viele Dateien enthalten Kreditkarteninformationen und in welchen Arbeitsumgebungen.

Verschlüsselung

Der Prozentsatz der Dateien, die Kreditkartendaten in verschlüsselten oder nicht verschlüsselten Arbeitsumgebungen enthalten. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Schutz Vor Ransomware

Der Prozentsatz von Dateien mit Kreditkarteninformationen, die in Arbeitsumgebungen gespeichert sind, für die der Ransomware-Schutz aktiviert ist oder nicht. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Aufbewahrung

Der Zeitrahmen, in dem die Dateien zuletzt geändert wurden. Dies ist hilfreich, weil Sie Ihre Kreditkartendaten nicht länger aufbewahren sollten, als Sie sie bearbeiten müssen.

Verteilung der Kreditkarteninformationen

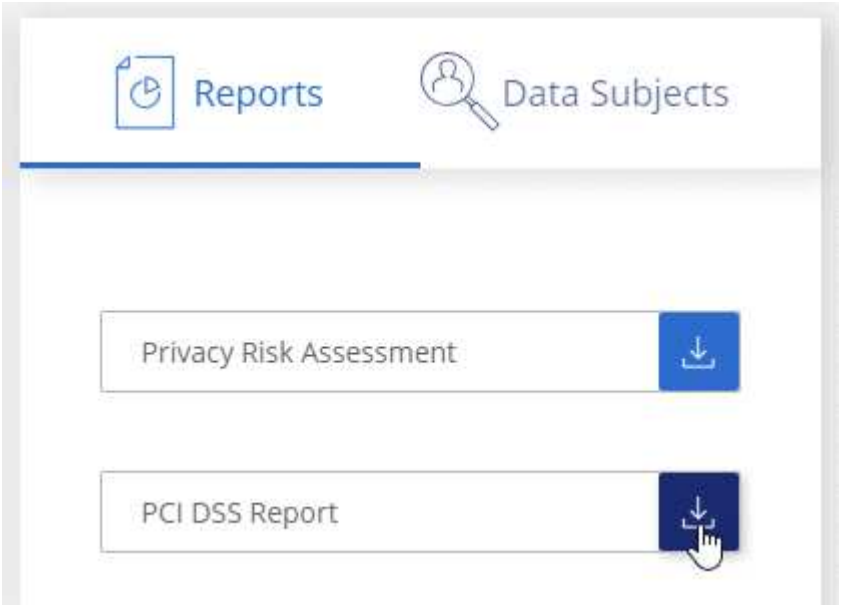
Die Arbeitsumgebungen, in denen Kreditkartendaten gefunden wurden und ob Verschlüsselung und Ransomware-Schutz aktiviert sind.

PCI DSS-Bericht wird erstellt

Rufen Sie die Registerkarte Compliance auf, um den Bericht zu erstellen.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
2. Klicken Sie unter **Reports** auf das Download-Symbol neben **PCI DSS Report**.



Ergebnis

Cloud Compliance generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

HIPAA-Bericht

Der HIPAA-Bericht (Health Insurance Portability and Accountability Act) hilft Ihnen bei der Identifizierung von Dateien, die Gesundheitsdaten enthalten. Es wurde entwickelt, um die Anforderung Ihres Unternehmens zu unterstützen, die HIPAA-Datenschutzgesetze einzuhalten. Die von Cloud Compliance gesucht werden, umfasst:

- Zustandsreferenzmuster
- ICD-10 CM medizinischer Code
- ICD-9 CM medizinischer Code
- HR – Kategorie Gesundheit
- Datenkategorie für Gesundheitsanwendungen

Der Bericht enthält die folgenden Informationen:

Überblick

Wie viele Dateien enthalten Gesundheitsinformationen und in welchen Arbeitsumgebungen.

Verschlüsselung

Der Prozentsatz der Dateien, die Gesundheitsinformationen in verschlüsselten oder nicht verschlüsselten Arbeitsumgebungen enthalten. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Schutz Vor Ransomware

Der Prozentsatz von Dateien mit Gesundheitsinformationen in Arbeitsumgebungen, in denen Ransomware-Schutz aktiviert ist oder nicht. Diese Informationen sind spezifisch für Cloud Volumes ONTAP.

Aufbewahrung

Der Zeitrahmen, in dem die Dateien zuletzt geändert wurden. Dies ist hilfreich, weil Sie Gesundheitsinformationen nicht länger aufbewahren sollten, als Sie sie verarbeiten müssen.

Verteilung von Gesundheitsinformationen

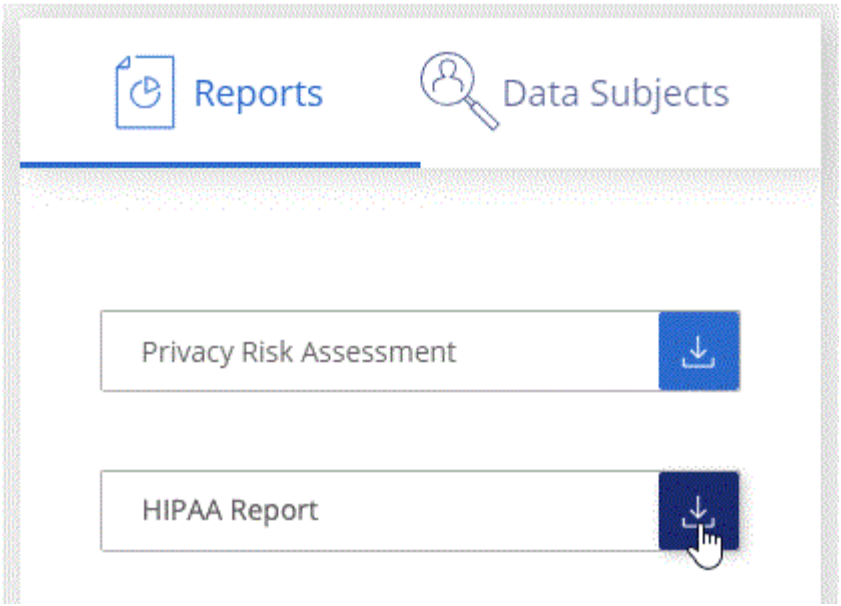
In den Arbeitsumgebungen, in denen die Gesundheitsdaten gefunden wurden und ob Verschlüsselung und Ransomware-Schutz aktiviert sind.

HIPAA-Bericht wird erstellt

Rufen Sie die Registerkarte Compliance auf, um den Bericht zu erstellen.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
2. Klicken Sie unter **Reports** auf das Download-Symbol neben **HIPAA Report**.



Ergebnis

Cloud Compliance generiert einen PDF-Bericht, den Sie nach Bedarf prüfen und an andere Gruppen senden können.

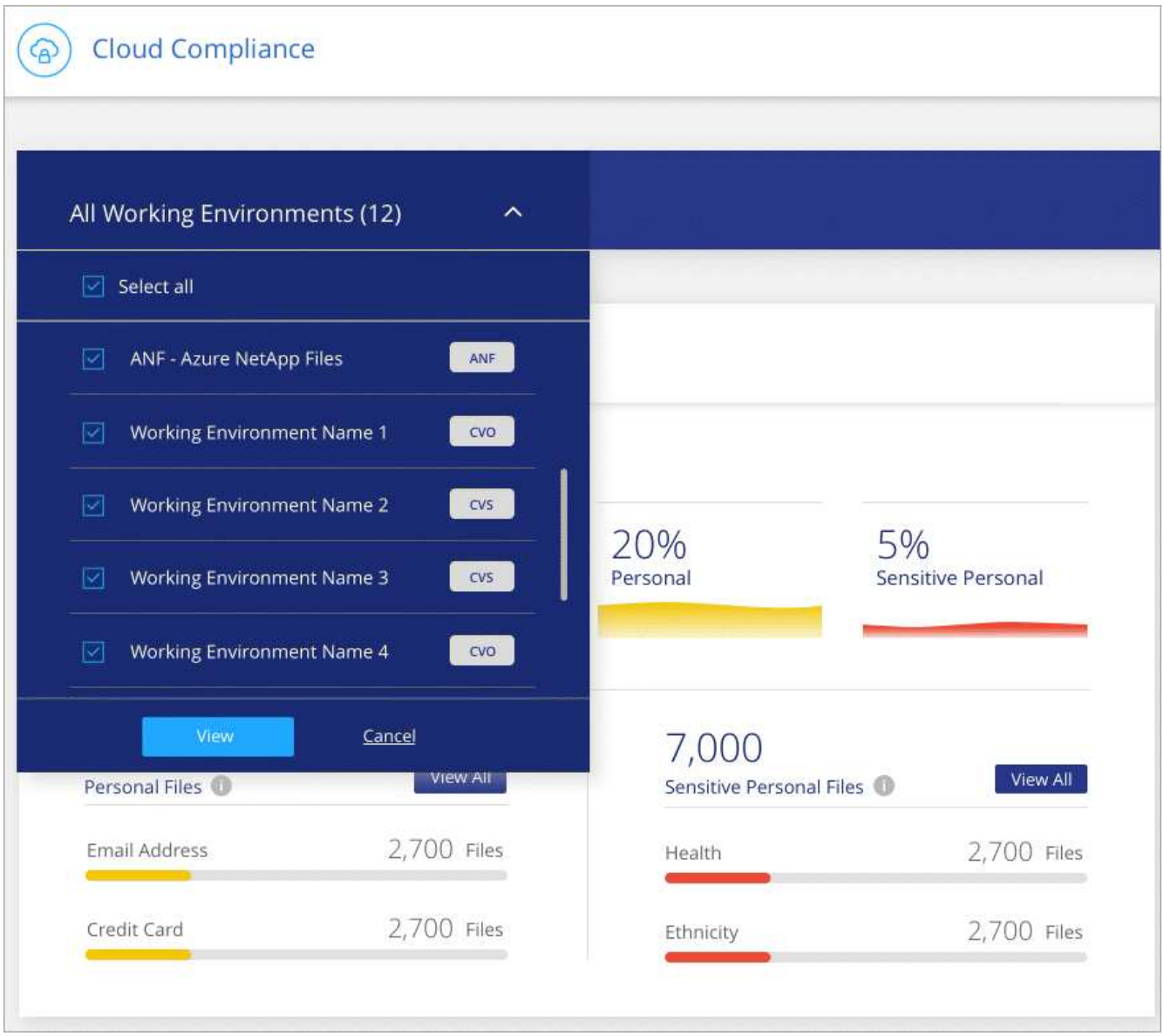
Auswählen der Arbeitsumgebungen für Berichte

Sie können die Inhalte des Cloud Compliance Dashboards filtern, um Compliance-Daten für alle Arbeitsumgebungen und Datenbanken oder nur für bestimmte Arbeitsumgebungen anzuzeigen.

Wenn Sie das Dashboard filtern, wird durch Cloud Compliance die Compliance-Daten und -Berichte genau den von Ihnen ausgewählten Arbeitsumgebungen beschrieben.

Schritte

1. Klicken Sie auf das Dropdown-Menü Filter, wählen Sie die Arbeitsumgebungen aus, für die Sie Daten anzeigen möchten, und klicken Sie auf **Ansicht**.



Reaktion auf eine Zugriffsanfrage für betroffene Person

Reagieren Sie auf eine DSAR (Data Subject Access Request), indem Sie nach dem vollständigen Namen oder der bekannten Kennung (z. B. einer E-Mail-Adresse) eines Studienteilnehmers suchen und dann einen Bericht herunterladen. Der Bericht soll Ihrem

Unternehmen helfen, die Vorgaben der DSGVO oder ähnlicher Datenschutzgesetze einzuhalten.

NetApp kann keine Garantie für 100 % Genauigkeit der persönlichen Daten und für sensible personenbezogene Daten, die Cloud Compliance identifiziert hat, geben. Überprüfen Sie die Informationen immer, indem Sie die Daten überprüfen.

Was ist ein Antrag auf Zugang für betroffene Person?

Datenschutzvorschriften wie die Europäische DSGVO erteilen Betroffenen (wie Kunden oder Mitarbeitern) das Recht, auf ihre personenbezogenen Daten zuzugreifen. Wenn eine betroffene Person diese Informationen anfordert, wird dies als DSAR (Zugriffsanfrage für betroffene Person) bezeichnet. Unternehmen sind verpflichtet, auf diese Anfragen „ohne unzumutbare Verzögerung“ und spätestens innerhalb eines Monats nach Eingang zu reagieren.

Wie kann Cloud Compliance Ihnen helfen, auf einen DSAR zu reagieren?

Wenn Sie eine Suche des Betroffenen durchführen, findet Cloud Compliance alle Dateien, die den Namen oder die Kennung der betreffenden Person enthalten. Cloud Compliance prüft die neuesten vorindizierten Daten auf den Namen oder die Kennung. Es wird kein neuer Scan gestartet.

Nachdem die Suche abgeschlossen ist, können Sie die Liste der Dateien für einen Bericht für die Anforderung von Datensubjekten herunterladen. Der Bericht sammelt Erkenntnisse aus den Daten und stellt die Daten zu rechtlichen Bedingungen bereit, die Sie an die Person zurücksenden können.

Suchen nach Betroffenen und Herunterladen von Berichten

Suchen Sie nach dem vollständigen Namen oder der bekannten Kennung des Betroffenen, und laden Sie dann einen Dateilistenbericht oder einen DSAR-Bericht herunter. Suchen Sie nach "Alle persönlichen Informationstypen".

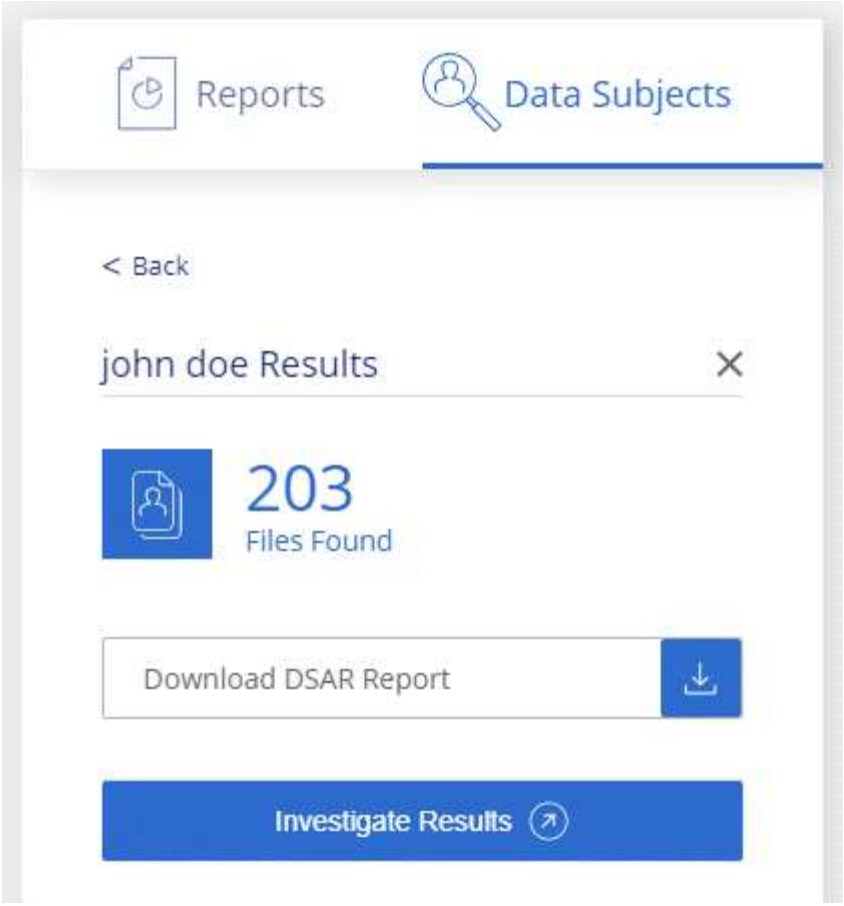
Nur Englisch wird bei der Suche nach den Namen von Betroffenen unterstützt. Support für weitere Sprachen wird später hinzugefügt.

Die Suche nach Betroffenen wird derzeit in Datenbanken nicht unterstützt.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Cloud Compliance**.
2. Klicken Sie Auf **Data Subjects**.
3. Suchen Sie nach dem vollständigen Namen oder der bekannten Kennung des Betroffenen.

   Hier ein Beispiel, das eine Suche nach dem Namen *john doe* zeigt:



4. Wählen Sie eine der folgenden Optionen:
   - **Download DSAR Report**: Eine formelle Antwort auf die Zugriffsanfrage, die Sie an den Betroffenen senden können. Dieser Bericht enthält automatisch generierte Informationen auf der Grundlage von Daten, die Cloud Compliance dem Betroffenen zur Verfügung stellte und für die Nutzung als Vorlage konzipiert wurde. Füllen Sie das Formular aus und überprüfen Sie es intern, bevor Sie es an den Betroffenen senden.
   - **Ergebnisse untersuchen**: Eine Seite, auf der Sie die Daten untersuchen können, indem Sie nach einer bestimmten Datei suchen, sortieren, Details erweitern und die Dateiliste herunterladen.

     Wenn es mehr als 10,000 Ergebnisse gibt, werden nur die Top 10,000 in der Dateiliste angezeigt.

Deaktivieren Von Cloud Compliance

Wenn Sie benötigen, können Sie verhindern, dass Cloud Compliance eine oder mehrere Arbeitsumgebungen oder Datenbanken scannt. Sie können auch die Cloud Compliance-Instanz löschen, wenn Sie Cloud Compliance nicht mehr in Ihrer Arbeitsumgebung verwenden möchten.

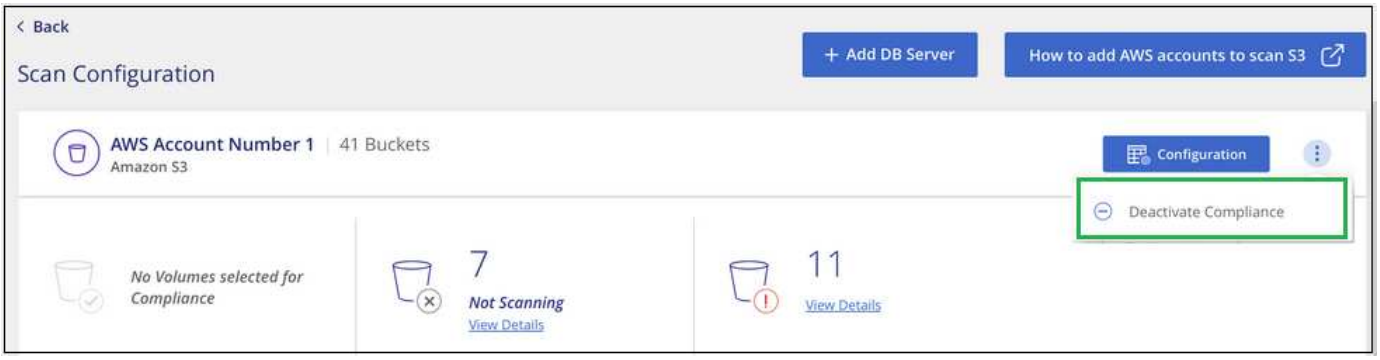
Deaktivieren von Compliance-Scans für eine Arbeitsumgebung

Wenn Sie Scans deaktivieren, scannt Cloud Compliance die Daten auf dem System nicht mehr und entfernt alle indizierten Compliance-Einblicke aus der Cloud Compliance Instanz (die Daten aus der Arbeitsumgebung

oder der Datenbank selbst werden nicht gelöscht).

Schritte

Klicken Sie auf der Seite *Scan Configuration* auf Klicken Sie in der Zeile für die Arbeitsumgebung auf **Compliance deaktivieren**.



Sie können bei der Auswahl der Arbeitsumgebung auch die Compliance-Scans für eine Arbeitsumgebung im Fenster „Services“ deaktivieren.

Löschen der Cloud-Compliance-Instanz

Sie können die Cloud Compliance-Instanz löschen, wenn Sie Cloud Compliance nicht mehr verwenden möchten. Durch das Löschen der Instanz werden auch die zugehörigen Festplatten gelöscht, auf denen sich die indizierten Daten befinden.

Schritt

1. Gehen Sie zur Konsole Ihres Cloud-Providers und löschen Sie die Instanz für Cloud Compliance.

   Der Name der Instanz ist *CloudCompliance* mit einem generierten Hash (UUID), der verknüpft ist. Beispiel: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

Häufig gestellte Fragen zur Cloud Compliance

Diese FAQ kann Ihnen helfen, wenn Sie nur eine schnelle Antwort auf eine Frage suchen.

Was ist Cloud Compliance?

Cloud Compliance ist ein Cloud-Angebot, das künstliche Intelligenz (KI) nutzt, um Unternehmen dabei zu unterstützen, den Datenkontext zu verstehen und sensible Daten in ihren Azure NetApp Files Konfigurationen zu identifizieren, Cloud Volumes ONTAP-Systeme in AWS oder Azure, Amazon S3 Buckets und Datenbanken zu hosten.

Cloud Compliance bietet vordefinierte Parameter (wie z. B. sensible Informationstypen und Kategorien), um neue Compliance-Anforderungen für Datenschutz und -Sensibilität wie DSGVO, CCPA, HIPAA usw. zu erfüllen.

Warum sollte ich Cloud-Compliance verwenden?

Cloud Compliance bietet Ihnen mehr Möglichkeiten für die Nutzung von Daten:

- Einhaltung von Daten-Compliance- und Datenschutzvorschriften
- Einhaltung von Richtlinien zur Datenaufbewahrung.
- Das Auffinden und Reporting von Daten zu bestimmten Daten als Antwort auf Betroffene kann ganz nach Bedarf auf DSGVO, CCPA, HIPAA und anderen Datenschutzvorschriften erfolgen.

Was sind die gängigsten Anwendungsfälle für Cloud Compliance?

- Ermitteln von personenbezogenen Daten
- Identifizieren Sie einen breiten Umfang sensibler Daten, wie sie im Sinne der DSGVO- und CCPA-Datenschutzvorschriften erforderlich sind.
- Einhaltung neuer und anstehender Datenschutzvorschriften

"Erfahren Sie mehr über die Anwendungsfälle für Cloud Compliance".

Welche Datentypen können mit Cloud Compliance gescannt werden?

Cloud Compliance unterstützt die Überprüfung unstrukturierter Daten über die von Cloud Volumes ONTAP und Azure NetApp Files gemanagten NFS- und CIFS-Protokolle. Cloud Compliance kann auch Daten scannen, die in Amazon S3 Buckets gespeichert sind.

Außerdem können mit Cloud Compliance Datenbanken gescannt werden, die sich an einem beliebigen Ort befinden - sie müssen nicht von Cloud Manager gemanagt werden.

"Lesen Sie, wie Scans funktionieren".

Welche Cloud-Provider werden unterstützt?

Cloud Compliance arbeitet als Teil von Cloud Manager und unterstützt derzeit AWS und Azure. Dadurch erhält Ihr Unternehmen Transparenz im Hinblick auf den Datenschutz bei verschiedenen Cloud-Providern. Demnächst wird auch Support für die Google Cloud Platform (GCP) verfügbar sein.

Wie erhalte ich Zugriff auf Cloud Compliance?

Cloud Compliance wird über Cloud Manager betrieben und gemanagt. Sie können Cloud Compliance-Funktionen über die Registerkarte **Compliance** in Cloud Manager aufrufen.

Wie funktioniert Cloud Compliance?

Cloud Compliance implementiert gemeinsam mit Ihrem Cloud Manager System und Ihren Storage-Systemen eine weitere Schicht künstlicher Intelligenz. Anschließend werden die Daten auf Volumes, Buckets und Datenbanken überprüft und die gefundenen Dateneinblicke indiziert.

"Funktionsweise von Cloud Compliance".

Wie viel kostet Cloud Compliance?

Die Kosten für die Verwendung von Cloud Compliance hängen von der Datenmenge ab, die Sie scannen. Es sind die ersten 1 TB an Daten, die Cloud Compliance in einem Cloud Manager Workspace scannt, kostenlos.

Danach ist ein Abonnement für AWS oder Azure Marketplace erforderlich, um mit dem Scannen der Daten fortzufahren. Siehe "Preisgestaltung" Entsprechende Details.

Wie oft scannt Cloud Compliance meine Daten?

Da sich die Daten häufig ändern, scannt Cloud Compliance Ihre Daten kontinuierlich, ohne Auswirkungen auf Ihre Daten. Während der erste Scan Ihrer Daten länger dauern kann, scannen nachfolgende Scans nur die inkrementellen Änderungen, was die Dauer des Systemscans verkürzt.

"Lesen Sie, wie Scans funktionieren".

Bietet Cloud Compliance Berichte an?

Ja. Die von Cloud Compliance angebotenen Informationen können für andere Beteiligte in Ihrem Unternehmen relevant sein. So können Sie Berichte erstellen und Einblicke erhalten.

Für Cloud Compliance stehen folgende Berichte zur Verfügung:

Datenschutzrisiko-Assessment-Bericht
: Bietet Einblicke in den Datenschutz und eine Bewertung des Datenschutzrisikos. "Weitere Informationen .".

Bericht für Anforderung von Datenfachzugriff
: Ermöglicht Ihnen, einen Bericht aller Dateien zu extrahieren, die Informationen über den spezifischen Namen oder die persönliche Kennung eines Betroffenen enthalten. "Weitere Informationen .".

PCI DSS-Bericht
: Unterstützt Sie bei der Identifizierung der Verteilung von Kreditkarteninformationen über Ihre Dateien. "Weitere Informationen .".

HIPAA-Bericht
: Hilft Ihnen dabei, die Verteilung von Gesundheitsinformationen über Ihre Dateien hinweg zu identifizieren. "Weitere Informationen .".

Berichte zu einem bestimmten Informationstyp
: Es stehen Berichte zur Verfügung, die Details zu den identifizierten Dateien enthalten, die personenbezogene Daten und sensible personenbezogene Daten enthalten. Sie können auch Dateien nach Kategorie und Dateityp aufgeschlüsselt sehen. "Weitere Informationen .".

Welcher Instanztyp oder VM ist für Cloud Compliance erforderlich?

- In Azure wird Cloud Compliance auf einer VM mit Standard_D16s_v3 mit einer Festplatte von 512 GB ausgeführt.
- In AWS wird Cloud-Compliance auf einer m5.4xlarge-Instanz mit einer 500-GB-GP2-Festplatte ausgeführt.

  In Regionen, in denen m5.4xlarge nicht verfügbar ist, wird Cloud Compliance stattdessen auf einer m4.4xlarge-Instanz ausgeführt.

Das Ändern oder Ändern der Größe des Instanz-/VM-Typs wird nicht unterstützt. Es muss die angegebene Standardgröße verwendet werden.

"Funktionsweise von Cloud Compliance".

Ist die Scanleistung unterschiedlich?

Die Scan-Performance kann je nach Netzwerkbandbreite und durchschnittlicher Dateigröße in der Cloud-Umgebung variieren.

Welche Dateitypen werden unterstützt?

Cloud Compliance scannt alle Dateien nach Informationen zu Kategorien und Metadaten und zeigt alle Dateitypen im Abschnitt Dateitypen im Dashboard an.

Wenn Cloud Compliance personenbezogene Daten (PII) erkennt oder eine DSAR-Suche durchführt, werden nur die folgenden Dateiformate unterstützt: .PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF UND .JSON.

Wie kann ich Cloud-Compliance aktivieren?

Zunächst müssen Sie eine Instanz von Cloud Compliance in Cloud Manager implementieren. Sobald die Instanz ausgeführt wurde, können Sie sie auf bestehenden Arbeitsumgebungen und Datenbanken über die Registerkarte **Compliance** oder durch Auswahl einer bestimmten Arbeitsumgebung aktivieren.

"Erste Schritte".

Durch die Aktivierung von Cloud Compliance wird ein sofortiger anfänglicher Scan durchgeführt. Ergebnisse der Compliance werden kurz danach angezeigt.

Wie deaktiviere ich Cloud Compliance?

Sie können Cloud-Compliance auf der Seite Arbeitsumgebung deaktivieren, nachdem Sie eine individuelle Arbeitsumgebung ausgewählt haben.

"Weitere Informationen .".

Wenn Sie die Cloud Compliance-Instanz vollständig entfernen möchten, können Sie die Cloud Compliance-Instanz manuell aus dem Portal Ihres Cloud-Providers entfernen.

Was geschieht, wenn das Daten-Tiering auf Cloud Volumes ONTAP aktiviert ist?

Es ist sinnvoll, Cloud-Compliance auf einem Cloud Volumes ONTAP System zu aktivieren, das kalte Daten auf Objekt-Storage abschichtet. Wenn das Daten-Tiering aktiviert ist, scannt Cloud Compliance alle Daten auf Festplatten, die sich auf kalten Daten befinden, die in Objekt-Storage verschoben werden.

Der Compliance-Scan erhitzt die nicht kalten Daten – es bleibt kalt und führt zu Objekt-Storage.

Kann ich Cloud Compliance verwenden, um den lokalen ONTAP Storage zu scannen?

Das Scannen der Daten direkt aus einer lokalen ONTAP-Arbeitsumgebung wird nicht unterstützt. Sie können Ihre lokalen ONTAP-Daten jedoch scannen, indem Sie die On-Premises-NFS- oder CIFS-Daten in eine Cloud Volumes ONTAP Arbeitsumgebung replizieren und anschließend die Compliance für diese Volumes aktivieren. Wir planen, Cloud Compliance durch zusätzliche Cloud-Angebote wie Cloud Volumes Service zu unterstützen.

"Weitere Informationen .".

Kann Cloud Compliance Benachrichtigungen an mein Unternehmen senden?

Nein, aber Sie können Statusberichte herunterladen, die Sie intern in Ihrem Unternehmen teilen können.

Kann ich den Service an die Bedürfnisse meiner Organisation anpassen?

Cloud Compliance bietet sofortige Einblicke in Ihre Daten. Diese Erkenntnisse können extrahiert und für die Bedürfnisse Ihres Unternehmens verwendet werden.

Kann ich die Daten zur Cloud Compliance auf bestimmte Benutzer begrenzen?

Ja, Cloud Compliance ist vollständig in Cloud Manager integriert. Cloud Manager-Benutzer können nur Informationen für die Arbeitsumgebungen anzeigen, die sie entsprechend ihren Arbeitsbereichsberechtigungen anzeigen können.

Wenn Sie bestimmten Benutzern die Möglichkeit geben möchten, die Ergebnisse des Cloud-Compliance-Scans einfach anzuzeigen, ohne Cloud-Compliance-Einstellungen verwalten zu können, können Sie diesen Benutzern die Rolle „*Cloud Compliance Viewer*“ zuweisen.

"Weitere Informationen .".

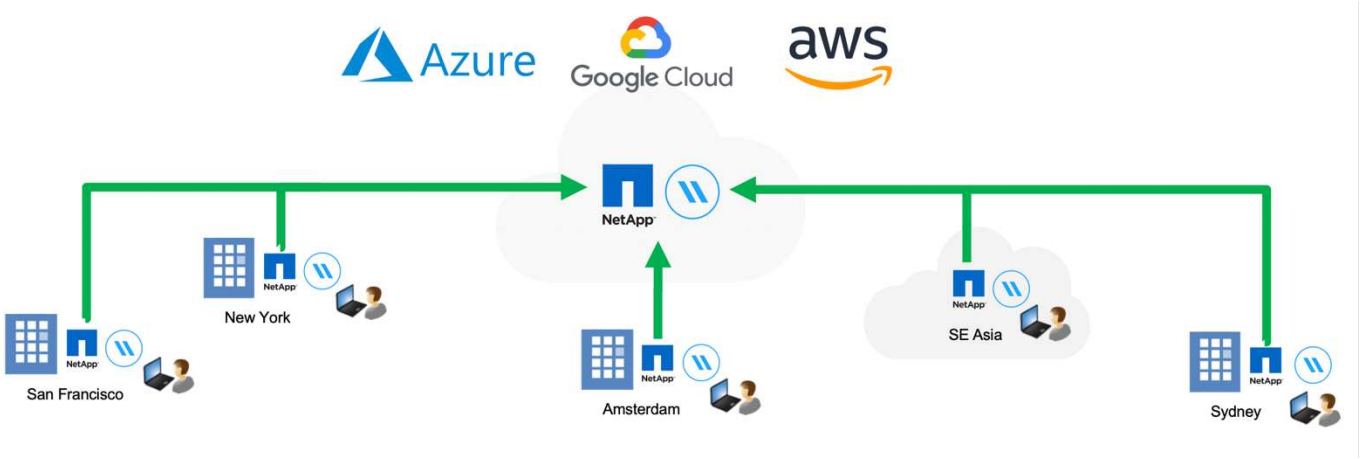
Globales File Sharing in Echtzeit

Erfahren Sie mehr über Global File Cache

Mit NetApp Global File Cache können Sie Silos verteilter File Server zu einem zusammenhängenden globalen Storage-System in der Public Cloud konsolidieren. Dadurch wird ein global zugängliches File-System in der Cloud geschaffen, das alle Remote-Standorte so nutzen kann, als ob sie lokal wären.

Überblick

Die Implementierung von Global File Cache verursacht gegenüber einer verteilten Storage-Architektur einen zentralen, einzigen Storage-Platzbedarf, der an jedem Standort lokales Datenmanagement, Backup, Sicherheitsmanagement, Storage und Infrastruktur erfordert.



Funktionen

Global File Cache ermöglicht die folgenden Funktionen:

- Konsolidieren und zentralisieren Sie Ihre Daten in die Public Cloud und profitieren Sie von der Skalierbarkeit und Performance von Storage-Lösungen der Enterprise-Klasse
- Erstellen Sie einen einzigen Datensatz für alle Benutzer weltweit und nutzen Sie intelligentes Datei-Caching, um globalen Datenzugriff, Zusammenarbeit und Performance zu verbessern
- Sie erhalten einen eigenständigen, automatisierten Cache, der vollständige Datenkopien und Backups überflüssig macht. Nutzen Sie lokales Datei-Caching für aktive Daten und senken Sie die Storage-Kosten
- Transparenter Zugriff von Remote-Standorten über einen globalen Namespace mit zentraler Dateisperrung in Echtzeit

Weitere Informationen zu den Funktionen und Anwendungsfällen von Global File Cache finden Sie hier "Hier".

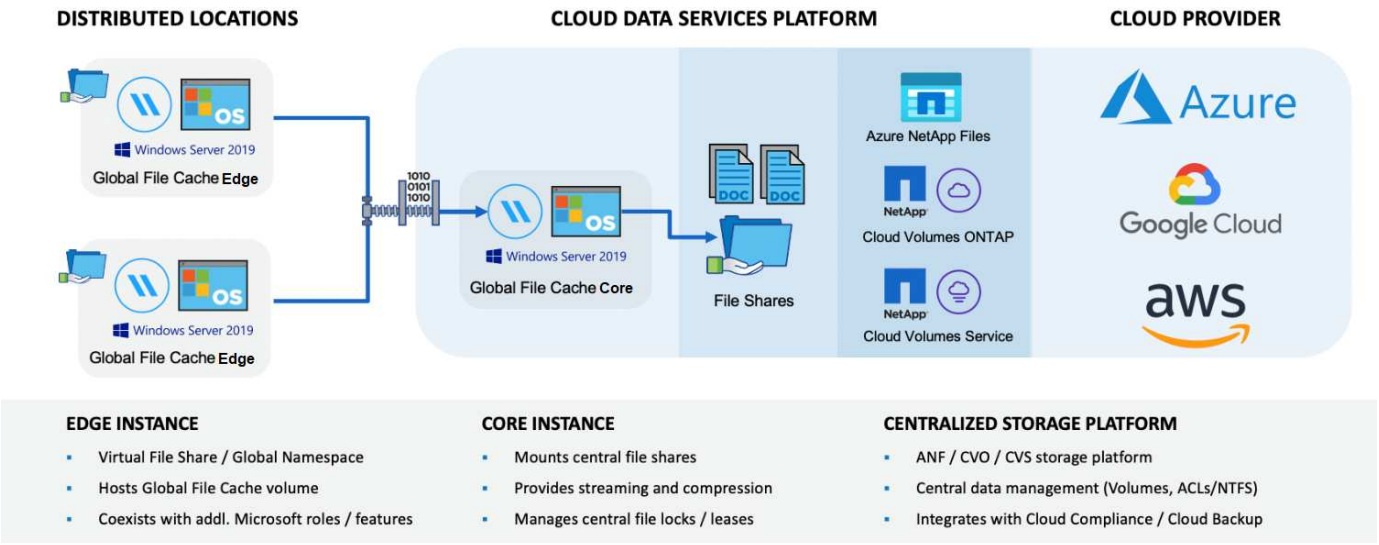
Globale File Cache-Komponenten

Global File Cache besteht aus folgenden Komponenten:

- Global File Cache Management Server

- Globaler File Cache-Kern
- Global File Cache Edge (an Remote-Standorten implementiert)

Die globale File Cache Core Instanz wird in die File Shares Ihres Unternehmens eingebunden, die auf der bevorzugten Back-End-Storage-Plattform gehostet werden (wie Cloud Volumes ONTAP, Cloud Volumes Service, Und Azure NetApp Files). Außerdem wurde eine globale File Cache-Fabric-Strategie entwickelt, mit der unstrukturierte Daten in einem einzigen Datensatz konsolidiert und zentralisiert werden können. Dabei spielt es keine Rolle, ob sich die Daten auf einer oder mehreren Storage-Plattformen in der Public Cloud befinden.



Unterstützte Storage-Plattformen

Die unterstützten Storage-Plattformen für Global File Cache unterscheiden sich je nach gewählter Implementierungsoption.

Automatisierte Implementierungsoptionen

Global File Cache wird bei Implementierung mit Cloud Manager für die folgenden Typen von Arbeitsumgebungen unterstützt:

- Cloud Volumes ONTAP in Azure
- Cloud Volumes ONTAP in AWS

Mit dieser Konfiguration können Sie die gesamte Implementierung des Global File Cache Servers einschließlich Global File Cache Management Server und Global File Cache Core in Cloud Manager implementieren und managen.

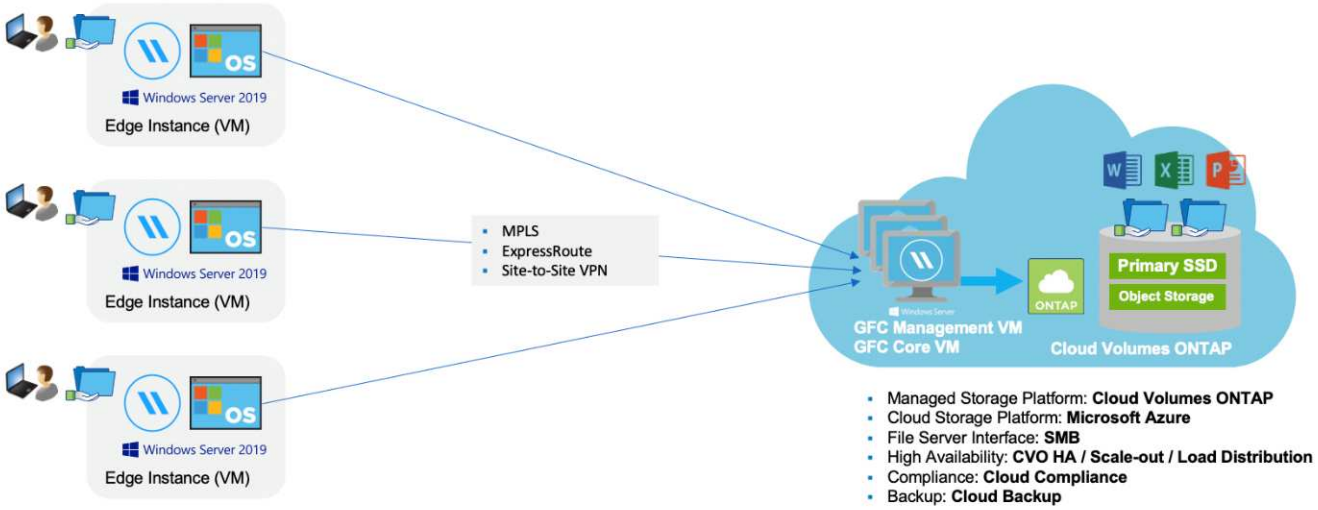
Optionen für manuelle Implementierung

Außerdem werden globale File-Cache-Konfigurationen mit Cloud Volumes ONTAP, Cloud Volumes Service oder Azure NetApp Files unterstützt, die auf der Public-Cloud-Storage-Infrastruktur von Microsoft Azure, Google Cloud Platform oder Amazon Web Services installiert sind. Lösungen vor Ort sind auch auf NetApp AFF und FAS Plattformen verfügbar. In diesen Installationen müssen die serverseitigen Komponenten des Global File Cache nicht mit Cloud Manager, sondern manuell konfiguriert und bereitgestellt werden.

Siehe "NetApp Global File Cache User Guide" Entsprechende Details.

Funktionsweise von Global File Cache

Global File Cache erstellt eine Software Fabric, in der aktive Datensätze an Remote-Standorten weltweit im Cache gespeichert werden. Geschäftliche Benutzer haben somit einen transparenten Datenzugriff und eine optimale Performance auf globaler Ebene.



Die in diesem Beispiel referenzierte Topologie ist ein Hub-and-Spoke-Modell, wobei das Netzwerk von Remote-Zweigstellen/-Standorten auf einen gemeinsamen Datensatz in der Cloud zugreift. Die wichtigsten Punkte dieses Beispiels sind:

- Zentralisierter Datastore:
  - Public-Cloud-Storage-Plattform der Enterprise-Klasse, wie Cloud Volumes ONTAP
- Global File Cache Fabric:
  - Erweiterung des zentralen Datenspeichers an die Remote-Standorte
  - Global File Cache Core Instance, Mounten in File Shares (SMB) des Unternehmens.
  - Global File Cache Edge-Instanzen, die an jedem Remote-Standort ausgeführt werden.
  - Stellt an jedem Remote-Standort einen virtuellen Dateifreigabe bereit, der Zugriff auf zentrale Daten ermöglicht.
  - Hostet den Intelligent File Cache auf einem benutzerdefinierten NTFS-Volume (`D:\`).
- Netzwerkkonfiguration:
  - Multi-Protokoll-Label-Switching (MPLS)-, ExpressRoute- oder VPN-Konnektivität
- Integration in die Active Directory-Domänendienste des Kunden.
- DFS-Namespace für die Verwendung eines globalen Namespace (empfohlen).

Kosten

Die Kosten für die Verwendung von Global File Cache hängen von der Art der Installation ab, die Sie ausgewählt haben.

- Bei allen Installationen müssen Sie ein oder mehrere Volumes in der Cloud (Cloud Volumes ONTAP, Cloud Volumes Service oder Azure NetApp Files) implementieren. Daraus entstehen Gebühren vom ausgewählten Cloud-Provider.
- Bei allen Installationen müssen Sie zudem zwei oder mehr Virtual Machines (VMs) in der Cloud implementieren. Daraus entstehen Gebühren vom ausgewählten Cloud-Provider.
    - Global File Cache Management-Server:

      In Azure wird dies auf einer D2S_V3 VM oder einer gleichwertigen (2 vCPU/8 GB RAM) mit 127GB Premium SSD ausgeführt

      In AWS wird dies auf einer m4.Large oder einer gleichwertigen Instanz (2 vCPU/8 GB RAM) mit 127GB Allzweck-SSD ausgeführt

    - Globaler File-Cache-Kern:

      In Azure wird dies auf einer D4s_V3 VM oder einer äquivalenten VM (4 vCPU/16 GB RAM) mit 127GB Premium SSD ausgeführt

  In AWS wird dies auf einer m4.xlarge oder einer äquivalenten Instanz (4 vCPU/16 GB RAM) mit einer universell einsetzbaren 127-GB-SSD ausgeführt

- Bei der Installation mit Cloud Volumes ONTAP in Azure oder AWS (die unterstützten Konfigurationen sind vollständig über Cloud Manager implementiert) fallen pro Standort 3,000 US-Dollar an (für jede Global File Cache Edge Instanz).
- Bei der Installation mit den manuellen Bereitstellungsoptionen ist die Preisgestaltung unterschiedlich. Eine allgemeine Einschätzung der Kosten finden Sie unter "Berechnen Sie Ihr Einsparungspotenzial" Oder wenden Sie sich an Ihren Global File Cache Solutions Engineer, um die besten Optionen für die Implementierung in Ihrem Unternehmen zu besprechen.

Lizenzierung

Global File Cache umfasst einen Software-basierten License Management Server (LMS), mit dem Sie Ihr Lizenzmanagement konsolidieren und Lizenzen mithilfe eines automatisierten Mechanismus auf alle Core- und Edge-Instanzen implementieren können.

Wenn Sie Ihre erste Core-Instanz im Datacenter oder in der Cloud implementieren, können Sie diese Instanz als LMS für Ihr Unternehmen festlegen. Diese LMS-Instanz ist einmal konfiguriert, stellt eine Verbindung zum Abonnementdienst (über HTTPS) her und validiert Ihr Abonnement mit der Kunden-ID, die unsere Support-/Operations-Abteilung bei Aktivierung des Abonnements bereitstellt. Nachdem Sie diese Bezeichnung erstellt haben, verknüpfen Sie Ihre Edge-Instanzen mit dem LMS, indem Sie Ihre Kunden-ID und die IP-Adresse der LMS-Instanz angeben.

Wenn Sie zusätzliche Edge-Lizenzen erwerben oder Ihr Abonnement verlängern, aktualisiert unsere Support-/Operations-Abteilung die Lizenzdetails, beispielsweise die Anzahl der Websites oder das Enddatum des Abonnements. Nachdem das LMS den Abonnementdienst abgefragt hat, werden die Lizenzdetails automatisch auf der LMS-Instanz aktualisiert und gelten für Ihre GFC Core- und Edge-Instanzen.

Siehe "NetApp Global File Cache User Guide" Weitere Details zur Lizenzierung.

Einschränkungen

- Die in Cloud Manager unterstützte Version des globalen Datei-Caches setzt voraus, dass die als zentraler Storage verwendete Back-End-Storage-Plattform eine Arbeitsumgebung sein muss, in der Sie einen

einzelnen Cloud Volumes ONTAP Node oder ein HA-Paar in Azure oder AWS implementiert haben.

Andere Storage-Plattformen und andere Cloud-Provider werden derzeit nicht mit Cloud Manager unterstützt, können jedoch mit älteren Implementierungsverfahren implementiert werden.

Diese anderen Konfigurationen, beispielsweise Global File Cache Using Cloud Volumes ONTAP, Cloud Volumes Service, and Azure NetApp Files on Microsoft Azure, Google Cloud und AWS, werden weiterhin mit den älteren Verfahren unterstützt. Siehe "Global File Cache: Überblick und Onboarding" Entsprechende Details.

Bevor Sie mit der Bereitstellung von Global File Cache beginnen

Bevor Sie Global File Cache in der Cloud und an Ihren Remote-Standorten implementieren, müssen Sie zahlreiche Anforderungen beachten.

Überlegungen zum Design von Global File Cache Core

Je nach Ihren Anforderungen müssen Sie möglicherweise eine oder mehrere Global File Cache Core-Instanzen bereitstellen, um die Global File Cache Fabric zu erstellen. Die Kerninstanz dient als Traffic COP zwischen Ihren verteilten Global File Cache Edge Instanzen und den File Server-Ressourcen im Datacenter, beispielsweise File Shares, Ordner und Dateien.

Wenn Sie Ihre Global File Cache-Bereitstellung entwerfen, müssen Sie entscheiden, was für Ihre Umgebung im Hinblick auf Skalierung, Verfügbarkeit von Ressourcen und in Bezug auf Redundanz das Richtige ist. Global File Cache Core kann auf folgende Weise implementiert werden:

- GFC Core Standalone-Instanz
- GFC Core Load Distributed-Design (Cold Standby)

Siehe Richtlinien für die Dimensionierung So ermitteln Sie die maximale Anzahl an Edge-Instanzen und die Gesamtanzahl der Benutzer, die jede Konfiguration unterstützen kann:

Wenden Sie sich an Ihren Global File Cache Solutions Engineer, um die besten Optionen für die Implementierung in Ihrem Unternehmen zu besprechen.

Richtlinien für die Dimensionierung

Bei der Konfiguration des ersten Systems sind einige Richtlinien zur Dimensionierung zu beachten. Sie sollten diese Verhältnisse noch einmal überprüfen, nachdem sich einige Verwendungsdaten angesammelt haben, um sicherzustellen, dass Sie das System optimal nutzen. Dazu zählen:

- Global File Cache-Kanten/Core-Verhältnis
- Verhältnis von verteilten Benutzern/Global File Cache Edge
- Dezentrale Benutzer/Global File Cache Core Ratio

Anzahl der Edge-Instanzen pro Core-Instanz

Unsere Richtlinien empfehlen bis zu 10 Edge-Instanzen pro Global File Cache Core-Instanz mit maximal 20 Rändern pro Global File Cache Core-Instanz. Dies hängt stark vom Typ und der mittleren Dateigröße des am häufigsten verwendeten Workloads ab. In einigen Fällen können bei den geläufigeren Workloads mehr Edge-

Instanzen pro Kern hinzugefügt werden. In diesen Fällen sollten Sie sich jedoch an den NetApp Support wenden, um die Anzahl der Edge- und Core-Instanzen abhängig von den Typen und der Größe der Datensets korrekt zu dimensionieren.

> Sie können mehrere Global File Cache Edge- und Core-Instanzen gleichzeitig nutzen, um Ihre Infrastruktur je nach Anforderungen horizontal zu skalieren.

Anzahl gleichzeitiger Benutzer pro Edge Instanz

Global File Cache Edge bewältigt die Schwerarbeit hinsichtlich Caching-Algorithmen und Unterschieden auf Dateiebene. Eine einzige globale File Cache Edge Instanz kann bis zu 400 Benutzer pro dedizierter physischer Edge Instanz sowie bis zu 200 Benutzer für dedizierte virtuelle Bereitstellungen bereitstellen. Dies hängt stark vom Typ und der mittleren Dateigröße des am häufigsten verwendeten Workloads ab. Bei größeren Dateitypen für die Zusammenarbeit können Sie angeben, dass 50 % der maximalen Benutzer pro Global File Cache Edge untere Grenze (je nach physischer oder virtueller Bereitstellung) vorliegen. Für häufiger Office-Objekte mit einer mittleren Dateigröße von <1 MB, Leitfaden zu den 100 % Benutzern pro Global File Cache Edge Obergrenze (je nach physischer oder virtueller Bereitstellung).

> Global File Cache Edge erkennt, ob er auf einer virtuellen oder physischen Instanz ausgeführt wird, und beschränkt die Anzahl der SMB-Verbindungen auf die lokale virtuelle Dateifreigabe auf maximal 200 oder 400 gleichzeitige Verbindungen.

Anzahl gleichzeitiger Benutzer pro Core-Instanz

Die Global File Cache Core Instanz ist äußerst skalierbar und hat eine empfohlene gleichzeitige Benutzeranzahl von 3,000 Benutzern pro Core. Dies hängt stark vom Typ und der mittleren Dateigröße des am häufigsten verwendeten Workloads ab.

Wenden Sie sich an Ihren Global File Cache Solutions Engineer, um die besten Optionen für die Implementierung in Ihrem Unternehmen zu besprechen.

Voraussetzungen

Die in diesem Abschnitt beschriebenen Voraussetzungen gelten für die in der Cloud installierten Komponenten: Den Global File Cache Management Server und den Global File Cache Core.

Die Voraussetzungen für Global File Cache Edge werden beschrieben "Hier".

Cloud Manager-Instanz

Wenn Sie Cloud Volumes ONTAP für Azure als Storage-Plattform verwenden, stellen Sie sicher, dass Cloud Manager über Berechtigungen verfügt, wie in der aktuellen Version dargestellt "Cloud Manager-Richtlinie für Azure".

Neu erstellte Instanzen verfügen standardmäßig über alle erforderlichen Berechtigungen. Wenn Sie Ihre Instanz vor Version 3.8.7 (3. August 2020) bereitgestellt haben, müssen Sie diese Elemente hinzufügen.

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

Storage-Plattform (Volumes)

Die Back-End-Storage-Plattform – in diesem Fall Ihre implementierte Cloud Volumes ONTAP Instanz – sollte SMB-Dateifreigaben bereitstellen. Alle Freigaben, die durch den globalen Dateicache freigelegt werden, müssen der Gruppe „Alle“ die volle Kontrolle auf Share-Ebene ermöglichen, während sie die Berechtigungen durch NTFS-Berechtigungen einschränken.

Wenn Sie auf der Cloud Volumes ONTAP Instanz nicht mindestens eine SMB-Dateifreigabe eingerichtet haben, müssen Sie die folgenden Informationen bereithalten, damit Sie diese Informationen während der Installation konfigurieren können:

- Active Directory-Domänenname, Name-Server-IP-Adresse, Active Directory-Anmeldedaten.
- Name und Größe des Volumes, das Sie erstellen möchten, sowie Name des Aggregats, auf dem das Volume erstellt wird, und Share-Name.

Wir empfehlen, das Volume so groß wie das gesamte Datenset für die Applikation zu sein, und die Möglichkeit zu einer entsprechend skalierbaren Skalierung bei wachsendem Datensatz. Wenn Sie in der Arbeitsumgebung über mehrere Aggregate verfügen, lesen Sie "Management vorhandener Aggregate" Um zu bestimmen, welches Aggregat den meisten verfügbaren Platz für das neue Volume hat.

Global File Cache Management Server

Dieser Global File Cache Management Server erfordert externen Zugriff über HTTPS (TCP Port 443), um eine Verbindung zum Abonnementdienst des Cloud-Providers herzustellen und auf diese URLs zuzugreifen:

- "https://talonazuremicroservices.azurewebsites.net"
- "https://talonlicensing.table.core.windows.net"

Dieser Port muss von allen WAN-Optimierungsgeräten oder Firewall-Restriktionsrichtlinien ausgeschlossen werden, damit die Global File Cache-Software ordnungsgemäß funktioniert.

Der Global File Cache Management Server benötigt für die Instanz außerdem einen eindeutigen (geografischen) NetBIOS-Namen (wie z. B. GFC-MS1).

Ein Management-Server kann mehrere globale File Cache Core-Instanzen unterstützen, die in verschiedenen Arbeitsumgebungen implementiert werden. Bei einer Implementierung über Cloud Manager verfügt jede Arbeitsumgebung über einen eigenen separaten Backend-Storage und enthält nicht dieselben Daten.

Globaler File Cache-Kern

Dieser Global File Cache Core wartet auf TCP-Port-Bereich 6618-6630. Je nach Ihrer Firewall- oder NSG-Konfiguration müssen Sie möglicherweise den Zugriff auf diese Ports über Inbound Port Rules ausdrücklich zulassen. Darüber hinaus müssen diese Ports von allen WAN-Optimierungsgeräten oder Firewallbeschränkungen-Richtlinien ausgeschlossen werden, damit die Global File Cache Software ordnungsgemäß funktioniert.

Die zentralen Anforderungen an Global File Cache sind:

- Ein eindeutiger (geografischer) NetBIOS-Name für die Instanz (z. B. GFC-CORE1)
- Active Directory-Domänenname
  - Global File Cache-Instanzen sollten mit Ihrer Active Directory-Domäne verbunden werden.
  - Global File Cache-Instanzen sollten in einer OU (Global File Cache Specific Organizational Unit) verwaltet und von den übernommenen Gruppenrichtlinienobjekten des Unternehmens ausgeschlossen werden.
- Servicekonto. Die Dienste auf diesem Global File Cache Core werden als ein spezifisches Domain-Benutzerkonto ausgeführt. Dieses Konto, auch als Dienstkonto bezeichnet, muss für jeden der SMB-Server über die folgenden Berechtigungen verfügen, die mit der Global File Cache Core-Instanz verknüpft werden:
  - Das bereitgestellte Servicekonto muss ein Domänenbenutzer sein.

Abhängig von den Einschränkungen und GPOs in der Netzwerkumgebung kann für dieses Konto Administratorrechte für die Domäne erforderlich sein.

- Die IT muss über die Berechtigungen „als Dienst ausführen“ verfügen.
- Das Passwort sollte auf „Never Expire“ gesetzt werden.
- Die Kontooption „Benutzer muss Passwort bei der nächsten Anmeldung ändern“ sollte DEAKTIVIERT werden (deaktiviert).
- Es muss Mitglied der Back-End-Dateiserver-Gruppe sein, die in Backup Operators integriert ist (dies wird automatisch aktiviert, wenn sie über Cloud Manager bereitgestellt wird).

Lizenzverwaltungsserver

- Der Global File Cache License Management Server (LMS) sollte auf einem Microsoft Windows Server 2016 Standard oder Datacenter Edition oder Windows Server 2019 Standard oder Datacenter Edition konfiguriert werden, vorzugsweise auf der Global File Cache Core Instanz im Datacenter oder in der Cloud.
- Wenn Sie eine separate LMS-Instanz für Global File Cache benötigen, müssen Sie das neueste Installationspaket für Global File Cache auf einer makellosen Microsoft Windows Server-Instanz installieren.
- Die LMS-Instanz muss eine Verbindung zum Abonnementdienst (Azure Services / öffentliches Internet) über HTTPS (TCP-Port 443) herstellen können.
- Die Core- und Edge-Instanzen müssen über HTTPS (TCP-Port 443) eine Verbindung zur LMS-Instanz herstellen.

Netzwerkbetrieb

- Firewall: TCP-Ports sollten zwischen Global File Cache Edge und Core Instanzen erlaubt sein.
- Global File Cache TCP Ports: 443 (HTTPS), 6618–6630.

- Netzwerkoptimierungs-Geräte (wie Riverbed Steelhead) müssen so konfiguriert werden, dass sie über die für Global File Cache spezifischen Ports (TCP 6618-6630) weitergeleitet werden.

Erste Schritte

Mit Cloud Manager können Sie den Global File Cache Management Server und die Software Global File Cache Core in der Arbeitsumgebung bereitstellen.

Aktivieren Sie Global File Cache mit Cloud Manager

In dieser Konfiguration werden Sie den Global File Cache Management-Server und den globalen Datei-Cache-Kern in der gleichen Arbeitsumgebung bereitstellen, in der Sie Ihr Cloud Volumes ONTAP-System mit Cloud Manager erstellt haben.

Ansehen "Dieses Video" Um die Schritte von Anfang bis Ende zu sehen.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten:

Implementieren Sie Cloud Volumes ONTAP

Implementierung von Cloud Volumes ONTAP in Azure oder AWS und Konfiguration von SMB-Dateifreigaben. Weitere Informationen finden Sie unter "Starten von Cloud Volumes ONTAP in Azure" Oder "Starten von Cloud Volumes ONTAP in AWS".

Stellen Sie den Global File Cache Management Server bereit

Stellen Sie eine Instanz des Global File Cache Management-Servers in derselben Arbeitsumgebung bereit wie die Instanz von Cloud Volumes ONTAP.

Implementieren Sie den Global File Cache Core

Stellen Sie eine oder mehrere Instanzen des globalen Datei-Cache-Kerns in derselben Arbeitsumgebung wie die Instanz von Cloud Volumes ONTAP bereit und fügen Sie sie in Ihre Active Directory-Domäne ein.

Lizenz Für Globalen Datei-Cache

Konfigurieren Sie den Service für Global File Cache License Management Server (LMS) auf einer globalen File Cache Core-Instanz. Sie benötigen Ihre NSS-Anmeldedaten oder eine von NetApp bereitgestellte Kunden-ID, um Ihr Abonnement zu aktivieren.

Implementieren Sie die globalen File Cache Edge-Instanzen

Siehe "Bereitstellung von Global File Cache Edge-Instanzen" Um die Global File Cache Edge-Instanzen an jedem Remote-Standort bereitzustellen. Dieser Schritt wurde nicht mit Cloud Manager ausgeführt.

Implementieren Sie Cloud Volumes ONTAP als Storage-Plattform

In der aktuellen Version unterstützt Global File Cache Cloud Volumes ONTAP, die in Azure oder AWS implementiert wurden. Detaillierte Voraussetzungen, Anforderungen und Implementierungsanleitungen finden Sie unter "Starten von Cloud Volumes ONTAP in Azure" Oder "Starten von Cloud Volumes ONTAP in AWS".

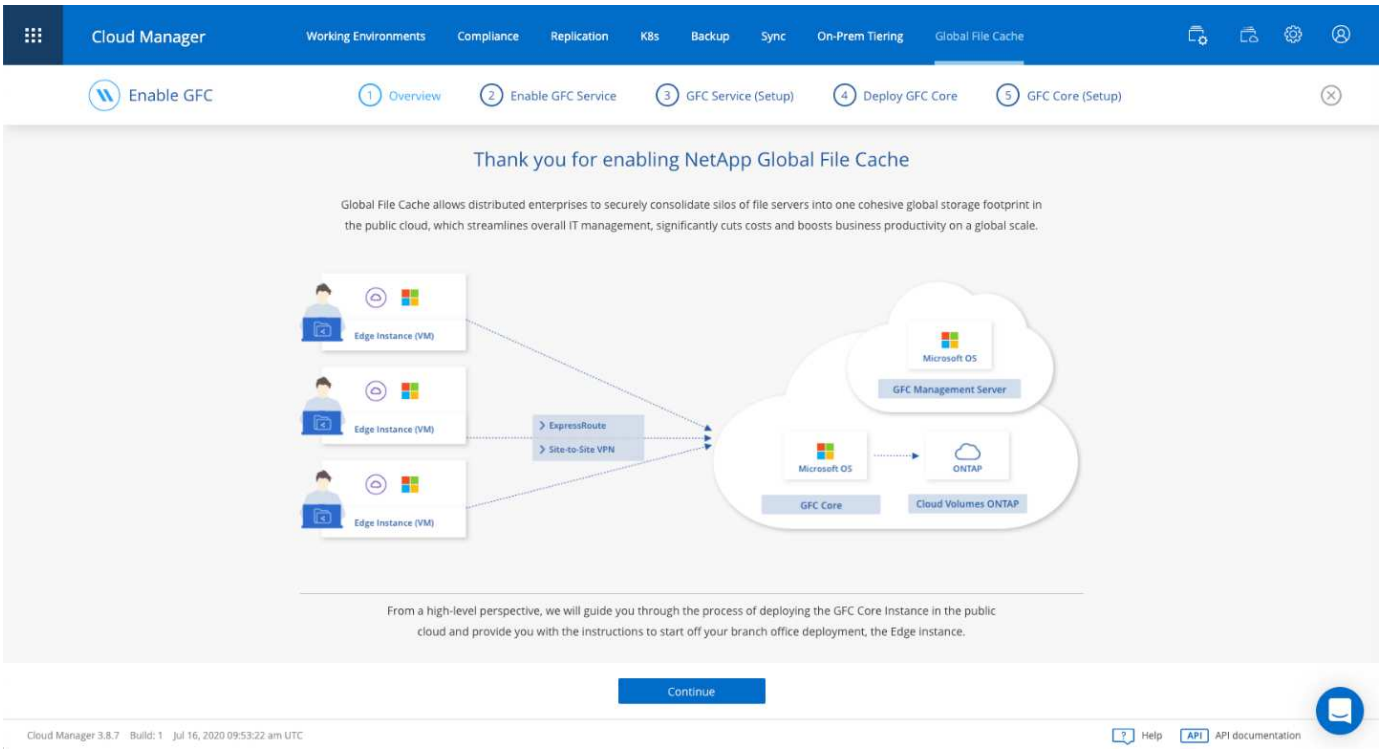
Beachten Sie die folgenden zusätzlichen Anforderungen an Global File Cache:

- Sie sollten SMB-Dateifreigaben auf der Instanz von Cloud Volumes ONTAP konfigurieren.

  Wenn auf der Instanz keine SMB-Dateifreigaben eingerichtet sind, werden Sie aufgefordert, die SMB-Freigaben während der Installation der Komponenten des Global File Cache zu konfigurieren.

Aktivieren Sie den globalen Datei-Cache in Ihrer Arbeitsumgebung

Der Assistent für Global File Cache führt Sie durch die Schritte zur Bereitstellung der Instanz für Global File Cache Management Server und der globalen Datei-Cache Core-Instanz, wie unten hervorgehoben.



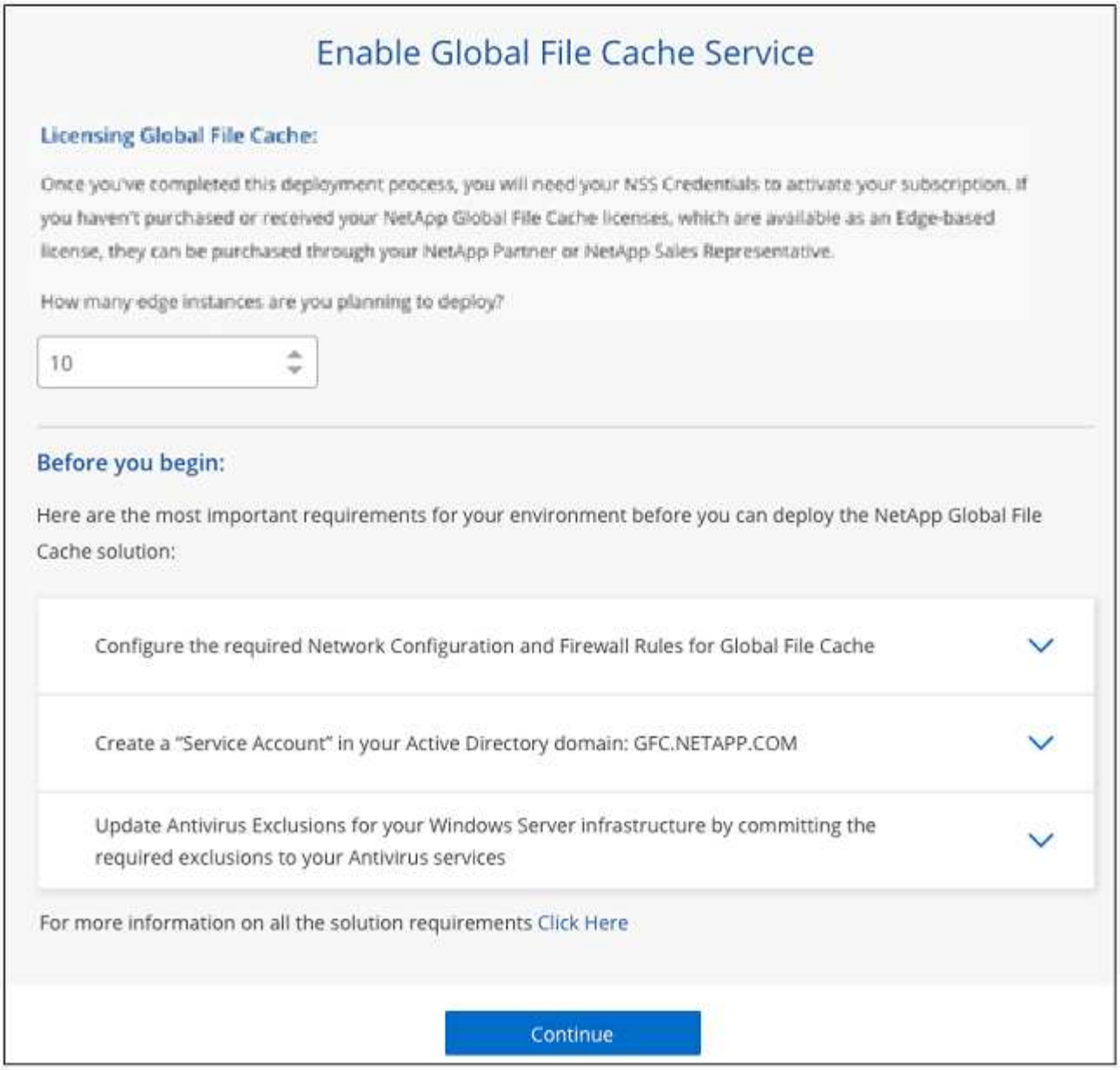
Schritte

1. Wählen Sie die Arbeitsumgebung aus, in der Cloud Volumes ONTAP implementiert wurde.
2. Klicken Sie im Bereich Dienste auf **GFC aktivieren**.

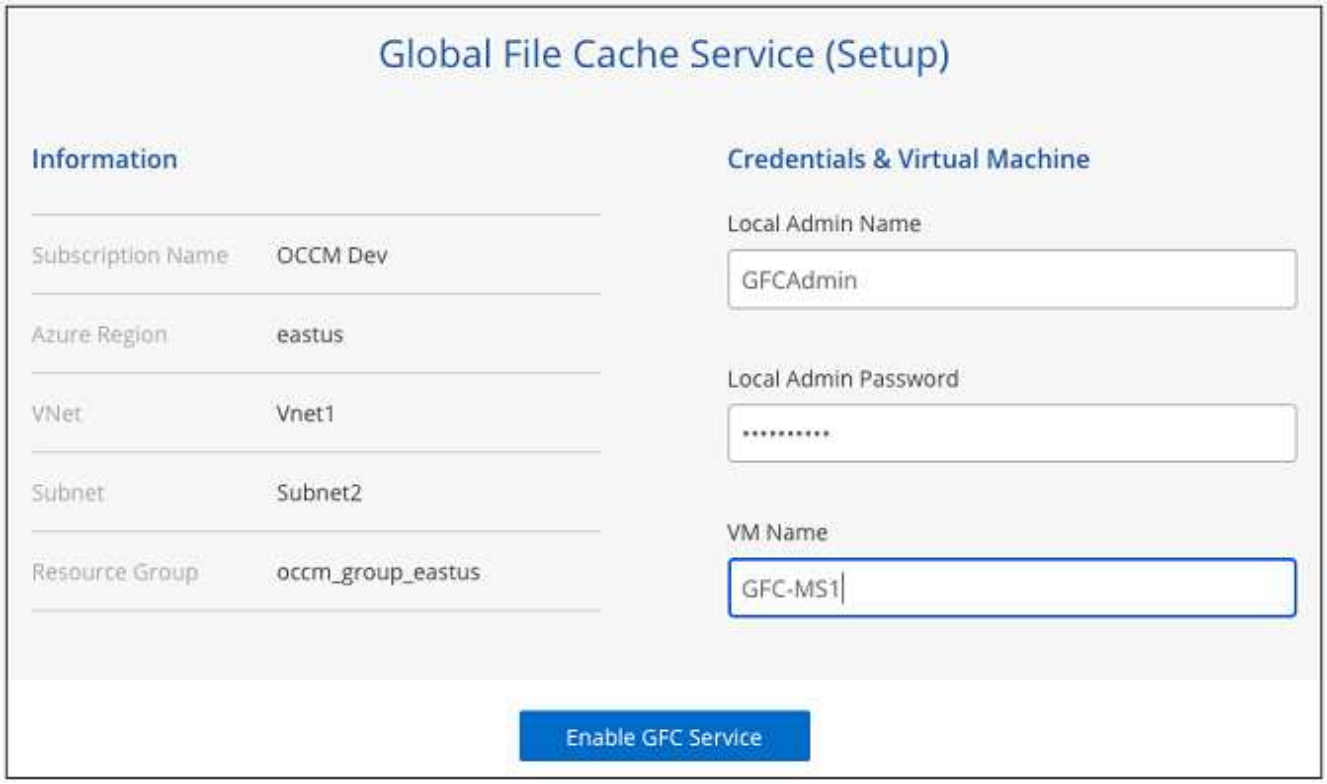
3. Lesen Sie die Übersichtsseite und klicken Sie auf **Weiter**.
4. Wenn auf der Cloud Volumes ONTAP-Instanz keine SMB-Freigaben verfügbar sind, werden Sie aufgefordert, die Details zur SMB-Server- und SMB-Freigabe einzugeben, um die Freigabe jetzt zu erstellen. Weitere Informationen zur SMB-Konfiguration finden Sie unter "Storage-Plattform".

   Wenn Sie fertig sind, klicken Sie auf **Weiter**, um die SMB-Freigabe zu erstellen.

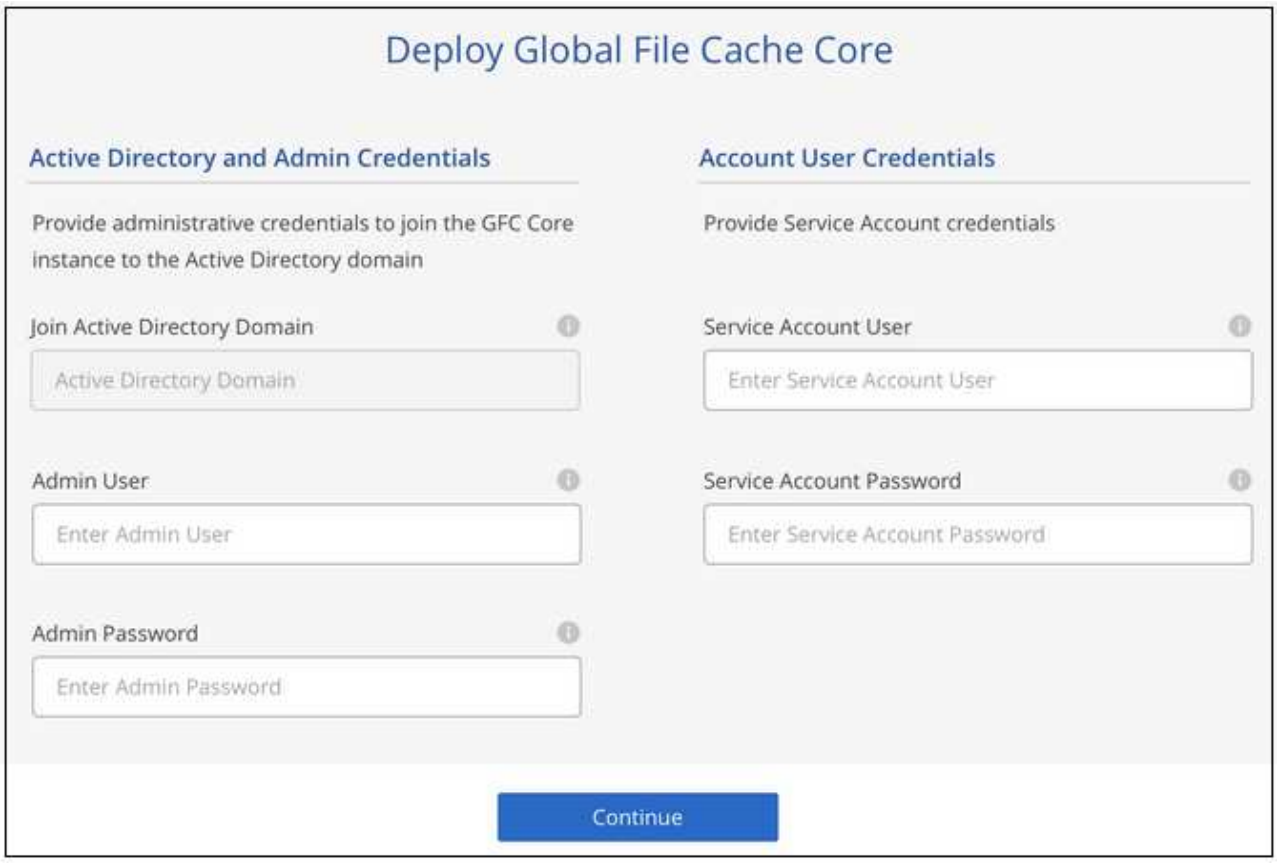
5. Geben Sie auf der Seite Global File Cache Service die Anzahl der zu implementierenden Instanzen für Global File Cache Edge ein und stellen Sie anschließend sicher, dass Ihr System die Anforderungen für Netzwerkkonfigurations- und Firewall-Regeln, Active Directory-Einstellungen und Antivirus-Ausschlüsse erfüllt. Siehe "Voraussetzungen" Entnehmen.



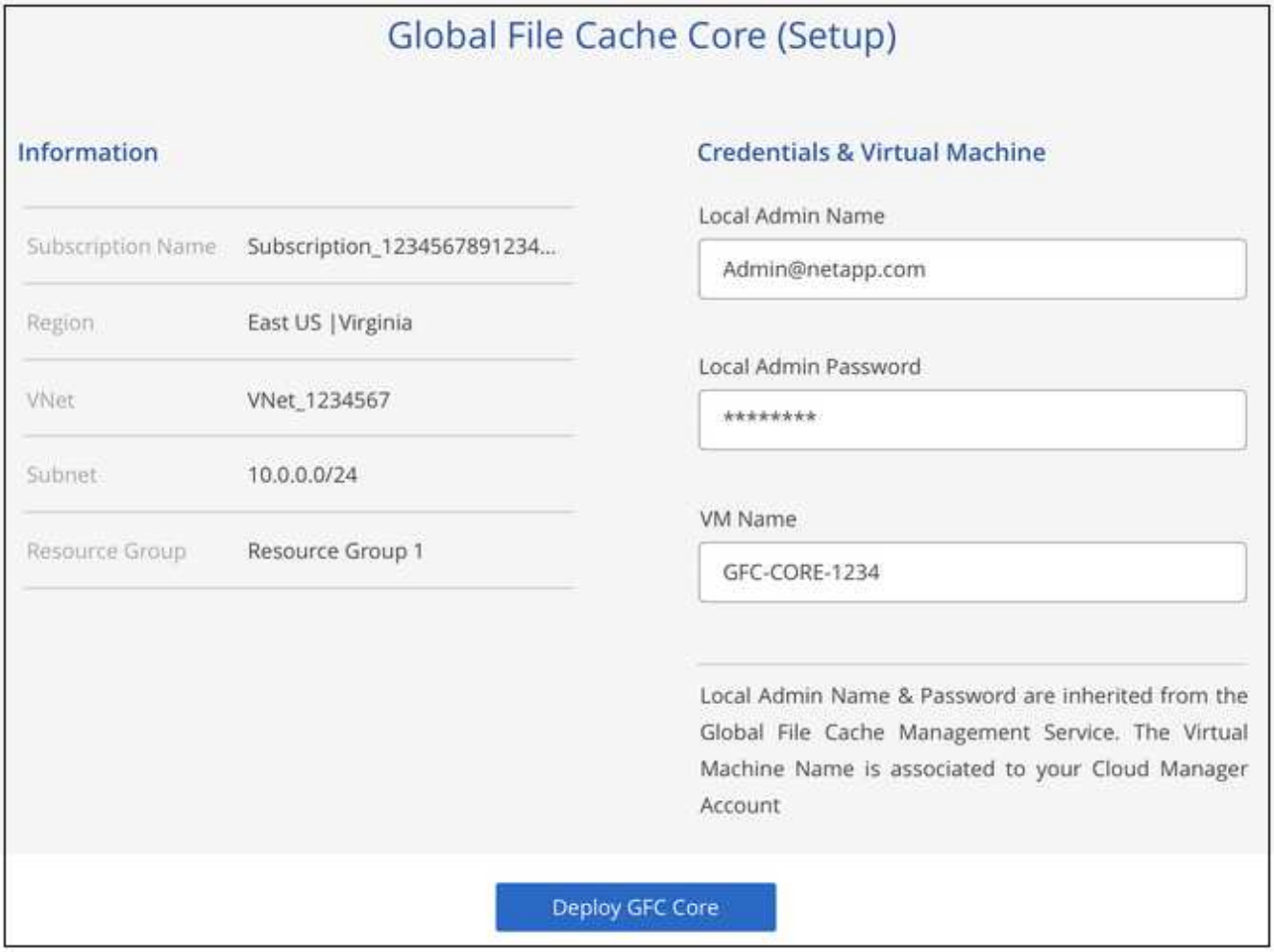
6. Nachdem Sie bestätigt haben, dass die Anforderungen erfüllt wurden oder dass Sie über die entsprechenden Informationen verfügen, klicken Sie auf **Weiter**.
7. Geben Sie die Admin-Zugangsdaten ein, die Sie für den Zugriff auf die VM des Global File Cache Management Servers verwenden möchten, und klicken Sie auf **GFC Service aktivieren**. Bei Azure geben Sie die Zugangsdaten als Benutzernamen und Passwort ein. Bei AWS wählen Sie das entsprechende Schlüsselpaar aus. Sie können den Namen der VM/Instanz bei Bedarf ändern.



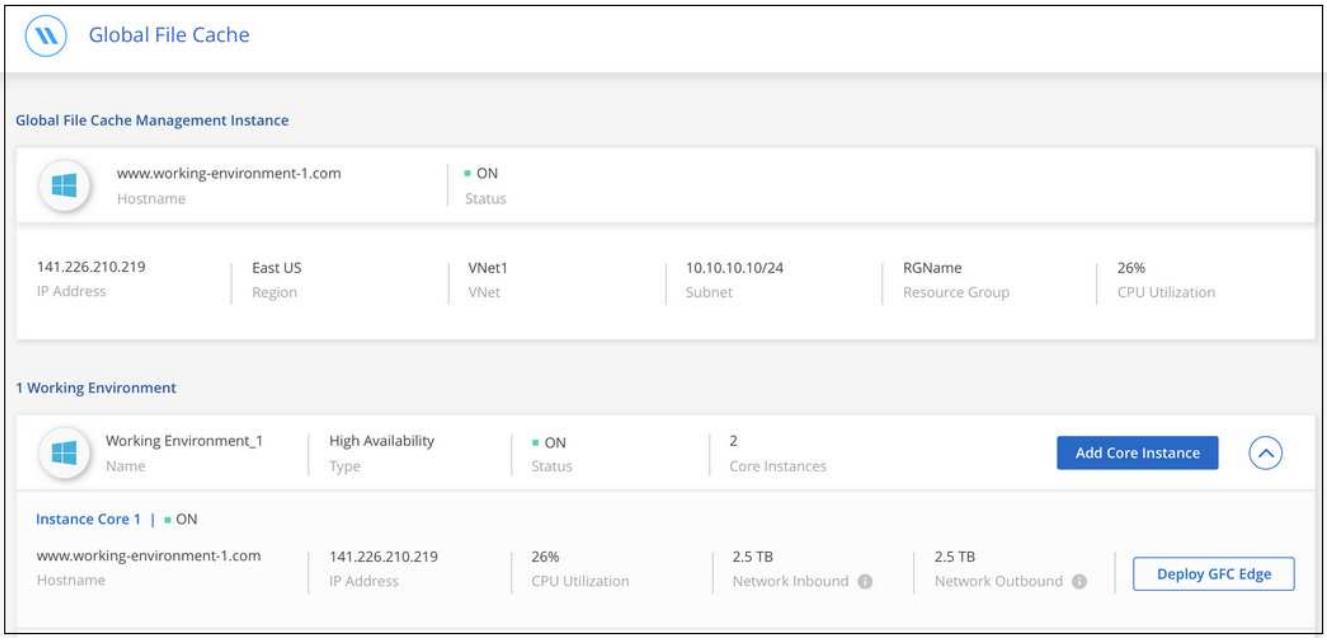
8. Klicken Sie nach der erfolgreichen Bereitstellung des Global File Cache Management Service auf **Weiter**.
9. Geben Sie für den Global File Cache Core die Anmeldedaten für Admin-Benutzer ein, um der Active Directory-Domäne beizutreten, und die Benutzeranmeldeinformationen für das Servicekonto. Klicken Sie dann auf **Weiter**.
   - Die Kern-Instanz des globalen Datei-Caches muss in derselben Active Directory-Domäne wie die Cloud Volumes ONTAP-Instanz bereitgestellt werden.
   - Das Dienstkonto ist ein DomainUser und ist Teil der BUILTIN\Backup Operators Gruppe auf der Cloud Volumes ONTAP Instanz.



10. Geben Sie die Admin-Zugangsdaten ein, die Sie für den Zugriff auf die Global File Cache Core VM verwenden möchten, und klicken Sie auf **GFC Core bereitstellen**. Bei Azure geben Sie die Zugangsdaten als Benutzernamen und Passwort ein. Bei AWS wählen Sie das entsprechende Schlüsselpaar aus. Sie können den Namen der VM/Instanz bei Bedarf ändern.



11. Wenn der Global File Cache Core erfolgreich bereitgestellt wurde, klicken Sie auf **Gehe zu Dashboard**.



Das Dashboard zeigt an, dass die Management-Server-Instanz und die Core-Instanz beide **an** und arbeiten.

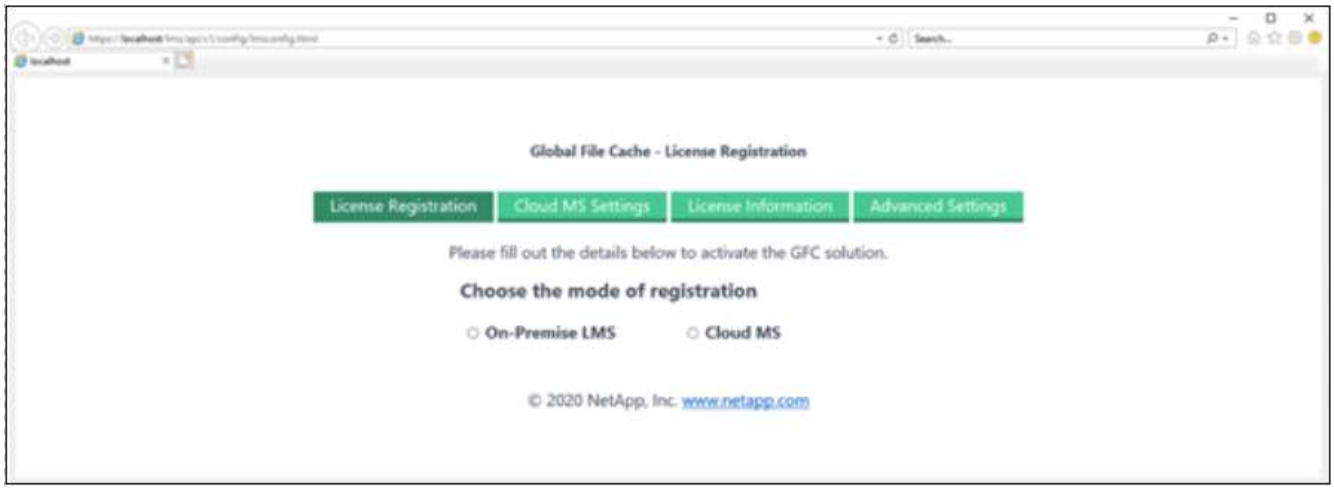
Lizenzieren Sie die Installation Ihres Global File Cache

Bevor Sie Global File Cache verwenden können, müssen Sie den LMS-Service (Global File Cache License Management Server) auf einer globalen File Cache Core-Instanz konfigurieren. Sie benötigen Ihre NSS-Zugangsdaten oder eine von NetApp bereitgestellte Kunden-ID, um Ihr Abonnement zu aktivieren.

In diesem Beispiel konfigurieren wir den LMS-Service auf einer Kerninstanz, die Sie gerade in der Public Cloud implementiert haben. Dies ist ein einmalige Prozess, mit dem Ihr LMS-Service eingerichtet wird.

Schritte

1. Öffnen Sie die Seite Registrierung für die Global File Cache Lizenz auf dem Global File Cache Core (der Kern, den Sie als LMS-Service bezeichnen) unter Verwendung der folgenden URL. Ersetzen Sie *<ip_Address>* durch die IP-Adresse des Global File Cache Core:https://<ip_address>/lms/api/v1/config/lmsconfig.html[]
2. Klicken Sie auf „Weiter zu dieser Website (nicht empfohlen)“, um fortzufahren. Es wird eine Seite angezeigt, auf der Sie das LMS konfigurieren oder vorhandene Lizenzinformationen prüfen können.



3. Wählen Sie den Registrierungsmodus, indem Sie „On-Premise LMS“ oder „Cloud MS“ auswählen.
   - „On-Premises LMS“ wird für bestehende oder Testkunden verwendet, die über den NetApp Support eine Kunden-ID erhalten haben.
   - „Cloud MS“ wird für Kunden verwendet, die NetApp Global File Cache Edge Lizenzen von NetApp oder seinen zertifizierten Partnern erworben haben und über ihre NetApp Zugangsdaten verfügen.
4. Klicken Sie für Cloud MS auf **Cloud MS**, geben Sie Ihre NSS-Anmeldeinformationen ein und klicken Sie auf **Absenden**.

5. Für lokale LMS klicken Sie auf **On-Premise LMS**, geben Sie Ihre Kunden-ID ein und klicken Sie auf **LMS registrieren**.

Nächste Schritte

Wenn Sie festgestellt haben, dass Sie mehrere Global File Cache-Kerne bereitstellen müssen, um Ihre Konfiguration zu unterstützen, klicken Sie im Dashboard auf **Core-Instanz hinzufügen** und folgen Sie dem Bereitstellungsassistenten.

Nachdem Sie die Kernbereitstellung abgeschlossen haben, müssen Sie sie durchführen "Implementieren Sie die globalen File Cache Edge-Instanzen" In allen Ihren Remote-Standorten aus.

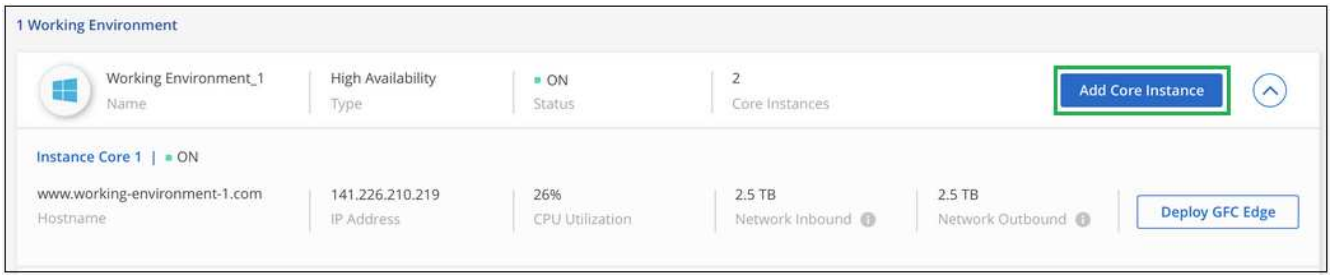
Implementierung zusätzlicher Core-Instanzen

Wenn Ihre Konfiguration mehr als einen globalen Datei-Cache-Kern benötigt, um installiert zu werden, weil eine große Anzahl von Edge-Instanzen, können Sie einen weiteren Kern in der Arbeitsumgebung hinzufügen.

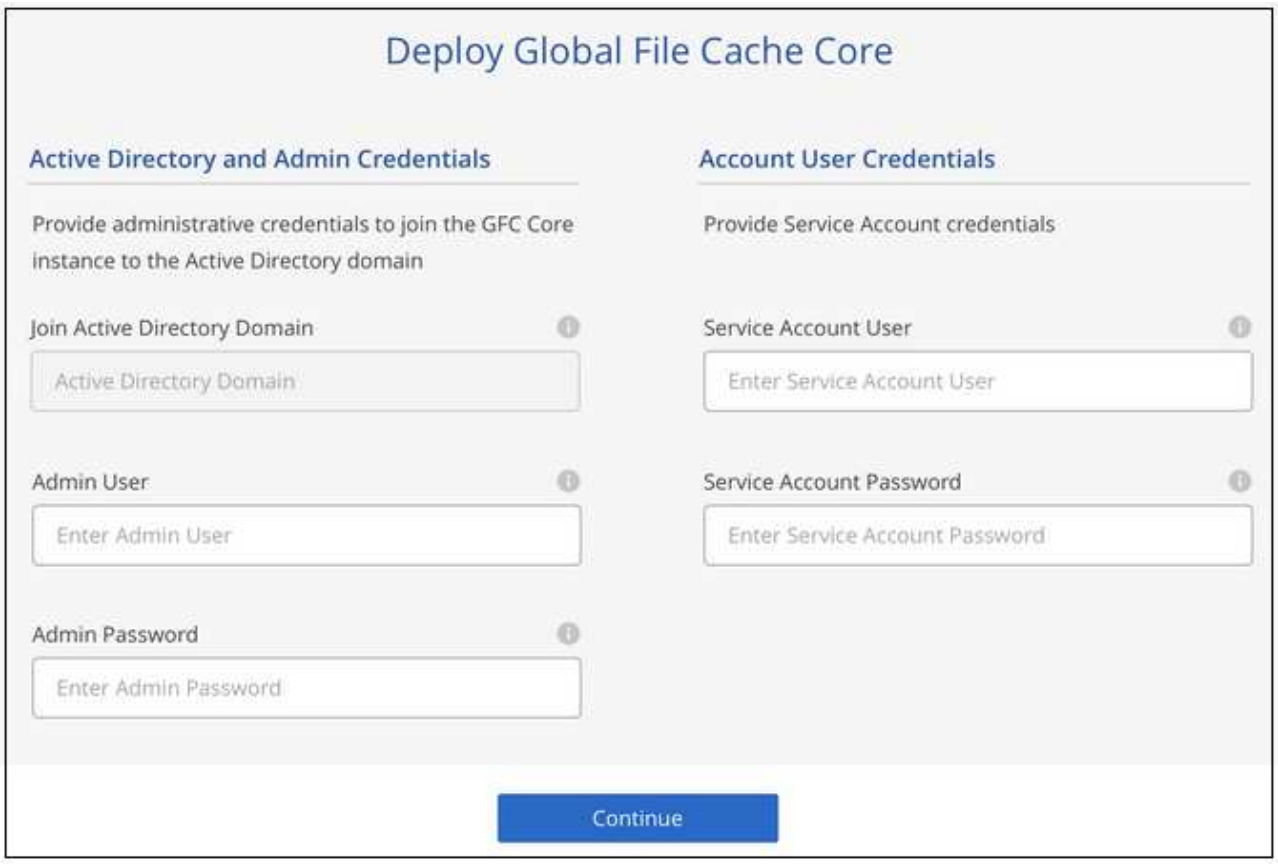
Wenn Sie Edge-Instanzen bereitstellen, konfigurieren Sie einige, um eine Verbindung zum ersten Kern und anderen zum zweiten Kern herzustellen. Beide Kerninstanzen greifen auf denselben Backend-Storage (Ihre

Cloud Volumes ONTAP-Instanz) in der Arbeitsumgebung zu.

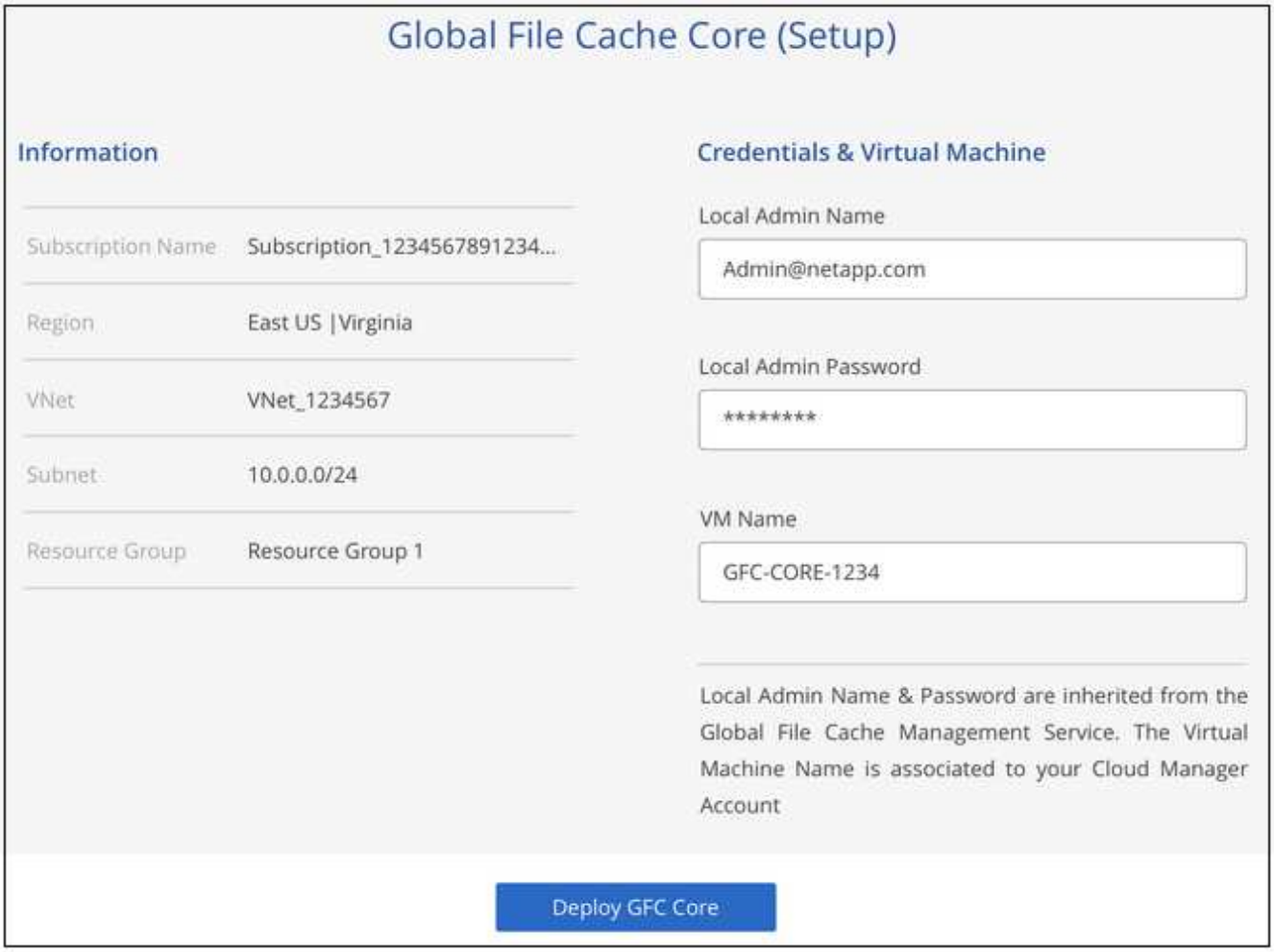
1. Klicken Sie im Global File Cache Dashboard auf **Core Instance hinzufügen**.



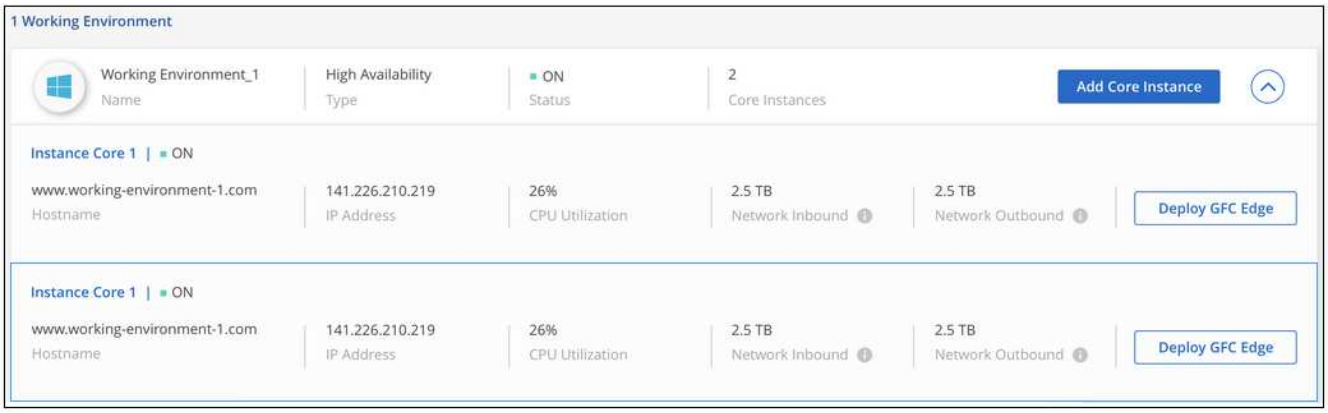
2. Geben Sie die Anmeldedaten des Admin-Benutzers ein, um der Active Directory-Domäne beizutreten, und die Benutzeranmeldeinformationen für das Dienstkonto. Klicken Sie dann auf **Weiter**.
   - Die Kern-Instanz des globalen Datei-Caches muss sich in derselben Active Directory-Domäne befinden wie die Cloud Volumes ONTAP-Instanz.
   - Das Dienstkonto ist ein DomainUser und ist Teil der BUILTIN\Backup Operators Gruppe auf der Cloud Volumes ONTAP Instanz.



3. Geben Sie die Admin-Zugangsdaten ein, die Sie für den Zugriff auf die Global File Cache Core VM verwenden möchten, und klicken Sie auf **GFC Core bereitstellen**. Bei Azure geben Sie die Zugangsdaten als Benutzernamen und Passwort ein. Bei AWS wählen Sie das entsprechende Schlüsselpaar aus. Sie können den Namen der VM auch bei Bedarf ändern.



4. Wenn der Global File Cache Core erfolgreich bereitgestellt wurde, klicken Sie auf **Gehe zu Dashboard**.



Das Dashboard gibt die zweite Kerninstanz für die Arbeitsumgebung wieder.

Bevor Sie mit der Bereitstellung von Global File Cache Edge-Instanzen beginnen

Es gibt viele Anforderungen, die Sie beachten müssen, bevor Sie beginnen, die Global File Cache Edge Software in Ihren Remote-Standorten zu installieren.

Laden Sie die erforderlichen Ressourcen herunter

Laden Sie die virtuellen Vorlagen für Global File Cache herunter, die Sie in Ihren Zweigstellen, im Software-Installationspaket und in zusätzlicher Referenzdokumentation verwenden möchten:

- Virtuelle Windows Server 2016-Vorlage:

  "Windows Server 2016 .OVA einschließlich NetApp GFC (VMware vSphere 6.5+)"
  "Windows Server 2016 .VHDX einschließlich NetApp GFC (Microsoft Hyper-V)"

- Virtuelle Windows Server 2019-Vorlage:

  "Windows Server 2019 .OVA einschließlich NetApp GFC (VMware vSphere 6.5+)"
  "Windows Server 2019 .VHDX einschließlich NetApp GFC (Microsoft Hyper-V)"

- Global File Cache Edge Software:

  "NetApp GFC-Software (EXE)"

- Global File Cache-Dokumentation:

  "NetApp Global File Cache User Guide"

Design und Bereitstellung von Global File Cache Edge

Je nach Ihren Anforderungen müssen Sie möglicherweise eine oder mehrere Global File Cache Edge-Instanzen basierend auf den gleichzeitigen Benutzersitzungen in einer Zweigstelle bereitstellen. Die Edge Instanz stellt die virtuelle Dateifreigabe für die Endbenutzer innerhalb der Zweigstelle dar, die auf transparente Weise von der zugehörigen globalen File Cache Core-Instanz erweitert wurde. Der Global File Cache Edge sollte einen enthalten `D:\` NTFS-Volume, das die zwischengespeicherten Dateien innerhalb der Zweigstelle enthält.

> Für den Global File Cache Edge ist es wichtig, die zu verstehen "Richtlinien für die Dimensionierung". Auf diese Weise können Sie das richtige Design für Ihre Global File Cache-Bereitstellung erstellen. Außerdem sollten Sie in Bezug auf Skalierbarkeit, Verfügbarkeit von Ressourcen und Redundanz die richtige Lösung für Ihre Umgebung bestimmen.

Global File Cache Edge Instanz

Wenn Sie eine globale File Cache Edge-Instanz bereitstellen, müssen Sie eine einzelne VM bereitstellen, entweder durch Bereitstellung von Windows Server 2016 Standard oder Datacenter Edition, Windows Server 2019 Standard oder Datacenter Edition oder durch Verwendung des Global File Cache `.OVA` Oder `.VHD` Vorlage, die das Betriebssystem der Wahl von Windows Server und die Software Global File Cache umfasst.

Schnelle Schritte

1. Stellen Sie die virtuelle Vorlage für Global File Cache oder Windows Server 2016 VM oder Windows Server 2019 Standard oder Datacenter Edition bereit.
2. Stellen Sie sicher, dass die VM mit dem Netzwerk verbunden ist, mit der Domäne verbunden ist und über RDP zugänglich ist.
3. Installieren Sie die neueste Software Global File Cache Edge.
4. Ermitteln Sie den Global File Cache Management Server und die Kerninstanz.

5. Konfigurieren Sie die Instanz für Global File Cache Edge.

Global File Cache Edge Anforderungen

Global File Cache Edge funktioniert plattformübergreifend und unterstützt Windows Server 2016 und 2019. Dadurch wird DIE IT an Remote-Standorten von Unternehmen vereinfacht. Global File Cache kann beispielsweise auf Ihrer vorhandenen Hardware-Infrastruktur, Virtualisierung oder Hybrid/Public Cloud-Umgebungen implementiert werden, wenn einige grundlegende Anforderungen erfüllt werden.

Global File Cache Edge erfordert für einen optimalen Betrieb die folgenden Hardware- und Software-Ressourcen. Weitere Informationen zu den allgemeinen Größenbemessungs-Richtlinien finden Sie unter "Richtlinien für die Dimensionierung".

Stabile Server-Appliance

Mit dem Global File Cache Installationspaket wird eine gesicherte Software Appliance auf jeder Microsoft Windows Server-Instanz erstellt. *Global File Cache Package nicht deinstallieren*. Durch die Deinstallation von Global File Cache wird die Funktionalität der Serverinstanz beeinträchtigt und möglicherweise muss die Serverinstanz vollständig neu erstellt werden.

Physische Hardwareanforderungen

- Mindestens 4 CPU-Kerne
- Mindestens 16 GB RAM
- Dedizierte Single- oder redundante 1-Gbit/s-NIC
- SAS-HDD mit 10.000 U/min oder SSD (bevorzugt)
- RAID-Controller mit Write-Back-Cache-Funktion aktiviert

Anforderungen für virtuelle Bereitstellung

Hypervisor-Plattformen sind hinsichtlich des Storage-Subsystems (beispielsweise Latenz) durch eine Performance-Verschlechterung bekannt. Um eine optimale Performance mit Global File Cache zu erzielen, wird eine physische Serverinstanz mit SSD empfohlen.

Zusätzlich zu den physischen Host-Anforderungen müssen für eine optimale Performance in virtuellen Umgebungen die folgenden Anforderungen und Ressourcenreservierungen erfüllt werden:

Microsoft Hyper-V 2012 R2 und höher:

- Prozessor (CPU): CPUs müssen als **statisch** gesetzt werden: Minimum: 4 vCPU Cores.
- Arbeitsspeicher (RAM): Mindestens 16 GB als **statisch** eingestellt.
- Festplattenbereitstellung: Festplatten müssen als **feste Festplatte** konfiguriert werden.

VMware vSphere 6.x und höher:

- Prozessor (CPU): Die Reservierung der CPU-Zyklen muss festgelegt werden. Minimum: 4 vCPU Cores @ 10000 MHz.
- Speicher (RAM): Minimum: Reservierung von 16 GB.
- Bereitstellung von Festplatten:
  - Disk Provisioning muss als **Thick Provisioning Eager Zeroed** eingerichtet werden.

    - Festplatten-Shares müssen auf **hoch** gesetzt werden.
    - Devices.hotplug muss mit dem vSphere Client auf **False** gesetzt werden, um zu verhindern, dass Microsoft Windows Global File Cache-Laufwerke als austauschbar präsentiert.
- Netzwerk: Netzwerkschnittstelle muss auf **VMXNET3** eingestellt sein (erfordert VM-Tools).

Global File Cache läuft unter Windows Server 2016 und 2019. Daher muss die Virtualisierungsplattform das Betriebssystem unterstützen sowie mit Utilities integriert werden, welche die Performance des Gastbetriebssystems der VM und das Management der VM verbessern, wie z. B. VM Tools.

Anforderungen für die Partitionsgröße

- C:\ - mindestens 250 GB (System-/Boot-Volume)
- D:\ - mindestens 1 TB (separates Datenvolumen für Global File Cache Intelligent File Cache*)

*Die Mindestgröße beträgt 2x der aktive Datensatz. Das Cache-Volume (D:\) kann erweitert werden und wird nur durch die Einschränkungen des Microsoft Windows NTFS-Dateisystems eingeschränkt.

Anforderungen an Global File Cache Intelligent File Cache-Festplatten

Die Festplattenlatenz auf der intelligenten File Cache-Festplatte (D:\) von Global File Cache sollte eine durchschnittliche I/O-Plattenlatenz von < 0,5 ms und einen Durchsatz von 1 MiPS pro paralleler Benutzer bieten.

Weitere Informationen finden Sie im "NetApp Global File Cache User Guide".

Netzwerkbetrieb

- Firewall: TCP-Ports sollten zwischen dem Global File Cache Edge und Management Server und Core Instanzen erlaubt sein.

  Global File Cache TCP Ports: 443 (HTTPS - LMS), 6618 – 6630.

- Netzwerkoptimierungs-Geräte (wie Riverbed Steelhead) müssen so konfiguriert werden, dass sie über die für Global File Cache spezifischen Ports (TCP 6618-6630) weitergeleitet werden.

Best Practices für Client-Workstations und Anwendungen

Global File Cache lässt sich transparent in die Umgebungen des Kunden integrieren, sodass Benutzer über ihre Client-Workstations auf zentrale Daten zugreifen können, auf denen Unternehmensanwendungen ausgeführt werden. Über Global File Cache wird der Zugriff auf Daten über eine direkte Laufwerkszuordnung oder über einen DFS-Namespace ermöglicht. Weitere Informationen zum Global File Cache Fabric, zum intelligenten File Caching und zu wichtigen Aspekten der Software finden Sie im "Bevor Sie mit der Bereitstellung von Global File Cache beginnen" Abschnitt.

Um eine optimale Erfahrung und Leistung zu gewährleisten, ist es wichtig, die Anforderungen und Best Practices des Microsoft Windows Clients gemäß dem Benutzerhandbuch für den Global File Cache zu erfüllen. Dies gilt für alle Versionen von Microsoft Windows.

Weitere Informationen finden Sie im "NetApp Global File Cache User Guide".

Best Practices für Firewall und Virenschutz

Obwohl Global File Cache in angemessenem Umfang die Validierung der Kompatibilität der gängigsten

Antivirus-Applikationssuiten mit Global File Cache prüfen kann, kann NetApp keine Garantie übernehmen und ist nicht verantwortlich für Inkompatibilitäten oder Performance-Probleme, die durch diese Programme oder die damit verbundenen Updates, Service Packs oder Änderungen verursacht werden.

Global File Cache empfiehlt weder die Installation noch die Anwendung von Monitoring- oder Antivirenlösungen auf einer Global File Cache-fähigen Instanz (Core oder Edge). Sollte eine Lösung nach Wahl oder Richtlinie installiert werden, müssen folgende Best Practices und Empfehlungen umgesetzt werden: Allgemeine Virenschutzsuiten finden Sie in Anhang A im "NetApp Global File Cache User Guide".

Firewall-Einstellungen

- Microsoft Firewall:
  - Behalten Sie die Firewall-Einstellungen als Standard bei.
  - Empfehlung: Belassen Sie die Microsoft Firewall-Einstellungen und -Dienste bei der Standardeinstellung AUS und nicht gestartet für Standard Global File Cache Edge-Instanzen.
  - Empfehlung: Belassen Sie die Microsoft Firewall-Einstellungen und -Dienste bei der Standardeinstellung EIN und starten Sie für Edge-Instanzen, die auch die Domain Controller-Rolle ausführen.
- Unternehmens-Firewall:
  - Global File Cache Core Instance wartet auf TCP-Ports 6618-6630, stellen Sie sicher, dass Global File Cache Edge-Instanzen eine Verbindung zu diesen TCP-Ports herstellen können.
  - Global File Cache-Instanzen erfordern eine Kommunikation mit dem Global File Cache Management Server auf TCP-Port 443 (HTTPS).
- Lösungen/Geräte zur Netzwerkoptimierung müssen für spezifische Ports des Global File Cache konfiguriert sein.

Best Practices für Antiviren-Software

Dieser Abschnitt enthält Informationen zu den Anforderungen, die beim Ausführen von Antivirensoftware auf einer Windows Server-Instanz mit Global File Cache erforderlich sind. Global File Cache hat die am häufigsten verwendeten Antivirenprodukte wie Cylance, McAfee, Symantec, Sophos, Trend Micro, Kaspersky und Windows Defender zur Verwendung in Verbindung mit Global File Cache.

Das Hinzufügen von Antiviren-Software zu einer Edge Appliance kann 10 bis 20 % Auswirkungen auf die Benutzer-Performance haben.

Weitere Informationen finden Sie im "NetApp Global File Cache User Guide".

Konfigurationsausschlüsse

Antivirus-Software oder andere Indexierung oder Scan-Dienstprogramme von Drittanbietern sollten niemals Laufwerk D:\ auf der Edge-Instanz scannen. Diese Scans des Edge Server-Laufwerks D:\ führen zu zahlreichen offenen Datei-Anfragen für den gesamten Cache-Namespace. Dadurch werden Dateiabholungen über das WAN auf alle Dateiserver im Rechenzentrum optimiert. Eine Überflutung der WAN-Verbindung und eine unnötige Belastung der Edge-Instanz führen zu Leistungseinbußen.

Zusätzlich zum Laufwerk D:\ sollten in der Regel das folgende Verzeichnis und die folgenden Prozesse des Global File Cache von allen Antivirenanwendungen ausgeschlossen werden:

- `C:\Program Files\TalonFAST\`

- `C:\Program Files\TalonFAST\Bin\LMClientService.exe`
- `C:\Program Files\TalonFAST\Bin\LMServerService.exe`
- `C:\Program Files\TalonFAST\Bin\Optimus.exe`
- `C:\Program Files\TalonFAST\Bin\tafsexport.exe`
- `C:\Program Files\TalonFAST\Bin\tafsutils.exe`
- `C:\Program Files\TalonFAST\Bin\tapp.exe`
- `C:\Program Files\TalonFAST\Bin\tfs.exe`
- `C:\Program Files\TalonFAST\Bin\TService.exe`
- `C:\Program Files\TalonFAST\Bin\tum.exe`
- `C:\Program Files\TalonFAST\FastDebugLogs\`
- `C:\Windows\System32\drivers\tfast.sys`
- `\\?\TafsMtPt:\ or \\?\TafsMtPt*`
- `\Device\TalonCacheFS\`
- `\\?\GLOBALROOT\Device\TalonCacheFS\`
- `\\?\GLOBALROOT\Device\TalonCacheFS\*`

NetApp Support-Richtlinie

Global File Cache-Instanzen wurden speziell für Global File Cache als primäre Applikation konzipiert, die auf einer Windows Server 2016- und 2019-Plattform ausgeführt wird. Global File Cache erfordert bevorzugten Zugriff auf Plattformressourcen, z. B. Festplatte, Speicher, Netzwerkschnittstellen Und kann hohe Anforderungen an diese Ressourcen stellen. Für virtuelle Bereitstellungen sind Arbeitsspeicher-/CPU-Reservierungen und hochperformante Festplatten erforderlich.

- Für Bereitstellungen von Global File Cache in Zweigstellen sind unterstützte Services und Applikationen auf dem Server mit Global File Cache beschränkt auf:
  - DNS/DHCP
  - Active Directory Domain Controller (globaler Datei-Cache muss sich auf einem separaten Volume befinden)
  - Druckservices
  - Microsoft System Center Configuration Manager (SCCM)
  - Global File Cache genehmigte Client-seitige Systemagenten und Virenschutzapplikationen
- NetApp Support und Wartung gilt nur für Global File Cache.
- Eine Line-of-Business-Produktivitätssoftware, die normalerweise ressourcenintensiv sind, z. B. Datenbankserver, Mail-Server usw. Werden nicht unterstützt.
- Der Kunde ist für alle nicht-Global File Cache-Software verantwortlich, die auf dem Server installiert werden kann, auf dem Global File Cache ausgeführt wird:
  - Wenn ein Software-Paket von Drittanbietern Software- oder Ressourcenkonflikte mit Global File Cache verursacht oder die Leistung beeinträchtigt wird, kann die Support-Organisation von Global File Cache den Kunden dazu zwingen, die Software aus dem Server zu deaktivieren oder zu entfernen, auf dem Global File Cache ausgeführt wird.

    - Es liegt in der Verantwortung des Kunden für die Installation, Integration, Unterstützung und das Upgrade jeder Software, die dem Server hinzugefügt wird, auf dem die Global File Cache-Anwendung ausgeführt wird.
- System Management Utilities/Agents wie Antivirus-Tools und Lizenzagenten können möglicherweise koexistieren. Mit Ausnahme der oben aufgeführten unterstützten Services und Applikationen werden diese Applikationen jedoch nicht von Global File Cache unterstützt, und es müssen immer noch die oben genannten Richtlinien befolgt werden:
    - Der Kunde ist für die Installation, Integration, Unterstützung und Aktualisierung von Software verantwortlich.
    - Wenn ein Kunde ein Softwarepaket von Drittanbietern installiert, das dazu führt, dass Software- oder Ressourcenkonflikte mit dem Global File Cache oder der Performance auftreten, kann es erforderlich sein, dass die Support-Abteilung von Global File Cache die Software deaktiviert/entfernt.

Implementierung globaler File Cache Edge-Instanzen

Nachdem Sie überprüft haben, ob Ihre Umgebung alle Anforderungen erfüllt, installieren Sie die Software Global File Cache Edge an jedem Remote Standort.

Bevor Sie beginnen

Zum Abschließen der Konfigurationsaufgaben für Global File Cache Edge benötigen Sie die folgenden Informationen:

- Statische IP-Adressen für jede Global File Cache-Instanz
- Subnetzmaske
- Gateway-IP-Adresse
- Der FQDN, den Sie jedem Global File Cache-Server zuweisen möchten
- Das DNS-Suffix (optional)
- Benutzername und Passwort eines administrativen Benutzers in der Domäne
- Der FQDN und/oder die IP-Adresse der zugehörigen Core-Server
- Ein Volume, das als intelligenter Datei-Cache verwendet werden soll. Es wird empfohlen, dass dieser mindestens die doppelte Größe des aktiven Datensatzes hat. Dies sollte als NTFS formatiert und als zugewiesen werden `D:\`.

Häufig verwendete TCP-Ports

Es gibt mehrere TCP-Ports, die von Global File Cache-Diensten verwendet werden. Es ist zwingend erforderlich, dass die Geräte über diese Ports kommunizieren können und von allen WAN-Optimierungsgeräten oder Firewall-Einschränkungsrichtlinien ausgeschlossen werden:

- Global File Cache Licensing TCP-Port: 443
- Global File Cache TCP Ports: 6618-6630

Stellen Sie die virtuelle Vorlage für Global File Cache bereit

Die virtuelle Vorlage `.OVA` Und `.VHD`) Bilder enthalten die neueste Version der Software Global File Cache. Wenn Sie Global File Cache mit bereitstellen `.OVA` Oder `.VHD` Virtual Machine (VM)-Vorlage, befolgen Sie die in diesem Abschnitt beschriebenen Schritte. Es wird vorausgesetzt, dass Sie die korrekte Implementierung des

kennen `.OVA` Oder `.VHD` Vorlage auf der designierten Hypervisor-Plattform.

Stellen Sie sicher, dass die VM-Einstellungen, einschließlich Ressourcenreservierungen, den in aufgeführten Anforderungen entsprechen "Anforderungen für virtuelle Bereitstellung".

Schritte

1. Extrahieren Sie das Paket aus der von Ihnen heruntergeladenen Vorlage.
2. Implementieren Sie die virtuelle Vorlage. Lesen Sie sich vor Beginn der Implementierung die folgenden Videos durch:
   - "Implementieren Sie die virtuelle Vorlage auf VMware"
   - "Implementieren Sie die virtuelle Vorlage auf Hyper-V"
3. Starten Sie nach der Implementierung der virtuellen Vorlage und beim Konfigurieren der VM-Einstellungen die VM.
4. Wenn das Betriebssystem Windows Server 2016 oder 2019 sich für den ersten Einsatz vorbereitet, füllen Sie das sofort einsetzbare Erlebnis aus, indem Sie die richtigen Treiber installieren und die erforderlichen Komponenten für die jeweilige Hardware installieren.
5. Wenn die Basisinstallation der Global File Cache Edge-Instanz abgeschlossen ist, führt das Betriebssystem Windows Server 2016 oder 2019 Sie durch einen Assistenten zur Erstkonfiguration, um Betriebssystemspezifika wie Lokalisierung und Produktschlüssel zu konfigurieren.
6. Melden Sie sich nach Abschluss des Assistenten für die Erstkonfiguration lokal beim Betriebssystem Windows Server 2016 oder 2019 an, wobei die folgenden Anmeldedaten verwendet werden:
   - Benutzername: **FASTAdmin**
   - Passwort: **Tal0nFAST!**
7. Konfigurieren Sie Ihre Windows Server-VM, fügen Sie sich der Active Directory-Domäne des Unternehmens bei und fahren Sie mit dem Abschnitt Konfiguration des globalen Datei-Cache fort.

Konfigurieren Sie die Instanz für Global File Cache Edge

Die globale File Cache Edge-Instanz stellt eine Verbindung zu einem globalen File Cache Core her, um Benutzern in der Zweigstelle Zugriff auf die File-Server-Ressourcen des Datacenters zu ermöglichen.

> Die Edge-Instanz muss im Rahmen Ihrer Cloud Volumes ONTAP-Implementierung lizenziert sein, bevor mit der Konfiguration beginnt. Siehe "Lizenzierung" Weitere Informationen zur Lizenzierung.

Wenn Ihre Konfiguration aufgrund einer großen Anzahl von Edge-Instanzen mehr als einen globalen Datei-Cache-Kern benötigt, konfigurieren Sie einige Edge-Instanzen, um eine Verbindung mit dem ersten Kern und anderen zu verbinden, um eine Verbindung mit dem zweiten Kern herzustellen. Stellen Sie sicher, dass Sie über den FQDN oder die IP-Adresse und weitere erforderliche Informationen für die richtige Kerninstanz verfügen.

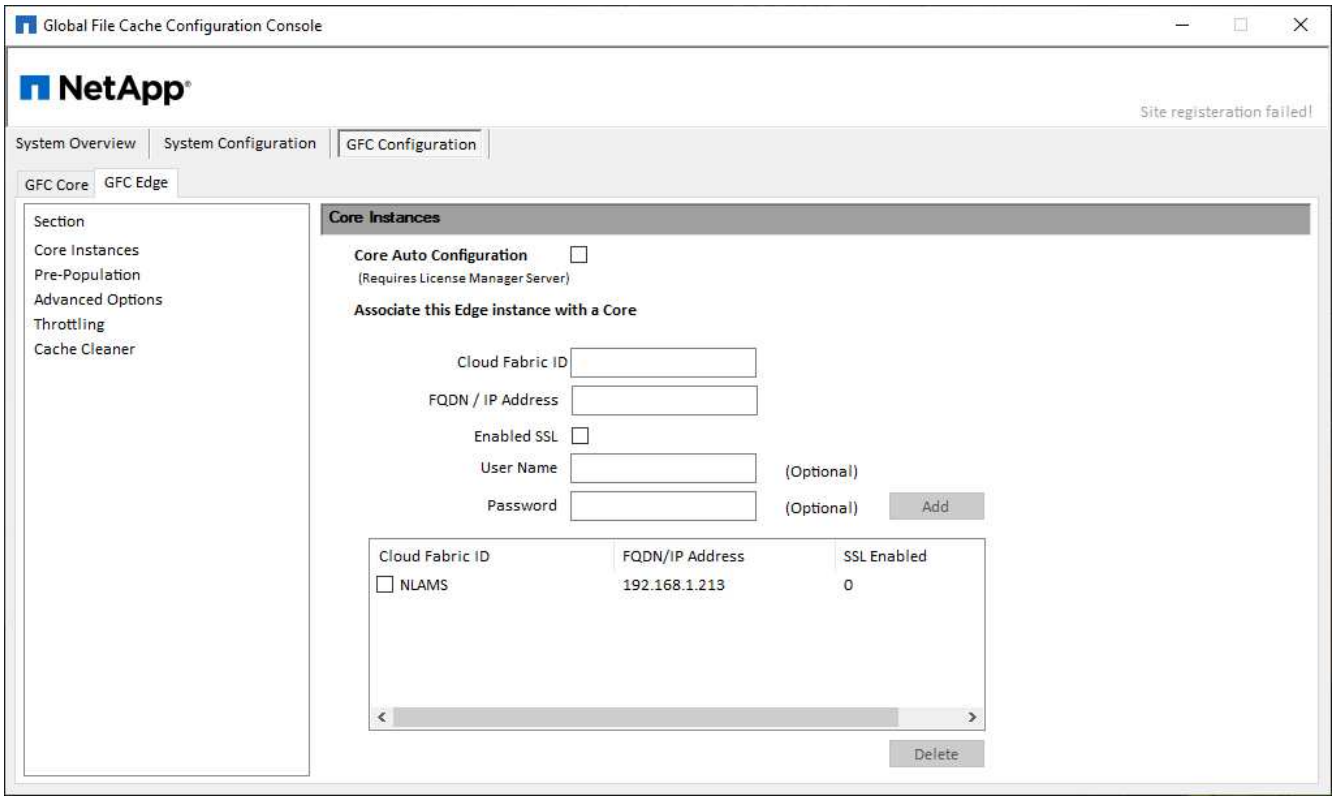
Führen Sie die folgenden Schritte aus, um die Edge-Instanz zu konfigurieren:

Schritte

1. Klicken Sie neben dem Schritt nicht markiert Core Configuration im Abschnitt „Edge Configuration Steps“ des Assistenten für die Erstkonfiguration auf **Ausführen**. Dadurch wird eine neue Registerkarte, GFC Edge, geöffnet und der Abschnitt *Core-Instanzen* angezeigt.
2. Geben Sie die **Cloud Fabric ID** des Global File Cache Core Servers an. Die Cloud-Fabric-ID ist

normalerweise der NetBIOS-Name oder der geografische Standort des Back-End-Fileservers.

3. Geben Sie die **FQDN/IP-Adresse** des Global File Cache Core-Servers an:
   a. (Optional) Aktivieren Sie die **SSL**-Box, um SSL-Unterstützung für erweiterte Verschlüsselung von Edge zu Core zu aktivieren.
   b. Geben Sie den Benutzernamen und das Kennwort ein. Dies sind die Anmeldeinformationen des im Core verwendeten Dienstkontos.
4. Klicken Sie auf **Hinzufügen**, um das Hinzufügen der Global File Cache Core-Appliance zu bestätigen. Es wird ein Bestätigungsfeld angezeigt. Klicken Sie auf **OK**, um es zu schließen.



Aktualisierung der Software Global File Cache Edge

Global File Cache veröffentlicht regelmäßig Software-Updates, entweder Patches, Erweiterungen oder neue Funktionen. Obwohl die virtuelle Vorlage (`.OVA` Und `.VHD`) Images enthalten die neueste Version der Global File Cache Software. Es kann sein, dass eine neuere Version im NetApp Support Download Portal verfügbar ist.

Stellen Sie sicher, dass Ihre Global File Cache-Instanzen mit der neuesten Version auf dem neuesten Stand sind.

> Dieses Softwarepaket kann auch für makellose Installationen auf Microsoft Windows Server 2016 Standard oder Datacenter Edition oder Windows Server 2019 Standard oder Datacenter Edition verwendet oder als Teil Ihrer Upgrade-Strategie verwendet werden.

Im Folgenden finden Sie die Schritte, die zum Aktualisieren des Installationspakets für den Global File Cache erforderlich sind:

Schritte

1. Nachdem Sie das neueste Installationspaket auf der gewünschten Windows Server-Instanz gespeichert haben, doppelklicken Sie darauf, um die ausführbare Installationsdatei auszuführen.
2. Klicken Sie auf **Weiter**, um den Vorgang fortzusetzen.
3. Klicken Sie auf **Weiter**, um fortzufahren.
4. Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
5. Wählen Sie den gewünschten Speicherort für das Installationsziel aus.

   NetApp empfiehlt, den Standardspeicherort für Installationen zu verwenden.
6. Klicken Sie auf **Weiter**, um fortzufahren.
7. Wählen Sie den Ordner Startmenü.
8. Klicken Sie auf **Weiter**, um fortzufahren.
9. Überprüfen Sie die gewünschten Installationsparameter und klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

   Die Installation wird ausgeführt.
10. Starten Sie nach Abschluss der Installation den Server neu, wenn Sie dazu aufgefordert werden.

Nächste Schritte

Weitere Informationen zur erweiterten Konfiguration von Global File Cache Edge finden Sie im "NetApp Global File Cache User Guide".

Endbenutzerschulung

Sie sollten Ihre Benutzer auf die Best Practices für den Zugriff auf gemeinsam genutzte Dateien über Global File Cache Schulen.

Dies ist die letzte Phase der Implementierung des Global File Cache, der Endanwender.

Um den Onboarding-Prozess für Endbenutzer vorzubereiten und zu optimieren, verwenden Sie die unten stehende E-Mail-Vorlage, mit der Sie die Endbenutzer darüber informieren können, was es bedeutet, in einer „zentralen Data“-Umgebung zu arbeiten. Auf diese Weise können Ihre Benutzer alle Vorteile der Global File Cache-Lösung nutzen. Außerdem haben wir ein Video veröffentlicht, das freigegeben werden kann, um Benutzer bei Bedarf zu „Schulen“.

Anpassen und Weiterleiten folgender Ressourcen an Endbenutzer zur Vorbereitung der Implementierung:

- Video zur Benutzerschulung"Schulungsvideo für Endbenutzer"
- E-Mail-Vorlage"Mac E-Mail-Vorlage (.emltpl)"

  "Windows E-Mail-Vorlage (.msg)"
- Onboarding-Kommunikation"Word-Dokument (.docx)"

Siehe Kapitel 12 im "NetApp Global File Cache User Guide" Für zusätzliches Material.

Weitere Informationen

Über die folgenden Links erhalten Sie weitere Informationen zu Global File Cache und anderen NetApp Produkten:

- Häufig gestellte Fragen zum Global File Cache
  - Sehen Sie sich eine Liste mit häufig gestellten Fragen und Antworten an "Hier"
- "NetApp Global File Cache User Guide"
- NetApp Produktdokumentation
  - Siehe zusätzliche Dokumentation für NetApp Cloud-Produkte "Hier"
  - Siehe zusätzliche Dokumentation für alle NetApp Produkte "Hier"
- Kunden-Support für Global File Cache-Benutzer mit Cloud Volumes ONTAP steht über folgende Kanäle zur Verfügung:
  - Geführte Problemlösung, Case-Management, Knowledgebase, Downloads, Tools, Und weitere gehen "Hier"
  - Melden Sie sich beim NetApp Support unter an https://mysupport.netapp.com Mit Ihren NSS-Anmeldedaten
  - Sofortige Unterstützung für P1-Fehler: +1 856.481.3990 (Option 2)
- Kunden-Support für globale File Cache-Benutzer, die Cloud Volumes Services und Azure NetApp Files nutzen, ist über Standardsupport Ihres Providers erhältlich. Wenden Sie sich an den Google-Kundendienst bzw. den Microsoft-Kundendienst.

Cloud-Computing-Kosten optimieren

Weitere Informationen zum Computing-Service

Durch den Einsatz "Spot Cloud Analyzer Service", Cloud Manager bietet eine allgemeine Kostenanalyse Ihrer Cloud-Computing-Ausgaben und zeigt potenzielle Einsparungen auf.

Cloud Analyzer ist eine Cloud-Infrastrukturmanagement-Lösung mit erweiterten Analysefunktionen, die Transparenz und Einblicke in Ihre Cloud-Kosten ermöglicht. Es zeigt Ihnen, wo Sie diese Kosten optimieren können und lässt Sie diese Optimierung mit Spot-Portfolio von kontinuierlichen Optimierungsprodukten in nur wenigen Klicks implementieren.

Funktionen

- Eine Kostenanalyse, die die aktuellen Kosten des Monats, die prognostizierten monatlichen Kosten und verpasste Einsparungen aufzeigt
- Eine Übersicht über die Ausgabeneffizienz nach Account, einschließlich der geschätzten zusätzlichen Einsparungen
- Ein Link zum Cloud Analyzer von Spot zu Einzelheiten über die Ausgaben für alle Accounts

Unterstützte Cloud-Provider

Dieser Service wird mit AWS unterstützt.

Kosten

Die Nutzung dieses Service ist über Cloud Manager kostenlos.

Funktionsweise von Cloud Analyzer mit Cloud Manager

Die Cloud Analyzer Integration auf höherer Ebene in Cloud Manager funktioniert folgendermaßen:

1. Klicken Sie auf **berechnen** und verbinden Sie Ihr AWS Master Payer Konto.
2. NetApp konfiguriert Ihre Umgebung wie folgt:
   a. Aufbau einer Organisation in der Spot-Plattform
   b. Sendet eine E-Mail, die Sie zu Spot empfängt.

      Sie können sich mit denselben Single-Sign-On-Anmeldedaten wie Cloud Central und Cloud Manager beim Spot-Service anmelden.

   c. Cloud Analyzer beginnt mit der Verarbeitung Ihrer AWS Kontodaten.
3. In Cloud Manager wird die Seite „Computing“ aktualisiert. Anhand der Informationen werden vergangene, aktuelle und zukünftige Cloud-Kosten analysiert.
4. Klicken Sie jederzeit auf **vollständige Analyse**, um zu Spot’s Cloud Analyzer zu gelangen, das eine vollständige Analyse Ihrer Cloud-Ausgaben und Einsparungsmöglichkeiten ermöglicht.

Datensicherheit

Cloud Analyzer-Daten sind im Ruhezustand verschlüsselt und es werden keine Anmeldedaten für ein Konto gespeichert.

Beginnen Sie damit, Ihre Cloud-Computing-Kosten zu optimieren

Binden Sie Ihren AWS Konto ein und nutzen Sie anschließend die Analyse, um Ihre Cloud-Computing-Kosten zu optimieren.

Verbinden Sie Cloud Analyzer mit Ihrem AWS Konto

Klicken Sie auf **Computing** und verbinden Sie Ihr AWS-Konto.

Schritte

1. Klicken Sie Auf **Computing**.
2. Klicken Sie auf **AWS Zugangsdaten zum Start** hinzufügen.
3. Folgen Sie den Schritten auf der Seite, um Ihr AWS Konto zu verbinden:

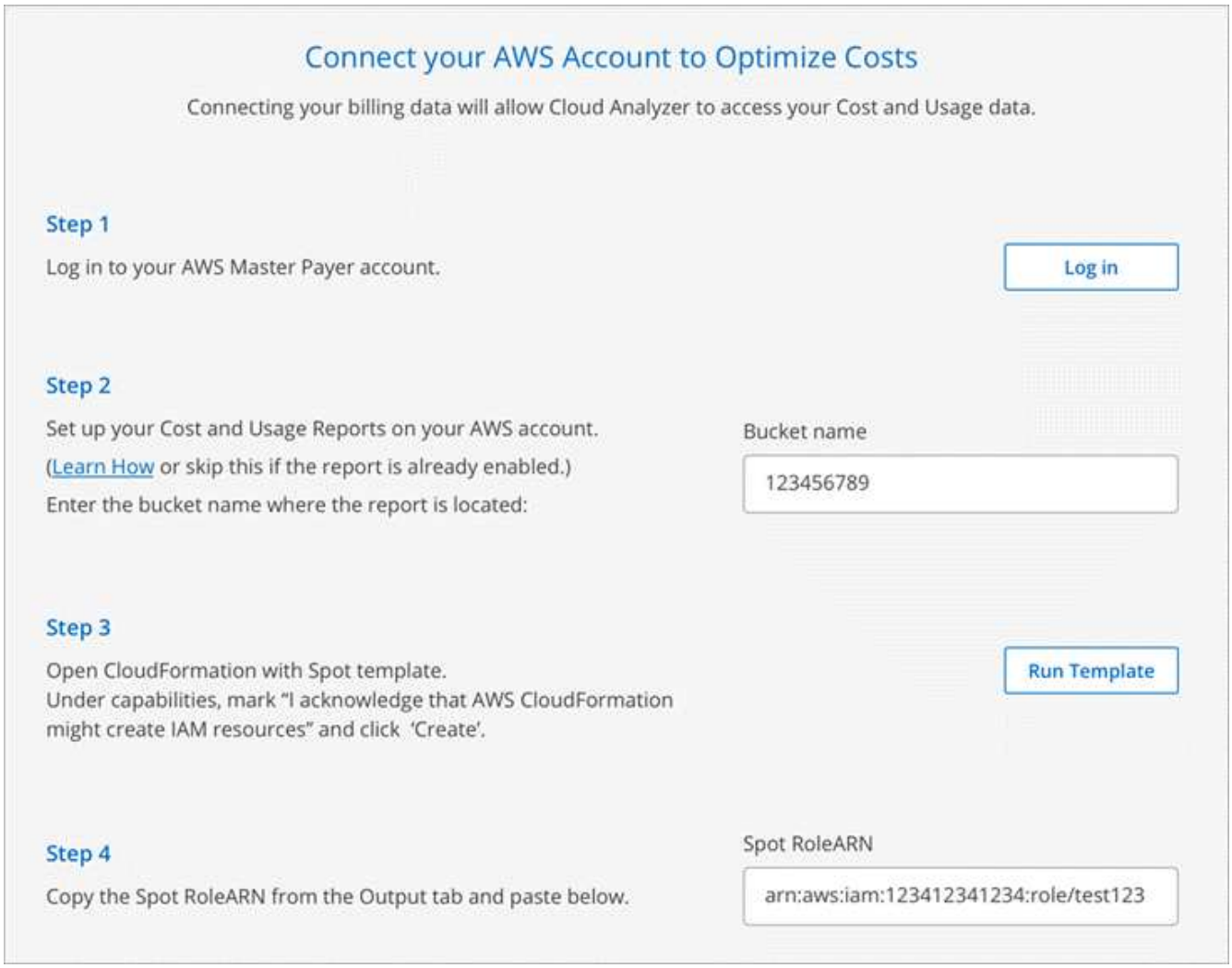
    a. Melden Sie sich bei Ihrem AWS Master Payer Konto an.

    b. Kostenberichte und Nutzungsberichte für das AWS Konto einrichten

    c. Führen Sie die CloudFormation-Vorlage aus.

    d. Fügen Sie die SonderrollenARN ein.

    "Zeigen Sie weitere Details zu diesen Schritten an".

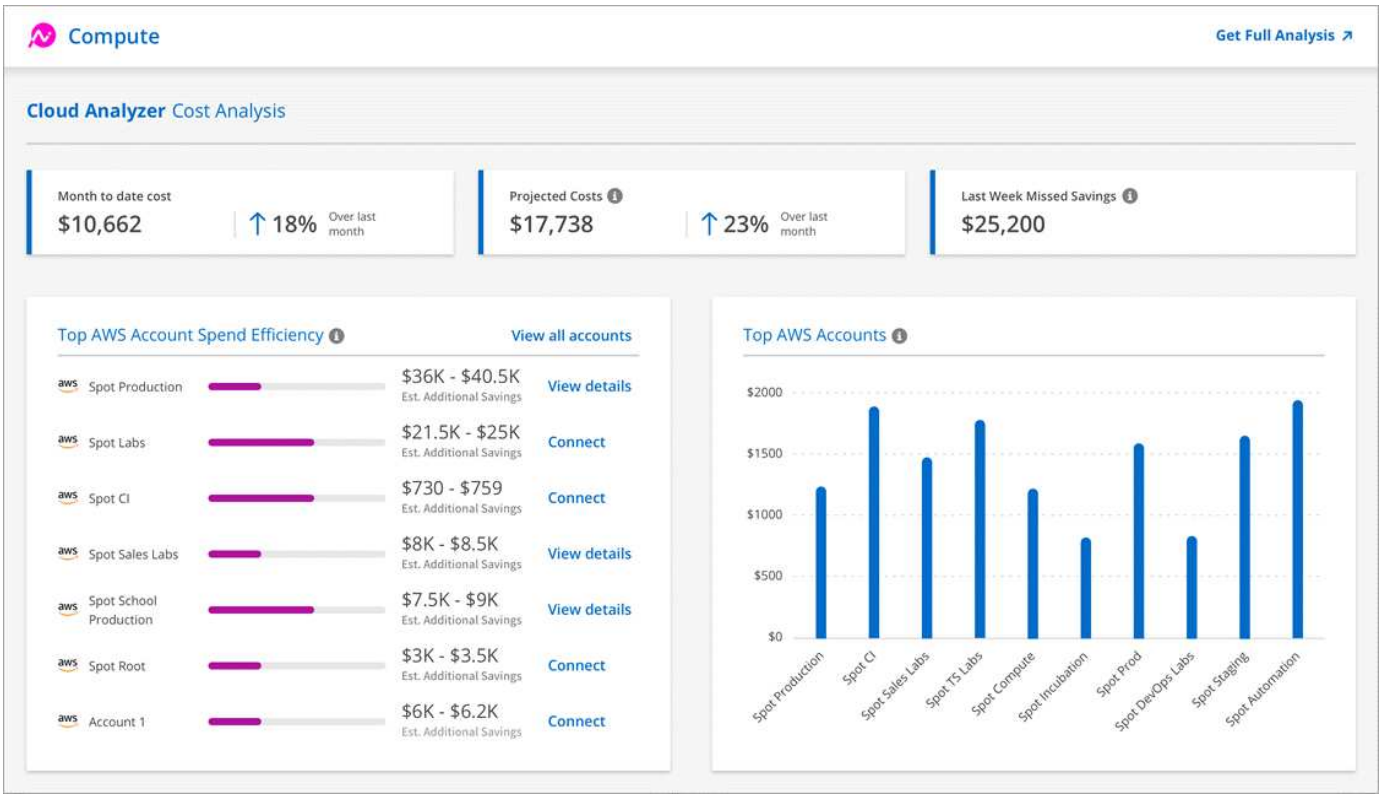


Ergebnis

Cloud Analyzer beginnt mit der Verarbeitung Ihrer AWS Kontodaten. Wenn Sie über mehrere Konten verfügen, beginnt Cloud Analyzer mit schreibgeschützten Funktionen für alle verknüpften Konten unter dem Hauptzahlerkonto. Wenn Sie mehr Details zu den potenziellen Einsparungen für diese Accounts erhalten möchten, müssen Sie sie ebenfalls anschließen. Weitere Informationen zu diesem Prozess finden Sie im folgenden Abschnitt.

Analysieren Sie Ihre Computing-Kosten

Nach der Verarbeitung Ihrer Account-Daten durch Cloud Analyzer erhalten Sie auf der Registerkarte „Computing“ Einblicke in vergangene, aktuelle und zukünftige Cloud-Kosten.



Aktuelle Kosten

Die Gesamtkosten für Ihre Workloads vom Beginn des aktuellen Monats bis zur Präsentation.

Prognostizierte Kosten

Die prognostizierten Kosten am Ende des Monats basierend auf einer Analyse Ihres Nutzungsmusters.

Letzte Woche Verpasste Einsparungen

Einsparungen, die in den letzten sieben Tagen durch Optimierung von Spot-Instanzen und Reservierungen erzielt werden könnten.

Wichtigste Ausgaben für AWS Konten Effizienz

Die Top 10 Accounts abhängig von der größten Menge an geschätzten zusätzlichen Einsparungen.

Jedem Account wird eine Effizienzbewertung zugewiesen, die auf aktuellen und zusätzlichen potentiellen Einsparungen basiert. Die geschätzten zusätzlichen Einsparungen zeigen, wie viel zusätzlich durch den Einsatz von Spot-Instanzen und reservierten Instanzen eingespart werden kann.

Sie können folgende Maßnahmen ergreifen, um Ihre Konten weiter zu optimieren:

- **Details anzeigen**: Sehen Sie sich Ihre Möglichkeiten zur Kostenoptimierung an, indem Sie zu Spot's Cloud Analyzer gehen.
- **Verbinden**: Schließen Sie ein noch nicht verwaltetes Konto an. Sie werden zu dem Assistenten weitergeleitet, der das Konto verbindet.

Top AWS Accounts

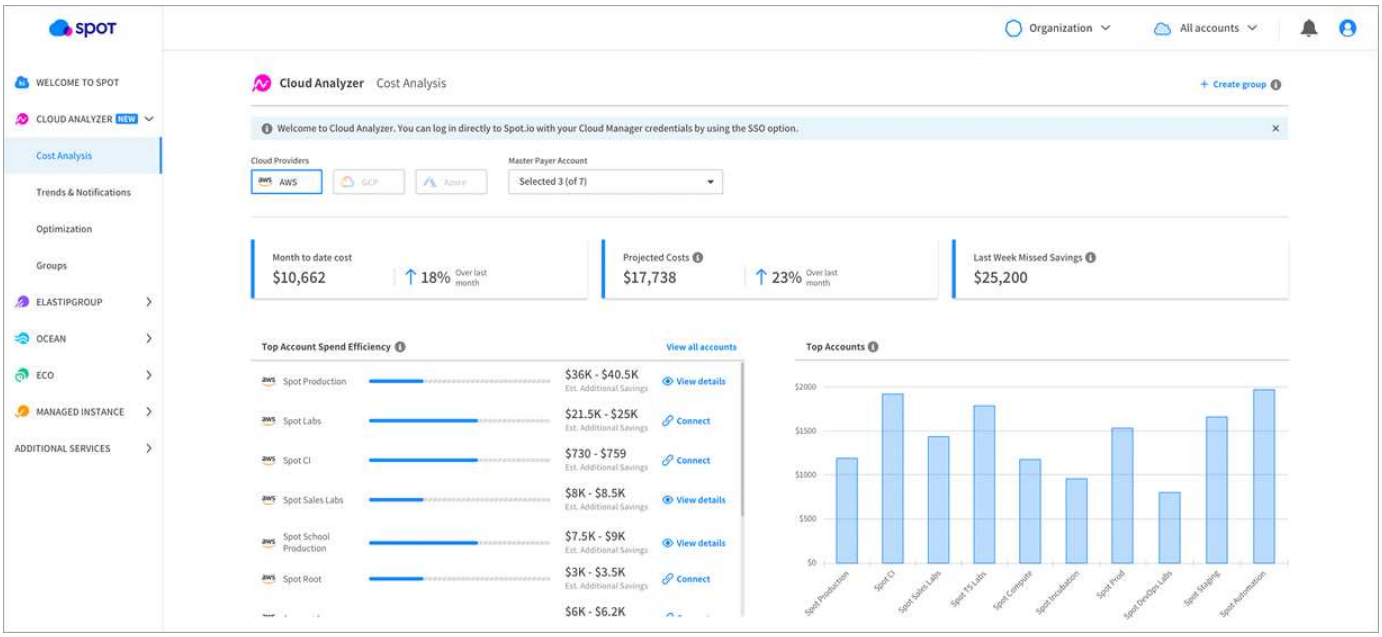
Dies ist ein Balkendiagramm mit den zehn wichtigsten Konten nach Kosten. Die Grafik basiert auf den letzten 30 Tagen der Ausgabenaktivität.

"Erfahren Sie mehr über die Seite „Kostenanalyse“ im Spot Cloud Analyzer".

Weitere Analysen und Empfehlungen finden Sie im Cloud Analyzer

Klicken Sie jederzeit auf **vollständige Analyse**, um weitere Diagramme und Analysen, ausführliche Empfehlungen, eine Aufschlüsselung von Anwendungsfällen (Container, ElasticApps und Reservierungen) und mehr aufzurufen.

Das folgende Beispiel zeigt Cloud Analyzer auf:



- "Auf der Produktseite für Cloud Analyzer erfahren Sie mehr über die Möglichkeiten dieser Technologie".
- "Hilfe zur Verwendung von Cloud Analyzer erhalten Sie in der Dokumentation zu Spot".

Tiering von Daten in die Cloud

Erfahren Sie mehr über Cloud Tiering

Der Cloud-Tiering-Service von NetApp erweitert das Datacenter auf die Cloud, indem inaktive Daten automatisch von On-Premises-ONTAP-Clustern in den Objekt-Storage verschoben werden. Dies setzt wertvollen Speicherplatz im Cluster für mehr Workloads frei, ohne Änderungen an der Applikationsebene vornehmen zu müssen. Cloud Tiering kann die Kosten in Ihrem Datacenter senken und einen Wechsel von einem CAPEX- zu einem OPEX-Modell ermöglichen.

Der Cloud Tiering Service nutzt die Funktionen von *FabricPool*. FabricPool ist eine NetApp Data-Fabric-Technologie für automatisiertes Tiering von Daten auf kostengünstigen Objekt-Storage. Aktive Daten bleiben auf hochperformanten SSDs, während inaktive Daten auf kostengünstigen Objekt-Storage verschoben werden, ohne die Dateneffizienz von ONTAP zu beeinträchtigen.

Funktionen

Cloud Tiering bietet Automatisierung, Monitoring, Berichte und eine zentrale Managementoberfläche:

- Durch Automatisierung wird das Einrichten und Managen von Daten-Tiering von ONTAP Clustern vor Ort in die Cloud vereinfacht
- Dank einer einzigen Konsole muss FabricPool über mehrere Cluster hinweg unabhängig gemanagt werden
- Berichte zeigen die Menge der aktiven und inaktiven Daten auf jedem Cluster an
- Ein Tiering-Integritätsstatus unterstützt Sie dabei, Probleme zu identifizieren und zu korrigieren, sobald diese auftreten
- Wenn Sie Cloud Volumes ONTAP Systeme verwenden, finden Sie sie im Cluster Dashboard, sodass Sie einen umfassenden Überblick über Daten-Tiering in Ihrer Hybrid-Cloud-Infrastruktur erhalten

Cloud Volumes ONTAP Systeme sind schreibgeschützt aus Cloud Tiering. "Sie richten Tiering für Cloud Volumes ONTAP aus der Arbeitsumgebung in Cloud Manager ein".

Weitere Informationen zu dem Mehrwert von Cloud Tiering finden Sie im "Sehen Sie sich die Cloud Tiering Seite auf NetApp Cloud Central an".

Cloud Tiering kann den Storage-Platzbedarf deutlich senken, aber es ist keine Backup-Lösung.

Unterstützte Objekt-Storage-Provider

Sie können inaktive Daten von einem ONTAP Cluster zu Amazon S3, Microsoft Azure Blob Storage, Google Cloud Storage oder StorageGRID (Private Cloud) verschieben.

Preise und Lizenzen

Sie bezahlen für Cloud Tiering über ein Pay-as-you-go-Abonnement, eine ONTAP Tiering-Lizenz namens *FabricPool* oder eine Kombination aus beidem. Eine kostenlose 30-Tage-Testversion ist für Ihren ersten Cluster verfügbar, wenn Sie keine Lizenz haben.

Beim Tiering von Daten zu StorageGRID fallen keine Kosten an. Es ist keine BYOL-Lizenz oder PAYGO-Registrierung erforderlich.

"Preisdetails anzeigen".

30 Tage kostenlos testen mit unserer

Wenn Sie keine FabricPool Lizenz haben, beginnt eine 30-Tage-kostenlose Testversion von Cloud Tiering, wenn Sie das Tiering auf Ihrem ersten Cluster einrichten. Nach Ablauf dieser 30-Tage-Testsoftware müssen Sie für Cloud Tiering bezahlen – über ein Pay-as-you-go-Abonnement, eine FabricPool Lizenz oder eine Kombination aus beiden.

Wenn Ihre kostenlose Testversion endet und Sie keine Lizenz abonniert oder hinzugefügt haben, stellt ONTAP keine „kalten" Daten mehr in den Objekt-Storage bereit. Die bestehenden Daten stehen aber weiterhin für den Zugriff zur Verfügung.

Pay-as-you-go-Abonnement

Cloud Tiering bietet nutzungsbasierte Lizenzierung in einem Pay-as-you-go-Modell. Nach dem Abonnieren über den Marktplatz Ihres Cloud-Anbieters zahlen Sie pro GB für Daten, die gestaffelt sind - es gibt keine Vorkasse. Die Abrechnung erfolgt von Ihrem Cloud-Provider über Ihre monatliche Abrechnung.

Sie sollten sich auch dann abonnieren, wenn Sie eine kostenlose Testversion haben oder Ihre eigene Lizenz mitbringen (BYOL):

- Das Abonnieren sorgt dafür, dass es keine Serviceunterbrechung gibt, nachdem Ihre kostenlose Testversion endet.

  Wenn die Studie endet, werden Sie stündlich nach der Menge der Daten, die Sie Tier geladen werden.

- Wenn Sie Ihre FabricPool Lizenz für mehr Daten als zulässig erteilen, wird Daten-Tiering über Ihr Pay-as-you-go-Abonnement fortgesetzt.

  Wenn Sie beispielsweise eine 10-TB-Lizenz besitzen, wird die gesamte Kapazität über 10 TB hinaus über das nutzungsbasierte Abonnement abgerechnet.

Das nutzungsbasierte Abonnement wird Ihnen während der kostenlosen Testversion oder bei Nichtüberschreitung Ihrer FabricPool Lizenz nicht in Rechnung gestellt.

"Erfahren Sie, wie Sie ein Pay-as-you-go-Abonnement einrichten".

Mit Ihrer eigenen Lizenz

Sie können Ihre eigene Lizenz beim Kauf einer ONTAP FabricPool Lizenz von NetApp erwerben. Sie können term-basierte oder unbefristete Lizenzen erwerben.

Nachdem Sie eine FabricPool Lizenz erworben haben, müssen Sie sie dem Cluster hinzufügen "Was Sie direkt über Cloud Tiering durchführen können".

Wenn Sie die Lizenz nach der Aktivierung über Cloud Tiering zu einem späteren Zeitpunkt zusätzliche Kapazität erwerben, wird die Lizenz für das Cluster automatisch mit der neuen Kapazität aktualisiert. Es ist nicht erforderlich, eine neue NetApp Lizenzdatei (NetApp License File, NLF) auf das Cluster anzuwenden.

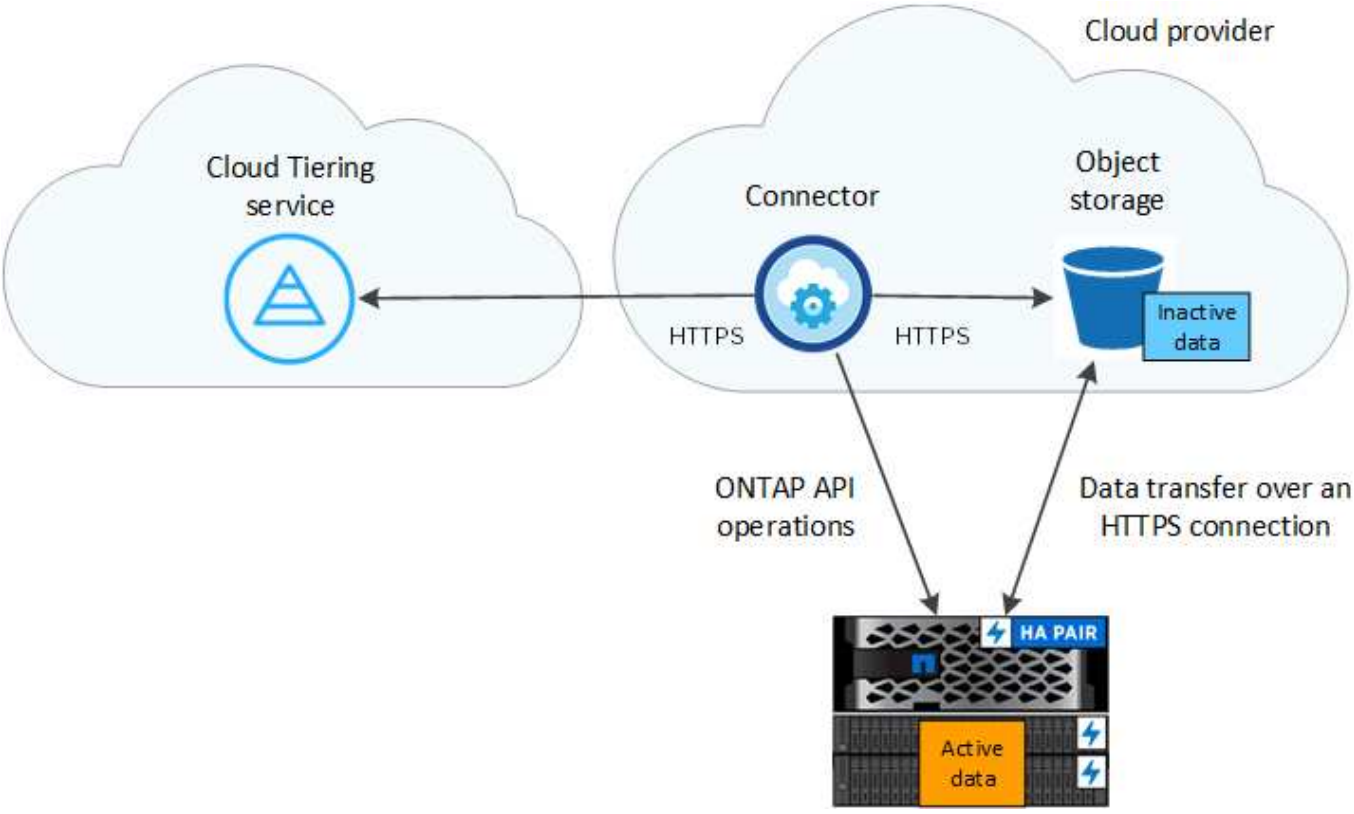
Wie oben erwähnt, empfehlen wir, ein Pay-as-you-go-Abonnement einzurichten, selbst wenn das Cluster über eine BYOL-Lizenz verfügt.

Mailto:ng-cloud-tiering@netapp.com?subject=Lizenzierung[Kontaktieren Sie uns, um eine Lizenz zu erwerben].

Funktionsweise von Cloud Tiering

Cloud Tiering ist ein von NetApp gemanagter Service, mit dem Sie inaktive („kalte“) Daten automatisch mithilfe von FabricPool Technologie aus Ihren lokalen ONTAP Clustern in Objekt-Storage in Ihrer Public Cloud oder Private Cloud verschieben. Verbindungen zu ONTAP erfolgen über einen Anschluss.

Die folgende Abbildung zeigt die Beziehung zwischen den einzelnen Komponenten:



Cloud Tiering funktioniert auf hohem Niveau wie folgt:

1. Der lokale Cluster wird über Cloud Manager ermittelt.
2. Sie erstellen ein Tiering, indem Sie Details zu Ihrem Objekt-Storage angeben, einschließlich Bucket/Container, Storage-Klasse oder Zugriffsebene.
3. Cloud Manager konfiguriert ONTAP so, dass er den Objekt-Storage-Provider verwendet. Dabei wird die Menge der aktiven und inaktiven Daten auf dem Cluster erkannt.
4. Sie wählen die zu Tier zupassenden Volumes und die Tiering-Richtlinie für diese Volumes aus.
5. ONTAP beginnt mit dem Tiering inaktiver Daten zum Objektspeicher, sobald die Daten die Schwellenwerte erreicht haben, die als inaktiv eingestuft werden sollen (siehe Richtlinien für das Volume-Tiering).

Objekt-Storage

Jedes ONTAP Cluster verschiebt inaktive Daten auf einen einzelnen Objektspeicher. Wenn Sie Daten-Tiering einrichten, haben Sie die Wahl, einen neuen Bucket/Container hinzuzufügen oder einen vorhandenen Bucket/Container zusammen mit einer Storage-Klasse oder Zugriffsebene auszuwählen.

- "Erfahren Sie mehr über unterstützte S3 Storage-Klassen"
- "Erfahren Sie mehr über unterstützte Azure Blob Zugriffsebenen"
- "Erfahren Sie mehr über unterstützte Google Cloud Storage-Klassen"

Richtlinien für das Volume-Tiering

Wenn Sie die Volumes auswählen, die Sie abstufen möchten, wählen Sie eine *Volume Tiering Policy* aus, die für jedes Volume angewendet werden soll. Eine Tiering-Richtlinie bestimmt, wann oder ob Blöcke der Benutzerdaten eines Volumes in die Cloud verschoben werden.

Keine Tiering-Richtlinie

Aufbewahrung der Daten auf einem Volume in der Performance-Tier, sodass diese nicht in die Cloud verschoben werden

Cold Snapshots (nur Snapshot)

ONTAP schichtet kalte Snapshot Blöcke im Volume aus, die nicht gemeinsam mit dem aktiven Filesystem zum Objekt-Storage genutzt werden. Wenn gelesen werden, werden kalte Datenblöcke auf der Cloud-Tier heiß und werden auf die Performance-Tier verschoben.

Daten werden erst dann verteilt, wenn ein Aggregat eine Kapazität von 50 % erreicht hat und wenn die Daten den Kühlungszeitraum erreicht haben. Die standardmäßige Anzahl der Kühltage beträgt 2, Sie können jedoch die Anzahl der Tage anpassen.

Schreibvorgänge vom Cloud-Tier auf die Performance-Tier werden deaktiviert, wenn die Kapazität der Performance-Tier größer als 70 % ist. In diesem Fall erfolgt der Zugriff auf Blöcke direkt aus dem Cloud-Tier.

Kalte Benutzerdaten (automatisch)

ONTAP führt das Tiering aller kalten Blöcke im Volume (ohne Metadaten) zu Objekt-Storage durch. Die kalten Daten umfassen nicht nur Snapshot Kopien, sondern auch kalte Benutzerdaten aus dem aktiven Dateisystem.

Wenn durch zufällige Lesevorgänge gelesen werden, werden kalte Datenblöcke auf der Cloud-Tier heiß und werden auf die Performance-Tier verschoben. Wenn sequenzielle Lesevorgänge lesen, z. B. Index- und Virenschutz-Scans, bleiben kalte Datenblöcke auf der Cloud-Tier kalt und werden nicht auf die Performance-Tier geschrieben.

Daten werden erst dann verteilt, wenn ein Aggregat eine Kapazität von 50 % erreicht hat und wenn die Daten den Kühlungszeitraum erreicht haben. Der Kühlzeitraum bezeichnet die Zeit, die Benutzerdaten in einem Volume inaktiv bleiben müssen, damit die Daten als „kalt“ eingestuft werden und zum Objektspeicher verschoben werden können. Die standardmäßige Anzahl der Kühltage beträgt 31, Sie können jedoch die Anzahl der Tage anpassen.

Schreibvorgänge vom Cloud-Tier auf die Performance-Tier werden deaktiviert, wenn die Kapazität der Performance-Tier größer als 70 % ist. In diesem Fall erfolgt der Zugriff auf Blöcke direkt aus dem Cloud-Tier.

Alle Benutzerdaten (Alle)

Alle Daten (ohne Metadaten) werden sofort als „kalt“ markiert und in den Objektspeicher verschoben, sobald wie möglich. Es ist nicht mehr nötig, 48 Stunden auf neue Blöcke in einem Volume zu warten, die kalt werden. Beachten Sie, dass für Blöcke, die sich vor der Festlegung der All-Richtlinie im Volume befinden, 48 Stunden zum Kaltstart benötigt werden.

Beim Lesen bleiben kalte Datenblöcke auf der Cloud-Tier kalt und werden nicht zurück in die Performance-Tier geschrieben. Diese Richtlinie ist ab ONTAP 9.6 verfügbar.

Berücksichtigen Sie vor der Auswahl dieser Tiering-Richtlinie folgende Punkte:

- Durch das Tiering von Daten werden die Storage-Effizienzfunktionen sofort reduziert (nur Inline).
- Diese Richtlinie sollte nur dann eingesetzt werden, wenn sich ungenutzte Daten auf dem Volume nicht ändern.
- Objekt-Storage ist kein transaktionsorientiertes System und führt bei Änderungen zu einer erheblichen Fragmentierung.
- Bedenken Sie die Auswirkungen von SnapMirror Transfers, bevor Sie die Richtlinie Alle Angaben zu Quell-Volumes in Datensicherungsbeziehungen zuweisen.

  Da die Daten sofort in Tiers verschoben werden, liest SnapMirror die Daten nicht aus der Performance-Tier, sondern aus der Cloud-Tier. Dies führt zu langsameren SnapMirror Vorgängen – möglicherweise werden andere SnapMirror Vorgänge später in der Warteschlange verschoben, selbst wenn sie unterschiedliche Tiering-Richtlinien verwenden.

Alle DP-Benutzerdaten (Backup)

Alle Daten auf einem Datensicherungs-Volume (ohne Metadaten) werden sofort in die Cloud-Tier verschoben. Bei Lesezugriffen bleiben kalte Datenblöcke auf der Cloud-Tier nur selten und werden nicht zurück auf die Performance-Tier geschrieben (ab ONTAP 9.4).

Diese Richtlinie ist für ONTAP 9.5 oder früher verfügbar. Es wurde ab ONTAP 9.6 durch die **All** Tiering Policy ersetzt.

Los geht's

Tiering von Daten von lokalen ONTAP Clustern zu Amazon S3

Freier Speicherplatz an ONTAP-Clustern vor Ort durch Tiering von Daten an Amazon S3 Das Daten-Tiering wird durch den NetApp Cloud Tiering Service unterstützt.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

1 Tiering von Daten auf Amazon S3 vorbereiten

Sie benötigen Folgendes:

- Ein AFF oder FAS System mit reinen SSD-Aggregaten, auf denen ONTAP 9.2 oder höher ausgeführt wird und eine HTTPS-Verbindung zu Amazon S3 besitzt.
- Ein AWS Konto mit Zugriffsschlüssel und Die erforderlichen Berechtigungen ONTAP Cluster können also inaktive Daten in und aus S3 verschieben.
- In einer AWS VPC oder am Unternehmensstandort ein Connector installiert.

- Networking für den Connector, der eine ausgehende HTTPS-Verbindung zum ONTAP-Cluster, den S3-Storage und den Cloud-Tiering-Service ermöglicht.

2 Tiering einrichten

Wählen Sie in Cloud Manager eine lokale Arbeitsumgebung aus, klicken Sie auf **Setup Tiering** und folgen Sie den Aufforderungen zum Tiering von Daten in Amazon S3.

3 Lizenzierung einrichten

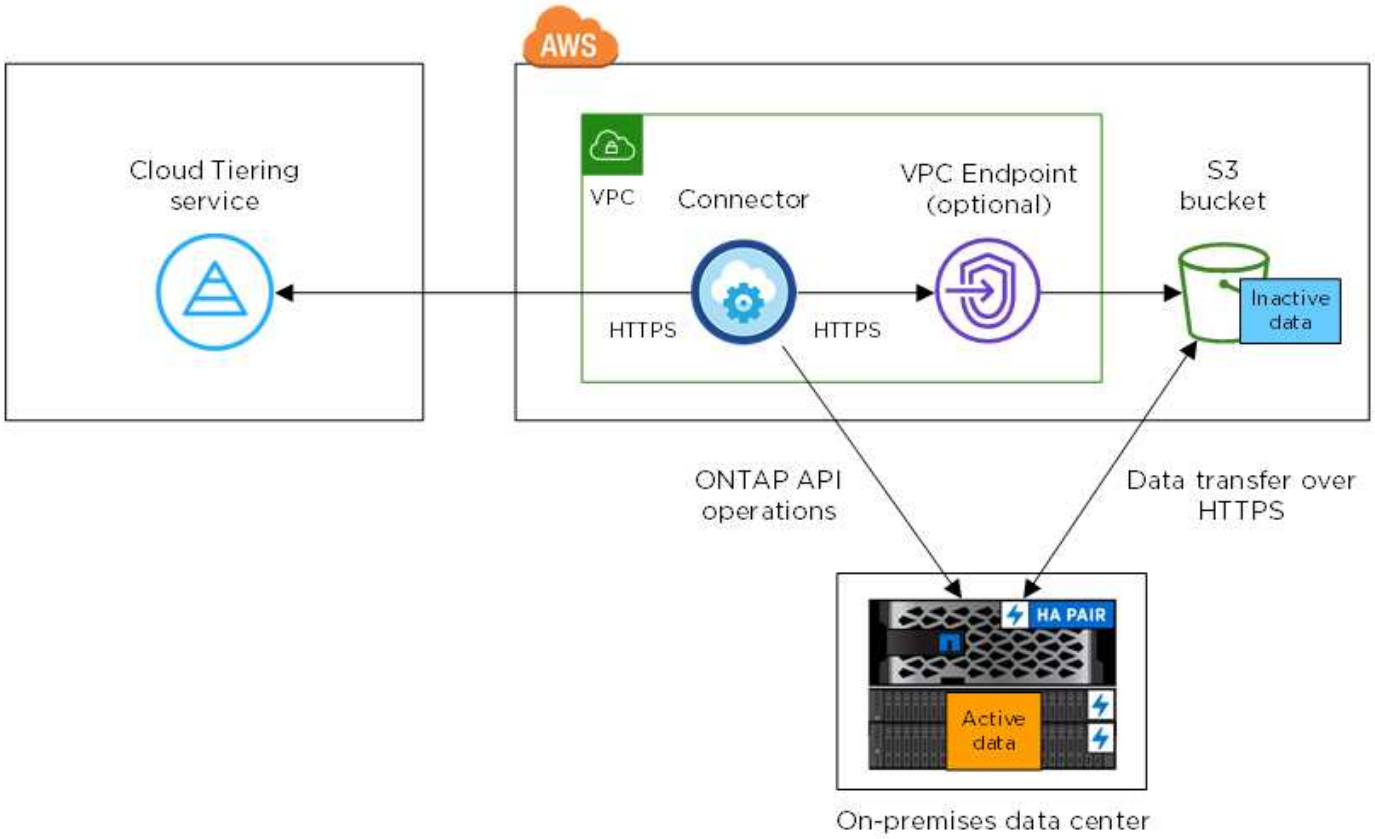
Nach Abschluss der kostenlosen Testversion zahlen Sie für Cloud Tiering über ein Pay-as-you-go-Abonnement, eine ONTAP-Tiering-Lizenz oder eine Kombination aus den beiden Optionen:

- Wenn Sie sich über den AWS Marketplace anmelden möchten, klicken Sie auf **Tiering > Lizenzierung**, klicken Sie auf **Abonnieren** und folgen Sie dann den Anweisungen.
- Um mit einer Tiering-Lizenz zu bezahlen, Kontaktieren Sie uns, und dann "Fügen Sie ihn von Cloud Tiering zu Ihrem Cluster hinzu".

Anforderungen

Überprüfen Sie die Unterstützung für Ihr ONTAP Cluster, richten Sie Ihr Netzwerk ein und bereiten Sie den Objekt-Storage vor.

Die folgende Abbildung zeigt die einzelnen Komponenten und die Verbindungen, die zwischen den Komponenten vorbereitet werden müssen:



Die Kommunikation zwischen einem Connector und S3 dient nur der Einrichtung von Objekt-Storage. Der Connector kann lokal statt in der Cloud residieren.

Vorbereiten der ONTAP Cluster

Ihre ONTAP-Cluster müssen beim Tiering von Daten zu Amazon S3 die folgenden Anforderungen erfüllen.

Unterstützte ONTAP Plattformen

Cloud Tiering unterstützt AFF Systeme und rein SSD-basierte Aggregate auf FAS Systemen.

Unterstützte ONTAP Version

ONTAP 9.2 oder höher

Netzwerkanforderungen für Cluster

- Das ONTAP-Cluster initiiert eine HTTPS-Verbindung über Port 443 zu Amazon S3.

  ONTAP liest und schreibt Daten auf und aus dem Objekt-Storage. Objekt-Storage startet nie, er reagiert einfach nur.

  AWS Direct Connect bietet zwar eine bessere Performance und geringere Datentransferkosten, ist aber nicht zwischen dem ONTAP Cluster und S3 erforderlich. Da die Performance bei der Nutzung von AWS Direct Connect deutlich besser ist, empfiehlt sich dies als Best Practice.

- Über den Connector ist eine eingehende Verbindung erforderlich. Dieser kann in einer AWS VPC oder an Ihrem Standort residieren.

  Es ist keine Verbindung zwischen dem Cluster und dem Cloud Tiering Service erforderlich.

- Auf jedem ONTAP Node, der Tiered Volumes hostet, ist eine Intercluster-LIF erforderlich. Die LIF muss dem *IPspace* zugewiesen sein, den ONTAP zur Verbindung mit Objekt-Storage verwenden sollte.

  IPspaces ermöglichen die Trennung des Netzwerkdatenverkehrs und ermöglichen die Trennung des Client-Datenverkehrs für Datenschutz und Sicherheit. "Erfahren Sie mehr über IPspaces".

  Wenn Sie Daten-Tiering einrichten, werden Sie von Cloud Tiering aufgefordert, den IP-Speicherplatz zu verwenden. Sie sollten den IPspace auswählen, dem jede LIF zugeordnet ist. Dies kann der „Standard"-IPspace oder ein benutzerdefinierter IPspace sein, den Sie erstellt haben.

Unterstützte Volumes und Aggregate

Die Gesamtzahl der Volumes, die in Cloud Tiering Tiers möglich sind, ist unter Umständen kleiner als die Anzahl der Volumes in Ihrem ONTAP System. Das liegt daran, dass Volumes von einigen Aggregaten nicht abgestuft werden können. Sie können beispielsweise keine Daten-Tiers von SnapLock Volumes oder MetroCluster Konfigurationen erstellen. In der ONTAP-Dokumentation finden Sie weitere Informationen "Funktionalität oder Funktionen, die nicht von FabricPool unterstützt werden".

Cloud Tiering unterstützt FlexGroup Volumes ab ONTAP 9.5. Setup funktioniert wie jedes andere Volume.

Erstellen oder Umschalten von Anschlüssen

Für das Tiering von Daten in die Cloud ist ein Connector erforderlich. Beim Tiering von Daten zu AWS S3 kann ein Connector verwendet werden, der in einer AWS VPC oder vor Ort ist. Entweder müssen Sie einen neuen Konnektor erstellen oder sicherstellen, dass der aktuell ausgewählte Connector in AWS oder On-Prem liegt.

- "Erfahren Sie mehr über Steckverbinder"
- "Erstellen eines Konnektors in AWS"
- "Connector-Host-Anforderungen"
- "Installieren des Connectors auf einem vorhandenen Linux-Host"
- "Wechseln zwischen den Anschlüssen"

Vorbereiten der Vernetzung für den Connector

Stellen Sie sicher, dass der Connector über die erforderlichen Netzwerkverbindungen verfügt. Ein Connector kann lokal oder in AWS installiert werden.

Schritte

1. Stellen Sie sicher, dass das Netzwerk, in dem der Connector installiert ist, folgende Verbindungen ermöglicht:
   - Eine ausgehende Internetverbindung zum Cloud Tiering-Service über Port 443 (HTTPS)
   - Eine HTTPS-Verbindung über Port 443 zu S3
   - Eine HTTPS-Verbindung über Port 443 zu Ihren ONTAP Clustern
2. Aktivieren Sie bei Bedarf einen VPC-Endpunkt zum S3.

   Ein VPC-Endpunkt zu S3 wird empfohlen, wenn Sie über eine Direct-Connect- oder VPN-Verbindung vom ONTAP-Cluster zum VPC verfügen und dann die Kommunikation zwischen dem Connector und S3 im internen AWS Netzwerk verbleiben soll.

Amazon S3 wird vorbereitet

Wenn Sie Daten-Tiering auf einem neuen Cluster einrichten, werden Sie aufgefordert, einen S3-Bucket zu erstellen oder einen vorhandenen S3-Bucket im AWS-Konto auszuwählen, wo der Connector eingerichtet ist.

Das AWS-Konto muss über Berechtigungen und einen Zugriffsschlüssel verfügen, den Sie in Cloud Tiering eingeben können. Das ONTAP-Cluster verwendet den Zugriffsschlüssel für das Tiering von Daten in und aus S3.

Schritte

1. Stellen Sie dem IAM-Benutzer folgende Berechtigungen bereit:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetBucketLocation",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject"
```

   "AWS Documentation: Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer"

2. Zugriffsschlüssel erstellen oder suchen.

   Cloud Tiering leitet den Zugriffsschlüssel an den ONTAP Cluster weiter. Die Anmeldedaten werden im Cloud Tiering Service nicht gespeichert.

   "AWS Dokumentation: Management von Zugriffsschlüsseln für IAM-Benutzer"

Tiering inaktiver Daten von dem ersten Cluster zu Amazon S3

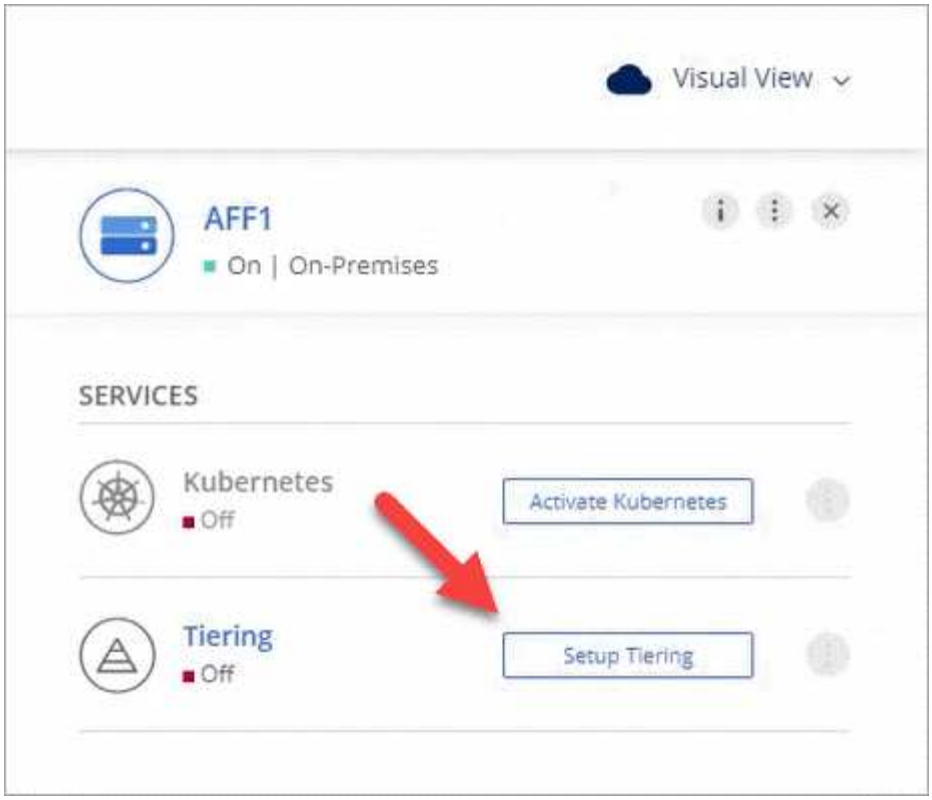
Nach der Vorbereitung der AWS Umgebung können Sie das Tiering inaktiver Daten vom ersten Cluster aus starten.

Was Sie benötigen

- "Eine Arbeitsumgebung vor Ort".
- Ein AWS-Zugriffsschlüssel für einen IAM-Benutzer mit den erforderlichen S3-Berechtigungen.

Schritte

1. Wählen Sie ein On-Premises-Cluster aus.
2. Klicken Sie Auf **Tiering Einrichten**.



Sie befinden sich jetzt im Tiering Dashboard.

3. Klicken Sie neben dem Cluster auf **Tiering einrichten**.
4. Führen Sie die Schritte auf der Seite **Tiering Setup** aus:

    a. **S3 Bucket**: Fügen Sie einen neuen S3-Bucket hinzu oder wählen Sie einen vorhandenen S3-Bucket aus, der mit dem Präfix *Fabric-Pool* beginnt und klicken Sie auf **Weiter**.

    Das Präfix *Fabric-Pool* ist erforderlich, da die IAM-Richtlinie für den Connector ermöglicht, S3-Aktionen auf Buckets auszuführen, die mit diesem exakten Präfix benannt sind.

    Beispielsweise könnten Sie den S3-Bucket-Fabric-Pool-AFF1 benennen, wobei AFF1 der Name des Clusters ist.

    a. **Speicherklasse**: Wählen Sie die S3-Speicherklasse aus, auf die Sie die Daten nach 30 Tagen verschieben möchten, und klicken Sie auf **Weiter**.

    Wenn Sie sich für „Standard“ entscheiden, verbleiben die Daten in dieser Storage-Klasse.

    b. **Anmeldeinformationen**: Geben Sie die Zugriffsschlüssel-ID und den geheimen Schlüssel für einen IAM-Benutzer ein, der über die erforderlichen S3-Berechtigungen verfügt.

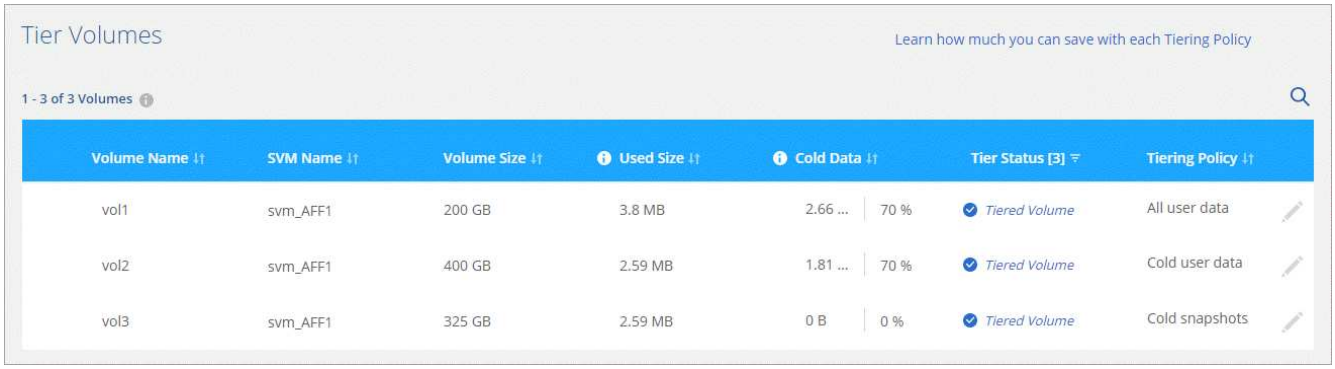
    Der IAM-Benutzer muss sich im gleichen AWS-Konto wie der Bucket befinden, den Sie auf der Seite **S3 Bucket** ausgewählt oder erstellt haben.

    c. **Clusternetzwerk**: Wählen Sie den IPspace aus, den ONTAP verwenden soll, um eine Verbindung zum Objekt-Storage herzustellen, und klicken Sie auf **Weiter**.

    Durch die Auswahl des richtigen IPspaces wird sichergestellt, dass Cloud Tiering eine Verbindung von ONTAP mit dem Objekt-Storage Ihres Cloud-Providers einrichten kann.

5. Klicken Sie auf **Weiter**, um die Volumes auszuwählen, die Sie abstufen möchten.
6. Richten Sie auf der Seite **Tier Volumes** Tiering für jedes Volume ein. Klicken Sie auf das Symbol, wählen Sie eine Tiering-Richtlinie aus, passen Sie optional die Kühltage an und klicken Sie auf **Apply**.

   "Weitere Informationen zu Volume Tiering Policies".



Ergebnis

Sie haben Daten-Tiering von Volumes im Cluster erfolgreich in den S3-Objekt-Storage eingerichtet.

Was kommt als Nächstes?

"Denken Sie daran, den Cloud Tiering Service zu abonnieren".

Sie können auch weitere Cluster hinzufügen oder Informationen zu den aktiven und inaktiven Daten auf dem Cluster prüfen. Weitere Informationen finden Sie unter "Managen von Daten-Tiering von Clustern".

Tiering von Daten von lokalen ONTAP Clustern zu Azure Blob Storage

Durch Tiering von Daten in Azure Blob Storage wird freier Speicherplatz auf ONTAP Clustern vor Ort bereitgestellt. Das Daten-Tiering wird durch den NetApp Cloud Tiering Service unterstützt.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

Vorbereiten von Daten auf Azure Blob Storage

Sie benötigen Folgendes:

- Ein AFF oder FAS System mit reinen SSD-Aggregaten, auf denen ONTAP 9.4 oder höher ausgeführt wird und eine HTTPS-Verbindung zum Azure Blob Storage verfügt.
- Ein Connector in einem Azure vnet installiert.
- Networking für einen Connector, der eine ausgehende HTTPS-Verbindung zum ONTAP Cluster in Ihrem Datacenter, zu Azure Blob Storage und zum Cloud Tiering Service ermöglicht

Tiering einrichten

Wählen Sie in Cloud Manager eine lokale Arbeitsumgebung aus und klicken Sie auf **Setup Tiering** und folgen Sie den Aufforderungen zum Tiering von Daten auf Azure Blob Storage.

Lizenzierung einrichten

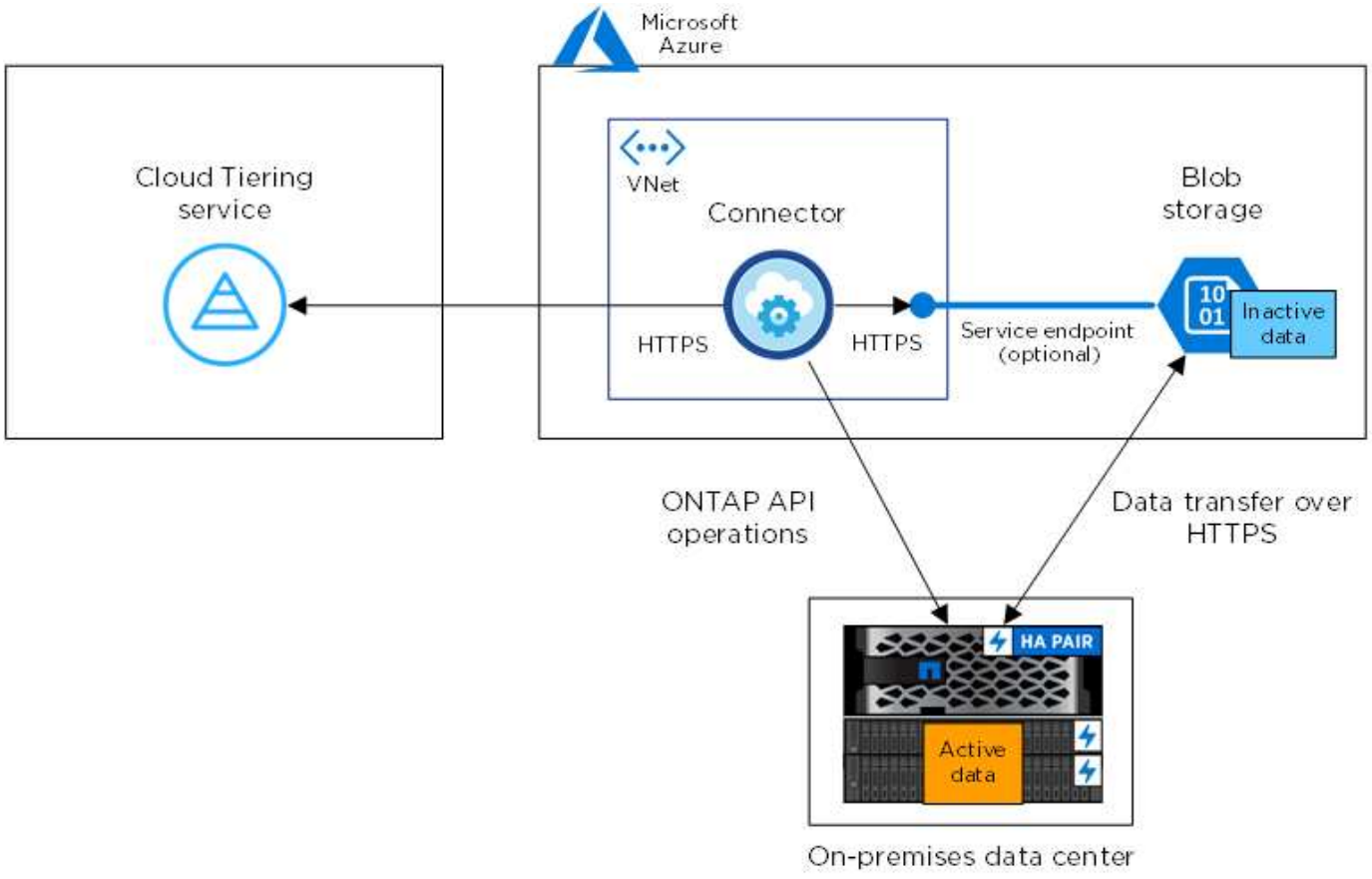
Nach Abschluss der kostenlosen Testversion zahlen Sie für Cloud Tiering über ein Pay-as-you-go-Abonnement, eine ONTAP-Tiering-Lizenz oder eine Kombination aus den beiden Optionen:

- Wenn Sie einen Azure Marketplace abonnieren möchten, klicken Sie auf **Tiering > Lizenzierung**, klicken Sie auf **Abonnieren** und folgen Sie dann den Anweisungen.
- Um eine Tiering-Lizenz hinzuzufügen, Kontaktieren Sie uns, und dann "Fügen Sie ihn von Cloud Tiering zu Ihrem Cluster hinzu".

Anforderungen

Überprüfen Sie die Unterstützung für Ihr ONTAP Cluster, richten Sie Ihr Netzwerk ein und bereiten Sie den Objekt-Storage vor.

Die folgende Abbildung zeigt die einzelnen Komponenten und die Verbindungen, die zwischen den Komponenten vorbereitet werden müssen:



Die Kommunikation zwischen dem Connector und Blob-Storage dient ausschließlich der Objekt-Storage-Einrichtung.

Vorbereiten der ONTAP Cluster

Ihre ONTAP-Cluster müssen beim Tiering von Daten zu Azure Blob Storage die folgenden Anforderungen erfüllen:

Unterstützte ONTAP Plattformen

Cloud Tiering unterstützt AFF Systeme und rein SSD-basierte Aggregate auf FAS Systemen.

Unterstützte ONTAP Version

ONTAP 9.4 oder höher

Netzwerkanforderungen für Cluster

- Das ONTAP Cluster initiiert eine HTTPS-Verbindung über Port 443 zum Azure Blob Storage.

  ONTAP liest und schreibt Daten auf und aus dem Objekt-Storage. Objekt-Storage startet nie, er reagiert einfach nur.

  ExpressRoute bietet zwar eine bessere Performance und niedrigere Datentransferkosten, er ist jedoch nicht zwischen dem ONTAP Cluster und Azure Blob Storage erforderlich. Da die Performance mit ExpressRoute signifikant höher ist, empfiehlt sich daher die Best Practice.

- Eine eingehende Verbindung ist über den NetApp Service Connector erforderlich, der sich in einem Azure vnet befindet.

  Es ist keine Verbindung zwischen dem Cluster und dem Cloud Tiering Service erforderlich.

- Auf jedem ONTAP Node, der Tiered Volumes hostet, ist eine Intercluster-LIF erforderlich. Die LIF muss dem *IPspace* zugewiesen sein, den ONTAP zur Verbindung mit Objekt-Storage verwenden sollte.

  IPspaces ermöglichen die Trennung des Netzwerkdatenverkehrs und ermöglichen die Trennung des Client-Datenverkehrs für Datenschutz und Sicherheit. "Erfahren Sie mehr über IPspaces".

  Wenn Sie Daten-Tiering einrichten, werden Sie von Cloud Tiering aufgefordert, den IP-Speicherplatz zu verwenden. Sie sollten den IPspace auswählen, dem jede LIF zugeordnet ist. Dies kann der „Standard“-IPspace oder ein benutzerdefinierter IPspace sein, den Sie erstellt haben.

Unterstützte Volumes und Aggregate

Die Gesamtzahl der Volumes, die in Cloud Tiering Tiers möglich sind, ist unter Umständen kleiner als die Anzahl der Volumes in Ihrem ONTAP System. Das liegt daran, dass Volumes von einigen Aggregaten nicht abgestuft werden können. Sie können beispielsweise keine Daten-Tiers von SnapLock Volumes oder MetroCluster Konfigurationen erstellen. In der ONTAP-Dokumentation finden Sie weitere Informationen "Funktionalität oder Funktionen, die nicht von FabricPool unterstützt werden".

Cloud Tiering unterstützt FlexGroup Volumes ab ONTAP 9.5. Setup funktioniert wie jedes andere Volume.

Erstellen oder Umschalten von Anschlüssen

Für das Tiering von Daten in die Cloud ist ein Connector erforderlich. Beim Tiering von Daten zu Azure Blob Storage muss ein Connector in einer Azure vnet verfügbar sein. Sie müssen entweder einen neuen Konnektor

erstellen oder sicherstellen, dass der aktuell ausgewählte Connector in Azure gespeichert ist.

- "Erfahren Sie mehr über Steckverbinder"
- "Erstellen eines Connectors in Azure"
- "Wechseln zwischen den Anschlüssen"

Vorbereiten der Vernetzung für den Connector

Stellen Sie sicher, dass der Connector über die erforderlichen Netzwerkverbindungen verfügt.

Schritte

1. Stellen Sie sicher, dass das vnet, in dem der Steckverbinder installiert ist, die folgenden Anschlüsse ermöglicht:
   - Eine ausgehende Internetverbindung zum Cloud Tiering-Service über Port 443 (HTTPS)
   - Eine HTTPS-Verbindung über Port 443 zum Azure Blob Storage
   - Eine HTTPS-Verbindung über Port 443 zu Ihren ONTAP Clustern
2. Aktivieren Sie bei Bedarf einen vnet-Service-Endpunkt zum Azure Storage.

   Wenn Sie über eine ExpressRoute oder eine VPN-Verbindung zwischen Ihrem ONTAP Cluster und dem vnet verfügen, wird ein vnet-Service-Endpunkt zum Azure Storage empfohlen, um in Ihrem virtuellen privaten Netzwerk die Kommunikation zwischen Connector und Blob-Storage zu bestehen.

Tiering inaktiver Daten von dem ersten Cluster zu Azure Blob Storage

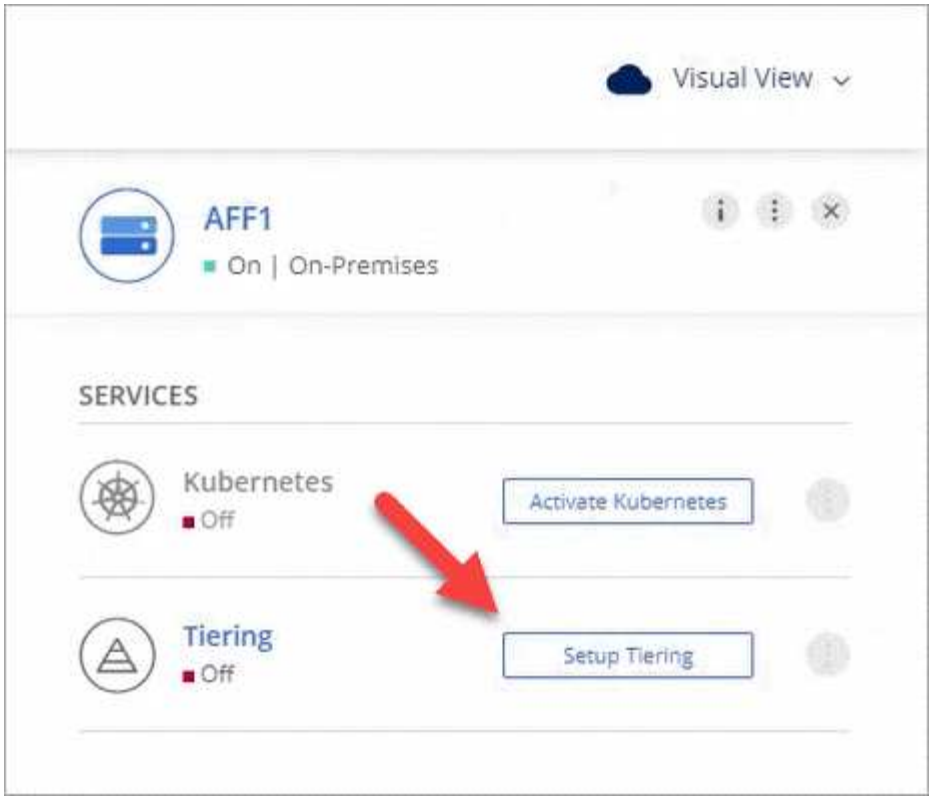
Starten Sie nach der Vorbereitung der Azure Umgebung das Tiering inaktiver Daten aus dem ersten Cluster.

Was Sie benötigen

"Eine Arbeitsumgebung vor Ort".

Schritte

1. Wählen Sie ein On-Premises-Cluster aus.
2. Klicken Sie Auf **Tiering Einrichten**.



Sie befinden sich jetzt im Tiering Dashboard.

3. Klicken Sie neben dem Cluster auf **Tiering einrichten**.
4. Führen Sie die Schritte auf der Seite **Tiering Setup** aus:
   a. **Ressourcengruppe**: Wählen Sie eine Ressourcengruppe aus, in der ein vorhandener Container verwaltet wird oder wo Sie einen neuen Container für Tiered Data erstellen möchten.
   b. **Azure Container**: Fügen Sie einen neuen Blob-Container zu einem Storage-Konto hinzu oder wählen Sie einen vorhandenen Container aus und klicken Sie auf **Weiter**.

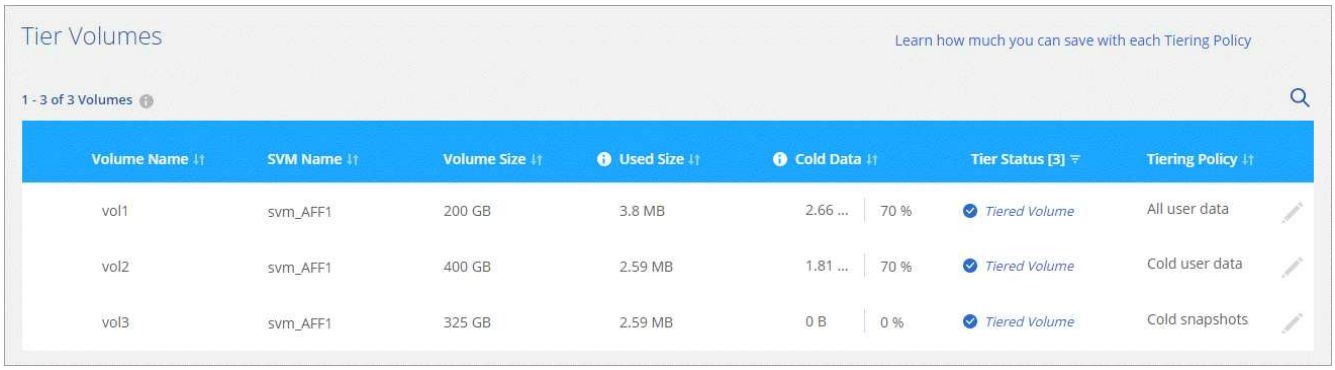
      Das Speicherkonto und die Container, die in diesem Schritt angezeigt werden, gehören zur Ressourcengruppe, die Sie im vorherigen Schritt ausgewählt haben.

   c. **Zugangsstufe**: Wählen Sie die Zugriffsebene aus, die Sie für die Tiered-Daten verwenden möchten, und klicken Sie auf **Weiter**.
   d. **Clusternetzwerk**: Wählen Sie den IPspace aus, den ONTAP verwenden soll, um eine Verbindung zum Objekt-Storage herzustellen, und klicken Sie auf **Weiter**.

      Durch die Auswahl des richtigen IPspaces wird sichergestellt, dass Cloud Tiering eine Verbindung von ONTAP mit dem Objekt-Storage Ihres Cloud-Providers einrichten kann.

5. Klicken Sie auf **Weiter**, um die Volumes auszuwählen, die Sie abstufen möchten.
6. Richten Sie auf der Seite **Tier Volumes** Tiering für jedes Volume ein. Klicken Sie auf das Symbol, wählen Sie eine Tiering-Richtlinie aus, passen Sie optional die Kühltage an und klicken Sie auf **Apply**.

   "Weitere Informationen zu Volume Tiering Policies".



Ergebnis

Sie haben Daten-Tiering von Volumes auf dem Cluster erfolgreich in den Azure Blob Objekt-Storage eingerichtet.

Was kommt als Nächstes?

"Denken Sie daran, den Cloud Tiering Service zu abonnieren".

Sie können auch weitere Cluster hinzufügen oder Informationen zu den aktiven und inaktiven Daten auf dem Cluster prüfen. Weitere Informationen finden Sie unter "Managen von Daten-Tiering von Clustern".

Tiering von Daten aus lokalen ONTAP Clustern in Google Cloud Storage

Durch Tiering von Daten in Google Cloud Storage können Sie Speicherplatz auf Ihren ONTAP-Clustern vor Ort freigeben. Das Daten-Tiering wird durch den NetApp Cloud Tiering Service unterstützt.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

1 Vorbereitung auf das Tiering von Daten auf Google Cloud Storage

Sie benötigen Folgendes:

- Ein AFF oder FAS System mit reinen SSD-Aggregaten, auf denen ONTAP 9.6 oder höher ausgeführt wird und eine HTTPS-Verbindung zu Google Cloud Storage besitzt.
- Ein Servicekonto mit der vordefinierten Storage-Administratorrolle und Speicherzugriffsschlüsseln.
- In einer Google Cloud Platform VPC wurde ein Connector installiert.
- Networking für den Connector, der eine ausgehende HTTPS-Verbindung zum ONTAP-Cluster in Ihrem Datacenter, zu Google Cloud Storage und zum Cloud-Tiering-Service ermöglicht.

2 Tiering einrichten

Wählen Sie in Cloud Manager eine lokale Arbeitsumgebung aus, klicken Sie auf **Setup Tiering** und folgen Sie den Aufforderungen, Daten auf Google Cloud Storage zu verschieben.

Lizenzierung einrichten

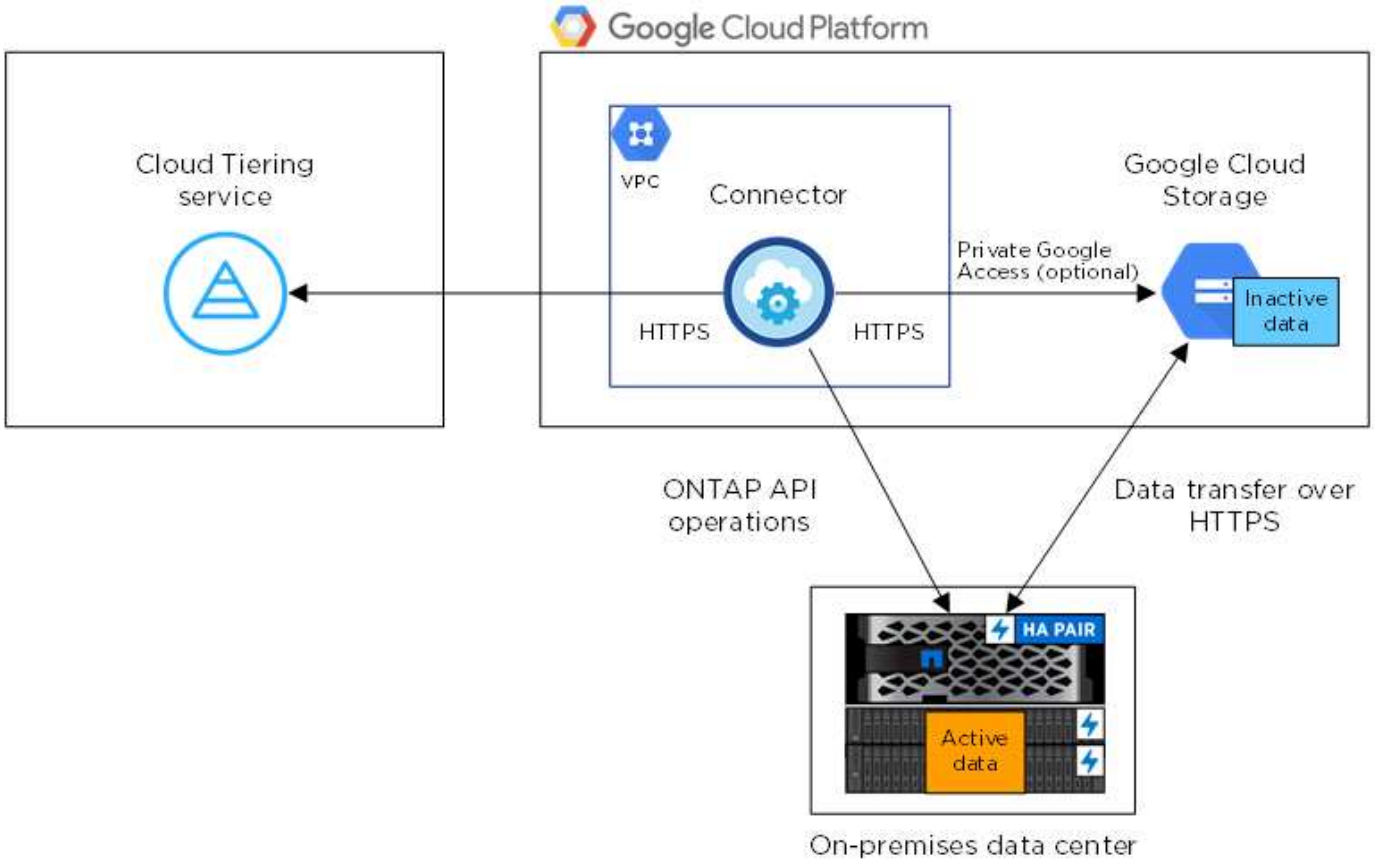
Nach Abschluss der kostenlosen Testversion zahlen Sie für Cloud Tiering über ein Pay-as-you-go-Abonnement, eine ONTAP-Tiering-Lizenz oder eine Kombination aus den beiden Optionen:

- Wenn Sie sich für den GCP Marketplace anmelden möchten, klicken Sie auf **Tiering > Lizenzierung**, klicken Sie auf **Abonnieren** und folgen Sie dann den Anweisungen.
- Um eine Tiering-Lizenz hinzuzufügen, Kontaktieren Sie uns, und dann "Fügen Sie ihn von Cloud Tiering zu Ihrem Cluster hinzu".

Anforderungen

Überprüfen Sie die Unterstützung für Ihr ONTAP Cluster, richten Sie Ihr Netzwerk ein und bereiten Sie den Objekt-Storage vor.

Die folgende Abbildung zeigt die einzelnen Komponenten und die Verbindungen, die zwischen den Komponenten vorbereitet werden müssen:



Die Kommunikation zwischen dem Connector und Google Cloud Storage ist nur für die Einrichtung von Objektspeichern bestimmt.

Vorbereiten der ONTAP Cluster

Ihre ONTAP-Cluster müssen beim Tiering von Daten auf Google Cloud Storage die folgenden Anforderungen erfüllen.

Unterstützte ONTAP Plattformen

Cloud Tiering unterstützt AFF Systeme und rein SSD-basierte Aggregate auf FAS Systemen.

Unterstützte ONTAP-Versionen

ONTAP 9.6 oder höher

Netzwerkanforderungen für Cluster

- Der ONTAP-Cluster initiiert eine HTTPS-Verbindung über Port 443 zu Google Cloud Storage.

  ONTAP liest und schreibt Daten auf und aus dem Objekt-Storage. Objekt-Storage startet nie, er reagiert einfach nur.

  Obwohl Google Cloud Interconnect eine bessere Performance bietet und geringere Datentransferkosten erzielt, ist dies nicht zwischen dem ONTAP Cluster und Google Cloud Storage erforderlich. Da die Performance beim Einsatz von Google Cloud Interconnect deutlich besser ist, wird dies als Best Practice empfohlen.

- Vom NetApp Service Connector, der sich in einer Google Cloud Platform VPC befindet, ist eine eingehende Verbindung erforderlich.

  Es ist keine Verbindung zwischen dem Cluster und dem Cloud Tiering Service erforderlich.

- Auf jedem ONTAP Node, der Tiered Volumes hostet, ist eine Intercluster-LIF erforderlich. Die LIF muss dem *IPspace* zugewiesen sein, den ONTAP zur Verbindung mit Objekt-Storage verwenden sollte.

  IPspaces ermöglichen die Trennung des Netzwerkdatenverkehrs und ermöglichen die Trennung des Client-Datenverkehrs für Datenschutz und Sicherheit. "Erfahren Sie mehr über IPspaces".

  Wenn Sie Daten-Tiering einrichten, werden Sie von Cloud Tiering aufgefordert, den IP-Speicherplatz zu verwenden. Sie sollten den IPspace auswählen, dem jede LIF zugeordnet ist. Dies kann der „Standard“-IPspace oder ein benutzerdefinierter IPspace sein, den Sie erstellt haben.

Unterstützte Volumes und Aggregate

Die Gesamtzahl der Volumes, die in Cloud Tiering Tiers möglich sind, ist unter Umständen kleiner als die Anzahl der Volumes in Ihrem ONTAP System. Das liegt daran, dass Volumes von einigen Aggregaten nicht abgestuft werden können. Sie können beispielsweise keine Daten-Tiers von SnapLock Volumes oder MetroCluster Konfigurationen erstellen. In der ONTAP-Dokumentation finden Sie weitere Informationen "Funktionalität oder Funktionen, die nicht von FabricPool unterstützt werden".

Cloud Tiering unterstützt FlexGroup Volumes. Setup funktioniert wie jedes andere Volume.

Erstellen oder Umschalten von Anschlüssen

Für das Tiering von Daten in die Cloud ist ein Connector erforderlich. Bei einem Tiering von Daten zu Google Cloud Storage muss ein Connector in einer Google Cloud Platform VPC verfügbar sein. Entweder müssen Sie einen neuen Konnektor erstellen oder sicherstellen, dass der aktuell ausgewählte Connector in der GCP liegt.

- "Erfahren Sie mehr über Steckverbinder"
- "Erstellen eines Konnektors in GCP"
- "Wechseln zwischen den Anschlüssen"

Vorbereiten der Vernetzung für den Connector

Stellen Sie sicher, dass der Connector über die erforderlichen Netzwerkverbindungen verfügt.

Schritte

1. Sicherstellen, dass die VPC, an der der Connector installiert ist, die folgenden Verbindungen ermöglicht:
   - Eine ausgehende Internetverbindung zum Cloud Tiering-Service über Port 443 (HTTPS)
   - Eine HTTPS-Verbindung über Port 443 zu Google Cloud Storage
   - Eine HTTPS-Verbindung über Port 443 zu Ihren ONTAP Clustern
2. Optional: Aktivieren Sie den privaten Google-Zugang im Subnetz, in dem Sie den Service Connector bereitstellen möchten.

   "Privater Zugriff Auf Google" Empfiehlt sich, wenn Sie eine direkte Verbindung von Ihrem ONTAP Cluster zur VPC haben und Sie eine Kommunikation zwischen dem Connector und Google Cloud Storage wünschen, um in Ihrem virtuellen privaten Netzwerk zu bleiben. Beachten Sie, dass Private Google Access mit VM-Instanzen funktioniert, die nur interne (private) IP-Adressen haben (keine externen IP-Adressen).

Vorbereitung von Google Cloud Storage für Daten-Tiering

Wenn Sie Tiering einrichten, müssen Sie Speicherzugriffsschlüssel für ein Servicekonto mit Storage Admin-Berechtigungen bereitstellen. Über ein Servicekonto kann Cloud Tiering die für das Daten-Tiering verwendeten Cloud Storage Buckets authentifizieren und darauf zugreifen. Die Schlüssel sind erforderlich, damit Google Cloud Storage weiß, wer die Anfrage stellt.

Schritte

1. "Erstellen Sie ein Servicekonto mit der vordefinierten Rolle „Storage Admin“".
2. Gehen Sie zu "GCP-Speichereinstellungen" Außerdem Zugriffsschlüssel für das Servicekonto erstellen:
   a. Wählen Sie ein Projekt aus, und klicken Sie auf **Interoperabilität**. Falls Sie dies noch nicht getan haben, klicken Sie auf **Interoperabilitätszugriff aktivieren**.
   b. Klicken Sie unter **Zugriffsschlüssel für Servicekonten** auf **Schlüssel für ein Servicekonto erstellen**, wählen Sie das gerade erstellte Servicekonto aus und klicken Sie auf **Schlüssel erstellen**.

      Das müssen Sie unbedingt "Geben Sie die Schlüssel in Cloud Tiering ein" Später, wenn Sie Tiering einrichten.

Tiering inaktiver Daten vom ersten Cluster zu Google Cloud Storage

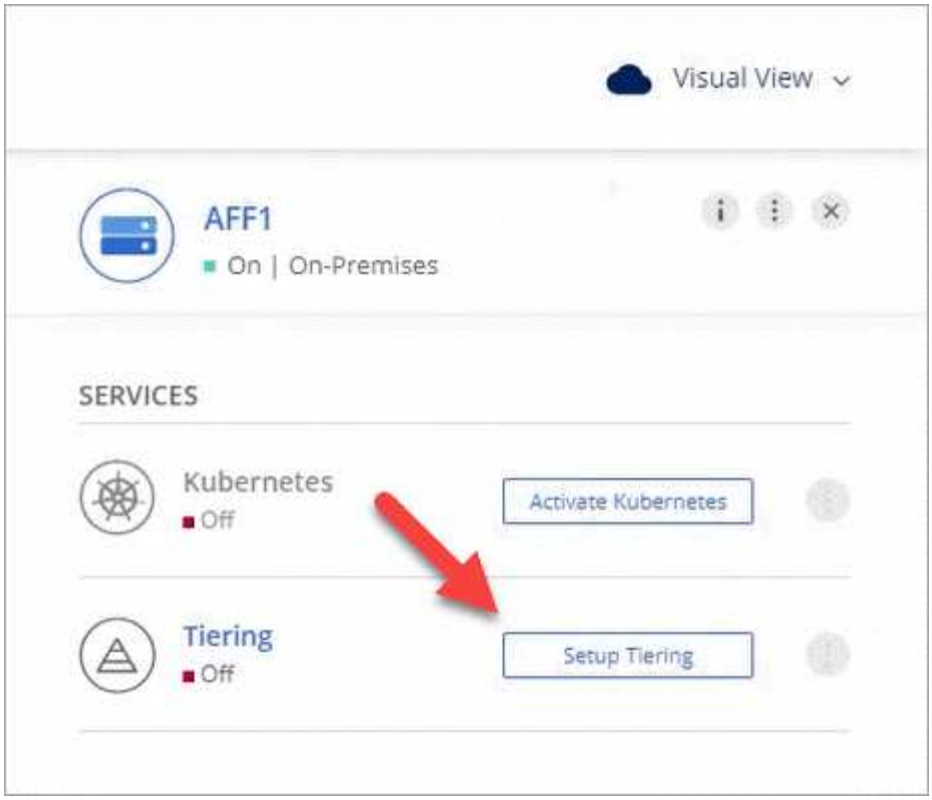
Nach der Vorbereitung Ihrer Google Cloud Umgebung können Sie vom ersten Cluster aus inaktive Daten per Tiering verschieben.

Was Sie benötigen

- "Eine Arbeitsumgebung vor Ort".
- Speicherzugriffsschlüssel für ein Servicekonto, das die Rolle Storage Admin hat.

Schritte

1. Wählen Sie ein On-Premises-Cluster aus.
2. Klicken Sie Auf **Tiering Einrichten**.

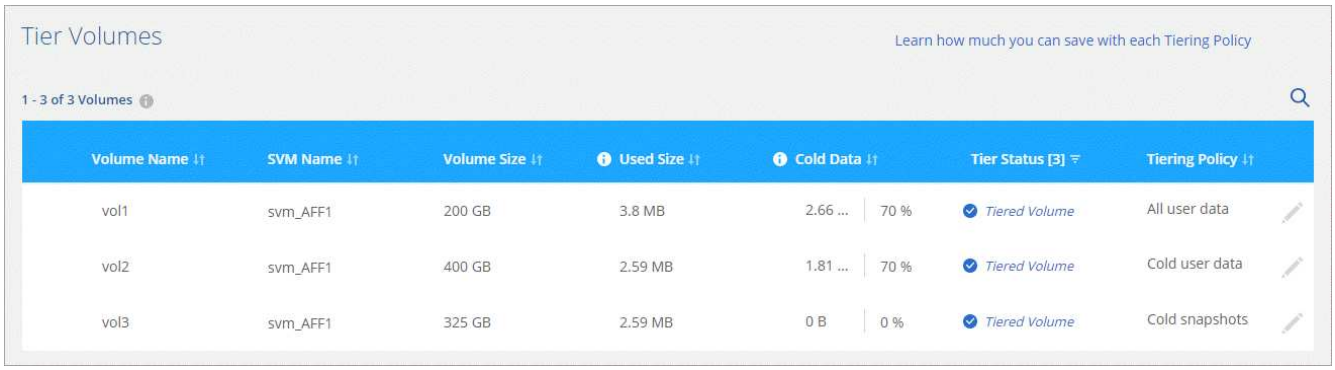


Sie befinden sich jetzt im Tiering Dashboard.

3. Klicken Sie neben dem Cluster auf **Tiering einrichten**.
4. Führen Sie die Schritte auf der Seite **Tiering Setup** aus:
   a. **Bucket**: Fügen Sie einen neuen Google Cloud Storage-Bucket hinzu oder wählen Sie einen vorhandenen Bucket aus und klicken Sie auf **Weiter**.
   b. **Speicherklasse**: Wählen Sie die Speicherklasse aus, die Sie für die Tiered-Daten verwenden möchten, und klicken Sie auf **Weiter**.
   c. **Anmeldeinformationen**: Geben Sie den Speicherzugriffsschlüssel und den geheimen Schlüssel für ein Servicekonto ein, das die Rolle Storage Admin hat.
   d. **Clusternetzwerk**: Wählen Sie den IPspace aus, den ONTAP verwenden soll, um eine Verbindung zum Objekt-Storage herzustellen, und klicken Sie auf **Weiter**.

      Durch die Auswahl des richtigen IPspaces wird sichergestellt, dass Cloud Tiering eine Verbindung von ONTAP mit dem Objekt-Storage Ihres Cloud-Providers einrichten kann.
5. Klicken Sie auf **Weiter**, um die Volumes auszuwählen, die Sie abstufen möchten.
6. Richten Sie auf der Seite **Tier Volumes** Tiering für jedes Volume ein. Klicken Sie auf das Symbol, wählen Sie eine Tiering-Richtlinie aus, passen Sie optional die Kühltage an und klicken Sie auf **Apply**.

   "Weitere Informationen zu Volume Tiering Policies".



Ergebnis

Sie haben das Daten-Tiering von Volumes im Cluster erfolgreich in den Google Cloud Objektspeicher eingerichtet.

Was kommt als Nächstes?

"Denken Sie daran, den Cloud Tiering Service zu abonnieren".

Sie können auch weitere Cluster hinzufügen oder Informationen zu den aktiven und inaktiven Daten auf dem Cluster prüfen. Weitere Informationen finden Sie unter "Managen von Daten-Tiering von Clustern".

Tiering von Daten von lokalen ONTAP Clustern zu StorageGRID

Durch Tiering von Daten an StorageGRID wird Speicherplatz für ONTAP-Cluster vor Ort freigegeben. Das Daten-Tiering wird durch den NetApp Cloud Tiering Service unterstützt.

Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

1 Daten werden auf StorageGRID-Ebene vorbereitet

Sie benötigen Folgendes:

- Ein AFF- oder FAS-System mit reinen SSD-Aggregaten, auf denen ONTAP 9.4 oder höher ausgeführt wird, und eine Verbindung über einen vom Benutzer angegebenen Port an StorageGRID.
- StorageGRID 10.3 oder höher mit AWS-Zugriffsschlüsseln mit S3-Berechtigungen.
- Ein Connector, der auf Ihrem Gelände installiert ist.
- Networking für den Connector, der eine ausgehende HTTPS-Verbindung zum ONTAP-Cluster, zu StorageGRID und zum Cloud Tiering-Service ermöglicht.

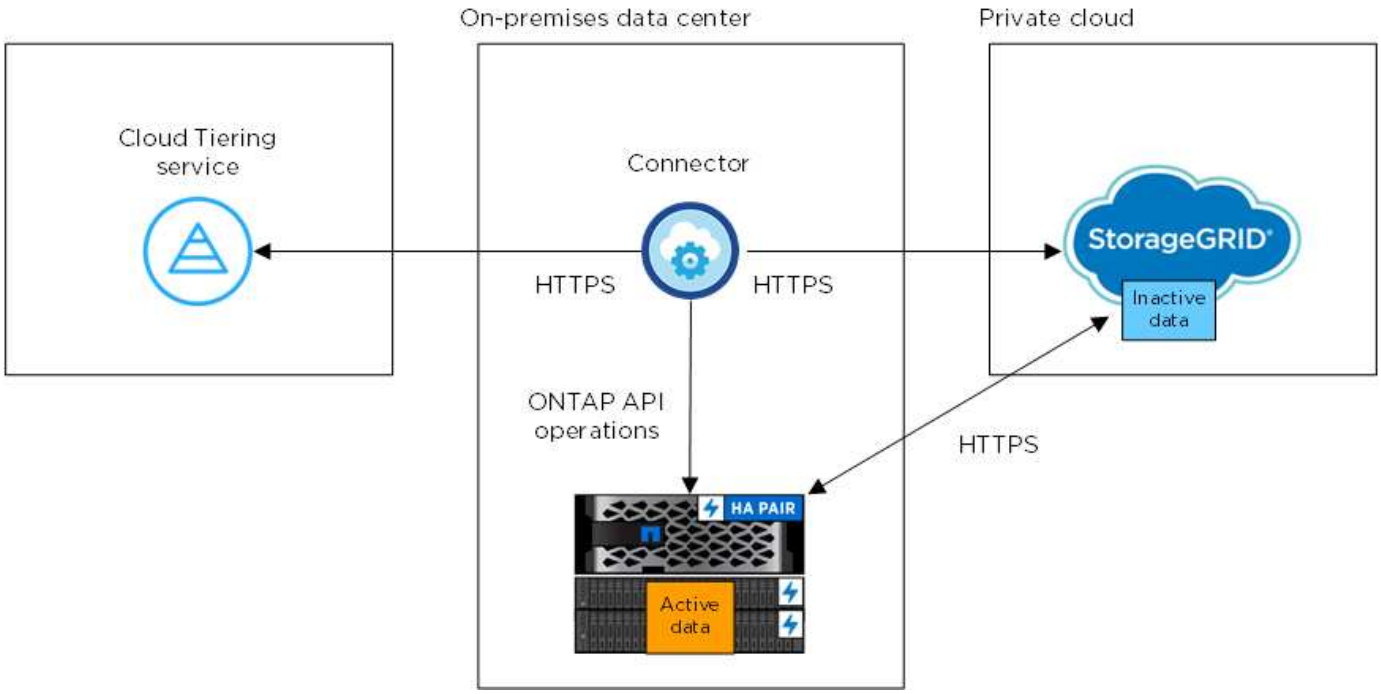
2 Tiering einrichten

Wählen Sie eine lokale Arbeitsumgebung aus, klicken Sie auf **Tiering einrichten** und folgen Sie den Anweisungen zum Tiering von Daten auf StorageGRID.

Anforderungen

Überprüfen Sie die Unterstützung für Ihr ONTAP Cluster, richten Sie Ihr Netzwerk ein und bereiten Sie den Objekt-Storage vor.

Die folgende Abbildung zeigt die einzelnen Komponenten und die Verbindungen, die zwischen den Komponenten vorbereitet werden müssen:



Die Kommunikation zwischen Connector und StorageGRID dient nur der Einrichtung des Objektspeichers.

Vorbereiten der ONTAP Cluster

Ihre ONTAP-Cluster müssen beim Tiering von Daten zu StorageGRID die folgenden Anforderungen erfüllen.

Unterstützte ONTAP Plattformen

Cloud Tiering unterstützt AFF Systeme und rein SSD-basierte Aggregate auf FAS Systemen.

Unterstützte ONTAP Version

ONTAP 9.4 oder höher

Lizenzierung

Eine FabricPool Lizenz ist nicht erforderlich auf dem ONTAP Cluster wenn Tiering von Daten zu StorageGRID.

Netzwerkanforderungen für Cluster

- Das ONTAP-Cluster initiiert eine HTTPS-Verbindung über einen vom Benutzer angegebenen Port zum StorageGRID (der Port ist während der Tiering-Einrichtung konfigurierbar).

  ONTAP liest und schreibt Daten auf und aus dem Objekt-Storage. Objekt-Storage startet nie, er reagiert einfach nur.

- Über den Konnektor ist eine eingehende Verbindung erforderlich, die sich in Ihrem Haus befinden muss.

  Es ist keine Verbindung zwischen dem Cluster und dem Cloud Tiering Service erforderlich.

- Auf jedem ONTAP Node, der Tiered Volumes hostet, ist eine Intercluster-LIF erforderlich. Die LIF muss dem *IPspace* zugewiesen sein, den ONTAP zur Verbindung mit Objekt-Storage verwenden sollte.

  IPspaces ermöglichen die Trennung des Netzwerkdatenverkehrs und ermöglichen die Trennung des Client-Datenverkehrs für Datenschutz und Sicherheit. "Erfahren Sie mehr über IPspaces".

  Wenn Sie Daten-Tiering einrichten, werden Sie von Cloud Tiering aufgefordert, den IP-Speicherplatz zu verwenden. Sie sollten den IPspace auswählen, dem jede LIF zugeordnet ist. Dies kann der „Standard"-IPspace oder ein benutzerdefinierter IPspace sein, den Sie erstellt haben.

Unterstützte Volumes und Aggregate

Die Gesamtzahl der Volumes, die in Cloud Tiering Tiers möglich sind, ist unter Umständen kleiner als die Anzahl der Volumes in Ihrem ONTAP System. Das liegt daran, dass Volumes von einigen Aggregaten nicht abgestuft werden können. Sie können beispielsweise keine Daten-Tiers von SnapLock Volumes oder MetroCluster Konfigurationen erstellen. In der ONTAP-Dokumentation finden Sie weitere Informationen "Funktionalität oder Funktionen, die nicht von FabricPool unterstützt werden".

Cloud Tiering unterstützt FlexGroup Volumes ab ONTAP 9.5. Setup funktioniert wie jedes andere Volume.

StorageGRID wird vorbereitet

StorageGRID muss folgende Anforderungen erfüllen:

Unterstützte StorageGRID-Versionen

StorageGRID 10.3 und höher werden unterstützt.

S3-Anmeldedaten

Wenn Sie Tiering in StorageGRID einrichten, müssen Sie Cloud Tiering mit einem S3-Zugriffsschlüssel und einem geheimen Schlüssel bereitstellen. Cloud Tiering verwendet die Schlüssel für den Zugriff auf Ihre Buckets.

Diese Zugriffsschlüssel müssen einem Benutzer mit den folgenden Berechtigungen zugeordnet sein:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Objektversionierung

Sie dürfen die StorageGRID Objektversionierung auf dem Objektspeicher-Bucket nicht aktivieren.

Erstellen oder Umschalten von Anschlüssen

Für das Tiering von Daten in die Cloud ist ein Connector erforderlich. Beim Tiering von Daten zu StorageGRID muss an Ihrem Standort ein Connector verfügbar sein. Sie müssen entweder einen neuen Konnektor installieren oder sicherstellen, dass sich der aktuell ausgewählte Connector auf der Prem befindet.

- "Erfahren Sie mehr über Steckverbinder"
- "Connector-Host-Anforderungen"
- "Installieren des Connectors auf einem vorhandenen Linux-Host"
- "Wechseln zwischen den Anschlüssen"

Vorbereiten der Vernetzung für den Connector

Stellen Sie sicher, dass der Connector über die erforderlichen Netzwerkverbindungen verfügt.

Schritte

1. Stellen Sie sicher, dass das Netzwerk, in dem der Connector installiert ist, folgende Verbindungen ermöglicht:
    - Eine ausgehende Internetverbindung zum Cloud Tiering-Service über Port 443 (HTTPS)
    - Eine HTTPS-Verbindung über Port 443 zu StorageGRID
    - Eine HTTPS-Verbindung über Port 443 zu Ihren ONTAP Clustern

Tiering inaktiver Daten von dem ersten Cluster zu StorageGRID

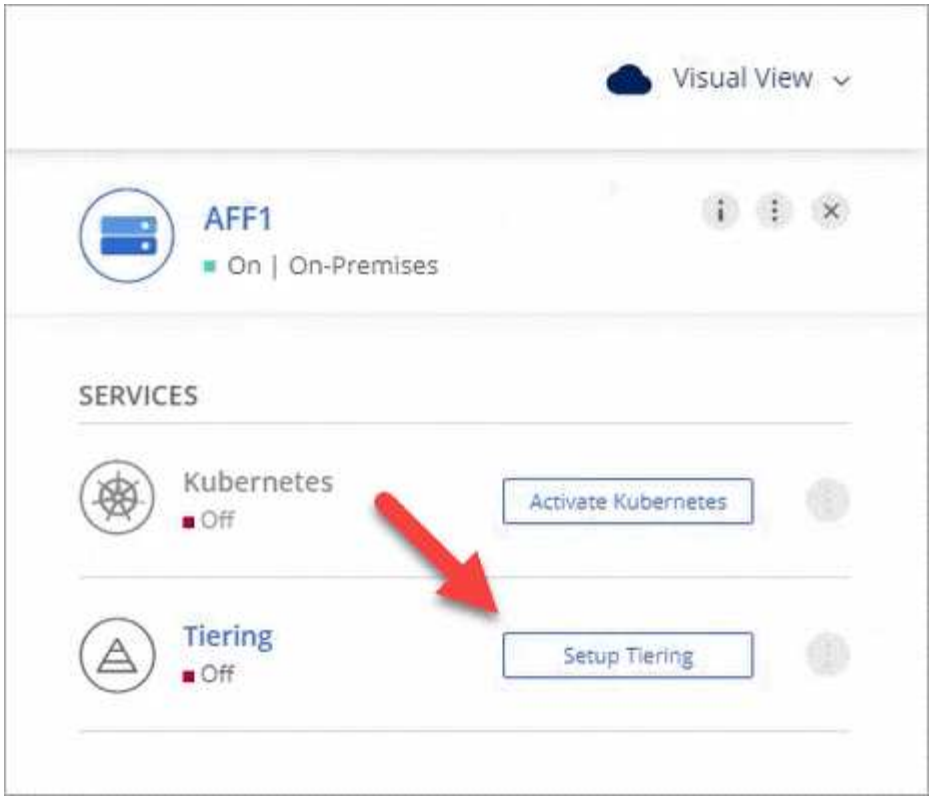
Starten Sie nach der Vorbereitung der Umgebung das Tiering inaktiver Daten aus dem ersten Cluster.

Was Sie benötigen

- "Eine Arbeitsumgebung vor Ort".
- Einen AWS-Zugriffsschlüssel mit den erforderlichen S3-Berechtigungen.

Schritte

1. Wählen Sie ein On-Premises-Cluster aus.
2. Klicken Sie Auf **Tiering Einrichten**.

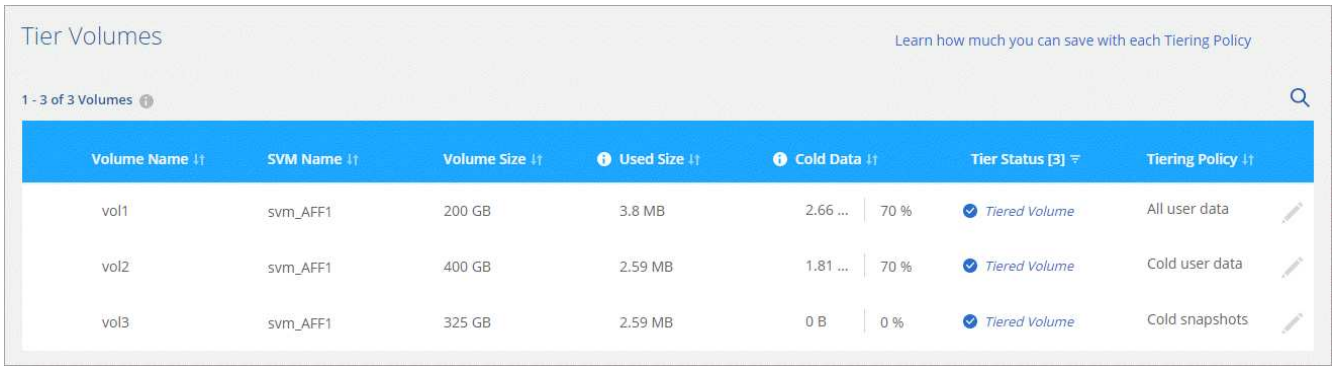


Sie befinden sich jetzt im Tiering Dashboard.

3. Klicken Sie neben dem Cluster auf **Tiering einrichten**.
4. Führen Sie die Schritte auf der Seite **Tiering Setup** aus:
   a. **Wählen Sie Ihren Anbieter**: Wählen Sie StorageGRID.
   b. **Server**: Geben Sie den FQDN des StorageGRID-Servers ein, geben Sie den Port ein, den ONTAP für die HTTPS-Kommunikation mit StorageGRID verwenden soll, und geben Sie den Zugriffsschlüssel und den geheimen Schlüssel für ein AWS-Konto ein, das über die erforderlichen S3-Berechtigungen verfügt.
   c. **Bucket**: Fügen Sie einen neuen Bucket hinzu oder wählen Sie einen vorhandenen Bucket für die Tiered Data aus.
   d. **Clusternetzwerk**: Wählen Sie den IPspace aus, den ONTAP verwenden soll, um eine Verbindung zum Objekt-Storage herzustellen, und klicken Sie auf **Weiter**.

      Durch die Auswahl des richtigen IPspaces wird sichergestellt, dass Cloud Tiering eine Verbindung von ONTAP mit dem Objekt-Storage Ihres Cloud-Providers einrichten kann.
5. Klicken Sie auf **Weiter**, um die Volumes auszuwählen, die Sie abstufen möchten.
6. Richten Sie auf der Seite **Tier Volumes** Tiering für jedes Volume ein. Klicken Sie auf das Symbol, wählen Sie eine Tiering-Richtlinie aus, passen Sie optional die Kühltage an und klicken Sie auf **Apply**.

   "Weitere Informationen zu Volume Tiering Policies".



Ergebnis

Sie haben erfolgreich das Daten-Tiering von Volumes auf dem Cluster zu StorageGRID eingerichtet.

Was kommt als Nächstes?

Sie können weitere Cluster hinzufügen oder Informationen zu den aktiven und inaktiven Daten auf dem Cluster prüfen. Weitere Informationen finden Sie unter "Managen von Daten-Tiering von Clustern".

Lizenzierung für Cloud Tiering einrichten

Sie bezahlen für Cloud Tiering über ein Pay-as-you-go-Abonnement, eine ONTAP Tiering-Lizenz namens *FabricPool* oder eine Kombination aus beidem. Wenn Sie ein nutzungsbasiertes Zahlungsmodell nutzen möchten, müssen Sie den Cloud-Provider abonnieren, für den Sie kalte Daten Tiering möchten. Sie müssen sich nicht von jedem Markt anmelden.

Ein paar Notizen, bevor Sie weitere lesen:

- Wenn eine FabricPool-Lizenz bereits auf Ihrem Cluster installiert ist, dann sind Sie alle eingestellt – es gibt nichts anderes, was Sie tun müssen.
- Wenn Sie das Cloud Manager Abonnement bereits im Markt Ihres Cloud-Providers abonniert haben, haben Sie sich auch automatisch für Cloud Tiering angemeldet. Auf der Registerkarte Cloud Tiering **Licensing** sehen Sie ein aktives Abonnement. Sie müssen sich nicht erneut anmelden.
- Beim Tiering von Daten zu StorageGRID fallen keine Kosten an. Es ist keine BYOL-Lizenz oder PAYGO-Registrierung erforderlich.

"Erfahren Sie mehr über die Funktionsweise der Lizenzierung für Cloud Tiering".

Abonnieren im AWS Marketplace

Abonnieren Sie über den AWS Marketplace ein Cloud-Tiering, um ein Pay-as-you-go-Abonnement für Daten-Tiering von ONTAP-Clustern in AWS S3 einzurichten.

Schritte

1. Klicken Sie in Cloud Manager auf **Tiering > Lizenzierung**.
2. Klicken Sie unter AWS Marketplace auf **Abonnieren** und dann auf **Weiter**.
3. Melden Sie sich über den AWS Marketplace an, und melden Sie sich anschließend bei Cloud Central an, um die Registrierung abzuschließen.

Das folgende Video zeigt den Prozess:

► https://docs.netapp.com/de-de/occm38//media/video_subscribing_aws_tiering.mp4 *(video)*

Abonnieren im Azure Marketplace

Abonnieren Sie Cloud Tiering über den Azure Marketplace, um ein Pay-as-you-go-Abonnement für Daten-Tiering von ONTAP-Clustern in den Azure Blob-Storage einzurichten.

Schritte

1. Klicken Sie in Cloud Manager auf **Tiering > Lizenzierung**.
2. Klicken Sie unter Azure Marketplace auf **Abonnieren** und dann auf **Weiter**.
3. Melden Sie sich im Azure Marketplace an, und melden Sie sich anschließend bei Cloud Central an, um die Registrierung abzuschließen.

   Das folgende Video zeigt den Prozess:

   ► https://docs.netapp.com/de-de/occm38//media/video_subscribing_azure_tiering.mp4 *(video)*

Abonnieren im GCP Marketplace

Über den GCP Marketplace können Sie Cloud Tiering abonnieren, um ein Pay-as-you-go-Abonnement für Daten-Tiering von ONTAP-Clustern in Google Cloud Storage einzurichten.

Schritte

1. Klicken Sie in Cloud Manager auf **Tiering > Lizenzierung**.
2. Klicken Sie unter GCP Marketplace auf **Abonnieren** und dann auf **Weiter**.
3. Melden Sie sich für den GCP Marketplace an und melden Sie sich dann bei Cloud Central an, um die Registrierung abzuschließen.

   das folgende Video zeigt den Vorgang:

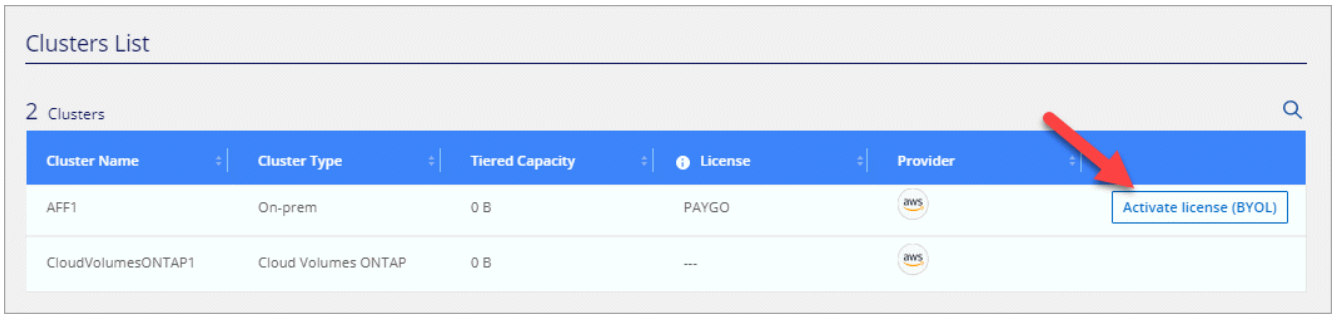
   ► https://docs.netapp.com/de-de/occm38//media/video_subscribing_gcp_tiering.mp4 *(video)*

Hinzufügen einer Tiering-Lizenz zum ONTAP

Sie können Ihre eigene Lizenz beim Kauf einer ONTAP FabricPool Lizenz von NetApp erwerben.

Schritte

1. Wenn Sie keine FabricPool-Lizenz besitzen, Kontaktieren Sie uns.
2. Klicken Sie in Cloud Manager auf **Tiering > Lizenzierung**.
3. Klicken Sie in der Tabelle Cluster List auf **Activate License (BYOL)** für einen On-Prem ONTAP-Cluster.



4. Geben Sie die Seriennummer der Lizenz ein, und geben Sie anschließend das mit der Seriennummer verbundene NetApp Support Site Konto ein.
5. Klicken Sie auf **Lizenz aktivieren**.

Ergebnis

Cloud Tiering registriert die Lizenz und installiert sie im Cluster.

Nachdem Sie fertig sind

Wenn Sie zu einem späteren Zeitpunkt zusätzliche Kapazität erwerben, wird die Lizenz für das Cluster automatisch mit der neuen Kapazität aktualisiert. Es ist nicht erforderlich, eine neue NetApp Lizenzdatei (NetApp License File, NLF) auf das Cluster anzuwenden.

Managen von Daten-Tiering von Clustern

Nachdem Sie jetzt Daten-Tiering von Ihren ONTAP Clustern einrichten, können Sie Daten von zusätzlichen Volumes abstufen, die Tiering-Richtlinie eines Volumes ändern und vieles mehr.

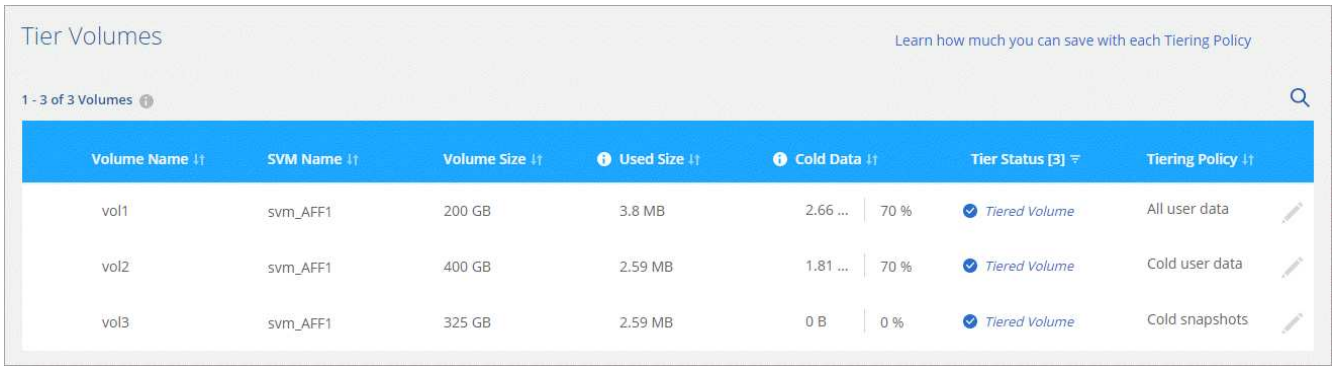
Tiering von Daten aus zusätzlichen Volumes

Sie können das Daten-Tiering für zusätzliche Volumes jederzeit einrichten, beispielsweise nach der Erstellung eines neuen Volumes.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Tiering**.
2. Klicken Sie im **Cluster Dashboard** auf **Tier Volumes** für den Cluster.
3. Klicken Sie für jedes Volume auf das Symbol, wählen Sie eine Tiering-Richtlinie aus, passen Sie optional die Kühltage an und klicken Sie auf **Apply**.

   "Weitere Informationen zu Volume Tiering Policies".



Sie müssen den Objekt-Storage nicht konfigurieren, da er bereits bei der erstmaligen Einrichtung von Tiering für den Cluster konfiguriert wurde. ONTAP verschiebt inaktive Daten von diesen Volumes auf denselben Objektspeicher.

4. Wenn Sie fertig sind, klicken Sie auf **Schließen**.

Ändern der Tiering-Richtlinie eines Volumes

Durch die Änderung der Tiering-Richtlinie für ein Volume wird die ONTAP Tiering von „kalten“ Daten zu Objekt-Storage geändert. Die Änderung beginnt ab dem Zeitpunkt, an dem Sie die Richtlinie ändern - es ändert nur das nachfolgende Tiering-Verhalten für das Volume.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Tiering**.
2. Klicken Sie im **Cluster Dashboard** auf **Tier Volumes** für den Cluster.
3. Klicken Sie auf das Symbol, wählen Sie eine Tiering-Richtlinie aus, passen Sie optional die Kühltage an und klicken Sie auf **Apply**.

   "Weitere Informationen zu Volume Tiering Policies".

Verwalten von Tiering-Einstellungen auf Aggregaten

Sie können für jedes Aggregat zwei Einstellungen anpassen: Den Tiering-Auslastungsschwellenwert und den aktivierten Status der inaktiven Datenberichterstellung.

Schwellenwert für Tiering-Fülle

Wenn Sie den Schwellenwert auf eine niedrigere Zahl setzen, wird die Datenmenge reduziert, die vor der Durchführung des Tiering auf der Performance-Tier gespeichert werden muss. Dies könnte nützlich sein für große Aggregate, die wenig aktive Daten enthalten.

Wenn Sie den Schwellenwert auf eine höhere Anzahl setzen, erhöht sich die Datenmenge, die Sie vor dem Tiering auf der Performance-Tier speichern müssen. Dies ist vielleicht bei Lösungen nützlich, die nur auf Tiers ausgelegt sind, wenn Aggregate nahe der maximalen Kapazität sind.

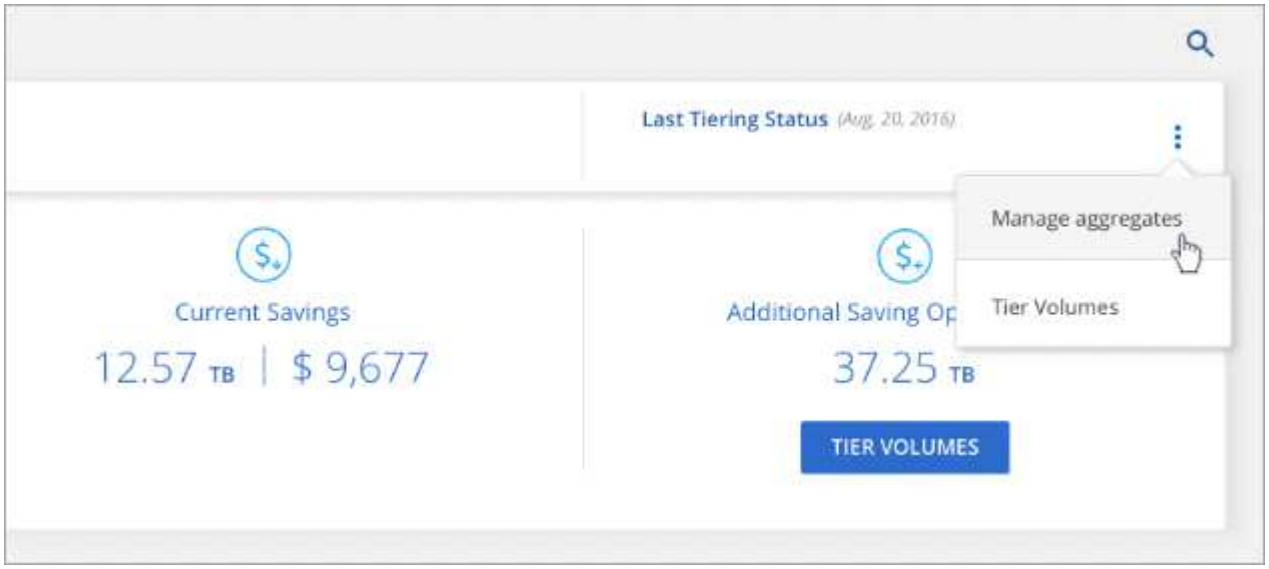
Berichterstellung für inaktive Daten

Berichte für inaktive Daten (Inactive Data Reporting, IDR) bestimmen anhand eines 31-Tage-Kühlzeitraums, welche Daten als inaktiv erachtet werden. Die Menge der Tier-basierten „kalten“ Daten hängt von den auf Volumes festgelegten Tiering-Richtlinien ab. Diese Menge kann sich von der Menge an kalten Daten unterscheiden, die von IDR in einer 31-Tage-Kühlzeit erkannt wurden.

Am besten lässt sich das IDR aktivieren, da es dabei hilft, Ihre inaktiven Daten zu identifizieren und Einsparmöglichkeiten zu nutzen. IDR muss aktiviert bleiben, wenn das Daten-Tiering auf einem Aggregat aktiviert wäre.

Schritte

1. Klicken Sie oben im Cloud Manager auf **Tiering**.
2. Klicken Sie auf der Seite **Cloud Tiering** auf das Menüsymbol für einen Cluster und wählen Sie **Aggregate verwalten**.



3. Klicken Sie auf der Seite * Aggregate verwalten* auf das Symbol für ein Aggregat in der Tabelle.
4. Ändern Sie den Schwellenwert für die Fülle, und wählen Sie aus, ob inaktive Datenberichte aktiviert oder deaktiviert werden sollen.

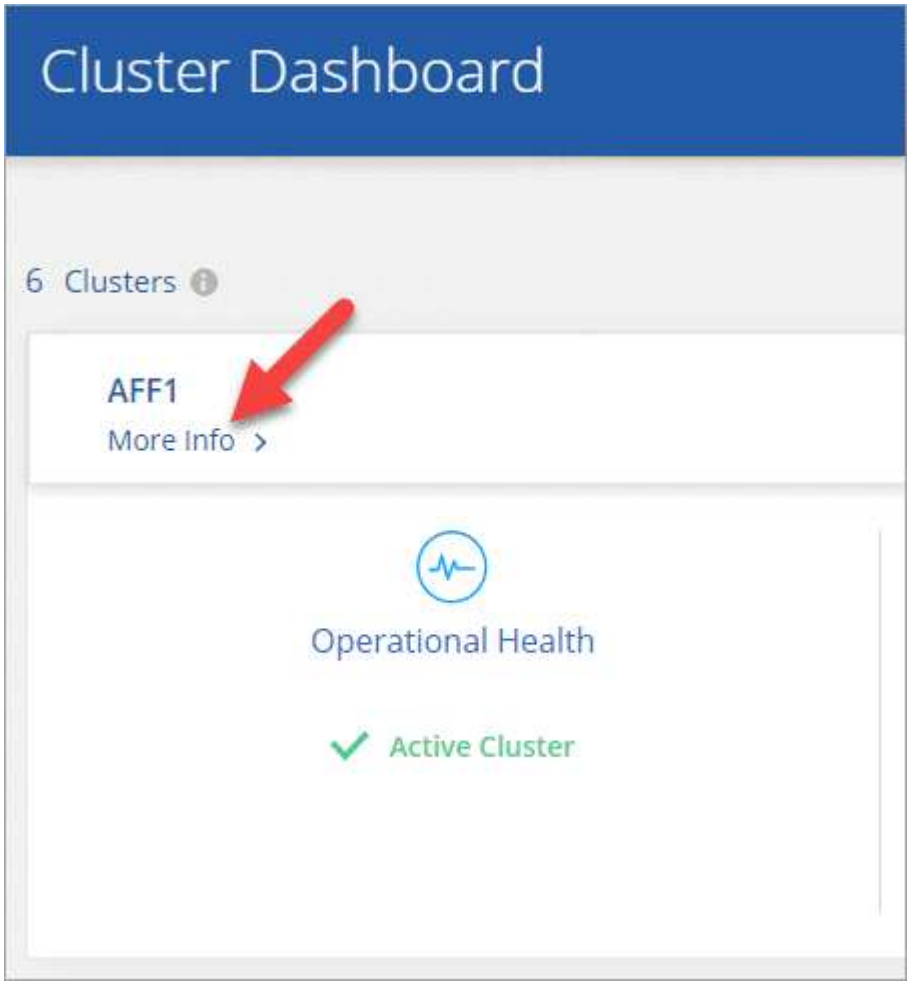
5. Klicken Sie Auf **Anwenden**.

Überprüfen von Tiering-Informationen für ein Cluster

Es empfiehlt sich möglicherweise, zu sehen, wie viele Daten sich im Cloud-Tier befinden und wie viele Daten auf Festplatten gespeichert sind. Außerdem ist es möglich, die Menge der „heißen“ und „kalten“ Daten auf den Festplatten des Clusters anzuzeigen. Cloud Tiering bietet diese Informationen für jeden Cluster.

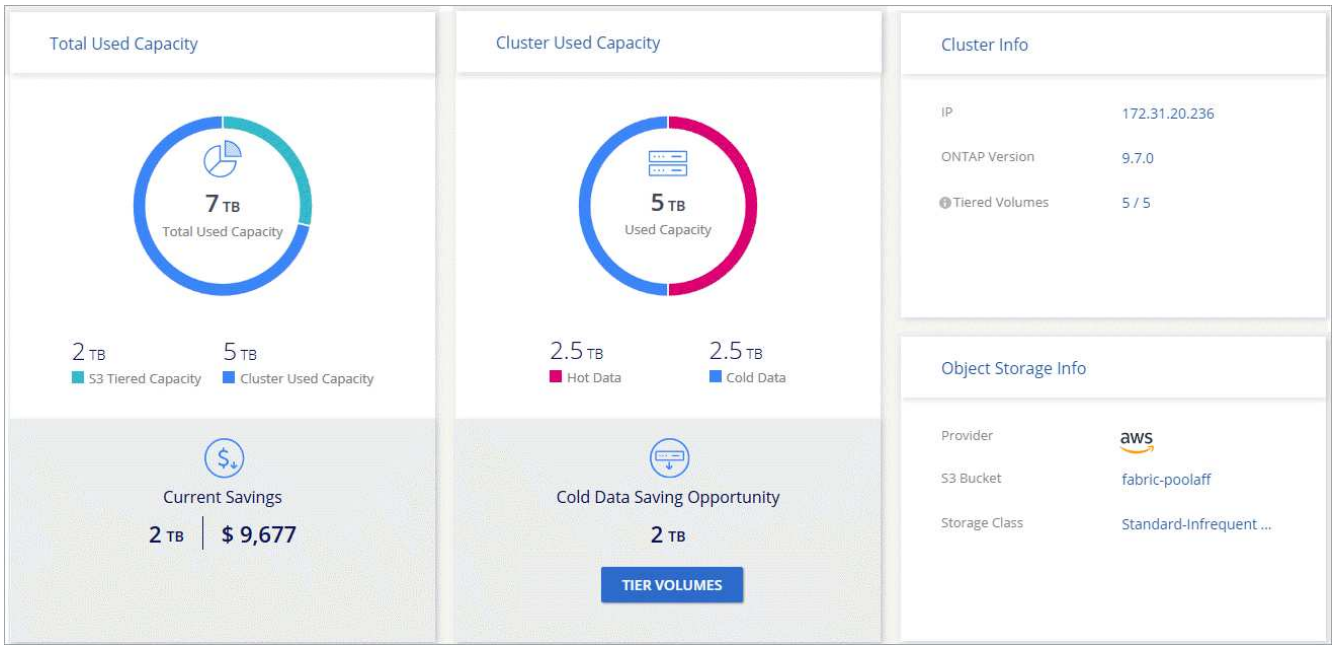
Schritte

1. Klicken Sie oben im Cloud Manager auf **Tiering**.
2. Klicken Sie im **Cluster Dashboard** auf **Weitere Informationen** für einen Cluster.



3. Überprüfen Sie die Details zum Cluster.

   Hier ein Beispiel:

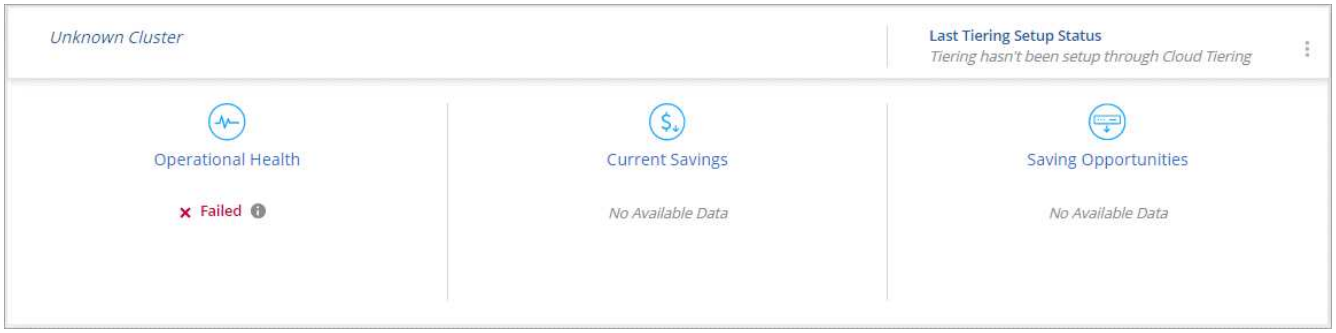


Korrektur des Betriebszustands

Ausfälle können auftreten. Ist dies der Fall, zeigt Cloud Tiering auf dem Cluster Dashboard einen „ausgefallenen“ Betriebszustand an. Der Systemzustand gibt den Status des ONTAP Systems und Cloud Manager wieder.

Schritte

1. Ermitteln Sie alle Cluster, deren Betriebszustand „ausgefallen“ ist.



2. Fahren Sie mit dem Mauszeiger auf Symbol, um den Fehlergrund anzuzeigen.
3. Korrigieren Sie das Problem:
   a. Vergewissern Sie sich, dass das ONTAP-Cluster betriebsbereit ist und über eine ein- und ausgehende Verbindung zu Ihrem Objekt-Storage-Provider verfügt.
   b. Vergewissern Sie sich, dass Cloud Manager über ausgehende Verbindungen zum Cloud Tiering Service, zum Objektspeicher und zu den erkannte ONTAP-Clustern verfügt.

Cloud Tiering – technische FAQ

Diese FAQ kann Ihnen helfen, wenn Sie nur nach einer schnellen Antwort auf eine Frage suchen.

ONTAP

Die nachfolgenden Fragen betreffen ONTAP.

Welche Anforderungen gelten für mein ONTAP Cluster?

Es hängt davon ab, wo Sie die „kalten“ Daten Tiering verschieben. Beachten Sie Folgendes:

- "Tiering von Daten von lokalen ONTAP Clustern zu Amazon S3"
- "Tiering von Daten von lokalen ONTAP Clustern zu Azure Blob Storage"
- "Tiering von Daten aus lokalen ONTAP Clustern in Google Cloud Storage"
- "Tiering von Daten von lokalen ONTAP Clustern zu StorageGRID"

Ermöglicht Cloud Tiering die Berichterstellung inaktiver Daten?

Ja, mit Cloud Tiering können Sie auf jedem Aggregat inaktive Daten erstellen. Durch diese Einstellung können wir die Menge inaktiver Daten ermitteln, die zu kostengünstigem Objekt-Storage verschoben werden können.

Kann ich Daten von NAS-Volumes und SAN-Volumes verschieben?

Mit Cloud Tiering lassen sich Daten von NAS Volumes in die Public Cloud und von SAN Volumes in eine Private Cloud mithilfe von StorageGRID verschieben.

Wie sieht es mit Cloud Volumes ONTAP aus?

Wenn Sie über Cloud Volumes ONTAP Systeme verfügen, finden Sie sie im Cluster Dashboard, sodass Sie einen umfassenden Überblick über Daten-Tiering in Ihrer Hybrid-Cloud-Infrastruktur erhalten.

Über die Cluster-Konsole können Sie Tiering-Informationen anzeigen, die ähnlich wie bei einem ONTAP-Cluster vor Ort sind: Systemzustand, aktuelle Einsparungen, Einsparmöglichkeiten, Details zu Volumes und Aggregaten usw.

Cloud Volumes ONTAP Systeme sind schreibgeschützt aus Cloud Tiering. Sie können kein Daten-Tiering auf Cloud Volumes ONTAP über Cloud Tiering einrichten. Sie werden weiterhin Tiering auf die gleiche Weise einrichten: Aus der Arbeitsumgebung in Cloud Manager.

Objekt-Storage

Die folgenden Fragen betreffen den Objekt-Storage.

Welche Objekt-Storage-Anbieter werden unterstützt?

Es werden Amazon S3, Azure Blob Storage, Google Cloud Storage und StorageGRID über das S3-Protokoll unterstützt.

Kann ich meinen eigenen Bucket/Container verwenden?

Ja, können Sie. Wenn Sie Daten-Tiering einrichten, können Sie einen neuen Bucket/Container hinzufügen oder einen vorhandenen Bucket/Container auswählen.

Welche Regionen werden unterstützt?

- "Unterstützte AWS-Regionen"
- "Unterstützte Azure Regionen"
- "Unterstützte Google Cloud Regionen"

Welche S3-Storage-Klassen werden unterstützt?

Cloud Tiering unterstützt Daten-Tiering in die Storage-Klasse *Standard*, *Standard-infrequent Access*, *One Zone-IA* oder *Intelligent*. Siehe "Unterstützte S3-Storage-Klassen" Entnehmen.

Welche Azure Blob-Zugriffsebenen werden unterstützt?

Cloud-Tiering nutzt automatisch die Zugriffsebene „*Hot*“ für Ihre inaktiven Daten.

Welche Storage-Klassen werden für Google Cloud Storage unterstützt?

Cloud Tiering nutzt die *Standard* Storage-Klasse für inaktive Daten.

Verwendet Cloud Tiering einen Objektspeicher für den gesamten Cluster oder einen pro Aggregat?

Ein Objektspeicher für das gesamte Cluster.

Kann ich Richtlinien auf meinen Objektspeicher anwenden, um Daten unabhängig vom Tiering zu verschieben?

Nein, Cloud Tiering unterstützt keine Objekt-Lifecycle-Managementregeln, die Daten aus Objektspeichern verschieben oder löschen.

Anschlüsse

Die folgenden Fragen beziehen sich auf Steckverbinder.

Wo muss der Connector installiert werden?

- Beim Tiering von Daten zu S3 kann ein Connector in einer AWS VPC oder am Standort des Unternehmens residieren.
- Beim Tiering von Daten zu Blob Storage muss ein Connector in einer Azure vnet residieren.
- Bei einem Tiering von Daten zu Google Cloud Storage muss ein Connector in einer Google Cloud Platform VPC abgelegt werden.
- Beim Tiering von Daten zu StorageGRID muss ein Connector auf einem lokalen Linux-Host residieren.

Netzwerkbetrieb

Die folgenden Fragen beziehen sich auf das Netzwerk.

Welche Netzwerkanforderungen gibt es?

- Das ONTAP Cluster initiiert eine HTTPS-Verbindung über Port 443 zum Objekt-Storage-Provider.

  ONTAP liest und schreibt Daten auf und aus dem Objekt-Storage. Objekt-Storage startet nie, er reagiert einfach nur.

- Bei StorageGRID initiiert das ONTAP-Cluster eine HTTPS-Verbindung über einen vom Benutzer angegebenen Port zum StorageGRID (der Port ist während der Tiering-Einrichtung konfigurierbar).
- Für einen Connector wird eine ausgehende HTTPS-Verbindung über Port 443 zu Ihren ONTAP-Clustern, zum Objektspeicher und zum Cloud Tiering-Service benötigt.

Weitere Informationen finden Sie unter:

- "Tiering von Daten von lokalen ONTAP Clustern zu Amazon S3"
- "Tiering von Daten von lokalen ONTAP Clustern zu Azure Blob Storage"
- "Tiering von Daten aus lokalen ONTAP Clustern in Google Cloud Storage"
- "Tiering von Daten von lokalen ONTAP Clustern zu StorageGRID"

Berechtigungen

Die folgenden Fragen beziehen sich auf Berechtigungen.

Welche Berechtigungen sind in AWS erforderlich?

Berechtigungen erforderlich "Zum Managen des S3-Buckets".

Welche Berechtigungen sind in Azure erforderlich?

Außerhalb der Berechtigungen, die zur Bereitstellung für Cloud Manager erforderlich sind, sind keine zusätzlichen Berechtigungen erforderlich.

Welche Berechtigungen sind bei der Google Cloud Platform erforderlich?

Storage-Admin-Berechtigungen sind für ein Servicekonto mit Speicherzugriffsschlüsseln erforderlich.

Welche Berechtigungen sind für StorageGRID erforderlich?

"S3 Berechtigungen sind erforderlich".

Referenz

Unterstützte S3-Storage-Klassen und Regionen

Cloud Tiering unterstützt mehrere S3-Storage-Klassen und meisten Regionen.

Unterstützte S3-Storage-Klassen

Cloud Tiering kann eine Lifecycle-Regel anwenden, sodass die Daten nach 30 Tagen von der *Standard* Storage-Klasse zur anderen Storage-Klasse wechseln. Sie können aus folgenden Speicherklassen wählen:

- Standardzugriff
- Eine Zone-IA
- Smart

Wenn Sie sich für „Standard“ entscheiden, verbleiben die Daten in dieser Storage-Klasse.

"Erfahren Sie mehr über S3-Storage-Klassen".

Unterstützte AWS-Regionen

Cloud-Tiering unterstützt die folgenden AWS Regionen.

Asien/Pazifik

- Mumbai
- Seoul
- Singapur
- Sydney
- Tokio

Europa

- Frankfurt
- Irland
- London
- Paris
- Stockholm

Nordamerika

- Kanada Mitte
- GovCloud (USA-West) – ab ONTAP 9.3
- US-Osten (N. Virginia)
- US-Osten (Ohio)
- US West (N. Kalifornien)
- US West (Oregon)

Südamerika

- São Paulo

Unterstützte Azure Blob-Zugriffsebenen und Regionen

Cloud Tiering unterstützt die Zugriffsebene *Hot* und die meisten Regionen.

Unterstützte Azure Blob-Zugriffsebenen

Wenn Sie Daten-Tiering zu Azure einrichten, verwendet Cloud Tiering automatisch die Zugriffsebene „*Hot*“ für Ihre inaktiven Daten.

Unterstützte Azure Regionen

Cloud-Tiering unterstützt die folgenden Azure Regionen.

Afrika

- Südafrika, Norden

Asien/Pazifik

- Australien Ost
- Australien Südosten
- Ostasien
- Japan Ost
- Japan West
- Korea Central
- Korea Süd
- Südostasien

Europa

- Frankreich, Mitte
- Deutschland Mitte
- Deutschland Nordosten
- Nordeuropa
- Großbritannien Süd
- UK West
- Westeuropa

Nordamerika

- Kanada Mitte
- Kanada Ost
- Zentral USA
- Osten US
- Osten US 2
- North Central USA
- South Central USA
- Westen USA
- West USA 2
- West Central USA

Südamerika

- Brasilien Süd

Unterstützte Google Cloud-Storage-Klassen und Regionen

Cloud Tiering unterstützt die Standard-Storage-Klasse und die meisten Google Cloud Regionen.

Unterstützte Zugriffstufen

Cloud Tiering verwendet die Zugriffsebene *Standard* für inaktive Daten.

Unterstützte Google Cloud Regionen

Cloud-Tiering unterstützt die folgenden Regionen.

Nord- Und Südamerika

- Iowa
- Los Angeles
- Montreal
- N. Virginia
- Oregon –
- Sao Paulo, Brasilien
- South Carolina

Asien/Pazifik

- Hongkong
- Mumbai
- Osaka
- Singapur
- Sydney
- Taiwan
- Tokio

Europa

- Belgien
- Finnland
- Frankfurt
- London
- Niederlande
- Zürich

Anzeigen Ihrer Amazon S3 Buckets

Nach der Installation eines Connectors in AWS erkennt Cloud Manager automatisch Informationen zu den Amazon S3 Buckets, die sich im AWS Konto befinden und dort installiert sind.

Sie sehen Details zu Ihren S3 Buckets, einschließlich Region, Zugriffsebene, Storage-Klasse und ob der Bucket in Verbindung mit Cloud Volumes ONTAP für Backups oder Daten-Tiering verwendet wird. Zudem haben Sie die Möglichkeit, die S3 Buckets mithilfe von Cloud Compliance zu scannen.

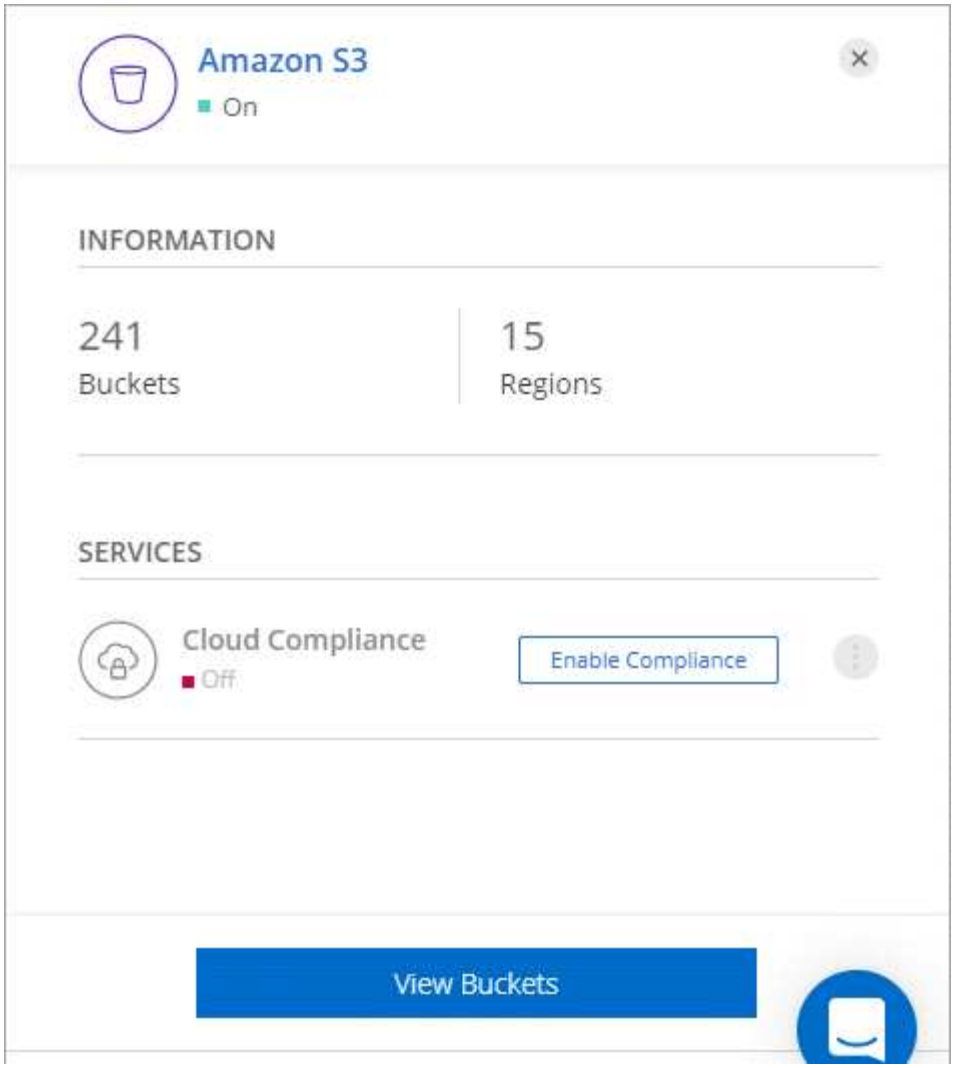
Schritte

1. "Installieren Sie einen Anschluss" In dem AWS Konto, wo Sie Ihre Amazon S3 Buckets anzeigen möchten.

   Sie sollten bald automatisch eine Amazon S3-Arbeitsumgebung sehen.

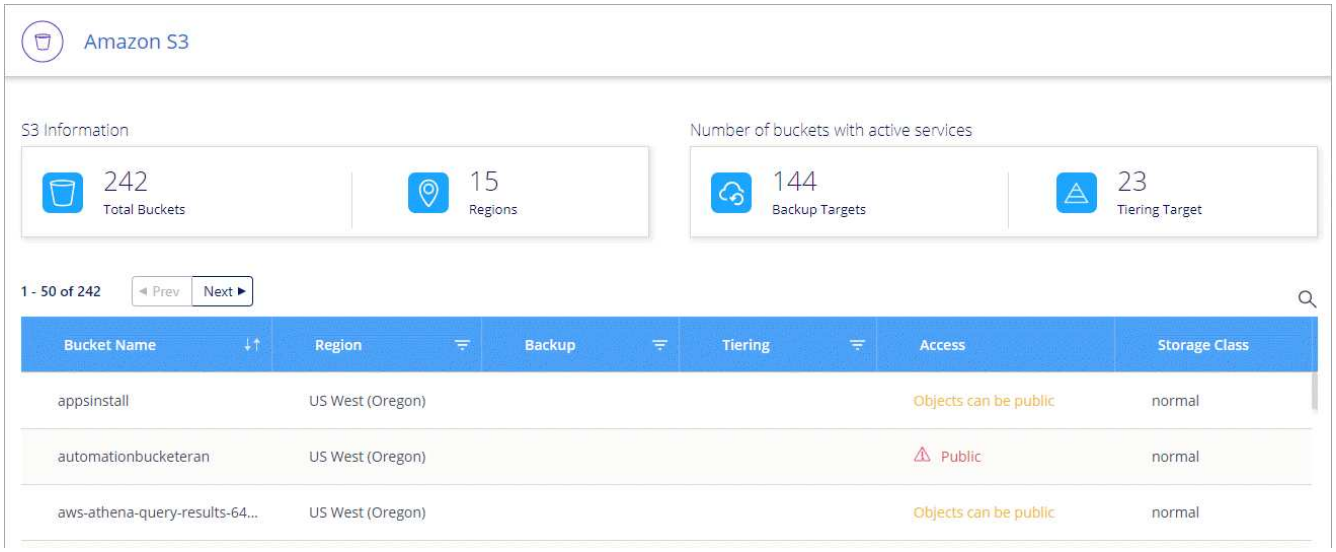
2. Klicken Sie auf die Arbeitsumgebung, und wählen Sie eine Aktion im rechten Fensterbereich aus.



3. Klicken Sie auf **Compliance aktivieren**, um die S3-Buckets nach persönlichen und sensiblen Daten zu scannen.

   Weitere Informationen finden Sie unter "Erste Schritte mit Cloud Compliance für Amazon S3".

4. Klicken Sie auf **Buckets anzeigen**, um Details zu den S3-Buckets in Ihrem AWS-Konto anzuzeigen.



Management Von Cloud Manager

Suchen der System-ID des Cloud Manager

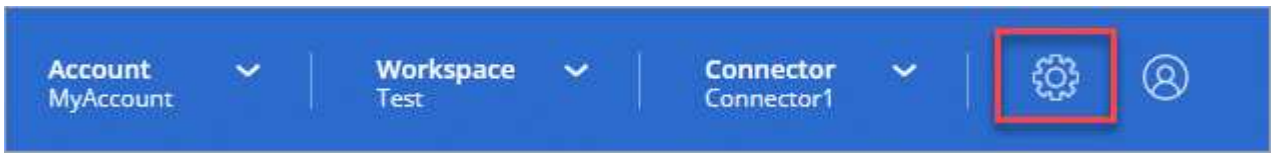
Um Ihnen bei den ersten Schritten zu helfen, wird Sie möglicherweise von Ihrem NetApp Vertriebsmitarbeiter nach Ihrer Cloud Manager System-ID gefragt. Die ID wird in der Regel für Lizenzierungs- und Fehlerbehebungszwecke verwendet.

Was Sie benötigen

Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. "Erfahren Sie, wie".

Schritte

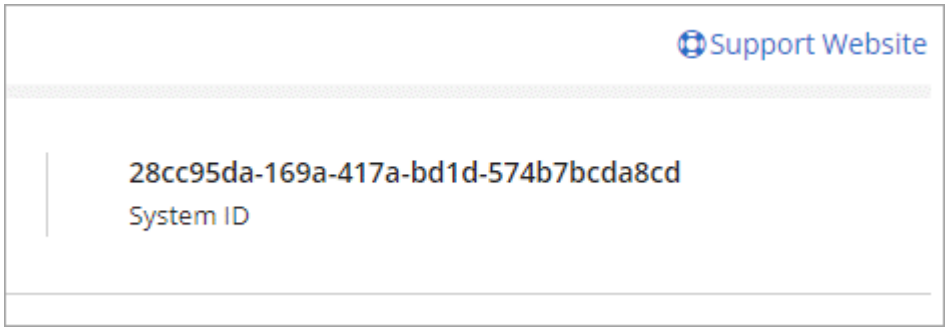
1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen.



2. Klicken Sie Auf **Support Dashboard**.

   Ihre System-ID wird oben rechts angezeigt.

   Beispiel



Anschlüsse Verwalten

Verwalten vorhandener Anschlüsse

Nachdem Sie einen oder mehrere Anschlüsse erstellt haben, können Sie diese verwalten, indem Sie zwischen den Anschlüssen wechseln, eine Verbindung zur lokalen Benutzeroberfläche herstellen, die auf einem Connector ausgeführt wird, und mehr.

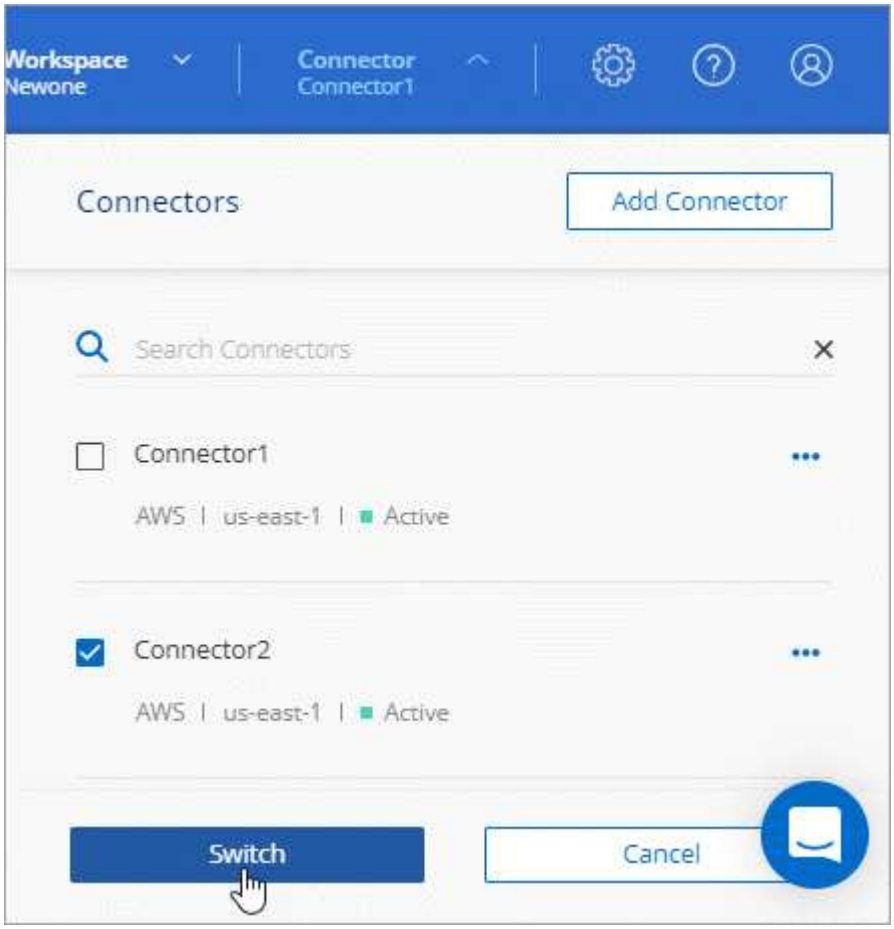
Wechseln zwischen den Anschlüssen

Wenn Sie über mehrere Anschlüsse verfügen, können Sie zwischen diesen wechseln, um die Arbeitsumgebungen zu sehen, die mit einem bestimmten Konnektor verknüpft sind.

Nehmen wir zum Beispiel an, dass Sie in einer Multi-Cloud-Umgebung arbeiten. Möglicherweise verfügen Sie über einen Connector in AWS und einen anderen in Google Cloud. Zum Managen der Cloud Volumes ONTAP Systeme, die in diesen Clouds ausgeführt werden, müsste zwischen diesen Anschlüssen gewechselt werden.

Schritt

1. Klicken Sie auf das Dropdown-Menü **Connector**, wählen Sie einen anderen Anschluss aus und klicken Sie dann auf **Switch**.



Cloud Manager aktualisiert und zeigt die Arbeitsumgebungen an, die mit dem ausgewählten Connector verknüpft sind.

Zugriff auf die lokale Benutzeroberfläche

Während Sie fast alle Aufgaben über die SaaS-Benutzeroberfläche ausführen sollten, steht auf dem Connector weiterhin eine lokale Benutzeroberfläche zur Verfügung. Diese Schnittstelle wird für einige Aufgaben benötigt, die über den Connector selbst ausgeführt werden müssen:

- "Festlegen eines Proxyservers"
- Installation eines Patches (Sie arbeiten in der Regel mit NetApp Mitarbeitern zusammen, um einen Patch zu installieren)
- Herunterladen von AutoSupport-Meldungen (normalerweise gerichtet von NetApp Mitarbeitern, wenn Sie Probleme haben)

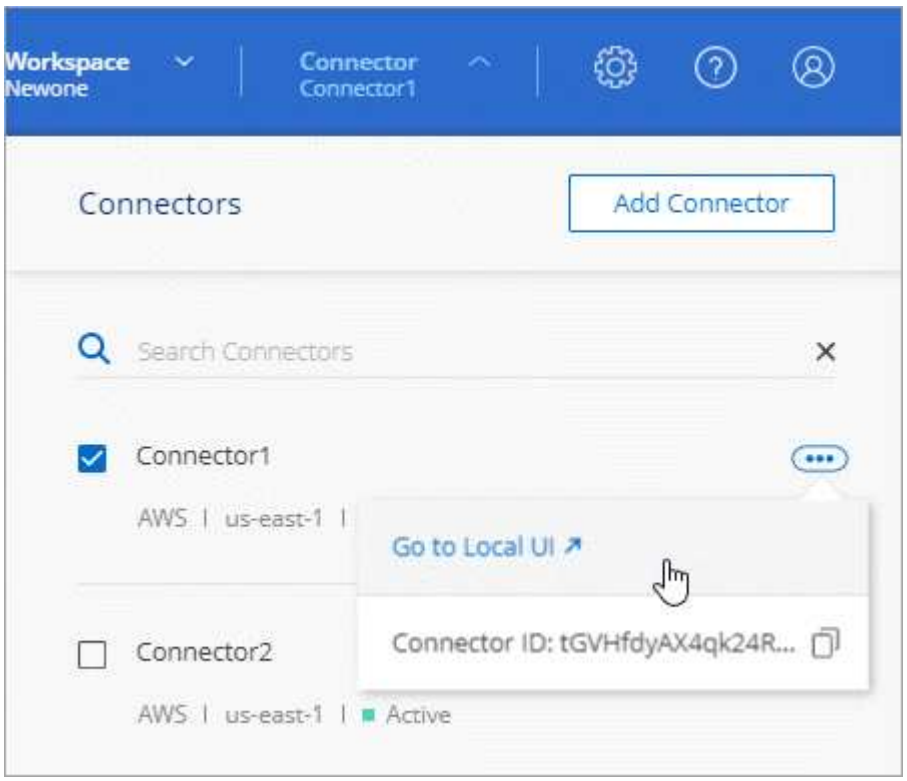
Schritte

1. "Melden Sie sich bei der SaaS-Schnittstelle von Cloud Manager an" Von einem Computer mit einer

Netzwerkverbindung zur Instanz des Connectors.

Wenn der Connector keine öffentliche IP-Adresse hat, benötigen Sie eine VPN-Verbindung oder Sie müssen eine Verbindung von einem Jump-Host herstellen, der sich im gleichen Netzwerk wie der Connector befindet.

2. Klicken Sie auf das Dropdown-Menü **Connector**, klicken Sie auf das Aktionsmenü für einen Connector und dann auf **Gehe zu lokaler Benutzeroberfläche**.



Die Cloud Manager-Schnittstelle, die auf dem Connector ausgeführt wird, wird in einer neuen Browser-Registerkarte geladen.

Entfernen von Anschlüssen aus Cloud Manager

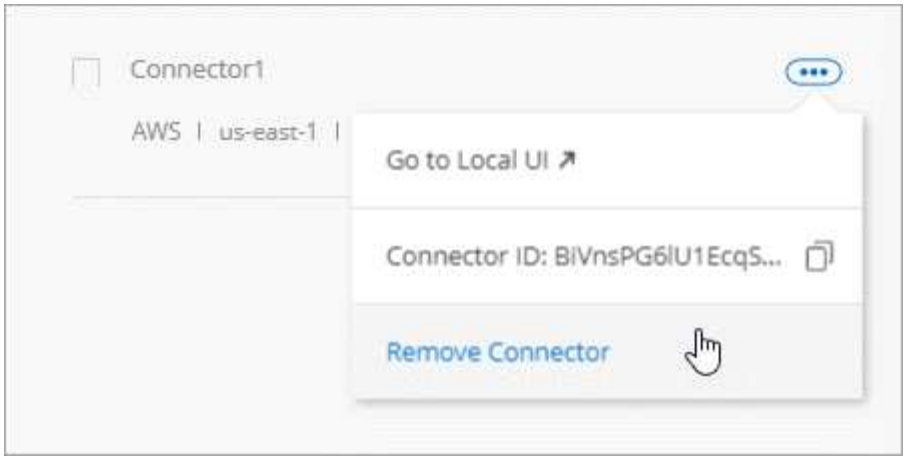
Wenn ein Connector inaktiv ist, können Sie ihn aus der Liste der Anschlüsse in Cloud Manager entfernen. Sie können dies tun, wenn Sie die virtuelle Connector-Maschine gelöscht oder die Connector-Software deinstalliert haben.

Beachten Sie Folgendes zum Entfernen eines Konnektors:

- Durch diese Aktion wird die virtuelle Maschine nicht gelöscht.
- Diese Aktion kann nicht rückgängig gemacht werden: Sobald ein Connector aus Cloud Manager entfernt wurde, kann er nicht wieder zu Cloud Manager hinzugefügt werden.

Schritte

1. Klicken Sie in der Kopfzeile des Cloud Manager auf das Dropdown-Menü Connector.
2. Klicken Sie auf das Aktionsmenü für einen inaktiven Konnektor und klicken Sie auf **Connector entfernen**.



3. Geben Sie den Namen des zu bestätigenden Connectors ein, und klicken Sie anschließend auf Entfernen.

Ergebnis

Cloud Manager entfernt den Connector aus seinen Datensätzen.

Deinstallieren der Connector-Software

Der Connector enthält ein Deinstallationsskript, mit dem Sie die Software deinstallieren können, um Probleme zu beheben oder die Software dauerhaft vom Host zu entfernen.

Schritt

1. Führen Sie auf dem Linux-Host das Deinstallationsskript aus:

   /opt/Application/netapp/cloudmanager/bin/uninstall.sh [Silent]

   Silent führt das Skript aus, ohne dass Sie zur Bestätigung aufgefordert werden.

Wie sieht es mit Software-Upgrades aus?

Der Connector aktualisiert seine Software automatisch auf die neueste Version, solange er hat "Outbound-Internetzugang" Um das Softwareupdate zu erhalten.

Weitere Möglichkeiten zum Erstellen von Anschlüssen

Connector-Host-Anforderungen

Die Connector-Software muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Port-Anforderungen usw. erfüllt.

Ein dedizierter Host ist erforderlich

Der Connector wird nicht auf einem Host unterstützt, der für andere Anwendungen freigegeben ist. Der Host muss ein dedizierter Host sein.

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Instanztyp für AWS EC2

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen t3.xlarge und verwenden diesen Instanztyp, wenn Sie den Connector direkt über Cloud Manager bereitstellen.

Azure VM-Größe

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen DS3 v2 und verwenden die VM-Größe, wenn Sie den Connector direkt aus Cloud Manager implementieren.

GCP-Maschinentyp

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen n1-Standard-4 und verwenden diesen Maschinentyp, wenn Sie den Connector direkt von Cloud Manager bereitstellen.

Unterstützte Betriebssysteme

- CentOS 7.6
- CentOS 7.7
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7

  Das Red Hat Enterprise Linux System muss beim Red Hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann das System während der Connector-Installation nicht auf Repositories zugreifen, um die erforderliche Software von Drittanbietern zu aktualisieren.

  Der Connector wird auf Englisch-sprachigen 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?"^]

Speicherplatz in /opt

100 GB Speicherplatz müssen verfügbar sein

Outbound-Internetzugang

Für die Installation des Connectors und des Connectors ist ein Outbound-Internetzugang erforderlich, um Ressourcen und Prozesse in Ihrer Public-Cloud-Umgebung zu managen. Eine Liste der Endpunkte finden Sie unter "Netzwerkanforderungen für den Connector".

Erstellen eines Connectors über den AWS Marketplace

Es empfiehlt sich, einen Connector direkt aus Cloud Manager zu erstellen, aber Sie können einen Connector aus dem AWS Marketplace starten, wenn Sie keine AWS Zugriffsschlüssel angeben möchten. Nachdem Sie den Connector erstellt und eingerichtet haben, wird er automatisch bei der Erstellung neuer Arbeitsumgebungen verwendet.

Schritte

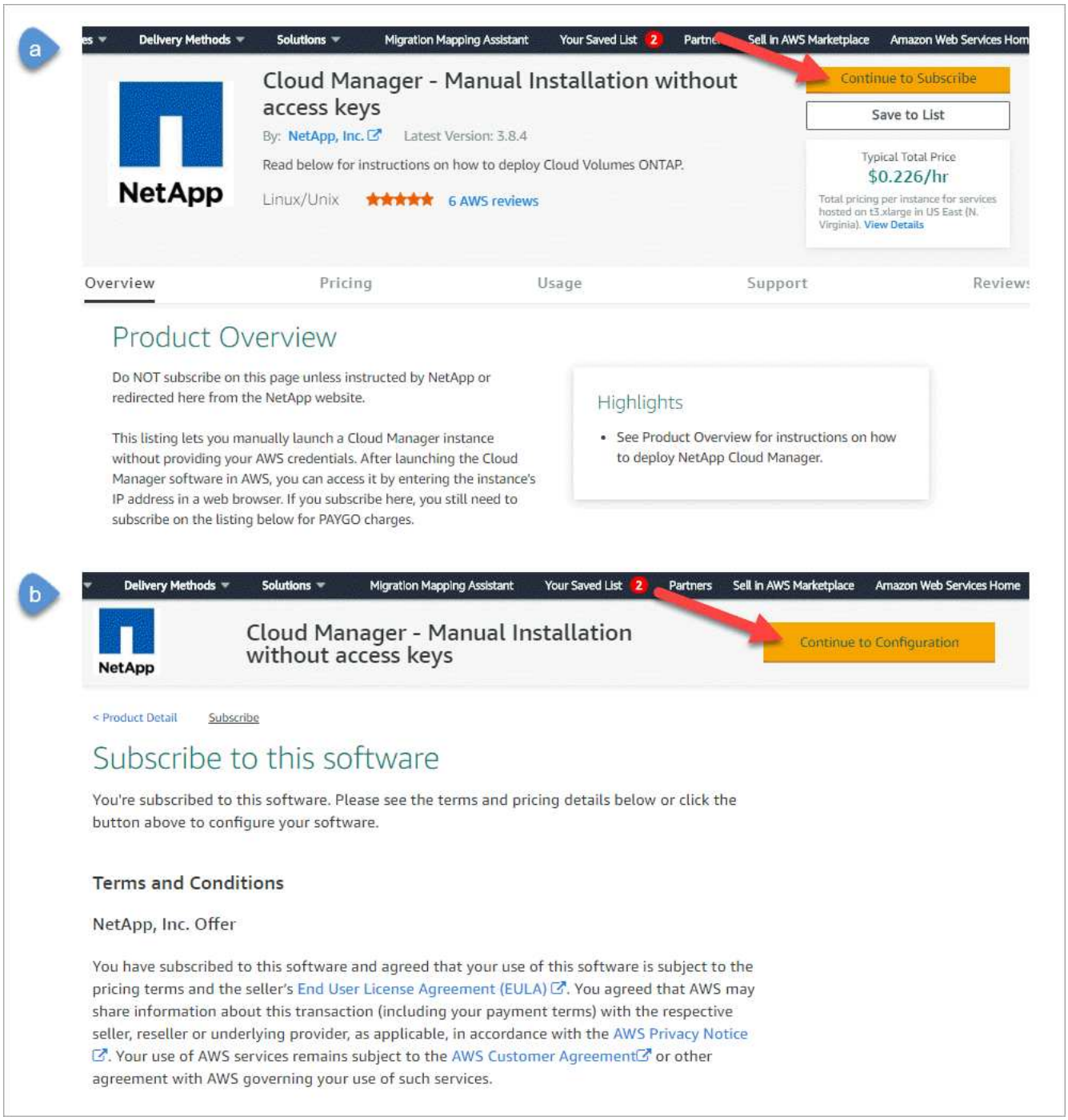
1. IAM-Richtlinie und -Rolle für die EC2-Instanz erstellen:
   a. Laden Sie die Cloud Manager IAM-Richtlinie von folgendem Speicherort herunter:

      "NetApp Cloud Manager: AWS, Azure und GCP-Richtlinien"

   b. Erstellen Sie über die IAM-Konsole Ihre eigene Richtlinie, indem Sie den Text aus der Cloud Manager IAM-Richtlinie kopieren und einfügen.
   c. Erstellen Sie eine IAM-Rolle mit dem Rollentyp Amazon EC2, und hängen Sie die im vorherigen Schritt erstellte Richtlinie an die Rolle an.
2. Gehen Sie jetzt zum "Seite zu Cloud Manager im AWS Marketplace" Um Cloud Manager über eine AMI bereitzustellen.

   Der IAM-Benutzer muss über AWS Marketplace-Berechtigungen zum Abonnieren und Abbestellen verfügen.

3. Klicken Sie auf der Marketplace-Seite auf **Weiter zur Anmeldung** und dann auf **Weiter zur Konfiguration**.



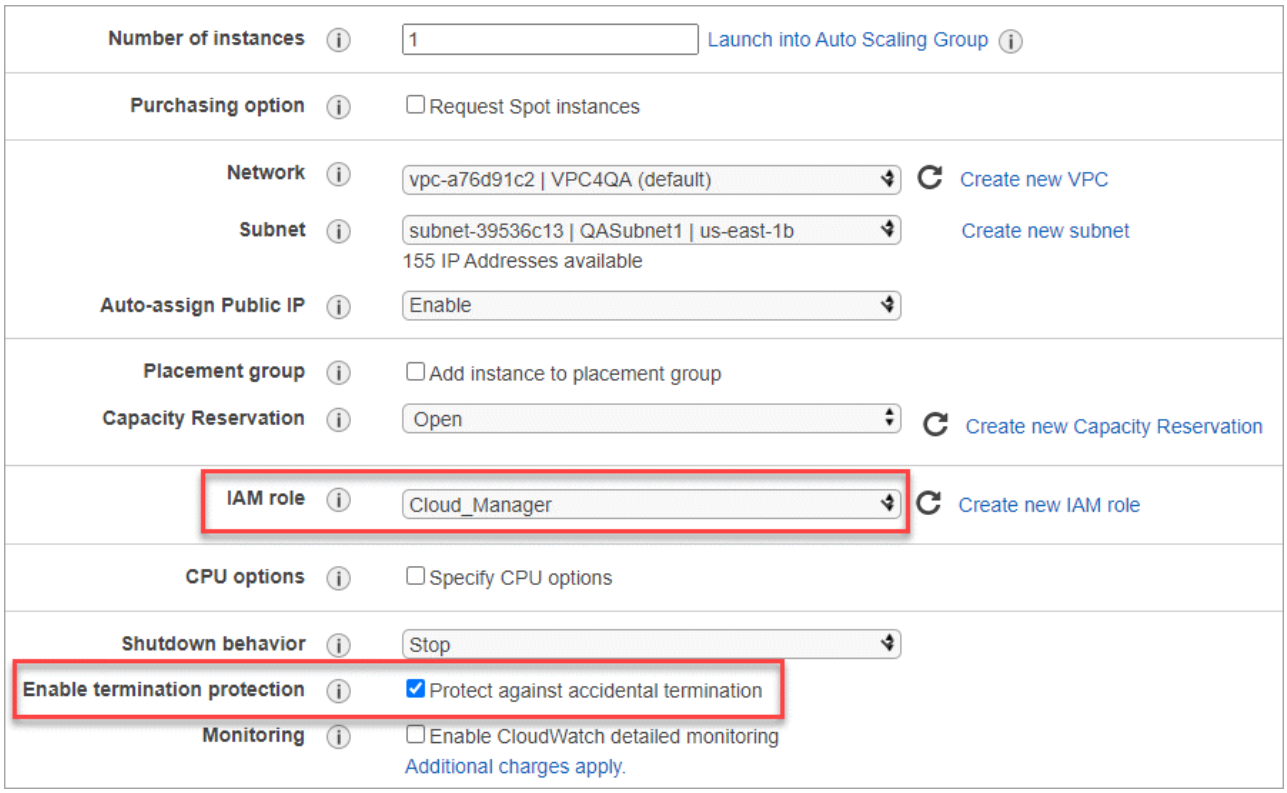
4. Ändern Sie eine der Standardoptionen, und klicken Sie auf **Weiter zum Starten**.
5. Wählen Sie unter **Aktion auswählen über EC2 starten** und klicken Sie dann auf **Start**.

   In diesen Schritten wird beschrieben, wie Sie die Instanz über die EC2-Konsole starten, da Sie über die Konsole eine IAM-Rolle an die Cloud Manager-Instanz anhängen können. Dies ist mit der Aktion * von Website starten* nicht möglich.

6. Befolgen Sie die Anweisungen zur Konfiguration und Bereitstellung der Instanz:
   - **Wählen Sie Instanztyp**: Wählen Sie je nach Verfügbarkeit der Region einen der unterstützten Instanztypen (t3.xlarge wird empfohlen).

     "Prüfen Sie die Anforderungen an die Instanz".

- **Instanz konfigurieren**: Wählen Sie eine VPC und ein Subnetz aus, wählen Sie die IAM-Rolle aus, die Sie in Schritt 1 erstellt haben, aktivieren Sie den Terminierungsschutz (empfohlen) und wählen Sie andere Konfigurationsoptionen aus, die Ihren Anforderungen entsprechen.



- **Speicher hinzufügen**: Behalten Sie die Standard-Speicheroptionen.
- **Tags hinzufügen**: Geben Sie bei Bedarf Tags für die Instanz ein.
- **Sicherheitsgruppe konfigurieren**: Geben Sie die erforderlichen Verbindungsmethoden für die Connector-Instanz an: SSH, HTTP und HTTPS.
- **Review**: Überprüfen Sie Ihre Auswahl und klicken Sie auf **Start**.

  AWS startet die Software mit den angegebenen Einstellungen. Die Connector-Instanz und -Software sollten in etwa fünf Minuten ausgeführt werden.

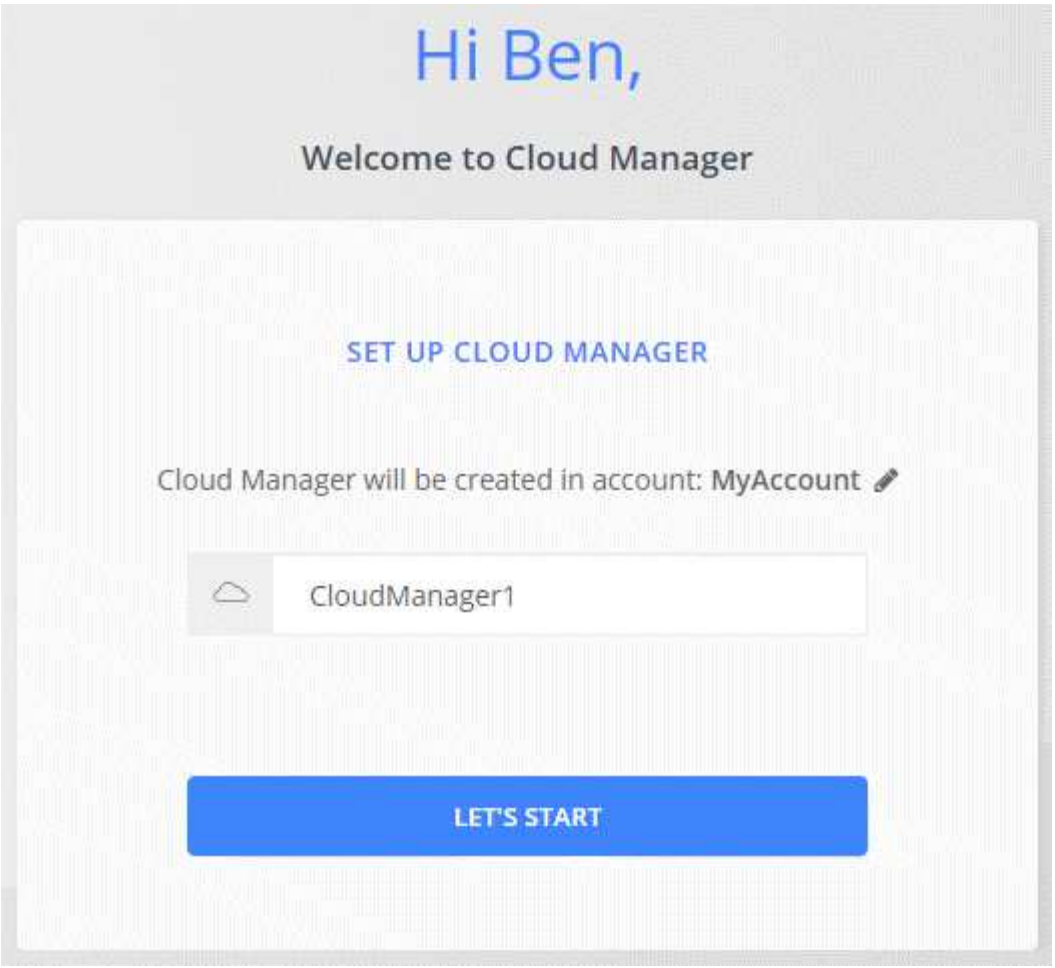
7. Öffnen Sie einen Webbrowser von einem Host, der eine Verbindung zur Verbindungsinstanz hat, und geben Sie die folgende URL ein:

   http://ipaddress:80

8. Richten Sie nach der Anmeldung den Konnektor ein:
   a. Geben Sie das Cloud Central-Konto an, das mit dem Connector verknüpft werden soll.

      "Weitere Informationen zu Cloud Central Accounts".

   b. Geben Sie einen Namen für das System ein.



Ergebnis

Der Connector ist jetzt mit Ihrem Cloud Central-Konto installiert und eingerichtet. Cloud Manager nutzt diesen Connector automatisch bei der Erstellung neuer Arbeitsumgebungen. Aber wenn Sie mehr als einen Connector haben, müssen Sie dies tun "Wechseln Sie zwischen ihnen".

Erstellen eines Connectors über den Azure Marketplace

Am besten sollte ein Connector direkt aus Cloud Manager erstellt werden, aber Sie können einen Connector auf Wunsch im Azure Marketplace starten. Nachdem Sie den Connector erstellt und eingerichtet haben, wird er automatisch bei der Erstellung neuer Arbeitsumgebungen verwendet.

Erstellen eines Connectors in Azure

Implementieren Sie den Connector in Azure mithilfe des Images im Azure Marketplace. Melden Sie sich dann bei Connector an, um Ihr Cloud Central Konto anzugeben.

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 VM-Größe aus, die den CPU- und RAM-Anforderungen entspricht. Wir empfehlen DS3 v2.

  "VM-Anforderungen prüfen".

- Für die Netzwerksicherheitsgruppe benötigt der Connector eingehende Verbindungen unter Verwendung von SSH, HTTP und HTTPS.

  "Erfahren Sie mehr über die Regeln für Sicherheitsgruppen für den Connector".

- Aktivieren Sie unter **Management** * * die vom System zugewiesene verwaltete Identität* für den Connector, indem Sie **ein** wählen.

  Diese Einstellung ist wichtig, da sich die Virtual Machine Connector mit Azure Active Directory identifizieren kann, ohne dass Anmeldedaten vorhanden sind. "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 Connector-Software sollten in etwa fünf Minuten ausgeführt werden.

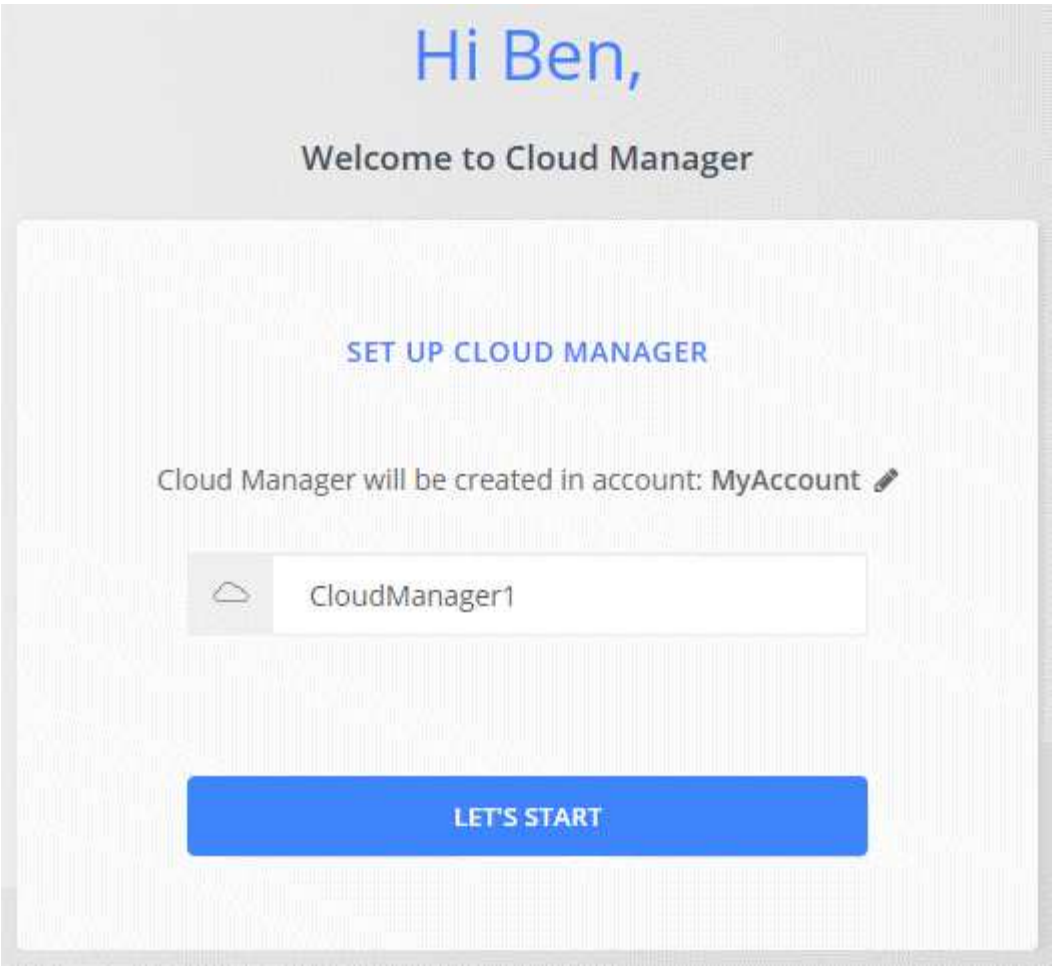
5. Öffnen Sie einen Webbrowser von einem Host, der eine Verbindung mit der virtuellen Verbindungsmaschine hat, und geben Sie die folgende URL ein:

   http://ipaddress:80

6. Richten Sie nach der Anmeldung den Konnektor ein:
   a. Geben Sie das Cloud Central-Konto an, das mit dem Connector verknüpft werden soll.

      "Weitere Informationen zu Cloud Central Accounts".

   b. Geben Sie einen Namen für das System ein.



Ergebnis

Der Connector ist jetzt installiert und eingerichtet. Sie müssen Azure Berechtigungen erteilen, bevor Benutzer Cloud Volumes ONTAP in Azure bereitstellen können.

Azure-Berechtigungen werden gewährt

Bei der Implementierung des Connectors in Azure sollten Sie a aktiviert haben "Vom System zugewiesene verwaltete Identität". Sie müssen nun die erforderlichen Azure-Berechtigungen erteilen, indem Sie eine benutzerdefinierte Rolle erstellen und dann die Rolle der virtuellen Connector-Maschine für ein oder mehrere Abonnements zuweisen.

Schritte

1. Erstellen Sie eine benutzerdefinierte Rolle mithilfe der Cloud Manager-Richtlinie:

   a. Laden Sie die herunter "Cloud Manager Azure-Richtlinie".

   b. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

      Sie sollten die ID für jedes Azure Abonnement hinzufügen, aus dem Benutzer Cloud Volumes ONTAP Systeme erstellen.

      Beispiel

      "AssignableScopes": ["/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzzzzzzzz", "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzzzz", "/subscriptions/398e471c-3b42-4zzae7-

9b59-zzz"

c. Verwenden Sie die JSON-Datei, um eine benutzerdefinierte Rolle in Azure zu erstellen.

   Im folgenden Beispiel wird gezeigt, wie eine benutzerdefinierte Rolle mithilfe der Azure CLI 2.0 erstellt wird:

   ```
   az role definition create --role-definition
   C:\Policy_for_cloud_Manager_Azure_3.8.7.json
   ```

Sie sollten nun eine benutzerdefinierte Rolle namens Cloud Manager Operator haben, die Sie der virtuellen Connector-Maschine zuweisen können.

2. Weisen Sie der virtuellen Verbindungsmaschine die Rolle für eine 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 **Cloud Manager Operator** aus.

        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 Connector-Maschine erstellt wurde.
      - Wählen Sie die virtuelle Verbindungsmaschine 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

Der Connector verfügt nun über die Berechtigungen, die die IT für das Management von Ressourcen und Prozessen in Ihrer Public Cloud-Umgebung benötigt. Cloud Manager nutzt diesen Connector automatisch bei der Erstellung neuer Arbeitsumgebungen. Aber wenn Sie mehr als einen Connector haben, müssen Sie dies tun "Wechseln Sie zwischen ihnen".

Installieren der Connector-Software auf einem vorhandenen Linux-Host

Die geläufigste Methode zur Erstellung eines Connectors besteht direkt über Cloud Manager oder über den Markt eines Cloud-Providers. Sie haben jedoch die Möglichkeit, die Connector-Software auf einem bestehenden Linux-Host in Ihrem Netzwerk oder in der Cloud herunterzuladen und zu installieren.

Wenn Sie ein Cloud Volumes ONTAP-System in Google Cloud erstellen möchten, dann müssen Sie einen Connector in Google Cloud laufen, sowie. Sie können keinen Konnektor verwenden, der an einem anderen Standort ausgeführt wird.

Anforderungen

- Der Host muss sich erfüllen "Anforderungen an den Steckverbinder".
- Ein Red Hat Enterprise Linux-System muss bei Red Hat Subscription Management registriert sein. Wenn sie nicht registriert ist, kann das System während der Installation nicht auf Repositorys zugreifen, um die erforderliche Software von Drittanbietern zu aktualisieren.
- Das Connector-Installationsprogramm greift während der Installation auf mehrere URLs zu. Sie müssen sicherstellen, dass für folgende Endpunkte der ausgehende Internetzugang zugelassen ist:
  - 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

    Der Host versucht möglicherweise, während der Installation Betriebssystempakete zu aktualisieren. Der Host kann verschiedene Spiegelungsstandorte für diese Betriebssystempakete kontaktieren.

Über diese Aufgabe

- Root-Berechtigungen sind zur Installation des Connectors nicht erforderlich.
- Die Installation installiert die AWS Befehlszeilen-Tools (awscli), um Recovery-Verfahren durch den NetApp Support zu ermöglichen.

  Wenn Sie eine Meldung erhalten, dass die Installation des awscli fehlgeschlagen ist, können Sie die Meldung ignorieren. Der Steckverbinder kann ohne Werkzeuge erfolgreich betrieben werden.
- Das Installationsprogramm, das auf der NetApp Support-Website verfügbar ist, kann möglicherweise eine frühere Version sein. Nach der Installation aktualisiert sich der Connector automatisch, wenn eine neue Version verfügbar ist.

Schritte

1. Laden Sie die Software von Cloud Manager 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".

2. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

   Beispiel

   ```
    chmod +x OnCommandCloudManager-V3.8.4.sh
   . Führen Sie das Installationsskript aus:
   ```

   ```
   ./OnCommandCloudManager-V3.8.4.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 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.

3. 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.

   Cloud Manager ist jetzt installiert. Nach Abschluss der Installation wird der Cloud Manager-Dienst (occm) zweimal neu gestartet, wenn Sie einen Proxyserver angegeben haben.

4. Öffnen Sie einen Webbrowser, und geben Sie die folgende URL ein:

   https://ipaddress:port

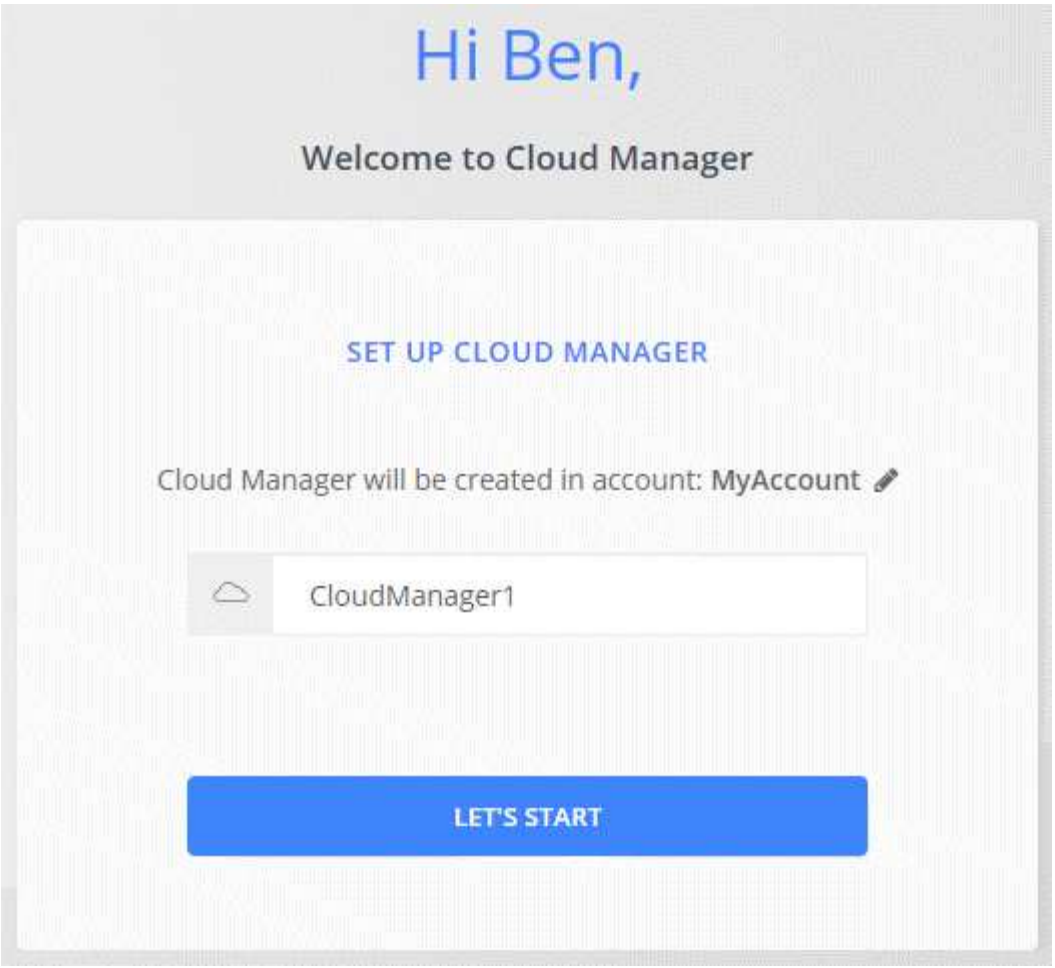
   Ipaddress kann abhängig von der Konfiguration des Hosts localhost, eine private IP-Adresse oder eine öffentliche IP-Adresse sein. Wenn sich der Connector beispielsweise ohne öffentliche IP-Adresse in der Public Cloud befindet, müssen Sie eine private IP-Adresse von einem Host eingeben, der eine Verbindung zum Connector-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

5. Melden Sie sich bei NetApp Cloud Central an oder melden Sie sich an.
6. Richten Sie Cloud Manager nach dem Einloggen ein:
   a. Geben Sie das Cloud Central-Konto an, das mit dem Connector verknüpft werden soll.

      "Weitere Informationen zu Cloud Central Accounts".

   b. Geben Sie einen Namen für das System ein.



Ergebnis

Der Connector ist jetzt mit Ihrem Cloud Central-Konto installiert und eingerichtet. Cloud Manager nutzt diesen Connector automatisch bei der Erstellung neuer Arbeitsumgebungen.

Nachdem Sie fertig sind

Einrichtung von Berechtigungen, damit Cloud Manager Ressourcen und Prozesse in Ihrer Public-Cloud-Umgebung managen kann:

- AWS, "AWS Konto einrichten und dann zu Cloud Manager hinzufügen".
- Azure: "Richten Sie ein Azure-Konto ein, und fügen Sie es anschließend zu Cloud Manager hinzu".
- GCP: Richten Sie ein Service-Konto ein, das über die Berechtigungen verfügt, die Cloud Manager für die Erstellung und das Management von Cloud Volumes ONTAP-Systemen in Projekten benötigt.
  a. "Rolle in GCP anlegen" Dazu gehören die im definierten Berechtigungen "Cloud Manager-Richtlinie für GCP".
  b. "Erstellen Sie ein GCP-Service-Konto und wenden Sie die benutzerdefinierte Rolle an, die Sie gerade erstellt haben".
  c. "Verknüpfen Sie dieses Servicekonto mit der Connector-VM".
  d. Wenn Sie Cloud Volumes ONTAP in anderen Projekten implementieren möchten, "Sie gewähren Zugriff, indem Sie dem Projekt das Service-Konto mit der Rolle Cloud Manager hinzufügen". Sie müssen diesen Schritt für jedes Projekt wiederholen.

Standardkonfiguration für den Konnektor

Wenn Sie eine Fehlerbehebung für den Konnektor benötigen, können Sie die Konfiguration des Connectors unter Umständen besser verstehen.

- Bei der Implementierung des Connectors über Cloud Manager (oder direkt über den Marketplace eines Cloud-Providers) ist Folgendes zu beachten:
  - In AWS lautet der Benutzername für die EC2 Linux-Instanz ec2-user.
  - Das Betriebssystem für das Image lautet wie folgt:
    - AWS: Red hat Enterprise Linux 7.5 (HVM)
    - Azure: Red hat Enterprise Linux 7.6 (HVM)
    - GCP: CentOS 7.6

      Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.
- Der Installationsordner des Connectors befindet sich an folgender Stelle:

  /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
  - Docker
  - Java
  - Kubectl
  - MySQL
  - Tridentctl
  - Ziehen
  - Wget
- Der Connector verwendet die folgenden Ports auf dem Linux-Host:
  - 80 für HTTP-Zugriff
  - 443 für HTTPS-Zugriff
  - 3306 für die Cloud Manager-Datenbank
  - 8080 für den Cloud Manager-API-Proxy
  - 8666 für die Service Manager API

- 8777 für die Health-Checker Container Service API

Anmeldeinformationen verwalten

AWS

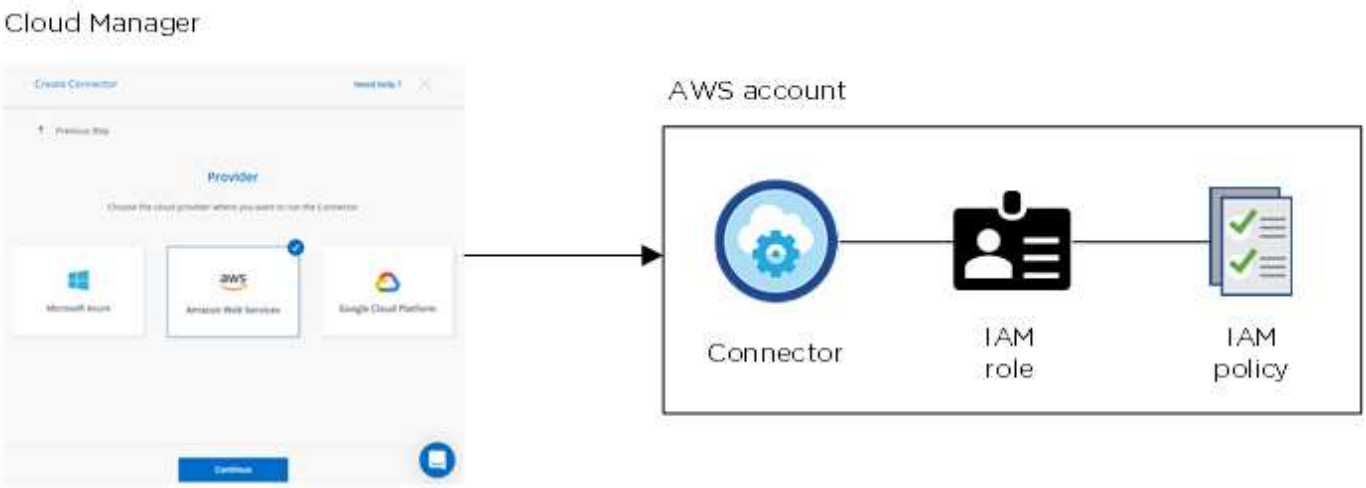
AWS Zugangsdaten und Berechtigungen

Mit Cloud Manager können Sie die AWS Zugangsdaten auswählen, die Sie bei der Implementierung von Cloud Volumes ONTAP verwenden möchten. Alle Cloud Volumes ONTAP Systeme können über die ersten AWS Zugangsdaten implementiert oder zusätzliche Anmeldedaten hinzugefügt werden.

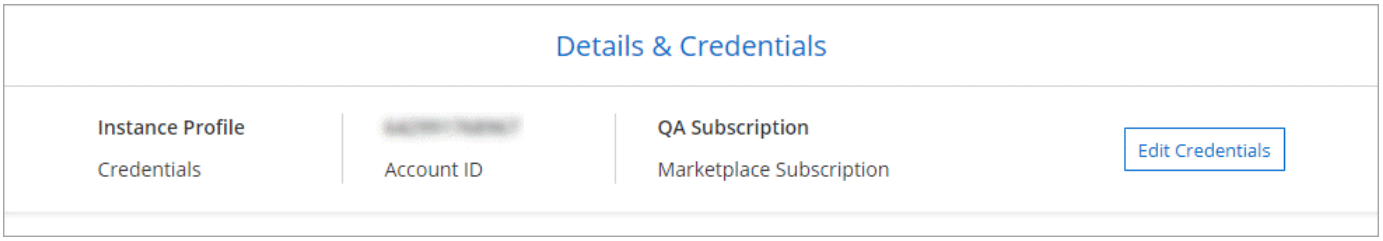
Erste AWS Zugangsdaten

Wenn Sie einen Connector von Cloud Manager bereitstellen, müssen Sie ein AWS-Konto mit Berechtigungen zum Starten der Connector-Instanz verwenden. Die erforderlichen Berechtigungen werden im aufgeführt "Connector-Implementierungsrichtlinie für AWS".

Wenn Cloud Manager die Connector-Instanz in AWS startet, erstellt sie eine IAM-Rolle und ein Instanzprofil für die Instanz. Zudem wird eine Richtlinie angehängt, die Cloud Manager Berechtigungen für das Management von Ressourcen und Prozessen innerhalb dieses AWS-Kontos bietet. "Überprüfen Sie, wie Cloud Manager die Berechtigungen verwendet".

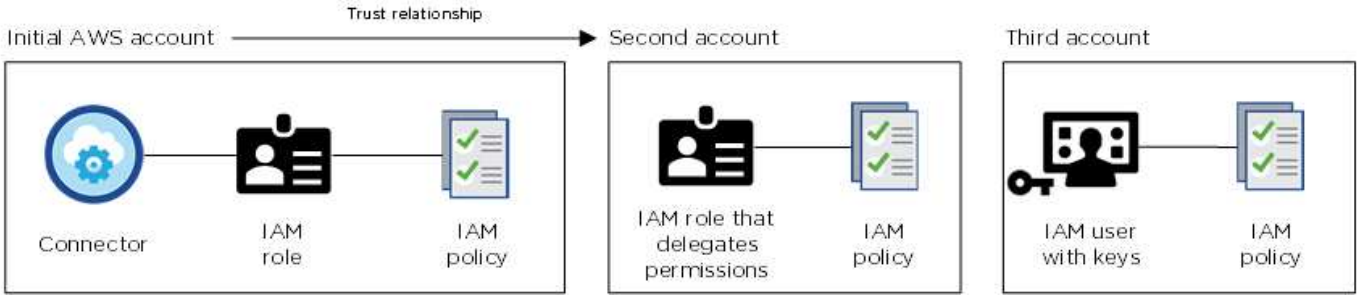


Cloud Manager wählt die AWS Zugangsdaten standardmäßig aus, wenn Sie eine neue Arbeitsumgebung für Cloud Volumes ONTAP erstellen:



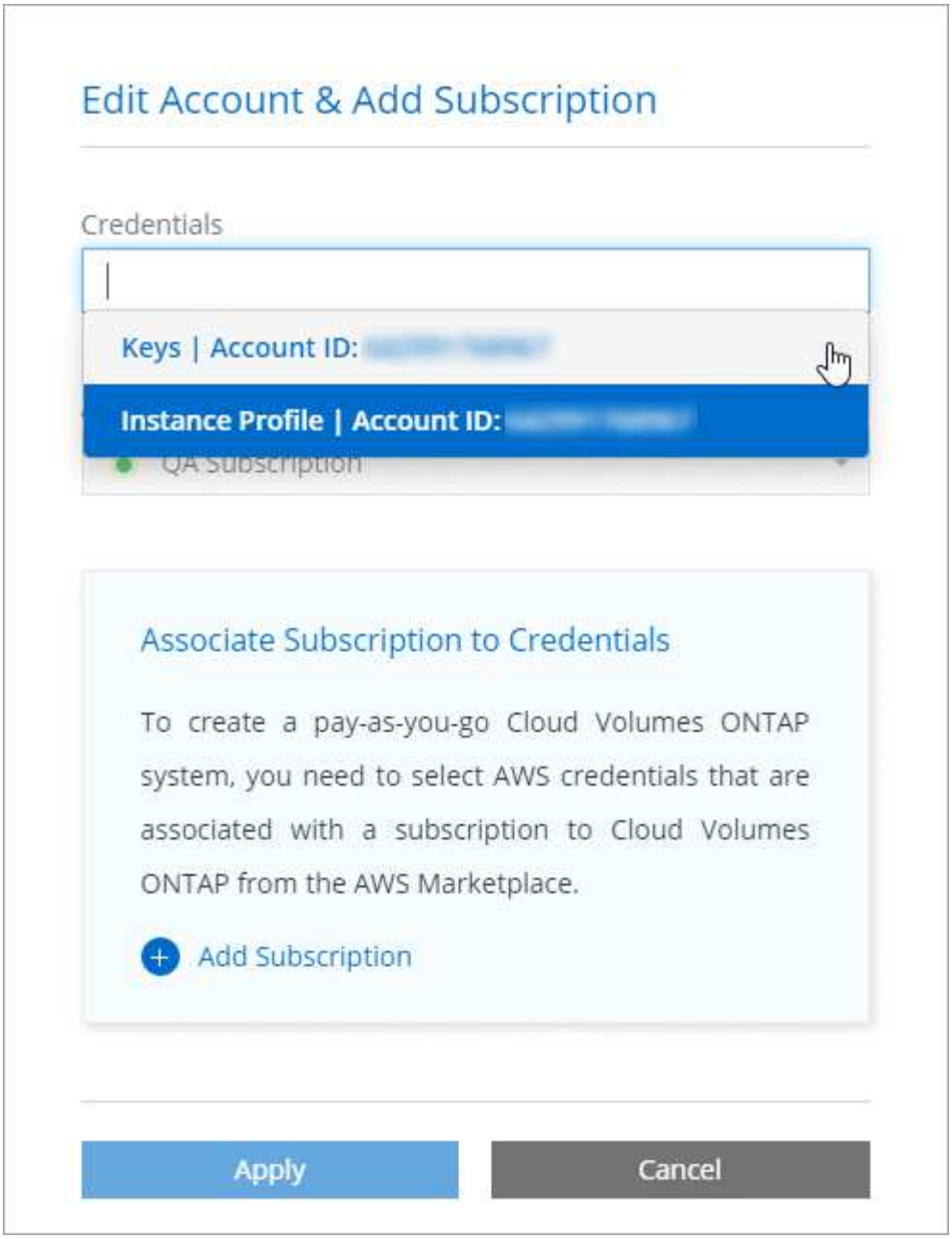
Zusätzliche AWS Zugangsdaten

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 Kontoanmeldeinformationen 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 einen weiteren Satz von Anmeldeinformationen hinzugefügt haben, können Sie zu ihnen 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 für den Connector, der aus Cloud Manager stammt, beschrieben. Sie können auch einen Connector in AWS von der bereitstellen "AWS Marketplace" Und das können Sie auch "Installieren Sie den Steckverbinder vor Ort".

Wenn Sie den Marktplatz nutzen, werden Berechtigungen auf die gleiche Weise bereitgestellt. Sie müssen lediglich die IAM-Rolle manuell erstellen und einrichten und dann Berechtigungen für weitere Konten bereitstellen.

Bei On-Premises-Implementierungen können nicht eine IAM-Rolle für das Cloud Manager-System eingerichtet werden, Sie können aber Berechtigungen wie bei zusätzlichen AWS-Konten bereitstellen.

Wie kann ich meine AWS Zugangsdaten sicher drehen?

Wie oben beschrieben, können Sie mit Cloud Manager AWS Zugangsdaten auf verschiedene Arten

bereitstellen: Eine mit der Connector-Instanz verknüpfte IAM-Rolle, eine IAM-Rolle in einem vertrauenswürdigen Konto oder AWS-Zugriffsschlüssel.

Bei den ersten beiden Optionen verwendet Cloud Manager den AWS Security Token Service, um temporäre Anmeldedaten zu erhalten, die sich ständig drehen. Dies ist die Best Practice, also automatisch und sicher.

Wenn Sie Cloud Manager mit AWS-Zugriffsschlüsseln bereitstellen, sollten Sie die Schlüssel drehen, indem Sie sie in Cloud Manager in einem regelmäßigen Intervall aktualisieren. Es handelt sich hierbei um einen vollständig manuellen Prozess.

Verwalten von AWS Anmeldedaten und Abonnements für Cloud Manager

Wenn Sie ein Cloud Volumes ONTAP System erstellen, müssen Sie die AWS Zugangsdaten und das Abonnement auswählen, die mit diesem System verwendet werden sollen. Wenn Sie mehrere AWS-Abonnements verwalten, können Sie jedes davon auf der Seite „Anmeldeinformationen“ verschiedenen AWS Zugangsdaten zuweisen.

Bevor Sie Cloud Manager mit AWS Zugangsdaten ergänzen, müssen Sie die erforderlichen Berechtigungen für dieses Konto bereitstellen. Mit den Berechtigungen kann Cloud Manager Ressourcen und Prozesse innerhalb dieses AWS Kontos verwalten. Wie Sie die Berechtigungen bereitstellen, hängt davon ab, ob Sie Cloud Manager mit AWS Schlüsseln oder dem ARN einer Rolle in einem vertrauenswürdigen Konto bereitstellen möchten.

Bei der Bereitstellung eines Connectors von Cloud Manager fügte Cloud Manager automatisch AWS Zugangsdaten für das Konto hinzu, in dem Sie den Connector implementiert haben. Dieses erste Konto wird nicht hinzugefügt, wenn Sie die Connector-Software manuell auf einem vorhandenen System installiert haben. "Weitere Informationen zu AWS Zugangsdaten und Berechtigungen".

Auswahl

- Erteilen von Berechtigungen durch die Bereitstellung von AWS Schlüsseln
- Gewährung von Berechtigungen durch Annahme von IAM-Rollen in anderen Konten

Wie kann ich meine AWS Zugangsdaten sicher drehen?

Mit Cloud Manager können Sie AWS Zugangsdaten auf verschiedene Arten bereitstellen: Eine mit der Connector-Instanz verknüpfte IAM-Rolle, eine IAM-Rolle in einem vertrauenswürdigen Konto oder die Bereitstellung von AWS Zugriffsschlüssel. "Weitere Informationen zu AWS Zugangsdaten und Berechtigungen".

Bei den ersten beiden Optionen verwendet Cloud Manager den AWS Security Token Service, um temporäre Anmeldedaten zu erhalten, die sich ständig drehen. Dieser Prozess gilt als Best Practice, also automatisch und sicher.

Wenn Sie Cloud Manager mit AWS-Zugriffsschlüsseln bereitstellen, sollten Sie die Schlüssel drehen, indem Sie sie in Cloud Manager in einem regelmäßigen Intervall aktualisieren. Es handelt sich hierbei um einen vollständig manuellen Prozess.

Erteilen von Berechtigungen durch die Bereitstellung von AWS Schlüsseln

Wenn Sie Cloud Manager mit AWS Schlüsseln für einen IAM-Benutzer bereitstellen möchten, müssen Sie diesem Benutzer die erforderlichen Berechtigungen erteilen. Die Cloud Manager IAM-Richtlinie definiert die AWS-Aktionen und -Ressourcen, die Cloud Manager verwenden darf.

Schritte

1. Laden Sie die IAM-Richtlinie von Cloud Manager aus herunter "Seite „Cloud Manager Policies“ aufgeführt".
2. Erstellen Sie über die IAM-Konsole Ihre eigene Richtlinie, indem Sie den Text aus der Cloud Manager IAM-Richtlinie kopieren und einfügen.

   "AWS Dokumentation: Erstellung von IAM-Richtlinien"

3. Hängen Sie die Richtlinie an eine IAM-Rolle oder einen IAM-Benutzer an.
   - "AWS Documentation: Erstellung von IAM-Rollen"
   - "AWS Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"

Ergebnis

Das Konto verfügt nun über die erforderlichen Berechtigungen. Sie können es jetzt zu Cloud Manager hinzufügen.

Gewährung von Berechtigungen durch Annahme von IAM-Rollen in anderen Konten

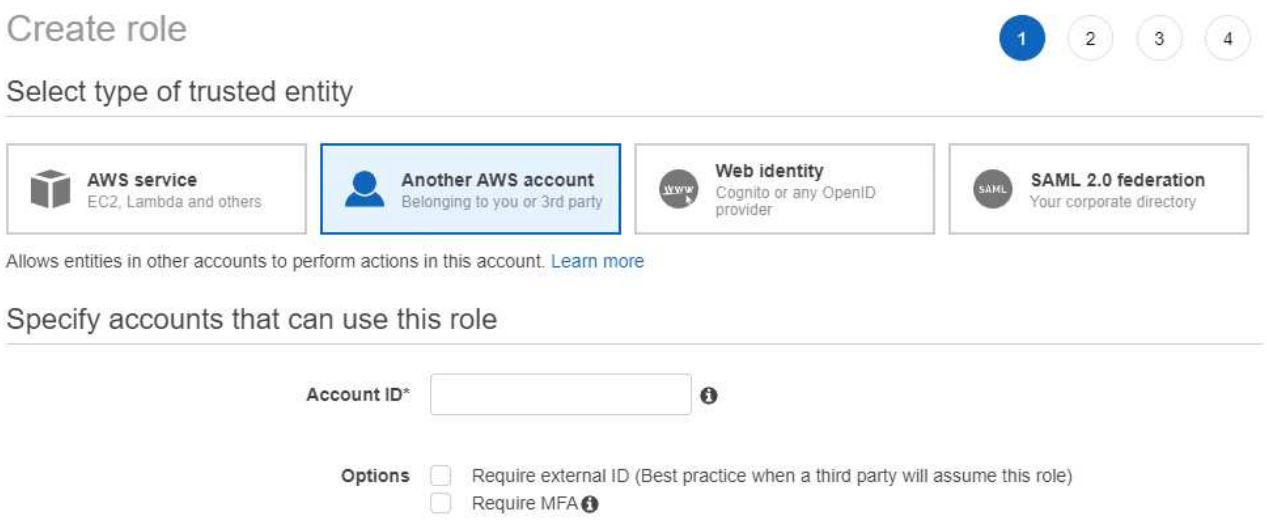
Sie können eine Vertrauensbeziehung zwischen dem Quell-AWS-Konto einrichten, in dem Sie die Connector-Instanz und anderen AWS-Konten mithilfe von IAM-Rollen bereitgestellt haben. Dann würden Sie Cloud Manager über die vertrauenswürdigen Konten mit dem ARN der IAM-Rollen versorgen.

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 Connector-Instanz befindet.
   - Hängen Sie die Cloud Manager IAM-Richtlinie an, die über die erhältlich ist "Seite „Cloud Manager Policies“ aufgeführt".



2. Gehen Sie zum Quellkonto, auf dem sich die Konnektorinstanz befindet, und wählen Sie die IAM-Rolle aus, die an die Instanz angehängt ist.

   a. Klicken Sie auf **Richtlinien anhängen** und dann auf **Richtlinien erstellen**.

   b. Erstellen Sie eine Richtlinie, die die Aktion „STS:AssumeRole“ und den ARN der Rolle umfasst, 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

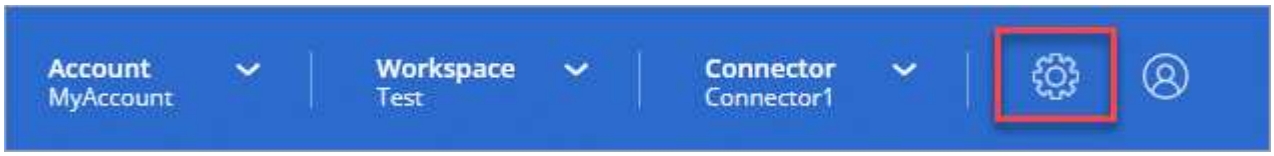
Das Konto verfügt nun über die erforderlichen Berechtigungen. Sie können es jetzt zu Cloud Manager hinzufügen.

AWS Zugangsdaten zu Cloud Manager hinzufügen

Nachdem Sie ein AWS Konto mit den erforderlichen Berechtigungen eingerichtet haben, können Sie die Anmeldedaten für dieses Konto bei Cloud Manager hinzufügen. Damit können Sie Cloud Volumes ONTAP Systeme in diesem Konto starten.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.



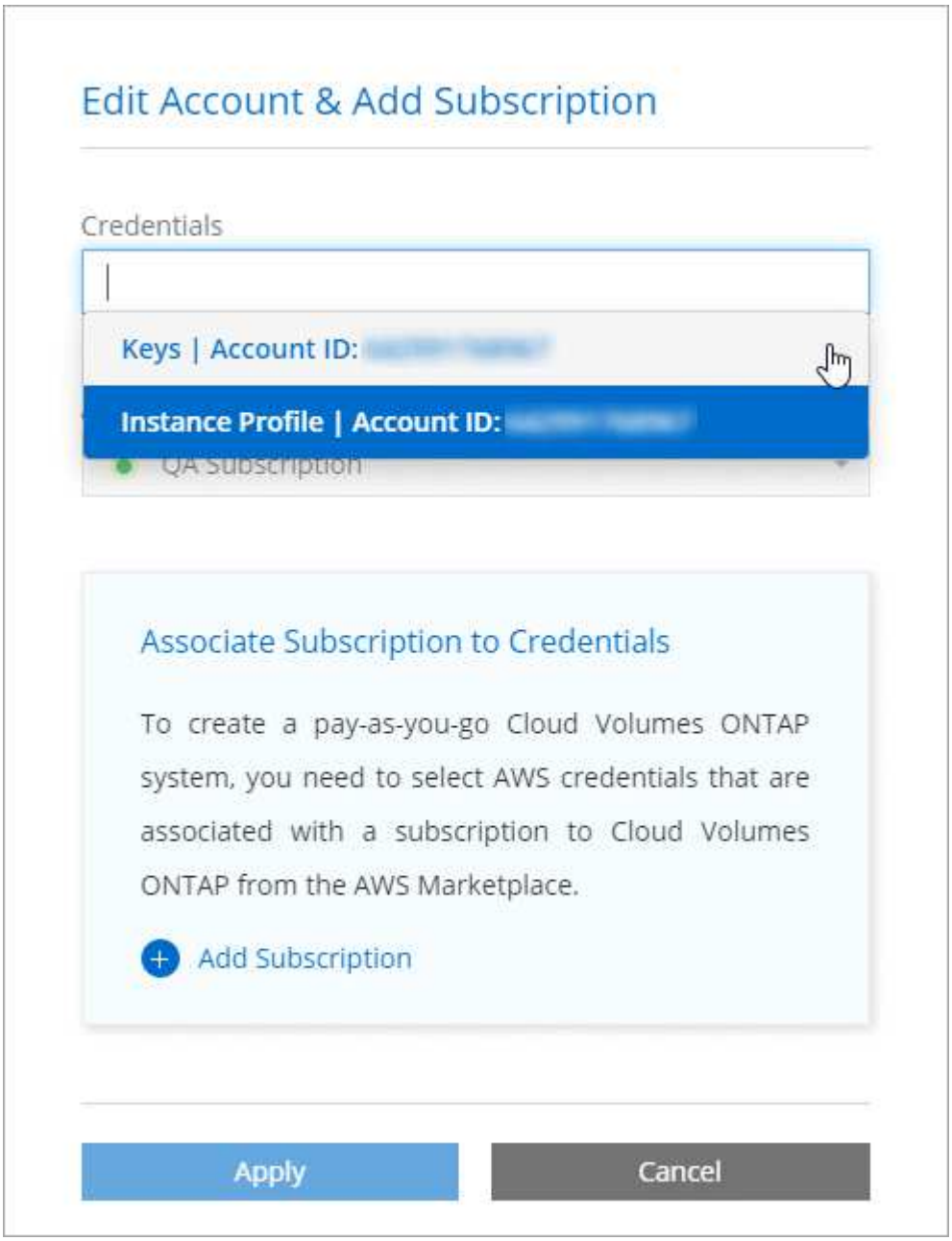
2. Klicken Sie auf **Anmeldedaten hinzufügen** und wählen Sie **AWS**.
3. Bereitstellen von AWS Schlüsseln oder dem ARN einer vertrauenswürdigen IAM-Rolle
4. Bestätigen Sie, dass die Richtlinienanforderungen erfüllt wurden, und klicken Sie auf **Weiter**.
5. Wählen Sie das Pay-as-you-go-Abonnement aus, das Sie mit den Anmeldedaten verknüpfen möchten, oder klicken Sie auf **Abonnement hinzufügen**, wenn Sie noch nicht über ein Abonnement verfügen.

   Um ein Pay-as-you-go Cloud Volumes ONTAP System zu erstellen, müssen AWS Zugangsdaten über den AWS Marketplace mit einem Abonnement für Cloud Volumes ONTAP verknüpft werden.

6. Klicken Sie Auf **Hinzufügen**.

Ergebnis

Sie können jetzt bei der Erstellung einer neuen Arbeitsumgebung auf eine andere Gruppe von Anmeldeinformationen von der Seite Details und Anmeldeinformationen wechseln:



Verknüpfen eines AWS Abonnements mit den Zugangsdaten

Nachdem Sie Ihre AWS Zugangsdaten zu Cloud Manager hinzugefügt haben, können Sie ein AWS Marketplace Abonnement mit diesen Anmeldedaten verknüpfen. Mithilfe des Abonnements können Sie ein nutzungsbasiertes Cloud Volumes ONTAP System erstellen und andere NetApp Cloud-Services nutzen.

Es gibt zwei Szenarien, in denen Sie ein AWS Marketplace-Abonnement verknüpfen können, nachdem Sie bereits die Anmeldedaten zu Cloud Manager hinzugefügt haben:

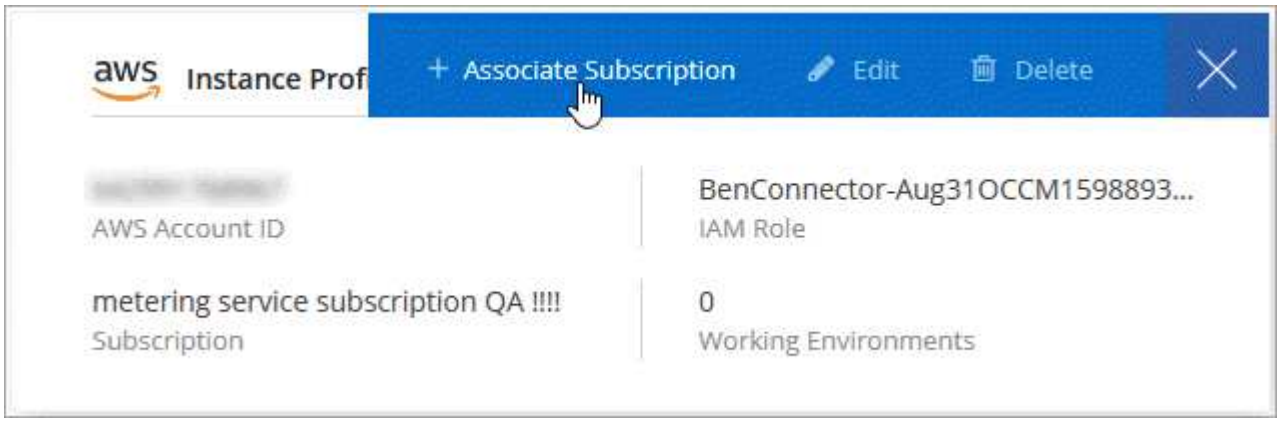
- Sie haben ein Abonnement nicht zugeordnet, wenn Sie zum ersten Mal die Anmeldedaten zu Cloud Manager hinzugefügt haben.
- Sie möchten ein vorhandenes AWS Marketplace Abonnement durch ein neues Abonnement ersetzen.

Was Sie benötigen

Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. "Erfahren Sie, wie".

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Bewegen Sie den Mauszeiger über einen Satz von Anmeldeinformationen, und klicken Sie auf das Aktivitätsmenü.
3. Klicken Sie im Menü auf **Abonnement verknüpfen**.



4. Wählen Sie ein Abonnement aus der Down-Liste aus, oder klicken Sie auf **Abonnement hinzufügen** und befolgen Sie die Schritte, um ein neues Abonnement zu erstellen.

   ► https://docs.netapp.com/de-de/occm38//media/video_subscribing_aws.mp4 *(video)*

Azure

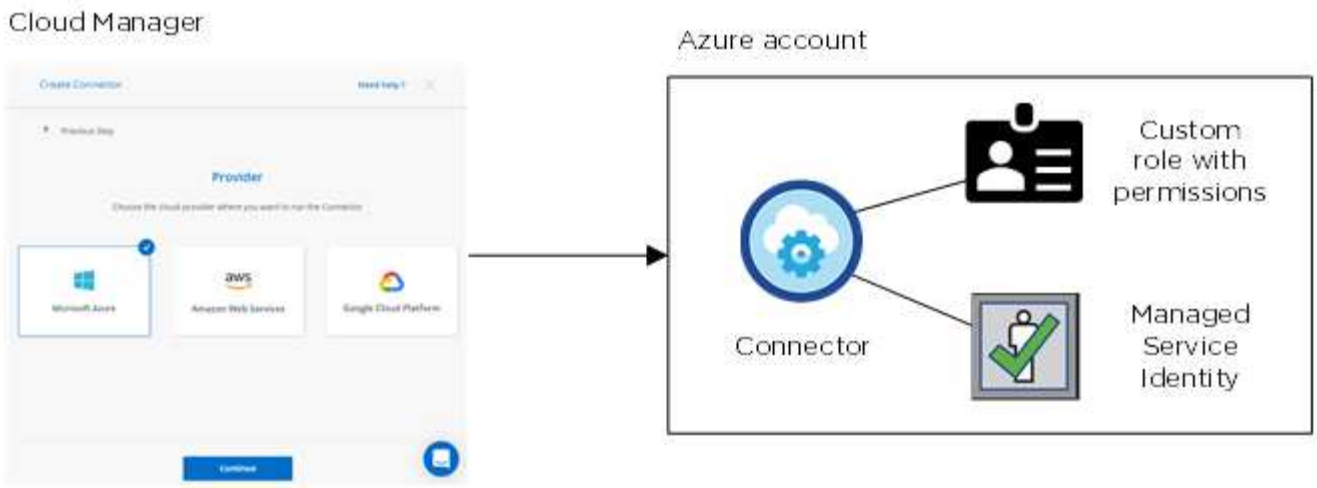
Azure Zugangsdaten und Berechtigungen

Mit Cloud Manager können Sie die Azure Zugangsdaten auswählen, die Sie bei der Implementierung von Cloud Volumes ONTAP verwenden möchten. Alle Cloud Volumes ONTAP Systeme können über die ersten Azure Zugangsdaten implementiert oder zusätzliche Anmeldedaten hinzugefügt werden.

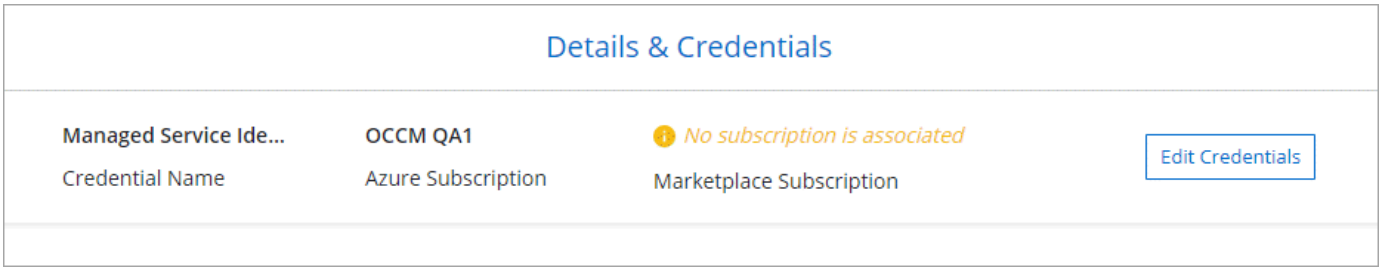
Erste Azure Zugangsdaten

Wenn Sie einen Connector von Cloud Manager bereitstellen, müssen Sie ein Azure-Konto mit Berechtigungen verwenden, um die Virtual Machine Connector bereitzustellen. Die erforderlichen Berechtigungen werden im aufgeführt "Connector-Implementierungsrichtlinie für Azure".

Wenn Cloud Manager die Connector Virtual Machine in Azure implementiert, kann sie ein "Vom System zugewiesene verwaltete Identität" Erstellt auf einer virtuellen Maschine eine benutzerdefinierte Rolle und weist sie der virtuellen Maschine zu. Cloud Manager erhält Berechtigungen für das Management von Ressourcen und Prozessen im Rahmen des Azure Abonnements. "Überprüfen Sie, wie Cloud Manager die Berechtigungen verwendet".



Cloud Manager wählt die Azure Zugangsdaten standardmäßig aus, wenn Sie eine neue Arbeitsumgebung für Cloud Volumes ONTAP erstellen:

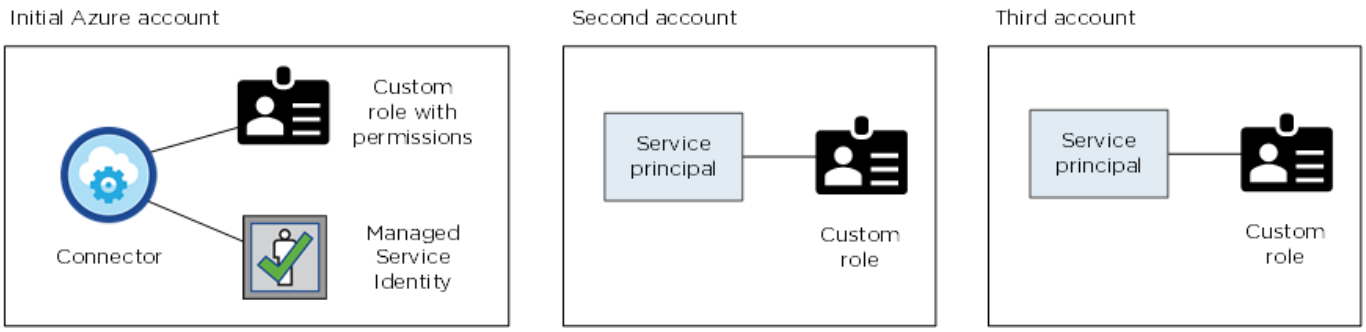


Zusätzliche Azure-Abonnements für eine gemanagte Identität

Die verwaltete Identität ist mit dem Abonnement verbunden, in dem Sie den Connector gestartet haben. Wenn Sie ein anderes Azure Abonnement auswählen möchten, müssen Sie es ausführen "Verknüpfen Sie die verwaltete Identität mit diesen Abonnements".

Zusätzliche Azure Zugangsdaten

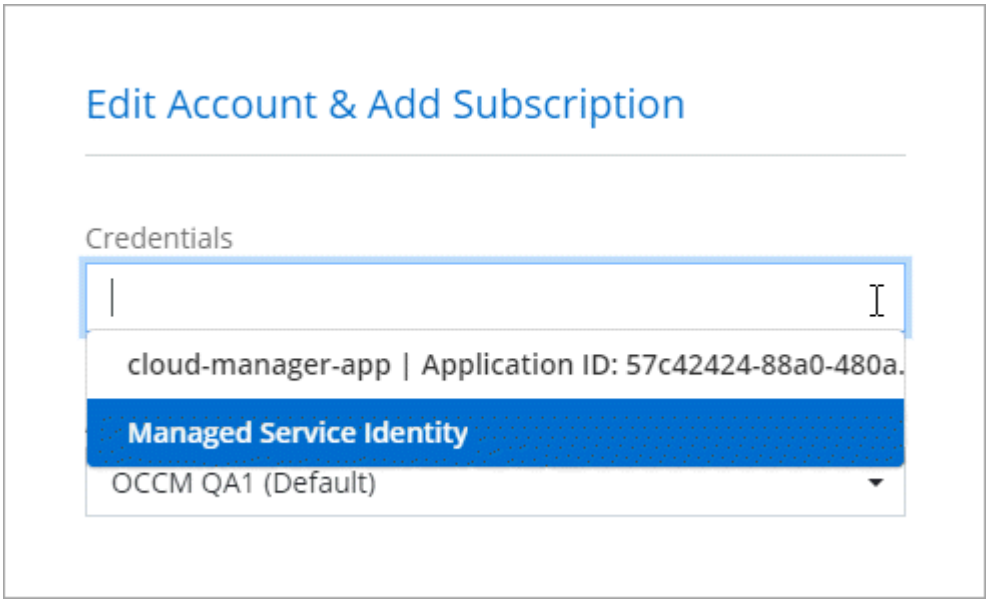
Wenn Sie Cloud Volumes ONTAP mit unterschiedlichen Azure Zugangsdaten implementieren möchten, müssen Sie die erforderlichen Berechtigungen von erteilen "Erstellen und Einrichten eines Service Principal in Azure Active Directory" Für jedes Azure Konto. Das folgende Bild zeigt zwei zusätzliche Konten, die jeweils mit einer Dienstprinzipal- und einer benutzerdefinierten Rolle eingerichtet sind, die Berechtigungen bereitstellt:



Das würden Sie dann tun "Fügen Sie die Kontoanmeldeinformationen zu Cloud Manager hinzu" Durch Angabe von Details zum AD-Dienstprinzipal.

Nachdem Sie einen weiteren Satz von Anmeldeinformationen hinzugefügt haben, können Sie zu ihnen

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 für den Connector beschrieben, der aus NetApp Cloud Central stammt. Sie können auch einen Connector in Azure über die bereitstellen "Azure Marketplace", Und Sie können "Installieren Sie den Steckverbinder vor Ort".

Wenn Sie den Marktplatz nutzen, werden Berechtigungen auf die gleiche Weise bereitgestellt. Sie müssen lediglich die verwaltete Identität für den Connector manuell erstellen und einrichten und dann Berechtigungen für weitere Konten bereitstellen.

Für On-Premises-Bereitstellungen können Sie keine verwaltete Identität für den Connector einrichten, aber Sie können Berechtigungen wie bei zusätzlichen Konten mit einem Service-Principal bereitstellen.

Verwalten von Azure Anmeldedaten und Abonnements für Cloud Manager

Wenn Sie ein Cloud Volumes ONTAP System erstellen, müssen Sie die Azure Zugangsdaten und das Marketplace-Abonnement auswählen, die mit diesem System verwendet werden sollen. Wenn Sie mehrere Azure Marketplace-Abonnements verwalten, können Sie jedes davon auf der Seite „Anmeldeinformationen“ verschiedenen Azure Zugangsdaten zuweisen.

Es gibt zwei Möglichkeiten, die Azure Zugangsdaten in Cloud Manager zu managen: Wenn Sie Cloud Volumes ONTAP zunächst in verschiedenen Azure-Konten bereitstellen möchten, müssen Sie die erforderlichen Berechtigungen angeben und die Zugangsdaten zu Cloud Manager hinzufügen. Die zweite Möglichkeit besteht darin, zusätzliche Abonnements mit der verwalteten Identität von Azure zu verknüpfen.

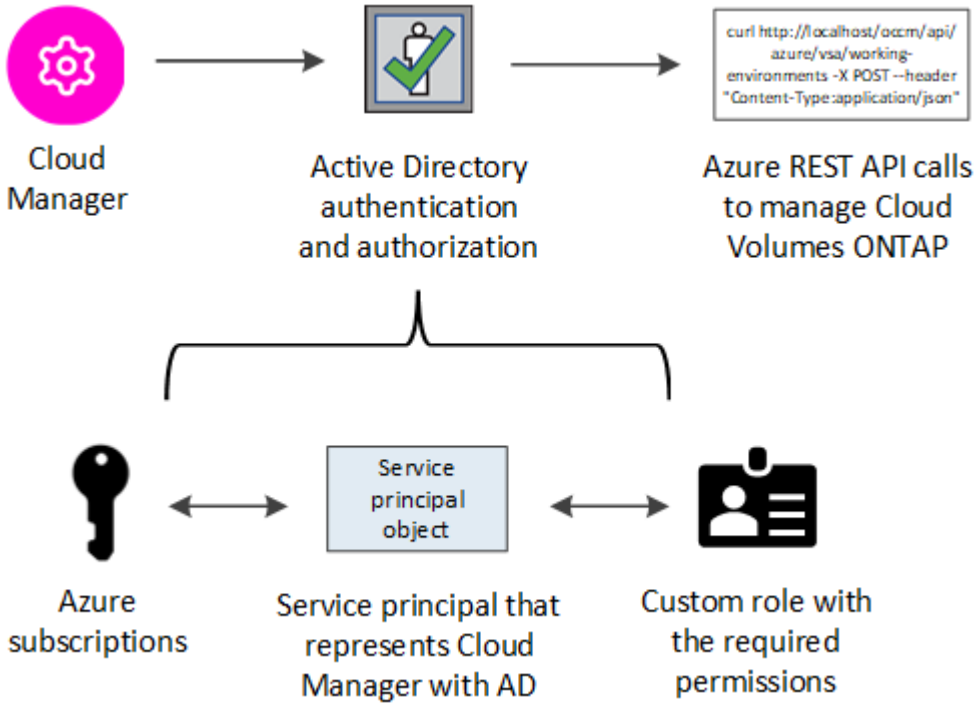
Wenn Sie einen Connector von Cloud Manager bereitstellen, fügt Cloud Manager automatisch das Azure-Konto hinzu, in dem Sie den Connector bereitgestellt haben. Ein erstes Konto wird nicht hinzugefügt, wenn Sie die Connector-Software manuell auf einem vorhandenen System installiert haben. "Weitere Informationen zu Azure Konten und Berechtigungen".

Azure-Berechtigungen über einen Service-Principal gewähren

Cloud Manager benötigt Berechtigungen zum Ausführen von Aktionen in Azure. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie einen Service-Principal in Azure Active Directory erstellen und einrichten, sowie die für Cloud Manager erforderlichen Azure Zugangsdaten erhalten.

Über diese Aufgabe

In der folgenden Abbildung wird dargestellt, wie Cloud Manager Berechtigungen zum Ausführen von Vorgängen in Azure erhält. Ein Service-Prinzipalobjekt, das an ein oder mehrere Azure Subscriptions gebunden ist, stellt Cloud Manager in Azure Active Directory dar und wird einer benutzerdefinierten Rolle zugewiesen, die die erforderlichen Berechtigungen zulässt.



Schritte

1. Erstellen Sie eine Azure Active Directory-Anwendung.
2. Anwendung einer Rolle zuweisen.
3. Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu.
4. Holen Sie die Anwendungs-ID und die Verzeichnis-ID ab.
5. Erstellen Sie einen Clientschlüssel.

Erstellen einer Azure Active Directory-Anwendung

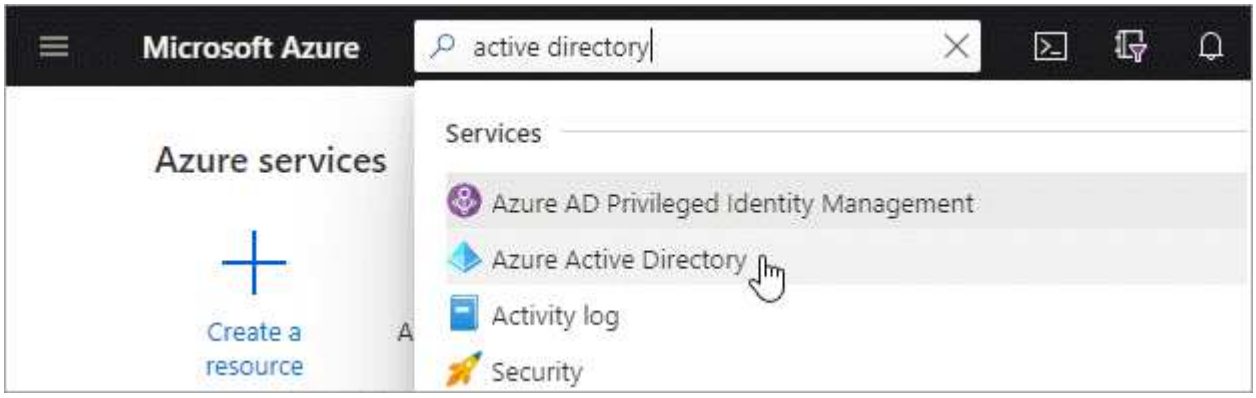
Erstellen einer Azure Active Directory (AD)-Applikation und eines Service-Principal, den Cloud Manager für die rollenbasierte Zugriffssteuerung nutzen kann

Bevor Sie beginnen

Sie müssen über die richtigen Berechtigungen in Azure verfügen, um eine Active Directory-Anwendung zu erstellen und die Anwendung einer Rolle zuzuweisen. Weitere Informationen finden Sie unter "Microsoft Azure-Dokumentation: Erforderliche Berechtigungen".

Schritte

1. Öffnen Sie über das Azure-Portal den **Azure Active Directory**-Service.



2. Klicken Sie im Menü auf **App-Registrierungen**.
3. Klicken Sie auf **Neue Registrierung**.
4. Geben Sie Details zur Anwendung an:
   - **Name**: Geben Sie einen Namen für die Anwendung ein.
   - **Kontotyp**: Wählen Sie einen Kontotyp aus (jeder funktioniert mit Cloud Manager).
   - **Redirect URI**: Wählen Sie **Web** und geben Sie dann eine beliebige URL ein – z. B. https://url
5. Klicken Sie Auf **Registrieren**.

Ergebnis

Sie haben die AD-Anwendung und den Service-Principal erstellt.

Anwendung einer Rolle zuweisen

Sie müssen den Service-Principal an ein oder mehrere Azure-Abonnements binden und ihm die benutzerdefinierte Rolle „OnCommand Cloud Manager Operator“ zuweisen, damit Cloud Manager über Berechtigungen in Azure verfügt.

Schritte

1. Erstellen einer benutzerdefinierten Rolle:

   a. Laden Sie die herunter "Cloud Manager Azure-Richtlinie".

   b. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

      Sie sollten die ID für jedes Azure Abonnement hinzufügen, aus dem Benutzer Cloud Volumes ONTAP Systeme erstellen.

      Beispiel

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

   c. Verwenden Sie die JSON-Datei, um eine benutzerdefinierte Rolle in Azure zu erstellen.

Im folgenden Beispiel wird gezeigt, wie eine benutzerdefinierte Rolle mithilfe der Azure CLI 2.0 erstellt wird:

```
az role definition create --role-definition
C:\Policy_for_cloud_Manager_Azure_3.8.7.json
```

Sie sollten nun über eine benutzerdefinierte Rolle namens *Cloud Manager Operator* verfügen.

2. Applikation der Rolle zuweisen:

   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.

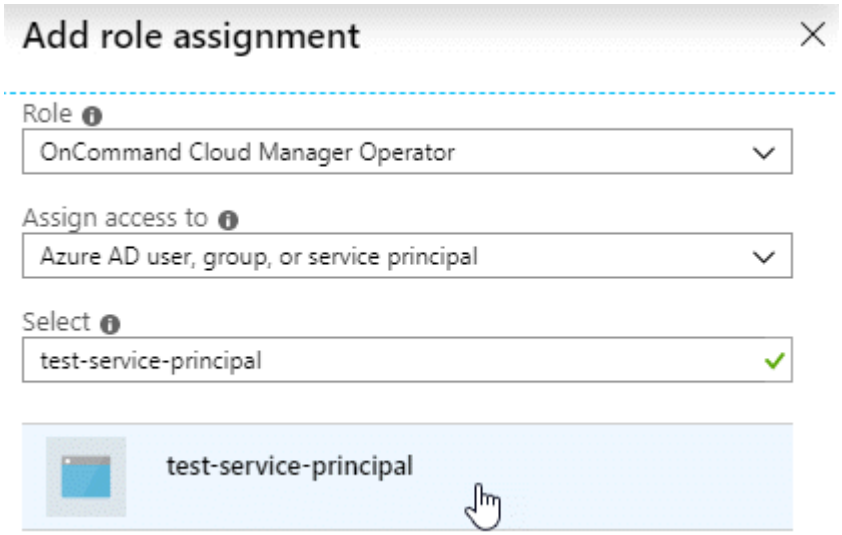
   b. Wählen Sie das Abonnement aus.

   c. Klicken Sie auf **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.

   d. Wählen Sie die Rolle **Cloud Manager Operator** aus.

   e. * Azure AD Benutzer, Gruppe oder Serviceprincipal* ausgewählt lassen.

   f. Suchen Sie nach dem Namen der Anwendung (Sie finden sie nicht in der Liste durch Scrollen).



   g. Wählen Sie die Anwendung aus und klicken Sie auf **Speichern**.

   Der Service Principal für den Cloud Manager verfügt jetzt über die erforderlichen Azure Berechtigungen für das Abonnement.

Wenn Sie Cloud Volumes ONTAP aus mehreren Azure Subscriptions bereitstellen möchten, müssen Sie den Service-Prinzipal an jedes dieser Subscriptions binden. Mit Cloud Manager können Sie das Abonnement auswählen, das Sie bei der Implementierung von Cloud Volumes ONTAP verwenden möchten.

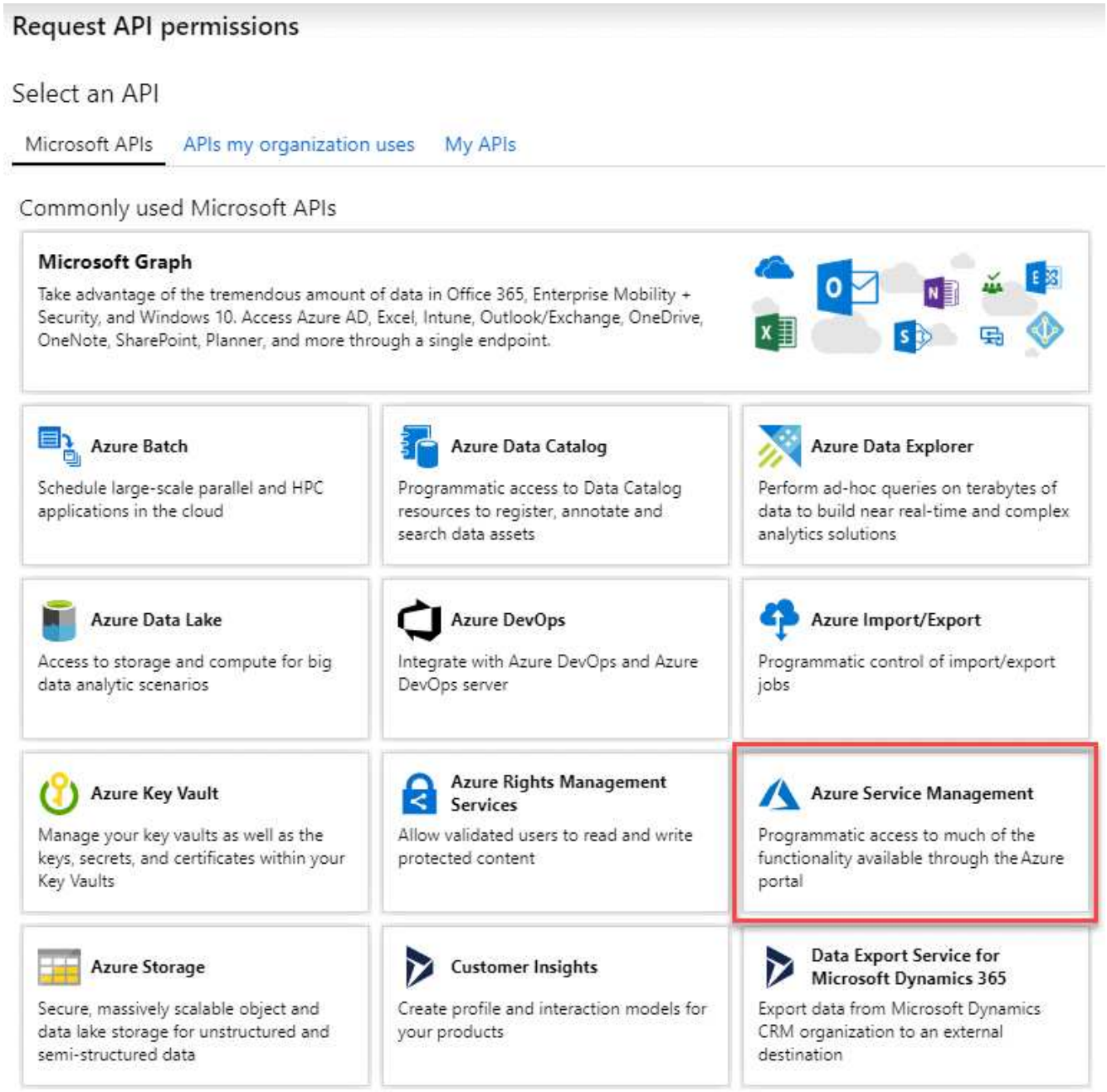
Windows Azure Service Management-API-Berechtigungen werden hinzugefügt

Der Service-Principal muss über die Berechtigungen „Windows Azure Service Management API“ verfügen.

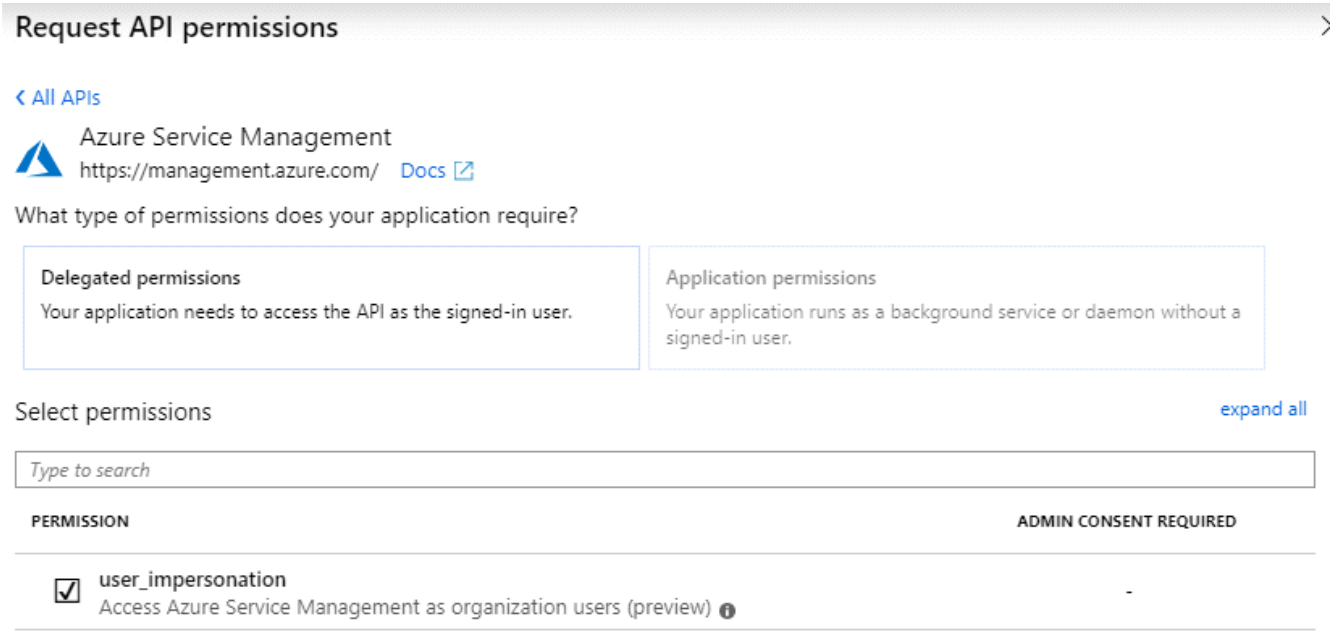
Schritte

1. Klicken Sie im **Azure Active Directory**-Dienst auf **App-Registrierungen** und wählen Sie die Anwendung aus.

2. Klicken Sie auf **API-Berechtigungen > Berechtigung hinzufügen**.
3. Wählen Sie unter **Microsoft APIs Azure Service Management** aus.



4. Klicken Sie auf **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann auf **Berechtigungen hinzufügen**.

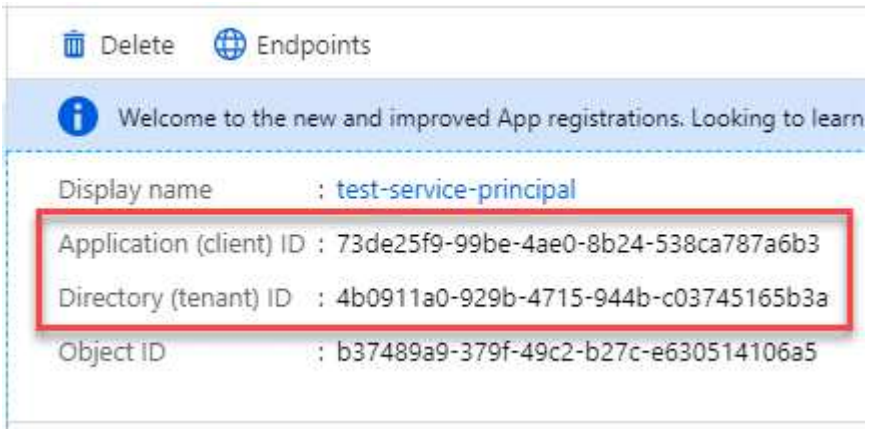


Abrufen der Anwendungs-ID und der Verzeichnis-ID

Wenn Sie dem Cloud Manager das Azure-Konto hinzufügen, müssen Sie die Anwendungs- (Client-) ID und die Verzeichnis- (Mandanten-)ID für die Applikation angeben. Cloud Manager verwendet die IDs, um sich programmatisch anzumelden.

Schritte

1. Klicken Sie im **Azure Active Directory**-Dienst auf **App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Application (Client) ID** und die **Directory (Tenant) ID**.



Erstellen eines Clientgeheimnisses

Sie müssen ein Client-Geheimnis erstellen und Cloud Manager dann den Wert des Geheimnisses zur Verfügung stellen, damit Cloud Manager es zur Authentifizierung mit Azure AD verwenden kann.

Wenn Sie das Konto zu Cloud Manager hinzufügen, bezieht sich Cloud Manager auf das Kundengeheimnis als Applikationsschlüssel.

Schritte

1. Öffnen Sie den Dienst **Azure Active Directory**.
2. Klicken Sie auf **App-Registrierungen** und wählen Sie Ihre Anwendung aus.
3. Klicken Sie auf **Zertifikate & Geheimnisse > Neuer Client Secret**.
4. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
5. Klicken Sie Auf **Hinzufügen**.
6. Kopieren Sie den Wert des Clientgeheimnisses.

Ergebnis

Ihr Service-Principal ist jetzt eingerichtet und Sie sollten die Anwendungs- (Client-)ID, die Verzeichnis- (Mandanten-)ID und den Wert des Clientgeheimnisses kopiert haben. Sie müssen diese Informationen in Cloud Manager eingeben, wenn Sie ein Azure-Konto hinzufügen.

Hinzufügen von Azure Zugangsdaten zu Cloud Manager

Nachdem Sie ein Azure Konto mit den erforderlichen Berechtigungen angegeben haben, können Sie die Anmeldedaten für dieses Konto Cloud Manager hinzufügen. Damit können Sie Cloud Volumes ONTAP Systeme in diesem Konto starten.

Was Sie benötigen

Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. "Erfahren Sie, wie".

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.

2. Klicken Sie auf **Anmeldeinformationen hinzufügen** und wählen Sie **Microsoft Azure**.
3. Geben Sie Informationen zum Azure Active Directory Service Principal ein, der die erforderlichen Berechtigungen erteilt:
   - Anwendungs-ID (Client): Siehe Abrufen der Anwendungs-ID und der Verzeichnis-ID.
   - Verzeichnis-ID (Mandant): Siehe Abrufen der Anwendungs-ID und der Verzeichnis-ID.
   - Client Secret: Siehe Erstellen eines Clientgeheimnisses.

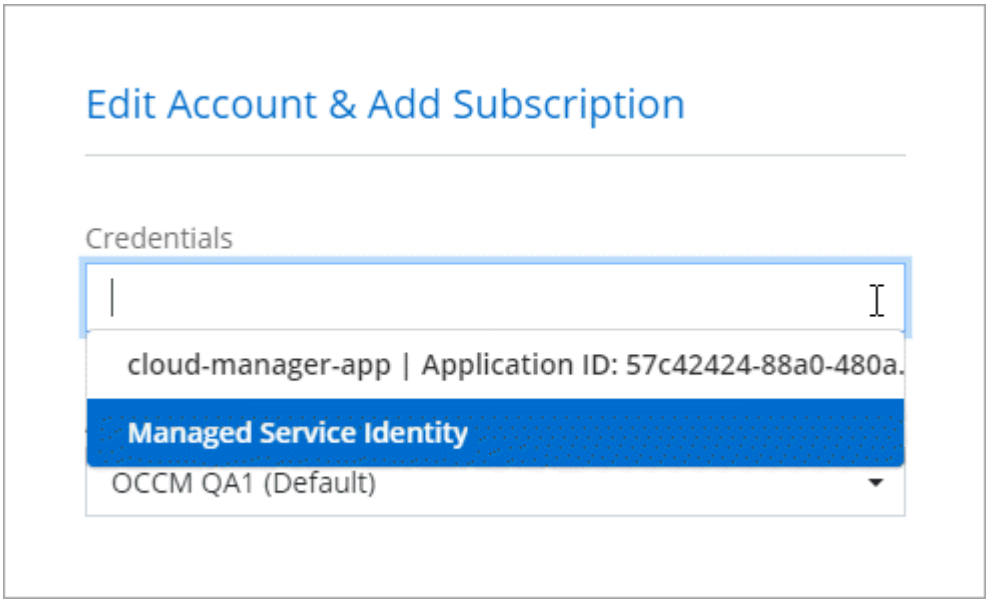
4. Bestätigen Sie, dass die Richtlinienanforderungen erfüllt wurden, und klicken Sie dann auf **Weiter**.
5. Wählen Sie das Pay-as-you-go-Abonnement aus, das Sie mit den Anmeldedaten verknüpfen möchten, oder klicken Sie auf **Abonnement hinzufügen**, wenn Sie noch nicht über ein Abonnement verfügen.

   Um ein Pay-as-you-go Cloud Volumes ONTAP System zu erstellen, müssen Azure Zugangsdaten über den Azure Marketplace mit einem Abonnement für Cloud Volumes ONTAP verknüpft werden.

6. Klicken Sie Auf **Hinzufügen**.

Ergebnis

Auf der Seite Details und Anmeldeinformationen können Sie nun zu verschiedenen Anmeldeinformationen wechseln "Beim Erstellen einer neuen Arbeitsumgebung":



Verknüpfen eines Azure Marketplace Abonnements mit den Zugangsdaten

Nachdem Sie Ihre Azure Zugangsdaten zu Cloud Manager hinzugefügt haben, können Sie diesen Anmeldedaten ein Azure Marketplace Abonnement zuweisen. Mithilfe des Abonnements können Sie ein nutzungsbasiertes Cloud Volumes ONTAP System erstellen und andere NetApp Cloud-Services nutzen.

Es gibt zwei Szenarien, in denen Sie ein Azure Marketplace-Abonnement verknüpfen können, nachdem Sie bereits die Anmeldedaten zu Cloud Manager hinzugefügt haben:

- Sie haben ein Abonnement nicht zugeordnet, wenn Sie zum ersten Mal die Anmeldedaten zu Cloud Manager hinzugefügt haben.
- Sie möchten ein vorhandenes Azure Marketplace Abonnement durch ein neues Abonnement ersetzen.

Was Sie benötigen

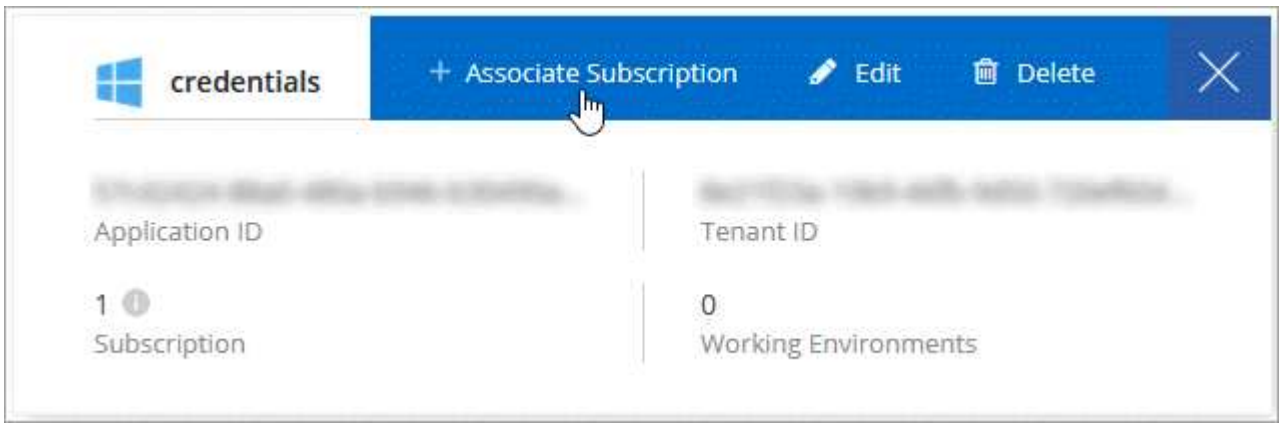
Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. "Erfahren Sie, wie".

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Bewegen Sie den Mauszeiger über einen Satz von Anmeldeinformationen, und klicken Sie auf das

Aktivitätsmenü.

3. Klicken Sie im Menü auf **Abonnement verknüpfen**.



4. Wählen Sie ein Abonnement aus der Down-Liste aus, oder klicken Sie auf **Abonnement hinzufügen** und befolgen Sie die Schritte, um ein neues Abonnement zu erstellen.

   Das folgende Video beginnt im Kontext des Assistenten zur Arbeitsumgebung, zeigt Ihnen aber den gleichen Workflow, nachdem Sie auf **Abonnement hinzufügen** geklickt haben:

   ► https://docs.netapp.com/de-de/occm38//media/video_subscribing_azure.mp4 *(video)*

Verknüpfen weiterer Azure-Abonnements mit einer gemanagten Identität

Mit Cloud Manager können Sie die Azure Zugangsdaten und das Azure Abonnement auswählen, in dem Sie Cloud Volumes ONTAP implementieren möchten. Sie können kein anderes Azure-Abonnement für das verwaltete Identitätsprofil auswählen, es sei denn, Sie verknüpfen das "Verwaltete Identität" Mit diesen Abonnements.

Über diese Aufgabe

Eine verwaltete Identität ist "Zunächst das Azure-Konto" Wenn Sie einen Connector von Cloud Manager bereitstellen. Wenn Sie den Connector bereitgestellt haben, hat Cloud Manager die Rolle Cloud Manager Operator erstellt und der virtuellen Maschine Connector zugewiesen.

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 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 **Cloud Manager Operator** aus.

        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.

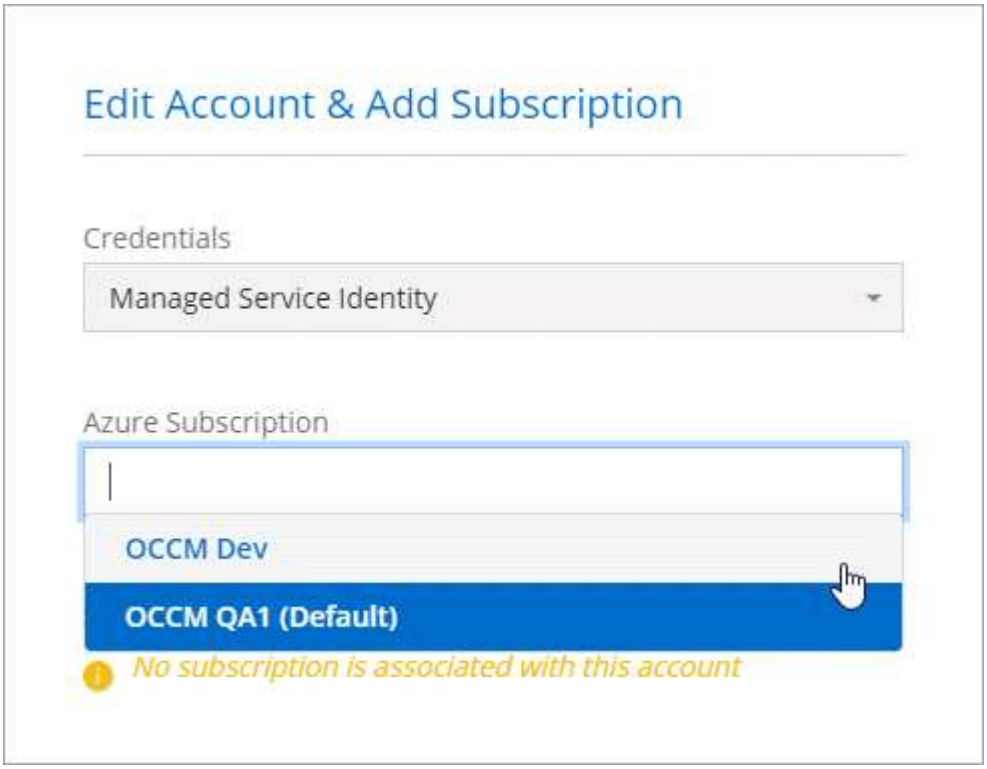
      - Weisen Sie einer **virtuellen Maschine** Zugriff zu.

- Wählen Sie das Abonnement aus, in dem die virtuelle Connector-Maschine erstellt wurde.
- Wählen Sie die virtuelle Verbindungsmaschine 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.



GCP

Google Cloud Projekte, Berechtigungen und Konten

Ein Service-Konto bietet Cloud Manager Berechtigungen für die Implementierung und das Management von Cloud Volumes ONTAP Systemen in demselben Projekt wie Cloud Manager oder in verschiedenen Projekten.

Projekt und Berechtigungen für Cloud Manager

Bevor Sie Cloud Volumes ONTAP in Google Cloud bereitstellen können, müssen Sie zunächst einen Connector in einem Google Cloud-Projekt bereitstellen. Der Connector kann nicht vor Ort oder bei einem anderen Cloud-Provider ausgeführt werden.

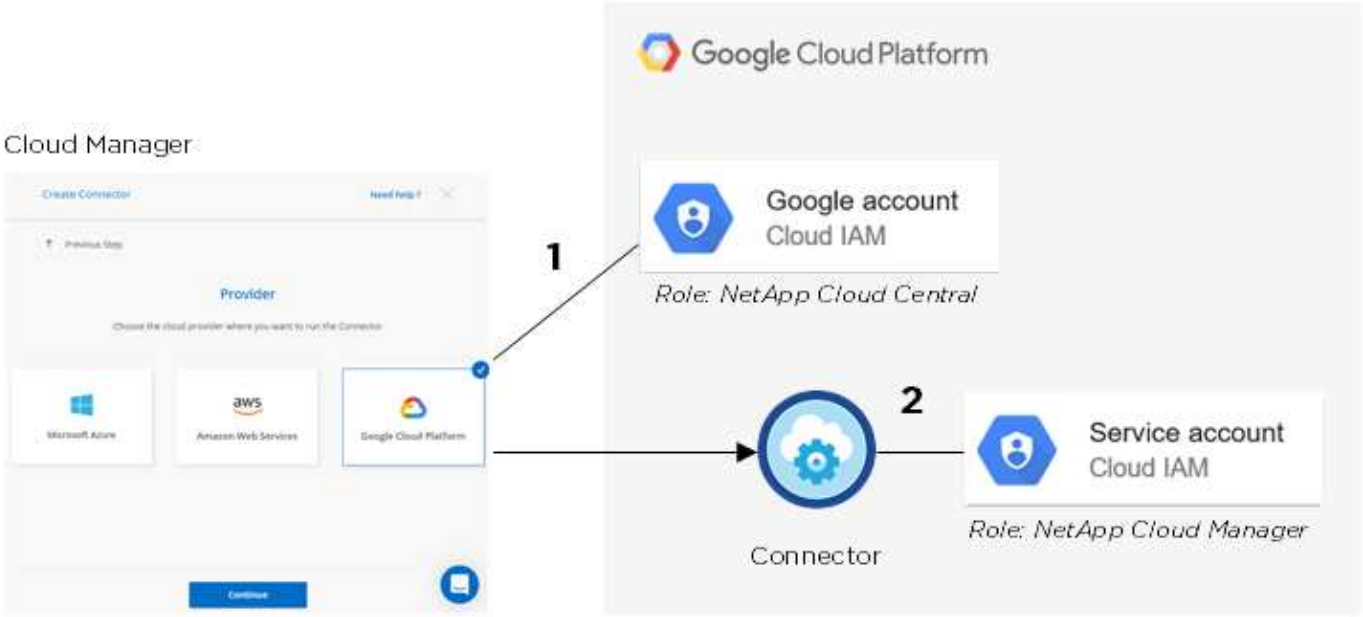
Vor der Bereitstellung eines Connectors direkt aus Cloud Manager müssen zwei Berechtigungssätze vorhanden sein:

1. Sie müssen einen Connector mit einem Google-Konto bereitstellen, das über Berechtigungen zum Starten der Connector-VM-Instanz von Cloud Manager verfügt.

2. Bei der Bereitstellung des Connectors werden Sie aufgefordert, ein auszuwählen "Servicekonto" Für die VM-Instanz. Cloud Manager erhält Berechtigungen vom Service-Konto, um Cloud Volumes ONTAP Systeme in Ihrem Auftrag zu erstellen und zu managen. Berechtigungen werden durch Hinzufügen einer benutzerdefinierten Rolle an das Servicekonto bereitgestellt.

Wir haben zwei YAML-Dateien eingerichtet, die die erforderlichen Berechtigungen für den Benutzer und das Dienstkonto enthalten. "Erfahren Sie, wie Sie mit den YAML-Dateien Berechtigungen einrichten".

Das folgende Bild zeigt die in den Nummern 1 und 2 oben beschriebenen Berechtigungsanforderungen:



Projekt für Cloud Volumes ONTAP

Cloud Volumes ONTAP kann im selben Projekt wie der Connector oder in einem anderen Projekt residieren. Um Cloud Volumes ONTAP in einem anderen Projekt bereitzustellen, müssen Sie zunächst das Connector-Servicekonto und die Rolle zu diesem Projekt hinzufügen.

- "Informationen zur Einrichtung eines Service-Kontos (siehe Schritt 2)".
- "Erfahren Sie, wie Cloud Volumes ONTAP in GCP implementiert und ein Projekt ausgewählt wird".

Konto für Daten-Tiering

Cloud Manager erfordert ein GCP-Konto für Cloud Volumes ONTAP 9.6, nicht jedoch für 9.7 und höher. Wenn Sie Daten-Tiering mit Cloud Volumes ONTAP 9.7 verwenden möchten, folgen Sie Schritt 4 in "Erste Schritte mit Cloud Volumes ONTAP in der Google Cloud Platform".

Um Daten-Tiering auf einem Cloud Volumes ONTAP 9.6 System zu ermöglichen, ist das Hinzufügen eines Google Cloud Kontos zu Cloud Manager erforderlich. Daten-Tiering verlagert selten genutzte Daten automatisch auf kostengünstigen Objekt-Storage, sodass Sie Speicherplatz auf dem primären Storage freigeben und den sekundären Storage reduzieren können.

Wenn Sie das Konto hinzufügen, müssen Sie Cloud Manager mit einem Speicherzugriffsschlüssel für ein Servicekonto bereitstellen, das Storage Admin-Berechtigungen hat. Cloud Manager verwendet die Zugriffssteuerung zum Einrichten und Managen eines Cloud Storage-Buckets für Daten-Tiering.

Nachdem Sie ein Google Cloud Konto hinzugefügt haben, können Sie auf einzelnen Volumes das Daten-

Tiering aktivieren, wenn Sie sie erstellen, ändern oder replizieren.

- "Erfahren Sie, wie Sie GCP-Konten in Cloud Manager einrichten und hinzufügen".
- "Verschieben Sie inaktive Daten auf kostengünstigen Objekt-Storage".

Verwalten von GCP-Anmeldedaten und -Abonnements für Cloud Manager

Sie können zwei Arten von Anmeldeinformationen für die Google Cloud-Plattform über Cloud Manager verwalten: Die Anmeldeinformationen, die der VM-Instanz von Connector zugewiesen sind, und die mit einem Cloud Volumes ONTAP 9.6-System für verwendeten Storage-Zugriffsschlüssel "Daten-Tiering".

Verknüpfen eines Marketplace-Abonnements mit GCP-Zugangsdaten

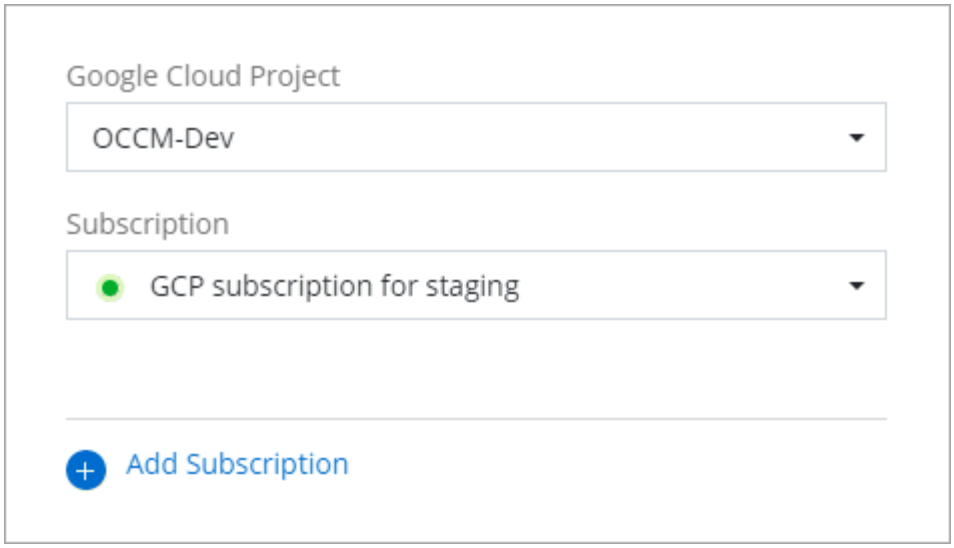
Wenn Sie einen Connector in GCP bereitstellen, erstellt Cloud Manager einen Standardsatz von Anmeldeinformationen, die der Connector-VM-Instanz zugeordnet sind. Diese sind die Zugangsdaten, die Cloud Manager zur Implementierung von Cloud Volumes ONTAP verwendet.

Sie können das Marketplace-Abonnement jederzeit ändern, das mit diesen Anmeldedaten verknüpft ist. Mithilfe des Abonnements können Sie ein nutzungsbasiertes Cloud Volumes ONTAP System erstellen und andere NetApp Cloud-Services nutzen.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Bewegen Sie den Mauszeiger über einen Satz von Anmeldeinformationen, und klicken Sie auf das Aktivitätsmenü.
3. Klicken Sie im Menü auf **Abonnement verknüpfen**.

4. Wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Down-Liste aus, oder klicken Sie auf **Abonnement hinzufügen** und befolgen Sie die Schritte, um ein neues Abonnement zu erstellen.



5. Klicken Sie Auf **Mitarbeiter**.

Einrichten und Hinzufügen von GCP-Konten für Daten-Tiering mit Cloud Volumes ONTAP 9.6

Wenn Sie ein Cloud Volumes ONTAP 9.6-System für aktivieren möchten "Daten-Tiering", Sie müssen Cloud Manager mit einem Storage-Zugriffschlüssel für ein Service-Konto bereitstellen, das Storage-Admin-Berechtigungen hat. Cloud Manager verwendet die Zugriffssteuerung zum Einrichten und Managen eines Cloud Storage-Buckets für Daten-Tiering.

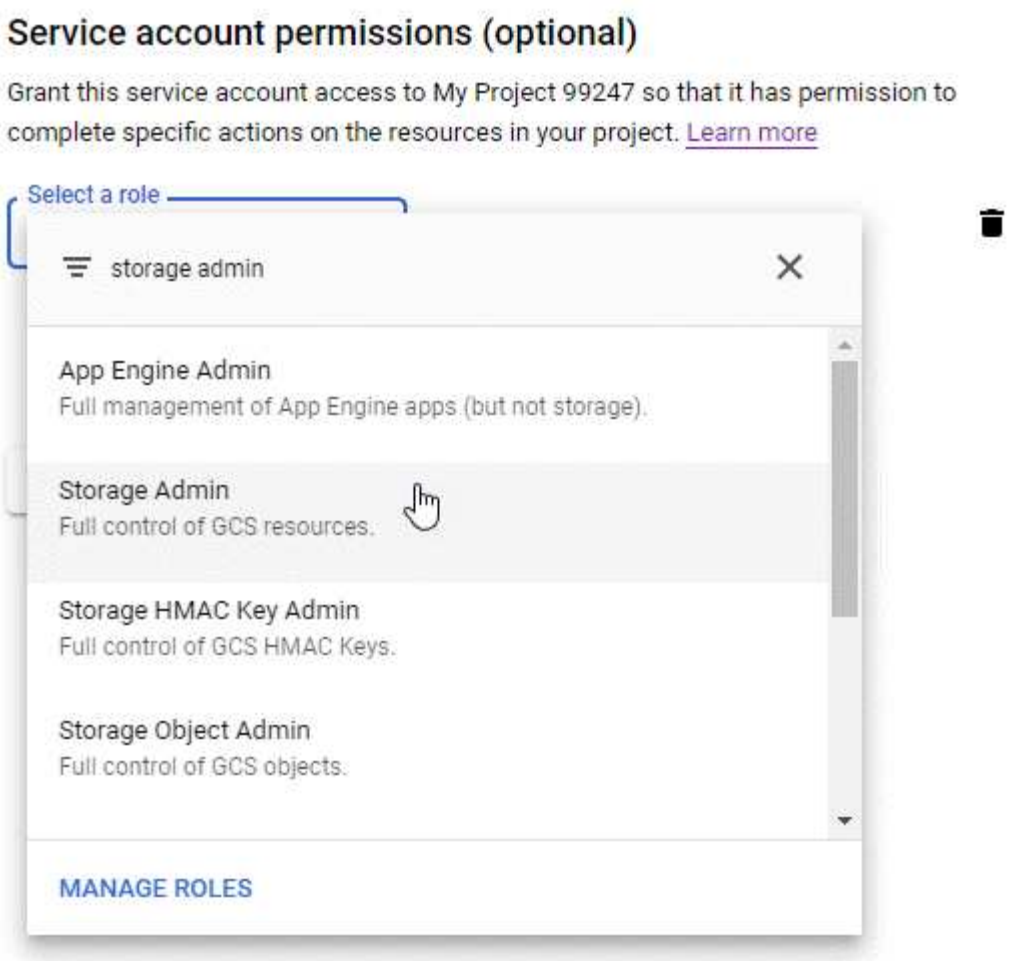
Wenn Sie Daten-Tiering mit Cloud Volumes ONTAP 9.7 verwenden möchten, folgen Sie Schritt 4 in "Erste Schritte mit Cloud Volumes ONTAP in der Google Cloud Platform".

Einrichten eines Servicekontos und Zugriffsschlüssel für Google Cloud Storage

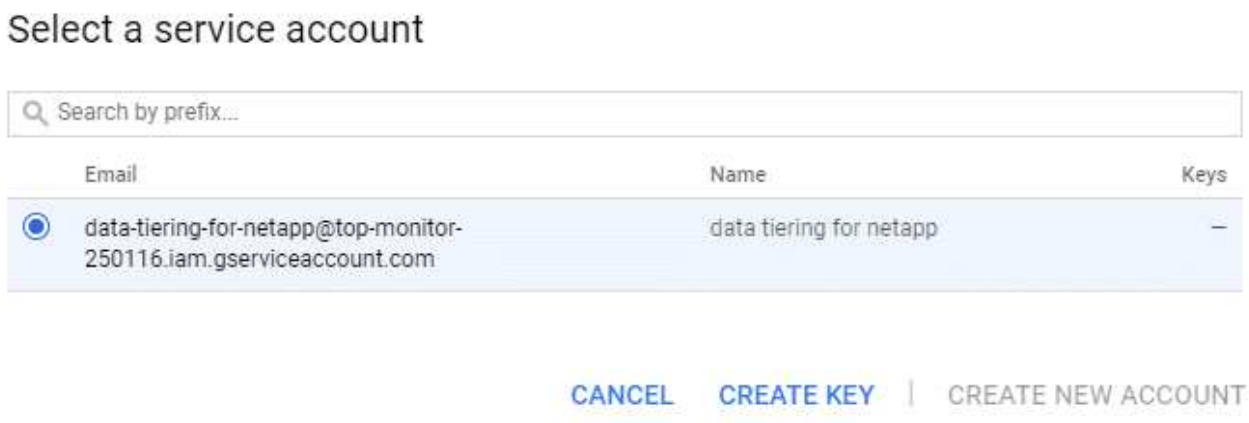
Mithilfe eines Service-Kontos kann Cloud Manager Cloud Storage-Buckets authentifizieren und auf sie zugreifen, die für Daten-Tiering verwendet werden. Die Schlüssel sind erforderlich, damit Google Cloud Storage weiß, wer die Anfrage stellt.

Schritte

1. Öffnen Sie die GCP IAM-Konsole und "Erstellen Sie ein Dienstkonto mit der Rolle Storage Admin".



2. Gehen Sie zu "GCP-Speichereinstellungen".
3. Wenn Sie aufgefordert werden, wählen Sie ein Projekt aus.
4. Klicken Sie auf die Registerkarte **Interoperabilität**.
5. Falls Sie dies noch nicht getan haben, klicken Sie auf **Interoperabilitätszugriff aktivieren**.
6. Klicken Sie unter **Zugriffsschlüssel für Servicekonten** auf **Schlüssel für ein Servicekonto erstellen**.
7. Wählen Sie das Servicekonto aus, das Sie in Schritt 1 erstellt haben.



8. Klicken Sie Auf **Schlüssel Erstellen**.

9. Kopieren Sie den Zugriffsschlüssel und den Schlüssel.

   Sie müssen diese Informationen in Cloud Manager eingeben, wenn Sie das GCP-Konto für das Daten-Tiering hinzufügen.

Hinzufügen eines GCP-Kontos zu Cloud Manager

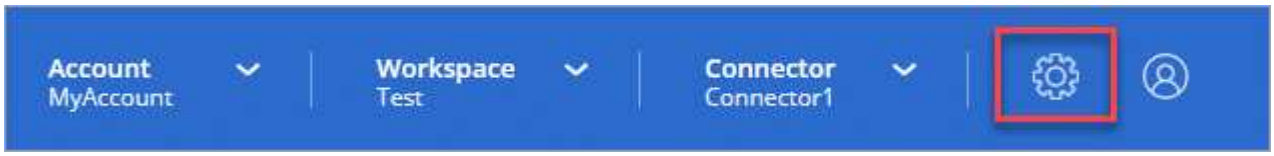
Nachdem Sie nun über einen Zugriffsschlüssel für ein Service-Konto verfügen, können Sie ihn dem Cloud Manager hinzufügen.

Was Sie benötigen

Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. "Erfahren Sie, wie".

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.



2. Klicken Sie auf **Anmeldeinformationen hinzufügen** und wählen Sie **Google Cloud**.
3. Geben Sie den Zugriffsschlüssel und den Schlüssel für das Servicekonto ein.

   Mithilfe der Schlüssel kann Cloud Manager einen Cloud Storage-Bucket für das Daten-Tiering einrichten.

4. Bestätigen Sie, dass die Richtlinienanforderungen erfüllt wurden, und klicken Sie dann auf **Konto erstellen**.

Was kommt als Nächstes?

Sie können jetzt Daten-Tiering für einzelne Volumes auf einem Cloud Volumes ONTAP 9.6 System aktivieren, wenn Sie sie erstellen, ändern oder replizieren. Weitere Informationen finden Sie unter "Tiering inaktiver Daten in kostengünstigen Objektspeicher".

Bevor Sie jedoch das tun, stellen Sie sicher, dass das Subnetz, in dem sich Cloud Volumes ONTAP befindet, für privaten Google-Zugriff konfiguriert ist. Anweisungen finden Sie unter "Google Cloud Documentation: Configuring Private Google Access".

Hinzufügen von NetApp Support Site Konten zu Cloud Manager

Um ein BYOL-System zu implementieren, muss ein NetApp Support Site Konto in Cloud Manager hinzugefügt werden. Zudem müssen Pay-as-you-go-Systeme registriert und ein Upgrade der ONTAP Software durchgeführt werden.

Sehen Sie sich das folgende Video an und erfahren Sie, wie Sie NetApp Support Site Accounts in Cloud Manager hinzufügen. Oder blättern Sie nach unten, um die Schritte zu lesen.

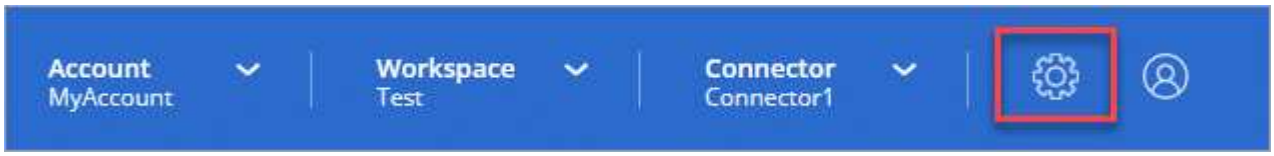
[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

Was Sie benötigen

Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. "Erfahren Sie, wie".

Schritte

1. Wenn Sie noch keinen NetApp Support Site Account haben, "Eine anmeldung".
2. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.



3. Klicken Sie auf **Anmeldedaten hinzufügen** und wählen Sie **NetApp Support Site**.
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"

Verwalten von Benutzern, Arbeitsbereichen, Connectors und Abonnements

"Nach der ersten Einrichtung", Möglicherweise müssen Sie Ihre Kontoeinstellungen später durch die Verwaltung von Benutzern, Workspaces, Connectors und Abonnements verwalten.

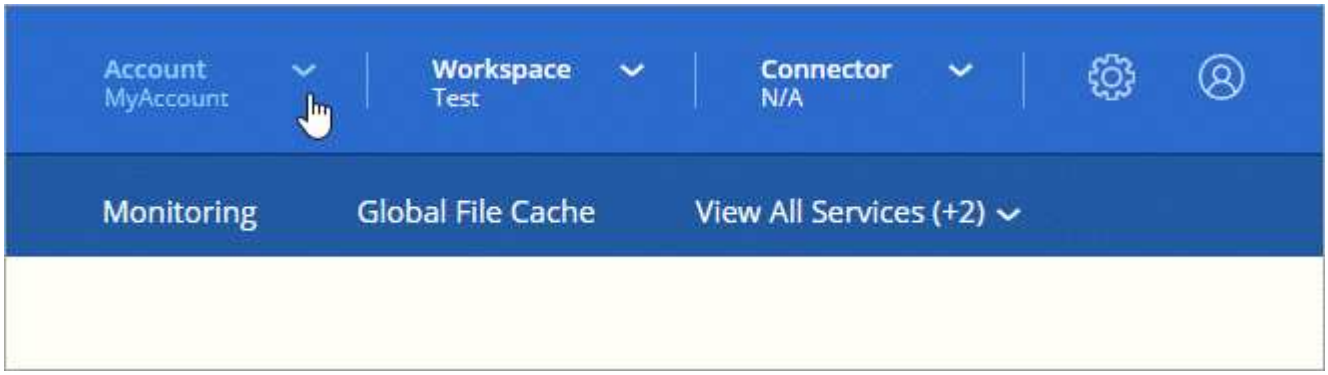
"Erfahren Sie mehr über die Funktionsweise von Cloud Central-Accounts".

Benutzer hinzufügen

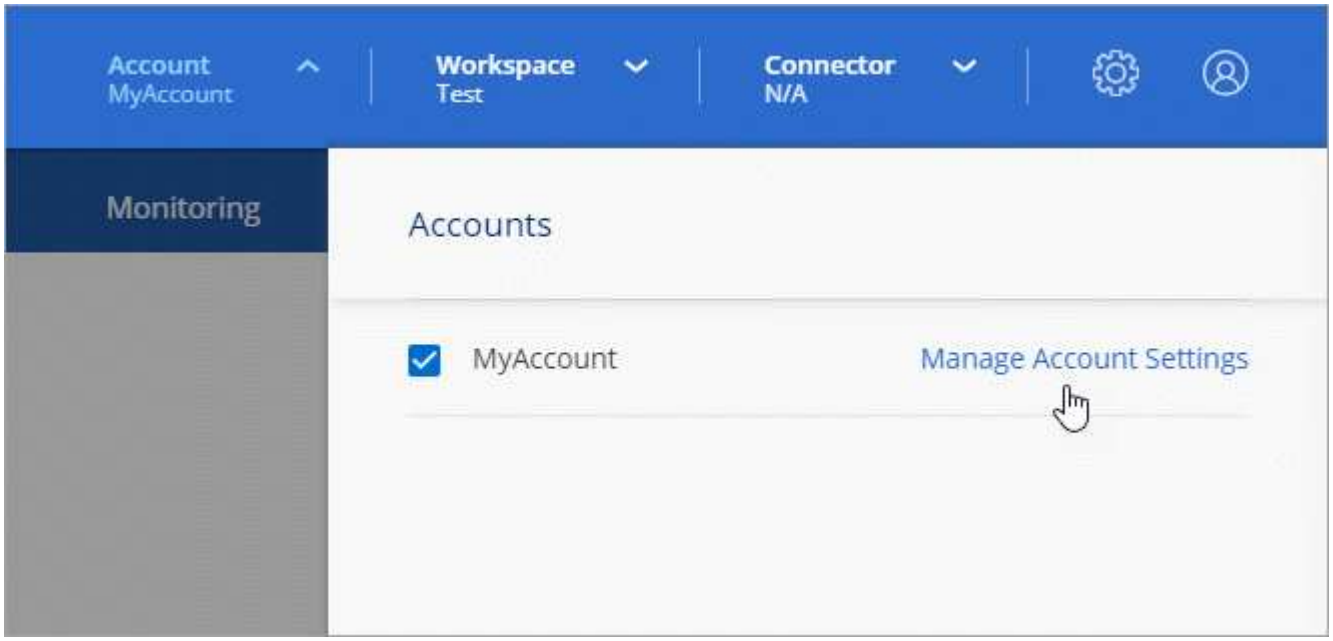
Cloud Central Benutzer werden mit dem Cloud Central Konto verknüpft, damit diese Arbeitsumgebungen in Cloud Manager erstellen und verwalten können.

Schritte

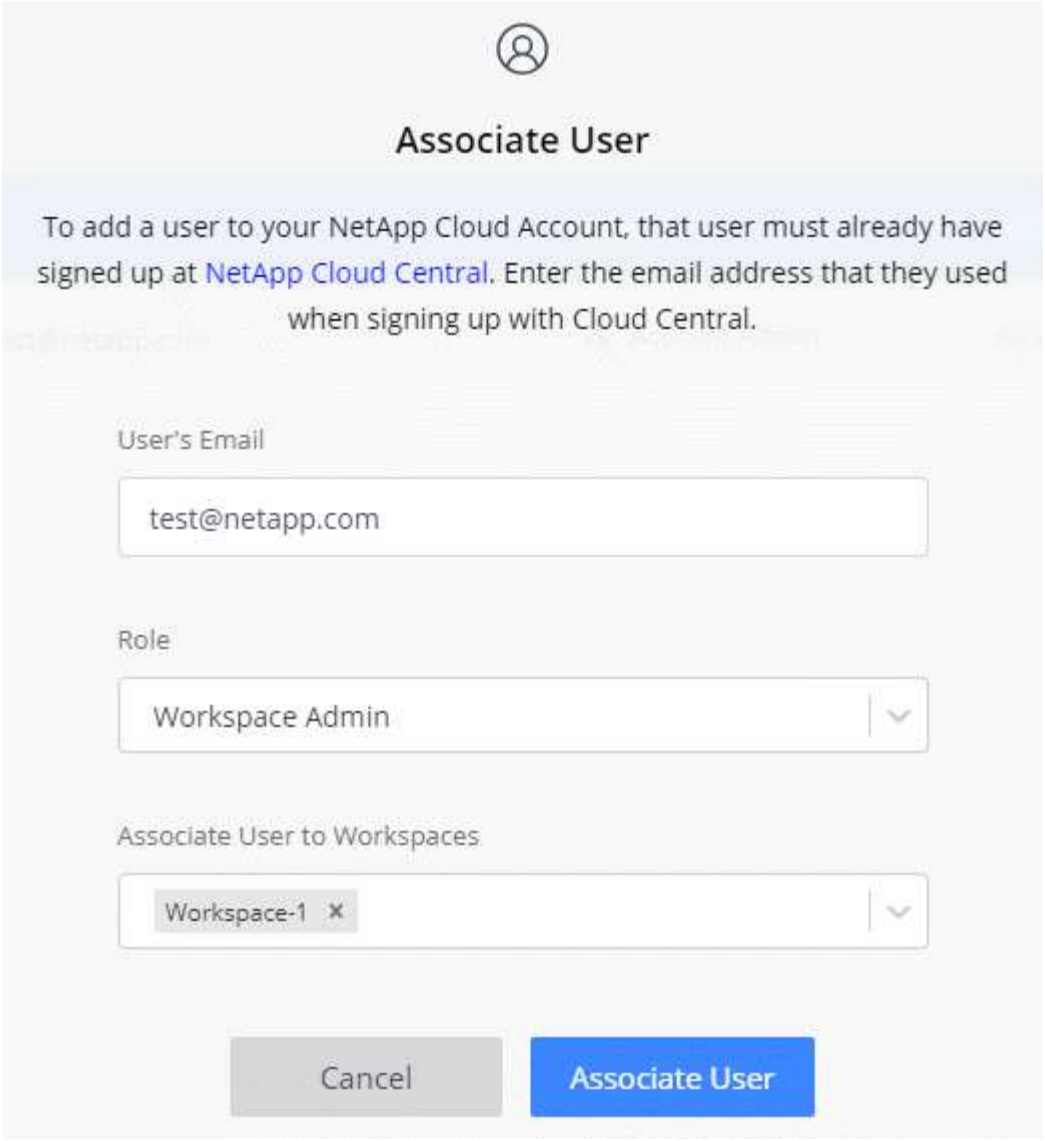
1. Wenn der Benutzer dies noch nicht getan hat, bitten Sie den Benutzer, zu wechseln "NetApp Cloud Central" Und melden Sie sich an.
2. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto**.



3. Klicken Sie neben dem aktuell ausgewählten Konto auf **Konto verwalten**.



4. Klicken Sie auf der Registerkarte Benutzer auf **Benutzer verknüpfen**.
5. Geben Sie die E-Mail-Adresse des Benutzers ein, und wählen Sie eine Rolle für den Benutzer aus:
   - **Account Admin**: Kann jede Aktion in Cloud Manager ausführen.
   - **Workspace Admin**: Kann Ressourcen in zugewiesenen Workspaces erstellen und verwalten.
   - **Compliance Viewer**: Kann nur Compliance-Informationen anzeigen und Berichte für Arbeitsbereiche erstellen, auf die sie zugreifen können.
6. Wenn Sie Workspace Admin oder Compliance Viewer ausgewählt haben, wählen Sie eine oder mehrere Arbeitsbereiche aus, die diesem Benutzer zugeordnet werden sollen.



7. Klicken Sie Auf * Benutzer Verknüpfen*.

Ergebnis

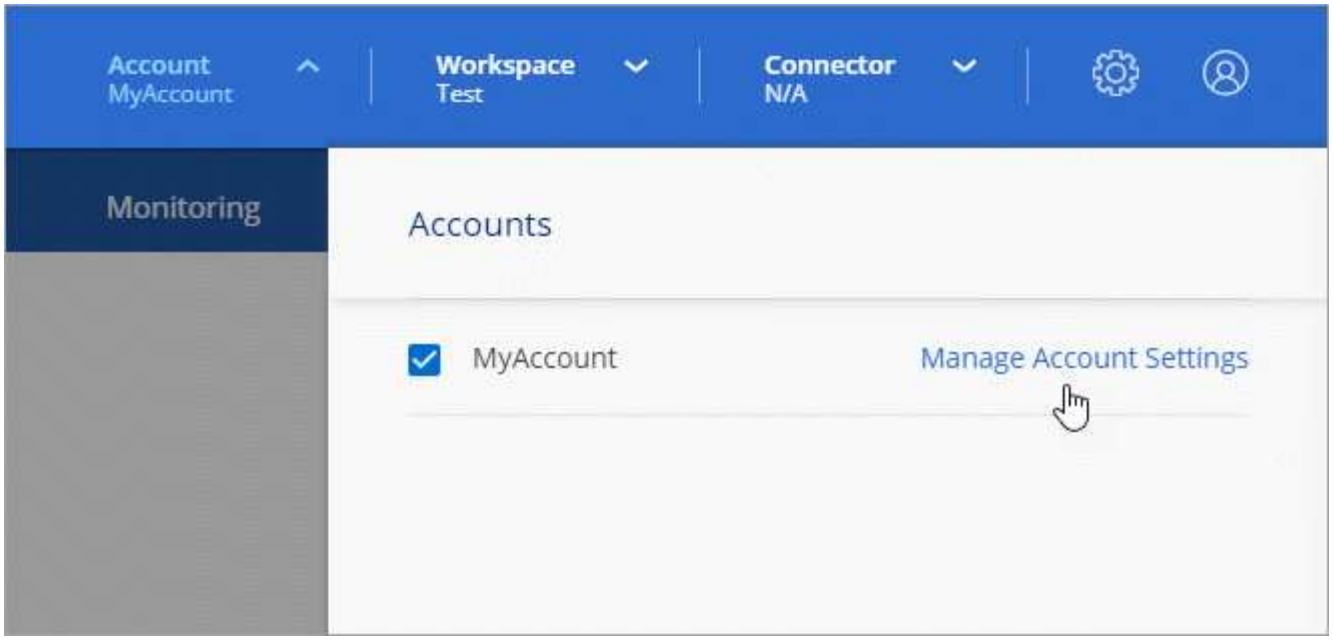
Der Benutzer sollte eine E-Mail von NetApp Cloud Central mit dem Titel „Account Association“ erhalten. Die E-Mail enthält die für den Zugriff auf Cloud Manager erforderlichen Informationen.

Benutzer werden entfernt

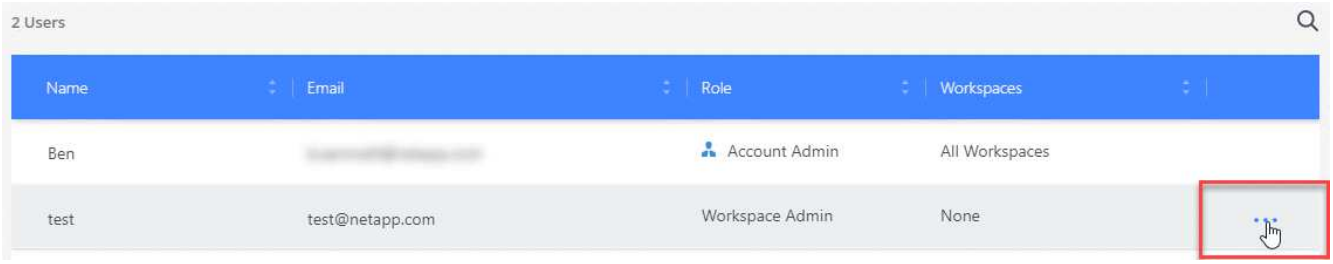
Die Trennung der Verknüpfung eines Benutzers wird dadurch erschwert, dass er nicht mehr auf die Ressourcen eines Cloud Central Kontos zugreifen kann.

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.



2. Klicken Sie auf der Registerkarte Benutzer auf das Aktionsmenü in der Zeile, die dem Benutzer entspricht.



3. Klicken Sie zur Bestätigung auf **Benutzer entzuordnen** und klicken Sie zur Bestätigung auf **Mitarbeiter nicht zuordnen**.

Ergebnis

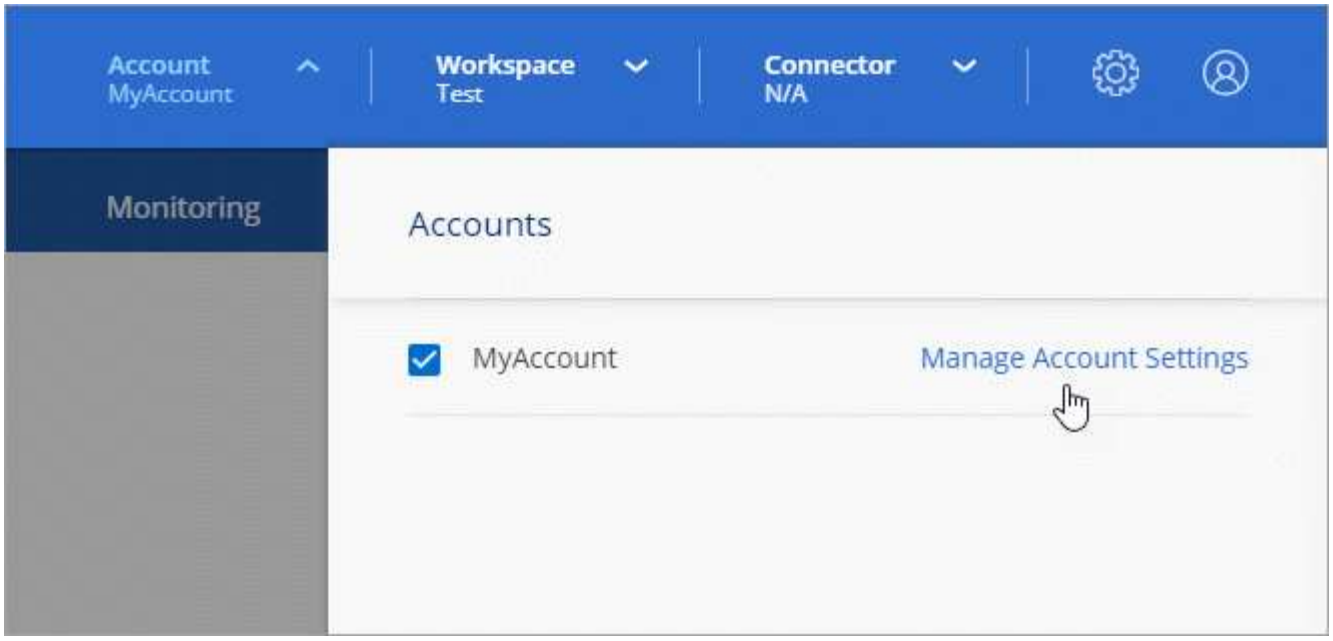
Der Benutzer kann nicht mehr auf die Ressourcen in diesem Cloud Central Konto zugreifen.

Arbeitsbereiche eines Arbeitsbereichs-Administrators verwalten

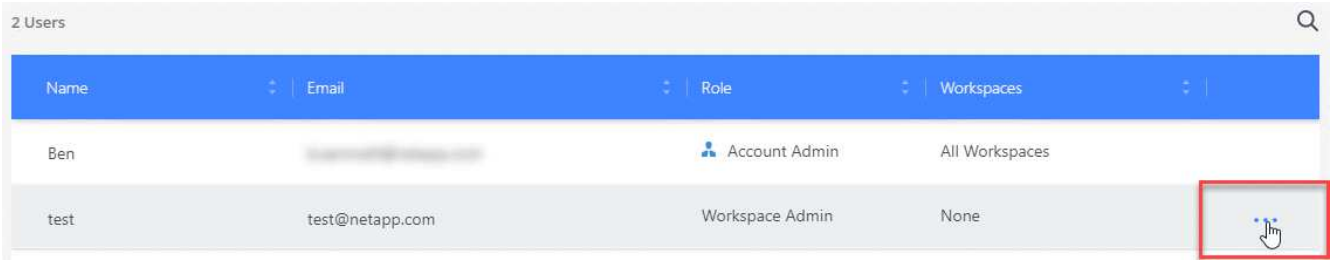
Sie können Workspace-Administratoren jederzeit mit Arbeitsbereichen verknüpfen und sie ablösen. Durch die Verknüpfung des Benutzers können die Arbeitsumgebungen in diesem Arbeitsbereich erstellt und angezeigt werden.

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.



2. Klicken Sie auf der Registerkarte Benutzer auf das Aktionsmenü in der Zeile, die dem Benutzer entspricht.



3. Klicken Sie Auf **Arbeitsbereiche Verwalten**.
4. Wählen Sie die Arbeitsbereiche aus, die dem Benutzer zugeordnet werden sollen, und klicken Sie auf **Anwenden**.

Ergebnis

Der Benutzer kann jetzt über Cloud Manager auf diese Arbeitsbereiche zugreifen, solange der Connector auch mit den Arbeitsbereichen verknüpft war.

Arbeitsbereiche verwalten

Verwalten Sie Ihre Arbeitsbereiche, indem Sie sie erstellen, umbenennen und löschen. Beachten Sie, dass Sie einen Arbeitsbereich nicht löschen können, wenn er Ressourcen enthält. Er muss leer sein.

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Klicken Sie Auf **Arbeitsbereiche**.
3. Wählen Sie eine der folgenden Optionen:
   - Klicken Sie auf **Neuen Arbeitsbereich hinzufügen**, um einen neuen Arbeitsbereich zu erstellen.
   - Klicken Sie auf **Umbenennen**, um den Arbeitsbereich umzubenennen.
   - Klicken Sie auf **Löschen**, um den Arbeitsbereich zu löschen.

Verwalten von Arbeitsumgebungen eines Connectors

Sie müssen den Connector mit Arbeitsbereichen verknüpfen, damit Workspace-Administratoren über Cloud Manager auf diese Arbeitsbereiche zugreifen können.

Wenn Sie nur Kontoadministratoren haben, ist es nicht erforderlich, den Connector mit Arbeitsbereichen zu verknüpfen. Account-Administratoren haben standardmäßig die Möglichkeit, auf alle Workspaces in Cloud Manager zuzugreifen.

"Erfahren Sie mehr über Benutzer, Arbeitsbereiche und Connectors".

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Klicken Sie Auf **Connector**.
3. Klicken Sie auf **Arbeitsbereiche verwalten** für den Konnektor, den Sie verknüpfen möchten.
4. Wählen Sie die Arbeitsbereiche aus, die mit dem Connector verknüpft werden sollen, und klicken Sie auf **Anwenden**.

Verwalten von Abonnements

Nachdem Sie den Marketplace eines Cloud-Providers abonniert haben, steht jedes Abonnement über das Widget „Account Settings“ (Kontoeinstellungen) zur Verfügung. Sie haben die Möglichkeit, ein Abonnement umzubenennen und das Abonnement von einem oder mehreren Konten zu entfernen.

Nehmen wir zum Beispiel an, dass Sie zwei Konten haben und jedes über separate Abonnements abgerechnet wird. Sie können ein Abonnement von einem der Konten ablösen, so dass die Benutzer in diesem Konto nicht versehentlich das falsche Abonnement wählen, wenn Sie eine Cloud Volume ONTAP Arbeitsumgebung erstellen.

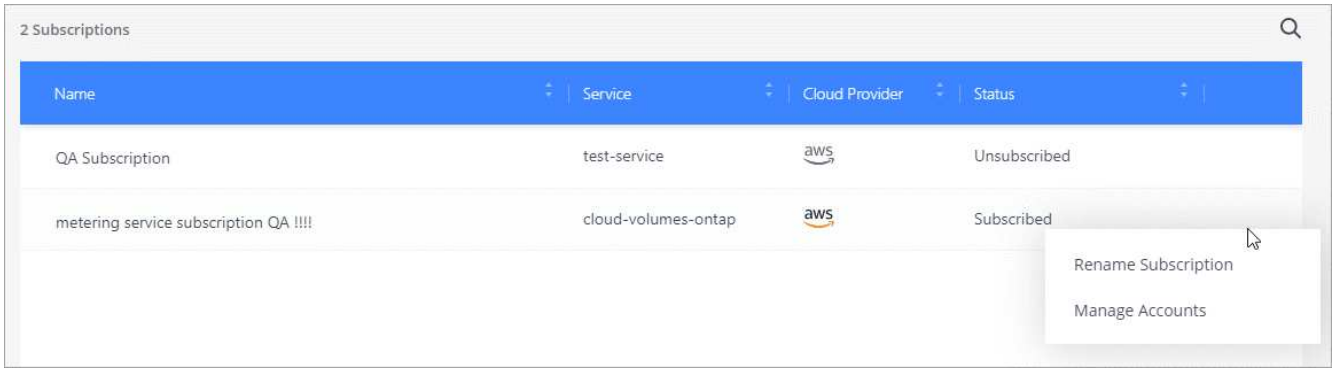
"Weitere Informationen zu Abonnements".

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Klicken Sie Auf **Abonnements**.

   Sie sehen nur die Abonnements, die mit dem Konto verknüpft sind, das Sie derzeit anzeigen.

3. Klicken Sie in der Zeile auf das Aktionsmenü, das dem Abonnement entspricht, das Sie verwalten möchten.



4. Wählen Sie diese Option, um das Abonnement umzubenennen oder um die Konten zu verwalten, die mit dem Abonnement verbunden sind.

Ändern des Kontonamens

Ändern Sie Ihren Kontonamen jederzeit, um ihn in etwas Sinnvolles für Sie zu ändern.

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Klicken Sie auf der Registerkarte **Übersicht** neben dem Kontonamen auf das Bearbeiten-Symbol.
3. Geben Sie einen neuen Kontonamen ein und klicken Sie auf **Speichern**.

Aktivieren oder Deaktivieren der SaaS-Plattform

Wir empfehlen nicht, die SaaS-Plattform zu deaktivieren, es sei denn, Sie müssen, um die Sicherheitsrichtlinien Ihres Unternehmens zu erfüllen. Durch die Deaktivierung der SaaS-Plattform ist Ihre Fähigkeit zur Nutzung von integrierten NetApp Cloud-Services begrenzt.

Die folgenden Services stehen bei Cloud Manager nicht zur Verfügung, wenn Sie die SaaS-Plattform deaktivieren:

- Cloud-Compliance
- Kubernetes
- Cloud Tiering
- Globaler Datei-Cache
- Monitoring (Cloud Insights)

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Aktivieren Sie auf der Registerkarte **Übersicht** die Option zur Nutzung der SaaS-Plattform.

Verwalten 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.

Bevor Sie beginnen

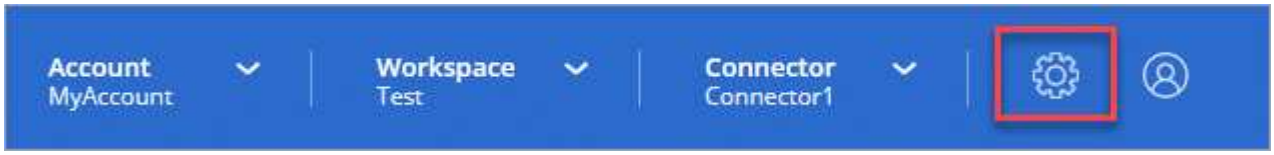
Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. "Erfahren Sie, wie".

Installieren eines HTTPS-Zertifikats

Installieren Sie ein von einer Zertifizierungsstelle signiertes Zertifikat, um den sicheren Zugriff zu gewährleisten.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **HTTPS-Setup**.

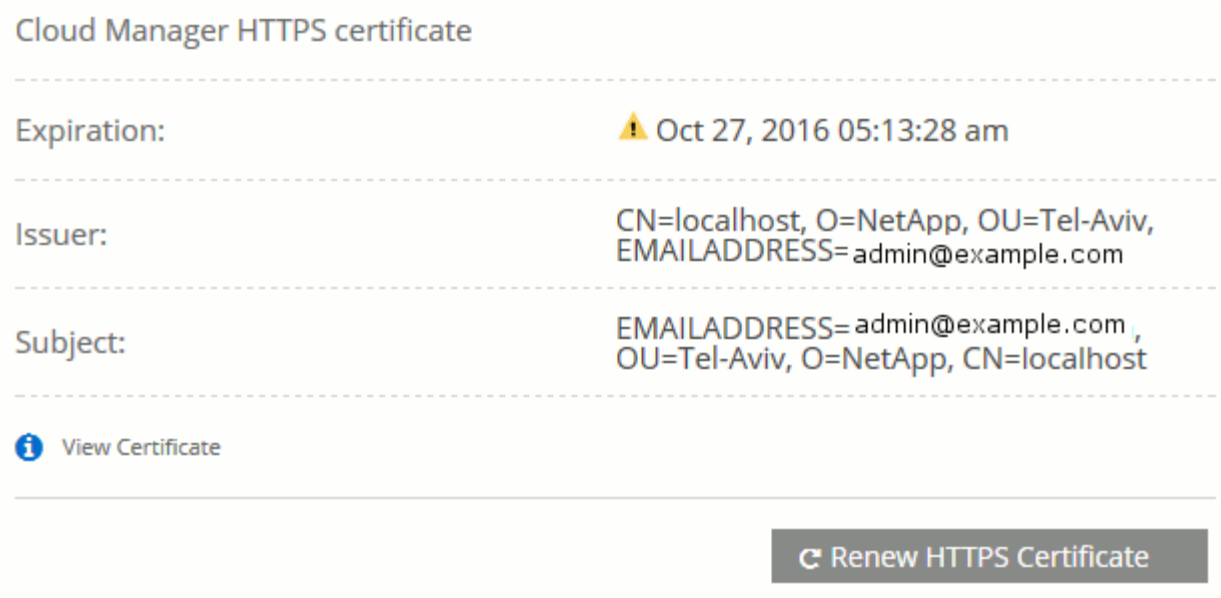


2. Installieren Sie auf der Seite HTTPS Setup ein Zertifikat, indem Sie eine Zertifikatsignierungsanforderung (CSR) erstellen oder Ihr eigenes, von der Zertifizierungsstelle signiertes Zertifikat installieren:

Option	Beschreibung
Erstellen Sie eine CSR	a. Geben Sie den Hostnamen oder den DNS des Connector-Hosts (dessen allgemeiner Name) ein, und klicken Sie dann auf **CSR erstellen**. 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:



Erneuerung des Cloud Manager HTTPS-Zertifikats

Sie sollten das HTTPS-Zertifikat von Cloud Manager vor dessen Ablauf erneuern, um einen sicheren Zugriff auf die Cloud Manager-Webkonsole zu gewährleisten. Wenn Sie das Zertifikat nicht vor Ablauf erneuern, wird eine Warnung angezeigt, wenn Benutzer über HTTPS auf die Webkonsole zugreifen.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **HTTPS-Setup**.

   Details zum Cloud Manager-Zertifikat werden angezeigt, einschließlich des Ablaufdatums.

2. Klicken Sie auf **HTTPS-Zertifikat erneuern** und befolgen Sie die Schritte, um eine CSR zu erstellen oder Ihr eigenes CA-signiertes Zertifikat zu installieren.

Ergebnis

Cloud Manager verwendet das neue CA-signierte Zertifikat, um sicheren HTTPS-Zugriff zu ermöglichen.

Entfernen von Cloud Volumes ONTAP Arbeitsumgebungen

Der Kontoadministrator kann eine Cloud Volumes ONTAP Arbeitsumgebung entfernen, in der sie auf ein anderes System verschoben oder Fehler bei der Erkennung behoben werden.

Über diese Aufgabe

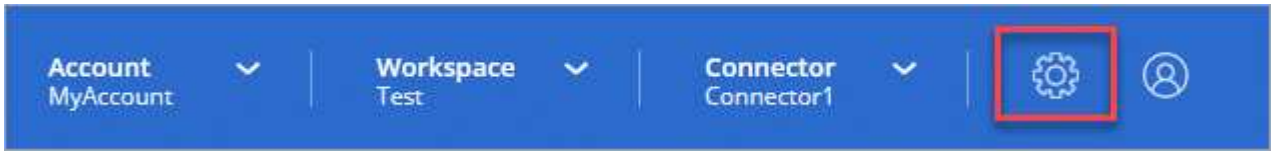
Durch das Entfernen einer Cloud Volumes ONTAP Arbeitsumgebung wird sie aus Cloud Manager entfernt. Das Cloud Volumes ONTAP System wird nicht gelöscht. Sie können die Arbeitsumgebung später neu entdecken.

Durch das Entfernen einer Arbeitsumgebung aus Cloud Manager können Sie Folgendes tun:

- In einem anderen Arbeitsbereich neu entdecken
- Entdecken Sie es von einem anderen Cloud Manager-System neu
- Entdecken Sie es erneut, wenn Sie während der ersten Erkennung Probleme hatten

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Tools**.



2. Klicken Sie auf der Seite Extras auf **Starten**.
3. Wählen Sie die Cloud Volumes ONTAP Arbeitsumgebung aus, die Sie entfernen möchten.
4. Klicken Sie auf der Seite „Prüfen und genehmigen“ auf **Los**.

Ergebnis

Cloud Manager entfernt die Arbeitsumgebung. Benutzer können diese Arbeitsumgebung jederzeit über die Seite Arbeitsumgebungen neu entdecken.

Konfigurieren eines Connectors für die Verwendung eines Proxy-Servers

Wenn Ihre Unternehmensrichtlinien festlegen, dass Sie für die gesamte HTTP-Kommunikation mit dem Internet einen Proxyserver verwenden, müssen Sie Ihre Connectors so konfigurieren, dass sie diesen Proxy-Server verwenden. Der Proxyserver kann sich in der Cloud oder im Netzwerk befinden.

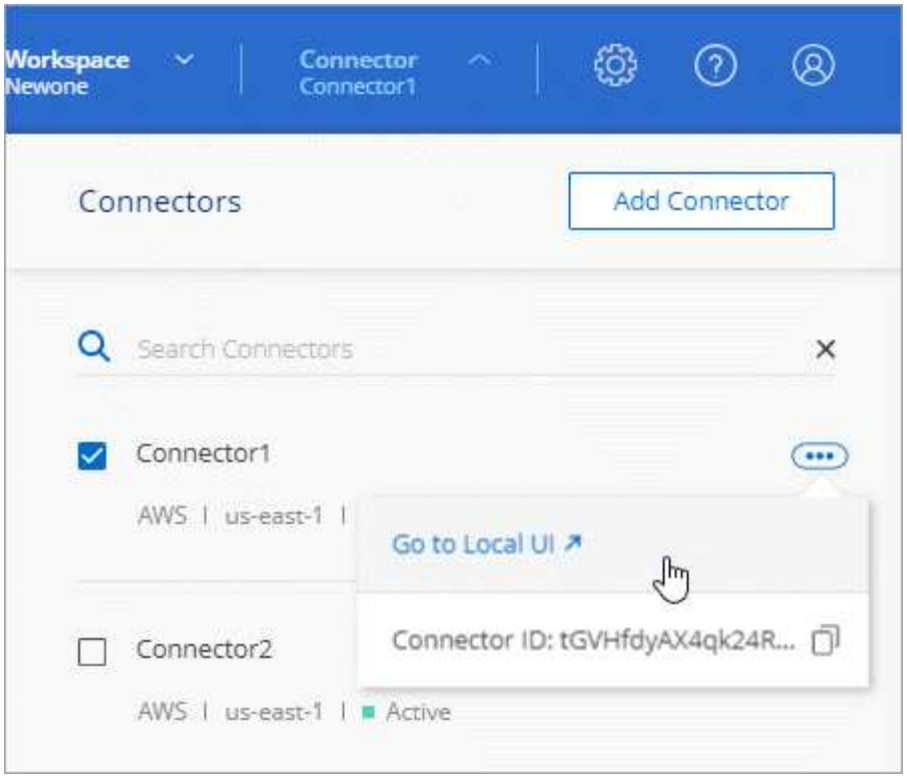
Wenn Sie einen Connector so konfigurieren, dass er einen Proxy-Server verwendet, verwenden dieser Connector und die von ihm verwalteten Cloud Volumes ONTAP-Systeme (einschließlich aller HA-Mediatoren) den Proxy-Server.

Schritte

1. "Melden Sie sich bei der SaaS-Schnittstelle von Cloud Manager an" Von einem Computer mit einer Netzwerkverbindung zur Instanz des Connectors.

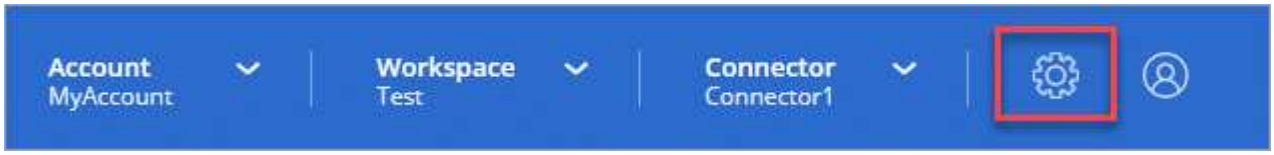
   Wenn der Connector keine öffentliche IP-Adresse hat, benötigen Sie eine VPN-Verbindung oder Sie müssen eine Verbindung von einem Jump-Host herstellen, der sich im gleichen Netzwerk wie der Connector befindet.

2. Klicken Sie auf das Dropdown-Menü **Connector** und dann auf **zur lokalen Benutzeroberfläche** für einen bestimmten Konnektor.



Die Cloud Manager-Schnittstelle, die auf dem Connector ausgeführt wird, wird in einer neuen Browser-Registerkarte geladen.

3. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Cloud Manager-Einstellungen**.



4. 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 Passwörter, 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 Proxy-Server nicht angegeben haben, bevor Benutzer Cloud Volumes ONTAP-Systeme erstellen, müssen sie mit System Manager den Proxyserver manuell in den AutoSupport-Optionen für jedes System festlegen.

Überschreiben von CIFS-Sperren für Cloud Volumes ONTAP HA in Azure

Der Kontoadministrator kann eine Einstellung in Cloud Manager aktivieren, die Probleme

mit dem Cloud Volumes ONTAP Storage Failover bei Azure-Wartungereignissen verhindert. Wenn Sie diese Einstellung aktivieren, sperrt Cloud Volumes ONTAP Vetoes CIFS und setzt aktive CIFS-Sitzungen zurück.

Über diese Aufgabe

Microsoft Azure plant regelmäßige Wartungsereignisse auf seinen Virtual Machines. Wenn auf einem Node in einem Cloud Volumes ONTAP HA-Paar ein Wartungsereignis stattfindet, initiiert das HA-Paar das Storage Takeover. Wenn während dieses Wartungsereignisses aktive CIFS-Sitzungen vorhanden sind, können die Sperren von CIFS-Dateien das Storage-Failover verhindern.

Wenn Sie diese Einstellung aktivieren, setzt Cloud Volumes ONTAP die Sperren zurück und setzt die aktiven CIFS-Sitzungen zurück. So kann das HA-Paar während dieser Wartungsereignisse das Storage Failover abschließen.

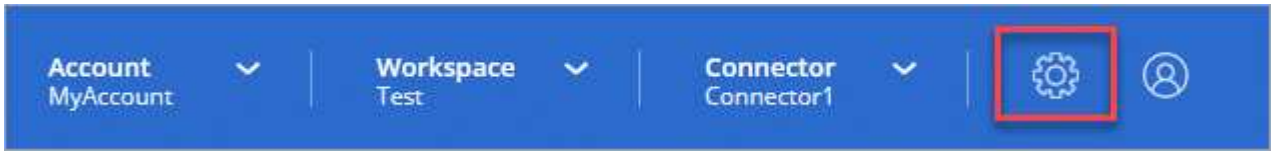
Dieser Prozess kann CIFS-Clients stören. Daten, die nicht von CIFS-Clients übertragen werden, können verloren gehen.

Was Sie benötigen

Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. "Erfahren Sie, wie".

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Cloud Manager-Einstellungen**.



2. Aktivieren Sie unter **HA CIFS locks** das Kontrollkästchen und klicken Sie auf **Speichern**.

Referenz

Rollen

Die Rollen Kontoverwaltung, Workspace Admin und Cloud Compliance Viewer bieten Benutzern spezifische Berechtigungen.

Aufgabe	Kontoadministrator	Workspace-Verwaltung	Cloud Compliance Viewer
Verwalten von Arbeitsumgebungen	Ja.	Ja.	Nein
Services in Arbeitsumgebungen ermöglichen	Ja.	Ja.	Nein
Anzeigen des Status der Datenreplizierung	Ja.	Ja.	Nein
Zeitachse anzeigen	Ja.	Ja.	Nein

Aufgabe	Kontoadministrator	Workspace-Verwaltung	Cloud Compliance Viewer
Wechseln Sie zwischen Arbeitsbereichen	Ja.	Ja.	Ja.
Anzeigen von Compliance-Scanergebnissen	Ja.	Ja.	Ja.
Arbeitsumgebungen löschen	Ja.	Nein	Nein
Kubernetes-Cluster mit Arbeitsumgebungen verbinden	Ja.	Nein	Nein
Cloud Volumes ONTAP Bericht erhalten	Ja.	Nein	Nein
Anschlüsse Erstellen	Ja.	Nein	Nein
Managen von Cloud Central Konten	Ja.	Nein	Nein
Anmeldeinformationen verwalten	Ja.	Nein	Nein
Ändern der Cloud Manager-Einstellungen	Ja.	Nein	Nein
Anzeigen und Verwalten des Support-Dashboards	Ja.	Nein	Nein
Entfernen Sie Arbeitsumgebungen aus Cloud Manager	Ja.	Nein	Nein
Installieren Sie ein HTTPS-Zertifikat	Ja.	Nein	Nein

Weiterführende Links

- "Einrichtung von Workspaces und Benutzern im Cloud Central Konto"
- "Managen von Workspaces und Benutzern im Cloud Central Konto"

Wie Cloud Manager die Berechtigungen von Cloud-Providern nutzt

Für die Ausführung von Aktionen bei Ihrem Cloud-Provider sind für Cloud Manager Berechtigungen erforderlich. Diese Berechtigungen sind in enthalten "Die von NetApp bereitgestellten Richtlinien". Sie möchten vielleicht wissen, was Cloud Manager mit diesen Berechtigungen macht.

Was Cloud Manager mit AWS-Berechtigungen macht

Cloud Manager verwendet ein AWS-Konto, um API-Aufrufe an mehrere AWS-Services durchzuführen, darunter EC2, S3, CloudFormation, IAM, den Security Token Service (STS) und den Key Management Service (KMS).

Aktionen	Zweck
„ec2:StartInstances“, „ec2:StopInstances“, „ec2:DescribeInstances“, „ec2:DescribeInstanceStatus“, „ec2:RunInstances“, „ec2:TerminateInstances“, „ec2:ModifyInstanceAttribut“,	Startet eine Cloud Volumes ONTAP Instanz und stoppt, startet und überwacht die Instanz.
"EC2:DescribeInstanceAttribute",	Überprüft, ob das erweiterte Netzwerk für unterstützte Instanztypen aktiviert ist.
„ec2:DescribeRouteTables“, „ec2:DescribeImages“,	Startet eine Cloud Volumes ONTAP HA-Konfiguration.
"EC2:CreateTags",	Kennzeichnet jede Ressource, die Cloud Manager erstellt, mit den Tags "workingenvironment" und "WorkingEnvironmentId". Cloud Manager verwendet diese Tags für Wartung und Kostenzuordnung.
„ec2:CreateVolume“, „ec2:DescribeVolumes“, „ec2:ModifyVolumeAttribute“, „ec2:AttachVolume“, „ec2:DeleteVolume“, „ec2:DetachVolume“,	Managt die EBS Volumes, die Cloud Volumes ONTAP als Back-End Storage verwendet.
„ec2:CreateSecurityGroup“, „ec2:DeleteSecurityGroup“, „ec2:DescribeSecurityGroups“, „ec2:RevokeSecurityGroupEgress“, „ec2:AuthoriseSecurityGroupEgress“, „ec2:AuthoriseSecurityGroupIngress“, „ec2:RevokeSecurityGroupIngress“,	Erstellt vordefinierte Sicherheitsgruppen für Cloud Volumes ONTAP.
„ec2:CreateNetworkInterface“, „ec2:DescribeNetworkInterfaces“, „ec2:DeleteNetworkInterface“, „ec2:ModifyNetworkInterface“,	Erstellt und managt Netzwerkschnittstellen für Cloud Volumes ONTAP im Ziel-Subnetz.
„ec2:DescribeSubnets“, „ec2:DescribeVpcs“,	Ruft die Liste der Zielsubnetze und Sicherheitsgruppen ab, die beim Erstellen einer neuen Arbeitsumgebung für Cloud Volumes ONTAP benötigt wird.
"EC2:DescribeDhcpOptions",	Bestimmt DNS-Server und den Standarddomänennamen beim Starten von Cloud Volumes ONTAP Instanzen.
„ec2:CreateSnapshot“, „ec2:DeleteSnapshot“, „ec2:DescribeSnapshots“,	Erstellt Snapshots von EBS Volumes während der Ersteinrichtung und bei jedem Anhalten einer Cloud Volumes ONTAP Instanz.
"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“, „s3:GetBucketPolicyStatus“, „s3:GetBucketPublicAccessBlock“, „s3:GetBucketAcl“, „s3:GetBucketPolicy“, „s3:PutBucketPublicAccessBlock“	Managt den S3-Bucket, den ein Cloud Volumes ONTAP System als Kapazitäts-Tier für das Daten-Tiering verwendet
„Kms:Liste*“, „Kms:Reverschlüsselt*“, „Kms:Beschreiben*“, „Kms:CreateGrant“,	Aktiviert die Datenverschlüsselung von Cloud Volumes ONTAP mithilfe des AWS KMS (Key Management Service).
„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.
„ec2:DescribeReserviertInstanceAngebote“	Cloud Manager verwendet die Berechtigung als Teil der Cloud Compliance-Implementierung, um den Instanztyp auszuwählen, der verwendet werden soll.

Aktionen	Zweck
„s3:DeleteBucket“, „s3:GetLifecycleConfiguration“, „s3:PutLifecycleConfiguration“, „s3:PutBucketTagging“, „s3:ListBucketVersions“, „s3:GetObject“, „s3:ListBucket“, „s3:ListAllMyBuckets“, „s3:GetBucketTagging“, „s3:GetBucketLocation“ „s3:GetBucketPolicyStatus“, „s3:GetBucketPublicAccessBlock“, „s3:GetBucketAcl“, „s3:GetBucketPolicy“, „s3:PutBucketPublicAccessBlock“	Cloud Manager verwendet diese Berechtigungen, wenn Sie den Service „Backup in S3“ aktivieren.

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.

Aktionen	Zweck
„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.
„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.

Aktionen	Zweck
„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
„Microsoft.Network/privateEndpoints/write", „Microsoft.Storage/StoragebAccounts/PrivateEndpointConnectionsApproval/Action“, „Microsoft.Storage/storageAccounts/privateEndpointConnections/read“, „Microsoft.Network/privateEndpoints/read", „Microsoft.Network/privateDnsZones/write", „Microsoft.Network/privateDnsZones/virtualNetworkLinks/write", „Microsoft.Network/virtualNetworks/join/action", „Microsoft.Network/privateDnsZones/A/write", „Microsoft.Network/privateDnsZones/read", „Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",	Ermöglicht das Management privater Endpunkte. Private Endpunkte werden verwendet, wenn keine Konnektivität außerhalb des Subnetzes bereitgestellt wird. Cloud Manager erstellt das Storage-Konto für HA mit nur der internen Konnektivität im Subnetz.
„Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",	Ermöglicht Cloud Manager das Löschen von Volumes für Azure NetApp Files.
„Microsoft.Resources/Deployments/OperationStatuses/read“	Azure erfordert diese Berechtigung für einige Implementierungen von Virtual Machines (das hängt von der zugrunde liegenden physischen Hardware ab, die während der Implementierung verwendet wird).
„Microsoft.Resources/Deployments/OperationStatuses/read“, „Microsoft.Insights/Metrics/Read“, „Microsoft.Compute/virtualMachines/extensions/write", „Microsoft.Compute/virtualMachines/extensions/read", „Microsoft.Compute/virtualMachines/extensions/delete", „Microsoft.Compute/virtualMachines/delete", „Microsoft.Network/networkInterfaces/delete", „Microsoft.Network/networkSecurityGroups/delete", „Microsoft.Resources/Deployments/delete“,	Ermöglicht die Verwendung von Global File Cache.

Aktionen	Zweck
„Microsoft.Compute/diskEncryptionSets/read"	Cloud Manager ermöglicht die Verschlüsselung von über Azure gemanagten Festplatten auf Cloud Volumes ONTAP-Systemen mit einem einzelnen Node mithilfe von externen Schlüsseln eines anderen Kontos. Diese Funktion wird durch APIs unterstützt.

Was Cloud Manager mit GCP-Berechtigungen macht

Die Cloud Manager-Richtlinie für GCP beinhaltet die Berechtigungen, die Cloud Manager für die Implementierung und das Management von Cloud Volumes ONTAP benötigt.

Aktionen	Zweck
- Compute.Disks.create - Compute.Disks.createSnapshot - compute.disks.delete - Compute.Disks.get - Compute.Disks.list - compute.disks.setLabels - compute.disks.use	Zum Erstellen und Verwalten von Festplatten für Cloud Volumes ONTAP.
- Compute.Firewalls.create - compute.firewalls.delete - Compute.Firewalls.get - Compute.Firewalls.list	Um Firewall-Regeln für Cloud Volumes ONTAP zu erstellen.
- Compute.globalOperations.get	Um den Status von Vorgängen anzuzeigen.
- Compute.images.get - Compute.images.getFromFamily - Compute.images.list - compute.images.useReadOnly	Um Images für VM-Instanzen zu erhalten.
- compute.instances.attachDisk - compute.instances.detachDisk	Zum Verbinden und Trennen von Festplatten mit Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Um Cloud Volumes ONTAP VM-Instanzen zu erstellen und zu löschen.
- compute.instances.get	Um VM-Instanzen aufzulisten.
- compute.instances.getSerialPortOutput	Um Konsolenprotokolle zu erhalten.
- compute.instances.list	Um die Liste der Instanzen in einer Zone abzurufen.
- compute.instances.setDeletionProtection	So legen Sie den Löschschutz für die Instanz fest:
- compute.instances.setLabels	So fügen Sie Etiketten hinzu:
- compute.instances.setMachineType	So ändern Sie den Maschinentyp für Cloud Volumes ONTAP.
- compute.instances.setMetadata	Um Metadaten hinzuzufügen.
- compute.instances.setTags	Um Tags für Firewall-Regeln hinzuzufügen.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Um Cloud Volumes ONTAP zu starten und anzuhalten.
- Compute.machineTypes.get	Um die Anzahl der Kerne zu erhalten, um qouten zu überprüfen.
- compute.projects.get	Zur Unterstützung mehrerer Projekte.

Aktionen	Zweck
- Compute.Snapshots.create - compute.snapshots.delete - Compute.Snapshots.get - Compute.Snapshots.list - compute.snapshots.setLabels	Um persistente Festplatten-Snapshots zu erstellen und zu managen.
- compute.networks.get - compute.networks.list - Compute.Regions.get - Compute.Regions.list - Compute.subNetworks.get - Compute.subNetworks.list - Compute.zoneOperations.get - Compute.Zones.get - Compute.Zones.list	Um die Netzwerkinformationen zu erhalten, die für die Erstellung einer neuen Instanz einer Cloud Volumes ONTAP Virtual Machine erforderlich sind.
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - istmentmanager.Manifeste.get - istmentmanager.manifeste.list - istmentmanager.Operations.get - istmentmanager.Operations.list - bereitsmanager.Resources.get - bereitsmanager.Resources.list - Bereitstellungmanager.typeProviders.get - istmentmanager.tyArten.list	Um die Cloud Volumes ONTAP VM-Instanz mithilfe von Google Cloud Deployment Manager bereitzustellen.
- Logging.logEntries.list - Logging.privateLogEntries.list	Zum Abrufen von Stack-Protokolllaufwerken.
- resourcemanager.projects.get	Zur Unterstützung mehrerer Projekte.
- Storage.Buckets.create - storage.buckets.delete - Storage.Buckets.get - Storage.Buckets.list - Storage.Buckets.Update	Zur Erstellung und Verwaltung eines Google Cloud Storage Buckets für Daten-Tiering
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.kryptoKeys.get - cloudkms.kryptoKeys.list - cloudkms.Keyrings.list	Verwenden von vom Kunden gemanagten Verschlüsselungen aus dem Cloud-Verschlüsselungsmanagement-Service mit Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list	So legen Sie ein Servicekonto für die Cloud Volumes ONTAP-Instanz fest: Dieses Servicekonto bietet Berechtigungen für Daten-Tiering zu einem Google Cloud Storage Bucket.

AWS Marketplace-Seiten für Cloud Manager und Cloud Volumes ONTAP

Im AWS Marketplace für Cloud Manager und Cloud Volumes ONTAP sind diverse Angebote erhältlich. Wenn Sie Hilfe zum Verständnis des Zwecks jeder Seite benötigen, lesen Sie die Beschreibungen unten.

Vergessen Sie in jedem Fall nicht, dass Sie Cloud Volumes ONTAP nicht über den AWS Marketplace in AWS starten können. Sie müssen es direkt über Cloud Manager starten.

Ziel	Zu verwendende AWS Marketplace Seite	Weitere Informationen
Ermöglichen Sie die Nutzung von Cloud Volumes ONTAP PAYGO, Cloud Tiering, Cloud Compliance und anderen Add-on-Services	"Cloud Manager – Implementierung und Management von NetApp Cloud Data Services"	Mit diesem Abonnement können Sie die PAYGO-Version von Cloud Volumes ONTAP 9.6 und höher berechnen. Es ermöglicht zudem eine Abrechnung auf Cloud Tiering, Cloud Compliance und weitere Add-on-Services. Sie sollten dieses Angebot abonnieren, wenn Sie von Cloud Manager aufgefordert werden und Sie zur Seite umgeleitet werden. Cloud Manager fordert Sie auf, sich im Assistenten für die Arbeitsumgebung zu befinden oder neue Anmeldedaten in den Einstellungen hinzuzufügen. Auf dieser Seite können Sie Cloud Manager nicht in AWS starten. Das sollte von geschehen "NetApp Cloud Central", Oder alternativ das AMI in Zeile 3 dieser Tabelle verwenden.
Ermöglichen Sie die Nutzung von Cloud Volumes ONTAP-PAYGO, Cloud Tiering, Cloud Compliance und anderen Add-on-Services *unter Verwendung eines jährlichen Vertrags*	"Cloud Manager (Verträge) – Deploy amp; Manage NetApp Cloud Data Services"	Dieses Abonnement ist eine Alternative zum Abonnement in der ersten Zeile. Es ermöglicht Ihnen, eine jährliche Vorauszahlung für die Angebote zu erhalten. Das gilt vor allem für NetApp Partner.
Implementieren Sie Cloud Manager über AWS Marketplace über ein AMI	"Cloud Manager - Manuelle Installation ohne Zugriffsschlüssel"	Wir empfehlen Ihnen, Cloud Manager in AWS ab zu starten "NetApp Cloud Central", Aber Sie können es auf dieser AWS Marketplace Seite starten, wenn Sie es bevorzugen.
Implementierung von Cloud Volumes ONTAP PAYGO (9.5 oder früher) ermöglichen	• "Cloud Volumes ONTAP für AWS" • "Cloud Volumes ONTAP für AWS – Hochverfügbarkeit"	Auf diesen AWS Marketplace-Seiten können Sie für Version 9.5 und früher die Single Node- oder HA-Versionen von Cloud Volumes ONTAP PAYGO abonnieren. Ab Version 9.6 müssen Sie die Anmeldung über die in Zeile 1 dieser Tabelle aufgeführten AWS Marketplace-Seite für PAYGO-Implementierungen durchführen.

Verwendung von APIs und Automatisierung

Automatisierungsressourcen 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. Ein solches Werkzeug ist Terraform. Wir haben einen Terraform-Provider entwickelt, den DevOps-Teams mit Cloud Manager verwenden können, um Cloud Volumes ONTAP zu automatisieren und mit Infrastruktur als Code zu integrieren.

"Hier finden Sie den netapp-Cloudmmanager Provider".

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"

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.

- "NetApp Cloud Volumes ONTAP Support"

  Greifen Sie auf Support-Ressourcen zu, um Hilfe zu erhalten und Probleme mit Cloud Volumes ONTAP zu beheben.

- "Videos für Cloud Manager und Cloud Volumes ONTAP"

  In diesem Video sehen Sie, wie Sie Cloud Volumes ONTAP implementieren und managen und wie Sie Daten in Ihrer gesamten Hybrid Cloud replizieren.

- "Richtlinien für Cloud Manager"

  Laden Sie JSON-Dateien herunter, die die Berechtigungen enthalten, die Cloud Manager für Aktionen in einem Cloud-Provider benötigt.

- "Cloud Manager API-Entwicklerleitfaden"

  Lesen Sie einen Überblick über die APIs, Beispiele für deren Verwendung und eine API-Referenz.

- Training für Cloud Volumes ONTAP
  - "Grundlagen von Cloud Volumes ONTAP"
  - "Implementierung und Management von Cloud Volumes ONTAP für Azure"
  - "Implementierung und Management von Cloud Volumes ONTAP für AWS"
- Technische Berichte
  - "NetApp Technical Report 4383: Performance Characterization of Cloud Volumes ONTAP in Amazon Web Services with Application Workloads"
  - "Technischer Bericht von NetApp 4671: Performance-Charakterisierung von Cloud Volumes ONTAP in Azure mit Applikations-Workloads"
  - "Technischer Bericht 4816: Performance-Merkmale von Cloud Volumes ONTAP für Google Cloud"
- Disaster Recovery für SVM

  Bei der SVM Disaster Recovery wird die asynchrone Spiegelung von SVM-Daten und -Konfiguration von einer Quell-SVM zu einer Ziel-SVM erstellt. Sie können eine Ziel-SVM für den Datenzugriff schnell aktivieren, wenn die Quell-SVM nicht mehr verfügbar ist.

  - "Cloud Volumes ONTAP 9 SVM Disaster Recovery Preparation Express-Leitfaden"

    Beschreibt, wie eine Ziel-SVM zur Vorbereitung auf die Disaster Recovery schnell konfiguriert wird.

  - "Cloud Volumes ONTAP 9 SVM Disaster Recovery Express Guide"

    Beschreibt, wie Sie eine Ziel-SVM nach einem Notfall schnell aktivieren und dann die Quell-SVM erneut aktivieren.

- "FlexCache Volumes für schnelleren Datenzugriff – Power Guide"

Beschreibt, wie FlexCache Volumes in demselben Cluster oder verschiedenen Clustern erstellt und gemanagt werden, um den Datenzugriff zu beschleunigen.

- "Sicherheitsratschläge"

  Bekannte Schwachstellen (CVEs) für NetApp Produkte, einschließlich ONTAP ermitteln Beachten Sie, dass Sie Sicherheitslücken bei Cloud Volumes ONTAP mithilfe der folgenden ONTAP Dokumentation beheben können.

- "ONTAP 9 Dokumentationszentrum"

  Greifen Sie auf die Produktdokumentation für ONTAP zu, die Ihnen bei der Verwendung von Cloud Volumes ONTAP helfen kann.

- "NetApp Community: Cloud Data Services"

  Tauschen Sie sich mit Kollegen aus, stellen Sie Fragen, tauschen Sie Ideen aus, suchen Sie nach Ressourcen und tauschen Sie Best Practices aus.

- "NetApp Cloud Central"

  Hier finden Sie weitere Informationen zu NetApp Produkten und Lösungen für die Cloud.

- "NetApp Produktdokumentation"

  In der NetApp Produktdokumentation finden Sie Anleitungen, Ressourcen und Antworten.

Frühere Versionen der Cloud Manager-Dokumentation

Dokumentation für vorherige Versionen von Cloud Manager steht zur Verfügung, falls Sie die neueste Version nicht ausführen.

- "Cloud Manager 3.7"
- "Cloud Manager 3.6"

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

http://www.netapp.com/us/legal/copyright.aspx

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/us/media/patents-page.pdf

Datenschutzrichtlinie

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

- "Hinweis zu Cloud Manager 3.8.7"
- "Hinweis zu Cloud Manager 3.8.6"
- "Hinweis zu Cloud Manager 3.8.5"
- "Hinweis zu Cloud Manager 3.8.4"
- "Hinweis zu Cloud Manager 3.8.3"
- "Hinweis zu Cloud Manager 3.8.2"
- "Hinweis zu Cloud Manager 3.8.1"
- "Hinweis zu Cloud Manager 3.8"
- "Hinweis zum Cloud Backup Service"
- "Hinweis für Global File Cache"
- "Hinweis zu Cloud Compliance"