Cloud Volumes ONTAP-Dokumentation

Cloud Volumes ONTAP

NetApp
June 11, 2024

Inhalt

Cloud Volumes ONTAP-Dokumentation

Versionshinweise

Was ist neu

Erfahren Sie mehr über Neuerungen beim Cloud Volumes ONTAP Management in BlueXP.

Die auf dieser Seite beschriebenen Verbesserungen beziehen sich nur auf BlueXP-Funktionen, die das Management von Cloud Volumes ONTAP ermöglichen. Lesen Sie, was mit der Cloud Volumes ONTAP Software selbst neu ist, "Wechseln Sie zu den Versionshinweisen zu Cloud Volumes ONTAP"

10 Juni 2024

Cloud Volumes ONTAP 9.15.0

BlueXP kann jetzt Cloud Volumes ONTAP 9.15.0 in AWS, Azure und Google Cloud implementieren und managen.

"Erfahren Sie mehr über die neuen Funktionen in dieser Version von Cloud Volumes ONTAP".

17 Mai 2024

Unterstützung von Amazon Web Services Local Zones

Für Cloud Volumes ONTAP HA-Implementierungen ist jetzt Unterstützung für AWS Local Zones verfügbar. AWS Local Zones sind eine Infrastrukturimplementierung, bei der Storage, Computing, Datenbanken und andere ausgewählte AWS Services in der Nähe von großen Städten und Branchenbereichen liegen.

> AWS Local Zones werden beim Einsatz von BlueXP im Standardmodus unterstützt. Derzeit werden AWS Lokale Zonen nicht unterstützt, wenn BlueXP im eingeschränkten Modus oder im privaten Modus verwendet wird.

Weitere Informationen zu AWS Local Zones mit HA-Implementierungen finden Sie unter "AWS lokale Zonen".

Bis 23. April 2024

Unterstützung neuer Regionen für Implementierungen mit mehreren Verfügbarkeitszonen in Azure

Die folgenden Regionen unterstützen jetzt HA-Implementierungen mit mehreren Verfügbarkeitszonen in Azure für Cloud Volumes ONTAP 9.12.1 GA und höher:

- Deutschland West Central
- Polen, Mitte
- USA, Westen 3
- Israel, Mitte
- Italien Nord
- Kanada Mitte

Eine Liste aller Regionen finden Sie im "Karte der globalen Regionen unter Azure".

Johannesburg Region jetzt in Google Cloud unterstützt

Der Region Johannesburg (`africa-south1` Wird jetzt in Google Cloud für Cloud Volumes ONTAP 9.12.1 GA und höher unterstützt.

Eine Liste aller Regionen finden Sie im "Karte der globalen Regionen unter Google Cloud".

Volume-Vorlagen und -Tags werden nicht mehr unterstützt

Sie können kein Volume mehr aus einer Vorlage erstellen oder die Tags eines Volumes bearbeiten. Diese Aktionen wurden mit dem BlueXP Korrekturservice verknüpft, der nicht mehr verfügbar ist.

8 März 2024

Unterstützung für Amazon Instant Metadata Service v2

In AWS unterstützen Cloud Volumes ONTAP, der Mediator und der Connector nun den Amazon Instant Metadata Service v2 (IMDSv2) für alle Funktionen. IMDSv2 bietet einen verbesserten Schutz vor Schwachstellen. Bisher wurde nur IMDSv1 unterstützt.

Falls von Ihren Sicherheitsrichtlinien gefordert, können Sie Ihre EC2-Instanzen für die Verwendung von IMDSv2 konfigurieren. Anweisungen finden Sie unter "BlueXP Installations- und Administrationsdokumentation für das Management vorhandener Connectors".

5 März 2024

Cloud Volumes ONTAP 9.14.1 GA

BlueXP kann jetzt Cloud Volumes ONTAP 9.14.1 General Availability Release in AWS, Azure und Google Cloud implementieren und managen.

2 Februar 2024

Unterstützung für VMs der Edv5-Serie in Azure

Cloud Volumes ONTAP unterstützt ab Version 9.14.1 jetzt die folgenden VMs der Edv5-Serie.

- E4ds_v5
- E8ds_v5
- E20s_v5
- E32ds_v5
- E48ds_v5
- E64ds_v5

"Unterstützte Konfigurationen in Azure"

16 Januar 2024

Patch-Versionen in BlueXP

Patch-Releases sind in BlueXP nur für die drei neuesten Cloud Volumes ONTAP Versionen verfügbar.

"Upgrade von Cloud Volumes ONTAP"

8 Januar 2024

Neue VMs für Azure: Mehrere Verfügbarkeitszonen

Ab Cloud Volumes ONTAP 9.13.1 unterstützen die folgenden VM-Typen Azure mehrere Verfügbarkeitszonen für neue und bestehende Implementierungen von Hochverfügbarkeitspaaren:

- L16s_v3
- L32s_v3
- L48s_v3
- L64s_v3

"Unterstützte Konfigurationen in Azure"

Bis 6. Dezember 2023

Cloud Volumes ONTAP 9.14.1 RC1

BlueXP kann jetzt Cloud Volumes ONTAP 9.14.1 in AWS, Azure und Google Cloud implementieren und managen.

"Erfahren Sie mehr über die neuen Funktionen in dieser Version von Cloud Volumes ONTAP".

Max. Limit von 300 tib FlexVol-Volumes

Erstellen Sie jetzt ein FlexVol Volume bis zu einer Maximalgröße von 300 tib mit System Manager und der ONTAP CLI ab Cloud Volumes ONTAP 9.12.1 P2 und 9.13.0 P2 sowie in BlueXP ab Cloud Volumes ONTAP 9.13.1.

- "Storage-Grenzen in AWS"
- "Storage-Grenzen in Azure"
- "Storage-Grenzen in Google Cloud"

Bis 5. Dezember 2023

Folgende Änderungen wurden eingeführt.

Neue regionale Unterstützung in Azure

Unterstützung einer einzelnen Verfügbarkeitszone

Die folgenden Regionen unterstützen jetzt hochverfügbare Einzelverfügbarkeitszonen-Implementierungen in Azure für Cloud Volumes ONTAP 9.12.1 GA und höher:

- Tel Aviv
- Mailand

Unterstützung mehrerer Verfügbarkeitszonen

Die folgenden Regionen unterstützen jetzt hochverfügbare Implementierungen mit mehreren Verfügbarkeitszonen in Azure für Cloud Volumes ONTAP 9.12.1 GA und höher:

- Zentralindien
- Norwegen Osten
- Schweiz Nord
- Südafrika, Norden
- Vereinigte Arabische Emirate Nord
- China Nord 3

Eine Liste aller Regionen finden Sie im "Karte der globalen Regionen unter Azure".

Bis 10. November 2023

Die folgende Änderung wurde mit der Version 3.9.35 des Connectors eingeführt.

Berlin Region jetzt in Google Cloud unterstützt

Die Region Berlin wird jetzt in Google Cloud für Cloud Volumes ONTAP 9.12.1 GA und höher unterstützt.

Eine Liste aller Regionen finden Sie im "Karte der globalen Regionen unter Google Cloud".

Bis 8. November 2023

Die folgende Änderung wurde mit der Version 3.9.35 des Connectors eingeführt.

Die Region Tel Aviv wird jetzt in AWS unterstützt

Die Region Tel Aviv wird jetzt in AWS für Cloud Volumes ONTAP 9.12.1 GA und höher unterstützt.

Eine Liste aller Regionen finden Sie im "Karte der globalen Regionen unter AWS".

November 2023

Die folgende Änderung wurde mit der Version 3.9.34 des Connectors eingeführt.

Saudi-Arabien Region jetzt in Google Cloud unterstützt

Die Region Saudi-Arabien wird jetzt in Google Cloud für Cloud Volumes ONTAP und dem Connector für Cloud Volumes ONTAP 9.12.1 GA und später unterstützt.

Eine Liste aller Regionen finden Sie im "Karte der globalen Regionen unter Google Cloud".

23 Oktober 2023

Die folgende Änderung wurde mit der Version 3.9.34 des Connectors eingeführt.

Unterstützung neuer Regionen für HA-Implementierungen mit mehreren Verfügbarkeitszonen in Azure

Die folgenden Regionen in Azure unterstützen jetzt hochverfügbare Implementierungen mit mehreren Verfügbarkeitszonen für Cloud Volumes ONTAP 9.12.1 GA und höher:

- Australien Ost
- Ostasien
- Frankreich, Mitte
- Nordeuropa
- Qatar Central
- Schweden, Mitte
- Westeuropa
- West USA 2

Eine Liste aller Regionen, die mehrere Verfügbarkeitszonen unterstützen, finden Sie im "Karte der globalen Regionen unter Azure".

6 Oktober 2023

Die folgende Änderung wurde mit der Version 3.9.34 des Connectors eingeführt.

Cloud Volumes ONTAP 9.14.0

BlueXP kann jetzt die Cloud Volumes ONTAP 9.14.0 General Availability Version in AWS, Azure und Google Cloud implementieren und managen.

"Erfahren Sie mehr über die neuen Funktionen in dieser Version von Cloud Volumes ONTAP".

10 September 2023

Die folgende Änderung wurde mit der Version 3.9.33 des Connectors eingeführt.

Unterstützung für VMs der Lsv3-Serie in Azure

Die Instanztypen L48s_v3 und L64s_v3 werden nun mit Cloud Volumes ONTAP in Azure unterstützt. Dies gilt für Single-Node- und Hochverfügbarkeitspaare-Implementierungen mit gemeinsam genutzten verwalteten Festplatten in einzelnen und mehreren Verfügbarkeitszonen, beginnend mit Version 9.13.1. Diese Instanztypen unterstützen Flash Cache.

"Zeigen Sie unterstützte Konfigurationen für Cloud Volumes ONTAP in Azure an"
"Storage-Limits für Cloud Volumes ONTAP in Azure anzeigen"

30 Juli 2023

Die folgenden Änderungen wurden mit der Version 3.9.32 des Connectors eingeführt.

Flash Cache und Unterstützung für High-Write-Geschwindigkeit in Google Cloud

Flash Cache und hohe Schreibgeschwindigkeit können separat in Google Cloud für Cloud Volumes ONTAP 9.13.1 und höher aktiviert werden. Bei allen unterstützten Instanztypen ist eine hohe Schreibgeschwindigkeit verfügbar. Flash Cache wird in den folgenden Instanztypen unterstützt:

- n2-Standard-16
- n2-Standard-32
- n2-Standard-48
- n2-Standard-64

Diese Funktionen können einzeln oder gemeinsam auf Single Node-Implementierungen und Hochverfügbarkeitspaaren eingesetzt werden.

"Starten Sie Cloud Volumes ONTAP in Google Cloud"

Verbesserte Nutzungsberichte

Verschiedene Verbesserungen der angezeigten Informationen in den Nutzungsberichten sind jetzt verfügbar. Die folgenden Verbesserungen an den Nutzungsberichten:

- Die tib-Einheit ist jetzt im Namen der Spalten enthalten.
- Das neue Feld „Node(s)“ für die Seriennummern ist jetzt enthalten.
- Der Bericht zur Auslastung von Storage-VMs enthält jetzt eine neue Spalte „Workload-Typ“.
- Namen der Arbeitsumgebung, die jetzt in Berichten zu Storage-VMs und Volume-Nutzung enthalten sind
- Volume-Typ „File“ ist jetzt mit „Primary (Read/Write)“ beschriftet.
- Volume-Typ „sekundär“ ist jetzt mit der Bezeichnung „sekundär (DP)“ gekennzeichnet.

Weitere Informationen zu Nutzungsberichten finden Sie unter "Nutzungsberichte herunterladen".

26 Juli 2023

Die folgenden Änderungen wurden mit der Version 3.9.31 des Connectors eingeführt.

Cloud Volumes ONTAP 9.13.1 GA

BlueXP kann jetzt die Cloud Volumes ONTAP 9.13.1 General Availability Version in AWS, Azure und Google Cloud implementieren und managen.

"Erfahren Sie mehr über die neuen Funktionen in dieser Version von Cloud Volumes ONTAP".

2 Juli 2023

Die folgenden Änderungen wurden mit der Version 3.9.31 des Connectors eingeführt.

Unterstützung für HA-Implementierungen mit mehreren Verfügbarkeitszonen in Azure

Der japanische Osten und Korea Zentral in Azure unterstützen jetzt HA-Implementierungen mit mehreren Verfügbarkeitszonen für Cloud Volumes ONTAP 9.12.1 GA und höher.

Eine Liste aller Regionen, die mehrere Verfügbarkeitszonen unterstützen, finden Sie im "Karte der globalen Regionen unter Azure".

Unterstützung für autonomen Ransomware-Schutz

Autonomous Ransomware Protection (ARP) wird jetzt auf Cloud Volumes ONTAP unterstützt. ARP-Unterstützung ist auf Cloud Volumes ONTAP Version 9.12.1 und höher verfügbar.

Weitere Informationen über ARP with Cloud Volumes ONTAP finden Sie unter "Autonomer Schutz Durch Ransomware".

26 Juni 2023

Die folgende Änderung wurde mit der Version 3.9.30 des Connectors eingeführt.

Cloud Volumes ONTAP 9.13.1 RC1

BlueXP kann jetzt Cloud Volumes ONTAP 9.13.1 in AWS, Azure und Google Cloud implementieren und managen.

"Erfahren Sie mehr über die neuen Funktionen in dieser Version von Cloud Volumes ONTAP".

4 Juni 2023

Die folgende Änderung wurde mit der Version 3.9.30 des Connectors eingeführt.

Aktualisierung der Cloud Volumes ONTAP-Upgrade-Versionsauswahl

Auf der Seite Upgrade Cloud Volumes ONTAP können Sie jetzt wählen, ob Sie ein Upgrade auf die neueste verfügbare Version von Cloud Volumes ONTAP oder eine ältere Version durchführen möchten.

Weitere Informationen zum Upgrade von Cloud Volumes ONTAP über BlueXP finden Sie unter "Upgrade von Cloud Volumes ONTAP".

7 Mai 2023

Die folgenden Änderungen wurden mit der Version 3.9.29 des Connectors eingeführt.

Katar unterstützt jetzt in Google Cloud

Die Region Katar wird jetzt in Google Cloud für Cloud Volumes ONTAP und dem Connector für Cloud Volumes ONTAP 9.12.1 GA und höher unterstützt.

Schweden Zentralregion jetzt in Azure unterstützt

Die Zentralregion Schweden wird jetzt in Azure für Cloud Volumes ONTAP und der Connector für Cloud Volumes ONTAP 9.12.1 GA und höher unterstützt.

Unterstützung für Implementierungen mit mehreren Verfügbarkeitszonen in Azure Australia East

Die Region Australien/Osten in Azure unterstützt jetzt HA-Implementierungen mit mehreren Verfügbarkeitszonen für Cloud Volumes ONTAP 9.12.1 GA und höher.

Aufladeaufschlüsselung

Jetzt finden Sie heraus, für welche Gebühren Sie zahlen, wenn Sie kapazitätsbasierte Lizenzen abonniert haben. Die folgenden Nutzungsberichte können aus dem Digital Wallet in BlueXP heruntergeladen werden. Die Nutzungsberichte enthalten Kapazitätsdetails zu Ihren Abonnements und geben an, wie Sie für die Ressourcen in Ihren Cloud Volumes ONTAP Abonnements in Rechnung gestellt werden. Die herunterladbaren Berichte können leicht mit anderen geteilt werden.

- Verwendung des Cloud Volumes ONTAP-Pakets
- Allgemeine Nutzung
- Verwendung von Storage VMs
- Volumennutzung

Weitere Informationen finden Sie unter "Management kapazitätsbasierter Lizenzen".

Wenn Sie ohne Marketplace-Abonnement auf BlueXP zugreifen, wird jetzt eine Benachrichtigung angezeigt

Sobald Sie ohne Marketplace-Abonnement auf Cloud Volumes ONTAP in BlueXP zugreifen, wird jetzt eine Benachrichtigung angezeigt. Die Benachrichtigung besagt, dass „ein Marketplace-Abonnement für diese Arbeitsumgebung erforderlich ist, um die Cloud Volumes ONTAP-Bedingungen zu erfüllen."

Bis 4. April 2023

Ab Cloud Volumes ONTAP 9.12.1 GA werden China-Regionen jetzt wie folgt in AWS unterstützt.

- Systeme mit Single Node werden unterstützt.
- Lizenzen, die direkt von NetApp erworben wurden, werden unterstützt.

Informationen zur regionalen Verfügbarkeit finden Sie unter "Karten für globale Regionen für Cloud Volumes ONTAP".

Bis 3. April 2023

Die folgenden Änderungen wurden mit der Version 3.9.28 des Connectors eingeführt.

Turin Region jetzt in Google Cloud unterstützt

Die Region Turin wird jetzt in Google Cloud für Cloud Volumes ONTAP und dem Connector für Cloud Volumes ONTAP 9.12.1 GA und höher unterstützt.

Erweiterung der digitalen Wallet von BlueXP

Das Digital Wallet von BlueXP zeigt jetzt die lizenzierte Kapazität an, die Sie mit privaten Marketplace-Angeboten erworben haben.

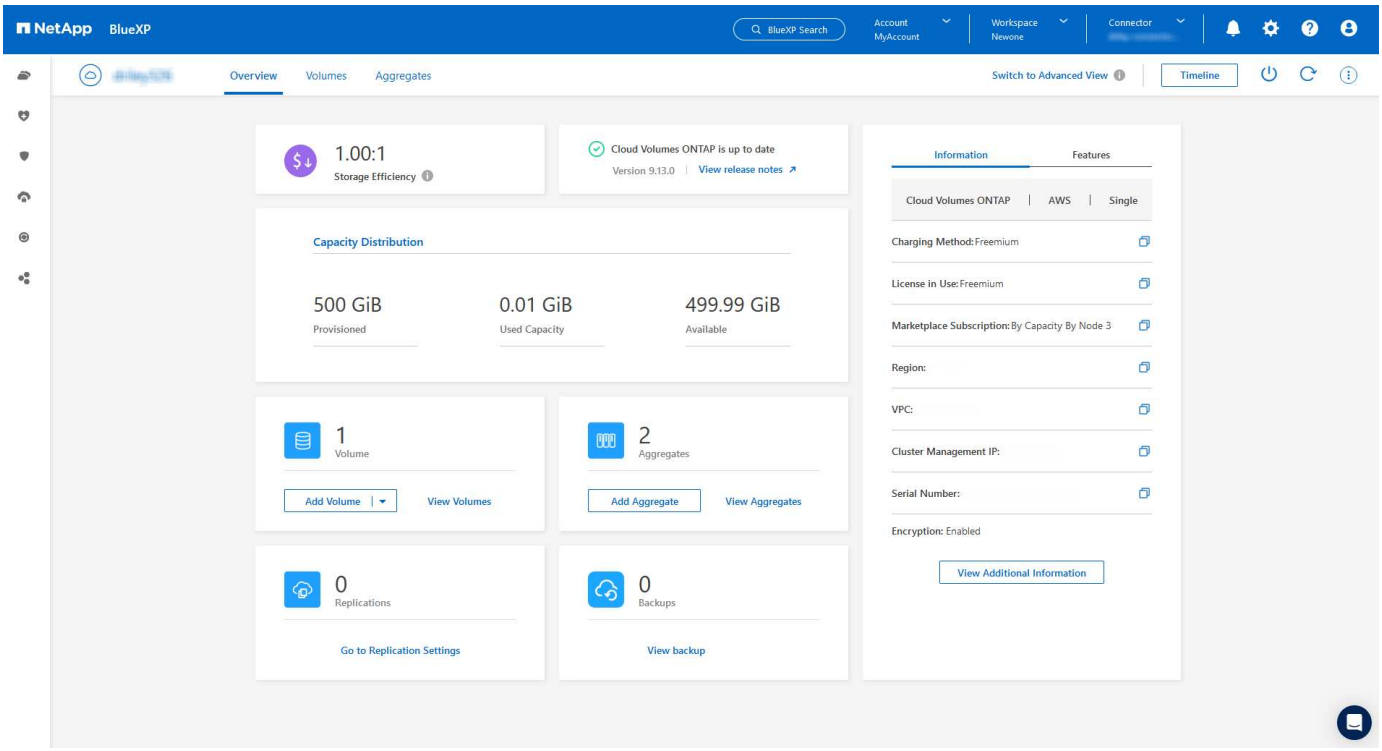
"Erfahren Sie, wie Sie die verbrauchte Kapazität in Ihrem Konto anzeigen".

Unterstützung für Kommentare während der Volume-Erstellung

Mit diesem Release können Sie bei der Erstellung eines Cloud Volumes ONTAP FlexGroup Volumes oder FlexVol Volumes unter Verwendung der API Kommentare abgeben.

Umgestaltung der Benutzeroberfläche von BlueXP für Cloud Volumes ONTAP Übersichtsseiten, Volumes und Aggregationsseiten

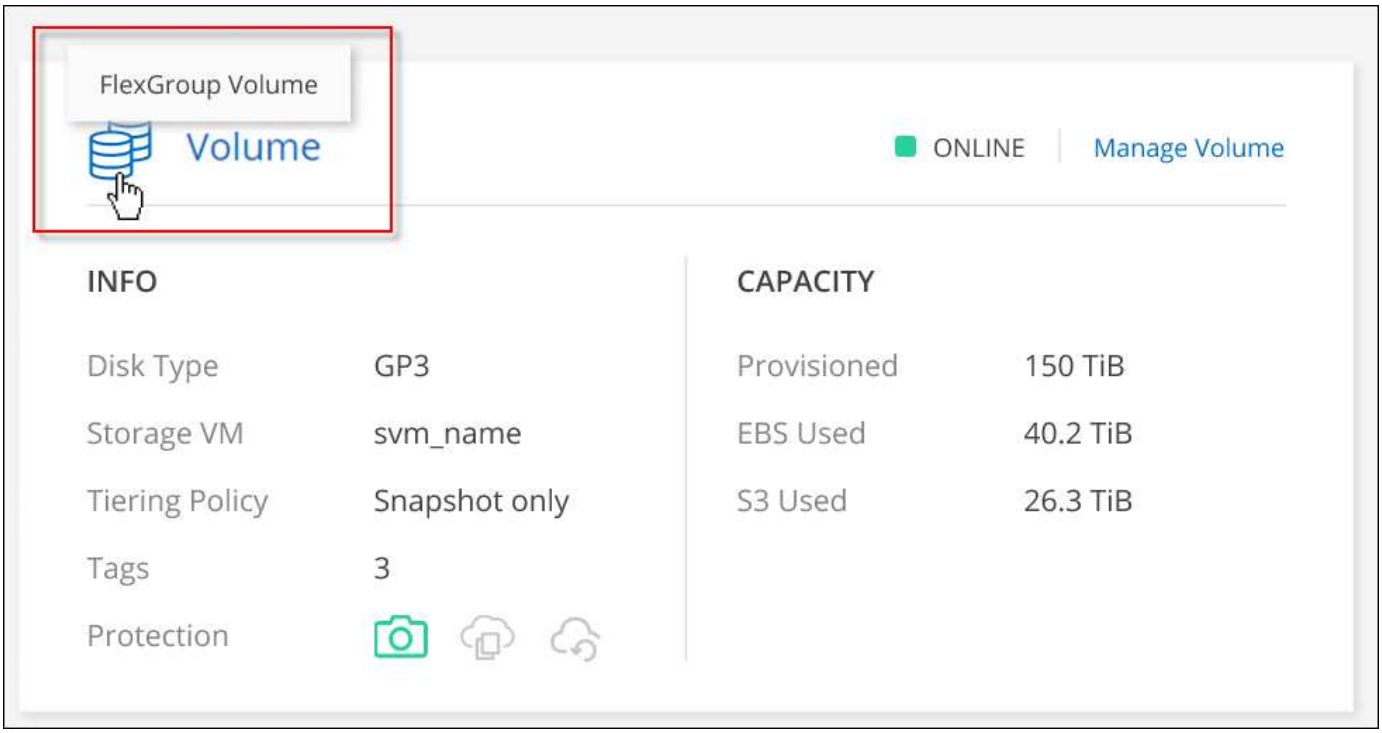
BlueXP hat jetzt eine neu gestaltete Benutzeroberfläche für die Seiten „Cloud Volumes ONTAP Übersicht", „Volumes" und „Aggregate" überarbeitet. Das auf Kacheln basierende Design präsentiert umfassendere Informationen in jeder Kachel für eine bessere Benutzererfahrung.



FlexGroup Volumes können mit Cloud Volumes ONTAP angezeigt werden

FlexGroup Volumes, die direkt über CLI oder System Manager erstellt wurden, sind nun über die neu gestaltete Volume-Kachel in BlueXP sichtbar. Ähnlich wie bei FlexVol Volumes bietet BlueXP über eine dedizierte Volume-Kachel detaillierte Informationen zu erstellten FlexGroup Volumes.

Derzeit können Sie vorhandene FlexGroup Volumes nur unter BlueXP anzeigen. Die Möglichkeit zum Erstellen von FlexGroup Volumes in BlueXP ist nicht verfügbar, aber für eine zukünftige Version geplant.



"Erfahren Sie mehr über das Anzeigen von erstellten FlexGroup Volumes."

13 März 2023

Unterstützung der Region China

Ab Cloud Volumes ONTAP 9.12.1 GA wird die Unterstützung für China-Regionen jetzt wie folgt in Azure unterstützt.

- Cloud Volumes ONTAP wird in China Nord 3 unterstützt.
- Systeme mit Single Node werden unterstützt.
- Lizenzen, die direkt von NetApp erworben wurden, werden unterstützt.

Informationen zur regionalen Verfügbarkeit finden Sie unter "Karten für globale Regionen für Cloud Volumes ONTAP".

5 März 2023

Die folgenden Änderungen wurden mit der Version 3.9.27 des Connectors eingeführt.

Cloud Volumes ONTAP 9.13.0

BlueXP kann jetzt Cloud Volumes ONTAP 9.13.0 in AWS, Azure und Google Cloud implementieren und managen.

"Erfahren Sie mehr über die neuen Funktionen in dieser Version von Cloud Volumes ONTAP".

Unterstützung für 16 tib und 32 TIB in Azure

Cloud Volumes ONTAP unterstützt jetzt 16 tib und 32 tib Festplatten für Hochverfügbarkeitsimplementierungen auf verwalteten Festplatten in Azure.

Weitere Informationen zu "Unterstützte Festplattengrößen in Azure".

MTEKM-Lizenz

Die MTEKM-Lizenz (Multi-Tenant Encryption Key Management) ist jetzt auch in neuen und bestehenden Cloud Volumes ONTAP Systemen mit Version 9.12.1 GA oder höher enthalten.

Das mandantenfähige externe Verschlüsselungsmanagement ermöglicht individuelle Storage VMs (SVMs) beim Einsatz von NetApp Volume Encryption, ihre eigenen Schlüssel über einen KMIP Server beizubehalten.

"So verschlüsseln Sie Volumes mit NetApp Verschlüsselungslösungen".

Unterstützung für Umgebungen ohne Internet

Cloud Volumes ONTAP wird jetzt in allen Cloud-Umgebungen unterstützt, die vollständig vom Internet isoliert sind. In diesen Umgebungen wird nur Node-basierte Lizenzierung (BYOL) unterstützt. Kapazitätsbasierte Lizenzierung wird nicht unterstützt. Um zu beginnen, installieren Sie die Connector Software manuell, melden Sie sich bei der BlueXP Konsole an, die auf dem Connector ausgeführt wird, fügen Sie Ihre BYOL-Lizenz zur BlueXP Digital Wallet hinzu und implementieren Sie dann Cloud Volumes ONTAP.

- "Installieren Sie den Connector an einem Ort ohne Internetzugang"

- "Greifen Sie über den Connector auf die BlueXP Konsole zu"
- "Fügen Sie eine nicht zugewiesene Lizenz hinzu"

Flash Cache und hohe Schreibgeschwindigkeit in Google Cloud

Ab Version Cloud Volumes ONTAP 9.13.0 werden Flash Cache, hohe Schreibgeschwindigkeit und eine High Maximum Transmission Unit (MTU) von 8,896 Byte unterstützt.

Weitere Informationen zu "Unterstützte Konfigurationen per Lizenz für Google Cloud".

5 Februar 2023

Die folgenden Änderungen wurden mit der Version 3.9.26 des Connectors eingeführt.

Erstellung von Platzierungsgruppen in AWS

Für die Erstellung von Platzierungsgruppen ist jetzt eine neue Konfigurationseinstellung mit AWS HA-Implementierung in einer Verfügbarkeitszone (AZ) verfügbar. Jetzt können Kunden ausgefallene Platzierungsgruppen umgehen und die erfolgreiche Implementierung von AWS HA-einzelnen AZ ermöglichen.

Ausführliche Informationen zum Konfigurieren der Einstellung für die Erstellung von Platzierungsgruppen finden Sie unter "Konfiguration der Erstellung von Platzierungsgruppen für AWS HA Single AZ".

Aktualisierung der Konfiguration der privaten DNS-Zone

Eine neue Konfigurationseinstellung ist jetzt verfügbar, sodass Sie bei der Verwendung von Azure Private Links vermeiden können, eine Verbindung zwischen einer privaten DNS-Zone und einem virtuellen Netzwerk zu erstellen. Die Erstellung ist standardmäßig aktiviert.

"Stellen Sie BlueXP Einzelheiten zu Ihrem Azure Private DNS zur Verfügung"

WORM-Storage und Daten-Tiering

Sie können jetzt bei der Erstellung eines Cloud Volumes ONTAP 9.8 Systems oder höher sowohl Daten-Tiering als AUCH WORM-Storage gemeinsam aktivieren. Wenn Sie Daten-Tiering mit WORM-Storage aktivieren, können Sie die Daten auf einen Objektspeicher in der Cloud verschieben.

"Erfahren Sie mehr über WORM Storage."

Januar 2023

Die folgenden Änderungen wurden mit der Version 3.9.25 des Connectors eingeführt.

Lizenzierungspakete in Google Cloud verfügbar

Optimierte und kapazitätsbasierte Edge Cache Lizenzpakete stehen für Cloud Volumes ONTAP im Google Cloud Marketplace als Pay-as-you-go-Angebot oder als Jahresvertrag zur Verfügung.

Siehe "Cloud Volumes ONTAP Lizenzierung".

Standardkonfiguration für Cloud Volumes ONTAP

Die MTEKM-Lizenz (Multi-Tenant Encryption Key Management) ist in neuen Cloud Volumes ONTAP Implementierungen nicht mehr enthalten.

Weitere Informationen zu den automatisch mit Cloud Volumes ONTAP installierten ONTAP-Funktionslizenzen finden Sie unter "Standardkonfiguration für Cloud Volumes ONTAP".

Bis 15. Dezember 2022

Cloud Volumes ONTAP 9.12.0

BlueXP kann jetzt Cloud Volumes ONTAP 9.12.0 in AWS und Google Cloud implementieren und verwalten.

"Erfahren Sie mehr über die neuen Funktionen in dieser Version von Cloud Volumes ONTAP".

Bis 8. Dezember 2022

Cloud Volumes ONTAP 9.12.1

BlueXP kann jetzt Cloud Volumes ONTAP 9.12.1 implementieren und verwalten, was auch Unterstützung für neue Funktionen und zusätzliche Regionen von Cloud-Providern umfasst.

"Erfahren Sie mehr über die neuen Funktionen in dieser Version von Cloud Volumes ONTAP"

Bis 4. Dezember 2022

Die folgenden Änderungen wurden mit der Version 3.9.24 des Connectors eingeführt.

WORM + Cloud Backup sind jetzt bei der Cloud Volumes ONTAP-Erstellung verfügbar

Im Rahmen der Cloud Volumes ONTAP-Erstellung können DIE Funktionen für WORM (Write Once, Read Many) und Cloud Backup aktiviert werden.

Israel Region jetzt in Google Cloud unterstützt

Die Region Israel wird nun in Google Cloud für Cloud Volumes ONTAP und der Connector für Cloud Volumes ONTAP 9.11.1 P3 und höher unterstützt.

15. November 2022

Die folgenden Änderungen wurden mit der Version 3.9.23 des Connectors eingeführt.

ONTAP S3-Lizenz in Google Cloud

Eine ONTAP S3 Lizenz ist jetzt auf neuen und vorhandenen Cloud Volumes ONTAP Systemen mit Version 9.12.1 oder höher in der Google Cloud Platform enthalten.

"Lesen Sie, wie Sie S3-Objekt-Storage-Services in ONTAP konfigurieren und managen"

6. November 2022

Die folgenden Änderungen wurden mit der Version 3.9.23 des Connectors eingeführt.

Verschieben von Ressourcengruppen in Azure

Sie können nun eine Arbeitsumgebung innerhalb desselben Azure Abonnements von einer Ressourcengruppe auf eine andere Ressourcengruppe in Azure verschieben.

Weitere Informationen finden Sie unter "Verschieben von Ressourcengruppen".

NDMP-Kopie-Zertifizierung

NDMP-Copy ist jetzt für die Verwendung mit Cloud Volume ONTAP zertifiziert.

Weitere Informationen zum Konfigurieren und Verwenden von NDMP finden Sie unter "NDMP-Konfiguration – Überblick".

Unterstützung der gemanagten Festplattenverschlüsselung für Azure

Es wurde eine neue Azure-Berechtigung hinzugefügt, mit der Sie nun alle verwalteten Festplatten bei der Erstellung verschlüsseln können.

Weitere Informationen zu dieser neuen Funktion finden Sie unter "Cloud Volumes ONTAP einrichten, um einen vom Kunden gemanagten Schlüssel in Azure zu verwenden".

18. September 2022

Die folgenden Änderungen wurden mit der Version 3.9.22 des Connectors eingeführt.

Verbesserungen für Digital Wallet

- Das Digital Wallet zeigt jetzt eine Zusammenfassung des optimierten I/O-Lizenzpakets und der bereitgestellten WORM-Kapazität für Cloud Volumes ONTAP-Systeme auf Ihrem Konto an.

  Mit diesen Angaben können Sie besser verstehen, wie abgerechnet wird und ob Sie zusätzliche Kapazität erwerben müssen.

  "Erfahren Sie, wie Sie die verbrauchte Kapazität in Ihrem Konto anzeigen".

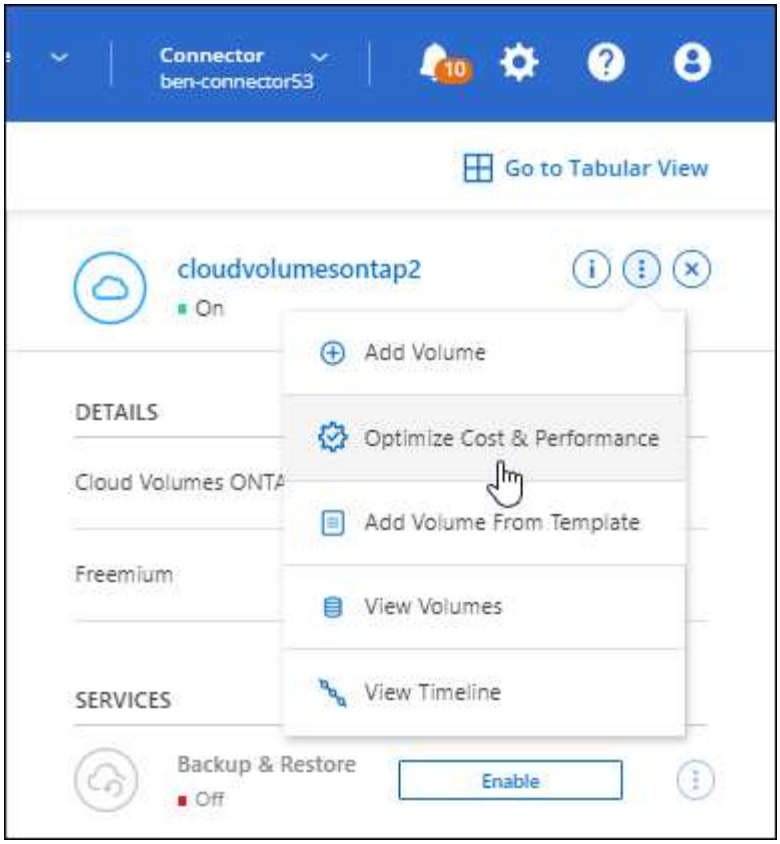
- Jetzt können Sie von einer Lademethode zur optimierten Lademethode wechseln.

  "Erfahren Sie, wie Sie Lademethoden ändern können".

Optimierte Kosten und Performance

Sie können jetzt die Kosten und Leistung eines Cloud Volumes ONTAP-Systems direkt aus dem Canvas optimieren.

Nachdem Sie eine Arbeitsumgebung ausgewählt haben, können Sie die Option **Kosten & Leistung optimieren** wählen, um den Instanztyp für Cloud Volumes ONTAP zu ändern. Die Auswahl einer kleineren Instanz kann zur Senkung der Kosten beitragen, während Sie durch einen Wechsel zu einer größeren Instanz die Performance optimieren können.



AutoSupport-Benachrichtigungen

BlueXP generiert jetzt eine Benachrichtigung, wenn ein Cloud Volumes ONTAP System keine AutoSupport-Nachrichten senden kann. Die Benachrichtigung enthält einen Link zu Anweisungen, mit denen Sie Netzwerkprobleme beheben können.

31 Juli 2022

Die folgenden Änderungen wurden mit der Version 3.9.21 des Connectors eingeführt.

MTEKM-Lizenz

Die MTEKM-Lizenz (Multi-Tenant Encryption Key Management) ist nun in neuen und bestehenden Cloud Volumes ONTAP-Systemen mit Version 9.11.1 oder höher enthalten.

Das mandantenfähige externe Verschlüsselungsmanagement ermöglicht individuelle Storage VMs (SVMs) beim Einsatz von NetApp Volume Encryption, ihre eigenen Schlüssel über einen KMIP Server beizubehalten.

"So verschlüsseln Sie Volumes mit NetApp Verschlüsselungslösungen".

Proxy-Server

BlueXP konfiguriert Ihre Cloud Volumes ONTAP-Systeme jetzt automatisch für die Verwendung des Connectors als Proxyserver, wenn keine ausgehende Internetverbindung zum Senden von AutoSupport-Nachrichten verfügbar ist.

AutoSupport überwacht proaktiv den Zustand Ihres Systems und sendet Meldungen an den technischen Support von NetApp.

Die einzige Anforderung besteht darin, sicherzustellen, dass die Sicherheitsgruppe des Connectors *eingehende* -Verbindungen über Port 3128 zulässt. Nach der Bereitstellung des Connectors müssen Sie diesen Port öffnen.

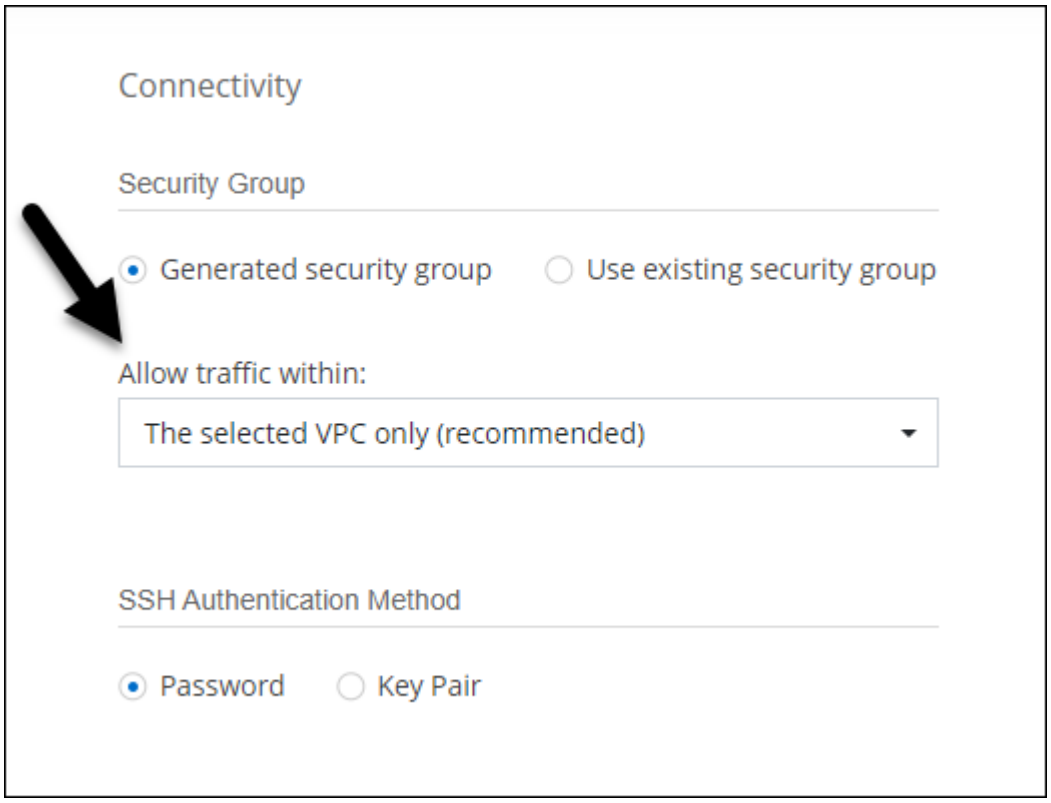
Lademethode ändern

Sie können nun die Gebührenmethode für ein Cloud Volumes ONTAP System ändern, das kapazitätsbasierte Lizenzierung nutzt. Wenn Sie beispielsweise ein Cloud Volumes ONTAP-System mit dem Essentials-Paket bereitgestellt haben, können Sie es in das Professional-Paket ändern, wenn sich Ihre Geschäftsanforderungen ändern. Diese Funktion ist über das Digital Wallet verfügbar.

"Erfahren Sie, wie Sie Lademethoden ändern können".

Verbesserung von Sicherheitsgruppen

Wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen, können Sie jetzt über die Benutzeroberfläche festlegen, ob die vordefinierte Sicherheitsgruppe nur den Datenverkehr innerhalb des ausgewählten Netzwerks (empfohlen) oder in allen Netzwerken zulassen soll.



18 Juli 2022

Neue Lizenzierungspakete in Azure

Zwei neue kapazitätsbasierte Lizenzpakete stehen für Cloud Volumes ONTAP in Azure zur Verfügung, wenn diese über ein Azure Marketplace-Abonnement abgerechnet werden:

- * Optimiert*: Bezahlung der bereitgestellten Kapazität und I/O-Operationen separat
- **Edge Cache**: Lizenzierung für "Cloud Volumes Edge Cache"

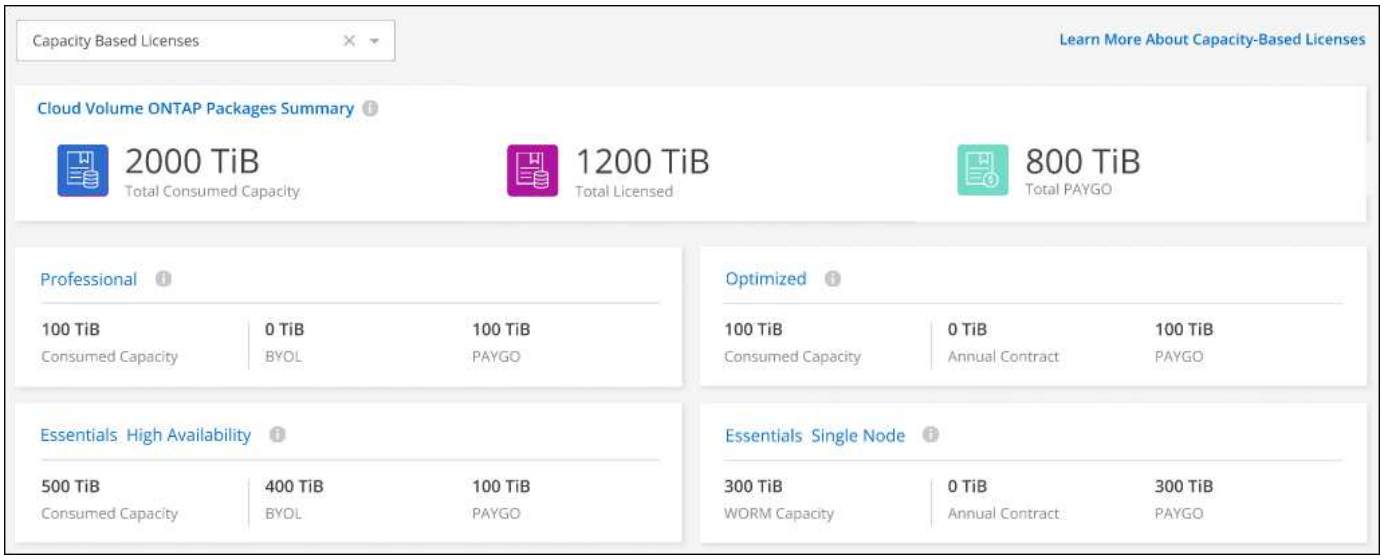
"Erfahren Sie mehr über diese Lizenzierungspakete".

3 Juli 2022

Die folgenden Änderungen wurden mit der Version 3.9.20 des Connectors eingeführt.

Digital Wallet

Auf der Digital Wallet werden jetzt die verbrauchte Gesamtkapazität Ihres Kontos und die verbrauchte Kapazität nach Lizenzpaket angezeigt. Dadurch können Sie nachvollziehen, wie Sie belastet sind und ob Sie zusätzliche Kapazität erwerben müssen.



Verbesserung von elastischen Volumes

BlueXP unterstützt jetzt die Funktion Amazon EBS Elastic Volumes beim Erstellen einer Cloud Volumes ONTAP Arbeitsumgebung über die Benutzeroberfläche. Die Funktion Elastic Volumes ist standardmäßig aktiviert, wenn gp3- oder io1-Festplatten verwendet werden. Sie können die ursprüngliche Kapazität auf Grundlage Ihrer Storage-Anforderungen auswählen und nach der Bereitstellung von Cloud Volumes ONTAP überarbeiten.

"Erfahren Sie mehr über die Unterstützung von Elastic Volumes in AWS".

ONTAP S3-Lizenz in AWS

ONTAP S3 ist jetzt auf neuen und vorhandenen Cloud Volumes ONTAP Systemen mit Version 9.11.0 oder höher in AWS enthalten.

"Lesen Sie, wie Sie S3-Objekt-Storage-Services in ONTAP konfigurieren und managen"

Neue Unterstützung für Azure Cloud Region

Ab Version 9.10.1 wird Cloud Volumes ONTAP jetzt auch in Azure West US 3 Region unterstützt.

"Hier finden Sie die vollständige Liste der unterstützten Regionen für Cloud Volumes ONTAP"

ONTAP S3 Lizenz in Azure

Jetzt ist eine ONTAP S3 Lizenz auf neuen und vorhandenen Cloud Volumes ONTAP Systemen mit Version 9.9.1 oder höher in Azure enthalten.

"Lesen Sie, wie Sie S3-Objekt-Storage-Services in ONTAP konfigurieren und managen"

7. Juni 2022

Die folgenden Änderungen wurden mit der Version 3.9.19 des Connectors eingeführt.

Cloud Volumes ONTAP 9.11.1

BlueXP kann jetzt Cloud Volumes ONTAP 9.11.1 implementieren und verwalten, was auch Unterstützung für neue Funktionen und zusätzliche Regionen von Cloud-Providern umfasst.

"Erfahren Sie mehr über die neuen Funktionen in dieser Version von Cloud Volumes ONTAP"

Neue Erweiterte Ansicht

Wenn Sie die erweiterte Verwaltung von Cloud Volumes ONTAP durchführen müssen, können Sie dies tun mit ONTAP System Manager, das ist eine Management-Schnittstelle, die mit einem ONTAP-System zur Verfügung gestellt wird. Die System Manager-Schnittstelle haben wir direkt in BlueXP integriert, damit Sie BlueXP nicht für die erweiterte Verwaltung verlassen müssen.

Diese erweiterte Ansicht ist als Vorschau für Cloud Volumes ONTAP 9.10.0 und höher verfügbar. Wir planen, diese Erfahrungen weiter zu verbessern und in zukünftigen Versionen Verbesserungen hinzuzufügen. Bitte senden Sie uns Ihr Feedback über den Product-Chat.

"Erfahren Sie mehr über die erweiterte Ansicht".

Unterstützung von Amazon EBS Elastic Volumes

Die Unterstützung der Elastic Volumes von Amazon EBS mit einem Cloud Volumes ONTAP Aggregat bietet eine bessere Performance und zusätzliche Kapazität, während BlueXP die zugrunde liegende Festplattenkapazität nach Bedarf automatisch erhöht.

Unterstützung für elastische Volumes ist ab *neuen* Cloud Volumes ONTAP 9.11.0 Systemen und mit gp3- und io1-EBS-Festplattentypen verfügbar.

"Erfahren Sie mehr über den Support für Elastic Volumes".

Beachten Sie, dass die Unterstützung von Elastic Volumes neue AWS Berechtigungen für den Connector erforderlich macht:

```
"ec2:DescribeVolumesModifications",
"ec2:ModifyVolume",
```

Stellen Sie sicher, dass Sie diese Berechtigungen für jeden Satz von AWS Zugangsdaten bereitstellen, den Sie BlueXP hinzugefügt haben. "Sehen Sie sich die neueste Connector-Richtlinie für AWS an".

Unterstützung für Implementierung von HA-Paaren in Shared AWS-Subnetzen

Cloud Volumes ONTAP 9.11.1 unterstützt auch AWS VPC Sharing. Diese Version des Connectors ermöglicht Ihnen die Bereitstellung eines HA-Paars in einem gemeinsamen AWS Subnetz, wenn Sie die API verwenden.

"Erfahren Sie, wie ein HA-Paar in einem gemeinsamen Subnetz implementiert wird".

Eingeschränkter Netzwerkzugriff bei Verwendung von Service-Endpunkten

BlueXP beschränkt jetzt den Netzwerkzugriff bei der Verwendung eines vnet-Service-Endpunkts für Verbindungen zwischen Cloud Volumes ONTAP- und Storage-Konten. BlueXP verwendet einen Dienstendpunkt, wenn Sie Azure Private Link-Verbindungen deaktivieren.

"Erfahren Sie mehr über Azure Private Link Connections with Cloud Volumes ONTAP".

Unterstützung für die Erstellung von Storage-VMs in Google Cloud

Cloud Volumes ONTAP unterstützt ab Version 9.11.1 mehrere Storage VMs in Google Cloud. Ab dieser Version des Connectors können Sie mit BlueXP Speicher-VMs auf Cloud Volumes ONTAP HA-Paaren in Google Cloud über die API erstellen.

Für die Unterstützung bei der Erstellung von Speicher-VMs sind neue Google Cloud-Berechtigungen für den Connector erforderlich:

```
- compute.instanceGroups.get
- compute.addresses.get
```

Beachten Sie, dass Sie zum Erstellen einer Storage VM auf einem System mit einem einzelnen Node die ONTAP CLI oder System Manager verwenden müssen.

- "Erfahren Sie mehr über Storage-VM-Limits in Google Cloud"
- "Lesen Sie, wie Sie in Google Cloud Daten-Serving-Storage-VMs für Cloud Volumes ONTAP erstellen"

Mai 2022

Die folgenden Änderungen wurden mit der Version 3.9.18 des Connectors eingeführt.

Cloud Volumes ONTAP 9.11.0

BlueXP kann jetzt Cloud Volumes ONTAP 9.11.0 bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen in dieser Version von Cloud Volumes ONTAP".

Verbesserung der Mediator-Upgrades

Wenn BlueXP den Mediator für ein HA-Paar aktualisiert, überprüft er nun, ob ein neues Mediator-Image verfügbar ist, bevor die Boot-Festplatte gelöscht wird. Durch diese Änderung wird sichergestellt, dass der Mediator weiterhin erfolgreich arbeiten kann, wenn das Upgrade nicht erfolgreich durchgeführt wird.

Registerkarte K8s wurde entfernt

Die Registerkarte K8s wurde in einer früheren Version veraltet und wurde jetzt entfernt. Wenn Sie Kubernetes mit Cloud Volumes ONTAP verwenden möchten, können Sie Managed-Kubernetes-Cluster als Arbeitsumgebung für erweitertes Datenmanagement auf den Canvas hinzufügen.

"Erfahren Sie mehr über das Management von Kubernetes-Daten in BlueXP"

Jahresvertrag in Azure

Die Essentials- und Professional-Pakete sind ab sofort im Rahmen eines Jahres in Azure erhältlich. Sie können sich an Ihren NetApp Ansprechpartner wenden, um einen Jahresvertrag zu abschließen. Der Vertrag ist als Privatangebot im Azure Marketplace erhältlich.

Wenn NetApp Ihnen das private Angebot teilt, können Sie den Jahresplan auch auswählen, wenn Sie während der Erstellung der Arbeitsumgebung im Azure Marketplace abonnieren.

"Weitere Informationen zur Lizenzierung".

Sofortiges Abrufen von S3 Glacier

Sie können jetzt Tiered Daten in der Storage-Klasse von Amazon S3 Glacier Instant Retrieval speichern.

"Erfahren Sie, wie Sie die Storage-Klasse für Tiered Daten ändern".

Für den Connector sind neue AWS Berechtigungen erforderlich

Bei der Implementierung eines HA-Paars in einer einzelnen Verfügbarkeitszone (AZ) sind nun die folgenden Berechtigungen erforderlich, um eine AWS Spread-Placement-Gruppe zu erstellen:

```
"ec2:DescribePlacementGroups",
"iam:GetRolePolicy",
```

Diese Berechtigungen sind jetzt erforderlich, um zu optimieren, wie BlueXP die Platzierungsgruppe erstellt.

Stellen Sie sicher, dass Sie diese Berechtigungen für jeden Satz von AWS Zugangsdaten bereitstellen, den Sie BlueXP hinzugefügt haben. "Sehen Sie sich die neueste Connector-Richtlinie für AWS an".

Neue regionale Unterstützung für Google Cloud

Ab Version 9.10.1 wird Cloud Volumes ONTAP nun in den folgenden Google Cloud Regionen unterstützt:

- Delhi (asien-Süd-2)
- Melbourne (australien-Südheast2)
- Mailand (europa-West8) - nur ein Knoten
- Santiago (southamerica-west1) - nur ein Knoten

"Hier finden Sie die vollständige Liste der unterstützten Regionen für Cloud Volumes ONTAP"

Unterstützung für n2-Standard-16 in Google Cloud

Der maschinentyp n2-Standard-16 wird ab Version 9.10.1 mit Cloud Volumes ONTAP in Google Cloud unterstützt.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in Google Cloud anzeigen"

Erweiterungen der Google Cloud Firewallrichtlinien

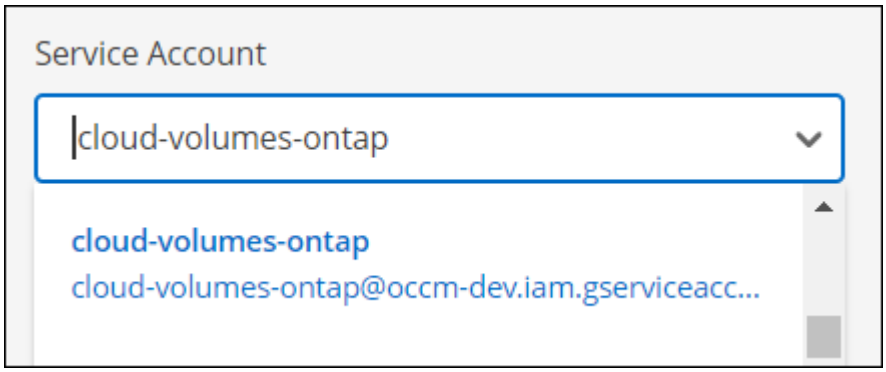
- Wenn Sie ein Cloud Volumes ONTAP-HA-Paar in Google Cloud erstellen, zeigt BlueXP jetzt alle bestehenden Firewall-Richtlinien in einer VPC an.

Bisher wurden bei BlueXP keine Richtlinien in VPC-1, VPC-2 oder VPC-3 angezeigt, für die kein Ziel-Tag vorhanden war.

- Wenn Sie ein Cloud Volumes ONTAP Single-Node-System in Google Cloud erstellen, können Sie nun festlegen, ob die vordefinierte Firewall-Richtlinie den Datenverkehr nur innerhalb der ausgewählten VPC (empfohlen) oder aller VPCs zulassen soll.

Erweiterung um Google Cloud-Servicekonten

Wenn Sie das Google Cloud-Dienstkonto auswählen, das mit Cloud Volumes ONTAP verwendet werden soll, zeigt BlueXP jetzt die E-Mail-Adresse an, die mit jedem Dienstkonto verknüpft ist. Durch das Anzeigen der E-Mail-Adresse kann es leichter sein, zwischen Servicekonten, die denselben Namen haben, zu unterscheiden.



3. April 2022

Der Link „System Manager“ wurde entfernt

Wir haben den zuvor verfügbaren Link zum System Manager aus einer Cloud Volumes ONTAP Arbeitsumgebung entfernt.

Sie können noch immer eine Verbindung zu System Manager herstellen, indem Sie die Cluster-Management-IP-Adresse in einem Webbrowser, der eine Verbindung mit dem Cloud Volumes ONTAP System hat, eingeben. "Weitere Informationen zum Herstellen einer Verbindung mit System Manager".

Worm-Speicherung wird geladen

Nachdem der einführende Sonderpreis abgelaufen ist, werden Sie nun für DIE Verwendung VON WORM-Speicher in Rechnung gestellt. Abrechnung erfolgt stündlich, entsprechend der insgesamt bereitgestellten Kapazität der WORM Volumes. Dies gilt für neue und bestehende Cloud Volumes ONTAP Systeme.

"Informieren Sie sich über die Preisgestaltung für WORM Storage".

27 Februar 2022

Die folgenden Änderungen wurden mit der Version 3.9.16 des Connectors eingeführt.

Assistent zum Neugestalten von Volumes

Der Assistent zum Erstellen eines neuen Volumes, den wir kürzlich eingeführt haben, ist jetzt verfügbar, wenn ein Volume auf einem bestimmten Aggregat aus der Option **Erweiterte Zuweisung** erstellt wird.

"Erfahren Sie, wie Sie Volumes auf einem bestimmten Aggregat erstellen".

9 Februar 2022

Marketplace-Updates

- Das Essentials-Paket und das Professional-Paket sind jetzt in allen Cloud-Provider-Marktplätzen verfügbar.

  Dank dieser Gebührenarten können Sie stundenweise bezahlen oder einen Jahresvertrag direkt von Ihrem Cloud-Provider abschließen. Sie haben weiterhin die Möglichkeit, eine kapazitätsstarke Lizenz direkt bei NetApp zu erwerben.

  Wenn Sie bereits über ein Abonnement auf einem Cloud Marketplace verfügen, haben Sie auch diese neuen Angebote automatisch abonniert. Sie können sich bei der Implementierung einer neuen Cloud Volumes ONTAP Arbeitsumgebung nach Kapazitätsgebühren entscheiden.

  Wenn Sie ein neuer Kunde sind, werden Sie von BlueXP aufgefordert, sich anzumelden, wenn Sie eine neue Arbeitsumgebung erstellen.

- Die Lizenzierung nach Node aus allen Marketplace eines Cloud-Providers ist veraltet und für neue Abonnenten nicht mehr verfügbar. Dazu zählen Jahresverträge und stündliche Abonnements (Explore, Standard und Premium).

  Diese Lademethode ist weiterhin für bestehende Kunden verfügbar, die über ein aktives Abonnement verfügen.

"Informieren Sie sich über die Lizenzierungsoptionen für Cloud Volumes ONTAP".

6 Februar 2022

Exchange nicht zugewiesene Lizenzen

Wenn Sie über eine nicht zugewiesene Node-basierte Lizenz für Cloud Volumes ONTAP verfügen, die Sie nicht verwendet haben, können Sie die Lizenz jetzt austauschen, indem Sie sie in eine Cloud Backup Lizenz, eine Cloud Data Sense Lizenz oder eine Cloud Tiering Lizenz konvertieren.

Durch diese Aktion wird die Cloud Volumes ONTAP-Lizenz erneut gelöscht und für den Service eine mit dem gleichen Ablaufdatum vergleichbare Lizenz erstellt.

"Erfahren Sie, wie Sie nicht zugewiesene knotenbasierte Lizenzen austauschen".

30 Januar 2022

Die folgenden Änderungen wurden mit der Version 3.9.15 des Connectors eingeführt.

Neu gestaltete Lizenzauswahl

Beim Erstellen einer neuen Cloud Volumes ONTAP-Arbeitsumgebung haben wir den Bildschirm für die Lizenzauswahl neu gestaltet. Die Änderungen unterstreichen die im Juli 2021 eingeführten Methoden zum Kapazitätsverbrauch und unterstützen zukünftige Angebote über die Cloud-Provider-Märkte.

Aktualisierung digitaler Geldbörse

Wir haben die **Digitale Geldbörse** aktualisiert, indem wir Cloud Volumes ONTAP Lizenzen auf einem einzigen Tab konsolidieren.

Januar 2022

Die folgenden Änderungen wurden mit der Version 3.9.14 des Connectors eingeführt.

Unterstützung für weitere Azure VM-Typen

Cloud Volumes ONTAP wird ab Version 9.10.1 bei den folgenden VM-Typen in Microsoft Azure unterstützt:

- E4ds_v4
- E8ds_v4
- E32ds_v4
- E48ds_v4

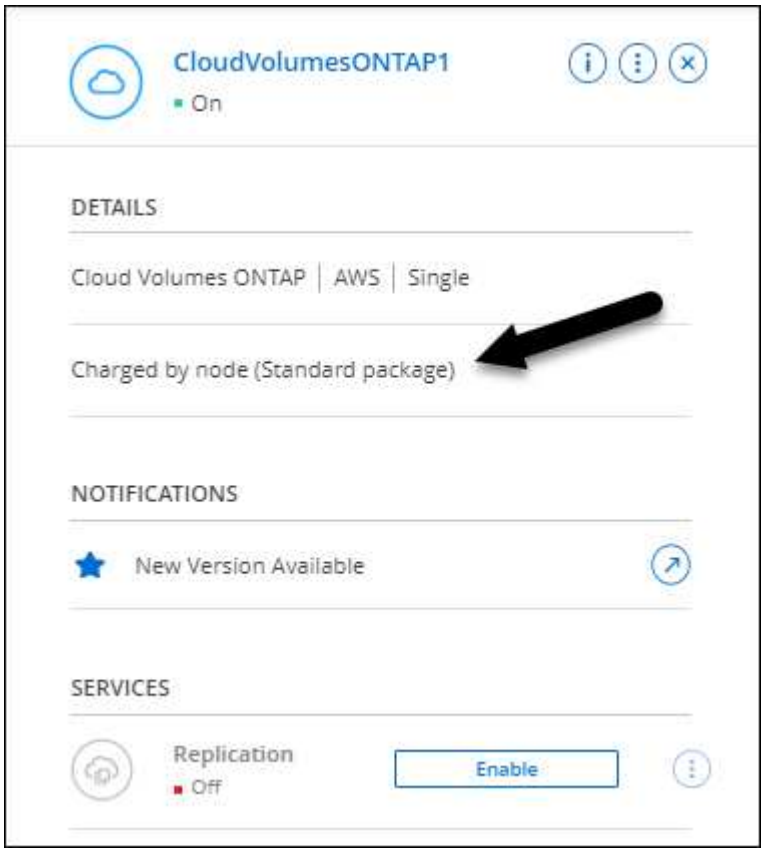
Wechseln Sie zum "Versionshinweise zu Cloud Volumes ONTAP" Weitere Informationen zu unterstützten Konfigurationen

FlexClone Ladeaktualisierung

Wenn Sie ein verwenden "Kapazitätsbasierte Lizenz" Bei Cloud Volumes ONTAP wird die von FlexClone Volumes genutzte Kapazität nicht mehr berechnet.

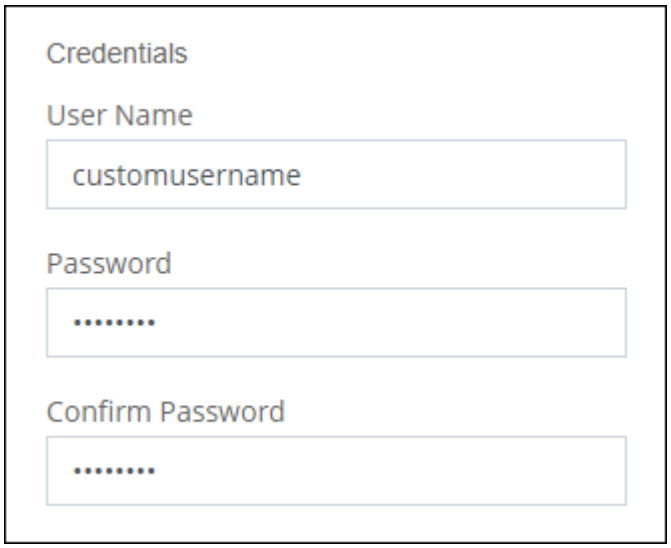
Lademethode wird jetzt angezeigt

BlueXP zeigt nun die Lademethode für jede Cloud Volumes ONTAP Arbeitsumgebung im rechten Bereich des Canvas an.



Wählen Sie Ihren Benutzernamen aus

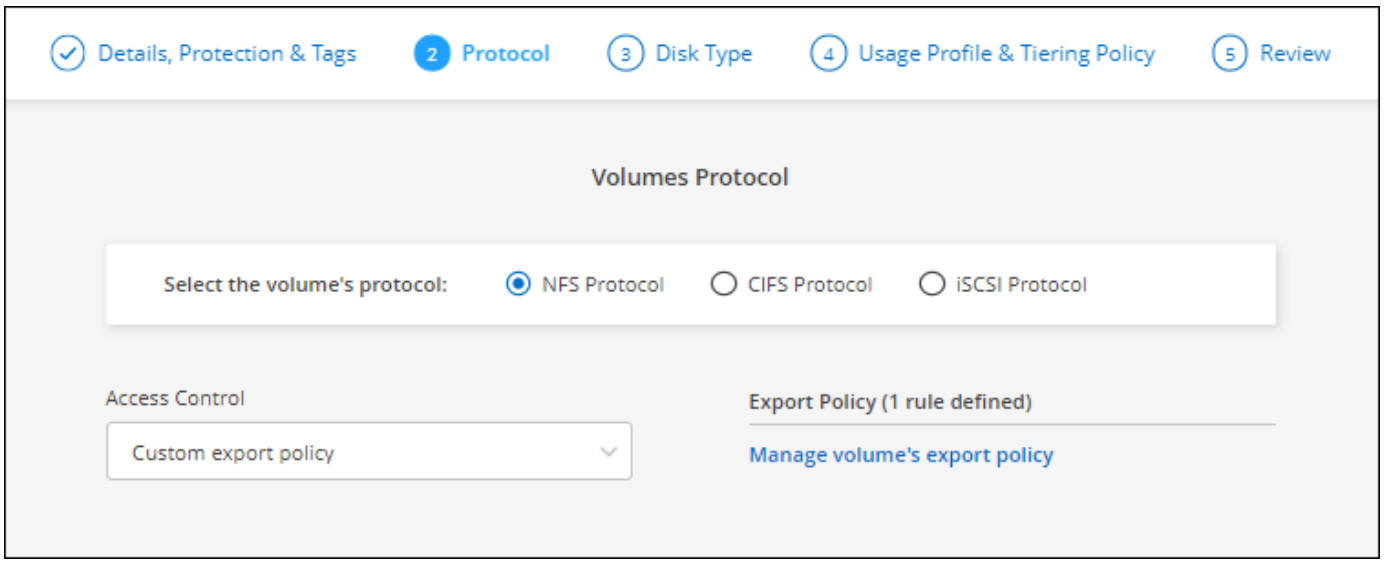
Wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen, können Sie jetzt anstatt des standardmäßigen Admin-Benutzernamens Ihren bevorzugten Benutzernamen eingeben.



Verbesserte Volume-Erstellung

Es wurden einige Verbesserungen bei der Volume-Erstellung vorgenommen:

- Der Create Volume Wizard hat zur Erleichterung der Anwendung neu gestaltet.
- Sie können jetzt eine benutzerdefinierte Exportrichtlinie für NFS auswählen.



28. November 2021

Die folgenden Änderungen wurden mit der Version 3.9.13 des Connectors eingeführt.

Cloud Volumes ONTAP 9.10.1

BlueXP kann jetzt Cloud Volumes ONTAP 9.10.1 bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen in dieser Version von Cloud Volumes ONTAP".

NetApp Keystone-Abonnements

Sie können jetzt Keystone Abonnements verwenden, um für Cloud Volumes ONTAP HA-Paare zu bezahlen.

Ein Keystone Subscription ist ein nutzungsbasierter Abonnementservice, der eine nahtlose Hybrid Cloud-Erfahrung bietet, wenn Sie lieber auf Betriebskosten basierende Nutzungsmodelle als Vorabinvestitionen oder Leasing nutzen möchten.

Eine Keystone Subscription wird von allen neuen Cloud Volumes ONTAP Versionen unterstützt, die Sie über BlueXP implementieren können.

- "Weitere Informationen zu NetApp Keystone Abonnements".
- "Erste Schritte mit Keystone Abonnements in BlueXP".

Neue Unterstützung für AWS Region

Cloud Volumes ONTAP wird nun in der Region AWS Asia Pacific (Osaka) unterstützt (AP-Nordost-3).

Reduzierung der Ports

Die Ports 8023 und 49000 sind bei Cloud Volumes ONTAP Systemen in Azure nicht mehr für Single-Node-Systeme und HA-Paare geöffnet.

Diese Änderung gilt für *neue* Cloud Volumes ONTAP Systeme ab der Version 3.9.13 des Steckers.

Oktober 4 2021

Die folgenden Änderungen wurden mit der Version 3.9.11 des Connectors eingeführt.

Cloud Volumes ONTAP 9.10.0

BlueXP kann jetzt Cloud Volumes ONTAP 9.10.0 bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen in dieser Version von Cloud Volumes ONTAP".

Kürzere Implementierungszeit

Wir haben die zur Implementierung einer Cloud Volumes ONTAP-Arbeitsumgebung in Microsoft Azure oder in Google Cloud benötigte Zeit bei aktivierter normaler Schreibgeschwindigkeit reduziert. Die Implementierungszeit ist im Durchschnitt jetzt 3-4 Minuten kürzer.

September 2021

Die folgenden Änderungen wurden mit der Version 3.9.10 des Connectors eingeführt.

Vom Kunden gemanagte Verschlüsselung in Azure

Die Daten werden auf Cloud Volumes ONTAP in Azure automatisch verschlüsselt "Azure Storage Service Encryption" Mit einem von Microsoft gemanagten Schlüssel Sie können nun jedoch Ihren eigenen, vom Kunden gemanagten Verschlüsselungsschlüssel verwenden, indem Sie die folgenden Schritte ausführen:

1. Aus Azure erstellen Sie einen Schlüsselspeicher und generieren Sie anschließend einen Schlüssel in

diesem Vault.

2. Verwenden Sie für BlueXP die API, um eine Cloud Volumes ONTAP-Arbeitsumgebung zu erstellen, in der der Schlüssel zum Einsatz kommt.

"Weitere Informationen zu diesen Schritten".

7 Juli 2021

Die folgenden Änderungen wurden mit der Version 3.9.8 des Connectors eingeführt.

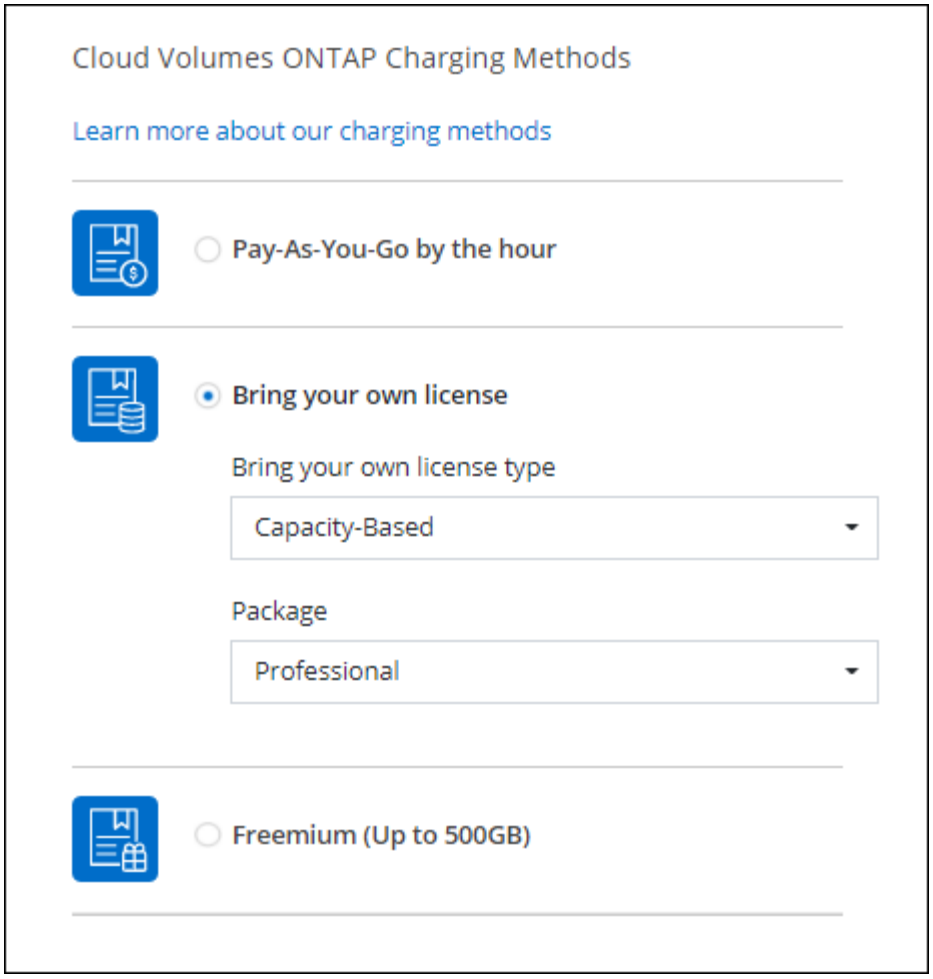
Neue Lademethoden

Für Cloud Volumes ONTAP stehen neue Lademethoden zur Verfügung.

- **Kapazitätsbasiertes BYOL**: Eine kapazitätsbasierte Lizenz ermöglicht die Zahlung von Cloud Volumes ONTAP pro tib Kapazität. Die Lizenz ist mit Ihrem NetApp Konto verknüpft und ermöglicht es Ihnen, so viele Cloud Volumes ONTAP-Systeme zu erstellen, solange über Ihre Lizenz genügend Kapazität verfügbar ist. Kapazitätsbasierte Lizenzierung ist in Form eines Pakets verfügbar, entweder *Essentials* oder *Professional*.
- **Freimium Angebot**: Mit Freimium können Sie alle Cloud Volumes ONTAP Funktionen kostenlos von NetApp nutzen (Cloud-Provider fallen weiterhin an). Sie verfügen über eine bereitgestellte Kapazität von 500 gib pro System, und es besteht kein Support-Vertrag. Sie können bis zu 10 Freemium-Systeme haben.

  "Erfahren Sie mehr über diese Lizenzierungsoptionen".

  Hier sehen Sie ein Beispiel für die Lademethoden, die Sie wählen können:



WORM-Speicher steht allgemein zur Verfügung

WORM-Speicher (Write Once, Read Many) befindet sich nicht mehr im Preview und steht nun für den allgemeinen Gebrauch mit Cloud Volumes ONTAP zur Verfügung. "Erfahren Sie mehr über WORM Storage".

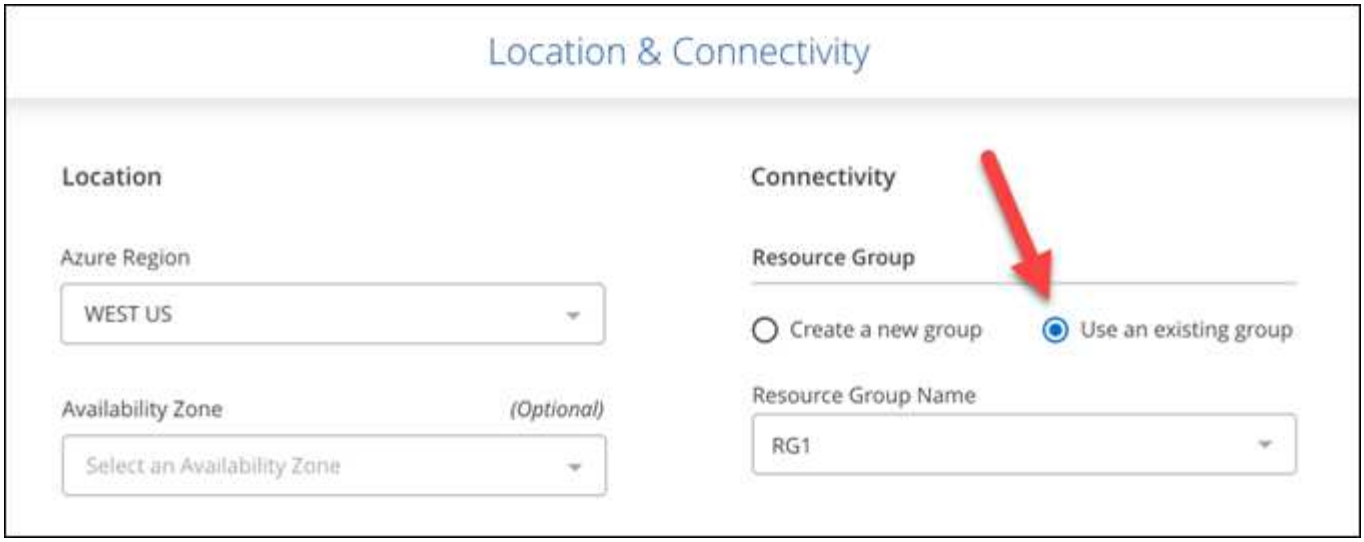
Unterstützung für m5dn.24xlarge in AWS

Ab Version 9.9.1 unterstützt Cloud Volumes ONTAP jetzt den Instanztyp m5dn.24xlarge mit den folgenden Lademethoden: PAYGO Premium, Bring your own License (BYOL) und Freemium.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in AWS".

Wählen Sie vorhandene Azure Ressourcengruppen aus

Beim Erstellen eines Cloud Volumes ONTAP Systems in Azure haben Sie nun die Möglichkeit, eine vorhandene Ressourcengruppe für die VM und ihre zugehörigen Ressourcen auszuwählen.



Mit den folgenden Berechtigungen kann BlueXP Cloud Volumes ONTAP-Ressourcen aus einer Ressourcengruppe entfernen, wenn die Bereitstellung ausfällt oder gelöscht wird:

```
"Microsoft.Network/privateEndpoints/delete",
"Microsoft.Compute/availabilitySets/delete",
```

Stellen Sie sicher, dass Sie diese Berechtigungen für jeden Satz von Azure Zugangsdaten bereitstellen, den Sie BlueXP hinzugefügt haben. "Sehen Sie sich die neueste Connector-Richtlinie für Azure an".

Öffentlicher Blob-Zugriff ist jetzt in Azure deaktiviert

Als Verbesserung der Sicherheit deaktiviert BlueXP bei der Erstellung eines Storage-Kontos für Cloud Volumes ONTAP jetzt **öffentlichen Blob-Zugriff**.

Verbesserung von Azure Private Link

Standardmäßig aktiviert BlueXP jetzt eine Azure Private Link-Verbindung auf dem Boot Diagnostics-Speicherkonto für neue Cloud Volumes ONTAP-Systeme.

Das heißt, *all* Storage-Konten für Cloud Volumes ONTAP werden jetzt einen privaten Link verwenden.

"Erfahren Sie mehr über die Verwendung eines Azure Private Links mit Cloud Volumes ONTAP".

Persistente Festplatten in Google Cloud ausgewogen

Ab Version 9.9.1 unterstützt Cloud Volumes ONTAP jetzt ausgeglichene persistente Festplatten (pd-ausgewogen).

Diese SSDs sorgen mit weniger IOPS pro gib für ausgewogene Performance und Kosten.

Custom-4-16384 wird in Google Cloud nicht mehr unterstützt

Der Maschinentyp Custom-4-16384 wird von neuen Cloud Volumes ONTAP-Systemen nicht mehr unterstützt.

Wenn auf diesem Maschinentyp ein System ausgeführt wird, können Sie es weiterhin verwenden, wir empfehlen jedoch, auf den Maschinentyp n2-Standard-4 umzuschalten.

"Zeigt unterstützte Konfigurationen für Cloud Volumes ONTAP in GCP an".

30 Mai 2021

Die folgenden Änderungen wurden mit der Version 3.9.7 des Connectors eingeführt.

Neues Professional Package in AWS

Mit einem neuen Professional-Paket können Sie Cloud Volumes ONTAP und Cloud Backup Service unter Verwendung eines jährlichen Vertrags über AWS Marketplace bündeln. Die Zahlung erfolgt pro tib. Durch dieses Abonnement können Sie Backups von Daten vor Ort nicht erstellen.

Bei Auswahl dieser Zahlungsoption können Sie bis zu 2 PiB pro Cloud Volumes ONTAP-System über EBS Festplatten und Tiering zu S3 Objekt-Storage (Single Node oder HA) bereitstellen.

Wechseln Sie zum "AWS Marketplace Seite" Weitere Informationen zu Preisen finden Sie im "Versionshinweise zu Cloud Volumes ONTAP" Erfahren Sie mehr über diese Lizenzoption.

Tags auf EBS Volumes in AWS

BlueXP fügt EBS Volumes jetzt Tags hinzu, wenn es eine neue Cloud Volumes ONTAP Arbeitsumgebung schafft. Die Tags wurden bereits nach der Implementierung von Cloud Volumes ONTAP erstellt.

Diese Änderung kann hilfreich sein, wenn Ihr Unternehmen die Service-Kontrollrichtlinien (SCPs) für das Management von Berechtigungen verwendet.

Mindestkühldauer für automatische Tiering-Richtlinie

Wenn Sie das Daten-Tiering auf einem Volume mithilfe der Richtlinie „*Auto*“ aktiviert haben, können Sie jetzt den minimalen Kühlzeitraum mithilfe der API anpassen.

"Erfahren Sie, wie Sie die minimale Kühldauer einstellen."

Verbesserung der benutzerdefinierten Exportrichtlinien

Wenn Sie ein neues NFS-Volume erstellen, zeigt BlueXP jetzt benutzerdefinierte Exportrichtlinien in aufsteigender Reihenfolge an. Dadurch können Sie einfacher die Exportrichtlinie finden, die Sie benötigen.

Löschen alter Cloud-Snapshots

BlueXP löscht jetzt ältere Cloud-Snapshots von Root- und Boot-Festplatten, die erstellt werden, wenn ein Cloud Volumes ONTAP-System bereitgestellt wird und jedes Mal, wenn es heruntergefahren wird. Nur die beiden letzten Snapshots werden sowohl für die Root- als auch für Boot-Volumes beibehalten.

Dies senkt die Kosten für Cloud-Provider durch das Entfernen von Snapshots, die nicht mehr benötigt werden.

Beachten Sie, dass für einen Konnektor eine neue Berechtigung zum Löschen von Azure-Snapshots erforderlich ist. "Sehen Sie sich die neueste Connector-Richtlinie für Azure an".

```
"Microsoft.Compute/snapshots/delete"
```

24 Mai 2021

Cloud Volumes ONTAP 9.9.1

BlueXP kann jetzt Cloud Volumes ONTAP 9.9 bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen in dieser Version von Cloud Volumes ONTAP".

11 April 2021

Die folgenden Änderungen wurden mit der Version 3.9.5 des Connectors eingeführt.

Berichterstellung für logischen Speicherplatz

BlueXP ermöglicht jetzt die Erstellung logischer Speicherplatzberichte für die ursprüngliche, für Cloud Volumes ONTAP erstellten Storage-VM.

Wenn der Speicherplatz logisch gemeldet wird, meldet ONTAP den Volume-Speicherplatz, sodass der gesamte durch die Storage-Effizienzfunktionen eingesparte physische Speicherplatz ebenfalls in seiner Nutzung gemeldet wird.

Unterstützung von gp3-Festplatten in AWS

Cloud Volumes ONTAP unterstützt jetzt *General Purpose SSD (gp3)* Festplatten ab Version 9.7. gp3-Festplatten sind die kostengünstigsten SSDs, die für ein breites Spektrum an Workloads ein ausgewogenes Verhältnis zwischen Kosten und Performance bieten.

"Erfahren Sie mehr über die Verwendung von gp3-Datenträgern mit Cloud Volumes ONTAP".

Kalte Festplatten werden in AWS nicht mehr unterstützt

Cloud Volumes ONTAP unterstützt keine sc1-Festplatten (Cold HDD) mehr.

TLS 1.2 für Azure Storage-Konten

Wenn BlueXP Storage-Konten in Azure für Cloud Volumes ONTAP erstellt, ist die TLS-Version für das Storage-Konto jetzt Version 1.2.

8 März 2021

Die folgenden Änderungen wurden mit der Version 3.9.4 des Connectors eingeführt.

Cloud Volumes ONTAP 9.9.0

BlueXP kann jetzt Cloud Volumes ONTAP 9.9 bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen in dieser Version von Cloud Volumes ONTAP".

Unterstützung für die AWS C2S-Umgebung

Die Implementierung von Cloud Volumes ONTAP 9.8 ist nun in der Umgebung der AWS Commercial Cloud Services (C2S) möglich.

"Erfahren Sie, wie Sie mit C2S beginnen".

AWS Verschlüsselung mit vom Kunden gemanagten CMKs

Mit BlueXP können Sie Cloud Volumes ONTAP-Daten immer mithilfe des AWS KMS (Key Management Service) verschlüsseln. Ab Cloud Volumes ONTAP 9.9 werden Daten auf EBS-Festplatten und auf S3 abgestufte Daten verschlüsselt, wenn Sie sich für einen vom Kunden gemanagten CMK entscheiden. Bisher wurden nur EBS-Daten verschlüsselt.

Beachten Sie, dass Sie für die Cloud Volumes ONTAP IAM-Rolle Zugriff zur Verwendung des CMK bereitstellen müssen.

"Erfahren Sie mehr über die Einrichtung des AWS KMS mit Cloud Volumes ONTAP".

Unterstützung für Azure DoD

Sie können Cloud Volumes ONTAP 9.8 jetzt im Azure Department of Defense (DoD) Impact Level 6 (IL6) implementieren.

Verringerung der IP-Adresse in Google Cloud

In Google Cloud haben wir die Anzahl der für Cloud Volumes ONTAP 9.8 und höher erforderlichen IP-Adressen reduziert. Standardmäßig ist eine niedrigere IP-Adresse erforderlich (wir vereinheitlichen die Intercluster LIF mit der Node-Management-LIF). Darüber hinaus besteht die Möglichkeit, bei Verwendung der API die Erstellung der SVM-Management-LIF zu überspringen, was den Bedarf an einer zusätzlichen IP-Adresse verringert.

"Informieren Sie sich in Google Cloud über die IP-Adressanforderungen".

Gemeinsame VPC-Unterstützung in Google Cloud

Durch die Implementierung eines Cloud Volumes ONTAP HA-Paars in Google Cloud haben Sie nun die Möglichkeit, gemeinsame VPCs für VPC-1, VPC-2 und VPC-3 auszuwählen. Bisher könnte nur die VPC-0 eine gemeinsame VPC sein. Diese Änderung wird unterstützt durch Cloud Volumes ONTAP 9.8 und höher.

"Erfahren Sie mehr über die Netzwerkanforderungen von Google Cloud".

4. Januar 2021

Die folgenden Änderungen wurden mit der Version 3.9.2 des Connectors eingeführt.

AWS Outposts

Vor einigen Monaten gaben wir bekannt, dass Cloud Volumes ONTAP den Status „bereit“ für Amazon Web Services (AWS) nicht mehr auflegen sollte. Heute können wir bekanntgeben, dass wir die Outposts von BlueXP und Cloud Volumes ONTAP mit AWS validiert haben.

Wenn Sie einen AWS-Outpost haben, können Sie Cloud Volumes ONTAP in diesem Outpost implementieren, indem Sie die VPC-Outpost im Assistenten zur Arbeitsumgebung auswählen. Die Erfahrung ist mit jeder anderen VPC, die in AWS residiert. Beachten Sie, dass Sie zunächst einen Connector in Ihrem AWS Outpost implementieren müssen.

Es bestehen einige Einschränkungen, die darauf hinweisen:

- Derzeit werden nur Cloud Volumes ONTAP Systeme mit einzelnen Nodes unterstützt
- Die EC2 Instanzen, die Sie mit Cloud Volumes ONTAP verwenden können, sind auf die in Ihrem Outpost

verfügbaren EC2-Instanzen beschränkt

- Derzeit werden nur General Purpose SSDs (gp2) unterstützt

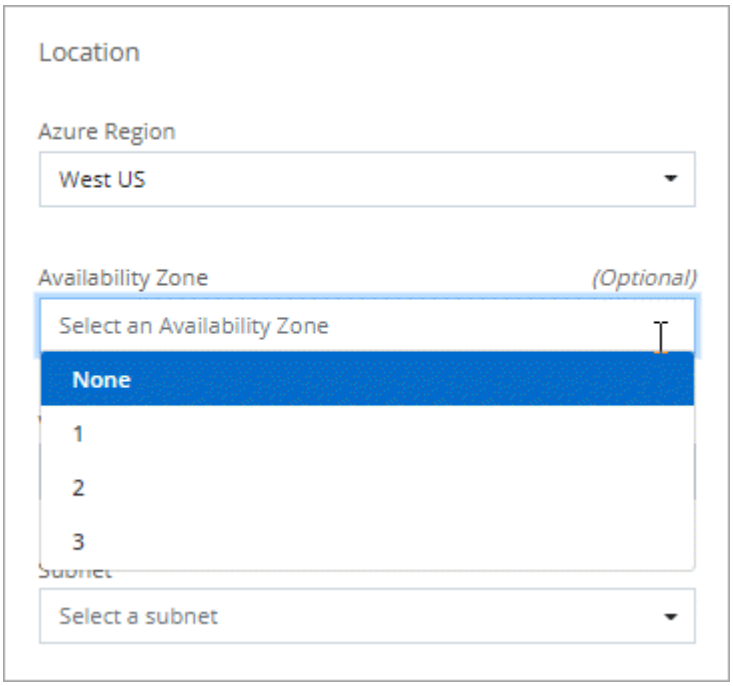
Ultra SSD VNVRAM in unterstützten Azure Regionen

Cloud Volumes ONTAP kann nun eine Ultra SSD als VNVRAM verwenden, wenn Sie den E32s_v3-VM-Typ mit einem Single-Node-System verwenden "In jeder unterstützten Azure-Region".

VNVRAM bietet eine bessere Schreib-Performance.

Wählen Sie eine Verfügbarkeitszone in Azure aus

Sie können nun die Verfügbarkeitszone auswählen, in der Sie ein Cloud Volumes ONTAP-System mit einem einzelnen Node implementieren möchten. Wenn Sie keine AZ auswählen, wählt BlueXP eine für Sie aus.



Größere Festplatten in Google Cloud

Cloud Volumes ONTAP unterstützt jetzt 64-TB-Festplatten in GCP.

Die maximale Systemkapazität mit Festplatten allein beträgt aufgrund der GCP-Limits nur 256 TB.

Neue Maschinentypen in Google Cloud

Cloud Volumes ONTAP unterstützt jetzt die folgenden Maschinentypen:

- n2-Standard-4 mit Explore-Lizenz und mit BYOL
- n2-Standard-8 mit Standard-Lizenz und BYOL
- n2-Standard-32 mit Premium-Lizenz und BYOL

3. November 2020

Die folgenden Änderungen wurden mit der Version 3.9.0 des Connectors eingeführt.

Azure Private Link for Cloud Volumes ONTAP

Standardmäßig aktiviert BlueXP jetzt eine private Azure-Link-Verbindung zwischen Cloud Volumes ONTAP und den zugehörigen Speicherkonten. Ein Private Link sichert Verbindungen zwischen Endpunkten in Azure.

- "Erfahren Sie mehr über Azure Private Links"
- "Erfahren Sie mehr über die Verwendung eines Azure Private Links mit Cloud Volumes 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.

Diese Einschränkungen gelten speziell für das Cloud Volumes ONTAP-Management in BlueXP. Um Einschränkungen an der Cloud Volumes ONTAP Software selbst anzuzeigen, "Wechseln Sie zu den Versionshinweisen zu Cloud Volumes ONTAP"

BlueXP unterstützt nicht die Erstellung von FlexGroup Volumes

Cloud Volumes ONTAP unterstützt zwar FlexGroup Volumes, doch BlueXP unterstützt derzeit nicht die Erstellung von FlexGroup Volumes. Wenn Sie ein FlexGroup-Volume aus dem System Manager oder aus der CLI erstellen, sollten Sie den Kapazitätsmanagement-Modus von BlueXP auf manuell einstellen. Der automatische Modus funktioniert möglicherweise nicht ordnungsgemäß mit FlexGroup-Volumes.

Die Möglichkeit zum Erstellen von FlexGroup Volumes in BlueXP ist für eine zukünftige Version geplant.

BlueXP unterstützt S3 nicht mit Cloud Volumes ONTAP

Cloud Volumes ONTAP unterstützt zwar S3 als Option für Scale-out Storage, BlueXP bietet jedoch keine Managementfunktionen für diese Funktion. Als Best Practice empfiehlt sich die Konfiguration des S3-Client-Zugriffs über Cloud Volumes ONTAP mithilfe der CLI. Weitere Informationen finden Sie im "S3 Configuration Power Guide".

"Weitere Informationen zur Cloud Volumes ONTAP-Unterstützung für S3 und andere Client-Protokolle".

BlueXP unterstützt keine Disaster Recovery für Storage VMs

BlueXP bietet keine Unterstützung für die Einrichtung oder Orchestrierung von Disaster Recovery für Storage VMs (SVM). Sie müssen System Manager oder die CLI verwenden.

"Erfahren Sie mehr über SVM Disaster Recovery".

Versionshinweise zu Cloud Volumes ONTAP

Die Versionshinweise für Cloud Volumes ONTAP enthalten versionsspezifische

Informationen. Neu in dieser Version, unterstützte Konfigurationen, Storage-Einschränkungen und alle bekannten Einschränkungen oder Probleme, die sich auf die Produktfunktionen auswirken können.

"Wechseln Sie zu den Versionshinweisen zu Cloud Volumes ONTAP"

Los geht’s

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.

  Cloud Volumes ONTAP lässt sich auch in BlueXP Backup und Recovery integrieren, um Backup- und Restore-Funktionen zum Schutz und zur langfristigen Archivierung Ihrer Cloud-Daten zu bieten.

  "Erfahren Sie mehr über Backup und Recovery von BlueXP"

- 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.

  "Weitere Informationen zu SnapCenter"

- Datensicherheit

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

- Kontrolloptionen für die Einhaltung des Datenschutzes

  Die Integration in die BlueXP Klassifizierung erleichtert Ihnen das Verständnis des Datenkontexts und die Identifizierung sensibler Daten.

  "Weitere Informationen zur BlueXP Klassifizierung"

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"

Unterstützte ONTAP-Versionen für neue Implementierungen

Mit BlueXP können Sie bei der Erstellung einer neuen Cloud Volumes ONTAP-Arbeitsumgebung aus verschiedenen ONTAP-Versionen auswählen.

Andere als die hier aufgeführten Cloud Volumes ONTAP-Versionen sind nicht für neue Implementierungen verfügbar. Informationen zum Upgrade finden Sie unter "Unterstützte Upgrade-Pfade".

AWS

Single Node

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

HA-Paar

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3

- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

Azure

Single Node

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6
- 9.5 P6

HA-Paar

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6

Google Cloud

Single Node

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

HA-Paar

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

Erste Schritte in Amazon Web Services

Schnellstart für Cloud Volumes ONTAP in AWS

Erste Schritte mit Cloud Volumes ONTAP in AWS

1 **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 Cloud Volumes ONTAP in einem Subnetz bereitstellen möchten, in dem kein Internetzugang verfügbar ist, müssen Sie den Connector manuell installieren und auf die BlueXP Benutzeroberfläche zugreifen, die auf diesem Connector ausgeführt wird. "Erfahren Sie, wie Sie den Connector manuell an einem Ort ohne Internetzugang installieren"

2 Planen Sie Ihre Konfiguration

BlueXP 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 .".

3 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. Outbound-Internetzugang über die Ziel-VPC für NetApp AutoSupport aktivieren

   Dieser Schritt ist nicht erforderlich, wenn Sie Cloud Volumes ONTAP an einem Ort bereitstellen, an dem kein Internetzugang verfügbar ist.

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".

4 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 .".

5 Starten Sie Cloud Volumes ONTAP mit BlueXP

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

- "Erstellen Sie einen Connector in AWS von BlueXP"
- "Erstellen Sie einen Connector aus dem AWS Marketplace"
- "Installieren und Einrichten eines Connectors auf dem Gelände"
- "AWS-Berechtigungen für den Connector"

Planen Sie Ihre Cloud Volumes ONTAP-Konfiguration in AWS

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.

Wählen Sie eine Cloud Volumes ONTAP Lizenz

Für Cloud Volumes ONTAP sind verschiedene Lizenzierungsoptionen verfügbar. Jede Option ermöglicht Ihnen, ein Nutzungsmodell auszuwählen, das Ihren Anforderungen entspricht.

- "Informieren Sie sich über Lizenzoptionen für Cloud Volumes ONTAP"
- "Erfahren Sie, wie Sie eine Lizenzierung einrichten"

Wählen Sie eine unterstützte Region aus

Cloud Volumes ONTAP wird in den meisten AWS Regionen unterstützt. "Hier finden Sie die vollständige Liste der unterstützten Regionen".

Neuere AWS Regionen müssen aktiviert sein, bevor Ressourcen in diesen Regionen erstellt und gemanagt werden können. "Erfahren Sie, wie Sie eine Region aktivieren".

Wählen Sie eine unterstützte lokale Zone aus

Cloud Volumes ONTAP wird in einigen AWS lokalen Zonen unterstützt, einschließlich Singapur. Die Auswahl einer lokalen Zone ist optional.

"Sehen Sie sich die vollständige Liste der lokalen Zonen an".
Lokale Zonen müssen aktiviert sein, bevor Sie Ressourcen in diesen Zonen erstellen und verwalten können.

"Erfahren Sie, wie Sie eine lokale Zone aktivieren".

Phoenix ist keine unterstützte lokale Zone.

Wählen Sie eine unterstützte Instanz aus

Cloud Volumes ONTAP unterstützt je nach gewähltem Lizenztyp mehrere Instanztypen.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in AWS"

Analysieren Sie Ihre Storage-Grenzen

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 in AWS"

Größe des 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

Auf höherer Ebene unterscheiden sich die EBS-Festplattentypen wie folgt. Weitere Informationen zu den Anwendungsfällen für EBS-Festplatten finden Sie unter "AWS Dokumentation: EBS Volume-Typen".

- *General Purpose SSD (gp3)* Festplatten sind die kostengünstigsten SSDs, die ein ausgewogenes Verhältnis zwischen Kosten und Performance für ein breites Spektrum an Workloads bieten. Die Performance wird hinsichtlich IOPS und Durchsatz definiert. gp3-Festplatten werden von Cloud Volumes ONTAP 9.7 und höher unterstützt.

  Wenn Sie eine gp3-Festplatte auswählen, füllt BlueXP die Standard-IOPS- und Durchsatzwerte, die eine Performance liefern, die einer gp2-Festplatte entspricht, die auf der ausgewählten Festplattengröße basiert. Sie können die Werte erhöhen, um eine bessere Leistung zu einem höheren Preis zu erhalten, aber wir unterstützen keine niedrigeren Werte, weil es zu einer minderwertigen Leistung führen kann. Kurz gesagt: Halten Sie bei den Standardwerten an, oder erhöhen Sie sie. Senken Sie Ihre Storage-Kosten nicht. "Erfahren Sie mehr über gp3-Festplatten und deren Leistung".

  Beachten Sie, dass Cloud Volumes ONTAP die Funktion Amazon EBS Elastic Volumes mit gp3-Festplatten unterstützt. "Weitere Informationen zur Unterstützung von Elastic Volumes".

- *General Purpose SSD (gp2)* Festplatten ausgewogenes Verhältnis zwischen Kosten und Performance für ein breites Spektrum an Workloads. Die Performance wird in Bezug auf IOPS definiert.
- *Bereitgestellte IOPS-SSD (io1)* Festplatten sind für kritische Applikationen geeignet, die die höchste Performance zu höheren Kosten erfordern.

  Beachten Sie, dass Cloud Volumes ONTAP die elastische Amazon EBS Volumes-Funktion mit io1-Festplatten unterstützt. "Weitere Informationen zur Unterstützung von Elastic Volumes".

- *Throughput Optimized HDD (st1)* Festplatten sind für häufig abgerufene Workloads, die einen schnellen und konsistenten Durchsatz zu einem niedrigeren Preis erfordern.

  Bei der Verwendung von durchsatzoptimierten HDDs (st1) wird kein Tiering von Daten zu Objekt-Storage empfohlen.

EBS-Festplattengröße

Wenn Sie eine Konfiguration wählen, die das nicht unterstützt "Amazon EBS Elastic Volumes Funktion", Dann müssen Sie eine anfängliche Festplattengröße wählen, wenn Sie ein Cloud Volumes ONTAP-System starten. Danach können Sie "BlueXP verwaltet 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.
- Auch wenn Sie größere Festplatten wählen (zum Beispiel sechs 4-tib-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".

  Wie bereits erwähnt, wird die Auswahl einer Festplattengröße mit Cloud Volumes ONTAP-Konfigurationen, die die Elastic Volumes-Funktion von Amazon EBS unterstützen, nicht unterstützt. "Weitere Informationen zur Unterstützung von Elastic Volumes".

Anzeigen von Standard-Systemfestplatten

Neben dem Storage für Benutzerdaten erwirbt BlueXP auch Cloud-Storage für Cloud Volumes ONTAP Systemdaten (Boot-Daten, Root-Daten, Core-Daten und NVRAM). Für die Planung können Sie diese Details überprüfen, bevor Sie Cloud Volumes ONTAP implementieren.

"Zeigen Sie die Standardfestplatten für Cloud Volumes ONTAP-Systemdaten in AWS an".

Für den Connector ist außerdem eine Systemfestplatte erforderlich. "Zeigen Sie Details zur Standardkonfiguration des Connectors an".

Bereiten Sie sich auf die Implementierung von Cloud Volumes ONTAP in einem AWS-Outpost vor

Wenn Sie einen AWS-Outpost haben, können Sie Cloud Volumes ONTAP in diesem Outpost implementieren, indem Sie die VPC-Outpost im Assistenten zur Arbeitsumgebung auswählen. Die Erfahrung ist mit jeder anderen VPC, die in AWS residiert. Beachten Sie, dass Sie zunächst einen Connector in Ihrem AWS Outpost implementieren müssen.

Es bestehen einige Einschränkungen, die darauf hinweisen:

- Derzeit werden nur Cloud Volumes ONTAP Systeme mit einzelnen Nodes unterstützt
- Die EC2 Instanzen, die Sie mit Cloud Volumes ONTAP verwenden können, sind auf die in Ihrem Outpost verfügbaren EC2-Instanzen beschränkt
- Derzeit werden nur General Purpose SSDs (gp2) unterstützt

Sammeln von Netzwerkinformationen

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.

Single Node oder HA-Paar in einer einzelnen Verfügbarkeitszone

AWS-Informationen	Ihr Wert
Region	
VPC	

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

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	

Wählen Sie eine Schreibgeschwindigkeit

Mit BlueXP können Sie eine Schreibgeschwindigkeitseinstellung für Cloud Volumes ONTAP auswählen. 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. "Erfahren Sie mehr über Schreibgeschwindigkeit".

Wählen Sie ein Volume-Auslastungsprofil aus

ONTAP umfasst mehrere Storage-Effizienzfunktionen, mit denen Sie die benötigte Storage-Gesamtmenge reduzieren können. Wenn Sie ein Volume in BlueXP 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

BlueXP übernimmt die Einrichtung von Netzwerkkomponenten für Cloud Volumes ONTAP, z. B. IP-Adressen, Netzmasken und Routen. Sie müssen sicherstellen, dass Outbound-Internetzugang verfügbar ist, dass genügend private IP-Adressen verfügbar sind, dass die richtigen Verbindungen vorhanden sind und vieles mehr.

Allgemeine Anforderungen

Die folgenden Anforderungen müssen in AWS erfüllt sein.

Outbound-Internetzugang für Cloud Volumes ONTAP Nodes

Cloud Volumes ONTAP Nodes benötigen Outbound-Internetzugang für NetApp AutoSupport, der den Zustand Ihres Systems proaktiv überwacht und Meldungen an den technischen Support von NetApp sendet.

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

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

Wenn keine ausgehende Internetverbindung zum Senden von AutoSupport-Nachrichten verfügbar ist, konfiguriert BlueXP Ihre Cloud Volumes ONTAP-Systeme automatisch so, dass der Connector als Proxy-Server verwendet wird. Die einzige Anforderung besteht darin, sicherzustellen, dass die Sicherheitsgruppe des Connectors *eingehende* -Verbindungen über Port 3128 zulässt. Nach der Bereitstellung des Connectors müssen Sie diesen Port öffnen.

Wenn Sie strenge ausgehende Regeln für Cloud Volumes ONTAP definiert haben, müssen Sie auch sicherstellen, dass die Cloud Volumes ONTAP-Sicherheitsgruppe *Outbound*-Verbindungen über Port 3128 zulässt.

Nachdem Sie bestätigt haben, dass der ausgehende Internetzugang verfügbar ist, können Sie AutoSupport testen, um sicherzustellen, dass er Nachrichten senden kann. Anweisungen finden Sie unter "ONTAP Dokumentation: Einrichten von AutoSupport".

Wenn Sie von BlueXP darüber informiert werden, dass AutoSupport-Meldungen nicht gesendet werden können, "Fehler bei der AutoSupport Konfiguration beheben".

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)".

Private IP-Adressen

BlueXP weist Cloud Volumes ONTAP automatisch die erforderliche Anzahl privater IP-Adressen zu. Sie müssen sicherstellen, dass Ihrem Netzwerk genügend private IP-Adressen zur Verfügung stehen.

Die Anzahl der LIFs, die BlueXP für Cloud Volumes ONTAP zuweist, hängt davon ab, ob Sie ein Single Node-System oder ein HA-Paar implementieren. Ein LIF ist eine IP-Adresse, die einem physischen Port zugewiesen ist.

IP-Adressen für ein Single Node-System

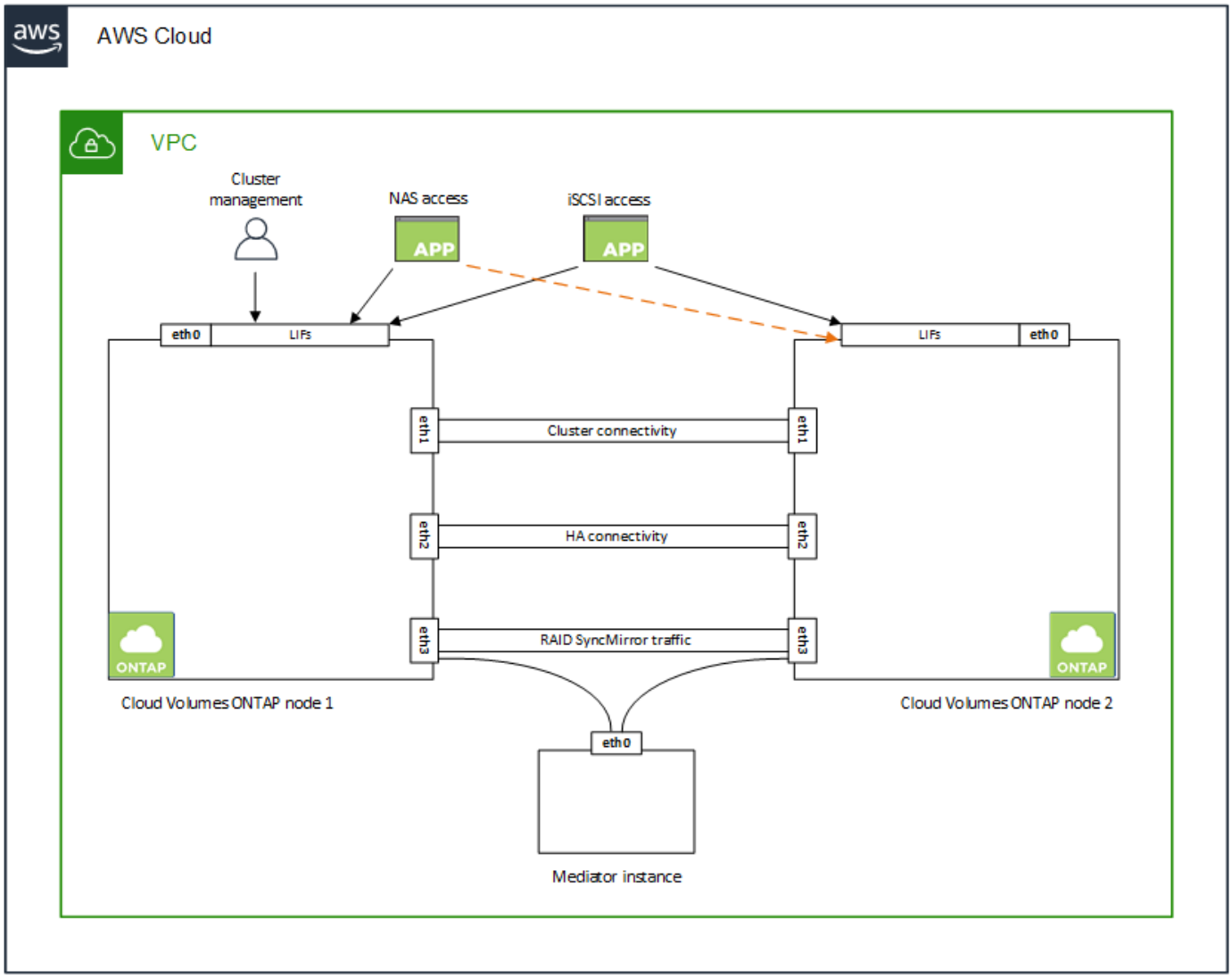
BlueXP weist einem System mit einem einzelnen Node 6 IP-Adressen zu.

Die folgende Tabelle enthält Details zu den LIFs, die mit jeder privaten IP-Adresse verknüpft sind.

LIF	Zweck
Cluster-Management	Administrative Verwaltung des gesamten Clusters (HA-Paar).
Node-Management	Administrationsmanagement eines Node
Intercluster	Cluster-übergreifende Kommunikation, Backup und Replizierung
NAS-Daten	Client-Zugriff über NAS-Protokolle.
ISCSI-Daten	Client-Zugriff über das iSCSI-Protokoll. Wird vom System auch für andere wichtige Netzwerk-Workflows eingesetzt. Dieses LIF ist erforderlich und sollte nicht gelöscht werden.
Storage-VM-Management	Ein Storage-VM-Management-LIF wird mit Managementtools wie SnapCenter verwendet.

IP-Adressen für HA-Paare

HA-Paare benötigen mehr IP-Adressen als ein System mit einem einzelnen Node. Diese IP-Adressen werden über verschiedene ethernet-Schnittstellen verteilt, wie im folgenden Bild dargestellt:



Die Anzahl der für ein HA-Paar erforderlichen privaten IP-Adressen hängt vom ausgewählten Implementierungsmodell ab. Ein in einer *Single* AWS Availability Zone (AZ) implementiertes HA-Paar benötigt 15 Private IP-Adressen, während ein in *multiple* AZS implementiertes HA-Paar 13 Private IP-Adressen erfordert.

Die folgenden Tabellen enthalten Details zu den LIFs, die mit den einzelnen privaten IP-Adressen verknüpft sind.

LIFs für HA-Paare in einer einzelnen Verfügbarkeitszone

LIF	Schnittstelle	Knoten	Zweck
Cluster-Management	Eth0	Knoten 1	Administrative Verwaltung des gesamten Clusters (HA-Paar).
Node-Management	Eth0	Node 1 und Node 2	Administrationsmanagement eines Node
Intercluster	Eth0	Node 1 und Node 2	Cluster-übergreifende Kommunikation, Backup und Replizierung
NAS-Daten	Eth0	Knoten 1	Client-Zugriff über NAS-Protokolle.

LIF	Schnittstelle	Knoten	Zweck
ISCSI-Daten	Eth0	Node 1 und Node 2	Client-Zugriff über das iSCSI-Protokoll. Wird vom System auch für andere wichtige Netzwerk-Workflows eingesetzt. Diese LIFs sind erforderlich und sollten nicht gelöscht werden.
Cluster-Konnektivität	Eth1	Node 1 und Node 2	Ermöglicht die Kommunikation der Nodes und das Verschieben von Daten innerhalb des Clusters.
HA-Konnektivität	Eth2	Node 1 und Node 2	Kommunikation zwischen den beiden Knoten im Failover-Fall.
RSM-iSCSI-Datenverkehr	Eth3	Node 1 und Node 2	RAID SyncMirror iSCSI-Datenverkehr sowie die Kommunikation zwischen den beiden Cloud Volumes ONTAP-Nodes und dem Mediator.
Mediator	Eth0	Mediator	Kommunikationskanal zwischen den Nodes und dem Mediator zur Unterstützung bei Storage-Takeover- und Giveback-Prozessen

LIFs für HA-Paare in mehreren Verfügbarkeitszonen

LIF	Schnittstelle	Knoten	Zweck
Node-Management	Eth0	Node 1 und Node 2	Administrationsmanagement eines Node
Intercluster	Eth0	Node 1 und Node 2	Cluster-übergreifende Kommunikation, Backup und Replizierung
ISCSI-Daten	Eth0	Node 1 und Node 2	Client-Zugriff über das iSCSI-Protokoll. Diese LIFs managen zudem die Migration von fließenden IP-Adressen zwischen Nodes. Diese LIFs sind erforderlich und sollten nicht gelöscht werden.
Cluster-Konnektivität	Eth1	Node 1 und Node 2	Ermöglicht die Kommunikation der Nodes und das Verschieben von Daten innerhalb des Clusters.
HA-Konnektivität	Eth2	Node 1 und Node 2	Kommunikation zwischen den beiden Knoten im Failover-Fall.
RSM-iSCSI-Datenverkehr	Eth3	Node 1 und Node 2	RAID SyncMirror iSCSI-Datenverkehr sowie die Kommunikation zwischen den beiden Cloud Volumes ONTAP-Nodes und dem Mediator.
Mediator	Eth0	Mediator	Kommunikationskanal zwischen den Nodes und dem Mediator zur Unterstützung bei Storage-Takeover- und Giveback-Prozessen

Wenn eine Implementierung in mehreren Verfügbarkeitszonen erstellt wird, werden mehrere LIFs zugeordnet "Floating-IP-Adressen", Die nicht gegen die private IP-Beschränkung von AWS gezählt werden.

Sicherheitsgruppen

Sie müssen keine Sicherheitsgruppen erstellen, weil BlueXP das für Sie tut. Wenn Sie Ihr eigenes verwenden müssen, lesen Sie "Regeln für Sicherheitsgruppen".

Sie suchen Informationen über den Connector? "Zeigen Sie die Sicherheitsgruppenregeln für den Konnektor an"

Verbindung für Daten-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

Um Daten zwischen einem Cloud Volumes ONTAP System in AWS und ONTAP Systemen in anderen Netzwerken zu replizieren, müssen Sie eine VPN-Verbindung zwischen der AWS VPC und dem anderen Netzwerk herstellen, beispielsweise das 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".

VPC-Sharing

Ab Version 9.11.1 werden Cloud Volumes ONTAP HA-Paare in AWS mit VPC-Sharing unterstützt. Die VPC-Freigabe ermöglicht Ihrem Unternehmen, Subnetze mit anderen AWS Konten gemeinsam zu nutzen. Um diese Konfiguration zu verwenden, müssen Sie Ihre AWS-Umgebung einrichten und dann das HA-Paar mithilfe der API implementieren.

"Erfahren Sie, wie ein HA-Paar in einem gemeinsamen Subnetz implementiert wird".

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 überprüfen, bevor Sie ein HA-Paar starten, da Sie beim Erstellen der Arbeitsumgebung die Netzwerkdetails in BlueXP 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.

In jeder Verfügbarkeitszone sollte ein Subnetz verfügbar sein.

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".

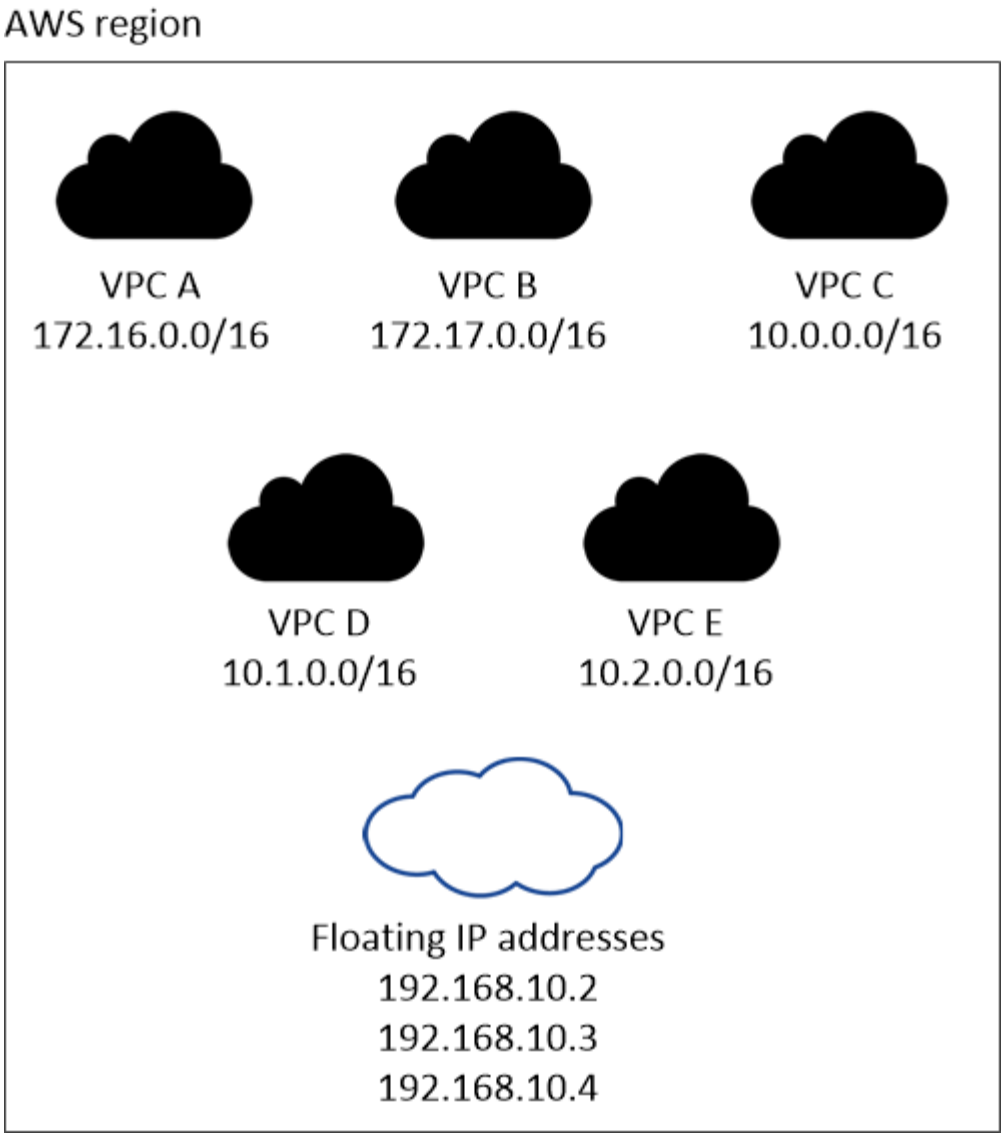
Eine Floating-IP-Adresse ist für das Cluster-Management, eine für NFS/CIFS-Daten auf Node 1 und eine für NFS/CIFS-Daten auf Node 2. Eine vierte Floating IP-Adresse für SVM-Management ist optional.

> Wenn Sie SnapDrive für Windows oder SnapCenter mit dem HA-Paar verwenden, ist eine unverankerte IP-Adresse für die SVM-Management-LIF erforderlich.

Sie müssen die unverankerten IP-Adressen in BlueXP eingeben, wenn Sie eine Arbeitsumgebung mit Cloud Volumes ONTAP HA erstellen. BlueXP weist dem HA-Paar die IP-Adressen zu, wenn das System gestartet wird.

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.



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

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

Bei Bedarf "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 BlueXP die unverankerten IP-Adressen angegeben haben, werden Sie dann aufgefordert, die Routingtabellen auszuwählen, die Routen zu den unverankerten IP-Adressen enthalten sollen. Dies ermöglicht den Client-Zugriff auf das HA-Paar.

Wenn Sie nur eine Routingtabelle für die Subnetze in Ihrem VPC (der Hauptroutingtabelle) haben, fügt BlueXP automatisch die fließenden IP-Adressen zu dieser Routingtabelle 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".

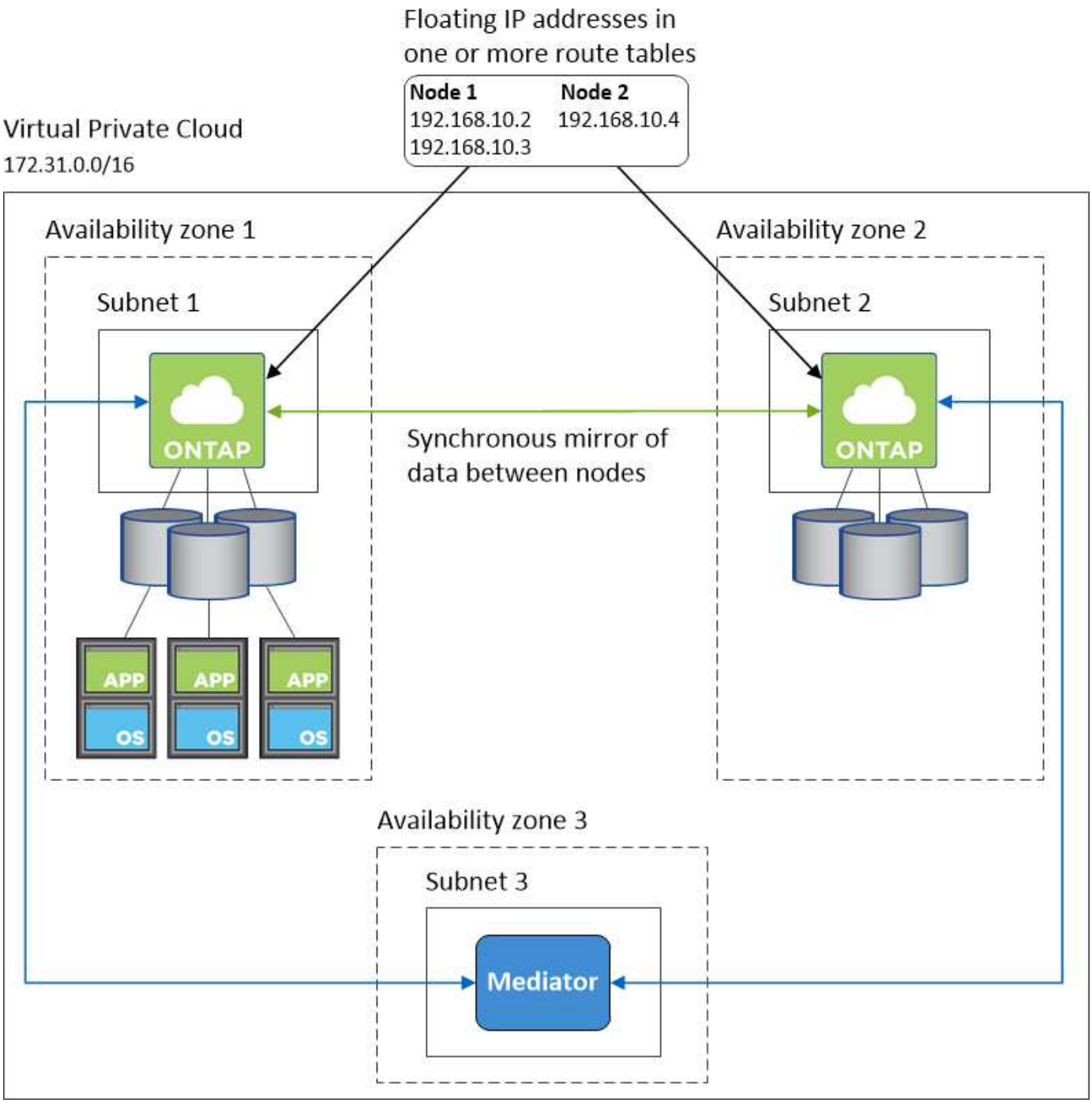
Anbindung an NetApp Management Tools

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

Das folgende Bild zeigt die Netzwerkkomponenten, die für ein HA-Paar in mehreren Verfügbarkeitszonen spezifisch sind: Drei Verfügbarkeitszonen, drei Subnetze, fließende IP-Adressen und eine Routingtabelle.



Anforderungen an den Steckverbinder

Wenn Sie noch keinen Connector erstellt haben, sollten Sie auch die Netzwerkanforderungen für den Connector prüfen.

- "Zeigen Sie die Netzwerkanforderungen für den Connector an"
- "Sicherheitsgruppenregeln in AWS"

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

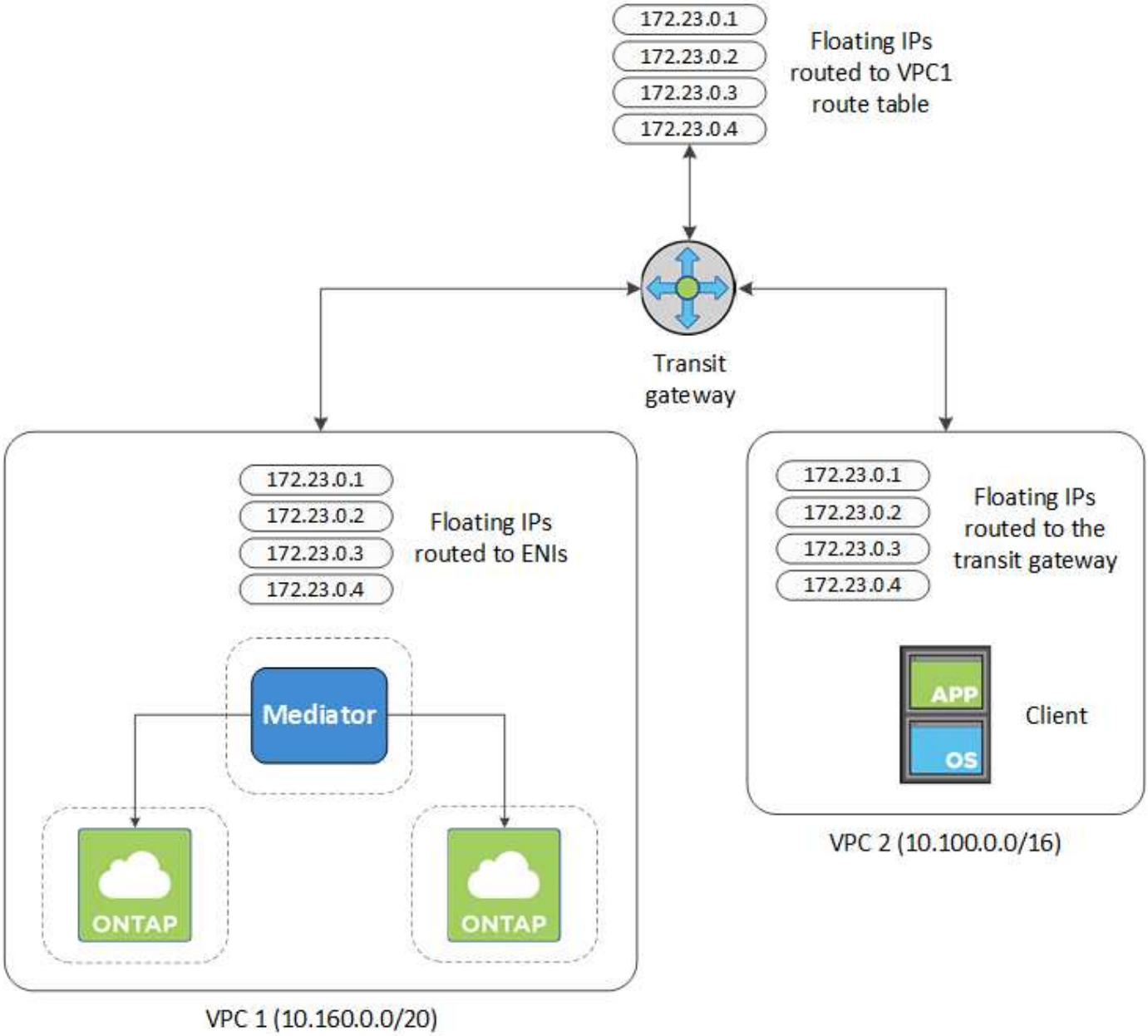
Einrichten eines AWS Transit-Gateways für den Zugriff auf HA-Paare "Floating-IP-Adressen" Von außerhalb der VPC, wo das HA-Paar residiert.

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.

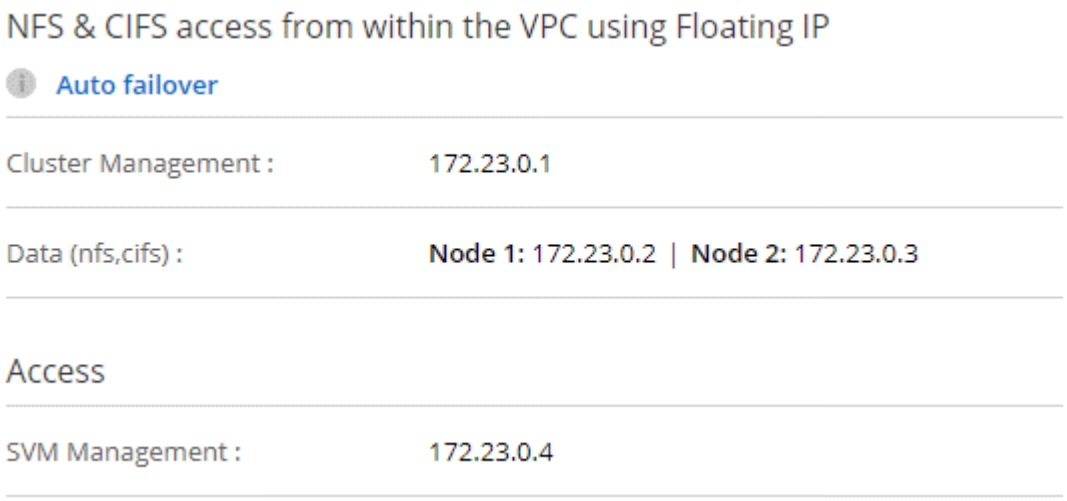


Die folgenden Schritte veranschaulichen die Einrichtung einer ähnlichen Konfiguration.

Schritte

1. "Erstellen Sie ein Transit-Gateway, und verbinden Sie die VPCs mit dem Gateway".
2. Weisen Sie die VPCs der Routing-Gateway-Routingtabelle zu.
   a. Klicken Sie im Dienst * VPC* auf **Transit Gateway Route Tables**.
   b. Wählen Sie die Routentabelle aus.
   c. Klicken Sie auf **Verknüpfungen** und wählen Sie dann **Verknüpfung erstellen** aus.
   d. Wählen Sie die Anhänge (die VPCs) aus, die Sie verknüpfen möchten, und klicken Sie dann auf **Verknüpfung erstellen**.
3. 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 BlueXP. Hier ein Beispiel:



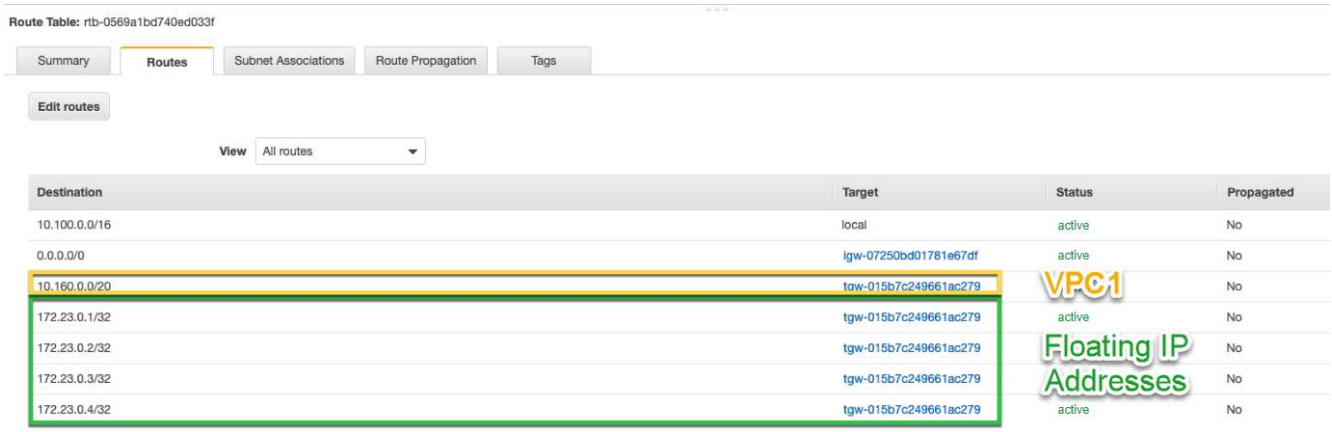
   Das folgende Beispielbild zeigt die Routingtabelle für das Transit Gateway. Er umfasst Routen zu den CIDR-Blöcken der zwei VPCs und vier von Cloud Volumes ONTAP verwendete Floating IP-Adressen.

4. 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.

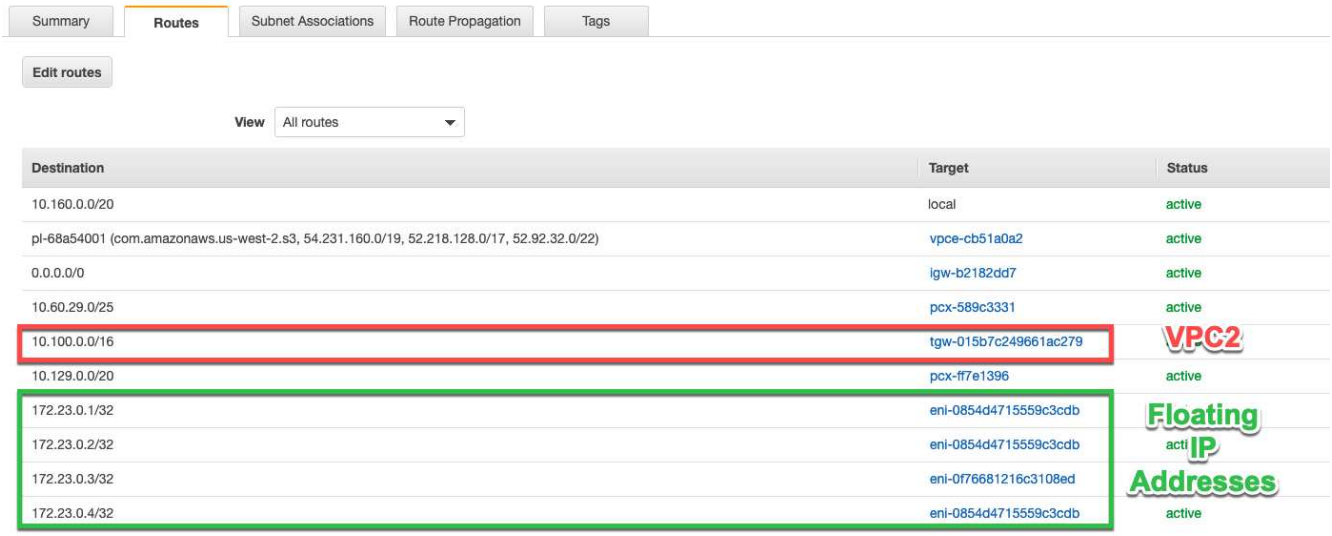
      Das folgende Beispielbild zeigt die Routingtabelle für VPC 2, die auch Routen zu VPC 1 und die fließenden IP-Adressen umfasst.



5. 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. BlueXP hat beim Einsatz des HA-Paars automatisch die unverankerten IPs zur Routingtabelle hinzugefügt.



6. Aktualisieren Sie die Einstellungen der Sicherheitsgruppen auf Alle Daten für die VPC.

   a. Klicken Sie unter Virtual Private Cloud auf **Subnetze**.

   b. Klicken Sie auf die Registerkarte **Route table** und wählen Sie die gewünschte Umgebung für eine der fließenden IP-Adressen für ein HA-Paar aus.

   c. Klicken Sie auf **Sicherheitsgruppen**.

d. Wählen Sie **Inbound Rules Bearbeiten**.

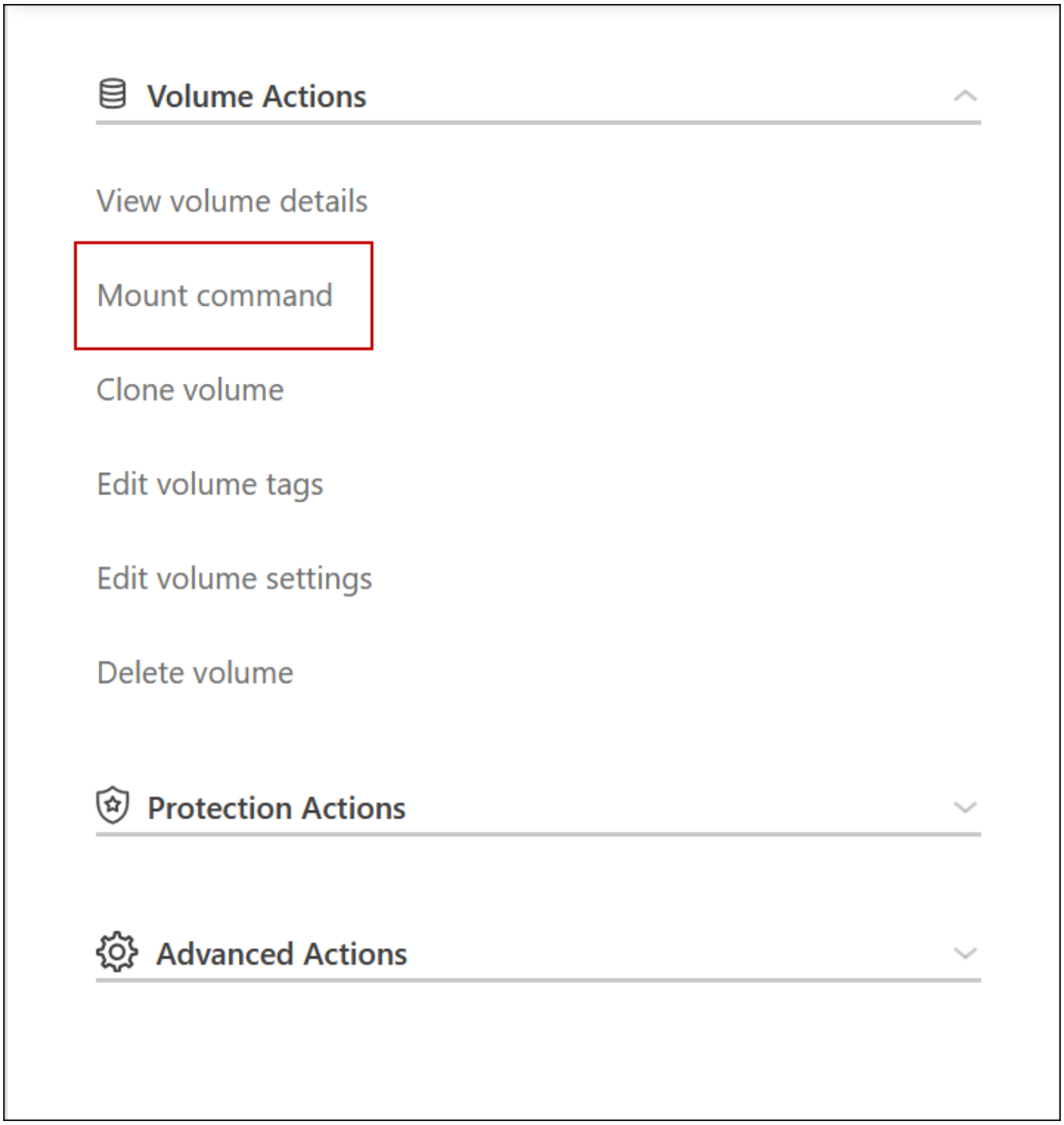
e. Klicken Sie auf **Regel hinzufügen**.

f. Wählen Sie unter Typ **All Traffic** aus, und wählen Sie dann die VPC-IP-Adresse aus.

g. Klicken Sie auf **Regeln speichern**, um die Änderungen anzuwenden.

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

   Die richtige IP-Adresse finden Sie in BlueXP über die Option **Mount Command** im Bereich Volumes verwalten in BlueXP.



8. Wenn Sie ein NFS-Volume mounten, konfigurieren Sie die Exportrichtlinie entsprechend dem Subnetz der Client-VPC.

"Erfahren Sie, wie Sie ein Volume bearbeiten".

Verwandte Links

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

Implementieren Sie ein HA-Paar in einem gemeinsamen Subnetz

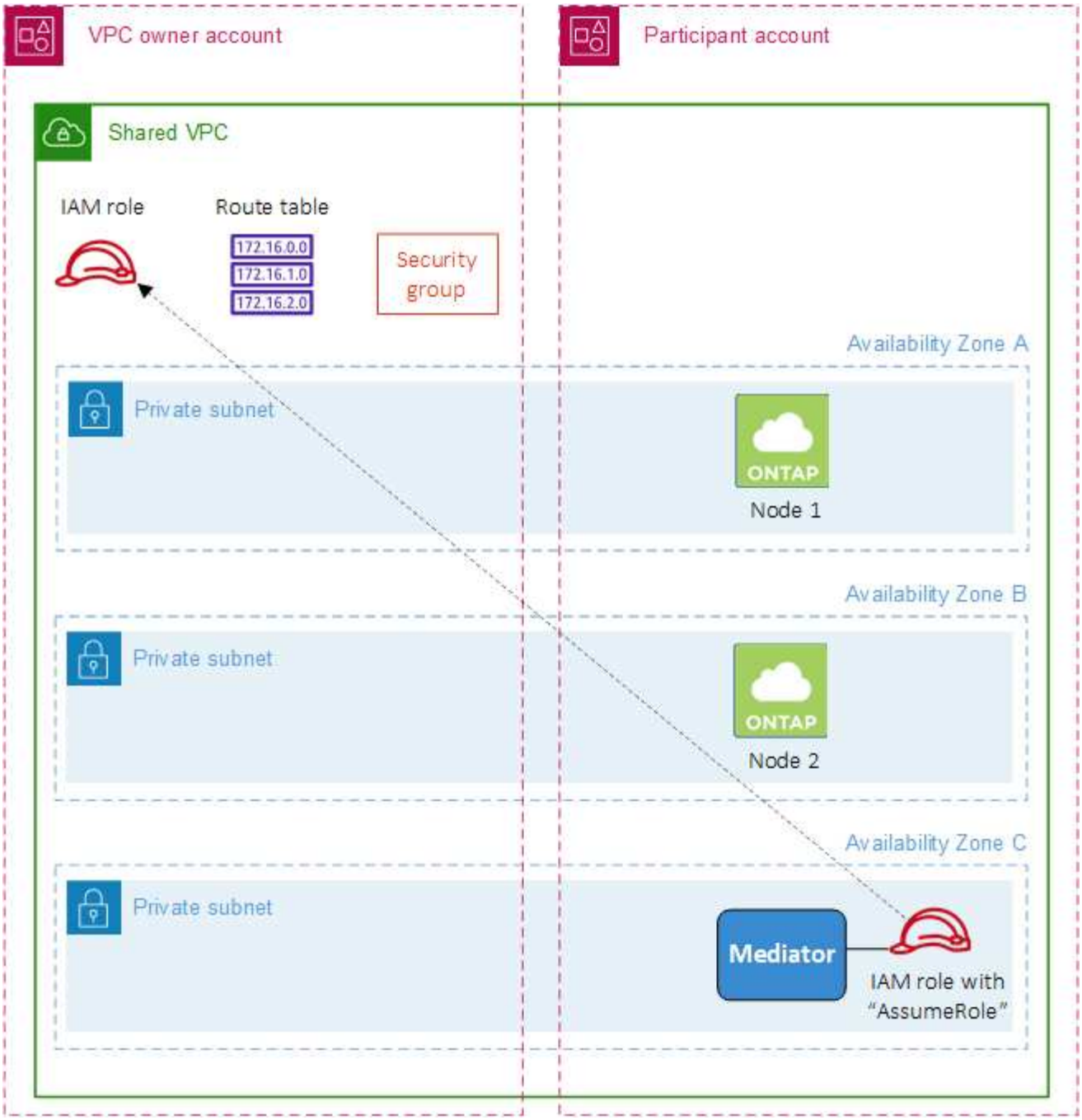
Ab Version 9.11.1 werden Cloud Volumes ONTAP HA-Paare in AWS mit VPC-Sharing unterstützt. Die VPC-Freigabe ermöglicht Ihrem Unternehmen, Subnetze mit anderen AWS Konten gemeinsam zu nutzen. Um diese Konfiguration zu verwenden, müssen Sie Ihre AWS-Umgebung einrichten und dann das HA-Paar mithilfe der API implementieren.

Mit "VPC-Sharing", Eine Cloud Volumes ONTAP HA-Konfiguration ist auf zwei Konten verteilt:

- Das VPC-Owner-Konto, zu dem das Netzwerk gehört (VPC, Subnetze, Routing-Tabellen und Cloud Volumes ONTAP-Sicherheitsgruppe)
- Das Teilnehmerkonto, bei dem die EC2 Instanzen in gemeinsam genutzten Subnetzen implementiert werden (dazu gehören die zwei HA-Nodes und der Mediator)

Bei einer Cloud Volumes ONTAP HA-Konfiguration, die über mehrere Verfügbarkeitszonen hinweg implementiert wird, benötigt der HA-Mediator spezifische Berechtigungen, um die Routing-Tabellen im VPC-Owner-Konto zu schreiben. Sie müssen diese Berechtigungen bereitstellen, indem Sie eine IAM-Rolle einrichten, die der Mediator übernehmen kann.

Das folgende Bild zeigt die betroffenen Komponenten für die Implementierung:



Wie in den unten beschriebenen Schritten beschrieben, müssen Sie die Subnetze dem Teilnehmerkonto teilen und anschließend die IAM-Rolle und Sicherheitsgruppe im VPC-Owner-Konto erstellen.

Beim Erstellen der Arbeitsumgebung von Cloud Volumes ONTAP erstellt BlueXP automatisch eine IAM-Rolle und fügt sie dem Mediator an. Bei dieser Rolle wird die IAM-Rolle angenommen, die Sie im VPC-Owner-Konto erstellt haben, um Änderungen an den Routingtabellen vorzunehmen, die mit dem HA-Paar verknüpft sind.

Schritte

1. Teilen Sie die Subnetze im VPC-Owner-Konto mit dem Teilnehmerkonto.

   Dieser Schritt ist erforderlich, um das HA-Paar in gemeinsam genutzten Subnetzen zu implementieren.

   "AWS Dokumentation: Ein Subnetz gemeinsam nutzen"

2. Erstellen Sie im VPC-Owner-Konto eine Sicherheitsgruppe für Cloud Volumes ONTAP.

   "Beachten Sie die Regeln für Cloud Volumes ONTAP in den Sicherheitsgruppen". Beachten Sie, dass Sie keine Sicherheitsgruppe für den HA Mediator erstellen müssen. BlueXP ist das für Sie.

3. Erstellen Sie im VPC-Owner-Konto eine IAM-Rolle, die die folgenden Berechtigungen enthält:

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. Verwenden Sie die BlueXP API, um eine neue Cloud Volumes ONTAP-Arbeitsumgebung zu erstellen.

   Beachten Sie, dass Sie die folgenden Felder angeben müssen:

   - „SicherheitGruppeID“

     Im Feld „securityGroupID“ sollte die Sicherheitsgruppe angegeben werden, die Sie im VPC-Owner-Konto erstellt haben (siehe Schritt 2 oben).

   - "AssumeeRoleArn" im Objekt "haParams"

     Das Feld „assumeRoleArn“ sollte den ARN der IAM-Rolle enthalten, die Sie im VPC-Owner-Konto erstellt haben (siehe Schritt 3 oben).

     Beispiel:

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

   +
   "Erfahren Sie mehr über die Cloud Volumes ONTAP-API"

Sicherheitsgruppenregeln für AWS

BlueXP erstellt AWS Sicherheitsgruppen mit den ein- und ausgehenden Regeln, die für den erfolgreichen Betrieb von Cloud Volumes ONTAP erforderlich sind. Sie können sich zu Testzwecken auf die Ports beziehen oder wenn Sie Ihre eigenen Sicherheitsgruppen verwenden möchten.

Regeln für Cloud Volumes ONTAP

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

Regeln für eingehende Anrufe

Wenn Sie eine Arbeitsumgebung erstellen und eine vordefinierte Sicherheitsgruppe auswählen, können Sie den Datenverkehr innerhalb einer der folgenden Optionen zulassen:

- **Nur gewählte VPC**: Die Quelle für eingehenden Datenverkehr ist der Subnetz-Bereich des VPC für das Cloud Volumes ONTAP-System und der Subnetz-Bereich des VPC, in dem sich der Connector befindet. Dies ist die empfohlene Option.
- **Alle VPCs**: Die Quelle für eingehenden Datenverkehr ist der IP-Bereich 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	Konnektivität mit dem Connector und 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

Protokoll	Port	Zweck
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
AutoSupport	HTTPS	443	Node Management-LIF	support.netapp.com	AutoSupport (HTTPS ist der Standard)
	HTTP	80	Node Management-LIF	support.netapp.com	AutoSupport (nur wenn das Transportprotokoll von HTTPS zu HTTP geändert wird)
	TCP	3128	Node Management-LIF	Stecker	Senden von AutoSupport-Nachrichten über einen Proxy-Server auf dem Connector, falls keine ausgehende Internetverbindung verfügbar ist
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)
Konfigurations-Backups	HTTP	80	Node Management-LIF	\Http://<connector-IP-address>/occm/offboxconfig	Senden Sie Konfigurationssicherungen an den Connector. "Informationen zu Backup-Dateien für die Konfiguration".
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

Service	Protokoll	Port	Quelle	Ziel	Zweck
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 vordefinierte Sicherheitsgruppe für den HA-Mediator umfasst die folgende eingehende Regel.

Protokoll	Port	Quelle	Zweck
TCP	3000	CIDR des Connectors	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	IP-Adresse des Connectors auf der AWS EC2 Instanz	Lade Upgrades für den Mediator herunter
HTTPS	443	ec2.amazonaws.com	Unterstützung bei Storage Failover
UDP	53	ec2.amazonaws.com	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 der HA-Konfiguration

Die vordefinierte interne Sicherheitsgruppe für eine Cloud Volumes ONTAP HA-Konfiguration umfasst die folgenden Regeln: Diese Sicherheitsgruppe ermöglicht die Kommunikation zwischen den HA-Nodes und zwischen dem Mediator und den Nodes.

BlueXP erstellt diese Sicherheitsgruppe immer. 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

"Zeigen Sie die Sicherheitsgruppenregeln für den Konnektor an"

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 BlueXP 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 BlueXP Berechtigungen als *Key-Benutzer* bereitstellt.

   Wenn Sie die IAM-Rolle als Schlüsselbenutzer hinzufügen, erhalten Sie BlueXP Berechtigungen zur Verwendung des CMK mit Cloud Volumes ONTAP.

   "AWS Dokumentation: Schlüssel bearbeiten"

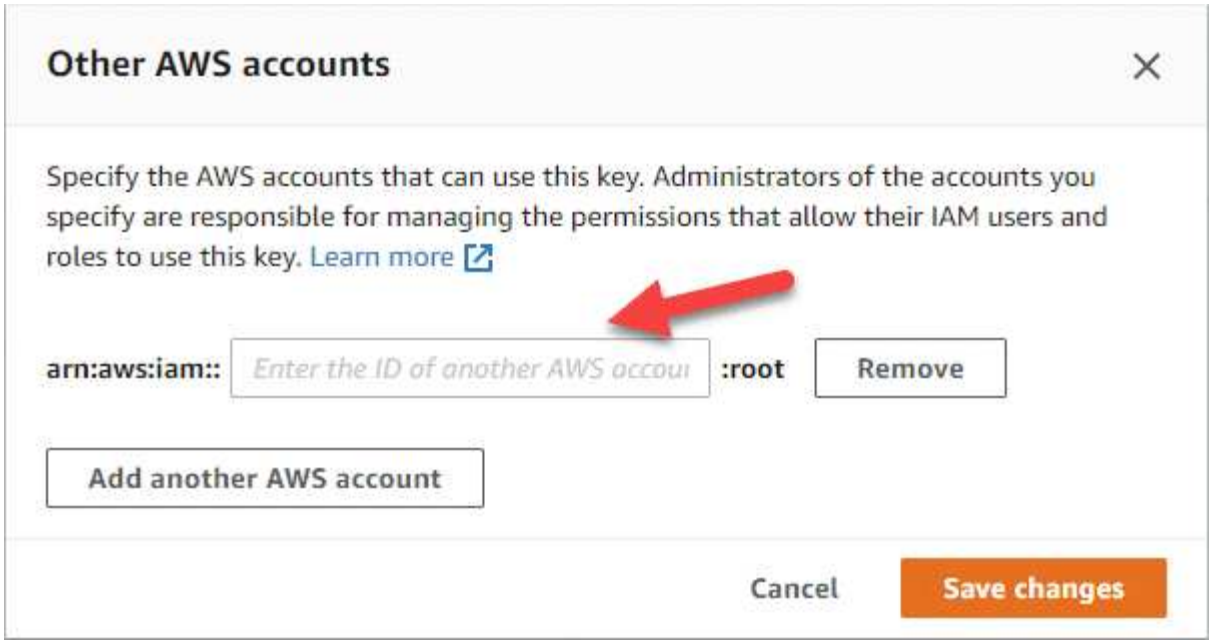
3. Wenn sich das CMK in einem anderen AWS Konto befindet, führen Sie folgende Schritte aus:

   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 BlueXP das ARN zur Verfügung stellen.

   d. Fügen Sie im Bereich **andere AWS-Konten** das AWS-Konto hinzu, das BlueXP mit Berechtigungen versorgt.

      In den meisten Fällen ist dies das Konto, in dem sich BlueXP befindet. Wenn BlueXP nicht in AWS installiert wurde, wäre es das Konto, für das Sie AWS-Zugriffsschlüssel für BlueXP zur Verfügung gestellt haben.



e. Wechseln Sie nun zu dem AWS Konto, das BlueXP mit Berechtigungen versorgt, 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 BlueXP bereitstellt.

   Die folgende Richtlinie enthält die Berechtigungen, die BlueXP zur Verwendung des CMK über das externe 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: Benutzer in anderen Konten können einen KMS-Schlüssel verwenden".

4. Wenn Sie ein vom Kunden verwaltetes CMK verwenden, ändern Sie die Schlüsselrichtlinie für das CMK, indem Sie die Cloud Volumes ONTAP IAM-Rolle als *Key User* hinzufügen.

Dieser Schritt ist erforderlich, wenn Sie Daten-Tiering auf Cloud Volumes ONTAP aktiviert und die im S3-Bucket gespeicherten Daten verschlüsseln möchten.

Sie müssen diesen Schritt durchführen *nach* Sie implementieren Cloud Volumes ONTAP, da die IAM-Rolle beim Erstellen einer Arbeitsumgebung erstellt wird. (Natürlich haben Sie die Möglichkeit, eine vorhandene Cloud Volumes ONTAP IAM-Rolle zu verwenden, sodass Sie diesen Schritt zuvor ausführen können.)

"AWS Dokumentation: Schlüssel bearbeiten"

Einrichten von IAM-Rollen für Cloud Volumes ONTAP

IAM-Rollen mit den erforderlichen Berechtigungen müssen an jeden Cloud Volumes ONTAP-Knoten angeschlossen sein. Das gleiche gilt für den HA Mediator. Es ist am einfachsten, BlueXP die IAM-Rollen für Sie erstellen zu lassen, aber Sie können Ihre eigenen Rollen verwenden.

Diese Aufgabe ist optional. Wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen, können Sie mit BlueXP standardmäßig die IAM-Rollen für Sie erstellen. Wenn Sie in den Sicherheitsrichtlinien Ihres Unternehmens die IAM-Rollen selbst erstellen müssen, befolgen Sie die folgenden Schritte.

In der AWS Secret Cloud muss Ihre eigene IAM-Rolle angegeben werden. "Erfahren Sie, wie Cloud Volumes ONTAP in C2S eingesetzt wird".

Schritte

1. Wechseln Sie zur AWS IAM-Konsole.
2. IAM-Richtlinien erstellen, die die folgenden Berechtigungen enthalten:
    - Basisrichtlinie für Cloud Volumes ONTAP-Nodes

Standardregionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud (USA) Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Top Secret Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Geheime Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- Backup-Richtlinie für Cloud Volumes ONTAP-Nodes

  Falls Sie BlueXP Backup und Recovery für Ihre Cloud Volumes ONTAP Systeme nutzen möchten, muss die IAM-Rolle für die Nodes die zweite unten dargestellte Richtlinie enthalten.

Standardregionen

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud (USA) Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Top Secret Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Geheime Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- Ha Mediator

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "sts:AssumeRole",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Erstellen Sie eine IAM-Rolle, und hängen Sie die von Ihnen erstellten Richtlinien an die Rolle an.

Ergebnis

Sie können jetzt IAM-Rollen auswählen, wenn Sie eine neue Cloud Volumes ONTAP-Arbeitsumgebung erstellen.

Weitere Informationen

- "AWS Dokumentation: Erstellung von IAM-Richtlinien"
- "AWS Dokumentation: Erstellen von IAM-Rollen"

Lizenzierung für Cloud Volumes ONTAP in AWS einrichten

Nachdem Sie sich für die Lizenzoption entschieden haben, die Sie mit Cloud Volumes ONTAP verwenden möchten, sind einige Schritte erforderlich, bevor Sie beim Erstellen einer neuen Arbeitsumgebung die Lizenzoption wählen können.

Freimium

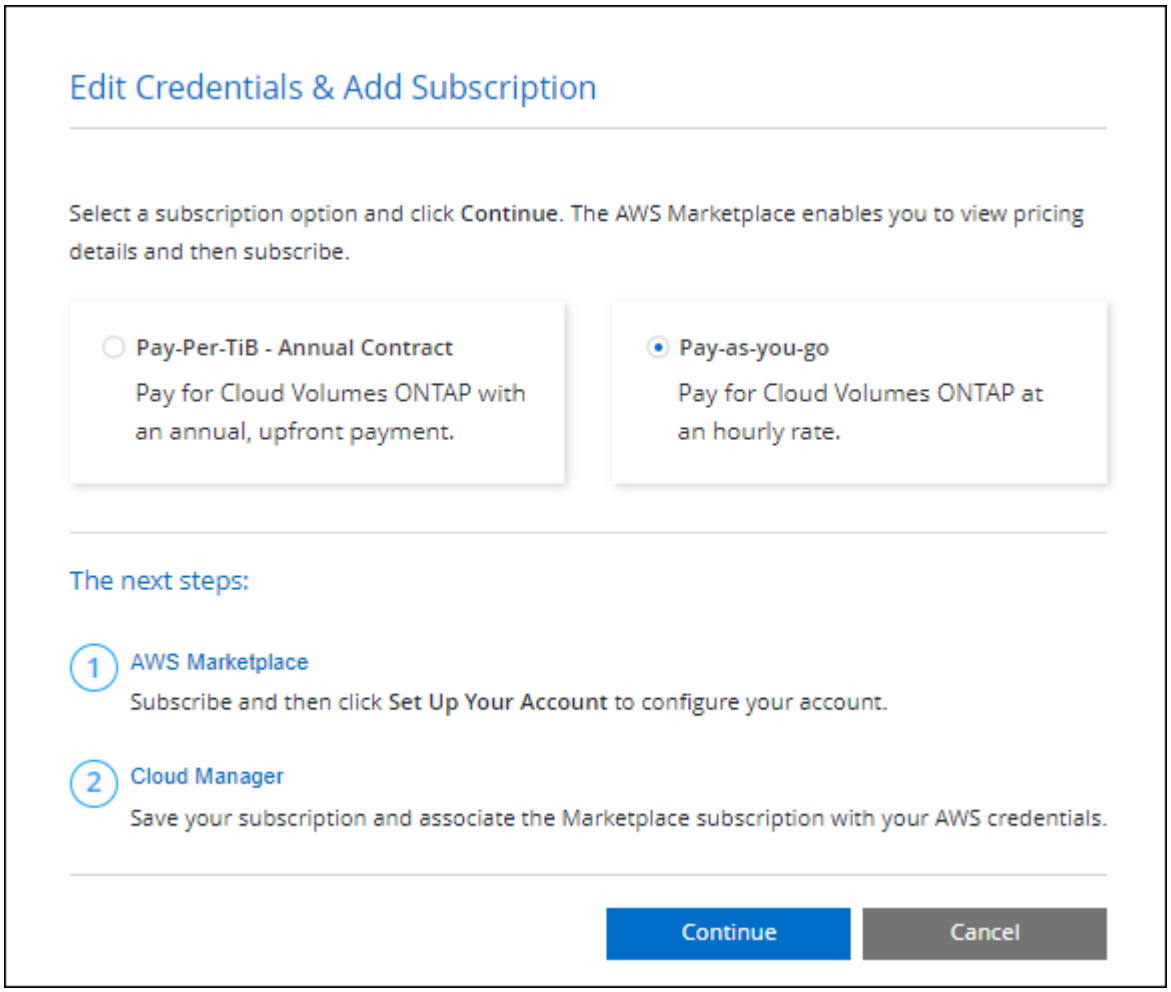
Wählen Sie das Freimium-Angebot aus, um Cloud Volumes ONTAP mit bis zu 500 gib bereitgestellter Kapazität kostenlos zu nutzen. "Erfahren Sie mehr über das Freemium Angebot".

Schritte

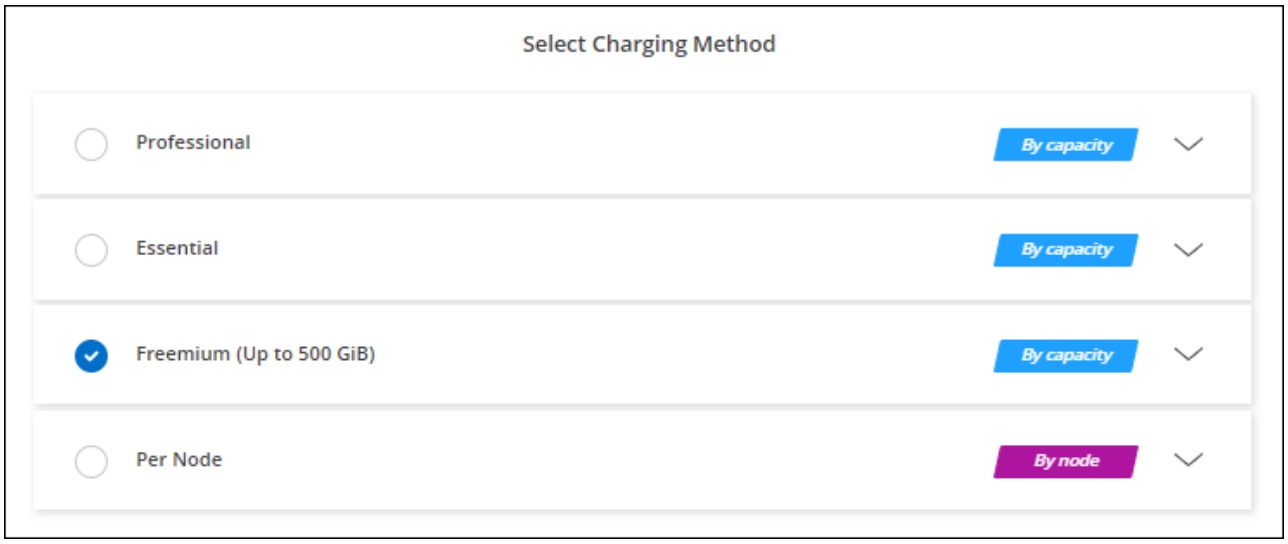
1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.

a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um das Pay-as-you-go-Angebot im AWS Marketplace zu abonnieren.

   Sie werden über das Marketplace-Abonnement nicht belastet, es sei denn, Sie überschreiten 500 gib der bereitgestellten Kapazität. Zu dieser Zeit wird das System automatisch in das konvertiert "Essentials-Paket".



a. Wenn Sie zu BlueXP zurückkehren, wählen Sie **Freemium**, wenn Sie die Seite mit den Lademethoden aufrufen.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen zum Starten von Cloud Volumes ONTAP in AWS an".

Kapazitätsbasierte Lizenz

Dank der kapazitätsbasierten Lizenzierung können Sie für Cloud Volumes ONTAP pro tib Kapazität bezahlen. Kapazitätsbasierte Lizenzierung ist in Form eines *package*, dem Essentials-Paket oder dem Professional-Paket verfügbar.

Die Essentials- und Professional-Pakete sind mit den folgenden Verbrauchsmodellen erhältlich:

- Eine Lizenz (BYOL) von NetApp erworben
- Ein stündliches PAYGO-Abonnement (Pay-as-you-go) über den AWS Marketplace
- Ein Jahresvertrag aus dem AWS Marketplace

"Hier erhalten Sie weitere Informationen zur kapazitätsbasierten Lizenzierung".

In den folgenden Abschnitten werden die ersten Schritte mit jedem dieser Nutzungsmodelle beschrieben.

BYOL

Bezahlen Sie vorab, indem Sie eine Lizenz (BYOL) von NetApp erwerben und Cloud Volumes ONTAP Systeme bei jedem Cloud-Provider implementieren.

Schritte

1. "Wenden Sie sich an den NetApp Sales, um eine Lizenz zu erhalten"
2. "Fügen Sie Ihr Konto für die NetApp Support Website zu BlueXP hinzu"

   BlueXP fragt den NetApp Lizenzierungsservice automatisch ab, um Details zu den Lizenzen zu erhalten, die mit Ihrem NetApp Support Site Konto verknüpft sind. Sollte es keine Fehler geben, fügt BlueXP die Lizenzen automatisch zum Digital Wallet hinzu.

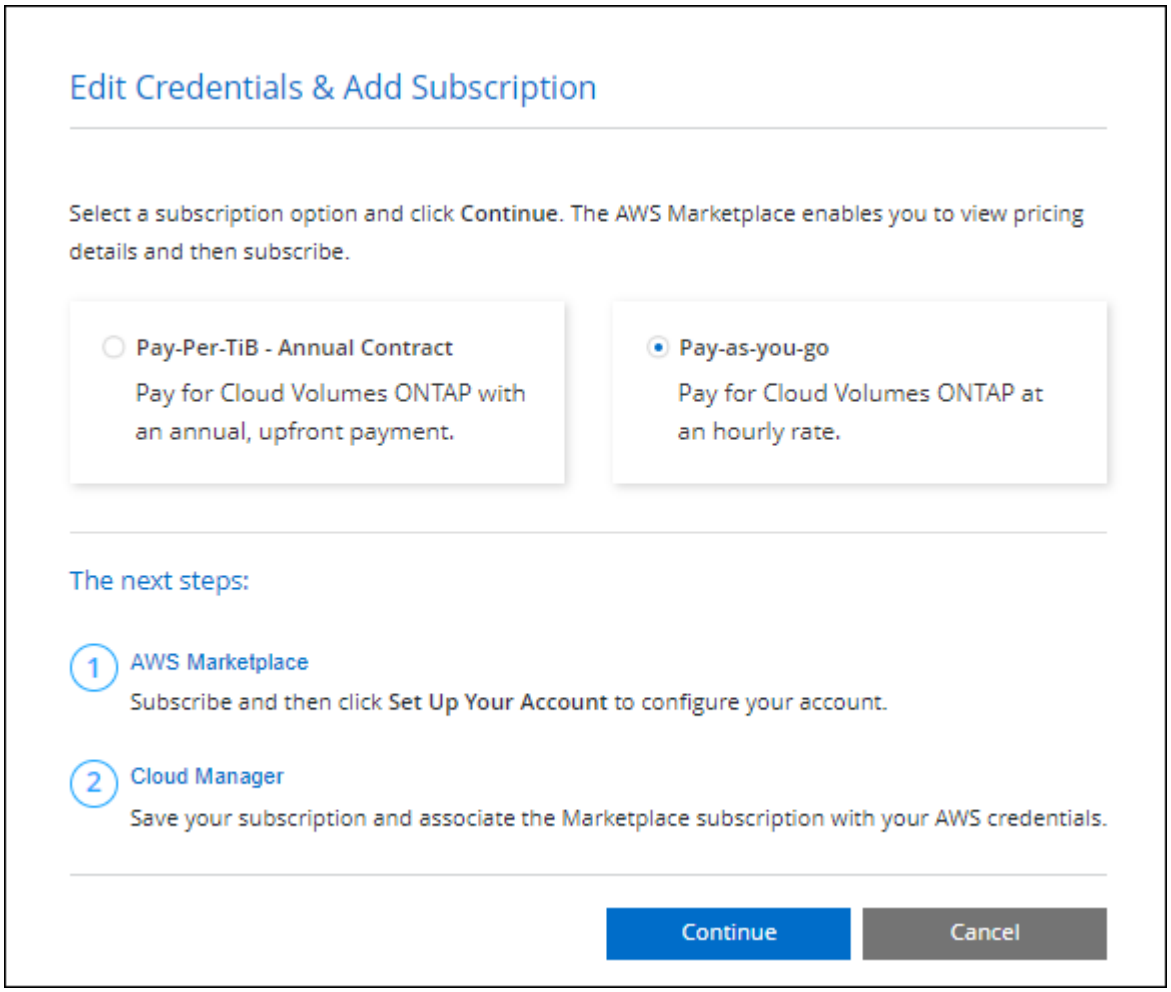
   Bevor Sie Ihre Lizenz mit Cloud Volumes ONTAP verwenden können, muss sie über das Digital Wallet von BlueXP erhältlich sein. Wenn nötig, können Sie "Fügen Sie die Lizenz manuell zum Digital Wallet von BlueXP hinzu".

3. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in

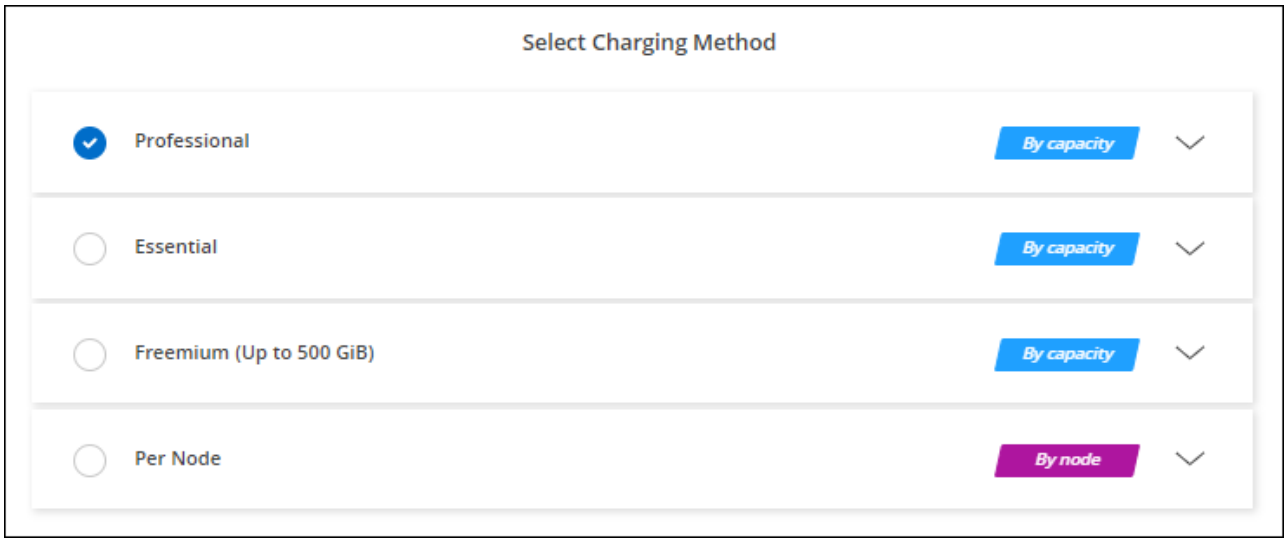
BlueXP.

a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um das Pay-as-you-go-Angebot im AWS Marketplace zu abonnieren.

   Die Lizenz, die Sie bei NetApp erworben haben, wird immer zuerst berechnet. Wenn Sie Ihre lizenzierte Kapazität überschreiten oder die Lizenzlaufzeit abgelaufen ist, werden Sie vom Stundensatz auf dem Markt in Rechnung gestellt.



a. Wenn Sie zu BlueXP zurückkehren, wählen Sie ein kapazitätsbasiertes Paket aus, wenn Sie die Seite mit den Lademethoden aufrufen.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen zum Starten von Cloud Volumes ONTAP in AWS an".

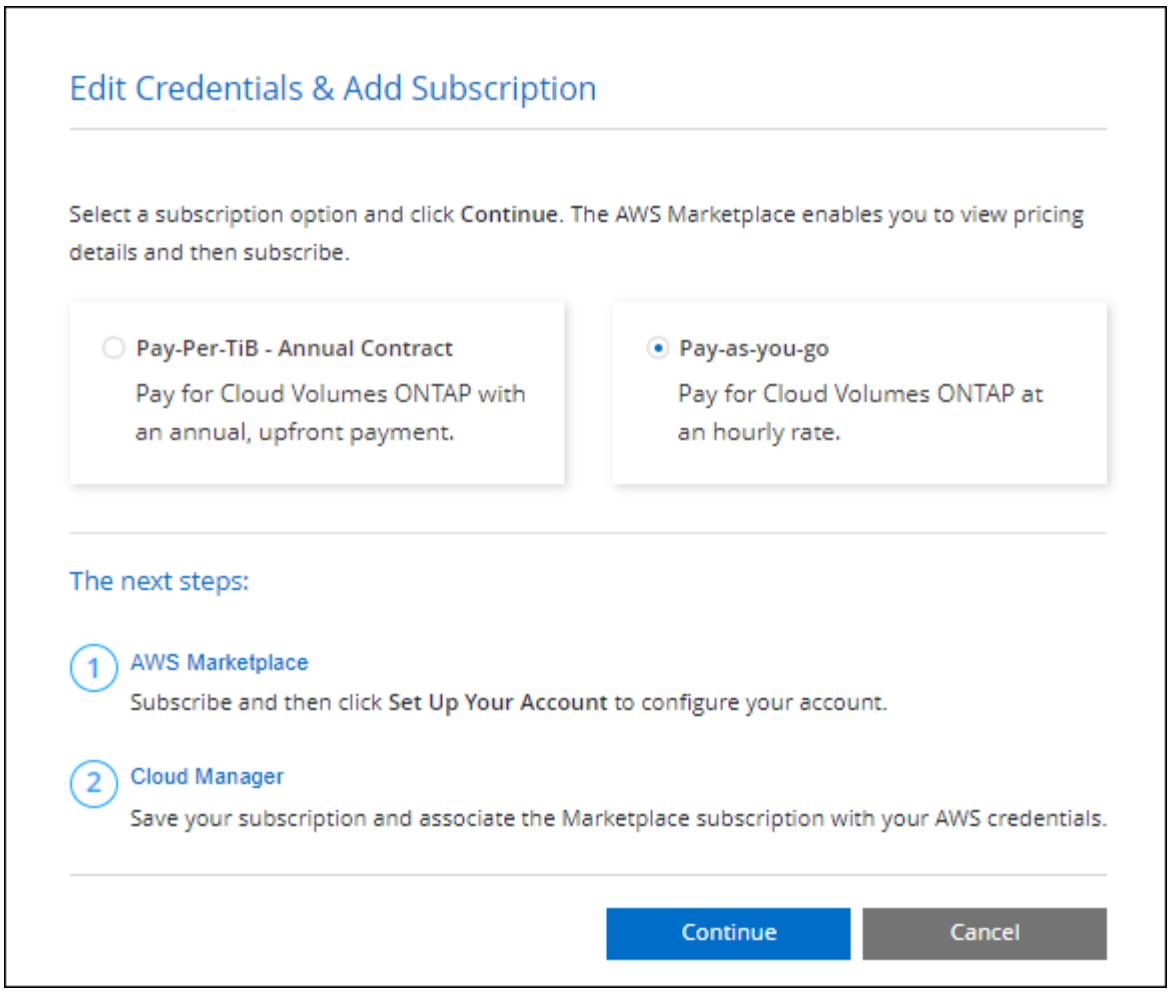
PAYGO-Abonnement

Sie bezahlen stündlich, indem Sie sich für das Angebot über den Marketplace Ihres Cloud-Providers anmelden.

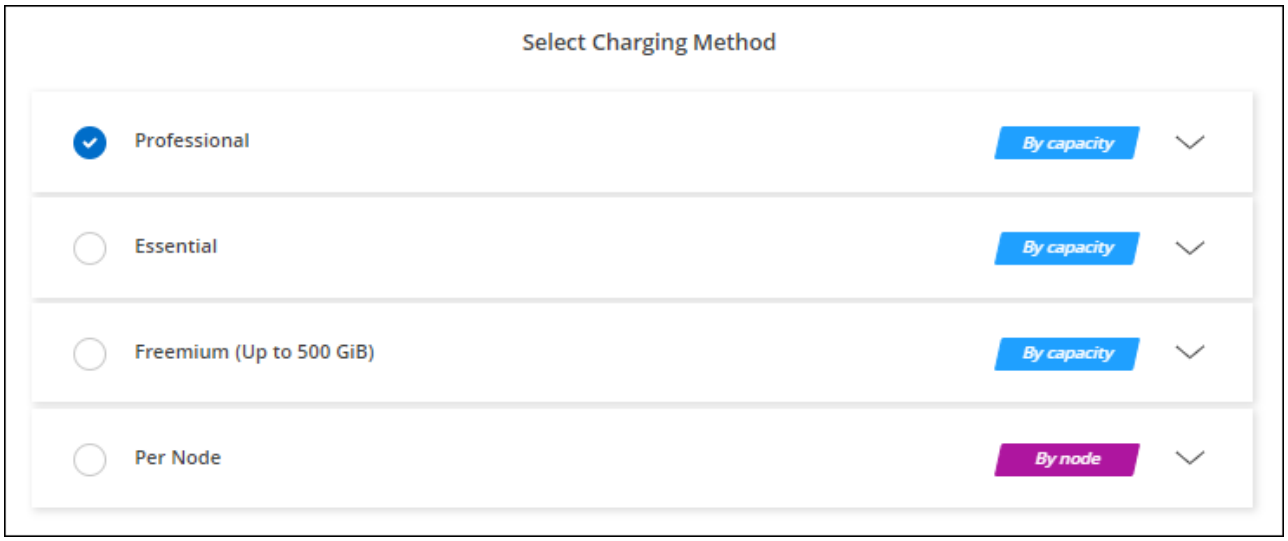
Wenn Sie eine Arbeitsumgebung für Cloud Volumes ONTAP erstellen, werden Sie von BlueXP aufgefordert, den Vertrag im AWS Marketplace zu abonnieren. Dieses Abonnement wird dann zur Verrechnung mit der Arbeitsumgebung verknüpft. Sie können das gleiche Abonnement auch für zusätzliche Arbeitsumgebungen nutzen.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um das Pay-as-you-go-Angebot im AWS Marketplace zu abonnieren.



b. Wenn Sie zu BlueXP zurückkehren, wählen Sie ein kapazitätsbasiertes Paket aus, wenn Sie die Seite mit den Lademethoden aufrufen.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen zum Starten von Cloud Volumes ONTAP in AWS an".

Sie können die mit Ihren AWS-Konten verbundenen AWS Marketplace-Abonnements über die Seite „Einstellungen“ > „Anmeldeinformationen“ managen. "Managen Sie Ihre AWS-Konten und -Abonnements"

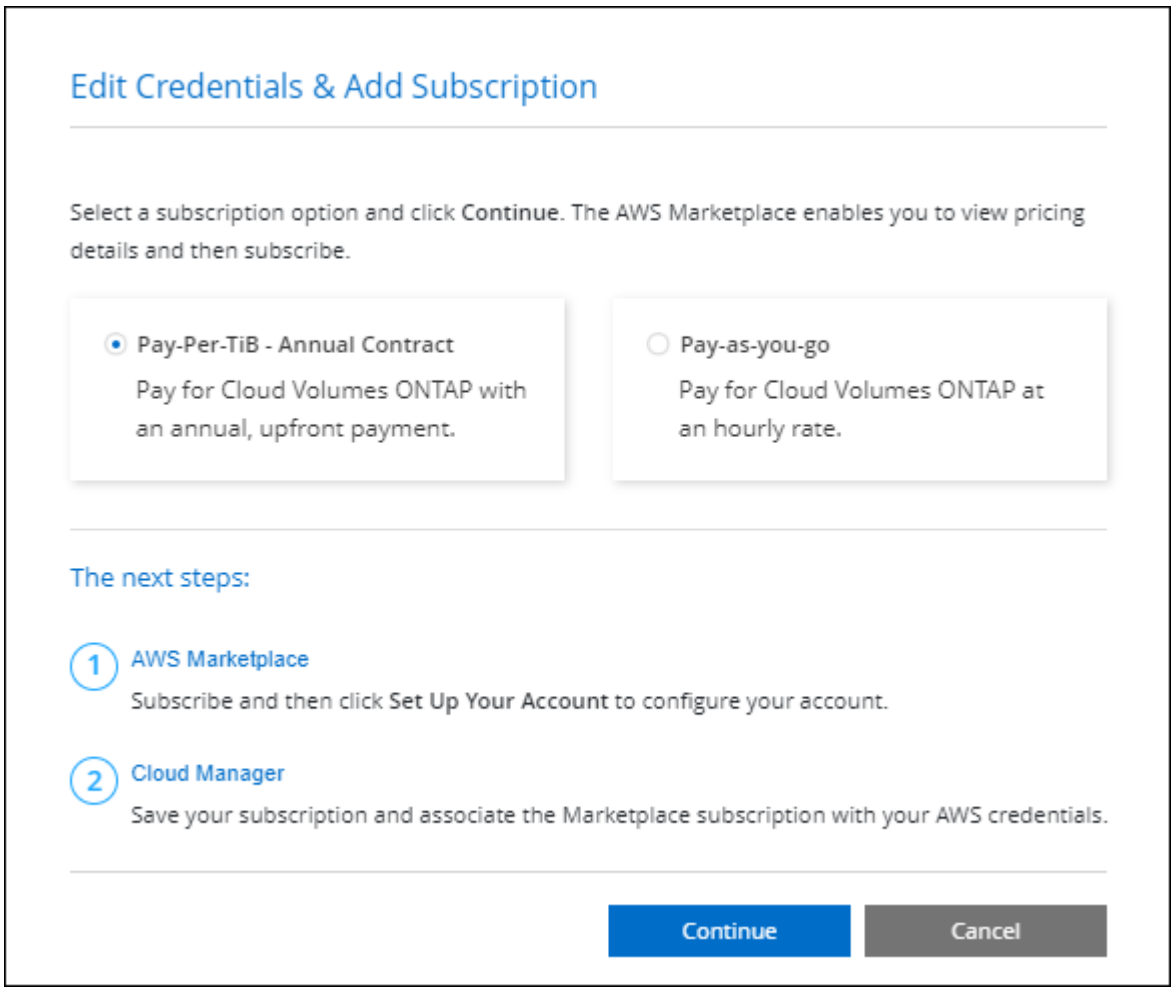
Jahresvertrag

Jährliche Zahlung durch Erwerb eines Jahresvertrags über den Markt Ihres Cloud-Providers.

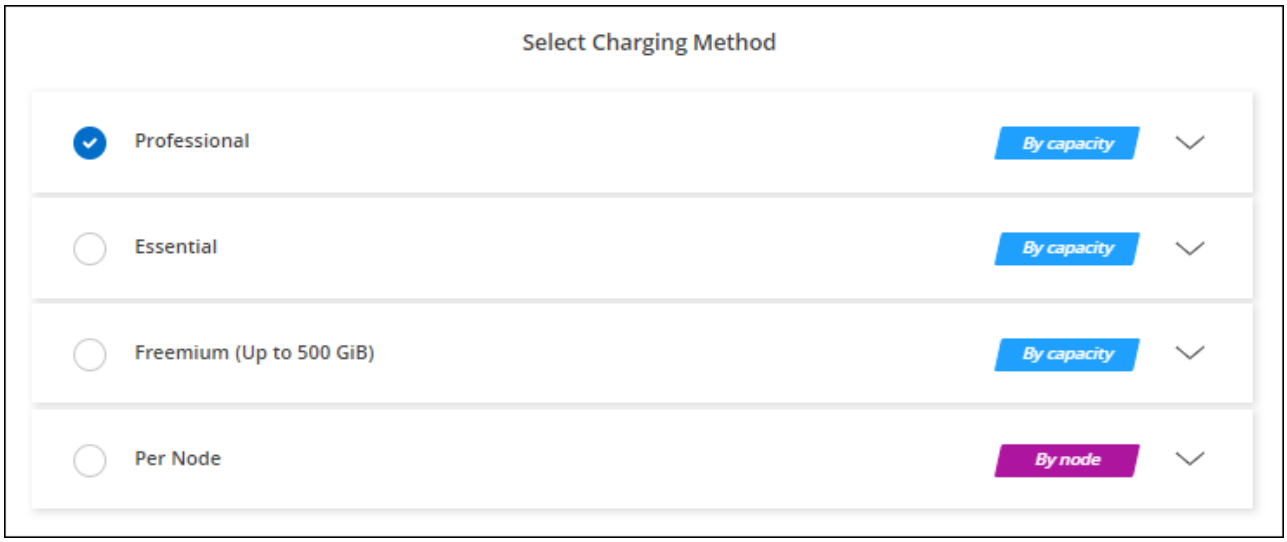
Ähnlich wie bei einem stündlichen Abonnement werden Sie von BlueXP aufgefordert, den Jahresvertrag zu abonnieren, der im AWS Marketplace verfügbar ist.

Schritte

1. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um den Jahresvertrag im AWS Marketplace zu abonnieren.



   b. Wenn Sie zu BlueXP zurückkehren, wählen Sie ein kapazitätsbasiertes Paket aus, wenn Sie die Seite mit den Lademethoden aufrufen.



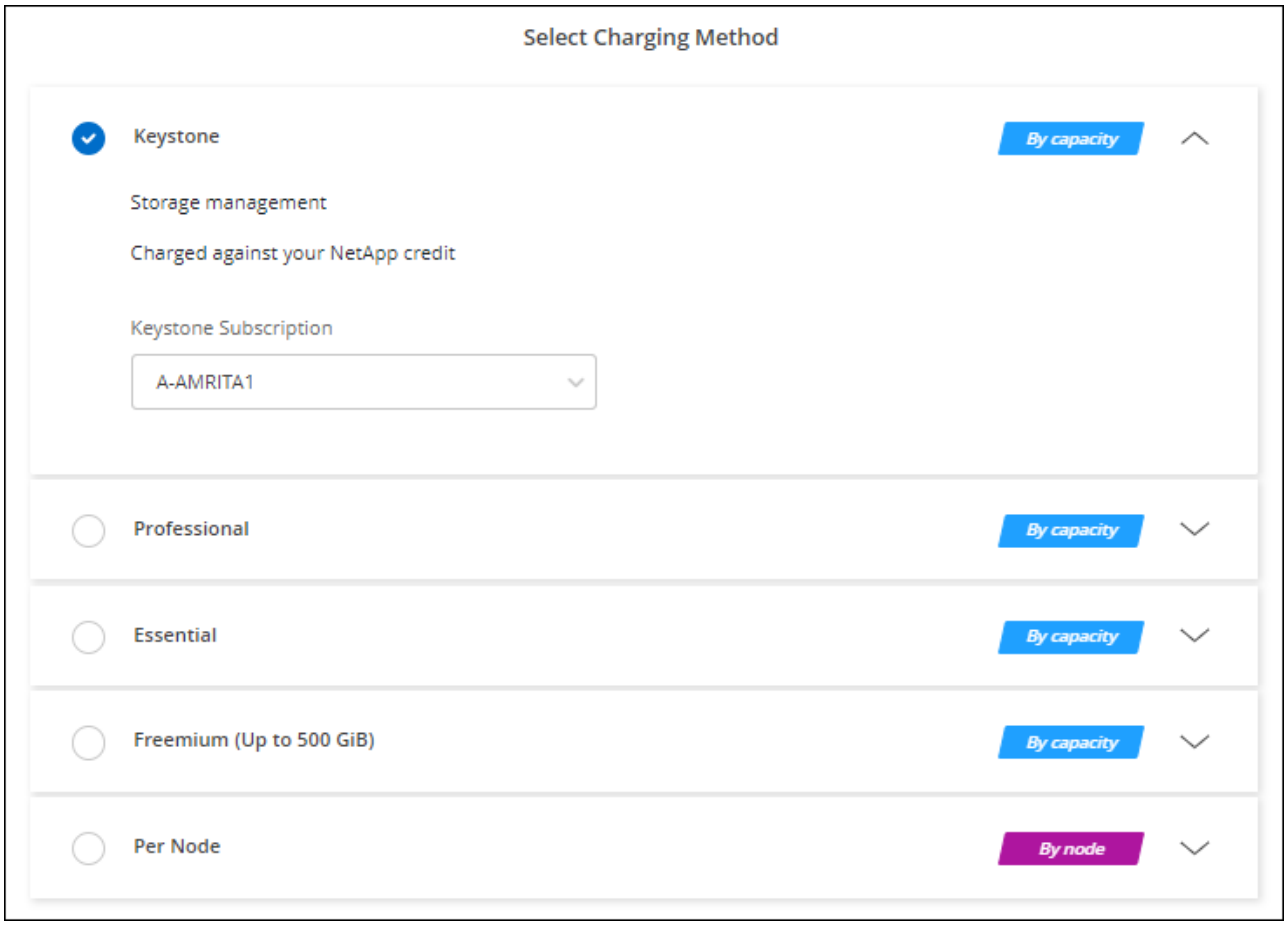
"Sehen Sie sich Schritt-für-Schritt-Anleitungen zum Starten von Cloud Volumes ONTAP in AWS an".

Keystone Abonnement

Ein Keystone Abonnement ist ein nutzungsbasierter Abonnementservice. "Weitere Informationen zu NetApp Keystone Abonnements".

Schritte

1. Wenn Sie noch kein Abonnement haben, "Kontakt zu NetApp"
2. Mailto:ng-keystone-success@netapp.com[NetApp kontaktieren]: Wir autorisieren Ihr BlueXP Benutzerkonto für eine oder mehrere Keystone Abonnements.
3. Nachdem NetApp den Account autorisiert hat, "Verknüpfen Sie Ihre Abonnements für die Verwendung mit Cloud Volumes ONTAP".
4. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
   a. Wählen Sie die Abrechnungsmethode für Keystone Abonnements aus, wenn Sie zur Auswahl einer Lademethode aufgefordert werden.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen zum Starten von Cloud Volumes ONTAP in AWS an".

Starten von Cloud Volumes ONTAP in AWS

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

Bevor Sie beginnen

Um eine Arbeitsumgebung zu schaffen, benötigen Sie Folgendes.

- Ein Anschluss, der betriebsbereit ist.
  - Sie sollten ein haben "Anschluss, der Ihrem Arbeitsbereich zugeordnet ist".
  - "Sie sollten darauf vorbereitet sein, den Konnektor jederzeit in Betrieb zu nehmen".
- Ein Verständnis der zu verwendenden Konfiguration.

  Sie sollten eine Konfiguration ausgewählt und AWS-Netzwerkinformationen von Ihrem Administrator erhalten haben. Weitere Informationen finden Sie unter "Planung Ihrer Cloud Volumes ONTAP Konfiguration".
- Kenntnisse über die erforderlichen Voraussetzungen zur Einrichtung der Lizenzierung für Cloud Volumes ONTAP.

  "Erfahren Sie, wie Sie eine Lizenzierung einrichten".

- DNS und Active Directory für CIFS-Konfigurationen.

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

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 BlueXP schaffen

Über diese Aufgabe

Unmittelbar nach der Erstellung der Arbeitsumgebung startet BlueXP eine Testinstanz in der angegebenen VPC, um die Konnektivität zu überprüfen. Wenn der Vorgang erfolgreich war, beendet BlueXP die Instanz sofort und beginnt dann mit der Bereitstellung des Cloud Volumes ONTAP-Systems. Wenn BlueXP die Verbindung 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. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Bildschirmseite auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.
3. **Wählen Sie einen Standort**: Wählen Sie **Amazon Web Services** und **Cloud Volumes ONTAP Single Node**.
4. Wenn Sie dazu aufgefordert werden, "Einen Konnektor erstellen".
5. **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:

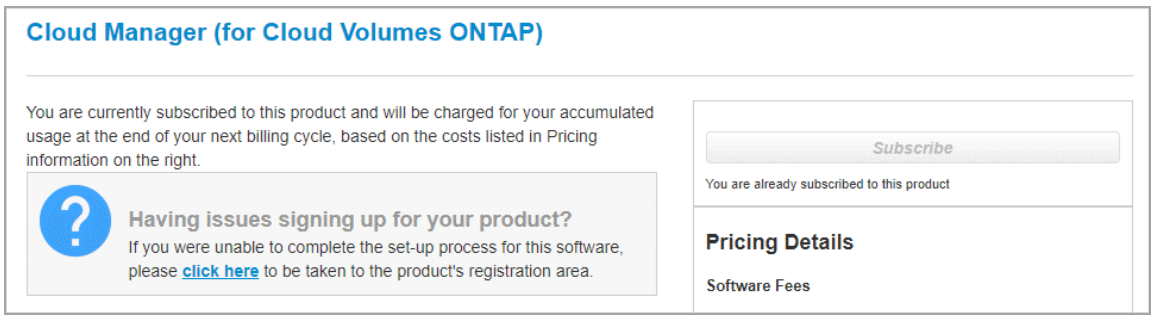
Feld	Beschreibung
Name der Arbeitsumgebung	BlueXP verwendet den Namen der Arbeitsumgebung, um sowohl das Cloud Volumes ONTAP System als auch die Amazon EC2 Instanz zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.
Tags hinzufügen	AWS-Tags sind Metadaten für Ihre AWS-Ressourcen. BlueXP fügt die Tags zur Cloud Volumes ONTAP-Instanz und jeder der Instanz zugeordneten 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 Anmeldeinformationen 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. Behalten Sie den Standardbenutzernamen „*admin*“ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.

Feld	Beschreibung
Anmeldedaten Bearbeiten	Wählen Sie die AWS Zugangsdaten für das Konto aus, in dem Sie dieses System bereitstellen möchten. Sie können das AWS Marketplace Abonnement auch für dieses Cloud Volumes ONTAP-System zuordnen. Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen mit einem neuen AWS Marketplace-Abonnement zu verknüpfen. Bei dem Abonnement kann es sich um einen Jahresvertrag oder um die Bezahlung von Cloud Volumes ONTAP auf Stundenbasis handelt. "Erfahren Sie, wie Sie BlueXP zusätzliche AWS Zugangsdaten hinzufügen".

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

Abonnieren Sie BlueXP über den AWS Marketplace

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 Sie die unten angezeigte Meldung sehen, klicken Sie auf den Link **click here**, um zur BlueXP-Website zu gelangen und den Vorgang
abzuschließen.



6. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie nicht mit Cloud Volumes ONTAP verwenden möchten.
   - "Weitere Informationen zur BlueXP Klassifizierung"
   - "Erfahren Sie mehr über Backup und Recovery von BlueXP"

   Wenn SIE WORM und Daten-Tiering nutzen möchten, müssen Sie BlueXP Backup und Recovery deaktivieren und eine Cloud Volumes ONTAP Arbeitsumgebung mit Version 9.8 oder höher implementieren.

7. **Standort & Konnektivität**: Geben Sie die Netzwerkinformationen ein, die Sie im aufgezeichnet haben "AWS Worksheet".

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

Feld	Beschreibung
VPC	Wenn Sie über einen AWS Outpost verfügen, können Sie ein Cloud Volumes ONTAP System mit einem einzelnen Node in diesem Outpost implementieren, indem Sie die Outpost VPC auswählen. Die Erfahrung ist mit jeder anderen VPC, die in AWS residiert.
Sicherheitsgruppe wurde generiert	Wenn Sie BlueXP die Sicherheitsgruppe für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Selected VPC Only** wählen, ist die Quelle für eingehenden Datenverkehr der Subnetz-Bereich des ausgewählten VPC und der Subnetz-Bereich des VPC, in dem sich der Connector befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VPCs** wählen, ist die Quelle für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene Sicherheitsgruppe verwenden	Wenn Sie eine vorhandene Firewallrichtlinie verwenden, stellen Sie sicher, dass diese die erforderlichen Regeln enthält. "Informieren Sie sich über die Firewall-Regeln für Cloud Volumes ONTAP".

8. **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".

9. **Charging Methods and NSS Account**: Geben Sie an, welche Ladungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site Konto an.
   - "Informieren Sie sich über Lizenzoptionen für Cloud Volumes ONTAP".
   - "Erfahren Sie, wie Sie eine Lizenzierung einrichten".
10. **Cloud Volumes ONTAP Konfiguration** (nur Jahresvertrag für AWS Marketplace): Überprüfen Sie die Standardkonfiguration und klicken Sie auf **Weiter** oder klicken Sie auf **Konfiguration ändern**, um Ihre eigene Konfiguration auszuwählen.

    Wenn die Standardkonfiguration beibehalten wird, müssen Sie nur ein Volume angeben und anschließend die Konfiguration prüfen und genehmigen.

11. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete aus, um schnell Cloud Volumes ONTAP zu starten, oder klicken Sie auf **Konfiguration ändern**, um Ihre eigene Konfiguration auszuwählen.

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

12. **IAM-Rolle**: Es ist am besten, die Standardoption zu behalten, mit der BlueXP die Rolle für Sie erstellen lässt.

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

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

> Wenn für die ausgewählte Version eine neuere Version von Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert BlueXP das System auf diese Version, wenn die Arbeitsumgebung erstellt wird. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.10.1 und 9.10.1 P4 auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.6 bis 9.7.

14. **Zugrunde liegende Speicherressourcen**: Wählen Sie einen Festplattentyp, konfigurieren Sie den zugrunde liegenden Speicher und wählen Sie, ob das Daten-Tiering aktiviert bleiben soll.

    Beachten Sie Folgendes:

    - Der Festplattentyp wird für das ursprüngliche Volume (und Aggregat) durchgeführt. Für nachfolgende Volumes (und Aggregate) kann ein anderer Festplattentyp ausgewählt werden.
    - Wenn Sie eine gp3- oder io1-Festplatte auswählen, verwendet BlueXP die Funktion Elastic Volumes in AWS, um bei Bedarf automatisch die zugrunde liegende Storage-Festplattenkapazität zu erhöhen. Sie können die ursprüngliche Kapazität auf Grundlage Ihrer Storage-Anforderungen auswählen und nach der Bereitstellung von Cloud Volumes ONTAP überarbeiten. "Erfahren Sie mehr über die Unterstützung von Elastic Volumes in AWS".
    - Wenn Sie eine gp2- oder st1-Festplatte auswählen, können Sie eine Festplattengröße für alle Festplatten im ursprünglichen Aggregat sowie für alle zusätzlichen Aggregate auswählen, die BlueXP erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuweisungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.
    - 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".

15. **Schreibgeschwindigkeit und WURM**:

    a. Wählen Sie bei Bedarf * Normal* oder **High** Schreibgeschwindigkeit.

       "Erfahren Sie mehr über Schreibgeschwindigkeit".

    b. Aktivieren Sie auf Wunsch den WORM-Storage (Write Once, Read Many).

       WORM kann nicht aktiviert werden, wenn Daten-Tiering für Cloud Volumes ONTAP-Versionen 9.7 und darunter aktiviert wurde. Ein Wechsel- oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach Aktivierung VON WORM und Tiering gesperrt.

    "Erfahren Sie mehr über WORM Storage".

    a. Wenn Sie DEN WORM-Speicher aktivieren, wählen Sie den Aufbewahrungszeitraum aus.

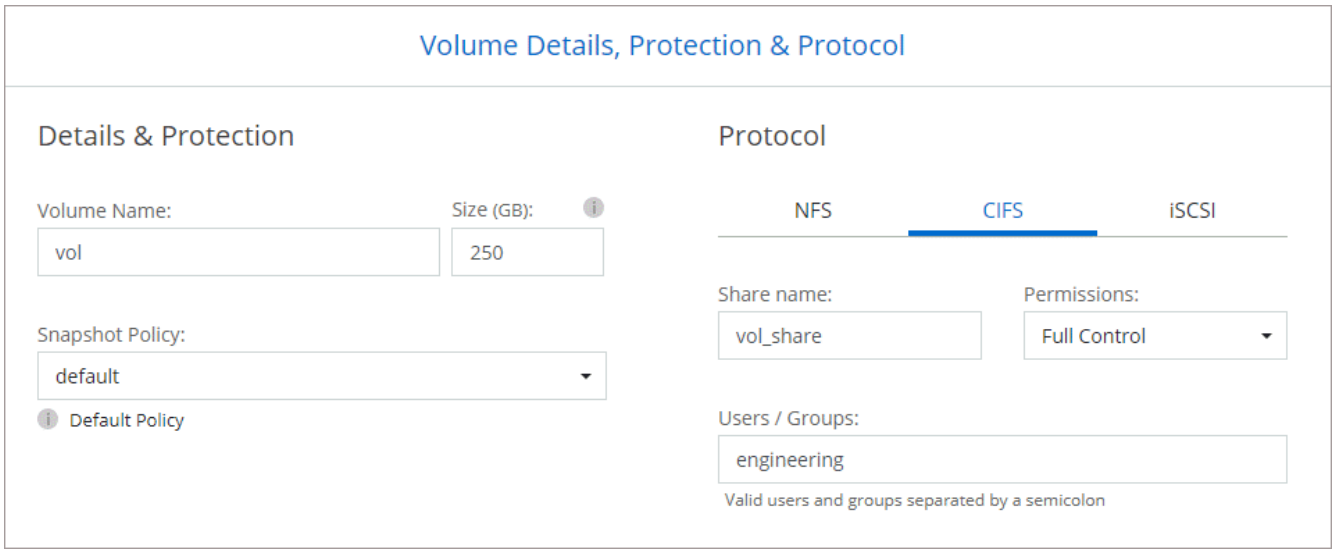
16. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

    "Hier erhalten Sie Informationen zu den unterstützten Client-Protokollen und -Versionen".

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 BlueXP einen Wert ein, der Zugriff auf alle Instanzen im Subnetz bietet.
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 BlueXP 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:



17. **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 "BlueXP Automation Dokumentation" Entsprechende Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Er ist nicht konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

18. **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".

19. **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 AWS Ressourcen zu erhalten, die BlueXP kaufen wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie Auf **Go**.

Ergebnis

BlueXP 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 BlueXP erstellen.

Einschränkung

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

Über diese Aufgabe

Unmittelbar nach der Erstellung der Arbeitsumgebung startet BlueXP eine Testinstanz in der angegebenen VPC, um die Konnektivität zu überprüfen. Wenn der Vorgang erfolgreich war, beendet BlueXP die Instanz sofort und beginnt dann mit der Bereitstellung des Cloud Volumes ONTAP-Systems. Wenn BlueXP die Verbindung 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. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.
3. **Wählen Sie einen Standort**: Wählen Sie **Amazon Web Services** und **Cloud Volumes ONTAP HA**.

   Einige AWS lokale Zonen sind verfügbar.

Bevor Sie AWS Local Zones verwenden können, müssen Sie lokale Zonen aktivieren und in Ihrem AWS-Konto ein Subnetz in der lokalen Zone erstellen. Folgen Sie den Schritten **in einer AWS Local Zone** und **Extend Your Amazon VPC to the Local Zone** im "AWS Tutorial „erste Schritte mit der Bereitstellung von Anwendungen mit niedriger Latenz mit AWS Local Zones".

Wenn Sie eine Connector-Version 3.9.36 oder niedriger ausführen, müssen Sie die folgende Berechtigung zur AWS Connector-Rolle in der AWS EC2-Konsole hinzufügen: DescribeAvailability Zones.

4. **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.

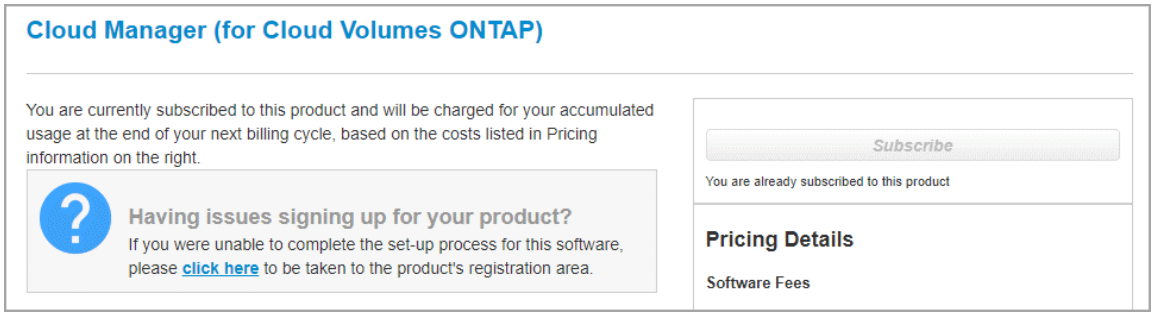
   Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Name der Arbeitsumgebung	BlueXP 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. BlueXP fügt die Tags zur Cloud Volumes ONTAP-Instanz und jeder der Instanz zugeordneten 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 Anmeldeinformationen 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. Behalten Sie den Standardbenutzernamen „*admin*“ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Anmeldedaten Bearbeiten	AWS Zugangsdaten und das Marketplace-Abonnement für dieses Cloud Volumes ONTAP System auswählen Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen mit einem neuen AWS Marketplace-Abonnement zu verknüpfen. Bei dem Abonnement kann es sich um einen Jahresvertrag oder um die Bezahlung von Cloud Volumes ONTAP auf Stundenbasis handelt. Wenn eine Lizenz direkt über NetApp (BYOL) erworben wird, ist kein AWS Abonnement erforderlich. "Erfahren Sie, wie Sie BlueXP zusätzliche AWS Zugangsdaten hinzufügen".

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

Abonnieren Sie BlueXP über den AWS Marketplace

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 Sie die unten angezeigte Meldung sehen, klicken Sie auf den Link **click here**, um zur BlueXP-Website zu gelangen und den Vorgang
abzuschließen.



5. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie mit diesem Cloud Volumes ONTAP-System nicht verwenden möchten.
   - "Weitere Informationen zur BlueXP Klassifizierung"
   - "Erfahren Sie mehr über Backup und Recovery von BlueXP"

   Wenn SIE WORM und Daten-Tiering nutzen möchten, müssen Sie BlueXP Backup und Recovery deaktivieren und eine Cloud Volumes ONTAP Arbeitsumgebung mit Version 9.8 oder höher implementieren.

6. **HA-Bereitstellungsmodelle**: Wählen Sie eine HA-Konfiguration.

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

7. **Standort und Konnektivität** (Single AZ) oder **Region & VPC** (Multiple AZS): Geben Sie die Netzwerkinformationen ein, die Sie im AWS-Arbeitsblatt aufgezeichnet haben.

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

Feld	Beschreibung
Sicherheitsgruppe wurde generiert	Wenn Sie BlueXP die Sicherheitsgruppe für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Selected VPC Only** wählen, ist die Quelle für eingehenden Datenverkehr der Subnetz-Bereich des ausgewählten VPC und der Subnetz-Bereich des VPC, in dem sich der Connector befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VPCs** wählen, ist die Quelle für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene Sicherheitsgruppe verwenden	Wenn Sie eine vorhandene Firewallrichtlinie verwenden, stellen Sie sicher, dass diese die erforderlichen Regeln enthält. "Informieren Sie sich über die Firewall-Regeln für Cloud Volumes ONTAP".

8. **Konnektivität und SSH Authentifizierung**: Wählen Sie Verbindungsmethoden für das HA-Paar und den Mediator.
9. **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".

10. **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".

11. **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".

12. **Charging Methods and NSS Account**: Geben Sie an, welche Ladungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site Konto an.
    - "Informieren Sie sich über Lizenzoptionen für Cloud Volumes ONTAP".
    - "Erfahren Sie, wie Sie eine Lizenzierung einrichten".
13. **Cloud Volumes ONTAP Konfiguration** (nur Jahresvertrag für AWS Marketplace): Überprüfen Sie die Standardkonfiguration und klicken Sie auf **Weiter** oder klicken Sie auf **Konfiguration ändern**, um Ihre eigene Konfiguration auszuwählen.

    Wenn die Standardkonfiguration beibehalten wird, müssen Sie nur ein Volume angeben und anschließend die Konfiguration prüfen und genehmigen.

14. **Vorkonfigurierte Pakete** (nur stündlich oder BYOL): Wählen Sie eines der Pakete aus, um schnell Cloud Volumes ONTAP zu starten, oder klicken Sie auf **Konfiguration ändern**, um Ihre eigene Konfiguration auszuwählen.

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

15. **IAM-Rolle**: Es ist am besten, die Standardoption zu behalten, mit der BlueXP die Rolle für Sie erstellen lässt.

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

16. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP-Version nach Bedarf und wählen Sie einen

Instanztyp und die Instanzenfähigkeit aus.

> Wenn für die ausgewählte Version eine neuere Version von Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert BlueXP das System auf diese Version, wenn die Arbeitsumgebung erstellt wird. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.10.1 und 9.10.1 P4 auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.6 bis 9.7.

17. **Zugrunde liegende Speicherressourcen**: Wählen Sie einen Festplattentyp, konfigurieren Sie den zugrunde liegenden Speicher und wählen Sie, ob das Daten-Tiering aktiviert bleiben soll.

    Beachten Sie Folgendes:

    - Der Festplattentyp wird für das ursprüngliche Volume (und Aggregat) durchgeführt. Für nachfolgende Volumes (und Aggregate) kann ein anderer Festplattentyp ausgewählt werden.
    - Wenn Sie eine gp3- oder io1-Festplatte auswählen, verwendet BlueXP die Funktion Elastic Volumes in AWS, um bei Bedarf automatisch die zugrunde liegende Storage-Festplattenkapazität zu erhöhen. Sie können die ursprüngliche Kapazität auf Grundlage Ihrer Storage-Anforderungen auswählen und nach der Bereitstellung von Cloud Volumes ONTAP überarbeiten. "Erfahren Sie mehr über die Unterstützung von Elastic Volumes in AWS".
    - Wenn Sie eine gp2- oder st1-Festplatte auswählen, können Sie eine Festplattengröße für alle Festplatten im ursprünglichen Aggregat sowie für alle zusätzlichen Aggregate auswählen, die BlueXP erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuweisungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.
    - 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".

18. **Schreibgeschwindigkeit und WURM**:

    a. Wählen Sie bei Bedarf * Normal* oder **High** Schreibgeschwindigkeit.

       "Erfahren Sie mehr über Schreibgeschwindigkeit".

    b. Aktivieren Sie auf Wunsch den WORM-Storage (Write Once, Read Many).

       WORM kann nicht aktiviert werden, wenn Daten-Tiering für Cloud Volumes ONTAP-Versionen 9.7 und darunter aktiviert wurde. Ein Wechsel- oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach Aktivierung VON WORM und Tiering gesperrt.

    "Erfahren Sie mehr über WORM Storage".

    a. Wenn Sie DEN WORM-Speicher aktivieren, wählen Sie den Aufbewahrungszeitraum aus.

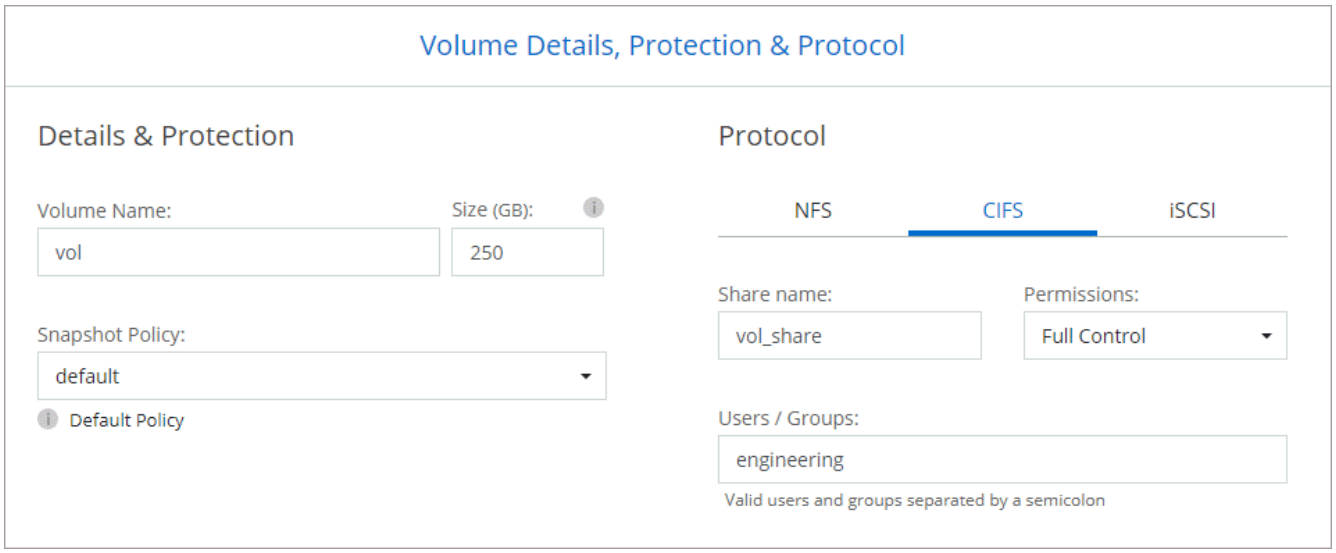
19. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

    "Hier erhalten Sie Informationen zu den unterstützten Client-Protokollen und -Versionen".

    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 BlueXP einen Wert ein, der Zugriff auf alle Instanzen im Subnetz bietet.
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 BlueXP 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:



20. **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.
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 "BlueXP Automation Dokumentation" Entsprechende Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Er ist nicht konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

21. **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 "Wählen Sie ein Volume-Auslastungsprofil aus" Und "Data Tiering - Übersicht".

22. **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 AWS Ressourcen zu erhalten, die BlueXP kaufen wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie Auf **Go**.

Ergebnis

BlueXP startet das Cloud Volumes ONTAP HA-Paar. 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.

Implementieren Sie Cloud Volumes ONTAP in AWS Secret Cloud und Top Secret Cloud-Regionen

Wie in einer Standardregion von AWS können Sie BlueXP auch einsetzen "AWS Secret Cloud" Und ein "Top Secret Cloud von AWS" Zur Implementierung von Cloud Volumes ONTAP mit Funktionen der Enterprise-Klasse für Ihren Cloud-Storage. AWS Secret Cloud und Top Secret Cloud sind geschlossene Regionen speziell für die USA Intelligence Community: Die Anweisungen auf dieser Seite gelten nur für Benutzer der AWS Secret Cloud und der Region Top Secret Cloud.

Bevor Sie beginnen

Bevor Sie beginnen, sehen Sie sich die unterstützten Versionen in AWS Secret Cloud und Top Secret Cloud an, und informieren Sie sich über den Private-Modus in BlueXP.

- Prüfen Sie die folgenden unterstützten Versionen in AWS Secret Cloud und Top Secret Cloud:
  - Cloud Volumes ONTAP 9.12.1 P2
  - Version 3.9.32 des Connectors

    Der Connector ist eine Software, die für die Implementierung und das Management von Cloud Volumes ONTAP in AWS benötigt wird. Sie melden sich bei BlueXP über die Software an, die auf der Connector-Instanz installiert wird. Die SaaS-Website für BlueXP wird in AWS Secret Cloud und Top Secret Cloud nicht unterstützt.

- Weitere Informationen zum privaten Modus

  In AWS Secret Cloud und Top Secret Cloud arbeitet BlueXP im *Private Mode*. Im privaten Modus ist keine Konnektivität zur BlueXP SaaS-Ebene vorhanden. Benutzer greifen lokal über die webbasierte Konsole auf BlueXP zu, die über den Connector verfügbar ist und nicht über die SaaS-Schicht.

  Weitere Informationen zur Funktionsweise des privaten Modus finden Sie unter "Privater Implementierungsmodus von BlueXP".

Schritt 1: Richten Sie Ihr Netzwerk ein

Richten Sie Ihr AWS Netzwerk ein, um Cloud Volumes ONTAP ordnungsgemäß zu betreiben.

Schritte

1. Wählen Sie die VPC und Subnetze aus, in denen die Connector-Instanz und die Cloud Volumes ONTAP-Instanzen gestartet werden sollen.
2. Stellen Sie sicher, dass Ihre VPC und Subnetze die Konnektivität zwischen dem Connector und Cloud Volumes ONTAP unterstützen.
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.

Schritt 2: Berechtigungen einrichten

Richten Sie IAM-Richtlinien und -Rollen ein, die dem Connector und Cloud Volumes ONTAP die erforderlichen Berechtigungen für Aktionen in der AWS Secret Cloud oder Top Secret Cloud bieten.

Für die folgenden Bereiche benötigen Sie eine IAM-Richtlinie und eine IAM-Rolle:

- Die Instanz des Connectors
- Cloud Volumes ONTAP Instanzen
- Bei HA-Paaren ist die Cloud Volumes ONTAP HA-Mediatorinstanz (wenn HA-Paare implementiert werden sollen)

Schritte

1. Gehen Sie zur AWS IAM-Konsole und klicken Sie auf **Policies**.
2. Erstellen Sie eine Richtlinie für die Connector-Instanz.

> Sie erstellen diese Richtlinien, um die S3-Buckets in Ihrer AWS-Umgebung zu unterstützen. Stellen Sie beim Erstellen der Buckets zu einem späteren Zeitpunkt sicher, dass den Bucket-Namen vorangestellt werden `fabric-pool-`. Diese Anforderung gilt sowohl für die Regionen AWS Secret Cloud als auch Top Secret Cloud.

Geheime Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Top Secret Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
```

```
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
```

```
}
```

3. Erstellen einer Richtlinie für Cloud Volumes ONTAP

Geheime Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Top Secret Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Wenn Sie bei HA-Paaren ein Cloud Volumes ONTAP HA-Paar implementieren möchten, erstellen Sie eine Richtlinie für den HA-Mediator.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

4. Erstellen Sie IAM-Rollen mit dem Rollentyp Amazon EC2 und hängen Sie die Richtlinien an, die Sie in den vorherigen Schritten erstellt haben.

   Erstellen Sie die Rolle:

   Ähnlich wie bei den Richtlinien sollten Sie eine IAM-Rolle für den Konnektor und eine für die Cloud Volumes ONTAP-Knoten haben.
   Für HA-Paare: Ähnlich wie bei den Richtlinien sollten Sie über eine IAM-Rolle für den Connector, eine für die Cloud Volumes ONTAP-Nodes und eine für den HA-Mediator verfügen (wenn Sie HA-Paare implementieren möchten).

   Wählen Sie die Rolle aus:

   Sie müssen die Connector IAM-Rolle auswählen, wenn Sie die Connector-Instanz starten. Sie können die IAM-Rollen für Cloud Volumes ONTAP auswählen, wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung aus BlueXP erstellen.
   Bei HA-Paaren können Sie beim Erstellen einer Cloud Volumes ONTAP Arbeitsumgebung aus BlueXP die IAM-Rollen für Cloud Volumes ONTAP und den HA-Mediator auswählen.

Schritt 3: Einrichtung des AWS-KMS

Wenn Sie Amazon Verschlüsselung mit Cloud Volumes ONTAP nutzen möchten, stellen Sie sicher, dass die Anforderungen für den AWS Key Management Service (KMS) erfüllt sind.

Schritte

1. Stellen Sie sicher, dass ein aktiver Kunden-Master-Schlüssel (CMK) in Ihrem Konto oder in einem anderen AWS-Konto vorhanden ist.

   Bei CMK kann es sich um ein von AWS gemanagtes CMK oder um ein vom Kunden gemanagtes CMK handeln.

2. Wenn sich das CMK in einem AWS Konto befindet und nicht über das Konto, in dem Sie Cloud Volumes ONTAP implementieren möchten, müssen Sie die ARN dieses Schlüssels erhalten.

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

3. Fügen Sie die IAM-Rolle für die Connector-Instanz der Liste der wichtigsten Benutzer für ein CMK hinzu.

   Dadurch erhalten BlueXP die Berechtigung zur Verwendung des CMK mit Cloud Volumes ONTAP.

Schritt 4: Installieren Sie den Connector und richten Sie BlueXP ein

Bevor Sie BlueXP zur Implementierung von Cloud Volumes ONTAP in AWS nutzen können, müssen Sie den BlueXP Connector installieren und einrichten. Mit dem Connector kann BlueXP Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen (einschließlich Cloud Volumes ONTAP).

Schritte

1. Sie erhalten ein Root-Zertifikat, das von einer Zertifizierungsstelle (CA) im Format Privacy Enhanced Mail (PEM) Base-64-codiert X.509 signiert ist. Wenden Sie sich an die Richtlinien und Verfahren Ihres Unternehmens, um das Zertifikat zu erhalten.

   > Laden Sie für AWS Secret Cloud-Regionen die hoch `NSS Root CA 2` Zertifikat, und für Top Secret Cloud, die `Amazon Root CA 4` Zertifikat: Stellen Sie sicher, dass Sie nur diese Zertifikate und nicht die gesamte Kette hochladen. Die Datei für die Zertifikatskette ist groß, und der Upload kann fehlschlagen. Wenn Sie weitere Zertifikate haben, können Sie diese später hochladen, wie im nächsten Schritt beschrieben.

   Sie müssen das Zertifikat während des Setup-Vorgangs hochladen. BlueXP verwendet das vertrauenswürdige Zertifikat, wenn Anfragen über HTTPS an AWS gesendet werden.

2. Starten Sie die Connector-Instanz:
   a. Besuchen Sie die AWS Intelligence Community Marketplace Seite für BlueXP.
   b. Wählen Sie auf der Registerkarte Benutzerdefinierter Start die Option, um die Instanz von der EC2-Konsole aus zu starten.
   c. Befolgen Sie die Anweisungen, um die Instanz zu konfigurieren.

      Beachten Sie beim Konfigurieren der Instanz Folgendes:

      - Wir empfehlen t3.xlarge.
      - Sie müssen die IAM-Rolle auswählen, die Sie beim Einrichten von Berechtigungen erstellt haben.
      - Sie sollten die standardmäßigen Speicheroptionen beibehalten.
      - Für den Connector sind folgende Verbindungsmethoden erforderlich: SSH, HTTP und HTTPS.
3. Richten Sie BlueXP von einem Host aus, der eine Verbindung zur Connector-Instanz hat:
   a. Öffnen Sie einen Webbrowser, und geben Sie ein https://ipaddress Wobei ipaddress die IP-Adresse des Linux-Hosts ist, auf dem Sie den Connector installiert haben.
   b. Geben Sie einen Proxy-Server für die Verbindung zu AWS-Services an.
   c. Laden Sie das Zertifikat, das Sie in Schritt 1 erhalten haben, hoch.

d. Wählen Sie **Set up New BlueXP** und folgen Sie den Anweisungen, um das System einzurichten.

- **Systemdetails**: Geben Sie einen Namen für den Connector und Ihren Firmennamen ein.
- **Admin-Benutzer erstellen**: Erstellen Sie den Admin-Benutzer für das System.

  Dieses Benutzerkonto wird lokal auf dem System ausgeführt. Über BlueXP ist keine Verbindung zum aut0-Service verfügbar.

- **Review**: Überprüfen Sie die Details, akzeptieren Sie die Lizenzvereinbarung und wählen Sie dann **Setup**.

e. Um die Installation des CA-signierten Zertifikats abzuschließen, starten Sie die Connector-Instanz von der EC2-Konsole aus neu.

4. Melden Sie sich nach dem Neustart des Connectors mit dem Administratorkonto an, das Sie im Setup-Assistenten erstellt haben.

Schritt 5: (Optional) Installieren Sie ein Zertifikat für den privaten Modus

Dieser Schritt ist optional für die Regionen AWS Secret Cloud und Top Secret Cloud und nur erforderlich, wenn Sie neben den im vorherigen Schritt installierten Stammzertifikaten über zusätzliche Zertifikate verfügen.

Schritte

1. Vorhandene installierte Zertifikate auflisten.

   a. Führen Sie den folgenden Befehl aus, um die occm Container Docker id (identifizierter Name „ds-occm-1“) zu erfassen:

   ```
   docker ps
   ```

   b. Um in den occm-Container zu gelangen, führen Sie den folgenden Befehl aus:

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   c. Um das Passwort aus der Umgebungsvariable „TRUST_STORE_PASSWORD“ zu erfassen, führen Sie den folgenden Befehl aus:

   ```
   env
   ```

   d. Um alle installierten Zertifikate im Truststore aufzulisten, führen Sie den folgenden Befehl aus und verwenden Sie das im vorherigen Schritt gesammelte Passwort:

   ```
   keytool -list -v -keystore occm.truststore
   ```

2. Fügen Sie ein Zertifikat hinzu.

   a. Führen Sie den folgenden Befehl aus, um die occm Container Docker id (identifizierter Name „ds-occm-1“) zu erfassen:

```
docker ps
```

b. Um in den occm-Container zu gelangen, führen Sie den folgenden Befehl aus:

```
docker exec -it <docker-id> /bin/sh
```

Speichern Sie die neue Zertifikatdatei in.

c. Um das Passwort aus der Umgebungsvariable „TRUST_STORE_PASSWORD“ zu erfassen, führen Sie den folgenden Befehl aus:

```
env
```

d. Um das Zertifikat zum Truststore hinzuzufügen, führen Sie den folgenden Befehl aus und verwenden Sie das Kennwort aus dem vorherigen Schritt:

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob das Zertifikat installiert ist:

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. Führen Sie den folgenden Befehl aus, um den occm-Container zu beenden:

```
exit
```

g. Führen Sie den folgenden Befehl aus, um den occm-Container zurückzusetzen:

```
docker restart <docker-id>
```

Schritt 6: Erweitern Sie das Digital Wallet von BlueXP um eine Lizenz

Wenn Sie eine Lizenz von NetApp erworben haben, müssen Sie sie zur Digital Wallet von BlueXP hinzufügen, damit Sie bei der Erstellung eines neuen Cloud Volumes ONTAP Systems die Lizenz auswählen können. Die Digital Wallet identifiziert diese Lizenzen als nicht zugewiesen.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie im Dropdown-Menü auf der Registerkarte **Cloud Volumes ONTAP** die Option **Node-basierte Lizenzen** aus.

3. Klicken Sie Auf **Nicht Zugewiesen**.
4. Klicken Sie Auf **Nicht Zugewiesene Lizenzen Hinzufügen**.
5. Geben Sie die Seriennummer der Lizenz ein oder laden Sie die Lizenzdatei hoch.
6. Wenn Sie die Lizenzdatei noch nicht besitzen, müssen Sie die Lizenzdatei manuell von netapp.com hochladen.
   a. Wechseln Sie zum "NetApp Lizenzdatei-Generator" Und loggen Sie sich mit Ihren Anmeldedaten für die NetApp Support Site ein.
   b. 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**.
   c. Wählen Sie aus, ob Sie die Datei serialnumber.NLF JSON per E-Mail oder direkt herunterladen möchten.
7. Klicken Sie Auf **Lizenz Hinzufügen**.

Ergebnis

BlueXP erweitert das Digital Wallet um die Lizenz. Die Lizenz wird erst dann als nicht zugewiesen identifiziert, wenn Sie sie einem neuen Cloud Volumes ONTAP-System zuordnen. Anschließend wird die Lizenz auf die Registerkarte BYOL im Digital Wallet verschoben.

Schritt 7: Starten Sie Cloud Volumes ONTAP von BlueXP

Sie können Cloud Volumes ONTAP-Instanzen in der AWS Secret Cloud und Top Secret Cloud starten, indem Sie neue Arbeitsumgebungen in BlueXP erstellen.

Bevor Sie beginnen

Bei HA-Paaren ist ein Schlüsselpaar erforderlich, um eine schlüssbasierte SSH-Authentifizierung beim HA-Mediator zu aktivieren.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen**.
2. Wählen Sie unter **Erstellen** die Option Cloud Volumes ONTAP.

   Für HA: Wählen Sie unter **Erstellen** Cloud Volumes ONTAP oder Cloud Volumes ONTAP HA aus.

3. Führen Sie die Schritte im Assistenten aus, um das Cloud Volumes ONTAP-System zu starten.

> Wählen Sie während der Auswahl über den Assistenten nicht **Data Sense & Compliance** und **Backup in der Cloud** unter **Services** aus. Wählen Sie unter **vorkonfigurierte Pakete nur Konfiguration ändern** aus, und stellen Sie sicher, dass Sie keine andere Option ausgewählt haben. Vorkonfigurierte Pakete werden in den Regionen AWS Secret Cloud und Top Secret Cloud nicht unterstützt. Wenn Sie diese Option auswählen, schlägt die Bereitstellung fehl.

Hinweise zur Bereitstellung von Cloud Volumes ONTAP HA in mehreren Verfügbarkeitszonen

Beachten Sie Folgendes, wenn Sie den Assistenten für HA-Paare abschließen.

- Wenn Sie Cloud Volumes ONTAP HA in Multiple Availability Zones (AZS) implementieren, sollten Sie ein Transit-Gateway konfigurieren. Siehe "AWS Transit Gateway einrichten".

- Implementieren Sie die Konfiguration wie folgt, da zum Zeitpunkt der Veröffentlichung nur zwei AZS in der AWS Top Secret Cloud verfügbar waren:
  - Node 1: Verfügbarkeitszone A
  - Node 2: Verfügbarkeitszone B
  - Mediator: Verfügbarkeit Zone A oder B

Hinweise zur Implementierung von Cloud Volumes ONTAP in Einzel- und HA-Nodes

Beachten Sie beim Abschließen des Assistenten Folgendes:

- Sie sollten die Standardoption verlassen, um eine generierte Sicherheitsgruppe zu verwenden.

  Die vordefinierte Sicherheitsgruppe enthält die Regeln, die Cloud Volumes ONTAP für den erfolgreichen Betrieb benötigen. Wenn Sie eine Anforderung haben, Ihre eigene zu verwenden, können Sie den folgenden Abschnitt der Sicherheitsgruppe lesen.

- Sie müssen die IAM-Rolle auswählen, die Sie bei der Vorbereitung der AWS-Umgebung erstellt haben.
- Der zugrunde liegende AWS Festplattentyp gilt für das erste Cloud Volumes ONTAP Volume.

  Sie können einen anderen Festplattentyp für nachfolgende Volumes auswählen.

- Die Performance von AWS Festplatten ist an die Festplattengröße gebunden.

  Sie sollten die Festplattengröße wählen, die Ihnen die benötigte kontinuierliche Performance bietet. Weitere Details zur EBS-Performance finden Sie in der AWS Dokumentation.

- Die Festplattengröße ist die Standardgröße für alle Festplatten im System.

> Wenn Sie später eine andere Größe benötigen, können Sie die Option Erweiterte Zuweisung verwenden, um ein Aggregat zu erstellen, das Festplatten einer bestimmten Größe verwendet.

Ergebnis

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

Schritt 8: Sicherheitszertifikate für Data Tiering installieren

Sicherheitszertifikate müssen manuell installiert werden, um Daten-Tiering in den Regionen AWS Secret Cloud und Top Secret Cloud zu aktivieren.

Bevor Sie beginnen

1. Erstellung von S3 Buckets:

> Stellen Sie sicher, dass den Bucket-Namen vorangestellt ist `fabric-pool-`. Beispiel `fabric-pool-testbucket`.

2. Behalten Sie die in installierten Stammzertifikate bei `step 4` Praktisch.

Schritte

1. Kopieren Sie den Text aus den Stammzertifikaten, die Sie in installiert haben `step 4`.

2. Stellen Sie über die CLI eine sichere Verbindung zum Cloud Volumes ONTAP System her.
3. Installieren Sie die Stammzertifikate. Drücken Sie möglicherweise die Taste `ENTER` Mehrmals drücken:

```
security certificate install -type server-ca -cert-name <certificate-
name>
```

4. Wenn Sie dazu aufgefordert werden, geben Sie den gesamten kopierten Text ein, einschließlich und aus `----- BEGIN CERTIFICATE -----` Bis `----- END CERTIFICATE -----`.
5. Bewahren Sie eine Kopie des CA-signierten digitalen Zertifikats zur späteren Verwendung auf.
6. Behalten Sie den Namen der Zertifizierungsstelle und die Seriennummer des Zertifikats bei.
7. Konfigurieren Sie den Objektspeicher für AWS Secret Cloud und Top Secret Cloud-Regionen: `set -privilege advanced -confirmations off`
8. Führen Sie diesen Befehl aus, um den Objektspeicher zu konfigurieren.

> ⓘ Alle Amazon Resource Names (Arns) sollten mit einer Suffix versehen werden `-iso-b`, Wie z. B. `arn:aws-iso-b`. Wenn eine Ressource beispielsweise ein ARN mit einer Region erfordert, verwenden Sie für Top Secret Cloud die Namenskonvention als `us-iso-b` Für das `-server` Flagge. Für AWS Secret Cloud verwenden Sie `us-iso-b-1`.

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. Überprüfen Sie, ob der Objektspeicher erfolgreich erstellt wurde: `storage aggregate object-store show -instance`
10. Fügen Sie den Objektspeicher dem Aggregat zu. Dies sollte für jedes neue Aggregat wiederholt werden: `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

Erste Schritte in Microsoft Azure

Schnellstart für Cloud Volumes ONTAP in Azure

Erste Schritte mit Cloud Volumes ONTAP für Azure

1 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 Cloud Volumes ONTAP in einem Subnetz bereitstellen möchten, in dem kein Internetzugang verfügbar ist, müssen Sie den Connector manuell installieren und auf die BlueXP Benutzeroberfläche zugreifen, die auf diesem Connector ausgeführt wird. "Erfahren Sie, wie Sie den Connector manuell an einem

Ort ohne Internetzugang installieren"

2 Planen Sie Ihre Konfiguration

BlueXP 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 .".

3 Richten Sie Ihr Netzwerk ein

1. Stellen Sie sicher, dass Ihre vnet und Subnetze Verbindungen zwischen dem Connector und Cloud Volumes ONTAP unterstützen.
2. Outbound-Internetzugang über die Ziel-VPC für NetApp AutoSupport aktivieren

   Dieser Schritt ist nicht erforderlich, wenn Sie Cloud Volumes ONTAP an einem Ort bereitstellen, an dem kein Internetzugang verfügbar ist.

"Erfahren Sie mehr über Netzwerkanforderungen".

4 Starten Sie Cloud Volumes ONTAP mit BlueXP

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

- "Erstellen eines Connectors von BlueXP"
- "Erstellen eines Connectors über den Azure Marketplace"
- "Installieren der Connector-Software auf einem Linux-Host"
- "Was BlueXP mit Berechtigungen macht"

Planen Sie Ihre 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.

Wählen Sie eine Cloud Volumes ONTAP Lizenz

Für Cloud Volumes ONTAP sind verschiedene Lizenzierungsoptionen verfügbar. Jede Option ermöglicht Ihnen, ein Nutzungsmodell auszuwählen, das Ihren Anforderungen entspricht.

- "Informieren Sie sich über Lizenzoptionen für Cloud Volumes ONTAP"
- "Erfahren Sie, wie Sie eine Lizenzierung einrichten"

Wählen Sie eine unterstützte Region aus

Cloud Volumes ONTAP wird in den meisten Microsoft Azure Regionen unterstützt. "Hier finden Sie die vollständige Liste der unterstützten Regionen".

Wählen Sie einen unterstützten VM-Typ aus

Cloud Volumes ONTAP unterstützt je nach Lizenztyp mehrere VM-Typen.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in Azure"

Analysieren Sie Ihre Storage-Grenzen

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 in Azure"

Größe 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 mit Single-Node-Systemen

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

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.

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

Azure-Festplattentyp mit HA-Paaren

HA-Systeme verwenden Shared Managed Disks mit Premium-SSDs, die beide eine hohe Performance für I/O-intensive Workloads mit höheren Kosten bieten. HA-Implementierungen, die vor der Version 9.12.1 erstellt wurden, verwenden Premium-Blobs auf Seite.

Festplattengröße Azure

Wenn Sie Cloud Volumes ONTAP Instanzen starten, müssen Sie die standardmäßige Festplattengröße für Aggregate auswählen. BlueXP verwendet diese Festplattengröße für das anfängliche Aggregat und für alle zusätzlichen Aggregate, die es beim Verwenden der einfachen Bereitstellungsoption erstellt. 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. Beispiel: Durch das Auswählen von 1 tib Festplatten kann eine bessere Performance als 500 gib Festplatten zu höheren Kosten erzielt werden.

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"

Anzeigen von Standard-Systemfestplatten

Neben dem Storage für Benutzerdaten erwirbt BlueXP auch Cloud-Storage für Cloud Volumes ONTAP Systemdaten (Boot-Daten, Root-Daten, Core-Daten und NVRAM). Für die Planung können Sie diese Details überprüfen, bevor Sie Cloud Volumes ONTAP implementieren.

"Zeigen Sie die Standardfestplatten für Cloud Volumes ONTAP-Systemdaten in Azure an".

Für den Connector ist außerdem eine Systemfestplatte erforderlich. "Zeigen Sie Details zur Standardkonfiguration des Connectors an".

Sammeln von Netzwerkinformationen

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)	

Wählen Sie eine Schreibgeschwindigkeit

Mit BlueXP können Sie eine Schreibgeschwindigkeitseinstellung für Cloud Volumes ONTAP auswählen. 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. "Erfahren Sie mehr über Schreibgeschwindigkeit".

Wählen Sie ein Volume-Auslastungsprofil aus

ONTAP umfasst mehrere Storage-Effizienzfunktionen, mit denen Sie die benötigte Storage-Gesamtmenge reduzieren können. Wenn Sie ein Volume in BlueXP 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 Cloud Volumes ONTAP in Azure

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

Anforderungen für Cloud Volumes ONTAP

Die folgenden Netzwerkanforderungen müssen in Azure erfüllt werden.

Outbound-Internetzugang

Cloud Volumes ONTAP Nodes benötigen Outbound-Internetzugang für NetApp AutoSupport, der den Zustand Ihres Systems proaktiv überwacht und Meldungen an den technischen Support von NetApp sendet.

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

Wenn keine ausgehende Internetverbindung zum Senden von AutoSupport-Nachrichten verfügbar ist, konfiguriert BlueXP Ihre Cloud Volumes ONTAP-Systeme automatisch so, dass der Connector als Proxy-Server verwendet wird. Die einzige Anforderung besteht darin, sicherzustellen, dass die Sicherheitsgruppe des Connectors *eingehende* -Verbindungen über Port 3128 zulässt. Nach der Bereitstellung des Connectors

müssen Sie diesen Port öffnen.

Wenn Sie strenge ausgehende Regeln für Cloud Volumes ONTAP definiert haben, müssen Sie auch sicherstellen, dass die Cloud Volumes ONTAP-Sicherheitsgruppe *Outbound*-Verbindungen über Port 3128 zulässt.

Nachdem Sie bestätigt haben, dass der ausgehende Internetzugang verfügbar ist, können Sie AutoSupport testen, um sicherzustellen, dass er Nachrichten senden kann. Anweisungen finden Sie unter "ONTAP Dokumentation: Einrichten von AutoSupport".

Wenn Sie von BlueXP darüber informiert werden, dass AutoSupport-Meldungen nicht gesendet werden können, "Fehler bei der AutoSupport Konfiguration beheben".

IP-Adressen

BlueXP weist Cloud Volumes ONTAP in Azure automatisch die erforderliche Anzahl privater IP-Adressen zu. Sie müssen sicherstellen, dass Ihr Netzwerk über genügend private IP-Adressen verfügt.

Die Anzahl der LIFs, die BlueXP für Cloud Volumes ONTAP zuweist, hängt davon ab, ob Sie ein Single Node-System oder ein HA-Paar implementieren. Ein LIF ist eine IP-Adresse, die einem physischen Port zugewiesen ist. Für Managementtools wie SnapCenter ist eine SVM-Management-LIF erforderlich.

> Ein iSCSI LIF bietet Client-Zugriff über das iSCSI-Protokoll und wird vom System für andere wichtige Netzwerk-Workflows verwendet. Diese LIFs sind erforderlich und sollten nicht gelöscht werden.

IP-Adressen für ein Single Node-System

BlueXP weist 5 oder 6 IP-Adressen einem System mit einem Knoten zu:

- Cluster-Management-IP
- Node-Management-IP
- Intercluster IP für SnapMirror
- NFS/CIFS-IP
- ISCSI-IP

> Die iSCSI-IP ermöglicht den Client-Zugriff über das iSCSI-Protokoll. Es wird vom System auch für andere wichtige Netzwerk-Workflows verwendet. Dieses LIF ist erforderlich und sollte nicht gelöscht werden.

- SVM-Management (optional – nicht standardmäßig konfiguriert)

IP-Adressen für HA-Paare

BlueXP weist während der Bereitstellung 4 NICs (pro Node) IP-Adressen zu.

Beachten Sie, dass BlueXP in Azure eine SVM Management-LIF auf HA-Paaren erstellt, nicht jedoch auf Systemen mit einzelnen Nodes.

NIC0

- Node-Management-IP

- Intercluster-IP
- ISCSI-IP

> Die iSCSI-IP ermöglicht den Client-Zugriff über das iSCSI-Protokoll. Es wird vom System auch für andere wichtige Netzwerk-Workflows verwendet. Dieses LIF ist erforderlich und sollte nicht gelöscht werden.

NIC1

- Cluster-Netzwerk-IP

NIC2

- Cluster Interconnect IP (HA-IC)

NIC3

- PageBLOB NIC-IP (Festplattenzugriff)

> NIC3 gilt nur für HA-Implementierungen, die BLOB Storage auf Seite verwenden.

Die oben genannten IP-Adressen migrieren nicht bei Failover-Ereignissen.

Zusätzlich werden 4 Frontend-IPs (FIPS) für die Migration bei Failover-Ereignissen konfiguriert. Diese Frontend-IPs sind im Load Balancer aktiv.

- Cluster-Management-IP
- NodeA Daten-IP (NFS/CIFS)
- NodeB-Daten-IP (NFS/CIFS)
- SVM-Management-IP

Sichere Verbindung zu Azure Services

Standardmäßig aktiviert BlueXP einen Azure Private Link für Verbindungen zwischen Blob-Storage-Konten auf der Cloud Volumes ONTAP- und Azure-Seite.

In den meisten Fällen ist nichts für Sie erforderlich – BlueXP managt den Azure Private Link für Sie. Aber wenn Sie Azure Private DNS verwenden, dann müssen Sie eine Konfigurationsdatei bearbeiten. Sie sollten auch eine Anforderung für den Connector-Standort in Azure kennen.

Sie können die Private Link-Verbindung auch deaktivieren, wenn dies von Ihren geschäftlichen Anforderungen erforderlich ist. Wenn Sie den Link deaktivieren, konfiguriert BlueXP stattdessen Cloud Volumes ONTAP für die Verwendung eines Service-Endpunkts.

"Weitere Informationen zur Verwendung von Azure Private Links oder Service-Endpunkten mit Cloud Volumes ONTAP".

Verbindungen zu anderen ONTAP Systemen

Um Daten zwischen einem Cloud Volumes ONTAP System in Azure und ONTAP Systemen in anderen Netzwerken zu replizieren, benötigen Sie eine VPN-Verbindung zwischen dem Azure vnet und dem anderen Netzwerk, beispielsweise Ihrem Unternehmensnetzwerk.

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

Port für den HA Interconnect

Ein Cloud Volumes ONTAP HA-Paar enthält einen HA Interconnect, der jedem Knoten erlaubt, kontinuierlich zu überprüfen, ob sein Partner funktioniert und um Protokolldaten für den anderen nichtflüchtigen Speicher zu spiegeln. Das HA Interconnect verwendet TCP Port 10006 für die Kommunikation.

Standardmäßig ist die Kommunikation zwischen den HA Interconnect LIFs offen, und es gibt keine Sicherheitsgruppenregeln für diesen Port. Wenn Sie jedoch eine Firewall zwischen den HA Interconnect LIFs erstellen, müssen Sie sicherstellen, dass TCP Traffic für Port 10006 offen ist, damit das HA-Paar ordnungsgemäß arbeiten kann.

Nur ein HA-Paar in einer Azure-Ressourcengruppe

Sie müssen für jedes Cloud Volumes ONTAP HA-Paar, das Sie in Azure implementieren, eine *dedizierte* Ressourcengruppe verwenden. Es wird nur ein HA-Paar in einer Ressourcengruppe unterstützt.

Bei BlueXP treten Verbindungsprobleme auf, wenn Sie versuchen, ein zweites Cloud Volumes ONTAP HA-Paar in einer Azure Ressourcengruppe bereitzustellen.

Regeln für Sicherheitsgruppen

BlueXP erstellt Azure-Sicherheitsgruppen mit den ein- und ausgehenden Regeln, die für den erfolgreichen Betrieb von Cloud Volumes ONTAP erforderlich sind. Sie können sich zu Testzwecken auf die Ports beziehen oder wenn Sie Ihre eigenen Sicherheitsgruppen verwenden möchten.

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

Sie suchen Informationen über den Connector? "Zeigen Sie die Sicherheitsgruppenregeln für den Konnektor an"

Eingehende Regeln für Single-Node-Systeme

Wenn Sie eine Arbeitsumgebung erstellen und eine vordefinierte Sicherheitsgruppe auswählen, können Sie den Datenverkehr innerhalb einer der folgenden Optionen zulassen:

- **Nur vnet ausgewählt**: Die Quelle für eingehenden Datenverkehr ist der Subnetz-Bereich des vnet für das Cloud Volumes ONTAP-System und der Subnetz-Bereich des vnet, in dem sich der Connector befindet. Dies ist die empfohlene Option.
- **Alle VNets**: Die Quelle für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.

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

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
1001 Inbound_http	80 TCP	Beliebige Art	HTTP-Zugriff auf die System Manager Webkonsole mit der IP-Adresse der Cluster-Management-LIF
1002 Inbound_111_tcp	111 TCP	Beliebige Art	Remote-Prozeduraufruf für NFS
1003 Inbound_111_udp	111 UDP	Beliebige Art	Remote-Prozeduraufruf für NFS
1004 eingehend_139	139 TCP	Beliebige Art	NetBIOS-Servicesitzung für CIFS
1005 Inbound_161-162 _tcp	161-162 TCP	Beliebige Art	Einfaches Netzwerkverwaltungsprotokoll
1006 Inbound_161-162 _udp	161-162 UDP	Beliebige Art	Einfaches Netzwerkverwaltungsprotokoll
1007 eingehend_443	443 TCP	Beliebige Art	Konnektivität mit dem Connector und 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

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
3000 Inbound_Deny_all_tcp	Alle TCP-Ports	Beliebige Art	Blockieren Sie den gesamten anderen TCP-eingehenden Datenverkehr
3001 Inbound_Deny_all_udp	Alle Ports UDP	Beliebige Art	Alle anderen UDP-eingehenden Datenverkehr blockieren
65000 AllowVnetInBound	Alle Ports und Protokolle	VirtualNetwork zu VirtualNetwork	Eingehender Verkehr aus dem vnet
65001 AllowAzureLoad BalancerInBound	Alle Ports und Protokolle	AzureLoadBalancer zu jedem	Datenverkehr vom Azure Standard Load Balancer
65500 DenyAllInBound	Alle Ports und Protokolle	Beliebige Art	Alle anderen eingehenden Datenverkehr blockieren

Eingehende Regeln für HA-Systeme

Wenn Sie eine Arbeitsumgebung erstellen und eine vordefinierte Sicherheitsgruppe auswählen, können Sie den Datenverkehr innerhalb einer der folgenden Optionen zulassen:

- **Nur vnet ausgewählt**: Die Quelle für eingehenden Datenverkehr ist der Subnetz-Bereich des vnet für das Cloud Volumes ONTAP-System und der Subnetz-Bereich des vnet, in dem sich der Connector befindet. Dies ist die empfohlene Option.
- **Alle VNets**: Die Quelle für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.

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	Konnektivität mit dem Connector und 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

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
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)

Service	Port	Protokoll	Quelle	Ziel	Zweck
AutoSupport	HTTPS	443	Node Management-LIF	support.netapp.com	AutoSupport (HTTPS ist der Standard)
	HTTP	80	Node Management-LIF	support.netapp.com	AutoSupport (nur wenn das Transportprotokoll von HTTPS zu HTTP geändert wird)
	TCP	3128	Node Management-LIF	Stecker	Senden von AutoSupport-Nachrichten über einen Proxy-Server auf dem Connector, falls keine ausgehende Internetverbindung verfügbar ist
Konfigurations-Backups	HTTP	80	Node Management-LIF	\Http://<connector-IP-address>/occm/offboxconfig	Senden Sie Konfigurationssicherungen an den Connector. "Informationen zu Backup-Dateien für die Konfiguration".
DHCP	68	UDP	Node Management-LIF	DHCP	DHCP-Client für die erstmalige Einrichtung
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

Anforderungen an den Steckverbinder

Wenn Sie noch keinen Connector erstellt haben, sollten Sie auch die Netzwerkanforderungen für den Connector prüfen.

- "Zeigen Sie die Netzwerkanforderungen für den Connector an"
- "Für Sicherheitsgruppen gibt es in Azure Regeln"

Cloud Volumes ONTAP einrichten, um einen vom Kunden gemanagten Schlüssel in Azure zu verwenden

Die Daten werden auf Cloud Volumes ONTAP in Azure automatisch verschlüsselt "Azure Storage Service Encryption" Mit einem von Microsoft gemanagten Schlüssel Aber Sie können Ihren eigenen Verschlüsselungsschlüssel verwenden, indem Sie die Schritte auf dieser Seite befolgen.

Übersicht über die Datenverschlüsselung

Cloud Volumes ONTAP-Daten werden in Azure automatisch verschlüsselt "Azure Storage Service Encryption". Bei der Standardimplementierung wird ein von Microsoft verwalteter Schlüssel verwendet. Es ist keine Einrichtung erforderlich.

Wenn Sie einen vom Kunden gemanagten Schlüssel mit Cloud Volumes ONTAP verwenden möchten, müssen Sie folgende Schritte ausführen:

1. Aus Azure erstellen Sie einen Schlüsselspeicher und generieren Sie anschließend einen Schlüssel in diesem Vault
2. Verwenden Sie für BlueXP die API, um eine Cloud Volumes ONTAP-Arbeitsumgebung zu erstellen, in der der Schlüssel zum Einsatz kommt

Rotation von Schlüsseln

Wenn Sie eine neue Version Ihres Schlüssels erstellen, verwendet Cloud Volumes ONTAP automatisch die neueste Schlüsselversion.

Verschlüsselte Daten

BlueXP verwendet einen Satz Festplattenverschlüsselung, der das Management von Verschlüsselungen mit gemanagten Festplatten und nicht mit Page-Blobs ermöglicht. Neue Festplatten verwenden ebenfalls denselben Festplattenverschlüsselungssatz. Bei niedrigeren Versionen wird der von Microsoft verwaltete Schlüssel anstelle des vom Kunden verwalteten Schlüssels verwendet.

Nachdem Sie eine Cloud Volumes ONTAP Arbeitsumgebung erstellt haben, in der ein vom Kunden gemanagter Schlüssel verwendet wird, werden Cloud Volumes ONTAP Daten wie folgt verschlüsselt.

Cloud Volumes ONTAP-Konfiguration	Systemfestplatten, die für die Schlüsselverschlüsselung verwendet werden	Datenfestplatten, die für die Verschlüsselung des Schlüssels verwendet werden
Single Node	• Booten • Kern • NVRAM	• Stamm • Daten
Azure HA, eine einzelne Verfügbarkeitszone mit Page-Blobs	• Booten • Kern • NVRAM	Keine
Azure HA, eine einzelne Verfügbarkeitszone mit gemeinsam genutzten verwalteten Festplatten	• Booten • Kern • NVRAM	• Stamm • Daten
Azure HA mehrere Verfügbarkeitszonen mit gemeinsam genutzten gemanagten Festplatten	• Booten • Kern • NVRAM	• Stamm • Daten

Alle Azure-Storage-Konten für Cloud Volumes ONTAP werden über einen vom Kunden gemanagten Schlüssel verschlüsselt. Wenn Sie Ihre Speicherkonten während ihrer Erstellung verschlüsseln möchten, müssen Sie in der CVO-Erstellungsanforderung die ID der Ressource erstellen und angeben. Dies gilt für alle Implementierungsarten. Wenn Sie es nicht bereitstellen, werden die Speicherkonten immer noch verschlüsselt, aber BlueXP erstellt zuerst die Speicherkonten mit von Microsoft administrierter Verschlüsselungsmethode und aktualisiert dann die Speicherkonten, um den vom Kunden verwalteten Schlüssel zu verwenden.

Erstellen Sie eine vom Benutzer zugewiesene verwaltete Identität

Sie haben die Möglichkeit, eine Ressource zu erstellen, die als benutzerzugewiesene verwaltete Identität bezeichnet wird. Auf diese Weise können Sie Ihre Storage-Konten verschlüsseln, wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen. Wir empfehlen, diese Ressource zu erstellen, bevor Sie einen Schlüsseltresor erstellen und einen Schlüssel erzeugen.

Die Ressource hat die folgende ID: `userassignedidentity`.

Schritte

1. Gehen Sie in Azure zu Azure Services und wählen Sie **verwaltete Identitäten** aus.
2. Klicken Sie Auf **Erstellen**.
3. Geben Sie folgende Informationen an:
   - **Abonnement**: Wählen Sie ein Abonnement. Wir empfehlen, dasselbe Abonnement wie das Connector-Abonnement zu wählen.
   - **Ressourcengruppe**: Verwenden Sie eine vorhandene Ressourcengruppe oder erstellen Sie eine neue.
   - **Region**: Wählen Sie optional die gleiche Region wie der Connector.

- **Name**: Geben Sie einen Namen für die Ressource ein.

4. Optional können Sie Tags hinzufügen.
5. Klicken Sie Auf **Erstellen**.

Erstellen eines Schlüsselgewölbes und Generieren eines Schlüssels

Der Schlüsselspeicher muss in demselben Azure Abonnement und derselben Region liegen, in der Sie das Cloud Volumes ONTAP System erstellen möchten.

Wenn Sie Eine vom Benutzer zugewiesene verwaltete Identität wurde erstellt, Beim Erstellen des Schlüsseltresors sollten Sie auch eine Zugangsrichtlinie für den Schlüsseltresor erstellen.

Schritte

1. "Erstellen Sie einen Schlüsselspeicher in Ihrem Azure-Abonnement".

   Beachten Sie die folgenden Anforderungen für den Schlüsselspeicher:

   - Der Schlüsselgewölbe muss sich in derselben Region wie das Cloud Volumes ONTAP System befinden.
   - Die folgenden Optionen sollten aktiviert sein:
     - **Soft-delete** (diese Option ist standardmäßig aktiviert, muss aber nicht_ deaktiviert sein)
     - **Schutz löschen**
     - **Azure Festplattenverschlüsselung für Volume Encryption** (für Single Node-Systeme oder HA-Paare in mehreren Zonen)
   - Die folgende Option sollte aktiviert sein, wenn Sie eine vom Benutzer zugewiesene verwaltete Identität erstellt haben:
     - **Vault-Zugangsrichtlinie**
2. Wenn Sie die Vault-Zugriffsrichtlinie ausgewählt haben, klicken Sie auf Erstellen, um eine Zugriffsrichtlinie für den Schlüsseltresor zu erstellen. Falls nicht, fahren sie mit Schritt 3 fort.
   a. Wählen Sie die folgenden Berechtigungen aus:
      - Get
      - Liste
      - Entschlüsseln
      - Verschlüsseln
      - Taste zum Auspacken
      - Umbruch-Taste
      - Verifizieren
      - signieren
   b. Wählen Sie die vom Benutzer zugewiesene verwaltete Identität (Ressource) als Prinzipal aus.
   c. Überprüfen und erstellen Sie die Zugriffsrichtlinie.
3. "Einen Schlüssel im Schlüsselspeicher erzeugen".

   Beachten Sie die folgenden Anforderungen für den Schlüssel:

- Der Schlüsseltyp muss **RSA** sein.
- Die empfohlene RSA-Schlüsselgröße beträgt **2048**, andere Größen werden unterstützt.

Erstellen Sie eine Arbeitsumgebung, in der der Verschlüsselungsschlüssel verwendet wird

Nachdem Sie den Schlüsselspeicher erstellt und einen Verschlüsselungsschlüssel generiert haben, können Sie ein neues Cloud Volumes ONTAP-System erstellen, das für die Verwendung des Schlüssels konfiguriert ist. Diese Schritte werden von der BlueXP API unterstützt.

Erforderliche Berechtigungen

Wenn Sie einen vom Kunden verwalteten Schlüssel mit einem Cloud Volumes ONTAP-System mit einem einzelnen Knoten verwenden möchten, stellen Sie sicher, dass der BlueXP-Connector über die folgenden Berechtigungen verfügt:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"Zeigen Sie die aktuelle Liste der Berechtigungen an"

Schritte

1. Nutzen Sie den folgenden BlueXP API-Aufruf, um die Liste der Schlüsselvaults in Ihrem Azure-Abonnement zu erhalten.

   Bei einem HA-Paar: `GET /azure/ha/metadata/vaults`

   Für Single Node: `GET /azure/vsa/metadata/vaults`

   Notieren Sie sich den **Namen** und die **resourceGroup**. Im nächsten Schritt müssen Sie diese Werte angeben.

   "Weitere Informationen zu diesem API-Aufruf".

2. Rufen Sie die Liste der Schlüssel im Tresor mithilfe des folgenden BlueXP API-Aufrufs ab.

   Bei einem HA-Paar: `GET /azure/ha/metadata/keys-vault`

   Für Single Node: `GET /azure/vsa/metadata/keys-vault`

   Notieren Sie sich den **Keyname**. Im nächsten Schritt müssen Sie diesen Wert (zusammen mit dem Vault-Namen) angeben.

   "Weitere Informationen zu diesem API-Aufruf".

3. Erstellen Sie ein Cloud Volumes ONTAP-System mithilfe des folgenden BlueXP-API-Aufrufs.

   a. Bei einem HA-Paar:

`POST /azure/ha/working-environments`

Der Text der Anforderung muss die folgenden Felder enthalten:

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

Nehmen Sie die auf `"userAssignedIdentity": " userAssignedIdentityId"` Feld, wenn Sie diese Ressource für die Verschlüsselung von Speicherkontos erstellt haben.

"Weitere Informationen zu diesem API-Aufruf".

b. System mit einem einzelnen Node:

`POST /azure/vsa/working-environments`

Der Text der Anforderung muss die folgenden Felder enthalten:

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

Nehmen Sie die auf `"userAssignedIdentity": " userAssignedIdentityId"` Feld, wenn Sie diese Ressource für die Verschlüsselung von Speicherkontos erstellt haben.

"Weitere Informationen zu diesem API-Aufruf".

Ergebnis

Sie verfügen über ein neues Cloud Volumes ONTAP System, das so konfiguriert ist, dass Sie Ihren vom Kunden gemanagten Schlüssel zur Datenverschlüsselung nutzen können.

Lizenzierung für Cloud Volumes ONTAP in Azure einrichten

Nachdem Sie sich für die Lizenzoption entschieden haben, die Sie mit Cloud Volumes ONTAP verwenden möchten, sind einige Schritte erforderlich, bevor Sie beim Erstellen einer neuen Arbeitsumgebung die Lizenzoption wählen können.

Freimium

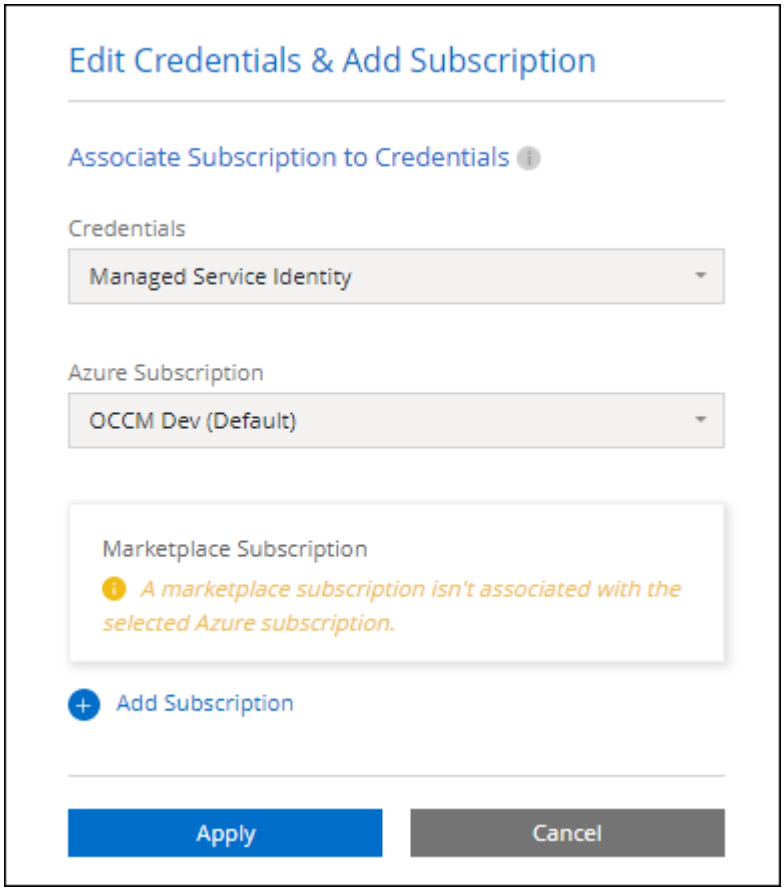
Wählen Sie das Freimium-Angebot aus, um Cloud Volumes ONTAP mit bis zu 500 gib bereitgestellter Kapazität kostenlos zu nutzen. "Erfahren Sie mehr über das Freemium Angebot".

Schritte

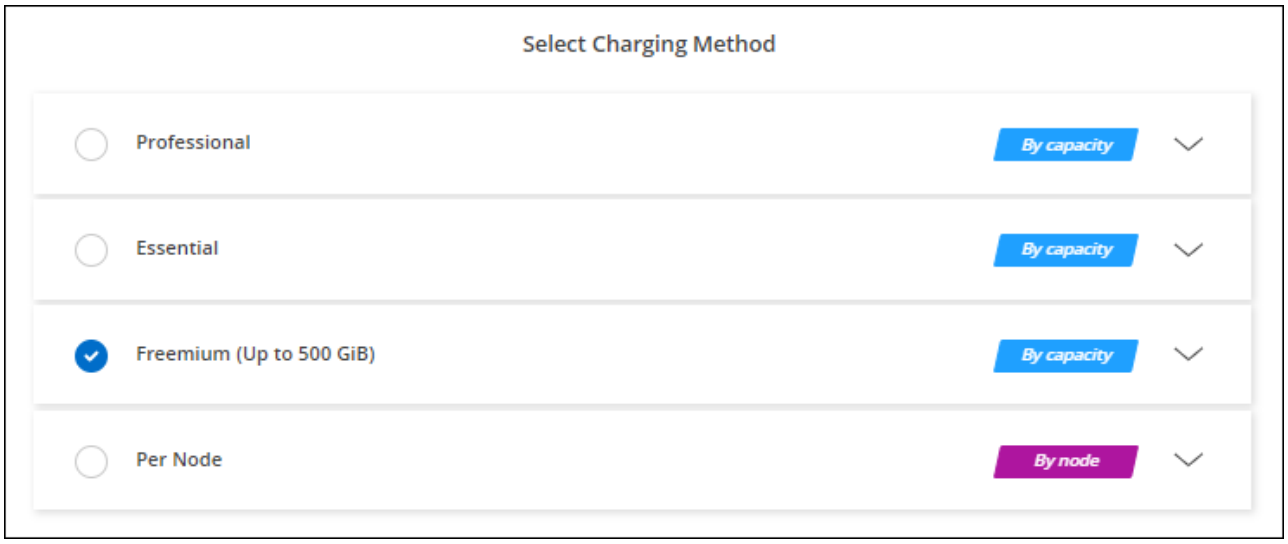
1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.

   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um das Pay-as-you-go-Angebot im Azure Marketplace zu abonnieren.

      Sie werden über das Marketplace-Abonnement nicht belastet, es sei denn, Sie überschreiten 500 gib der bereitgestellten Kapazität. Zu dieser Zeit wird das System automatisch in das konvertiert "Essentials-Paket".



   a. Wenn Sie zu BlueXP zurückkehren, wählen Sie **Freemium**, wenn Sie die Seite mit den Lademethoden aufrufen.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Azure zu starten".

Kapazitätsbasierte Lizenz

Dank der kapazitätsbasierten Lizenzierung können Sie für Cloud Volumes ONTAP pro tib Kapazität bezahlen. Kapazitätsbasierte Lizenzierung ist in Form eines *package*, dem Essentials-Paket oder dem Professional-Paket verfügbar.

Die Essentials- und Professional-Pakete sind mit den folgenden Verbrauchsmodellen erhältlich:

- Eine Lizenz (BYOL) von NetApp erworben
- Ein stündliches PAYGO-Abonnement (Pay-as-you-go) im Azure Marketplace
- Einem Jahresvertrag

"Hier erhalten Sie weitere Informationen zur kapazitätsbasierten Lizenzierung".

In den folgenden Abschnitten werden die ersten Schritte mit jedem dieser Nutzungsmodelle beschrieben.

BYOL

Bezahlen Sie vorab, indem Sie eine Lizenz (BYOL) von NetApp erwerben und Cloud Volumes ONTAP Systeme bei jedem Cloud-Provider implementieren.

Schritte

1. "Wenden Sie sich an den NetApp Sales, um eine Lizenz zu erhalten"
2. "Fügen Sie Ihr Konto für die NetApp Support Website zu BlueXP hinzu"

   BlueXP fragt den NetApp Lizenzierungsservice automatisch ab, um Details zu den Lizenzen zu erhalten, die mit Ihrem NetApp Support Site Konto verknüpft sind. Sollte es keine Fehler geben, fügt BlueXP die Lizenzen automatisch zum Digital Wallet hinzu.

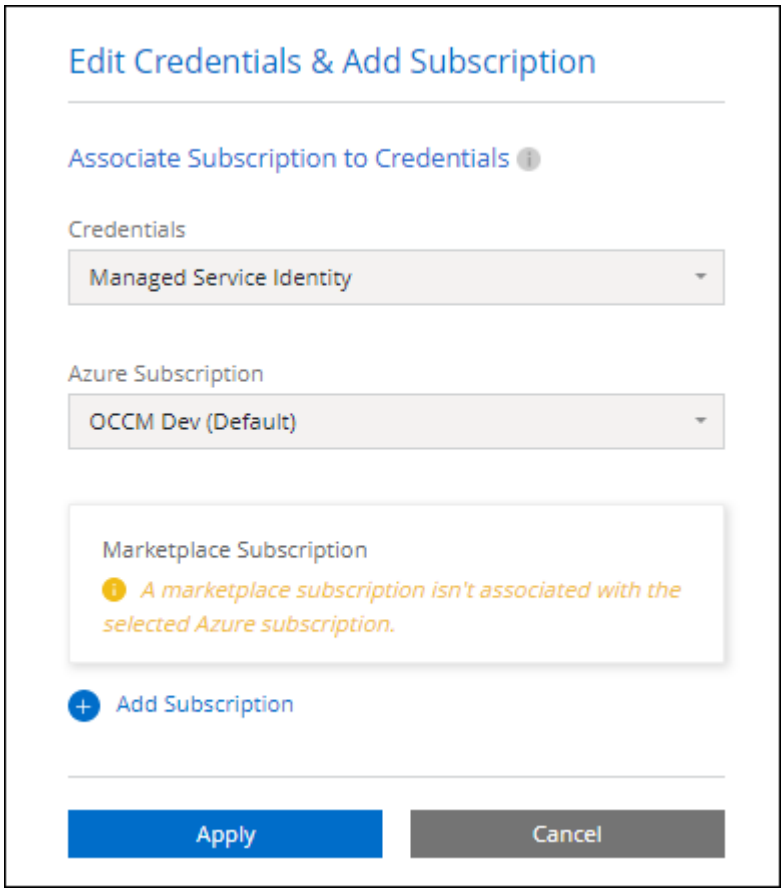
   Bevor Sie Ihre Lizenz mit Cloud Volumes ONTAP verwenden können, muss sie über das Digital Wallet von BlueXP erhältlich sein. Wenn nötig, können Sie "Fügen Sie die Lizenz manuell zum Digital Wallet von BlueXP hinzu".

3. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in

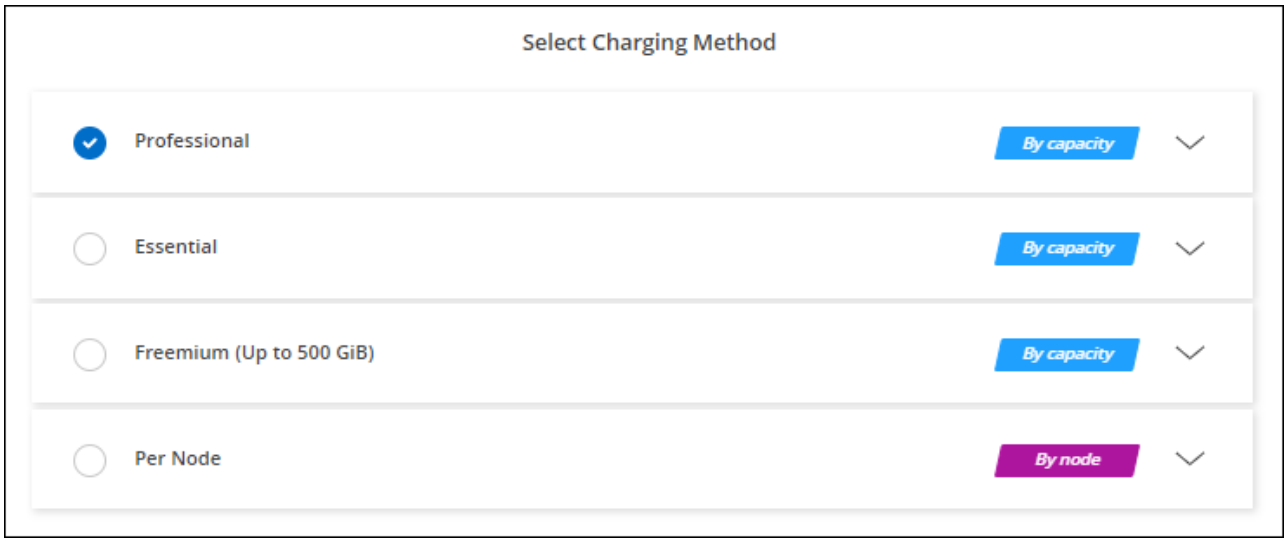
BlueXP.

a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um das Pay-as-you-go-Angebot im Azure Marketplace zu abonnieren.

   Die Lizenz, die Sie bei NetApp erworben haben, wird immer zuerst berechnet. Wenn Sie Ihre lizenzierte Kapazität überschreiten oder die Lizenzlaufzeit abgelaufen ist, werden Sie vom Stundensatz auf dem Markt in Rechnung gestellt.



a. Wenn Sie zu BlueXP zurückkehren, wählen Sie ein kapazitätsbasiertes Paket aus, wenn Sie die Seite mit den Lademethoden aufrufen.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Azure zu starten".

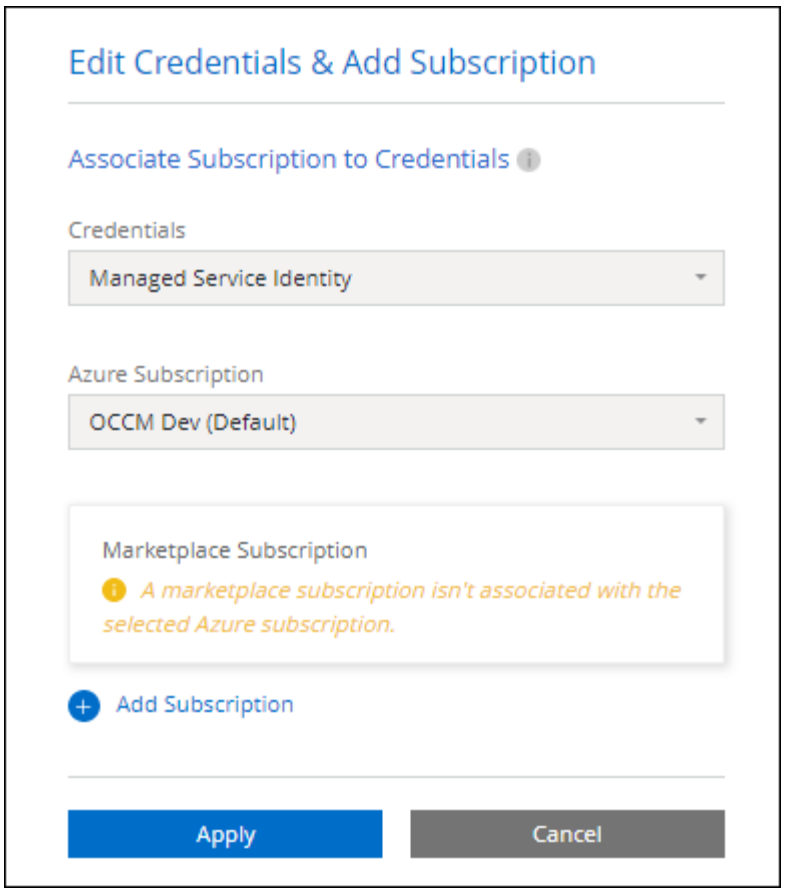
PAYGO-Abonnement

Sie bezahlen stündlich, indem Sie sich für das Angebot über den Marketplace Ihres Cloud-Providers anmelden.

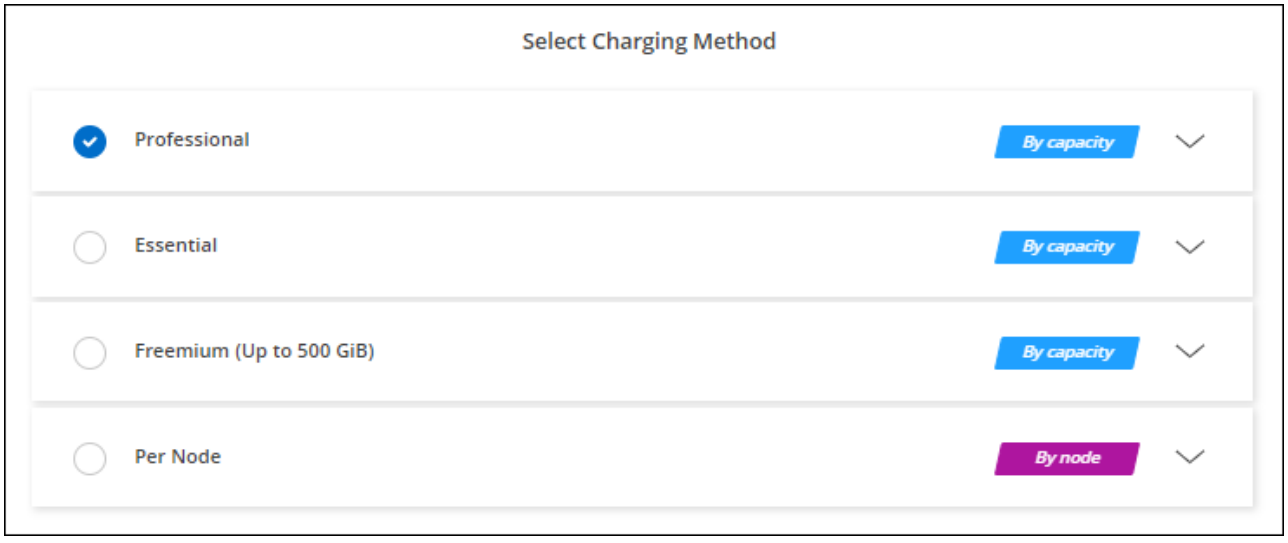
Wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von BlueXP aufgefordert, den Vertrag zu abonnieren, der im Azure Marketplace verfügbar ist. Dieses Abonnement wird dann zur Verrechnung mit der Arbeitsumgebung verknüpft. Sie können das gleiche Abonnement auch für zusätzliche Arbeitsumgebungen nutzen.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um das Pay-as-you-go-Angebot im Azure Marketplace zu abonnieren.



b. Wenn Sie zu BlueXP zurückkehren, wählen Sie ein kapazitätsbasiertes Paket aus, wenn Sie die Seite mit den Lademethoden aufrufen.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Azure zu starten".

Sie können die mit Ihren Azure-Konten verbundenen Azure Marketplace-Abonnements auf der Seite „Einstellungen“ > „Anmeldeinformationen“ managen. "Managen Sie Ihre Azure-Konten und -Abonnements"

Jahresvertrag

Sie bezahlen jährlich für Cloud Volumes ONTAP durch den Kauf eines Jahresvertrags.

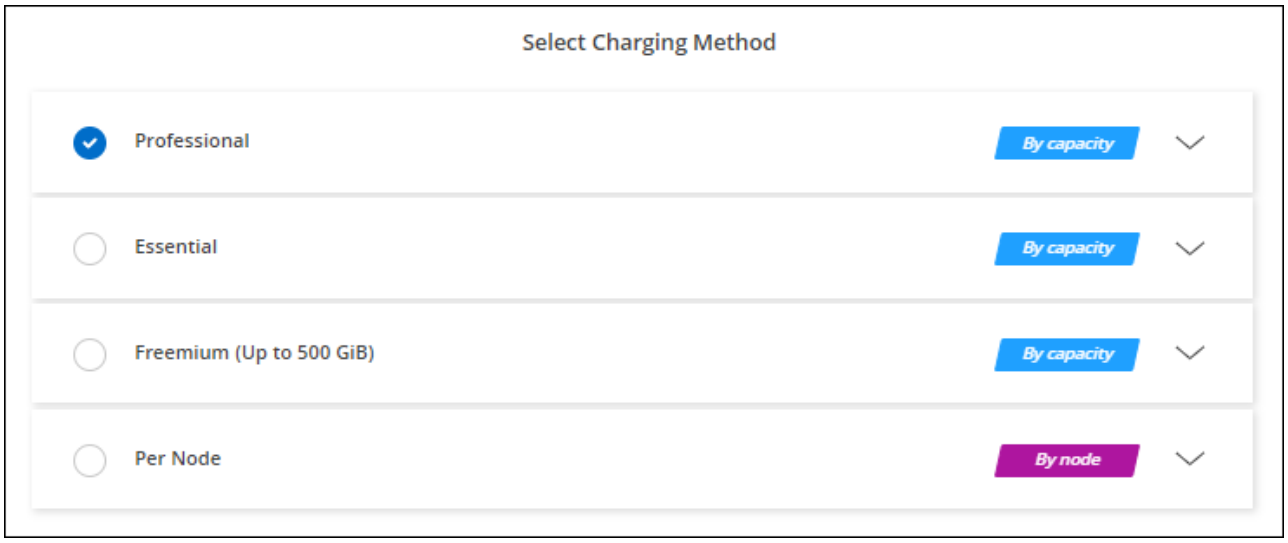
Schritte

1. Wenden Sie sich an Ihren NetApp Ansprechpartner, um einen Jahresvertrag zu erwerben.

   Der Vertrag ist als *privates* Angebot im Azure Marketplace erhältlich.

   Wenn NetApp Ihnen das private Angebot teilt, können Sie den Jahresplan auch auswählen, wenn Sie während der Erstellung der Arbeitsumgebung im Azure Marketplace abonnieren.

2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen > Weiter**.
   b. Wählen Sie im Azure-Portal den Jahresplan aus, der mit Ihrem Azure-Konto geteilt wurde, und klicken Sie anschließend auf **Abonnieren**.
   c. Wenn Sie zu BlueXP zurückkehren, wählen Sie ein kapazitätsbasiertes Paket aus, wenn Sie die Seite mit den Lademethoden aufrufen.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Azure zu starten".

Keystone Abonnement

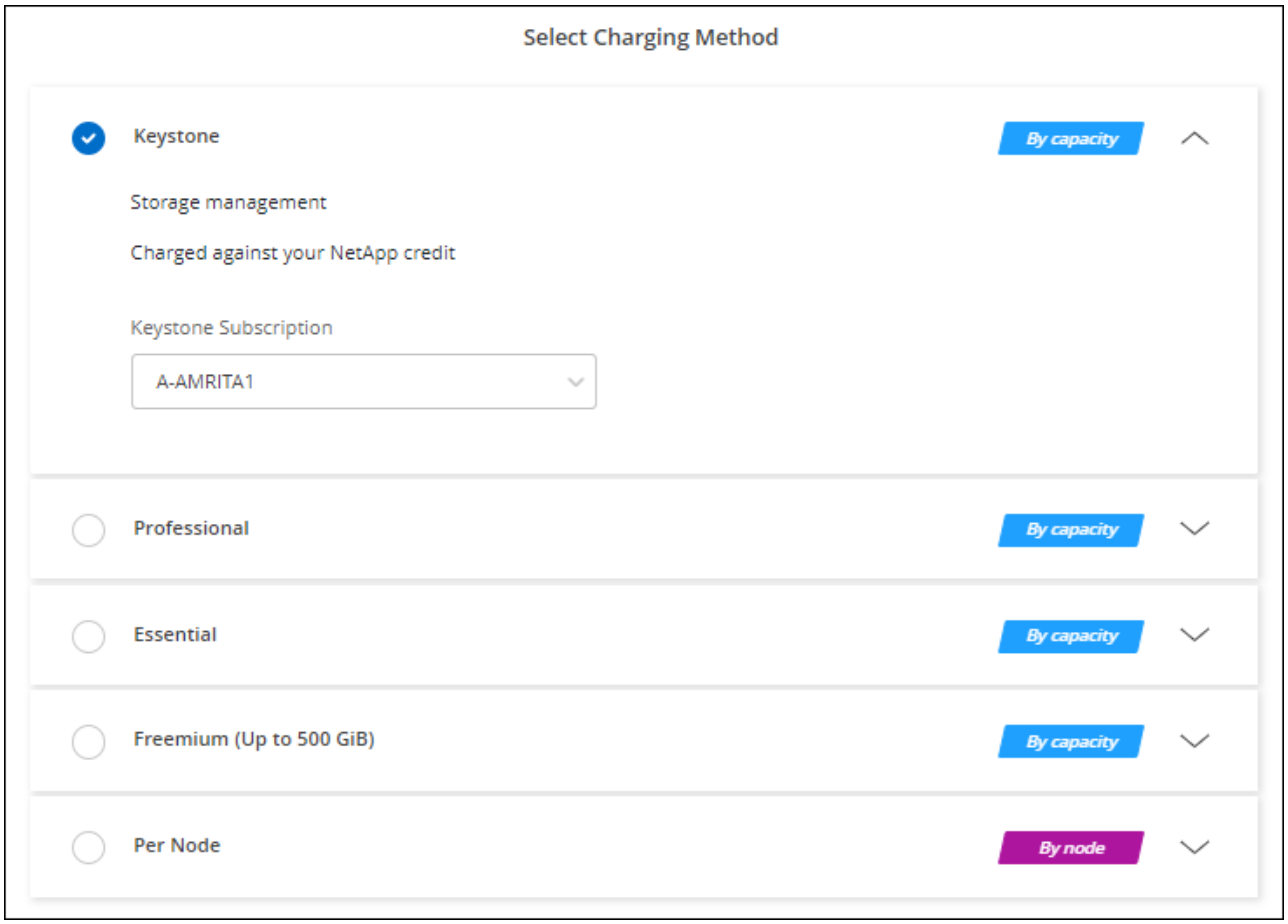
Ein Keystone Abonnement ist ein nutzungsbasierter Abonnementservice. "Weitere Informationen zu NetApp Keystone Abonnements".

Schritte

1. Wenn Sie noch kein Abonnement haben, "Kontakt zu NetApp"
2. Mailto:ng-keystone-success@netapp.com[NetApp kontaktieren]: Wir autorisieren Ihr BlueXP Benutzerkonto für eine oder mehrere Keystone Abonnements.
3. Nachdem NetApp den Account autorisiert hat, "Verknüpfen Sie Ihre Abonnements für die Verwendung mit Cloud Volumes ONTAP".
4. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in

BlueXP.

a. Wählen Sie die Abrechnungsmethode für Keystone Abonnements aus, wenn Sie zur Auswahl einer Lademethode aufgefordert werden.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Azure zu starten".

Aktivieren Sie den Hochverfügbarkeits-Modus in Azure

Der Hochverfügbarkeits-Modus von Microsoft Azure sollte aktiviert sein, um ungeplante Failover-Zeiten zu verringern und die NFSv4-Unterstützung für Cloud Volumes ONTAP zu aktivieren.

Ab der Version Cloud Volumes ONTAP 9.10.1 reduzierten wir die ungeplante Failover-Zeit für Cloud Volumes ONTAP HA-Paare, die in Microsoft Azure laufen, und fügten Unterstützung für NFSv4 hinzu. Um diese Verbesserungen für Cloud Volumes ONTAP verfügbar zu machen, müssen Sie die Hochverfügbarkeitsfunktion Ihres Azure Abonnements aktivieren.

In BlueXP werden Sie diese Angaben in einer Meldung „Aktion erforderlich“ eingeben, wenn die Funktion auf einem Azure-Abonnement aktiviert werden muss.

Beachten Sie Folgendes:

- Es gibt keine Probleme mit der Hochverfügbarkeit Ihres Cloud Volumes ONTAP HA-Paars. Diese Azure Funktion arbeitet in Kombination mit ONTAP, um die von Clients beobachteten Applikationsausfallzeiten für NFS-Protokolle zu reduzieren, die aus ungeplanten Failover-Ereignissen resultieren.

- Wenn Sie diese Funktion aktivieren, wird für Cloud Volumes ONTAP HA-Paare keine Unterbrechung verursacht.
- Wenn Sie diese Funktion auf Ihrem Azure-Abonnement aktivieren, treten keine Probleme bei anderen VMs auf.

Ein Azure-Benutzer mit „Owner“-Berechtigungen kann die Funktion über die Azure-CLI aktivieren.

Schritte

1. "Greifen Sie über das Azure-Portal auf die Azure Cloud Shell zu"
2. Registrieren der Funktion des Hochverfügbarkeits-Modus:

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. Überprüfen Sie optional, ob die Funktion jetzt registriert ist:

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Die Azure CLI sollte ein Ergebnis wie die folgenden zurückgeben:

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

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 BlueXP erstellen.

Was Sie benötigen

Um eine Arbeitsumgebung zu schaffen, benötigen Sie Folgendes.

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

- "Sie sollten darauf vorbereitet sein, den Konnektor jederzeit in Betrieb zu nehmen".

- Ein Verständnis der zu verwendenden Konfiguration.

  Sie sollten eine Konfiguration auswählen und Azure Netzwerkinformationen von Ihrem Administrator erhalten haben. Weitere Informationen finden Sie unter "Planung Ihrer Cloud Volumes ONTAP Konfiguration".

- Kenntnisse über die erforderlichen Voraussetzungen zur Einrichtung der Lizenzierung für Cloud Volumes ONTAP.

  "Erfahren Sie, wie Sie eine Lizenzierung einrichten".

Über diese Aufgabe

Wenn BlueXP in Azure ein Cloud Volumes ONTAP-System erstellt, werden mehrere Azure-Objekte erstellt, z. B. eine Ressourcengruppe, Netzwerkschnittstellen und Speicherkonten. Sie können eine Zusammenfassung der Ressourcen am Ende des Assistenten überprüfen.

Risiko von Datenverlusten

Als Best Practice empfiehlt es sich, für jedes Cloud Volumes ONTAP System eine neue, dedizierte Ressourcengruppe zu verwenden.

Aufgrund des Risikos eines Datenverlusts wird die Bereitstellung von Cloud Volumes ONTAP in einer vorhandenen, gemeinsam genutzten Ressourcengruppe nicht empfohlen. Während BlueXP Cloud Volumes ONTAP-Ressourcen im Falle eines Ausfalls oder Löschvorgangs aus einer gemeinsam genutzten Ressourcengruppe entfernen kann, kann ein Azure Benutzer aus Versehen Cloud Volumes ONTAP-Ressourcen aus einer gemeinsam genutzten Ressourcengruppe löschen.

Starten eines Cloud Volumes ONTAP Systems mit einem Node in Azure

Wenn Sie ein Cloud Volumes ONTAP-System mit einem Node in Azure starten möchten, müssen Sie in BlueXP eine Arbeitsumgebung mit einem einzelnen Knoten erstellen.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Bildschirmseite auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.
3. **Wählen Sie einen Standort**: Wählen Sie **Microsoft Azure** und **Cloud Volumes ONTAP Single Node**.
4. Wenn Sie dazu aufgefordert werden, "Einen Konnektor erstellen".
5. **Details und Anmeldeinformationen**: Optional können Sie die Azure-Anmeldedaten und das Abonnement ändern, einen Clusternamen angeben, bei Bedarf Tags hinzufügen und dann Anmeldedaten angeben.

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

Feld	Beschreibung
Name der Arbeitsumgebung	BlueXP 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
Tags Für Ressourcengruppen	Tags sind Metadaten für Ihre Azure Ressourcen. Wenn Sie in dieses Feld Tags eingeben, fügt BlueXP diese der Ressourcengruppe hinzu, 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 Anmeldeinformationen 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. Behalten Sie den Standardbenutzernamen „*admin*“ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
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:

Abonnieren Sie BlueXP über den Azure Marketplace

6. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie nicht mit Cloud Volumes ONTAP verwenden möchten.
   - "Weitere Informationen zur BlueXP Klassifizierung"
   - "Erfahren Sie mehr über Backup und Recovery von BlueXP"

   Wenn SIE WORM und Daten-Tiering nutzen möchten, müssen Sie BlueXP Backup und Recovery deaktivieren und eine Cloud Volumes ONTAP Arbeitsumgebung mit Version 9.8 oder höher implementieren.

7. **Standort**: Wählen Sie eine Region, eine Verfügbarkeitszone, vnet und ein Subnetz aus, und aktivieren Sie dann das Kontrollkästchen, um die Netzwerkverbindung zwischen dem Connector und dem Zielspeicherort zu bestätigen.

   Bei Single-Node-Systemen können Sie die Verfügbarkeitszone auswählen, in der Sie Cloud Volumes ONTAP implementieren möchten. Wenn Sie keine AZ auswählen, wählt BlueXP eine für Sie aus.

8. **Konnektivität**: Wählen Sie eine neue oder bestehende Ressourcengruppe und wählen Sie dann aus, ob Sie die vordefinierte Sicherheitsgruppe verwenden oder Ihre eigene verwenden möchten.

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

Feld	Beschreibung
Ressourcengruppe	Erstellen Sie eine neue Ressourcengruppe für Cloud Volumes ONTAP, oder verwenden Sie eine vorhandene Ressourcengruppe. 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 bereitzustellen, jedoch wird dies aufgrund des Risikos eines Datenverlusts nicht empfohlen. Weitere Informationen finden Sie in der oben stehenden Warnung. Wenn im Azure Konto, das Sie verwenden, der angezeigt wird "Erforderliche Berechtigungen", BlueXP entfernt Cloud Volumes ONTAP-Ressourcen aus einer Ressourcengruppe, bei Ausfall oder Löschung der Bereitstellung.
Sicherheitsgruppe wurde generiert	Wenn Sie BlueXP die Sicherheitsgruppe für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Selected vnet Only** wählen, ist die Quelle für eingehenden Datenverkehr der Subnetz-Bereich des ausgewählten vnet und der Subnetz-Bereich des vnet, in dem sich der Connector befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VNets** wählen, ist die Quelle für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Verwenden Sie vorhandene	Wenn Sie eine vorhandene Sicherheitsgruppe auswählen, muss diese die Cloud Volumes ONTAP-Anforderungen erfüllen. "Zeigen Sie die Standardsicherheitsgruppe an".

9. **Charging Methods and NSS Account**: Geben Sie an, welche Ladungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site Konto an.
   - "Informieren Sie sich über Lizenzoptionen für Cloud Volumes ONTAP".
   - "Erfahren Sie, wie Sie eine Lizenzierung einrichten".
10. **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.
11. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP-Version nach Bedarf und wählen Sie einen virtuellen Maschinentyp.

    Wenn für die ausgewählte Version eine neuere Version von Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert BlueXP das System auf diese Version, wenn die Arbeitsumgebung erstellt wird. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.10.1 und 9.10.1 P4 auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.6 bis 9.7.
12. **Abonnieren Sie den Azure Marketplace**: Sie sehen diese Seite, ob BlueXP programmatische Bereitstellungen von Cloud Volumes ONTAP nicht aktivieren könnte. Befolgen Sie die auf dem Bildschirm aufgeführten Schritte. Siehe "Programmatische Bereitstellung von Marketplace-Produkten" Finden Sie

weitere Informationen.

13. **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 ist für alle Festplatten im ursprünglichen Aggregat und für alle zusätzlichen Aggregate bestimmt, die BlueXP erzeugt, 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".

14. **Schreibgeschwindigkeit und WURM**:

    a. Wählen Sie bei Bedarf * Normal* oder **High** Schreibgeschwindigkeit.

       "Erfahren Sie mehr über Schreibgeschwindigkeit".

    b. Aktivieren Sie auf Wunsch den WORM-Storage (Write Once, Read Many).

       Diese Option ist nur für bestimmte VM-Typen verfügbar. Informationen darüber, welche VM-Typen unterstützt werden, finden Sie unter "Unterstützte Konfigurationen per Lizenz für HA-Paare".

       WORM kann nicht aktiviert werden, wenn Daten-Tiering für Cloud Volumes ONTAP-Versionen 9.7 und darunter aktiviert wurde. Ein Wechsel- oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach Aktivierung VON WORM und Tiering gesperrt.

    "Erfahren Sie mehr über WORM Storage".

    a. Wenn Sie DEN WORM-Speicher aktivieren, wählen Sie den Aufbewahrungszeitraum aus.

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

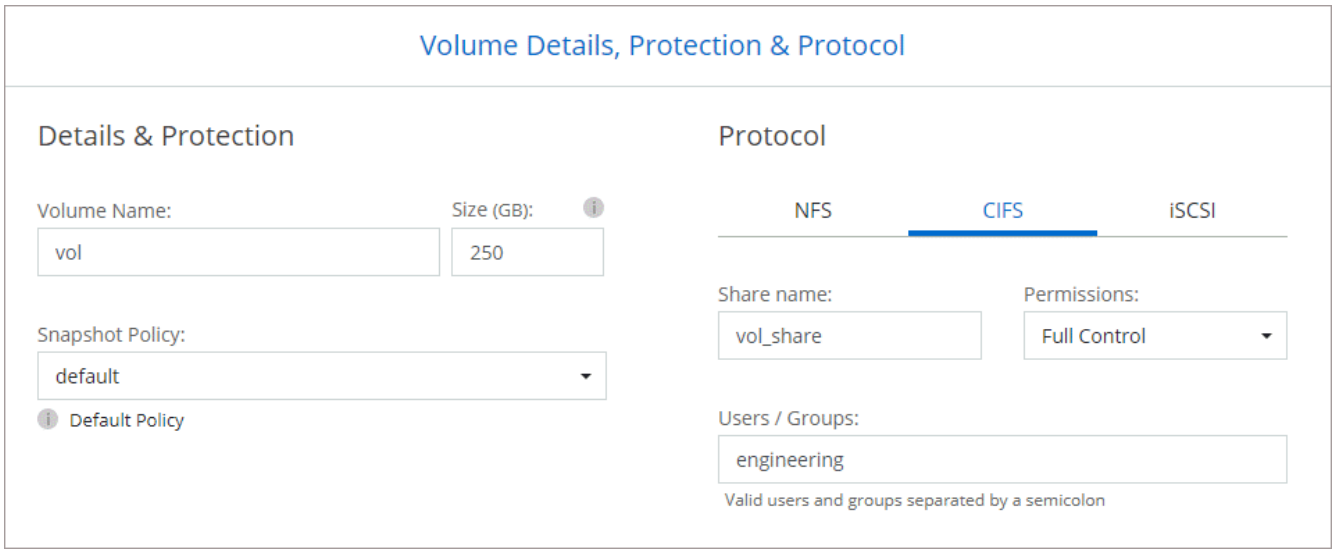
    "Hier erhalten Sie Informationen zu den unterstützten Client-Protokollen und -Versionen".

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

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren, wodurch Sie ein Volume erstellen können, das größer ist als der derzeit verfügbare physische Storage.

Feld	Beschreibung
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt BlueXP einen Wert ein, der Zugriff auf alle Instanzen im Subnetz bietet.
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 BlueXP 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:



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

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. Um Azure AD-Domänendienste als AD-Server für Cloud Volumes ONTAP zu konfigurieren, müssen Sie in diesem Feld **OU=AADDC-Computer** oder **OU=AADDC-Benutzer** eingeben.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure-Dokumentation: Erstellen Sie eine Organisationseinheit (Organisationseinheit, OU) in einer von Azure AD-Domänendiensten gemanagten Domäne"^]
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden** aus, um einen NTP-Server mit Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Siehe "BlueXP Automation Dokumentation" Entsprechende Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Er ist nicht konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

17. **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".

18. **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 den Azure-Ressourcen zu erhalten, die BlueXP kaufen wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie Auf **Go**.

Ergebnis

BlueXP 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.

Starten eines Cloud Volumes ONTAP HA-Paars in Azure

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

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Bildschirmseite auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.
3. Wenn Sie dazu aufgefordert werden, "Einen Konnektor erstellen".
4. **Details und Anmeldeinformationen**: Optional können Sie die Azure-Anmeldedaten und das Abonnement ändern, einen Clusternamen angeben, bei Bedarf Tags hinzufügen und dann Anmeldedaten angeben.

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

Feld	Beschreibung
Name der Arbeitsumgebung	BlueXP 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.
Tags Für Ressourcengruppen	Tags sind Metadaten für Ihre Azure Ressourcen. Wenn Sie in dieses Feld Tags eingeben, fügt BlueXP diese der Ressourcengruppe hinzu, 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 Anmeldeinformationen 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. Behalten Sie den Standardbenutzernamen „*admin*“ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.

Feld	Beschreibung
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:

Abonnieren Sie BlueXP über den Azure Marketplace

5. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie nicht mit Cloud Volumes ONTAP verwenden möchten.
   - "Weitere Informationen zur BlueXP Klassifizierung"
   - "Erfahren Sie mehr über Backup und Recovery von BlueXP"

   Wenn SIE WORM und Daten-Tiering nutzen möchten, müssen Sie BlueXP Backup und Recovery deaktivieren und eine Cloud Volumes ONTAP Arbeitsumgebung mit Version 9.8 oder höher implementieren.

6. * HA-Bereitstellungsmodelle*:
   a. Wählen Sie **Single Availability Zone** oder **Multiple Availability Zone** aus.
   b. **Lage und Konnektivität** (Single AZ) und **Region und Konnektivität** (mehrere AZS)
      - Wählen Sie für eine einzelne AZ eine Region, eine Vnet und ein Subnetz aus.
      - Wählen Sie für mehrere AZS eine Region, vnet, Subnetz, Zone für Node 1 und Zone für Node 2 aus.
   c. Aktivieren Sie das Kontrollkästchen * Ich habe die Netzwerkverbindung verifiziert…*.
7. **Konnektivität**: Wählen Sie eine neue oder bestehende Ressourcengruppe und wählen Sie dann aus, ob Sie die vordefinierte Sicherheitsgruppe verwenden oder Ihre eigene verwenden möchten.

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

Feld	Beschreibung
Ressourcengruppe	Erstellen Sie eine neue Ressourcengruppe für Cloud Volumes ONTAP, oder verwenden Sie eine vorhandene Ressourcengruppe. 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 bereitzustellen, jedoch wird dies aufgrund des Risikos eines Datenverlusts nicht empfohlen. Weitere Informationen finden Sie in der oben stehenden Warnung. Sie müssen für jedes Cloud Volumes ONTAP HA-Paar, das Sie in Azure implementieren, eine dedizierte Ressourcengruppe verwenden. Es wird nur ein HA-Paar in einer Ressourcengruppe unterstützt. Bei BlueXP treten Verbindungsprobleme auf, wenn Sie versuchen, ein zweites Cloud Volumes ONTAP HA-Paar in einer Azure Ressourcengruppe bereitzustellen. Wenn im Azure Konto, das Sie verwenden, der angezeigt wird "Erforderliche Berechtigungen", BlueXP entfernt Cloud Volumes ONTAP-Ressourcen aus einer Ressourcengruppe, bei Ausfall oder Löschung der Bereitstellung.
Sicherheitsgruppe wurde generiert	Wenn Sie BlueXP die Sicherheitsgruppe für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Selected vnet Only** wählen, ist die Quelle für eingehenden Datenverkehr der Subnetz-Bereich des ausgewählten vnet und der Subnetz-Bereich des vnet, in dem sich der Connector befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VNets** wählen, ist die Quelle für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Verwenden Sie vorhandene	Wenn Sie eine vorhandene Sicherheitsgruppe auswählen, muss diese die Cloud Volumes ONTAP-Anforderungen erfüllen. "Zeigen Sie die Standardsicherheitsgruppe an".

8. **Charging Methods and NSS Account**: Geben Sie an, welche Ladungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site Konto an.
   - "Informieren Sie sich über Lizenzoptionen für Cloud Volumes ONTAP".
   - "Erfahren Sie, wie Sie eine Lizenzierung einrichten".
9. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete aus, um ein Cloud Volumes ONTAP-System schnell bereitzustellen, oder klicken Sie auf **Konfiguration ändern**.

   Wenn Sie eines der Pakete auswählen, müssen Sie nur ein Volume angeben und dann die Konfiguration prüfen und genehmigen.
10. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP-Version nach Bedarf und wählen Sie einen virtuellen Maschinentyp.

Wenn für die ausgewählte Version eine neuere Version von Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert BlueXP das System auf diese Version, wenn die Arbeitsumgebung erstellt wird. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.10.1 und 9.10.1 P4 auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.6 bis 9.7.

11. **Vom Azure Marketplace abonnieren**: Folgen Sie den Schritten, wenn BlueXP programmatische Bereitstellungen von Cloud Volumes ONTAP nicht aktivieren kann.
12. **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:

    - Die Festplattengröße ist für alle Festplatten im ursprünglichen Aggregat und für alle zusätzlichen Aggregate bestimmt, die BlueXP erzeugt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuweisungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

      Hilfe zur Auswahl einer Festplattengröße finden Sie unter "Größe 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".

13. **Schreibgeschwindigkeit und WURM**:

    a. Wählen Sie bei Bedarf * Normal* oder **High** Schreibgeschwindigkeit.

       "Erfahren Sie mehr über Schreibgeschwindigkeit".

    b. Aktivieren Sie auf Wunsch den WORM-Storage (Write Once, Read Many).

       Diese Option ist nur für bestimmte VM-Typen verfügbar. Informationen darüber, welche VM-Typen unterstützt werden, finden Sie unter "Unterstützte Konfigurationen per Lizenz für HA-Paare".

       WORM kann nicht aktiviert werden, wenn Daten-Tiering für Cloud Volumes ONTAP-Versionen 9.7 und darunter aktiviert wurde. Ein Wechsel- oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach Aktivierung VON WORM und Tiering gesperrt.

    "Erfahren Sie mehr über WORM Storage".

    a. Wenn Sie DEN WORM-Speicher aktivieren, wählen Sie den Aufbewahrungszeitraum aus.

14. **Sichere Kommunikation zu Storage & WORM**: Wählen Sie, ob eine HTTPS-Verbindung zu Azure-Speicherkonten aktiviert und, falls gewünscht, den WORM-Speicher (Write Once, Read Many) aktiviert werden soll.

    Die HTTPS-Verbindung besteht aus einem Cloud Volumes ONTAP 9.7 HA-Paar zu Blob-Storage-Konten auf der Azure-Seite. 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".

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

"Erfahren Sie mehr über WORM Storage".

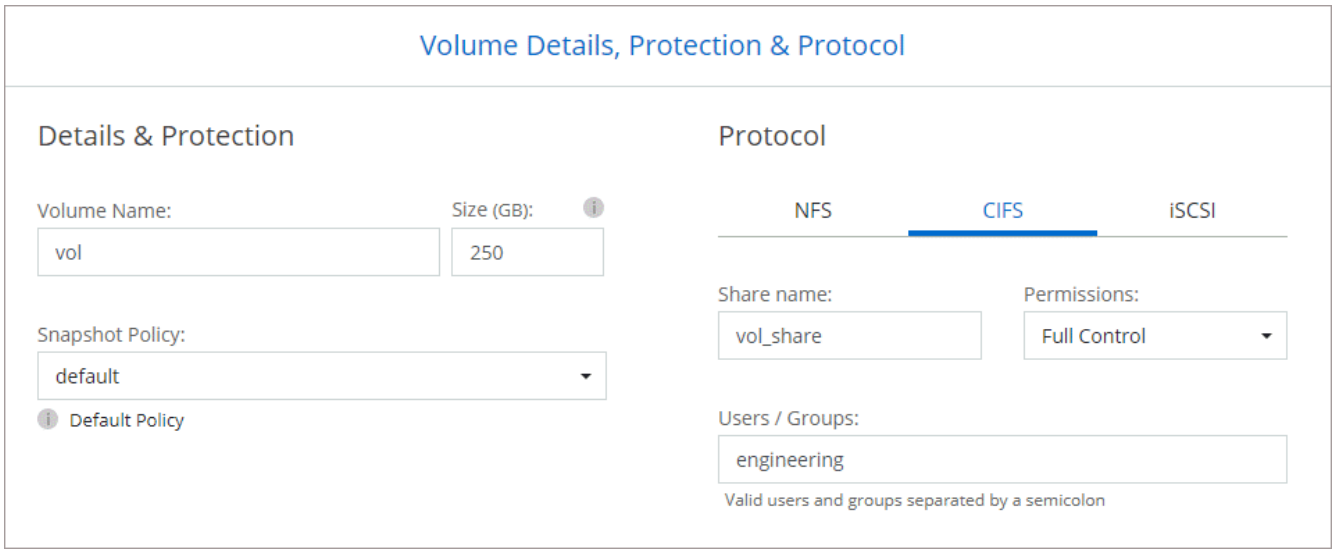
15. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

    "Hier erhalten Sie Informationen zu den unterstützten Client-Protokollen und -Versionen".

    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 BlueXP einen Wert ein, der Zugriff auf alle Instanzen im Subnetz bietet.
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 BlueXP 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:



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

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. Um Azure AD-Domänendienste als AD-Server für Cloud Volumes ONTAP zu konfigurieren, müssen Sie in diesem Feld **OU=AADDC-Computer** oder **OU=AADDC-Benutzer** eingeben.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure-Dokumentation: Erstellen Sie eine Organisationseinheit (Organisationseinheit, OU) in einer von Azure AD-Domänendiensten gemanagten Domäne"^]
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden** aus, um einen NTP-Server mit Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Siehe "BlueXP Automation Dokumentation" Entsprechende Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Er ist nicht konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

17. **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 "Wählen Sie ein Volume-Auslastungsprofil aus" Und "Data Tiering - Übersicht".

18. **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 den Azure-Ressourcen zu erhalten, die BlueXP kaufen wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie Auf **Go**.

Ergebnis

BlueXP 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.

Image-Verifizierung Für Azure Plattform

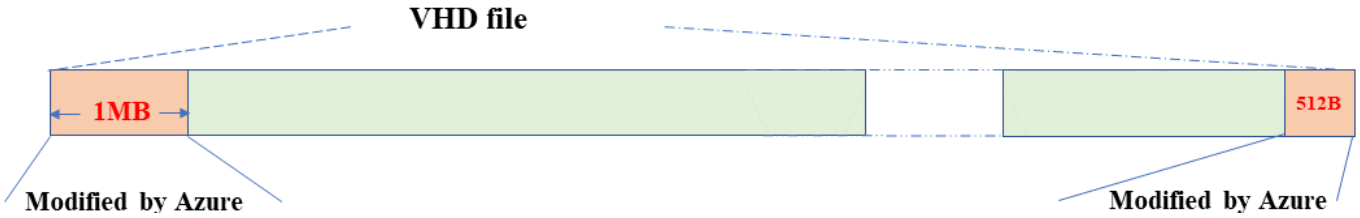
Azure Image Verifizierung – Übersicht

Die Azure-Image-Verifizierung erfüllt erweiterte Sicherheitsanforderungen von NetApp. Die Verifizierung einer Bilddatei ist zwar ein einfacher Vorgang, doch aufgrund eines Wechsels des Azure Marketplace erfordert die Überprüfung der Bildsignaturen bei Azure aufgrund einer speziellen Übergabe an die bekannte Azure VHD Bilddatei.

Die Azure-Image-Verifizierung wird von der Cloud Volumes ONTAP Softwareversion 9.15.0 oder höher unterstützt.

Änderung veröffentlichter VHD-Dateien in Azure

Die führende 1MB (1048576 Byte) und die letzte 512 Byte VHD-Datei wird von Azure geändert. NetApp Image Signing überspringt die ersten 1 MB und die letzten 512 Byte und signiert den verbleibenden VHD-Bildbereich.



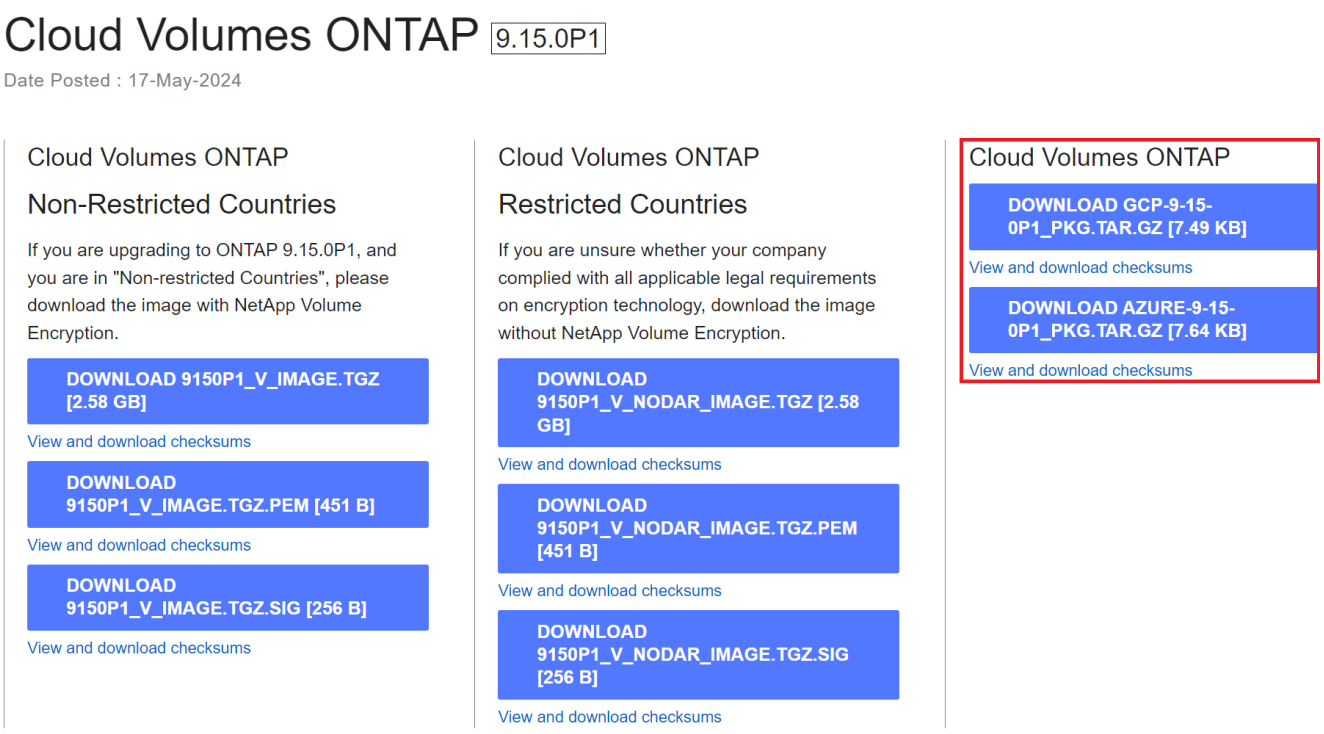
Das obige Diagramm zeigt als Beispiel eine VHD-Datei mit einer Größe von 10 GB. Aber der NetApp-signierte Teil ist grün mit einer Größe von 10GB - 1MB - 512B markiert.

Azure Image Digest Datei herunterladen

Die Azure Image Digest-Datei kann von der heruntergeladen werden "NetApp Support Website". Der Download wurde im Format tar.gz heruntergeladen und enthält Dateien zur Überprüfung der Bildsignatur.

Schritte

1. Wechseln Sie zum "Cloud Volumes ONTAP Produktseite auf der NetApp Support-Website" Und laden Sie die gewünschte Softwareversion im Abschnitt Downloads herunter.
2. Klicken Sie auf der Cloud Volumes ONTAP-Download-Seite auf den **Download-Button** für die Azure-Image-Digest-Datei, um den TAR herunterzuladen. GZ-Datei.



3. Für Linux und MacOS müssen Sie Folgendes ausführen, um md5sum und sha256sum für die heruntergeladene Azure Image Digest-Datei zu erhalten.
   a. Geben Sie für md5sum den ein `md5sum` Befehl.
   b. Geben Sie für sha256sum den ein `sha256sum` Befehl.
4. Überprüfen Sie die `md5sum` Und `sha256sum` Die Werte stimmen mit dem Download der Azure Image Digest Datei überein.

5. Führen Sie unter Linux und Mac OS die aus `tar -xzf` Befehl, um die Datei tar.gz zu extrahieren.

   Das extrahierte TAR. Die GZ-Datei enthält die Digest-Datei(.SIG), die Zertifikatdatei mit öffentlichem Schlüssel (.pem) und die Zertifikatdatei mit Kettenzertifikat (.pem).

   Ergebnis der untar tar.gz-Datei auflisten

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

Bildexport aus Azure Marketplace

Nachdem das VHD-Image in der Azure Cloud veröffentlicht wurde, wird das Image nicht mehr von NetApp gemanagt. Stattdessen wird das veröffentlichte Bild auf dem Azure Marketplace platziert. Die Änderung der führenden 1 MB und der letzten 512 B der VHD durch Azure tritt auf, wenn das Image bereitgestellt und auf dem Azure Marketplace veröffentlicht wird. Um die Signatur der VHD-Datei zu überprüfen, muss das von Azure geänderte VHD-Image zuerst aus dem Azure Marketplace exportiert werden.

Was Sie benötigen

Sie müssen die erforderlichen Programme auf Ihrem System installieren.

- Azure CLI ist installiert oder Azure Cloud Shell ist über das Azure-Portal jederzeit verfügbar.

  Weitere Informationen zum Installieren der Azure-CLI finden Sie unter "Azure-Dokumentation: Installieren von Azure CLI".

Schritte

1. Ordnen Sie die ONTAP-Version mithilfe des Inhalts der Datei „Version_readme“ der Azure Marketplace-Bildversion zu.

   Für jede Versionszuordnung, die in der Datei Version_readme aufgeführt ist, wird die ONTAP-Version durch „buildname“ und die Azure Marketplace Image-Version durch „Version“ dargestellt.

   In der folgenden Datei „Version_readme“ ist beispielsweise die ONTAP-Version „915.0P1“ der Azure Marketplace-Image-Version „9150.01000024.05090105“ zugeordnet. Diese Azure Marketplace-Image-Version wird später verwendet, um die Image-URN festzulegen.

```
[
    {
        "buildname": "9.15.0P1",
        "publisher": "netapp",
        "version": "9150.01000024.05090105"
    }
]
```

2. Geben Sie den Namen der Region an, in der Sie VMs erstellen möchten.

   Dieser Name der Region wird als Wert für die Variable „locName“ verwendet, wenn die URN des Marktplatzbildes festgelegt wird.

   a. Um eine Liste der verfügbaren Regionen zu erhalten, geben Sie den ein `az account list-locations -o table` Befehl.

      In der folgenden Tabelle wird der Name der Region als Feld „Name“ bezeichnet.

```
$ az account list-locations -o table
DisplayName               Name                 RegionalDisplayName
------------------------  -------------------
-------------------------------------
East US                   eastus               (US) East US
East US 2                 eastus2              (US) East US 2
South Central US          southcentralus       (US) South Central US
...
```

3. Überprüfen Sie den SKU-Namen für den entsprechenden VM-Bereitstellungstyp aus der folgenden Tabelle.

   Der SKU-Name wird als Wert für die Variable „skuName“ verwendet, wenn die URN des Marketplace-Images festgelegt wird.

   Beispielsweise sollten für Single-Node-Implementierungen der SKU-Name „ontap_Cloud_byol“ verwendet werden.

VM-Bereitstellungstyp	SKU-Name
Single Node	ontap_Cloud_byol
Hochverfügbarkeit	ontap_Cloud_byol_ha

4. Sobald die ONTAP Version und das Azure Marketplace Image zugeordnet sind, exportieren Sie die VHD-Datei aus dem Azure Marketplace über die Azure Cloud Shell oder die Azure CLI.

Exportieren Sie die VHD-Datei über Azure Cloud Shell im Azure-Portal

1. Exportieren Sie das Marketplace-Image von Azure Cloud Shell in ein vhd (image2, z. B. 9150.01000024.05090105.vhd), und laden Sie es auf Ihren lokalen Rechner (z. B. einen Linux-Rechner

oder einen Windows-PC) herunter.

Klicken Sie zum Anzeigen auf

```
#Azure Cloud Shell on Azure portal to get VHD image from Azure
Marketplace
a) Set the URN and other parameters of the marketplace image. URN is
with format "<publisher>:<offer>:<sku>:<version>". Optionally, a
user can list NetApp marketplace images to confirm the proper image
version.
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName
$pubName -Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...

b) Create a new managed disk from the Marketplace image with the
matching image version
PS /home/user1> $diskName = “9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = “fnf1”
PS /home/user1> az disk create -g $diskRG -n $diskName --image
-reference $urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds
3600 --access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-
Json)[0].accessSas

c) Export a VHD from the managed disk to Azure Storage
Create a container with proper access level. As an example, a
container named 'vm-images' with 'Container' access level is used
here.
Get storage account access key, on Azure portal, 'Storage
Accounts'/'examplesaname'/'Access Key'/'key1'/'key'/'show'/<copy>.
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
```

```
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri
$diskAccessSAS -DestContainer $containerName -DestContext
$destContext -DestBlob $destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container
$containerName –Context $destContext -Blob $destBlobName

d) Download the generated image to your server, e.g., a Linux
machine.
Use "wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>".
The URL is organized in a formatted way. For automation tasks, the
following example could be used to derive the URL string. Otherwise,
Azure CLI 'az' command could be issued to get the URL, which is not
covered in this guide. URL Example:
https://examplesaname.blob.core.windows.net/vm-
images/9150.01000024.05090105.vhd

e) Clean up the managed disk
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG
-DiskName $diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Exportieren Sie die VHD-Datei über die Azure CLI von einem lokalen Linux-Computer

1. Exportieren Sie das Marketplace-Image über die Azure CLI von einem lokalen Linux-Rechner in ein VHD.

Klicken Sie zum Anzeigen auf

```
#Azure CLI on local Linux machine to get VHD image from Azure
Marketplace
a) Login Azure CLI and list marketplace images
% az login --use-device-code
To sign in, use a web browser to open the page
https://microsoft.com/devicelogin and enter the code XXXXXXXXX to
authenticate.

% az vm image list --all --publisher netapp --offer netapp-ontap-
cloud --sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...

b) Create a new managed disk from the Marketplace image with the
matching image version
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level
Read --name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxx"
}

% export diskAccessSAS="https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxx"
#To automate the process, the SAS needs to be extracted from the
standard output. This is not included in this guide.
```

```
c) export vhd from managed disk
Create a container with proper access level. As an example, a
container named 'vm-images' with 'Container' access level is used
here.
Get storage account access key, on Azure portal, 'Storage
Accounts'/'examplesaname'/'Access Key'/'key1'/'key'/'show'/<copy>.
There should be az command that can achieve the same, but this is
not included in this guide.
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS
--destination-container $containerName --account-name
$storageAccountName --account-key $storageAccountKey --destination
-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}

#to check the status of the blob copying
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.blob.core.windows.net/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
```

```
    },
....

d) Download the generated image to your server, e.g., a Linux
machine.
Use "wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>".
The URL is organized in a formatted way. For automation tasks, the
following example could be used to derive the URL string. Otherwise,
Azure CLI 'az' command could be issued to get the URL, which is not
covered in this guide. URL Example:
https://examplesaname.blob.core.windows.net/vm-
images/9150.01000024.05090105.vhd

e) Clean up the managed disk
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

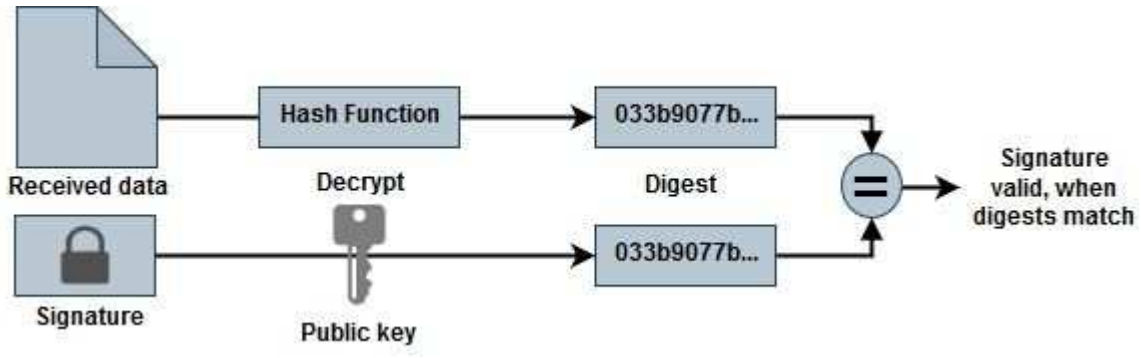
Überprüfung der Dateisignatur

Überprüfung der Dateisignatur

Bei der Azure-Image-Verifizierung wird mithilfe der Hash-Funktion ein Digest aus der VHD-Datei mit den führenden 1 MB und dem endenden 512B-Striping generiert. Um die Signaturverfahren anzupassen, wird SHA256 zum Hash verwendet. Sie müssen die führenden 1MB und die letzten 512B aus der VHD-Datei entfernen und dann den verbleibenden Teil der VHD-Datei überprüfen.

Zusammenfassung des Dateisignaturüberprüfungs-Workflows

Im Folgenden finden Sie eine Übersicht über den Prozess zur Überprüfung der Dateisignatur.



- Laden Sie die Datei Azure Image Digest von der herunter "NetApp Support Website" Und extrahieren Sie die Digest-Datei(.SIG), die Zertifikatdatei des öffentlichen Schlüssels(.pem) und die Zertifikatdatei der Kette(.pem).

  Siehe "Azure Image Digest Datei herunterladen" Finden Sie weitere Informationen.

- Überprüfen Sie die Vertrauenskette.
- Extrahieren Sie den öffentlichen Schlüssel(.Pub) aus dem öffentlichen Schlüsselzertifikat(.pem).
- Der extrahierte öffentliche Schlüssel wird verwendet, um die Digest-Datei zu entschlüsseln. Das Ergebnis wird dann mit einem neuen unverschlüsselten Digest der aus der Image-Datei erstellten temporären Datei mit führenden 1MB und enden 512 Bytes entfernt verglichen.

  Dieser Schritt wird durch den folgenden Befehl openssl erreicht.

  - Die allgemeine CLI-Anweisung wird wie folgt angezeigt:

    ```
    openssl dgst -verify <public_key> -keyform <form> <hash_function>
    -signature <digest_file> -binary <temporary_file>
    ```

  - OpenSSL CLI-Tool gibt eine "Verified OK"-Meldung, wenn beide Dateien übereinstimmen und "Verification Failure", wenn sie nicht übereinstimmen.

Überprüfung der Dateisignatur unter Linux

Sie können eine exportierte VHD-Dateisignatur für Linux überprüfen, indem Sie die folgenden Schritte ausführen.

Schritte

1. Laden Sie die Datei Azure Image Digest von der herunter "NetApp Support Website" Und extrahieren Sie die Digest-Datei(.SIG), die Zertifikatdatei des öffentlichen Schlüssels(.pem) und die Zertifikatdatei der Kette(.pem).

   Siehe "Azure Image Digest Datei herunterladen" Finden Sie weitere Informationen.

2. Überprüfen Sie die Vertrauenskette.

   ```
   % openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
   Certificate-9.15.0P1_azure.pem
   Certificate-9.15.0P1_azure.pem: OK
   ```

3. Entfernen Sie die führenden 1 MB (1048576 Byte) und die letzten 512 Byte VHD-Datei.

   Wenn 'Tail' verwendet wird, gibt die Option '-c +K' Bytes ab den KTH Bytes der angegebenen Datei aus. Daher wird 1048577 an 'tail -c' übergeben.

   ```
   % tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
   % head -c -512 ./sign.tmp.tail > sign.tmp
   % rm ./sign.tmp.tail
   ```

4. Verwenden Sie openssl, um den öffentlichen Schlüssel aus dem Zertifikat zu extrahieren und die gestreifte Datei (sign.tmp) mit der Signaturdatei und dem öffentlichen Schlüssel zu überprüfen.

   Wenn die Eingabedatei die Überprüfung bestanden hat, wird der Befehl angezeigt

„Verifizierung OK“. Andernfalls wird „Überprüfungsfehler“ angezeigt.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Den Arbeitsbereich bereinigen.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Überprüfung der Dateisignatur auf Mac OS

Sie können eine exportierte VHD-Dateisignatur für Mac OS überprüfen, indem Sie die folgenden Schritte ausführen.

Schritte

1. Laden Sie die Datei Azure Image Digest von der herunter "NetApp Support Website" Und extrahieren Sie die Digest-Datei(.SIG), die Zertifikatdatei des öffentlichen Schlüssels(.pem) und die Zertifikatdatei der Kette(.pem).

   Siehe "Azure Image Digest Datei herunterladen" Finden Sie weitere Informationen.

2. Überprüfen Sie die Vertrauenskette.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Entfernen Sie die führende 1 MB (1048576 Byte) und die letzte 512 Byte VHD-Datei.

   Wenn 'Tail' verwendet wird, gibt die Option '-c +K' Bytes beginnend mit den KTH Bytes aus Der angegebenen Datei. Daher wird 1048577 an 'tail -c' übergeben. Es dauert ca. 13m Damit der tail-Befehl unter Mac OS abgeschlossen wird.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Verwenden Sie openssl, um den öffentlichen Schlüssel aus dem Zertifikat zu extrahieren und den gestreiften Schlüssel zu überprüfen
Datei(sign.tmp) mit Signaturdatei und öffentlichem Schlüssel.

   Wenn die Eingabedatei die Überprüfung besteht, wird im Befehl „Überprüfung OK“ angezeigt. Andernfalls wird „Überprüfungsfehler“ angezeigt.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Den Arbeitsbereich bereinigen.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Weitere Informationen zur Azure-Image-Verifizierung

Weitere Informationen zur Azure-Image-Verifizierung finden Sie unter den folgenden Links. Die unten stehenden Links führen Sie zu Websites, die nicht von NetApp stammen.

Quellen

- "Page Fault Blog: Wie signieren und überprüfen Sie mit OpenSSL"
- "Erstellen Sie mit Azure Marketplace Image ein VM-Image für Ihre Azure Stack Edge Pro GPU im Microsoft Learn"
- "Exportieren/Kopieren einer verwalteten Festplatte in ein Storage-Konto mithilfe der Azure CLI in Microsoft Learn"
- "Azure Cloud Shell Quickstart – Bash Microsoft Learn"
- "So installieren Sie die Azure CLI von Microsoft Learn"
- "az Storage Blob copy – Microsoft Learn"

- "Anmelden mit Azure CLI – Anmeldung und Authentifizierung – Microsoft Learn"

Erste Schritte in Google Cloud

Schnellstart für Cloud Volumes ONTAP in Google Cloud

Erste Schritte in wenigen Schritten mit Cloud Volumes ONTAP für Google Cloud

1 Einen Konnektor erstellen

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

Wenn Sie Cloud Volumes ONTAP in einem Subnetz bereitstellen möchten, in dem kein Internetzugang verfügbar ist, müssen Sie den Connector manuell installieren und auf die BlueXP Benutzeroberfläche zugreifen, die auf diesem Connector ausgeführt wird. "Erfahren Sie, wie Sie den Connector manuell an einem Ort ohne Internetzugang installieren"

2 Planen Sie Ihre Konfiguration

BlueXP 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.

"Erfahren Sie mehr über die Planung der Konfiguration".

3 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. Wenn Sie Daten-Tiering aktivieren möchten, "Konfigurieren Sie das Cloud Volumes ONTAP-Subnetz für privaten Google-Zugriff".
3. Wenn Sie ein HA-Paar implementieren, stellen Sie sicher, dass Sie über vier VPCs verfügen, die jeweils über ein eigenes Subnetz verfügen.
4. Wenn Sie eine gemeinsame VPC verwenden, geben Sie die Rolle „*Compute Network User*“ für das Connector Service-Konto an.
5. Outbound-Internetzugang über die Ziel-VPC für NetApp AutoSupport aktivieren

   Dieser Schritt ist nicht erforderlich, wenn Sie Cloud Volumes ONTAP an einem Ort bereitstellen, an dem kein Internetzugang verfügbar ist.

"Erfahren Sie mehr über Netzwerkanforderungen".

4 Erstellen eines Servicekontos

Für Cloud Volumes ONTAP ist ein Google Cloud-Servicekonto aus zwei Gründen erforderlich. Die erste lautet, wenn Sie aktivieren "Daten-Tiering" Tiering selten genutzter Daten auf kostengünstigen Objekt-Storage in Google Cloud. Die zweite lautet, wenn Sie den aktivieren "BlueXP Backup und Recovery" Um Volumes auf

kostengünstigen Objekt-Storage zu sichern.

Sie können ein Service-Konto einrichten und für beide Zwecke verwenden. Das Servicekonto muss über die Rolle **Storage Admin** verfügen.

"Lesen Sie Schritt-für-Schritt-Anleitungen".

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 BlueXP

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

- "Erstellen eines Connectors von BlueXP"
- "Installieren der Connector-Software auf einem Linux-Host"
- "Was BlueXP mit Google Cloud-Berechtigungen macht"

Planen Sie Ihre Cloud Volumes ONTAP-Konfiguration in Google Cloud

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.

Wählen Sie eine Cloud Volumes ONTAP Lizenz

Für Cloud Volumes ONTAP sind verschiedene Lizenzierungsoptionen verfügbar. Jede Option ermöglicht Ihnen, ein Nutzungsmodell auszuwählen, das Ihren Anforderungen entspricht.

- "Informieren Sie sich über Lizenzoptionen für Cloud Volumes ONTAP"
- "Erfahren Sie, wie Sie eine Lizenzierung einrichten"

Wählen Sie eine unterstützte Region aus

Cloud Volumes ONTAP wird in den meisten Google Cloud Regionen unterstützt. "Hier finden Sie die vollständige Liste der unterstützten Regionen".

Wählen Sie einen unterstützten Maschinentyp aus

Je nach gewähltem Lizenztyp unterstützt Cloud Volumes ONTAP mehrere Maschinentypen.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in GCP"

Analysieren Sie Ihre Storage-Grenzen

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 in GCP ein"

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 einer der folgenden sein:

- *Zonal SSD persistente Festplatten*: Persistente SSD-Festplatten eignen sich am besten für Workloads, die eine hohe Anzahl an zufälligen IOPS erfordern.
- *Zonal Balance persistente Festplatten*: Diese SSDs sorgen durch niedrigere IOPS pro GB für ein ausgewogenes Verhältnis zwischen Performance und Kosten.
- *Zonal Standard persistente Festplatten* : Standard persistente Festplatten sind wirtschaftlich und können sequenzielle Lese-/Schreibvorgänge verarbeiten.

  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 BlueXP die Kapazität eines Systems für Sie verwalten lassen. Wenn Sie jedoch 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"

Anzeigen von Standard-Systemfestplatten

Neben dem Storage für Benutzerdaten erwirbt BlueXP auch Cloud-Storage für Cloud Volumes ONTAP Systemdaten (Boot-Daten, Root-Daten, Core-Daten und NVRAM). Für die Planung können Sie diese Details überprüfen, bevor Sie Cloud Volumes ONTAP implementieren.

- "Zeigen Sie die Standardfestplatten für Cloud Volumes ONTAP-Systemdaten in Google Cloud an".
- "Google Cloud Docs: Ressourcenkontingente"

  Google Cloud Compute Engine setzt Quoten für die Ressourcenauslastung durch. Damit sollten Sie vor der Implementierung von Cloud Volumes ONTAP sicherstellen, dass Sie das Limit nicht erreicht haben.

Für den Connector ist außerdem eine Systemfestplatte erforderlich. "Zeigen Sie Details zur Standardkonfiguration des Connectors an".

Sammeln von Netzwerkinformationen

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.

Netzwerkinformationen für ein Single-Node-System

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

Netzwerkinformationen für ein HA-Paar in mehreren Zonen

GCP-Informationen	Ihr Wert
Region	
Zone für Knoten 1	
Zone für Knoten 2	

GCP-Informationen	Ihr Wert
Zone für den Mediator	
VPC-0 und Subnetz	
VPC-1 und Subnetz	
VPC-2 und Subnetz	
VPC-3 und Subnetz	
Firewallrichtlinie (bei Nutzung eigener Richtlinien)	

Netzwerkinformationen für ein HA-Paar in einer einzelnen Zone

GCP-Informationen	Ihr Wert
Region	
Zone	
VPC-0 und Subnetz	
VPC-1 und Subnetz	
VPC-2 und Subnetz	
VPC-3 und Subnetz	
Firewallrichtlinie (bei Nutzung eigener Richtlinien)	

Wählen Sie eine Schreibgeschwindigkeit

Mit BlueXP können Sie eine Schreibgeschwindigkeitseinstellung für Cloud Volumes ONTAP auswählen, außer für HA-Paare in Google Cloud. 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. "Erfahren Sie mehr über Schreibgeschwindigkeit".

Wählen Sie ein Volume-Auslastungsprofil aus

ONTAP umfasst mehrere Storage-Effizienzfunktionen, mit denen Sie die benötigte Storage-Gesamtmenge reduzieren können. Wenn Sie ein Volume in BlueXP 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 Cloud Volumes ONTAP in Google Cloud

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

Wenn Sie ein HA-Paar bereitstellen möchten, sollten Sie dies tun "Funktionsweise von HA-Paaren in Google Cloud".

Anforderungen für Cloud Volumes ONTAP

In Google Cloud müssen die folgenden Anforderungen erfüllt sein:

Spezifische Anforderungen für Single Node-Systeme

Wenn Sie ein Single Node-System implementieren möchten, stellen Sie sicher, dass Ihr Netzwerk die folgenden Anforderungen erfüllt.

Eine VPC

Für ein System mit einem einzelnen Node ist eine Virtual Private Cloud (VPC) erforderlich.

Private IP-Adressen

BlueXP weist 3 oder 4 private IP-Adressen einem System mit einem Knoten in Google Cloud zu.

Sie können die Erstellung der Storage-VM (SVM)-Management-LIF überspringen, wenn Sie Cloud Volumes ONTAP mithilfe der API implementieren und folgende Flag angeben:

```
skipSvmManagementLif: true
```

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

Spezifischen Anforderungen für HA-Paare

Wenn Sie ein HA-Paar bereitstellen möchten, stellen Sie sicher, dass Ihr Netzwerk die folgenden Anforderungen erfüllt.

Eine oder mehrere Zonen

Durch Implementierung einer HA-Konfiguration für mehrere oder in einer einzelnen Zone werden die Hochverfügbarkeit der Daten gewährleistet. Bei der Erstellung des HA-Paars werden Sie von BlueXP aufgefordert, mehrere Zonen oder eine einzelne Zone auszuwählen.

- Mehrere Zonen (empfohlen)

  Durch die Implementierung einer HA-Konfiguration über drei Zonen hinweg wird eine kontinuierliche Datenverfügbarkeit sichergestellt, wenn ein Ausfall innerhalb einer Zone auftritt. Beachten Sie, dass die Schreibleistung im Vergleich zu einer einzelnen Zone etwas geringer ist, aber sie ist minimal.

- Einzelne Zone zu erreichen

  Wenn eine Cloud Volumes ONTAP HA-Konfiguration in einer einzelnen Zone implementiert wird, kommt eine Richtlinie zur Platzierung der Verteilung zum Einsatz. Diese Richtlinie sorgt dafür, dass eine HA-Konfiguration innerhalb der Zone vor einem Single Point of Failure geschützt ist, ohne dass zur Fehlereingrenzung separate Zonen erforderlich sind.

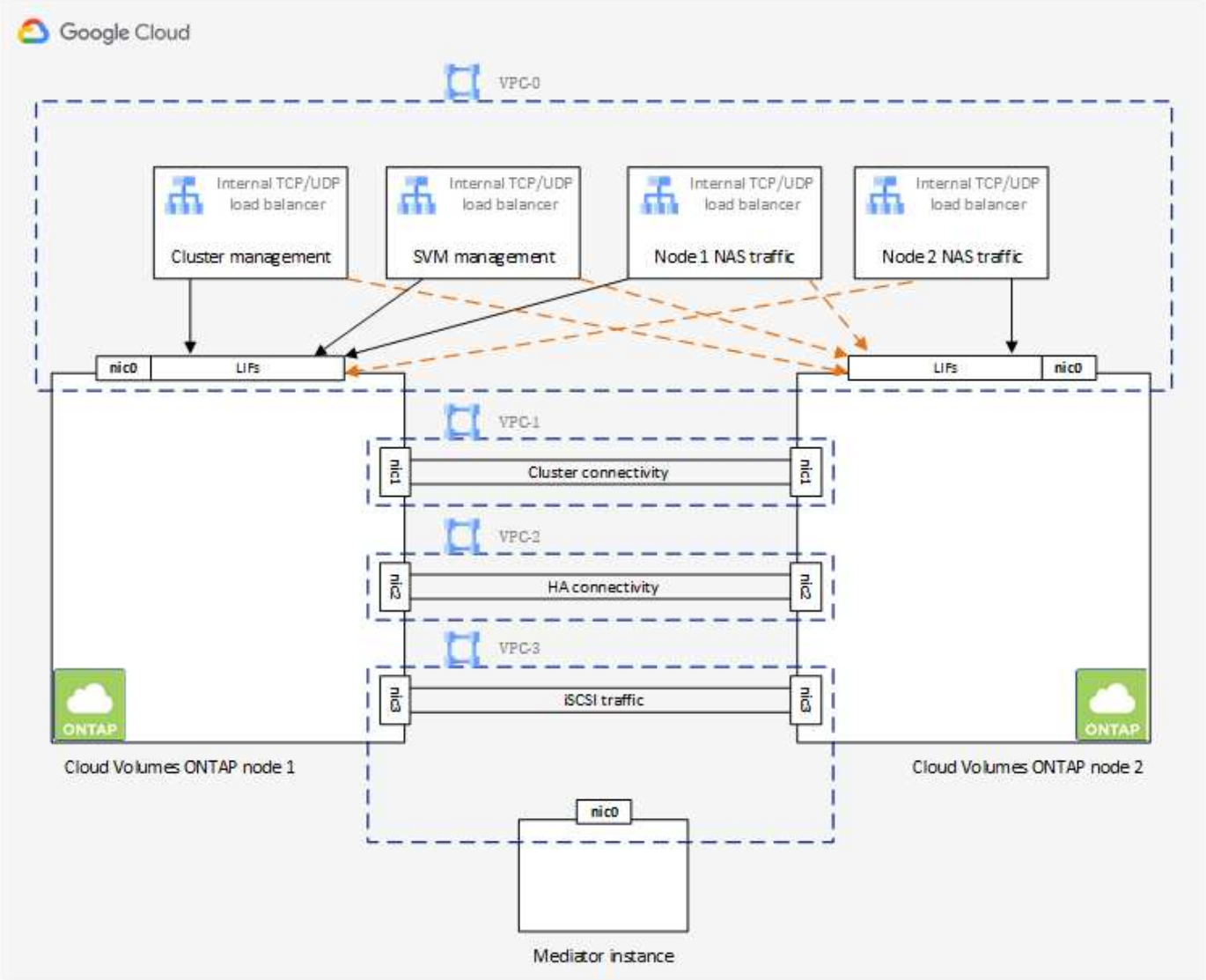
  Dieses Implementierungsmodell senkt Ihre Kosten, da zwischen den Zonen keine Kosten für den Datenausgang anfallen.

Vier Virtuelle Private Clouds

Für eine HA-Konfiguration sind vier Virtual Private Clouds (VPCs) erforderlich. Es sind vier VPCs erforderlich, da Google Cloud erfordert, dass sich jede Netzwerkschnittstelle in einem separaten VPC-Netzwerk befindet.

Bei der Erstellung des HA-Paars werden Sie von BlueXP aufgefordert, vier VPCs auszuwählen:

- VPC-0 für eingehende Verbindungen zu den Daten und Nodes
- VPC-1, VPC-2 und VPC-3 für die interne Kommunikation zwischen den Nodes und dem HA-Mediator



Subnetze

Für jede VPC ist ein privates Subnetz erforderlich.

Wenn Sie den Connector in VPC-0 platzieren, müssen Sie einen privaten Google-Zugriff im Subnetz aktivieren, um auf die APIs zuzugreifen und Daten-Tiering zu ermöglichen.

Die Subnetze in diesen VPCs müssen über unterschiedliche CIDR-Bereiche verfügen. Sie können keine überlappenden CIDR-Bereiche haben.

Private IP-Adressen

BlueXP weist Cloud Volumes ONTAP in Google Cloud automatisch die erforderliche Anzahl privater IP-Adressen zu. Sie müssen sicherstellen, dass in Ihrem Netzwerk genügend private Adressen verfügbar sind.

Die Anzahl der LIFs, die BlueXP für Cloud Volumes ONTAP zuweist, hängt davon ab, ob Sie ein Single Node-System oder ein HA-Paar implementieren. Ein LIF ist eine IP-Adresse, die einem physischen Port zugewiesen ist. Für Managementtools wie SnapCenter ist eine SVM-Management-LIF erforderlich.

- **Single Node** BlueXP weist 4 IP-Adressen einem System mit einem einzigen Knoten zu:
  - Node Management-LIF
  - Cluster-Management-LIF
  - ISCSI-Daten-LIF

    Ein iSCSI LIF bietet Client-Zugriff über das iSCSI-Protokoll und wird vom System für andere wichtige Netzwerk-Workflows verwendet. Diese LIFs sind erforderlich und sollten nicht gelöscht werden.

  - NAS-LIF

    Sie können die Erstellung der Storage-VM (SVM)-Management-LIF überspringen, wenn Sie Cloud Volumes ONTAP mithilfe der API implementieren und folgende Flag angeben:

```
skipSvmManagementLif: true
```

- **HA-Paar** BlueXP weist 12-13 IP-Adressen einem HA-Paar zu:
  - LIFs für das Management von 2 Nodes (e0a)
  - 1 LIF zum Cluster-Management (e0a)
  - 2 iSCSI LIFs (e0a)

    Ein iSCSI LIF bietet Client-Zugriff über das iSCSI-Protokoll und wird vom System für andere wichtige Netzwerk-Workflows verwendet. Diese LIFs sind erforderlich und sollten nicht gelöscht werden.

  - 1 oder 2 NAS LIFs (e0a)
  - 2 logische Cluster-Schnittstellen (e0b)
  - 2 HA Interconnect IP-Adressen (e0c)
  - 2 RSM iSCSI IP-Adressen (e0d)

Sie können die Erstellung der Storage-VM (SVM)-Management-LIF überspringen, wenn Sie Cloud Volumes ONTAP mithilfe der API implementieren und folgende Flag angeben:

```
skipSvmManagementLif: true
```

Interner Lastausgleich

BlueXP erstellt automatisch vier interne Google Cloud Load Balancer (TCP/UDP), die den eingehenden Datenverkehr zum Cloud Volumes ONTAP HA-Paar verwalten. Am Ende ist keine Konfiguration erforderlich Diese Anforderung ist lediglich, Sie über den Netzwerkverkehr zu informieren und Sicherheitsbedenken abzumildern.

Ein Load Balancer für das Cluster-Management eignet sich zum Management von Storage-VM (SVM), einer für NAS-Datenverkehr zu Node 1 und der letzte für NAS-Datenverkehr zu Node 2.

Die Einrichtung für die einzelnen Load Balancer lautet wie folgt:

- Eine gemeinsame private IP-Adresse
- Eine globale Zustandsprüfung

  Die von der Integritätsprüfung verwendeten Ports sind standardmäßig 63001, 63002 und 63003.

- Ein regionaler TCP-Backend-Service
- Ein regionaler UDP-Backend-Service
- Eine TCP-Weiterleitungsregel
- Eine UDP-Weiterleitungsregel
- Globaler Zugriff ist deaktiviert

  Obwohl der globale Zugriff standardmäßig deaktiviert ist, wird die Aktivierung der IT-Bereitstellung unterstützt. Wir haben sie deaktiviert, da der Datenverkehr zwischen Regionen erheblich höhere Latenzen aufweisen wird. Wir wollten sicherstellen, dass Sie keine negativen Erfahrungen durch zufällige, überregionale Montierungen hatten. Wenn Sie diese Option aktivieren, passt sie sich Ihren geschäftlichen Anforderungen an.

Gemeinsam genutzte VPCs

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

Bei einem Single-Node-System kann die VPC entweder eine gemeinsame VPC oder eine Standalone-VPC sein.

Bei einem HA-Paar sind vier VPCs erforderlich. Alle diese VPCs können entweder gemeinsam genutzt oder eigenständig genutzt werden. So könnte es sich beispielsweise um eine gemeinsam genutzte VPC-0, während VPC-1, VPC-2 und VPC-3 eigenständige VPCs sein könnten.

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".

"Erforderliche gemeinsame VPC-Berechtigungen für die Connector-Implementierung prüfen"

Paketspiegelung in VPCs

"Paketspiegelung" Muss im Google Cloud-Subnetz, in dem Sie Cloud Volumes ONTAP bereitstellen, deaktiviert sein. Cloud Volumes ONTAP kann nicht ordnungsgemäß ausgeführt werden, wenn die Paketspiegelung aktiviert ist.

Outbound-Internetzugang

Für Cloud Volumes ONTAP ist ein Outbound-Internetzugang für NetApp AutoSupport erforderlich, der den Zustand Ihres Systems proaktiv überwacht und Meldungen an den technischen Support von NetApp sendet.

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

Wenn keine ausgehende Internetverbindung zum Senden von AutoSupport-Nachrichten verfügbar ist, konfiguriert BlueXP Ihre Cloud Volumes ONTAP-Systeme automatisch so, dass der Connector als Proxy-Server verwendet wird. Die einzige Anforderung besteht darin, sicherzustellen, dass die Firewall des Connectors *Inbound*-Verbindungen über Port 3128 zulässt. Nach der Bereitstellung des Connectors müssen Sie diesen Port öffnen.

Wenn Sie strenge ausgehende Regeln für Cloud Volumes ONTAP festgelegt haben, müssen Sie auch sicherstellen, dass die Cloud Volumes ONTAP-Firewall *Outbound*-Verbindungen über Port 3128 zulässt.

Nachdem Sie bestätigt haben, dass der ausgehende Internetzugang verfügbar ist, können Sie AutoSupport testen, um sicherzustellen, dass er Nachrichten senden kann. Anweisungen finden Sie unter "ONTAP Dokumentation: Einrichten von AutoSupport".

Wenn Sie ein HA-Paar verwenden, benötigt der HA Mediator keinen Outbound-Internetzugang.

Wenn Sie von BlueXP darüber informiert werden, dass AutoSupport-Meldungen nicht gesendet werden können, "Fehler bei der AutoSupport Konfiguration beheben".

Firewall-Regeln

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

Beachten Sie, dass für eine HA-Konfiguration zwei Gruppen von Firewall-Regeln erforderlich sind:

- Ein Regelsatz für HA-Komponenten in VPC-0. Diese Regeln ermöglichen den Datenzugriff auf Cloud Volumes ONTAP. Weitere Informationen ..
- Weiterer Regelsatz für HA-Komponenten in VPC-1, VPC-2 und VPC-3. Diese Regeln sind für die Kommunikation zwischen den HA-Komponenten ein- und ausgehender Anruf offen. Weitere Informationen ..

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 (wenn Sie ein HA-Paar verwenden, ist dies das Subnetz in VPC-0). Anweisungen finden Sie unter "Google Cloud-Dokumentation: Privaten Google Access konfigurieren".

Weitere Schritte zur Einrichtung von Daten-Tiering in BlueXP 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 Google Cloud und ONTAP Systemen in anderen Netzwerken müssen Sie eine VPN-Verbindung zwischen der VPC und dem anderen Netzwerk herstellen, beispielsweise das Unternehmensnetzwerk.

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

Firewall-Regeln

BlueXP erstellt Google Cloud Firewall-Regeln, die die ein- und ausgehenden Regeln enthalten, die Cloud Volumes ONTAP für den erfolgreichen Betrieb benötigt. Sie können zu Testzwecken auf die Ports verweisen oder Ihre eigenen Firewall-Regeln verwenden.

Die Firewall-Regeln für Cloud Volumes ONTAP erfordern sowohl ein- als auch ausgehende Regeln. Bei der Implementierung einer HA-Konfiguration handelt es sich um die Firewall-Regeln für Cloud Volumes ONTAP in VPC-0.

Beachten Sie, dass für eine HA-Konfiguration zwei Gruppen von Firewall-Regeln erforderlich sind:

- Ein Regelsatz für HA-Komponenten in VPC-0. Diese Regeln ermöglichen den Datenzugriff auf Cloud Volumes ONTAP.
- Weiterer Regelsatz für HA-Komponenten in VPC-1, VPC-2 und VPC-3. Diese Regeln sind für die Kommunikation zwischen den HA-Komponenten ein- und ausgehender Anruf offen. Weitere Informationen ..

Sie suchen Informationen über den Connector? "Zeigen Sie Firewall-Regeln für den Connector an"

Regeln für eingehende Anrufe

Wenn Sie eine Arbeitsumgebung erstellen, können Sie den Quellfilter für die vordefinierte Firewall-Richtlinie während der Bereitstellung auswählen:

- **Nur gewählte VPC**: Der Quellfilter für eingehenden Datenverkehr ist der Subnetz-Bereich des VPC für das Cloud Volumes ONTAP-System und der Subnetz-Bereich des VPC, in dem sich der Connector befindet. Dies ist die empfohlene Option.
- **Alle VPCs**: Der Quellfilter für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.

Wenn Sie Ihre eigene Firewallrichtlinie verwenden, stellen Sie sicher, dass Sie alle Netzwerke hinzufügen, die zur Kommunikation mit Cloud Volumes ONTAP erforderlich sind, aber auch sicherstellen, dass beide Adressbereiche hinzugefügt werden, damit der interne Google Load Balancer korrekt funktioniert. Dies sind die Adressen 130.211.0.0/22 und 35.191.0.0/16. Weitere Informationen finden Sie unter "Google Cloud Dokumentation: Load Balancer Firewall Rules".

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

Protokoll	Port	Zweck
HTTPS	443	Konnektivität mit dem Connector und 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
TCP	63001-63050	Ports zur Lastausgleichssonde zur Ermittlung des ordnungsgemäßen Node (nur für HA-Paare erforderlich)
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
AutoSupport	HTTPS	443	Node Management-LIF	support.netapp.com	AutoSupport (HTTPS ist der Standard)
	HTTP	80	Node Management-LIF	support.netapp.com	AutoSupport (nur wenn das Transportprotokoll von HTTPS zu HTTP geändert wird)
	TCP	3128	Node Management-LIF	Stecker	Senden von AutoSupport-Nachrichten über einen Proxy-Server auf dem Connector, falls keine ausgehende Internetverbindung verfügbar ist
Cluster	Gesamter Datenverkehr	Gesamter Datenverkehr	Alle LIFs auf einem Node	Alle LIFs auf dem anderen Node	Kommunikation zwischen Clustern (nur Cloud Volumes ONTAP HA)
Konfigurations-Backups	HTTP	80	Node Management-LIF	\Http://<connector-IP-address>/occm/offboxconfig	Senden Sie Konfigurationssicherungen an den Connector. "Informationen zu Backup-Dateien für die Konfiguration".
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

Service	Protokoll	Port	Quelle	Ziel	Zweck
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 VPC-1, VPC-2 und VPC-3

In Google Cloud wird eine HA-Konfiguration über vier VPCs hinweg bereitgestellt. Die für die HA-Konfiguration in VPC-0 erforderlichen Firewall-Regeln sind O. g. für Cloud Volumes ONTAP.

Gleichzeitig ermöglichen die vordefinierten Firewall-Regeln, die BlueXP für Instanzen in VPC-1, VPC-2 und VPC-3 erstellt, die Ingress-Kommunikation über *all* Protokolle und Ports. Diese Regeln ermöglichen die Kommunikation zwischen HA-Nodes.

Die Kommunikation zwischen den HA-Nodes und dem HA Mediator erfolgt über Port 3260 (iSCSI).

> Um eine hohe Schreibgeschwindigkeit für neue Implementierungen des Google Cloud HA-Paars zu ermöglichen, ist für VPC-1, VPC-2 und VPC-3 eine maximale Übertragungseinheit (MTU) von mindestens 8,896 Byte erforderlich. Wenn Sie ein Upgrade vorhandener VPC-1, VPC-2 und VPC-3 auf eine MTU von 8,896 Byte vornehmen möchten, müssen Sie während des Konfigurationsprozesses alle vorhandenen HA-Systeme mit diesen VPCs herunterfahren.

Anforderungen an den Steckverbinder

Wenn Sie noch keinen Connector erstellt haben, sollten Sie auch die Netzwerkanforderungen für den Connector prüfen.

- "Zeigen Sie die Netzwerkanforderungen für den Connector an"
- "Firewall-Regeln in Google Cloud"

Planung von VPC-Service-Kontrollen in GCP

Wenn Sie sich für die Sperrung Ihrer Google Cloud-Umgebung mit VPC-Servicekontrollen entscheiden, sollten Sie verstehen, wie BlueXP und Cloud Volumes ONTAP mit den Google Cloud-APIs interagieren. Außerdem sollten Sie erfahren, wie Sie Ihre Service-Umgebung für die Bereitstellung von BlueXP und Cloud Volumes ONTAP konfigurieren.

Mit den VPC-Service-Kontrollen können Sie den Zugriff auf von Google gemanagte Services außerhalb einer vertrauenswürdigen Umgebung steuern, den Datenzugriff von nicht vertrauenswürdigen Standorten aus blockieren und die Risiken bei nicht autorisierten Datentransfers minimieren. "Erfahren Sie mehr über Google Cloud VPC Service Controls".

Kommunikation von NetApp Services mit VPC Service Controls

BlueXP kommuniziert direkt mit den Google Cloud APIs. Dies wird entweder von einer externen IP-Adresse außerhalb von Google Cloud (z. B. von api.services.cloud.netapp.com) oder innerhalb von Google Cloud von einer dem BlueXP Connector zugewiesenen internen Adresse ausgelöst.

Abhängig vom Bereitstellungsstil des Connectors müssen möglicherweise bestimmte Ausnahmen für Ihren Service-Umfang gemacht werden.

Bilder

Sowohl Cloud Volumes ONTAP als auch BlueXP verwenden Images eines Projekts in GCP, das von NetApp gemanagt wird. Dies kann sich auf die Bereitstellung von BlueXP Connector und Cloud Volumes ONTAP auswirken, wenn Ihr Unternehmen über eine Richtlinie verfügt, die die Verwendung von Bildern blockiert, die nicht im Unternehmen gehostet werden.

Sie können einen Connector manuell mit Hilfe der manuellen Installationsmethode bereitstellen, aber Cloud Volumes ONTAP muss auch Bilder aus dem NetApp Projekt abrufen. Zur Bereitstellung eines Connectors und Cloud Volumes ONTAP müssen Sie eine Liste mit zulässigen Inhalten bereitstellen.

Bereitstellen eines Connectors

Der Benutzer, der einen Connector implementiert, muss in der Lage sein, auf ein Image verweisen, das im ProjectID *netapp-CloudManager* und der Projektnummer *14190056516* gehostet wird.

Implementierung von Cloud Volumes ONTAP

- Das BlueXP-Servicekonto muss ein im ProjectID *netapp-CloudManager* gehostetes Image und die Projektnummer *14190056516* aus dem Serviceprojekt referenzieren.
- Das Servicekonto für den Google APIs Service Agent muss auf ein Image verweisen, das im ProjectID *netapp-CloudManager* und die Projektnummer *14190056516* aus dem Serviceprojekt gehostet wird.

Im Folgenden sind Beispiele für Regeln aufgeführt, die für das Abrufen dieser Images an VPC-Service-Kontrollen nötig sind.

VPC-Service steuert Perimeterrichtlinien

Richtlinien erlauben Ausnahmen von den VPC Service Controls-Regelsätzen. Weitere Informationen über Richtlinien finden Sie auf der "Dokumentation der GCP VPC Service Controls Policy".

Um die Richtlinien festzulegen, die für BlueXP erforderlich sind, navigieren Sie zu Ihrem VPC Service Controls Perimeter in Ihrem Unternehmen und fügen Sie die folgenden Richtlinien hinzu. Die Felder sollten mit den Optionen übereinstimmen, die auf der Seite „VPC Service Controls Policy“ angegeben sind. Beachten Sie auch, dass **alle** Regeln erforderlich sind und die **ODER** Parameter im Regelsatz verwendet werden sollen.

Ingress-Regeln

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

ODER

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

ODER

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

Für ausgehenden Datenverkehr

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

Die oben beschriebene Projektnummer gilt als das Projekt *netapp-CloudManager*, das von NetApp zur Speicherung von Bildern für den Connector und für Cloud Volumes ONTAP verwendet wird.

Erstellen eines Servicekontos für Daten-Tiering und Backups

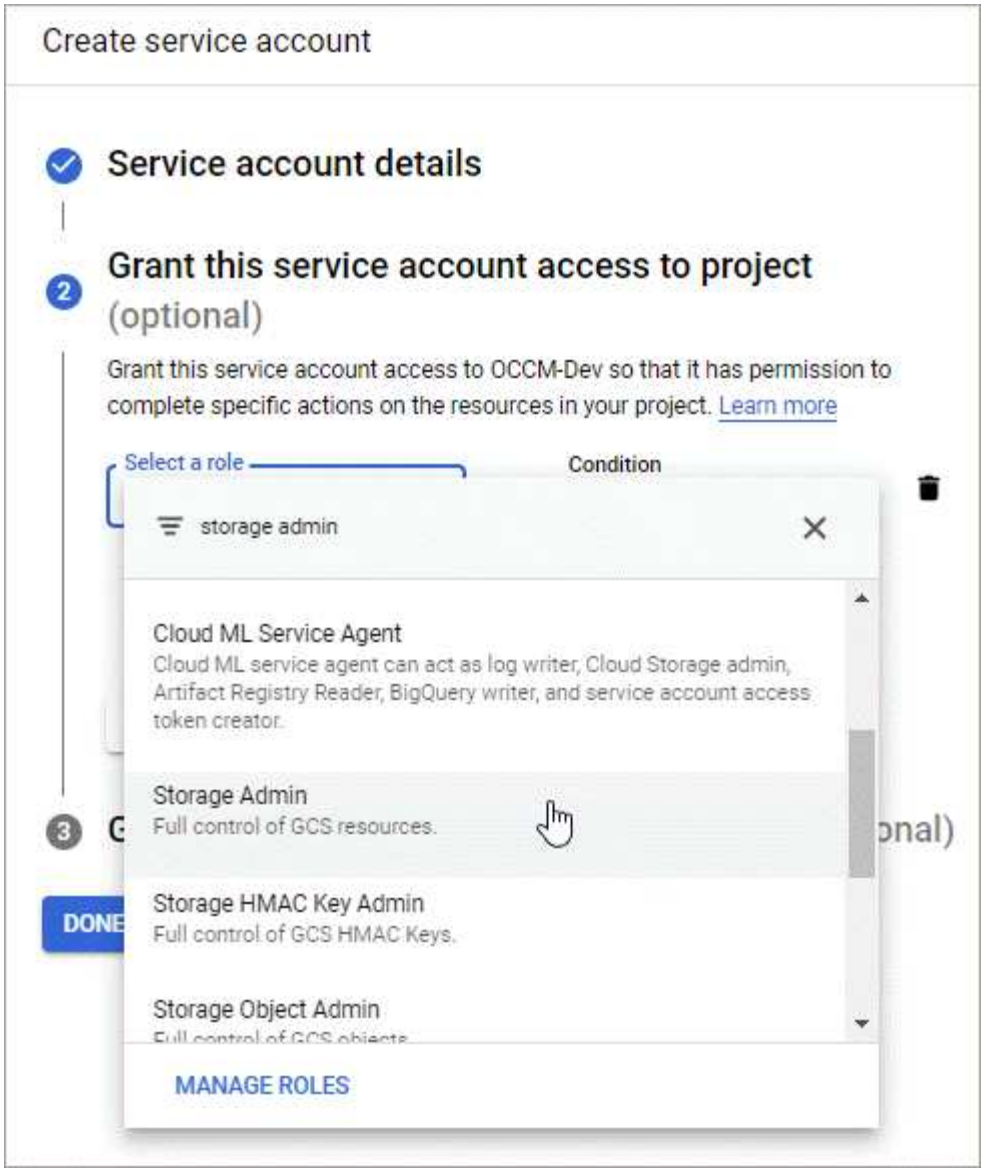
Für Cloud Volumes ONTAP ist ein Google Cloud-Servicekonto aus zwei Gründen erforderlich. Die erste lautet, wenn Sie aktivieren "Daten-Tiering" Tiering selten genutzter Daten auf kostengünstigen Objekt-Storage in Google Cloud. Die zweite lautet, wenn Sie den aktivieren "BlueXP Backup und Recovery" Um Volumes auf kostengünstigen Objekt-Storage zu sichern.

Cloud Volumes ONTAP verwendet das Service-Konto, um auf einen Bucket für Tiering-Daten und einen anderen Bucket für Backups zuzugreifen und diese zu verwalten.

Sie können ein Service-Konto einrichten und für beide Zwecke verwenden. Das Servicekonto muss über die Rolle **Storage Admin** verfügen.

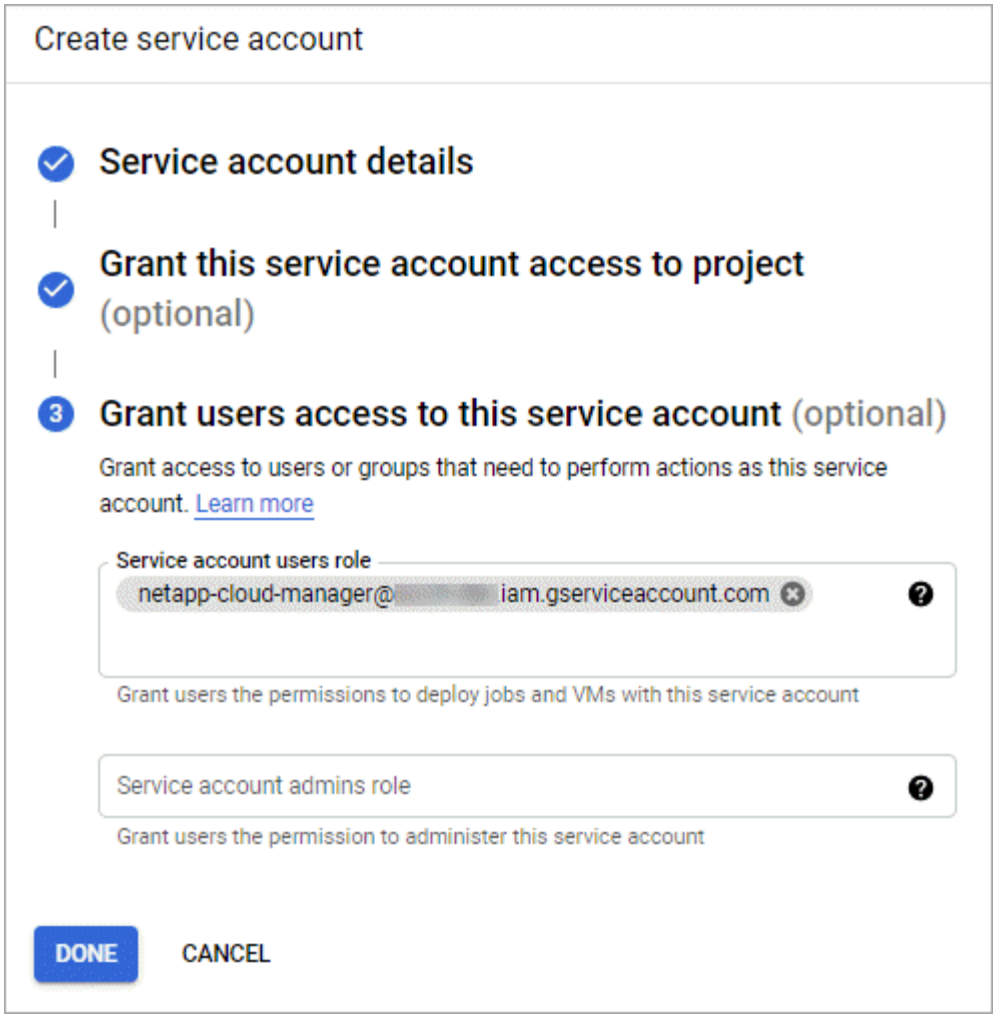
Schritte

1. In der Google Cloud Konsole "Rufen Sie die Seite Servicekonten auf".
2. Wählen Sie Ihr Projekt aus.
3. Klicken Sie auf **Dienstkonto erstellen** und geben Sie die erforderlichen Informationen ein.
    a. **Service Account Details**: Geben Sie einen Namen und eine Beschreibung ein.
    b. **Begeben Sie diesem Servicekonto Zugriff auf das Projekt**: Wählen Sie die Rolle **Storage Admin**.



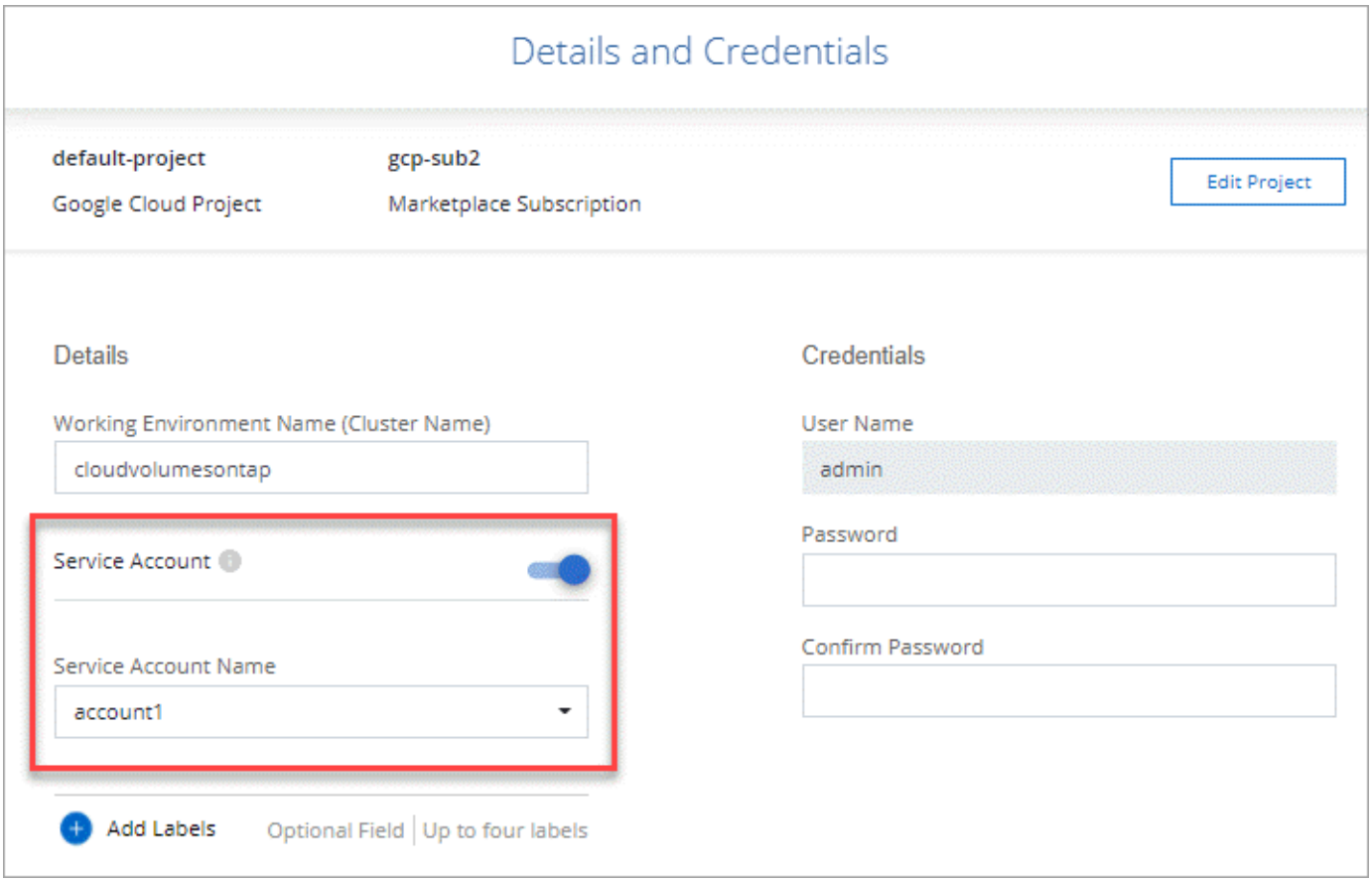
c. **Benutzern Zugriff auf dieses Servicekonto gewähren**: Fügen Sie das Connector Service-Konto als *Service Account User* zu diesem neuen Service-Konto hinzu.

   Dieser Schritt ist nur für das Daten-Tiering erforderlich. Sie ist für Backup und Recovery von BlueXP nicht erforderlich.



Was kommt als Nächstes?

Sie müssen das Servicekonto später auswählen, wenn Sie eine Cloud Volumes ONTAP Arbeitsumgebung erstellen.



Nutzung von vom Kunden gemanagten Schlüsseln mit Cloud Volumes ONTAP

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

Schritte

1. Stellen Sie sicher, dass das Servicekonto BlueXP Connector im Projekt, in dem der Schlüssel gespeichert ist, über die entsprechenden Berechtigungen auf Projektebene verfügt.

   Die Berechtigungen werden im bereitgestellt "Standardmäßig sind die Berechtigungen für das Connector-Dienstkonto festgelegt", Kann aber nicht angewendet werden, wenn Sie ein alternatives Projekt für den Cloud Key Management Service verwenden.

   Folgende Berechtigungen stehen zur Auswahl:

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

2. Stellen Sie sicher, dass das Servicekonto für das "Google Compute Engine Service Agent" Hat Cloud

KMS-Verschlüsselung/Dekrypter-Berechtigungen auf dem Schlüssel.

Der Name des Dienstkontos verwendet das folgende Format: "Service-[Service_project_number]@compute-system.iam.gserviceaccount.com".

"Google Cloud Documentation: IAM mit Cloud KMS nutzen - Rollenverteilung auf einer Ressource"

3. Rufen Sie die „id“ des Schlüssels ab, indem Sie den Befehl get für das aufrufen `/gcp/vsa/metadata/gcp-encryption-keys` API-Anruf oder durch Auswahl des „Copy Resource Name“ auf dem Schlüssel in der GCP-Konsole.
4. Wenn Sie vom Kunden verwaltete Schlüssel und Tiering-Daten in Objekt-Storage verwenden, versucht BlueXP, dieselben Schlüssel zu verwenden, die zur Verschlüsselung der persistenten Festplatten verwendet werden. Zunächst müssen Sie Google Cloud Storage Buckets aktivieren, um die Schlüssel zu verwenden:

   a. Suchen Sie den Google Cloud Storage Service Agent, indem Sie den folgenden folgen "Google Cloud Documentation: Die Bereitstellung des Cloud Storage-Service-Agenten".

   b. Navigieren Sie zum Verschlüsselungsschlüssel und weisen Sie den Google Cloud Storage Service Agent mit Cloud KMS Verschlüsselungs-/Dekrypter-Berechtigungen zu.

   Weitere Informationen finden Sie unter "Google Cloud Documentation: Nutzung von vom Kunden gemanagten Verschlüsselungsschlüsseln"

5. Verwenden Sie bei der Erstellung einer Arbeitsumgebung den Parameter „GcpEncryption“ in Verbindung mit Ihrer API-Anforderung.

   Beispiel

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-1/cryptoKeys/generatedkey1"
  }
```

Siehe "BlueXP Automation Dokumentation" Weitere Informationen zur Verwendung des Parameters „GcpEncryption“.

Lizenzierung für Cloud Volumes ONTAP in Google Cloud einrichten

Nachdem Sie sich für die Lizenzoption entschieden haben, die Sie mit Cloud Volumes ONTAP verwenden möchten, sind einige Schritte erforderlich, bevor Sie beim Erstellen einer neuen Arbeitsumgebung die Lizenzoption wählen können.

Freimium

Wählen Sie das Freimium-Angebot aus, um Cloud Volumes ONTAP mit bis zu 500 gib bereitgestellter Kapazität kostenlos zu nutzen. "Erfahren Sie mehr über das Freemium Angebot".

Schritte

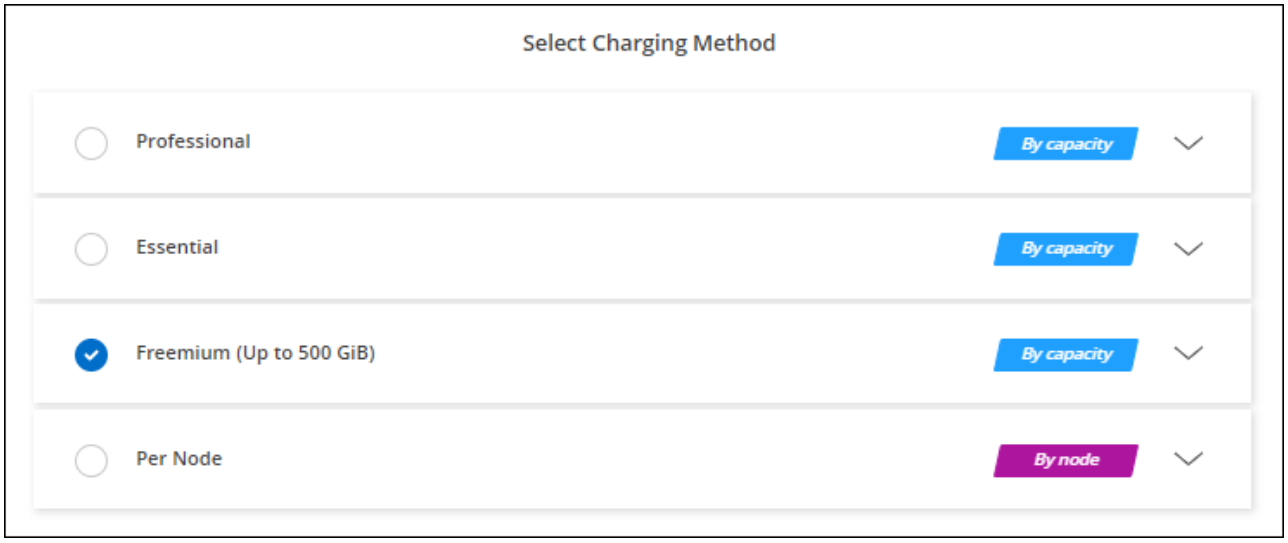
1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in

BlueXP.

a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um das Pay-as-you-go-Angebot im Google Cloud Marketplace zu abonnieren.

   Sie werden über das Marketplace-Abonnement nicht belastet, es sei denn, Sie überschreiten 500 gib der bereitgestellten Kapazität. Zu dieser Zeit wird das System automatisch in das konvertiert "Essentials-Paket".

b. Wenn Sie zu BlueXP zurückkehren, wählen Sie **Freemium**, wenn Sie die Seite mit den Lademethoden aufrufen.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Google Cloud zu starten".

Kapazitätsbasierte Lizenz

Dank der kapazitätsbasierten Lizenzierung können Sie für Cloud Volumes ONTAP pro tib Kapazität bezahlen. Kapazitätsbasierte Lizenzierung ist in Form eines *package*, dem Essentials-Paket oder dem Professional-Paket verfügbar.

Die Essentials- und Professional-Pakete sind mit den folgenden Verbrauchsmodellen erhältlich:

- Eine Lizenz (BYOL) von NetApp erworben
- Ein stündliches PAYGO-Abonnement (Pay-as-you-go) über den Google Cloud Marketplace
- Einem Jahresvertrag

"Hier erhalten Sie weitere Informationen zur kapazitätsbasierten Lizenzierung".

In den folgenden Abschnitten werden die ersten Schritte mit jedem dieser Nutzungsmodelle beschrieben.

BYOL

Bezahlen Sie vorab, indem Sie eine Lizenz (BYOL) von NetApp erwerben und Cloud Volumes ONTAP Systeme bei jedem Cloud-Provider implementieren.

Schritte

1. "Wenden Sie sich an den NetApp Sales, um eine Lizenz zu erhalten"
2. "Fügen Sie Ihr Konto für die NetApp Support Website zu BlueXP hinzu"

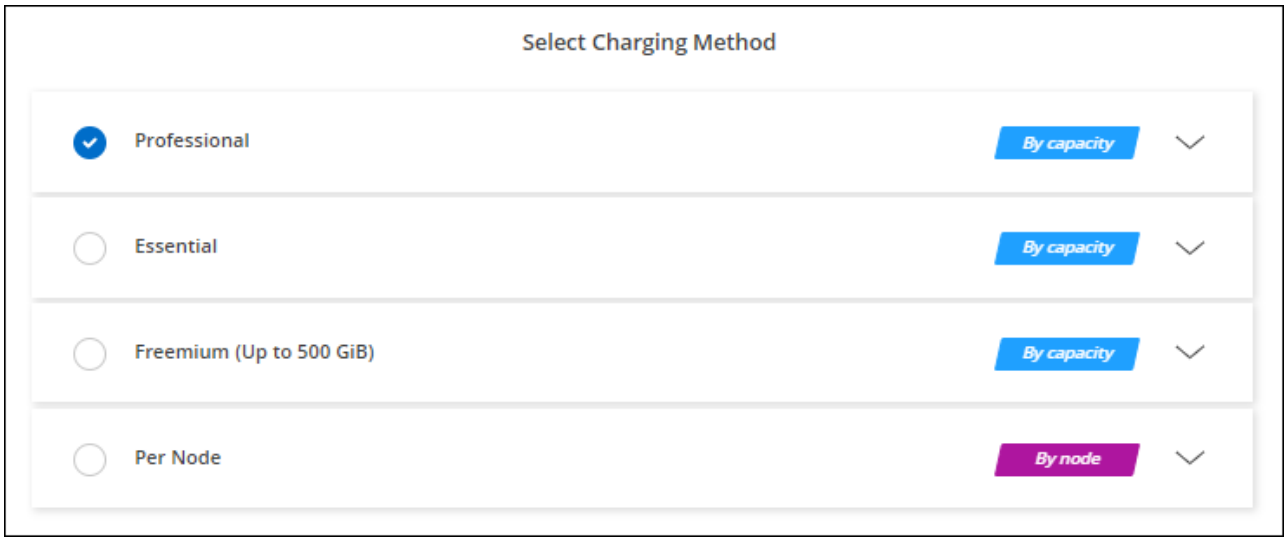
   BlueXP fragt den NetApp Lizenzierungsservice automatisch ab, um Details zu den Lizenzen zu erhalten, die mit Ihrem NetApp Support Site Konto verknüpft sind. Sollte es keine Fehler geben, fügt BlueXP die Lizenzen automatisch zum Digital Wallet hinzu.

   Bevor Sie Ihre Lizenz mit Cloud Volumes ONTAP verwenden können, muss sie über das Digital Wallet von BlueXP erhältlich sein. Wenn nötig, können Sie "Fügen Sie die Lizenz manuell zum Digital Wallet von BlueXP hinzu".

3. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um das Pay-as-you-go-Angebot im Google Cloud Marketplace zu abonnieren.

      Die Lizenz, die Sie bei NetApp erworben haben, wird immer zuerst berechnet. Wenn Sie Ihre lizenzierte Kapazität überschreiten oder die Lizenzlaufzeit abgelaufen ist, werden Sie vom Stundensatz auf dem Markt in Rechnung gestellt.

   b. Wenn Sie zu BlueXP zurückkehren, wählen Sie ein kapazitätsbasiertes Paket aus, wenn Sie die Seite mit den Lademethoden aufrufen.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Google Cloud zu starten".

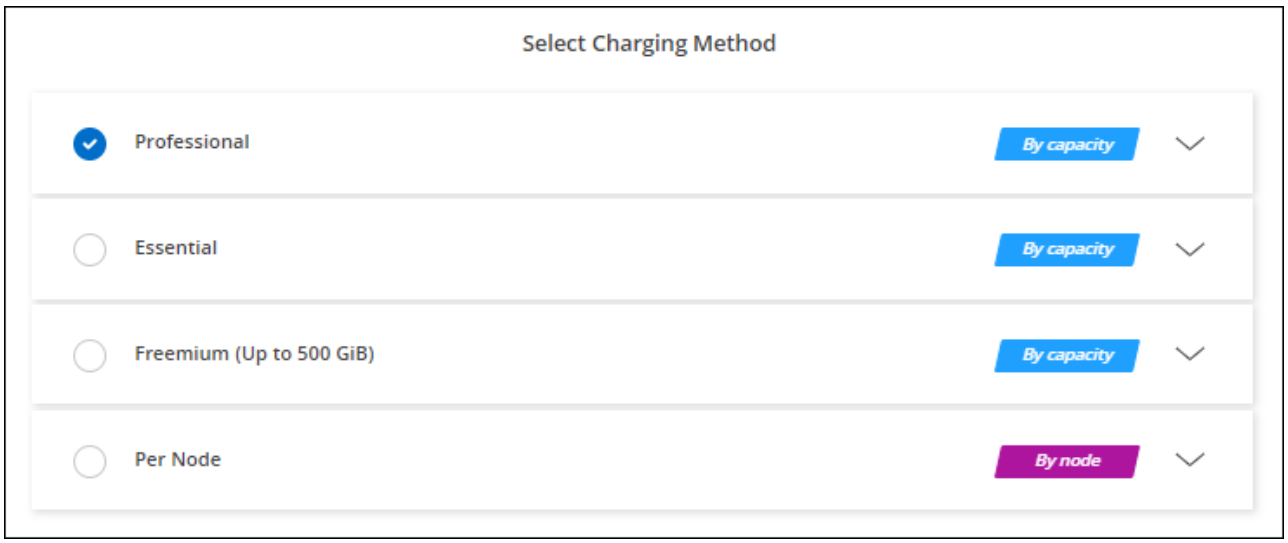
PAYGO-Abonnement

Sie bezahlen stündlich, indem Sie sich für das Angebot über den Marketplace Ihres Cloud-Providers anmelden.

Wenn Sie eine Arbeitsumgebung von Cloud Volumes ONTAP erstellen, werden Sie von BlueXP aufgefordert, den Vertrag zu abonnieren, der im Google Cloud Marketplace verfügbar ist. Dieses Abonnement wird dann zur Verrechnung mit der Arbeitsumgebung verknüpft. Sie können das gleiche Abonnement auch für zusätzliche Arbeitsumgebungen nutzen.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um das Pay-as-you-go-Angebot im Google Cloud Marketplace zu abonnieren.
   b. Wenn Sie zu BlueXP zurückkehren, wählen Sie ein kapazitätsbasiertes Paket aus, wenn Sie die Seite mit den Lademethoden aufrufen.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Google Cloud zu starten".

Sie können die mit Ihren Konten verbundenen Google Cloud Marketplace-Abonnements über die Seite Einstellungen > Anmeldeinformationen verwalten. "So managen Sie Ihre Google Cloud-Anmeldedaten und -Abonnements"

Jahresvertrag

Sie bezahlen jährlich für Cloud Volumes ONTAP durch den Kauf eines Jahresvertrags.

Schritte

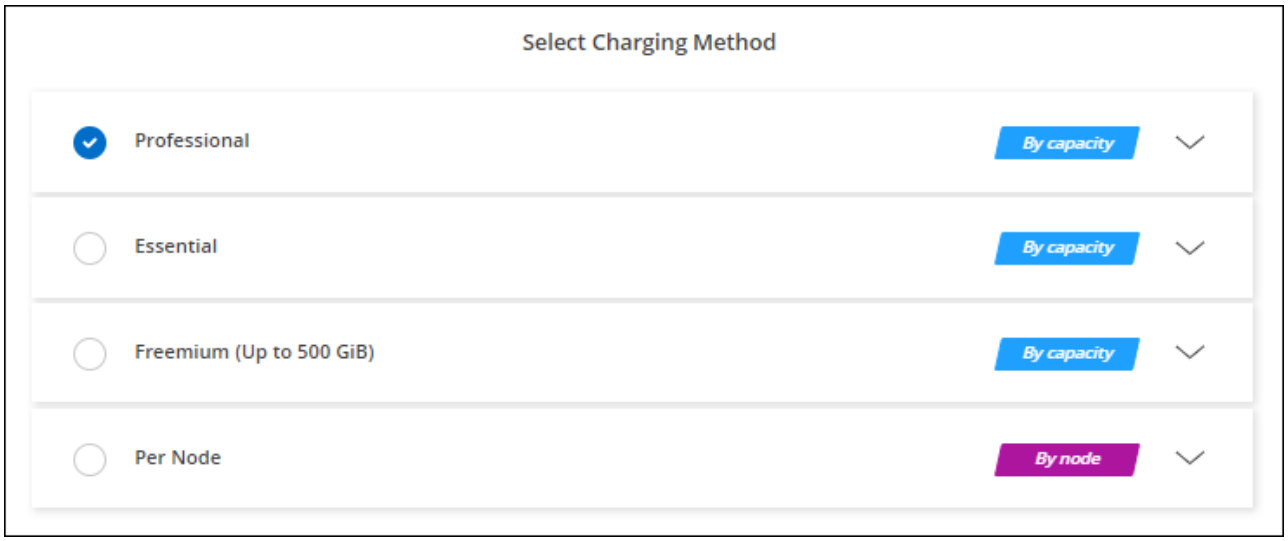
1. Wenden Sie sich an Ihren NetApp Ansprechpartner, um einen Jahresvertrag zu erwerben.

   Der Vertrag ist als *private* Angebot im Google Cloud Marketplace erhältlich.

   Nachdem NetApp das private Angebot mit Ihnen geteilt hat, können Sie den Jahresplan auswählen, wenn Sie während der Erstellung der Arbeitsumgebung den Google Cloud Marketplace abonniert haben.

2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um den Jahresplan im Google Cloud Marketplace zu abonnieren.
   b. Wählen Sie in Google Cloud den Jahresplan aus, der mit Ihrem Konto geteilt wurde, und klicken Sie dann auf **Abonnieren**.

c. Wenn Sie zu BlueXP zurückkehren, wählen Sie ein kapazitätsbasiertes Paket aus, wenn Sie die Seite mit den Lademethoden aufrufen.



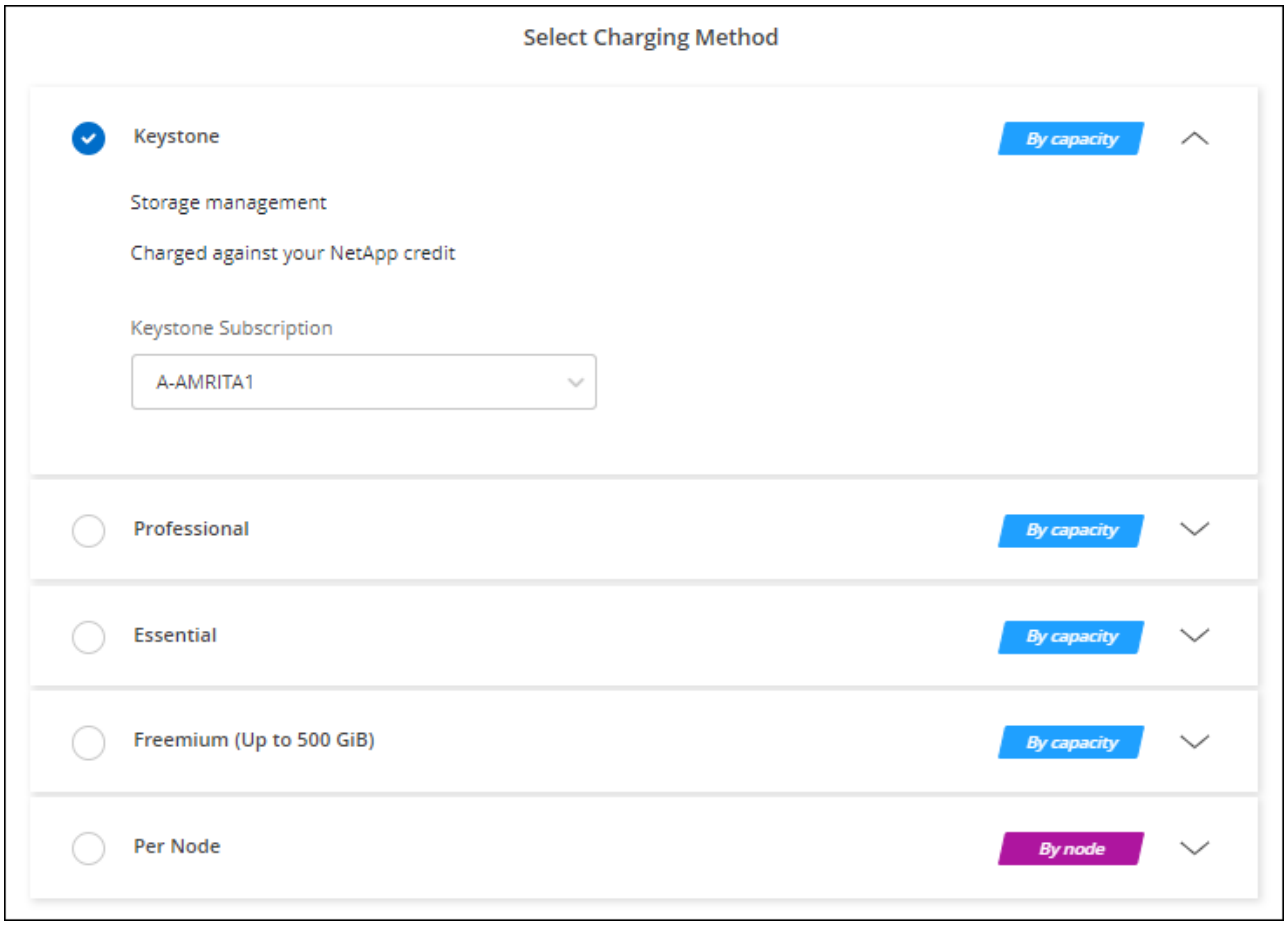
"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Google Cloud zu starten".

Keystone Abonnement

Ein Keystone Abonnement ist ein nutzungsbasierter Abonnementservice. "Weitere Informationen zu NetApp Keystone Abonnements".

Schritte

1. Wenn Sie noch kein Abonnement haben, "Kontakt zu NetApp"
2. Mailto:ng-keystone-success@netapp.com[NetApp kontaktieren]: Wir autorisieren Ihr BlueXP Benutzerkonto für eine oder mehrere Keystone Abonnements.
3. Nachdem NetApp den Account autorisiert hat, "Verknüpfen Sie Ihre Abonnements für die Verwendung mit Cloud Volumes ONTAP".
4. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
   a. Wählen Sie die Abrechnungsmethode für Keystone Abonnements aus, wenn Sie zur Auswahl einer Lademethode aufgefordert werden.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Google Cloud zu starten".

Cloud Volumes ONTAP in Google Cloud wird gestartet

Cloud Volumes ONTAP lässt sich in einer Single-Node-Konfiguration oder als HA-Paar in Google Cloud starten.

Bevor Sie beginnen

Um eine Arbeitsumgebung zu schaffen, benötigen Sie Folgendes.

- Ein Anschluss, der betriebsbereit ist.
  - Sie sollten ein haben "Anschluss, der Ihrem Arbeitsbereich zugeordnet ist".
  - "Sie sollten darauf vorbereitet sein, den Konnektor jederzeit in Betrieb zu nehmen".
  - Das mit dem Connector verbundene Servicekonto "Sollte über die erforderlichen Berechtigungen verfügen"
- Ein Verständnis der zu verwendenden Konfiguration.

  Sie sollten sich darauf vorbereiten, indem Sie eine Konfiguration auswählen und die Netzwerkinformationen zu Google Cloud von Ihrem Administrator erhalten. Weitere Informationen finden Sie unter "Planung Ihrer Cloud Volumes ONTAP Konfiguration".

- Kenntnisse über die erforderlichen Voraussetzungen zur Einrichtung der Lizenzierung für Cloud Volumes ONTAP.

"Erfahren Sie, wie Sie eine Lizenzierung einrichten".

- Es sollten Google Cloud APIs sein "In Ihrem Projekt aktiviert":
  - Cloud Deployment Manager V2-API
  - Cloud-ProtokollierungsAPI
  - Cloud Resource Manager API
  - Compute Engine-API
  - IAM-API (Identitäts- und Zugriffsmanagement

Starten eines Single-Node-Systems in Google Cloud

Schaffen Sie eine Arbeitsumgebung in BlueXP, um Cloud Volumes ONTAP in Google Cloud zu starten.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Bildschirmseite auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.
3. **Wählen Sie einen Standort**: Wählen Sie **Google Cloud** und **Cloud Volumes ONTAP**.
4. Wenn Sie dazu aufgefordert werden, "Einen Konnektor erstellen".
5. **Details & Anmeldeinformationen**: Wählen Sie ein Projekt aus, geben Sie einen Cluster-Namen an, wählen Sie optional ein Servicekonto aus, 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	BlueXP verwendet den Namen der Arbeitsumgebung, um sowohl das Cloud Volumes ONTAP System als auch die Google Cloud VM Instanz zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.
Name Des Servicekontos	Wenn Sie Vorhaben zu verwenden "Daten-Tiering" Oder "BlueXP Backup und Recovery" Mit Cloud Volumes ONTAP müssen Sie dann **Dienstkonto** aktivieren und ein Servicekonto auswählen, das über die vordefinierte Rolle Speicheradministrator verfügt. "Erfahren Sie, wie Sie ein Servicekonto erstellen".
Etiketten Hinzufügen	Etiketten sind Metadaten für Ihre Google Cloud-Ressourcen. BlueXP fügt die Etiketten zum Cloud Volumes ONTAP-System und den dem System zugeordneten Google-Cloud-Ressourcen hinzu. 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".

Feld	Beschreibung
Benutzername und Passwort	Dies sind die Anmeldeinformationen 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. Behalten Sie den Standardbenutzernamen „*admin*“ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Projekt Bearbeiten	Wählen Sie das Projekt aus, in dem Cloud Volumes ONTAP gespeichert werden soll. Das Standardprojekt ist das Projekt, in dem sich BlueXP befindet. Wenn in der Dropdown-Liste keine weiteren Projekte angezeigt werden, haben Sie das BlueXP-Servicekonto noch nicht mit anderen Projekten verknüpft. Rufen Sie die Google Cloud-Konsole auf, öffnen Sie den IAM-Service und wählen Sie das Projekt aus. Fügen Sie dem Projekt das Servicekonto mit der Rolle BlueXP hinzu. Sie müssen diesen Schritt für jedes Projekt wiederholen. Dies ist das Servicekonto, das Sie für BlueXP eingerichtet haben. "Wie auf dieser Seite beschrieben". Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen einem Abonnement zuzuordnen. Um ein Pay-as-you-go Cloud Volumes ONTAP System zu erstellen, müssen Sie im Google Cloud Marketplace ein Google Cloud-Projekt auswählen, das mit einem Abonnement für Cloud Volumes ONTAP verknüpft ist.

Im folgenden Video wird gezeigt, wie Sie Ihrem Google Cloud-Projekt ein Pay-as-you-go Marketplace-Abonnement zuordnen. Sie können auch die Schritte befolgen, um sich im anzumelden "Verknüpfen eines Marketplace-Abonnements mit Google Cloud-Anmeldedaten" Abschnitt.

Abonnieren Sie BlueXP über den Google Cloud Marketplace

6. **Services**: Wählen Sie die Dienste aus, die Sie auf diesem System verwenden möchten. Um BlueXP Backup und Recovery auszuwählen oder BlueXP Tiering zu verwenden, müssen Sie das Servicekonto in Schritt 3 angegeben haben.

   Wenn SIE WORM und Daten-Tiering nutzen möchten, müssen Sie BlueXP Backup und Recovery deaktivieren und eine Cloud Volumes ONTAP Arbeitsumgebung mit Version 9.8 oder höher implementieren.

7. **Standort & Konnektivität**: Wählen Sie einen Speicherort, wählen Sie eine Firewall-Richtlinie und bestätigen Sie die Netzwerkverbindung mit Google Cloud Speicher für Daten-Tiering.

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

Feld	Beschreibung
Konnektivitätsprüfung	Für das Tiering selten genutzter Daten auf einen Google Cloud Storage-Bucket 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".

Feld	Beschreibung
Generierte Firewallrichtlinie	Wenn Sie BlueXP die Firewall-Richtlinie für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Selected VPC Only** wählen, ist der Quellfilter für eingehenden Datenverkehr der Subnetz-Bereich des ausgewählten VPC und der Subnetz-Bereich des VPC, in dem sich der Connector befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VPCs** wählen, ist der Quellfilter für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene Firewallrichtlinie verwenden	Wenn Sie eine vorhandene Firewallrichtlinie verwenden, stellen Sie sicher, dass diese die erforderlichen Regeln enthält. Link: Learn über Firewall-Regeln für Cloud Volumes ONTAP.

8. **Charging Methods and NSS Account**: Geben Sie an, welche Ladungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site Konto an.
   - "Informieren Sie sich über Lizenzoptionen für Cloud Volumes ONTAP".
   - "Erfahren Sie, wie Sie eine Lizenzierung einrichten".
9. **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.
10. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP-Version nach Bedarf und wählen Sie einen Maschinentyp.

    Wenn für die ausgewählte Version eine neuere Version von Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert BlueXP das System auf diese Version, wenn die Arbeitsumgebung erstellt wird. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.10.1 und 9.10.1 P4 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 und die Größe für jede Platte.

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

    Die Festplattengröße ist für alle Festplatten im ursprünglichen Aggregat und für alle zusätzlichen Aggregate bestimmt, die BlueXP erzeugt, 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 "Dimensionieren Sie Ihr System in Google Cloud".
12. **Flash Cache, Schreibgeschwindigkeit und WORM**:

    a. Aktivieren Sie **Flash Cache**, falls gewünscht.

Ab Cloud Volumes ONTAP 9.13.1 wird *Flash Cache* auf den Instanztypen n2-Standard-16, n2-Standard-32, n2-Standard-48 und n2-Standard-64 unterstützt. Sie können Flash Cache nach der Bereitstellung nicht deaktivieren.

b. Wählen Sie bei Bedarf * Normal* oder **High** Schreibgeschwindigkeit.

"Erfahren Sie mehr über Schreibgeschwindigkeit".

Über die Option **High** Write Speed stehen eine hohe Schreibgeschwindigkeit und eine höhere maximale Übertragungseinheit (MTU) von 8,896 Byte zur Verfügung. Darüber hinaus erfordert die höhere MTU von 8,896 die Auswahl von VPC-1, VPC-2 und VPC-3 für die Implementierung. Weitere Informationen zu VPC-1, VPC-2 und VPC-3 finden Sie unter "Regeln für VPC-1, VPC-2 und VPC-3".

c. Aktivieren Sie auf Wunsch den WORM-Storage (Write Once, Read Many).

WORM kann nicht aktiviert werden, wenn Daten-Tiering für Cloud Volumes ONTAP-Versionen 9.7 und darunter aktiviert wurde. Ein Wechsel- oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach Aktivierung VON WORM und Tiering gesperrt.

"Erfahren Sie mehr über WORM Storage".

a. Wenn Sie DEN WORM-Speicher aktivieren, wählen Sie den Aufbewahrungszeitraum aus.

13. **Daten-Tiering in Google Cloud Platform**: Wählen Sie, ob Daten-Tiering auf dem ursprünglichen Aggregat aktiviert werden soll, wählen Sie eine Speicherklasse für die Tiered Data aus und wählen Sie dann entweder ein Servicekonto mit der vordefinierten Storage Admin-Rolle aus (erforderlich für Cloud Volumes ONTAP 9.7 oder höher), Oder wählen Sie ein Google Cloud Konto aus (erforderlich für Cloud Volumes ONTAP 9.6).

Beachten Sie Folgendes:

- BlueXP legt das Servicekonto 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 Connector-Dienstkonto als Benutzer des Tiering-Dienstkontos hinzufügen, andernfalls können Sie es nicht in BlueXP auswählen
- Hilfe zum Hinzufügen eines Google Cloud-Kontos finden Sie unter "Einrichten und Hinzufügen von Google Cloud-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 bei nachfolgenden Aggregaten aktivieren. Sie müssen das System jedoch deaktivieren und ein Service-Konto über die Google Cloud Konsole hinzufügen.

"Weitere Informationen zum Daten-Tiering".

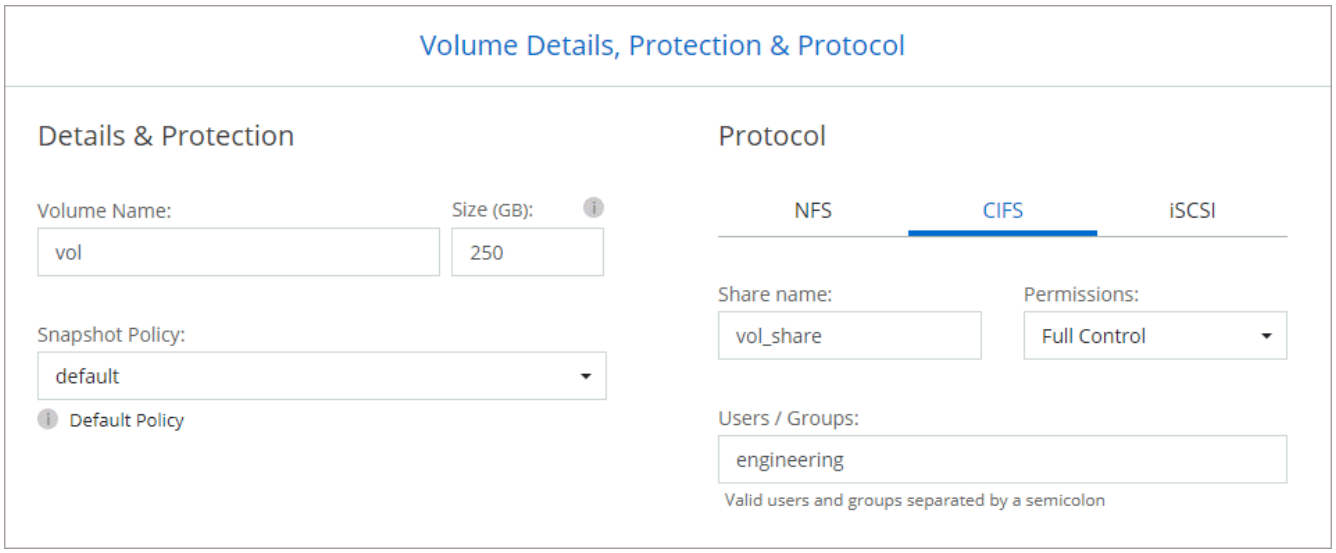
14. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

"Hier erhalten Sie Informationen zu den unterstützten Client-Protokollen und -Versionen".

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 BlueXP einen Wert ein, der Zugriff auf alle Instanzen im Subnetz bietet.
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 BlueXP 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:



15. **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. Wenn Sie Google Managed Active Directory konfigurieren, kann standardmäßig mit der IP-Adresse 169.254.169.254 auf AD zugegriffen werden.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. Um von Google verwaltete Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in diesem Feld **OU=Computer,OU=Cloud** ein.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD"^]
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.

Feld	Beschreibung
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden** aus, um einen NTP-Server mit Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Siehe "BlueXP Automation Dokumentation" Entsprechende Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Er ist nicht konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

16. **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 "Wählen Sie ein Volume-Auslastungsprofil aus" Und "Data Tiering - Übersicht".

17. **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 den Google Cloud-Ressourcen zu erhalten, die BlueXP kaufen wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie Auf **Go**.

Ergebnis

BlueXP 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.

Starten eines HA-Paars in Google Cloud

Schaffen Sie eine Arbeitsumgebung in BlueXP, um Cloud Volumes ONTAP in Google Cloud zu starten.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.

3. **Wählen Sie einen Standort**: Wählen Sie **Google Cloud** und **Cloud Volumes ONTAP HA**.
4. **Details & Anmeldeinformationen**: Wählen Sie ein Projekt aus, geben Sie einen Cluster-Namen an, wählen Sie optional ein Servicekonto aus, 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	BlueXP verwendet den Namen der Arbeitsumgebung, um sowohl das Cloud Volumes ONTAP System als auch die Google Cloud VM Instanz zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.
Name Des Servicekontos	Wenn Sie die verwenden möchten "BlueXP Tiering" Oder "BlueXP Backup und Recovery" Services. Sie müssen den Schalter **Service-Konto** aktivieren und dann das Servicekonto auswählen, das die vordefinierte Rolle Storage-Admin hat.
Etiketten Hinzufügen	Etiketten sind Metadaten für Ihre Google Cloud-Ressourcen. BlueXP fügt die Etiketten zum Cloud Volumes ONTAP-System und den dem System zugeordneten Google-Cloud-Ressourcen hinzu. 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 Anmeldeinformationen 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. Behalten Sie den Standardbenutzernamen „*admin*“ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Projekt Bearbeiten	Wählen Sie das Projekt aus, in dem Cloud Volumes ONTAP gespeichert werden soll. Das Standardprojekt ist das Projekt, in dem sich BlueXP befindet. Wenn in der Dropdown-Liste keine weiteren Projekte angezeigt werden, haben Sie das BlueXP-Servicekonto noch nicht mit anderen Projekten verknüpft. Rufen Sie die Google Cloud-Konsole auf, öffnen Sie den IAM-Service und wählen Sie das Projekt aus. Fügen Sie dem Projekt das Servicekonto mit der Rolle BlueXP hinzu. Sie müssen diesen Schritt für jedes Projekt wiederholen. Dies ist das Servicekonto, das Sie für BlueXP eingerichtet haben. "Wie auf dieser Seite beschrieben". Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen einem Abonnement zuzuordnen. Um ein Pay-as-you-go Cloud Volumes ONTAP System zu erstellen, müssen Sie im Google Cloud Marketplace ein Google Cloud-Projekt auswählen, das mit einem Abonnement für Cloud Volumes ONTAP verknüpft ist.

Im folgenden Video wird gezeigt, wie Sie Ihrem Google Cloud-Projekt ein Pay-as-you-go Marketplace-Abonnement zuordnen. Sie können auch die Schritte befolgen, um sich im anzumelden "Verknüpfen eines Marketplace-Abonnements mit Google Cloud-Anmeldedaten" Abschnitt.

Abonnieren Sie BlueXP über den Google Cloud Marketplace

5. **Services**: Wählen Sie die Dienste aus, die Sie auf diesem System verwenden möchten. Um BlueXP Backup und Recovery auszuwählen oder BlueXP Tiering zu verwenden, müssen Sie das Servicekonto in Schritt 3 angegeben haben.

   Wenn SIE WORM und Daten-Tiering nutzen möchten, müssen Sie BlueXP Backup und Recovery deaktivieren und eine Cloud Volumes ONTAP Arbeitsumgebung mit Version 9.8 oder höher implementieren.

6. **HA-Implementierungsmodelle**: Wählen Sie mehrere Zonen (empfohlen) oder eine einzelne Zone für die HA-Konfiguration. Wählen Sie anschließend eine Region und Zonen aus.

   "Weitere Informationen zu den HA-Implementierungsmodellen".

7. **Konnektivität**: Wählen Sie vier verschiedene VPCs für die HA-Konfiguration, ein Subnetz in jedem VPC und wählen Sie dann eine Firewall-Richtlinie.

   "Erfahren Sie mehr über Netzwerkanforderungen".

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

Feld	Beschreibung
Generierte Richtlinie	Wenn Sie BlueXP die Firewall-Richtlinie für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Selected VPC Only** wählen, ist der Quellfilter für eingehenden Datenverkehr der Subnetz-Bereich des ausgewählten VPC und der Subnetz-Bereich des VPC, in dem sich der Connector befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VPCs** wählen, ist der Quellfilter für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Verwenden Sie vorhandene	Wenn Sie eine vorhandene Firewallrichtlinie verwenden, stellen Sie sicher, dass diese die erforderlichen Regeln enthält. "Informieren Sie sich über die Firewall-Regeln für Cloud Volumes ONTAP".

8. **Charging Methods and NSS Account**: Geben Sie an, welche Ladungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site Konto an.
   - "Informieren Sie sich über Lizenzoptionen für Cloud Volumes ONTAP".
   - "Erfahren Sie, wie Sie eine Lizenzierung einrichten".
9. **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.

10. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP-Version nach Bedarf und wählen Sie einen Maschinentyp.

> Wenn für die ausgewählte Version eine neuere Version von Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert BlueXP das System auf diese Version, wenn die Arbeitsumgebung erstellt wird. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.10.1 und 9.10.1 P4 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 und die Größe für jede Platte.

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

    Die Festplattengröße ist für alle Festplatten im ursprünglichen Aggregat und für alle zusätzlichen Aggregate bestimmt, die BlueXP erzeugt, 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 "Dimensionieren Sie Ihr System in Google Cloud".

12. **Flash Cache, Schreibgeschwindigkeit und WORM**:

    a. Aktivieren Sie **Flash Cache**, falls gewünscht.

    > Ab Cloud Volumes ONTAP 9.13.1 wird *Flash Cache* auf den Instanztypen n2-Standard-16, n2-Standard-32, n2-Standard-48 und n2-Standard-64 unterstützt. Sie können Flash Cache nach der Bereitstellung nicht deaktivieren.

    b. Wählen Sie bei Bedarf * Normal* oder **High** Schreibgeschwindigkeit.

    "Erfahren Sie mehr über Schreibgeschwindigkeit".

    > Hohe Schreibgeschwindigkeit und eine höhere maximale Übertragungseinheit (MTU) von 8,896 Byte sind über die Option **High** Write Speed mit den Instanztypen n2-Standard-16, n2-Standard-32, n2-Standard-48 und n2-Standard-64 verfügbar. Darüber hinaus erfordert die höhere MTU von 8,896 die Auswahl von VPC-1, VPC-2 und VPC-3 für die Implementierung. Hohe Schreibgeschwindigkeit und eine MTU von 8,896 sind funktionsabhängig und können nicht einzeln innerhalb einer konfigurierten Instanz deaktiviert werden. Weitere Informationen zu VPC-1, VPC-2 und VPC-3 finden Sie unter "Regeln für VPC-1, VPC-2 und VPC-3".

    c. Aktivieren Sie auf Wunsch den WORM-Storage (Write Once, Read Many).

    WORM kann nicht aktiviert werden, wenn Daten-Tiering für Cloud Volumes ONTAP-Versionen 9.7 und darunter aktiviert wurde. Ein Wechsel- oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach Aktivierung VON WORM und Tiering gesperrt.

"Erfahren Sie mehr über WORM Storage".

    a. Wenn Sie DEN WORM-Speicher aktivieren, wählen Sie den Aufbewahrungszeitraum aus.

13. **Daten-Tiering in Google Cloud**: Wählen Sie, ob Daten-Tiering auf dem ursprünglichen Aggregat aktiviert werden soll, wählen Sie eine Speicherklasse für die Tiered-Daten und wählen Sie dann ein Service-Konto aus, das die vordefinierte Storage Admin-Rolle hat.

    Beachten Sie Folgendes:

    - BlueXP legt das Servicekonto 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 Connector-Dienstkonto als Benutzer des Tiering-Dienstkontos hinzufügen, andernfalls können Sie es nicht in BlueXP auswählen.
    - 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. Sie müssen das System jedoch deaktivieren und ein Service-Konto über die Google Cloud Konsole hinzufügen.

      "Weitere Informationen zum Daten-Tiering".

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

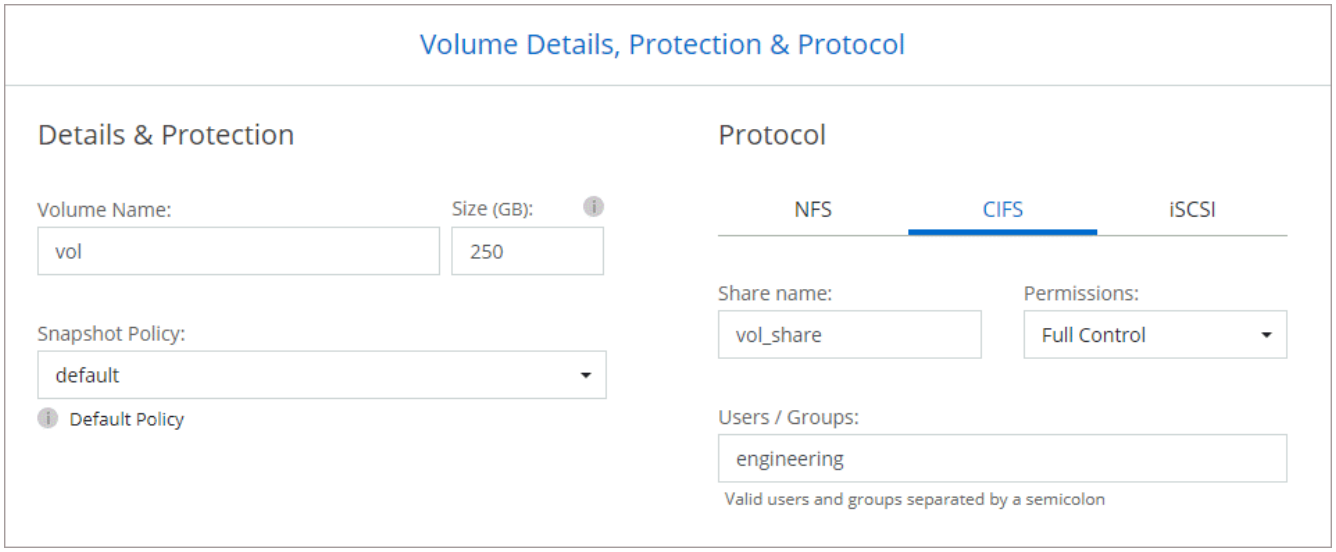
    "Hier erhalten Sie Informationen zu den unterstützten Client-Protokollen und -Versionen".

    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 BlueXP einen Wert ein, der Zugriff auf alle Instanzen im Subnetz bietet.
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 BlueXP 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:



15. **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. Wenn Sie Google Managed Active Directory konfigurieren, kann standardmäßig mit der IP-Adresse 169.254.169.254 auf AD zugegriffen werden.
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 von Google verwaltete Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in diesem Feld **OU=Computer,OU=Cloud** ein.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD"^]
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 "BlueXP Automation Dokumentation" Entsprechende Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Er ist nicht konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

16. **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 "Wählen Sie ein Volume-Auslastungsprofil aus" Und "Data Tiering - Übersicht".

17. **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 den Google Cloud-Ressourcen zu erhalten, die BlueXP kaufen wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie Auf **Go**.

Ergebnis

BlueXP 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.

Bildüberprüfung Der Google Cloud Platform

Google Cloud Bild Verifizierung Überblick

Die Google Cloud Image-Verifizierung erfüllt erweiterte NetApp Sicherheitsanforderungen. Es wurden Änderungen am Skript vorgenommen, das die Bilder generiert, um das Bild unterwegs mit privaten Schlüsseln zu signieren, die speziell für diese Aufgabe generiert wurden. Sie können die Integrität des GCP-Images mit dem signierten Digest und öffentlichen Zertifikat für Google Cloud überprüfen, das über heruntergeladen werden kann "NSS" Für eine bestimmte Version.

Die Google Cloud-Image-Verifizierung wird auf der Cloud Volumes ONTAP Softwareversion 9.13.0 oder höher unterstützt.

Konvertieren Sie Bild in RAW-Format auf Google Cloud

Das Image, das zur Bereitstellung neuer Instanzen, Upgrades oder zur Verwendung in vorhandenen Images verwendet wird, wird über mit den Clients geteilt "Die NetApp Support Site (NSS)". Der signierte Digest und die Zertifikate können über das NSS-Portal heruntergeladen werden. Laden Sie unbedingt die Digest und Zertifikate für die rechte Version herunter, die dem von NetApp Support geteilten Image entspricht. 9.13.0 Bilder verfügen beispielsweise über einen 9.13.0 signierten Digest und Zertifikate, die auf NSS verfügbar sind.

Warum ist dieser Schritt erforderlich?

Die Bilder von Google Cloud können nicht direkt heruntergeladen werden. Um das Bild mit dem signierten Digest und den Zertifikaten vergleichen zu können, benötigen Sie einen Mechanismus, um die beiden Dateien zu vergleichen und das Bild herunterzuladen. Dazu müssen Sie das Bild in ein Disk.RAW-Format exportieren/konvertieren und die Ergebnisse in einem Storage-Bucket auf Google Cloud speichern. Die Datei Disk.RAW wird getarbt und gzippt.

Das Benutzer-/Servicekonto benötigt Berechtigungen, um Folgendes auszuführen:

- Zugriff auf Google Storage-Bucket
- In Google Storage-Bucket schreiben
- Erstellen von Cloud-Build-Jobs (während des Exportvorgangs verwendet)
- Zugriff auf das gewünschte Bild
- Erstellen Sie Aufgaben für Exportbilder

Um das Image zu überprüfen, muss es in ein Disk.RAW-Format konvertiert und anschließend heruntergeladen werden.

Verwenden Sie die Google Cloud-Befehlszeile, um Google Cloud-Bild zu exportieren

Die bevorzugte Methode zum Exportieren eines Bildes in Cloud Storage ist die Verwendung von "Exportbefehl für gcloudCompute-Bilder". Dieser Befehl nimmt das bereitgestellte Image und konvertiert es in eine Disk.RAW-Datei, die tarred und gzipped wird. Die generierte Datei wird unter der Ziel-URL gespeichert und kann zur Überprüfung heruntergeladen werden.

Der Benutzer/das Konto muss über Berechtigungen verfügen, um auf den gewünschten Bucket zuzugreifen und in diesen zu schreiben, das Bild zu exportieren und Cloud-Builds (die von Google zum Exportieren des Bildes verwendet werden) zu erstellen, um diesen Vorgang auszuführen.

Export Google Cloud Bild mit gcloud

Klicken Sie zum Anzeigen auf

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

Extrahiere gezippte Dateien

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

Siehe "Google Cloud-Dokument beim Exportieren eines Bildes" Weitere Informationen zum Exportieren von Bildern über Google Cloud.

Überprüfung der Bildsignatur

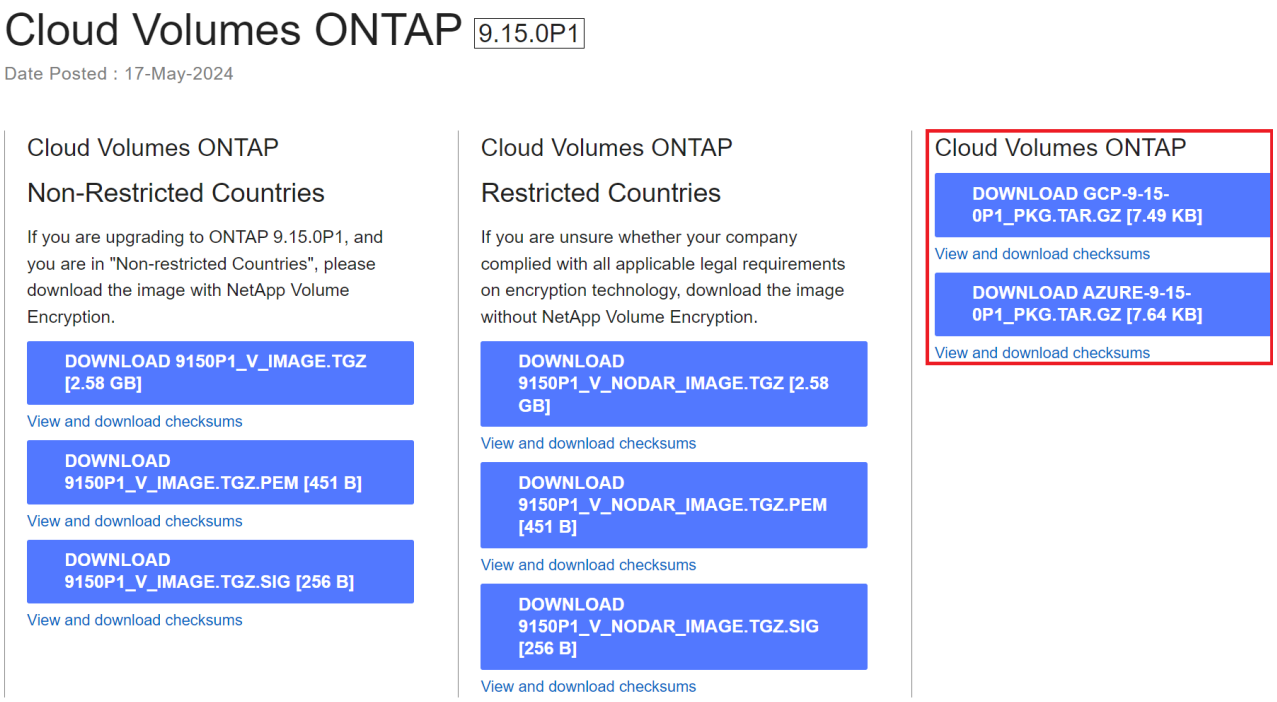
Verifizieren von durch Google Cloud signierten Bildern

Um das exportierte, von Google Cloud signierte Image zu überprüfen, müssen Sie die Image Digest-Datei vom NSS herunterladen, um die Datei Disk.RAW zu validieren und den Inhalt der Datei Digest zu prüfen.

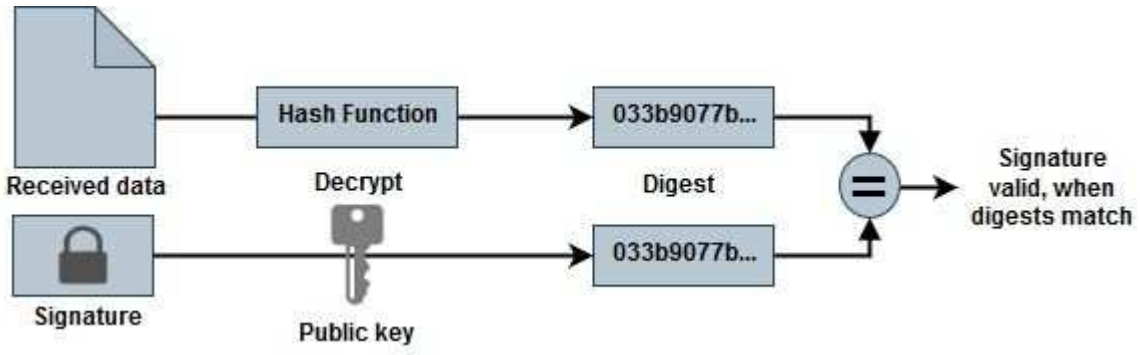
Workflow-Zusammenfassung für die signierte Bildüberprüfung

Im Folgenden finden Sie eine Übersicht über den Workflow zur Verifizierung von Google Cloud signierten Bildern.

- Von "NSS", Laden Sie das Google Cloud-Archiv mit den folgenden Dateien herunter:
  - Signierter Digest (.SIG)
  - Zertifikat mit dem öffentlichen Schlüssel (.pem)
  - Zertifikatskette (.pem)



- Laden Sie die konvertierte Datei Disk.RAW herunter
- Validieren Sie das Zertifikat mithilfe der Zertifikatskette
- Validieren Sie den signierten Digest mit dem Zertifikat, das den öffentlichen Schlüssel enthält
  - Entschlüsseln Sie den signierten Digest mit dem öffentlichen Schlüssel, um den Digest der Bilddatei zu extrahieren
  - Erstellen Sie einen Digest der heruntergeladenen Datei Disk.RAW
  - Vergleichen Sie die beiden Digest-Dateien zur Validierung



Überprüfung der Datei Disk.RAW und Digest Dateiinhalte mit OpenSSL

Sie können die heruntergeladene Datei „Disk.RAW“ von Google Cloud anhand der über den verfügbaren Inhalte der Digest-Datei überprüfen "NSS" OpenSSL verwenden.

Die OpenSSL-Befehle zur Validierung des Images sind mit Linux, Mac OS und Windows-Maschinen kompatibel.

Schritte

1. Überprüfen Sie das Zertifikat mit OpenSSL.

Klicken Sie zum Anzeigen auf

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
         e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
         22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
         38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
         fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
         bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. Legen Sie die heruntergeladene Datei Disk.RAW, die Signatur und Zertifikate in ein Verzeichnis.
3. Extrahieren Sie den öffentlichen Schlüssel mit OpenSSL aus dem Zertifikat.
4. Entschlüsseln Sie die Signatur mit dem extrahierten öffentlichen Schlüssel und überprüfen Sie den Inhalt der heruntergeladenen Datei Disk.RAW.

Klicken Sie zum Anzeigen auf

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

Verwenden Sie Cloud Volumes ONTAP

Lizenzmanagement

Management kapazitätsbasierter Lizenzen

Managen Sie Ihre kapazitätsbasierten Lizenzen aus dem Digital Wallet von BlueXP, um sicherzustellen, dass Ihr NetApp Konto über genügend Kapazitäten für Ihre Cloud Volumes ONTAP Systeme verfügt.

Kapazitätsbasierte Lizenzen ermöglichen es Ihnen, Cloud Volumes ONTAP pro tib Kapazität zu bezahlen.

Mit der *BlueXP Digital Wallet* können Sie Lizenzen für Cloud Volumes ONTAP von einem einzigen Standort aus managen. Sie können neue Lizenzen hinzufügen und vorhandene Lizenzen aktualisieren.

> Während die tatsächliche Nutzung und Nutzungsmessung für die in BlueXP gemanagten Produkte und Services immer in gib und tib berechnet werden, werden die Begriffe GB/gib und TB/tib synonym verwendet. Dies spiegelt sich in den Angeboten, Preisangeboten, Listenbeschreibungen und anderen Begleitdokumenten des Cloud Marketplace wider

"Weitere Informationen zu Cloud Volumes ONTAP Lizenzen".

Hinzufügen von Lizenzen zum Digital Wallet von BlueXP

Nach dem Kauf einer Lizenz bei Ihrem NetApp Vertriebsmitarbeiter sendet NetApp Ihnen eine E-Mail mit der Seriennummer und den zusätzlichen Lizenzdetails.

In der Zwischenzeit fragt BlueXP automatisch den NetApp Lizenzservice ab, um Informationen zu den Lizenzen zu erhalten, die mit Ihrem NetApp Support Site Konto verknüpft sind. Sollte es keine Fehler geben, fügt BlueXP die Lizenzen automatisch zum Digital Wallet hinzu.

Wenn BlueXP die Lizenz nicht hinzufügen kann, müssen Sie sie manuell zum Digital Wallet hinzufügen. Wenn der Connector z. B. an einem Standort installiert ist, der keinen Internetzugang hat, müssen Sie die Lizenzen selbst hinzufügen. Erfahren Sie, wie Sie Ihrem Konto erworbene Lizenzen hinzufügen.

Zeigen Sie die verbrauchte Kapazität in Ihrem Konto an

Das Digital Wallet von BlueXP zeigt Ihnen die verbrauchte Gesamtkapazität in Ihrem Konto und die verbrauchte Kapazität per Lizenzpaket an. Dadurch können Sie nachvollziehen, wie Sie belastet sind und ob Sie zusätzliche Kapazität erwerben müssen.

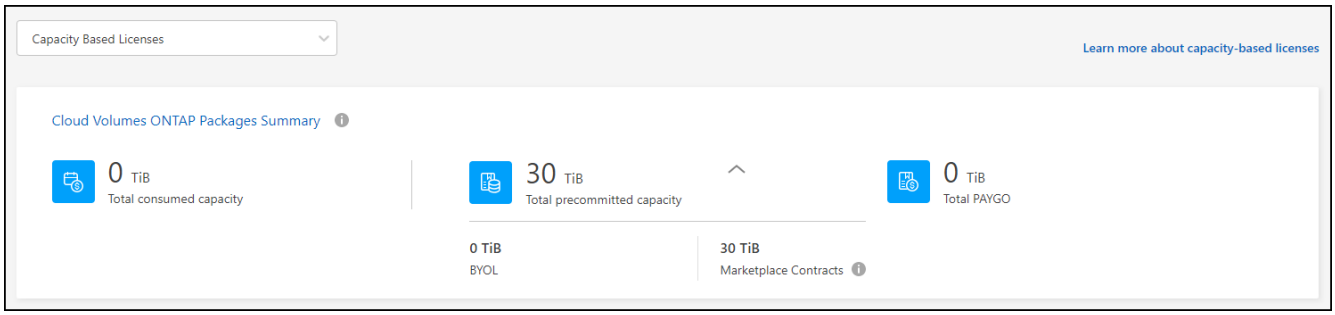
Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Lassen Sie auf der Registerkarte **Cloud Volumes ONTAP Capacity Based Licenses** ausgewählt.
3. Sehen Sie sich die Paketübersicht an, in der Sie die verbrauchte Kapazität, die gesamte vorab gebuchte Kapazität und die gesamte PAYGO-Kapazität anzeigen lassen.

    - *Verbrauchte Gesamtkapazität* ist die insgesamt bereitgestellte Kapazität aller Cloud Volumes ONTAP Systeme in Ihrem NetApp Konto. Die Abrechnung basiert auf der bereitgestellten Größe eines jeden Volumes, unabhängig vom lokalen, genutzten, gespeicherten oder effektiven Speicherplatz innerhalb des Volumes.

- *Gesamte vorab gebuchte Kapazität* ist die gesamte lizenzierte Kapazität (BYOL oder Marketplace Contract), die Sie von NetApp erworben haben.
- *Total PAYGO* ist die insgesamt bereitgestellte Kapazität anhand von Cloud-Marketplace-Abonnements. Die Abrechnung über PAYGO wird nur dann genutzt, wenn die verbrauchte Kapazität über der lizenzierten Kapazität liegt oder wenn im Digital Wallet von BlueXP keine BYOL-Lizenz verfügbar ist.

  Hier ein Beispiel für eine Zusammenfassung der Cloud Volumes ONTAP Pakete in der BlueXP Digital Wallet:



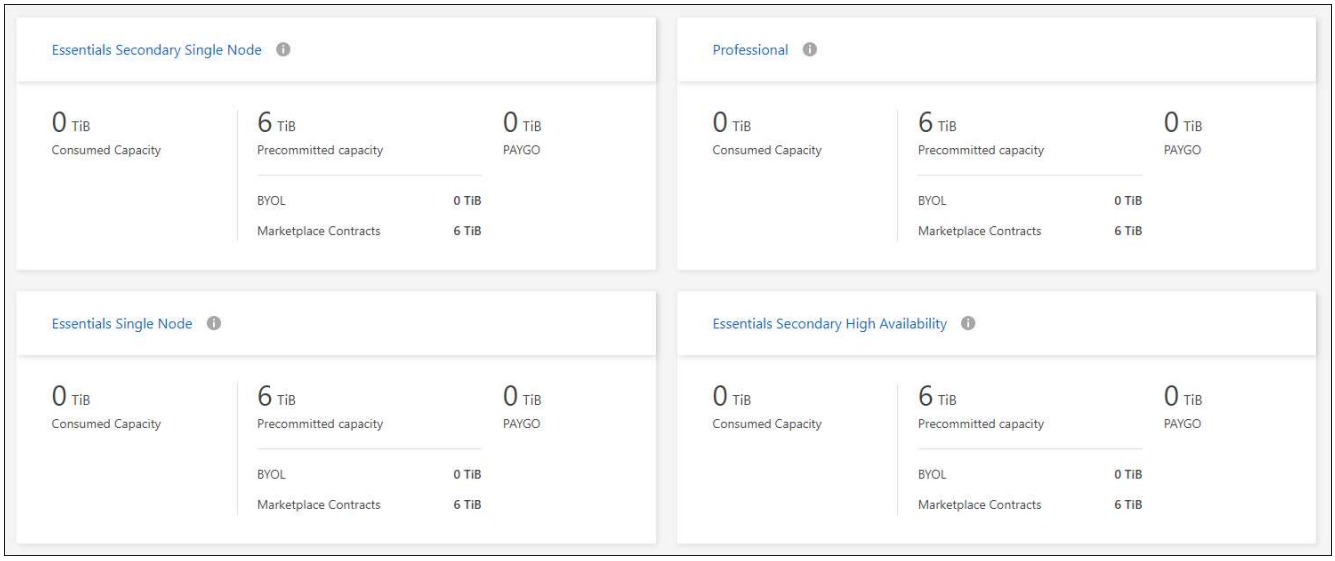
4. Zeigen Sie unter der Zusammenfassung die verbrauchte Kapazität für jedes Ihrer Lizenzierungspakete an.

   - *Verbrauchte Kapazität* zeigt die Kapazität der Volumes für dieses Paket an. Wenn Sie weitere Informationen zu einem bestimmten Paket wünschen, bewegen Sie den Mauszeiger über die QuickInfo.

     Um die Kapazitäten besser zu verstehen, die für das Essentials-Paket angezeigt werden, sollten Sie mit der Funktionsweise des Ladevorgangs vertraut sein. "Erfahren Sie mehr über das Laden des Essentials-Pakets".

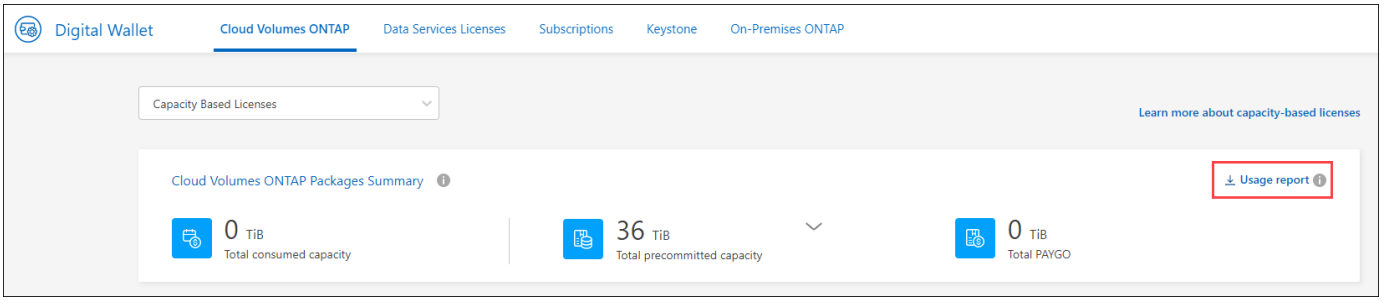
   - *Recommited Capacity* ist die von Ihnen bei NetApp erworbene lizenzierte Kapazität (BYOL oder Marketplace Contract).
     - *BYOL* zeigt die von Ihnen für diesen Pakettyp bei NetApp erworbene lizenzierte Kapazität an.
     - *Marketplace Contracts* zeigt die lizenzierte Kapazität an, die Sie mit einem Marketplace-Vertrag für diesen Pakettyp erworben haben.
   - *PAYGO* zeigt Ihnen die verbrauchte Kapazität nach Lizenzmodell.

     Hier ein Beispiel für ein Konto mit mehreren Lizenzierungspaketen:



Nutzungsberichte herunterladen

Account-Administratoren können vier Nutzungsberichte aus dem Digital Wallet von BlueXP herunterladen. Diese Nutzungsberichte enthalten Kapazitätsdetails zu Ihren Abonnements und geben an, wie Sie für die Ressourcen in Ihren Cloud Volumes ONTAP Abonnements in Rechnung gestellt werden. Die herunterladbaren Berichte erfassen Daten zu einem bestimmten Zeitpunkt und können problemlos mit anderen geteilt werden.



Die folgenden Berichte stehen zum Download zur Verfügung. Die angegebenen Kapazitätswerte werden in tib angezeigt.

- **High-Level-Nutzung**: Dieser Bericht zeigt Ihnen genau, was sich in der "Cloud Volumes ONTAP-Paketübersicht"-Karte in der digitalen Brieftasche befindet. Sie enthält folgende Informationen:
  - Insgesamt verbrauchte Kapazität
  - Gesamte vorab gebuchte Kapazität
  - Gesamte BYOL-Kapazität
  - Gesamtmarkt Verträge Kapazität
  - Gesamte PAYGO-Kapazität
- **Cloud Volumes ONTAP-Paketverwendung**: Dieser Bericht zeigt Ihnen genau, was sich auf den Paketkarten in der digitalen Brieftasche befindet. Es enthält die folgenden Informationen für jedes Paket außer dem optimierten I/O-Paket:
  - Insgesamt verbrauchte Kapazität
  - Gesamte vorab gebuchte Kapazität
  - Gesamte BYOL-Kapazität

    - Gesamtmarkt Verträge Kapazität
    - Gesamte PAYGO-Kapazität
- **Nutzung von Storage-VMs**: Dieser Bericht zeigt, wie die geladene Kapazität auf Cloud Volumes ONTAP Systeme und Storage Virtual Machines (SVMs) aufgeteilt wird. Diese Informationen sind auf keinem Bildschirm in der Digital Wallet verfügbar. Sie enthält folgende Informationen:
    - Arbeitsumgebungs-ID und -Name (wird als UUID angezeigt)
    - Cloud
    - NetApp Konto-ID
    - Konfiguration der Arbeitsumgebung
    - SVM-Name
    - Bereitgestellte Kapazität
    - Zusammenfassung der geladenen Kapazität
    - Abrechnungszeitraum für Marktplatz
    - Cloud Volumes ONTAP Paket oder Feature
    - Abonnementname des SaaS Marketplace wird berechnet
    - Abonnement-ID des SaaS Marketplace wird berechnet
    - Workload-Typ
- **Volumennutzung**: Dieser Bericht zeigt, wie die berechnete Kapazität nach Volumen in einer Arbeitsumgebung aufgeschlüsselt wird. Diese Informationen sind auf keinem Bildschirm in der Digital Wallet verfügbar. Sie enthält folgende Informationen:
    - Arbeitsumgebungs-ID und -Name (wird als UUID angezeigt)
    - SVN Name
    - Volume-ID
    - Volume-Typ
    - Auf Volume bereitgestellte Kapazität

FlexClone Volumes sind nicht in diesem Bericht enthalten, da für diese Volume-Typen keine Kosten anfallen.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Lassen Sie auf der Registerkarte **Cloud Volumes ONTAP Capacity Based Licenses** ausgewählt und klicken Sie auf **Nutzungsbericht**.

   Der Nutzungsbericht wird heruntergeladen.
3. Öffnen Sie die heruntergeladene Datei, um auf die Berichte zuzugreifen.

Fügen Sie gekaufte Lizenzen zu Ihrem Konto hinzu

Wenn Ihre erworbenen Lizenzen noch nicht in der Digital Wallet von BlueXP enthalten sind, müssen Sie BlueXP noch um die Lizenzen erweitern, damit die Kapazität auch für Cloud Volumes ONTAP nutzbar ist.

Was Sie benötigen

- Sie müssen BlueXP die Seriennummer der Lizenz oder der Lizenzdatei angeben.
- Wenn Sie die Seriennummer eingeben möchten, müssen Sie zunächst eingeben "Fügen Sie Ihr Konto für die NetApp Support Website zu BlueXP hinzu". Hierbei handelt es sich um das Konto für die NetApp Support Site, das befugt ist, auf die Seriennummer zuzugreifen.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Halten Sie auf der Registerkarte **Cloud Volumes ONTAP** die Option **kapazitätsbasierte Lizenzen** ausgewählt und klicken Sie auf **Lizenz hinzufügen**.
3. Geben Sie die Seriennummer für Ihre kapazitätsbasierte Lizenz ein, oder laden Sie die Lizenzdatei hoch.

   Wenn Sie eine Seriennummer eingegeben haben, müssen Sie auch das NetApp Support Site Konto auswählen, über das Sie Zugriff auf die Seriennummer haben.

4. Klicken Sie Auf **Lizenz Hinzufügen**.

Aktualisieren einer kapazitätsbasierten Lizenz

Wenn Sie zusätzliche Kapazität erworben oder die Laufzeit Ihrer Lizenz verlängert haben, aktualisiert BlueXP automatisch die Lizenz im Digital Wallet. Es gibt nichts, was Sie tun müssen.

Wenn Sie BlueXP jedoch an einem Standort bereitgestellt haben, der keinen Internetzugang hat, müssen Sie die Lizenz in BlueXP manuell aktualisieren.

Was Sie benötigen

Die Lizenzdatei (oder *Files* wenn Sie ein HA-Paar haben).

Weitere Informationen zum Abrufen einer Lizenzdatei finden Sie unter "Holen Sie sich eine Systemlizenzdatei".

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Klicken Sie auf der Registerkarte **Cloud Volumes ONTAP** auf das Aktionsmenü neben der Lizenz und wählen Sie **Lizenz aktualisieren**.
3. Laden Sie die Lizenzdatei hoch.
4. Klicken Sie Auf **Lizenz Hochladen**.

Ändern Sie die Lademethoden

Kapazitätsbasierte Lizenzierung ist in Form eines *package* erhältlich. Wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen, können Sie je nach Ihren Geschäftsanforderungen aus mehreren Lizenzierungspaketen wählen. Wenn sich Ihre Anforderungen ändern, nachdem Sie die Arbeitsumgebung erstellt haben, können Sie das Paket jederzeit ändern. Sie können z. B. vom Essentials-Paket zum Professional-Paket wechseln.

"Erfahren Sie mehr über kapazitätsbasierte Lizenzierungspakete".

Über diese Aufgabe

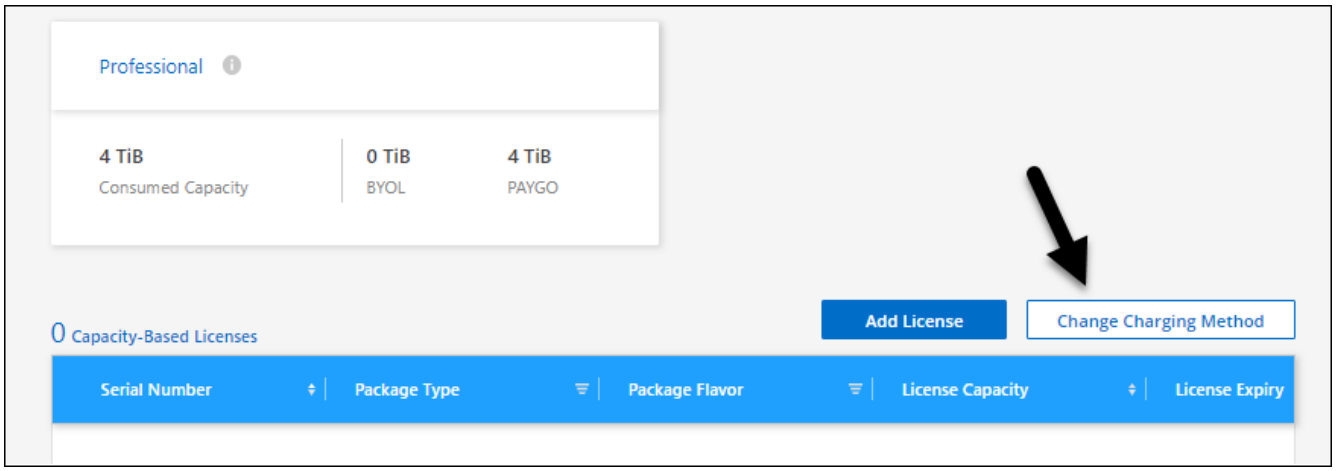
- Eine Änderung der Abrechnungsmethode hat keine Auswirkung darauf, ob die Abrechnung über eine von NetApp (BYOL) erworbene Lizenz oder über den Marketplace des Cloud-Providers (Pay-as-you-go) erfolgt.

BlueXP versucht immer zuerst, eine Lizenz zu berechnen. Wenn eine Lizenz nicht verfügbar ist, wird sie für ein Marketplace-Abonnement berechnet. Für das BYOL-Abonnement für Marketplace ist keine „Konvertierung“ erforderlich und umgekehrt.

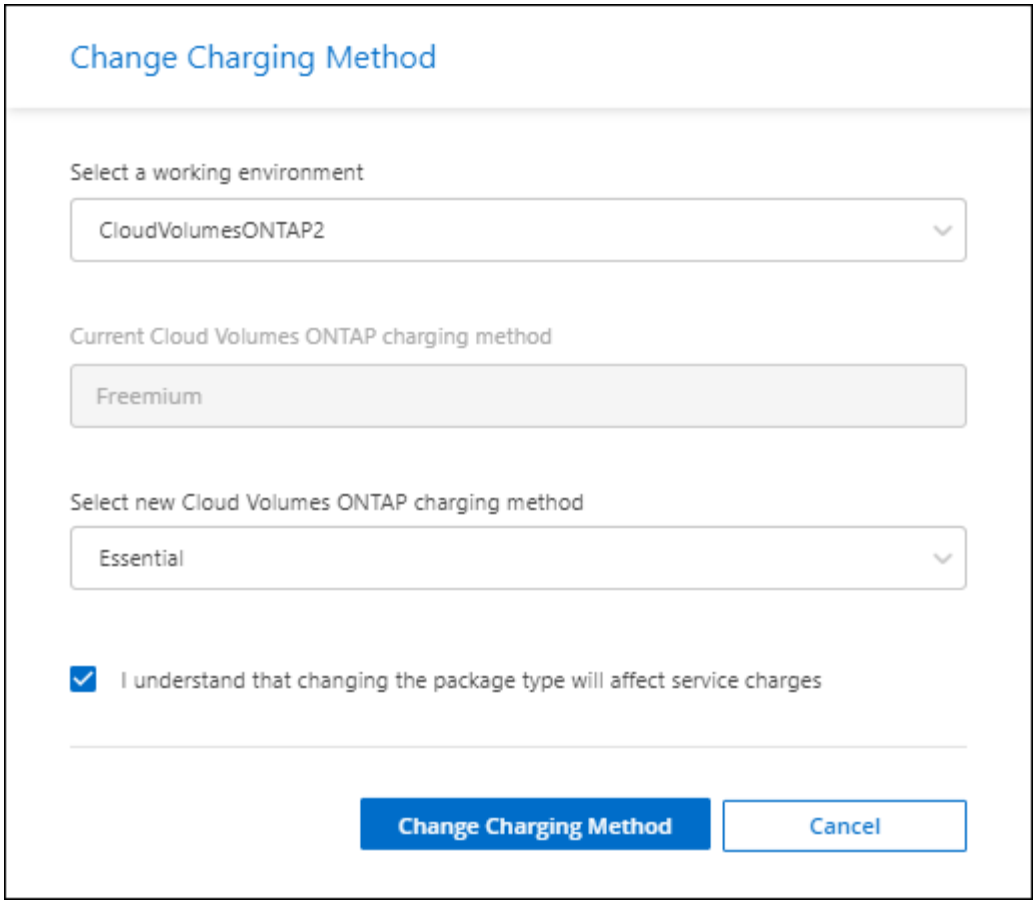
- Wenn Sie über ein privates Angebot oder einen Vertrag von Ihrem Cloud-Provider-Markt verfügen, wird eine Änderung auf eine Abrechnungsmethode, die nicht im Vertrag enthalten ist, zu einer Abrechnung für BYOL (bei dem Kauf einer Lizenz von NetApp) oder PAYGO führen.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Klicken Sie auf der Registerkarte **Cloud Volumes ONTAP** auf **Lademethode ändern**.



3. Wählen Sie eine Arbeitsumgebung aus, wählen Sie die neue Lademethode aus, und bestätigen Sie anschließend, dass sich eine Änderung des Paketyps auf Servicegebühren auswirkt.



4. Klicken Sie Auf **Lademethode Ändern**.

Ergebnis

BlueXP ändert die Lademethode des Cloud Volumes ONTAP-Systems.

Vielleicht ist Ihnen auch aufgefallen, dass das Digital Wallet von BlueXP die verbrauchte Kapazität für jeden Pakettyp aktualisiert, um die soeben vorgenommene Änderung zu berücksichtigen.

Entfernen einer kapazitätsbasierten Lizenz

Wenn eine kapazitätsbasierte Lizenz abgelaufen ist und nicht mehr verwendet wird, können Sie sie jederzeit entfernen.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Klicken Sie auf der Registerkarte **Cloud Volumes ONTAP** auf das Aktionsmenü neben der Lizenz und wählen Sie **Lizenz entfernen**.
3. Klicken Sie zur Bestätigung auf **Entfernen**.

Keystone Abonnements managen und

Managen Sie Ihre Keystone Abonnements über das Digital Wallet von BlueXP, indem Sie Abonnements für die Nutzung von Cloud Volumes ONTAP aktivieren und Änderungen der gebuchten Kapazität für die Service-Level Ihres Abonnements anfordern. Die Anforderung zusätzlicher Kapazität für ein Service-Level stellt mehr Storage für lokale

ONTAP Cluster oder für Cloud Volumes ONTAP Systeme bereit.

NetApp Keystone ist ein flexibler abonnementbasierter Pay-as-you-grow-Service. Kunden, die lieber auf Betriebskosten oder als auf Leasing setzen, profitieren von einer Hybrid-Cloud-Erfahrung.

"Weitere Informationen zu Keystone"

Autorisieren Sie Ihr Konto

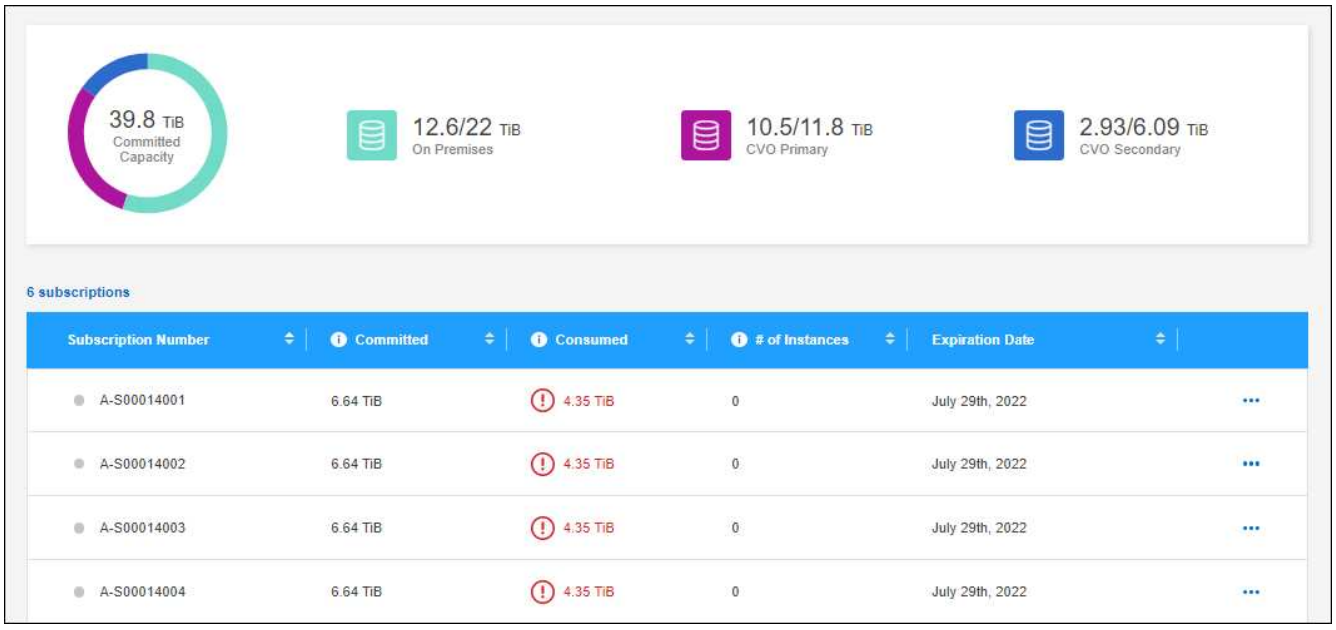
Bevor Sie Keystone Abonnements in BlueXP nutzen und managen können, müssen Sie zunächst NetApp kontaktieren, um Ihr BlueXP Benutzerkonto für Ihre Keystone Abonnements zu autorisieren.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie **Keystone**.
3. Wenn Sie die Seite **Willkommen bei NetApp Keystone** sehen, senden Sie eine E-Mail an die auf der Seite angegebene Adresse.

   Ein Vertreter von NetApp verarbeitet Ihre Anfrage, indem er Ihr Benutzerkonto für den Zugriff auf die Abonnements autorisiert.

4. Kehren Sie zum **Keystone Abonnement** zurück, um sich Ihre Abonnements anzusehen.

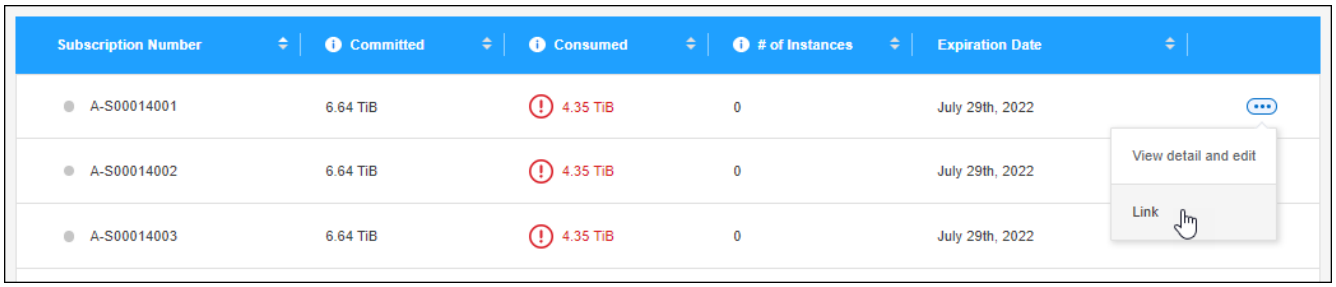


Ein Abonnement verknüpfen

Nachdem NetApp Ihr Konto autorisiert hat, können Sie Keystone Abonnements zur Verwendung mit Cloud Volumes ONTAP verknüpfen. Mit dieser Aktion können Benutzer das Abonnement als Lademethode für neue Cloud Volumes ONTAP-Systeme auswählen.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie **Keystone**.
3. Klicken Sie für das Abonnement, das Sie verknüpfen möchten, auf ••• Und wählen Sie **Link**.



Ergebnis

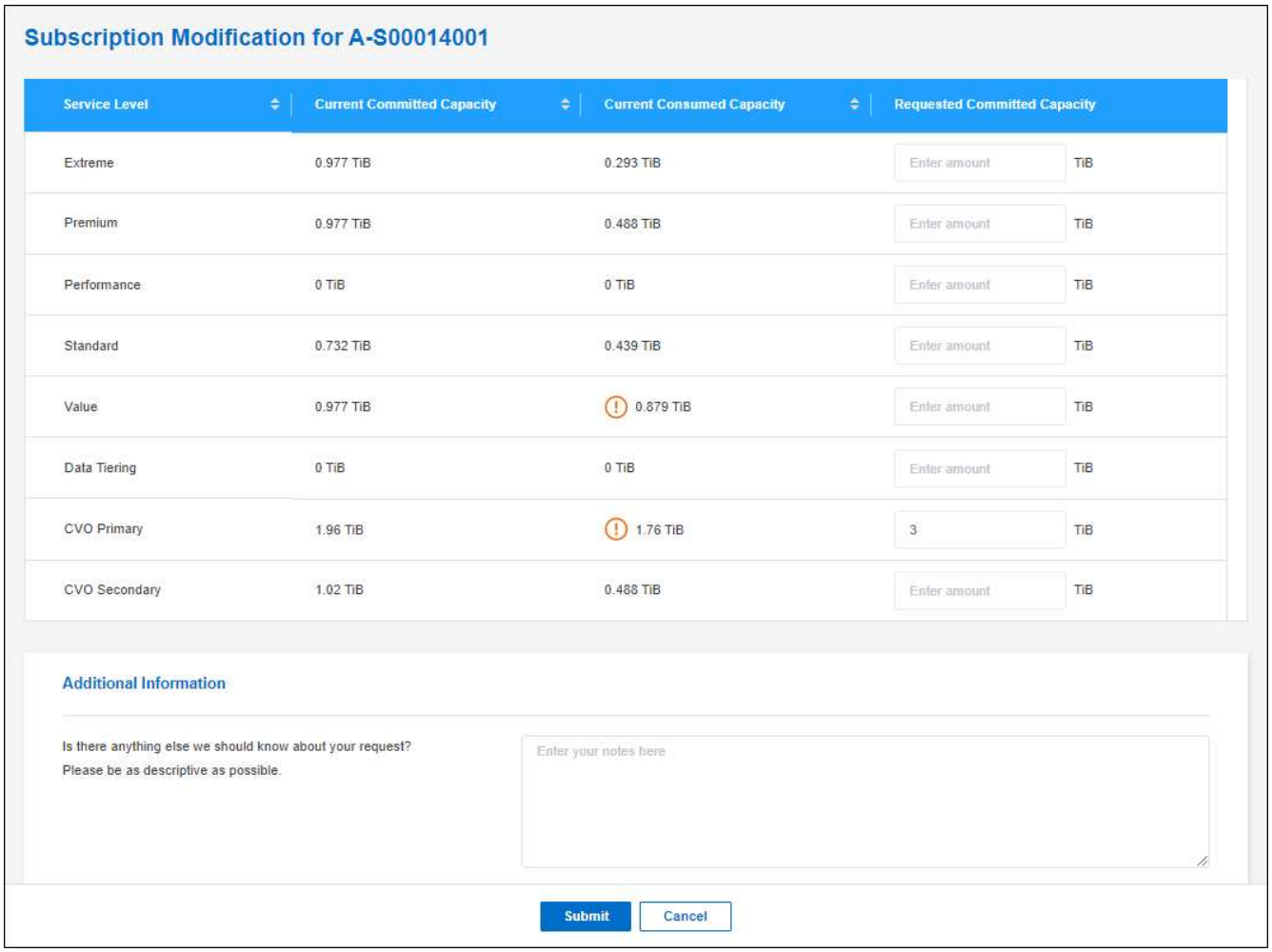
Das Abonnement ist nun mit Ihrem BlueXP-Konto verknüpft und kann bei der Erstellung einer Cloud Volumes ONTAP-Arbeitsumgebung ausgewählt werden.

Fordern Sie mehr oder weniger fest verplante Kapazität an

Wenn Sie die gebuchte Kapazität für die Service-Level Ihres Abonnements ändern möchten, können Sie direkt von BlueXP eine Anfrage an NetApp senden. Die Anforderung zusätzlicher Kapazität für ein Service-Level stellt mehr Storage für lokale Cluster oder Cloud Volumes ONTAP Systeme bereit.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie **Keystone**.
3. Klicken Sie für das Abonnement, das Sie an die Kapazität anpassen möchten, auf ••• Und wählen Sie **Details anzeigen und bearbeiten**.
4. Geben Sie die angeforderte engagierte Kapazität für ein oder mehrere Abonnements ein.



5. Scrollen Sie nach unten, geben Sie weitere Details für die Anfrage ein und klicken Sie dann auf **Absenden**.

Ergebnis

Ihre Anfrage erstellt ein Ticket im NetApp System zur Verarbeitung.

Überwachung der Nutzung

Über das Digital Advisor Dashboard von BlueXP können Sie die Nutzung von Keystone Abonnements überwachen und Berichte generieren.

"Erfahren Sie mehr über das Monitoring der Abonnementnutzung"

Aufheben der Verknüpfung eines Abonnements

Wenn Sie kein Keystone Abonnement mehr mit BlueXP nutzen möchten, können Sie die Verknüpfung zum Abonnement aufheben. Beachten Sie, dass Sie die Verknüpfung eines Abonnements, das nicht mit einem vorhandenen Cloud Volumes ONTAP-Abonnement verbunden ist, nur aufheben können.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie **Keystone**.
3. Klicken Sie für das Abonnement, das Sie aufheben möchten, auf ••• Und wählen Sie **Link aufheben**.

Ergebnis

Das Abonnement wird von Ihrem BlueXP-Konto getrennt und kann bei der Erstellung einer Cloud Volumes ONTAP-Arbeitsumgebung nicht mehr ausgewählt werden.

Management knotenbasierter Lizenzen

Managen Sie Node-basierte Lizenzen in der BlueXP Digital Wallet, um sicherzustellen, dass für jedes Cloud Volumes ONTAP System eine gültige Lizenz mit der erforderlichen Kapazität vorhanden ist.

Node-basierte Lizenzen sind das Lizenzmodell der vorherigen Generation (und für neue Kunden nicht verfügbar):

- Byol-Lizenzen, die von NetApp erworben wurden
- PAYGO-Abonnements (Pay-as-you-go) vom Markt Ihres Cloud-Providers

Mit der *BlueXP Digital Wallet* können Sie Lizenzen für Cloud Volumes ONTAP von einem einzigen Standort aus managen. Sie können neue Lizenzen hinzufügen und vorhandene Lizenzen aktualisieren.

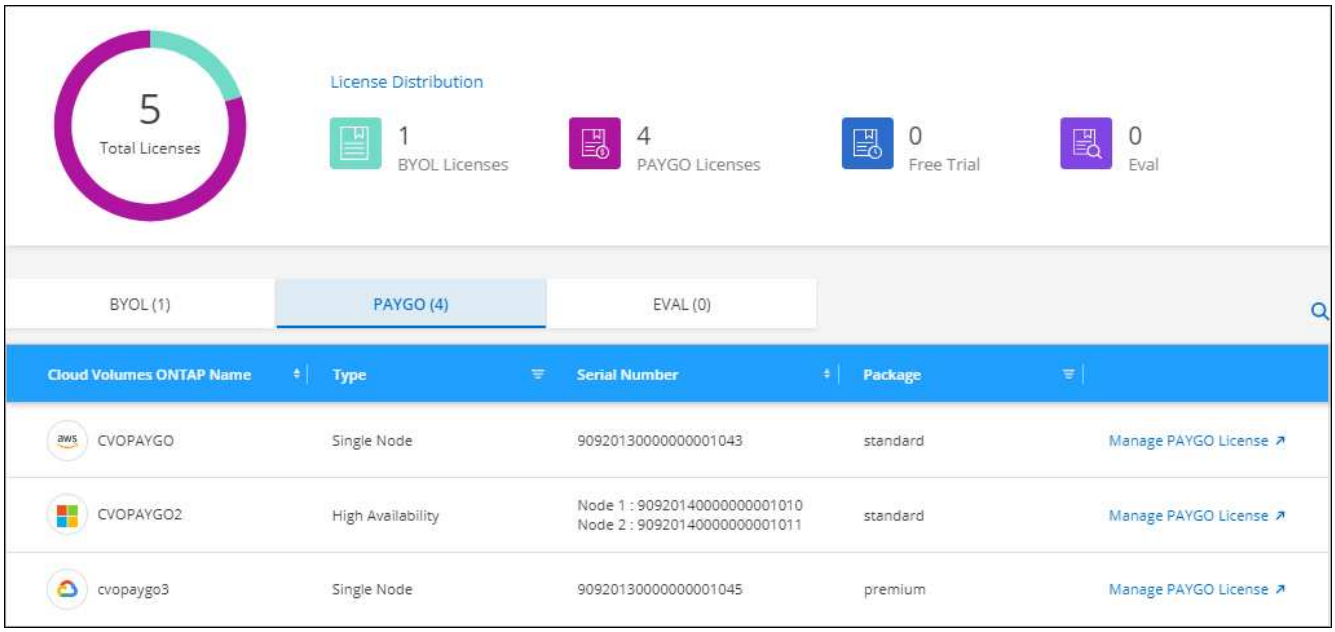
"Weitere Informationen zu Cloud Volumes ONTAP Lizenzen".

Managen von PAYGO-Lizenzen

Auf der BlueXP Digital Wallet-Seite können Sie Details zu jedem PAYGO Cloud Volumes ONTAP System einschließlich Seriennummer und PAYGO Lizenztyp einsehen.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie im Dropdown-Menü auf der Registerkarte **Cloud Volumes ONTAP** die Option **Node-basierte Lizenzen** aus.
3. Klicken Sie auf **PAYGO**.
4. Zeigen Sie Details zu den einzelnen PAYGO-Lizenzen in der Tabelle an.



5. Klicken Sie bei Bedarf auf **PAYGO-Lizenz verwalten**, um die PAYGO-Lizenz zu ändern oder den Instanztyp zu ändern.

Byol-Lizenzen managen

Managen Sie die Lizenzen, die Sie direkt bei NetApp erworben haben, indem Sie Systemlizenzen und zusätzliche Kapazitätslizenzen hinzufügen bzw. entfernen.

Fügen Sie nicht zugewiesene Lizenzen hinzu

Erweitern Sie das Digital Wallet von BlueXP um eine Node-basierte Lizenz, sodass Sie bei der Erstellung eines neuen Cloud Volumes ONTAP Systems die Lizenz auswählen können. Die Digital Wallet identifiziert diese Lizenzen als *unassigned*.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie im Dropdown-Menü auf der Registerkarte **Cloud Volumes ONTAP** die Option **Node-basierte Lizenzen** aus.
3. Klicken Sie Auf **Nicht Zugewiesen**.
4. Klicken Sie Auf **Nicht Zugewiesene Lizenzen Hinzufügen**.
5. Geben Sie die Seriennummer der Lizenz ein oder laden Sie die Lizenzdatei hoch.

   Wenn Sie die Lizenzdatei noch nicht haben, lesen Sie den Abschnitt weiter unten.

6. Klicken Sie Auf **Lizenz Hinzufügen**.

Ergebnis

BlueXP erweitert das Digital Wallet um die Lizenz. Die Lizenz wird erst dann als nicht zugewiesen identifiziert, wenn Sie sie einem neuen Cloud Volumes ONTAP-System zuordnen. Danach wird die Lizenz auf die Registerkarte **BYOL** im Digital Wallet verschoben.

Nicht zugewiesene knotenbasierte Exchange-Lizenzen

Wenn Sie eine nicht zugewiesene Node-basierte Lizenz für Cloud Volumes ONTAP verwenden, können Sie die Lizenz austauschen. Konvertieren Sie sie in eine BlueXP Backup- und Recovery-Lizenz, eine BlueXP Klassifizierungslizenz oder eine BlueXP Tiering Lizenz.

Beim Austausch der Lizenz wird die Cloud Volumes ONTAP-Lizenz zurückgerufen und eine Dollaräquivalente Lizenz für den Service erstellt:

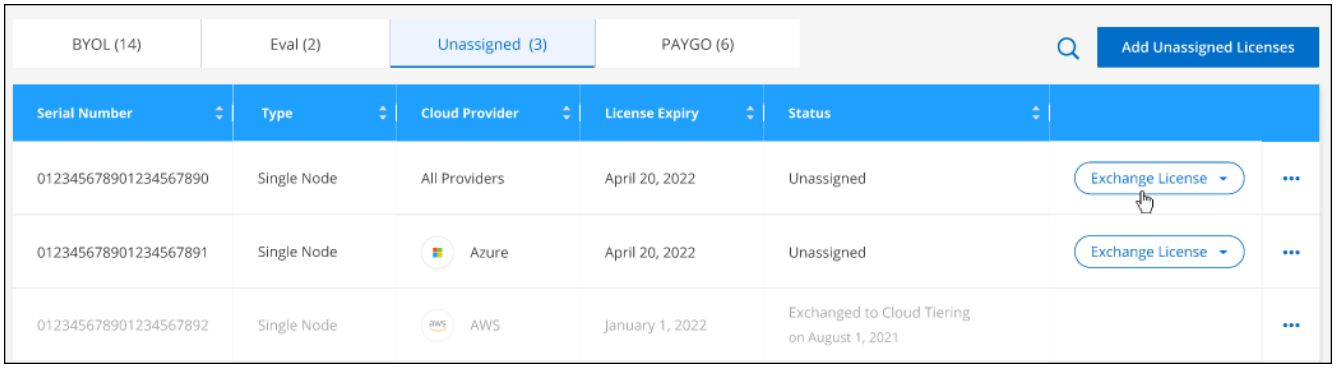
- Die Lizenzierung für ein Cloud Volumes ONTAP HA-Paar wird in eine 51 tib Datenservice-Lizenz umgewandelt
- Die Lizenzierung für einen Cloud Volumes ONTAP-Single-Node wird in eine 32 tib Datenservice-Lizenz umgewandelt

Die konvertierte Lizenz hat das gleiche Ablaufdatum wie die Cloud Volumes ONTAP-Lizenz.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie im Dropdown-Menü auf der Registerkarte **Cloud Volumes ONTAP** die Option **Node-basierte Lizenzen** aus.

3. Klicken Sie Auf **Nicht Zugewiesen**.
4. Klicken Sie Auf **Exchange-Lizenz**.



5. Wählen Sie den Dienst aus, mit dem Sie die Lizenz austauschen möchten.
6. Wenn Sie dazu aufgefordert werden, wählen Sie eine zusätzliche Lizenz für das HA-Paar aus.
7. Lesen Sie die gesetzliche Einwilligung und klicken Sie auf **Zustimmen**.

Ergebnis

BlueXP konvertiert die nicht zugewiesene Lizenz in den von Ihnen ausgewählten Dienst. Sie können die neue Lizenz auf der Registerkarte **Datendienste Lizenzen** anzeigen.

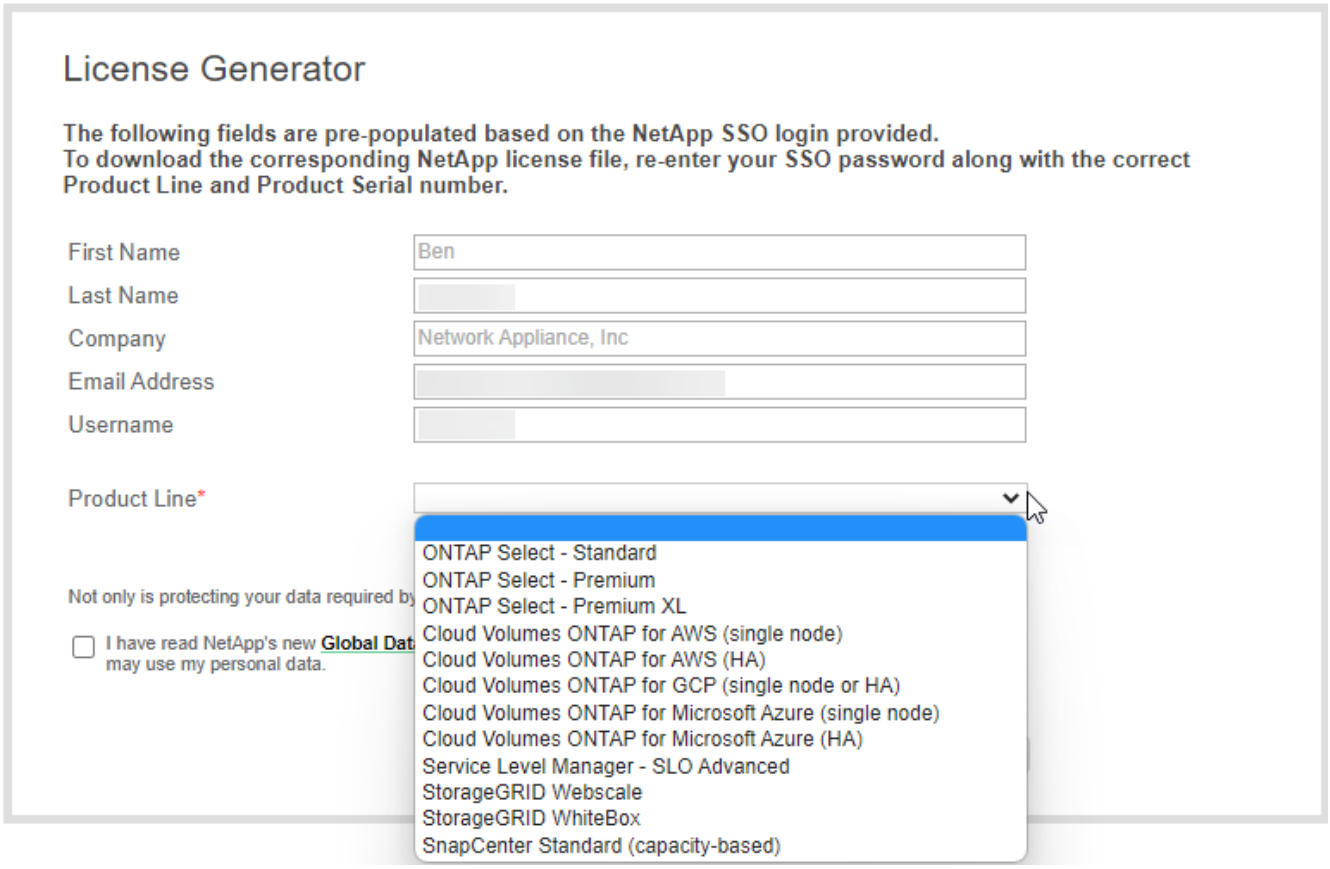
Holen Sie sich eine Systemlizenzdatei

In den meisten Fällen kann BlueXP 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.

Aktualisieren einer Systemlizenz

Wenn Sie ein BYOL-Abonnement verlängern, indem Sie sich an einen NetApp Ansprechpartner wenden, erhält BlueXP automatisch die neue Lizenz von NetApp und installiert sie auf dem Cloud Volumes ONTAP System.

Wenn BlueXP nicht über die sichere Internetverbindung auf die Lizenzdatei zugreifen kann, können Sie die Datei selbst beziehen und die Datei anschließend manuell auf BlueXP hochladen.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie im Dropdown-Menü auf der Registerkarte **Cloud Volumes ONTAP** die Option **Node-basierte Lizenzen** aus.
3. Erweitern Sie auf der Registerkarte **BYOL** die Details für ein Cloud Volumes ONTAP-System.
4. Klicken Sie auf das Aktionsmenü neben der Systemlizenz und wählen Sie **Lizenz aktualisieren**.
5. Laden Sie die Lizenzdatei (oder Dateien, wenn Sie ein HA-Paar haben) hoch.
6. Klicken Sie Auf **Lizenz Aktualisieren**.

Ergebnis

BlueXP aktualisiert die Lizenz auf dem Cloud Volumes ONTAP-System.

Management von zusätzlichen Kapazitätslizenzen

Sie können zusätzliche Kapazitätslizenzen für ein Cloud Volumes ONTAP BYOL-System erwerben, um mehr als 368 tib Kapazität zuzuweisen, die mit einer BYOL-Systemlizenz bereitgestellt wird. Beispielsweise können Sie eine zusätzliche Lizenzkapazität erwerben, um Cloud Volumes ONTAP bis zu 736 tib Kapazität zuzuweisen. Alternativ können Sie drei zusätzliche Kapazitätslizenzen erwerben, um bis zu 1.4 PiB zu erhalten.

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

Fügen Sie Kapazitätslizenzen hinzu

Erwerben Sie eine Lizenz für zusätzliche Kapazität, indem Sie uns über das Chat-Symbol rechts unten von BlueXP kontaktieren. Nach dem Kauf der Lizenz können Sie sie auf ein Cloud Volumes ONTAP System anwenden.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie im Dropdown-Menü auf der Registerkarte **Cloud Volumes ONTAP** die Option **Node-basierte Lizenzen** aus.
3. Erweitern Sie auf der Registerkarte **BYOL** die Details für ein Cloud Volumes ONTAP-System.
4. Klicken Sie Auf **Kapazitätslizenz Hinzufügen**.
5. Geben Sie die Seriennummer ein, oder laden Sie die Lizenzdatei (oder Dateien, wenn Sie ein HA-Paar haben) hoch.
6. Klicken Sie Auf **Kapazitätslizenz Hinzufügen**.

Kapazitätslizenzen aktualisieren

Wenn Sie die Laufzeit einer zusätzlichen Kapazitätslizenz verlängern, müssen Sie die Lizenz in BlueXP aktualisieren.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie im Dropdown-Menü auf der Registerkarte **Cloud Volumes ONTAP** die Option **Node-basierte Lizenzen** aus.
3. Erweitern Sie auf der Registerkarte **BYOL** die Details für ein Cloud Volumes ONTAP-System.
4. Klicken Sie auf das Aktionsmenü neben der Kapazitätslizenz und wählen Sie **Lizenz aktualisieren**.
5. Laden Sie die Lizenzdatei (oder Dateien, wenn Sie ein HA-Paar haben) hoch.
6. Klicken Sie Auf **Lizenz Aktualisieren**.

Kapazitätslizenzen entfernen

Wenn eine Lizenz für zusätzliche Kapazität abgelaufen ist und nicht mehr verwendet wird, können Sie sie jederzeit entfernen.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie im Dropdown-Menü auf der Registerkarte **Cloud Volumes ONTAP** die Option **Node-basierte**

Lizenzen aus.

3. Erweitern Sie auf der Registerkarte **BYOL** die Details für ein Cloud Volumes ONTAP-System.
4. Klicken Sie auf das Aktionsmenü neben der Kapazitätslizenz und wählen Sie **Lizenz entfernen**.
5. Klicken Sie Auf **Entfernen**.

Konvertieren einer Eval-Lizenz in einen BYOL-Modell

Eine Evaluierungslizenz ist 30 Tage lang gut. Für ein in-Place-Upgrade kann eine neue BYOL-Lizenz auf die Evaluierungslizenz angewendet werden.

Wenn Sie eine Eval-Lizenz in einen Byol konvertieren, startet BlueXP das Cloud Volumes ONTAP-System neu.

- Bei einem Single-Node-System führt der Neustart zu I/O-Unterbrechungen während des Neubootens.
- Bei einem HA-Paar initiiert der Neustart Takeover und Giveback, um den I/O-Vorgängen weiterhin an die Clients bereitzustellen.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie im Dropdown-Menü auf der Registerkarte **Cloud Volumes ONTAP** die Option **Node-basierte Lizenzen** aus.
3. Klicken Sie Auf **Eval**.
4. Klicken Sie in der Tabelle auf **in Byol-Lizenz konvertieren** für ein Cloud Volumes ONTAP-System.
5. Geben Sie die Seriennummer ein, oder laden Sie die Lizenzdatei hoch.
6. Klicken Sie Auf **Lizenz Konvertieren**.

Ergebnis

BlueXP startet den Konvertierungsprozess. Cloud Volumes ONTAP wird im Rahmen dieses Prozesses automatisch neu gestartet. Wenn es gesichert ist, werden die Lizenzinformationen die neue Lizenz enthalten.

Wechseln Sie zwischen PAYGO und BYOL

Das Konvertieren eines Systems von der PAYGO-Lizenzierung pro Node in BYOL-by-Node-Lizenzierung (und umgekehrt) wird nicht unterstützt. Um zwischen einem nutzungsbasierten Abonnement und einem BYOL-Abonnement zu wechseln, müssen Sie ein neues System implementieren und Daten vom vorhandenen System auf das neue System replizieren.

Schritte

1. Erstellen Sie eine neue Cloud Volumes ONTAP Arbeitsumgebung.
2. Richten Sie für jedes zu replizierende Volume eine einmalige Datenreplizierung zwischen den Systemen ein.

   "Erfahren Sie, wie Daten zwischen Systemen repliziert werden"

3. Beenden Sie das Cloud Volumes ONTAP System, das Sie nicht mehr benötigen, indem Sie die ursprüngliche Arbeitsumgebung löschen .

   "Erfahren Sie, wie Sie eine Cloud Volumes ONTAP-Arbeitsumgebung löschen".

Volume- und LUN-Administration

FlexVol Volumes erstellen

Falls Sie nach dem Start des Cloud Volumes ONTAP-Systems mehr Speicherplatz benötigen, können Sie aus BlueXP neue FlexVol Volumes für NFS, CIFS oder iSCSI erstellen.

BlueXP bietet verschiedene Möglichkeiten zur Erstellung eines neuen Volumes:

- Geben Sie Details für ein neues Volume an, und BlueXP kann die zugrunde liegenden Datenaggregate für Sie verarbeiten. Weitere Informationen .
- Erstellen Sie ein Volume auf einem Datenaggregat Ihrer Wahl. Weitere Informationen .
- Erstellung eines Volumes auf dem zweiten Node in einer HA-Konfiguration Weitere Informationen .

Bevor Sie beginnen

Ein paar Anmerkungen zur Volume-Bereitstellung:

- Wenn Sie ein iSCSI-Volume erstellen, erstellt BlueXP 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.
- 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".
- Wenn Ihre Cloud Volumes ONTAP Konfiguration die Elastic Volumes Funktion von Amazon EBS unterstützt, könnten Sie dies möglicherweise tun "Erfahren Sie mehr darüber, was bei der Erstellung eines Volumes passiert".

Erstellen eines Volumes

Die häufigste Methode zur Erstellung eines Volumes besteht darin, den erforderlichen Volume-Typ anzugeben, und BlueXP übernimmt dann die Festplattenzuordnung für Sie. Aber Sie haben auch die Möglichkeit, das spezifische Aggregat zu wählen, auf dem Sie das Volume erstellen möchten.

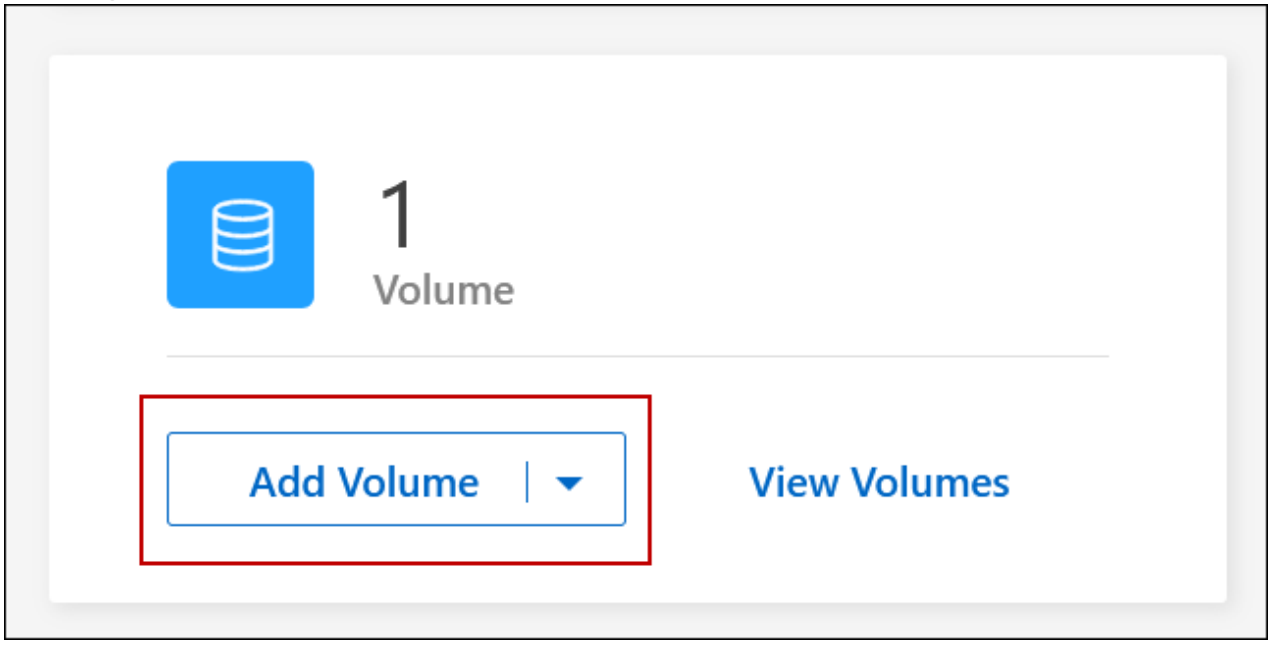
Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Doppelklicken Sie auf der Seite Arbeitsfläche auf den Namen des Cloud Volumes ONTAP-Systems, auf dem Sie ein FlexVol-Volume bereitstellen möchten.
3. Erstellen Sie ein neues Volume, indem Sie BlueXP die Festplattenzuordnung für Sie übernehmen oder ein bestimmtes Aggregat für das Volume auswählen.

   Die Auswahl eines bestimmten Aggregats ist nur dann empfehlenswert, wenn Sie Verständnis der Datenaggregate auf Ihrem Cloud Volumes ONTAP System haben.

Alle Aggregate

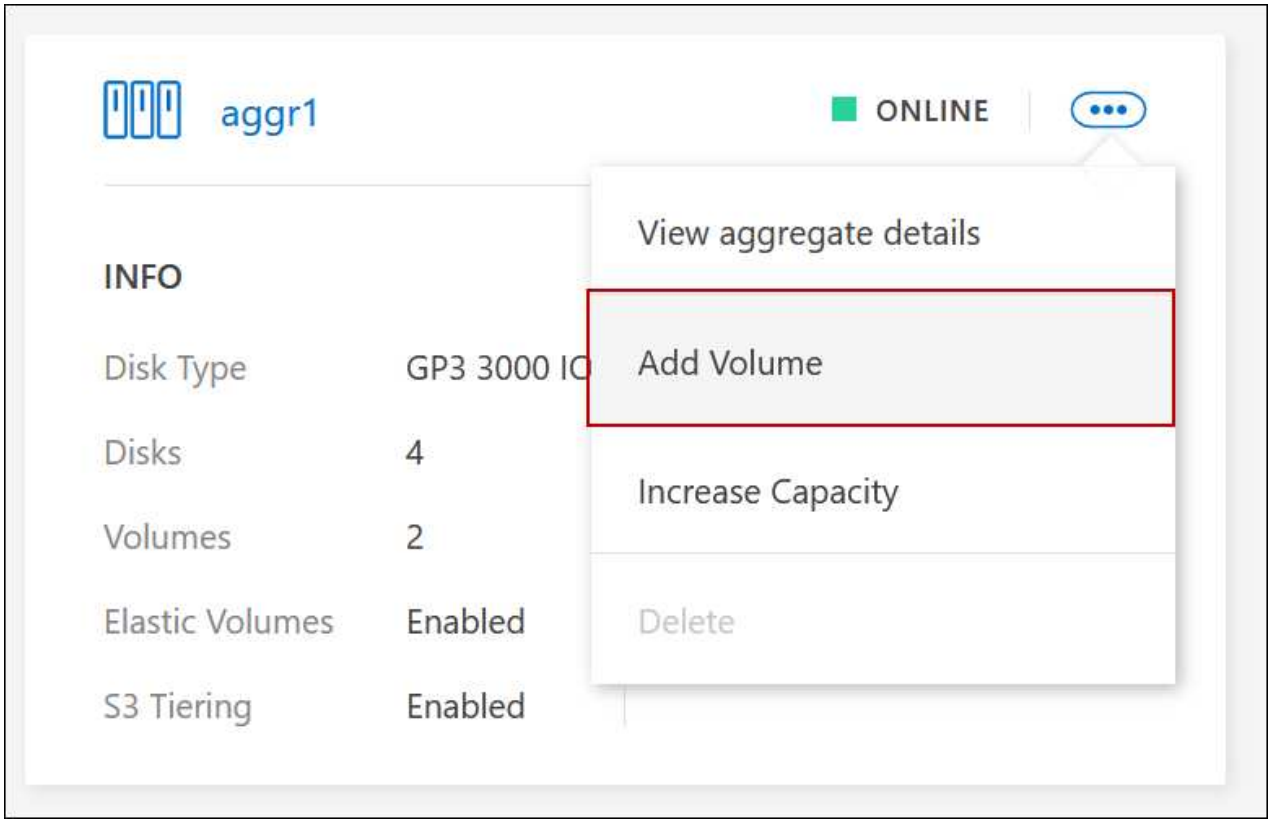
Navigieren Sie auf der Registerkarte Übersicht zur Kachel Volumes, und klicken Sie auf **Volume hinzufügen**.



Spezifische Aggregate

Navigieren Sie auf der Registerkarte Aggregate zur gewünschten Aggregat-Kachel. Klicken Sie auf das Menüsymbol und dann auf **Volume hinzufügen**

.



4. Befolgen Sie die Schritte im Assistenten, um das Volume zu erstellen.

a. **Details, Schutz und Tags**: Geben Sie grundlegende Details zum Volume ein und wählen Sie eine Snapshot-Richtlinie aus.

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

Feld	Beschreibung
Volume-Name	Der identifizierbare Name, den Sie für das neue Volume eingeben können.
Volume-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.
Storage-VM (SVM)	Eine Storage VM ist eine Virtual Machine, die in ONTAP ausgeführt wird und Ihren Kunden Storage und Datenservices zur Verfügung stellt. Sie können dies als SVM oder vServer wissen. Cloud Volumes ONTAP ist standardmäßig mit einer Storage-VM konfiguriert, aber einige Konfigurationen unterstützen zusätzliche Storage-VMs. Sie können die Storage-VM für das neue Volume angeben.
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.

b. **Protokoll**: Wählen Sie ein Protokoll für das Volume (NFS, CIFS oder iSCSI) und geben Sie dann die erforderlichen Informationen.

   Wenn Sie CIFS auswählen und ein Server nicht eingerichtet ist, werden Sie von BlueXP aufgefordert, eine CIFS-Verbindung einzurichten, nachdem Sie auf **Weiter** klicken.

   "Hier erhalten Sie Informationen zu den unterstützten Client-Protokollen und -Versionen".

   In den folgenden Abschnitten werden die Felder beschrieben, für die Sie ggf. Hilfestellung benötigen. Die Beschreibungen sind nach Protokoll geordnet.

NFS

Zugriffssteuerung

Wählen Sie eine benutzerdefinierte Exportrichtlinie aus, um das Volume den Clients zur Verfügung zu stellen.

Exportrichtlinie

Definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt BlueXP einen Wert ein, der Zugriff auf alle Instanzen im Subnetz bietet.

CIFS

Berechtigungen und Benutzer/Gruppen

Ermöglicht Ihnen, die Zugriffsebene für eine SMB-Freigabe für Benutzer und Gruppen (auch Zugriffssteuerungslisten oder ACLs) zu steuern. Sie können lokale oder domänenbasierte Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Windows-Benutzernamen für die Domäne angeben, müssen Sie die Domäne des Benutzers mit dem Format Domäne\Benutzername einschließen.

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.

Wenn Sie Google Managed Active Directory konfigurieren, kann standardmäßig mit der IP-Adresse 169.254.169.254 auf AD zugegriffen werden.

Active Directory-Domäne, der Sie beitreten möchten

Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.

Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind

Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.

CIFS-Server-BIOS-Name

Ein CIFS-Servername, der in der AD-Domain eindeutig ist.

Organisationseinheit

Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers.

- Um von AWS verwaltete Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in diesem Feld **OU=Computers,OU=corp** ein.
- Um Azure AD-Domänendienste als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in diesem Feld **OU=AADDC-Computer** oder **OU=AADDC-Benutzer** ein.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"^]
- Um von Google verwaltete Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in diesem Feld **OU=Computer,OU=Cloud** ein.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-

objects#organizational_units["Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD"^]

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 "BlueXP Automation Dokumentation" Entsprechende Details.

Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Er ist nicht konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

ISCSI

LUN

ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Wenn Sie ein iSCSI-Volume erstellen, erstellt BlueXP automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so dass es keine Verwaltung beteiligt ist. Nachdem Sie das Volume erstellt haben, "Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen".

Initiatorgruppe

Initiatorgruppen geben an, welche Hosts auf angegebene LUNs im Storage-System zugreifen können

Host-Initiator (IQN)

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.

a. **Festplattentyp**: Wählen Sie einen zugrunde liegenden Disk-Typ für das Volumen basierend auf Ihren Leistungsanforderungen und Kostenanforderungen.
   - "Dimensionierung Ihres Systems in AWS"
     - "Dimensionierung Ihres Systems in Azure"
     - "Dimensionierung Ihres Systems in Google Cloud"

5. **Nutzungsprofil & Tiering Policy**: Wählen Sie aus, ob Sie Funktionen für die Speichereffizienz auf dem Volume aktivieren oder deaktivieren und dann ein auswählen "Volume Tiering-Richtlinie".

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

6. **Review**: Überprüfen Sie die Details über die Lautstärke und klicken Sie dann auf **Hinzufügen**.

Ergebnis

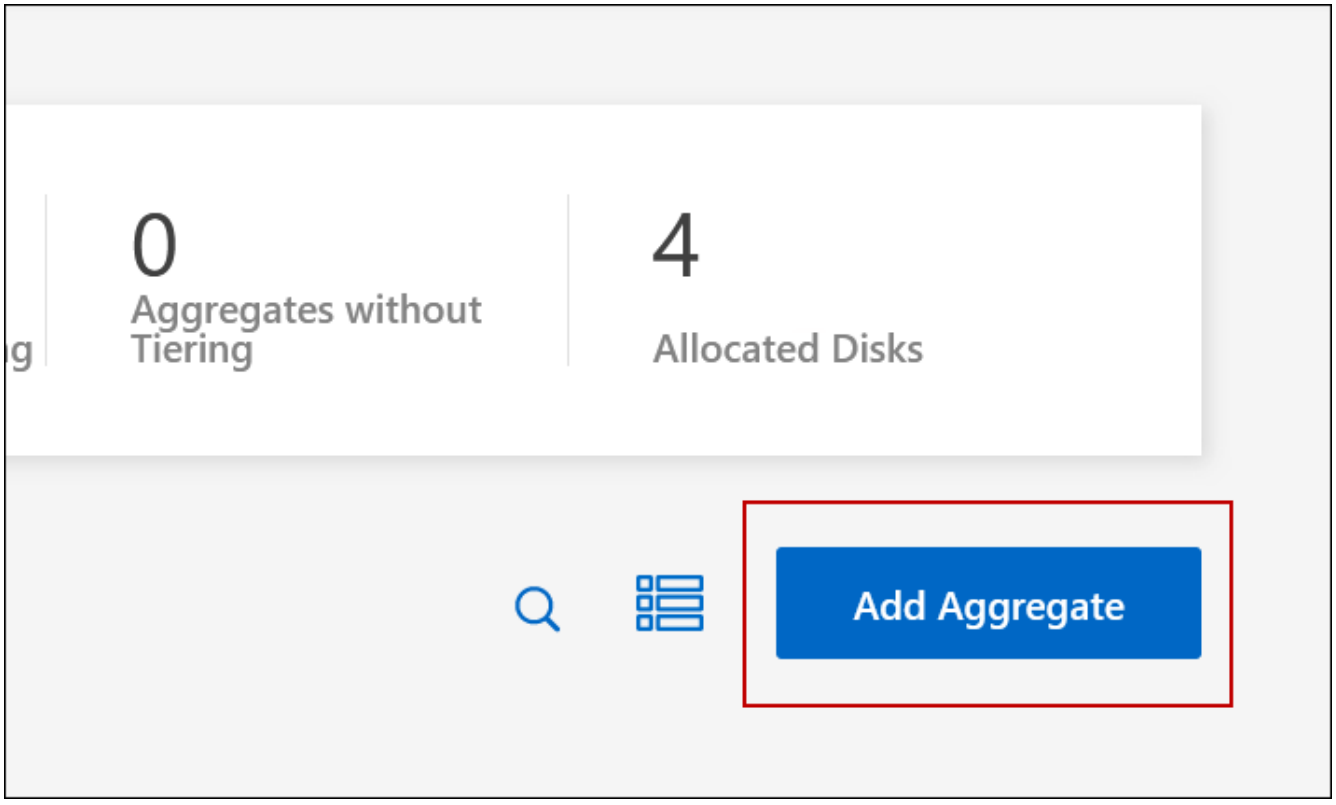
BlueXP erstellt das Volume auf dem Cloud Volumes ONTAP System.

Erstellung eines Volumes auf dem zweiten Node in einer HA-Konfiguration

Standardmäßig erstellt BlueXP Volumes auf dem ersten Knoten 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. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Doppelklicken Sie auf der Übersichtsseite auf den Namen der Cloud Volumes ONTAP Arbeitsumgebung, in der Sie Aggregate verwalten möchten.
3. Klicken Sie auf der Registerkarte Aggregate auf **Add Aggregate**.
4. Erstellen Sie im *Add Aggregate* -Bildschirm das Aggregat.



5. Wählen Sie für Home Node den zweiten Node im HA-Paar aus.

6. Nachdem BlueXP das Aggregat erstellt hat, wählen Sie es aus und klicken Sie dann auf **Create Volume**.
7. Geben Sie Details für den neuen Volume ein und klicken Sie dann auf **Erstellen**.

Ergebnis

BlueXP erstellt das Volume auf dem zweiten Knoten im HA-Paar.

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.

Nach der Erstellung eines Volumes

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.

Management vorhandener Volumes

Mit BlueXP können Sie Volumes und CIFS-Server verwalten. Außerdem werden Sie aufgefordert, Volumes zu verschieben, um Kapazitätsprobleme zu vermeiden.

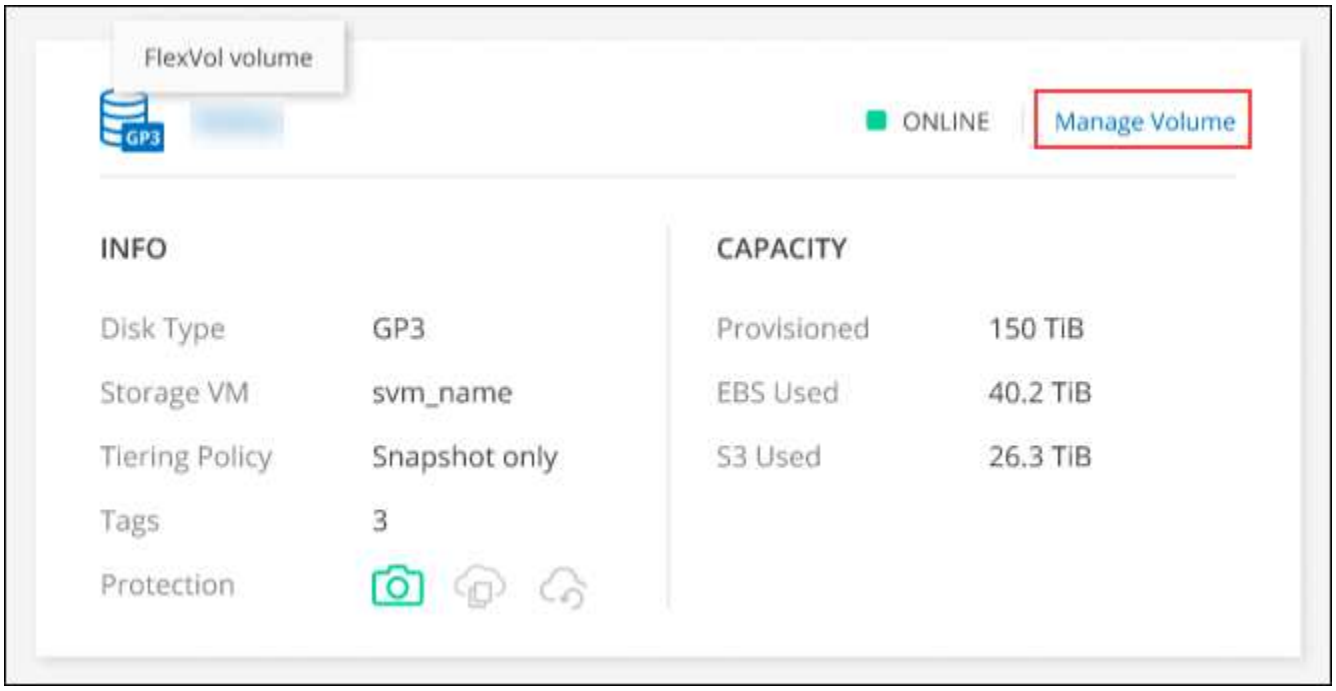
Sie können Volumes in der BlueXP Standard View oder Advanced View managen. Die Standardansicht bietet eine begrenzte Auswahl an Optionen zum Ändern der Volumes. Die erweiterte Ansicht bietet ein erweitertes Management, wie Klonen, Ändern der Größe, Ändern von Einstellungen für Ransomware-Schutz, Analyse, Schutz und Aktivitätsverfolgung und Verschieben von Volumes über Tiers hinweg. Siehe "Cloud Volumes ONTAP mit der erweiterten Ansicht verwalten".

Volumes managen

Mit der Standardansicht von BlueXP können Sie Volumes entsprechend Ihren Storage-Anforderungen managen. Sie können Volumes anzeigen, bearbeiten, klonen, wiederherstellen und löschen.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Doppelklicken Sie auf der Leinwand-Seite auf die Cloud Volumes ONTAP-Arbeitsumgebung, auf der Sie Volumes verwalten möchten.
3. Klicken Sie in der Arbeitsumgebung auf die Registerkarte **Volumes**.



4. Navigieren Sie auf der Registerkarte Volumes zum gewünschten Volume-Titel, und klicken Sie dann auf **Volume verwalten**, um auf das rechte Bedienfeld Volumes verwalten zuzugreifen.

Aufgabe	Aktion
Anzeigen von Informationen zu einem Volume	Klicken Sie unter Volume Actions im Bereich Manage Volumes auf **View Volume Details**.
Rufen Sie den NFS-Mount-Befehl ab	a. Klicken Sie unter Volume Actions im Fenster Manage Volumes auf **Mount Command**. b. Klicken Sie Auf **Kopieren**.
Klonen Sie ein Volume	a. Klicken Sie unter Volume Actions im Bereich Manage Volumes auf **Clone the Volume**. 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".

Aufgabe	Aktion
Bearbeiten eines Volumes (nur Volumes mit Lese-/Schreibzugriff)	a. Klicken Sie unter Volume Actions im Bereich Manage Volumes auf **Edit Volume settings** b. Ändern Sie die Snapshot-Richtlinie des Volumes, die NFS-Protokollversion, die NFS-Zugriffssteuerungsliste (Exportrichtlinie) oder die Freigabeberechtigungen, und klicken Sie dann auf **Apply**. Wenn Sie benutzerdefinierte Snapshot-Richtlinien benötigen, können Sie diese mit System Manager erstellen.
Löschen Sie ein Volume	a. Klicken Sie unter Volume Actions im Bereich Manage Volumes auf **Delete the Volume**. b. Geben Sie im Fenster Volume löschen den Namen des Volumes ein, das Sie löschen möchten. c. Klicken Sie zur Bestätigung erneut auf **Löschen**.
Erstellen Sie bei Bedarf eine Snapshot Kopie	a. Klicken Sie im Bereich Volumes verwalten unter Schutzaktionen auf **Snapshot-Kopie erstellen**. b. Ändern Sie ggf. den Namen und klicken Sie dann auf **Erstellen**.
Wiederherstellen von Daten aus einer Snapshot Kopie auf einem neuen Volume	a. Klicken Sie im Bereich Volumes verwalten unter Schutzaktionen auf **aus Snapshot-Kopie wiederherstellen**. b. Wählen Sie eine Snapshot Kopie aus, geben Sie einen Namen für das neue Volume ein und klicken Sie dann auf **Wiederherstellen**.
Ändern Sie den zugrunde liegenden Festplattentyp	a. Klicken Sie unter Erweiterte Aktionen im Bereich Volumes verwalten auf **Datenträgertyp ändern**. b. Wählen Sie den Laufwerkstyp aus und klicken Sie dann auf **Ändern**. BlueXP verschiebt das Volume in ein vorhandenes Aggregat, das den ausgewählten Festplattentyp nutzt oder ein neues Aggregat für das Volume erstellt.
Ändern Sie die Tiering Policy	a. Klicken Sie unter Erweiterte Aktionen im Bereich Volumes verwalten auf **Tiering-Richtlinie ändern**. b. Wählen Sie eine andere Richtlinie aus und klicken Sie auf **Ändern**. BlueXP verschiebt das Volume in ein vorhandenes Aggregat, das den ausgewählten Festplattentyp mit Tiering nutzt, oder erstellt ein neues Aggregat für das Volume.

Aufgabe	Aktion
Löschen Sie ein Volume	a. Wählen Sie ein Volume aus, und klicken Sie dann auf **Löschen**. b. Geben Sie den Namen des Volumes in das Dialogfeld ein. c. Klicken Sie zur Bestätigung erneut auf **Löschen**.

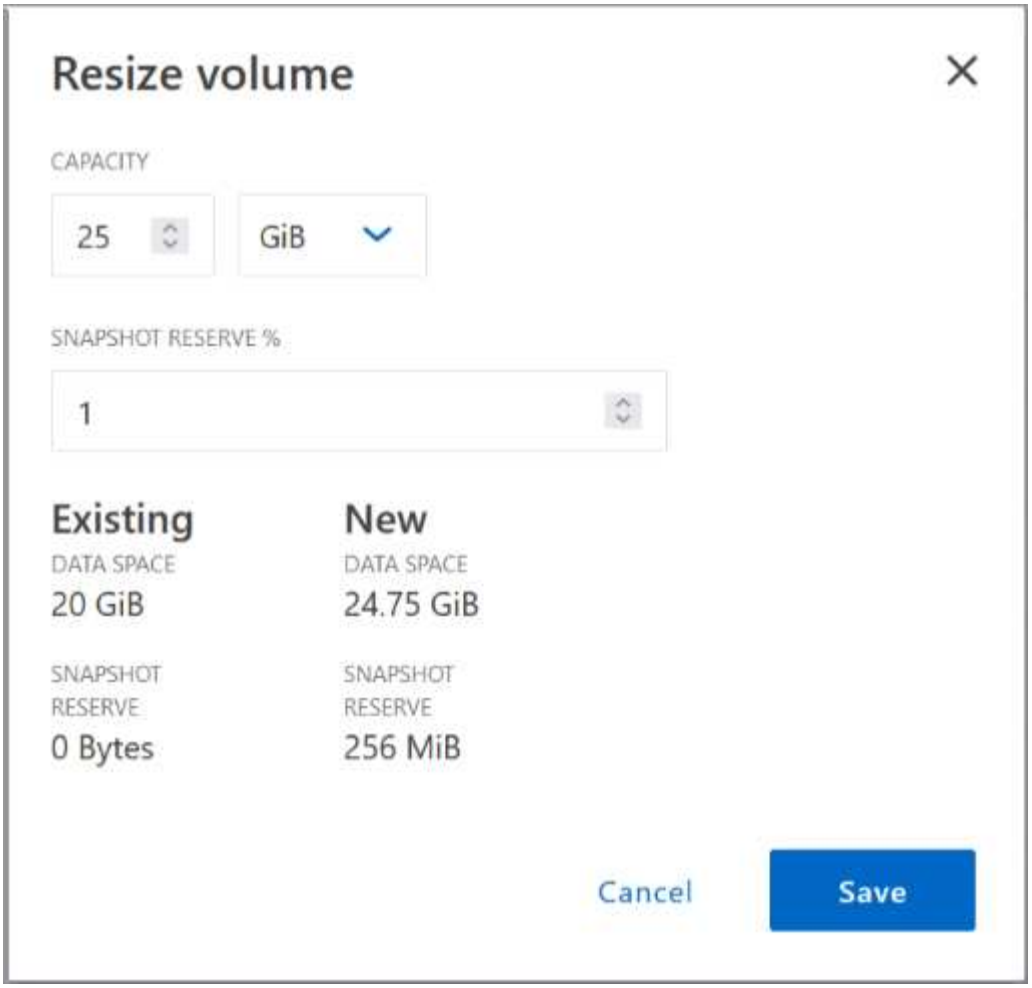
Die Größe eines Volumes ändern

Standardmäßig wird ein Volume automatisch auf eine Maximalgröße erweitert, wenn es sich um keinen Speicherplatz handelt. Der Standardwert ist 1,000. Das bedeutet, dass das Volume auf das 11-fache seiner Größe anwachsen kann. Dieser Wert kann in den Einstellungen des Connectors konfiguriert werden.

Wenn Sie die Größe Ihres Volumes ändern müssen, können Sie dies über die erweiterte Ansicht in BlueXP tun.

Schritte

1. Öffnen Sie die erweiterte Ansicht, um die Größe eines Volumes über System Manager zu ändern. Siehe "Erste Schritte".
2. Wählen Sie im linken Navigationsmenü **Speicher > Volumes**.
3. Wählen Sie aus der Liste der Volumes das Volume aus, das Sie anpassen sollten.
4. Klicken Sie auf das Optionssymbol .
5. Wählen Sie **Größe Ändern**.
6. Bearbeiten Sie auf dem Bildschirm **Resize Volume** den Prozentsatz der Kapazität und der Snapshot-Reserve nach Bedarf. Sie können den vorhandenen, verfügbaren Speicherplatz mit der geänderten Kapazität vergleichen.
7. Klicken Sie Auf **Speichern**.



Berücksichtigen Sie unbedingt die Kapazitätsgrenzen Ihres Systems, wenn Sie die Größe der Volumes ändern. Wechseln Sie zum "Versionshinweise zu Cloud Volumes ONTAP" Entnehmen.

Ändern Sie den CIFS-Server

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 der Registerkarte Übersicht auf die Registerkarte Funktion im rechten Fensterbereich.
2. Klicken Sie im Feld CIFS-Setup auf das Symbol **Bleistift**, um das CIFS-Setup-Fenster anzuzeigen.
3. Geben Sie die Einstellungen für den CIFS-Server an:

Aufgabe	Aktion
Storage VM (SVM) auswählen	Durch Auswahl der SVM (Storage Virtual Machine) des Cloud Volume ONTAP werden die konfigurierten CIFS-Informationen angezeigt.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.

Aufgabe	Aktion
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.
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. Ifdef::gcp[] Wenn Sie Google Managed Active Directory konfigurieren, kann AD standardmäßig mit der IP-Adresse 169.254.169.254 aufgerufen werden. Endif::gcp[]
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne 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, geben Sie in diesem Feld **OU=Computers,OU=corp** ein. • Um Azure AD-Domänendienste als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in diesem Feld **OU=AADDC-Computer** oder **OU=AADDC-Benutzer** ein."Azure-Dokumentation: Erstellen Sie eine Organisationseinheit (Organisationseinheit, OU) in einer von Azure AD-Domänendiensten gemanagten Domäne" • Um von Google verwaltete Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in diesem Feld **OU=Computer,OU=Cloud** ein."Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD"

4. Klicken Sie Auf **Set**.

Ergebnis

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

Verschieben Sie ein Volume

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".

Verschieben eines Volumes, wenn BlueXP eine Meldung Aktion erforderlich anzeigt

In BlueXP wird möglicherweise eine Meldung „Aktion erforderlich“ angezeigt, die besagt, dass das Verschieben eines Volumes erforderlich ist, um Kapazitätsprobleme zu vermeiden, aber Sie müssen das Problem selbst beheben. In diesem Fall müssen Sie herausfinden, wie das Problem behoben werden kann, und dann ein oder mehrere Volumes verschieben.

BlueXP zeigt diese „Aktion erforderlich“-Meldungen an, wenn ein Aggregat 90 % der verwendeten Kapazität erreicht hat. Wenn Daten-Tiering aktiviert ist, werden die Meldungen angezeigt, wenn ein Aggregat eine zu 80 % genutzte Kapazität erreicht hat. Standardmäßig werden 10 % freier Speicherplatz für das Daten-Tiering reserviert. "Erfahren Sie mehr über das freie Speicherplatzverhältnis für Daten-Tiering".

Schritte

1. Erkennen der Behebung von Kapazitätsproblemen.
2. Verschieben Sie Volumes basierend auf Ihrer Analyse, um Kapazitätsprobleme zu vermeiden:
   - um Kapazitätsprobleme zu vermeiden.
   - um Kapazitätsprobleme zu vermeiden.

Erkennen der Behebung von Kapazitätsproblemen

Wenn BlueXP keine Empfehlungen zum Verschieben eines Volumes zur Vermeidung von Kapazitätsproblemen bereitstellen kann, müssen Sie die Volumes identifizieren, die verschoben werden müssen und ob Sie sie zu einem anderen Aggregat auf demselben System oder einem anderen System verschieben möchten.

Schritte

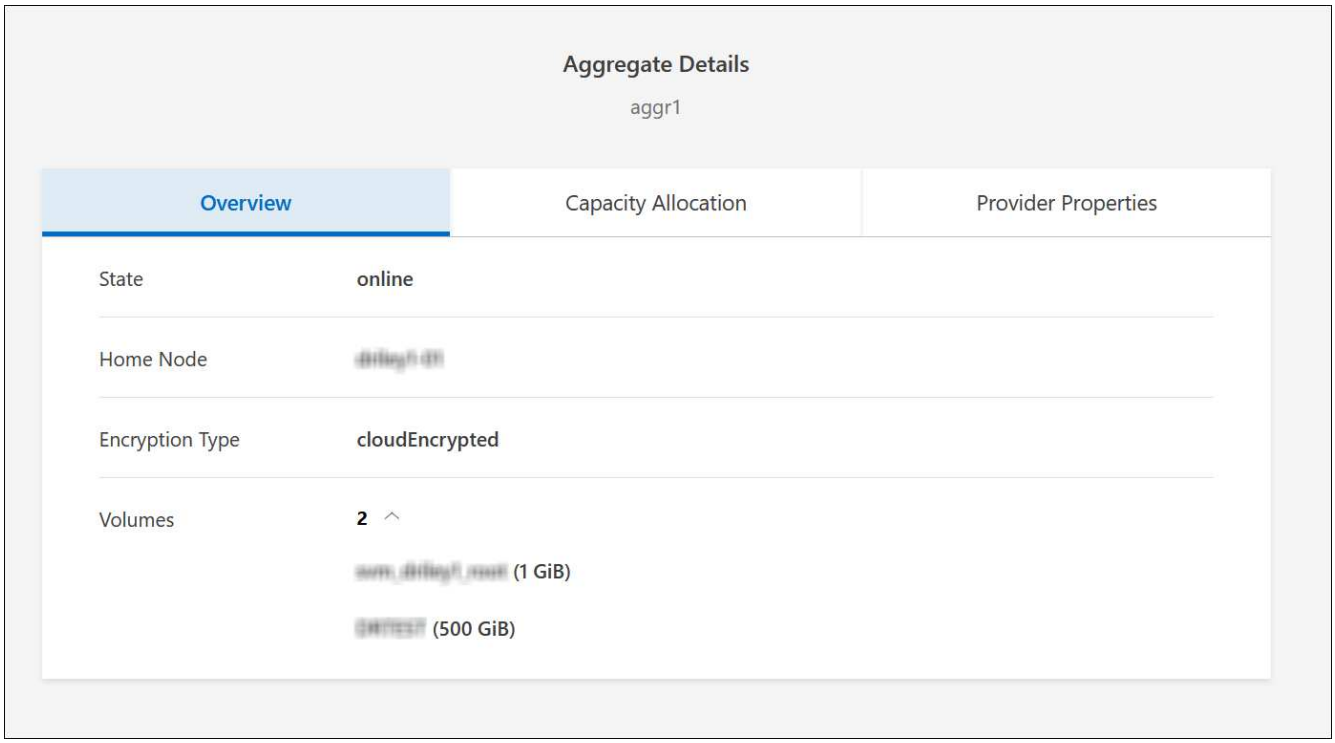
1. Zeigen Sie die erweiterten Informationen in der Meldung Aktion erforderlich an, um das Aggregat zu identifizieren, das seine Kapazitätsgrenze erreicht hat.

   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 die Registerkarte **Aggregate**.
   b. Navigieren Sie zur gewünschten Aggregat-Kachel, und klicken Sie dann auf **… (Ellipsen-Symbol) > Aggregatdetails anzeigen**.
   c. Überprüfen Sie auf der Registerkarte „Übersicht“ des Bildschirms „Aggregatdetails“ die Größe jedes Volumes, und wählen Sie ein oder mehrere Volumes aus dem Aggregat aus.

      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 Sie 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 Sie 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 Sie Volumes in ein anderes Aggregat, um Kapazitätsprobleme zu vermeiden.

Verschieben Sie Volumes in 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:

Das Verschieben eines Volumes ist notwendig, um Kapazitätsprobleme zu vermeiden. BlueXP kann diese Aktion jedoch nicht für Sie ausführen, da das System die Festplattengrenze erreicht hat.

Schritte

1. Identifizieren Sie ein Cloud Volumes ONTAP System mit verfügbarer Kapazität, oder implementieren Sie ein neues System.
2. 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".
3. 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".
4. 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".
5. Löschen Sie das ursprüngliche Volume.

   Weitere Informationen finden Sie unter "Volumes managen".

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

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

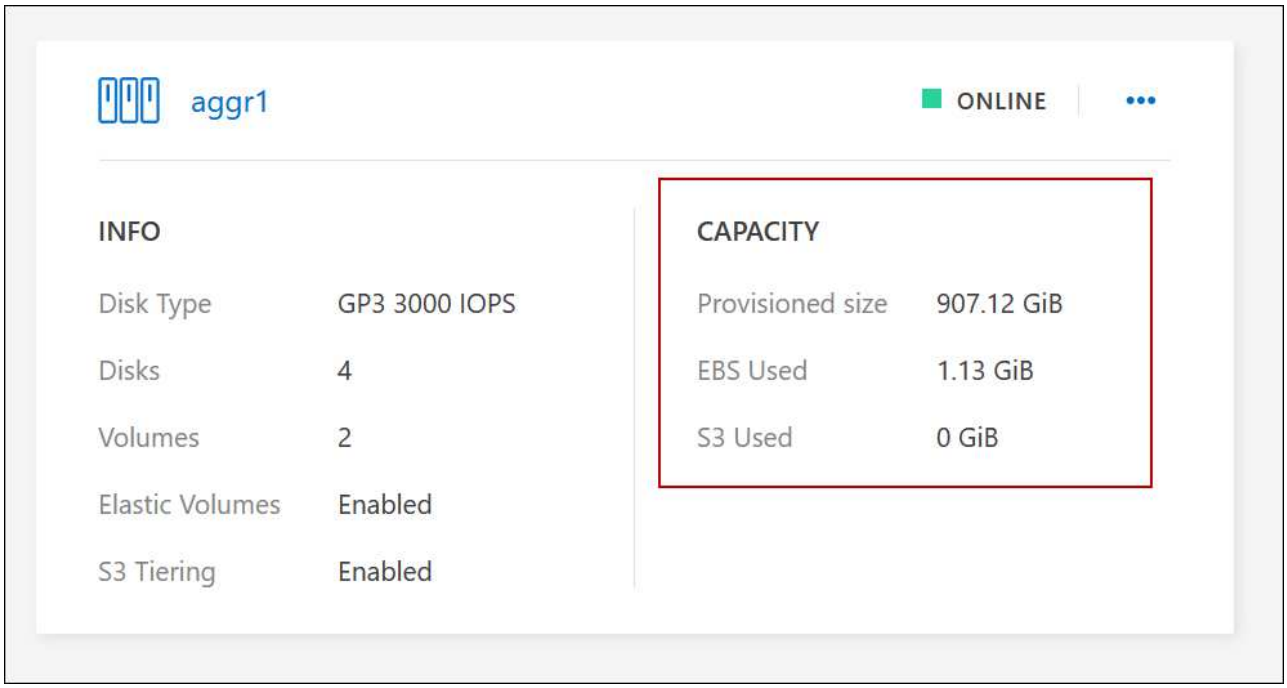
Über diese Aufgabe

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

Das Verschieben von zwei oder mehr Volumes ist notwendig, um Kapazitätsprobleme zu vermeiden, BlueXP kann diese Aktion jedoch nicht für Sie durchführen.

Schritte

1. Überprüfen Sie, ob ein vorhandenes Aggregat über die verfügbare Kapazität für die Volumes verfügt, die Sie verschieben müssen:
   a. Klicken Sie in der Arbeitsumgebung auf die Registerkarte **Aggregate**.
   b. Navigieren Sie zur gewünschten Aggregat-Kachel, und klicken Sie dann auf **… (Ellipsen-Symbol) > Aggregatdetails anzeigen**.
   c. Zeigen Sie unter der Kachel „Aggregat“ die verfügbare Kapazität an (bereitgestellte Größe minus genutzte Aggregatkapazität).



2. Fügen Sie bei Bedarf Festplatten zu einem vorhandenen Aggregat hinzu:
   a. Wählen Sie das Aggregat aus und klicken Sie dann auf **… (Ellipsen-Symbol) > Datenträger hinzufügen**.
   b. Wählen Sie die Anzahl der hinzuzufügenden Festplatten aus, und klicken Sie dann auf **Hinzufügen**.
3. Wenn keine Aggregate über verfügbare Kapazität verfügen, erstellen Sie ein neues Aggregat.

   Weitere Informationen finden Sie unter "Aggregate werden erstellt".
4. Verwenden Sie System Manager oder die CLI, um die Volumes in das Aggregat zu verschieben.
5. 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).
- Eines der Aggregate verwendet ein älteres Benennungsschema für Objekte. Beide Aggregate müssen das gleiche Namenformat verwenden.

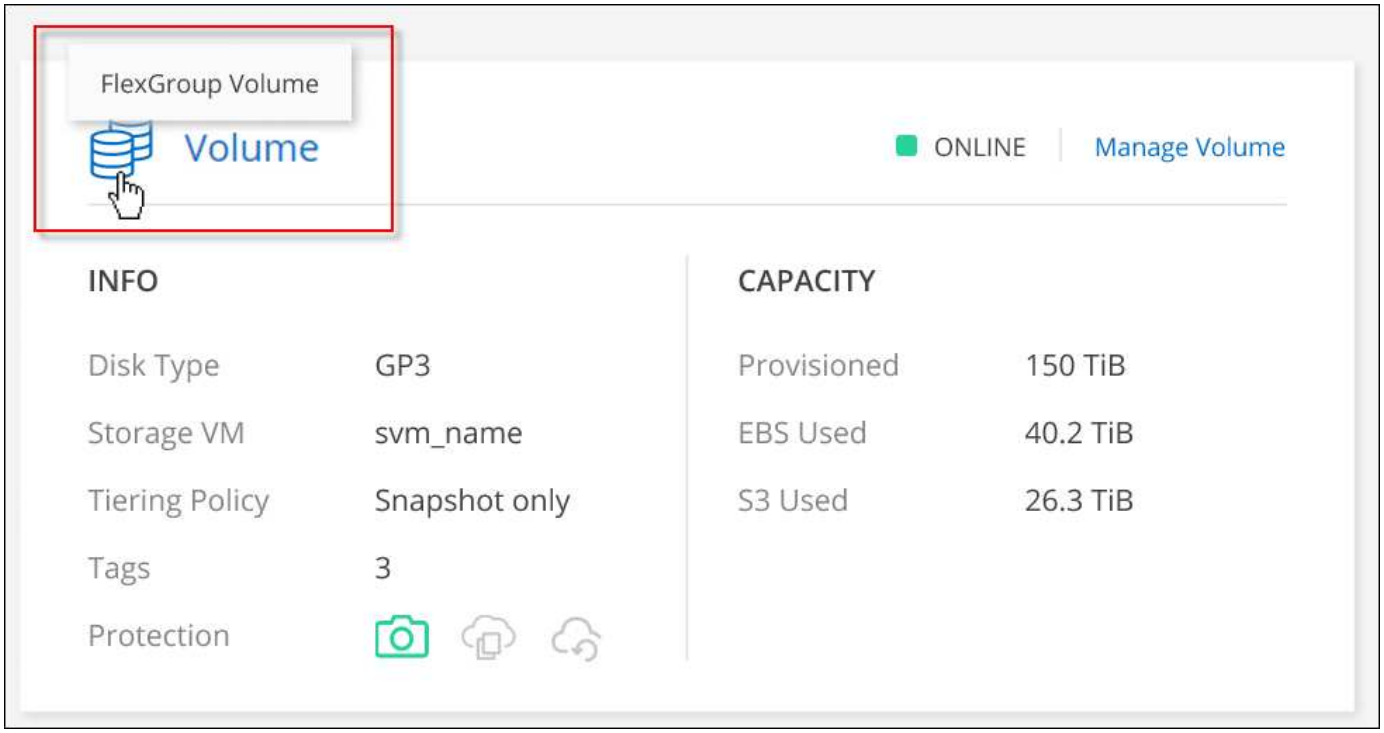
  Ein älteres Benennungsschema wird verwendet, wenn das Daten-Tiering auf einem Aggregat in Version 9.4 oder früher aktiviert wurde.
- Die Verschlüsselungseinstellungen stimmen nicht mit den Quell- und Zielaggregaten überein. Zudem wird ein Rekey ausgeführt.
- Die Option *-Tiering-Richtlinie* wurde bei der Verschiebung des Volumes angegeben, um die Tiering-

Richtlinie zu ändern.

- Die Option *-Generate-Destination-key* wurde für die Verschiebung des Volumes angegeben.

Zeigen Sie FlexGroup Volumes an

FlexGroup Volumes, die über CLI oder System Manager erstellt wurden, können direkt über die Registerkarte Volumes in BlueXP angezeigt werden. Wie bei FlexVol Volumes angegeben, bietet BlueXP über eine dedizierte Volume-Kachel detaillierte Informationen zu den erstellten FleGroup Volumes. Unter der Kachel „Volumes“ können Sie jede FlexGroup Volume-Gruppe über den Mauszeiger über das Symbol halten. Darüber hinaus können Sie FlexGroup-Volumes in der Listenansicht Volumes in der Spalte Volume-Stil identifizieren und sortieren.



Derzeit können Sie vorhandene FlexGroup Volumes nur unter BlueXP anzeigen. Die Möglichkeit zum Erstellen von FlexGroup Volumes in BlueXP ist nicht verfügbar, aber für eine zukünftige Version geplant.

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. Data Tiering wird durch FabricPool Technologie unterstützt. Eine allgemeine Übersicht finden Sie unter "Data Tiering - Übersicht".

Um Daten-Tiering einzurichten, müssen Sie die folgenden Schritte ausführen:

1. **Wählen Sie eine unterstützte Konfiguration aus**

Die meisten Konfigurationen werden unterstützt. Wenn Sie ein Cloud Volumes ONTAP System mit der

aktuellsten Version haben, sollten Sie gut zu gehen. "Weitere Informationen .".

2 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 müssen Sie nichts Unternehmen, solange BlueXP über die erforderlichen Berechtigungen verfügt. Weitere Informationen ..
- Für Google Cloud müssen Sie das Subnetz für privaten Google Access konfigurieren und ein Servicekonto einrichten. Weitere Informationen ..

3 Stellen Sie sicher, dass Sie über ein Aggregat mit aktiviertem Tiering verfügen

Daten-Tiering muss auf einem Aggregat aktiviert sein, um Daten-Tiering auf einem Volume zu ermöglichen. Die Anforderungen für neue Volumes und vorhandene Volumes sollten Sie kennen. dass das Tiering auf Aggregaten aktiviert ist,Weitere Informationen ..

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

BlueXP fordert Sie auf, beim Erstellen, Ändern oder Replizieren eines Volumes eine Tiering-Richtlinie auszuwählen.

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

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

- Für die Aktivierung von Daten-Tiering müssen Sie keine Funktionslizenz installieren.
- Sie müssen keinen Objektspeicher für die Kapazitäts-Tier erstellen. BlueXP ist das für Sie.
- Sie müssen das Daten-Tiering auf Systemebene nicht aktivieren.

  BlueXP erstellt bei der Systemerstellung einen Objektspeicher für „kalte“ Daten. Solange es keine Verbindungs- oder Berechtigungsprobleme gibt. Danach müssen Sie nur noch Daten-Tiering auf den Volumes aktivieren (und in einigen Fällen, dass das Tiering auf Aggregaten aktiviert ist,Auf Aggregaten).

Konfigurationen, die Daten-Tiering unterstützen

Sie können das Daten-Tiering unter Verwendung spezifischer Konfigurationen und Funktionen aktivieren.

Unterstützung in AWS

- Daten-Tiering wird in AWS ab Cloud Volumes ONTAP 9.2 unterstützt.
- Beim Performance-Tier können es sich um allgemeine SSDs (gp3 oder gp2) oder bereitgestellte IOPS-SSDs (io1) handelt.

Bei der Verwendung von durchsatzoptimierten HDDs (st1) wird kein Tiering von Daten zu Objekt-Storage empfohlen.

Unterstützung in Azure

- Daten-Tiering wird in Azure wie folgt unterstützt:
  - Version 9.4 in mit Single Node-Systemen
  - Version 9.6 in mit HA-Paaren
- Es kann sich bei dem Performance-Tier um von Premium-SSDs gemanagte Festplatten, von Standard-SSDs gemanagte Festplatten oder Standard-HDDs geben.

Support in Google Cloud

- Daten-Tiering wird in Google Cloud ab Cloud Volumes ONTAP 9.6 unterstützt.
- Beim Performance-Tier können es sich entweder um persistente SSD-Festplatten, ausgewogene persistente Festplatten oder um Standard-persistente Festplatten handeln.

Interoperabilität von Funktionen

- Daten-Tiering wird durch Verschlüsselungstechnologien unterstützt.
- Thin Provisioning muss auf Volumes aktiviert sein.

Anforderungen

Je nach Cloud-Provider müssen bestimmte Verbindungen und Berechtigungen eingerichtet werden, damit Cloud Volumes ONTAP selten genutzte Daten in den Objekt-Storage verschieben kann.

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

Sie müssen keine Verbindung zwischen der Performance- und der Kapazitäts-Tier einrichten, solange BlueXP die erforderlichen Berechtigungen hat. BlueXP ermöglicht Ihnen einen vnet-Service-Endpunkt, wenn die benutzerdefinierte Rolle für den Connector über folgende Berechtigungen verfügt:

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

Die Berechtigungen sind standardmäßig in die benutzerdefinierte Rolle enthalten. "Zeigen Sie die Azure-Berechtigung für den Connector an"

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".
- Ein Servicekonto muss mit Cloud Volumes ONTAP verbunden sein.

  "Erfahren Sie, wie Sie dieses Servicekonto einrichten".

  Sie werden aufgefordert, dieses Dienstkonto auszuwählen, wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen.

  Wenn Sie während der Implementierung kein Servicekonto auswählen, müssen Sie Cloud Volumes ONTAP herunterfahren, zur Google Cloud Konsole wechseln und dann das Service-Konto an die Cloud Volumes ONTAP Instanzen anhängen. Sie können dann das Daten-Tiering aktivieren, wie im nächsten Abschnitt beschrieben.

- Um den Bucket mit vom Kunden gemanagten Schlüsseln zu verschlüsseln, kann der Google Cloud Storage-Bucket den Schlüssel verwenden.

  "Verwenden Sie die vom Kunden gemanagten Schlüssel mit Cloud Volumes ONTAP".

Aktivieren des Daten-Tiering nach der Implementierung der Anforderungen

BlueXP erstellt bei der Erstellung des Systems einen Objektspeicher für kalte Daten, solange keine Verbindungs- oder Berechtigungsprobleme auftreten. Wenn Sie die oben aufgeführten Anforderungen erst nach dem Erstellen des Systems implementiert haben, müssen Sie Tiering manuell über die API oder den System Manager aktivieren, der den Objektspeicher erstellt.

Tiering über die BlueXP Benutzeroberfläche wird in einer zukünftigen Cloud Volumes ONTAP Version möglich sein.

Gewährleistung, dass das Tiering auf Aggregaten aktiviert ist

Daten-Tiering muss auf einem Aggregat aktiviert sein, um Daten-Tiering auf einem Volume zu ermöglichen. Die Anforderungen für neue Volumes und vorhandene Volumes sollten Sie kennen.

- **Neue Volumen**

  Wenn Sie Daten-Tiering auf einem neuen Volume aktivieren, müssen Sie sich keine Sorgen machen, dass Sie Daten-Tiering auf einem Aggregat aktivieren können. BlueXP erzeugt das Volume auf einem vorhandenen Aggregat mit aktiviertem Tiering oder erzeugt ein neues Aggregat für das Volume, wenn es noch kein Daten-Tiering-fähiges Aggregat gibt.

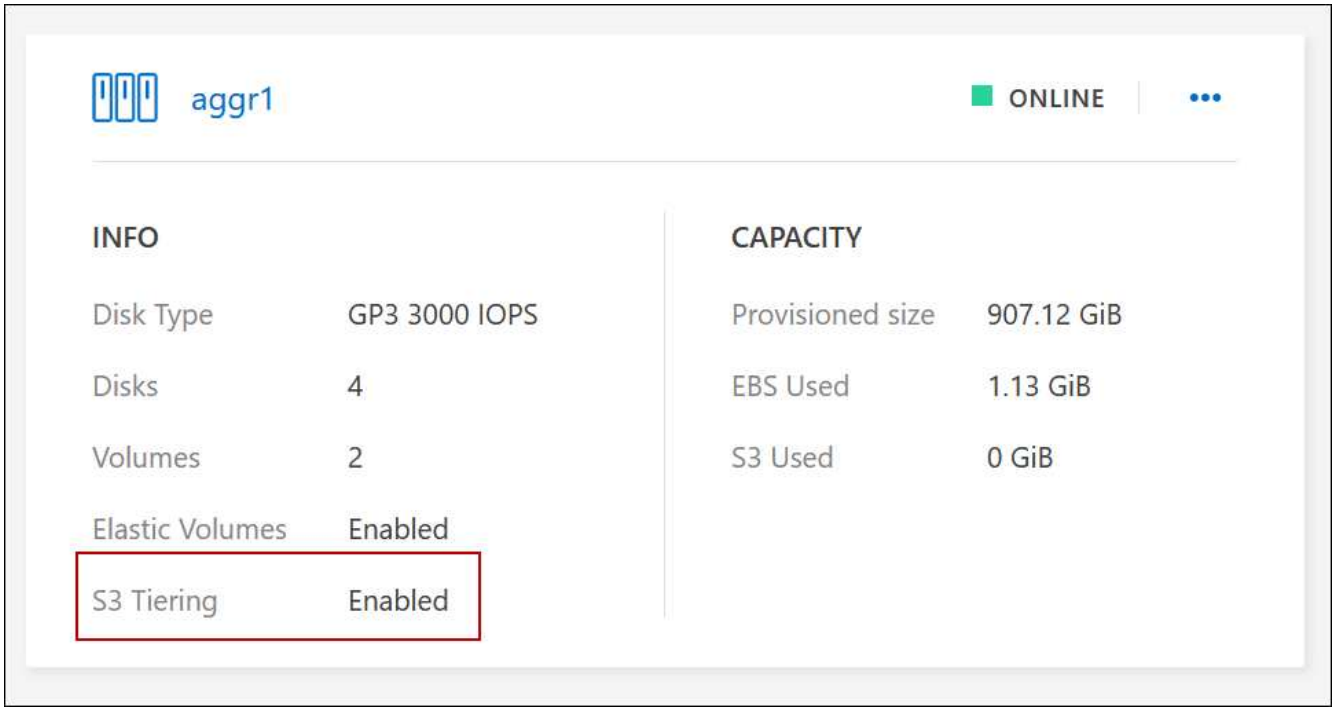
- **Vorhandene Bände**

  Wenn Sie Daten-Tiering auf einem vorhandenen Volume aktivieren möchten, müssen Sie sicherstellen, dass das Daten-Tiering auf dem zugrunde liegenden Aggregat aktiviert ist. Wenn das Daten-Tiering auf dem vorhandenen Aggregat nicht aktiviert ist, müssen Sie mit System Manager ein vorhandenes Aggregat an den Objektspeicher anhängen.

Schritte zur Bestätigung, ob Tiering auf einem Aggregat aktiviert ist

1. Öffnen Sie die Arbeitsumgebung in BlueXP.

2. Klicken Sie auf die Registerkarte Aggregate.
3. Navigieren Sie zu der gewünschten Kachel und überprüfen Sie, ob das Tiering auf dem Aggregat aktiviert oder deaktiviert ist.



Schritte zur Aktivierung des Tiering auf einem Aggregat

1. Klicken Sie im System Manager auf **Storage > Tiers**.
2. Klicken Sie auf das Aktionsmenü für das Aggregat und wählen Sie **Cloud Tiers anhängen**.
3. Wählen Sie den anzuhänden Cloud Tier aus und klicken Sie auf **Speichern**.

Was kommt als Nächstes?

Sie können jetzt Daten-Tiering auf neuen und vorhandenen Volumes aktivieren, wie im nächsten Abschnitt erläutert.

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 auf der Registerkarte Volumes in der Arbeitsumgebung ein neues Volume oder ändern Sie die Ebene eines vorhandenen Volumes:

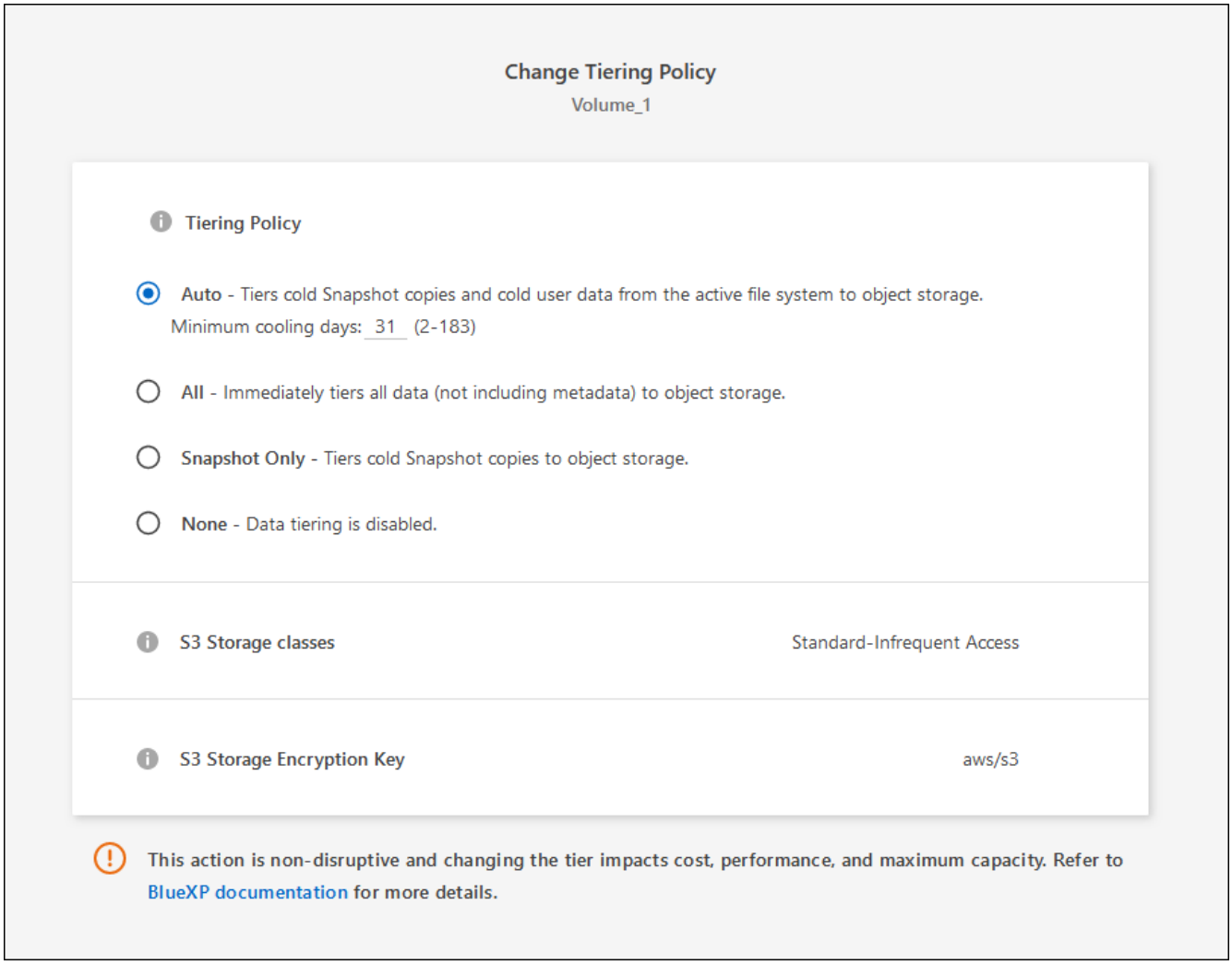
Aufgabe	Aktion
Erstellen Sie ein neues Volume	Klicken Sie Auf **Neues Volume Hinzufügen**.

Aufgabe	Aktion
Ändern Sie ein vorhandenes Volume	Wählen Sie die gewünschte Volume-Kachel aus, klicken Sie auf **Volume verwalten**, um auf das rechte Panel Volumes verwalten zuzugreifen, und klicken Sie dann im rechten Bereich auf **Erweiterte Aktionen** und **Tiering-Policy ändern**.

2. Wählen Sie eine Tiering-Richtlinie aus.

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

   Beispiel



   BlueXP erstellt ein neues Aggregat für das Volume, wenn es bereits ein Data Tiering-fähiges Aggregat gibt.

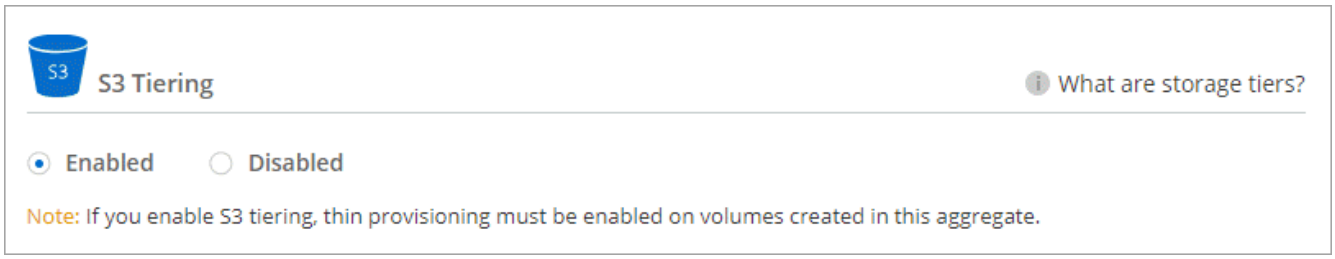
Tiering von Daten aus Datensicherungs-Volumes

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 im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Wählen Sie auf der Seite Arbeitsfläche die Arbeitsumgebung aus, die das Quellvolumen enthält, und ziehen Sie es dann in die Arbeitsumgebung, in die Sie das Volumen replizieren möchten.
3. 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**.

Ändern des freien Speicherplatzverhältnisses für das Daten-Tiering

Das Verhältnis von freiem Speicherplatz für Daten-Tiering bestimmt, wie viel freier Speicherplatz auf Cloud Volumes ONTAP SSDs/HDDs erforderlich ist, wenn Daten-Tiering zu Objekt-Storage erfolgt. Die Standardeinstellung ist 10 % freier Speicherplatz, Sie können die Einstellung jedoch entsprechend Ihren Anforderungen anpassen.

So können Sie beispielsweise weniger als 10 % freien Speicherplatz auswählen, um sicherzustellen, dass Sie die erworbene Kapazität nutzen. BlueXP kann dann zusätzliche Festplatten für Sie erwerben, wenn zusätzliche Kapazität benötigt wird (bis zur Obergrenze des Festplattenaggregats).

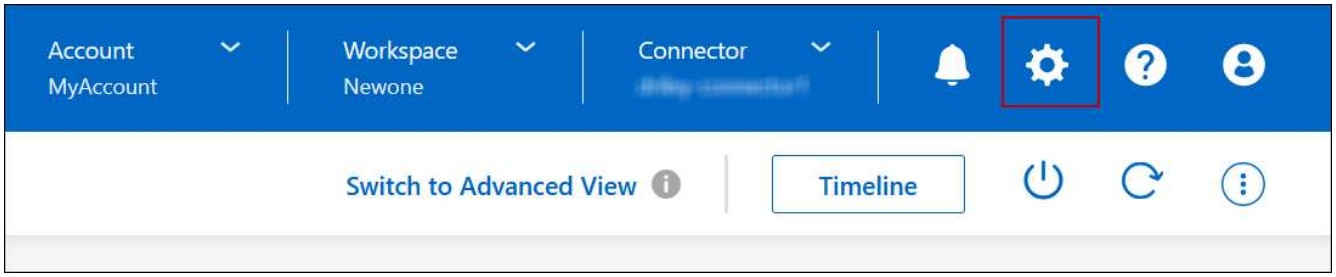
> Wenn nicht genügend Speicherplatz zur Verfügung steht, können die Daten mit Cloud Volumes ONTAP nicht verschoben werden. Möglicherweise kommt es zu Performance-Einbußen. Jede Änderung sollte mit Vorsicht vorgenommen werden. Wenn Sie sich nicht sicher sind, wenden Sie sich an den NetApp Support.

Das Verhältnis ist wichtig für Disaster-Recovery-Szenarien, da die Daten vom Objektspeicher gelesen werden,

verschiebt Cloud Volumes ONTAP die Daten auf SSDs/HDDs, um eine bessere Performance zu bieten. Wenn nicht genügend Speicherplatz vorhanden ist, dann kann Cloud Volumes ONTAP die Daten nicht verschieben. Wenn Sie das Verhältnis ändern, können Sie Ihre geschäftlichen Anforderungen erfüllen.

Schritte

1. Klicken Sie oben rechts auf der BlueXP-Konsole auf das Symbol **Einstellungen** und wählen Sie **Cloud Volumes ONTAP-Einstellungen** aus.



2. Klicken Sie unter **Kapazität** auf **Kapazitätsschwellenwerte für Aggregat - kostenloses Platzverhältnis für Daten-Tiering**.
3. Ändern Sie das Verhältnis des freien Speicherplatzes entsprechend Ihren Anforderungen und klicken Sie auf **Speichern**.

Ändern des Kühlzeitraums für die automatische Tiering-Richtlinie

Wenn Sie das Daten-Tiering auf einem Cloud Volumes ONTAP Volume mithilfe der Tiering-Richtlinie „*Auto*“ aktiviert haben, können Sie den standardmäßigen Kühlzeitraum je nach Ihren Geschäftsanforderungen anpassen. Diese Aktion wird nur über die API und CLI unterstützt.

Der Kühlzeitraum ist die Anzahl der Tage, die Benutzerdaten in einem Volume inaktiv bleiben müssen, bevor sie als „kalt“ eingestuft und in einen Objekt-Storage verschoben werden.

Der standardmäßige Kühlzeitraum für die Auto-Tiering-Richtlinie beträgt 31 Tage. Sie können den Kühlzeitraum wie folgt ändern:

- 9.8 oder höher: 2 Tage bis 183 Tage
- 9.7 oder früher: 2 Tage bis 63 Tage

Schritt

1. Verwenden Sie den Parameter *minimumCoolingDays* mit Ihrer API-Anforderung, wenn Sie ein Volume erstellen oder ein vorhandenes Volume ändern.

Verbinden Sie eine LUN mit einem Host

Wenn Sie ein iSCSI-Volume erstellen, erstellt BlueXP 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:

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

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

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Doppelklicken Sie auf der Leinwand-Seite auf die Cloud Volumes ONTAP-Arbeitsumgebung, auf der Sie Volumes verwalten möchten.
3. Klicken Sie in der Arbeitsumgebung auf die Registerkarte **Volumes**.
4. Navigieren Sie auf der Registerkarte Volumes zum gewünschten Volume-Titel, und klicken Sie dann auf **Volume verwalten**, um auf das rechte Bedienfeld Volumes verwalten zuzugreifen.
5. Klicken Sie auf **Target IQN**.
6. Klicken Sie auf **Kopieren**, um den IQN-Namen zu kopieren.
7. 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"
    - "ONTAP SAN-Host-Konfiguration"

Beschleunigter Datenzugriff mit FlexCache Volumes

Ein FlexCache Volume ist ein Storage-Volume, das SMB- und NFS-Lesedaten 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.

BlueXP ermöglicht das Management von FlexCache Volumes mit dem "BlueXP Volume-Caching" Service:

Zudem können Sie mit der ONTAP CLI oder mit ONTAP System Manager FlexCache Volumes erstellen und managen:

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

BlueXP generiert eine FlexCache Lizenz für alle neuen Cloud Volumes ONTAP Systeme. Die Lizenz umfasst ein Nutzungslimit von 500 gib.

Aggregatadministration

Erstellen von Aggregaten

Sie können Aggregate selbst erstellen oder BlueXP dies für Sie tun lassen, wenn es Volumes erstellt. 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.

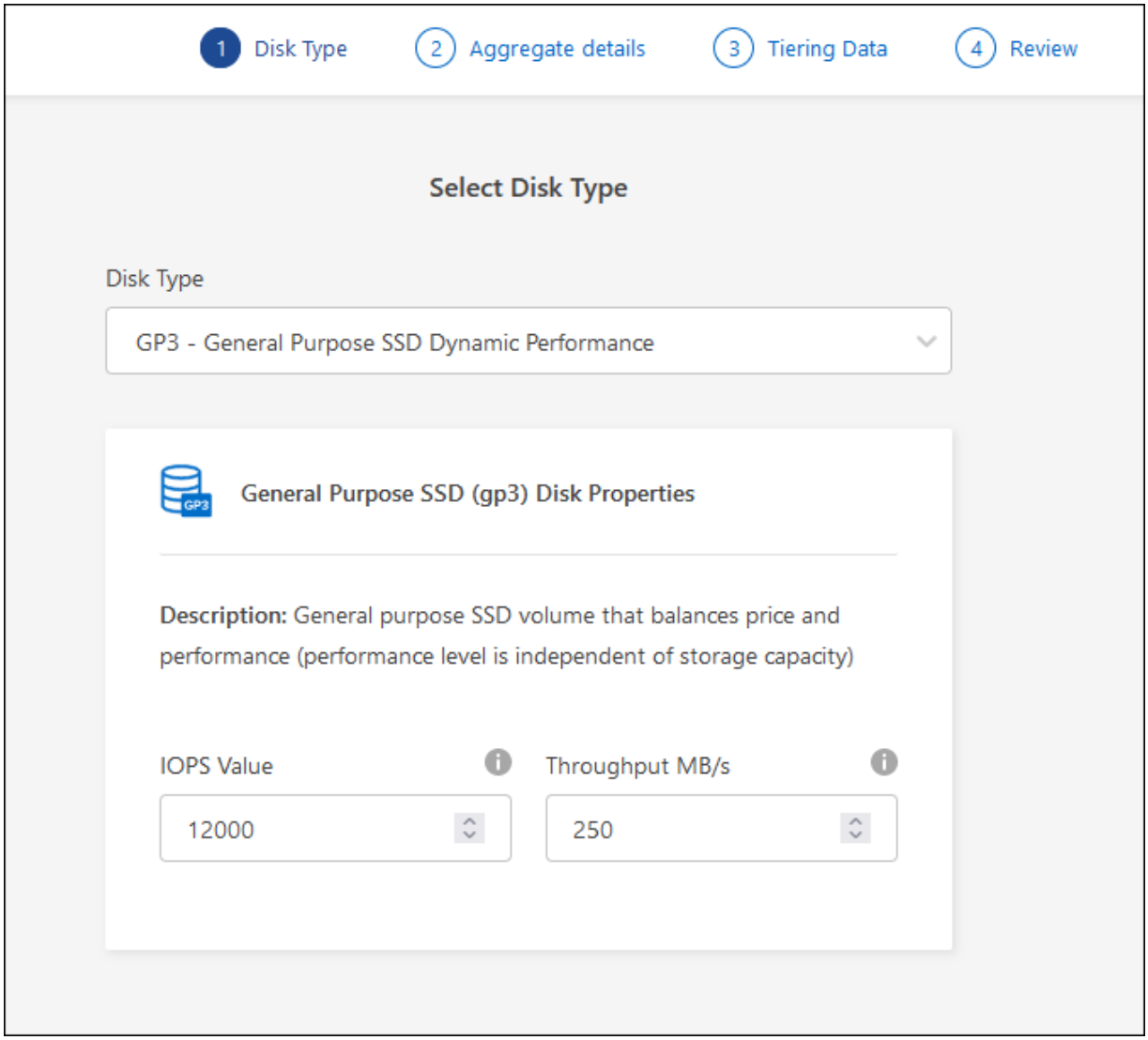
Alle Festplatten und Aggregate müssen direkt aus BlueXP erstellt und gelöscht werden. Sie sollten diese Aktionen nicht über ein anderes Management-Tool ausführen. Dies kann sich auf die Systemstabilität auswirken, die Fähigkeit zum Hinzufügen von Festplatten in der Zukunft beeinträchtigen und möglicherweise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

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Doppelklicken Sie auf der Seite Arbeitsfläche auf den Namen der Cloud Volumes ONTAP-Instanz, auf der Sie Aggregate verwalten möchten.
3. Klicken Sie auf der Registerkarte Aggregate auf **Add Aggregate** und geben Sie dann Details für das Aggregat an.

AWS

- Wenn Sie aufgefordert werden, einen Festplattentyp und eine Festplattengröße auszuwählen, lesen Sie "Planen Sie Ihre Cloud Volumes ONTAP-Konfiguration in AWS".
- Wenn Sie zur Eingabe der Kapazitätsgröße des Aggregats aufgefordert werden, erstellen Sie ein Aggregat auf einer Konfiguration, die die Elastic Volumes Funktion von Amazon EBS unterstützt. Der folgende Screenshot zeigt ein Beispiel für ein neues Aggregat, das aus gp3-Festplatten besteht.



"Erfahren Sie mehr über den Support für Elastic Volumes".

Azure

Hilfe zu Festplattentyp und Festplattengröße finden Sie unter "Planen Sie Ihre Cloud Volumes ONTAP-Konfiguration in Azure".

Google Cloud

Hilfe zu Festplattentyp und Festplattengröße finden Sie unter "Planen Sie Ihre Cloud Volumes ONTAP-Konfiguration in Google Cloud".

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

Management von Aggregaten

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

> Alle Festplatten und Aggregate müssen direkt aus BlueXP 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.

Bevor Sie beginnen

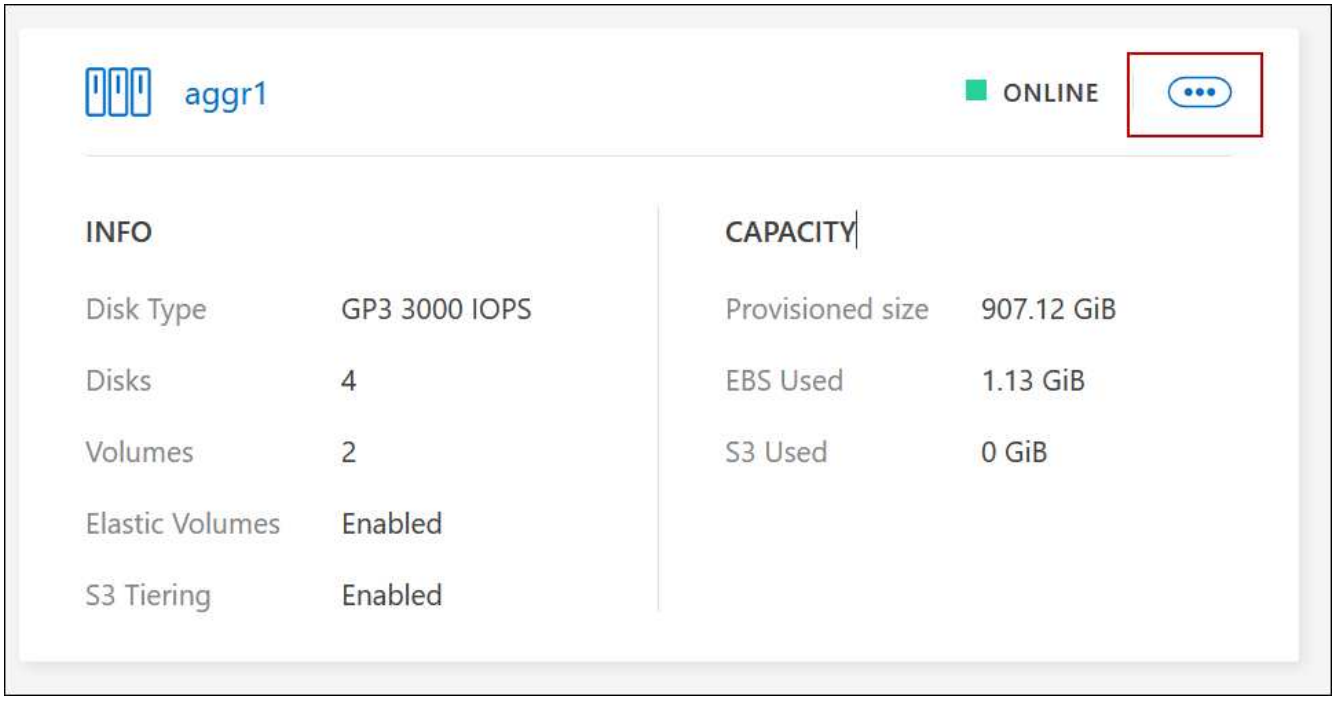
Wenn Sie ein Aggregat löschen möchten, müssen Sie zunächst die Volumes im Aggregat gelöscht haben.

Über diese Aufgabe

Wenn einem Aggregat nicht mehr genügend Platz vorhanden ist, können Sie Volumes mit System Manager zu einem anderen Aggregat verschieben.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Doppelklicken Sie auf der leinwand-Seite auf die Cloud Volumes ONTAP Arbeitsumgebung, auf der Sie Aggregate verwalten möchten.
3. Klicken Sie in der Arbeitsumgebung auf die Registerkarte **Aggregate**.
4. Navigieren Sie auf der Registerkarte Aggregate zum gewünschten Titel, und klicken Sie dann auf **… (Ellipsensymbol)**.



5. Verwalten Sie Ihre Aggregate:

Aufgabe	Aktion
Anzeigen von Informationen zu einem Aggregat	Klicken Sie im Menü … (Ellipsen-Symbol) auf **Aggregatdetails anzeigen**.
Erstellen Sie ein Volume auf einem bestimmten Aggregat	Klicken Sie im Menü … (Ellipsen-Symbol) auf **Lautstärke hinzufügen**.
Hinzufügen von Festplatten zu einem Aggregat	a. Klicken Sie im Menü … (Ellipsensymbol) auf **Datenträger 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.
Erhöhen Sie die Kapazität eines Aggregats, das Amazon EBS Elastic Volumes unterstützt	a. Klicken Sie im Menü … (Ellipsen-Symbol) auf **Kapazität erhöhen**. b. Geben Sie die zusätzliche Kapazität ein, die Sie hinzufügen möchten, und klicken Sie dann auf **Erhöhen**. Beachten Sie, dass Sie die Kapazität des Aggregats um mindestens 256 gib oder 10 % der Aggregatgröße erhöhen müssen. Wenn Sie beispielsweise ein 1.77 tib Aggregat haben, beträgt 10 % 181 gib. Das ist niedriger als 256 gib, daher muss die Größe des Aggregats um das Minimum von 256 gib erhöht werden.
Löschen Sie ein Aggregat	a. Wählen Sie eine Aggregat-Kachel, die keine Volumes enthält Klicken Sie auf **… (Ellipsensymbol) > Löschen**. b. Klicken Sie zur Bestätigung erneut auf **Löschen**.

Kapazitätseinstellungen auf einem Konnektor verwalten

Jeder Connector hat Einstellungen, die bestimmen, wie er die Aggregatskapazität für Cloud Volumes ONTAP verwaltet.

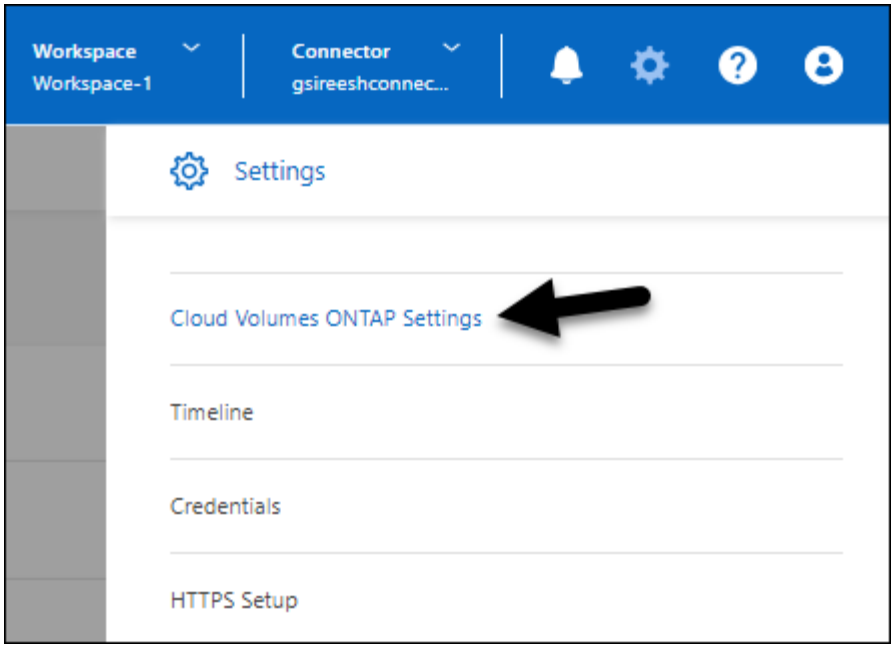
Diese Einstellungen betreffen alle Cloud Volumes ONTAP-Systeme, die von einem Connector verwaltet werden. Wenn Sie einen anderen Konnektor haben, kann er anders konfiguriert werden.

Erforderliche Berechtigungen

Zum Ändern der Cloud Volumes ONTAP-Einstellungen sind Administratorrechte erforderlich.

Schritte

1. Klicken Sie oben rechts in der BlueXP Konsole auf das Symbol Einstellungen und wählen Sie **Cloud Volumes ONTAP-Einstellungen** aus.



2. Ändern Sie unter **Capacity** eine der folgenden Einstellungen:

Kapazitätsmanagement -Modus

Legen Sie fest, ob BlueXP Sie über Entscheidungen zur Storage-Kapazität benachrichtigt oder ob BlueXP die Kapazitätsanforderungen automatisch managt.

"Erfahren Sie, wie der Capacity Management-Modus funktioniert".

Schwellenwert Für Aggregatkapazität – Verhältnis Für Freien Speicherplatz

Dieses Verhältnis ist ein wichtiger Parameter bei Entscheidungen zum Kapazitätsmanagement. Daher ist es unerlässlich, die Auswirkungen zu verstehen, unabhängig davon, ob Sie sich in einem automatischen oder manuellen Modus für das Kapazitätsmanagement befinden. Es wird empfohlen, diese Grenze unter Berücksichtigung Ihrer spezifischen Storage-Anforderungen und des voraussichtlichen Wachstums festzulegen, um die Ressourcenauslastung und die Kosten in Einklang zu bringen.

Wenn im manuellen Modus das Verhältnis des freien Speicherplatzes auf einem Aggregat unter den angegebenen Schwellenwert fällt, löst es eine Benachrichtigung aus, die Sie darauf hinweist, dass Sie Maßnahmen ergreifen sollten, um das Verhältnis des niedrigen freien Speicherplatzes zu beheben. Es ist wichtig, diese Benachrichtigungen zu überwachen und die aggregierte Kapazität manuell zu managen, um Serviceunterbrechungen zu vermeiden und eine optimale Performance sicherzustellen.

Das Verhältnis des freien Speicherplatzes berechnet sich wie folgt:
(Gesamtkapazität – genutzte Gesamtkapazität im Aggregat) / Gesamtkapazität des Aggregats

Siehe "Automatisches Kapazitätsmanagement" Um zu erfahren, wird die Kapazität jetzt automatisch in Cloud Volumes ONTAP gemanagt.

Aggregierte Kapazitätsschwellenwerte – Verhältnis des freien Speicherplatzes für Daten-Tiering

Definiert, wie viel freier Speicherplatz auf der Performance-Tier (Festplatten) benötigt wird, wenn Daten-Tiering auf eine Kapazitäts-Tier (Objekt-Storage) erfolgt.

Das Verhältnis ist für Disaster-Recovery-Szenarien von großer Bedeutung. Wenn Daten von der Kapazitäts-Tier gelesen werden, verschiebt Cloud Volumes ONTAP Daten in die Performance-Tier, um bessere Performance zu bieten. Wenn nicht genügend Speicherplatz vorhanden ist, dann kann Cloud

Volumes ONTAP die Daten nicht verschieben.

3. Klicken Sie Auf **Speichern**.

Storage VM-Administration

Managen Sie Storage-VMs in BlueXP

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.

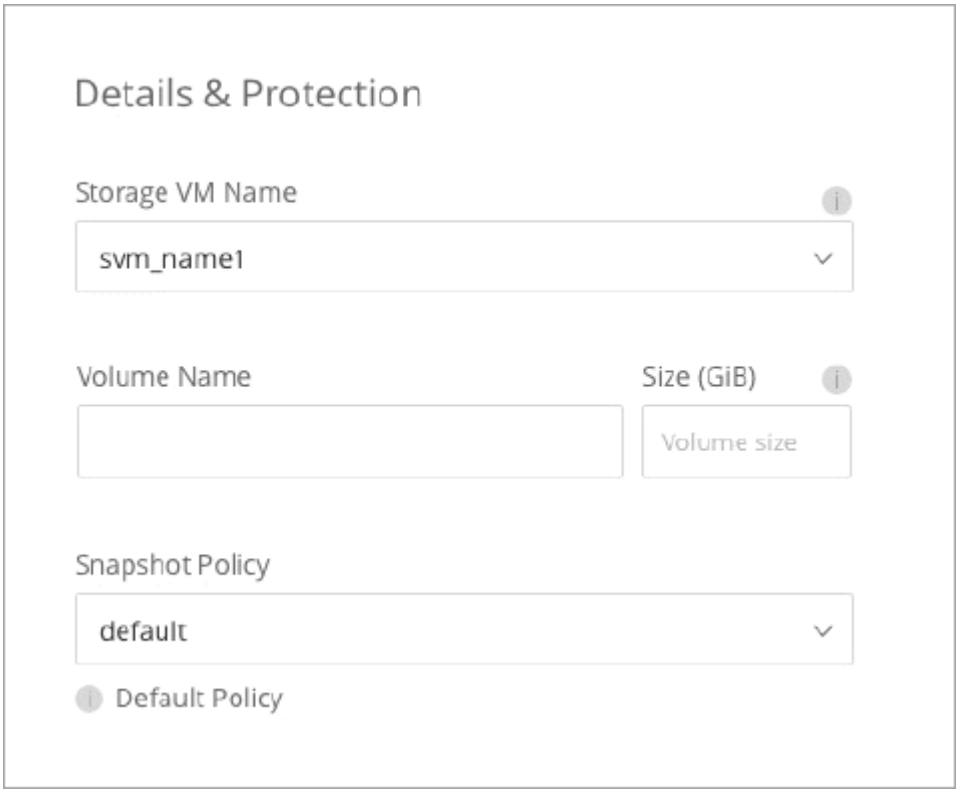
Unterstützte Anzahl von Storage-VMs

Bestimmte Konfigurationen unterstützen mehrere Storage-VMs. Wechseln Sie zum "Versionshinweise zu Cloud Volumes ONTAP" Um zu überprüfen, wie viele Storage VMs für Ihre Cloud Volumes ONTAP-Version unterstützt werden.

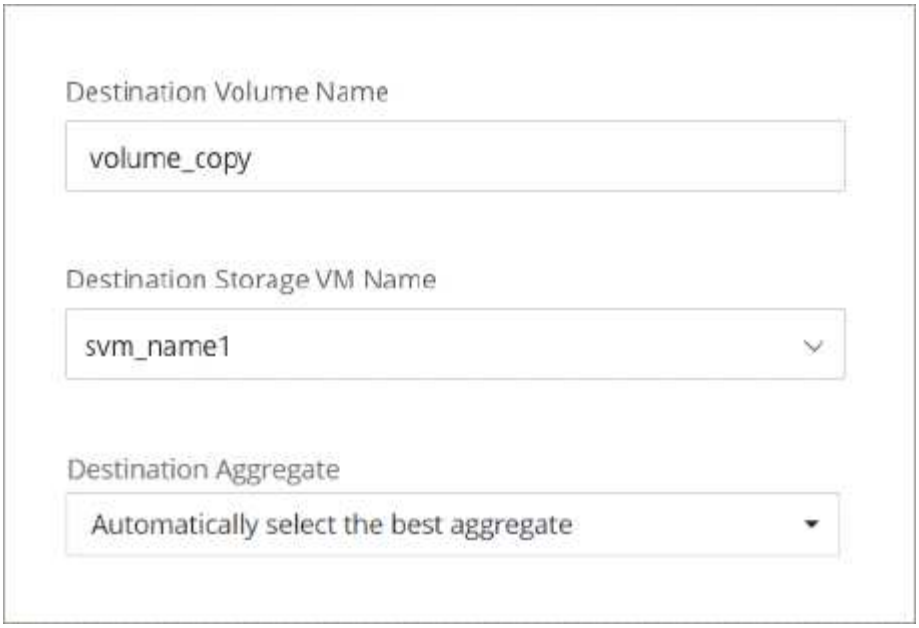
Arbeiten Sie mit mehreren Storage VMs

BlueXP 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.



Ändern Sie den Namen der Standard-Storage-VM

BlueXP benennt automatisch die einzelne Storage-VM, die sie für Cloud Volumes ONTAP erstellt. Über System Manager, CLI oder API können Sie 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.

Erstellen Sie Daten-Serving-Storage VMs für Cloud Volumes ONTAP in AWS

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.

Um zusätzliche Datenspeicher-VMs zu erstellen, müssen Sie IP-Adressen in AWS zuweisen und dann ONTAP-Befehle basierend auf Ihrer Cloud Volumes ONTAP Konfiguration ausführen.

Unterstützte Anzahl von Storage-VMs

Ab Version 9.7 werden mehrere Storage-VMs mit spezifischen Cloud Volumes ONTAP Konfigurationen unterstützt. Wechseln Sie zum "Versionshinweise zu Cloud Volumes ONTAP" Um zu überprüfen, wie viele Storage VMs für Ihre Cloud Volumes ONTAP-Version unterstützt werden.

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 Datenzugriff aktivieren, wenn es einen Ausfall auf der Quell-Storage-VM gibt.

Prüfen Sie die Grenzen für Ihre Konfiguration

Jede EC2-Instanz unterstützt eine maximale Anzahl privater IPv4-Adressen pro Netzwerkschnittstelle. Sie müssen das Limit überprüfen, bevor Sie der neuen Storage VM IP-Adressen in AWS zuweisen.

Schritte

1. Geh die "Abschnitt „Speicherbegrenzungen“ in den Versionshinweisen zu Cloud Volumes ONTAP".

2. Geben Sie für Ihren Instanztyp die maximale Anzahl an IP-Adressen pro Schnittstelle an.
3. Notieren Sie sich diese Zahl, da Sie sie im nächsten Abschnitt beim Zuweisen von IP-Adressen in AWS benötigen.

Weisen Sie IP-Adressen in AWS zu

Private IPv4-Adressen müssen Port e0a in AWS zugewiesen werden, bevor Sie LIFs für die neue Storage VM erstellen.

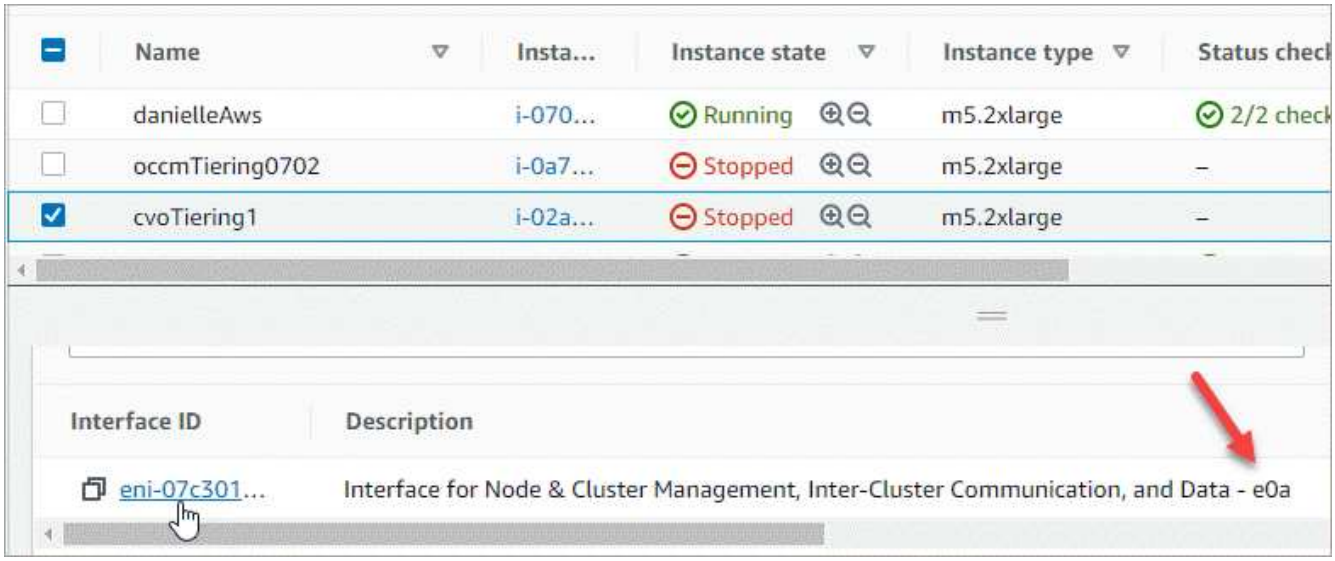
Beachten Sie, dass eine optionale Management-LIF für eine Storage-VM eine private IP-Adresse auf einem System mit einem einzelnen Node und auf einem HA-Paar in einer einzelnen Verfügbarkeitszone erfordert. Dieses Management-LIF bietet eine Verbindung zu Management-Tools wie SnapCenter.

Schritte

1. Melden Sie sich bei AWS an und öffnen Sie den EC2 Service.
2. Wählen Sie die Cloud Volumes ONTAP-Instanz aus und klicken Sie auf **Netzwerk**.

   Wenn Sie eine Storage VM auf einem HA-Paar erstellen, wählen Sie Node 1 aus.

3. Scrollen Sie nach unten zu **Netzwerkschnittstellen** und klicken Sie auf die **Schnittstellen-ID** für Port e0a.



4. Wählen Sie die Netzwerkschnittstelle aus und klicken Sie auf **Aktionen > IP-Adressen verwalten**.
5. Erweitern Sie die Liste der IP-Adressen für e0a.
6. Überprüfen Sie die IP-Adressen:
   a. Zählen Sie die Anzahl der zugewiesenen IP-Adressen, um zu bestätigen, dass der Port Platz für zusätzliche IP-Adressen hat.

      Im vorherigen Abschnitt dieser Seite sollten Sie die maximale Anzahl der unterstützten IP-Adressen pro Schnittstelle angegeben haben.

   b. Optional: Rufen Sie die CLI für Cloud Volumes ONTAP auf und führen Sie **Network Interface show** aus, um zu bestätigen, dass jede dieser IP-Adressen verwendet wird.

      Wenn keine IP-Adresse verwendet wird, können Sie sie zusammen mit der neuen Storage-VM verwenden.

7. Klicken Sie zurück in der AWS-Konsole auf **Neue IP-Adresse zuweisen**, um zusätzliche IP-Adressen basierend auf der Menge zuzuweisen, die Sie für die neue Speicher-VM benötigen.
   - Single Node-System: Eine ungenutzte sekundäre private IP ist erforderlich.

     Wenn Sie eine Management-LIF auf der Storage-VM erstellen möchten, ist eine optionale sekundäre private IP erforderlich.
   - HA-Paar in einer einzelnen AZ: Eine ungenutzte sekundäre private IP ist auf Node 1 erforderlich.

     Wenn Sie eine Management-LIF auf der Storage-VM erstellen möchten, ist eine optionale sekundäre private IP erforderlich.
   - HA-Paar in mehreren Verfügbarkeitszonen: Auf jedem Node ist eine nicht genutzte sekundäre private IP-Adresse erforderlich.
8. Wenn Sie die IP-Adresse einem HA-Paar in einer einzelnen AZ zuweisen, aktivieren Sie * erlauben Sie die erneute Zuweisung von sekundären privaten IPv4-Adressen*.
9. Klicken Sie Auf **Speichern**.
10. Wenn Sie ein HA-Paar in mehreren Verfügbarkeitszonen haben, müssen Sie diese Schritte für Node 2 wiederholen.

Erstellen einer Storage-VM auf einem System mit einzelnen Nodes

Mit diesen Schritten wird eine neue Storage-VM auf einem System mit einem einzelnen Node erstellt. Eine private IP-Adresse ist erforderlich, um eine NAS-LIF zu erstellen, und eine weitere optionale private IP-Adresse ist erforderlich, wenn Sie eine Management-LIF erstellen möchten.

Schritte

1. Erstellen Sie die Storage-VM und eine Route zur Storage-VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Erstellen Sie ein NAS-LIF.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node
```

   Wobei *private_ip_x* eine nicht genutzte sekundäre private IP auf e0a ist.

3. Optional: Erstellen Sie eine Storage-VM-Management-LIF.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

Wobei *private_ip_y* eine weitere nicht genutzte sekundäre private IP auf e0a ist.

4. Weisen Sie der Storage-VM ein oder mehrere Aggregate zu.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Dieser Schritt ist erforderlich, da die neue Storage-VM Zugriff auf mindestens ein Aggregat benötigt, bevor Sie Volumes auf der Storage-VM erstellen können.

Erstellen einer Storage VM auf einem HA-Paar in einer einzelnen Verfügbarkeitszone

Mit diesen Schritten wird eine neue Storage-VM auf einem HA-Paar in einer einzelnen Verfügbarkeitszone erstellt. Eine private IP-Adresse ist erforderlich, um eine NAS-LIF zu erstellen, und eine weitere optionale private IP-Adresse ist erforderlich, wenn Sie eine Management-LIF erstellen möchten.

Beide LIFs werden an Node 1 zugewiesen. Bei einem Ausfall können die privaten IP-Adressen zwischen Nodes verschoben werden.

Schritte

1. Erstellen Sie die Storage-VM und eine Route zur Storage-VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Erstellen Sie auf Node 1 ein NAS-LIF.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

Wobei *private_ip_x* eine nicht genutzte sekundäre private IP auf e0a von cvo-node1 ist. Diese IP-Adresse kann im Falle eines Takeover an den e0a von cvo-node2 verschoben werden, da die Service-Richtlinie Standard-Daten-Dateien darauf hinweist, dass IPs zum Partner-Node migrieren können.

3. Optional: Erstellen Sie eine Storage-VM-Management-LIF auf Node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

Wobei *private_ip_y* eine weitere nicht genutzte sekundäre private IP auf e0a ist.

4. Weisen Sie der Storage-VM ein oder mehrere Aggregate zu.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Dieser Schritt ist erforderlich, da die neue Storage-VM Zugriff auf mindestens ein Aggregat benötigt, bevor Sie Volumes auf der Storage-VM erstellen können.

5. Wenn Sie Cloud Volumes ONTAP 9.11.1 oder höher verwenden, ändern Sie die Netzwerk-Service-Richtlinien für die Storage VM.

Das Ändern der Services ist erforderlich, da Cloud Volumes ONTAP sicherstellen kann, dass die iSCSI-LIF für ausgehende Managementverbindungen verwendet werden kann.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

Erstellung einer Storage VM auf einem HA-Paar in mehreren Verfügbarkeitszonen

Durch diese Schritte wird eine neue Storage VM auf einem HA-Paar in mehreren Verfügbarkeitszonen erstellt.

Für eine NAS-LIF ist eine *floating* IP-Adresse erforderlich und ist optional für eine Management-LIF. Bei diesen fließenden IP-Adressen müssen Sie keine privaten IPs in AWS zuweisen. Stattdessen werden die unverankerten IPs automatisch in der Routing-Tabelle von AWS konfiguriert, um die ENI eines bestimmten Nodes in derselben VPC zu zeigen.

Damit schwimmende IPs mit ONTAP zusammenarbeiten können, muss auf jeder Storage-VM auf jedem Node eine private IP-Adresse konfiguriert werden. Dies spiegelt sich in den nachstehenden Schritten wider, wo eine iSCSI LIF auf Knoten 1 und auf Knoten 2 erstellt wird.

Schritte

1. Erstellen Sie die Storage-VM und eine Route zur Storage-VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Erstellen Sie auf Node 1 ein NAS-LIF.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

   - Die fließende IP-Adresse muss sich für alle VPCs in der AWS Region, in der Sie die HA-Konfiguration implementieren, außerhalb der CIDR-Blöcke befinden. 192.168.209.27 ist ein Beispiel für eine unverankerte IP-Adresse. "Erfahren Sie mehr über die Auswahl einer fließenden IP-Adresse".
   - `-service-policy default-data-files` Zeigt an, dass IPs auf den Partner-Node migrieren können.

3. Optional: Erstellen Sie eine Storage-VM-Management-LIF auf Node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. Erstellen Sie auf Knoten 1 ein iSCSI-LIF.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask nodei1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

   - Diese iSCSI-LIF ist erforderlich, um die LIF-Migration der Floating-IPs in der Storage-VM zu unterstützen. Er muss keine iSCSI LIF sein, kann aber nicht für die Migration zwischen den Knoten konfiguriert werden.
   - `-service-policy default-data-block` Zeigt an, dass eine IP-Adresse nicht zwischen Knoten migriert wird.
   - *Private_ip* ist eine nicht verwendete sekundäre private IP-Adresse auf eth0 (e0a) von cvo_node1.

5. Erstellen Sie auf Knoten 2 ein iSCSI-LIF.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif
ip_node2_iscsi_2 -home-node cvo-node2
```

- Diese iSCSI-LIF ist erforderlich, um die LIF-Migration der Floating-IPs in der Storage-VM zu unterstützen. Er muss keine iSCSI LIF sein, kann aber nicht für die Migration zwischen den Knoten konfiguriert werden.
- `-service-policy default-data-block` Zeigt an, dass eine IP-Adresse nicht zwischen Knoten migriert wird.
- *Private_ip* ist eine nicht verwendete sekundäre private IP-Adresse auf eth0 (e0a) von cvo_node2.

6. Weisen Sie der Storage-VM ein oder mehrere Aggregate zu.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Dieser Schritt ist erforderlich, da die neue Storage-VM Zugriff auf mindestens ein Aggregat benötigt, bevor Sie Volumes auf der Storage-VM erstellen können.

7. Wenn Sie Cloud Volumes ONTAP 9.11.1 oder höher verwenden, ändern Sie die Netzwerk-Service-Richtlinien für die Storage VM.

Das Ändern der Services ist erforderlich, da Cloud Volumes ONTAP sicherstellen kann, dass die iSCSI-LIF für ausgehende Managementverbindungen verwendet werden kann.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

Erstellen Sie Daten-Serving-Storage VMs für Cloud Volumes ONTAP in Azure

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 bei der Ausführung von Cloud Volumes ONTAP in Azure werden zusätzliche Storage-VMs unterstützt.

Um zusätzliche Storage VMs für Daten zu erstellen, müssen Sie IP-Adressen in Azure zuweisen und anschließend ONTAP Befehle ausführen, um die Storage-VM und Daten-LIFs zu erstellen.

Um weitere NIC-bezogene Aufgaben auszuführen, können Sie eine Rolle für den Netzwerkbeitrag oder eine benutzerdefinierte Rolle mit den entsprechenden Berechtigungen in Azure zuweisen. Weitere Informationen zu diesen NIC-bezogenen Berechtigungen finden Sie im "Microsoft Azure-Dokumentation".

Unterstützte Anzahl von Storage-VMs

Ab Version 9.9.0 werden mehrere Storage-VMs mit spezifischen Cloud Volumes ONTAP Konfigurationen unterstützt. Wechseln Sie zum "Versionshinweise zu Cloud Volumes ONTAP" Um zu überprüfen, wie viele Storage VMs für Ihre Cloud Volumes ONTAP-Version unterstützt werden.

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 Datenzugriff aktivieren, wenn es einen Ausfall auf der Quell-Storage-VM gibt.

Weisen Sie IP-Adressen in Azure zu

Bevor Sie eine Storage-VM erstellen und LIFs zuweisen, müssen Sie in Azure IP-Adressen zuweisen.

Single Node-System

IP-Adressen müssen nic0 in Azure zugewiesen werden, bevor Sie eine Storage-VM erstellen und LIFs zuweisen.

Sie müssen eine IP-Adresse für den Daten-LIF-Zugriff und eine weitere optionale IP-Adresse für eine Storage VM (SVM)-Management-LIF erstellen. Dieses Management-LIF bietet eine Verbindung zu Management-Tools wie SnapCenter.

Schritte

1. Melden Sie sich im Azure-Portal an und öffnen Sie den Service **Virtual Machine**.
2. Klicken Sie auf den Namen der Cloud Volumes ONTAP-VM.
3. Klicken Sie Auf **Networking**.
4. Klicken Sie auf den Namen der Netzwerkschnittstelle für nic0.
5. Klicken Sie unter **Einstellungen** auf **IP-Konfigurationen**.
6. Klicken Sie Auf **Hinzufügen**.
7. Geben Sie einen Namen für die IP-Konfiguration ein, wählen Sie **dynamisch** und klicken Sie dann auf **OK**.
8. Klicken Sie auf den Namen der gerade erstellten IP-Konfiguration, ändern Sie die **Zuordnung** in **statisch** und klicken Sie auf **Speichern**.

   Es empfiehlt sich, eine statische IP-Adresse zu verwenden, da eine statische IP sicherstellt, dass sich die IP-Adresse nicht ändert, was dazu beitragen kann, unnötige Ausfälle Ihrer Anwendung zu vermeiden.

Wenn Sie eine SVM-Management-LIF erstellen möchten, wiederholen Sie diese Schritte, um eine zusätzliche IP-Adresse zu erstellen.

Nachdem Sie fertig sind

Kopieren Sie die privaten IP-Adressen, die Sie gerade erstellt haben. Sie müssen diese IP-Adressen beim Erstellen von LIFs für die neue Storage-VM angeben.

HA-Paar

Wie Sie IP-Adressen für ein HA-Paar zuweisen, hängt vom verwendeten Storage-Protokoll ab.

ISCSI

ISCSI-IP-Adressen müssen nic0 in Azure zugewiesen werden, bevor Sie eine Storage-VM erstellen und LIFs zuweisen. IPS für iSCSI werden nic0 und nicht dem Load Balancer zugewiesen, da iSCSI ALUA für das Failover verwendet.

Sie müssen die folgenden IP-Adressen erstellen:

- Eine IP-Adresse für LIF-Zugriff auf iSCSI-Daten von Knoten 1
- Eine IP-Adresse für LIF-Zugriff auf iSCSI-Daten von Node 2
- Eine optionale IP-Adresse für eine Storage-VM (SVM)-Management-LIF

  Dieses Management-LIF bietet eine Verbindung zu Management-Tools wie SnapCenter.

Schritte

1. Melden Sie sich im Azure-Portal an und öffnen Sie den Service **Virtual Machine**.
2. Klicken Sie auf den Namen der Cloud Volumes ONTAP-VM für Node 1.
3. Klicken Sie Auf **Networking**.
4. Klicken Sie auf den Namen der Netzwerkschnittstelle für nic0.
5. Klicken Sie unter **Einstellungen** auf **IP-Konfigurationen**.
6. Klicken Sie Auf **Hinzufügen**.
7. Geben Sie einen Namen für die IP-Konfiguration ein, wählen Sie **dynamisch** und klicken Sie dann auf **OK**.
8. Klicken Sie auf den Namen der gerade erstellten IP-Konfiguration, ändern Sie die **Zuordnung** in **statisch** und klicken Sie auf **Speichern**.

   Es empfiehlt sich, eine statische IP-Adresse zu verwenden, da eine statische IP sicherstellt, dass sich die IP-Adresse nicht ändert, was dazu beitragen kann, unnötige Ausfälle Ihrer Anwendung zu vermeiden.

9. Wiederholen Sie diese Schritte auf Knoten 2.
10. Wenn Sie eine SVM-Management-LIF erstellen möchten, wiederholen Sie diese Schritte auf Node 1.

NFS

Die für NFS verwendeten IP-Adressen werden im Load Balancer zugewiesen, sodass bei einem Failover-Ereignis die IP-Adressen zu dem anderen Node migriert werden können.

Sie müssen die folgenden IP-Adressen erstellen:

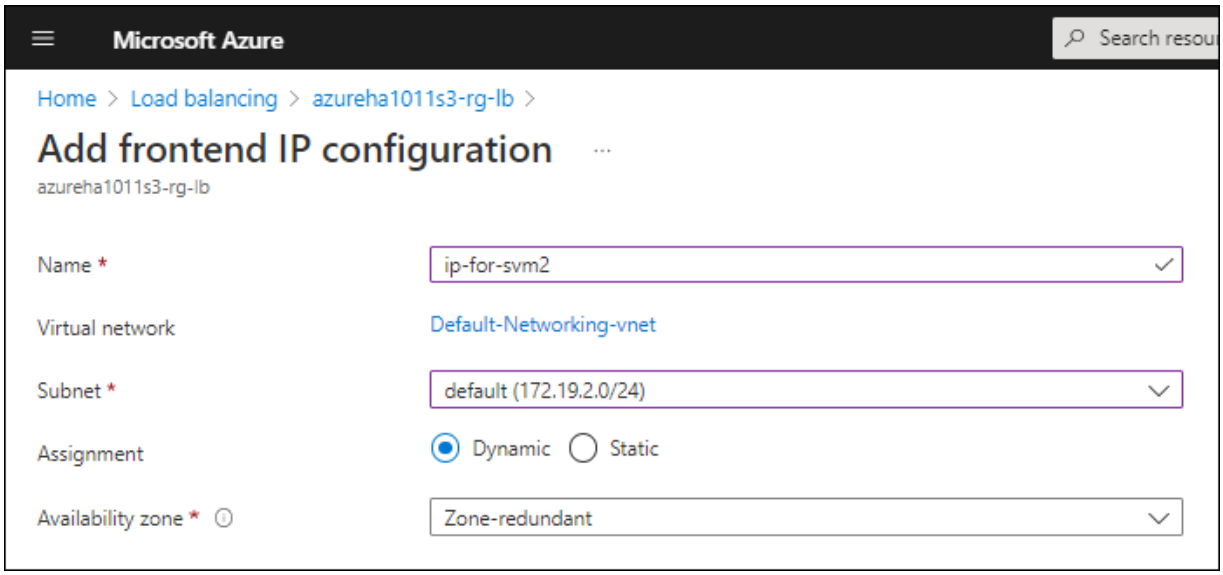
- Eine IP-Adresse für LIF-Zugriff auf NAS-Daten von Node 1
- Eine IP-Adresse für LIF-Zugriff auf NAS-Daten von Node 2
- Eine optionale IP-Adresse für eine Storage-VM (SVM)-Management-LIF

  Die iSCSI LIFs sind für die DNS-Kommunikation erforderlich. Dazu wird ein iSCSI-LIF verwendet, da bei einem Failover keine Migration durchgeführt wird.

  Dieses Management-LIF bietet eine Verbindung zu Management-Tools wie SnapCenter.

Schritte

1. Öffnen Sie im Azure-Portal den **Load Balancer**-Service.
2. Klicken Sie auf den Namen des Load Balancer für das HA-Paar.
3. Erstellung einer Frontend-IP-Konfiguration für den Daten-LIF-Zugriff von Node 1, eine andere für Daten-LIF-Zugriff von Node 2 und ein weiteres optionales Frontend-IP für eine Storage-VM (SVM)-Management-LIF.
   a. Klicken Sie unter **Einstellungen** auf **Frontend IP-Konfiguration**.
   b. Klicken Sie Auf **Hinzufügen**.
   c. Geben Sie einen Namen für die Frontend-IP ein, wählen Sie das Subnetz für das Cloud Volumes ONTAP HA-Paar aus, lassen Sie **dynamisch** ausgewählt, und lassen Sie in Regionen mit Verfügbarkeitszonen **Zone-redundant** die Option, um sicherzustellen, dass die IP-Adresse bei Ausfall einer Zone verfügbar bleibt.

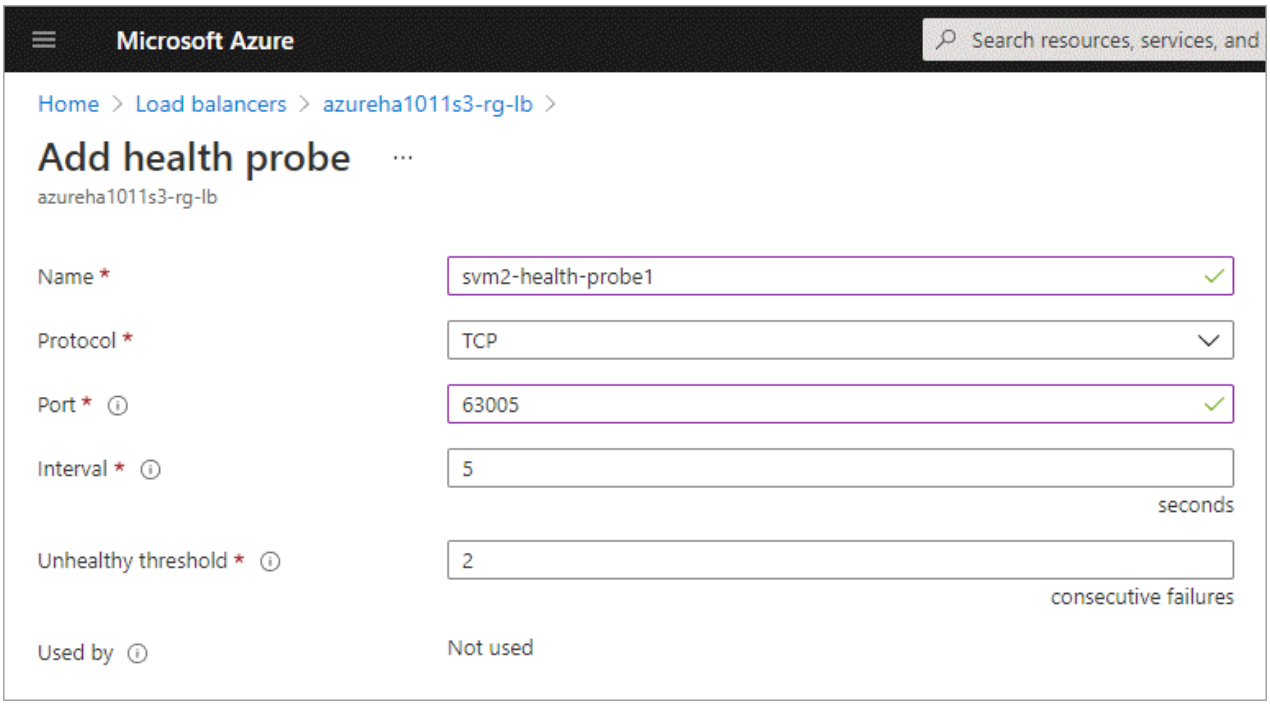


   d. Klicken Sie auf den Namen der gerade erstellten Frontend-IP-Konfiguration, ändern Sie die **Zuordnung** in **statisch** und klicken Sie auf **Speichern**.

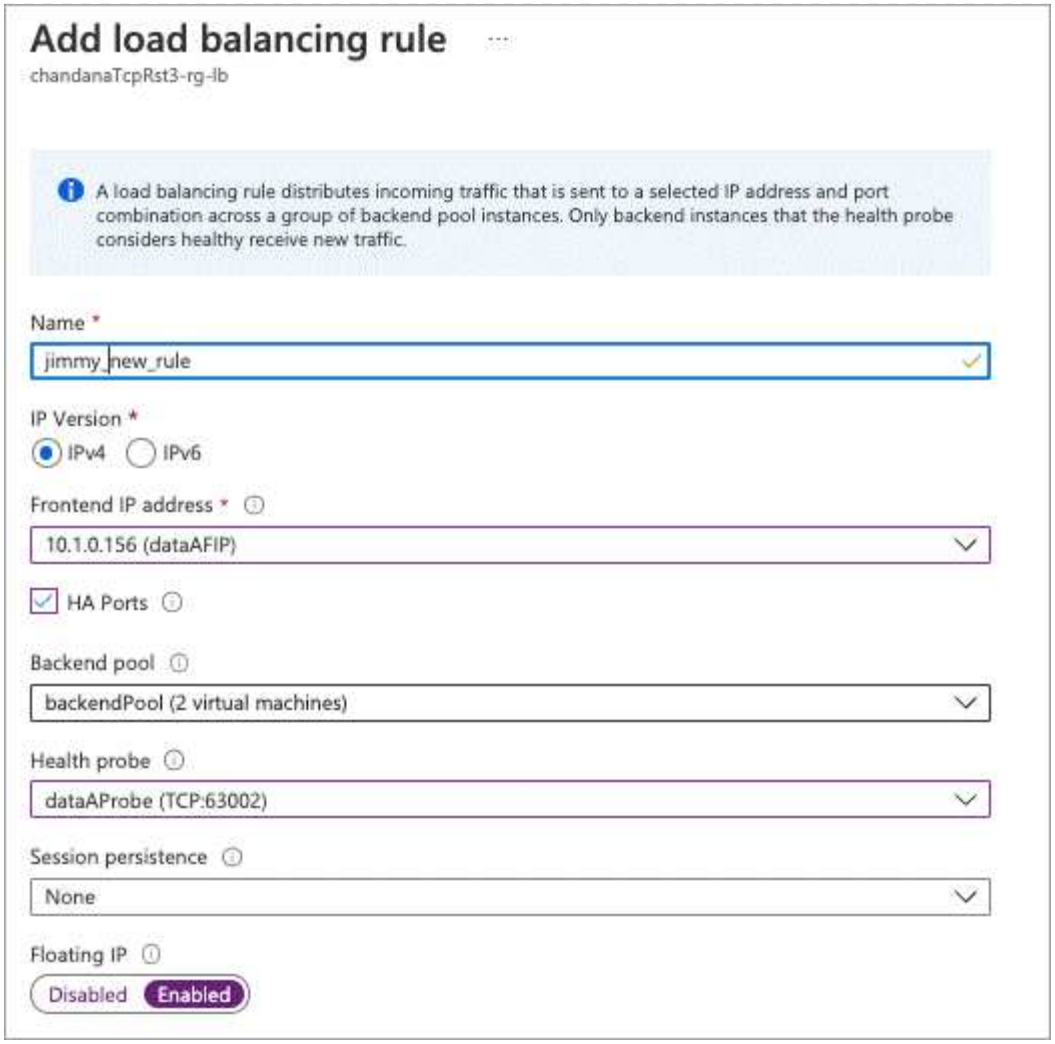
      Es empfiehlt sich, eine statische IP-Adresse zu verwenden, da eine statische IP sicherstellt, dass sich die IP-Adresse nicht ändert, was dazu beitragen kann, unnötige Ausfälle Ihrer Anwendung zu vermeiden.

4. Fügen Sie für jede gerade erstellte Frontend-IP eine Gesundheitssonde hinzu.
   a. Klicken Sie unter der Option **Einstellungen** des Load Balancer auf **Health Sonden**.
   b. Klicken Sie Auf **Hinzufügen**.
   c. Geben Sie einen Namen für die Gesundheitssonde ein, und geben Sie eine Portnummer zwischen 63005 und 65000 ein. Behalten Sie die Standardwerte für die anderen Felder bei.

      Es ist wichtig, dass die Portnummer zwischen 63005 und 65000 liegt. Wenn Sie beispielsweise drei Integritätssonden erstellen, können Sie Sonden eingeben, die die Portnummern 63005, 63006 und 63007 verwenden.



5. Erstellen neuer Regeln für den Lastausgleich für jedes Frontend-IP.
   a. Klicken Sie unter dem Load Balancer **Einstellungen** auf **Load Balancing rules**.
   b. Klicken Sie auf **Hinzufügen** und geben Sie die erforderlichen Informationen ein:
      - **Name**: Geben Sie einen Namen für die Regel ein.
      - **IP-Version**: Wählen Sie **IPv4**.
      - **Frontend IP-Adresse**: Wählen Sie eine der Front-end-IP-Adressen, die Sie gerade erstellt haben.
      - **HA-Ports**: Aktivieren Sie diese Option.
      - **Back-End-Pool**: Behalten Sie den bereits ausgewählten Standard-Back-End-Pool.
      - **Health Probe**: Wählen Sie die Gesundheitssonde aus, die Sie für die ausgewählte Frontend-IP erstellt haben.
      - **Sitzungspersistenz**: Wählen Sie **Keine**.
      - **Schwimmende IP**: Wählen Sie **aktiviert**.



6. Stellen Sie sicher, dass die Netzwerksicherheitsgruppenregeln für Cloud Volumes ONTAP es dem Load Balancer ermöglichen, TCP-Sonden für die in Schritt 4 erstellten Gesundheitssonden zu senden. Beachten Sie, dass dies standardmäßig zulässig ist.

SMB

Die für SMB-Daten verwendeten IP-Adressen werden im Load Balancer zugewiesen, sodass die IP-Adressen bei einem Failover-Ereignis auf den anderen Node migriert werden können.

Sie müssen die folgenden IP-Adressen im Load Balancer erstellen:

- Eine IP-Adresse für LIF-Zugriff auf NAS-Daten von Node 1
- Eine IP-Adresse für LIF-Zugriff auf NAS-Daten von Node 2
- Eine IP-Adresse für eine iSCSI-LIF auf Node 1 in der jeweiligen NIC0 jeder VM
- Eine IP-Adresse für eine iSCSI-LIF auf Knoten 2

  Die iSCSI LIFs sind für die DNS- und SMB-Kommunikation erforderlich. Dazu wird ein iSCSI-LIF verwendet, da bei einem Failover keine Migration durchgeführt wird.

- Eine optionale IP-Adresse für eine Storage-VM (SVM)-Management-LIF

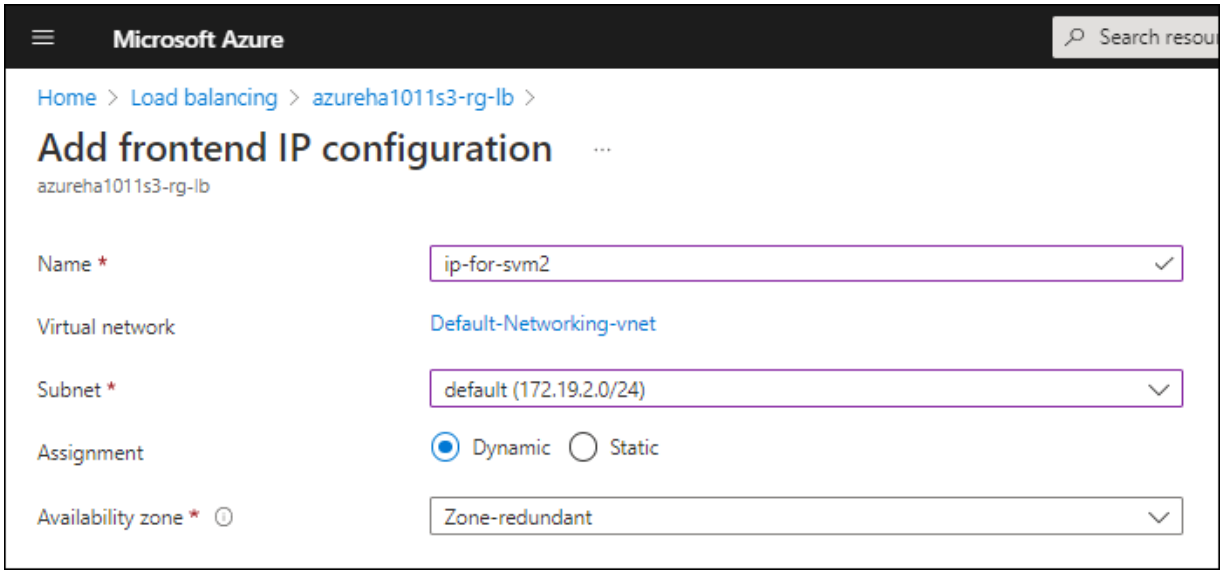
  Dieses Management-LIF bietet eine Verbindung zu Management-Tools wie SnapCenter.

Schritte

1. Öffnen Sie im Azure-Portal den **Load Balancer**-Service.
2. Klicken Sie auf den Namen des Load Balancer für das HA-Paar.
3. Erstellen Sie nur für die Daten und SVM-LIFs die erforderliche Anzahl von Frontend-IP-Konfigurationen:

   Eine Frontend-IP sollte nur unter der NIC0 für jede entsprechende SVM angelegt werden. Weitere Informationen zum Hinzufügen der IP-Adresse zum SVM NIC0 finden Sie unter „Schritt 7 [Hyperlink]“.

   a. Klicken Sie unter **Einstellungen** auf **Frontend IP-Konfiguration**.
   b. Klicken Sie Auf **Hinzufügen**.
   c. Geben Sie einen Namen für die Frontend-IP ein, wählen Sie das Subnetz für das Cloud Volumes ONTAP HA-Paar aus, lassen Sie **dynamisch** ausgewählt, und lassen Sie in Regionen mit Verfügbarkeitszonen **Zone-redundant** die Option, um sicherzustellen, dass die IP-Adresse bei Ausfall einer Zone verfügbar bleibt.



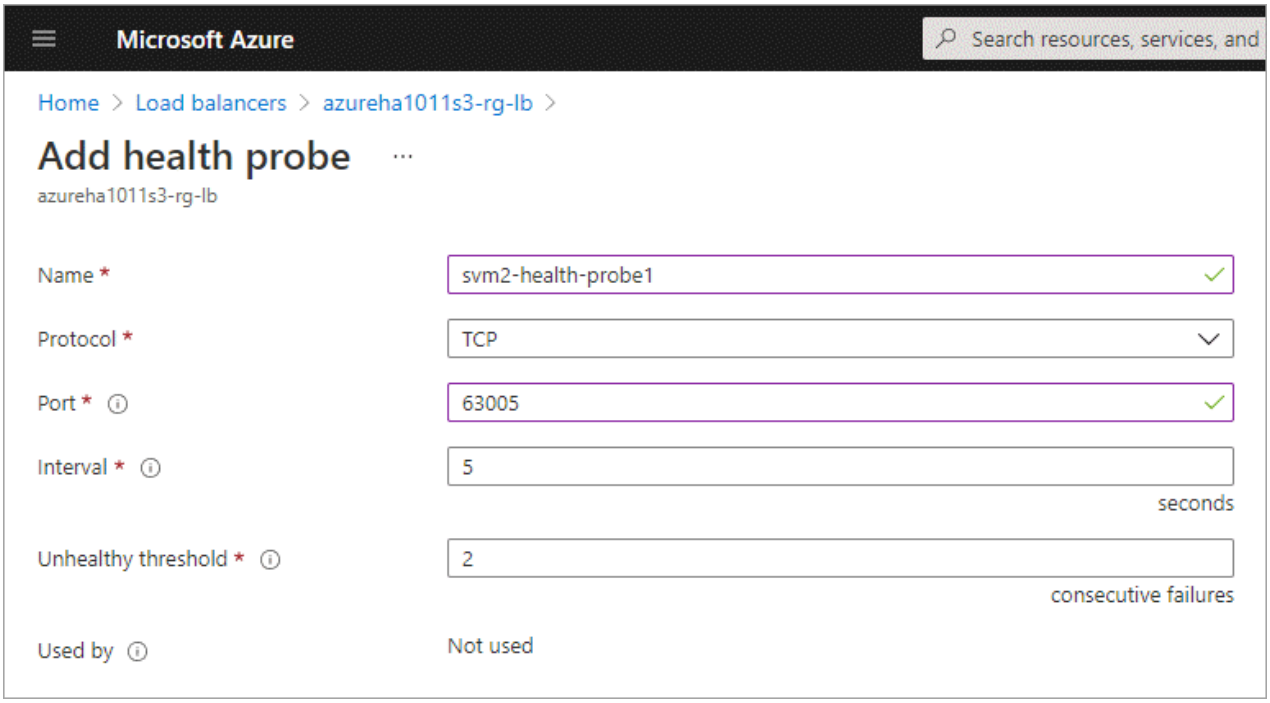
   d. Klicken Sie auf den Namen der gerade erstellten Frontend-IP-Konfiguration, ändern Sie die **Zuordnung** in **statisch** und klicken Sie auf **Speichern**.

      Es empfiehlt sich, eine statische IP-Adresse zu verwenden, da eine statische IP sicherstellt, dass sich die IP-Adresse nicht ändert, was dazu beitragen kann, unnötige Ausfälle Ihrer Anwendung zu vermeiden.

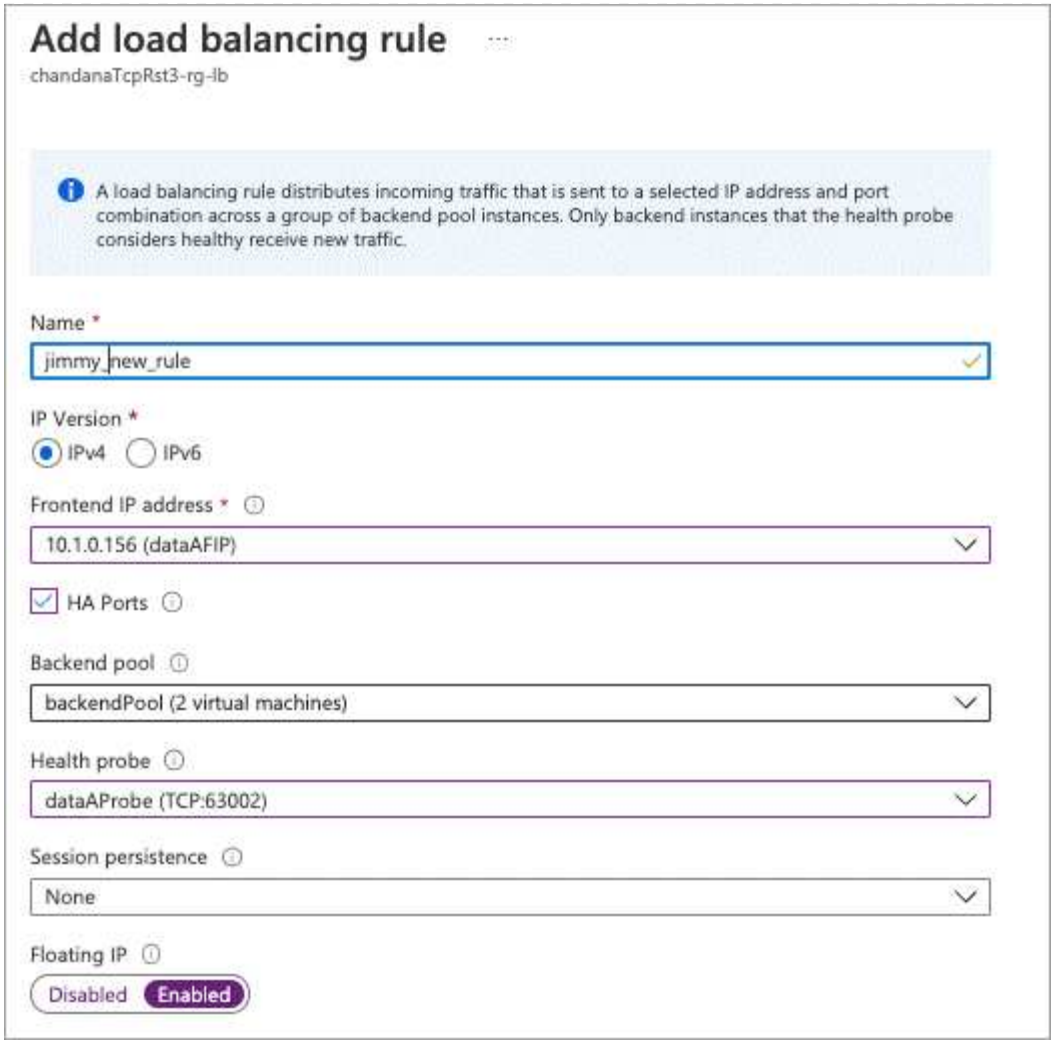
4. Fügen Sie für jede gerade erstellte Frontend-IP eine Gesundheitssonde hinzu.

   a. Klicken Sie unter der Option **Einstellungen** des Load Balancer auf **Health Sonden**.
   b. Klicken Sie Auf **Hinzufügen**.
   c. Geben Sie einen Namen für die Gesundheitssonde ein, und geben Sie eine Portnummer zwischen 63005 und 65000 ein. Behalten Sie die Standardwerte für die anderen Felder bei.

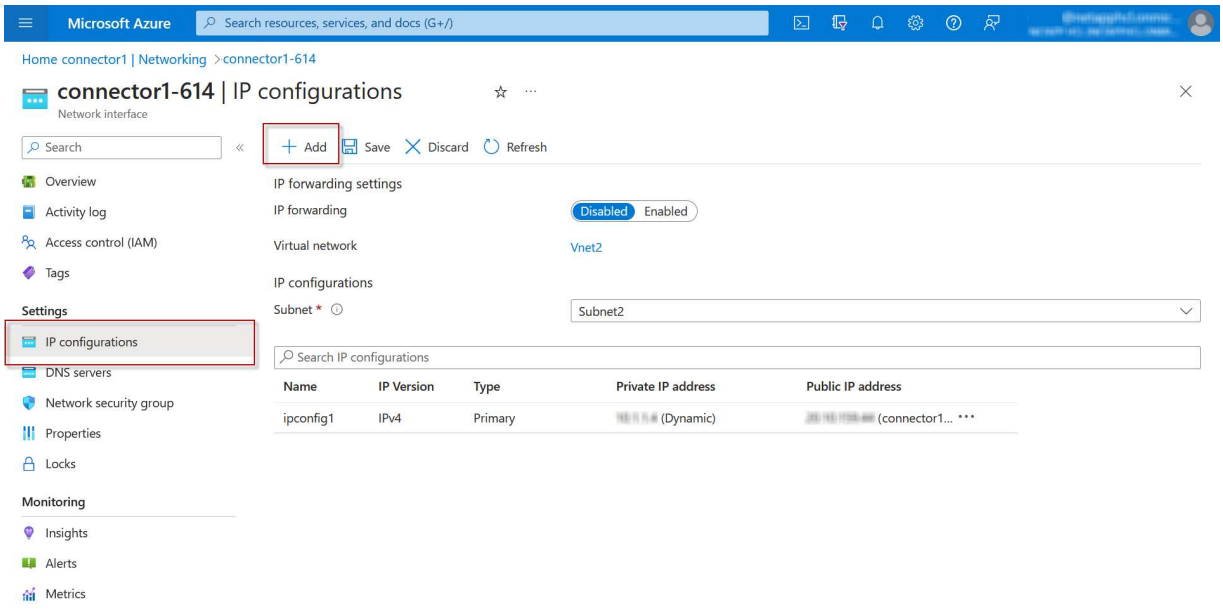
      Es ist wichtig, dass die Portnummer zwischen 63005 und 65000 liegt. Wenn Sie beispielsweise drei Integritätssonden erstellen, können Sie Sonden eingeben, die die Portnummern 63005, 63006 und 63007 verwenden.



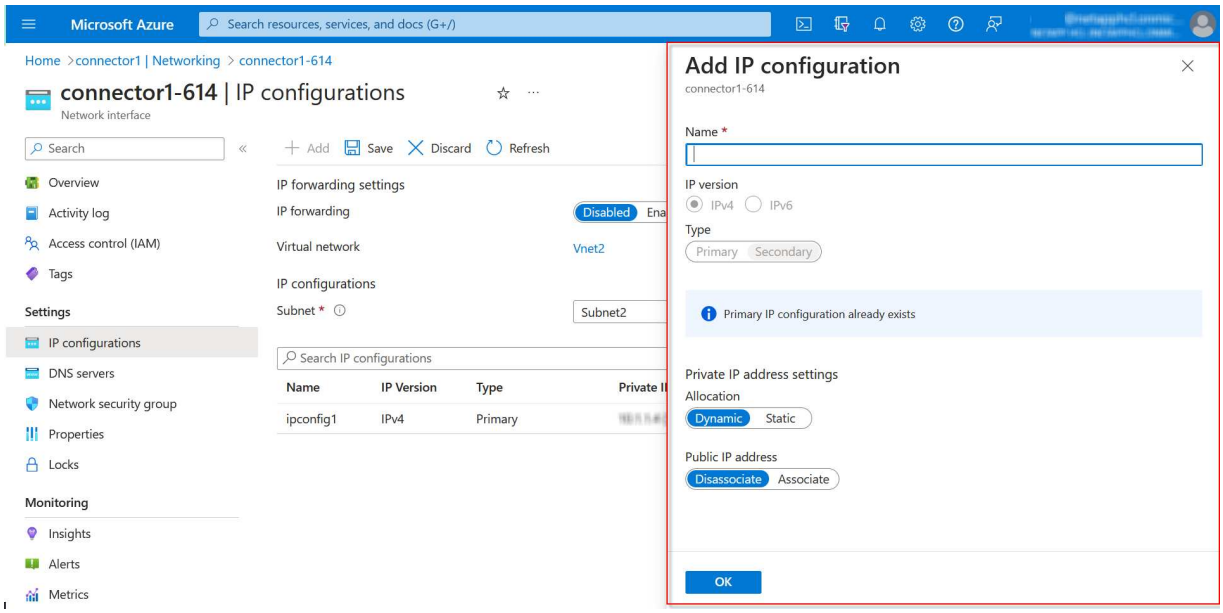
5. Erstellen neuer Regeln für den Lastausgleich für jedes Frontend-IP.
   a. Klicken Sie unter dem Load Balancer **Einstellungen** auf **Load Balancing rules**.
   b. Klicken Sie auf **Hinzufügen** und geben Sie die erforderlichen Informationen ein:
      - **Name**: Geben Sie einen Namen für die Regel ein.
      - **IP-Version**: Wählen Sie **IPv4**.
      - **Frontend IP-Adresse**: Wählen Sie eine der Front-end-IP-Adressen, die Sie gerade erstellt haben.
      - **HA-Ports**: Aktivieren Sie diese Option.
      - **Back-End-Pool**: Behalten Sie den bereits ausgewählten Standard-Back-End-Pool.
      - **Health Probe**: Wählen Sie die Gesundheitssonde aus, die Sie für die ausgewählte Frontend-IP erstellt haben.
      - **Sitzungspersistenz**: Wählen Sie **Keine**.
      - **Schwimmende IP**: Wählen Sie **aktiviert**.



6. Stellen Sie sicher, dass die Netzwerksicherheitsgruppenregeln für Cloud Volumes ONTAP es dem Load Balancer ermöglichen, TCP-Sonden für die in Schritt 4 erstellten Gesundheitssonden zu senden. Beachten Sie, dass dies standardmäßig zulässig ist.
7. Fügen Sie für iSCSI LIFs die IP-Adresse für NIC0 hinzu.
   a. Klicken Sie auf den Namen der Cloud Volumes ONTAP-VM.
   b. Klicken Sie Auf **Networking**.
   c. Klicken Sie auf den Namen der Netzwerkschnittstelle für nic0.
   d. Klicken Sie unter Einstellungen auf **IP-Konfigurationen**.
   e. Klicken Sie Auf **Hinzufügen**.



f. Geben Sie einen Namen für die IP-Konfiguration ein, wählen Sie dynamisch aus, und klicken Sie dann auf **OK**.



g. Klicken Sie auf den Namen der gerade erstellten IP-Konfiguration, ändern Sie die Zuweisung zu statisch und klicken Sie auf **Speichern**.

Es empfiehlt sich, eine statische IP-Adresse zu verwenden, da eine statische IP sicherstellt, dass sich die IP-Adresse nicht ändert, was dazu beitragen kann, unnötige Ausfälle Ihrer Anwendung zu vermeiden.

Nachdem Sie fertig sind

Kopieren Sie die privaten IP-Adressen, die Sie gerade erstellt haben. Sie müssen diese IP-Adressen beim Erstellen von LIFs für die neue Storage-VM angeben.

Erstellung einer Storage-VM und logischer Schnittstellen

Nachdem Sie in Azure IP-Adressen zugewiesen haben, können Sie eine neue Storage-VM auf einem Single Node-System oder auf einem HA-Paar erstellen.

Single Node-System

Wie Sie eine Storage-VM und LIFs auf einem einzelnen Node-System erstellen, hängt vom verwendeten Storage-Protokoll ab.

ISCSI

Befolgen Sie diese Schritte, um eine neue Storage-VM zusammen mit den erforderlichen LIFs zu erstellen.

Schritte

1. Erstellen Sie die Storage-VM und eine Route zur Storage-VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0
-gateway <ip-of-gateway-server>
```

2. Daten-LIF erstellen:

```
network interface create -vserver <svm-name> -home-port e0a -address
<iscsi-ip-address> -netmask-length <# of mask bits> -lif <lif-name>
-home-node <name-of-node1> -data-protocol iscsi
```

3. Optional: Erstellen Sie eine Storage-VM-Management-LIF.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. Weisen Sie der Storage-VM ein oder mehrere Aggregate zu.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

   Dieser Schritt ist erforderlich, da die neue Storage-VM Zugriff auf mindestens ein Aggregat benötigt, bevor Sie Volumes auf der Storage-VM erstellen können.

NFS

Befolgen Sie diese Schritte, um eine neue Storage-VM zusammen mit den erforderlichen LIFs zu erstellen.

Schritte

1. Erstellen Sie die Storage-VM und eine Route zur Storage-VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0
-gateway <ip-of-gateway-server>
```

2. Daten-LIF erstellen:

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nas-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

3. Optional: Erstellen Sie eine Storage-VM-Management-LIF.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. Weisen Sie der Storage-VM ein oder mehrere Aggregate zu.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Dieser Schritt ist erforderlich, da die neue Storage-VM Zugriff auf mindestens ein Aggregat benötigt, bevor Sie Volumes auf der Storage-VM erstellen können.

SMB

Befolgen Sie diese Schritte, um eine neue Storage-VM zusammen mit den erforderlichen LIFs zu erstellen.

Schritte

1. Erstellen Sie die Storage-VM und eine Route zur Storage-VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0
-gateway <ip-of-gateway-server>
```

2. Daten-LIF erstellen:

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nas-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

3. Optional: Erstellen Sie eine Storage-VM-Management-LIF.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. Weisen Sie der Storage-VM ein oder mehrere Aggregate zu.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Dieser Schritt ist erforderlich, da die neue Storage-VM Zugriff auf mindestens ein Aggregat benötigt, bevor Sie Volumes auf der Storage-VM erstellen können.

HA-Paar

Wie Sie eine Storage-VM und LIFs auf einem HA-Paar erstellen, hängt vom verwendeten Storage-Protokoll ab.

ISCSI

Befolgen Sie diese Schritte, um eine neue Storage-VM zusammen mit den erforderlichen LIFs zu erstellen.

Schritte

1. Erstellen Sie die Storage-VM und eine Route zur Storage-VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0
-gateway <ip-of-gateway-server>
```

2. Daten-LIFs erstellen:

   a. Verwenden Sie den folgenden Befehl, um eine iSCSI-LIF auf Knoten 1 zu erstellen.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

   b. Verwenden Sie den folgenden Befehl, um eine iSCSI-LIF auf Knoten 2 zu erstellen.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

3. Optional: Erstellen Sie eine Storage-VM-Management-LIF auf Node 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

   Dieses Management-LIF bietet eine Verbindung zu Management-Tools wie SnapCenter.

4. Weisen Sie der Storage-VM ein oder mehrere Aggregate zu.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Dieser Schritt ist erforderlich, da die neue Storage-VM Zugriff auf mindestens ein Aggregat benötigt, bevor Sie Volumes auf der Storage-VM erstellen können.

5. Wenn Sie Cloud Volumes ONTAP 9.11.1 oder höher verwenden, ändern Sie die Netzwerk-Service-Richtlinien für die Storage VM.

   a. Geben Sie den folgenden Befehl ein, um auf den erweiterten Modus zuzugreifen.

      ```
      ::> set adv -con off
      ```

      Das Ändern der Services ist erforderlich, da Cloud Volumes ONTAP sicherstellen kann, dass die iSCSI-LIF für ausgehende Managementverbindungen verwendet werden kann.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

NFS

Befolgen Sie diese Schritte, um eine neue Storage-VM zusammen mit den erforderlichen LIFs zu erstellen.

Schritte

1. Erstellen Sie die Storage-VM und eine Route zur Storage-VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0
-gateway <ip-of-gateway-server>
```

2. Daten-LIFs erstellen:
   a. Verwenden Sie den folgenden Befehl, um eine NAS-LIF auf Knoten 1 zu erstellen.

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node1> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe1>
```

   b. Verwenden Sie den folgenden Befehl, um eine NAS-LIF auf Knoten 2 zu erstellen.

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node2> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe2>
```

3. ISCSI LIFs erstellen, um DNS-Kommunikation bereitzustellen:
   a. Verwenden Sie den folgenden Befehl, um eine iSCSI-LIF auf Knoten 1 zu erstellen.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

   b. Verwenden Sie den folgenden Befehl, um eine iSCSI-LIF auf Knoten 2 zu erstellen.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

4. Optional: Erstellen Sie eine Storage-VM-Management-LIF auf Node 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

Dieses Management-LIF bietet eine Verbindung zu Management-Tools wie SnapCenter.

5. Optional: Erstellen Sie eine Storage-VM-Management-LIF auf Node 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

Dieses Management-LIF bietet eine Verbindung zu Management-Tools wie SnapCenter.

6. Weisen Sie der Storage-VM ein oder mehrere Aggregate zu.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Dieser Schritt ist erforderlich, da die neue Storage-VM Zugriff auf mindestens ein Aggregat benötigt, bevor Sie Volumes auf der Storage-VM erstellen können.

7. Wenn Sie Cloud Volumes ONTAP 9.11.1 oder höher verwenden, ändern Sie die Netzwerk-Service-Richtlinien für die Storage VM.

   a. Geben Sie den folgenden Befehl ein, um auf den erweiterten Modus zuzugreifen.

```
::> set adv -con off
```

Das Ändern der Services ist erforderlich, da Cloud Volumes ONTAP sicherstellen kann, dass die iSCSI-LIF für ausgehende Managementverbindungen verwendet werden kann.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

SMB

Befolgen Sie diese Schritte, um eine neue Storage-VM zusammen mit den erforderlichen LIFs zu erstellen.

Schritte

1. Erstellen Sie die Storage-VM und eine Route zur Storage-VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0
-gateway <ip-of-gateway-server>
```

2. NAS-Daten-LIFs erstellen:
   a. Verwenden Sie den folgenden Befehl, um eine NAS-LIF auf Knoten 1 zu erstellen.

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node1> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe1>
```

   b. Verwenden Sie den folgenden Befehl, um eine NAS-LIF auf Knoten 2 zu erstellen.

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node2> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe2>
```

3. ISCSI LIFs erstellen, um DNS-Kommunikation bereitzustellen:
   a. Verwenden Sie den folgenden Befehl, um eine iSCSI-LIF auf Knoten 1 zu erstellen.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

   b. Verwenden Sie den folgenden Befehl, um eine iSCSI-LIF auf Knoten 2 zu erstellen.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

4. Optional: Erstellen Sie eine Storage-VM-Management-LIF auf Node 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

Dieses Management-LIF bietet eine Verbindung zu Management-Tools wie SnapCenter.

5. Weisen Sie der Storage-VM ein oder mehrere Aggregate zu.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Dieser Schritt ist erforderlich, da die neue Storage-VM Zugriff auf mindestens ein Aggregat benötigt, bevor Sie Volumes auf der Storage-VM erstellen können.

6. Wenn Sie Cloud Volumes ONTAP 9.11.1 oder höher verwenden, ändern Sie die Netzwerk-Service-Richtlinien für die Storage VM.

   a. Geben Sie den folgenden Befehl ein, um auf den erweiterten Modus zuzugreifen.

   ```
   ::> set adv -con off
   ```

   Das Ändern der Services ist erforderlich, da Cloud Volumes ONTAP sicherstellen kann, dass die iSCSI-LIF für ausgehende Managementverbindungen verwendet werden kann.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

Was kommt als Nächstes?

Nachdem Sie eine Storage VM auf einem HA-Paar erstellt haben, warten Sie am besten 12 Stunden, bevor Sie Storage auf dieser SVM bereitstellen. Ab Version Cloud Volumes ONTAP 9.10.1 scannt BlueXP die Einstellungen für den Load Balancer eines HA-Paars in einem 12-Stunden-Intervall. Wenn neue SVMs vorhanden sind, aktiviert BlueXP eine Einstellung für kürzere ungeplante Failover.

Erstellen Sie Daten-Serving-Storage VMs für Cloud Volumes ONTAP in Google Cloud

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

In Google Cloud werden ab Version 9.11.1 mehrere Storage-VMs mit spezifischen Cloud Volumes ONTAP Konfigurationen unterstützt. Wechseln Sie zum "Versionshinweise zu Cloud Volumes ONTAP" Um zu überprüfen, wie viele Storage VMs für Ihre Cloud Volumes ONTAP-Version unterstützt werden.

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 Datenzugriff aktivieren, wenn es einen Ausfall auf der Quell-Storage-VM gibt.

Erstellen einer Storage-VM

Wenn Ihre Lizenz unterstützt wird, können Sie mehrere Storage-VMs auf einem System mit einzelnen Nodes oder auf einem HA-Paar erstellen. Beachten Sie, dass Sie die BlueXP API zum Erstellen einer Storage-VM auf einem HA-Paar verwenden müssen, während Sie mit der CLI oder mit System Manager eine Storage-VM auf einem System mit einem einzelnen Node erstellen können.

Single Node-System

Mit diesen Schritten wird eine neue Storage-VM auf einem System mit einem einzelnen Node mithilfe der CLI erstellt. Eine private IP-Adresse ist erforderlich, um eine Daten-LIF zu erstellen, und eine weitere optionale private IP-Adresse ist erforderlich, um eine Management-LIF zu erstellen.

Schritte

1. Gehen Sie in Google Cloud zur Cloud Volumes ONTAP-Instanz und fügen Sie nic0 für jede LIF eine IP-Adresse hinzu.

Sie benötigen eine IP-Adresse für eine Daten-LIF und eine andere optionale IP-Adresse, wenn Sie eine Management-LIF auf der Storage-VM erstellen möchten.

"Google Cloud Dokumentation: Hinzufügen von Alias-IP-Bereichen zu einer bestehenden Instanz"

2. Erstellen Sie die Storage-VM und eine Route zur Storage-VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-
volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway
<ip-of-gateway-server>
```

3. Erstellen Sie eine Daten-LIF, indem Sie die IP-Adresse angeben, die Sie in Google Cloud hinzugefügt haben.

ISCSI

```
network interface create -vserver <svm-name> -home-port e0a -address
<iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data
-protocol iscsi
```

NFS oder SMB

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

4. Optional: Erstellen Sie eine Storage-VM-Management-LIF, indem Sie die IP-Adresse angeben, die Sie in Google Cloud hinzugefügt haben.

```
network interface create -vserver <svm-name> -lif <lif-name> -role data
-data-protocol none -address <svm-mgmt-ip-address> -netmask-length
<length> -home-node <name-of-node1> -status-admin up -failover-policy
system-defined -firewall-policy mgmt -home-port e0a -auto-revert false
-failover-group Default
```

5. Weisen Sie der Storage-VM ein oder mehrere Aggregate zu.

```
vserver add-aggregates -vserver <svm-name> -aggregates <aggr1,aggr2>
```

Dieser Schritt ist erforderlich, da die neue Storage-VM Zugriff auf mindestens ein Aggregat benötigt, bevor Sie Volumes auf der Storage-VM erstellen können.

HA-Paar

Sie müssen die BlueXP API verwenden, um eine Speicher-VM auf einem Cloud Volumes ONTAP-System in Google Cloud zu erstellen. Die Verwendung der API (und nicht System Manager oder die CLI) ist erforderlich, da BlueXP die Storage VM mit den erforderlichen LIF-Diensten konfiguriert, sowie eine für die ausgehende SMB/CIFS-Kommunikation erforderliche iSCSI-LIF.

Beachten Sie, dass BlueXP die erforderlichen IP-Adressen in Google Cloud zuweist und die Storage VM mit einer Daten-LIF für SMB/NFS-Zugriff und einer iSCSI LIF für ausgehende SMB-Kommunikation erstellt.

Erforderliche Google Cloud Berechtigungen

Für den Connector sind bestimmte Berechtigungen erforderlich, um Storage-VMs für Cloud Volumes ONTAP

HA-Paare zu erstellen und zu managen. Die erforderlichen Berechtigungen sind in enthalten "Die von NetApp bereitgestellten Richtlinien".

Schritte

1. Verwenden Sie den folgenden API-Aufruf, um eine Storage-VM zu erstellen:

   ```
   POST /occm/api/gcp/ha/working-environments/{WE_ID}/svm/
   ```

   Der Anforderungsgremium sollte Folgendes umfassen:

   ```
   { "svmName": "myNewSvm1" }
   ```

Managen Sie Storage VMs auf HA-Paaren

Die BlueXP API unterstützt auch das Umbenennen und Löschen von Storage-VMs auf HA-Paaren.

Benennen Sie eine Storage-VM um

Bei Bedarf können Sie den Namen einer Storage-VM jederzeit ändern.

Schritte

1. Verwenden Sie den folgenden API-Aufruf, um eine Storage-VM umzubenennen:

   ```
   PUT /occm/api/gcp/ha/working-environments/{WE_ID}/svm
   ```

   Der Anforderungsgremium sollte Folgendes umfassen:

   ```
   {
   "svmNewName": "newSvmName",
   "svmName": "oldSvmName"
   }
   ```

Löschen einer Speicher-VM

Wenn Sie keine Storage-VM mehr benötigen, können Sie sie aus Cloud Volumes ONTAP löschen.

Schritte

1. Verwenden Sie den folgenden API-Aufruf, um eine Storage-VM zu löschen:

   ```
   DELETE /occm/api/gcp/ha/working-environments/{WE_ID}/svm/{SVM_NAME}
   ```

Disaster Recovery für SVMs einrichten

BlueXP bietet keine Unterstützung für die Einrichtung oder Orchestrierung von Disaster Recovery für Storage VMs (SVM). Sie müssen System Manager oder die CLI verwenden.

Wenn Sie die SnapMirror SVM-Replizierung zwischen zwei Cloud Volumes ONTAP Systemen einrichten, muss die Replizierung zwischen zwei HA-Paar-Systemen oder zwei Single Node-Systemen erfolgen. Sie können

keine SnapMirror SVM-Replizierung zwischen einem HA-Paar und einem System mit einem einzelnen Node einrichten.

CLI-Anweisungen finden Sie in den folgenden Dokumenten.

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

Sicherheit und Datenverschlüsselung

Verschlüsseln von Volumes mit NetApp Verschlüsselungslösungen

Cloud Volumes ONTAP unterstützt NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE). NVE und NAE sind softwarebasierte Lösungen, die die Verschlüsselung von Daten im Ruhezustand nach FIPS 140 ermöglichen. "Weitere Informationen zu diesen Verschlüsselungslösungen".

Sowohl NVE als auch NAE werden von einem externen Schlüsselmanager unterstützt.

Schlüsselmanagement mit AWS Key Management Service

Verwenden Sie können "AWS Key Management Service (KMS)" Zum Schutz Ihrer ONTAP Verschlüsselungen in einer über AWS bereitgestellten Applikation.

Verschlüsselungsmanagement mit AWS KMS kann über die CLI oder die ONTAP REST-API aktiviert werden.

Bei Verwendung des KMS ist zu beachten, dass standardmäßig die LIF einer Daten-SVM verwendet wird, um mit dem Endpunkt des Cloud-Schlüsselmanagements zu kommunizieren. Ein Node-Managementnetzwerk wird zur Kommunikation mit den Authentifizierungsdiensten von AWS verwendet. Wenn das Cluster-Netzwerk nicht korrekt konfiguriert ist, nutzt das Cluster den Verschlüsselungsmanagementservice nicht ordnungsgemäß.

Bevor Sie beginnen

- Cloud Volumes ONTAP muss Version 9.12.0 oder höher ausführen
- Sie müssen die Volume Encryption (VE)-Lizenz und installiert haben
- Sie müssen die MTEKM-Lizenz (Multi-Tenant Encryption Key Management) installiert haben.
- Sie müssen ein Cluster- oder SVM-Administrator sein
- Sie müssen über ein aktives AWS-Abonnement verfügen

Schlüssel können nur für eine Daten-SVM konfiguriert werden.

Konfiguration

AWS

1. Sie müssen einen erstellen "Gewähren" Für den AWS-KMS-Schlüssel, der von der IAM-Rolle zum Managen der Verschlüsselung verwendet wird. Die IAM-Rolle muss eine Richtlinie enthalten, die die folgenden Operationen zulässt:
   - `DescribeKey`

- `Encrypt`
- `Decrypt`
  Informationen zum Erstellen einer Erteilung finden Sie unter "AWS-Dokumentation".

2. "Fügen Sie der entsprechenden IAM-Rolle eine Richtlinie hinzu." Die Politik sollte die unterstützen `DescribeKey`, `Encrypt`, und `Decrypt` Betrieb:

Cloud Volumes ONTAP

1. Wechseln Sie zu Ihrer Cloud Volumes ONTAP Umgebung.
2. Wechseln zur erweiterten Berechtigungsebene:
   `set -privilege advanced`
3. Aktivieren Sie den AWS Schlüsselmanager:
   `security key-manager external aws enable -vserver` *`data_svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Geben Sie den geheimen Schlüssel ein, wenn Sie dazu aufgefordert werden.
5. Überprüfen Sie, ob der AWS-KMS ordnungsgemäß konfiguriert wurde:
   `security key-manager external aws show -vserver` *`svm_name`*

Verschlüsselungsmanagement mit Azure Key Vault

Verwenden Sie können "Azure Key Vault (AKV)" Um Ihre ONTAP Verschlüsselungen in einer von Azure implementierten Applikation zu schützen.

AKV kann zum Schutz verwendet werden "NetApp Volume Encryption (NVE)-Schlüssel" Nur für Data SVMs.

Die Schlüsselverwaltung mit AKV kann über die CLI oder die ONTAP REST API aktiviert werden.

Bei Verwendung von AKV ist zu beachten, dass standardmäßig eine LIF der Daten-SVM zur Kommunikation mit dem Endpunkt des Cloud-Verschlüsselungsmanagement verwendet wird. Zur Kommunikation mit den Authentifizierungsservices des Cloud-Providers wird ein Node-Managementnetzwerk verwendet (login.microsoftonline.com). Wenn das Cluster-Netzwerk nicht korrekt konfiguriert ist, nutzt das Cluster den Verschlüsselungsmanagementservice nicht ordnungsgemäß.

Bevor Sie beginnen

- Cloud Volumes ONTAP muss Version 9.10.1 oder höher ausführen
- Volume Encryption (VE)-Lizenz ist installiert. (NetApp Volume Encryption-Lizenz wird automatisch auf jedem Cloud Volumes ONTAP System installiert, das beim NetApp Support registriert ist).
- Sie benötigen eine Multi-Tenant Encryption Key Management (MT_EK_MGMT)-Lizenz
- Sie müssen ein Cluster- oder SVM-Administrator sein
- Ein Active Azure Abonnement

Einschränkungen

- AKV kann nur auf einer Daten-SVM konfiguriert werden
- NAE kann nicht mit AKV verwendet werden. NAE erfordert einen extern unterstützten KMIP-Server.

Konfigurationsprozess

In den beschriebenen Schritten wird erfasst, wie Sie Ihre Cloud Volumes ONTAP Konfiguration bei Azure

registrieren sowie wie ein Azure SchlüsselVault und -Schlüssel erstellt werden. Wenn Sie diese Schritte bereits ausgeführt haben, stellen Sie sicher, dass Sie über die richtigen Konfigurationseinstellungen verfügen, insbesondere in Erstellen Sie einen Azure Key Vault, Und dann weiter zu Cloud Volumes ONTAP-Konfiguration.

- Azure Application Registration
- Azure-Client Secret erstellen
- Erstellen Sie einen Azure Key Vault
- Erstellen eines Verschlüsselungsschlüssels
- Azure Active Directory Endpunkt erstellen (nur HA)
- Cloud Volumes ONTAP-Konfiguration

Azure Application Registration

1. Zunächst müssen Sie Ihre Applikation im Azure Abonnement registrieren, das Cloud Volumes ONTAP für den Zugriff auf Azure SchlüsselVault verwenden soll. Wählen Sie im Azure-Portal die Option **App-Registrierungen** aus.
2. Wählen Sie **Neu registrieren**.
3. Geben Sie einen Namen für Ihre Anwendung ein, und wählen Sie einen unterstützten Anwendungstyp aus. Der standardmäßige einzelne Mandant ist für die Verwendung von Azure Key Vault ausreichend. Wählen Sie **Register**.
4. Wählen Sie im Fenster Azure Overview die Anwendung aus, die Sie registriert haben. Kopieren Sie die **Anwendung (Client) ID** und die **Verzeichnis-ID** an einen sicheren Ort. Diese werden später bei der Registrierung benötigt.

Azure-Client Secret erstellen

1. Wählen Sie im Azure-Portal für Ihre Azure Key Vault-App-Registrierung den Fensterbereich **Zertifikate & Geheimnisse** aus.
2. Wählen Sie **Neuer Client Secret**. Geben Sie einen aussagekräftigen Namen für Ihr Kundengeheimnis ein. NetApp empfiehlt einen 24-monatigen Verfallszeitraum. Ihre spezifischen Cloud Governance-Richtlinien erfordern jedoch unter Umständen eine andere Einstellung.
3. Klicken Sie auf **Hinzufügen**, um das Clientgeheimnis zu erstellen. Kopieren Sie die in der Spalte **Wert** aufgeführte geheime Zeichenfolge und speichern Sie sie an einem sicheren Ort zur späteren Verwendung in Cloud Volumes ONTAP-Konfiguration. Der geheime Wert wird nach der Navigation von der Seite nicht erneut angezeigt.

Erstellen Sie einen Azure Key Vault

1. Falls Sie bereits über einen Azure Schlüsselault verfügen, können Sie ihn mit Ihrer Cloud Volumes ONTAP Konfiguration verbinden. Die Zugriffsrichtlinien müssen jedoch an die Einstellungen in diesem Prozess angepasst werden.
2. Navigieren Sie im Azure-Portal zum Abschnitt **Key Vaults**.
3. Klicken Sie auf **+Erstellen** und geben Sie die erforderlichen Informationen einschließlich Ressourcengruppe, Region und Preisebene ein. Geben Sie außerdem die Anzahl der Tage ein, um gelöschte Vaults zu behalten, und wählen Sie **Spülschutz aktivieren** auf dem Schlüsselgewölbe aus.
4. Wählen Sie **Weiter**, um eine Zugriffsrichtlinie auszuwählen.
5. Wählen Sie die folgenden Optionen aus:
    a. Wählen Sie unter **Zugriffskonfiguration** die Zugriffspolitik **Vault** aus.

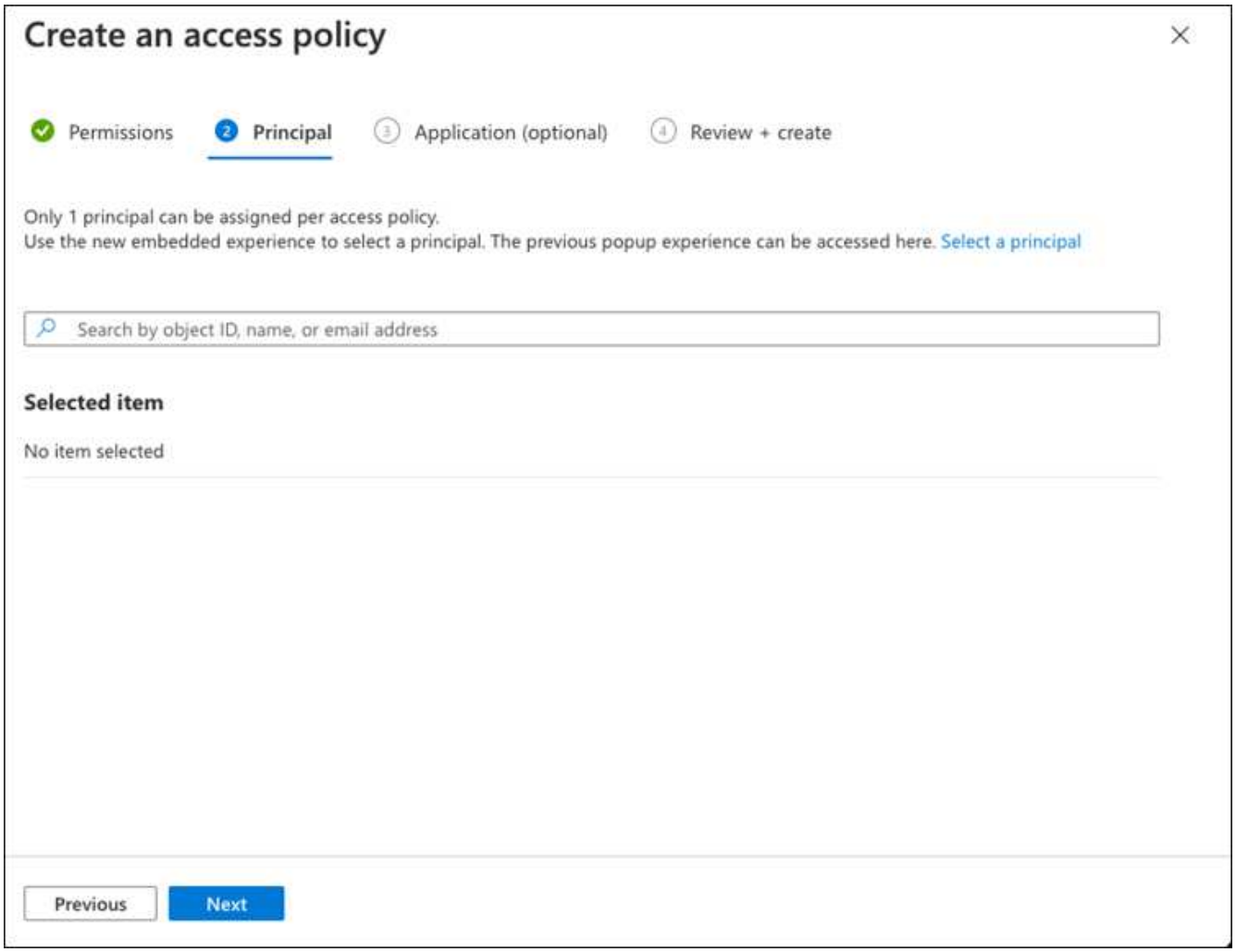
b. Wählen Sie unter **Resource Access Azure Disk Encryption für Volume Encryption** aus.

6. Wählen Sie **+Create**, um eine Zugriffsrichtlinie hinzuzufügen.
7. Klicken Sie unter **Konfigurieren aus einer Vorlage** auf das Dropdown-Menü und wählen Sie dann die Vorlage **Schlüssel, Schlüssel und Zertifikatmanagement** aus.
8. Wählen Sie die einzelnen Dropdown-Menüs für Berechtigungen (Schlüssel, Geheimnis, Zertifikat) und anschließend **Wählen Sie alle** oben in der Menüliste aus, um alle verfügbaren Berechtigungen auszuwählen. Sie sollten Folgendes haben:
   - **Hauptberechtigungen**: 20 ausgewählt
   - **Geheimberechtigungen**: 8 ausgewählt
   - **Zertifikatberechtigungen**: 16 ausgewählt


Create an access policy
1 Permissions
2 Principal
3 Application (optional)
4 Review + create
Configure from a template
Key, Secret, & Certificate Management
Key permissions
Key Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign
Privileged Key Operations
Select all
Purge
Release
Rotation Policy Operations
Select all
Rotate
Get Rotation Policy
Set Rotation Policy
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
List Certificate Authorities
Set Certificate Authorities
Delete Certificate Authorities
Privileged Certificate Operations
Select all
Purge
Previous
Next

9. Klicken Sie auf **Weiter**, um die in erstellte Anwendung **Principal** Azure auszuwählen Azure Application Registration. Wählen Sie **Weiter**.

   Pro Richtlinie kann nur ein Principal zugewiesen werden.



10. Klicken Sie zweimal auf **Weiter**, bis Sie bei **Review und create** angekommen sind. Klicken Sie dann auf **Erstellen**.
11. Wählen Sie **Weiter**, um zu **Networking**-Optionen zu gelangen.
12. Wählen Sie die geeignete Netzwerkzugangsmethode oder wählen Sie **Alle Netzwerke** und **Überprüfen + Erstellen**, um den SchlüsselTresor zu erstellen. (Netzwerkzugriffsmethode kann von einer Governance-Richtlinie oder einem Sicherheitsteam Ihres Unternehmens für Cloud-Sicherheit vorgeschrieben werden.)
13. Notieren Sie den Key Vault URI: Navigieren Sie im von Ihnen erstellten Schlüsselspeicher zum Menü Übersicht und kopieren Sie den **Vault URI** aus der rechten Spalte. Sie brauchen dies für einen späteren Schritt.

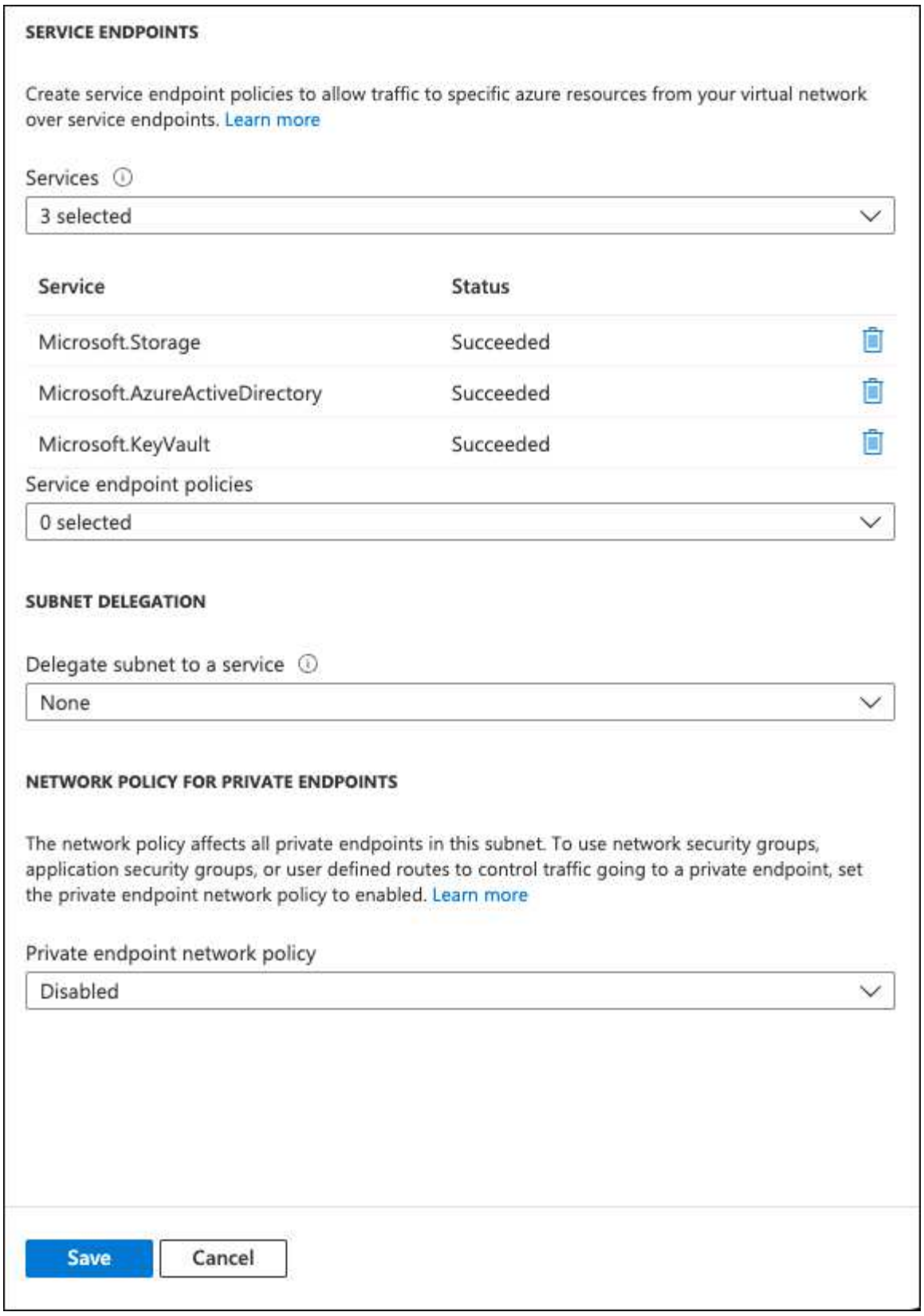
Erstellen eines Verschlüsselungsschlüssels

1. Navigieren Sie im Menü für den für Cloud Volumes ONTAP erstellten Schlüsseldefault zur Option **Schlüssel**.
2. Wählen Sie **Erzeugen/Importieren**, um einen neuen Schlüssel zu erstellen.
3. Lassen Sie die Standardoption auf **Erzeugen** gesetzt.

4. Geben Sie die folgenden Informationen an:
    - Name des Verschlüsselungsschlüssels
    - Schlüsseltyp: RSA
    - RSA-Schlüsselgröße: 2048
    - Aktiviert: Ja
5. Wählen Sie **Erstellen**, um den Verschlüsselungsschlüssel zu erstellen.
6. Kehren Sie zum Menü **Tasten** zurück und wählen Sie die Taste aus, die Sie gerade erstellt haben.
7. Wählen Sie die Schlüssel-ID unter **Aktuelle Version** aus, um die Schlüsseleigenschaften anzuzeigen.
8. Suchen Sie das Feld **Key Identifier**. Kopieren Sie den URI nach oben, jedoch nicht mit dem hexadezimalen String.

Azure Active Directory Endpunkt erstellen (nur HA)

1. Dieser Prozess ist nur erforderlich, wenn Sie Azure Key Vault für eine HA Cloud Volumes ONTAP Arbeitsumgebung konfigurieren.
2. Navigieren Sie im Azure-Portal zu **Virtual Networks**.
3. Wählen Sie das virtuelle Netzwerk aus, in dem Sie die Cloud Volumes ONTAP-Arbeitsumgebung bereitgestellt haben, und wählen Sie das Menü **Subnetze** auf der linken Seite aus.
4. Wählen Sie in der Liste den Subnetznamen für Ihre Cloud Volumes ONTAP-Bereitstellung aus.
5. Navigieren Sie zur Überschrift **Service-Endpunkte**. Wählen Sie im Dropdown-Menü Folgendes aus:
    - **Microsoft.AzureActiveDirectory**
    - **Microsoft.KeyVault**
    - **Microsoft.Storage** (optional)



6. Wählen Sie **Speichern**, um Ihre Einstellungen zu erfassen.

Cloud Volumes ONTAP-Konfiguration

1. Stellen Sie eine Verbindung zur Cluster-Management-LIF mit dem bevorzugten SSH-Client her.
2. Geben Sie in ONTAP den erweiterten Berechtigungsmodus ein:

```
set advanced -con off
```

3. Identifizieren Sie die gewünschte Daten-SVM und überprüfen Sie deren DNS-Konfiguration:
`vserver services name-service dns show`

   a. Wenn ein DNS-Eintrag für die gewünschte Daten-SVM existiert und ein Eintrag für den Azure DNS enthält, ist keine Aktion erforderlich. Ist dies nicht der Fall, fügen Sie einen DNS-Servereintrag für die Daten-SVM hinzu, der auf den Azure DNS, den privaten DNS oder den lokalen Server verweist. Dies sollte der Eintrag für die Cluster Admin SVM entsprechen:
   `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`

   b. Vergewissern Sie sich, dass der DNS-Service für die Daten-SVM erstellt wurde:
   `vserver services name-service dns show`

4. Aktivieren Sie Azure Key Vault mithilfe der Client-ID und der Mandanten-ID, die nach der Registrierung der Applikation gespeichert wurden:
`security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id full_key_URI`

   > Der `_full_key_URI` Wert muss den verwenden `<https:// <key vault host name>/keys/<key label>` Formatieren.

5. Nach der erfolgreichen Aktivierung von Azure Key Vault geben Sie den ein `client secret value` Wenn Sie dazu aufgefordert werden.

6. Überprüfen Sie den Status des Schlüsselmanagers:
`security key-manager external azure check`Die Ausgabe sieht wie folgt aus:

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
    Status: OK

Category: ekmip_server
    Status: OK

Category: kms_wrapped_key_status
    Status: UNKNOWN
    Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

   Wenn der `service_reachability` Status ist nicht `OK`, Die SVM kann den Azure Key Vault Service nicht mit allen erforderlichen Konnektivitäts- und Berechtigungen erreichen. Stellen Sie sicher, dass Ihre Azure Netzwerkrichtlinien und Ihr Routing Ihr privates vnet nicht an den öffentlichen Endpunkt von Azure

KeyVault blockieren. Falls dies der Fall ist, sollten sie einen Azure Private Endpunkt zum Zugriff auf den Schlüsselvaults innerhalb der vnet-Umgebung verwenden. Möglicherweise müssen Sie auch einen statischen Hosteintrag auf Ihrer SVM hinzufügen, um die private IP-Adresse für Ihren Endpunkt zu lösen.

Der `kms_wrapped_key_status` Wird berichten `UNKNOWN` Bei der Erstkonfiguration. Sein Status ändert sich in `OK` Nach der Verschlüsselung des ersten Volume.

7. OPTIONAL: Erstellen Sie ein Test-Volume, um die Funktionalität von NVE zu überprüfen.

   ```
   vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
   -state online -policy default
   ```

   Bei korrekter Konfiguration erstellt Cloud Volumes ONTAP automatisch das Volume und aktiviert die Volume-Verschlüsselung.

8. Bestätigen Sie, dass das Volume ordnungsgemäß erstellt und verschlüsselt wurde. Wenn das der Fall ist, wird der angezeigt `-is-encrypted` Der Parameter wird als angezeigt `true`.
   `vol show -vserver SVM_name -fields is-encrypted`

Verwalten Sie Schlüssel mit Google Cloud Key Management Service

Verwenden Sie können "Der Verschlüsselungsmanagement-Service (Cloud KMS) der Google Cloud-Plattform" Zum Schutz Ihrer ONTAP Verschlüsselungen in einer vom Google Cloud-Plattform bereitgestellten Applikation.

Das Verschlüsselungsmanagement mit Cloud KMS kann über die CLI oder die ONTAP REST-API aktiviert werden.

Bei der Verwendung von Cloud KMS ist zu beachten, dass standardmäßig die LIF einer Daten-SVM verwendet wird, um mit dem Endpunkt des Cloud-Schlüsselmanagements zu kommunizieren. Zur Kommunikation mit den Authentifizierungsservices des Cloud-Providers wird ein Node-Managementnetzwerk verwendet (oauth2.googleapis.com). Wenn das Cluster-Netzwerk nicht korrekt konfiguriert ist, nutzt das Cluster den Verschlüsselungsmanagementservice nicht ordnungsgemäß.

Bevor Sie beginnen

- Cloud Volumes ONTAP muss Version 9.10.1 oder höher ausführen
- Volume Encryption (VE)-Lizenz installiert
- Mandantenfähige MTEKM-Lizenz (Encryption Key Management) ist ab Cloud Volumes ONTAP 9.12.1 GA installiert.
- Sie müssen ein Cluster- oder SVM-Administrator sein
- Ein aktives Google Cloud Platform Abonnement

Einschränkungen

- Cloud KMS kann nur auf einer Daten-SVM konfiguriert werden

Konfiguration

Google Cloud

1. In Ihrer Google Cloud-Umgebung "Erstellen Sie einen symmetrischen GCP-Schlüsselring und -Schlüssel".
2. Erstellen Sie eine benutzerdefinierte Rolle für Ihr Cloud Volumes ONTAP-Servicekonto.

```
gcloud iam roles create kmsCustomRole
    --project=<project_id>
    --title=<kms_custom_role_name>
    --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourcemanager.projects.get
    --stage=GA
```

3. Weisen Sie den Cloud-KMS-Schlüssel und das Cloud Volumes ONTAP-Servicekonto die benutzerdefinierte Rolle zu:
`gcloud kms keys add-iam-policy-binding *key_name* --keyring *key_ring_name* --location *key_location* --member serviceAccount:_service_account_Name_ --role projects/*customer_project_id*/roles/kmsCustomRole`
4. Service-Konto-JSON-Schlüssel herunterladen:
`gcloud iam service-accounts keys create key-file --iam-account=*sa-name*@*project-id*.iam.gserviceaccount.com`

Cloud Volumes ONTAP

1. Stellen Sie eine Verbindung zur Cluster-Management-LIF mit dem bevorzugten SSH-Client her.
2. Wechseln zur erweiterten Berechtigungsebene:
`set -privilege advanced`
3. DNS für die Daten-SVM erstellen.
`dns create -domains c.<*project*>.internal -name-servers *server_address* -vserver *SVM_name*`
4. CMEK-Eintrag erstellen:
`security key-manager external gcp enable -vserver *SVM_name* -project-id *project* -key-ring-name *key_ring_name* -key-ring-location *key_ring_location* -key-name *key_name*`
5. Geben Sie bei der entsprechenden Aufforderung den JSON-Schlüssel Ihres GCP-Kontos ein.
6. Bestätigen Sie, dass der aktivierte Prozess erfolgreich war:
`security key-manager external gcp check -vserver *svm_name*`
7. OPTIONAL: Erstellen Sie ein Volume zum Testen der Verschlüsselung `vol create *volume_name* -aggregate *aggregate* -vserver *vserver_name* -size 10G`

Fehlerbehebung

Wenn Sie Fehler beheben müssen, können Sie die RAW REST API-Logs in den letzten beiden Schritten oben:

1. `set d`
2. `systemshell -node *node* -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Besserer Schutz gegen Ransomware

Ransomware-Angriffe können das Unternehmen Zeit, Ressourcen und Image-Schäden kosten. Mit BlueXP können Sie zwei NetApp Lösungen für Ransomware implementieren: Schutz vor gängigen Ransomware-Dateierweiterungen und Autonomer Ransomware-Schutz (ARP). Diese Lösungen bieten effektive Tools für Transparenz, Erkennung und Behebung von Problemen.

Schutz vor gängigen Ransomware-Dateiendungen

Die in BlueXP verfügbare Einstellung für den Schutz vor Ransomware ermöglicht Ihnen die Nutzung der ONTAP FPolicy Funktion zum Schutz vor gängigen Dateierweiterungen für Ransomware-Angriffe.

Schritte

1. Doppelklicken Sie auf der Seite Bildschirm auf den Namen des Systems, das Sie für den Ransomware-Schutz konfigurieren.
2. Klicken Sie auf der Registerkarte Übersicht auf das Bedienfeld Funktionen und dann auf das Bleistiftsymbol neben **Ransomware-Schutz**.

3. 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.

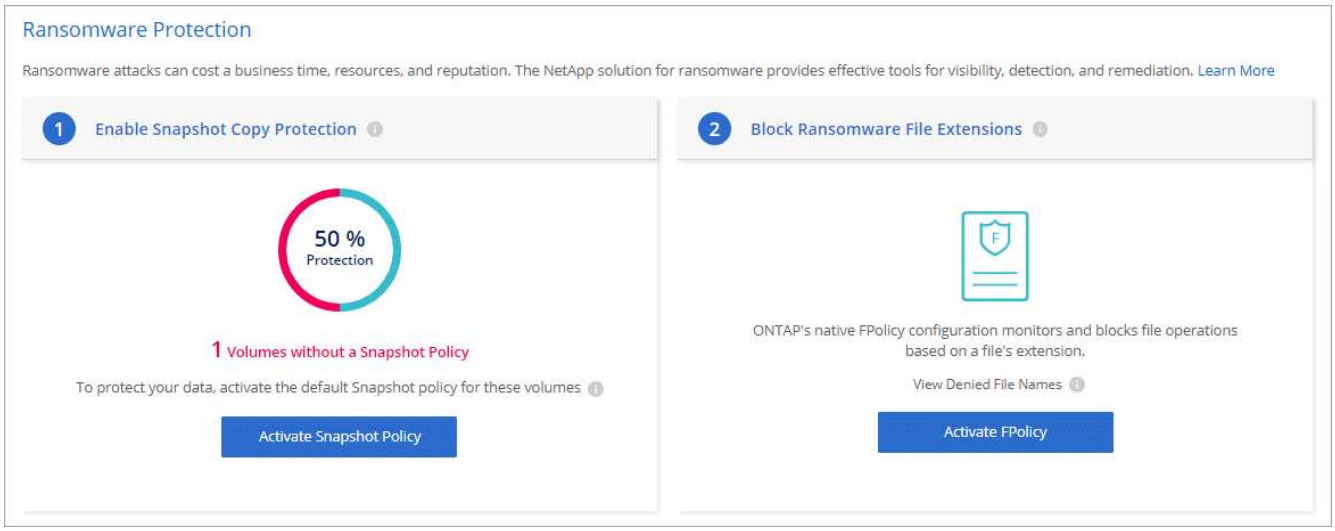
   b. Klicken Sie auf **FPolicy** aktivieren, um die FPolicy Lösung von ONTAP zu aktivieren, die Dateivorgänge auf Basis der Dateierweiterung blockieren kann.

      Diese präventive Lösung verbessert den Schutz vor Ransomware-Angriffen, indem sie gängige Ransomware-Dateitypen blockiert.

      Die standardmäßige FPolicy Scope blockiert Dateien, die die folgenden Erweiterungen haben:

      Micro, verschlüsselt, gesperrt, Crypto, Crypt, Crinf, r5a, XRNT, XTBL, R16M01D05, Pzdc, gut, LOL!, OMG!, RDM, RK, verschlüsseltedRS, Crjoker, entschlüsselt, LeChiffre

      BlueXP erstellt diesen Bereich, wenn Sie FPolicy auf Cloud Volumes ONTAP aktivieren. Die Liste basiert auf gängigen Ransomware-Dateitypen. Sie können die blockierten Dateierweiterungen mithilfe der Befehle *vserver fpolicy Scope* von der Cloud Volumes ONTAP CLI anpassen.



Autonomer Schutz Durch Ransomware

Cloud Volumes ONTAP unterstützt die ARP-Funktion (Autonomous Ransomware Protection), die Workload-Analysen durchführt, um abnormale Aktivitäten, die auf einen Ransomware-Angriff hinweisen, proaktiv zu erkennen und zu warnen.

Trennen Sie sich von den Schutzmaßnahmen für die Dateierweiterung, die im bereitgestellt werden "ransomware-Schutz-Einstellung", Die ARP-Funktion verwendet Workload-Analyse, um den Benutzer auf mögliche Angriffe auf der Grundlage erkannt “abnorme Aktivität“ zu warnen. Die Ransomware-Schutzeinstellung und die ARP-Funktion können in Verbindung für einen umfassenden Schutz vor Ransomware verwendet werden.

Die ARP-Funktion ist nur zur Verwendung mit BYOL-Lizenzen (Laufzeit von 1 bis 36 Monaten) sowohl für Node-basierte als auch für kapazitätsbasierte Lizenzmodell verfügbar. Wenden Sie sich an Ihren NetApp Vertriebsmitarbeiter, um eine neue, separate Add-on-Lizenz zur Verwendung mit der ARP-Funktion in Cloud Volumes ONTAP zu erwerben.

Die ARP Lizenz gilt als „fließende“ Lizenz, was bedeutet, dass sie nicht an eine einzelne Cloud Volumes ONTAP Instanz gebunden ist und auf mehrere Cloud Volumes ONTAP Umgebungen angewendet werden kann.

> Die Verwendung der ARP-Funktion mit Node-basierten Cloud Volumes ONTAP-Lizenzen ist derzeit nicht in Digital Wallet enthalten. Die Möglichkeit, die Node-basierte ARP-Nutzung anzuzeigen, wird in einer zukünftigen Version unter Digital Wallet verfügbar sein.

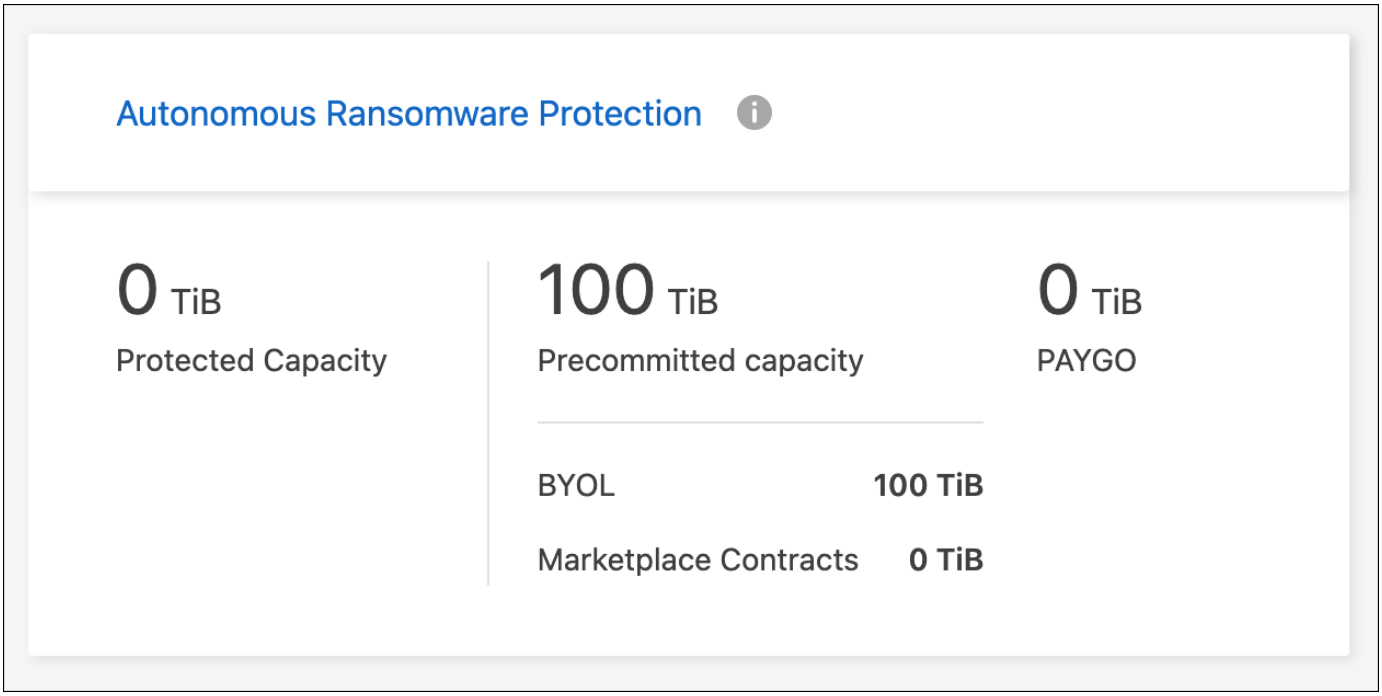
Beim Kauf einer Add-on-Lizenz und beim Hinzufügen zur Digital Wallet können Sie ARP mit Cloud Volumes ONTAP auf Volume-Basis aktivieren. Die Abrechnung für ARP erfolgt auf Volume-Ebene entsprechend der insgesamt bereitgestellten Kapazität von Volumes mit aktivierter ARP-Funktion. Die minimale Lizenzkapazität beträgt 1 TB. Es gibt jedoch keine Mindestkapazitätsgebühren für die ARP-Funktion.

ARP-aktivierte Volumes haben einen bestimmten Status als „Lernmodus“ oder „aktiv“. Jede Lautstärke mit dem ARP-Status „deaktiviert“ ist vom Laden ausgeschlossen. Bei einer Cloud Volumes ONTAP-Umgebung mit 30 tib bereitgestellter Kapazität kann beispielsweise nur eine Teilmenge von 15 tib Volumes mit aktivierter ARP-Funktion gewählt werden.

Die Konfiguration von ARP für Volumes wird über ONTAP System Manager und ONTAP CLI durchgeführt.

Weitere Informationen zur Aktivierung von ARP mit ONTAP System Manager und CLI finden Sie unter

"Autonomer Schutz Vor Ransomware".



Ohne Lizenz ist kein Support für die Nutzung lizenzierter Funktionen verfügbar.

Systemadministration

Upgrade der Cloud Volumes ONTAP Software

Aktualisieren Sie Cloud Volumes ONTAP von BlueXP, um Zugang zu den neuesten neuen Funktionen und Verbesserungen zu erhalten. Sie sollten Cloud Volumes ONTAP Systeme vor einem Upgrade der Software vorbereiten.

Upgrade-Übersicht

Beachten Sie die folgenden Punkte, bevor Sie mit dem Cloud Volumes ONTAP-Upgrade-Prozess beginnen.

Upgrade nur von BlueXP

Upgrades von Cloud Volumes ONTAP müssen von BlueXP abgeschlossen werden. Sie sollten kein Cloud Volumes ONTAP-Upgrade mit System Manager oder der CLI durchführen. Dies kann die Stabilität des Systems beeinträchtigen.

Upgrade-Tipps

BlueXP bietet zwei Möglichkeiten, Cloud Volumes ONTAP zu aktualisieren:

- Durch das Verfolgen von Upgrade-Benachrichtigungen, die in der Arbeitsumgebung angezeigt werden
- Indem Sie das Upgrade-Image an einem HTTPS-Speicherort platzieren und BlueXP dann die URL bereitstellen

Unterstützte Upgrade-Pfade

Die Cloud Volumes ONTAP Version, auf die Sie ein Upgrade durchführen können, hängt von der Version von Cloud Volumes ONTAP ab, auf der Sie derzeit ausgeführt werden.

Aktuelle Version	Versionen, auf die Sie direkt aktualisieren können
9.14.1	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

Beachten Sie Folgendes:

- Die unterstützten Upgrade-Pfade für Cloud Volumes ONTAP unterscheiden sich von denen für ein ONTAP Cluster vor Ort.

- Wenn Sie ein Upgrade durchführen, indem Sie die Upgrade-Benachrichtigungen befolgen, die in einer Arbeitsumgebung angezeigt werden, werden Sie von BlueXP aufgefordert, auf eine Version zu aktualisieren, die diesen unterstützten Upgrade-Pfaden folgt.
- Wenn Sie ein Upgrade-Image durch Platzieren eines Upgrade-Images an einem HTTPS-Standort aktualisieren, befolgen Sie diese unterstützten Upgrade-Pfade.
- In einigen Fällen müssen Sie möglicherweise ein paar Mal ein Upgrade durchführen, um Ihre Zielversion zu erreichen.

  Wenn Sie beispielsweise Version 9.8 verwenden und auf 9.10.1 aktualisieren möchten, müssen Sie zuerst auf Version 9.9.1 und dann auf 9.10.1 aktualisieren.

Patch-Versionen

Ab Januar 2024 sind Patch-Upgrades nur in BlueXP verfügbar, wenn es sich um ein Patch-Release für die drei neuesten Versionen von Cloud Volumes ONTAP handelt. Wir verwenden die neueste GA-Version, um zu bestimmen, welche drei neuesten Versionen in BlueXP angezeigt werden. Wenn beispielsweise die aktuelle GA-Version 9.13.1 lautet, werden Patches für 9.11.1-9.13.1 in BlueXP angezeigt. Wenn Sie ein Upgrade auf ein Patch-Release für Versionen 9.11.1 oder niedriger durchführen möchten, müssen Sie das manuelle Upgrade-Verfahren von verwenden das über eine URL verfügbar ist,ONTAP-Image wird heruntergeladen.

Als allgemeine Regel für Patch (P)-Versionen können Sie von einer Version auf eine beliebige P-Version der aktuellen oder der nächsten Version upgraden.

Hier ein paar Beispiele:

- 9.13.0 > 9,13,1P15
- 9.12.1 > 9,13,1P2

Zurücksetzen oder Downgrade

Das Zurücksetzen oder Downgrade von Cloud Volumes ONTAP auf eine vorherige Version wird nicht unterstützt.

Support-Registrierung

Cloud Volumes ONTAP muss beim NetApp Support registriert sein, um ein Upgrade der Software mit den auf dieser Seite beschriebenen Methoden durchführen zu können. Dies gilt sowohl für PAYGO als auch für BYOL. Das müssen Sie unbedingt "Manuelle Registrierung von PAYGO-Systemen", Während BYOL-Systeme standardmäßig registriert werden.

Ein System, das nicht für den Support registriert ist, erhält weiterhin die Benachrichtigungen zum Softwareupdate, die in BlueXP angezeigt werden, wenn eine neue Version verfügbar ist. Sie müssen das System aber registrieren, bevor Sie die Software aktualisieren können.

Upgrades des HA Mediators

BlueXP aktualisiert die Mediator-Instanz auch bei Bedarf während des Cloud Volumes ONTAP-Upgradevorgangs.

Upgrades in AWS mit EC2-Instanztypen c4, m4 und R4

Cloud Volumes ONTAP unterstützt die EC2-Instanztypen c4, m4 und R4 nicht mehr. Mit diesen Instanztypen können Sie vorhandene Implementierungen auf Cloud Volumes ONTAP Version 9.8-9.12.1 aktualisieren.

Bevor Sie ein Upgrade durchführen, empfehlen wir Ihnen, dass Sie Ändern Sie den Instanztyp. Wenn Sie den Instanztyp nicht ändern können, müssen Sie dies tun Erweiterte Netzwerkfunktionen aktivieren Vor dem Upgrade. Lesen Sie die folgenden Abschnitte, um mehr über das Ändern des Instanztyps und das Aktivieren von verbesserten Netzwerkfunktionen zu erfahren.

In Cloud Volumes ONTAP mit Versionen 9.13.0 und höher können keine Upgrades mit den EC2-Instanztypen c4, m4 und R4 durchgeführt werden. In diesem Fall müssen Sie die Anzahl der Festplatten reduzieren und dann Ändern Sie den Instanztyp Alternativ können Sie eine neue HA-Paar-Konfiguration mit den EC2-Instanztypen c5, m5 und R5 implementieren und die Daten migrieren.

Ändern Sie den Instanztyp

die Instanztypen c4, m4 und R4 EC2 ermöglichen mehr Festplatten pro Node als die Instanztypen c5, m5 und R5 EC2. Wenn die Anzahl der Festplatten pro Node bei der c4-, m4- oder R4-EC2-Instanz unter der maximalen Festplattenanzahl pro Node bei Instanzen mit c5-, m5- und r5-Systemen liegt, können Sie den EC2-Instanztyp in c5, m5 oder r5 ändern.

"Überprüfen Sie die Festplatten- und Tiering-Limits durch EC2-Instanz"
"Ändern des EC2 Instanztyps für Cloud Volumes ONTAP"

Wenn Sie den Instanztyp nicht ändern können, führen Sie die Schritte unter aus Erweiterte Netzwerkfunktionen aktivieren.

Erweiterte Netzwerkfunktionen aktivieren

Um ein Upgrade auf Cloud Volumes ONTAP Version 9.8 und höher durchzuführen, müssen Sie *enhanced Networking* auf dem Cluster aktivieren, auf dem der Instanztyp c4, m4 oder R4 ausgeführt wird. Informationen zum Aktivieren von ENA finden Sie in dem Artikel der Knowledge Base "Aktivieren von erweiterten Netzwerkfunktionen wie SR-IOV oder ENA auf AWS Cloud Volumes ONTAP Instanzen".

Upgrade wird vorbereitet

Bevor Sie ein Upgrade durchführen, müssen Sie überprüfen, ob die Systeme bereit sind und alle erforderlichen Konfigurationsänderungen vornehmen.

- Planung von Ausfallzeiten
- ob das automatische Giveback weiterhin aktiviert ist
- Unterbrechen Sie die SnapMirror Übertragung
- dass die Aggregate online sind
- dass alle LIFs an den Home Ports angeschlossen 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.

In vielen Fällen erfolgt das Upgrade eines HA-Paars unterbrechungsfrei und die I/O-Vorgänge werden unterbrechungsfrei ausgeführt. Während dieses unterbrechungsfreien Upgrade-Prozesses wird jeder Node entsprechend aktualisiert, um den I/O-Datenverkehr für die Clients weiterhin bereitzustellen.

Sitzungsorientierte Protokolle können während der Upgrades in bestimmten Bereichen negative Auswirkungen auf Clients und Anwendungen haben. Weitere Informationen "Weitere Informationen finden Sie in der ONTAP-Dokumentation"

Überprüfen Sie, ob 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"

Unterbrechen Sie die SnapMirror Übertragung

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.

> Obwohl bei BlueXP Backup und Recovery eine Implementierung von SnapMirror zur Erstellung von Backup-Dateien verwendet wird (genannt SnapMirror Cloud), müssen Backups bei einem System-Upgrade nicht ausgesetzt werden.

Über diese Aufgabe

In diesen Schritten wird die Verwendung von System Manager für Version 9.3 und höher beschrieben.

Schritte

1. Melden Sie sich vom Zielsystem aus bei System Manager an.

   Sie können sich bei System Manager anmelden, indem Sie im Webbrowser die IP-Adresse der Cluster-Management-LIF aufrufen. Die IP-Adresse finden Sie in der Cloud Volumes ONTAP-Arbeitsumgebung.

   > Der Computer, von dem aus Sie auf BlueXP zugreifen, muss über eine Netzwerkverbindung zu Cloud Volumes ONTAP verfügen. Beispielsweise müssen Sie sich über einen Jump-Host in Ihrem Cloud-Provider-Netzwerk bei BlueXP anmelden.

2. Klicken Sie Auf **Schutz > Beziehungen**.
3. Wählen Sie die Beziehung aus, und klicken Sie auf **Operationen > Quiesce**.

Vergewissern Sie sich, dass die Aggregate online sind

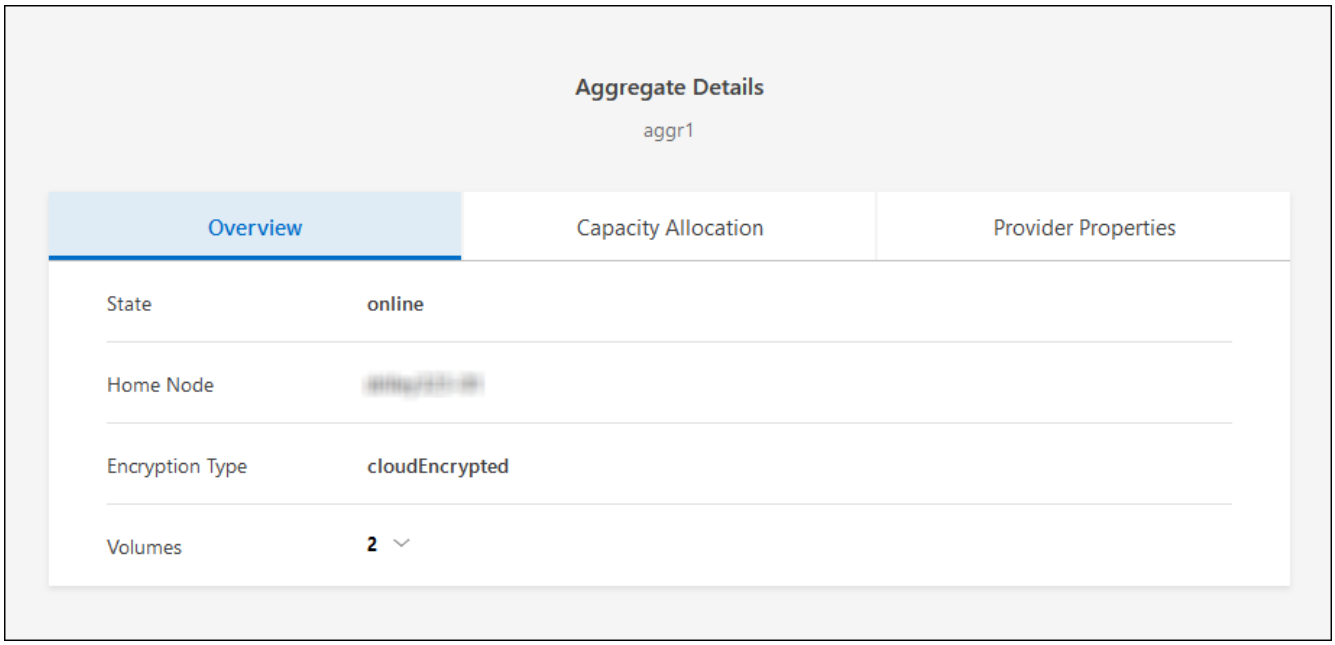
Aggregate für Cloud Volumes ONTAP muss online sein, bevor Sie die Software aktualisieren. Aggregate sollten in den meisten Konfigurationen online sein. Wenn dies nicht der Fall ist, sollten Sie sie jedoch online stellen.

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 die Registerkarte **Aggregate**.
2. Klicken Sie unter dem Aggregattitel auf die Schaltfläche Ellipsen, und wählen Sie dann **Aggregatdetails anzeigen**.



3. Wenn das Aggregat offline ist, verwenden Sie System Manager, um das Aggregat online zu schalten:
   a. Klicken Sie Auf **Storage > Aggregate & Disks > Aggregate**.
   b. Wählen Sie das Aggregat aus und klicken Sie dann auf **Weitere Aktionen > Status > Online**.

Vergewissern Sie sich, dass alle LIFs an den Home Ports angeschlossen sind

Vor dem Upgrade müssen sich alle LIFs auf Home Ports befinden. Weitere Informationen finden Sie in der ONTAP-Dokumentation unter "Vergewissern Sie sich, dass alle LIFs an den Home Ports angeschlossen sind".

Wenn ein Upgrade-Fehler auftritt, lesen Sie die "Knowledge Base Artikel „Cloud Volumes ONTAP Upgrade fehlschlägt fehl“".

Upgrade von Cloud Volumes ONTAP

BlueXP benachrichtigt Sie, wenn eine neue Version zur Aktualisierung verfügbar ist. Sie können den Upgrade-Prozess über diese Benachrichtigung starten. Weitere Informationen finden Sie unter Upgrade von BlueXP-Benachrichtigungen.

Eine andere Möglichkeit, Software-Upgrades mithilfe eines Images auf einer externen URL durchzuführen. Diese Option ist hilfreich, wenn BlueXP nicht auf den S3 Bucket zugreifen kann, um die Software zu aktualisieren oder wenn Sie mit einem Patch ausgestattet wurden. Weitere Informationen finden Sie unter das über eine URL verfügbar ist.

Upgrade von BlueXP-Benachrichtigungen

BlueXP zeigt eine Benachrichtigung in Cloud Volumes ONTAP-Arbeitsumgebungen 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.

Bevor Sie beginnen

BlueXP-Vorgänge wie die Erstellung von Volumes oder Aggregaten dürfen auf dem Cloud Volumes ONTAP-System nicht ausgeführt werden.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Wählen Sie eine Arbeitsumgebung aus.

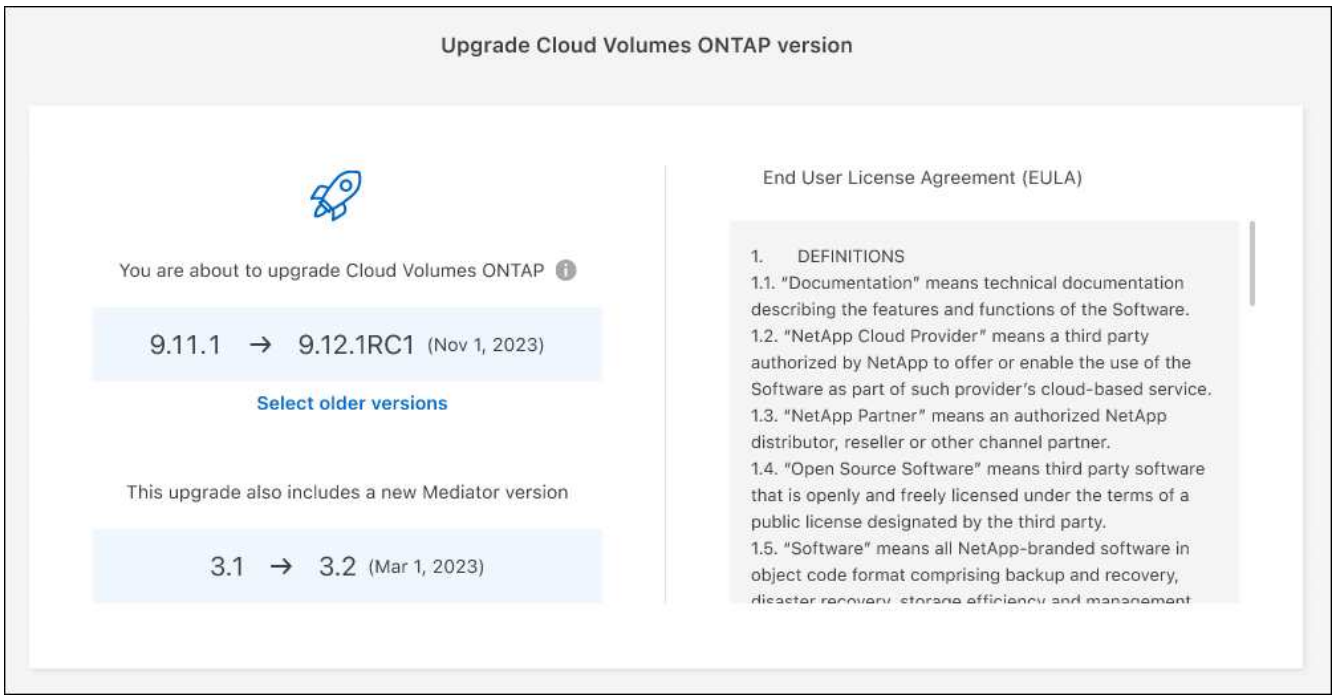
   Wenn eine neue Version verfügbar ist, wird auf der Registerkarte „Übersicht“ eine Benachrichtigung angezeigt:

3. Wenn eine neue Version verfügbar ist, klicken Sie auf **Jetzt aktualisieren!**

   Bevor Sie Cloud Volumes ONTAP über die BlueXP Benachrichtigung aktualisieren können, benötigen Sie ein NetApp Support Site Konto.

4. Lesen Sie auf der Seite Upgrade Cloud Volumes ONTAP die EULA, und wählen Sie dann **Ich habe die EULA gelesen und genehmigt**.
5. Klicken Sie Auf **Upgrade**.

Auf der Seite Upgrade Cloud Volumes ONTAP wird standardmäßig die neueste verfügbare Cloud Volumes ONTAP-Version für das Upgrade ausgewählt. Falls verfügbar, können Sie stattdessen ältere Versionen von Cloud Volumes ONTAP für Ihr Upgrade auswählen, indem Sie auf **Ältere Versionen auswählen** klicken.
Siehe "Liste der unterstützten Upgrade-Pfade" Sie erhalten basierend auf Ihrer aktuellen Cloud Volumes ONTAP Version die gewünschten Upgrade-Pfade.



6. Um den Status des Upgrades zu überprüfen, klicken Sie auf das Symbol Einstellungen und wählen Sie **Timeline**.

Ergebnis

BlueXP startet das Software-Upgrade. Sie können Aktionen in der Arbeitsumgebung durchführen, wenn die Softwareaktualisierung abgeschlossen ist.

Nachdem Sie fertig sind

Wenn Sie SnapMirror Transfers ausgesetzt haben, setzen Sie die Transfers mit System Manager fort.

Upgrade von einem Image, das über eine URL verfügbar ist

Sie können das Cloud Volumes ONTAP Software-Image auf dem Connector oder einem HTTP-Server platzieren und dann das Software-Upgrade von BlueXP starten. Möglicherweise verwenden Sie diese Option, wenn BlueXP zum Upgrade der Software nicht auf den S3-Bucket zugreifen kann.

Bevor Sie beginnen

- BlueXP-Vorgänge wie die Erstellung von Volumes oder Aggregaten dürfen auf dem Cloud Volumes ONTAP-System nicht ausgeführt werden.
- Wenn Sie HTTPS zum Hosten von ONTAP-Images verwenden, kann das Upgrade aufgrund von Problemen mit der SSL-Authentifizierung fehlschlagen, die durch fehlende Zertifikate verursacht werden. Dieses Problem besteht darin, ein von einer Zertifizierungsstelle signiertes Zertifikat zu generieren und zu installieren, das für die Authentifizierung zwischen ONTAP und BlueXP verwendet wird.

  In der NetApp Knowledge Base finden Sie Schritt-für-Schritt-Anleitungen:

"NetApp KB: So konfigurieren Sie BlueXP als HTTPS-Server, um Upgrade-Images zu hosten"

Schritte

1. Optional: Richten Sie einen HTTP-Server ein, der das Cloud Volumes ONTAP Software-Image hosten kann.

   Wenn Sie eine VPN-Verbindung zum virtuellen Netzwerk haben, können Sie das Cloud Volumes ONTAP Software-Image auf einem HTTP-Server in Ihrem eigenen Netzwerk platzieren. Andernfalls müssen Sie die Datei auf einem HTTP-Server in der Cloud platzieren.

2. Wenn Sie Ihre eigene Sicherheitsgruppe für Cloud Volumes ONTAP verwenden, stellen Sie sicher, dass die ausgehenden Regeln HTTP-Verbindungen zulassen, damit Cloud Volumes ONTAP auf das Software-Image zugreifen kann.

   Die vordefinierte Cloud Volumes ONTAP-Sicherheitsgruppe erlaubt standardmäßig ausgehende HTTP-Verbindungen.

3. Beziehen Sie das Software-Image von "Die NetApp Support Site".
4. Kopieren Sie das Software-Image in ein Verzeichnis auf dem Connector oder auf einem HTTP-Server, von dem die Datei bereitgestellt wird.

   Es sind zwei Pfade verfügbar. Der richtige Pfad hängt von Ihrer Connector-Version ab.

   - `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`
   - `/opt/application/netapp/cloudmanager/ontap/images/`

5. Klicken Sie in der Arbeitsumgebung von BlueXP auf die Schaltfläche **… (Ellipsen-Symbol)**, und klicken Sie dann auf **Cloud Volumes ONTAP aktualisieren**.
6. Geben Sie auf der Seite Cloud Volumes ONTAP-Version aktualisieren die URL ein, und klicken Sie dann auf **Bild ändern**.

   Wenn Sie das Software-Image auf den Connector in dem oben gezeigten Pfad kopiert haben, geben Sie die folgende URL ein:

   http://<Connector-private-IP-address>/ontap/images/<image-file-name>

   In der URL muss **image-file-Name** dem Format "cot.image.9.13.1P2.tgz" folgen.

7. Klicken Sie zur Bestätigung auf **Weiter**.

Ergebnis

BlueXP startet das Software-Update. 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.

Beheben Sie Download-Fehler bei Verwendung eines Google Cloud NAT-Gateways

Der Connector lädt automatisch Software-Updates für Cloud Volumes ONTAP herunter. Der Download kann fehlschlagen, wenn Ihre Konfiguration ein Google Cloud NAT Gateway verwendet. Sie können dieses Problem beheben, indem Sie die Anzahl der Teile begrenzen, in die das Software-Image unterteilt ist. Dieser Schritt

muss mithilfe der BlueXP API abgeschlossen werden.

Schritt

1. SENDEN SIE EINE PUT-Anforderung an /occm/config mit dem folgenden JSON als Text:

```
{
  "maxDownloadSessions": 32
}
```

Der Wert für *maxDownloadSessions* kann 1 oder eine beliebige Ganzzahl größer als 1 sein. Wenn der Wert 1 ist, wird das heruntergeladene Bild nicht geteilt.

Beachten Sie, dass 32 ein Beispielwert ist. Der Wert, den Sie verwenden sollten, hängt von Ihrer NAT-Konfiguration und der Anzahl der Sitzungen ab, die Sie gleichzeitig haben können.

"Erfahren Sie mehr über den Aufruf der /occm/config API".

Registrieren von Pay-as-you-go-Systemen

Der Support von NetApp ist bei Cloud Volumes ONTAP PAYGO Systemen enthalten. Sie müssen jedoch zuerst den Support aktivieren, indem Sie die Systeme bei NetApp registrieren.

Die Registrierung eines PAYGO-Systems bei NetApp ist für ein Upgrade der ONTAP Software anhand einer der Methoden erforderlich "Auf dieser Seite beschrieben".

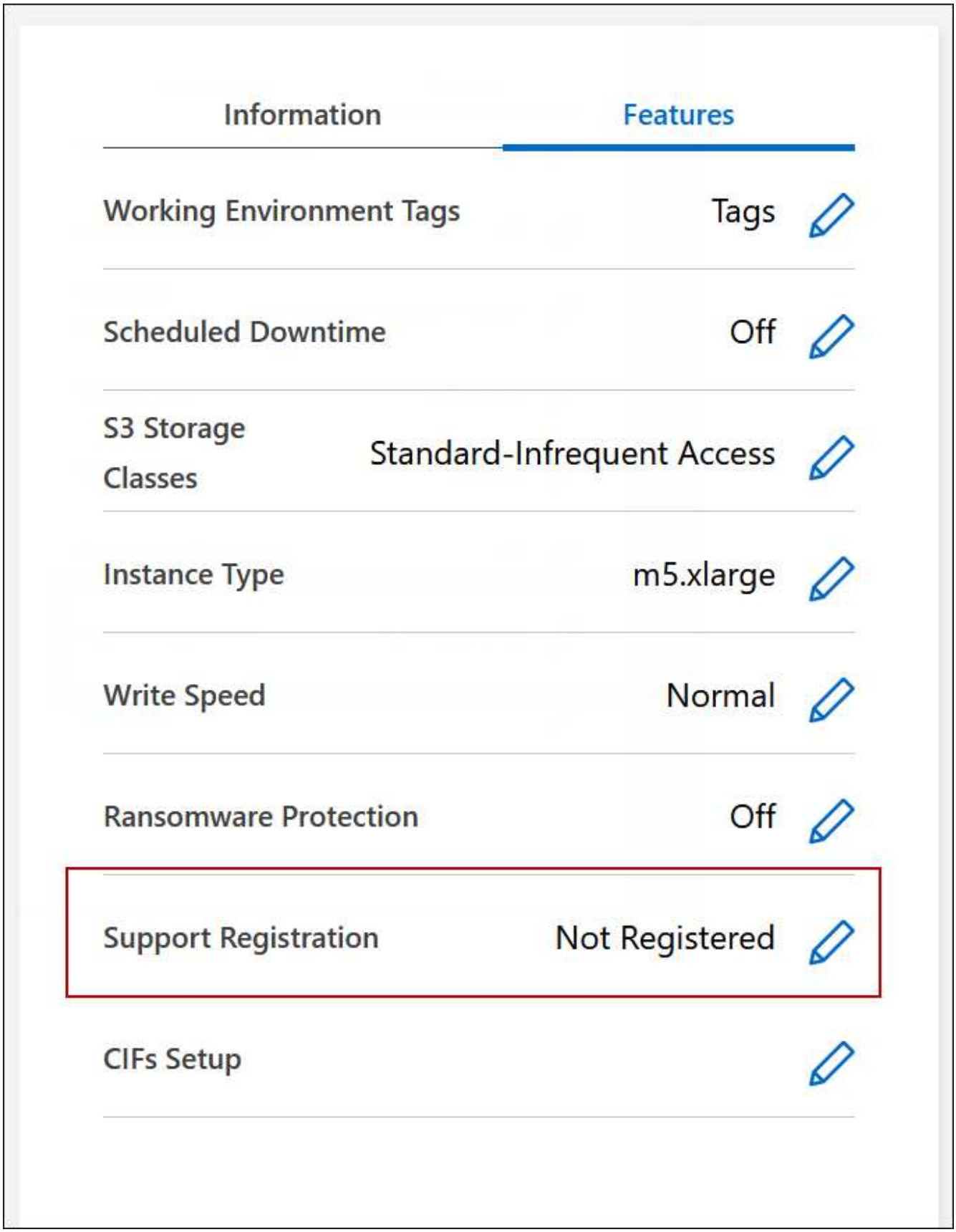
Ein System, das nicht für den Support registriert ist, erhält weiterhin die Benachrichtigungen zum Softwareupdate, die in BlueXP angezeigt werden, wenn eine neue Version verfügbar ist. Sie müssen das System aber registrieren, bevor Sie die Software aktualisieren können.

Schritte

1. Wenn Sie noch kein NetApp Support Site Konto bei BlueXP 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 Arbeitsfläche auf den Namen des Systems, das Sie registrieren möchten.
3. Klicken Sie auf der Registerkarte Übersicht auf das Bedienfeld Funktionen und dann auf das Bleistiftsymbol neben **Support-Registrierung**.



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

Ergebnis

BlueXP registriert das System bei NetApp.

Managen des Status von Cloud Volumes ONTAP

Sie können Cloud Volumes ONTAP von BlueXP stoppen 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 BlueXP so konfigurieren, dass es automatisch heruntergefahren wird und die Systeme zu bestimmten Zeiten neu gestartet werden.

Über diese Aufgabe

- Wenn Sie ein automatisches Herunterfahren des Cloud Volumes ONTAP-Systems planen, verschiebt BlueXP das Herunterfahren, wenn eine aktive Datenübertragung ausgeführt wird.

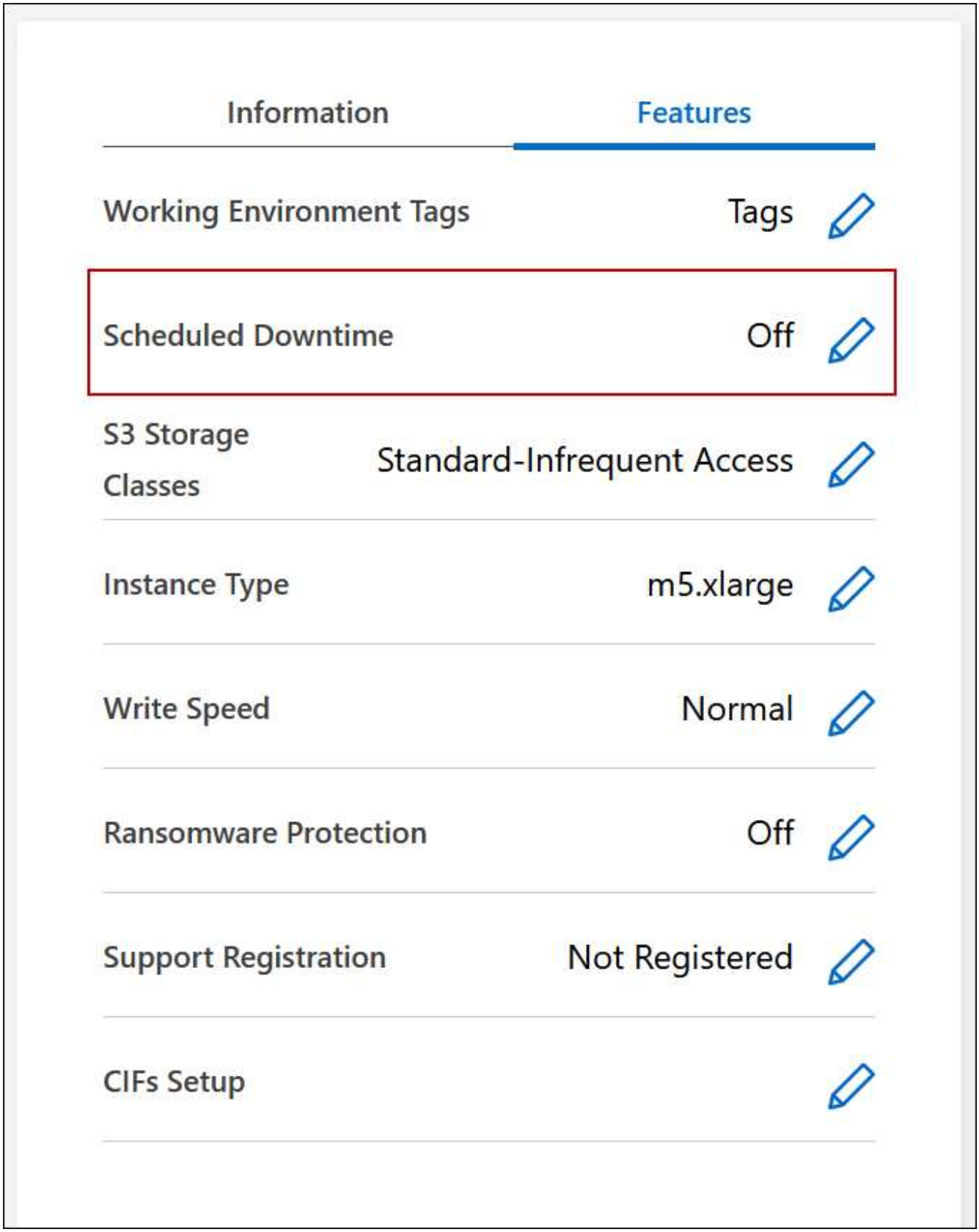
  BlueXP schaltet das System nach Abschluss der Übertragung aus.

- Diese Aufgabe plant das automatische Herunterfahren beider Nodes in einem HA-Paar.
- Snapshots von Boot- und Root-Festplatten werden nicht erstellt, wenn Cloud Volumes ONTAP durch geplante Herunterfahren ausgeschaltet wird.

  Snapshots werden automatisch nur beim manuellen Herunterfahren erstellt, wie im nächsten Abschnitt beschrieben.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsfläche auf die gewünschte Arbeitsumgebung.
2. Klicken Sie auf der Registerkarte Übersicht auf das Bedienfeld Funktionen und dann auf das Bleistiftsymbol neben **geplante Ausfallzeit**.



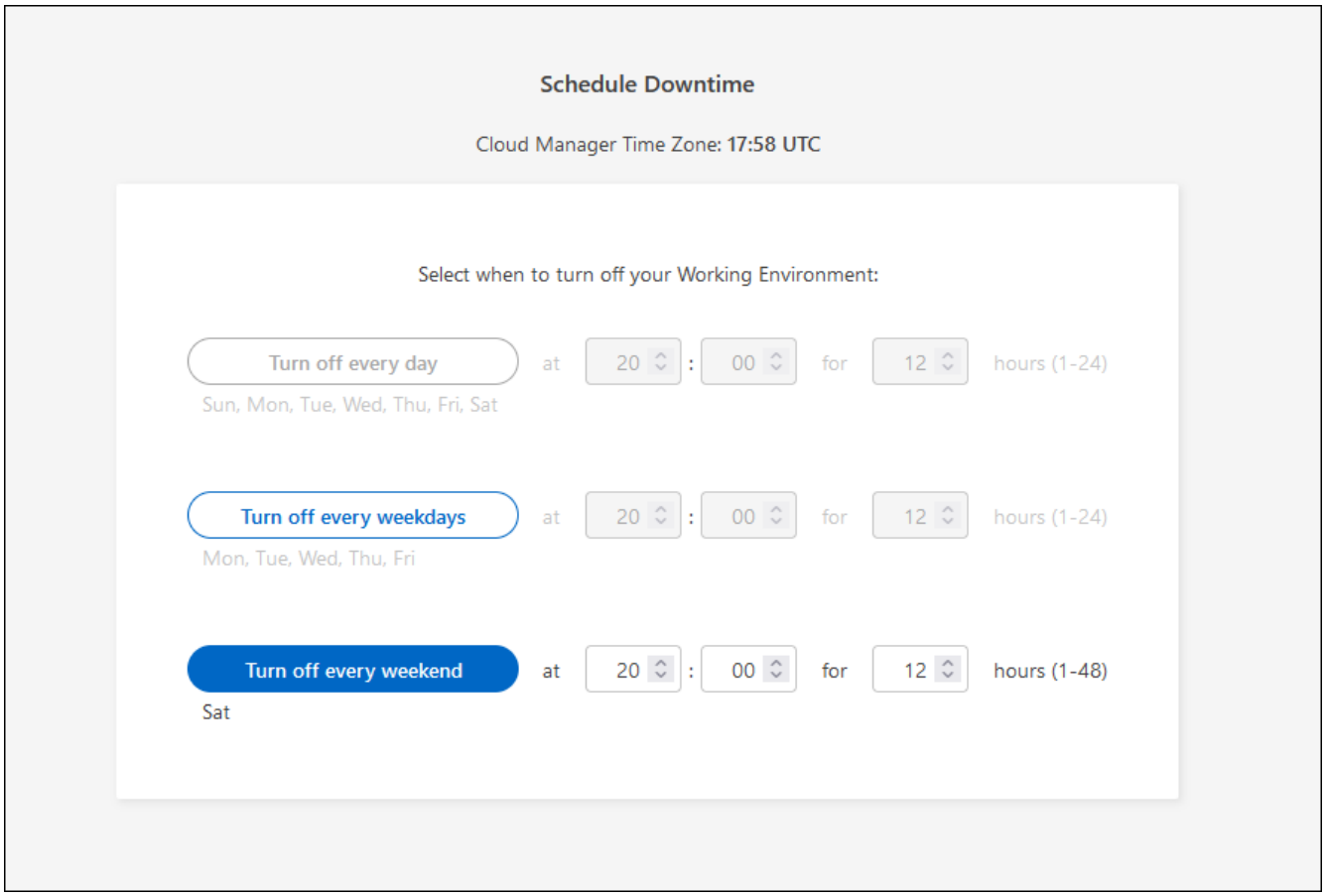
3. Geben Sie den Zeitplan für das Herunterfahren an:

   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, mit dem BlueXP anweist, das System jeden Samstag um 20:00 UHR herunterzufahren (8:00 Uhr) für 12 Stunden. BlueXP startet das System jeden Montag um 12:00 Uhr neu



4. Klicken Sie Auf **Speichern**.

Ergebnis

BlueXP speichert den Zeitplan. Der entsprechende Posten für geplante Ausfallzeiten im Bereich „Funktionen“ wird „ein“ angezeigt.

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.

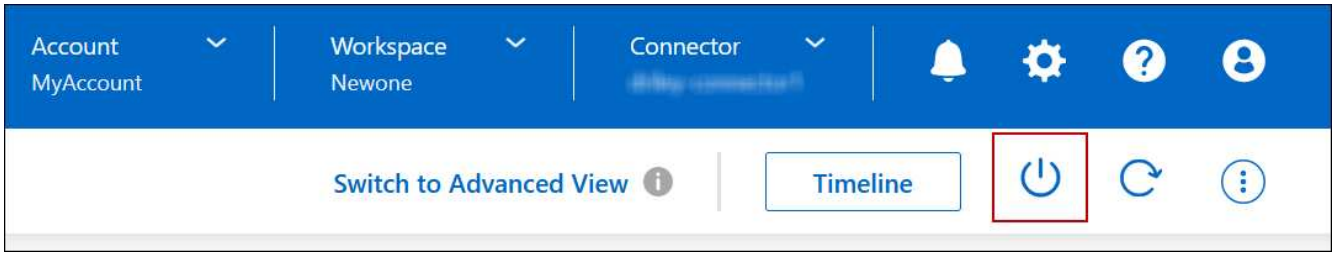
> Zur Senkung der Kosten löscht BlueXP in regelmäßigen Abständen ältere Snapshots von Root- und Boot-Festplatten. Nur die beiden letzten Snapshots werden sowohl für die Root- als auch für Boot Disks beibehalten.

Über diese Aufgabe

Wenn Sie ein HA-Paar anhalten, werden beide Nodes von BlueXP heruntergefahren.

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.

   Snapshots werden beim Neustart automatisch erstellt.

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 über den einen NTP-Server an "BlueXP API" Oder über die Benutzeroberfläche, wenn Sie möchten "Erstellen Sie einen CIFS-Server".

Ändern Sie die Schreibgeschwindigkeit des Systems

Mit BlueXP können Sie eine normale oder hohe Schreibgeschwindigkeit für Cloud Volumes ONTAP auswählen. Die standardmäßige Schreibgeschwindigkeit ist normal. Wenn für Ihren Workload eine hohe Schreib-Performance erforderlich ist, kann die hohe Schreibgeschwindigkeit geändert werden.

Eine hohe Schreibgeschwindigkeit wird bei allen Arten von Single-Node-Systemen und einigen HA-Paar-Konfigurationen unterstützt. Zeigen Sie unterstützte Konfigurationen in an "Versionshinweise zu Cloud Volumes ONTAP"

Bevor Sie die Schreibgeschwindigkeit ändern, sollten Sie dies tun "Die Unterschiede zwischen den normalen und den hohen Einstellungen verstehen".

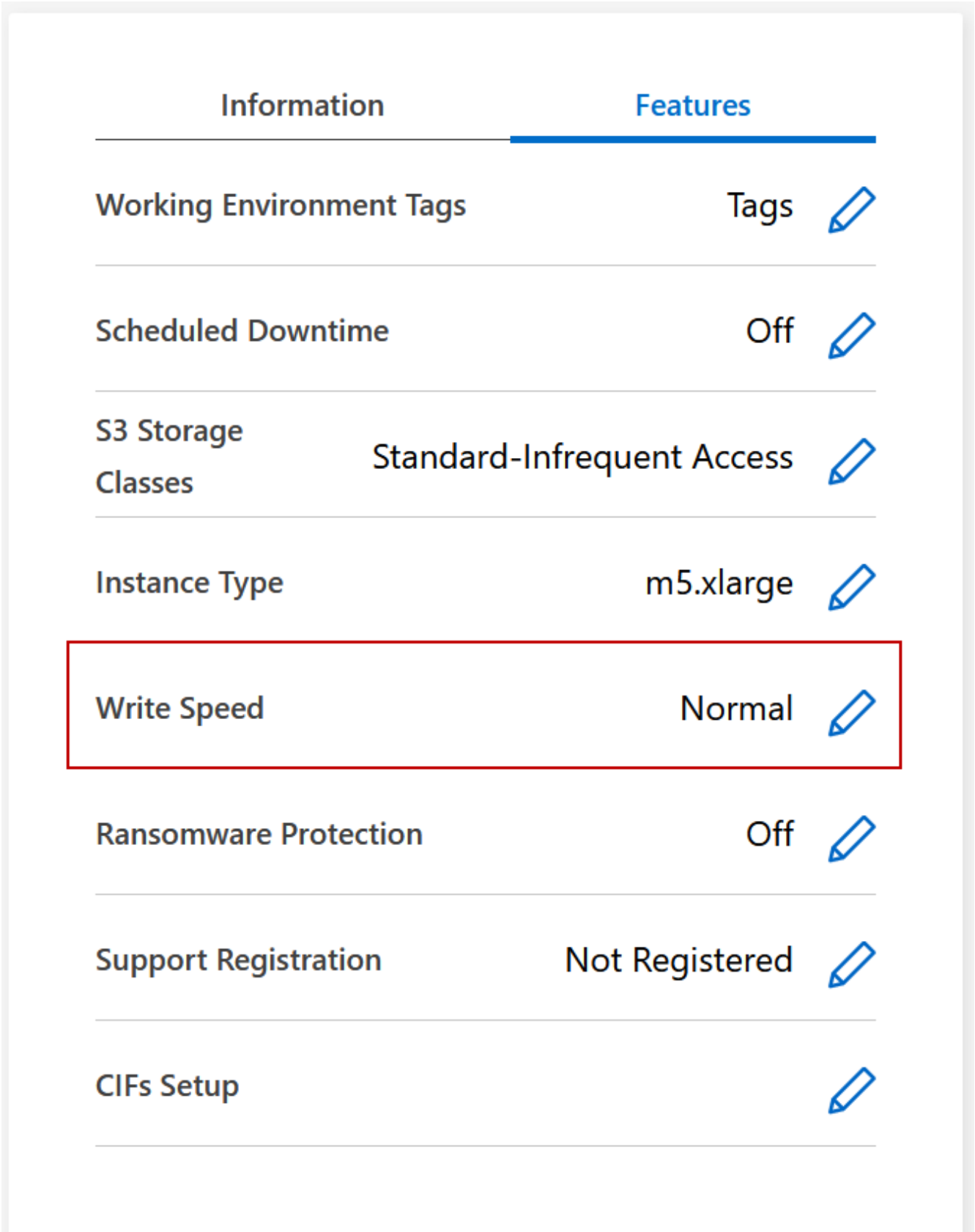
Über diese Aufgabe

- Stellen Sie sicher, dass Vorgänge wie die Volume- oder Aggregaterstellung nicht ausgeführt werden.
- Beachten Sie, dass durch diese Änderung das Cloud Volumes ONTAP-System neu gestartet wird. Dies ist ein disruptiver Prozess, der Downtime für das gesamte System erfordert.

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsfläche auf den Namen des Systems, das Sie für die Schreibgeschwindigkeit konfigurieren.

2. Klicken Sie auf der Registerkarte Übersicht auf das Bedienfeld Funktionen und dann auf das Bleistiftsymbol neben **Schreibgeschwindigkeit**.



3. Wählen Sie **normal** oder **hoch**.

Wenn Sie „hoch“ wählen, müssen Sie die „Ich verstehe…“-Aussage lesen und bestätigen, indem Sie das Kästchen aktivieren.

Die Option **High** Schreibgeschwindigkeit wird ab Version 9.13.0 von Cloud Volumes ONTAP HA-Paaren in Google Cloud unterstützt.

4. Klicken Sie auf **Speichern**, überprüfen Sie die Bestätigungsmeldung und klicken Sie dann auf **Approve**.

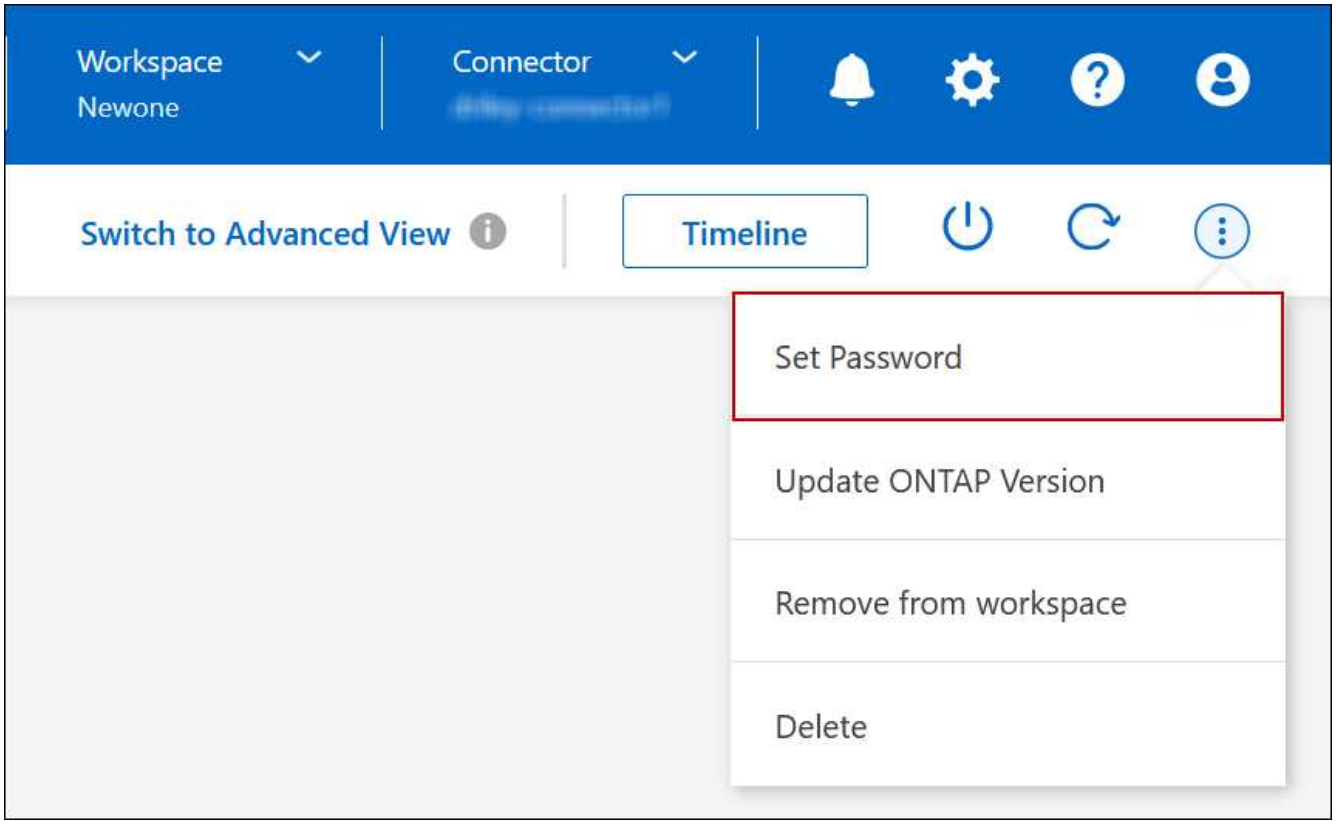
Ändern Sie das Passwort für Cloud Volumes ONTAP

Cloud Volumes ONTAP enthält ein Cluster-Administratorkonto. Sie können das Kennwort für dieses Konto bei Bedarf von BlueXP ändern.

Sie sollten das Kennwort für das Administratorkonto nicht über System Manager oder die CLI ändern. Das Kennwort wird in BlueXP nicht angezeigt. Daher kann BlueXP die Instanz nicht ordnungsgemäß überwachen.

Schritte

1. Doppelklicken Sie auf der Seite Bildschirm auf den Namen der Cloud Volumes ONTAP-Arbeitsumgebung.
2. Klicken Sie oben rechts auf der BlueXP-Konsole auf das Ellipsensymbol und wählen Sie **set password** aus.



Das neue Kennwort muss sich von einem der letzten sechs Kennwörter unterscheiden.

Hinzufügen, Entfernen oder Löschen von Systemen

Hinzufügen vorhandener Cloud Volumes ONTAP-Systeme zu BlueXP

Sie können vorhandene Cloud Volumes ONTAP-Systeme entdecken und zu BlueXP hinzufügen. Dies können Sie tun, wenn Sie ein neues BlueXP System implementiert haben.

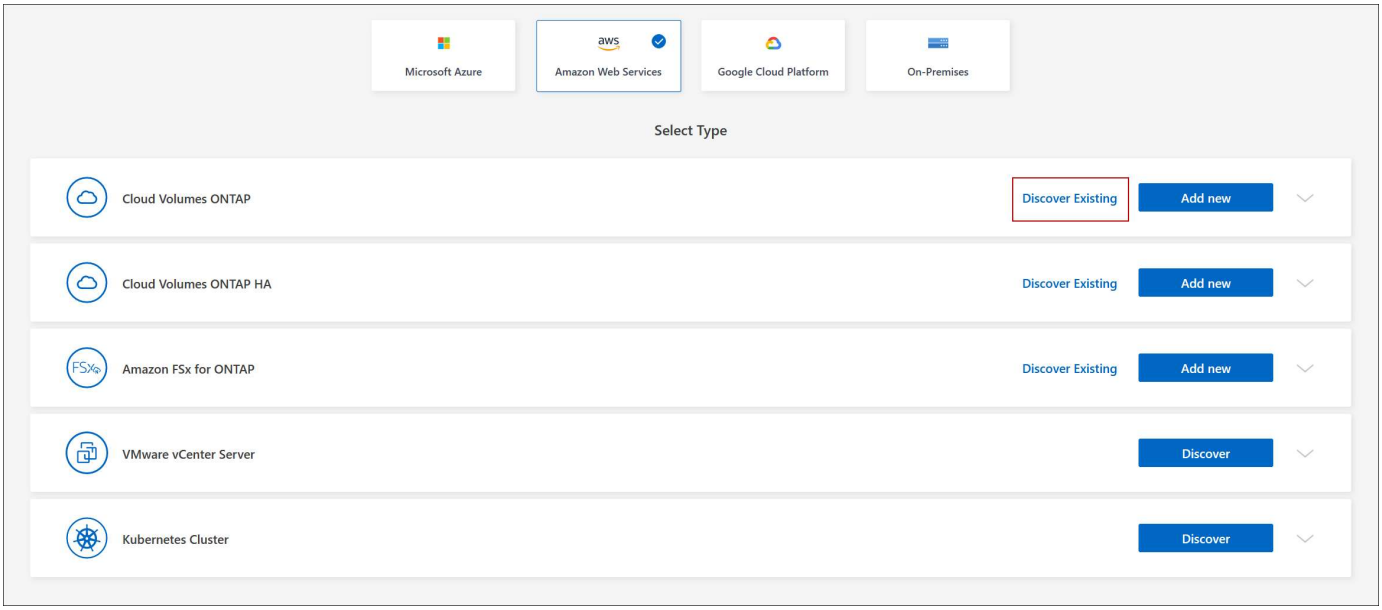
Bevor Sie beginnen

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

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen**.
3. Wählen Sie den Cloud-Provider aus, in dem sich das System befindet.
4. Wählen Sie den Typ des Cloud Volumes ONTAP Systems aus.
5. Klicken Sie auf den Link, um ein vorhandenes System zu ermitteln.

+



1. Wählen Sie auf der Seite Region den Bereich aus, in dem die Instanzen ausgeführt werden, und wählen Sie dann die Instanzen aus.
2. Geben Sie auf der Seite Anmeldeinformationen das Kennwort für den Cloud Volumes ONTAP-Admin-Benutzer ein, und klicken Sie dann auf **Los**.

Ergebnis

BlueXP fügt die Cloud Volumes ONTAP-Instanzen zum Arbeitsbereich hinzu.

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

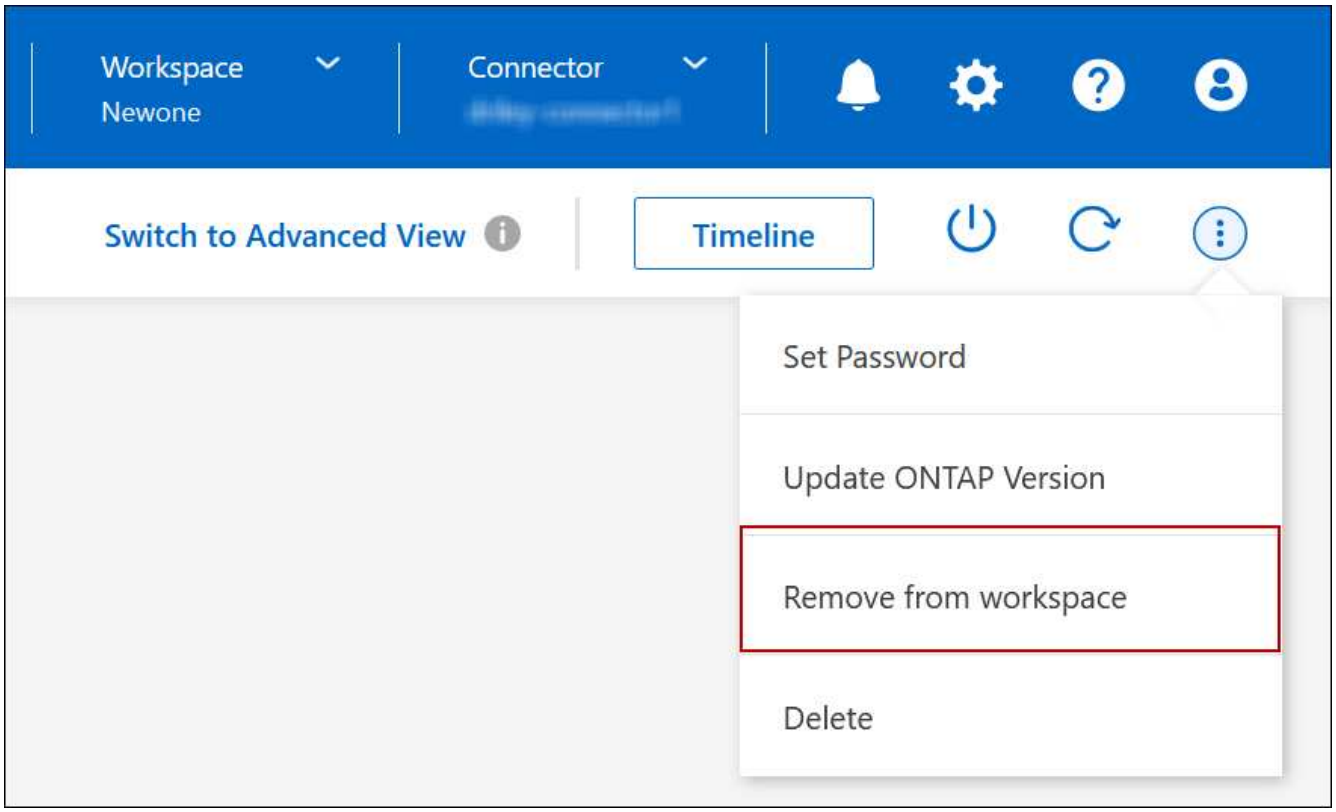
Durch Entfernen einer Cloud Volumes ONTAP-Arbeitsumgebung wird sie von BlueXP entfernt. Das Cloud Volumes ONTAP System wird nicht gelöscht. Sie können die Arbeitsumgebung später neu entdecken.

Durch das Entfernen einer Arbeitsumgebung aus BlueXP können Sie Folgendes tun:

- In einem anderen Arbeitsbereich neu entdecken
- Entdecken Sie sie von einem anderen BlueXP-System
- Entdecken Sie es erneut, wenn Sie während der ersten Erkennung Probleme hatten

Schritte

1. Doppelklicken Sie auf der Seite Arbeitsfläche auf die Arbeitsumgebung, die Sie entfernen möchten.
2. Klicken Sie oben rechts auf der BlueXP-Konsole auf das Ellipsensymbol und wählen Sie **aus Workspace entfernen** aus.



3. Klicken Sie im Fenster aus dem Arbeitsbereich überprüfen auf **Entfernen**.

Ergebnis

BlueXP beseitigt die Arbeitsumgebung. Benutzer können diese Arbeitsumgebung jederzeit von der Seite Canvas neu entdecken.

Löschen eines Cloud Volumes ONTAP Systems

Sie sollten Cloud Volumes ONTAP-Systeme immer von BlueXP löschen, anstatt von der Konsole Ihres Cloud-Providers. Wenn Sie beispielsweise eine lizenzierte Cloud Volumes ONTAP-Instanz von Ihrem Cloud-Provider beenden, können Sie den Lizenzschlüssel nicht für eine andere Instanz verwenden. Sie müssen die Arbeitsumgebung von BlueXP

löschen, um die Lizenz freizugeben.

Wenn Sie eine Arbeitsumgebung löschen, beendet BlueXP Cloud Volumes ONTAP-Instanzen und löscht Festplatten und Snapshots.

Ressourcen, die von anderen Services wie Backups für BlueXP Backup und Recovery sowie Instanzen für die BlueXP Klassifizierung gemanagt werden, werden beim Löschen einer Arbeitsumgebung nicht gelöscht. Sie müssen sie manuell löschen. Andernfalls erhalten Sie weiterhin Gebühren für diese Ressourcen.

Wenn BlueXP Cloud Volumes ONTAP bei Ihrem Cloud-Provider implementiert, ermöglicht es Ihnen, die Beendigung des Arbeitsabfalls zu gewährleisten. Diese Option verhindert versehentliches Beenden.

Schritte

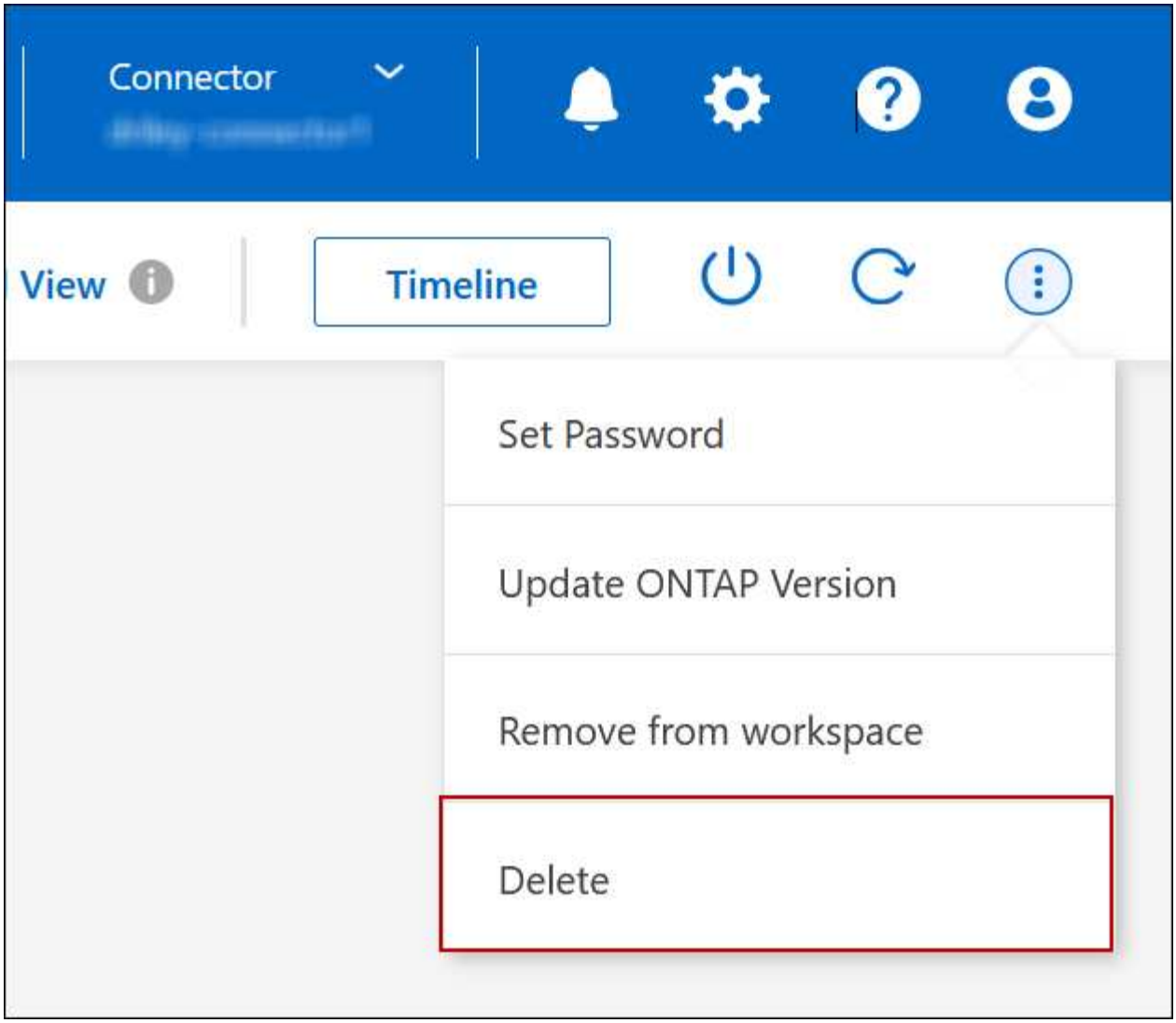
1. Wenn Sie das Backup und Recovery von BlueXP in der Arbeitsumgebung aktiviert haben, stellen Sie fest, ob die gesicherten Daten noch erforderlich sind, und legen Sie dann fest "Löschen Sie die Backups, falls erforderlich".

   BlueXP Backup und Recovery sind unabhängig von Cloud Volumes ONTAP. BlueXP Backup und Recovery löscht Backups nicht automatisch, wenn Sie ein Cloud Volumes ONTAP System löschen. Es gibt derzeit keine Unterstützung in der Benutzeroberfläche, um die Backups nach dem Löschen des Systems zu löschen.

2. Wenn Sie die BlueXP Klassifizierung in dieser Arbeitsumgebung aktiviert haben und keine anderen Arbeitsumgebungen diesen Service verwenden, müssen Sie die Instanz für den Service löschen.

   "Erfahren Sie mehr über die BlueXP Klassifizierungsinstanz".

3. Löschen Sie die Cloud Volumes ONTAP-Arbeitsumgebung.
   a. Doppelklicken Sie auf der Seite „Arbeitsfläche“ auf den Namen der Cloud Volumes ONTAP-Arbeitsumgebung, die Sie löschen möchten.
   b. Klicken Sie oben rechts auf der BlueXP-Konsole auf das Ellipsensymbol und wählen Sie **Löschen** aus.



c. Geben Sie im Fenster Arbeitsumgebung löschen den Namen der Arbeitsumgebung ein und klicken Sie dann auf **Löschen**.

   Das Löschen der Arbeitsumgebung kann bis zu 5 Minuten dauern.

AWS Administration

Ändern des EC2 Instanztyps für Cloud Volumes ONTAP

Beim Start von Cloud Volumes ONTAP in AWS können Sie zwischen verschiedenen Instanzen oder Typen wählen. Sie können den Instanztyp 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 Instanztyps kann sich auf die AWS Servicegebühren auswirken.

- 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.

BlueXP ändert den Knoten nacheinander 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.

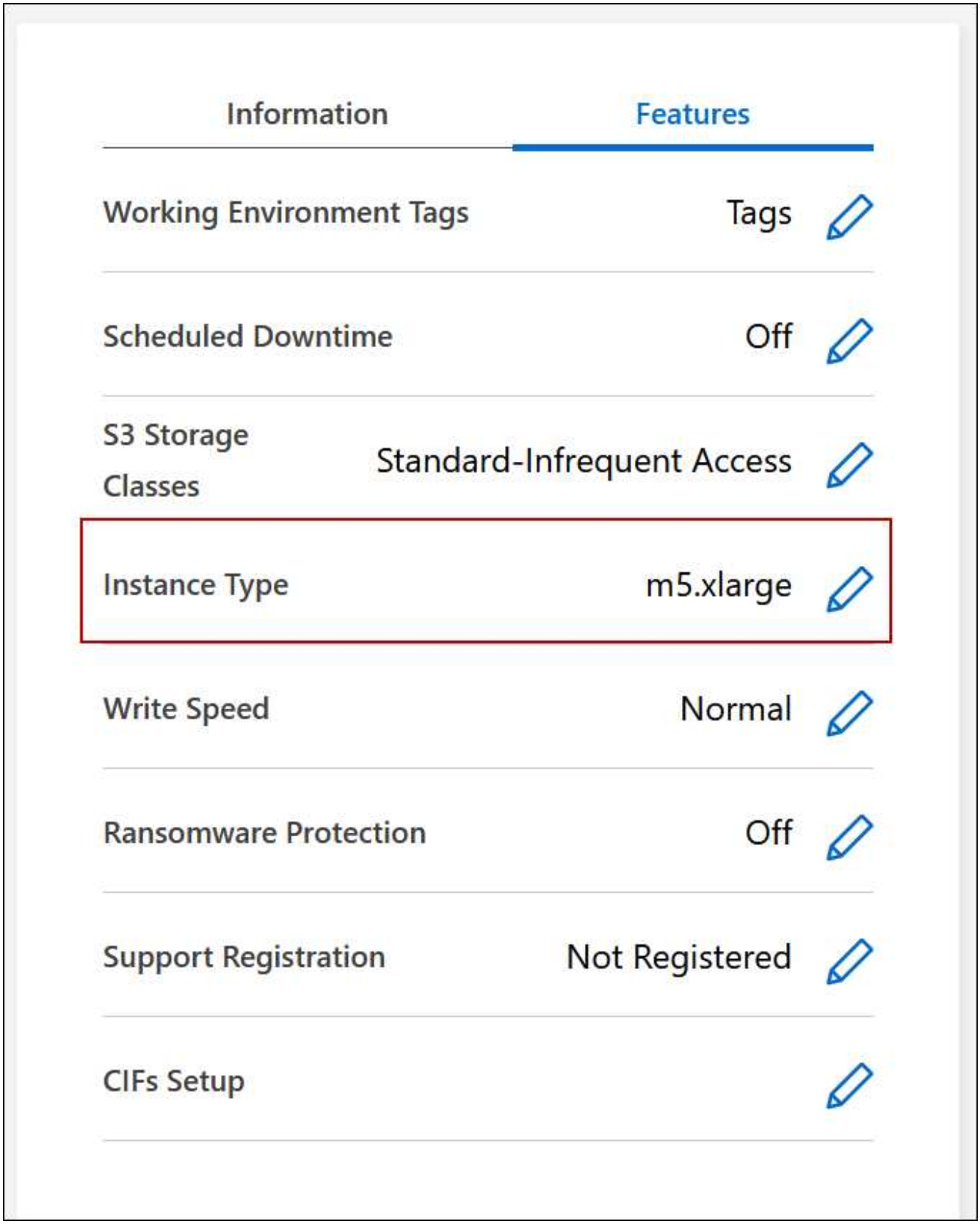
Referenz

Eine Liste der unterstützten Instanztypen in AWS finden Sie unter "Unterstützte EC2 Instanzen".

Wenn Sie den Instanztyp nicht von den Instanzen c4, m4 oder R4 ändern können, lesen Sie den KB-Artikel "Konvertieren einer AWS Xen CVO-Instanz in Nitro (KVM)".

Schritte

1. Wählen Sie auf der Seite Arbeitsfläche die Arbeitsumgebung aus.
2. Klicken Sie auf der Registerkarte Übersicht auf das Bedienfeld Funktionen und dann auf das Bleistiftsymbol neben **Instanztyp**.



a. Wenn Sie eine Node-basierte PAYGO-Lizenz verwenden, können Sie optional einen anderen Lizenz- und Instanztyp auswählen, indem Sie auf das Bleistiftsymbol neben **Lizenztyp** klicken.

3. Wählen Sie einen Instanztyp, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Auswirkungen der Änderung verstehen, und klicken Sie dann auf **Ändern**.

Ergebnis

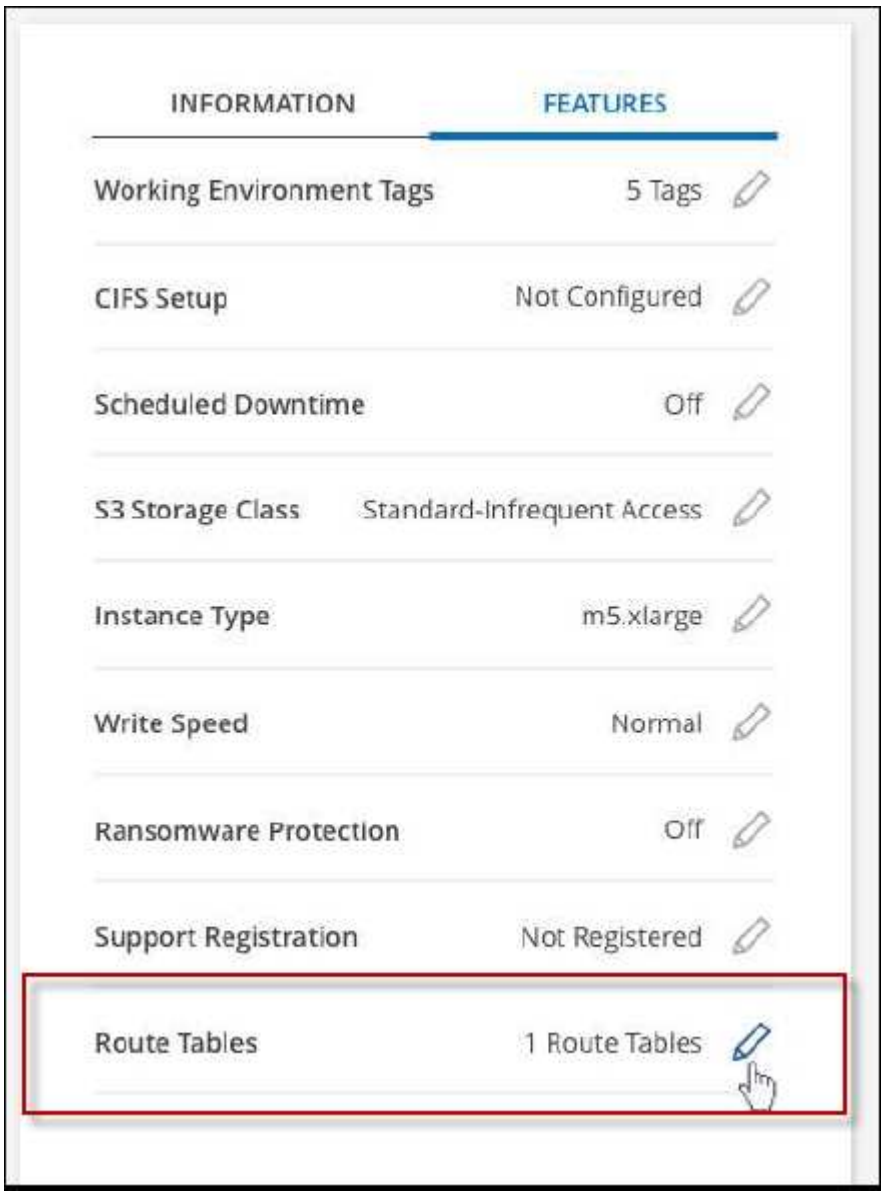
Cloud Volumes ONTAP wird mit der neuen Konfiguration neu gestartet.

Ändern Sie Routingtabellen für HA-Paare in mehreren AZS

Sie können die AWS-Routingtabellen ändern, die Routen zu den unverankerten IP-Adressen für ein HA-Paar einschließen, das in mehreren AWS Availability Zones (AZS) implementiert wird. Vielleicht möchten Sie dies tun, wenn neue NFS- oder CIFS-Clients auf ein HA-Paar in AWS zugreifen müssen.

Schritte

1. Wählen Sie auf der Seite Arbeitsfläche die Arbeitsumgebung aus.
2. Klicken Sie auf der Registerkarte Übersicht auf das Bedienfeld Funktionen und dann auf das Bleistiftsymbol neben **Routingtabellen**.



3. Ändern Sie die Liste der ausgewählten Routentabellen und klicken Sie dann auf **Speichern**.

Ergebnis

BlueXP sendet eine AWS-Anforderung, um die Routingtabellen zu ändern.

Azure-Administration

Ändern Sie den Azure VM-Typ für Cloud Volumes ONTAP

Sie können zwischen verschiedenen VM-Typen wählen, wenn Sie Cloud Volumes ONTAP in Microsoft Azure starten. Sie können den VM-Typ jederzeit ändern, wenn Sie die Größe entsprechend Ihren Anforderungen als zu groß oder zu groß definieren.

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 VM-Typs kann sich auf Microsoft Azure Servicegebühren auswirken.
- Der Vorgang startet Cloud Volumes ONTAP neu.

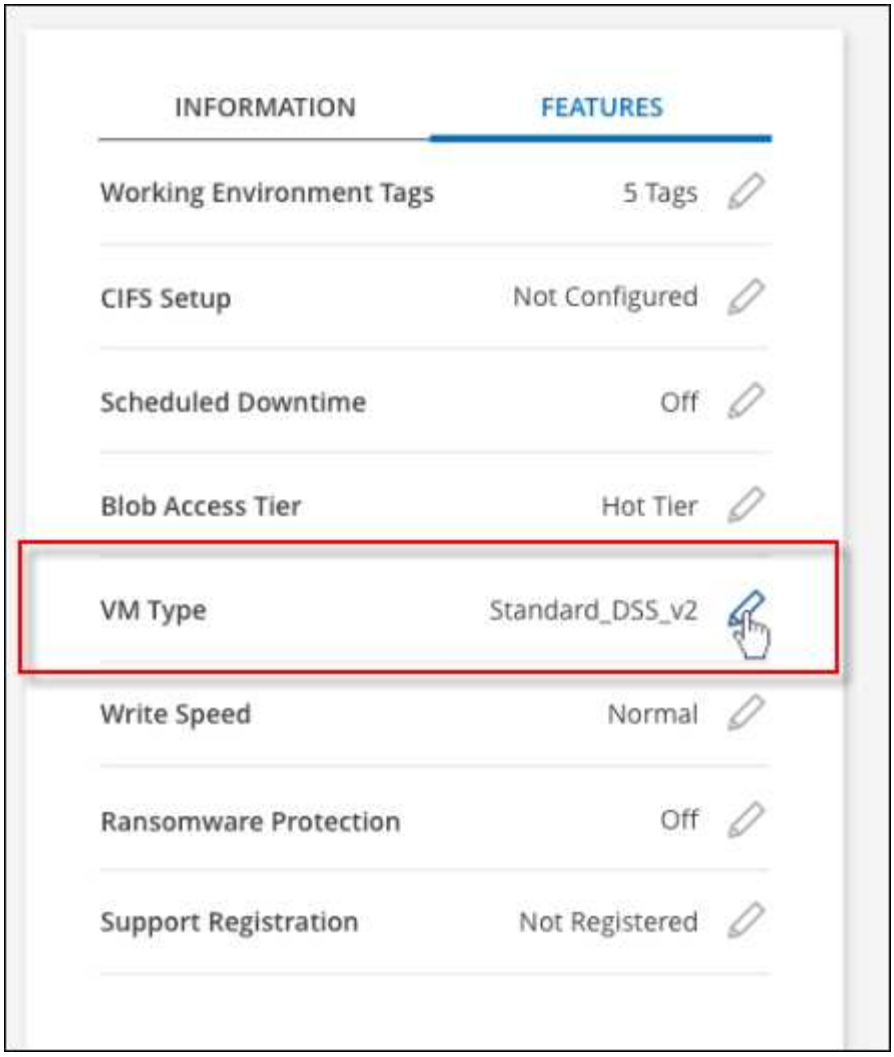
  Bei Systemen mit einem Node wird die I/O unterbrochen.

  Bei HA-Paaren ist die Änderung unterbrechungsfrei. Ha-Paare stellen weiterhin Daten bereit.

  BlueXP ändert den Knoten nacheinander 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. Wählen Sie auf der Seite Arbeitsfläche die Arbeitsumgebung aus.
2. Klicken Sie auf der Registerkarte Übersicht auf das Bedienfeld Funktionen und dann auf das Bleistiftsymbol neben **VM type**.



a. Wenn Sie eine Node-basierte PAYGO-Lizenz verwenden, können Sie optional eine andere Lizenz und einen anderen VM-Typ auswählen, indem Sie auf das Bleistiftsymbol neben **Lizenztyp** klicken.

3. Wählen Sie einen VM-Typ aus, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Auswirkungen der Änderung verstehen, und klicken Sie dann auf **Ändern**.

Ergebnis

Cloud Volumes ONTAP wird mit der neuen Konfiguration neu gestartet.

Überschreiben von CIFS-Sperren für Cloud Volumes ONTAP HA-Paare in Azure

Der Account Administrator kann in BlueXP eine Einstellung aktivieren, die Probleme mit der Cloud Volumes ONTAP Storage-Rückgabe bei Azure Wartungsereignissen 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 ein Wartungsereignis auf einem Cloud Volumes ONTAP HA-Paar stattfindet, initiiert das HA-Paar die Storage-Übernahme. Wenn während dieses Wartungsereignisses aktive CIFS-Sitzungen vorhanden sind, können die Sperren von CIFS-Dateien die Rückgabe von Storage 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-Giveback durchführen.

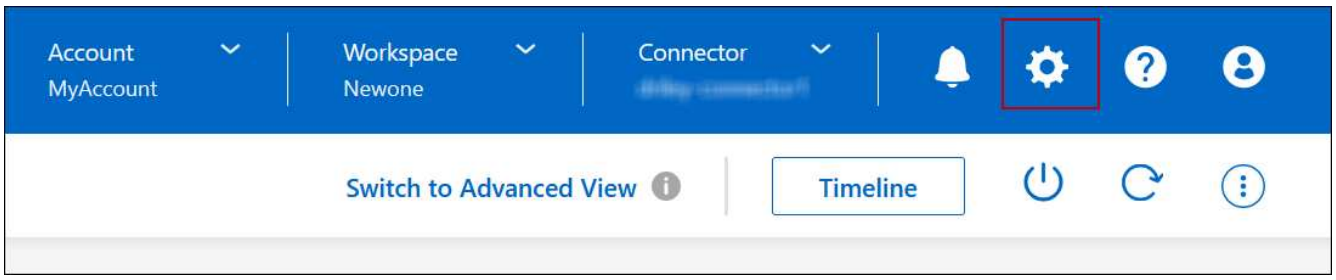
Dieser Prozess kann CIFS-Clients stören. Daten, die nicht von CIFS-Clients übertragen werden, können verloren gehen.

Was Sie benötigen

Sie müssen einen Konnektor erstellen, bevor Sie BlueXP-Einstellungen ändern können. "Erfahren Sie, wie".

Schritte

1. Klicken Sie oben rechts in der BlueXP Konsole auf das Symbol Einstellungen und wählen Sie **Cloud Volumes ONTAP-Einstellungen** aus.



2. Klicken Sie unter **Azure** auf **Azure CIFS Locks for Azure HA Working Environments**.
3. Klicken Sie auf das Kontrollkästchen, um die Funktion zu aktivieren, und klicken Sie dann auf **Speichern**.

Nutzen Sie einen Azure Private Link oder einen Service-Endpunkt

Für Verbindungen zu den zugehörigen Storage-Konten nutzt Cloud Volumes ONTAP einen Azure Private Link. Bei Bedarf können Sie Azure Private Links deaktivieren und stattdessen Service-Endpunkte verwenden.

Überblick

Standardmäßig aktiviert BlueXP einen Azure Private Link für Verbindungen zwischen Cloud Volumes ONTAP und den zugehörigen Speicherkonten. Ein Azure Private Link sichert die Verbindungen zwischen Endpunkten in Azure und bietet Performance-Vorteile.

Bei Bedarf können Sie Cloud Volumes ONTAP so konfigurieren, dass Service-Endpunkte anstelle einer Azure Private Link verwendet werden.

Bei beiden Konfigurationen schränkt BlueXP den Netzwerkzugriff für Verbindungen zwischen Cloud Volumes ONTAP- und Speicherkonten immer ein. Der Netzwerkzugriff ist auf das vnet beschränkt, in dem Cloud Volumes ONTAP bereitgestellt wird, und auf das vnet, wo der Connector bereitgestellt wird.

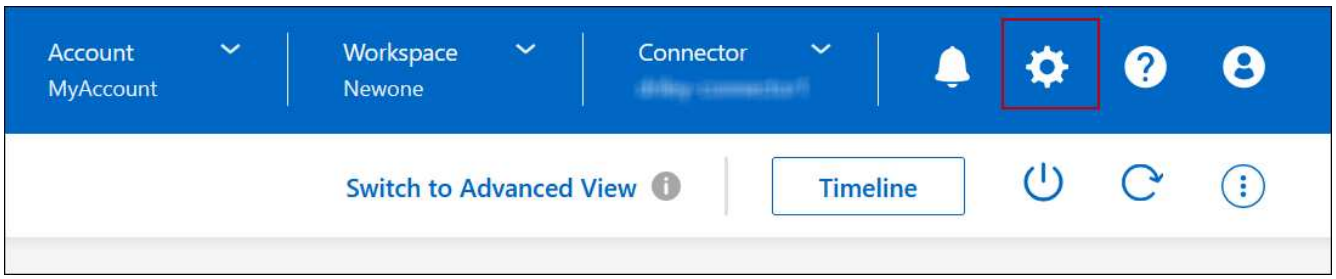
Deaktivieren Sie Azure Private Links, und verwenden Sie stattdessen Service-Endpunkte

Falls in Ihrem Unternehmen erforderlich, können Sie eine Einstellung in BlueXP ändern, sodass Cloud Volumes ONTAP für die Verwendung von Service-Endpunkten anstelle eines Azure Private Links konfiguriert wird. Das Ändern dieser Einstellung gilt für neue von Ihnen erstellte Cloud Volumes ONTAP Systeme. Service-Endpunkte werden nur in unterstützt "Azure Region-Paare" Zwischen Stecker und Cloud Volumes ONTAP VNets.

Der Connector sollte in derselben Azure-Region wie die Cloud Volumes ONTAP-Systeme, die er verwaltet, oder in der implementiert werden "Azure Region Paar" Für die Cloud Volumes ONTAP Systeme.

Schritte

1. Klicken Sie oben rechts in der BlueXP Konsole auf das Symbol Einstellungen und wählen Sie **Cloud Volumes ONTAP-Einstellungen** aus.



2. Klicken Sie unter **Azure** auf **Azure Private Link verwenden**.
3. Deaktivieren Sie **Private Link-Verbindung zwischen Cloud Volumes ONTAP und Speicherkonten**.
4. Klicken Sie Auf **Speichern**.

Nachdem Sie fertig sind

Wenn Sie Azure Private Links deaktiviert haben und der Connector einen Proxyserver verwendet, müssen Sie direkten API-Datenverkehr aktivieren.

"Erfahren Sie, wie Sie direkten API-Datenverkehr auf dem Connector aktivieren"

Arbeiten Sie mit Azure Private Links

In den meisten Fällen müssen Sie nichts tun, um Azure Private Links mit Cloud Volumes ONTAP einzurichten. BlueXP managt Azure Private Links für Sie. Wenn Sie jedoch eine bestehende Azure Private DNS-Zone verwenden, müssen Sie eine Konfigurationsdatei bearbeiten.

Anforderung für benutzerdefiniertes DNS

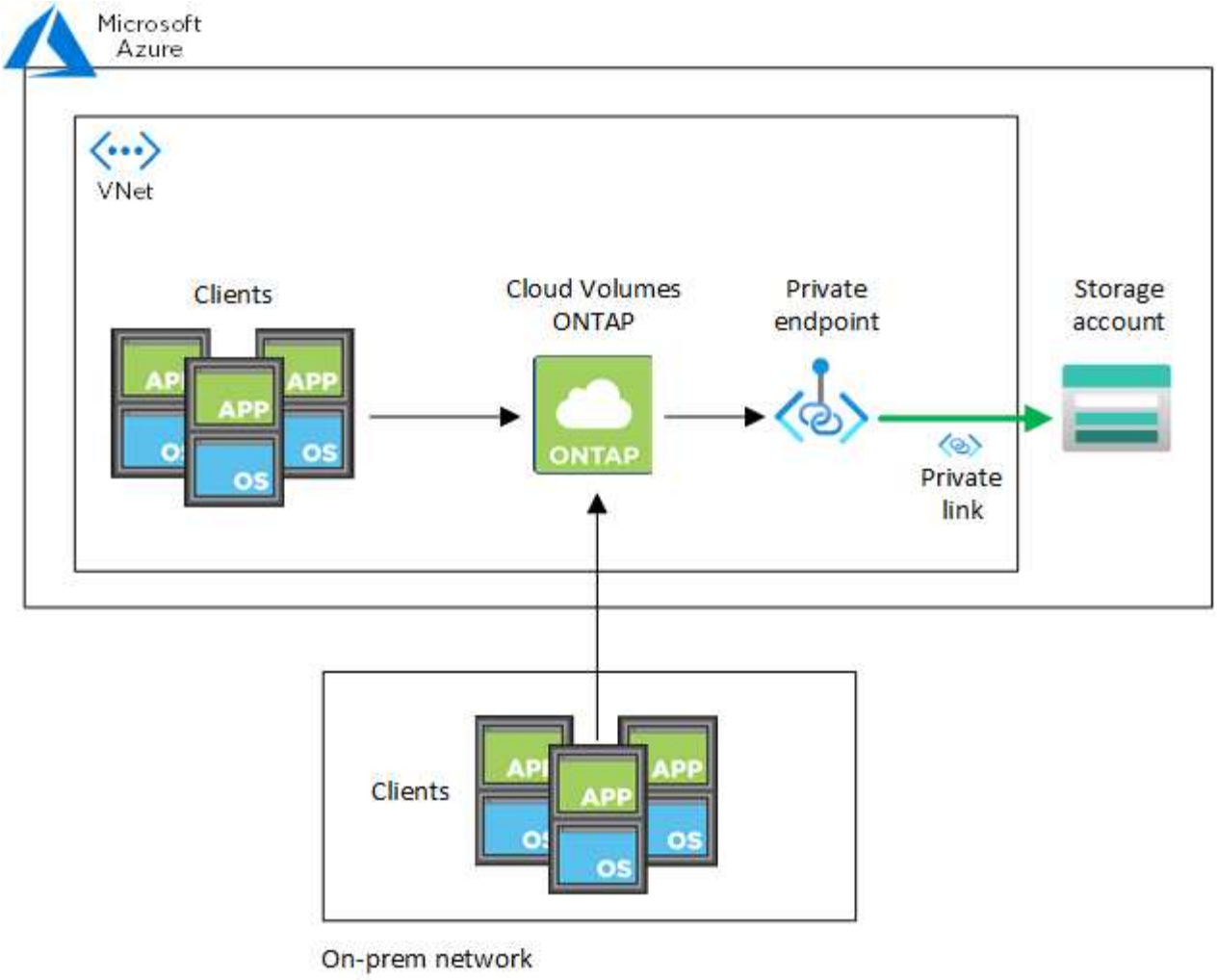
Wenn Sie optional mit benutzerdefinierten DNS arbeiten, müssen Sie von Ihren benutzerdefinierten DNS-Servern aus einen bedingten Forwarder zur Azure Private DNS Zone erstellen. Weitere Informationen finden Sie unter "Die Dokumentation von Azure über einen DNS-Forwarder".

Funktionsweise von Private Link-Verbindungen

Wenn BlueXP Cloud Volumes ONTAP in Azure implementiert, wird damit ein privater Endpunkt in der Ressourcengruppe erstellt. Der private Endpunkt ist mit Storage-Konten für Cloud Volumes ONTAP verknüpft. Dadurch wird der Zugriff auf Cloud Volumes ONTAP Storage über das Microsoft Backbone-Netzwerk übertragen.

Der Client-Zugriff erfolgt über den privaten Link, wenn sich Clients innerhalb desselben vnet wie Cloud Volumes ONTAP, innerhalb von Peered VNets oder in Ihrem lokalen Netzwerk befinden, wenn sie ein privates VPN oder eine ExpressRoute Verbindung zum vnet verwenden.

Das Beispiel zeigt den Client-Zugriff über einen privaten Link innerhalb desselben Netzwerks und von einem Netzwerk vor Ort, das entweder über ein privates VPN oder eine ExpressRoute Verbindung verfügt.



Wenn die Connector- und Cloud Volumes ONTAP-Systeme in verschiedenen VNets bereitgestellt werden, müssen Sie vnet Peering zwischen dem vnet einrichten, in dem der Connector bereitgestellt wird, und dem vnet, in dem die Cloud Volumes ONTAP-Systeme bereitgestellt werden.

Stellen Sie BlueXP Einzelheiten zu Ihrem Azure Private DNS zur Verfügung

Wenn Sie verwenden "Azure Private DNS", Dann müssen Sie eine Konfigurationsdatei auf jedem Connector ändern. Andernfalls kann BlueXP die private Link-Verbindung zu Azure zwischen Cloud Volumes ONTAP und den zugehörigen Speicherkonten nicht aktivieren.

Beachten Sie, dass der DNS-Name mit den Benennungsanforderungen für Azure DNS übereinstimmen muss "Wie in der Azure-Dokumentation zu sehen ist".

Schritte

1. SSH auf dem Connector-Host und melden Sie sich an.
2. Navigieren Sie zum folgenden Verzeichnis: /Opt/Application/netapp/cloudmanager/docker_occm/Data
3. Bearbeiten Sie App.conf, indem Sie den Parameter „user-private-dns-Zone-settings“ mit den folgenden Schlüsselwort-Wert-Paaren hinzufügen:

```
"user-private-dns-zone-settings" : {
   "resource-group" : "<resource group name of the DNS zone>",
   "subscription" : "<subscription ID>",
   "use-existing" : true,
   "create-private-dns-zone-link" : true
}
```

Der Parameter sollte auf derselben Ebene wie die „System-id“ eingegeben werden, wie unten gezeigt:

```
"system-id" : "<system ID>",
"user-private-dns-zone-settings" : {
```

Beachten Sie, dass das Abonnement-Schlüsselwort nur erforderlich ist, wenn die private DNS-Zone in einem anderen Abonnement als der Connector vorhanden ist.

4. Speichern Sie die Datei und melden Sie sich vom Connector ab.

   Ein Neustart ist nicht erforderlich.

Rollback bei Ausfällen aktivieren

Wenn BlueXP einen Azure Private Link nicht im Rahmen bestimmter Aktionen erstellt, führt er die Aktion ohne die Azure Private Link-Verbindung durch. Dies kann bei der Erstellung einer neuen Arbeitsumgebung (einzelner Node oder HA-Paar) oder bei folgenden Aktionen auf einem HA-Paar passieren: Das Erstellen eines neuen Aggregats, das Hinzufügen von Festplatten zu einem vorhandenen Aggregat oder das Erstellen eines neuen Storage-Kontos bei über 32 tib Anforderungen.

Sie können dieses Standardverhalten ändern, indem Sie Rollback aktivieren, wenn BlueXP den Azure Private Link nicht erstellt. Auf diese Weise können Sie sicherstellen, dass Sie die Sicherheitsvorschriften Ihres Unternehmens vollständig erfüllen.

Wenn Sie Rollback aktivieren, stoppt BlueXP die Aktion und führt alle Ressourcen zurück, die im Rahmen der Aktion erstellt wurden.

Sie können Rollback über die API oder durch Aktualisierung der Datei App.conf aktivieren.

Rollback über die API aktivieren

Schritt

1. Verwenden Sie die `PUT /occm/config` API-Aufruf mit folgender Anfraentext:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

Rollback durch Aktualisierung von App.conf aktivieren

Schritte

1. SSH auf dem Connector-Host und melden Sie sich an.

2. Navigieren Sie zum folgenden Verzeichnis: /Opt/Application/netapp/cloudmanager/docker_occm/Data
3. Bearbeiten Sie App.conf, indem Sie den folgenden Parameter und Wert hinzufügen:

```
 "rollback-on-private-link-failure": true
. Speichern Sie die Datei und melden Sie sich vom Connector ab.
```

Ein Neustart ist nicht erforderlich.

Verschieben von Ressourcengruppen

Cloud Volumes ONTAP unterstützt Azure Ressourcengruppen. Der Workflow wird jedoch nur in der Azure Konsole ausgeführt.

Sie können eine Arbeitsumgebung innerhalb eines Azure-Abonnements von einer Ressourcengruppe auf eine andere Ressourcengruppe in Azure verschieben. Das Verschieben von Ressourcengruppen zwischen verschiedenen Azure-Abonnements wird nicht unterstützt.

Schritte

1. Entfernen Sie die Arbeitsumgebung aus **Canvas**.

   Informationen zum Entfernen einer Arbeitsumgebung finden Sie unter "Entfernen von Cloud Volumes ONTAP Arbeitsumgebungen".

2. Führen Sie die Verschiebung der Ressourcengruppe in der Azure-Konsole aus.

   Informationen zum Abschließen des Verzuvöllig finden Sie unter "Verschieben Sie Ressourcen in eine neue Ressourcengruppe oder ein Abonnement in der Microsoft Azure-Dokumentation".

3. Entdecken Sie in **Canvas** die Arbeitsumgebung.
4. Suchen Sie in den Informationen für die Arbeitsumgebung nach der neuen Ressourcengruppe.

Ergebnis

Die Arbeitsumgebung und ihre Ressourcen (VMs, Festplatten, Speicherkonten, Netzwerkschnittstellen, Snapshots) befinden sich in der neuen Ressourcengruppe.

Trennen Sie SnapMirror Traffic in Azure

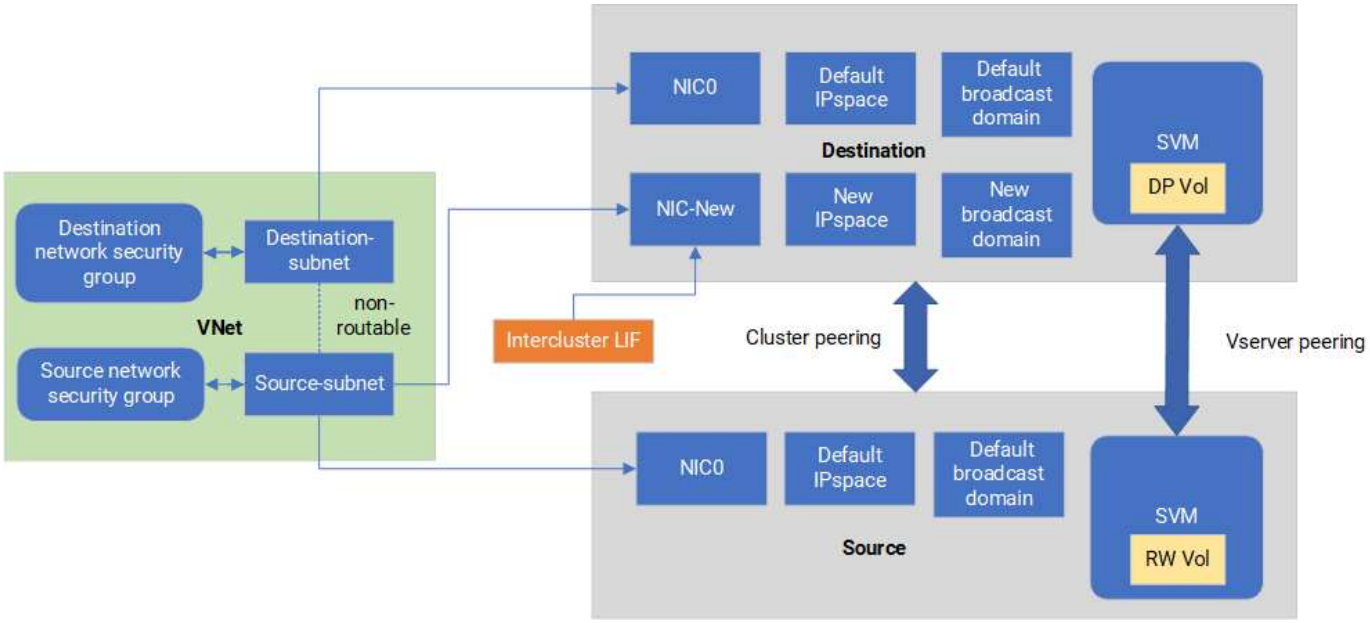
Mit Cloud Volumes ONTAP in Azure können Sie den SnapMirror Replizierungsverkehr von Daten- und Managementverkehr trennen. Um den SnapMirror Replizierungsverkehr von Ihrem Datenverkehr zu trennen, fügen Sie eine neue Netzwerkschnittstellenkarte (NIC), eine zugeordnete Intercluster LIF und ein nicht routingfähiges Subnetz hinzu.

Allgemeines zur Trennung von SnapMirror Datenverkehr in Azure

Standardmäßig konfiguriert BlueXP alle NICs und LIFs in einer Cloud Volumes ONTAP-Implementierung im selben Subnetz. In solchen Konfigurationen wird der Datenverkehr der SnapMirror Replizierung sowie der Daten- und Managementverkehr im gleichen Subnetz verarbeitet. Die Trennung von SnapMirror Traffic nutzt ein zusätzliches Subnetz, das nicht zu dem für Daten- und Managementdatenverkehr verwendeten Subnetz geleitet werden kann.

Abbildung 1

Die folgenden Diagramme zeigen die Trennung des SnapMirror Replizierungsdatenverkehrs zwischen einer zusätzlichen NIC, einer zugeordneten Intercluster LIF und einem nicht routingfähigen Subnetz in einer Implementierung mit einem einzelnen Node. Eine HA-Paar-Implementierung unterscheidet sich geringfügig.



Bevor Sie beginnen

Gehen Sie die folgenden Überlegungen durch:

- Es kann nur eine einzelne NIC zu einem einzelnen Cloud Volumes ONTAP-Knoten oder HA-Paar-Implementierung (VM-Instanz) für die SnapMirror-Traffic-Trennung hinzugefügt werden.
- Um einen neuen NIC hinzuzufügen, muss der zu implementierende VM-Instanztyp über eine nicht verwendete NIC verfügen.
- Die Quell- und Ziel-Cluster sollten Zugriff auf dasselbe virtuelle Netzwerk (vnet) haben. Ziel-Cluster ist ein Cloud Volumes ONTAP System in Azure. Beim Quell-Cluster kann es sich um ein Cloud Volumes ONTAP System in Azure oder um ein ONTAP System handeln.

Schritt: Erstellen Sie eine zusätzliche NIC und verbinden Sie sie mit der Ziel-VM

Dieser Abschnitt enthält Anweisungen zum Erstellen einer zusätzlichen NIC und zum Anhängen an die Ziel-VM. Die Ziel-VM ist das Single Node- oder HA-Paar-System in Cloud Volumes ONTAP in Azure, wo Sie Ihre zusätzliche NIC einrichten möchten.

Schritte

1. Beenden Sie den Node in der ONTAP CLI.

```
dest::> halt -node <dest_node-vm>
```

2. Überprüfen Sie im Azure-Portal, ob der Status der VM (Node) angehalten lautet.

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. Beenden Sie den Node mithilfe der Bash-Umgebung in Azure Cloud Shell.
   a. Stoppen Sie den Node.

   ```
   az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
   ```

   b. Zuordnung des Knotens aufheben.

   ```
   az vm deallocate --resource-group <dest_node-rg> --name <dest_node-
   vm>
   ```

4. Konfigurieren Sie Regeln für Netzwerksicherheitsgruppen, damit die beiden Subnetze (Subnetz des Quell-Clusters und Subnetz des Zielclusteres) nicht routingfähig sind.
   a. Erstellen Sie die neue NIC auf der Ziel-VM.
   b. Suchen Sie nach der Subnetz-ID für das Subnetz des Quell-Clusters.

   ```
   az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet
   -name <vnet> --query id
   ```

   c. Erstellen Sie die neue NIC auf der Ziel-VM mit der Subnetz-ID für das Quell-Cluster-Subnetz. Hier geben Sie den Namen für die neue NIC ein.

   ```
   az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new>
   --subnet <id_from_prev_command> --accelerated-networking true
   ```

   d. Speichern Sie die private IP-Adresse. Diese IP-Adresse, <new_added_nic_primary_addr>, wird verwendet, um eine Intercluster LIF in zu erstellen Broadcast-Domäne, Intercluster LIF für die neue NIC.
5. Verbinden Sie die neue NIC mit der VM.

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics
<dest_node-vm-nic-new>
```

6. Starten Sie die VM (Knoten).

```
az vm start --resource-group <dest_node-rg>  --name <dest_node-vm>
```

7. Gehen Sie im Azure-Portal zu **Networking** und bestätigen Sie, dass die neue NIC, z.B. nic-New, existiert und beschleunigte Vernetzung aktiviert ist.

```
az network nic list --resource-group azure-59806175-60147103-azure-rg
--query "[].{NIC: name, VM: virtualMachine.id}"
```

Wiederholen Sie bei HA-Paar-Implementierungen die Schritte für den Partner-Node.

Schritt 2: Erstellen Sie einen neuen IPspace, Broadcast-Domain und Intercluster LIF für die neue NIC

Durch einen separaten IPspace für Intercluster-LIFs wird die logische Trennung zwischen den Netzwerkfunktionen für die Replizierung zwischen Clustern ermöglicht.

Verwenden Sie die ONTAP-CLI für die folgenden Schritte.

Schritte

1. Erstellen Sie den neuen IPspace (New_ipspace).

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. Erstellen Sie eine Broadcast-Domain auf dem neuen IPspace (New_ipspace) und fügen Sie den nic-New-Port hinzu.

```
dest::> network port show
```

3. Für Systeme mit einem einzigen Node lautet der neu hinzugefügte Port *e0b*. Für HA-Paar-Implementierungen mit verwalteten Datenträgern lautet der neu hinzugefügte Port *e0d*. Für HA-Paar-Implementierungen mit Page Blobs ist der neu hinzugefügte Port *e0e*. Verwenden Sie den Node-Namen und nicht den VM-Namen. Suchen Sie den Node-Namen, indem Sie ausführen `node show`.

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. Erstellen Sie eine Intercluster LIF auf der neuen Broadcast-Domain (New_bd) und auf der neuen NIC (nic-New).

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. Überprüfung der Erstellung der neuen Intercluster LIF

```
dest::> net int show
```

Wiederholen Sie bei HA-Paar-Implementierungen die Schritte für den Partner-Node.

Schritt 3: Überprüfen Sie Cluster-Peering zwischen den Quell- und Zielsystemen

Dieser Abschnitt enthält Anweisungen zur Überprüfung von Peering zwischen Quell- und Zielsystemen.

Verwenden Sie die ONTAP-CLI für die folgenden Schritte.

Schritte

1. Vergewissern Sie sich, dass die Intercluster LIF des Ziel-Clusters die Intercluster LIF des Quell-Clusters anpingen kann. Da der Ziel-Cluster diesen Befehl ausführt, ist die Ziel-IP-Adresse die Intercluster LIF IP-Adresse auf der Quelle.

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. Vergewissern Sie sich, dass die Intercluster LIF des Quell-Clusters die Intercluster LIF des Ziel-Clusters anpingen kann. Das Ziel ist die IP-Adresse der neuen NIC, die auf dem Ziel erstellt wurde.

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

Wiederholen Sie bei HA-Paar-Implementierungen die Schritte für den Partner-Node.

Schritt 4: SVM-Peering zwischen Quell- und Zielsystem erstellen

Dieser Abschnitt enthält Anweisungen zum Erstellen von SVM-Peering zwischen dem Quell- und Zielsystem.

Verwenden Sie die ONTAP-CLI für die folgenden Schritte.

Schritte

1. Erstellen Sie Cluster-Peering auf dem Ziel mithilfe der Intercluster-Quell-IP-Adresse des `-peer-addrs`. Bei HA-Paaren sollten Sie die LIF-IP-Quelladresse für beide Nodes als auflisten `-peer-addrs`.

```
dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace
<new_ipspace>
```

2. Geben Sie die Passphrase ein und bestätigen Sie sie.
3. Erstellen Sie Cluster-Peering auf der Quelle mithilfe der LIF-IP-Adresse des Ziel-Clusters als `peer-addrs`. Bei HA-Paaren müssen die Ziel-Intercluster-LIF-IP-Adresse für beide Nodes als auflisten `-peer-addrs`.

```
src::> cluster peer create -peer-addrs <10.161.189.18>
```

4. Geben Sie die Passphrase ein und bestätigen Sie sie.
5. Prüfen Sie, ob das Cluster Peering ist.

```
src::> cluster peer show
```

Erfolgreiches Peering zeigt **verfügbar** im Verfügbarkeitsfeld an.

6. SVM-Peering auf dem Ziel erstellen. Quell- und Ziel-SVMs sollten Daten-SVMs sein.

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. SVM-Peering akzeptieren.

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. Prüfen Sie, ob die SVM einen Spitzeneinschlag hat.

```
dest::> vserver peer show
```

Peer-Status wird angezeigt **`peered`** Und Peering Anwendungen zeigt **`snapmirror`**.

Schritt 5: Erstellen einer SnapMirror Replizierungsbeziehung zwischen dem Quell- und Zielsystem

Dieser Abschnitt enthält Anweisungen zum Erstellen einer SnapMirror Replizierungsbeziehung zwischen dem Quell- und Zielsystem.

Um eine vorhandene SnapMirror Replizierungsbeziehung zu verschieben, müssen Sie zuerst die bestehende SnapMirror Replizierungsbeziehung trennen, bevor Sie eine neue SnapMirror Replizierungsbeziehung erstellen.

Verwenden Sie die ONTAP-CLI für die folgenden Schritte.

Schritte

1. Erstellung eines geschützten Volumes auf der Ziel-SVM

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. Erstellen Sie die SnapMirror Replizierungsbeziehung auf dem Ziel, das die SnapMirror Richtlinie und einen Zeitplan für die Replizierung umfasst.

```
dest::> snapmirror create -source-path src_svm:src_vol  -destination
-path  dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. Initialisieren Sie die SnapMirror Replizierungsbeziehung auf dem Ziel.

```
dest::> snapmirror initialize -destination-path  <dest_svm:new_dest_vol>
```

4. Überprüfen Sie in der ONTAP CLI den SnapMirror Beziehungsstatus, indem Sie den folgenden Befehl ausführen:

```
dest::> snapmirror show
```

   Der Beziehungsstatus lautet `Snapmirrored` Und die Gesundheit der Beziehung ist `true`.

5. Optional: Führen Sie in der ONTAP-CLI den folgenden Befehl aus, um den Aktionsverlauf für die SnapMirror Beziehung anzuzeigen.

```
dest::> snapmirror show-history
```

Optional können Sie die Quell- und Ziel-Volumes mounten, eine Datei auf die Quelle schreiben und überprüfen, ob das Volume auf das Ziel repliziert wird.

Google Cloud-Administration

Ändern Sie den Google Cloud-Maschinentyp für Cloud Volumes ONTAP

Sie können zwischen verschiedenen Maschinentypen wählen, wenn Sie Cloud Volumes ONTAP in Google Cloud starten. 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 Maschinentyps kann sich auf die Google Cloud-Servicegebühren auswirken.
- Der Vorgang startet Cloud Volumes ONTAP neu.

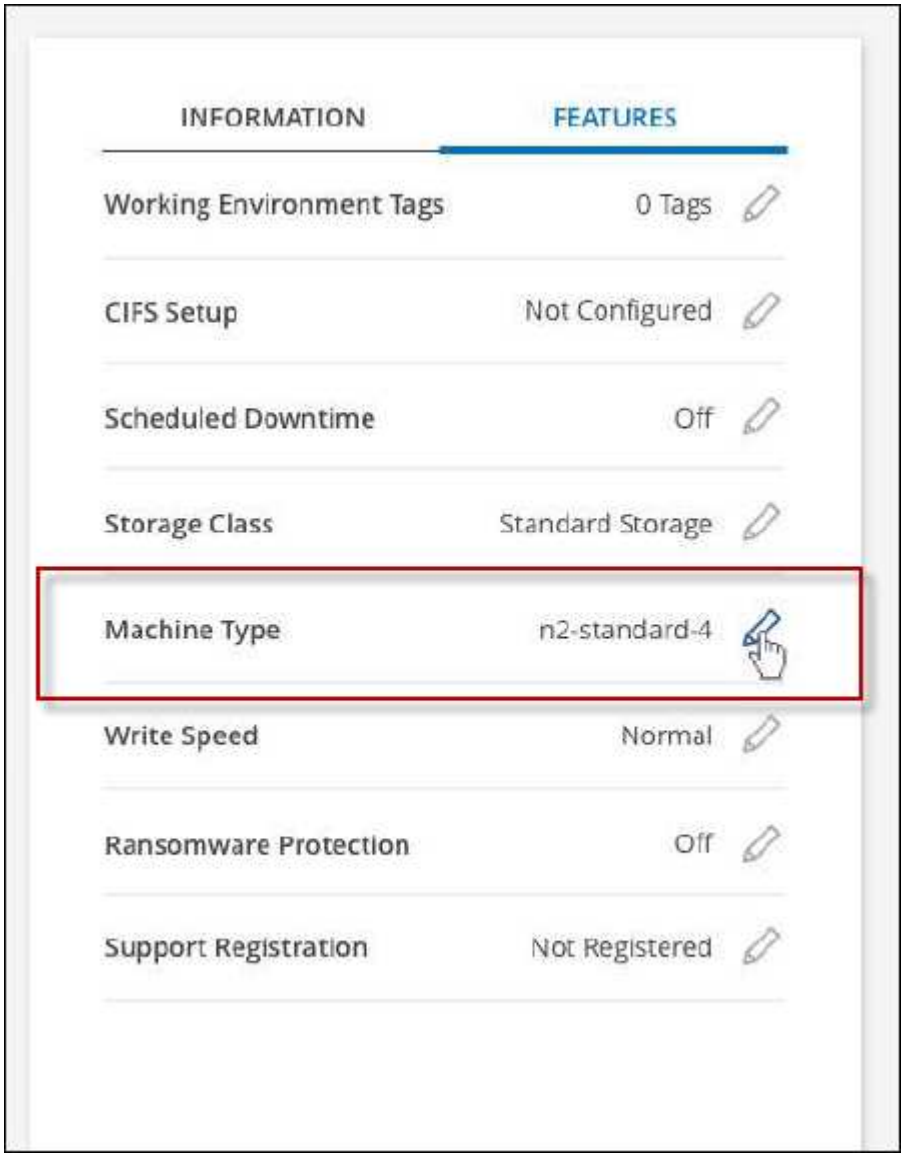
  Bei Systemen mit einem Node wird die I/O unterbrochen.

  Bei HA-Paaren ist die Änderung unterbrechungsfrei. Ha-Paare stellen weiterhin Daten bereit.

BlueXP ändert den Knoten nacheinander 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. Wählen Sie auf der Seite Arbeitsfläche die Arbeitsumgebung aus.
2. Klicken Sie auf der Registerkarte Übersicht auf das Bedienfeld Funktionen und dann auf das Bleistiftsymbol neben **Maschinentyp**.



   a. Wenn Sie eine Node-basierte PAYGO-Lizenz verwenden, können Sie optional eine andere Lizenz und einen anderen Maschinentyp auswählen, indem Sie auf das Bleistiftsymbol neben **Lizenztyp** klicken.
3. Wählen Sie einen Maschinentyp, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Auswirkungen der Änderung verstehen, und klicken Sie dann auf **Ändern**.

Ergebnis

Cloud Volumes ONTAP wird mit der neuen Konfiguration neu gestartet.

Cloud Volumes ONTAP mit der erweiterten Ansicht verwalten

Wenn Sie erweitertes Management von Cloud Volumes ONTAP durchführen möchten, können Sie dies mit ONTAP System Manager durchführen. Dabei handelt es sich um eine Managementoberfläche, die einem ONTAP System bereitgestellt wird. Die System Manager Schnittstelle ist direkt in BlueXP integriert, sodass Sie BlueXP nicht für erweitertes Management verlassen müssen.

Funktionen

Die erweiterte Ansicht in BlueXP bietet Ihnen zusätzliche Verwaltungsfunktionen:

- Erweitertes Storage-Management

  Managen von Konsistenzgruppen, Shares, qtrees, Quotas und Storage-VMs

- Netzwerkmanagement

  Managen Sie IPspaces, Netzwerkschnittstellen, Portsätze und ethernet-Ports.

- Ereignisse und Jobs

  Anzeige von Ereignisprotokollen, Systemwarnungen, Jobs und Prüfprotokollen.

- Erweiterte Datensicherung

  Sicherung von Storage VMs, LUNs und Konsistenzgruppen

- Host-Management

  Richten Sie SAN-Initiatorgruppen und NFS-Clients ein.

Unterstützte Konfigurationen

Das erweiterte Management wird über System Manager mit Cloud Volumes ONTAP 9.10.0 und höher in Standard-Cloud-Regionen unterstützt.

Die Integration von System Manager wird in GovCloud Regionen oder Regionen ohne Outbound-Internetzugang nicht unterstützt.

Einschränkungen

Einige Funktionen, die in der System Manager-Oberfläche angezeigt werden, werden bei Cloud Volumes ONTAP nicht unterstützt:

- BlueXP Tiering

  Der BlueXP Tiering Service wird von Cloud Volumes ONTAP nicht unterstützt. Bei der Erstellung von Volumes muss das Tiering von Daten in Objektspeicher direkt aus der Standardansicht von BlueXP eingerichtet werden.

- Tiers

  Das aggregierte Management (einschließlich lokaler Tiers und Cloud Tiers) wird von System Manager nicht

unterstützt. Sie müssen Aggregate direkt über die Standardansicht von BlueXP managen.

- Firmware-Upgrades

  Automatische Firmware-Updates von der Seite **Cluster > Einstellungen** werden von Cloud Volumes ONTAP nicht unterstützt.

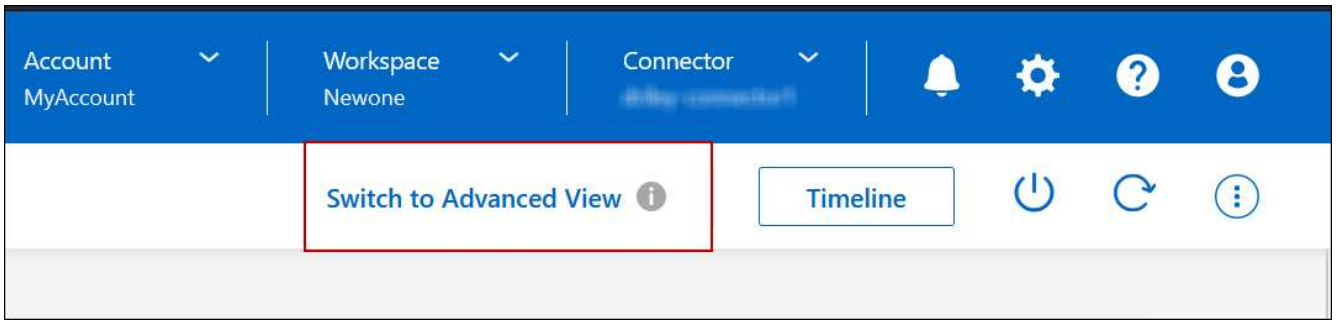
Darüber hinaus wird die rollenbasierte Zugriffssteuerung von System Manager nicht unterstützt.

Erste Schritte

Öffnen Sie eine Cloud Volumes ONTAP Arbeitsumgebung, und klicken Sie auf die Option Erweiterte Ansicht.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Doppelklicken Sie auf der Seite Arbeitsfläche auf den Namen eines Cloud Volumes ONTAP-Systems.
3. Klicken Sie oben rechts auf **zur erweiterten Ansicht wechseln**.



4. Wenn die Bestätigungsmeldung angezeigt wird, lesen Sie sie durch und klicken Sie auf **Schließen**.
5. Verwenden Sie System Manager zum Verwalten von Cloud Volumes ONTAP.
6. Klicken Sie bei Bedarf auf **zur Standardansicht wechseln**, um zur Standardverwaltung über BlueXP zurückzukehren.

Hilfe bei der Verwendung von System Manager

Wenn Sie Hilfe bei der Verwendung von System Manager mit Cloud Volumes ONTAP benötigen, finden Sie unter "ONTAP-Dokumentation" Schritt-für-Schritt-Anleitungen. Hier sind einige Links, die helfen könnten:

- "Volume- und LUN-Management"
- "Netzwerkmanagement"
- "Datensicherung"

Verwalten Sie Cloud Volumes ONTAP über die CLI

Die Cloud Volumes ONTAP CLI ermöglicht die Ausführung aller administrativen Befehle. Sie eignet sich für erweiterte Aufgaben oder bei komfortableren Verwendung der CLI. 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. Beispielsweise müssen Sie SSH von einem Jump-Host in Ihrem Cloud-Provider-Netzwerk aus starten.

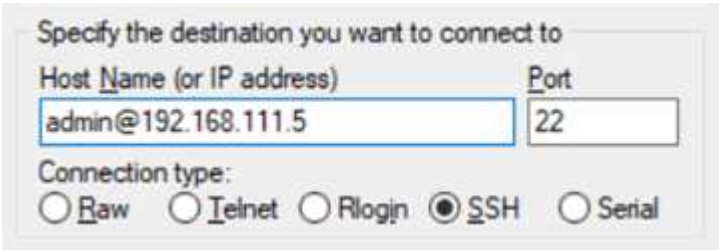
> Wenn Cloud Volumes ONTAP HA in mehreren AZS implementiert wird, verwenden sie eine Floating-IP-Adresse für die Cluster-Management-Schnittstelle, was bedeutet, dass externes Routing nicht verfügbar ist. Sie müssen eine Verbindung von einem Host herstellen, der Teil derselben Routingdomäne ist.

Schritte

1. Geben Sie in BlueXP die IP-Adresse der Cluster-Managementoberfläche an:
   a. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
   b. Wählen Sie auf der Seite Arbeitsfläche das Cloud Volumes ONTAP-System aus.
   c. 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::>
```

Systemzustand und Ereignisse

AutoSupport-Einrichtung überprüfen

AutoSupport überwacht proaktiv den Zustand Ihres Systems und sendet Meldungen an den technischen Support von NetApp. Standardmäßig ist AutoSupport auf jedem Node aktiviert, um Meldungen mithilfe des HTTPS-Transportprotokolls an den technischen Support zu senden. Überprüfen Sie am besten, ob AutoSupport diese Meldungen senden kann.

Der einzige erforderliche Konfigurationsschritt besteht darin, sicherzustellen, dass Cloud Volumes ONTAP über eine ausgehende Internetverbindung verfügt. Details finden Sie in den Netzwerkanforderungen Ihres Cloud-

Providers.

AutoSupport-Anforderungen erfüllt

Cloud Volumes ONTAP Nodes benötigen Outbound-Internetzugang für NetApp AutoSupport, der den Zustand Ihres Systems proaktiv überwacht und Meldungen an den technischen Support von NetApp sendet.

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

Wenn keine ausgehende Internetverbindung zum Senden von AutoSupport-Nachrichten verfügbar ist, konfiguriert BlueXP Ihre Cloud Volumes ONTAP-Systeme automatisch so, dass der Connector als Proxy-Server verwendet wird. Die einzige Anforderung besteht darin, sicherzustellen, dass die Sicherheitsgruppe des Connectors *eingehende* -Verbindungen über Port 3128 zulässt. Nach der Bereitstellung des Connectors müssen Sie diesen Port öffnen.

Wenn Sie strenge ausgehende Regeln für Cloud Volumes ONTAP definiert haben, müssen Sie auch sicherstellen, dass die Cloud Volumes ONTAP-Sicherheitsgruppe *Outbound*-Verbindungen über Port 3128 zulässt.

Nachdem Sie bestätigt haben, dass der ausgehende Internetzugang verfügbar ist, können Sie AutoSupport testen, um sicherzustellen, dass er Nachrichten senden kann. Anweisungen finden Sie unter "ONTAP Dokumentation: Einrichten von AutoSupport".

Fehler bei der AutoSupport Konfiguration beheben

Wenn keine ausgehende Verbindung verfügbar ist und BlueXP Ihr Cloud Volumes ONTAP-System nicht so konfigurieren kann, dass der Connector als Proxy-Server verwendet wird, erhalten Sie eine Benachrichtigung von BlueXP mit dem Titel „<Working Environment Name> kann keine AutoSupport-Nachrichten senden.“

Sie erhalten diese Nachricht wahrscheinlich aufgrund von Netzwerkproblemen.

Befolgen Sie diese Schritte, um dieses Problem zu lösen.

Schritte

1. SSH dem Cloud Volumes ONTAP System, sodass Sie das System von der CLI verwalten können.

   "Informieren Sie sich über SSH to Cloud Volumes ONTAP".

2. Anzeigen des detaillierten Status des AutoSupport-Subsystems:

   ```
   autosupport check show-details
   ```

   Die Antwort sollte wie folgt lauten:

```
    Category: smtp
          Component: mail-server
             Status: failed
             Detail: SMTP connectivity check failed for destination:
                     mailhost. Error: Could not resolve host -
'mailhost'
            Corrective Action: Check the hostname of the SMTP server

    Category: http-https
        Component: http-put-destination
            Status: ok
            Detail: Successfully connected to:
                    <https://support.netapp.com/put/AsupPut/>.

          Component: http-post-destination
             Status: ok
             Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

    Category: on-demand
          Component: ondemand-server
             Status: ok
             Detail: Successfully connected to:
                     https://support.netapp.com/aods/asupmessage.

    Category: configuration
            Component: configuration
                Status: ok
                Detail: No configuration issues found.
    5 entries were displayed.
```

Wenn der Status der Kategorie http-https „ok“ lautet, bedeutet dies, dass AutoSupport richtig konfiguriert ist und Meldungen gesendet werden können.

3. Wenn der Status nicht ok ist, überprüfen Sie die Proxy-URL für jeden Cloud Volumes ONTAP-Knoten:

   ```
   autosupport show -fields proxy-url
   ```

4. Wenn der Proxy-URL-Parameter leer ist, konfigurieren Sie Cloud Volumes ONTAP für die Verwendung des Connectors als Proxy:

   ```
   autosupport modify -proxy-url http://<connector private ip>:3128
   ```

5. Überprüfen Sie den AutoSupport-Status erneut:

   ```
   autosupport check show-details
   ```

6. Wenn der Status noch nicht erfolgreich ist, überprüfen Sie, ob Verbindungen zwischen Cloud Volumes ONTAP und dem Connector über Port 3128 bestehen.
7. Wenn die Status-ID nach der Überprüfung der Verbindung weiterhin fehlgeschlagen ist, SSH zum Connector.

   "Erfahren Sie mehr über die Verbindung zur Linux-VM für den Connector"

8. Gehen Sie zu `/opt/application/netapp/cloudmanager/docker_occm/data/`
9. Öffnen Sie die Proxy-Konfigurationsdatei `squid.conf`

   Die grundlegende Struktur der Datei ist wie folgt:

   ```
   http_port 3128
   acl localnet src 172.31.0.0/16
   acl azure_aws_metadata dst 169.254.169.254

   http_access allow localnet
   http_access deny azure_aws_metadata
   http_access allow localhost
   http_access deny all
   ```

   Der localnet src-Wert ist das CIDR des Cloud Volumes ONTAP-Systems.

10. Wenn sich der CIDR-Block des Cloud Volumes ONTAP-Systems nicht im in der Datei angegebenen Bereich befindet, aktualisieren Sie entweder den Wert oder fügen Sie einen neuen Eintrag wie folgt hinzu:

    ```
    acl cvonet src <cidr>
    ```

    Wenn Sie diesen neuen Eintrag hinzufügen, vergessen Sie nicht, auch einen Eintrag hinzufügen zu lassen:

    ```
    http_access allow cvonet
    ```

    Hier ein Beispiel:

    ```
    http_port 3128
    acl localnet src 172.31.0.0/16
    acl cvonet src 172.33.0.0/16
    acl azure_aws_metadata dst 169.254.169.254

    http_access allow localnet
    http_access allow cvonet
    http_access deny azure_aws_metadata
    http_access allow localhost
    http_access deny all
    ```

11. Starten Sie nach dem Bearbeiten der config-Datei den Proxy-Container wie sudo neu:

```
docker restart squid
```

12. Gehen Sie zurück zur Cloud Volumes ONTAP CLI und überprüfen Sie, ob Cloud Volumes ONTAP AutoSupport Meldungen senden kann:

```
autosupport check show-details
```

EMS konfigurieren

Das Event Management System (EMS) sammelt und zeigt Informationen zu Ereignissen auf ONTAP Systemen an. 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 finden Sie unter "ONTAP Dokumentation: EMS-Konfigurationsübersicht".

Konzepte

Cloud Volumes ONTAP Lizenzierung

Für Cloud Volumes ONTAP sind verschiedene Lizenzierungsoptionen verfügbar. Jede Option ermöglicht Ihnen, ein Nutzungsmodell auszuwählen, das Ihren Anforderungen entspricht.

Übersicht über die Lizenzierung

Die folgenden Lizenzierungsoptionen stehen für Neukunden zur Verfügung.

Kapazitätsbasierte Lizenzierung
: Bezahlen Sie für mehrere Cloud Volumes ONTAP Systeme Ihres NetApp Kontos durch bereitgestellte Kapazität. Mit der Möglichkeit, zusätzliche Cloud-Datenservices zu erwerben

Keystone Abonnement
: Ein abonnementbasierter Service mit Bezahlung nach Bedarf für eine nahtlose Hybrid Cloud-Nutzung für HA-Paare

Das vorherige Node-Lizenzmodell bleibt bestehenden Kunden, die bereits eine Lizenz erworben haben oder über ein aktives Marketplace-Abonnement verfügen, verfügbar.

In den folgenden Abschnitten werden die einzelnen Optionen näher beschrieben.

Ohne Lizenz ist kein Support für die Nutzung lizenzierter Funktionen verfügbar.

Kapazitätsbasierte Lizenzierung

Mit kapazitätsbasierten Lizenzpaketen können Sie für Cloud Volumes ONTAP pro tib Kapazität bezahlen. Die Lizenz ist mit Ihrem NetApp Konto verknüpft und ermöglicht es Ihnen, mehrere Systeme gegen die Lizenz aufzuladen, solange über die Lizenz genügend Kapazität verfügbar ist.

Beispielsweise könnten Sie eine einzelne 20-tib-Lizenz erwerben, vier Cloud Volumes ONTAP Systeme implementieren und jedem System dann ein 5-tib-Volume zuweisen, also insgesamt 20 tib. Die Kapazität ist für die Volumes auf jedem in diesem Konto implementierten Cloud Volumes ONTAP System verfügbar.

Kapazitätsbasierte Lizenzierung ist in Form eines *package* erhältlich. Bei der Implementierung eines Cloud Volumes ONTAP Systems haben Sie die Möglichkeit, je nach Ihren geschäftlichen Anforderungen aus mehreren Lizenzierungspaketen auszuwählen.

Während die tatsächliche Nutzung und Nutzungsmessung für die in BlueXP gemanagten Produkte und Services immer in gib und tib berechnet werden, werden die Begriffe GB/gib und TB/tib synonym verwendet. Dies spiegelt sich in den Angeboten, Preisangeboten, Listenbeschreibungen und anderen Begleitdokumenten des Cloud Marketplace wider.

Pakete

Die folgenden kapazitätsbasierten Pakete stehen für Cloud Volumes ONTAP zur Verfügung.

Eine Liste der unterstützten VM-Typen mit den folgenden kapazitätsbasierten Paketen finden Sie unter:

- "Unterstützte Konfigurationen in Azure"
- "Unterstützte Konfigurationen in Google Cloud"

Freimium

Bietet alle Cloud Volumes ONTAP-Funktionen kostenlos von NetApp an (Gebühren für Cloud-Provider gelten noch).

- Lizenz oder Vertrag sind nicht erforderlich.
- Support von NetApp ist nicht inbegriffen.
- Sie sind auf 500 gib der bereitgestellten Kapazität pro Cloud Volumes ONTAP System begrenzt.
- Sie können bis zu 10 Cloud Volumes ONTAP Systeme mit Freemium-Angebot pro NetApp Konto bei jedem Cloud-Provider nutzen.
- Wenn die bereitgestellte Kapazität für ein Cloud Volumes ONTAP-System 500 gib überschreitet, konvertiert BlueXP das System in das Essentials-Paket.

  Sobald ein System in das Essentials-Paket konvertiert wird, wird das verwendet Mindestgebühr Gilt.

  Alle anderen Systeme mit einer bereitgestellten Kapazität von weniger als 500 gib bleiben auf Freemium (sofern sie mit dem Freemium-Angebot bereitgestellt wurden).

Optimiert

Sie bezahlen für bereitgestellte Kapazität und I/O-Vorgänge separat.

- Cloud Volumes ONTAP Single Node oder HA
- Der Ladevorgang basiert auf zwei Kostenkomponenten: Speicher und Nutzung (I/O).

  Es fallen keine I/O-Kosten für Datenreplizierung (SnapMirror), Backups (SnapVault) oder NDMP an.

- Verfügbar im Azure Marketplace als Pay-as-you-go-Angebot oder als Jahresvertrag
- Verfügbar im Google Cloud Marketplace als Pay-as-you-go-Angebot oder als Jahresvertrag
- Fügen Sie die Cloud-Datenservices von NetApp zu zusätzlichen Kosten hinzu

Essentials

Bezahlung nach Kapazität für Cloud Volumes ONTAP in verschiedenen Konfigurationen

- Wählen Sie Ihre Cloud Volumes ONTAP Konfiguration:
  - Ein Single Node oder HA-System
  - Datei- und Block-Storage oder sekundäre Daten für die Disaster Recovery (DR)
- Fügen Sie die Cloud-Datenservices von NetApp zu zusätzlichen Kosten hinzu

Professionell

Sie bezahlen nach Kapazität für jede Art von Cloud Volumes ONTAP-Konfiguration mit unbegrenzten Backups.

- Ermöglicht die Lizenzierung jeder Cloud Volumes ONTAP Konfiguration

  Single Node oder HA, berechnet für primäre und sekundäre Volumes dieselbe Kapazität

- Umfasst unbegrenzte Volume-Backups mit BlueXP Backup und Recovery, aber nur für Cloud Volumes ONTAP Systeme, die das Professional Paket verwenden.

> Für das Backup und Recovery von BlueXP ist ein PAYGO-Abonnement erforderlich, allerdings sind für die Nutzung dieses Services keine Gebühren anfallen. Weitere Informationen zum Einrichten der Lizenzierung für Backup und Recovery von BlueXP finden Sie unter "Lizenzierung für Backup und Recovery von BlueXP einrichten".

- Fügen Sie die Cloud-Datenservices von NetApp zu zusätzlichen Kosten hinzu

Edge-Cache

Ermöglicht die Lizenzierung für Cloud Volumes Edge Cache.

- Dieselben Funktionen wie das Professional-Paket mit Business Continuity und Datenschutz für ein verteiltes Unternehmen
- Intelligentes Edge-Caching mithilfe einer Windows VM mit geringem Platzbedarf an jedem Standort
- Ein Edge-Node mit jeweils 3 TIBS Kapazität erworben
- Verfügbar im Azure Marketplace als Pay-as-you-go-Angebot oder als Jahresvertrag
- Verfügbar im Google Cloud Marketplace als Pay-as-you-go-Angebot oder als Jahresvertrag

"Erfahren Sie mehr darüber, wie Cloud Volumes Edge Cache Sie dabei unterstützen kann"

Verbrauchsmodelle

Kapazitätspakete erhalten Sie bei den folgenden Nutzungsmodellen:

- **BYOL**: Eine von NetApp erworbene Lizenz zur Implementierung von Cloud Volumes ONTAP bei einem beliebigen Cloud-Provider.

+ beachten Sie, dass die optimierten Pakete und Edge Cache nicht mit BYOL verfügbar sind.

- **PAYGO**: Ein stündliches Abonnement über den Markt Ihres Cloud-Providers.
- **Jahr**: Ein Jahresvertrag über den Markt Ihres Cloud-Providers.

Beachten Sie Folgendes:

- Wenn Sie eine Lizenz bei NetApp (BYOL) erwerben, müssen Sie auch das PAYGO-Angebot über den Markt Ihres Cloud-Providers abonnieren.

  Ihre Lizenz wird immer zuerst berechnet, aber in diesen Fällen wird Ihnen der Stundensatz auf dem Markt berechnet:

  - Wenn Sie Ihre lizenzierte Kapazität überschreiten
  - Wenn die Laufzeit Ihrer Lizenz abläuft
- Wenn Sie über einen jährlichen Vertrag eines Marktes verfügen, werden _alle Cloud Volumes ONTAP Systeme, die Sie implementieren, mit diesem Vertrag in Rechnung gestellt. Es ist nicht möglich, einen jährlichen Marktvertrag mit BYOL zu kombinieren.
- In China werden nur Single-Node-Systeme mit BYOL unterstützt.

Ändern von Paketen

Nach der Bereitstellung können Sie das Paket für ein Cloud Volumes ONTAP System ändern, das kapazitätsbasierte Lizenzierung verwendet. Wenn Sie beispielsweise ein Cloud Volumes ONTAP-System mit dem Essentials-Paket bereitgestellt haben, können Sie es in das Professional-Paket ändern, wenn sich Ihre Geschäftsanforderungen ändern.

"Erfahren Sie, wie Sie Lademethoden ändern können".

Preisgestaltung

Weitere Informationen zur Preisgestaltung finden Sie unter "NetApp BlueXP Website".

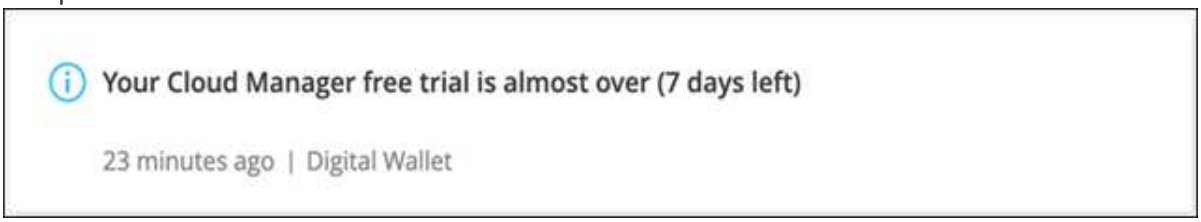
Testversionen

Eine kostenlose 30-Tage-Testversion steht Ihnen über das Pay-as-you-go-Abonnement im Markt Ihres Cloud-Providers zur Verfügung. Die kostenlose Testversion beinhaltet Backup und Recovery von Cloud Volumes ONTAP und BlueXP. Die Testversion beginnt, wenn Sie das Angebot auf dem Markt abonnieren.

Es gibt keine Instanz- oder Kapazitätsbeschränkungen. Sie können Cloud Volumes ONTAP Systeme beliebig viele bereitstellen und so viel Kapazität wie nötig zuweisen, wobei 30 Tage lang kostenlos zur Verfügung stehen. Die kostenlose Testversion wird nach 30 Tagen automatisch in ein kostenpflichtiges stündliches Abonnement konvertiert.

Für Cloud Volumes ONTAP fallen keine Lizenzgebühren für Software auf Stundenbasis an, allerdings fallen bei Ihrem Cloud-Provider nach wie vor Gebühren für die Infrastruktur an.

Sie erhalten in BlueXP eine Benachrichtigung, wenn die kostenlose Testversion beginnt, wenn noch 7 Tage Zeit bleibt und 1 Tag übrig ist.
Beispiel:



Unterstützte Konfigurationen

Kapazitätsbasierte Lizenzpakete sind mit Cloud Volumes ONTAP 9.7 und höher verfügbar.

Kapazitätsgrenze

Bei diesem Lizenzmodell unterstützt jedes einzelne Cloud Volumes ONTAP System bis zu 2 PiB Kapazität durch Festplatten und Tiering zu Objekt-Storage.

Bei der Lizenz selbst gibt es keine maximale Kapazitätsgrenze.

Maximale Anzahl an Systemen

Bei der kapazitätsbasierten Lizenzierung ist die maximale Anzahl von Cloud Volumes ONTAP Systemen auf 20 pro NetApp Konto begrenzt. Ein *System* ist ein Cloud Volumes ONTAP HA-Paar, ein Cloud Volumes ONTAP Single Node System oder zusätzliche, von Ihnen erstellte Storage VMs. Die standardmäßige Storage-VM wird nicht mit dem Grenzwert gezählt. Diese Begrenzung gilt für alle Lizenzmodelle.

Nehmen wir beispielsweise an, Sie haben drei Arbeitsumgebungen:

- Ein Cloud Volumes ONTAP-System mit einem einzelnen Node mit einer Storage-VM (dies ist die Standard-Storage-VM, die beim Implementieren von Cloud Volumes ONTAP erstellt wird)

  Diese Arbeitsumgebung zählt als ein System.

- Ein Single Node Cloud Volumes ONTAP System mit zwei Storage-VMs (die Standard-Storage-VM plus eine zusätzliche, von Ihnen erstellte Storage-VM)

  Diese Arbeitsumgebung zählt als zwei Systeme: Eines für das Single-Node-System und eines für die zusätzliche Storage-VM.

- Ein Cloud Volumes ONTAP HA-Paar mit drei Storage VMs (der Standard-Storage-VM plus zwei zusätzlichen Storage-VMs, die Sie erstellt haben)

  Diese Arbeitsumgebung zählt als drei Systeme: Eines für das HA-Paar und zwei für die zusätzlichen Storage VMs.

Das sind insgesamt sechs Systeme. Sie hätten dann Platz für weitere 14 Systeme in Ihrem Konto.

Wenn eine große Implementierung mehr als 20 Systeme erfordert, wenden Sie sich an Ihren Ansprechpartner oder Ihr Vertriebsteam.

"Weitere Informationen über NetApp Accounts".

Hinweise zum Laden

Die folgenden Details helfen Ihnen dabei, die Funktionsweise der Verrechnung mit kapazitätsbasierter Lizenzierung zu verstehen.

Mindestgebühr

Es gibt eine Mindestgebühr von 4 tib für jede Daten-Serving-Storage-VM mit mindestens einem primären (Lese-/Schreibzugriff) Volume. Wenn die Summe der primären Volumes weniger als 4 tib beträgt, wendet BlueXP die Mindestgebühr von 4 tib auf diese Storage-VM an.

Wenn Sie noch keine Volumes bereitgestellt haben, gilt die Mindestgebühr nicht.

Für das Essentials-Paket gilt die Mindestkapazitätsgebühr von 4 tib nicht für Storage-VMs, die nur sekundäre Volumes (Datensicherung) enthalten. Wenn Sie beispielsweise eine Storage-VM mit 1 tib sekundären Daten haben, werden Sie nur für die 1 tib Daten berechnet. Bei allen anderen nicht-Essentials-Pakettypen (optimiert, Professional und Edge Cache) gilt unabhängig vom Volume-Typ die Mindestkapazitätsladung von 4 tib.

Überalt

Wenn Sie Ihre BYOL-Kapazität überschreiten oder Ihre Lizenz abgelaufen ist, werden Ihnen auf Basis Ihres Marktabonnements für Überkapazitäten zum Stundensatz berechnet.

Essentials-Paket

Bei dem Essentials-Paket werden die Bereitstellungstyp (HA oder Single Node) und der Volume-Typ (primär oder sekundär) abgerechnet. Die Preise von „hoch“ bis „niedrig“ werden in der folgenden Reihenfolge angezeigt: *Essentials Primary HA*, *Essentials Primary Single Node*, *Essentials Secondary HA* und *Essentials Secondary Single Node*. Wenn Sie einen Marketplace-Vertrag erwerben oder ein privates Angebot annehmen,

sind die Kapazitätsgebühren für jede Bereitstellung oder jeden Volume-Typ gleich.

BYOL

Wenn Sie eine Essentials-Lizenz von NetApp (BYOL) erworben haben und die lizenzierte Kapazität für diese Implementierung und diesen Volume-Typ überschreiten, berechnet das Digital Wallet von BlueXP mehr als eine günstigere Essentials-Lizenz (sofern vorhanden). Dies geschieht, weil wir zuerst die verfügbare Kapazität nutzen, die Sie bereits als Prepaid-Kapazität gekauft haben, bevor wir die Rechnung gegen den Markt berechnen. Wenn mit Ihrer BYOL-Lizenz keine verfügbare Kapazität verfügbar ist, wird die überschrittene Kapazität zu dem jeweiligen On-Demand-Stundensatz (PAYGO) in Rechnung gestellt und rechnet dann mit Kosten für Ihre monatliche Rechnung.

Hier ein Beispiel Nehmen wir an, Sie haben die folgenden Lizenzen für das Essentials-Paket:

- Eine 500 tib *Essentials sekundäre HA* Lizenz, die 500 tib an engagierter Kapazität hat
- Eine 500 tib *Essentials Single Node*-Lizenz, die nur über 100 tib Speicherkapazität verfügt

Weitere 50 tib werden auf einem HA-Paar mit sekundären Volumes bereitgestellt. Das Digital Wallet von BlueXP berechnet nicht den 50 tib großen PAYGO-Service für die *Essentials Single Node* Lizenz, sondern den 50 tib zusätzlichen Aufpreis. Diese Lizenz ist teurer als *Essentials Secondary HA*, aber sie nutzt eine Lizenz, die Sie bereits erworben haben, und es werden keine Kosten zu Ihrer monatlichen Rechnung hinzugefügt.

In der Digital Wallet von BlueXP werden die 50 tib Daten mit der *Essentials Single Node* Lizenz verrechnet angezeigt.

Hier ein weiteres Beispiel. Nehmen wir an, Sie haben die folgenden Lizenzen für das Essentials-Paket:

- Eine 500 tib *Essentials sekundäre HA* Lizenz, die 500 tib an engagierter Kapazität hat
- Eine 500 tib *Essentials Single Node*-Lizenz, die nur über 100 tib Speicherkapazität verfügt

Weitere 100 tib werden auf einem HA-Paar mit primären Volumes bereitgestellt. Für die erworbene Lizenz ist keine *Essentials Primary HA* gebuchte Kapazität vorhanden. Die *Essentials Primary HA*-Lizenz ist höher als die *Essentials Primary Single Node*- und *Essentials Secondary HA*-Lizenzen.

In diesem Beispiel berechnet das Digital Wallet von BlueXP über den Marktpreis für die zusätzlichen 100 tib. Die Mehrkosten werden auf Ihrer monatlichen Rechnung angezeigt.

Marketplace-Verträge oder private Angebote

Wenn Sie eine Essentials-Lizenz im Rahmen eines Marketplace-Vertrags oder eines privaten Angebots erworben haben, gilt die BYOL-Logik nicht, und Sie müssen den genauen Lizenztyp für die Nutzung haben. Der Lizenztyp umfasst den Volume-Typ (primär oder sekundär) und den Bereitstellungstyp (HA oder Single Node).

Angenommen, Sie implementieren eine Cloud Volumes ONTAP Instanz mit der Essentials-Lizenz. Anschließend werden Lese- und Schreib-Volumes (primärer Single Node) und schreibgeschützte Volumes (sekundärer Single Node) bereitgestellt. Ihr Marketplace-Vertrag oder Ihr privates Angebot muss Kapazität für *Essentials Single Node* und *Essentials Secondary Single Node* enthalten, um die bereitgestellte Kapazität abzudecken. Bereitgestellte Kapazität, die nicht Bestandteil Ihres Marketplace-Vertrags oder Ihres privaten Angebots ist, wird zu den On-Demand-Stundensätzen (PAYGO) abgerechnet und addiert Ihre monatliche Rechnung.

Storage-VMs

- Für zusätzliche Storage VMs (SVMs) mit Datenbereitstellung fallen keine zusätzlichen Lizenzkosten an, allerdings entstehen pro Datenservice-SVM mindestens 4 tib.

- Die Kosten für Disaster-Recovery-SVMs werden entsprechend der bereitgestellten Kapazität berechnet.

HA-Paare

Bei HA-Paaren wird die bereitgestellte Kapazität auf einem Node nur in Rechnung gestellt. Sie werden nicht berechnet für Daten, die synchron zum Partner-Node gespiegelt sind.

FlexClone und FlexCache Volumes

- Die von FlexClone Volumes genutzte Kapazität wird nicht berechnet.
- Quell- und Ziel-FlexCache-Volumes gelten als Primärdaten und werden gemäß dem bereitgestellten Speicherplatz berechnet.

Erste Schritte

Erste Schritte mit kapazitätsbasierter Lizenzierung:

- "Lizenzierung für Cloud Volumes ONTAP in AWS einrichten"
- "Lizenzierung für Cloud Volumes ONTAP in Azure einrichten"
- "Lizenzierung für Cloud Volumes ONTAP in Google Cloud einrichten"

Keystone Abonnement

Dieser auf einem Abonnement basierende Pay-as-you-grow-Service bietet eine nahtlose Hybrid-Cloud-Lösung für all jene, die Betriebskosten von Anfang an oder im Leasing bevorzugen.

Die Abrechnung basiert auf der Größe der gebuchten Kapazität für ein oder mehrere Cloud Volumes ONTAP HA-Paare in Ihrer Keystone Subscription.

Die bereitgestellte Kapazität für jedes Volume wird aggregiert und regelmäßig mit der gebuchten Kapazität in Ihrem Keystone Abonnement verglichen. Etwaige Überkapazitäten werden als Burst-Kapazität in Ihrem Keystone Abonnement abgerechnet.

"Erfahren Sie mehr über NetApp Keystone".

Unterstützte Konfigurationen

Keystone Abonnements werden von HA-Paaren unterstützt. Diese Lizenzoption wird derzeit bei Systemen mit einzelnen Nodes nicht unterstützt.

Kapazitätsgrenze

Jedes einzelne Cloud Volumes ONTAP System unterstützt Kapazitäten von bis zu 2 PiB über Festplatten und Tiering zu Objekt-Storage.

Erste Schritte

So starten Sie mit einem Keystone Abonnement:

- "Lizenzierung für Cloud Volumes ONTAP in AWS einrichten"
- "Lizenzierung für Cloud Volumes ONTAP in Azure einrichten"
- "Lizenzierung für Cloud Volumes ONTAP in Google Cloud einrichten"

Node-basierte Lizenzierung

Bei der Node-basierten Lizenzierung handelt es sich um das Lizenzmodell der vorherigen Generation, mit dem Cloud Volumes ONTAP pro Node lizenziert werden können. Dieses Lizenzmodell ist für Neukunden nicht verfügbar und es sind keine kostenlosen Testversionen verfügbar. Das Laden durch Knoten wurde durch die oben beschriebenen Methoden zum Aufladen von Kapazität ersetzt.

Node-basierte Lizenzierung ist weiterhin für Bestandskunden verfügbar:

- Wenn Sie über eine aktive Lizenz verfügen, steht BYOL nur für Lizenzerneuerungen zur Verfügung.
- Wenn Sie über ein aktives Abonnement für den Marktplatz verfügen, können Sie die Gebühren auch weiterhin über dieses Abonnement berechnen.

Lizenzkonvertierungen

Das Konvertieren eines vorhandenen Cloud Volumes ONTAP-Systems in eine andere Lizenzmethode wird nicht unterstützt. Die drei aktuellen Lizenzierungsmethoden sind kapazitätsbasierte Lizenzierung, Keystone Abonnements und Node-basierte Lizenzierung. Beispielsweise kann ein System nicht von der Node-basierten Lizenzierung in die kapazitätsbasierte Lizenzierung konvertiert werden (und umgekehrt).

Wenn Sie auf eine andere Lizenzmethode wechseln möchten, können Sie eine Lizenz erwerben, ein neues Cloud Volumes ONTAP System mit dieser Lizenz implementieren und die Daten anschließend auf dieses neue System replizieren.

Beachten Sie, dass die Konvertierung eines Systems von der PAYGO-Lizenzierung pro Node in eine BYOL-by-Node-Lizenzierung (und umgekehrt) nicht unterstützt wird. Sie müssen ein neues System implementieren und anschließend Daten auf dieses System replizieren. "Wechseln zwischen PAYGO und BYOL".

Storage

Client-Protokolle

Cloud Volumes ONTAP unterstützt die Client-Protokolle iSCSI, NFS, SMB, NVMe-TCP und S3.

ISCSI

ISCSI ist ein Blockprotokoll, das in standardmäßigen Ethernet-Netzwerken ausgeführt werden kann. Die meisten Client-Betriebssysteme bieten einen Software-Initiator, der über einen Standard-Ethernet-Port ausgeführt wird.

NFS

NFS ist das herkömmliche File-Zugriffsprotokoll für UNIX- und LINUX-Systeme. Clients können über die Protokolle NFSv3, NFSv4 und NFSv4.1 auf Dateien in ONTAP Volumes zugreifen. Sie können den Dateizugriff mithilfe von UNIX-Berechtigungen, NTFS-Berechtigungen oder einer Kombination beider Berechtigungen steuern.

Clients können sowohl über NFS- als auch SMB-Protokolle auf dieselben Dateien zugreifen.

SMB

SMB ist das herkömmliche File-Zugriffsprotokoll für Windows-Systeme. Die Clients können über die Protokolle SMB 2.0, SMB 2.1, SMB 3.0 und SMB 3.1.1 auf Dateien in ONTAP Volumes zugreifen. Wie bei NFS werden auch hier verschiedene Berechtigungsstile unterstützt.

S3

Cloud Volumes ONTAP unterstützt S3 als Option für horizontal skalierbaren Storage. Über das S3-Protokoll können Sie den S3-Client-Zugriff auf Objekte konfigurieren, die in einem Bucket in einer Storage-VM (SVM) enthalten sind.

"Funktionsweise von S3-Multi-Protokoll"."Lesen Sie, wie Sie S3-Objekt-Storage-Services in ONTAP konfigurieren und managen".

NVMe-TCP

NVMe-TCP wird für Cloud-Provider unterstützt, wenn Sie Cloud Volumes ONTAP Version 9.12.1 oder höher verwenden. BlueXP bietet keine Managementfunktionen für NVMe-TCP.

Weitere Informationen zum Konfigurieren von NVMe über ONTAP finden Sie unter "Konfigurieren Sie eine Storage-VM für NVMe".

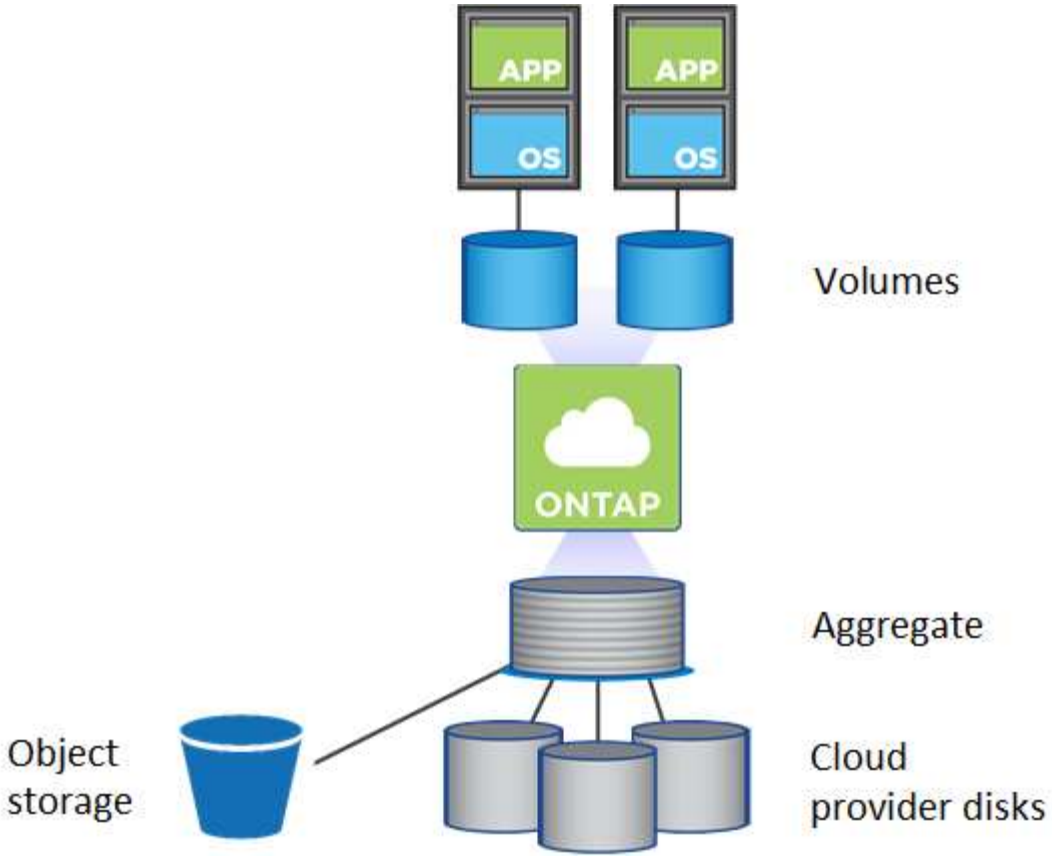
Festplatten und Aggregate

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

Alle Festplatten und Aggregate müssen direkt aus BlueXP 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 BlueXP beispielsweise ein Aggregat mit 500 gib erstellt, beträgt die nutzbare Kapazität 442.94 gib.

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. Wenn Sie aber eine Konfiguration haben, die die Amazon EBS Elastic Volumes Funktion unterstützt, kann ein Aggregat bis zu 8 Festplatten enthalten. "Erfahren Sie mehr über den Support für Elastic Volumes".

Die maximale Festplattengröße beträgt 16 tib.

Der zugrunde liegende EBS-Festplattentyp kann entweder universell einsetzbare SSDs (gp3 oder gp2), bereitgestellte IOPS-SSD (io1) oder durchsatzoptimierte Festplatte (st1) sein. Sie können eine EBS-Festplatte mit Amazon S3 zu koppeln "Verschieben inaktiver Daten in kostengünstigen Objektspeicher".

Bei der Verwendung von durchsatzoptimierten HDDs (st1) wird kein Tiering von Daten zu Objekt-Storage empfohlen.

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 tib.

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

HA-Paare

HA-Paare verwenden zwei Festplattenarten, die eine hohe Performance für I/O-intensive Workloads zu höheren Kosten bieten:

- *Premium Seite Blobs* mit einer maximalen Festplattengröße von 8 tib
- *Gemanagte Festplatten* mit einer maximalen Festplattengröße von 32 tib

Verwandte Links

- "Microsoft Azure-Dokumentation: Verwaltete Festplattentypen in Azure"
- "Microsoft Azure-Dokumentation: Übersicht über die Blobs der Azure-Seite"
- "Erfahren Sie, wie Sie Festplattentypen und Festplattengrößen für Ihre Systeme in Azure auswählen"
- "Prüfen Sie Storage-Limits für Cloud Volumes ONTAP in Azure"

Google Cloud Storage

In Google Cloud kann ein Aggregat bis zu 6 Festplatten enthalten, die alle gleich groß sind. Die maximale Festplattengröße beträgt 64 tib.

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

Verwandte Links

- "Google Cloud-Dokumentation: Storage-Optionen"
- "Überprüfen Sie die Storage-Limits für Cloud Volumes ONTAP in Google Cloud"

RAID-Typ

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

Hot Spares

RAID0 unterstützt die Verwendung von Hot Spares nicht für Redundanz.

Das Erstellen ungenutzter Festplatten (Hot Spares), die an eine Cloud Volumes ONTAP Instanz angeschlossen sind, ist ein unnötig hoher Aufwand und kann die Bereitstellung von zusätzlichem Speicherplatz bei Bedarf verhindern. Daher wird es nicht empfohlen.

Elastische Volumes in AWS

Die Unterstützung der Elastic Volumes von Amazon EBS mit einem Cloud Volumes ONTAP Aggregat bietet eine bessere Performance und zusätzliche Kapazität, während BlueXP die zugrunde liegende Festplattenkapazität nach Bedarf automatisch erhöht.

Vorteile

- Dynamisches Festplattenwachstum

  BlueXP kann die Größe der Festplatten dynamisch erhöhen, während Cloud Volumes ONTAP läuft und Festplatten noch angeschlossen sind.

- Bessere Performance

  Aggregate mit Elastic Volumes können bis zu acht Festplatten aufweisen, die über zwei RAID-Gruppen hinweg gleichermaßen genutzt werden. Diese Konfiguration bietet einen höheren Durchsatz und konsistente Performance.

- Größere Aggregate

  Die Unterstützung von acht Festplatten bietet eine maximale Aggregatskapazität von 128 tib. Diese Obergrenzen liegen über dem sechs-Plattenlimit und dem 96-tib-Limit für Aggregate, die mit der Elastic Volumes-Funktion nicht aktiviert sind.

  Beachten Sie, dass die Kapazitätsgrenzen des Systems insgesamt unverändert bleiben.

"Weitere Informationen zu Elastic Volumes von AWS"

Unterstützte Konfigurationen

Die Amazon EBS Elastic Volumes Funktion wird mit spezifischen Cloud Volumes ONTAP Versionen und spezifischen EBS Festplattentypen unterstützt.

Cloud Volumes ONTAP-Version

Die Elastic Volumes Funktion wird mit *neuen* Cloud Volumes ONTAP Systemen unterstützt, die ab Version 9.11.0 erstellt wurden. Die Funktion wird von vorhandenen Cloud Volumes ONTAP Systemen, die vor 9.11.0 implementiert wurden, *nicht* unterstützt.

Beispielsweise wird die Funktion Elastic Volumes nicht unterstützt, wenn Sie ein Cloud Volumes ONTAP 9.9.0 System erstellt und dann ein Upgrade auf Version 9.11.0 durchgeführt haben. Es muss sich um ein neues System mit Version 9.11.0 oder höher handelt.

EBS-Festplattentypen

Die Funktion Elastic Volumes wird automatisch auf Aggregatebene aktiviert, wenn General Purpose SSDs (gp3) oder bereitgestellte IOPS-SSDs (io1) verwendet werden. Die Funktion Elastic Volumes wird nicht mit Aggregaten unterstützt, die andere Festplattentypen verwenden.

Erforderliche AWS Berechtigungen

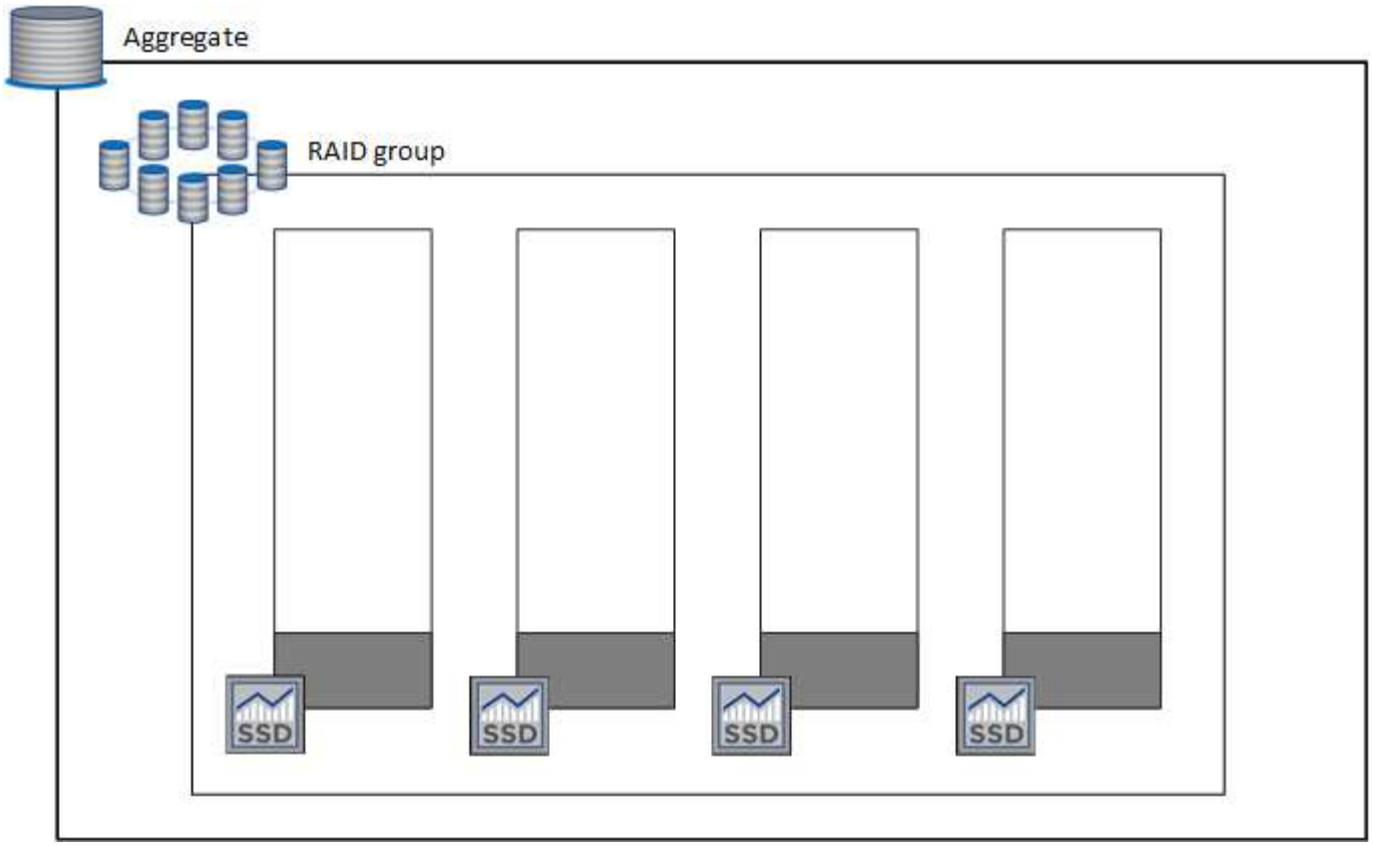
Ab Version 3.9.19 erfordert der Connector die folgenden Berechtigungen, um die Funktion Elastic Volumes auf einem Cloud Volumes ONTAP Aggregat zu aktivieren und zu managen:

- ec2:DescribeVolumiesModified
- ec2:ModifyVolume

Diese Berechtigungen sind in enthalten "Die von NetApp bereitgestellten Richtlinien"

Unterstützung von Elastic Volumes

Ein Aggregat mit aktivierter Elastic Volumes-Funktion besteht aus einer oder zwei RAID-Gruppen. Jede RAID-Gruppe verfügt über vier identische Festplatten mit derselben Kapazität. Hier ist ein Beispiel für ein 10-tib-Aggregat mit vier Festplatten, die jeweils 2.5 tib sind:



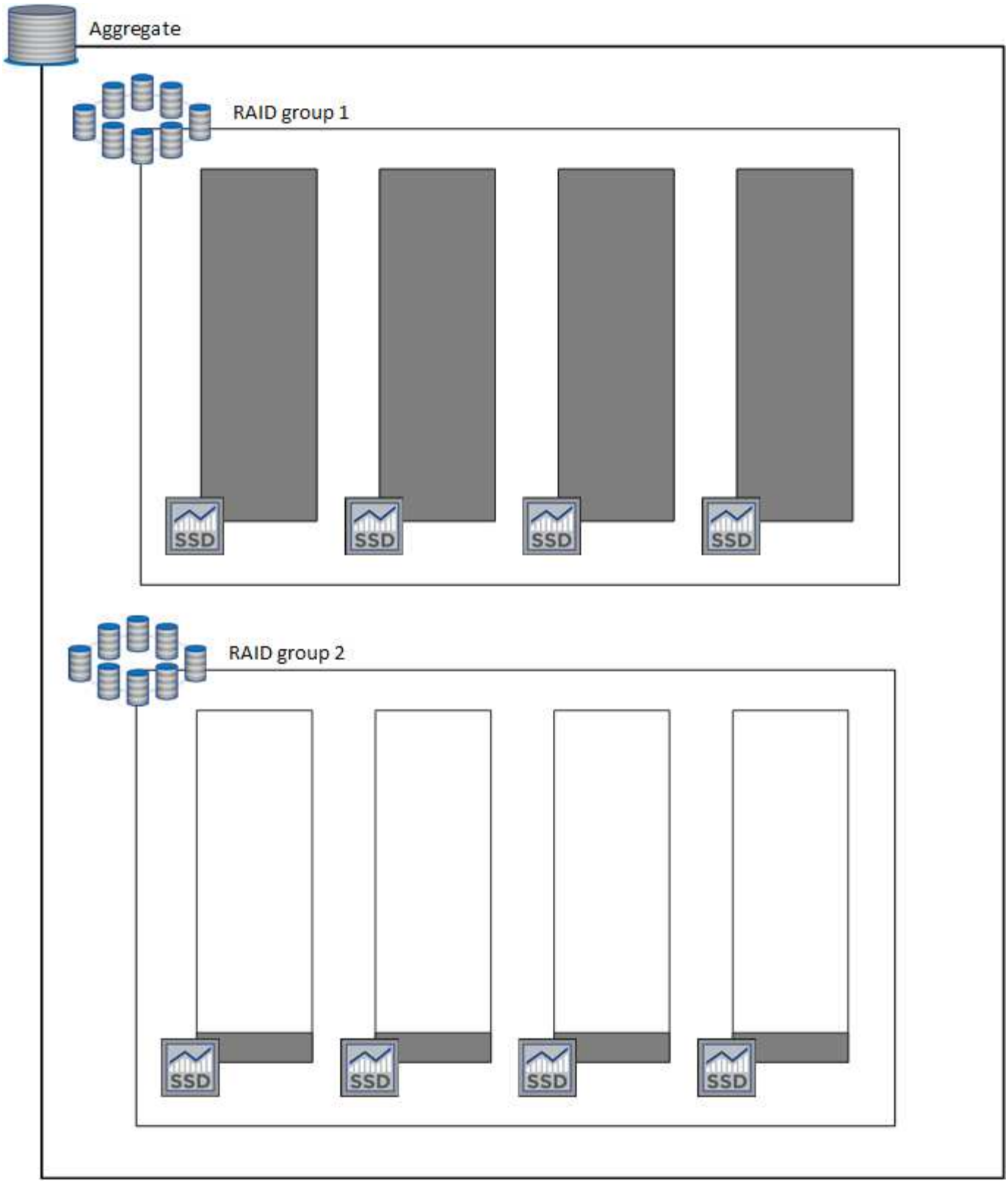
Wenn BlueXP ein Aggregat erstellt, beginnt es mit einer RAID-Gruppe. Falls zusätzliche Kapazität benötigt wird, wächst BlueXP das Aggregat, indem die Kapazität aller Festplatten in der RAID-Gruppe um dieselbe Menge erhöht wird. Die Kapazität erhöht sich entweder um mindestens 256 gib oder 10 % der Größe des Aggregats.

Wenn Sie beispielsweise ein 1 tib Aggregat haben, beträgt jede Festplatte 250 gib. 10 % der Kapazität des Aggregats ist 100 gib. Das ist niedriger als 256 gib, daher wird die Größe des Aggregats um das Minimum von 256 gib (oder 64 gib für jede Festplatte) erhöht.

BlueXP erhöht die Größe der Festplatten, während das Cloud Volumes ONTAP System ausgeführt wird und die Laufwerke noch angeschlossen sind. Die Änderung ist unterbrechungsfrei.

Wenn ein Aggregat 64 tib (oder 16 tib auf jeder Festplatte) erreicht, erstellt BlueXP im Hinblick auf zusätzliche Kapazität eine zweite RAID-Gruppe. Diese zweite RAID-Gruppe funktioniert genau wie die erste: Sie hat vier Festplatten mit exakt derselben Kapazität und kann bis auf 64 tib wachsen. Das bedeutet, dass ein Aggregat eine maximale Kapazität von 128 tib haben kann.

Hier ein Beispiel für ein Aggregat mit zwei RAID-Gruppen. Das Kapazitätslimit wurde bei der ersten RAID-Gruppe erreicht, während die Laufwerke in der zweiten RAID-Gruppe viel freien Speicherplatz haben.



Was passiert, wenn Sie ein Volume erstellen

Wenn Sie ein Volume erstellen, das gp3- oder io1-Festplatten verwendet, erstellt BlueXP das Volume auf einem Aggregat wie folgt:

- Wenn ein vorhandenes gp3- oder io1-Aggregat mit aktivierten Elastic Volumes aktiviert ist, erstellt BlueXP das Volume auf diesem Aggregat.

- Wenn mehrere gp3- oder io1-Aggregate aktiviert sind und elastische Volumes aktiviert sind, erstellt BlueXP das Volume auf dem Aggregat, das die geringste Menge an Ressourcen erfordert.
- Wenn das System nur gp3- oder io1-Aggregate enthält, die nicht für elastische Volumes aktiviert sind, wird das Volume auf diesem Aggregat erstellt.

  Dieses Szenario ist zwar unwahrscheinlich, aber in zwei Fällen ist dies möglich:

  - Sie haben die Funktion Elastic Volumes explizit deaktiviert, wenn Sie ein Aggregat aus der API erstellen.
  - Sie haben über die Benutzeroberfläche ein neues Cloud Volumes ONTAP System erstellt. In diesem Fall ist die Elastic Volumes Funktion auf dem anfänglichen Aggregat deaktiviert. Prüfen Einschränkungen Unten für weitere Informationen

- Wenn keine vorhandenen Aggregate genügend Kapazität haben, erstellt BlueXP das Aggregat mit aktivierten Elastic Volumes und erstellt dann das Volume auf dem neuen Aggregat.

  Die Größe des Aggregats basiert auf der angeforderten Volume-Größe plus einer zusätzlichen Kapazität von 10 %.

Kapazitätsmanagement -Modus

Der Capacity Management-Modus für einen Connector arbeitet mit elastischen Volumes zusammen, ähnlich wie er mit anderen Aggregattypen zusammenarbeitet:

- Wenn der Automatikmodus aktiviert ist (dies ist die Standardeinstellung), erhöht BlueXP automatisch die Aggregatgröße, wenn zusätzliche Kapazität benötigt wird.
- Wenn Sie den Modus für das Kapazitätsmanagement auf manuell ändern, fordert BlueXP Sie auf, zusätzliche Kapazitäten zu erwerben.

"Erfahren Sie mehr über den Capacity Management-Modus".

Einschränkungen

Eine Vergrößerung eines Aggregats kann bis zu 6 Stunden dauern. Während dieser Zeit kann BlueXP keine zusätzliche Kapazität für dieses Aggregat anfordern.

Wie Sie mit Elastic Volumes zusammenarbeiten

Die Arbeit mit Elastic Volumes ist in BlueXP wie folgt möglich:

- Erstellen Sie ein neues System, bei dem auf dem ursprünglichen Aggregat elastische Volumes aktiviert sind, wenn gp3- oder io1-Festplatten verwendet werden

  "Erfahren Sie, wie Sie ein Cloud Volumes ONTAP System erstellen"

- Erstellen Sie ein neues Volume auf einem Aggregat mit aktivierten Elastic Volumes

  Wenn Sie ein Volume erstellen, das gp3- oder io1-Festplatten verwendet, erstellt BlueXP das Volume automatisch auf einem Aggregat, in dem elastische Volumes aktiviert sind. Weitere Informationen finden Sie unter wenn Sie ein Volume erstellen.

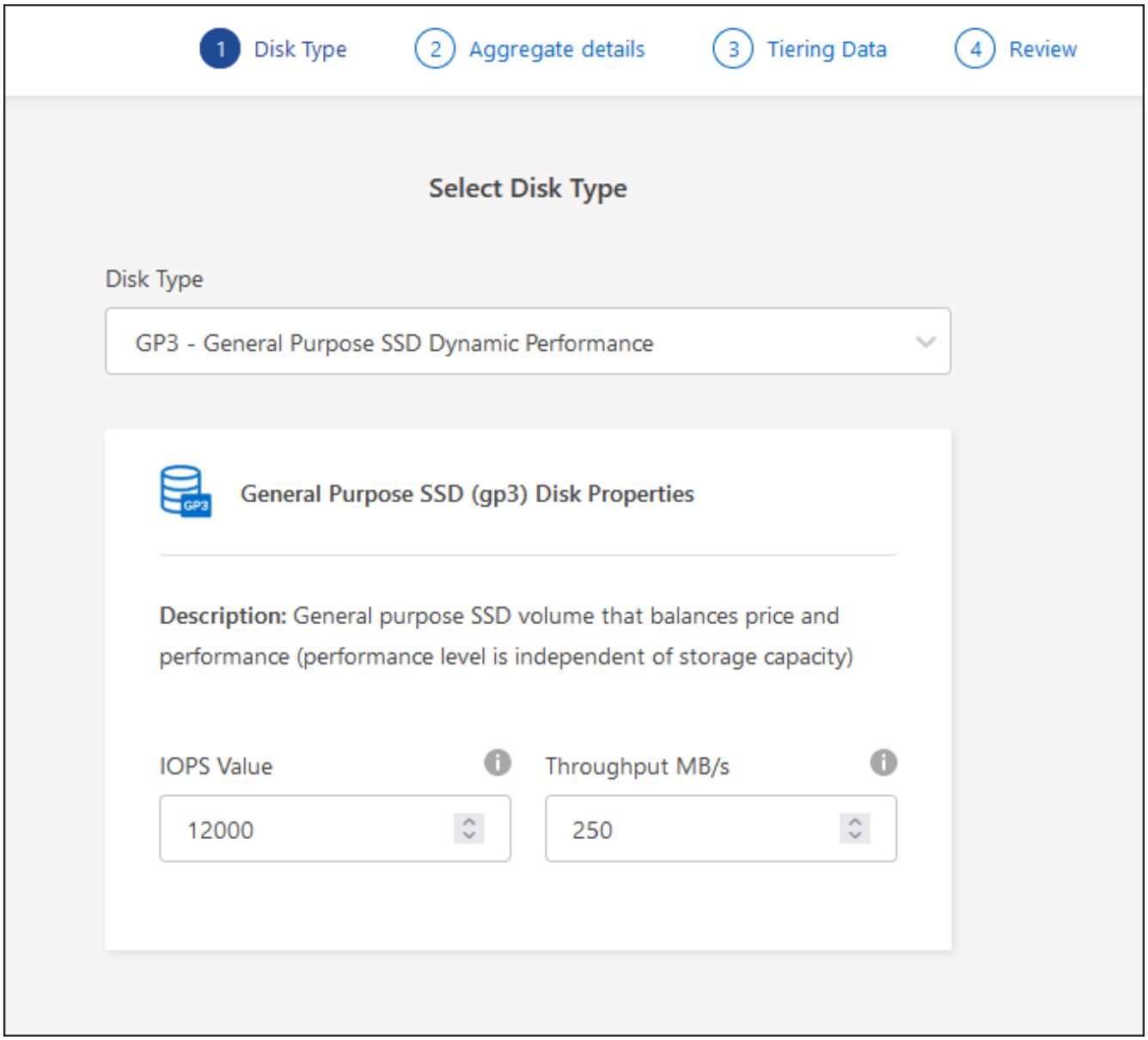
  "Lesen Sie, wie Sie Volumes erstellen".

- Erstellen Sie ein neues Aggregat mit aktivierten Elastic Volumes

  Elastische Volumes werden automatisch in neuen Aggregaten aktiviert, die gp3- oder io1-Festplatten verwenden, sofern das Cloud Volumes ONTAP-System aus Version 9.11.0 oder höher erstellt wurde.

  Wenn Sie das Aggregat erstellen, werden Sie von BlueXP zur Kapazitätsgröße des Aggregats aufgefordert. Dies unterscheidet sich von anderen Konfigurationen, bei denen Sie eine Festplattengröße und Anzahl der Festplatten wählen.

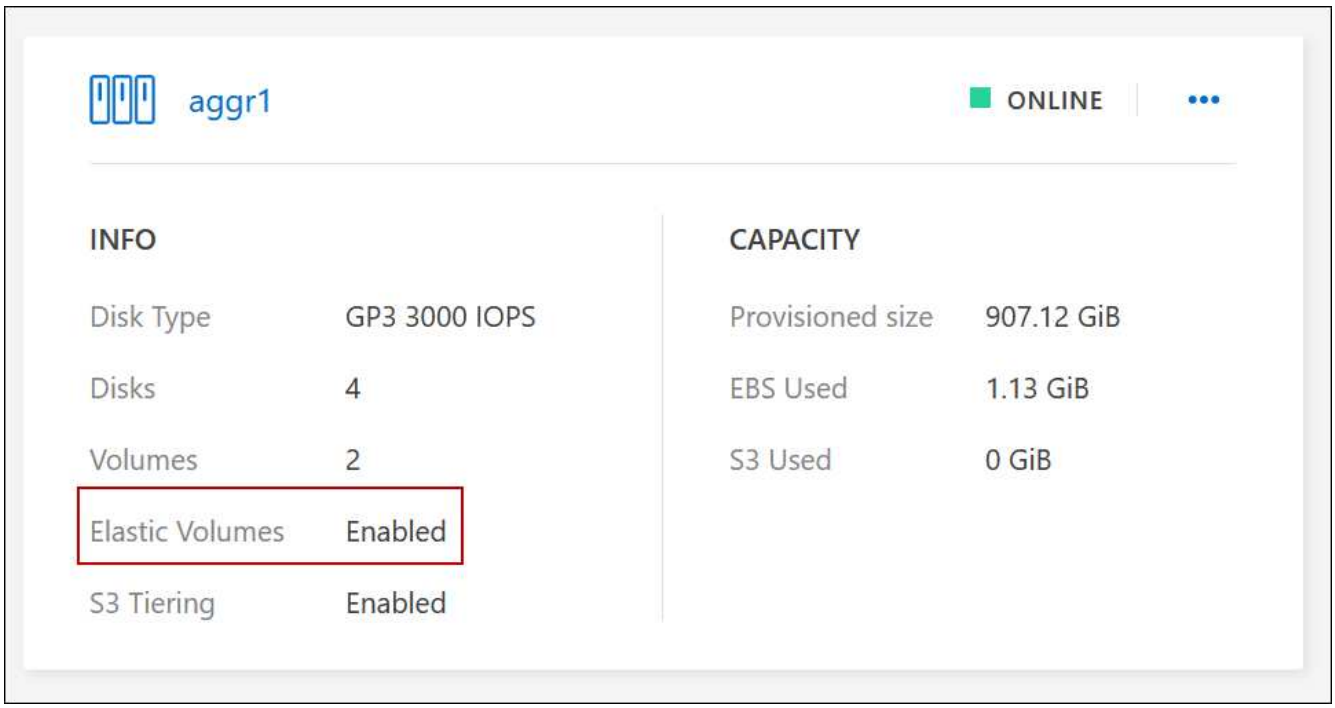
  Der folgende Screenshot zeigt ein Beispiel für ein neues Aggregat, das aus gp3-Festplatten besteht.



  "Lesen Sie, wie Aggregate erstellt werden".

- Identifizieren Sie Aggregate mit aktivierten Elastic Volumes

  Wenn Sie die Seite „Advanced Allocation“ aufrufen, können Sie ermitteln, ob die Funktion Elastic Volumes auf einem Aggregat aktiviert ist. Im folgenden Beispiel ist für aggr1 Elastic Volumes aktiviert.



- Hinzufügen von Kapazität zu einem Aggregat

  Während BlueXP Aggregate automatisch nach Bedarf erweitert, können Sie die Kapazität manuell erhöhen.

  "Erfahren Sie, wie Sie die Aggregatskapazität erhöhen".

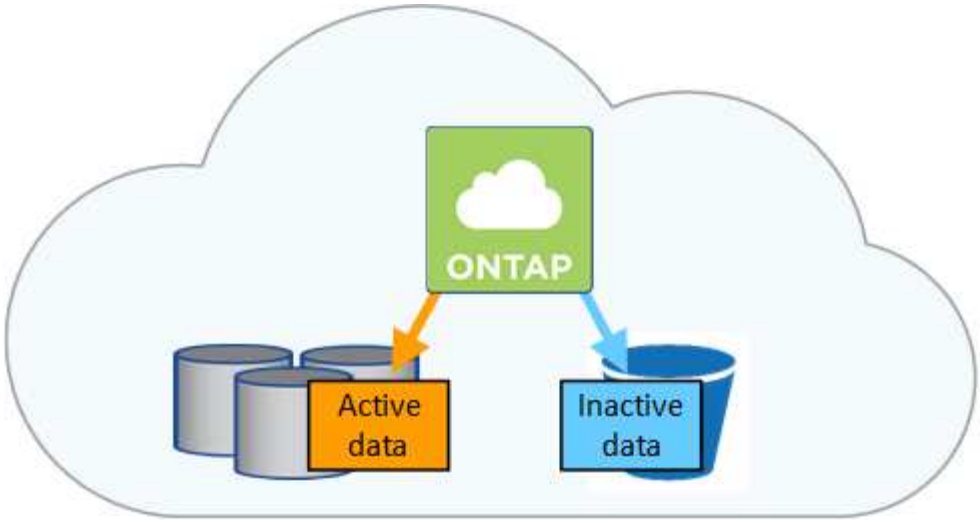
- Replizieren Sie Daten auf ein Aggregat, bei dem Elastic Volumes aktiviert sind

  Wenn das Ziel-Cloud Volumes ONTAP-System elastische Volumes unterstützt, wird ein Ziel-Volume auf einem Aggregat mit aktivierten elastischen Volumes platziert, sofern Sie eine gp3- oder io1-Festplatte wählen.

  "Hier erfahren Sie, wie Sie Datenreplizierung einrichten"

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.



Data Tiering wird durch FabricPool Technologie unterstützt. Cloud Volumes ONTAP bietet Daten-Tiering für alle Cloud Volumes ONTAP Cluster ohne zusätzliche Lizenz. Bei Aktivierung von Daten-Tiering fallen Gebühren für das Tiering von Daten in Objekt-Storage an. Weitere Informationen zu den Kosten für Objekt-Storage finden Sie in der Dokumentation Ihres Cloud-Providers.

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

Beim Performance-Tier können es sich um allgemeine SSDs (gp3 oder gp2) oder bereitgestellte IOPS-SSDs (io1) handelt.

Bei der Verwendung von durchsatzoptimierten HDDs (st1) wird kein Tiering von Daten zu Objekt-Storage empfohlen.

Kapazitäts-Tier

Ein Cloud Volumes ONTAP System verschiebt inaktive Daten auf einen einzelnen S3-Bucket.

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

Wenn BlueXP den S3-Bucket erstellt, werden die folgenden Standardeinstellungen verwendet:

- Storage-Klasse: Standard
- Standardverschlüsselung deaktiviert
- Öffentlichen Zugang blockieren: Alle öffentlichen Zugänge blockieren
- Objekteigentümer: ACLs aktiviert
- Bucket-Versionierung: Deaktiviert
- Objektsperre: Deaktiviert

Speicherklassen

Die Standard-Storage-Klasse für Tiered Daten in AWS ist *Standard*. Standard ist ideal für häufig aufgerufene Daten, die über mehrere Verfügbarkeitszonen gespeichert werden.

Wenn Sie keinen Zugriff auf inaktive Daten planen, können Sie die Storage-Kosten senken, indem Sie die Storage-Klasse auf eine der folgenden Komponenten ändern: *Intelligent Tiering*, *One-Zone infrequent Access*, *Standard-infrequent Access* oder *S3 Glacier Instant Retrieval*. 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 auf einen einzelnen Blob-Container ab.

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

BlueXP erstellt das Speicherkonto mit den folgenden Einstellungen:

- Zugriffsebene: Heiß
- Leistung: Standard
- Redundanz: Lokal redundanter Storage (LRS)
- Konto: StorageV2 (allgemeine Zwecke v2)
- Sichere Übertragung für REST-API-Vorgänge nötig: Aktiviert
- Zugriff auf Schlüssel des Storage-Kontos: Aktiviert
- Minimale TLS-Version: Version 1.2
- Infrastrukturverschlüsselung deaktiviert

Storage-Zugriffstufen

Die Standard-Storage-Zugriffs-Tier für Tiered Daten in Azure ist die *Hot*-Tier. Die Tier mit häufig benötigten Daten ist ideal für Daten in der Kapazitäts-Tier.

Wenn Sie nicht planen, auf die inaktiven Daten in der Kapazitäts-Tier zuzugreifen, können Sie Ihre Speicherkosten senken, indem Sie auf die Storage-Tier *cool* wechseln. Wenn Sie den Speicher-Tier zu kühlen ändern, werden inaktive Kapazitäts-Tier-Daten direkt in den kühlen Speicher-Tier verschoben.

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 Google Cloud

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

Performance-Tier

Beim Performance-Tier können es sich entweder um persistente SSD-Festplatten, ausgewogene persistente Festplatten oder um Standard-persistente Festplatten handeln.

Kapazitäts-Tier

Ein Cloud Volumes ONTAP System verschiebt inaktive Daten auf einen einzelnen Google Cloud Storage Bucket.

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

Wenn BlueXP den Bucket erstellt, verwendet er die folgenden Standardeinstellungen:

- Positionstyp: Region
- Storage-Klasse: Standard
- Öffentlicher Zugriff: Unterliegt Objekt-ACLs
- Zugriffssteuerung: Feingranular
- Schutz: Keine
- Datenverschlüsselung: Von Google verwalteter Schlüssel

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 Storage-Klasse ändern, werden nachfolgende inaktive Daten direkt in die von Ihnen ausgewählte Klasse verschoben.

Alle vorhandenen inaktiven Daten behalten die Standardspeicherklasse bei, wenn Sie die Speicherklasse ändern. Um die Speicherklasse für vorhandene inaktive Daten zu ändern, müssen Sie die Bezeichnung manuell vornehmen.

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. Die Kühldauer beginnt, wenn Daten in das Aggregat geschrieben werden.

Sie können den minimalen Kühlzeitraum und den standardmäßigen Aggregatschwellenwert von 50 % ändern (dazu unten). "Erfahren Sie, wie Sie die Kühlzeit ändern" Und "Erfahren Sie, wie Sie den Schwellenwert ändern".

Mit BlueXP können Sie bei der Erstellung oder Änderung eines Volumes aus den folgenden Volume Tiering-Richtlinien auswählen:

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 BlueXP die **Backup**-Richtlinie auf das Datenschutzvolumen 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 Sie längere Kühlzeiten haben.

Wenn Cloud Volumes ONTAP deaktiviert wird, bleibt die Temperatur jedes Blocks bis zum Neustart des Systems erhalten. Wenn die Temperatur eines Blocks z. B. bei ausgeschaltetem System 5 beträgt, beträgt die Temperatur nach dem Einschalten des Systems immer noch 5.

Einrichten von Data Tiering

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

Storage-Management

BlueXP ermöglicht vereinfachtes und erweitertes Management von Cloud Volumes ONTAP Storage.

Alle Festplatten und Aggregate müssen direkt aus BlueXP 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

BlueXP vereinfacht die Storage-Bereitstellung für Cloud Volumes ONTAP durch den Kauf von Festplatten und das Management von Aggregaten für Sie. 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. BlueXP erstellt Aggregate für Sie beim Starten einer Instanz sowie bei der Bereitstellung zusätzlicher Volumes.

Wenn Sie ein Volume erstellen, führt BlueXP eine von drei Dingen 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.

+ im Fall eines Aggregats in AWS, das Elastic Volumes unterstützt, erhöht BlueXP auch die Größe der Festplatten in einer RAID-Gruppe. "Erfahren Sie mehr über den Support für Elastic Volumes".

- Es kauft Festplatten für ein neues Aggregat und platziert das Volume auf diesem Aggregat.

BlueXP bestimmt, wo ein neues Volume platziert werden soll, indem es sich auf mehrere Faktoren ausschaut: Die maximale Größe eines Aggregats, ob Thin Provisioning aktiviert ist und die freien Speicherplatzschwellenwerte für Aggregate.

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

Auswahl der Festplattengröße für Aggregate in AWS

Wenn BlueXP neue Aggregate für Cloud Volumes ONTAP in AWS erstellt, erhöht es nach und nach die Festplattengröße in einem Aggregat, da die Anzahl der Aggregate im System zunimmt. BlueXP stellt dies sicher, dass Sie die maximale Kapazität des Systems nutzen können, bevor es die maximale Anzahl von Datenfestplatten erreicht, die von AWS zulässig sind.

BlueXP kann beispielsweise die folgenden Festplattengrößen wählen:

Aggregatnummer	Festplattengröße	Max. Gesamtkapazität
1	500 gib	3 tib
4	1 tib	6 tib
6	2 tib	12 tib

Dieses Verhalten gilt nicht für Aggregate, die die Amazon EBS Elastic Volumes Funktion unterstützen. Aggregate mit aktivierten elastischen Volumes bestehen aus einer oder zwei RAID-Gruppen. Jede RAID-Gruppe verfügt über vier identische Festplatten mit derselben Kapazität. "Erfahren Sie mehr über den Support für Elastic Volumes".

Sie können die Festplattengröße selbst mithilfe der erweiterten Zuweisungsoption auswählen.

Erweiterte Zuweisung

Statt BlueXP Aggregate für Sie verwalten zu lassen, können Sie es selbst erledigen. "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 auswählen, ob BlueXP Sie über Entscheidungen zur Storage-Kapazität benachrichtigt oder ob BlueXP die Kapazitätsanforderungen automatisch managt.

Dieses Verhalten wird durch den *Capacity Management Mode* auf einem Connector bestimmt. Der Capacity Management-Modus betrifft alle von diesem Connector verwalteten Cloud Volumes ONTAP-Systeme. Wenn Sie einen anderen Konnektor haben, kann er anders konfiguriert werden.

Automatisches Kapazitätsmanagement

Der Kapazitätsmanagement-Modus ist standardmäßig auf automatisch eingestellt. In diesem Modus überprüft BlueXP das Verhältnis des freien Speicherplatzes alle 15 Minuten, um zu ermitteln, ob das Verhältnis des freien Speicherplatzes unter den angegebenen Schwellenwert fällt. Falls mehr Kapazität erforderlich ist, initiiert BlueXP automatisch die Anschaffung neuer Festplatten, löscht ungenutzte Festplattensammlungen (Aggregate), verschiebt Volumes zwischen Aggregaten und versucht einen Festplattenausfall zu verhindern.

Die folgenden Beispiele veranschaulichen die Funktionsweise dieses Modus:

- Wenn ein Aggregat die Kapazitätsgrenze erreicht und mehr Festplatten zur Verfügung stehen, kauft BlueXP automatisch neue Festplatten für das Aggregat, sodass die Volumen weiter wachsen können.

Im Falle eines Aggregats in AWS, das Elastic Volumes unterstützt, vergrößert BlueXP auch die Festplatten einer RAID-Gruppe. "Erfahren Sie mehr über den Support für Elastic Volumes".

+
* Wenn ein Aggregat die Kapazitätsgrenze erreicht und keine zusätzlichen Festplatten unterstützt, verschiebt BlueXP automatisch ein Volume von diesem Aggregat zu einem Aggregat mit verfügbarer Kapazität oder zu einem neuen Aggregat.

+
Wenn BlueXP 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. In diesem Szenario kann der Speicherplatz nicht wieder an den Cloud-Provider übergeben werden.

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

Verwaltung von LUNs mit automatischem Kapazitätsmanagement

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

Manuelles Kapazitätsmanagement

Wenn der Kontoadministrator den Kapazitätsverwaltungsmodus auf manuell setzt, zeigt BlueXP Meldungen zu Maßnahmen erforderlich 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.

Weitere Informationen .

"Erfahren Sie, wie Sie den Modus für das Kapazitätsmanagement ändern".

Schreibgeschwindigkeit

Mit BlueXP können Sie für die meisten Cloud Volumes ONTAP-Konfigurationen normale oder hohe Schreibgeschwindigkeit 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.

Normale Schreibgeschwindigkeit

Wenn Sie die normale Schreibgeschwindigkeit wählen, werden die Daten direkt auf die Festplatte geschrieben. Wenn Daten direkt auf die Festplatte geschrieben werden, verringert sie die Wahrscheinlichkeit eines Datenverlusts bei einem ungeplanten Systemausfall oder bei einem kaskadierenden Ausfall eines ungeplanten Systemausfalls (nur HA-Paare).

Die normale Schreibgeschwindigkeit ist die Standardoption.

Hohe Schreibgeschwindigkeit

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 vom Cloud-Provider bereitgestellten Storage kann sich jedoch auf die Dauer der Konsistenzpunktverarbeitung auswirken.

Wann wird hohe Schreibgeschwindigkeit verwendet

Eine hohe Schreibgeschwindigkeit ist eine gute Wahl, wenn eine hohe Schreib-Performance für Ihren Workload benötigt wird und Sie das Risiko eines Datenverlusts im Fall eines ungeplanten Systemausfalls standhalten oder einen kaskadierenden Ausfall im Zusammenhang mit einem ungeplanten Systemausfall (nur HA-Paare) auftreten können.

Empfehlungen bei hoher Schreibgeschwindigkeit

Wenn Sie eine hohe Schreibgeschwindigkeit aktivieren, sollten Sie den Schreibschutz auf Applikationsebene sicherstellen oder dass die Applikationen Datenverlust tolerieren können, falls diese auftreten.

Hohe Schreibgeschwindigkeit mit einem HA-Paar in AWS

Wenn Sie hohe Schreibgeschwindigkeit für ein HA-Paar in AWS aktivieren möchten, sollten Sie die Unterschiede bei der Sicherung zwischen einer Implementierung mit mehreren Verfügbarkeitszonen und einer Implementierung mit einer einzelnen Verfügbarkeitszone verstehen. Die Implementierung eines HA-Paars über mehrere Verfügbarkeitszonen hinweg sorgt für mehr Ausfallsicherheit und hilft, das Risiko eines Datenverlusts zu minimieren.

"Erfahren Sie mehr über HA-Paare in AWS".

Konfigurationen mit hoher Schreibgeschwindigkeit

Nicht alle Cloud Volumes ONTAP Konfigurationen unterstützen eine hohe Schreibgeschwindigkeit. Diese Konfigurationen verwenden standardmäßig normale Schreibgeschwindigkeit.

AWS

Wenn Sie ein Single-Node-System verwenden, unterstützt Cloud Volumes ONTAP bei allen Instanztypen eine hohe Schreibgeschwindigkeit.

Ab Version 9.8 unterstützt Cloud Volumes ONTAP bei fast allen unterstützten EC2-Instanztypen eine hohe Schreibgeschwindigkeit mit HA-Paaren, ausgenommen m5.xlarge und r5.xlarge.

"Erfahren Sie mehr über die von Cloud Volumes ONTAP unterstützten Amazon EC2 Instanzen".

Azure

Wenn Sie ein Single-Node-System verwenden, unterstützt Cloud Volumes ONTAP für alle VM-Typen eine hohe Schreibgeschwindigkeit.

Wenn Sie ein HA-Paar verwenden, unterstützt Cloud Volumes ONTAP mit mehreren VM-Typen eine hohe Schreibgeschwindigkeit, beginnend mit Version 9.8. Wechseln Sie zum "Versionshinweise zu Cloud Volumes ONTAP" Um die VM-Typen anzuzeigen, die eine hohe Schreibgeschwindigkeit unterstützen.

Google Cloud

Wenn Sie ein Single-Node-System verwenden, unterstützt Cloud Volumes ONTAP bei allen Maschinentypen eine hohe Schreibgeschwindigkeit.

Wenn Sie ein HA-Paar verwenden, unterstützt Cloud Volumes ONTAP für mehrere VM-Typen, beginnend mit Version 9.13.0, eine hohe Schreibgeschwindigkeit. Wechseln Sie zum "Versionshinweise zu Cloud Volumes ONTAP" Um die VM-Typen anzuzeigen, die eine hohe Schreibgeschwindigkeit unterstützen.

"Erfahren Sie mehr über die von Cloud Volumes ONTAP unterstützten Google Cloud-Maschinentypen".

So wählen Sie eine Schreibgeschwindigkeit aus

Sie können eine Schreibgeschwindigkeit wählen, wenn Sie eine neue Arbeitsumgebung erstellen und Sie können "Ändern Sie die Schreibgeschwindigkeit für ein vorhandenes System".

Was bei einem Datenverlust zu erwarten ist

Wenn Datenverlust aufgrund hoher Schreibgeschwindigkeit auftritt, meldet das Event Management System (EMS) die folgenden beiden Ereignisse:

- Cloud Volumes ONTAP 9.12.1 oder höher

```
 NOTICE nv.data.loss.possible: An unexpected shutdown occurred while in
high write speed mode, which possibly caused a loss of data.
* Cloud Volumes ONTAP 9.11.0 auf 9.11.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown with High Write Speed mode"
```

```
 ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect..
* Cloud Volumes ONTAP 9.8 auf 9.10.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect.
```

Sollte dies der Fall sein, sollte Cloud Volumes ONTAP in der Lage sein, ohne Eingreifen des Benutzers weitere Daten bereitzustellen.

So wird der Datenzugriff bei Datenverlust verhindert

Wenn Sie sich Sorgen um Datenverlust machen, möchten Sie, dass die Anwendungen bei Datenverlust nicht mehr ausgeführt werden und der Datenzugriff wieder aufgenommen wird, nachdem das Problem mit Datenverlust behoben wurde, können Sie die Option NVFAIL aus der CLI verwenden, um dieses Ziel zu erreichen.

Aktivieren der Option „NVFAIL“

```
vol modify -volume <vol-name> -nvfail on
```

Zum Prüfen der NV-Fehler-Einstellungen

```
vol show -volume <vol-name> -fields nvfail
```

Um die Option „NV-Fehler“ zu deaktivieren

```
vol modify -volume <vol-name> -nvfail off
```

Wenn ein Datenverlust auftritt, sollte ein NFS- oder iSCSI-Volume mit aktiviertem NVFAIL die Bereitstellung von Daten beenden (es gibt keine Auswirkungen auf CIFS, was ein statusfreies Protokoll ist). Weitere Informationen finden Sie unter "Auswirkungen von NV-Fehler auf den Zugriff auf NFS-Volumes oder LUNs".

Um den Status „NV-Fehler“ zu überprüfen

```
vol show -fields in-nvfailed-state
```

Nachdem das Problem mit dem Datenverlust behoben wurde, können Sie den NV-Fehler-Status löschen und das Volume steht für den Datenzugriff zur Verfügung.

Zum Löschen des Status „NV-Fehler“

```
vol modify -volume <vol-name> -in-nvfailed-state false
```

Flash Cache

Einige Cloud Volumes ONTAP Konfigurationen umfassen lokalen NVMe-Storage, den Cloud Volumes ONTAP für bessere Performance als *Flash Cache* verwendet.

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 Konfigurationen

Flash Cache wird mit spezifischen Cloud Volumes ONTAP Konfigurationen unterstützt. Zeigen Sie unterstützte Konfigurationen in an "Versionshinweise zu Cloud Volumes ONTAP"

Einschränkungen

- Die Komprimierung muss auf allen Volumes deaktiviert sein, um die Performance-Verbesserungen durch Flash Cache bis zu Cloud Volumes ONTAP 9.12.0 nutzen zu können. Wenn Sie auf Cloud Volumes ONTAP 9.12.1 implementieren oder ein Upgrade durchführen, müssen Sie die Komprimierung nicht deaktivieren.

  Entscheiden Sie sich für keine Storage-Effizienz bei der Erstellung eines Volumes mit BlueXP, 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. Cloud-WORM-Storage wird durch SnapLock Technologie unterstützt, d. h., WORM-Dateien sind auf Dateiebene gesichert.

Funktionsweise VON WORM-Speicher

Sobald eine Datei im WORM-Storage gespeichert wurde, kann sie nicht mehr verändert werden, selbst wenn der Aufbewahrungszeitraum abgelaufen ist. 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.

Wird Geladen

Die Abrechnung FÜR WORM-Speicher erfolgt stündlich, entsprechend der insgesamt bereitgestellten Kapazität von WORM-Volumes.

Nur für PAYGO oder Jahresverpflichtung verfügbar, Lizenzierung für WORM kann über den Marketplace des Cloud-Providers erworben werden. WORM unterstützt sowohl Node- als auch kapazitätsbasierte Lizenzmodelle.

Die BYOL-Lizenzierung ist nicht für WORM Storage auf Cloud Volumes ONTAP verfügbar.

Sie sollten das folgende Ladeverhalten mit Cloud Volumes ONTAP 9.10.1 und höher verstehen:

- Ab ONTAP 9.10.1 KÖNNEN WORM Volumes und nicht-WORM-Volumes auf demselben Aggregat vorhanden sein.
- Wenn Sie WORM aktivieren, wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen, ist für jedes in BlueXP erstellte Volume WORM aktiviert. Allerdings können Sie mit der ONTAP CLI oder mit

System Manager Volumes erstellen, in denen WORM deaktiviert ist. Diese Volumes werden NICHT mit DER WORM-Rate berechnet.

- Wenn SIE WORM nicht aktivieren, wenn Sie eine Arbeitsumgebung erstellen, ist jedes mit BlueXP erstellte Volume WORM deaktiviert. FÜR diese Volumes werden die WORM-Rate nicht berechnet.

"Informieren Sie sich über die Preisgestaltung für WORM Storage"

WORM-Storage wird aktiviert

Wie Sie WORM-Speicher aktivieren, hängt von der verwendeten Cloud Volumes ONTAP Version ab.

Version 9.10.1 und höher

Ab Cloud Volumes ONTAP 9.10.1 haben Sie die Möglichkeit, WORM auf Volume-Ebene zu aktivieren oder zu deaktivieren.

Wenn Sie eine neue Cloud Volumes ONTAP Arbeitsumgebung erstellen, werden Sie aufgefordert, WORM-Speicher zu aktivieren oder zu deaktivieren:

- Wenn Sie WORM-Speicher beim Erstellen einer Arbeitsumgebung aktivieren, ist für jedes mit BlueXP erstellte Volume WORM aktiviert. Aber Sie können System Manager oder die CLI verwenden, um Volumes zu erstellen, bei denen WORM deaktiviert ist.
- Wenn Sie WORM-Storage bei der Erstellung einer Arbeitsumgebung deaktivieren, ist jedes von Ihnen aus BlueXP, System Manager oder der CLI erstellte Volume WORM deaktiviert. Wenn SIE WORM in einer Cloud Volumes ONTAP-Arbeitsumgebung aktivieren möchten, die bei der Erstellung nicht aktiviert wurde, müssen Sie ein Support-Ticket mit dem NetApp Support erstellen.

Mit beiden Optionen sollten Sie dies tun Erfahren Sie, wie das Laden funktioniert.

Version 9.10.0 und früher

Sie können WORM Storage auf einem Cloud Volumes ONTAP System aktivieren, wenn Sie eine neue Arbeitsumgebung erstellen. Jedes von Ihnen aus BlueXP erstellte Volume ist DURCH WORM aktiviert. WORM Storage kann nicht auf einzelnen Volumes deaktiviert werden.

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".

WORM-Dateien werden gelöscht

MIT der Funktion Privileged delete können SIE WORM-Dateien während des Aufbewahrungszeitraums löschen.

Anweisungen finden Sie unter "ONTAP-Dokumentation"

WORM- und Daten-Tiering

Wenn Sie ein neues Cloud Volumes ONTAP 9.8 System oder höher erstellen, können Sie sowohl Daten-Tiering als AUCH WORM Storage gemeinsam aktivieren. Wenn Sie Daten-Tiering mit WORM-Storage aktivieren, können Sie die Daten auf einen Objektspeicher in der Cloud verschieben.

Sie sollten Folgendes über die Aktivierung von Daten-Tiering und WORM-Storage wissen:

- Daten, die auf Objekt-Storage verschoben werden, enthalten nicht die ONTAP WORM-Funktion. Um die End-to-End-WORM-Fähigkeit sicherzustellen, müssen Sie die Bucket-Berechtigungen korrekt einrichten.
- Die auf Objekt-Storage abgelegten Daten verfügen nicht über DIE WORM-Funktionalität, d. h., jeder mit vollem Zugriff auf Buckets und Container kann die durch ONTAP abgestuften Objekte löschen.
- Ein Wechsel- oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach Aktivierung VON WORM und Tiering gesperrt.

Einschränkungen

- WORM Storage in Cloud Volumes ONTAP wird als „vertrauenswürdiger Storage-Administrator“ eingesetzt. WORM-Dateien sind vor Änderungen oder Änderungen geschützt, aber können von einem Cluster-Administrator gelöscht werden, selbst wenn diese Volumes nicht ABGELAUFENE WORM-Daten enthalten.
- Neben dem Modell eines vertrauenswürdigen Storage-Administrators arbeitet WORM Storage in Cloud Volumes ONTAP auch implizit unter einem Modell eines „vertrauenswürdigen Cloud-Administrators“. Ein Cloud-Administrator kann WORM-Daten vor dem Ablaufdatum löschen, indem er Cloud-Storage direkt vom Cloud-Provider entfernt oder bearbeitet.

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.

HA-Komponenten

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.

Mediator

Hier einige wichtige Details zur Mediator-Instanz in AWS:

Instanztyp
: t3-Micro

Festplatten
: Zwei st1-Festplatten mit 8 gib und 4 gib

Betriebssystem

Debian 11

Für Cloud Volumes ONTAP 9.10.0 und früher wurde Debian 10 auf dem Mediator installiert.

Upgrades

Bei einem Upgrade von Cloud Volumes ONTAP aktualisiert BlueXP auch die Mediator-Instanz nach Bedarf.

Zugriff auf die Instanz

Wenn Sie ein Cloud Volumes ONTAP HA-Paar aus BlueXP erstellen, werden Sie aufgefordert, ein Schlüsselpaar für die Instanz des Mediators bereitzustellen. Sie können dieses Schlüsselpaar für SSH-Zugriff mit verwenden `admin` Benutzer:

Agenten von Drittanbietern

Agents von Drittanbietern oder VM-Erweiterungen werden auf der Mediator-Instanz nicht unterstützt.

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.

Storage-Übernahme, -Resynchronisierung und -Rückgabe sind standardmäßig automatisch erfolgt. Es ist keine Benutzeraktion erforderlich.

RPO und RTO

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

- Das Recovery Point Objective (RPO) beträgt 0 Sekunden. Ihre Daten sind transaktionskonsistent und ohne Datenverlust.
- Die Recovery-Zeitvorgabe (RTO) beträgt 120 Sekunden. Bei einem Ausfall sollten die Daten in maximal 120 Sekunden verfügbar sein.

Ha-Bereitstellungsmodelle

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

Verfügbarkeitszonen

Durch die Implementierung einer HA-Konfiguration in mehreren Verfügbarkeitszonen (AZS) werden Ihre Daten bei einem Ausfall mit einer Verfügbarkeitszone oder einer Instanz, auf der ein Cloud Volumes ONTAP-Node ausgeführt wird, Hochverfügbarkeit sichergestellt. 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.

Sie sollten die Anforderungen für fließende IP-Adressen und Routingtabellen überprüfen, bevor Sie eine HA-Konfiguration über mehrere Verfügbarkeitszonen hinweg implementieren. Sie müssen die unverankerten IP-Adressen angeben, wenn Sie die Konfiguration bereitstellen. Die privaten IP-Adressen werden automatisch von BlueXP 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.

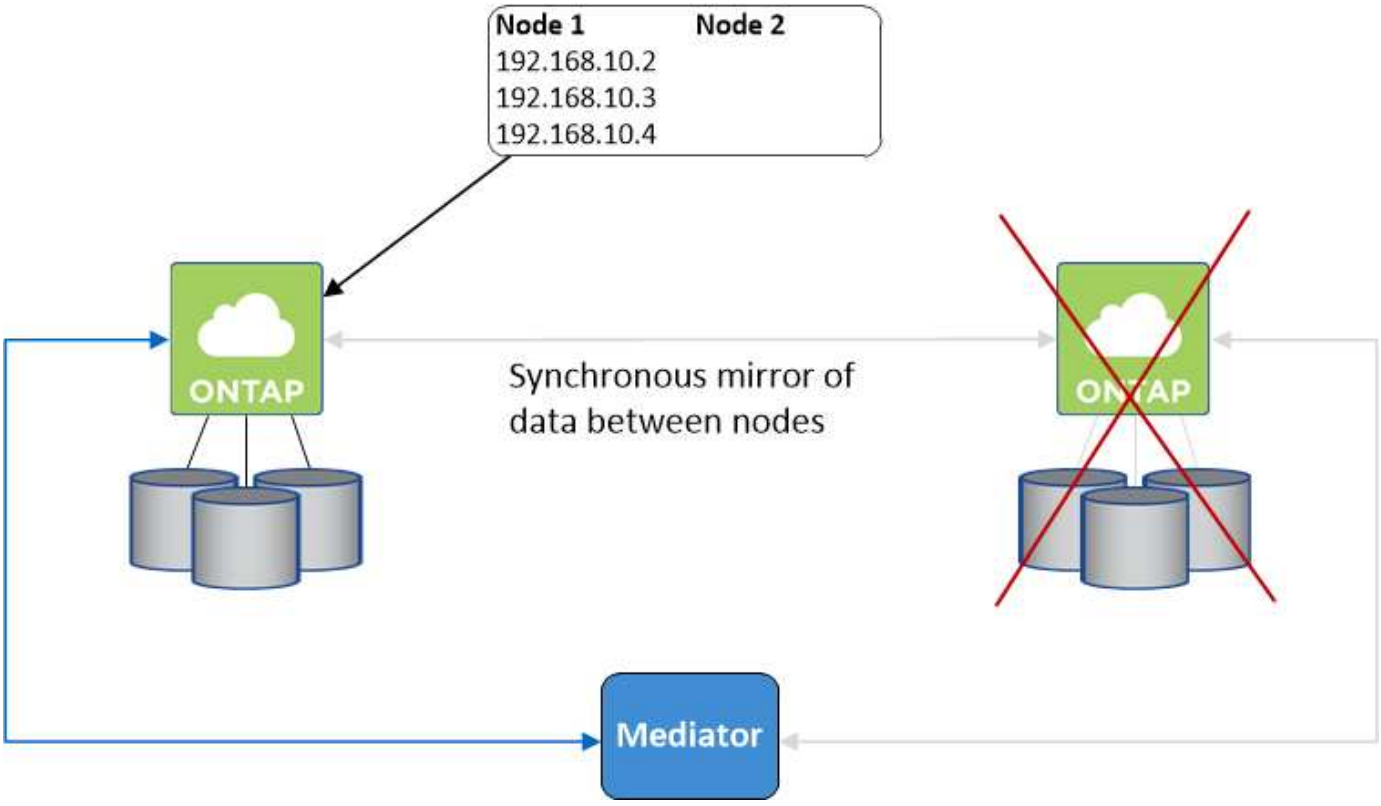
Takeover und Giveback für iSCSI

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.

Takeover 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 die richtige IP-Adresse von BlueXP leicht erkennen, indem Sie die Lautstärke auswählen und auf **Mount Command** klicken.

Einzelne Verfügbarkeitszone

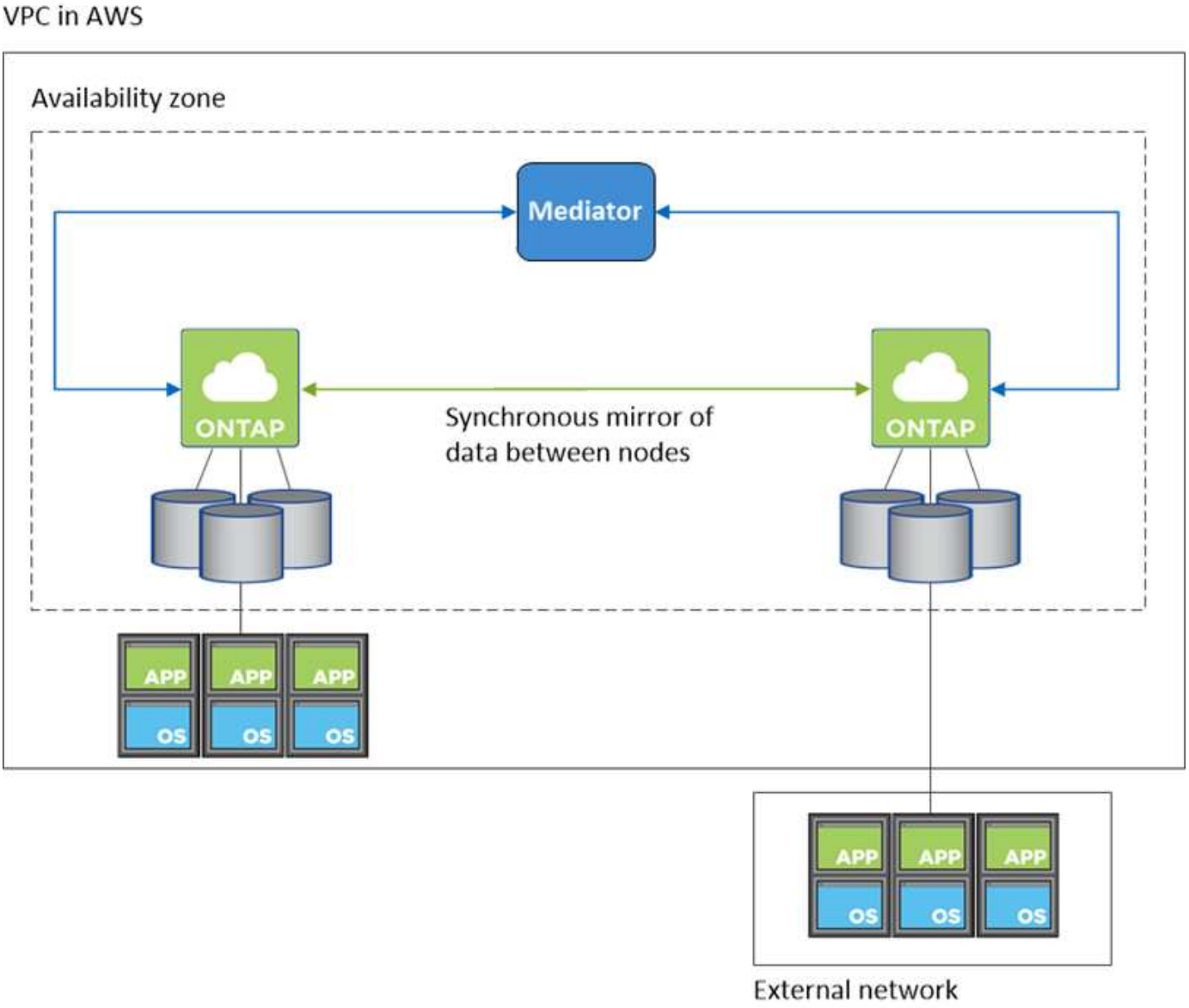
Die Implementierung einer HA-Konfiguration in einer einzelnen Verfügbarkeitszone (AZ) kann die Hochverfügbarkeit Ihrer Daten gewährleisten, wenn eine Instanz, auf der ein Cloud Volumes ONTAP Node ausgeführt wird, ausfällt. Alle Daten sind nativ von außerhalb des VPC zugänglich.

> BlueXP 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.



Takeover 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.

AWS lokale Zonen

AWS Local Zones sind eine Infrastrukturimplementierung, bei der Storage, Computing, Datenbanken und andere ausgewählte AWS Services in der Nähe von großen Städten und Branchenbereichen liegen. Mit AWS Local Zones bringen Sie AWS Services näher und verbessern so die Latenz Ihrer Workloads und pflegen Datenbanken lokal.

Sie können eine einzelne AZ- oder mehrere AZ-Konfiguration in AWS Local Zones implementieren.

> AWS Local Zones werden beim Einsatz von BlueXP im Standardmodus unterstützt. Derzeit werden AWS Lokale Zonen nicht unterstützt, wenn BlueXP im eingeschränkten Modus oder im privaten Modus verwendet wird.

Beispielkonfigurationen für die AWS Local Zone

Im Folgenden sind Beispielkonfigurationen aufgeführt:

- Einzelne Verfügbarkeitszone: Beide Clusterknoten und der Mediator befinden sich in derselben lokalen Zone.
- Verfügbarkeitszonen
  In Konfigurationen mit mehreren Verfügbarkeitszonen gibt es drei Instanzen, zwei Nodes und einen Mediator. Eine der drei Instanzen muss sich in einer separaten Zone befinden. Sie können wählen, wie Sie dies einrichten.

  Hier sind drei Beispielkonfigurationen:

  - Jeder Clusterknoten befindet sich in einer anderen lokalen Zone und der Mediator befindet sich in einer öffentlichen Verfügbarkeitszone.
  - Ein Clusterknoten in einer lokalen Zone, der Mediator in einer lokalen Zone und der zweite Clusterknoten befinden sich in einer Verfügbarkeitszone.
  - Jeder Clusterknoten und der Mediator befinden sich in separaten lokalen Zonen.

Unterstützte Festplatten- und Instanztypen

Der einzige unterstützte Festplattentyp ist GP2.

Die folgenden EC2 Instanztypen mit den Größen xlarge bis 4xlarge werden derzeit unterstützt:

- M5
- C5
- C5d
- R5
- R5d

"In AWS finden Sie die neuesten und vollständigen Details zu unterstützten EC2-Instanztypen in lokalen Zonen".

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 BlueXP beiden Nodes die gleiche Anzahl an Festplatten zu, erstellt ein gespiegeltes Aggregat und erstellt dann das neue Volume. Wenn zum Beispiel zwei Festplatten für das Volume benötigt werden, weist BlueXP zwei Festplatten

pro Node zu 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 BlueXP in der Storage System-Ansicht verwenden.

Leistungserwartungen

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.

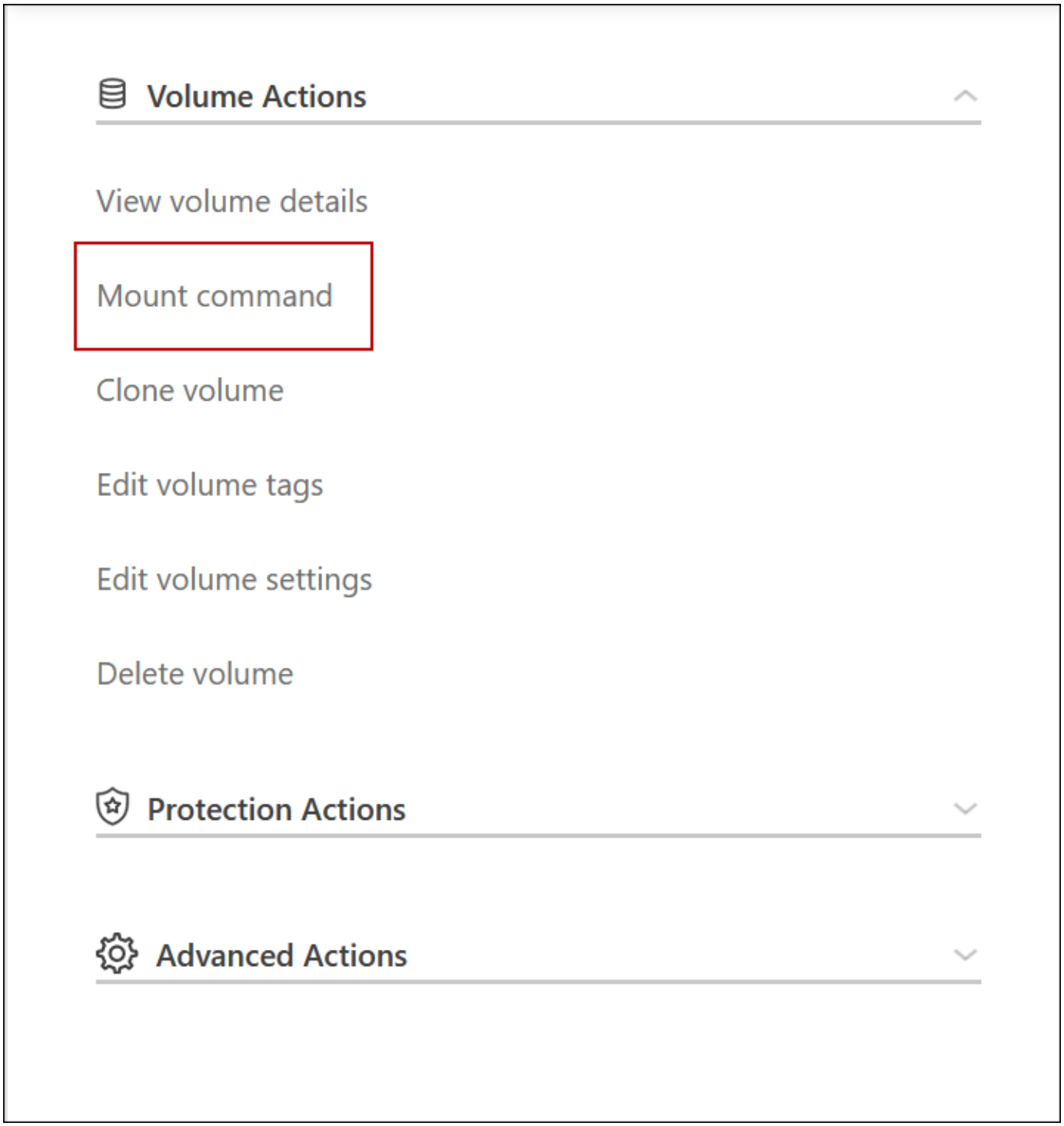
Weitere Informationen zur Performance von Cloud Volumes ONTAP finden Sie unter "Leistung".

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 die richtige IP-Adresse einfach über die Option „*Mount Command*“ im Bereich „Volumes verwalten“ in BlueXP identifizieren.



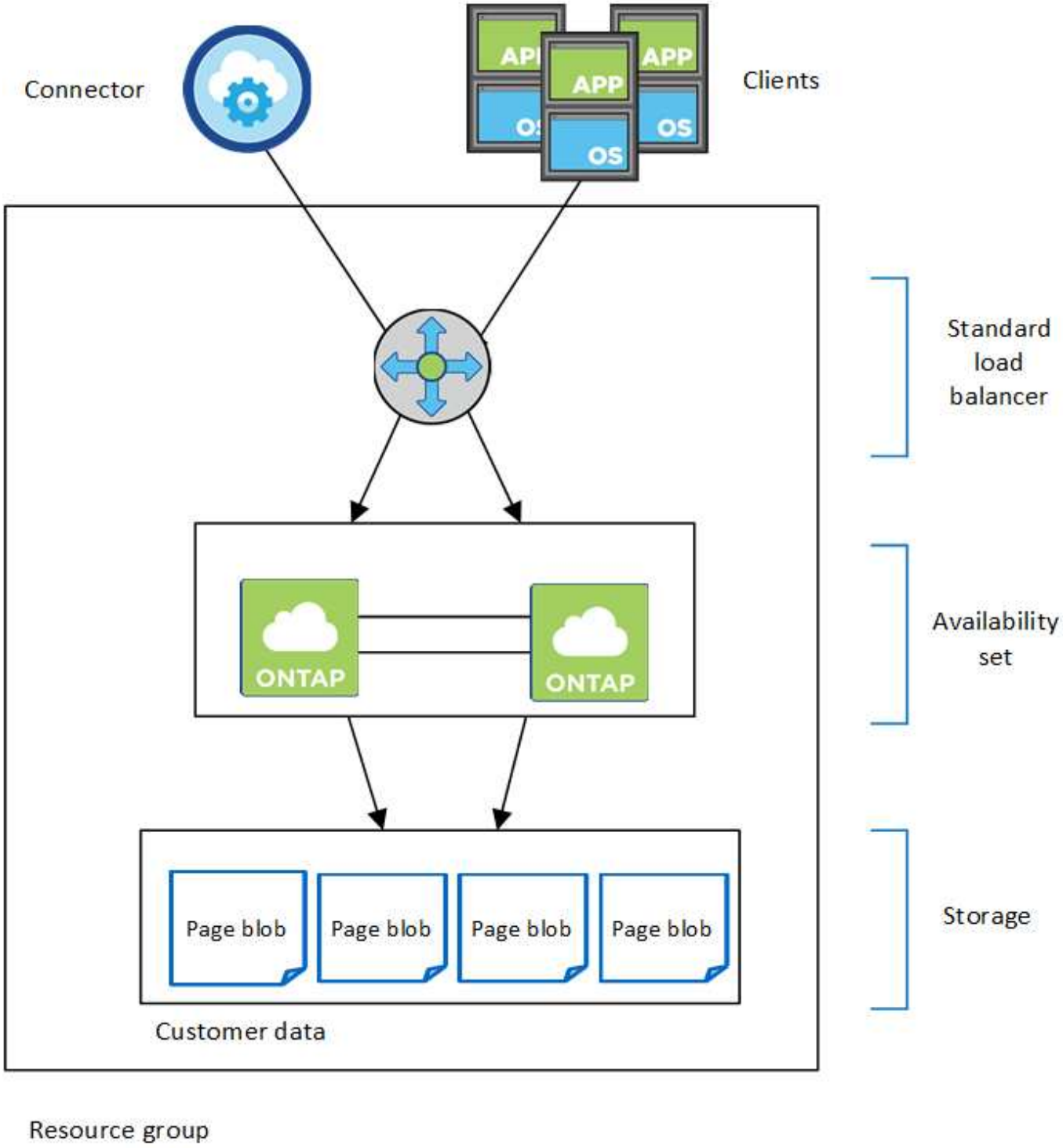
Hochverfügbarkeitspaare in Azure

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

HA-Konfiguration mit einer einzelnen Verfügbarkeitszone und Seitenlobs

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



Beachten Sie Folgendes zu den Azure Komponenten, die BlueXP für Sie implementiert:

Azure Standard Load Balancer

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

Verfügbarkeitsgruppe

Das Azure Availability Set ist eine logische Gruppierung der Cloud Volumes ONTAP Nodes. Das Verfügbarkeitsset stellt sicher, dass sich die Knoten in unterschiedlichen Fehler- und Updatedomänen befinden, um Redundanz und Verfügbarkeit zu gewährleisten. "Weitere Informationen zur Verfügbarkeit finden Sie in der Azure Dokumentation".

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

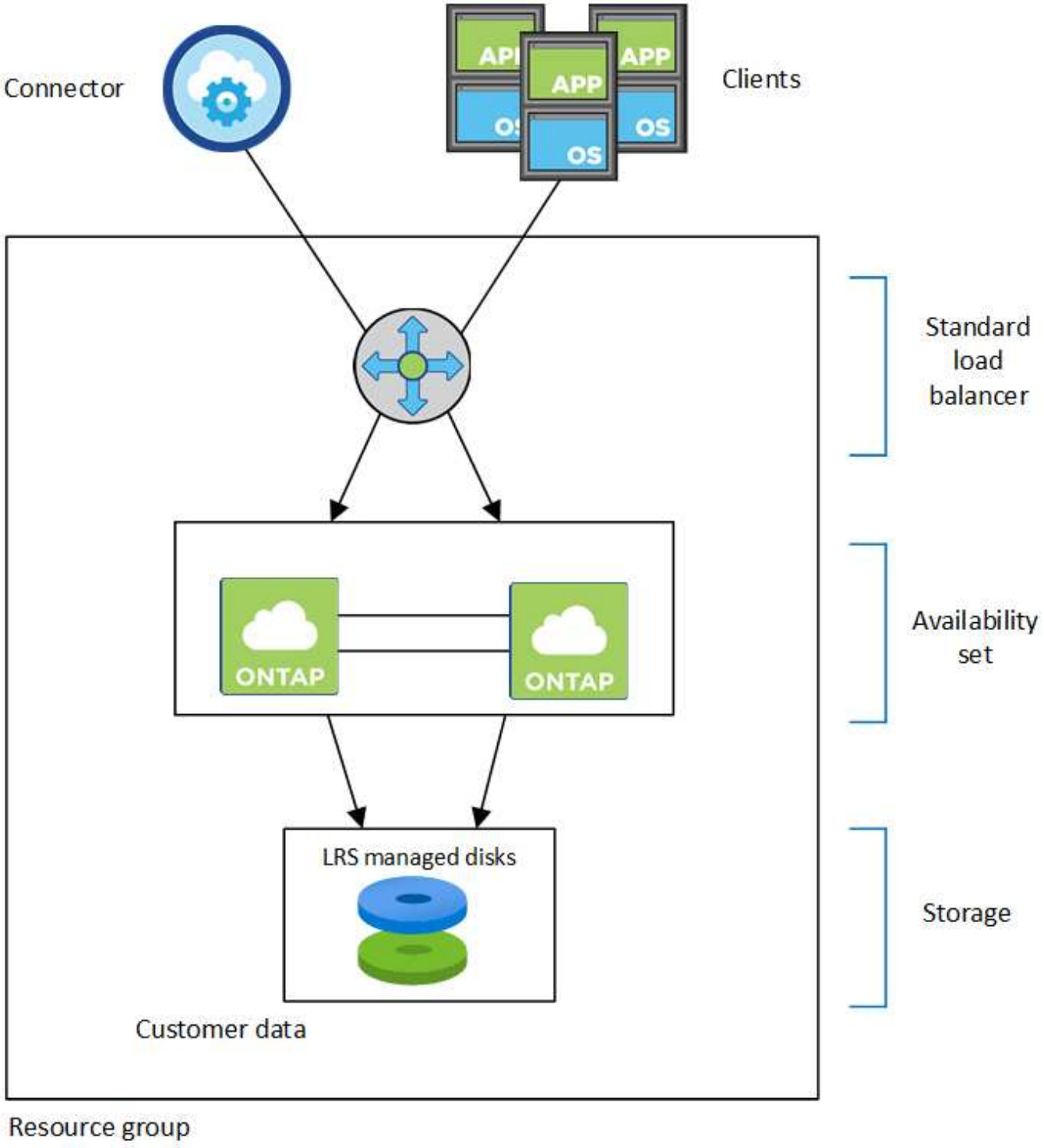
- Für verwaltete Festplatten ist ein Speicherkonto erforderlich.
- Für die Blobs auf Premium Storage-Seite sind mindestens ein Storage-Konto erforderlich, da das Kapazitätslimit pro Storage-Konto erreicht wird.

  "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 BlueXP 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.

HA-Konfiguration mit einer einzelnen Verfügbarkeitszone und gemeinsam genutzten gemanagten Festplatten

Eine Cloud Volumes ONTAP HA-Konfiguration für eine einzelne Verfügbarkeitszone, die auf gemeinsam genutzten, verwalteten Festplatten ausgeführt wird, umfasst die folgenden Komponenten:



Beachten Sie Folgendes zu den Azure Komponenten, die BlueXP für Sie implementiert:

Azure Standard Load Balancer

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

Verfügbarkeitsgruppe

Das Azure Availability Set ist eine logische Gruppierung der Cloud Volumes ONTAP Nodes. Das Verfügbarkeitsset stellt sicher, dass sich die Knoten in unterschiedlichen Fehler- und Updatedomänen befinden, um Redundanz und Verfügbarkeit zu gewährleisten. "Weitere Informationen zur Verfügbarkeit finden Sie in der Azure Dokumentation".

Festplatten

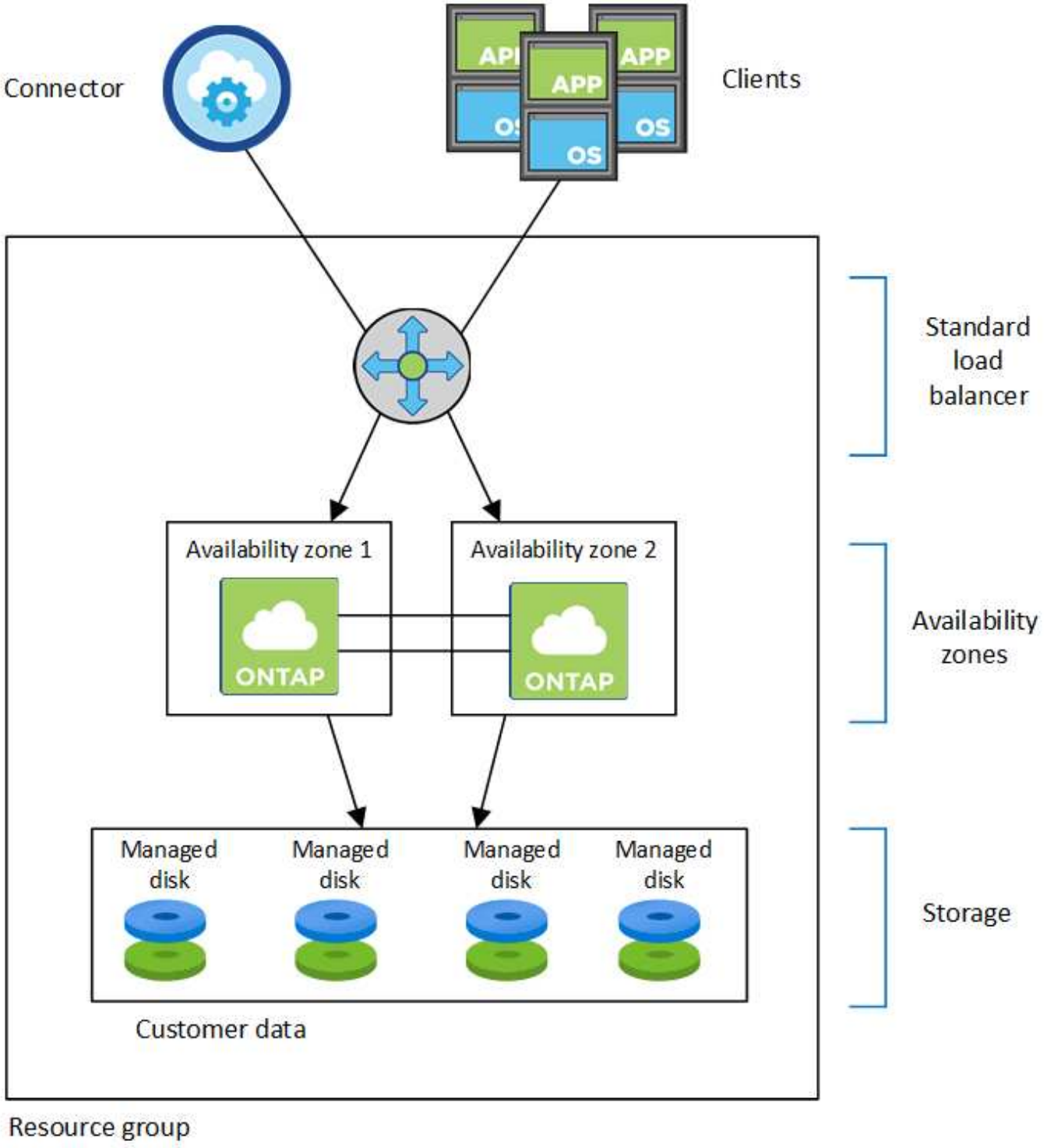
Kundendaten befinden sich auf lokal redundanten, von LRS (Storage) gemanagten Festplatten. Jeder Node hat Zugriff auf den Storage des anderen Nodes. Für ist auch zusätzlicher Speicher erforderlich "Boot-, Root-, Partner-Root-, Core- und NVRAM-Daten".

Konten mit Storage-Systemen

Storage-Konten werden für gemanagte, festplattenbasierte Implementierungen verwendet, um Diagnoseprotokolle und das Tiering an Blob-Storage zu verarbeiten.

KONFIGURATION der verschiedenen Verfügbarkeitszonen

Eine Cloud Volumes ONTAP HA Konfiguration mit mehreren Verfügbarkeitszonen in Azure umfasst die folgenden Komponenten:



Beachten Sie Folgendes zu den Azure Komponenten, die BlueXP für Sie implementiert:

Azure Standard Load Balancer

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

Verfügbarkeitszonen

Zwei Cloud Volumes ONTAP-Nodes werden in verschiedenen Verfügbarkeitszonen bereitgestellt. Verfügbarkeitszonen stellen sicher, dass sich die Nodes in unterschiedlichen Fehlerdomänen befinden. "Weitere Informationen zum zonenredundanten Azure-Speicher für verwaltete Festplatten finden Sie in den Azure-Dokumentationen".

Festplatten

Kundendaten befinden sich auf zonenredundanten Storage-Laufwerken (ZRS), die von gemanagt werden. Jeder Node hat Zugriff auf den Storage des anderen Nodes. Für ist auch zusätzlicher Speicher erforderlich "Boot-, Root-, Partner-Root- und Kerndaten".

Konten mit Storage-Systemen

Storage-Konten werden für gemanagte, festplattenbasierte Implementierungen verwendet, um Diagnoseprotokolle und das Tiering an Blob-Storage zu verarbeiten.

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.
- Die Recovery-Zeitvorgabe (RTO) beträgt 120 Sekunden. Bei einem Ausfall sollten die Daten in maximal 120 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-Übernahme, -Resynchronisierung und -Rückgabe sind standardmäßig automatisch erfolgt. Es ist keine Benutzeraktion erforderlich.

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.

Hochverfügbarkeitspaare in Google Cloud

Eine Cloud Volumes ONTAP Hochverfügbarkeitskonfiguration (HA) bietet unterbrechungsfreien Betrieb und Fehlertoleranz. In Google Cloud werden die Daten zwischen beiden Nodes synchron gespiegelt.

HA-Komponenten

Die Cloud Volumes ONTAP HA-Konfigurationen in Google Cloud umfassen 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.
- Eine Zone oder drei Zonen (empfohlen).

  Bei Auswahl von drei Zonen befinden sich die beiden Nodes und der Mediator in separaten Google Cloud Zonen.

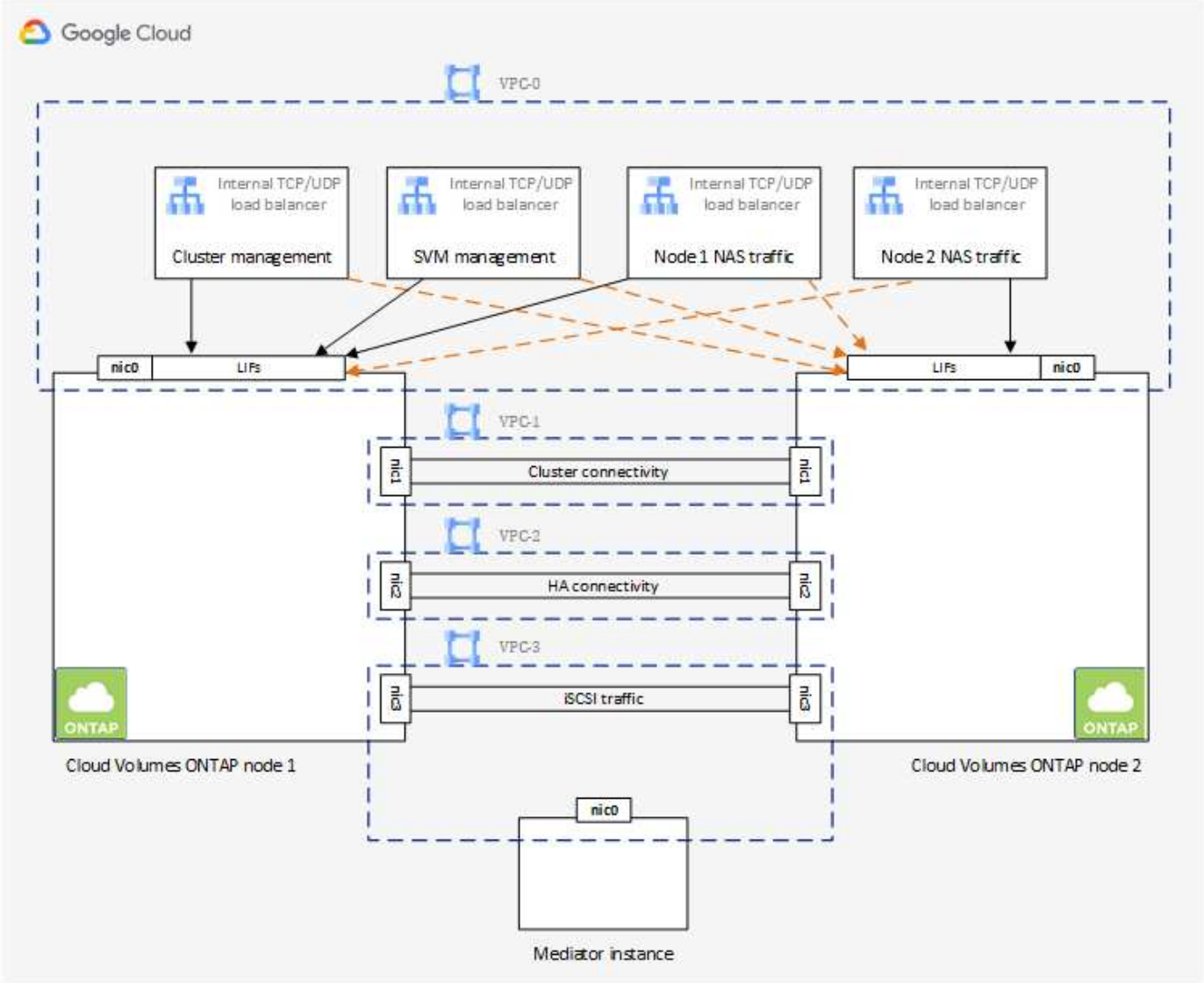
- Vier Virtual Private Clouds (VPCs):

  Bei der Konfiguration kommen vier VPCs zum Einsatz, da für GCP muss sich jede Netzwerkschnittstelle in einem separaten VPC-Netzwerk befinden.

- Vier interne Google Cloud-Load-Balancer (TCP/UDP), die den eingehenden Datenverkehr zum Cloud Volumes ONTAP-HA-Paar verwalten.

"Hier erhalten Sie Informationen zu den Netzwerkanforderungen", Darunter weitere Details zu Load Balancer, VPCs, internen IP-Adressen, Subnetzen und mehr.

Das folgende Konzept zeigt ein Cloud Volumes ONTAP HA-Paar und seine Komponenten:



Mediator

Hier einige wichtige Details zur Mediator-Instanz in Google Cloud:

Instanztyp

e2-Micro (zuvor wurde eine f1-Micro-Instanz verwendet)

Festplatten

Zwei persistente Standard-Festplatten mit 10 gib pro Laufwerk

Betriebssystem

Debian 11

Für Cloud Volumes ONTAP 9.10.0 und früher wurde Debian 10 auf dem Mediator installiert.

Upgrades

Bei einem Upgrade von Cloud Volumes ONTAP aktualisiert BlueXP auch die Mediator-Instanz nach Bedarf.

Zugriff auf die Instanz

Für Debian ist der Standard-Cloud-Benutzer `admin`. Google Cloud erstellt und fügt eine Bescheinigung für die ein `admin` Benutzer, wenn SSH-Zugriff über die Google Cloud-Konsole oder die gcloudbasierte Befehlszeile angefordert wird. Sie können angeben `sudo` Um Root-Rechte zu erhalten.

Agenten von Drittanbietern

Agents von Drittanbietern oder VM-Erweiterungen werden auf der Mediator-Instanz nicht unterstützt.

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.

Storage-Übernahme, -Resynchronisierung und -Rückgabe sind standardmäßig automatisch erfolgt. Es ist keine Benutzeraktion erforderlich.

RPO und RTO

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

- Das Recovery Point Objective (RPO) beträgt 0 Sekunden.

  Ihre Daten sind transaktionskonsistent und ohne Datenverlust.

- Die Recovery-Zeitvorgabe (RTO) beträgt 120 Sekunden.

  Bei einem Ausfall sollten die Daten in maximal 120 Sekunden verfügbar sein.

Ha-Bereitstellungsmodelle

Durch Implementierung einer HA-Konfiguration in mehreren Zonen oder in einer einzelnen Zone werden die Hochverfügbarkeit der Daten gewährleistet.

Mehrere Zonen (empfohlen)

Durch die Implementierung einer HA-Konfiguration über drei Zonen hinweg wird eine kontinuierliche Datenverfügbarkeit sichergestellt, wenn ein Ausfall innerhalb einer Zone auftritt. Beachten Sie, dass die Schreibleistung im Vergleich zu einer einzelnen Zone etwas geringer ist, aber sie ist minimal.

Einzelne Zone zu erreichen

Wenn eine Cloud Volumes ONTAP HA-Konfiguration in einer einzelnen Zone implementiert wird, kommt eine Richtlinie zur Platzierung der Verteilung zum Einsatz. Diese Richtlinie sorgt dafür, dass eine HA-Konfiguration innerhalb der Zone vor einem Single Point of Failure geschützt ist, ohne dass zur Fehlereingrenzung separate Zonen erforderlich sind.

Dieses Implementierungsmodell senkt Ihre Kosten, da zwischen den Zonen keine Kosten für den Datenausgang anfallen.

Funktionsweise von Storage in einem HA-Paar

Im Gegensatz zu einem ONTAP Cluster ist die Storage-Lösung in einem Cloud Volumes ONTAP HA-Paar in GCP nicht zwischen den Nodes gemeinsam genutzt. 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 BlueXP beiden Nodes die gleiche Anzahl an Festplatten zu, erstellt ein gespiegeltes Aggregat und erstellt dann das neue Volume. Wenn zum Beispiel zwei Festplatten für das Volume benötigt werden, weist BlueXP zwei Festplatten pro Node zu 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.

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.

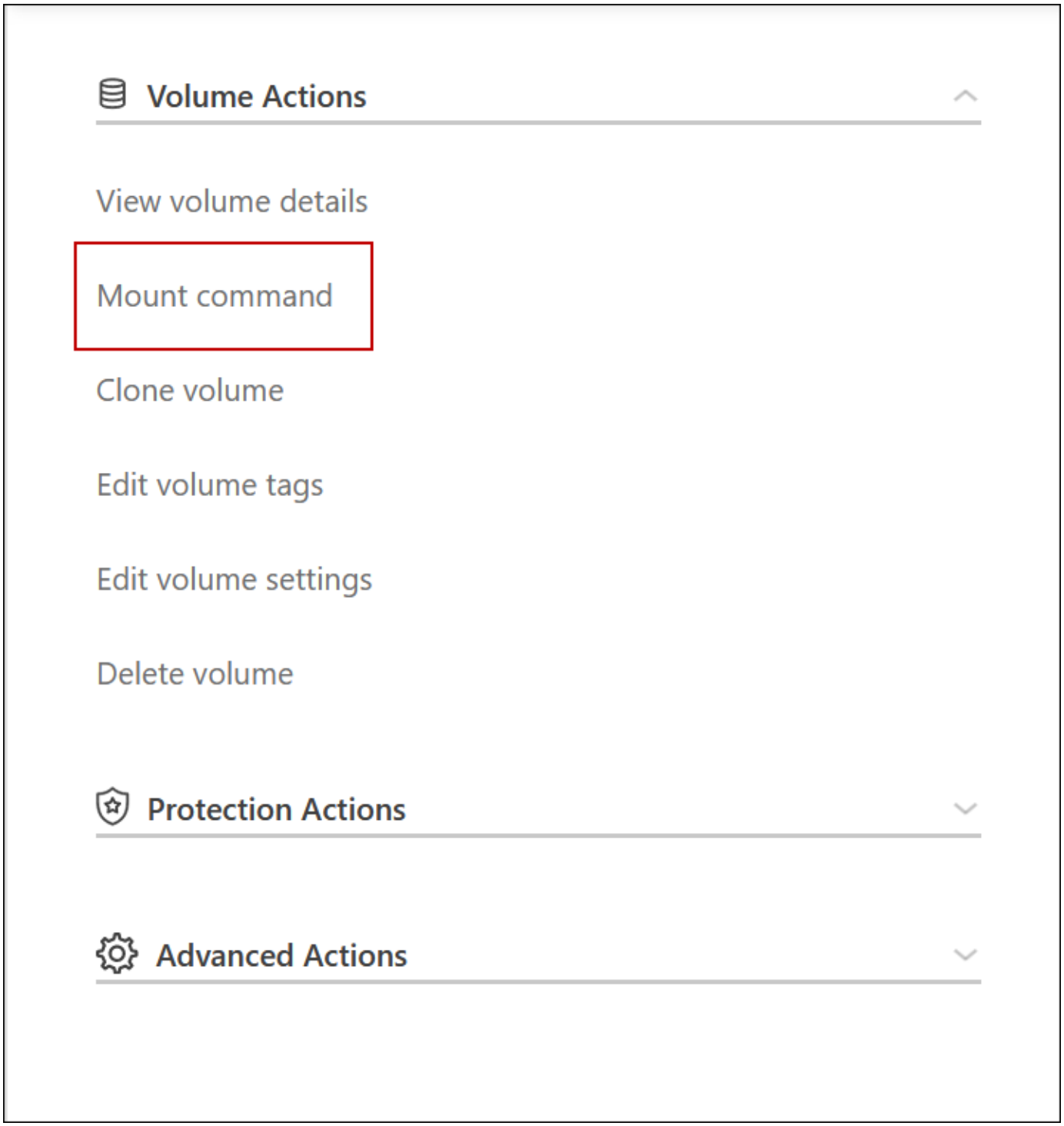
Weitere Informationen zur Performance von Cloud Volumes ONTAP finden Sie unter "Leistung".

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 die richtige IP-Adresse einfach über die Option „*Mount Command*“ im Bereich „Volumes verwalten“ in BlueXP identifizieren.



Weiterführende Links

- "Hier erhalten Sie Informationen zu den Netzwerkanforderungen"
- "Erste Schritte in GCP"

Aktionen während der Übernahme nicht verfügbar

Wenn ein Node in einem HA-Paar nicht verfügbar ist, stellt der andere Node Daten für seinen Partner bereit, um einen unterbrechungsfreien Daten-Service zu bieten. Dies wird als *Storage Takeover* bezeichnet. Bis der Rückübertragung im Storage-System

abgeschlossen ist, sind verschiedene Vorgänge nicht verfügbar.

Wenn ein Node in einem HA-Paar nicht verfügbar ist, lautet der Status der Arbeitsumgebung in BlueXP *degraded*.

Die folgenden Aktionen sind bei der Übernahme des BlueXP-Storage nicht verfügbar:

- Support-Registrierung
- Lizenzänderungen
- Änderungen am Instanz- oder VM-Typ
- Die Schreibgeschwindigkeit ändert sich
- CIFS Einrichtung
- Ändern des Speicherorts von Konfigurations-Backups
- Einstellen des Cluster-Passworts
- Managen von Festplatten und Aggregaten (erweiterte Zuweisung)

Diese Aktionen sind wieder verfügbar, nachdem das Storage-Giveback abgeschlossen ist und der Status der Arbeitsumgebung sich wieder auf „Normal“ ändert.

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 vom Cloud-Provider 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 "NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE)". NVE und NAE sind softwarebasierte Lösungen, mit denen die Verschlüsselung von Volumes im Ruhezustand (FIPS) 140-2-konform unterstützt wird. Sowohl NVE als auch NAE nutzen 256-Bit-Verschlüsselung nach AES.

- 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 werden von einem externen Schlüsselmanager unterstützt.

Neue Aggregate haben NetApp Aggregate Encryption (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)". BlueXP fordert Datenschlüssel mit einem Kundenstammschlüssel (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

Die Daten werden auf Cloud Volumes ONTAP in Azure automatisch verschlüsselt "Azure Storage Service Encryption" Mit einem von Microsoft gemanagten Schlüssel

Sie können Ihre eigenen Schlüssel verwenden. "Erfahren Sie, wie Sie Cloud Volumes ONTAP einrichten und einen vom Kunden gemanagten Schlüssel in Azure verwenden".

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 mit BlueXP APIs ein Cloud Volumes ONTAP-System erstellen, das *vom Kunden verwaltete 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".

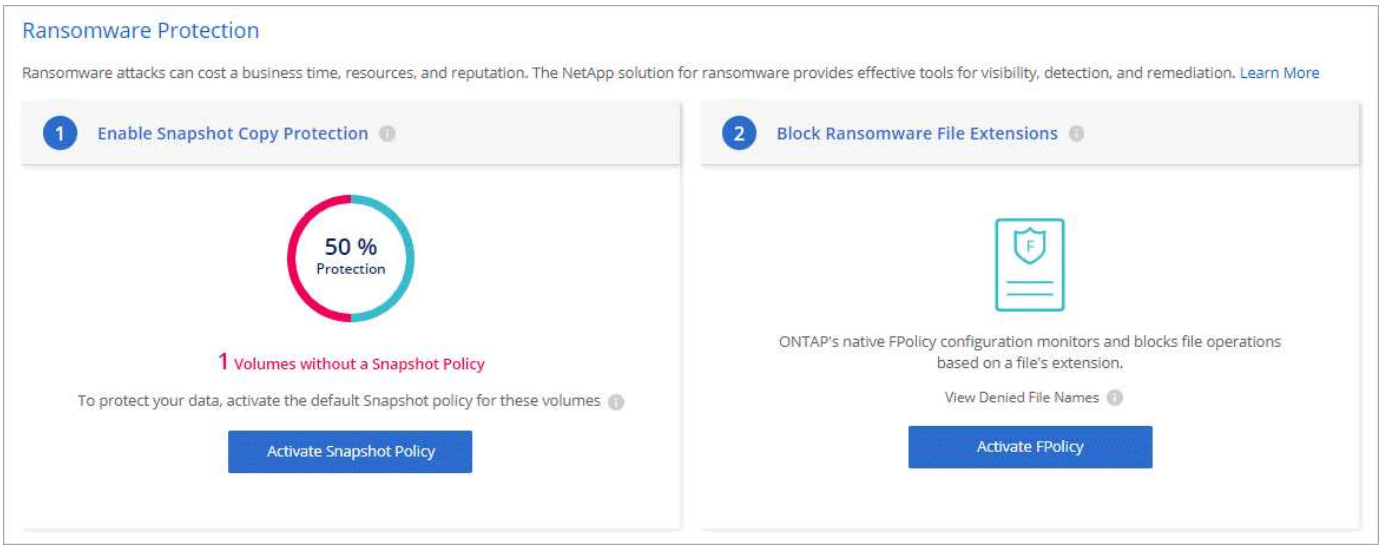
Schutz durch Ransomware

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

- BlueXP identifiziert Volumes, die nicht durch eine Snapshot-Richtlinie geschützt sind, und ermöglicht Ihnen die Aktivierung der standardmäßigen 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.

- BlueXP ermöglicht Ihnen auch, gängige Ransomware-Dateiendungen durch die Aktivierung der FPolicy-Lösung von ONTAP 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.

Technische Berichte zur Performance

- 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"

CPU-Performance

Cloud Volumes ONTAP-Nodes weisen eine hohe Auslastung (über 90 %) von den Monitoring-Tools Ihres Cloud-Providers auf. Dies liegt daran, dass ONTAP alle vCPUs, die der Virtual Machine zur Verfügung gestellt werden, so dass sie nach Bedarf verfügbar sind.

Hilfe finden Sie im "NetApp Knowledgebase Artikel dazu, wie die ONTAP-CPU-Auslastung mit der CLI überwacht wird"

Lizenzmanagement für Node-basiertes BYOL

Für jedes Cloud Volumes ONTAP System mit einem Node-basierten BYOL muss eine Systemlizenz mit einem aktiven Abonnement installiert werden. BlueXP vereinfacht den Prozess durch die Verwaltung von Lizenzen für Sie und durch das Anzeigen einer Warnung vor deren Ablauf.

Eine Node-basierte Lizenz ist das BYOL-Modell der vorherigen Generation für Cloud Volumes ONTAP. Eine Node-basierte Lizenz ist nur für Lizenzerneuerungen verfügbar.

"Erfahren Sie mehr über Cloud Volumes ONTAP Lizenzoptionen".

"Erfahren Sie mehr über das Management Node-basierter Lizenzen".

Byol-Systemlizenzen

Eine Node-basierte Lizenz bietet bis zu 368 tib Kapazität für ein einzelnes Node- oder HA-Paar.

Sie können mehrere Lizenzen für ein Cloud Volumes ONTAP BYOL-System erwerben, um mehr als 368 tib Kapazität zuzuweisen. Beispielsweise können Sie zwei Lizenzen erwerben, um Cloud Volumes ONTAP bis zu 736 tib Kapazität zuzuweisen. Alternativ können Sie vier Lizenzen erwerben, um bis zu 1.4 PiB 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 Node-basiertes BYOL-System erstellen, werden Sie von BlueXP zur Seriennummer Ihrer Lizenz und zum NetApp Support Site Konto aufgefordert. BlueXP nutzt das Konto, um die Lizenzdatei von NetApp

herunterzuladen und auf dem Cloud Volumes ONTAP System zu installieren.

"Erfahren Sie, wie Sie BlueXP um NetApp Support Site Konten erweitern".

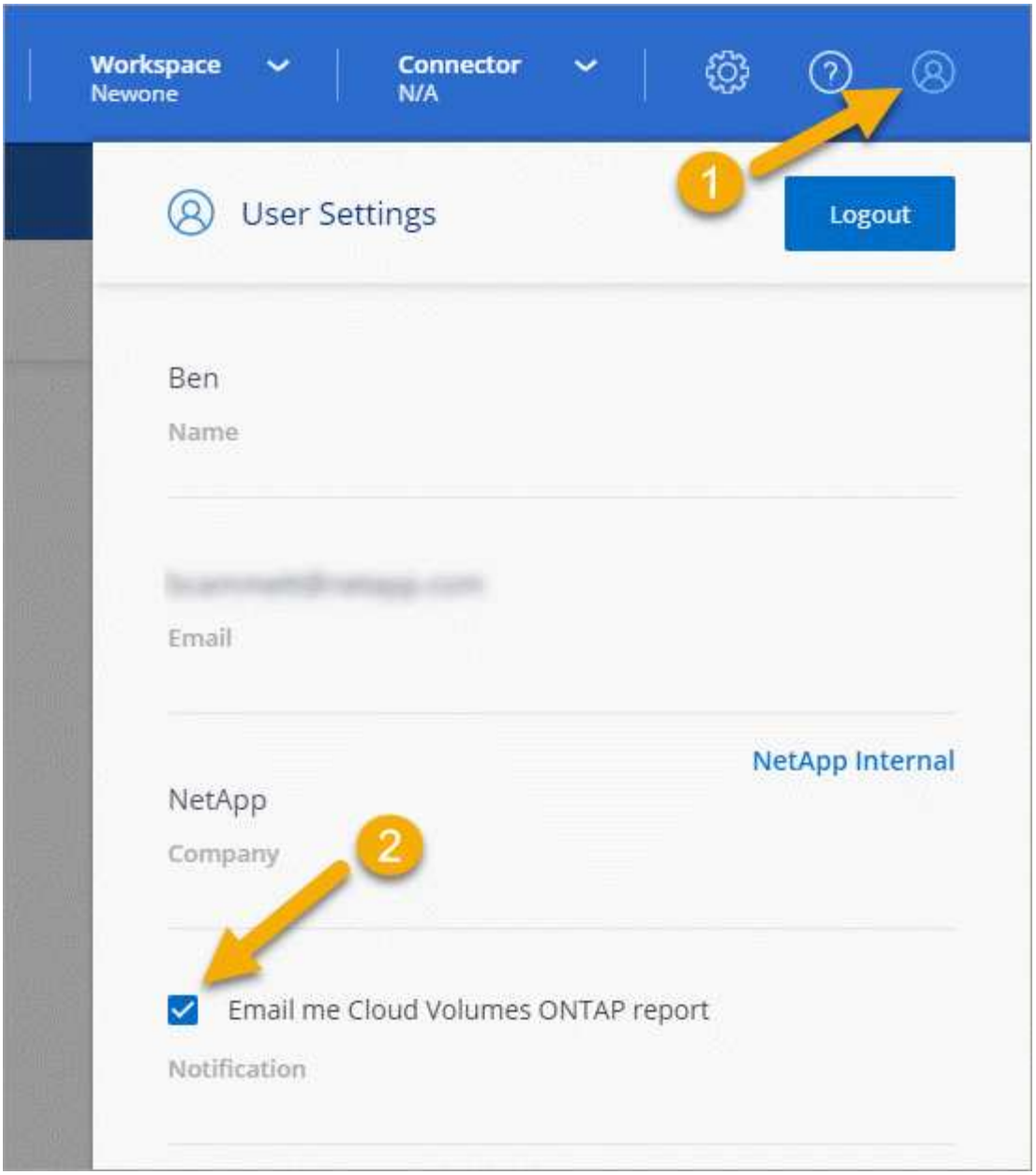
Wenn BlueXP über die sichere Internetverbindung nicht auf die Lizenzdatei zugreifen kann, können Sie dies auch tun "Holen Sie sich die Datei selbst ein und laden Sie die Datei anschließend manuell auf BlueXP hoch".

Ablauf der Lizenz

BlueXP zeigt eine Warnung an, die 30 Tage vor Ablauf einer knotenbasierten Lizenz und erneut nach Ablauf der Lizenz erfolgt. Das folgende Bild zeigt eine 30-tägige Warnung zum Ablauf, die in der Benutzeroberfläche angezeigt wird:

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

BlueXP enthält eine Warnung zum Ablauf der Lizenz im Cloud Volumes ONTAP-Bericht, die Ihnen per E-Mail zugesandt wurde, falls Sie als Kontoadministrator berechtigt sind und Sie die Option aktiviert haben:



Der E-Mail-Bericht enthält die Warnmeldung zum Ablauf der Lizenz alle zwei Wochen.

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

Lizenzerneuerung

Wenn Sie ein Node-basiertes BYOL-Abonnement verlängern, indem Sie sich an einen NetApp Vertreter wenden, erhält BlueXP automatisch die neue Lizenz von NetApp und installiert sie auf dem Cloud Volumes ONTAP System.

Wenn BlueXP über die sichere Internetverbindung nicht auf die Lizenzdatei zugreifen kann, können Sie dies auch tun "Holen Sie sich die Datei selbst ein und laden Sie die Datei anschließend manuell auf BlueXP hoch".

Lizenzübertragung auf ein neues System

Eine Node-basierte BYOL-Lizenz ist auf Cloud Volumes ONTAP Systeme übertragbar, wenn Sie ein vorhandenes System löschen und dann mit derselben Lizenz ein neues erstellen.

So können Sie beispielsweise ein vorhandenes Lizenzsystem löschen und die Lizenz anschließend mit einem neuen BYOL-System in einem anderen VPC/vnet- oder Cloud-Provider verwenden. Beachten Sie, dass nur *Cloud-unabhängige* Seriennummern bei jedem Cloud-Provider funktionieren. Die cloudunabhängigen Seriennummern beginnen mit dem Präfix *908xxxx*.

Es ist wichtig zu beachten, dass Ihre BYOL-Lizenz an Ihr Unternehmen und einen spezifischen Satz von NetApp Support Site Zugangsdaten gebunden ist.

AutoSupport und Active IQ Digital Advisor

Die AutoSupport-Komponente von ONTAP erfasst Telemetrie und sendet diese zur Analyse. Active IQ Digital Advisor analysiert die Daten von AutoSupport und bietet proaktive Betreuung und Optimierung. Mithilfe künstlicher Intelligenz erkennt Active IQ potenzielle Probleme und löst sie, bevor sie sich auf das Geschäft auswirken.

Mit Active IQ optimieren Kunden ihre Dateninfrastruktur in der gesamten globalen Hybrid Cloud. Dazu bieten sie konkrete prädiktive Analysen und proaktiven Support über ein Cloud-basiertes Portal und eine mobile App. NetApp Kunden mit aktivem SupportEdge-Vertrag profitieren von Daten-fokussierten Einblicken und Empfehlungen von Active IQ (Funktionen variieren je nach Produkt- und Support-Tier).

Folgende Möglichkeiten bietet Active IQ:

- Planung von Upgrades:

  Active IQ erkennt Probleme in Ihrer Umgebung, die durch ein Upgrade auf eine neuere Version von ONTAP behoben werden können, und die Upgrade Advisor Komponente unterstützt Sie bei der Planung eines erfolgreichen Upgrades.

- Sehen Sie sich das Wellness-System an.

  Ihr Active IQ Dashboard meldet alle Probleme im Zusammenhang mit dem Wellness-Bereich und hilft Ihnen, diese Probleme zu beheben. Überwachen Sie die Systemkapazität, um sicherzugehen, dass nie mehr Speicherplatz belegt wird. Zeigen Sie Support-Cases für Ihr System an.

- Performance-Management:

  Active IQ zeigt die System-Performance über einen längeren Zeitraum an, als Sie im ONTAP System Manager sehen können. Identifizieren Sie Konfigurations- und Systemprobleme, die Ihre Performance beeinträchtigen. Maximale Effizienz Anzeige von Storage-Effizienz-Metriken und Identifizierung von Möglichkeiten, mehr Daten auf weniger Speicherplatz zu speichern

- Anzeige von Inventar und Konfiguration

  Active IQ zeigt vollständige Informationen zur Bestands- und Software- und Hardwarekonfiguration an. Prüfen Sie, wann die Serviceverträge ablaufen und verlängern Sie sie, um sicherzustellen, dass der Support weiterhin gewährleistet ist.

Verwandte Informationen

- "NetApp Dokumentation: Active IQ Digital Advisor"
- "Starten Sie Active IQ"
- "SupportEdge Services"

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.

Standardeinrichtung

- BlueXP erstellt bei der Bereitstellung von Cloud Volumes ONTAP eine Storage-VM für Daten, die mit Daten arbeitet. Einige Konfigurationen unterstützen zusätzliche Storage VMs. "Erfahren Sie mehr über das Management von Storage VMs".

  Ab Version BlueXP 3.9.5 ist die Erstellung des logischen Speicherberichtes auf der ursprünglichen Speicher-VM aktiviert. Wenn der Speicherplatz logisch gemeldet wird, meldet ONTAP den Volume-Speicherplatz, sodass der gesamte durch die Storage-Effizienzfunktionen eingesparte physische Speicherplatz ebenfalls in seiner Nutzung gemeldet wird.

- BlueXP installiert automatisch die folgenden ONTAP-Funktionslizenzen auf Cloud Volumes ONTAP:
  - CIFS
  - FlexCache
  - FlexClone
  - ISCSI
  - Mandantenfähiges Verschlüsselungsmanagement (MTEKM) ab Cloud Volumes ONTAP 9.12.1 GA
  - 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
- Eine SVM-Management-LIF auf HA-Systemen in Azure
- Eine SVM-Management-LIF auf HA-Systemen in Google Cloud
- Eine SVM-Management-LIF auf Single-Node-Systemen in AWS
- Eine Node Management-LIF

+ in Google Cloud wird diese LIF mit dem intercluster LIF kombiniert.

- Eine iSCSI-Daten-LIF

- Eine CIFS- und NFS-Daten-LIF

> Das LIF-Failover ist für Cloud Volumes ONTAP standardmäßig aufgrund von Anforderungen des Cloud-Providers 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 HTTP an den Connector.

    Auf die Backups kann von http://ipaddress/occm/offboxconfig/ zugegriffen werden, wobei *ipaddress* die IP-Adresse des Connector-Hosts ist.

  - BlueXP setzt einige Volume-Attribute anders als andere Managementtools (z. B. System Manager oder die CLI).

    In der folgenden Tabelle sind die Volume-Attribute aufgeführt, die BlueXP anders als die Standardwerte setzt:

Attribut	Von BlueXP festgesetzt
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

+
Siehe "ONTAP_Volume create_ man page" Weitere Informationen zu diesen Attributen.

Interne Festplatten für Systemdaten

Neben dem Speicher für Benutzerdaten kauft BlueXP auch Cloud-Speicher für Systemdaten ein.

AWS

- Drei Festplatten pro Node für Boot-, Root- und Core-Daten:
  - 47 gib io1-Festplatte für Boot-Daten
  - 140 gib gp3-Festplatte für Stammdaten
  - 540 gib gp2-Festplatte für Core-Daten
- Bei HA-Paaren sind zwei st1-EBS-Volumes für die Mediator-Instanz, die ca. 8 gib und 4 gib betragen, sowie eine zusätzliche gp3-Festplatte mit 140 gib in jedem Node, die eine Kopie der Root-Daten des

anderen Node enthalten soll.

In einigen Zonen kann der verfügbare EBS-Festplattentyp nur gp2 sein.

- Ein EBS-Snapshot für jede Boot- und Root-Festplatte

  Snapshots werden beim Neustart automatisch erstellt.

- 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.

In AWS befindet sich NVRAM auf der Boot-Festplatte.

Azure (Single Node)

- Drei Premium-SSD-Festplatten:
  - Eine 10 gib Festplatte für Boot-Daten
  - Eine 140 gib-Festplatte für Root-Daten
  - Eine 512 gib-Festplatte für NVRAM

    Wenn die für Cloud Volumes ONTAP ausgewählte virtuelle Maschine Ultra SSDs unterstützt, verwendet das System statt einer Premium-SSD eine 32 gib Ultra SSD für NVRAM.
- Eine 1024 gib Standard-Festplatte zum Speichern der Kerne
- Ein Azure Snapshot für jedes Boot- und Root-Laufwerk
- Jede Festplatte ist standardmäßig in Azure verschlüsselt.

Azure (HA-Paar)

HA-Paare mit Seite Blob

- Zwei 10 gib Premium-SSD-Festplatten für das Boot-Volume (eine pro Node)
- Zwei Blobs für 140 gib Premium Storage für das Root-Volume (eine pro Node)
- Zwei 1024 gib Standard-HDD-Festplatten für das Speichern von Cores (eine pro Node)
- Zwei 512 gib Premium-SSD-Festplatten für NVRAM (eine pro Node)
- Ein Azure Snapshot für jedes Boot- und Root-Laufwerk

  Snapshots werden beim Neustart automatisch erstellt.

- Jede Festplatte ist standardmäßig in Azure verschlüsselt.

HA-Paare mit gemeinsam genutzten verwalteten Festplatten in mehreren Verfügbarkeitszonen

- Zwei 10 gib Premium-SSD-Festplatten für das Boot-Volume (eine pro Node)
- Zwei Blobs für 512 gib Premium Storage für das Root-Volume (eine pro Node)
- Zwei 1024 gib Standard-HDD-Festplatten für das Speichern von Cores (eine pro Node)

- Zwei 512 gib Premium-SSD-Festplatten für NVRAM (eine pro Node)
- Ein Azure Snapshot für jedes Boot- und Root-Laufwerk

  Snapshots werden beim Neustart automatisch erstellt.

- Jede Festplatte ist standardmäßig in Azure verschlüsselt.

Google Cloud (Single-Node)

- Eine 10 gib SSD persistente Festplatte für Boot-Daten
- Eine persistente SSD-Festplatte mit 64 gib für Root-Daten
- Eine persistente SSD-Festplatte mit 500 gib für NVRAM
- Eine persistente Platte mit 315 gib Standard zum Speichern von Kernen
- Snapshots für Boot- und Root-Daten

  Snapshots werden beim Neustart automatisch erstellt.

- Boot- und Root-Festplatten sind standardmäßig verschlüsselt.

Google Cloud (HA-Paar)

- Zwei persistente SSD-Festplatten mit 10 gib für Boot-Daten
- Vier persistente 64 gib SSD-Festplatte für Root-Daten
- Zwei persistente SSD-Festplatte mit 500 gib für NVRAM
- Zwei persistente 315 gib Standard-Festplatte zum Speichern von Cores
- Eine persistente 10 gib-Standardfestplatte für Mediator-Daten
- Eine persistente 10 gib Standard-Festplatte für den Mediator: Boot-Daten
- Snapshots für Boot- und Root-Daten

  Snapshots werden beim Neustart automatisch erstellt.

- Boot- und Root-Festplatten sind standardmäßig verschlüsselt.

Wo sich die Festplatten befinden

BlueXP 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.

Wissen und Support

Für den Support anmelden

Für den Support von BlueXP und seinen Storage-Lösungen und Services ist eine Support-Registrierung erforderlich. Um wichtige Workflows für Cloud Volumes ONTAP Systeme zu ermöglichen, ist außerdem eine Support-Registrierung erforderlich.

Durch die Registrierung für den Support wird die NetApp-Unterstützung für einen Fileservice eines Cloud-Providers nicht aktiviert. Technischen Support zu Fileservices von Cloud-Providern, zu seiner Infrastruktur oder zu beliebigen Lösungen, die den Service verwenden, finden Sie im Abschnitt „Hilfe erhalten“ in der BlueXP Dokumentation zu diesem Produkt.

- "Amazon FSX für ONTAP"
- "Azure NetApp Dateien"
- "Cloud Volumes Service für Google Cloud"

Übersicht über die Support-Registrierung

Es gibt zwei Registrierungsformulare, um die Support-Berechtigung zu aktivieren:

- Registrieren Ihres BlueXP-Konto-ID-Support-Abonnements (Ihre 20-stellige Seriennummer 960xxxxxxxxx auf der Seite Support-Ressourcen in BlueXP).

  Dies dient als Ihre einzige Support-Abonnement-ID für jeden Service in BlueXP. Jedes BlueXP-Abonnement für Support auf Kontoebene muss registriert werden.

- Registrieren der Cloud Volumes ONTAP Seriennummern für ein Abonnement auf dem Markt Ihres Cloud-Providers (dies sind 20-stellige Seriennummern von 909201xxxxxx).

  Diese Seriennummern werden als *PAYGO Seriennummern* bezeichnet und werden zum Zeitpunkt der Cloud Volumes ONTAP Implementierung von BlueXP generiert.

Durch das Registrieren beider Arten von Seriennummern können Kunden Funktionen wie das Öffnen von Support-Tickets und die automatische Erstellung von Support-Cases nutzen. Die Registrierung ist abgeschlossen, indem wie unten beschrieben Konten der NetApp Support Website (NSS) zu BlueXP hinzugefügt werden.

Registrieren Sie Ihr BlueXP Konto für NetApp Support

Um sich für den Support zu registrieren und die Supportberechtigung zu aktivieren, muss ein Benutzer in Ihrem BlueXP Konto ein NetApp Support Site Konto mit seinen BlueXP Anmeldedaten verknüpfen. Wie Sie sich für den NetApp Support registrieren, hängt davon ab, ob Sie bereits über einen NSS Account (NetApp Support Site) verfügen.

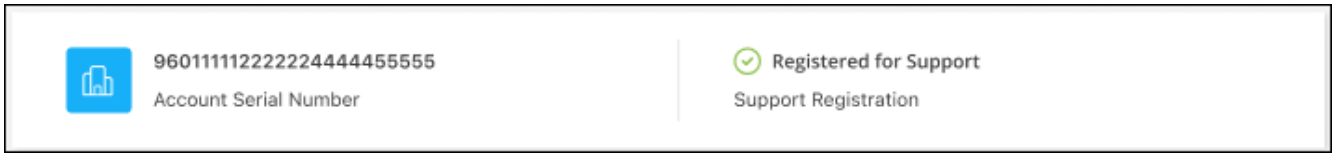
Bestandskunde mit NSS-Konto

Wenn Sie ein NetApp Kunde mit einem NSS-Konto sind, müssen Sie sich lediglich für den Support über BlueXP registrieren.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.
2. Wählen Sie **Benutzeranmeldeinformationen**.
3. Wählen Sie **NSS-Anmeldeinformationen hinzufügen** und folgen Sie der Eingabeaufforderung für die NetApp-Support-Website (NSS)-Authentifizierung.
4. Um zu bestätigen, dass die Registrierung erfolgreich war, wählen Sie das Hilfesymbol und dann **Support**.

   Auf der Seite **Ressourcen** sollte angezeigt werden, dass Ihr Konto für Support registriert ist.



   Beachten Sie, dass andere BlueXP Benutzer diesen Support-Registrierungsstatus nicht sehen, wenn sie ihrem BlueXP Login kein NetApp Support Site Konto zugeordnet haben. Das bedeutet jedoch nicht, dass Ihr BlueXP Konto nicht für den Support registriert ist. Solange ein Benutzer im Konto diese Schritte befolgt hat, wurde Ihr Konto registriert.

Vorhandener Kunde, aber kein NSS-Konto

Wenn Sie bereits NetApp Kunde sind und über vorhandene Lizenzen und Seriennummern sowie *No* NSS Konto verfügen, müssen Sie ein NSS Konto erstellen und es Ihren BlueXP Anmeldedaten zuordnen.

Schritte

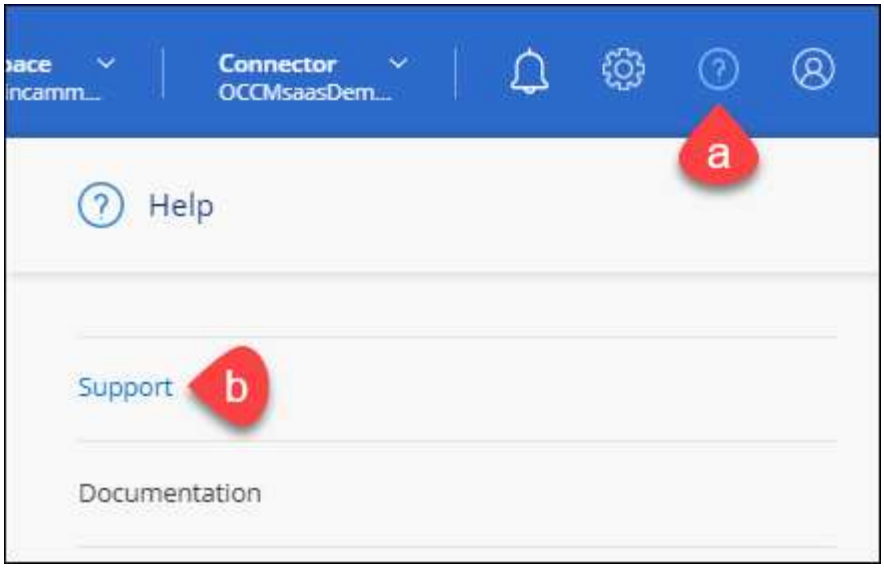
1. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen "NetApp Support Site-Formular zur Benutzerregistrierung"
   a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
   b. Kopieren Sie unbedingt die oben verwendete BlueXP-Kontonummer (960xxxx) für das Feld Seriennummer. Dadurch wird die Kontobearbeitung beschleunigt.
2. Ordnen Sie Ihr neues NSS-Konto Ihrer BlueXP Anmeldung zu, indem Sie die unter aufgeführten Schritte durchführen Bestandskunde mit NSS-Konto.

Neu bei NetApp

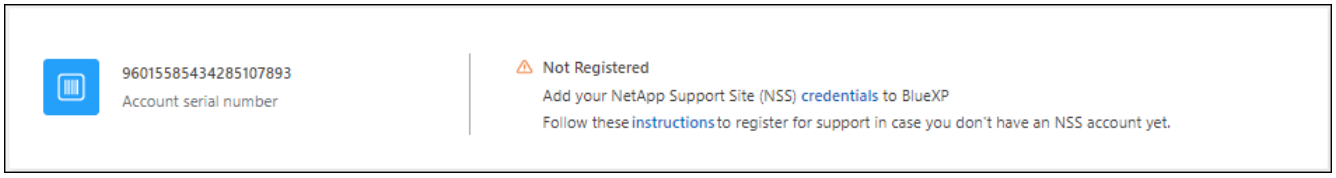
Wenn Sie neu bei NetApp sind und über keinen NSS-Account verfügen, befolgen Sie jeden Schritt unten.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.



2. Suchen Sie auf der Seite für die Support-Registrierung die Seriennummer Ihres Kontos.



3. Navigieren Sie zu "Die Support-Registrierungs-Website von NetApp" Und wählen Sie **Ich bin kein registrierter NetApp Kunde**.
4. Füllen Sie die Pflichtfelder aus (mit roten Sternchen).
5. Wählen Sie im Feld **Product Line** die Option **Cloud Manager** aus, und wählen Sie dann den gewünschten Abrechnungsanbieter aus.
6. Kopieren Sie die Seriennummer des Kontos von Schritt 2 oben, füllen Sie die Sicherheitsprüfung aus und bestätigen Sie dann, dass Sie die globale Datenschutzrichtlinie von NetApp lesen.

   Zur Fertigstellung dieser sicheren Transaktion wird sofort eine E-Mail an die angegebene Mailbox gesendet. Überprüfen Sie Ihre Spam-Ordner, wenn die Validierungs-E-Mail nicht in wenigen Minuten ankommt.

7. Bestätigen Sie die Aktion in der E-Mail.

   Indem Sie Ihre Anfrage an NetApp senden, wird Ihnen die Erstellung eines NetApp Support Site Kontos empfohlen.

8. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen "NetApp Support Site-Formular zur Benutzerregistrierung"
   a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
   b. Kopieren Sie die oben angegebene Seriennummer (960xxxx) für das Feld „Seriennummer“. Dadurch wird die Kontobearbeitung beschleunigt.

Nachdem Sie fertig sind

NetApp sollte sich bei diesem Prozess mit Ihnen in Verbindung setzen. Dies ist eine einmalige Onboarding-Übung für neue Benutzer.

Wenn Sie über Ihren NetApp Support Site Account verfügen, ordnen Sie das Konto Ihrer BlueXP Anmeldung zu, indem Sie die Schritte unter ausführen Bestandskunde mit NSS-Konto.

Verknüpfen von NSS-Anmeldeinformationen für den Cloud Volumes ONTAP-Support

Um die folgenden wichtigen Workflows für Cloud Volumes ONTAP zu ermöglichen, müssen die Zugangsdaten für die NetApp Support Website mit Ihrem BlueXP Konto verknüpft werden:

- Registrieren von Pay-as-you-go Cloud Volumes ONTAP Systemen für Support

  Die Bereitstellung Ihres NSS Kontos ist erforderlich, um Support für Ihr System zu aktivieren und Zugang zu den technischen Support-Ressourcen von NetApp zu erhalten.

- Implementierung von Cloud Volumes ONTAP unter Verwendung von BYOL (Bring-Your-Own-License)

  Die Bereitstellung Ihres NSS-Kontos ist erforderlich, damit BlueXP Ihren Lizenzschlüssel hochladen und das Abonnement für den von Ihnen erworbenen Zeitraum aktivieren kann. Dies schließt automatische Updates für Vertragsverlängerungen ein.

- Aktualisieren der Cloud Volumes ONTAP Software auf die neueste Version

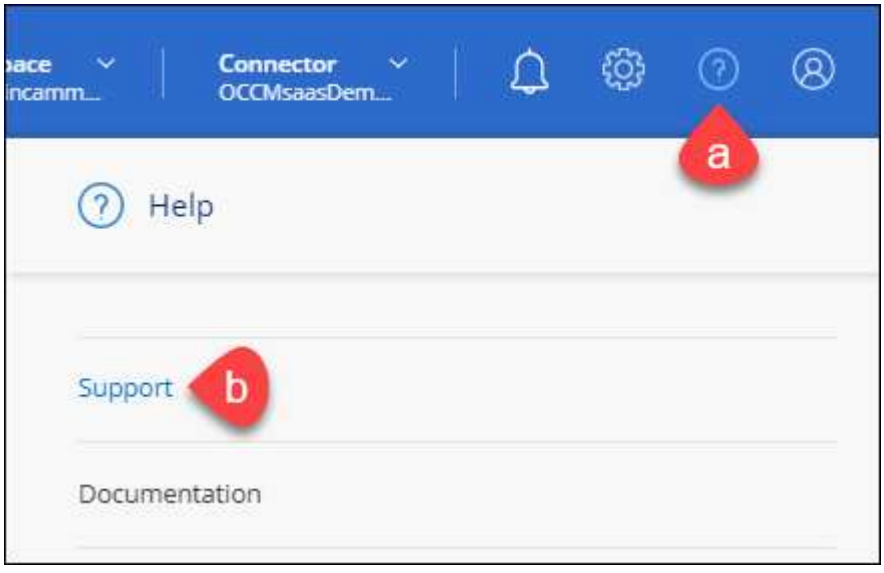
Das Zuordnen der NSS-Anmeldedaten zu Ihrem BlueXP Konto unterscheidet sich von dem NSS-Konto, das mit einer BlueXP Benutzeranmeldung verknüpft ist.

Diese NSS-Zugangsdaten sind mit Ihrer spezifischen BlueXP Konto-ID verknüpft. Benutzer, die zum BlueXP Konto gehören, können über **Support > NSS Management** auf diese Anmeldedaten zugreifen.

- Wenn Sie über ein Konto auf Kundenebene verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen.
- Wenn Sie einen Partner- oder Reseller-Account haben, können Sie ein oder mehrere NSS-Konten hinzufügen, können aber nicht neben Kunden-Level Accounts hinzugefügt werden.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.



2. Wählen Sie **NSS-Verwaltung > NSS-Konto hinzufügen**.
3. Wenn Sie dazu aufgefordert werden, wählen Sie **Weiter**, um zu einer Microsoft-Anmeldeseite umgeleitet zu werden.

   NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsservices, die speziell auf Support und Lizenzierung zugeschnitten sind.

4. Geben Sie auf der Anmeldeseite die registrierte E-Mail-Adresse und das Kennwort Ihrer NetApp Support Site an, um den Authentifizierungsvorgang durchzuführen.

   Mit diesen Aktionen kann BlueXP Ihr NSS-Konto für Dinge wie Lizenzdownloads, Softwareaktualisierungs-Verifizierung und zukünftige Support-Registrierungen verwenden.

   Beachten Sie Folgendes:

   - Das NSS-Konto muss ein Konto auf Kundenebene sein (kein Gast- oder Temporärkonto). Sie können mehrere NSS-Konten auf Kundenebene haben.
   - Es kann nur ein NSS-Konto vorhanden sein, wenn es sich bei diesem Konto um ein Partner-Level-Konto handelt. Wenn Sie versuchen, NSS-Konten auf Kundenebene hinzuzufügen und ein Konto auf Partnerebene vorhanden ist, erhalten Sie die folgende Fehlermeldung:

     „Der NSS-Kundentyp ist für dieses Konto nicht zulässig, da es bereits NSS-Benutzer unterschiedlichen Typs gibt.“

   Dasselbe gilt, wenn Sie bereits NSS-Konten auf Kundenebene haben und versuchen, ein Konto auf Partnerebene hinzuzufügen.

   - Bei der erfolgreichen Anmeldung wird NetApp den NSS-Benutzernamen speichern.

     Dies ist eine vom System generierte ID, die Ihrer E-Mail zugeordnet ist. Auf der Seite **NSS Management** können Sie Ihre E-Mail über anzeigen ••• Menü.

   - Wenn Sie jemals Ihre Anmeldeinformationen aktualisieren müssen, gibt es im auch eine **Anmeldeinformationen aktualisieren**-Option ••• Menü.

     Wenn Sie diese Option verwenden, werden Sie aufgefordert, sich erneut anzumelden. Beachten Sie, dass das Token für diese Konten nach 90 Tagen abläuft. Eine Benachrichtigung wird gesendet, um Sie darüber zu informieren.

Holen Sie sich Hilfe

NetApp bietet Unterstützung für BlueXP und seine Cloud-Services auf unterschiedliche Weise. Umfassende kostenlose Self-Support-Optionen stehen rund um die Uhr zur Verfügung, wie etwa Knowledge Base-Artikel (KB) und ein Community-Forum. Ihre Support-Registrierung umfasst technischen Remote-Support über Web-Ticketing.

Unterstützung für Fileservices von Cloud-Providern

Technischen Support zu Fileservices von Cloud-Providern, zu seiner Infrastruktur oder zu beliebigen Lösungen, die den Service verwenden, finden Sie im Abschnitt „Hilfe erhalten“ in der BlueXP Dokumentation zu diesem Produkt.

- "Amazon FSX für ONTAP"
- "Azure NetApp Dateien"
- "Cloud Volumes Service für Google Cloud"

Wenn Sie technischen Support für BlueXP und seine Storage-Lösungen und -Services erhalten möchten, nutzen Sie die unten beschriebenen Support-Optionen.

Nutzen Sie Self-Support-Optionen

Diese Optionen sind kostenlos verfügbar, 24 Stunden am Tag, 7 Tage die Woche:

- Dokumentation

  Die BlueXP-Dokumentation, die Sie gerade anzeigen.

- "Wissensdatenbank"

  Suchen Sie in der BlueXP Knowledge Base nach hilfreichen Artikeln zur Fehlerbehebung.

- "Communitys"

  Treten Sie der BlueXP Community bei, um laufende Diskussionen zu verfolgen oder neue zu erstellen.

Erstellen Sie einen Fall mit dem NetApp Support

Zusätzlich zu den oben genannten Self-Support-Optionen können Sie gemeinsam mit einem NetApp Support-Experten eventuelle Probleme nach der Aktivierung des Supports beheben.

Bevor Sie beginnen

- Um die Funktion **Fall erstellen** nutzen zu können, müssen Sie zunächst Ihre Anmeldedaten für die NetApp Support-Website mit Ihren BlueXP Anmeldedaten verknüpfen. "Managen Sie Zugangsdaten für Ihre BlueXP Anmeldung".
- Wenn Sie einen Fall für ein ONTAP System mit einer Seriennummer eröffnen, muss Ihr NSS-Konto mit der Seriennummer des Systems verknüpft sein.

Schritte

1. Wählen Sie in BlueXP **Hilfe > Support** aus.
2. Wählen Sie auf der Seite **Ressourcen** eine der verfügbaren Optionen unter Technischer Support:

   a. Wählen Sie **Rufen Sie uns an**, wenn Sie mit jemandem am Telefon sprechen möchten. Sie werden zu einer Seite auf netapp.com weitergeleitet, auf der die Telefonnummern aufgeführt sind, die Sie anrufen können.

   b. Wählen Sie **Fall erstellen**, um ein Ticket mit einem NetApp-Supportspezialisten zu öffnen:

      - **Service**: Wählen Sie den Dienst aus, mit dem das Problem verknüpft ist. Beispiel: BlueXP, wenn es sich um ein Problem des technischen Supports mit Workflows oder Funktionen im Service handelt.
      - **Arbeitsumgebung**: Wählen Sie **Cloud Volumes ONTAP** oder **On-Prem** und anschließend die zugehörige Arbeitsumgebung aus.

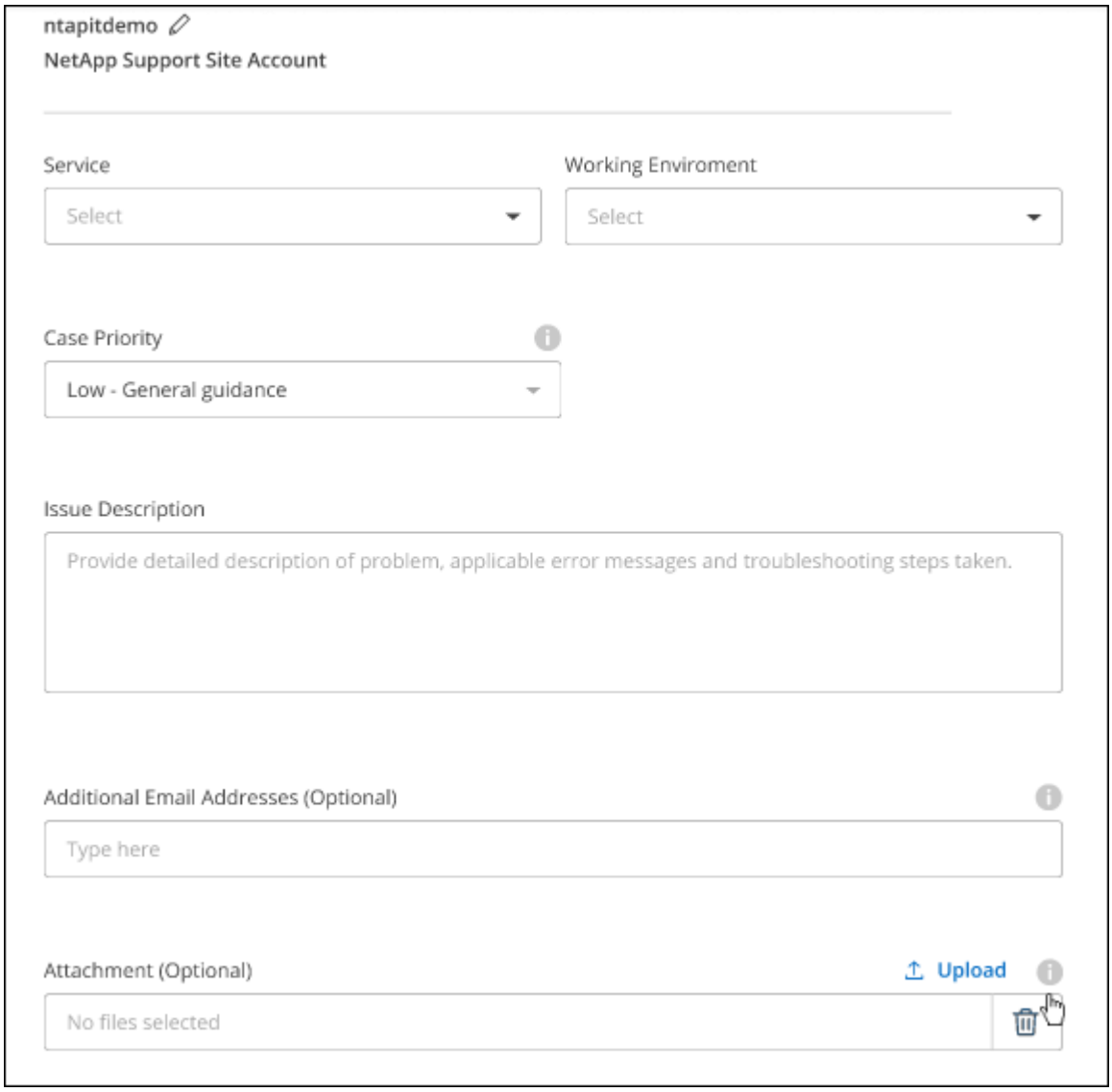
        Die Liste der Arbeitsumgebungen liegt im Bereich des BlueXP-Kontos, des Arbeitsbereichs und des Connectors, den Sie im oberen Banner des Dienstes ausgewählt haben.

- **Case Priority**: Wählen Sie die Priorität für den Fall, der niedrig, Mittel, hoch oder kritisch sein kann.

  Wenn Sie weitere Informationen zu diesen Prioritäten wünschen, bewegen Sie den Mauszeiger über das Informationssymbol neben dem Feldnamen.

- **Problembeschreibung**: Geben Sie eine detaillierte Beschreibung Ihres Problems an, einschließlich aller anwendbaren Fehlermeldungen oder Fehlerbehebungsschritte, die Sie durchgeführt haben.
- **Zusätzliche E-Mail-Adressen**: Geben Sie zusätzliche E-Mail-Adressen ein, wenn Sie jemand anderes auf dieses Problem aufmerksam machen möchten.
- **Anhang (optional)**: Laden Sie bis zu fünf Anhänge nacheinander hoch.

  Anhänge sind auf 25 MB pro Datei begrenzt. Folgende Dateierweiterungen werden unterstützt: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.



Nachdem Sie fertig sind

Es wird ein Popup-Fenster mit der Support-Fallnummer angezeigt. Ein NetApp Support-Experte prüft Ihren Fall und macht Sie umgehend mit.

Um eine Historie deiner Support-Fälle anzuzeigen, kannst du **Einstellungen > Chronik** auswählen und nach Aktionen mit dem Namen „Support-Case erstellen“ suchen. Mit einer Schaltfläche ganz rechts können Sie die Aktion erweitern, um Details anzuzeigen.

Es ist möglich, dass beim Versuch, einen Fall zu erstellen, möglicherweise die folgende Fehlermeldung angezeigt wird:

„Sie sind nicht berechtigt, einen Fall für den ausgewählten Service zu erstellen.“

Dieser Fehler könnte bedeuten, dass das NSS-Konto und das Unternehmen des Datensatzes, mit dem es verbunden ist, nicht das gleiche Unternehmen des Eintrags für die BlueXP Account Seriennummer (dh 960xxxx) oder Seriennummer der Arbeitsumgebung. Sie können Hilfe mit einer der folgenden Optionen anfordern:

- Verwenden Sie den Chat im Produkt
- Übermitteln eines nicht-technischen Cases unter https://mysupport.netapp.com/site/help

Managen Ihrer Support-Cases (Vorschau)

Sie können aktive und gelöste Support-Cases direkt über BlueXP anzeigen und managen. Sie können die mit Ihrem NSS-Konto und Ihrem Unternehmen verbundenen Fälle verwalten.

Case Management ist als Vorschau verfügbar. Wir planen, diese Erfahrungen weiter zu verbessern und in zukünftigen Versionen Verbesserungen hinzuzufügen. Bitte senden Sie uns Ihr Feedback über den Product-Chat.

Beachten Sie Folgendes:

- Das Case-Management-Dashboard oben auf der Seite bietet zwei Ansichten:
  - Die Ansicht auf der linken Seite zeigt die Gesamtzahl der Fälle, die in den letzten 3 Monaten durch das von Ihnen angegebene NSS-Benutzerkonto eröffnet wurden.
  - Die Ansicht auf der rechten Seite zeigt die Gesamtzahl der in den letzten 3 Monaten auf Unternehmensebene eröffneten Fälle basierend auf Ihrem NSS-Benutzerkonto an.

  Die Ergebnisse in der Tabelle geben die Fälle in Bezug auf die ausgewählte Ansicht wieder.
- Sie können interessante Spalten hinzufügen oder entfernen und den Inhalt von Spalten wie Priorität und Status filtern. Andere Spalten bieten nur Sortierfunktionen.

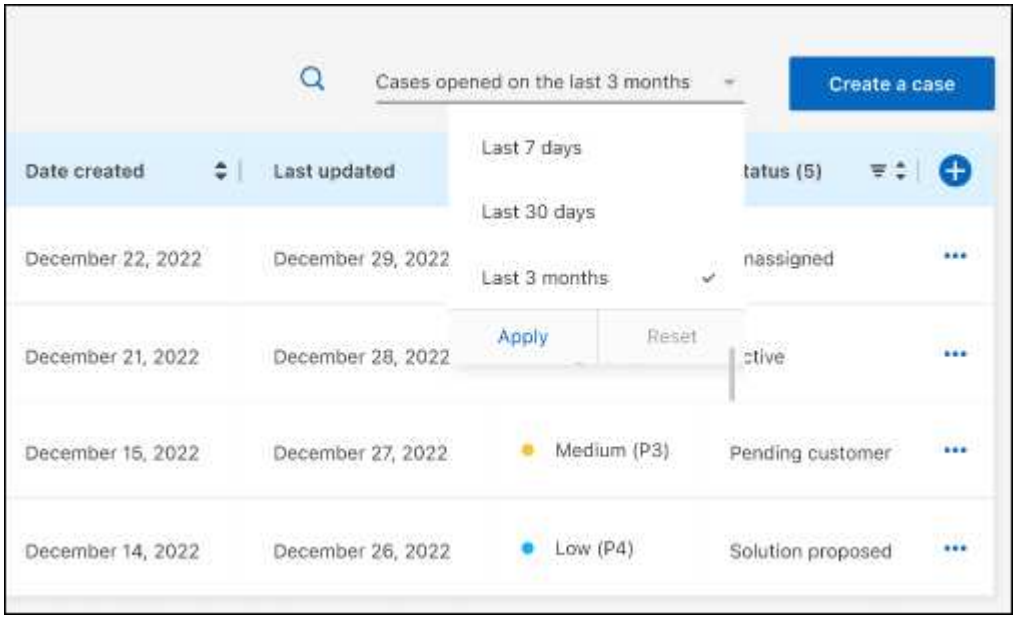
  Weitere Informationen erhalten Sie in den Schritten unten.
- Auf Fallebene bieten wir die Möglichkeit, Fallnotizen zu aktualisieren oder einen Fall zu schließen, der sich noch nicht im Status „Geschlossen“ oder „Geschlossen“ befindet.

Schritte

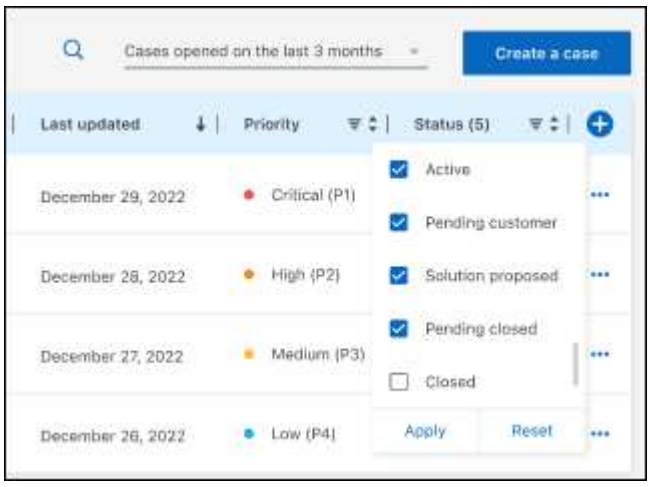
1. Wählen Sie in BlueXP **Hilfe > Support** aus.
2. Wählen Sie **Case Management** aus und fügen Sie bei Aufforderung Ihr NSS-Konto zu BlueXP hinzu.

   Auf der Seite **Case Management** werden offene Fälle im Zusammenhang mit dem NSS-Konto angezeigt, das mit Ihrem BlueXP Benutzerkonto verknüpft ist. Dies ist das gleiche NSS-Konto, das oben auf der Seite **NSS Management** angezeigt wird.
3. Ändern Sie optional die in der Tabelle angezeigten Informationen:

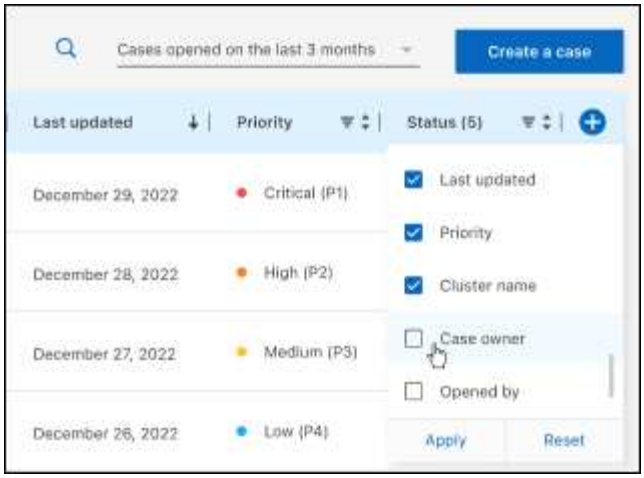
- Wählen Sie unter **Vorgänge der Organisation Ansicht** aus, um alle mit Ihrem Unternehmen verbundenen Fälle anzuzeigen.
- Ändern Sie den Datumsbereich, indem Sie einen genauen Datumsbereich oder einen anderen Zeitrahmen auswählen.



- Filtern Sie den Inhalt der Spalten.



- Ändern Sie die Spalten, die in der Tabelle angezeigt werden, indem Sie auswählen  Und wählen Sie dann die Spalten, die Sie anzeigen möchten.

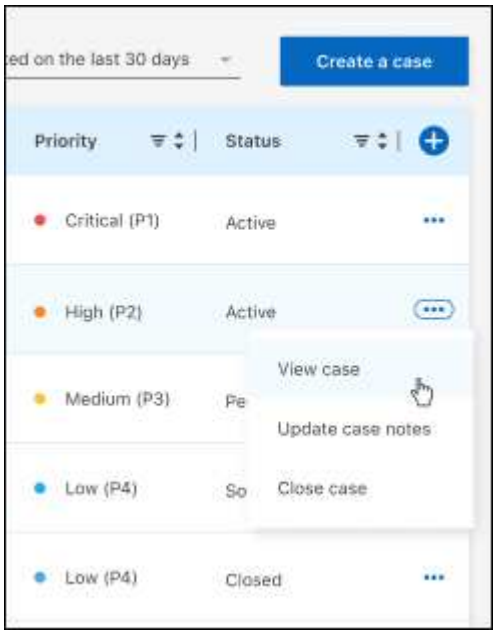


4. Managen Sie einen bestehenden Fall, indem Sie auswählen ••• Und eine der verfügbaren Optionen auswählen:

   - **Fall anzeigen**: Vollständige Details zu einem bestimmten Fall anzeigen.
   - **Aktennotizen aktualisieren**: Geben Sie zusätzliche Details zu Ihrem Problem an oder wählen Sie **Dateien hochladen**, um maximal fünf Dateien anzuhängen.

     Anhänge sind auf 25 MB pro Datei begrenzt. Folgende Dateierweiterungen werden unterstützt: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.

   - **Fall schließen**: Geben Sie Einzelheiten darüber an, warum Sie den Fall schließen und wählen Sie **Fall schließen**.



Rechtliche Hinweise

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

Urheberrecht

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

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

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

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

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

Datenschutzrichtlinie

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

Open Source

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

- "Hinweis für BlueXP"
- "Hinweise für den Cloud Volumes ONTAP Mediator"
- "Hinweis für ONTAP"