



Verwenden Sie Cloud Volumes ONTAP

Cloud Volumes ONTAP

NetApp
June 11, 2024

Inhalt

- Verwenden Sie Cloud Volumes ONTAP 1
- Lizenzmanagement 1
- Volume- und LUN-Administration 17
- Aggregatadministration 42
- Storage VM-Administration 47
- Sicherheit und Datenverschlüsselung 83
- Systemadministration 96
- Systemzustand und Ereignisse 136

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

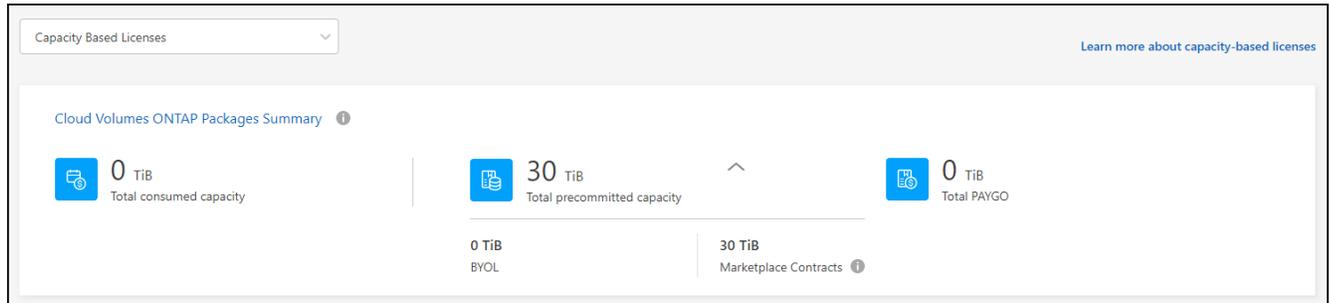
Das Digital Wallet von BlueXP zeigt Ihnen die verbrauchte Gesamtkapazität in Ihrem Konto und die verbrauchte Kapazität per Lizenzpaket an. Dadurch können Sie nachvollziehen, wie Sie belastet sind und ob Sie zusätzliche Kapazität erwerben müssen.

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:



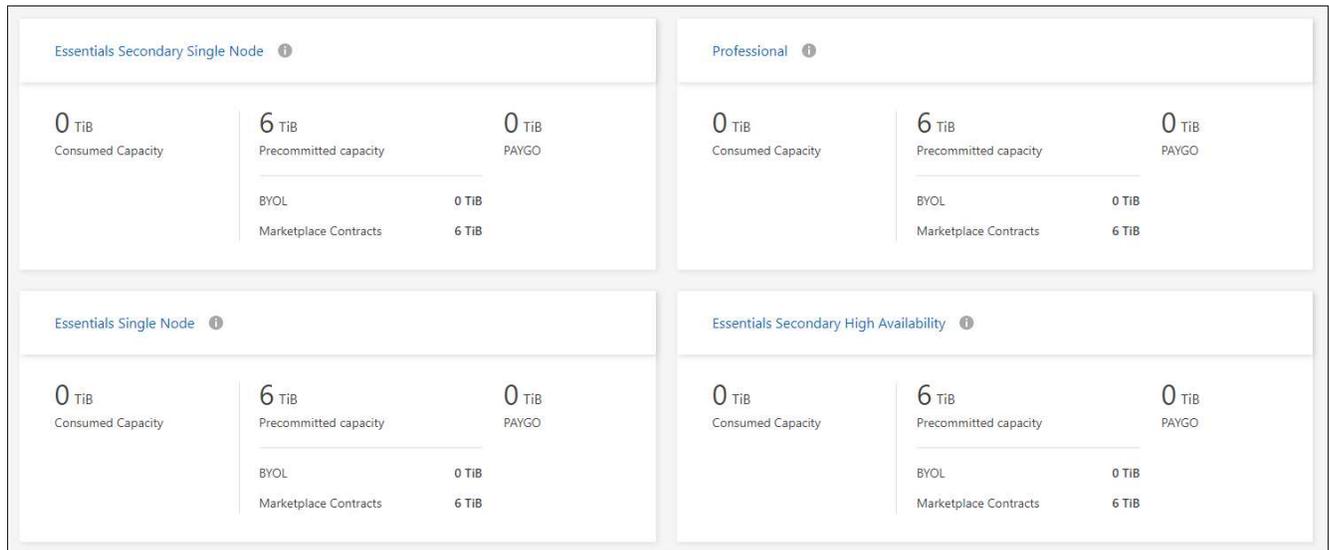
4. Zeigen Sie unter der Zusammenfassung die verbrauchte Kapazität für jedes Ihrer Lizenzierungspakete an.

- *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"](#).

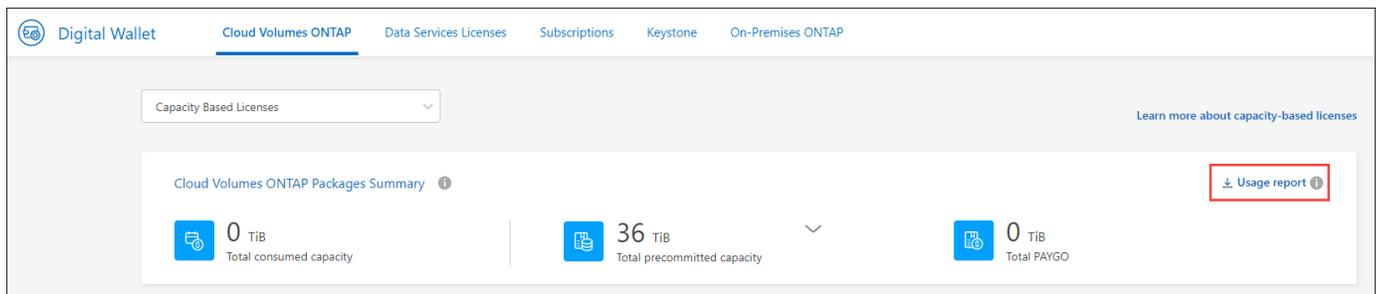
- *Recommited Capacity* ist die von Ihnen bei NetApp erworbene lizenzierte Kapazität (BYOL oder Marketplace Contract).
 - *BYOL* zeigt die von Ihnen für diesen Pakettyp bei NetApp erworbene lizenzierte Kapazität an.
 - *Marketplace Contracts* zeigt die lizenzierte Kapazität an, die Sie mit einem Marketplace-Vertrag 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

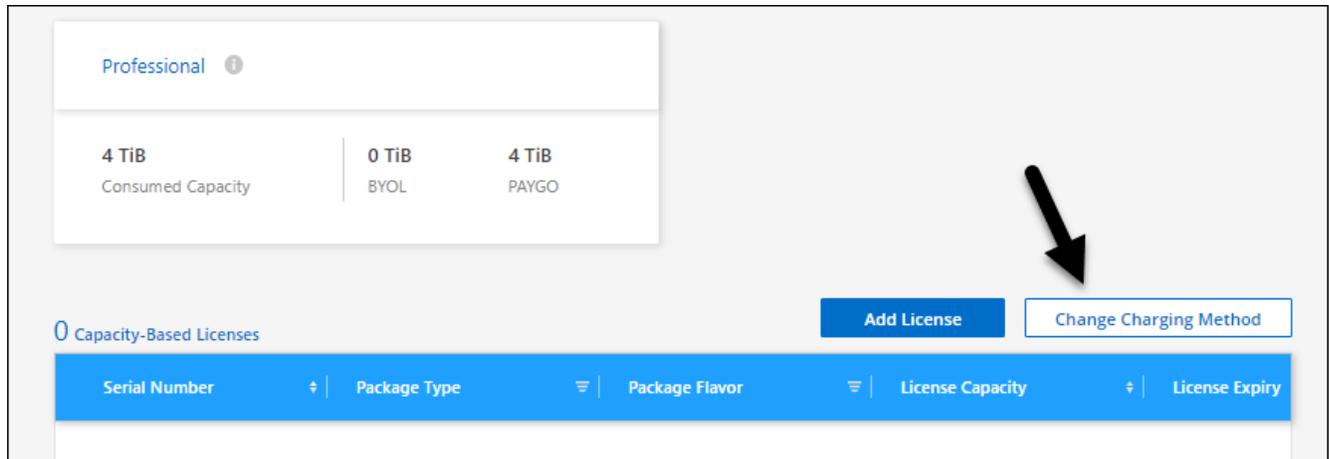
- Eine Änderung der Abrechnungsmethode hat keine Auswirkung darauf, ob die Abrechnung über eine von NetApp (BYOL) erworbene Lizenz oder über den Marketplace des Cloud-Providers (Pay-as-you-go) erfolgt.

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.

Change Charging Method

Select a working environment

CloudVolumesONTAP2

Current Cloud Volumes ONTAP charging method

Freemium

Select new Cloud Volumes ONTAP charging method

Essential

I understand that changing the package type will affect service charges

Change Charging Method Cancel

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 Pakettyt 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

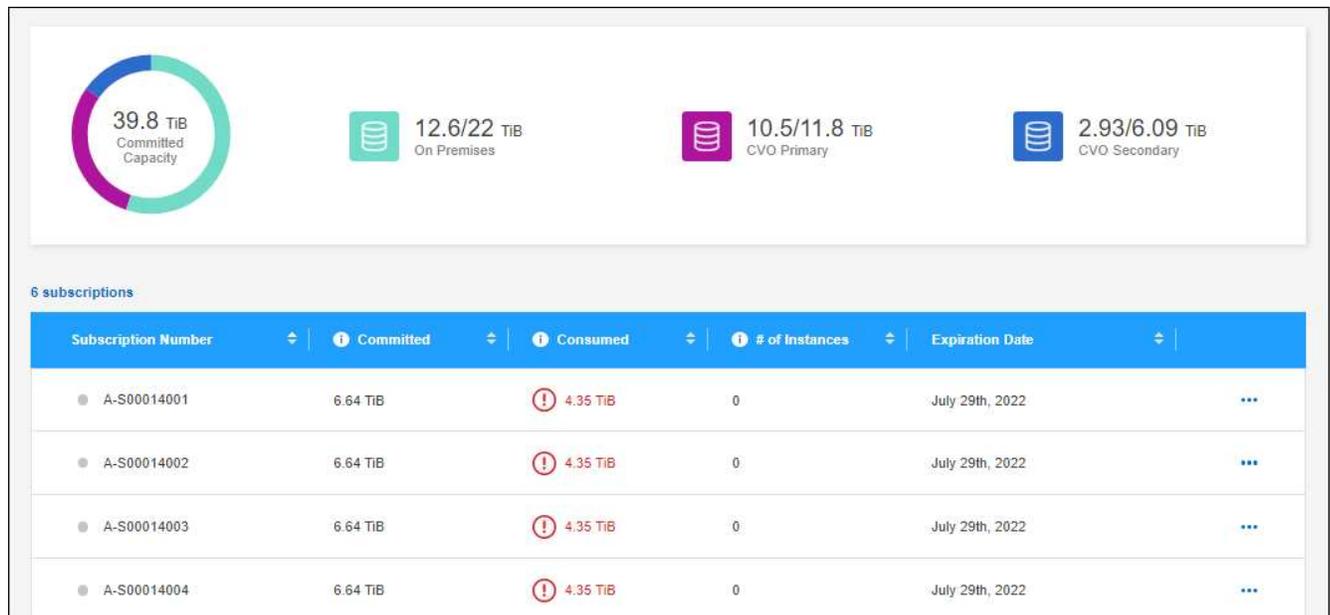
Bevor Sie Keystone Abonnements in BlueXP nutzen und managen können, müssen Sie zunächst NetApp kontaktieren, um Ihr BlueXP Benutzerkonto für Ihre Keystone Abonnements zu autorisieren.

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**.

Subscription Number	Committed	Consumed	# of Instances	Expiration Date	
A-S00014001	6.64 TiB	4.35 TiB	0	July 29th, 2022	⋮
A-S00014002	6.64 TiB	4.35 TiB	0	July 29th, 2022	View detail and edit
A-S00014003	6.64 TiB	4.35 TiB	0	July 29th, 2022	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.

Subscription Modification for A-S00014001

Service Level	Current Committed Capacity	Current Consumed Capacity	Requested Committed Capacity
Extreme	0.977 TiB	0.293 TiB	<input type="text" value="Enter amount"/> TiB
Premium	0.977 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB
Performance	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
Standard	0.732 TiB	0.439 TiB	<input type="text" value="Enter amount"/> TiB
Value	0.977 TiB	 0.879 TiB	<input type="text" value="Enter amount"/> TiB
Data Tiering	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
CVO Primary	1.96 TiB	 1.76 TiB	<input type="text" value="3"/> TiB
CVO Secondary	1.02 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB

Additional Information

Is there anything else we should know about your request?
Please be as descriptive as possible.

Enter your notes here

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.

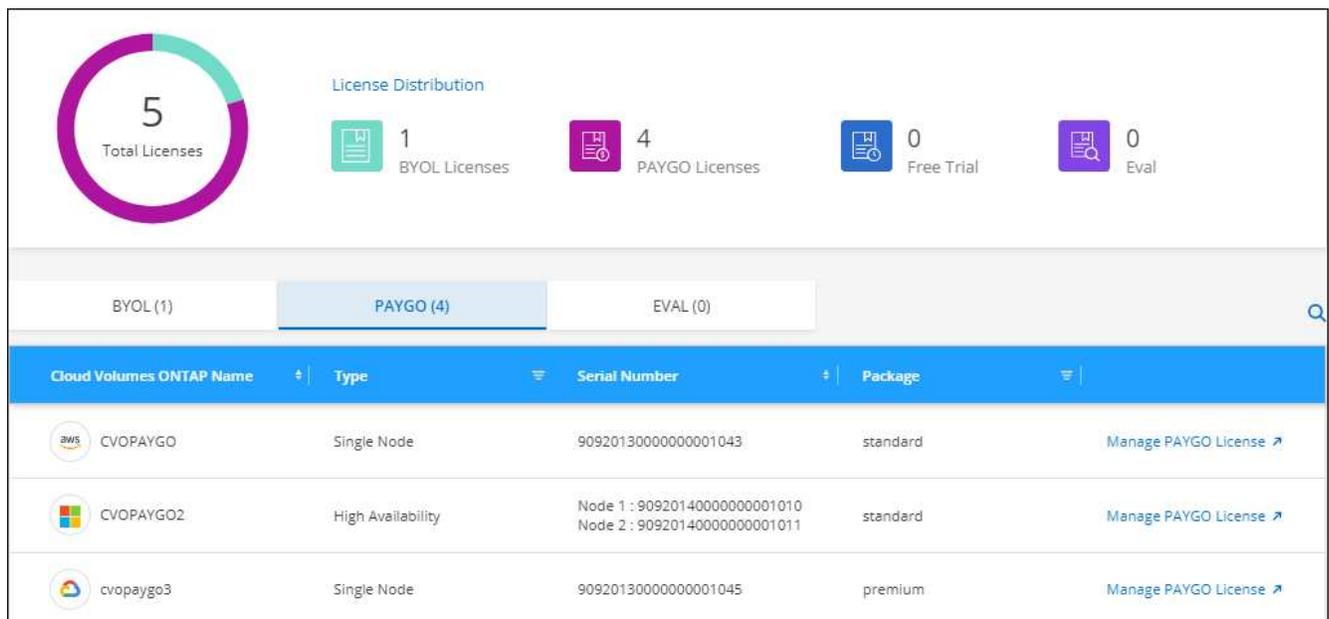
["Weitere Informationen zu Cloud Volumes ONTAP Lizenzen"](#).

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.



The screenshot displays the 'License Distribution' section of the BlueXP Digital Wallet. It features a donut chart showing 5 total licenses, with a breakdown: 1 BYOL License, 4 PAYGO Licenses, 0 Free Trial, and 0 Eval. Below this, there are tabs for 'BYOL (1)', 'PAYGO (4)', and 'EVAL (0)'. The 'PAYGO (4)' tab is selected, leading to a table of licenses.

Cloud Volumes ONTAP Name	Type	Serial Number	Package	
 CVOPAYGO	Single Node	90920130000000001043	standard	Manage PAYGO License
 CVOPAYGO2	High Availability	Node 1 : 90920140000000001010 Node 2 : 90920140000000001011	standard	Manage PAYGO License
 cvopaygo3	Single Node	90920130000000001045	premium	Manage PAYGO License

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**.

Serial Number	Type	Cloud Provider	License Expiry	Status	
012345678901234567890	Single Node	All Providers	April 20, 2022	Unassigned	Exchange License ▾
012345678901234567891	Single Node	Azure	April 20, 2022	Unassigned	Exchange License ▾
012345678901234567892	Single Node	AWS	January 1, 2022	Exchanged to Cloud Tiering on August 1, 2021	

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

License Generator

The following fields are pre-populated based on the NetApp SSO login provided.
To download the corresponding NetApp license file, re-enter your SSO password along with the correct Product Line and Product Serial number.

First Name	<input type="text" value="Ben"/>
Last Name	<input type="text"/>
Company	<input type="text" value="Network Appliance, Inc"/>
Email Address	<input type="text"/>
Username	<input type="text"/>

Product Line*

Not only is protecting your data required by law, but it's also the right thing to do.
 I have read NetApp's new **Global Data Privacy Policy** and agree that NetApp may use my personal data.

- ONTAP Select - Standard
- ONTAP Select - Premium
- ONTAP Select - Premium XL
- Cloud Volumes ONTAP for AWS (single node)
- Cloud Volumes ONTAP for AWS (HA)
- Cloud Volumes ONTAP for GCP (single node or HA)
- Cloud Volumes ONTAP for Microsoft Azure (single node)
- Cloud Volumes ONTAP for Microsoft Azure (HA)
- Service Level Manager - SLO Advanced
- StorageGRID Webscale
- StorageGRID WhiteBox
- SnapCenter Standard (capacity-based)

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.

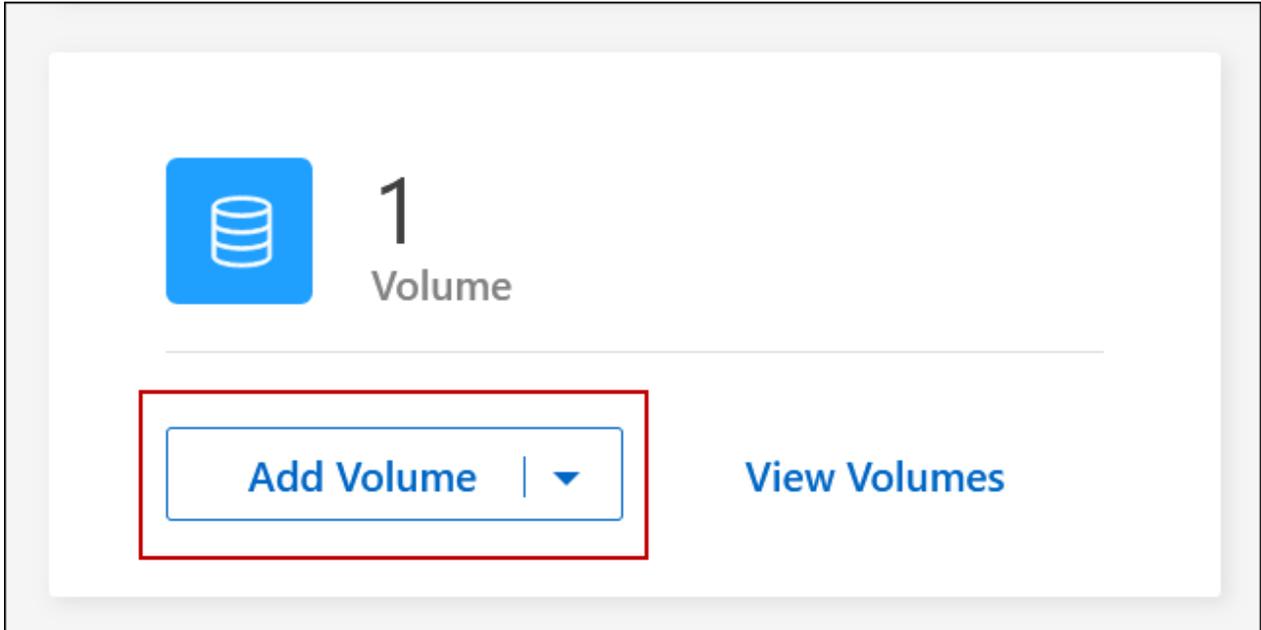
Schritte

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.

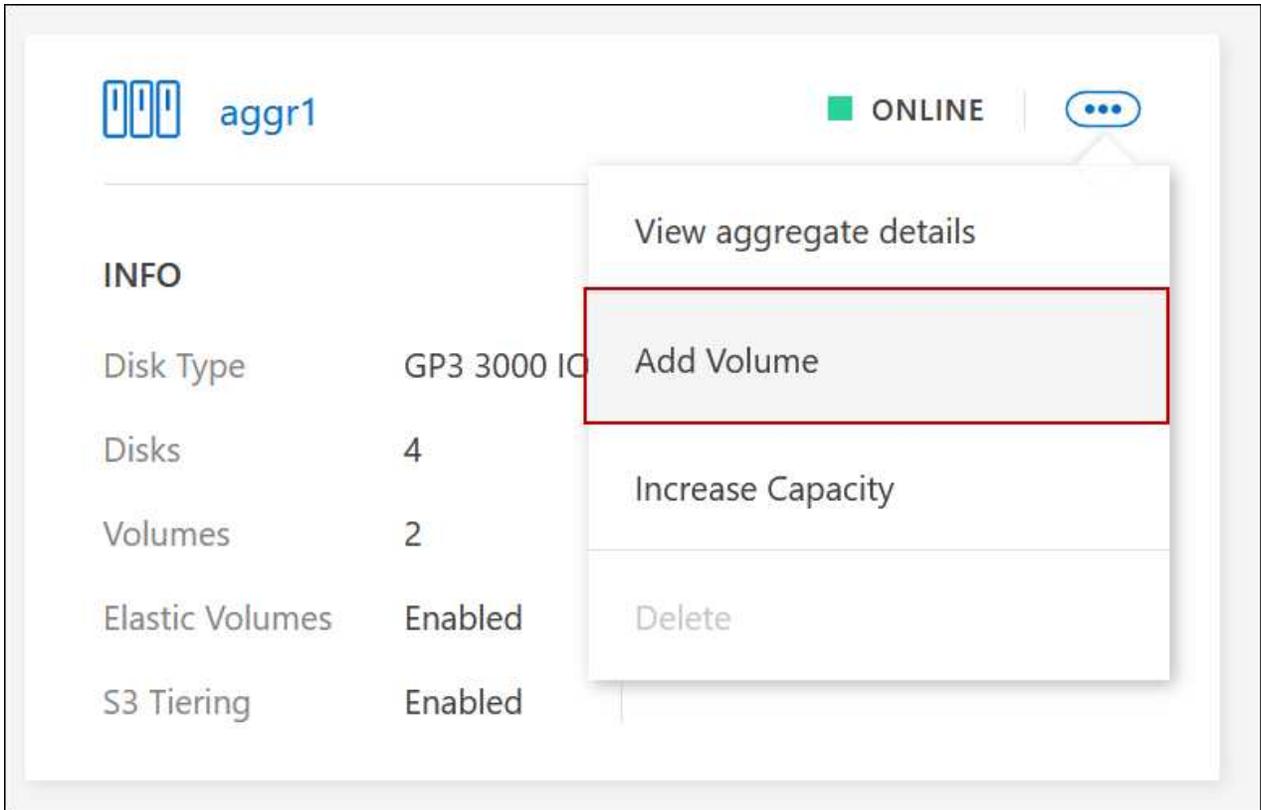
Alle Aggregate

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-Volumen 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 Volumen 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 Bus 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 Volumen 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 Volumen 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

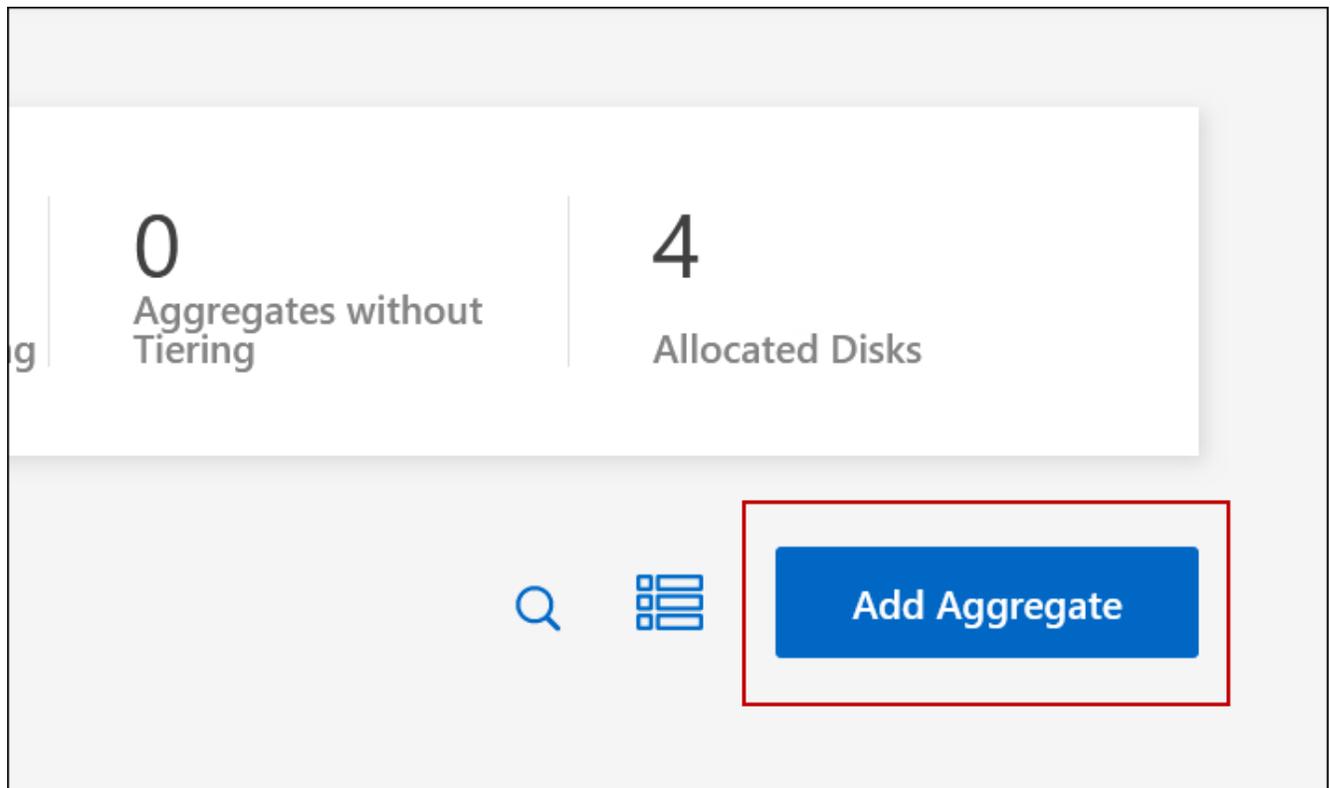
BlueXP erstellt das Volume auf dem Cloud Volumes ONTAP System.

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.

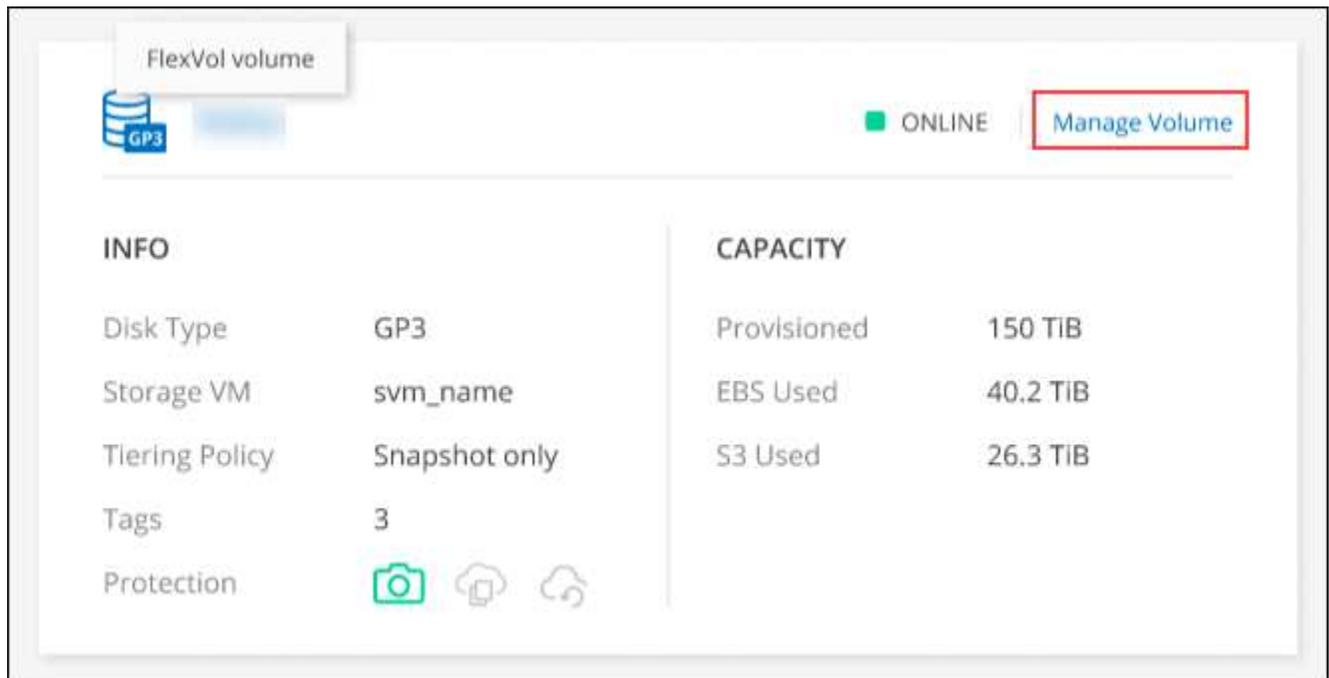
Sie können Volumes in der BlueXP Standard View oder Advanced View managen. Die Standardansicht bietet eine begrenzte Auswahl an Optionen zum Ändern der Volumes. Die erweiterte Ansicht bietet ein erweitertes Management, wie Klonen, Ändern der Größe, Ändern von Einstellungen für Ransomware-Schutz, Analyse, 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	<ol style="list-style-type: none"> Klicken Sie unter Volume Actions im Fenster Manage Volumes auf Mount Command. Klicken Sie Auf Kopieren.
Klonen Sie ein Volume	<ol style="list-style-type: none"> Klicken Sie unter Volume Actions im Bereich Manage Volumes auf Clone the Volume. Ändern Sie den Klonnenamen nach Bedarf, und klicken Sie dann auf Clone. <p>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.</p> <p>Weitere Informationen zu FlexClone Volumes finden Sie im "ONTAP 9 Leitfaden für das Management von logischem Storage".</p>

Aufgabe	Aktion
Bearbeiten eines Volumes (nur Volumes mit Lese-/Schreibzugriff)	<p>a. Klicken Sie unter Volume Actions im Bereich Manage Volumes auf Edit Volume settings</p> <p>b. Ändern Sie die Snapshot-Richtlinie des Volumes, die NFS-Protokollversion, die NFS-Zugriffssteuerungsliste (Exportrichtlinie) oder die Freigabeberechtigungen, und klicken Sie dann auf Apply.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> Wenn Sie benutzerdefinierte Snapshot-Richtlinien benötigen, können Sie diese mit System Manager erstellen.</p> </div>
Löschen Sie ein Volume	<p>a. Klicken Sie unter Volume Actions im Bereich Manage Volumes auf Delete the Volume.</p> <p>b. Geben Sie im Fenster Volume löschen den Namen des Volumes ein, das Sie löschen möchten.</p> <p>c. Klicken Sie zur Bestätigung erneut auf Löschen.</p>
Erstellen Sie bei Bedarf eine Snapshot Kopie	<p>a. Klicken Sie im Bereich Volumes verwalten unter Schutzaktionen auf Snapshot-Kopie erstellen.</p> <p>b. Ändern Sie ggf. den Namen und klicken Sie dann auf Erstellen.</p>
Wiederherstellen von Daten aus einer Snapshot Kopie auf einem neuen Volume	<p>a. Klicken Sie im Bereich Volumes verwalten unter Schutzaktionen auf aus Snapshot-Kopie wiederherstellen.</p> <p>b. Wählen Sie eine Snapshot Kopie aus, geben Sie einen Namen für das neue Volume ein und klicken Sie dann auf Wiederherstellen.</p>
Ändern Sie den zugrunde liegenden Festplattentyp	<p>a. Klicken Sie unter Erweiterte Aktionen im Bereich Volumes verwalten auf Datenträgertyp ändern.</p> <p>b. Wählen Sie den Laufwerkstyp aus und klicken Sie dann auf Ändern.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> BlueXP verschiebt das Volume in ein vorhandenes Aggregat, das den ausgewählten Festplattentyp nutzt oder ein neues Aggregat für das Volume erstellt.</p> </div>
Ändern Sie die Tiering Policy	<p>a. Klicken Sie unter Erweiterte Aktionen im Bereich Volumes verwalten auf Tiering-Richtlinie ändern.</p> <p>b. Wählen Sie eine andere Richtlinie aus und klicken Sie auf Ändern.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> BlueXP verschiebt das Volume in ein vorhandenes Aggregat, das den ausgewählten Festplattentyp mit Tiering nutzt, oder erstellt ein neues Aggregat für das Volume.</p> </div>

Aufgabe	Aktion
Löschen Sie ein Volume	<ol style="list-style-type: none"> Wählen Sie ein Volume aus, und klicken Sie dann auf Löschen. Geben Sie den Namen des Volumes in das Dialogfeld ein. 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

- Öffnen Sie die erweiterte Ansicht, um die Größe eines Volumes über System Manager zu ändern. Siehe ["Erste Schritte"](#).
- Wählen Sie im linken Navigationsmenü **Speicher > Volumes**.
- Wählen Sie aus der Liste der Volumes das Volume aus, das Sie anpassen sollten.
- Klicken Sie auf das Optionssymbol .
- Wählen Sie **Größe Ändern**.
- 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.
- Klicken Sie Auf **Speichern**.

Resize volume ✕

CAPACITY

25
⇅

GiB
▼

SNAPSHOT RESERVE %

1
⇅

Existing	New
DATA SPACE	DATA SPACE
20 GiB	24.75 GiB
SNAPSHOT RESERVE	SNAPSHOT RESERVE
0 Bytes	256 MiB

Cancel
Save

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. <ul style="list-style-type: none"> • 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.

Aggregate Details	
aggr1	
Overview	Capacity Allocation
State	online
Home Node	iblog1-01
Encryption Type	cloudEncrypted
Volumes	2 ^
	www_iblog1_root (1 GiB)
	iblog1 (500 GiB)

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.

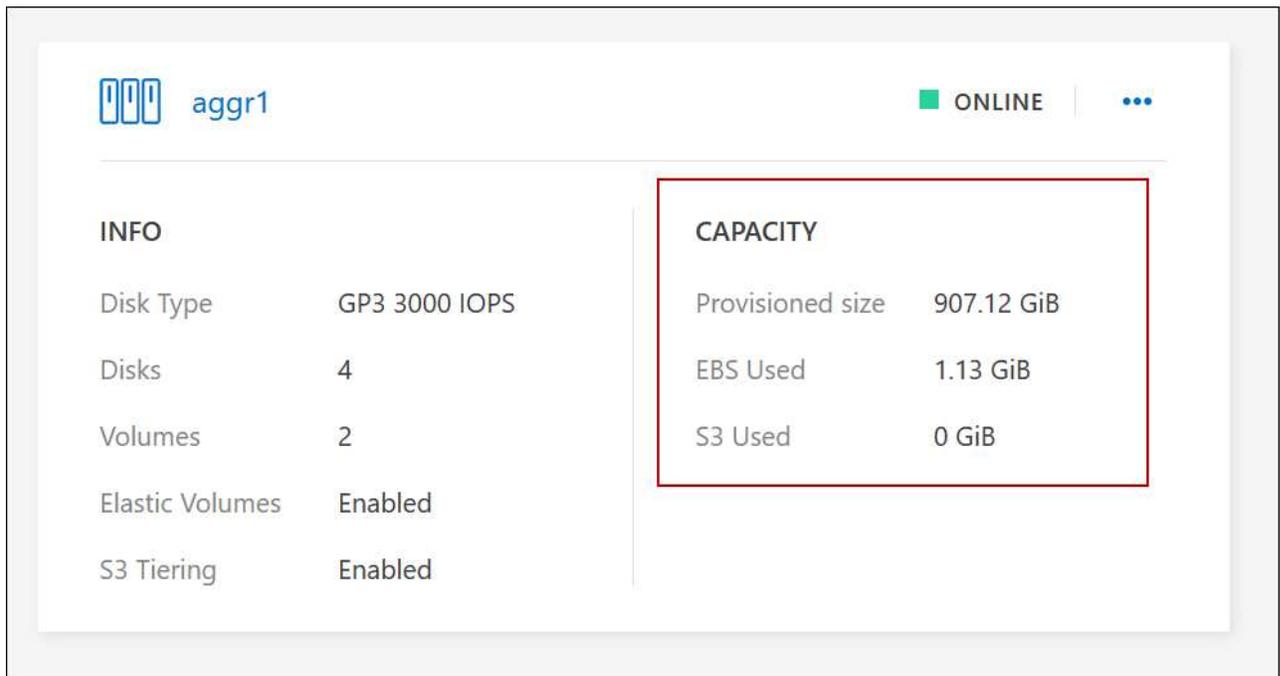
Über diese Aufgabe

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 FlexGroup 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.

INFO		CAPACITY	
Disk Type	GP3	Provisioned	150 TiB
Storage VM	svm_name	EBS Used	40.2 TiB
Tiering Policy	Snapshot only	S3 Used	26.3 TiB
Tags	3		
Protection	  		



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.

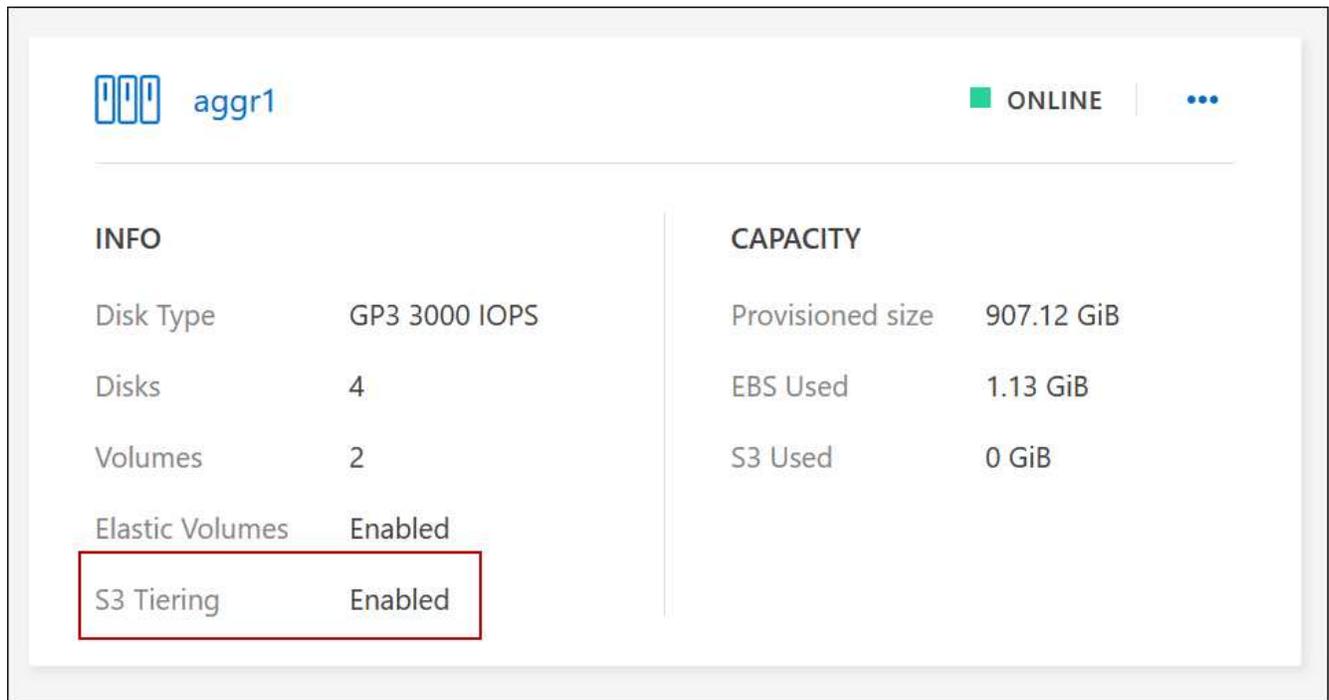
• Vorhandene Bände

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 anzuhängenden 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

Change Tiering Policy
Volume_1

Tiering Policy

Auto - Tiers cold Snapshot copies and cold user data from the active file system to object storage.
Minimum cooling days: 31 (2-183)

All - Immediately tiers all data (not including metadata) to object storage.

Snapshot Only - Tiers cold Snapshot copies to object storage.

None - Data tiering is disabled.

S3 Storage classes Standard-Infrequent Access

S3 Storage Encryption Key aws/s3

! This action is non-disruptive and changing the tier impacts cost, performance, and maximum capacity. Refer to [BlueXP documentation](#) for more details.

BlueXP erstellt ein neues Aggregat für das Volume, wenn es bereits ein Data Tiering-fähiges Aggregat gibt.

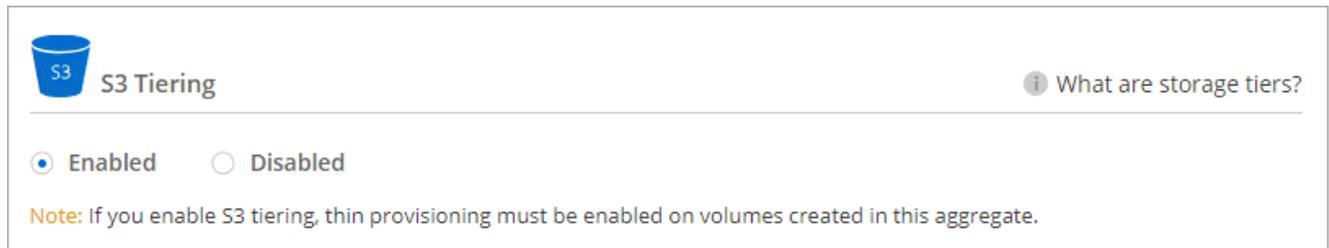
Tiering von Daten aus Datensicherungs-Volumes

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).



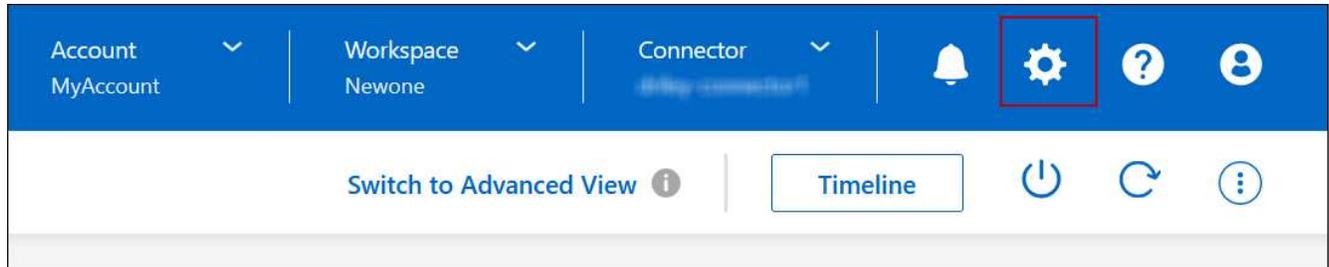
Wenn nicht genügend Speicherplatz zur Verfügung steht, können die Daten mit Cloud Volumes ONTAP nicht verschoben werden. Möglicherweise kommt es zu Performance-Einbußen. Jede Änderung sollte mit Vorsicht vorgenommen werden. Wenn Sie sich nicht sicher sind, wenden Sie sich an den NetApp Support.

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.

The screenshot displays the 'Select Disk Type' interface in the AWS console. At the top, there are four steps: 1. Disk Type, 2. Aggregate details, 3. Tiering Data, and 4. Review. The 'Disk Type' dropdown is set to 'GP3 - General Purpose SSD Dynamic Performance'. Below it, a card titled 'General Purpose SSD (gp3) Disk Properties' provides details: 'Description: General purpose SSD volume that balances price and performance (performance level is independent of storage capacity)'. Two performance metrics are shown: 'IOPS Value' at 12000 and 'Throughput MB/s' at 250.

["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**).

INFO		CAPACITY	
Disk Type	GP3 3000 IOPS	Provisioned size	907.12 GiB
Disks	4	EBS Used	1.13 GiB
Volumes	2	S3 Used	0 GiB
Elastic Volumes	Enabled		
S3 Tiering	Enabled		

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	<p>a. Klicken Sie im Menü ... (Ellipsensymbol) auf Datenträger hinzufügen.</p> <p>b. Wählen Sie die Anzahl der Festplatten aus, die Sie hinzufügen möchten, und klicken Sie auf Hinzufügen.</p> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>Alle Festplatten in einem Aggregat müssen dieselbe Größe haben.</p> </div>
Erhöhen Sie die Kapazität eines Aggregats, das Amazon EBS Elastic Volumes unterstützt	<p>a. Klicken Sie im Menü ... (Ellipsen-Symbol) auf Kapazität erhöhen.</p> <p>b. Geben Sie die zusätzliche Kapazität ein, die Sie hinzufügen möchten, und klicken Sie dann auf Erhöhen.</p> <p>Beachten Sie, dass Sie die Kapazität des Aggregats um mindestens 256 gib oder 10 % der Aggregatgröße erhöhen müssen.</p> <p>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.</p>
Löschen Sie ein Aggregat	<p>a. Wählen Sie eine Aggregat-Kachel, die keine Volumes enthält. Klicken Sie auf ... (Ellipsensymbol) > Löschen.</p> <p>b. Klicken Sie zur Bestätigung erneut auf Löschen.</p>

Kapazitätseinstellungen auf einem Konnektor verwalten

Jeder Connector hat Einstellungen, die bestimmen, wie er die Aggregatskapazität für Cloud Volumes ONTAP verwaltet.

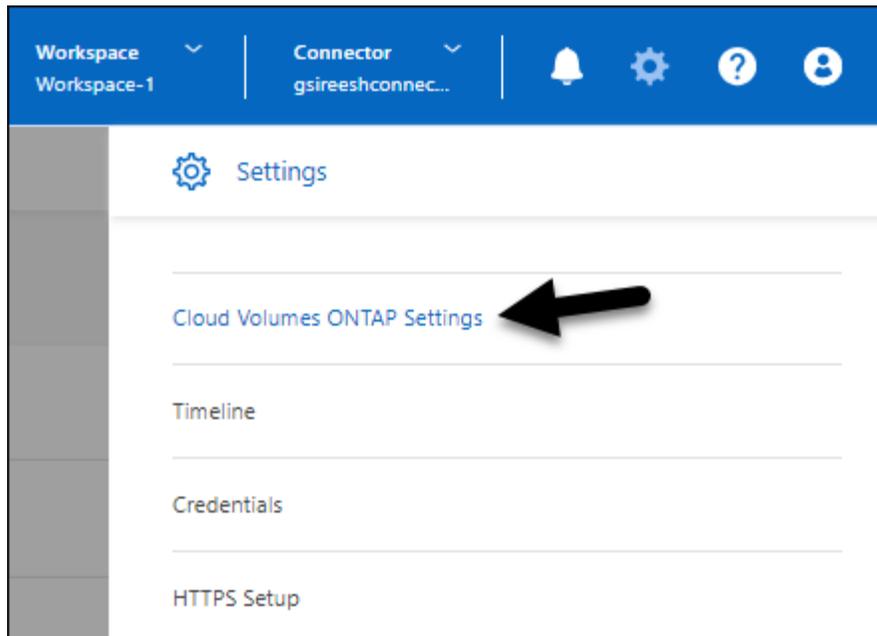
Diese Einstellungen betreffen alle Cloud Volumes ONTAP-Systeme, die von einem Connector verwaltet werden. Wenn Sie einen anderen Konnektor haben, kann er anders konfiguriert werden.

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.

The screenshot shows a configuration interface titled "Details & Protection". It contains the following elements:

- Storage VM Name:** A dropdown menu with "svm_name1" selected. An information icon (i) is to the right.
- Volume Name:** An empty text input field.
- Size (GiB):** A dropdown menu with "Volume size" selected. An information icon (i) is to the right.
- Snapshot Policy:** A dropdown menu with "default" selected. An information icon (i) is to the right.
- Default Policy:** A link with an information icon (i) and the text "Default Policy" below the Snapshot Policy dropdown.

Das folgende Bild zeigt, wie Sie bei der Replizierung eines Volumes in ein anderes System eine Storage VM auswählen können.

Destination Volume Name

volume_copy

Destination Storage VM Name

svm_name1

Destination Aggregate

Automatically select the best aggregate

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.

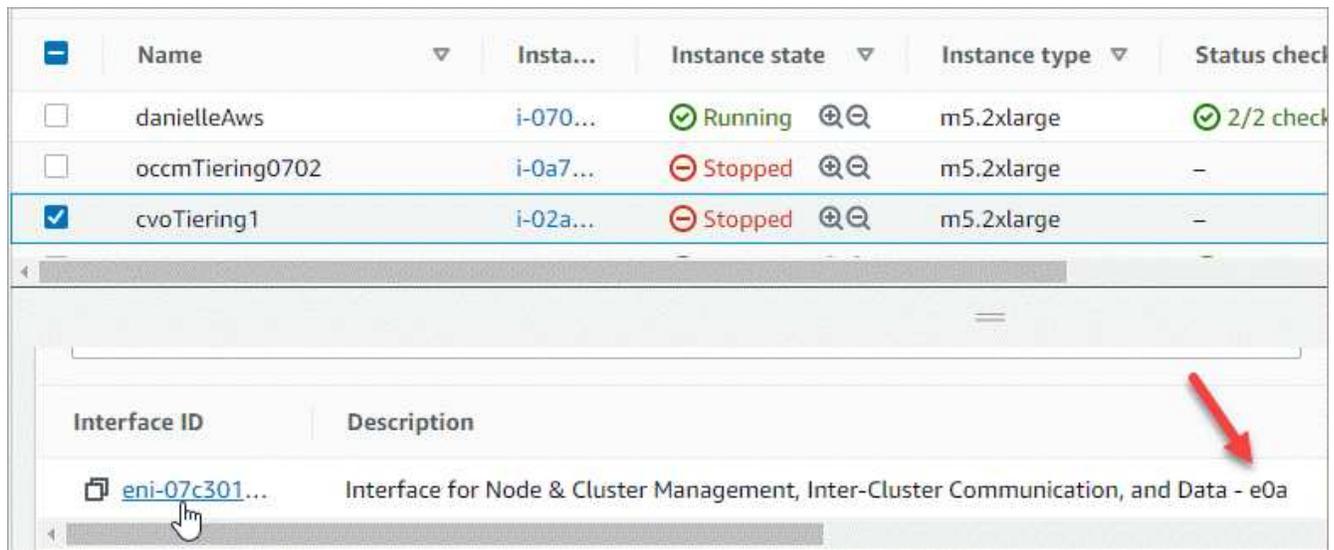
Beachten Sie, dass eine optionale Management-LIF für eine Storage-VM eine private IP-Adresse auf einem System mit einem einzelnen Node und auf einem HA-Paar in einer einzelnen Verfügbarkeitszone erfordert. Dieses Management-LIF bietet eine Verbindung zu Management-Tools wie SnapCenter.

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 node1Mask -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.

The screenshot shows the 'Add frontend IP configuration' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > Load balancing > azureha1011s3-rg-lb >'. The title is 'Add frontend IP configuration' with a three-dot menu icon. Below the title is the resource name 'azureha1011s3-rg-lb'. The form contains the following fields:

- Name ***: A text input field containing 'ip-for-svm2' with a checkmark icon on the right.
- Virtual network**: A dropdown menu showing 'Default-Networking-vnet'.
- Subnet ***: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow icon.
- Assignment**: Two radio buttons, 'Dynamic' (which is selected) and 'Static'.
- Availability zone * ⓘ**: A dropdown menu showing 'Zone-redundant' with a downward arrow icon.

- 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.

Microsoft Azure Search resources, services, and

Home > Load balancers > azureha1011s3-rg-lb >

Add health probe

azureha1011s3-rg-lb

Name *	<input type="text" value="svm2-health-probe1"/>	✓
Protocol *	<input type="text" value="TCP"/>	▼
Port * ⓘ	<input type="text" value="63005"/>	✓
Interval * ⓘ	<input type="text" value="5"/>	
		seconds
Unhealthy threshold * ⓘ	<input type="text" value="2"/>	
		consecutive failures
Used by ⓘ	Not used	

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**.

Add load balancing rule ⋮

chandanaTcpRst3-rg-lb

i A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name *

IP Version *
 IPv4 IPv6

Frontend IP address * ⓘ

HA Ports ⓘ

Backend pool ⓘ

Health probe ⓘ

Session persistence ⓘ

Floating IP ⓘ

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.

The screenshot shows the 'Add frontend IP configuration' page in the Azure portal. The breadcrumb navigation is 'Home > Load balancing > azureha1011s3-rg-lb >'. The title is 'Add frontend IP configuration' with a three-dot menu icon. Below the title is the resource name 'azureha1011s3-rg-lb'. The form contains the following fields:

- Name ***: A text input field containing 'ip-for-svm2' with a checkmark icon on the right.
- Virtual network**: A dropdown menu showing 'Default-Networking-vnet'.
- Subnet ***: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow icon.
- Assignment**: Two radio buttons, 'Dynamic' (selected) and 'Static'.
- Availability zone ***: A dropdown menu showing 'Zone-redundant' with a downward arrow icon and an information icon.

- 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.

Microsoft Azure Search resources, services, and

Home > Load balancers > azureha1011s3-rg-lb >

Add health probe ...

azureha1011s3-rg-lb

Name *	svm2-health-probe1 ✓
Protocol *	TCP ▾
Port * ⓘ	63005 ✓
Interval * ⓘ	5 seconds
Unhealthy threshold * ⓘ	2 consecutive failures
Used by ⓘ	Not used

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**.

Add load balancing rule

chandanaTcpRst3-rg-lb

i A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name *

jimmy_new_rule

IP Version *

IPv4 IPv6

Frontend IP address * ⓘ

10.1.0.156 (dataAFIP)

HA Ports ⓘ

Backend pool ⓘ

backendPool (2 virtual machines)

Health probe ⓘ

dataProbe (TCP:63002)

Session persistence ⓘ

None

Floating IP ⓘ

Disabled Enabled

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**.

connector1-614 | IP configurations

Network interface

Search << **+ Add** Save Discard Refresh

Overview
Activity log
Access control (IAM)
Tags

Settings
IP configurations
DNS servers
Network security group
Properties
Locks

Monitoring
Insights
Alerts
Metrics

IP forwarding settings
IP forwarding: Disabled Enabled
Virtual network: Vnet2
IP configurations
Subnet *: Subnet2

Search IP configurations

Name	IP Version	Type	Private IP address	Public IP address
ipconfig1	IPv4	Primary	10.0.0.1 (Dynamic)	20.100.100.1 (connector1... ***)

- f. Geben Sie einen Namen für die IP-Konfiguration ein, wählen Sie dynamisch aus, und klicken Sie dann auf **OK**.

connector1-614 | IP configurations

Network interface

Search << + Add Save Discard Refresh

Overview
Activity log
Access control (IAM)
Tags

Settings
IP configurations
DNS servers
Network security group
Properties
Locks

Monitoring
Insights
Alerts
Metrics

IP forwarding settings
IP forwarding: Disabled Enabled
Virtual network: Vnet2
IP configurations
Subnet *: Subnet2

Search IP configurations

Name	IP Version	Type	Private IP
ipconfig1	IPv4	Primary	10.0.0.1

Add IP configuration

connector1-614

Name *

IP version
 IPv4 IPv6

Type
 Primary Secondary

i Primary IP configuration already exists

Private IP address settings
Allocation
 Dynamic Static

Public IP address
 Disassociate Associate

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
```

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.

Edit network interface ^

Network *
default ▼ ?

Subnetwork *
default IPv4 (10.138.0.0/20) ▼ ?

i To use IPv6, you need an IPv6 subnet range. [LEARN MORE](#)

IP stack type

IPv4 (single-stack)

IPv4 and IPv6 (dual-stack)

Primary internal IP
gpcvo-vm-ip-nic0-nodemgmt (10.138.0.46) ▼ ?

Alias IP ranges

<p>Subnet range 1 Primary (10.138.0.0/20) ▼</p>	<p>Alias IP range 1 * 10.138.0.25/32 ?</p>
<p>Subnet range 2 Primary (10.138.0.0/20) ▼</p>	<p>Alias IP range 2 * 10.138.0.23/32 ?</p>
<p>Subnet range 3 Primary (10.138.0.0/20) ▼</p>	<p>Alias IP range 3 * 10.138.0.21/32 ?</p>
<p>Subnet range 4 Primary (10.138.0.0/20) ▼</p>	<p>Alias IP range 4 * 10.138.0.31/32 ?</p>

+ ADD IP RANGE

External IPv4 address
None ▼ ?

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>
```

- 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
```

- 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
```

- 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 Schlüsselvault 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.

Create an access policy

1 Permissions **2 Principal** 3 Application (optional) 4 Review + create

Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

Selected item

No item selected

Previous **Next**

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)

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

3 selected

Service	Status	
Microsoft.Storage	Succeeded	
Microsoft.AzureActiveDirectory	Succeeded	
Microsoft.KeyVault	Succeeded	

Service endpoint policies

0 selected

SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. [Learn more](#)

Private endpoint network policy

Disabled

Save **Cancel**

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.locat
ions.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-Dateierweiterungen

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.

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection



50 %
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

[Activate Snapshot Policy](#)

2 Block Ransomware File Extensions



ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

[View Denied File Names](#)

[Activate FPolicy](#)

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.



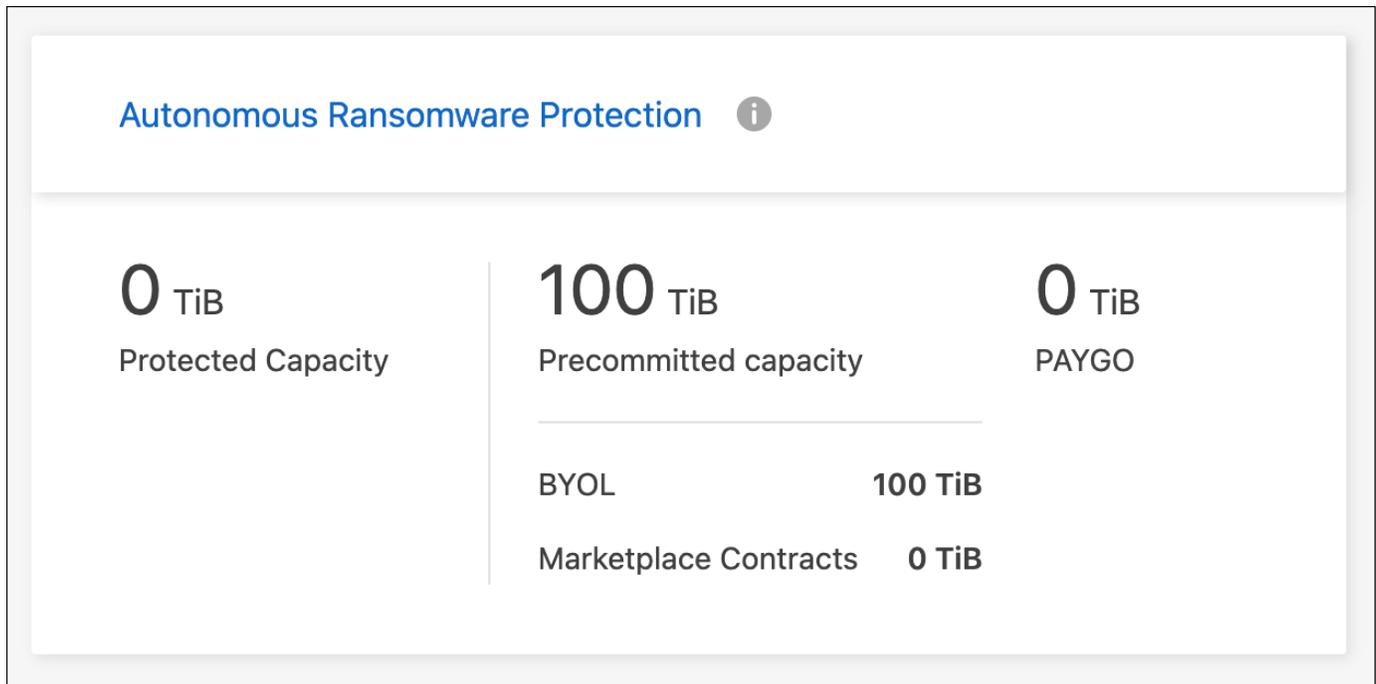
Die Verwendung der ARP-Funktion mit Node-basierten Cloud Volumes ONTAP-Lizenzen ist derzeit nicht in Digital Wallet enthalten. Die Möglichkeit, die Node-basierte ARP-Nutzung anzuzeigen, wird in einer zukünftigen Version unter Digital Wallet verfügbar sein.

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



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**.

Aggregate Details	
aggr1	
Overview	Capacity Allocation
State	online
Home Node	#####
Encryption Type	cloudEncrypted
Volumes	2 ∨

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“](#)".

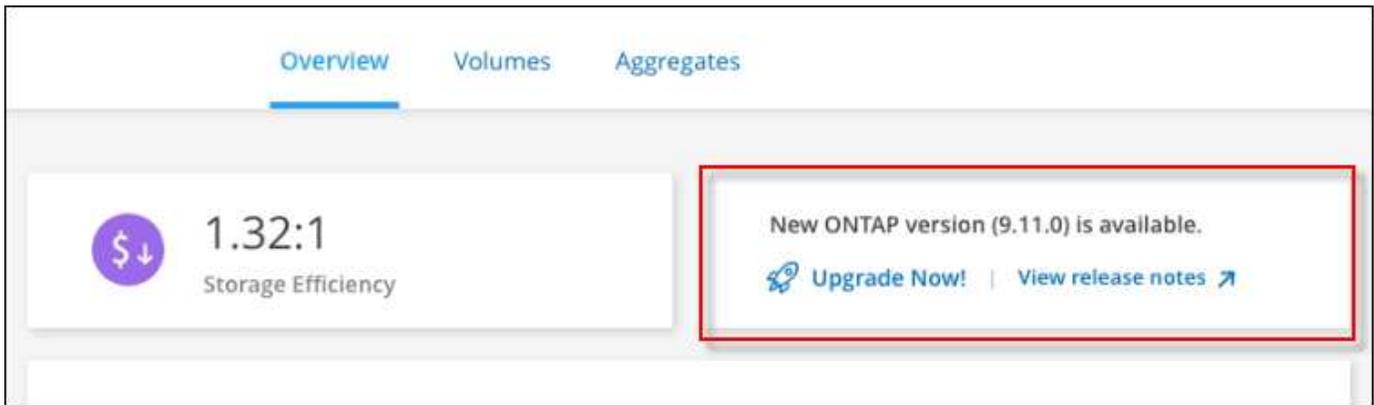
Upgrade von Cloud Volumes ONTAP

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.

Upgrade Cloud Volumes ONTAP version

You are about to upgrade Cloud Volumes ONTAP ⓘ

9.11.1 → 9.12.1RC1 (Nov 1, 2023)

[Select older versions](#)

This upgrade also includes a new Mediator version

3.1 → 3.2 (Mar 1, 2023)

End User License Agreement (EULA)

1. DEFINITIONS

1.1. "Documentation" means technical documentation describing the features and functions of the Software.

1.2. "NetApp Cloud Provider" means a third party authorized by NetApp to offer or enable the use of the Software as part of such provider's cloud-based service.

1.3. "NetApp Partner" means an authorized NetApp distributor, reseller or other channel partner.

1.4. "Open Source Software" means third party software that is openly and freely licensed under the terms of a public license designated by the third party.

1.5. "Software" means all NetApp-branded software in object code format comprising backup and recovery, disaster recovery, storage efficiency and management

- 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:

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**.

Information		Features
Working Environment Tags		Tags 
Scheduled Downtime		Off 
S3 Storage Classes	Standard-Infrequent Access	
Instance Type		m5.xlarge 
Write Speed		Normal 
Ransomware Protection		Off 
Support Registration	Not Registered	
CIFs Setup		

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**.

Information	Features
Working Environment Tags	Tags 
Scheduled Downtime	Off 
S3 Storage Classes	Standard-Infrequent Access 
Instance Type	m5.xlarge 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
CIFs Setup	

3. Geben Sie den Zeitplan für das Herunterfahren an:

- 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

Schedule Downtime
Cloud Manager Time Zone: 17:58 UTC

Select when to turn off your Working Environment:

Turn off every day at 20 : 00 for 12 hours (1-24)
Sun, Mon, Tue, Wed, Thu, Fri, Sat

Turn off every weekdays at 20 : 00 for 12 hours (1-24)
Mon, Tue, Wed, Thu, Fri

Turn off every weekend at 20 : 00 for 12 hours (1-48)
Sat

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.



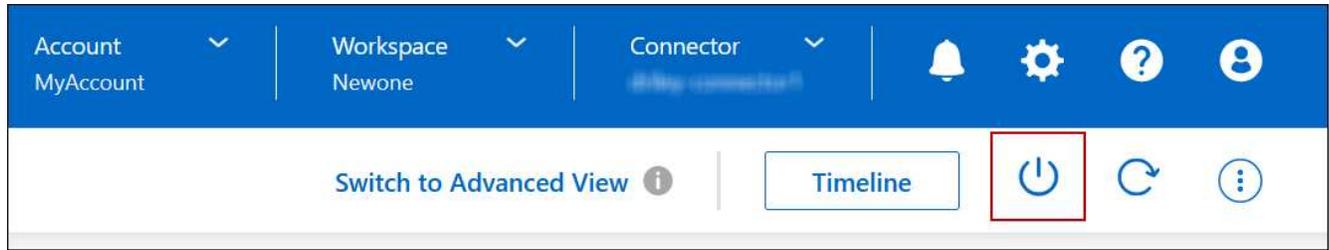
Zur Senkung der Kosten löscht BlueXP in regelmäßigen Abständen ältere Snapshots von Root- und Boot-Festplatten. Nur die beiden letzten Snapshots werden sowohl für die Root- als auch für Boot Disks beibehalten.

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**.

Information	Features
Working Environment Tags	Tags 
Scheduled Downtime	Off 
S3 Storage Classes	Standard-Infrequent Access 
Instance Type	m5.xlarge 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
CIFs Setup	

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

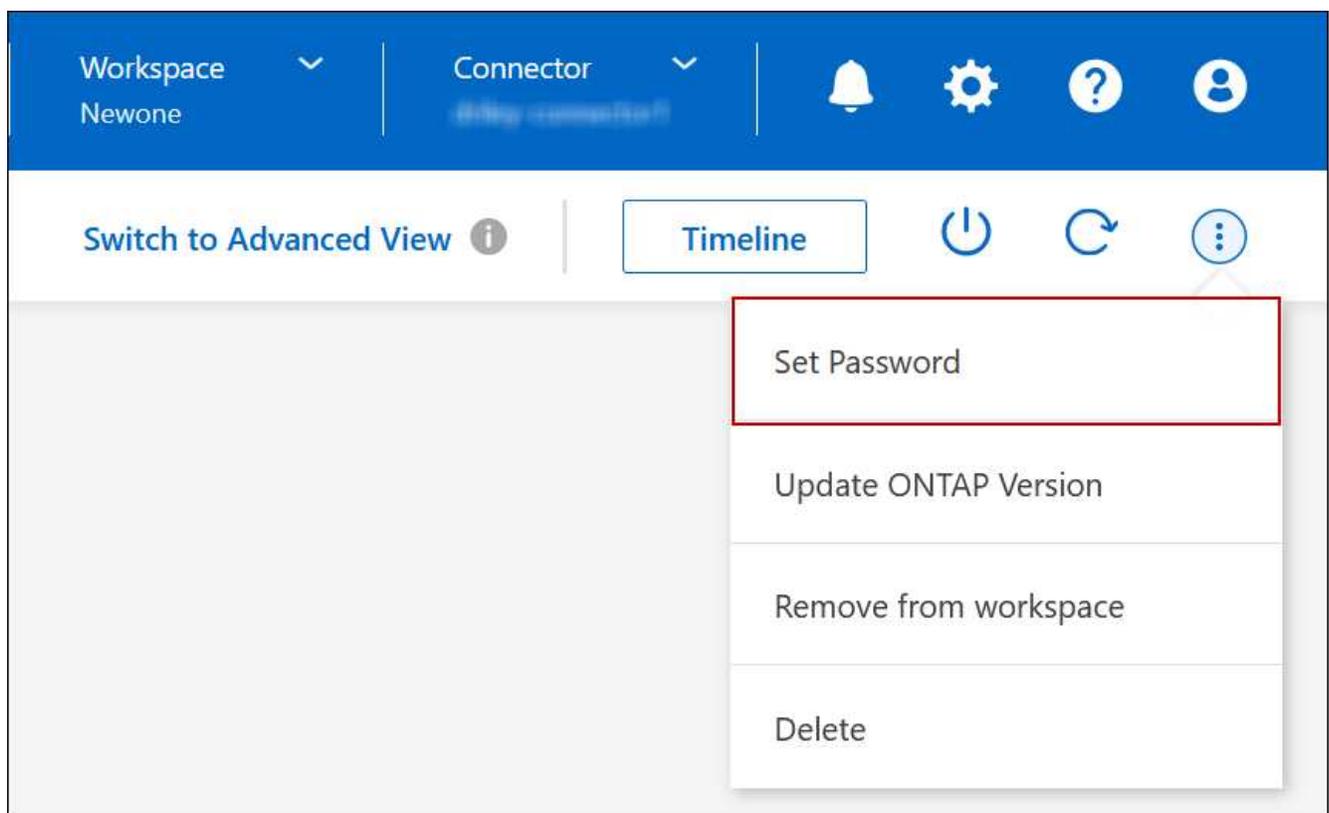
Cloud Volumes ONTAP enthält ein Cluster-Administratorkonto. Sie können das Kennwort für dieses Konto bei Bedarf von BlueXP ändern.



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

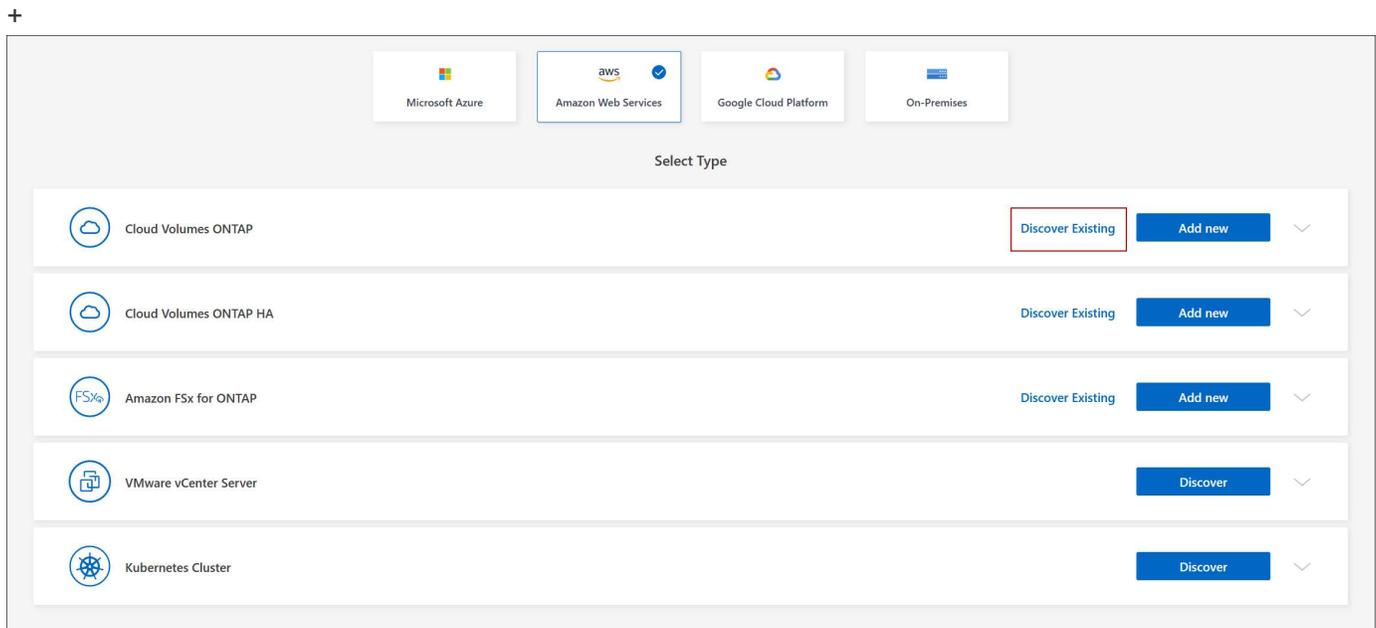
Sie können vorhandene Cloud Volumes ONTAP-Systeme entdecken und zu BlueXP hinzufügen. Dies können Sie tun, wenn Sie ein neues BlueXP System implementiert haben.

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

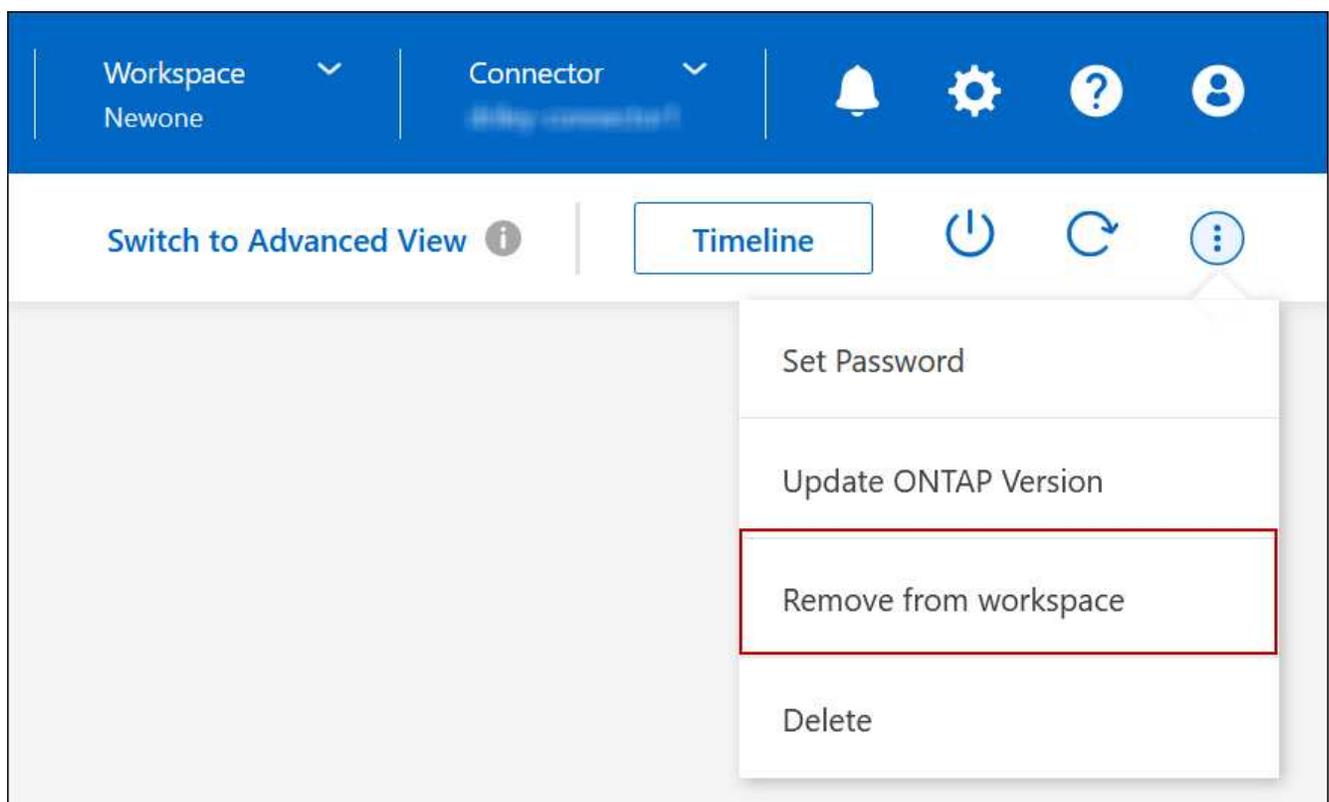
Durch Entfernen einer Cloud Volumes ONTAP-Arbeitsumgebung wird sie von BlueXP entfernt. Das Cloud Volumes ONTAP System wird nicht gelöscht. Sie können die Arbeitsumgebung später neu entdecken.

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

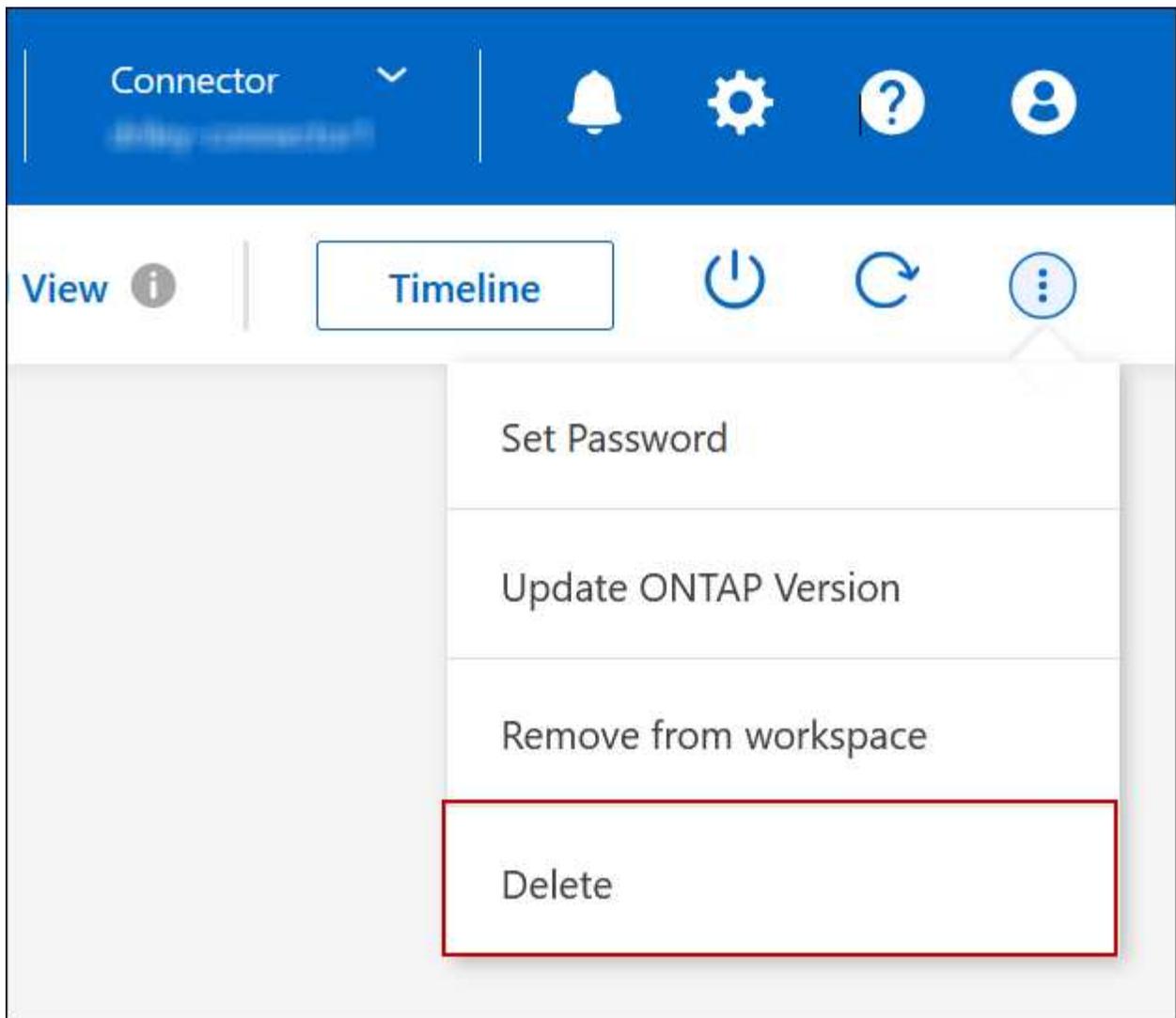
1. Wenn Sie das Backup und Recovery von BlueXP in der Arbeitsumgebung aktiviert haben, stellen Sie fest, ob die gesicherten Daten noch erforderlich sind, und legen Sie dann fest "[Löschen Sie die Backups, falls erforderlich](#)".

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**.

Information		Features
Working Environment Tags		Tags 
Scheduled Downtime		Off 
S3 Storage Classes	Standard-Infrequent Access	
Instance Type	m5.xlarge	
Write Speed		Normal 
Ransomware Protection		Off 
Support Registration	Not Registered	
CIFs Setup		

- 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

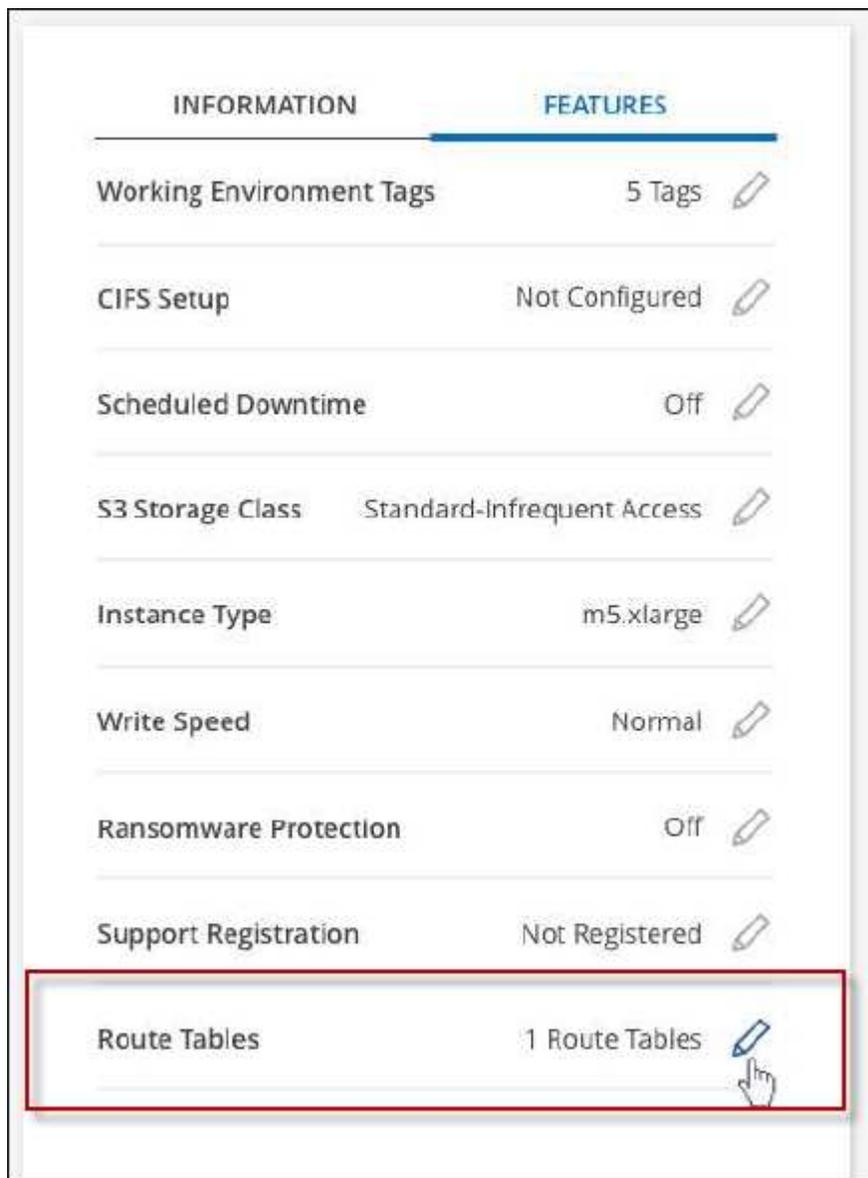
Cloud Volumes ONTAP wird mit der neuen Konfiguration neu gestartet.

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.

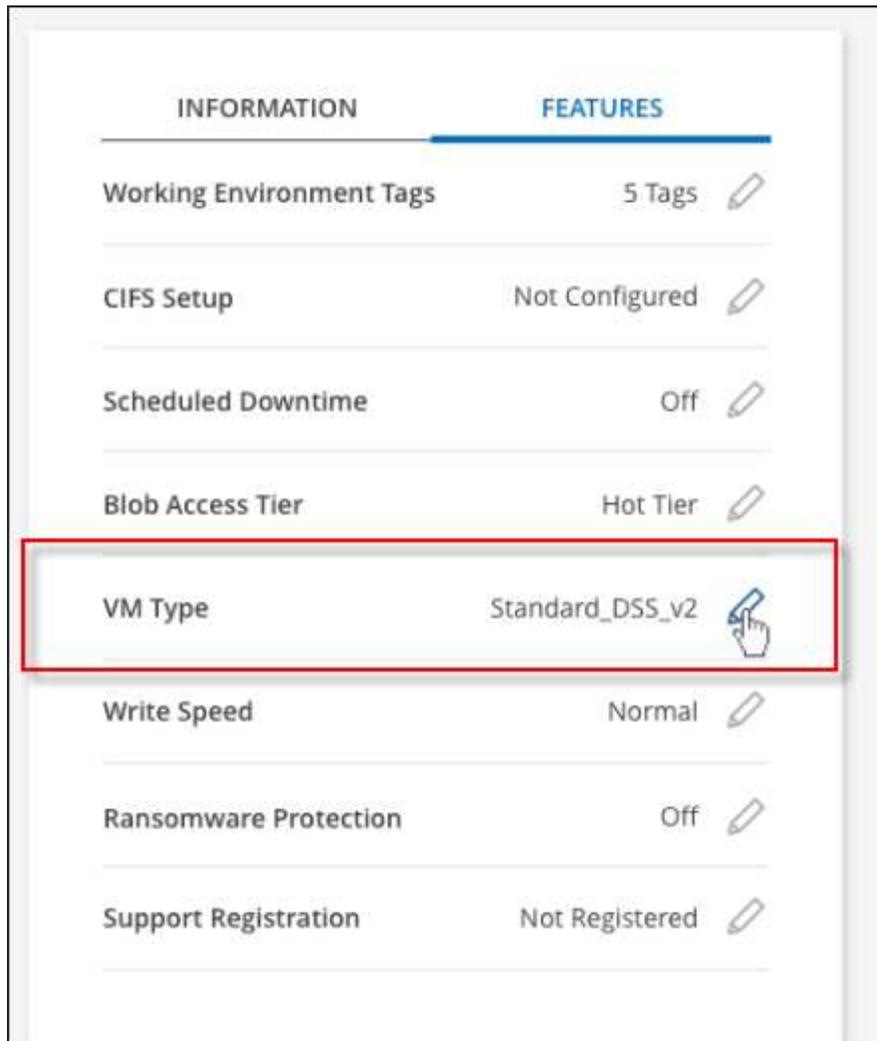
Bei HA-Paaren ist die Änderung unterbrechungsfrei. Ha-Paare stellen weiterhin Daten bereit.



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.



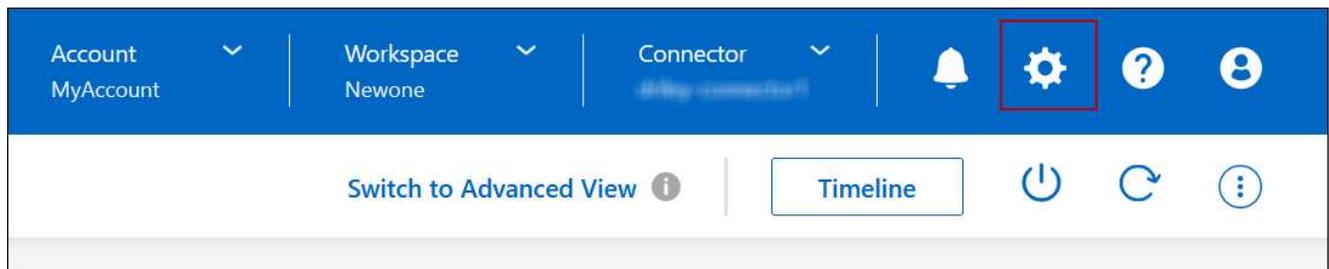
Dieser Prozess kann CIFS-Clients stören. Daten, die nicht von CIFS-Clients übertragen werden, können verloren gehen.

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.

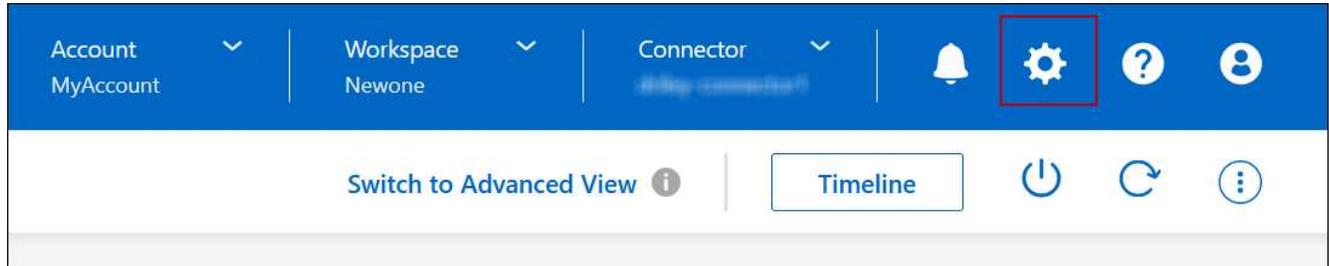
Deaktivieren Sie Azure Private Links, und verwenden Sie stattdessen Service-Endpunkte

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

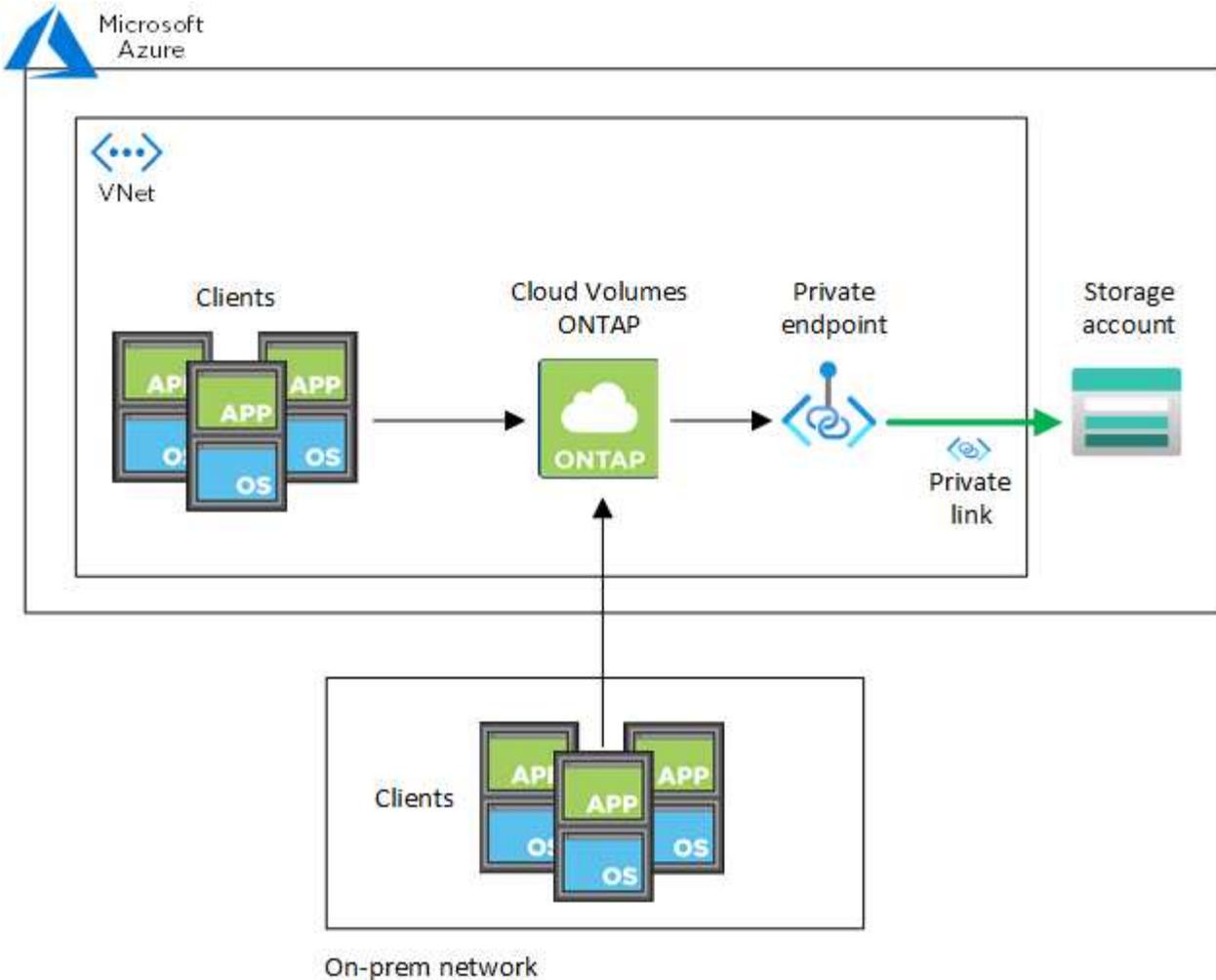
Wenn Sie optional mit benutzerdefinierten DNS arbeiten, müssen Sie von Ihren benutzerdefinierten DNS-Servern aus einen bedingten Forwarder zur Azure Private DNS Zone erstellen. Weitere Informationen finden Sie unter "[Die Dokumentation von Azure über einen DNS-Forwarder](#)".

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 (einzeln 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 Verzuwöllig 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

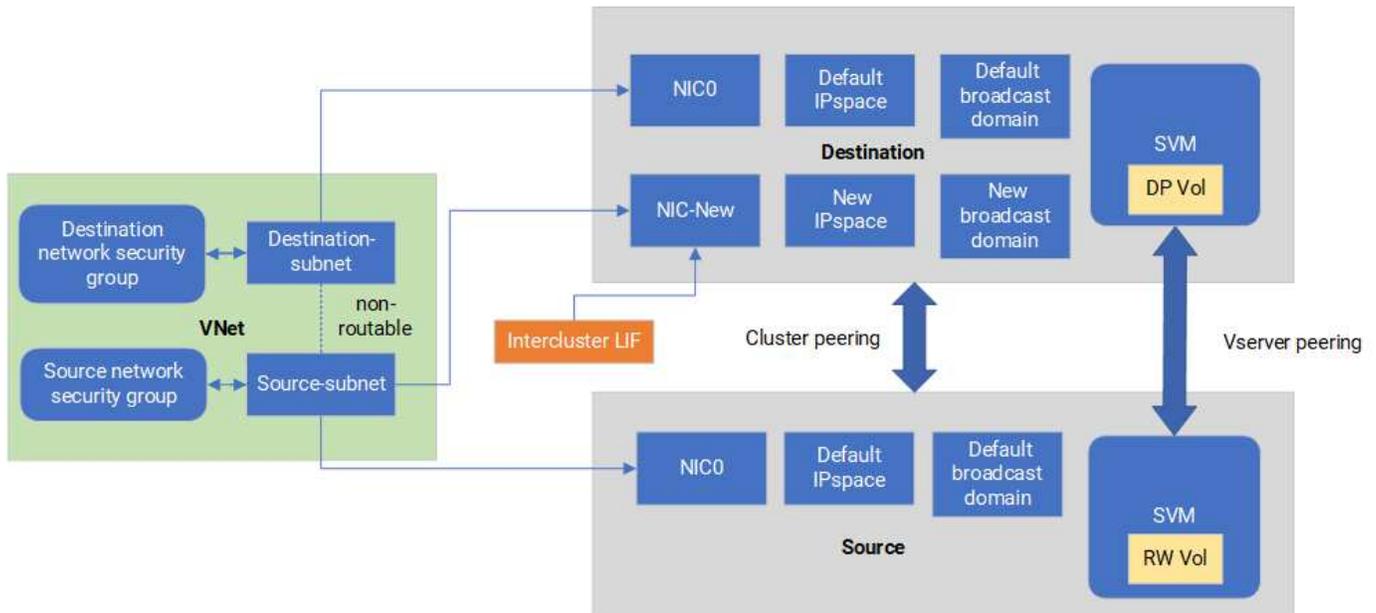
Mit Cloud Volumes ONTAP in Azure können Sie den SnapMirror Replizierungsverkehr von Daten- und Managementverkehr trennen. Um den SnapMirror Replizierungsverkehr von Ihrem Datenverkehr zu trennen, fügen Sie eine neue Netzwerkschnittstellenkarte (NIC), eine zugeordnete Intercluster LIF und ein nicht routingfähiges 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 routungsfähig 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-addr`s. Bei HA-Paaren sollten Sie die LIF-IP-Quelladresse für beide Nodes als auflisten `-peer-addr`s.

```
dest::> cluster peer create -peer-addr <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-addr`s. Bei HA-Paaren müssen die Ziel-Intercluster-LIF-IP-Adresse für beide Nodes als auflisten `-peer-addr`s.

```
src::> cluster peer create -peer-addr <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 `SnapshotMirrored` 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.

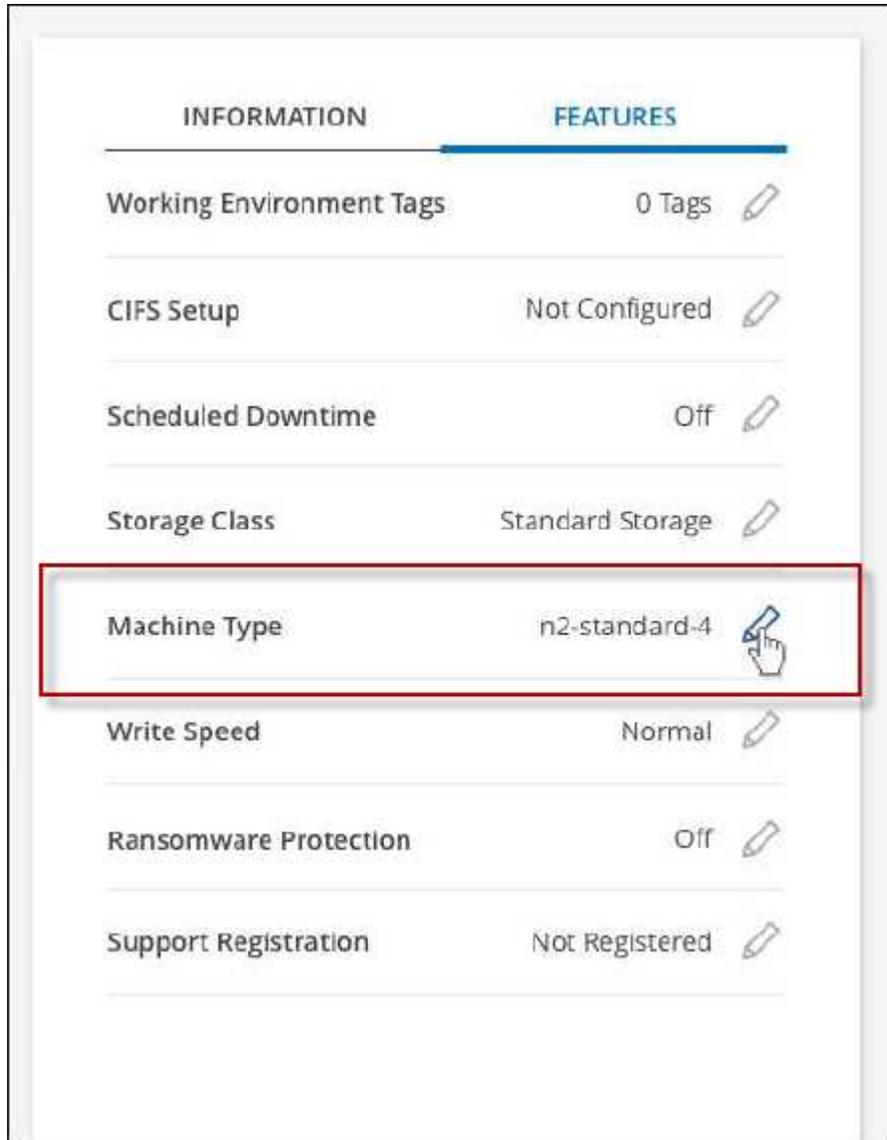
Bei HA-Paaren ist die Änderung unterbrechungsfrei. Ha-Paare stellen weiterhin Daten bereit.



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.

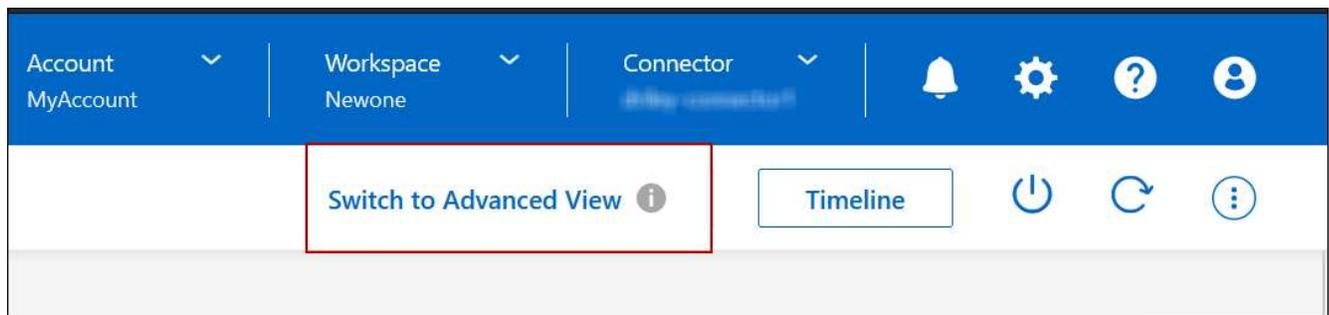
Darüber hinaus wird die rollenbasierte Zugriffssteuerung von System Manager nicht unterstützt.

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-Managementsschnittstelle 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"](#).

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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