



Verwenden Sie Cloud Volumes ONTAP

Cloud Volumes ONTAP

NetApp
December 05, 2022

Inhaltsverzeichnis

- Verwenden Sie Cloud Volumes ONTAP 1
 - Lizenzmanagement 1
 - Volume- und LUN-Administration 13
 - Aggregatadministration 37
 - Storage VM-Administration 40
 - Sicherheit und Datenverschlüsselung 73
 - Systemadministration 80
 - Systemzustand und Ereignisse 106

Verwenden Sie Cloud Volumes ONTAP

Lizenzmanagement

Management kapazitätsbasierter Lizenzen

Managen Sie Ihre kapazitätsbasierten Lizenzen über die digitale Geldbörse, um sicherzustellen, dass Ihr NetApp Konto über genügend Kapazität für Ihre Cloud Volumes ONTAP Systeme verfügt.

Kapazitätsbasierte Lizenzen ermöglichen es Ihnen, Cloud Volumes ONTAP pro tib Kapazität zu bezahlen.

Mit der *Digitalbörse* können Sie Lizenzen für Cloud Volumes ONTAP von einem einzigen Ort aus verwalten. Sie können neue Lizenzen hinzufügen und vorhandene Lizenzen aktualisieren.

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

Wie Lizenzen auf das Digital Wallet hinzugefügt werden

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. Wenn keine Fehler auftreten, fügt BlueXP die Lizenzen automatisch dem Digital Wallet hinzu.

Wenn BlueXP die Lizenz nicht hinzufügen kann, müssen Sie sie manuell zum Digital Wallet selbst hinzufügen. Wenn der Connector z. B. an einem Standort installiert ist, der keinen Internetzugang hat, müssen Sie die Lizenzen selbst hinzufügen. purchased licenses to your account, Erfahren Sie, wie Sie Ihrem Konto erworbene Lizenzen hinzufügen.

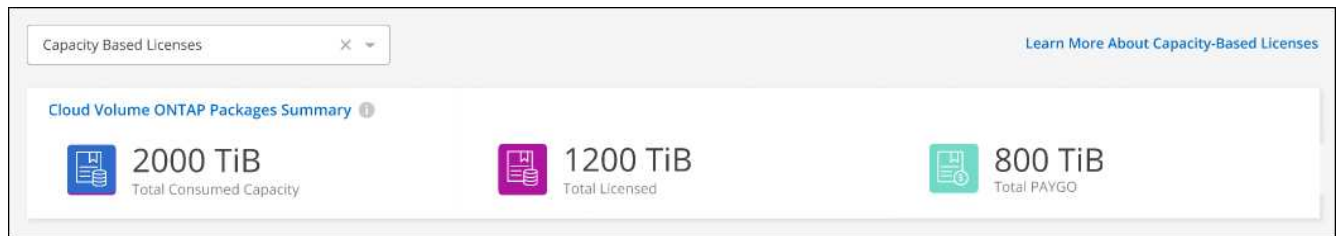
Zeigen Sie die verbrauchte Kapazität in Ihrem Konto an

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

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Digital Wallet** aus.
2. Zeigen Sie bei Auswahl von **kapazitätsbasierten Lizenzen** die Paketübersicht an, in der Sie die verbrauchte Kapazität, die gesamte lizenzierte Kapazität und die gesamte PAYGO-Gesamtkapazität angezeigt werden.
 - *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.
 - *Total lizenziert* ist die gesamte lizenzierte Kapazität (BYOL), die Sie von NetApp gekauft haben.
 - *Total PAYGO* ist die insgesamt bereitgestellte Kapazität anhand von Cloud-Marketplace-Abonnements. Das Aufladen über PAYGO erfolgt nur, wenn die verbrauchte Kapazität über der lizenzierten Kapazität liegt oder wenn in Digital Wallet keine BYOL-Lizenz verfügbar ist.

Hier ist ein Beispiel für ein Konto, das 2000 TiB verbrauchte Kapazität besitzt:



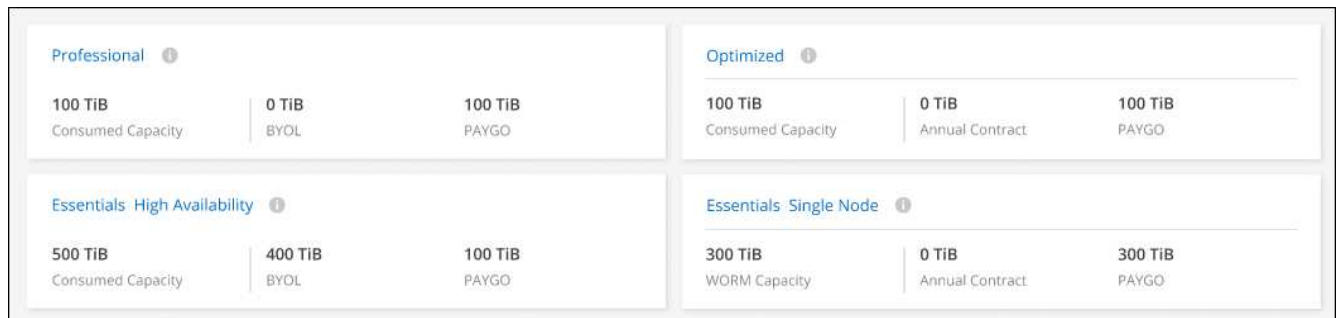
3. Zeigen Sie unter der Zusammenfassung die verbrauchte Kapazität für jedes Ihrer Lizenzierungspakete an.

- *Verbrauchte Kapazität* zeigt Ihnen die Gesamtkapazität 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"](#).

- *BYOL* zeigt Ihnen die lizenzierte Kapazität, die Sie von NetApp erworben haben.
- *PAYGO* zeigt Ihnen die insgesamt verbrauchte Kapazität nach Lizenzverbrauchsmodell.

Hier ein Beispiel für ein Konto mit mehreren Lizenzierungspaketen:



Fügen Sie gekaufte Lizenzen zu Ihrem Konto hinzu

Wenn Ihre erworbenen Lizenzen auf der digitalen Geldbörse nicht angezeigt werden, müssen Sie die Lizenzen zu BlueXP hinzufügen, damit die Kapazität für Cloud Volumes ONTAP verfügbar ist.

Was Sie und#8217;ll 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 linken Navigationsmenü die Option **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 die Lizenz automatisch 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.

Die Lizenzdatei (oder *Files* wenn Sie ein HA-Paar haben).

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **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

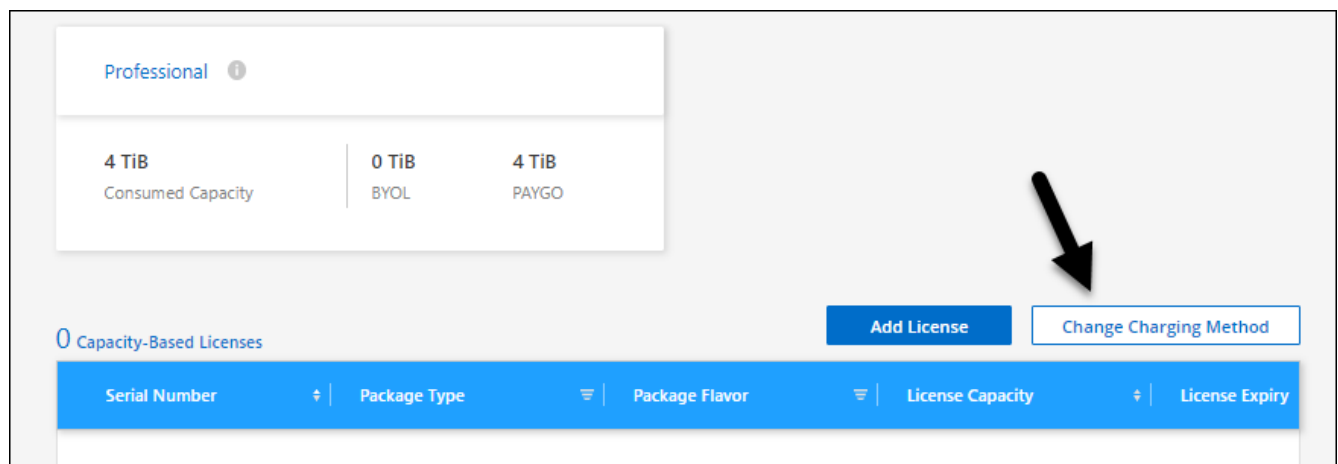
Sie können die Abrechnungsmethode für ein Cloud Volumes ONTAP System ändern, das kapazitätsbasierte Lizenzierung nutzt. Wenn Sie beispielsweise ein Cloud Volumes ONTAP-System mit dem Essentials-Paket bereitgestellt haben, können Sie es in das Professional-Paket ändern, wenn sich Ihre Geschäftsanforderungen ändern.

Das Ändern in oder von der Edge Cache Lizenz wird nicht unterstützt.

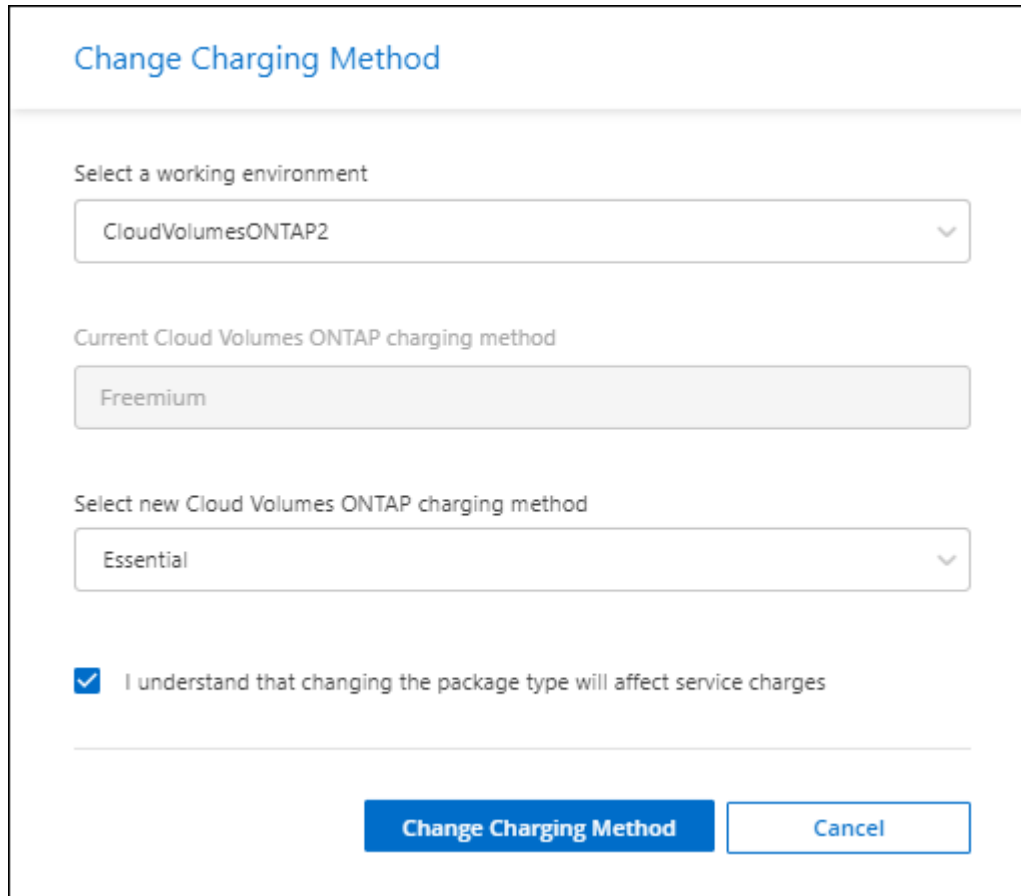
Wenn Sie über ein privates Angebot oder einen Vertrag von Ihrem Cloud-Provider-Markt verfügen, wird eine Änderung auf eine Abrechnungsmethode, die nicht im Vertrag enthalten ist, zu einer Abrechnung für BYOL (bei dem Kauf einer Lizenz von NetApp) oder PAYGO führen.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **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**.

BlueXP ändert die Lademethode des Cloud Volumes ONTAP-Systems.

Möglicherweise werden Sie auch feststellen, dass das Digital Wallet die verbrauchte Kapazität für jeden Pakettyp aktualisiert, um die soeben vorgenommene Änderung zu berücksichtigen.

Entfernen einer kapazitätsbasierten Lizenz

Wenn eine kapazitätsbasierte Lizenz abgelaufen ist und nicht mehr verwendet wird, können Sie sie jederzeit entfernen.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **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**.

Managen Sie Keystone Flex-Abonnements

Verwalten Sie Ihre Keystone Flex-Abonnements über das digitale Wallet, indem Sie Abonnements für die Verwendung mit Cloud Volumes ONTAP aktivieren. Sie können

auch Änderungen an der zugesagte Kapazität anfordern und die Verknüpfung von Abonnements aufheben.

Ein *Keystone Flex Subscription* ist ein von NetApp angebotene „Pay-as-you-grow“-Storage-Service.

Mit der *Digitalbörse* können Sie Lizenzen für Cloud Volumes ONTAP von einem einzigen Ort aus verwalten. Sie können neue Lizenzen hinzufügen und vorhandene Lizenzen aktualisieren.

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

Autorisieren Sie Ihr Konto

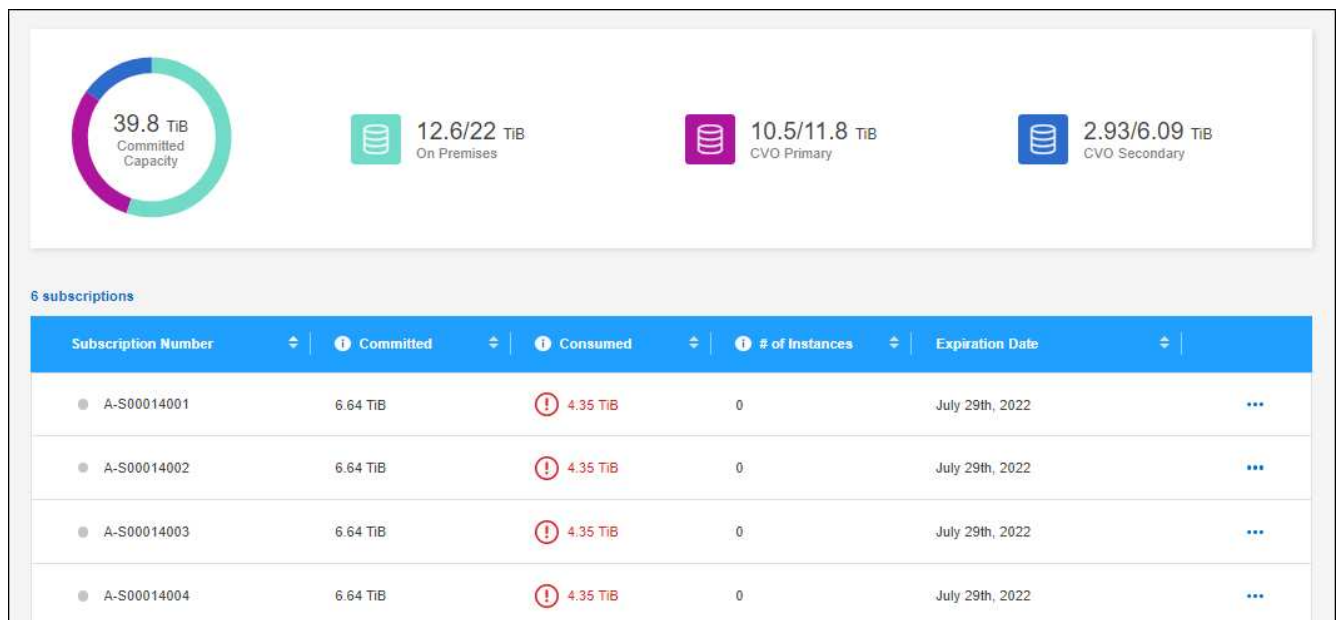
Bevor Sie Keystone Flex Abonnements in BlueXP verwenden und verwalten können, müssen Sie sich an NetApp wenden, um Ihr BlueXP Benutzerkonto mit Ihren Keystone Flex Abonnements zu autorisieren.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Digital Wallet** aus.
2. Klicken Sie Auf **Keystone Flex Abonnement**.
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 Flex Abonnement** zurück, um Ihre Abonnements anzuzeigen.



Verknüpfen Sie die Abonnements, die Sie mit Cloud Volumes ONTAP verwenden möchten.

Ein Abonnement verknüpfen

Nachdem NetApp Ihren Account autorisiert hat, müssen Sie die Keystone Flex Abonnements für die 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 linken Navigationsmenü die Option **Digital Wallet** aus.
2. Klicken Sie Auf **Keystone Flex Abonnement**.
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

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 Kapazität für ein Abonnement anpassen müssen, können Sie eine Anfrage direkt über die BlueXP-Schnittstelle senden.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Digital Wallet** aus.
2. Klicken Sie Auf **Keystone Flex Abonnement**.
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.

5. Scrollen Sie nach unten, geben Sie weitere Details für die Anfrage ein und klicken Sie dann auf **Absenden**.

Ihre Anfrage erstellt ein Ticket im NetApp System zur Verarbeitung.

Aufheben der Verknüpfung eines Abonnements

Wenn Sie kein Keystone Flex Abonnement mehr für neue Cloud Volumes ONTAP-Systeme verwenden möchten, können Sie die Verknüpfung des Abonnements 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 linken Navigationsmenü die Option **Digital Wallet** aus.
2. Klicken Sie Auf **Keystone Flex Abonnement**.
3. Klicken Sie für das Abonnement, das Sie aufheben möchten, auf **...** Und wählen Sie **Link aufheben**.

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

Verwalten Sie knotenbasierte Lizenzen in der digitalen Geldbörse, um sicherzustellen,

dass jedes Cloud Volumes ONTAP-System über eine gültige Lizenz mit der erforderlichen Kapazität verfügt.

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 *Digitalbörse* können Sie Lizenzen für Cloud Volumes ONTAP von einem einzigen Ort aus verwalten. Sie können neue Lizenzen hinzufügen und vorhandene Lizenzen aktualisieren.

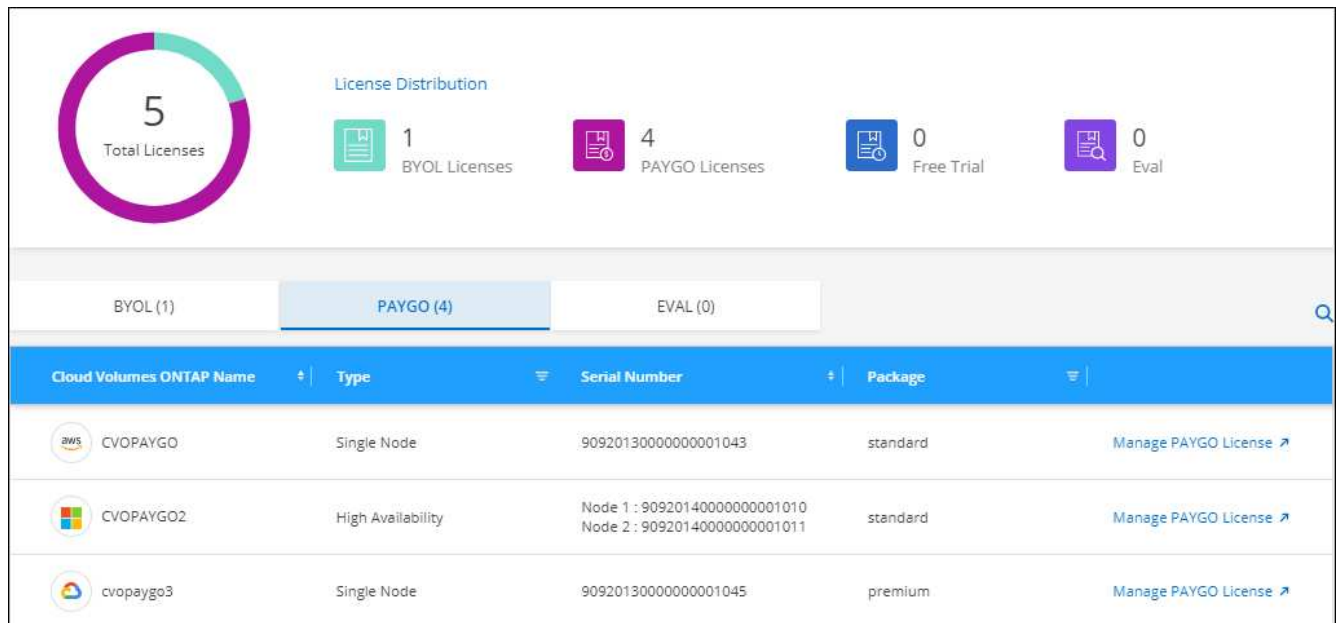
["Weitere Informationen zu Cloud Volumes ONTAP Lizenzen"](#).

Managen von PAYGO-Lizenzen

Auf der Seite „Digitale Geldbörse“ können Sie Details zu jedem Ihrer PAYGO Cloud Volumes ONTAP-Systeme anzeigen, einschließlich Seriennummer und PAYGO-Lizenztyp.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Digital Wallet** aus.
2. Wählen Sie im Dropdown-Menü auf der Registerkarte **Cloud Volumes ONTAP** die Option **Node-basierte Lizenzen** aus.
3. Klicken Sie auf **PAYGO**.
4. Zeigen Sie Details zu den einzelnen PAYGO-Lizenzen in der Tabelle an.



5. Klicken Sie bei Bedarf auf **PAYGO-Lizenz verwalten**, um die PAYGO-Lizenz zu ändern oder den Instanztyp zu ändern.

Byol-Lizenzen managen

Managen Sie die Lizenzen, die Sie direkt bei NetApp erworben haben, indem Sie Systemlizenzen und zusätzliche Kapazitätslizenzen hinzufügen bzw. entfernen.

Fügen Sie nicht zugewiesene Lizenzen hinzu

Fügen Sie dem digitalen Geldbeutel eine knotenbasierte Lizenz hinzu, sodass Sie beim Erstellen eines neuen Cloud Volumes ONTAP-Systems die Lizenz auswählen können. Die Digital Wallet identifiziert diese Lizenzen als *unassigned*.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **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**.

BlueXP fügt die Lizenz zum Digital Wallet hinzu. Die Lizenz wird erst dann als nicht zugewiesen identifiziert, wenn Sie sie einem neuen Cloud Volumes ONTAP-System zuordnen. Danach wechselt die Lizenz auf die Registerkarte **BYOL** im Digital Wallet.

Nicht zugewiesene knotenbasierte Exchange-Lizenzen

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

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 linken Navigationsmenü die Option **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**.

BYOL (14)	Eval (2)	Unassigned (3)	PAYGO (6)	<input type="text"/> <input type="button" value="Add Unassigned Licenses"/>		
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		...

- Wählen Sie den Dienst aus, mit dem Sie die Lizenz austauschen möchten.
- Wenn Sie dazu aufgefordert werden, wählen Sie eine zusätzliche Lizenz für das HA-Paar aus.
- Lesen Sie die gesetzliche Einwilligung und klicken Sie auf **Zustimmen**.

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

- Wechseln Sie zum "[NetApp Lizenzdatei-Generator](#)" Und loggen Sie sich mit Ihren Anmeldedaten für die NetApp Support Site ein.
- 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

Password*

Product Line*

Product Serial #*

NetApp ONTAP Cloud BYOL for AWS

90120130000000000555

Not only is protecting your data required by law, but your privacy is also very important to us. Please read and agree to the NetApp [Data Privacy Policy](#) before you continue. For information related to NetApp's privacy policy please click here [Privacy Policy](#) or contact privacy@netapp.com.

☒ I have read NetApp's new [Global Data Privacy Policy](#) and understand how NetApp and its selected partners may use my personal data.

- 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 linken Navigationsmenü die Option **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**.

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 linken Navigationsmenü die Option **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 linken Navigationsmenü die Option **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 linken Navigationsmenü die Option **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 linken Navigationsmenü die Option **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**.

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. [a volume,Weitere Informationen ..](#)
- Erstellen Sie ein Volume auf einem Datenaggregat Ihrer Wahl. [a volume,Weitere Informationen ..](#)
- Erstellen Sie ein Volume aus einer Vorlage, um das Volume gemäß den Workload-Anforderungen bestimmter Applikationen, wie z. B. Datenbanken oder Streaming-Services, zu optimieren. [a volume from a template,Weitere Informationen ..](#)
- Erstellung eines Volumes auf dem zweiten Node in einer HA-Konfiguration [a volume on the second node in an HA configuration,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, [a LUN to a host,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

Klicken Sie auf der Registerkarte Volumes auf **Volume hinzufügen > Neues Volume**.

Spezifische Aggregate

- a. Klicken Sie auf das Menüsymbol und dann auf **Erweitert > Erweiterte Zuweisung**.
- b. Klicken Sie auf das Menü für ein Aggregat.
- c. Klicken Sie auf **Create Volume**.

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-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.
Tags	Tags, die Sie einem Volume hinzufügen, werden dem zugeordnet " Applikationsvorlagen-Service ", Die Ihnen helfen, die Verwaltung Ihrer Ressourcen zu organisieren und zu vereinfachen.

Feld	Beschreibung
Snapshot-Richtlinie	Eine Snapshot Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot Kopien an. Bei einer NetApp Snapshot Kopie handelt es sich um ein zeitpunktgenaues Filesystem Image, das keine Performance-Einbußen aufweist und minimalen Storage erfordert. Sie können die Standardrichtlinie oder keine auswählen. Sie können keine für transiente Daten auswählen, z. B. tempdb für Microsoft SQL Server.

- 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 Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert.

a. **Festplattentyp:** Wählen Sie einen zugrunde liegenden Disk-Typ für das Volumen basierend auf Ihren Leistungsanforderungen und Kostenanforderungen.

- ["Dimensionierung Ihres Systems in AWS"](#)
- ["Dimensionierung Ihres Systems in Azure"](#)
- ["Dimensionierung Ihres Systems in Google Cloud"](#)

5. **Nutzungsprofil & Tiering Policy:** Wählen Sie aus, ob Sie Funktionen für die Speichereffizienz auf dem Volume aktivieren oder deaktivieren und dann ein auswählen ["Volume Tiering-Richtlinie"](#).

ONTAP umfasst mehrere Storage-Effizienzfunktionen, mit denen Sie die benötigte Storage-Gesamtmenge reduzieren können. NetApp Storage-Effizienzfunktionen bieten folgende Vorteile:

Thin Provisioning

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

Deduplizierung

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

Komprimierung

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

6. **Review:** Überprüfen Sie die Details über die Lautstärke und klicken Sie dann auf **Hinzufügen**.

BlueXP erstellt das Volume auf dem Cloud Volumes ONTAP System.

Erstellen Sie ein Volume anhand einer Vorlage

Wenn Ihr Unternehmen Cloud Volumes ONTAP Volume-Vorlagen erstellt hat, damit Sie Volumes implementieren können, die für die Workload-Anforderungen bestimmter Applikationen optimiert sind, befolgen Sie diese Schritte in diesem Abschnitt.

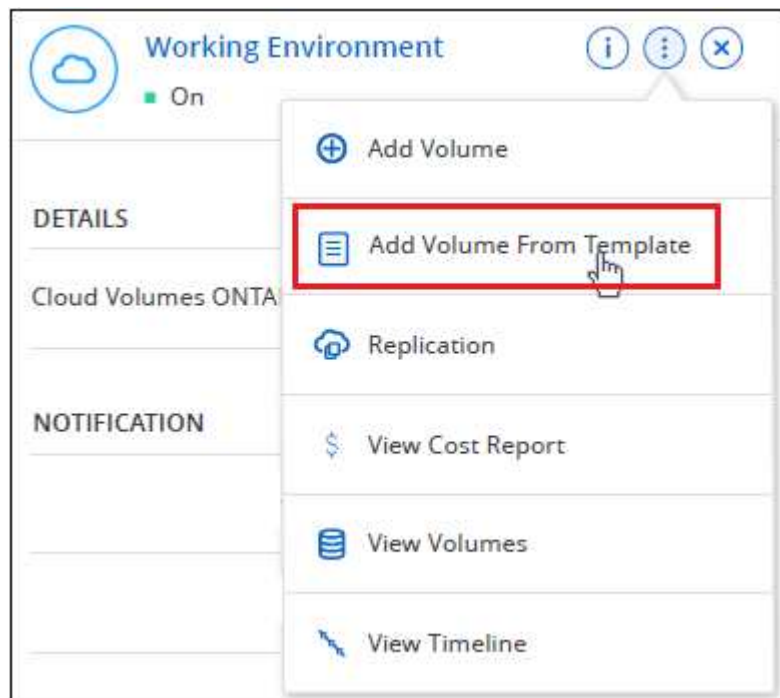
Die Vorlage sollte Ihnen die Arbeit erleichtern, da bestimmte Volume-Parameter bereits in der Vorlage definiert werden, z. B. Festplattentyp,-Größe, Protokoll, Snapshot-Richtlinie, Cloud-Provider, Und vieles mehr. Wenn ein Parameter bereits vordefiniert ist, können Sie einfach zum nächsten Volume-Parameter springen.



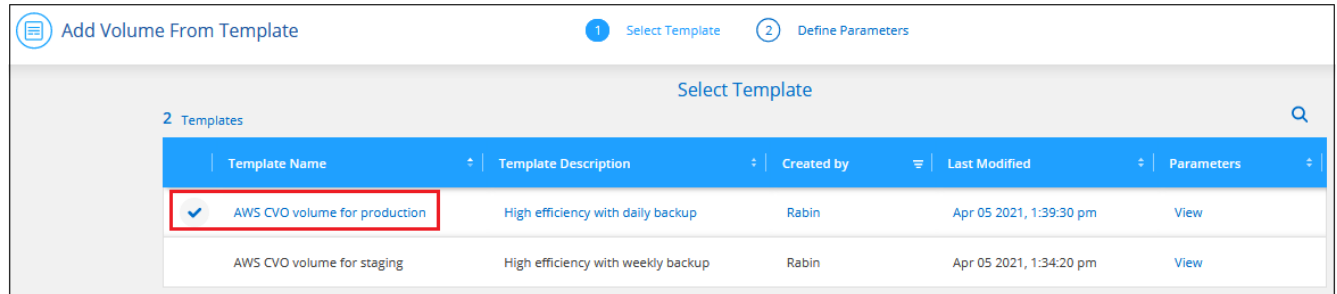
NFS- oder CIFS-Volumes können nur mit Vorlagen erstellt werden.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf den Namen des Cloud Volumes ONTAP-Systems, auf dem Sie ein Volume bereitstellen möchten.
3. Klicken Sie Auf > **Volumen Aus Vorlage Hinzufügen**.

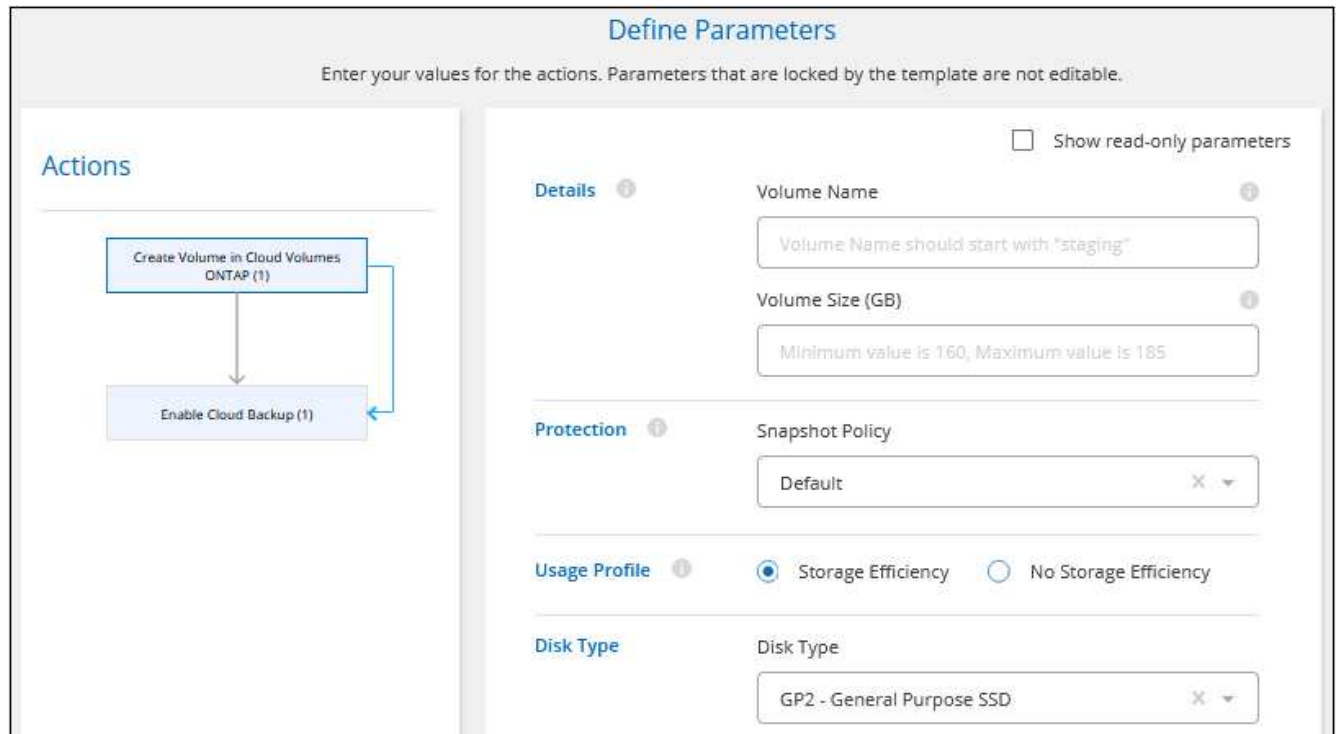


4. Wählen Sie auf der Seite *Vorlage auswählen* die Vorlage aus, die Sie zum Erstellen des Volumes verwenden möchten, und klicken Sie auf **Weiter**.



Template Name	Template Description	Created by	Last Modified	Parameters
✓ AWS CVO volume for production	High efficiency with daily backup	Rabin	Apr 05 2021, 1:39:30 pm	View
AWS CVO volume for staging	High efficiency with weekly backup	Rabin	Apr 05 2021, 1:34:20 pm	View

Die Seite *Define Parameters* wird angezeigt.



Define Parameters

Enter your values for the actions. Parameters that are locked by the template are not editable.

☐ Show read-only parameters

Actions

```
graph TD; A[Create Volume in Cloud Volumes ONTAP (1)] --> B[Enable Cloud Backup (1)];
```

Details

Volume Name
Volume Name should start with "staging"

Volume Size (GB)
Minimum value is 160, Maximum value is 185

Protection

Snapshot Policy
Default

Usage Profile

☒ Storage Efficiency ☐ No Storage Efficiency

Disk Type

Disk Type
GP2 - General Purpose SSD



Klicken Sie auf das Kontrollkästchen **schreibgeschützte Parameter anzeigen**, um alle Felder anzuzeigen, die von der Vorlage gesperrt wurden, wenn Sie die Werte für diese Parameter anzeigen möchten. Standardmäßig werden diese vordefinierten Felder ausgeblendet. Es werden nur die Felder angezeigt, die Sie ausfüllen müssen.

5. Im Bereich *context* wird die Arbeitsumgebung mit dem Namen der Arbeitsumgebung ausgefüllt, mit der Sie begonnen haben. Sie müssen die **Speicher-VM** auswählen, wo das Volume erstellt wird.
6. Fügen Sie Werte für alle Parameter hinzu, die nicht hartcodiert sind. Siehe a volume, Erstellen eines Volumes Sie finden Details zu allen Parametern, die Sie zur Implementierung eines Cloud Volumes ONTAP Volume abschließen müssen.
7. Wenn Sie keine weiteren Aktionen definieren müssen (z. B. Cloud-Backup konfigurieren), klicken Sie auf **Vorlage ausführen**.

Wenn es andere Aktionen gibt, klicken Sie im linken Fensterbereich auf die Aktion, um die erforderlichen Parameter anzuzeigen.



Wenn zum Beispiel die Aktion Cloud Backup aktivieren erfordert, dass Sie eine Backup-Richtlinie auswählen, können Sie dies jetzt tun.

8. Klicken Sie Auf **Ausführungsvorlage**.

Cloud Volumes ONTAP stellt das Volume bereit und zeigt eine Seite an, sodass der Fortschritt angezeigt wird.

Creating your resources

This process can take a few minutes.
Keep this page open to monitor progress, or you can close this page
and check the [Timeline](#) later for details.

Actions status

Create Volume in Cloud Volumes ONTAP	Success
Enable Cloud Backup	Pending

Außerdem werden, wenn sekundäre Aktionen in der Vorlage implementiert werden, z. B. wenn Sie Cloud Backup für das Volume aktivieren, diese Aktion ausgeführt.

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 das Menü-Symbol und dann auf **Erweitert > Erweiterte Zuweisung**.
4. Klicken Sie auf **Aggregat hinzufügen** und erstellen Sie dann 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**.

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.


Volumes managen


Sie können Volumes an neue Storage-Anforderungen anpassen. 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. Managen Sie Ihre Volumes:

Aufgabe	Aktion
Anzeigen von Informationen zu einem Volume	Wählen Sie ein Volume aus, und klicken Sie dann auf Info .
Bearbeiten eines Volumes (nur Volumes mit Lese-/Schreibzugriff)	<p>a. Wählen Sie ein Volume aus, und klicken Sie dann auf Bearbeiten.</p> <p>b. Ändern Sie die Snapshot-Richtlinie des Volumes, die NFS-Protokollversion, die NFS-Zugriffskontrollliste (Exportrichtlinie) oder die Freigabeberechtigungen und klicken Sie dann auf Update.</p> <div>  <p>Wenn Sie benutzerdefinierte Snapshot-Richtlinien benötigen, können Sie diese mit System Manager erstellen.</p> </div>

Aufgabe	Aktion
Klonen Sie ein Volume	<p>a. Wählen Sie ein Volume aus, und klicken Sie dann auf Clone.</p> <p>b. Ändern Sie den Klonnamen nach Bedarf, und klicken Sie dann auf Clone.</p> <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>
Wiederherstellen von Daten aus einer Snapshot Kopie auf einem neuen Volume	<p>a. Wählen Sie ein Volume aus, und klicken Sie dann auf Wiederherstellen aus Snapshot Kopie.</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>
Erstellen Sie bei Bedarf eine Snapshot Kopie	<p>a. Wählen Sie ein Volume aus, und klicken Sie dann auf Snapshot Kopie erstellen.</p> <p>b. Ändern Sie ggf. den Namen und klicken Sie dann auf Erstellen.</p>
Rufen Sie den NFS-Mount-Befehl ab	<p>a. Wählen Sie ein Volume aus, und klicken Sie dann auf Mount Command.</p> <p>b. Klicken Sie Auf Kopieren.</p>
Zeigen Sie die Ziel-IQN für ein iSCSI-Volume an	<p>a. Wählen Sie ein Volume aus, und klicken Sie dann auf Ziel-IQN.</p> <p>b. Klicken Sie Auf Kopieren.</p> <p>c. "Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen".</p>
Ändern Sie den zugrunde liegenden Festplattentyp	<p>a. Wählen Sie ein Volume aus, und klicken Sie dann auf Festplattentyp und Tiering Policy.</p> <p>b. Wählen Sie den Laufwerkstyp aus und klicken Sie dann auf Ändern.</p> <div>  <p>BlueXP verschiebt das Volume in ein vorhandenes Aggregat, das den ausgewählten Festplattentyp nutzt oder ein neues Aggregat für das Volume erstellt.</p> </div>

Aufgabe	Aktion
Ändern Sie die Tiering Policy	<p>a. Wählen Sie ein Volume aus, und klicken Sie dann auf Festplattentyp und Tiering Policy.</p> <p>b. Klicken Sie Auf Richtlinie Bearbeiten.</p> <p>c. Wählen Sie eine andere Richtlinie aus und klicken Sie auf Ändern.</p> <div>  <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>
Löschen Sie ein Volume	<p>a. Wählen Sie ein Volume aus, und klicken Sie dann auf Löschen.</p> <p>b. Klicken Sie zur Bestätigung erneut auf Löschen.</p>

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. Mit dieser Einstellung kann das Volume auf das 11-fache seiner Größe erweitert werden. Dieser Wert kann in den Einstellungen eines Connectors konfiguriert werden.

Wenn Sie die Größe Ihres Volumens ändern müssen, können Sie es durch ["ONTAP System Manager"](#). 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 das Menü-Symbol und dann auf **Erweitert > CIFS-Setup**.
2. Geben Sie die Einstellungen für den CIFS-Server an:

Aufgabe	Aktion
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind. <code>ifdef::gcp[]</code> Wenn Sie Google Managed Active Directory konfigurieren, kann AD standardmäßig mit der IP-Adresse 169.254.169.254 aufgerufen werden. <code>endif::gcp[]</code>
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.

Aufgabe	Aktion
Organisationseinheit	<p>Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers.</p> <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. 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 Dokumentation: 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.

3. Klicken Sie Auf **Speichern**.

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. how to correct capacity issues, Identifizieren, wie das Problem behoben werden kann.
2. Verschieben Sie Volumes basierend auf Ihrer Analyse, um Kapazitätsprobleme zu vermeiden:
 - volumes to another system to avoid capacity issues, Volumes werden in ein anderes System verschoben.
 - volumes to another aggregate to avoid capacity issues, Verschieben Sie Volumes zu einem anderen Aggregat auf demselben System.

Erkennen der Behebung von Kapazitätsproblemen

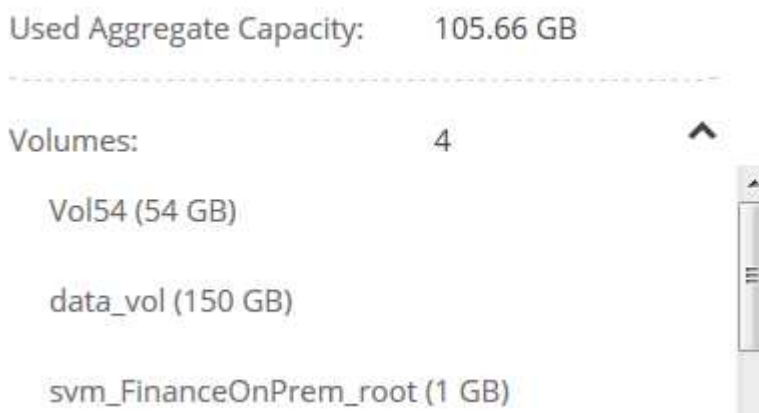
Wenn BlueXP keine Empfehlungen zum Verschieben eines Volumes zur Vermeidung von Kapazitätsproblemen bereitstellen kann, müssen Sie die Volumes identifizieren, die verschoben werden müssen und ob Sie sie zu einem anderen Aggregat auf demselben System oder einem anderen System verschieben möchten.

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 das Menüsymbol und dann auf **Erweitert > Erweiterte Zuweisung**.
 - b. Wählen Sie das Aggregat aus und klicken Sie dann auf **Info**.
 - c. Erweitern Sie die Liste der Volumes.



- d. Überprüfen Sie die Größe jedes Volumes, und wählen Sie ein oder mehrere Volumes aus, die aus dem Aggregat verschoben werden sollen.

Sie sollten Volumes auswählen, die groß genug sind, um Speicherplatz im Aggregat freizugeben, damit Sie in Zukunft zusätzliche Kapazitätsprobleme vermeiden können.

3. Wenn das System die Festplattengrenze nicht erreicht hat, sollten Sie die Volumes in ein vorhandenes Aggregat oder ein neues Aggregat auf demselben System verschieben.

Weitere Informationen finden Sie unter ["Verschieben von Volumes in ein anderes Aggregat, um Kapazitätsprobleme zu vermeiden"](#).

4. Wenn das System die Festplattengrenze erreicht hat, führen Sie einen der folgenden Schritte aus:
 - a. Löschen Sie nicht verwendete Volumes.
 - b. Ordnen Sie Volumes neu an, um Speicherplatz auf einem Aggregat freizugeben.

Weitere Informationen finden Sie unter ["Verschieben von Volumes in ein anderes Aggregat, um Kapazitätsprobleme zu vermeiden"](#).

- c. Verschieben Sie zwei oder mehr Volumes auf ein anderes System mit Speicherplatz.

Weitere Informationen finden Sie unter ["Verschieben von Volumes auf ein anderes System, um Kapazitätsprobleme zu vermeiden"](#).

Verschieben 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.

Sie können die folgenden Schritte in dieser Aufgabe ausführen, um die folgende Meldung "Aktion erforderlich" zu korrigieren:

```
Moving a volume is necessary to avoid capacity issues; however, BlueXP cannot perform this action for you because the system has reached the disk limit.
```

.Schritte

- . Identifizieren Sie ein Cloud Volumes ONTAP System mit verfügbarer Kapazität, oder implementieren Sie ein neues System.
- . Ziehen Sie die Quellarbeitsumgebung per Drag & Drop in die Ziellarbeitsumgebung, um eine einmalige Datenreplizierung des Volumes durchzuführen.

+

Weitere Informationen finden Sie unter ["Replizierung von Daten zwischen Systemen"](#).

1. Wechseln Sie zur Seite "Replication Status", und brechen Sie die SnapMirror Beziehung ab, um das replizierte Volume von einem Datensicherungsvolume in ein Lese-/Schreibvolume zu konvertieren.

Weitere Informationen finden Sie unter ["Managen von Plänen und Beziehungen zur Datenreplizierung"](#).

2. Konfigurieren Sie das Volume für den Datenzugriff.

Informationen über die Konfiguration eines Ziel-Volume für den Datenzugriff finden Sie unter ["ONTAP 9"](#)

[Express Guide für die Disaster Recovery von Volumes](#)".

3. Löschen Sie das ursprüngliche Volume.

Weitere Informationen finden Sie unter ["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.

Sie können die folgenden Schritte in dieser Aufgabe ausführen, um die folgende Meldung "Aktion erforderlich" zu korrigieren:

```
Moving two or more volumes is necessary to avoid capacity issues;  
however, BlueXP cannot perform this action for you.
```

.Schritte

. Überprüfen Sie, ob ein vorhandenes Aggregat über die verfügbare Kapazität für die Volumes verfügt, die Sie verschieben müssen:

+

.. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Erweiterte Zuweisung**.
.. Wählen Sie jedes Aggregat aus, klicken Sie auf **Info** und sehen Sie dann die verfügbare Kapazität (Aggregatskapazität minus genutzte Aggregatskapazität).

+

aggr1

Aggregate Capacity: 442.94 GB

Used Aggregate Capacity: 105.66 GB

1. Fügen Sie bei Bedarf Festplatten zu einem vorhandenen Aggregat hinzu:

a. Wählen Sie das Aggregat aus und klicken Sie dann auf **Add Disks**.

b. Wählen Sie die Anzahl der hinzuzufügenden Festplatten aus, und klicken Sie dann auf **Hinzufügen**.

2. Wenn keine Aggregate über verfügbare Kapazität verfügen, erstellen Sie ein neues Aggregat.

Weitere Informationen finden Sie unter ["Aggregate werden erstellt"](#).

3. Verwenden Sie System Manager oder die CLI, um die Volumes in das Aggregat zu verschieben.

4. In den meisten Fällen können Sie mit System Manager Volumes verschieben.

Anweisungen hierzu finden Sie im ["ONTAP 9 Volume Move Express Guide"](#).

Gründe, warum eine Volume-Verschiebung langsam durchführen könnte

Das Verschieben eines Volumes dauert möglicherweise länger, als erwartet wird, wenn eine der folgenden Bedingungen für Cloud Volumes ONTAP zutrifft:

- Das Volume ist ein Klon.
- Das Volume ist ein übergeordnetes Objekt eines Klons.
- Das Quell- oder Zielaggregat verfügt über eine einzige durchsatzoptimierte Festplatte (st1).
- 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.

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:

Die meisten Konfigurationen werden unterstützt. Wenn Sie ein Cloud Volumes ONTAP System mit der aktuellsten Version haben, sollten Sie gut zu gehen. "[Weitere Informationen](#)".

- Für AWS ist ein VPC Endpunkt zu S3 erforderlich. [to tier cold data to AWS S3,Weitere Informationen ..](#)
- Bei Azure müssen Sie nichts Unternehmen, solange BlueXP über die erforderlichen Berechtigungen verfügt. [to tier cold data to Azure Blob storage,Weitere Informationen ..](#)
- Für Google Cloud müssen Sie das Subnetz für privaten Google Access konfigurieren und ein Servicekonto einrichten. [to tier cold data to a Google Cloud Storage bucket,Weitere Informationen ..](#)

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. [that tiering is enabled on aggregates,Weitere Informationen ..](#)

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. data tiering after implementing the requirements, Solange es keine Verbindungs- oder Berechtigungsprobleme gibt. Danach müssen Sie nur noch Daten-Tiering auf den Volumes aktivieren (und in einigen Fällen, that tiering is enabled on aggregates, 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) handeln.



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"](#).

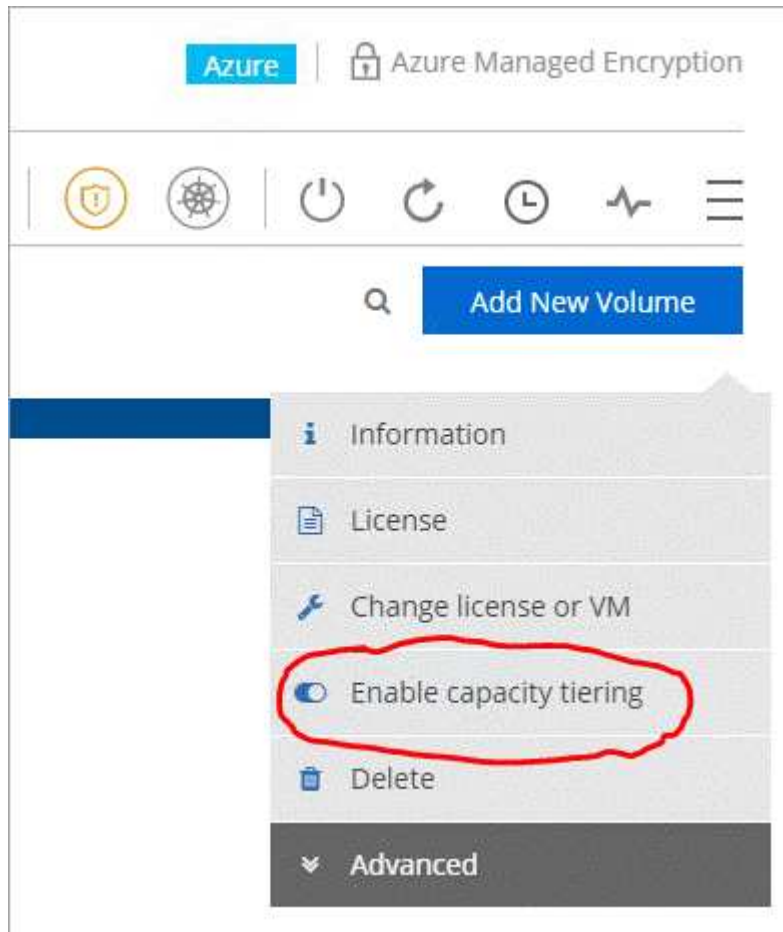
Aktivieren des Daten-Tiering nach der Implementierung der Anforderungen

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 aktivieren, wodurch der

Objektspeicher erstellt wird.

Schritte

1. „Stellen Sie sicher, dass Sie alle Anforderungen erfüllt haben.“
2. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
3. Doppelklicken Sie auf der Seite Arbeitsfläche auf den Namen der Cloud Volumes ONTAP-Instanz.
4. Klicken Sie auf das Menüsymbol und wählen Sie **Kapazitätsabteilung aktivieren**.



Diese Option wird nur angezeigt, wenn das Daten-Tiering nicht aktiviert werden konnte, wenn BlueXP das System erstellt hat.

In Google Cloud muss ein Servicekonto an Cloud Volumes ONTAP angehängt werden, bevor diese Option angezeigt wird. „Stellen Sie sicher, dass Sie alle Anforderungen erfüllt haben.“

5. Klicken Sie auf **Aktivieren**, damit BlueXP den Objektspeicher erstellen kann, den dieses Cloud Volumes ONTAP-System für Tiered-Daten verwendet.

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

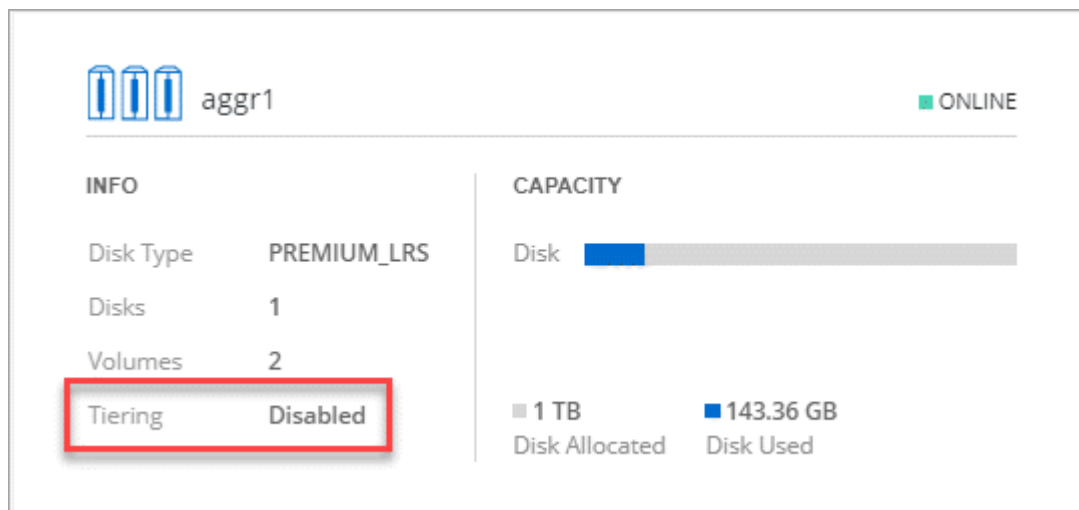
Sie Daten-Tiering auf einem Aggregat aktivieren können. BlueXP erzeugt das Volume auf einem vorhandenen Aggregat mit aktiviertem Tiering oder erzeugt ein neues Aggregat für das Volume, wenn es noch kein Daten-Tiering-fähiges Aggregat gibt.

- **Vorhandene Bänder**

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 das Menü-Symbol, klicken Sie auf **Erweitert** und dann auf **Erweiterte Zuweisung**.
3. 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**.

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

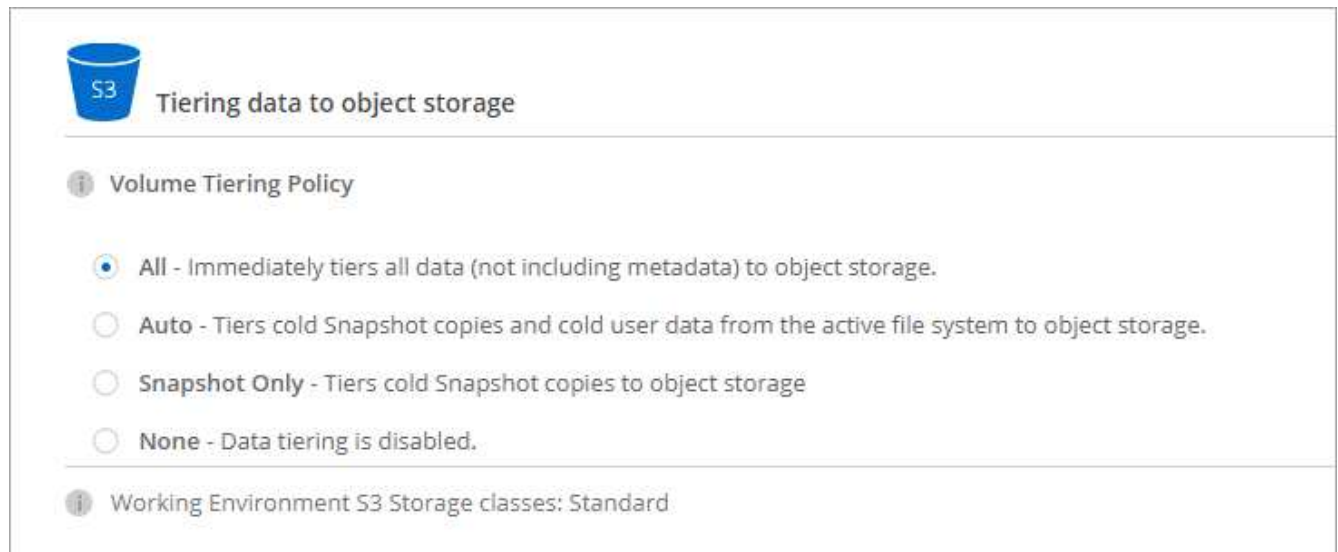
1. Erstellen Sie in der Arbeitsumgebung ein neues Volume, oder ändern Sie den Tier eines vorhandenen Volumes:

Aufgabe	Aktion
Erstellen Sie ein neues Volume	Klicken Sie Auf Neues Volume Hinzufügen .
Ändern Sie ein vorhandenes Volume	Wählen Sie das Volume aus und klicken Sie auf Disk Type & Tiering Policy .

2. Wählen Sie eine Tiering-Richtlinie aus.

Eine Beschreibung dieser Richtlinien finden Sie unter "[Data Tiering - Übersicht](#)".

Beispiel



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

 **S3 Tiering**

 What are storage tiers?

☒ **Enabled** ☐ **Disabled**

Note: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

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 lt 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 in der BlueXP-Konsole auf das Symbol **Einstellungen** und wählen Sie **Verbindungseinstellungen**.



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 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. Wählen Sie ein Volume aus, und klicken Sie dann auf **Ziel-IQN**.
4. Klicken Sie auf **Kopieren**, um den IQN-Namen zu kopieren.
5. 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 NFS-gelesene Daten aus einem Ursprungs-Volume (oder Quell-Volume) zwischenspeichert. Nachfolgende Lesezugriffe auf die zwischengespeicherten Daten führen zu einem schnelleren Zugriff auf diese Daten.

FlexCache Volumes beschleunigen den Zugriff auf Daten oder verlagern den Datenverkehr von Volumes, auf die stark zugegriffen wird. FlexCache Volumes tragen zu einer besseren Performance bei, insbesondere wenn Clients wiederholt auf dieselben Daten zugreifen müssen, da die Daten direkt ohne Zugriff auf das Ursprungs-Volume bereitgestellt werden können. FlexCache Volumes eignen sich gut für leseintensive System-Workloads.

BlueXP bietet derzeit kein Management von FlexCache Volumes, aber Sie können ONTAP FlexCache-Volumes mithilfe der Befehlszeilenschnittstelle oder des ONTAP System Managers erstellen und managen:

- "FlexCache Volumes für schnelleren Datenzugriff – Power Guide"
- "FlexCache Volumes werden in System Manager erstellt"

Ab Version 3.7.2 generiert BlueXP 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.



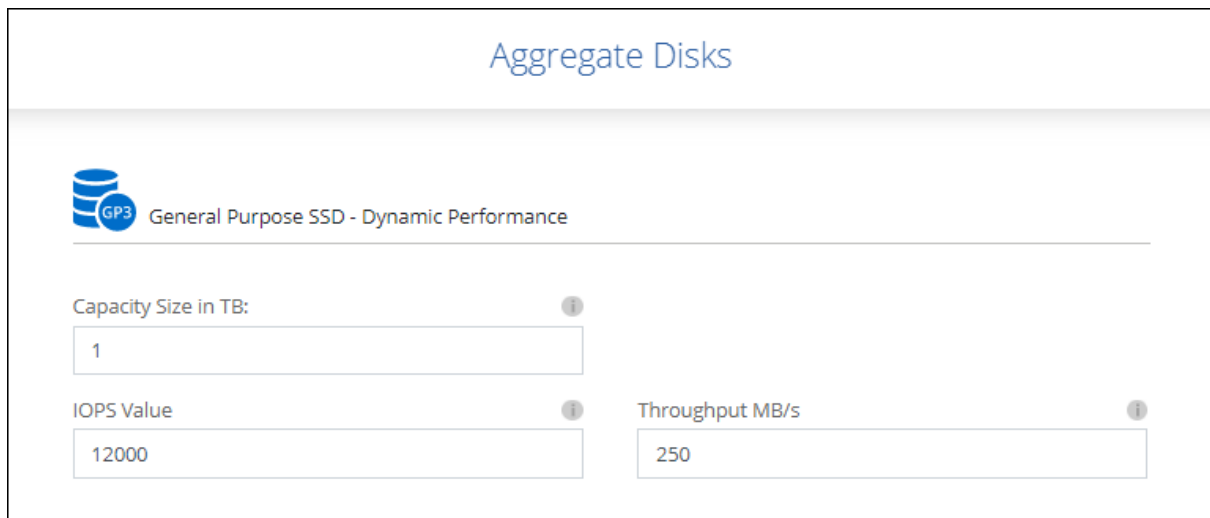
Alle Festplatten und Aggregate müssen direkt aus BlueXP erstellt und gelöscht werden. Sie sollten diese Aktionen nicht über ein anderes Management-Tool ausführen. Dies kann sich auf die Systemstabilität auswirken, die Fähigkeit zum Hinzufügen von Festplatten in der Zukunft beeinträchtigen und möglicherweise 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 das Menüsymbol und dann auf **Erweitert > Erweiterte Zuweisung**.
4. Klicken Sie auf **Add Aggregate** und geben Sie dann Details für das Aggregat an.

AWS

- Wenn Sie aufgefordert werden, einen Festplattentyp und eine Festplattengröße auszuwählen, lesen Sie ["Planen Sie Ihre Cloud Volumes ONTAP-Konfiguration in AWS"](#).
- Wenn Sie zur Eingabe der Kapazitätsgröße des Aggregats aufgefordert werden, erstellen Sie ein Aggregat auf einer Konfiguration, die die Elastic Volumes Funktion von Amazon EBS unterstützt. Der folgende Screenshot zeigt ein Beispiel für ein neues Aggregat, das aus gp3-Festplatten besteht.



["Erfahren Sie mehr über den Support für Elastic Volumes"](#).

Azure

Hilfe zu Festplattentyp und Festplattengröße finden Sie unter ["Planen Sie Ihre Cloud Volumes ONTAP-Konfiguration in Azure"](#).

Google Cloud

Hilfe zu Festplattentyp und Festplattengröße finden Sie unter ["Planen Sie Ihre Cloud Volumes ONTAP-Konfiguration in Google Cloud"](#).

5. 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.

Wenn Sie ein Aggregat löschen möchten, müssen Sie zunächst die Volumes im Aggregat gelöscht haben.

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 auf das Menü-Symbol und dann auf **Erweitert > Erweiterte Zuweisung**.
4. Verwalten Sie Ihre Aggregate:

Aufgabe	Aktion
Anzeigen von Informationen zu einem Aggregat	Wählen Sie ein Aggregat aus und klicken Sie auf Info .
Erstellen Sie ein Volume auf einem bestimmten Aggregat	Wählen Sie ein Aggregat aus und klicken Sie auf Create Volume .
Hinzufügen von Festplatten zu einem Aggregat	<div><div><div>a. Wählen Sie ein Aggregat aus und klicken Sie auf Add Disks.</div><div>b. Wählen Sie die Anzahl der Festplatten aus, die Sie hinzufügen möchten, und klicken Sie auf Hinzufügen.</div></div><div><div>Alle Festplatten in einem Aggregat müssen dieselbe Größe haben.</div></div></div>
Erhöhen Sie die Kapazität eines Aggregats, das Amazon EBS Elastic Volumes unterstützt	<div><div><div>a. Wählen Sie ein Aggregat aus und klicken Sie auf Kapazität erhöhen.</div><div>b. Geben Sie die zusätzliche Kapazität ein, die Sie hinzufügen möchten, und klicken Sie dann auf Hinzufügen.</div></div><div><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></div></div>
Löschen Sie ein Aggregat	<div><div><div>a. Wählen Sie ein Aggregat aus, das keine Volumes enthält, und klicken Sie auf Löschen.</div><div>b. Klicken Sie zur Bestätigung erneut auf Löschen.</div></div></div>

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.

Kontoadministratorrechte sind erforderlich, um Verbindungseinstellungen zu ändern.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Verbindungseinstellungen**.
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"](#).

Verhältnis Freier Speicherplatz

Löst eine Benachrichtigung aus, wenn das Verhältnis des freien Speicherplatzes auf einem Aggregat unter den angegebenen Schwellenwert fällt.

Das Verhältnis des freien Speicherplatzes berechnet sich wie folgt:

$$(\text{Gesamtkapazität} - \text{genutzte Gesamtkapazität im Aggregat}) / \text{Gesamtkapazität des Aggregats}$$

Kostenloses Speicherplatzverhältnis 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.

Details & Protection

Storage VM Name ?

svm_name1 ▼

Volume Name Size (GiB) ?

Snapshot Policy

default ▼

? Default Policy

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. Sie können den Namen der Storage VM ändern, wenn Sie strenge Namensstandards haben. Beispielsweise möchte der Name Ihnen entsprechen, wie Sie die Storage-VMs für Ihre ONTAP Cluster benennen.

Wenn Sie zusätzliche Storage-VMs für Cloud Volumes ONTAP erstellt haben, können Sie die Storage-VMs nicht aus BlueXP umbenennen. Sie müssen dies direkt von Cloud Volumes ONTAP mit System Manager oder



der CLI ausführen.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Information**.
2. Klicken Sie rechts neben dem Namen der Storage-VM auf das Bearbeiten-Symbol.

 **Working Environment Information**

ONTAP

Serial Number:	
System ID:	system-id-capacitytest
Cluster Name:	capacitytest
ONTAP Version:	9.7RC1
Date Created:	Jul 6, 2020 07:42:02 am
Storage VM Name:	svm_capacitytest 

3. Ändern Sie im Dialogfeld SVM-Name ändern den Namen und klicken Sie dann auf **Speichern**.

Managen von Storage VMs für Disaster Recovery

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

- ["Express Guide zur Vorbereitung des SVM-Disaster Recovery"](#)
- ["SVM Disaster Recovery Express Guide"](#)

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.

	Name	Insta...	Instance state	Instance type	Status check
<input type="checkbox"/>	danielleAws	i-070...	Running	m5.2xlarge	2/2 check
<input type="checkbox"/>	occmTiering0702	i-0a7...	Stopped	m5.2xlarge	-
<input checked="" type="checkbox"/>	cvoTiering1	i-02a...	Stopped	m5.2xlarge	-

Interface ID	Description
eni-07c301...	Interface for Node & Cluster Management, Inter-Cluster Communication, and Data - 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:

- 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.

- 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.

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.

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:

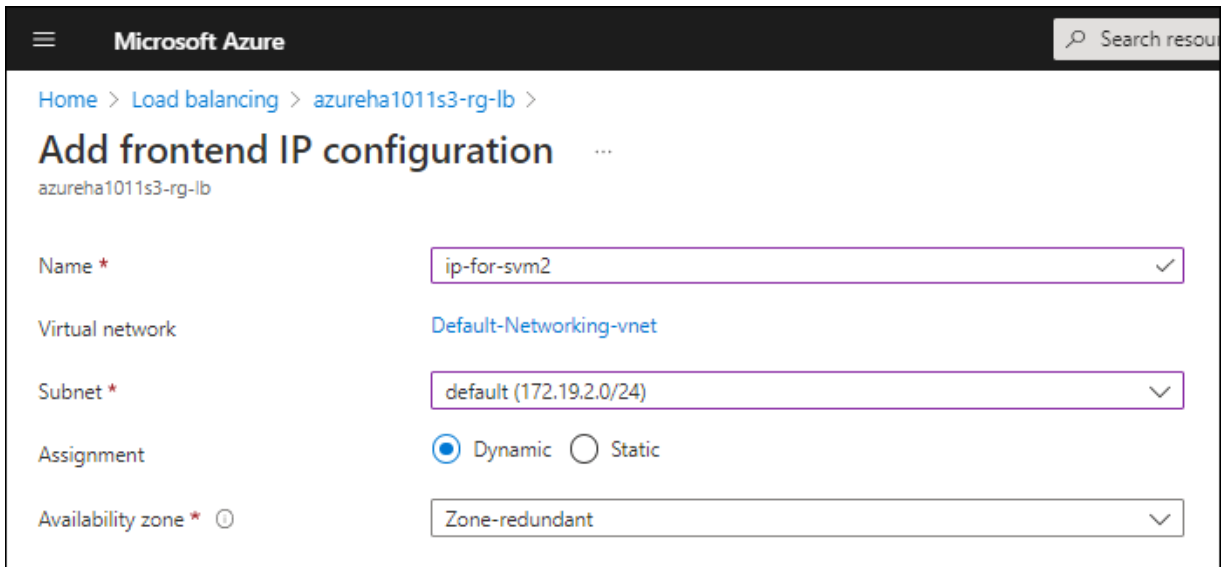
- Eine IP-Adresse für LIF-Zugriff auf NAS-Daten von Node 1
- Eine IP-Adresse für LIF-Zugriff auf NAS-Daten von Node 2
- Eine optionale IP-Adresse für eine Storage-VM (SVM)-Management-LIF

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 Microsoft Azure portal interface for adding a frontend IP configuration to a Load Balancer. The breadcrumb navigation is 'Home > Load balancing > azureha1011s3-rg-lb >'. The main heading is 'Add frontend IP configuration'. Below the heading, the resource name 'azureha1011s3-rg-lb' is displayed. The configuration form includes the following fields and options:

- 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 *

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.

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 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 Knoten 1
- Eine IP-Adresse für eine iSCSI-LIF auf Knoten 2

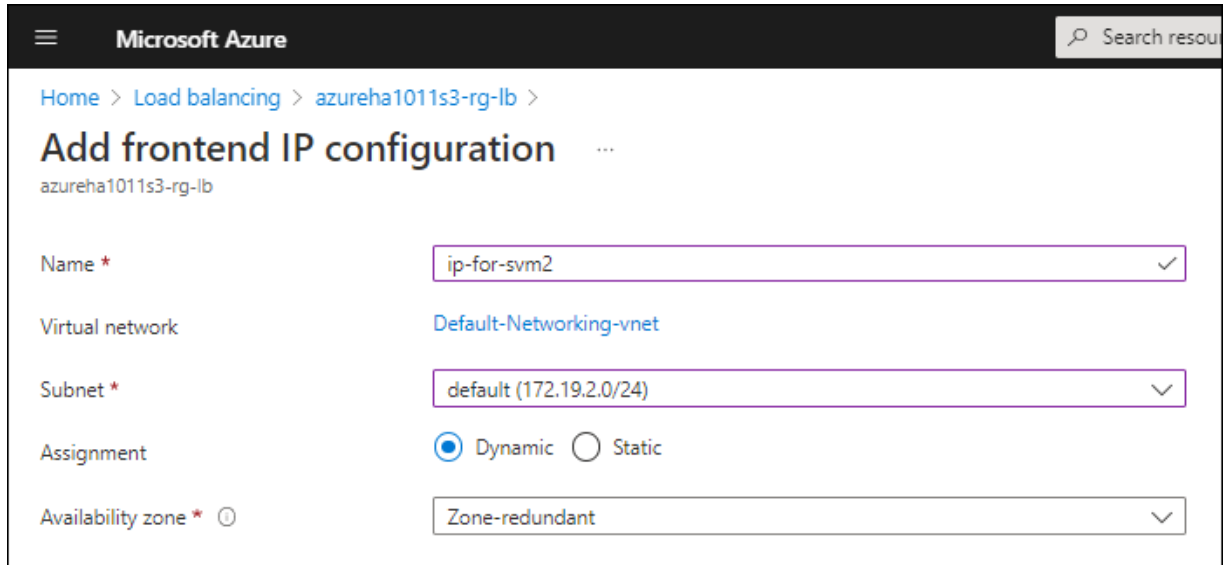
Die iSCSI LIFs sind für die DNS- und SMB-Kommunikation erforderlich. Dazu wird ein iSCSI-LIF verwendet, da bei einem Failover keine Migration durchgeführt wird.

- 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 die erforderliche Anzahl von Frontend-IP-Konfigurationen:
 - 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' (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 *

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

- 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.

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 -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. Daten-LIF erstellen:

```
network interface create -vserver <svm-name> -home-port e0a -address  
<iscsi-ip-address> -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 -destination 0.0.0.0/0 -vserver <svm-name>  
-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 <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
```

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 -destination 0.0.0.0/0 -vserver <svm-name>
-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 <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
```

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 -destination 0.0.0.0/0 -vserver <svm-name>  
-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> -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> -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.

Das Ändern der Services ist erforderlich, da Cloud Volumes ONTAP sicherstellen kann, dass die iSCSI-LIF für ausgehende Managementverbindungen verwendet werden kann.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

NFS

Befolgen Sie diese Schritte, um eine neue Storage-VM zusammen mit den erforderlichen LIFs zu erstellen.

Schritte

1. Erstellen Sie die Storage-VM und eine Route zur Storage-VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-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-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. 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.

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
```

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 -destination 0.0.0.0/0 -vserver <svm-name>  
-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-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 die Kommunikation zwischen DNS und SMB zu ermöglichen:

- 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> -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> -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.

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

```

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
gcpcvo-vm-ip-nic0-nodemgmt (10.138.0.46)

Alias IP ranges

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

+ 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](#)"

- Erstellen Sie die Storage-VM und eine Route zur Storage-VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway <ip-of-gateway-server>
```


3. Erstellen Sie eine Daten-LIF, indem Sie die IP-Adresse angeben, die Sie in Google Cloud hinzugefügt haben.

ISCSI

```
network interface create -vserver <svm-name> -home-port e0a -address  
<iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data  
-protocol iscsi
```

NFS oder SMB

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy disabled -firewall-policy data -home-port e0a -auto  
-revert true -failover-group Default
```

4. Optional: Erstellen Sie eine Storage-VM-Management-LIF, indem Sie die IP-Adresse angeben, die Sie in Google Cloud hinzugefügt haben.

```
network interface create -vserver <svm-name> -lif <lif-name> -role data  
-data-protocol none -address <svm-mgmt-ip-address> -netmask-length  
<length> -home-node <name-of-node1> -status-admin up -failover-policy  
system-defined -firewall-policy mgmt -home-port e0a -auto-revert false  
-failover-group Default
```

5. Weisen Sie der Storage-VM ein oder mehrere Aggregate zu.

```
vserver add-aggregates -vserver <svm-name> -aggregates <aggr1,aggr2>
```

Dieser Schritt ist erforderlich, da die neue Storage-VM Zugriff auf mindestens ein Aggregat benötigt, bevor Sie Volumes auf der Storage-VM erstellen können.

HA-Paar

Sie müssen die BlueXP API verwenden, um eine Speicher-VM auf einem Cloud Volumes ONTAP-System in Google Cloud zu erstellen. Die Verwendung der API (und nicht System Manager oder die CLI) ist erforderlich, da BlueXP die Storage VM mit den erforderlichen LIF-Diensten konfiguriert, sowie eine für die ausgehende SMB/CIFS-Kommunikation erforderliche iSCSI-LIF.

Beachten Sie, dass BlueXP die erforderlichen IP-Adressen in Google Cloud zuweist und die Storage VM mit einer Daten-LIF für SMB/NFS-Zugriff und einer iSCSI LIF für ausgehende SMB-Kommunikation erstellt.

Ab Version 3.9.19 erfordert der Connector folgende Berechtigungen zum Erstellen und Managen von Storage VMs für Cloud Volumes ONTAP HA-Paare:

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

Diese 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}
```

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.

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

Cloud Volumes ONTAP unterstützt kein Onboard-Verschlüsselungsmanagement.

Ihr Cloud Volumes ONTAP System sollte beim NetApp Support registriert sein. Auf jedem Cloud Volumes ONTAP System, das beim NetApp Support registriert ist, wird automatisch eine Lizenz für NetApp Volume Encryption installiert.

- ["Hinzufügen von Konten für die NetApp Support Site zu BlueXP"](#)
- ["Registrieren von Pay-as-you-go-Systemen"](#)



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

Schritte

1. Überprüfen Sie die Liste der unterstützten Schlüsselmanager im ["NetApp Interoperabilitäts-Matrix-Tool"](#).



Suchen Sie nach der **Key Manager**-Lösung.

2. ["Stellen Sie eine Verbindung zur Cloud Volumes ONTAP-CLI her"](#).
3. Externes Verschlüsselungsmanagement konfigurieren.
 - AWS, ["Die entsprechenden Anweisungen finden Sie in der ONTAP-Dokumentation"](#)
 - Azure: ["Azure Key Vault \(AKV\)"](#)
 - Google Cloud: ["Google Cloud Key Management Service"](#)

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.

Voraussetzungen

- 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).
- Multi-Tenant Encryption Key Management-Lizenz (MTEKM) installiert
- Sie müssen ein Cluster- oder SVM-Administrator sein
- Ein Active Azure Abonnement

Einschränkungen

- AKV kann nur auf einer Daten-SVM konfiguriert werden

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 , Und dann weiter zu .

*
*
*
*
*
*

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 Cloud Volumes ONTAP-Anwendung den Fensterbereich **Certificates & Secrets** aus.
2. Wählen Sie **Neues Kundegeheimnis** Geben Sie einen aussagekräftigen Namen für Ihr Kundegeheimnis ein. NetApp empfiehlt einen 24-monatigen Ablaufdatum, allerdings müssen Ihre spezifischen Cloud Governance-Richtlinien möglicherweise eine andere Einstellung erfordern.
3. Wählen Sie **Hinzufügen**, um den Client geheim zu speichern. Kopieren Sie sofort den **Wert** des Geheimnisses und speichern Sie ihn für zukünftige Konfigurationen sicher. Der geheime Wert wird nicht angezeigt, wenn Sie von der Seite wegnavigieren.

Erstellen Sie einen Azure Key Vault

1. Wenn Sie bereits über einen Azure Schlüsselaalt 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. Wählen Sie **Erstellen**. Geben Sie die erforderlichen Informationen einschließlich Ressourcengruppe, Region und Preisebene ein, und wählen Sie die Tage aus, um gelöschte Vaults zu behalten, und ob der Schutz zum Löschen aktiviert ist oder nicht. Für diese Konfiguration sind Standards ausreichend. Ihre spezifischen Cloud Governance-Richtlinien können jedoch unterschiedliche Einstellungen erfordern.
4. Wählen Sie **Weiter**, um eine Zugriffsrichtlinie auszuwählen.
5. Wählen Sie **Azure Disk Encryption** für die Option Volume Encryption und **Vault Access Policy** für das Berechtigungsmodell.
6. Wählen Sie **Zugangsrichtlinie Hinzufügen**.
7. Wählen Sie das Caret neben dem Feld **Configure from Template (optional)** aus. Wählen Sie dann **Schlüssel, Geheimnis und Zertifizierungsmanagement**.
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**: 19 ausgewählt
 - **Geheimberechtigungen**: 8 ausgewählt
 - **Zertifikatberechtigungen**: 16 ausgewählt
9. Wählen Sie **Hinzufügen**, um die Zugriffsrichtlinie zu erstellen.
10. Wählen Sie **Weiter**, um zu **Networking**-Optionen zu gelangen.
11. 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.)
12. 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 benötigen 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.

- 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)

- Dieser Prozess ist nur erforderlich, wenn Sie Azure Key Vault für eine HA Cloud Volumes ONTAP Arbeitsumgebung konfigurieren.
- Navigieren Sie im Azure-Portal zu **Virtual Networks**.
- 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.
- Wählen Sie in der Liste den Subnetznamen für Ihre Cloud Volumes ONTAP-Bereitstellung aus.
- Navigieren Sie zur Überschrift **Service-Endpunkte**. Wählen Sie im Dropdown-Menü in der Liste die Option **Microsoft.AzureActiveDirectory** aus.
- Wählen Sie **Speichern**, um Ihre Einstellungen zu erfassen.

Cloud Volumes ONTAP-Konfiguration

- Stellen Sie eine Verbindung zur Cluster-Management-LIF mit dem bevorzugten SSH-Client her.
- Geben Sie in ONTAP den erweiterten Berechtigungsmodus ein:
`set advanced -con off``
- Identifizieren Sie die gewünschte Daten-SVM und überprüfen Sie deren DNS-Konfiguration:
`vserver services name-service dns show`
 - 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`
 - Vergewissern Sie sich, dass der DNS-Service für die Daten-SVM erstellt wurde:
`vserver services name-service dns show`
- 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 Azure_key_name -key-id Azure_key_ID`
- Überprüfen Sie die Schlüsselmanager-Konfiguration:
`security key-manager external azure show`
- 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: ekvip_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. 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.

Beachten Sie bei der Verwendung von Cloud KMS, dass standardmäßig eine LIF der Daten-SVMs zur Kommunikation mit dem Endpunkt des Cloud-Verschlüsselungsmanagement verwendet wird. 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.

Voraussetzungen

- Cloud Volumes ONTAP muss Version 9.10.1 oder höher ausführen
- Volume Encryption (VE)-Lizenz installiert
- Multi-Tenant Encryption Key Management-Lizenz (MTEKM) installiert
- Sie müssen ein Cluster- oder SVM-Administrator sein
- Ein aktives Google Cloud Platform Abonnement

Einschränkungen

- Cloud KMS kann nur auf einer Daten-SVM konfiguriert werden

Konfiguration

Google Cloud

1. In Ihrer Google Cloud-Umgebung "[Erstellen Sie einen symmetrischen GCP-Schlüsselring und -Schlüssel](#)".
2. Erstellen Sie eine benutzerdefinierte Rolle für Ihr Cloud Volumes ONTAP-Servicekonto.

```
gcloud iam roles create kmsCustomRole
  --project=<project_id>
  --title=<kms_custom_role_name>
  --description=<custom_role_description>

  --permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA
```

3. Weisen Sie den Cloud-KMS-Schlüssel und das Cloud Volumes ONTAP-Servicekonto die benutzerdefinierte Rolle zu:

```
gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name
--location key_location --member serviceAccount:_service_account_Name_ --role
projects/customer_project_id/roles/kmsCustomRole
```

4. Service-Konto-JSON-Schlüssel herunterladen:

```
gcloud iam service-accounts keys create key-file --iam-account=sa-name
@project-id.iam.gserviceaccount.com
```

Cloud Volumes ONTAP

1. Stellen Sie eine Verbindung zur Cluster-Management-LIF mit dem bevorzugten SSH-Client her.

2. Wechseln zur erweiterten Berechtigungsebene:

```
set -privilege advanced
```

3. DNS für die Daten-SVM erstellen.

```
dns create -domains c.<project>.internal -name-servers server_address -vserver
SVM_name
```

4. CMEK-Eintrag erstellen:

```
security key-manager external gcp enable -vserver SVM_name -project-id project
-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name
```


`key_name`

5. Geben Sie bei der entsprechenden Aufforderung den JSON-Schlüssel Ihres GCP-Kontos ein.
6. Bestätigen Sie, dass der aktivierte Prozess erfolgreich war:
`security key-manager external gcp check -vserver svm_name`
7. OPTIONAL: Erstellen Sie ein Volume zum Testen der Verschlüsselung `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

Fehlerbehebung

Wenn Sie Fehler beheben müssen, können Sie die RAW REST API-Logs in den letzten beiden Schritten oben:

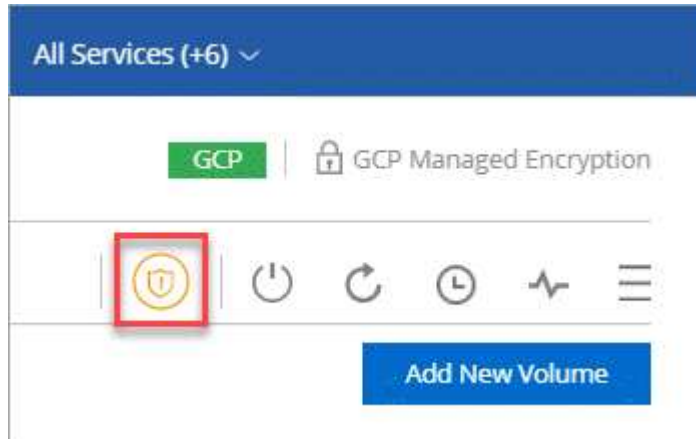
1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Besserer Schutz gegen Ransomware

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

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Symbol **Ransomware**.



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

Die NetApp Snapshot-Technologie bietet die branchenweit beste Lösung zur Behebung von Ransomware. Der Schlüssel zu einer erfolgreichen Recovery liegt im Restore aus einem nicht infizierten Backup. Snapshot Kopien sind schreibgeschützt, der Ransomware-Beschädigungen verhindert. Sie können außerdem die Granularität nutzen, um Images einer einzelnen Dateikopie oder einer kompletten Disaster-Recovery-Lösung zu erstellen.

- b. Klicken Sie auf **FPolicy** aktivieren, um die FPolicy Lösung von ONTAP zu aktivieren, die Dateivorgänge auf Basis der Dateierweiterung blockieren kann.

Diese präventive Lösung verbessert den Schutz vor Ransomware-Angriffen, indem sie gängige Ransomware-Dateitypen blockiert.

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

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
9.11.0	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.

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.

Upgrade wird vorbereitet

Bevor Sie ein Upgrade durchführen, müssen Sie überprüfen, ob die Systeme bereit sind und alle erforderlichen Konfigurationsänderungen vornehmen.

- for downtime
- that automatic giveback is still enabled
- SnapMirror transfers
- that aggregates are online

Planung von Ausfallzeiten

Wenn Sie ein Single-Node-System aktualisieren, stellt der Upgrade-Prozess das System für bis zu 25 Minuten offline, während dieser I/O-Unterbrechung ausgeführt wird.

Das Upgrade eines HA-Paars erfolgt unterbrechungsfrei und die I/O wird unterbrochen. Während dieses unterbrechungsfreien Upgrade-Prozesses wird jeder Node entsprechend aktualisiert, um den I/O-Datenverkehr für die Clients weiterhin bereitzustellen.

Überprüfen 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 Cloud Backup zur Erstellung von Backup-Dateien (so genannte SnapMirror Cloud) eine Implementierung von SnapMirror nutzt, müssen Backups bei einem Upgrade des Systems nicht ausgesetzt werden.

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.

In diesen Schritten wird die Verwendung von System Manager für Version 9.3 und höher beschrieben.

Schritte

1. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Erweiterte Zuweisung**.
2. Wählen Sie ein Aggregat aus, klicken Sie auf **Info** und überprüfen Sie dann, ob der Status online ist.

aggr1		
Aggregate Capacity:	88.57 GB	

Used Aggregate Capacity:	1.07 GB	

Volumes:	2	▼

AWS Disks:	1	▼

State:	online	

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**.

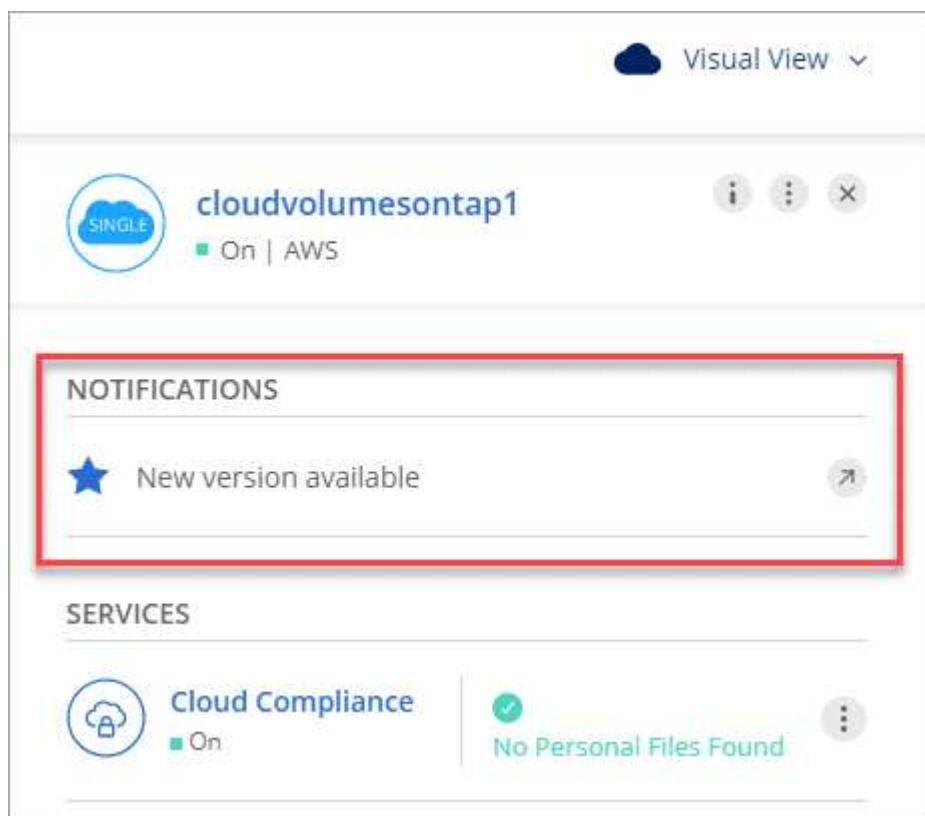
Upgrade von Cloud Volumes ONTAP

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 [from BlueXP notifications](#).

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 [an image available at a URL](#).

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.

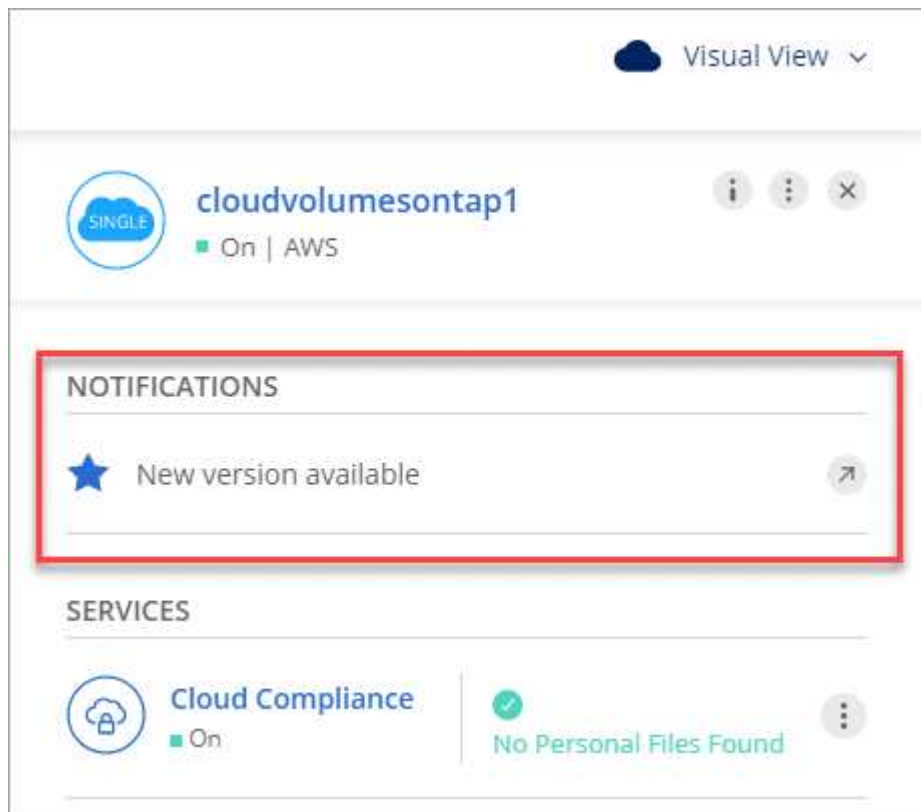
BlueXP-Vorgänge wie die Erstellung von Volumes oder Aggregaten dürfen auf dem Cloud Volumes ONTAP-System nicht ausgeführt werden.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.

2. Wählen Sie eine Arbeitsumgebung aus.

Im rechten Fensterbereich wird eine Benachrichtigung angezeigt, wenn eine neue Version verfügbar ist:



3. Wenn eine neue Version verfügbar ist, klicken Sie auf **Upgrade**.
4. Klicken Sie auf der Seite Release Information auf den Link, um die Versionshinweise für die angegebene Version zu lesen, und aktivieren Sie dann das Kontrollkästchen **Ich habe gelesen....**
5. Lesen Sie auf der Seite Endbenutzer-Lizenzvereinbarung (EULA) die EULA, und wählen Sie dann **Ich habe die EULA gelesen und genehmigt**.
6. Lesen Sie auf der Seite Prüfen und genehmigen die wichtigen Hinweise, wählen Sie **Ich verstehe...** und klicken Sie dann auf **Go**.

BlueXP startet das Software-Upgrade. Nach Abschluss der Softwareaktualisierung können Sie in der Arbeitsumgebung Aktionen ausführen.

Wenn Sie SnapMirror Transfers ausgesetzt haben, setzen Sie die Transfers mit System Manager fort.

Upgrade von einem Image, das über eine URL verfügbar ist

Sie können das Cloud Volumes ONTAP Software-Image auf dem Connector oder einem HTTP-Server platzieren und dann das Software-Upgrade von BlueXP starten. Möglicherweise verwenden Sie diese Option, wenn BlueXP zum Upgrade der Software nicht auf den S3-Bucket zugreifen kann.

Bevor Sie beginnen

- BlueXP-Vorgänge wie die Erstellung von Volumes oder Aggregaten dürfen auf dem Cloud Volumes ONTAP-System nicht ausgeführt werden.
- Wenn Sie HTTPS zum Hosten von ONTAP-Images verwenden, kann das Upgrade aufgrund von Problemen mit der SSL-Authentifizierung fehlschlagen, die durch fehlende Zertifikate verursacht werden.

Dieses Problem besteht darin, ein von einer Zertifizierungsstelle signiertes Zertifikat zu generieren und zu installieren, das für die Authentifizierung zwischen ONTAP und BlueXP verwendet wird.

In der NetApp Knowledge Base finden Sie Schritt-für-Schritt-Anleitungen:

["NetApp KB: So konfigurieren Sie BlueXP als HTTPS-Server, um Upgrade-Images zu hosten"](#)

Schritte

1. Optional: Richten Sie einen HTTP-Server ein, der das Cloud Volumes ONTAP Software-Image hosten kann.

Wenn Sie eine VPN-Verbindung zum virtuellen Netzwerk haben, können Sie das Cloud Volumes ONTAP Software-Image auf einem HTTP-Server in Ihrem eigenen Netzwerk platzieren. Andernfalls müssen Sie die Datei auf einem HTTP-Server in der Cloud platzieren.

2. Wenn Sie Ihre eigene Sicherheitsgruppe für Cloud Volumes ONTAP verwenden, stellen Sie sicher, dass die ausgehenden Regeln HTTP-Verbindungen zulassen, damit Cloud Volumes ONTAP auf das Software-Image zugreifen kann.



Die vordefinierte Cloud Volumes ONTAP-Sicherheitsgruppe erlaubt standardmäßig ausgehende HTTP-Verbindungen.

3. Beziehen Sie das Software-Image von ["Die NetApp Support Site"](#).
4. Kopieren Sie das Software-Image in ein Verzeichnis auf dem Connector oder auf einem HTTP-Server, von dem die Datei bereitgestellt wird.

Es sind zwei Pfade verfügbar. Der richtige Pfad hängt von Ihrer Connector-Version ab.

- `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`
- `/opt/application/netapp/cloudmanager/ontap/images/`

5. Klicken Sie in BlueXP in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Cloud Volumes ONTAP aktualisieren**.
6. Geben Sie auf der Seite Aktualisierungssoftware 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>`

7. Klicken Sie zur Bestätigung auf **Weiter**.

BlueXP startet das Software-Update. Nach Abschluss der Softwareaktualisierung können Sie in der Arbeitsumgebung Aktionen ausführen.

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. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**
3. Doppelklicken Sie auf der Seite Arbeitsfläche auf den Namen des Systems, das Sie registrieren möchten.
4. Klicken Sie auf das Menü-Symbol und dann auf **Support-Registrierung**:



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

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. Klicken Sie in der Arbeitsumgebung auf das Uhrensymbol:



2. Geben Sie den Zeitplan für das Herunterfahren an:

- a. Wählen Sie aus, ob Sie das System täglich, jeden Werktag, jedes Wochenende oder eine beliebige Kombination der drei Optionen herunterfahren möchten.

b. Geben Sie an, wann und wie lange das System ausgeschaltet werden soll.

Beispiel

Das folgende Bild zeigt einen Zeitplan, der BlueXP dazu auffordert, das System jeden Samstag um 12:00 Uhr herunterzufahren Für 48 Stunden. BlueXP startet das System jeden Montag um 12:00 Uhr neu

☐ **Turn off every weekday**
Mon, Tue, Wed, Thu, Fri

turn off at 08 : 00 PM for 12 Hours (1-24)

☒ **Turn off every weekend**
Sat

turn off at 12 : 00 AM for 48 Hours (1-48)

3. Klicken Sie Auf **Speichern**.

BlueXP speichert den Zeitplan. Das Uhrensymbol ändert sich, um anzuzeigen, dass ein Zeitplan festgelegt wurde:

Beenden von Cloud Volumes ONTAP

Stoppen von Cloud Volumes ONTAP erspart Ihnen das Ansteigen von Computing-Kosten und erstellt Snapshots der Root- und Boot-Festplatten, was bei der Fehlerbehebung hilfreich sein kann.



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.

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.

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. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Schreibgeschwindigkeit**.
2. Wählen Sie **normal** oder **hoch**.

Wenn Sie „hoch“ wählen, müssen Sie die „Ich verstehe...“-Aussage lesen und bestätigen, indem Sie das Kästchen aktivieren.

3. Klicken Sie auf **Speichern**, überprüfen Sie die Bestätigungsmeldung und klicken Sie dann auf **Weiter**.

Ändern 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. Klicken Sie in der Arbeitsumgebung auf das Menüsymbol und dann auf **Erweitert > Passwort festlegen**.
2. Geben Sie das neue Passwort zweimal ein und klicken Sie dann auf **Speichern**.

Das neue Kennwort muss sich von einem der letzten sechs Kennwörter unterscheiden.

Hinzufügen, Entfernen oder Löschen von Systemen

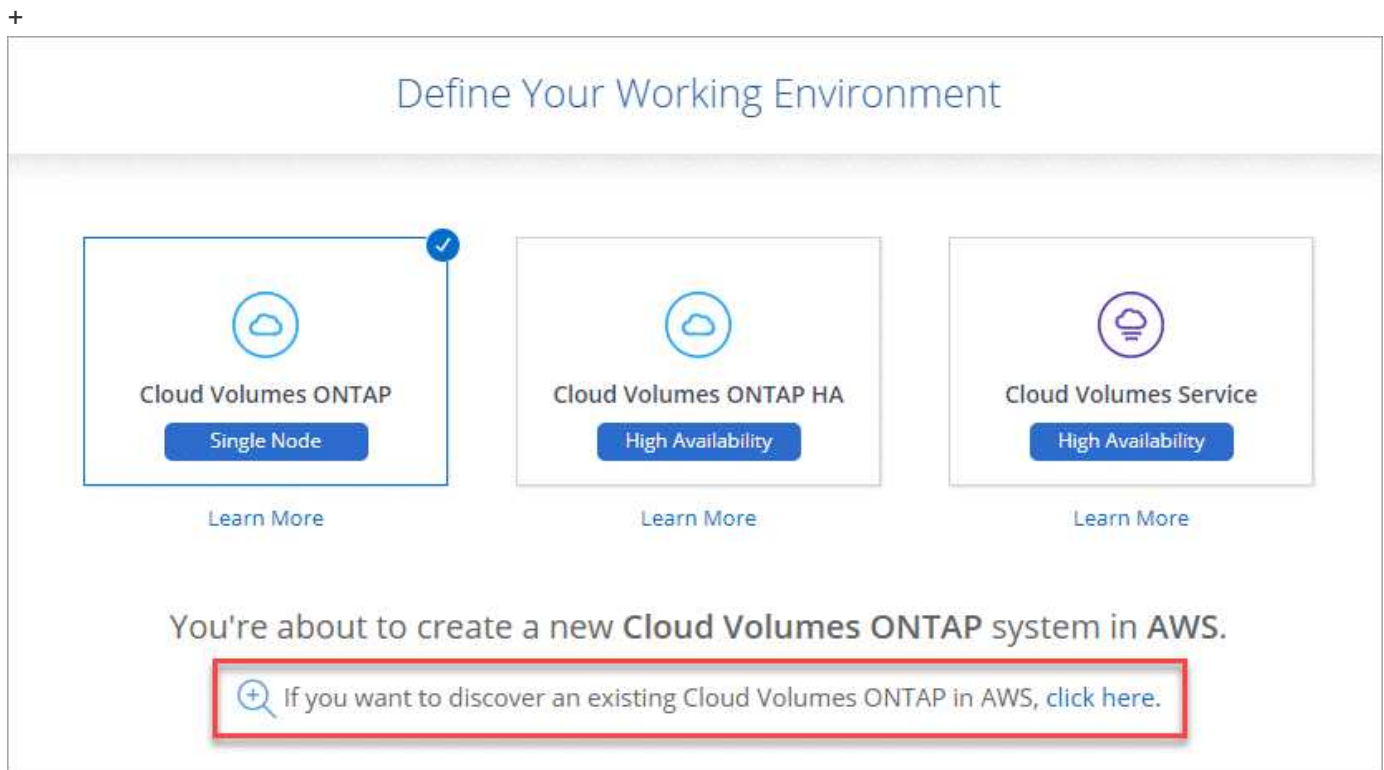
Hinzufügen vorhandener Cloud Volumes ONTAP-Systeme zu BlueXP

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

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**.

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.

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. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Tools**.



2. Klicken Sie auf der Seite Extras auf **Starten**.
3. Wählen Sie die Cloud Volumes ONTAP Arbeitsumgebung aus, die Sie entfernen möchten.
4. Klicken Sie auf der Seite „Prüfen und genehmigen“ auf **Los**.

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 Cloud-Backup und Instanzen für Cloud-Daten Sense und Monitoring verwaltet 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 Cloud Backup in der Arbeitsumgebung aktiviert haben, prüfen Sie, ob die gesicherten Daten weiterhin benötigt werden ["Löschen Sie die Backups, falls erforderlich"](#).

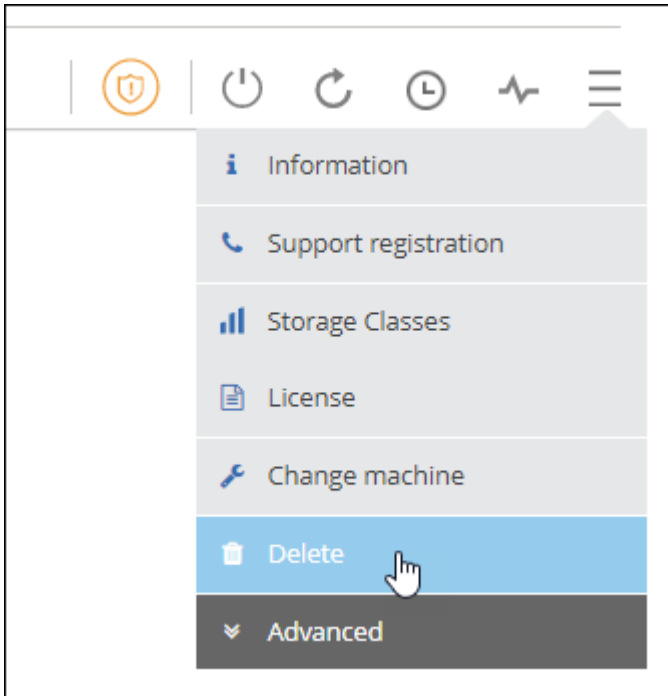
Cloud Backup ist durch das Design unabhängig von Cloud Volumes ONTAP. Cloud Backup nicht

automatisch löschen Backups, wenn Sie ein Cloud Volumes ONTAP-System löschen, und es gibt keine aktuelle Unterstützung in der UI, die Backups zu löschen, nachdem das System gelöscht wurde.

2. Wenn Sie Cloud Data Sense in dieser Arbeitsumgebung aktiviert haben und keine anderen Arbeitsumgebungen diesen Service verwenden, müssen Sie die Instanz für den Dienst löschen.

["Erfahren Sie mehr über die Instanz Cloud Data Sense"](#).

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 auf das Menüsymbol und dann auf **Löschen**.



- c. Geben Sie 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.

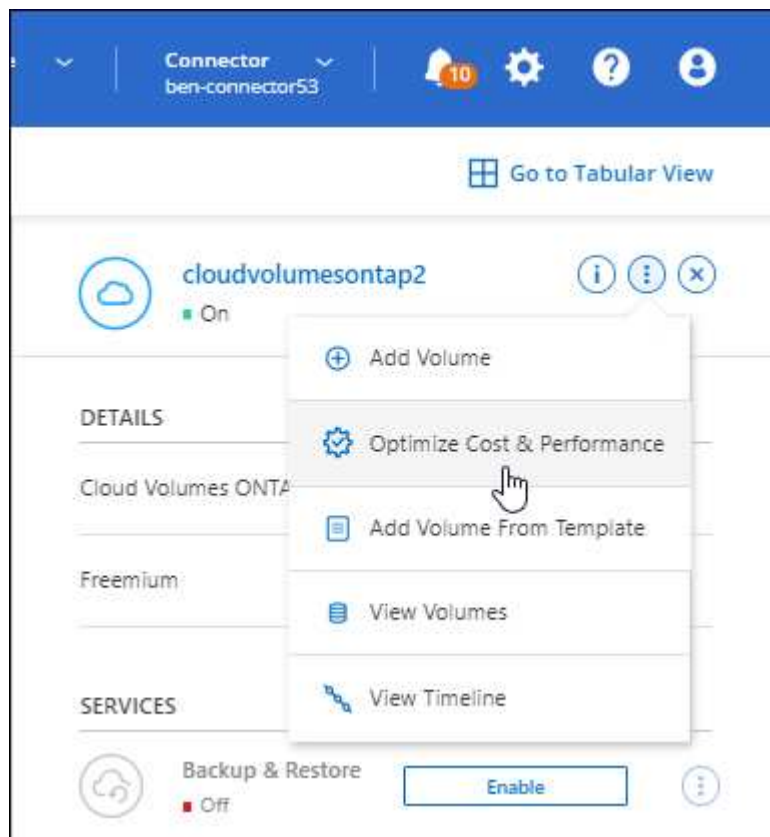
Bei HA-Paaren ist die Änderung unterbrechungsfrei. Ha-Paare stellen weiterhin Daten bereit.



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.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Wählen Sie auf der Arbeitsfläche die Arbeitsumgebung aus.
3. Klicken Sie im rechten Fensterbereich auf das Menüsymbol und wählen Sie **Kosten & Leistung optimieren**.



Diese Option ist auch verfügbar, indem Sie die Arbeitsumgebung aufrufen, das Aktionsmenü öffnen und **Instanz ändern** wählen.

4. Wenn Sie eine knotenbasierte PAYGO-Lizenz verwenden, können Sie optional eine andere Lizenz auswählen.
5. Wählen Sie einen Instanztyp aus, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Auswirkungen der Änderung verstehen, und klicken Sie dann auf **OK**.

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. Klicken Sie in der Arbeitsumgebung auf das Menü-Symbol und dann auf **Information**.
2. Klicken Sie Auf **Routentabellen**.
3. Ändern Sie die Liste der ausgewählten Routentabellen und klicken Sie dann auf **Speichern**.

BlueXP sendet eine AWS-Anforderung, um die Routingtabellen zu ändern.

Überwachung der AWS-Ressourcenkosten

Mit BlueXP können Sie sich die Ressourcenkosten anzeigen lassen, die für die Ausführung von Cloud Volumes ONTAP in AWS anfallen. Außerdem erfahren Sie, wie viel Geld Sie durch den Einsatz von NetApp Funktionen zur Senkung der Storage-Kosten gespart haben.

BlueXP aktualisiert die Kosten, wenn Sie die Seite aktualisieren. Die endgültigen Kostendetails finden Sie in AWS.

Schritt

1. Stellen Sie sicher, dass BlueXP Kosteninformationen von AWS beziehen kann:
 - a. Stellen Sie sicher, dass die IAM-Richtlinie, die BlueXP Berechtigungen bereitstellt, die erforderlichen Berechtigungen enthält.

["Zeigen Sie die erforderlichen Berechtigungen an"](#)

- b. ["Aktivieren Sie das Tag **WorkingEnvironment ID**"](#).

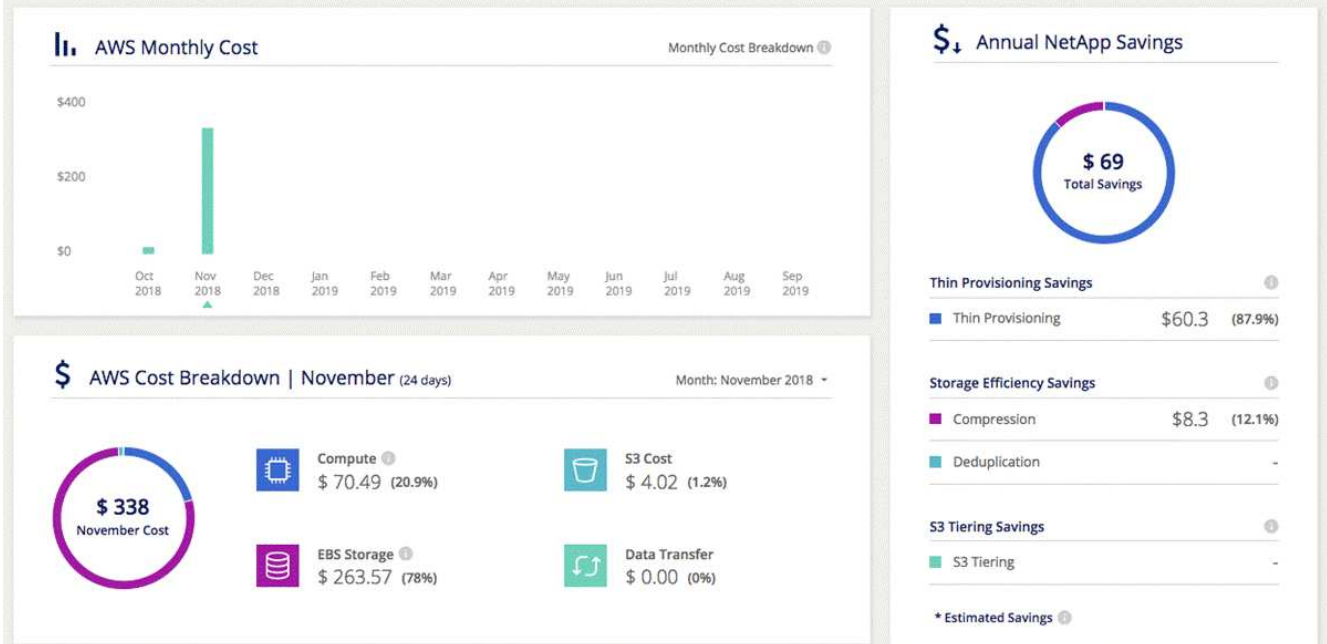
Um die AWS-Kosten zu verfolgen, weist BlueXP Cloud Volumes ONTAP-Instanzen ein Tag der Kostenzuteilung zu. Nachdem Sie Ihre erste Arbeitsumgebung erstellt haben, aktivieren Sie das Tag **WorkingEnvironment ID**. Benutzerdefinierte Tags werden erst in den AWS Abrechnungsberichten angezeigt, wenn Sie sie in der Konsole „Rechnungsstellung“ und „Kostenmanagement“ aktivieren.

2. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
3. Wählen Sie auf der Seite „Arbeitsfläche“ eine Cloud Volumes ONTAP-Arbeitsumgebung aus und klicken Sie dann auf **Kosten**.

Auf der Kostenseite werden die Kosten für die aktuelle und die vorherigen Monate angezeigt sowie Ihre jährlichen NetApp Einsparungen angezeigt, wenn Sie die kostensparenden Funktionen von NetApp auf den Volumes aktiviert haben.

Das folgende Bild zeigt eine Beispiel-Kostenseite:

Cloud Manager obtains AWS resource costs by using the AWS Cost Explorer service



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.

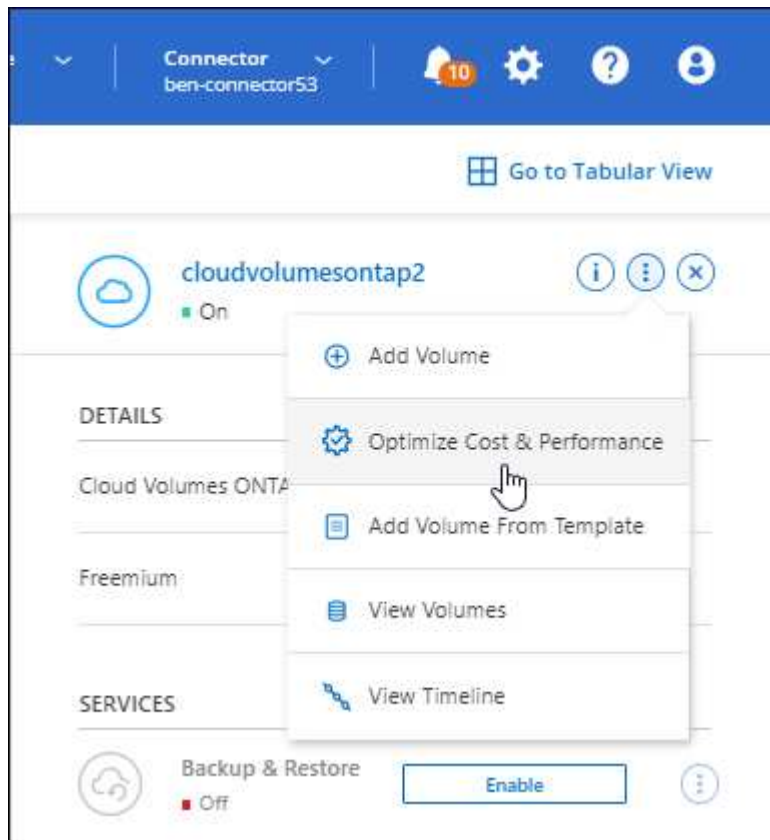


BlueXP ändert den Knoten nacheinander ordnungsgemäß, indem es Takeover und Warten auf Giveback initiiert. Das QA-Team von NetApp testete während dieses Prozesses sowohl das Schreiben als auch das Lesen der Dateien und sah keine Probleme auf Kundenseite. Wenn sich die Verbindungen änderten, wurden Wiederholungen auf I/O-Ebene gesehen, aber die Applikationsebene übergab diese kurze „Re-Wire“ der NFS/CIFS-Verbindungen.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.

2. Wählen Sie auf der Arbeitsfläche die Arbeitsumgebung aus.
3. Klicken Sie im rechten Fensterbereich auf das Menüsymbol und wählen Sie **Kosten & Leistung optimieren**.



Diese Option ist auch verfügbar, indem Sie die Arbeitsumgebung aufrufen, das Aktionsmenü öffnen und **VM ändern** wählen.

4. Wenn Sie eine knotenbasierte PAYGO-Lizenz verwenden, können Sie optional eine andere Lizenz auswählen.
5. 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 **OK**.

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 Vetoos CIFS und setzt aktive CIFS-Sitzungen zurück.

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.

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 **Verbindungseinstellungen**.



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.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Verbindungseinstellungen**.
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**.

Arbeiten Sie mit Azure Private Links

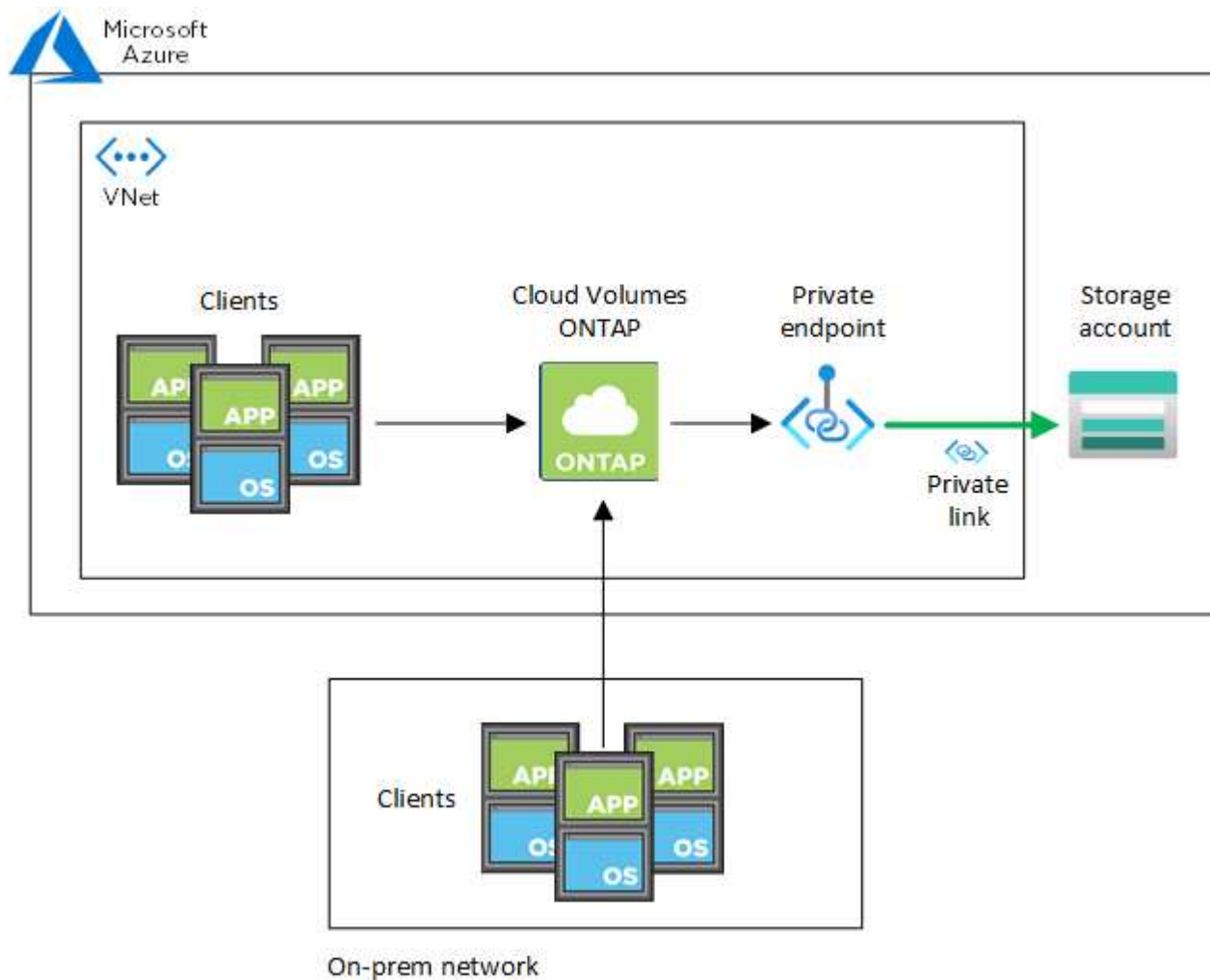
In den meisten Fällen gibt es nichts, was Sie tun müssen, um Azure private Verbindungen mit Cloud Volumes ONTAP einzurichten. BlueXP managt Azure Private Links für Sie. Aber wenn Sie Azure Private DNS verwenden, dann müssen Sie eine Konfigurationsdatei bearbeiten. Sie sollten auch eine Anforderung für den Connector-Standort in Azure kennen.

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.



Connector-Position in Azure

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. Diese Anforderung stellt sicher, dass eine Azure Private Link-Verbindung zwischen Cloud Volumes ONTAP und den zugehörigen Storage-Konten verwendet wird.

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  
}
```

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.

Das Aktivieren von Rollback wird nur über die API unterstützt.

Schritt

1. Verwenden Sie die PUT `/occm/config` API-Aufruf mit folgender Anfraentext:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

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.

Die Arbeitsumgebung und ihre Ressourcen (VMs, Festplatten, Speicherkonten, Netzwerkschnittstellen, Snapshots) befinden sich in der neuen Ressourcengruppe.

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.

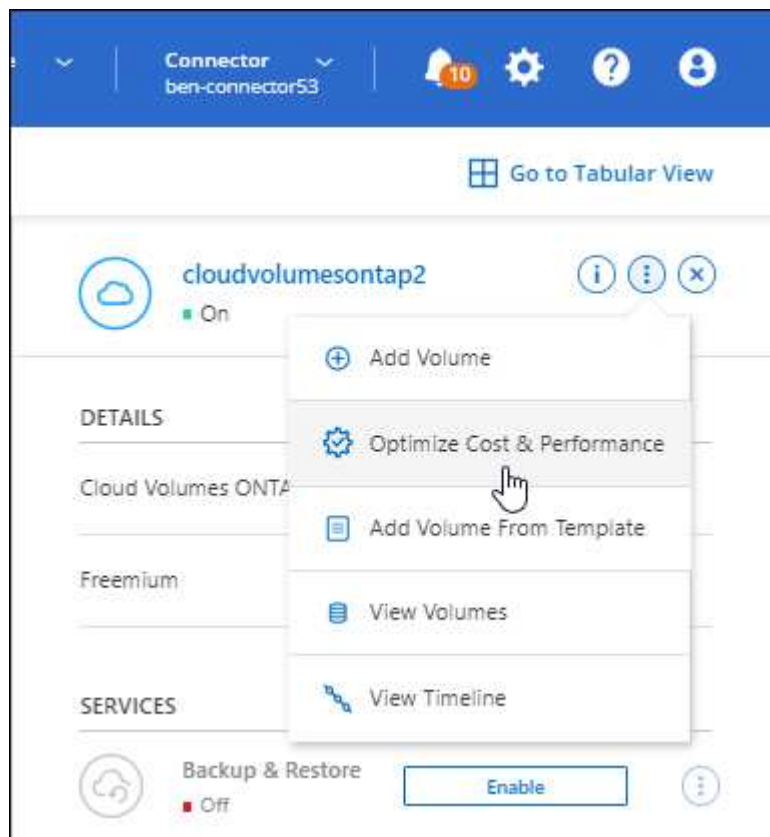
Bei HA-Paaren ist die Änderung unterbrechungsfrei. Ha-Paare stellen weiterhin Daten bereit.



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 Arbeitsfläche die Arbeitsumgebung aus.
2. Klicken Sie im rechten Fensterbereich auf das Menüsymbol und wählen Sie **Kosten & Leistung optimieren**.



Diese Option steht auch zur Verfügung, indem Sie die Arbeitsumgebung aufrufen, das Aktionsmenü öffnen und **Maschine ändern** wählen.

3. Wenn Sie eine knotenbasierte PAYGO-Lizenz verwenden, können Sie optional eine andere Lizenz auswählen.

4. Wählen Sie einen Maschinentyp aus, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Auswirkungen der Änderung verstehen, und klicken Sie dann auf **OK**.

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.

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

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:

- Cloud Tiering

Der Cloud-Tiering-Service wird mit 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.

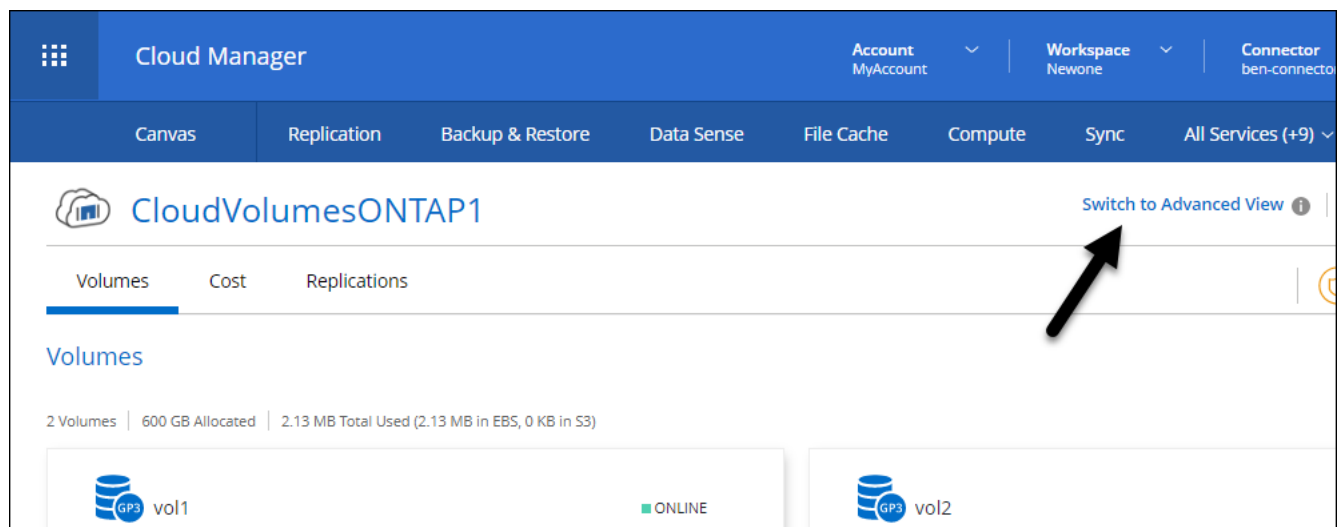
Darüber hinaus wird die rollenbasierte Zugriffssteuerung von System Manager nicht unterstützt.

Erste Schritte

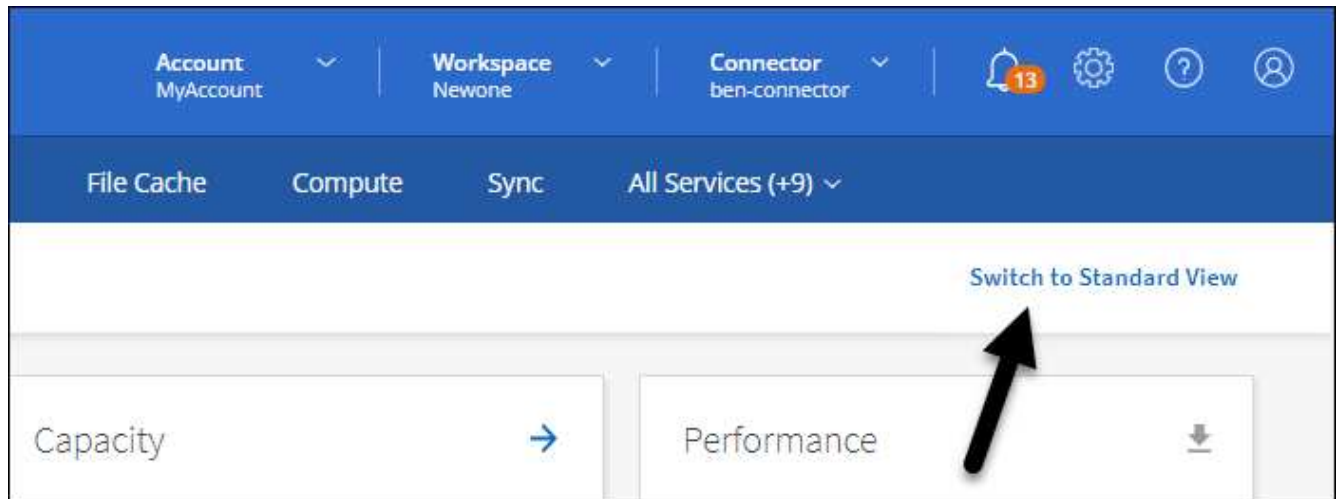
Öffnen Sie eine Cloud Volumes ONTAP Arbeitsumgebung, und klicken Sie auf die Option Erweiterte Ansicht.

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.

Der Host, von dem aus Sie SSH für die Verbindung zu Cloud Volumes ONTAP verwenden, muss über eine Netzwerkverbindung zu Cloud Volumes ONTAP verfügen. Beispielsweise müssen Sie SSH von einem Jump-Host in Ihrem Cloud-Provider-Netzwerk aus starten.



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

Schritte

1. Geben Sie in BlueXP die IP-Adresse der Cluster-Managementoberfläche an:
 - a. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
 - b. Wählen Sie auf der Seite Arbeitsfläche das Cloud Volumes ONTAP-System aus.
 - c. Kopieren Sie die IP-Adresse der Clusterverwaltung, die im rechten Fensterbereich angezeigt wird.
2. Verwenden Sie SSH, um über das Administratorkonto eine Verbindung zur IP-Adresse der Cluster-Managementschnittstelle herzustellen.

Beispiel

Das folgende Bild zeigt ein Beispiel mit PuTTY:



3. Geben Sie an der Anmeldeaufforderung das Kennwort für das Administratorkonto ein.

Beispiel

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

Systemzustand und Ereignisse

AutoSupport-Einrichtung überprüfen

AutoSupport überwacht proaktiv den Zustand Ihres Systems und sendet Meldungen an den technischen Support von NetApp. Standardmäßig ist AutoSupport auf jedem Node aktiviert, um Meldungen mithilfe des HTTPS-Transportprotokolls an den technischen Support zu senden. Überprüfen Sie am besten, ob AutoSupport diese Meldungen senden kann.

Der einzige erforderliche Konfigurationsschritt besteht darin, sicherzustellen, dass Cloud Volumes ONTAP über eine ausgehende Internetverbindung verfügt. Details finden Sie in den Netzwerkanforderungen Ihres Cloud-Providers.

AutoSupport-Anforderungen erfüllt

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

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

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

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

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

zulässt.

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

Fehler bei der AutoSupport Konfiguration beheben

Wenn keine ausgehende Verbindung verfügbar ist und BlueXP Ihr Cloud Volumes ONTAP-System nicht so konfigurieren kann, dass der Connector als Proxy-Server verwendet wird, erhalten Sie eine Benachrichtigung von BlueXP mit dem Titel „<Working Environment Name> kann keine AutoSupport-Nachrichten senden.“

Sie erhalten diese Nachricht wahrscheinlich aufgrund von Netzwerkproblemen.

Befolgen Sie diese Schritte, um dieses Problem zu lösen.

Schritte

1. SSH dem Cloud Volumes ONTAP System, sodass Sie das System von der CLI verwalten können.

["Informieren Sie sich über SSH to Cloud Volumes ONTAP"](#).

2. Anzeigen des detaillierten Status des AutoSupport-Subsystems:

```
autosupport check show-details
```

Die Antwort sollte wie folgt lauten:

```

Category: smtp
  Component: mail-server
    Status: failed
    Detail: SMTP connectivity check failed for destination:
            mailhost. Error: Could not resolve host -
'mailhost'
    Corrective Action: Check the hostname of the SMTP server

Category: http-https
  Component: http-put-destination
    Status: ok
    Detail: Successfully connected to:
            <https://support.netapp.com/put/AsupPut/>.

  Component: http-post-destination
    Status: ok
    Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

Category: on-demand
  Component: ondemand-server
    Status: ok
    Detail: Successfully connected to:
            https://support.netapp.com/aods/asupmessage.

Category: configuration
  Component: configuration
    Status: ok
    Detail: No configuration issues found.
5 entries were displayed.

```

Wenn der Status der Kategorie http-https „ok“ lautet, bedeutet dies, dass AutoSupport richtig konfiguriert ist und Meldungen gesendet werden können.

3. Wenn der Status nicht ok ist, überprüfen Sie die Proxy-URL für jeden Cloud Volumes ONTAP-Knoten:

```
autosupport show -fields proxy-url
```

4. Wenn der Proxy-URL-Parameter leer ist, konfigurieren Sie Cloud Volumes ONTAP für die Verwendung des Connectors als Proxy:

```
autosupport modify -proxy-url http://<connector private ip>:3128
```

5. Überprüfen Sie den AutoSupport-Status erneut:

```
autosupport check show-details
```

6. Wenn der Status noch nicht erfolgreich ist, überprüfen Sie, ob Verbindungen zwischen Cloud Volumes ONTAP und dem Connector über Port 3128 bestehen.
7. Wenn die Status-ID nach der Überprüfung der Verbindung weiterhin fehlgeschlagen ist, SSH zum Connector.

["Erfahren Sie mehr über die Verbindung zur Linux-VM für den Connector"](#)

8. Gehen Sie zu `/opt/application/netapp/cloudmanager/docker_occm/data/`
9. Öffnen Sie die Proxy-Konfigurationsdatei `squid.conf`

Die grundlegende Struktur der Datei ist wie folgt:

```
http_port 3128
acl localnet src 172.31.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

Der `localnet` `src`-Wert ist das CIDR des Cloud Volumes ONTAP-Systems.

10. Wenn sich der CIDR-Block des Cloud Volumes ONTAP-Systems nicht im in der Datei angegebenen Bereich befindet, aktualisieren Sie entweder den Wert oder fügen Sie einen neuen Eintrag wie folgt hinzu:

```
acl cvonet src <cidr>
```

Wenn Sie diesen neuen Eintrag hinzufügen, vergessen Sie nicht, auch einen Eintrag hinzufügen zu lassen:

```
http_access allow cvonet
```

Hier ein Beispiel:

```
http_port 3128
acl localnet src 172.31.0.0/16
acl cvonet src 172.33.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access allow cvonet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

11. Starten Sie nach dem Bearbeiten der `config`-Datei den Proxy-Container wie `sudo neu:`

```
docker restart squid
```

12. Gehen Sie zurück zur Cloud Volumes ONTAP CLI und überprüfen Sie, ob Cloud Volumes ONTAP AutoSupport Meldungen senden kann:

```
autosupport check show-details
```

EMS konfigurieren

Das Event Management System (EMS) sammelt und zeigt Informationen zu Ereignissen auf ONTAP Systemen an. Um Ereignisbenachrichtigungen zu erhalten, können Sie Ereignisziele (E-Mail-Adressen, SNMP-Trap-Hosts oder Syslog-Server) und Ereignisrouten für einen bestimmten Ereignisschweregrad festlegen.

Sie können EMS über die CLI konfigurieren. Anweisungen finden Sie unter ["ONTAP Dokumentation: EMS-Konfigurationsübersicht"](#).

Copyright-Informationen

Copyright © 2022 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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