



Azure-Administration

Cloud Volumes ONTAP

NetApp
June 11, 2024

Inhalt

- Azure-Administration 1
 - Ändern Sie den Azure VM-Typ für Cloud Volumes ONTAP 1
 - Überschreiben von CIFS-Sperren für Cloud Volumes ONTAP HA-Paare in Azure 2
 - Nutzen Sie einen Azure Private Link oder einen Service-Endpunkt 3
 - Verschieben von Ressourcengruppen 7
 - Trennen Sie SnapMirror Traffic in Azure 7

Azure-Administration

Ändern Sie den Azure VM-Typ für Cloud Volumes ONTAP

Sie können zwischen verschiedenen VM-Typen wählen, wenn Sie Cloud Volumes ONTAP in Microsoft Azure starten. Sie können den VM-Typ jederzeit ändern, wenn Sie die Größe entsprechend Ihren Anforderungen als zu groß oder zu groß definieren.

Über diese Aufgabe

- Automatisches Giveback muss auf einem Cloud Volumes ONTAP HA-Paar aktiviert sein (dies ist die Standardeinstellung). Wenn nicht, schlägt der Vorgang fehl.

["ONTAP 9 Dokumentation: Befehle zur Konfiguration von automatischem Giveback"](#)

- Eine Änderung des VM-Typs kann sich auf Microsoft Azure Servicegebühren auswirken.
- Der Vorgang startet Cloud Volumes ONTAP neu.

Bei Systemen mit einem Node wird die I/O unterbrochen.

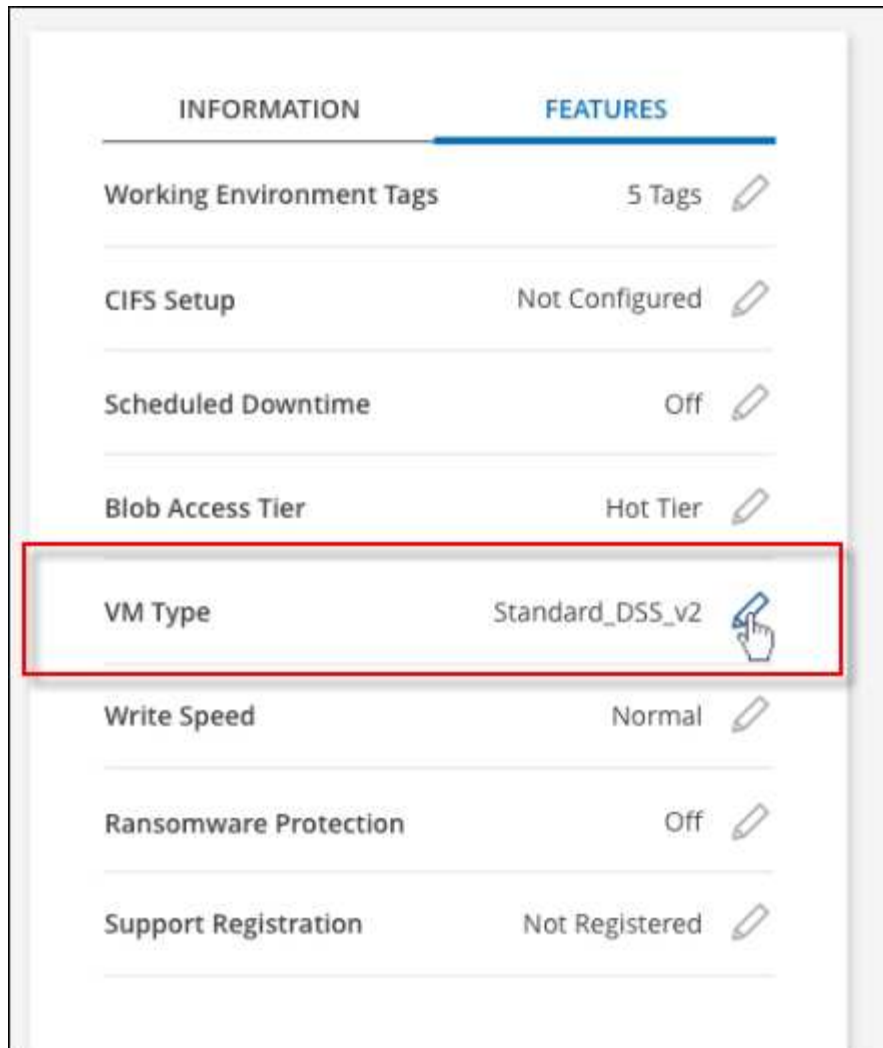
Bei HA-Paaren ist die Änderung unterbrechungsfrei. Ha-Paare stellen weiterhin Daten bereit.



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

Schritte

1. Wählen Sie auf der Seite Arbeitsfläche die Arbeitsumgebung aus.
2. Klicken Sie auf der Registerkarte Übersicht auf das Bedienfeld Funktionen und dann auf das Bleistiftsymbol neben **VM type**.



- a. Wenn Sie eine Node-basierte PAYGO-Lizenz verwenden, können Sie optional eine andere Lizenz und einen anderen VM-Typ auswählen, indem Sie auf das Bleistiftsymbol neben **Lizenztyp** klicken.
3. Wählen Sie einen VM-Typ aus, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Auswirkungen der Änderung verstehen, und klicken Sie dann auf **Ändern**.

Ergebnis

Cloud Volumes ONTAP wird mit der neuen Konfiguration neu gestartet.

Überschreiben von CIFS-Sperren für Cloud Volumes ONTAP HA-Paare in Azure

Der Account Administrator kann in BlueXP eine Einstellung aktivieren, die Probleme mit der Cloud Volumes ONTAP Storage-Rückgabe bei Azure Wartungsereignissen verhindert. Wenn Sie diese Einstellung aktivieren, sperrt Cloud Volumes ONTAP Vetoes CIFS und setzt aktive CIFS-Sitzungen zurück.

Über diese Aufgabe

Microsoft Azure plant regelmäßige Wartungsereignisse auf seinen Virtual Machines. Wenn ein Wartungsereignis auf einem Cloud Volumes ONTAP HA-Paar stattfindet, initiiert das HA-Paar die Storage-Übernahme. Wenn während dieses Wartungsereignisses aktive CIFS-Sitzungen vorhanden sind, können die

Sperren von CIFS-Dateien die Rückgabe von Storage verhindern.

Wenn Sie diese Einstellung aktivieren, setzt Cloud Volumes ONTAP die Sperren zurück und setzt die aktiven CIFS-Sitzungen zurück. So kann das HA-Paar während dieser Wartungsereignisse das Storage-Giveback durchführen.



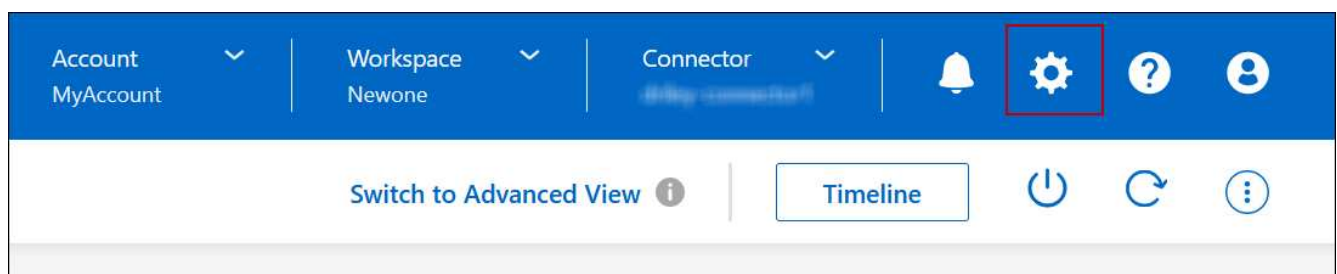
Dieser Prozess kann CIFS-Clients stören. Daten, die nicht von CIFS-Clients übertragen werden, können verloren gehen.

Was Sie benötigen

Sie müssen einen Konnektor erstellen, bevor Sie BlueXP-Einstellungen ändern können. ["Erfahren Sie, wie"](#).

Schritte

1. Klicken Sie oben rechts in der BlueXP Konsole auf das Symbol Einstellungen und wählen Sie **Cloud Volumes ONTAP-Einstellungen** aus.



2. Klicken Sie unter **Azure** auf **Azure CIFS Locks for Azure HA Working Environments**.
3. Klicken Sie auf das Kontrollkästchen, um die Funktion zu aktivieren, und klicken Sie dann auf **Speichern**.

Nutzen Sie einen Azure Private Link oder einen Service-Endpunkt

Für Verbindungen zu den zugehörigen Storage-Konten nutzt Cloud Volumes ONTAP einen Azure Private Link. Bei Bedarf können Sie Azure Private Links deaktivieren und stattdessen Service-Endpunkte verwenden.

Überblick

Standardmäßig aktiviert BlueXP einen Azure Private Link für Verbindungen zwischen Cloud Volumes ONTAP und den zugehörigen Speicherkonten. Ein Azure Private Link sichert die Verbindungen zwischen Endpunkten in Azure und bietet Performance-Vorteile.

Bei Bedarf können Sie Cloud Volumes ONTAP so konfigurieren, dass Service-Endpunkte anstelle einer Azure Private Link verwendet werden.

Bei beiden Konfigurationen schränkt BlueXP den Netzwerkzugriff für Verbindungen zwischen Cloud Volumes ONTAP- und Speicherkonten immer ein. Der Netzwerkzugriff ist auf das vnet beschränkt, in dem Cloud Volumes ONTAP bereitgestellt wird, und auf das vnet, wo der Connector bereitgestellt wird.

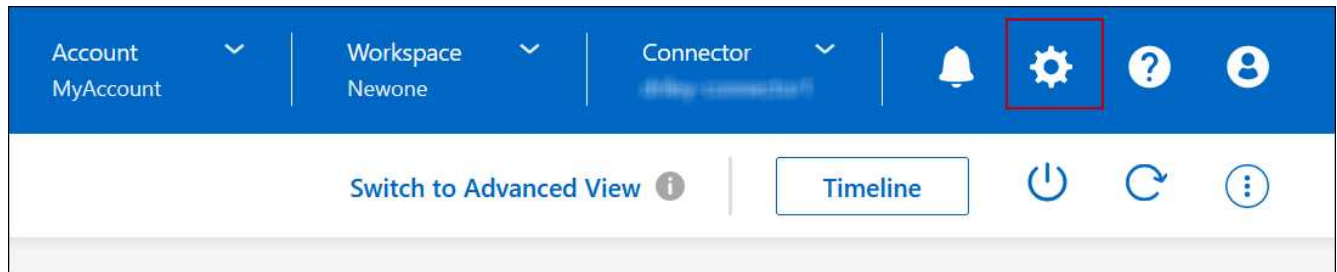
Deaktivieren Sie Azure Private Links, und verwenden Sie stattdessen Service-Endpunkte

Falls in Ihrem Unternehmen erforderlich, können Sie eine Einstellung in BlueXP ändern, sodass Cloud Volumes ONTAP für die Verwendung von Service-Endpunkten anstelle eines Azure Private Links konfiguriert wird. Das Ändern dieser Einstellung gilt für neue von Ihnen erstellte Cloud Volumes ONTAP Systeme. Service-Endpunkte werden nur in unterstütz "Azure Region-Paare" Zwischen Stecker und Cloud Volumes ONTAP VNets.

Der Connector sollte in derselben Azure-Region wie die Cloud Volumes ONTAP-Systeme, die er verwaltet, oder in der implementiert werden "Azure Region Paar" Für die Cloud Volumes ONTAP Systeme.

Schritte

1. Klicken Sie oben rechts in der BlueXP Konsole auf das Symbol Einstellungen und wählen Sie **Cloud Volumes ONTAP-Einstellungen** aus.



2. Klicken Sie unter **Azure** auf **Azure Private Link verwenden**.
3. Deaktivieren Sie **Private Link-Verbindung zwischen Cloud Volumes ONTAP und Speicherkonten**.
4. Klicken Sie Auf **Speichern**.

Nachdem Sie fertig sind

Wenn Sie Azure Private Links deaktiviert haben und der Connector einen Proxyserver verwendet, müssen Sie direkten API-Datenverkehr aktivieren.

["Erfahren Sie, wie Sie direkten API-Datenverkehr auf dem Connector aktivieren"](#)

Arbeiten Sie mit Azure Private Links

In den meisten Fällen müssen Sie nichts tun, um Azure Private Links mit Cloud Volumes ONTAP einzurichten. BlueXP managt Azure Private Links für Sie. Wenn Sie jedoch eine bestehende Azure Private DNS-Zone verwenden, müssen Sie eine Konfigurationsdatei bearbeiten.

Anforderung für benutzerdefiniertes DNS

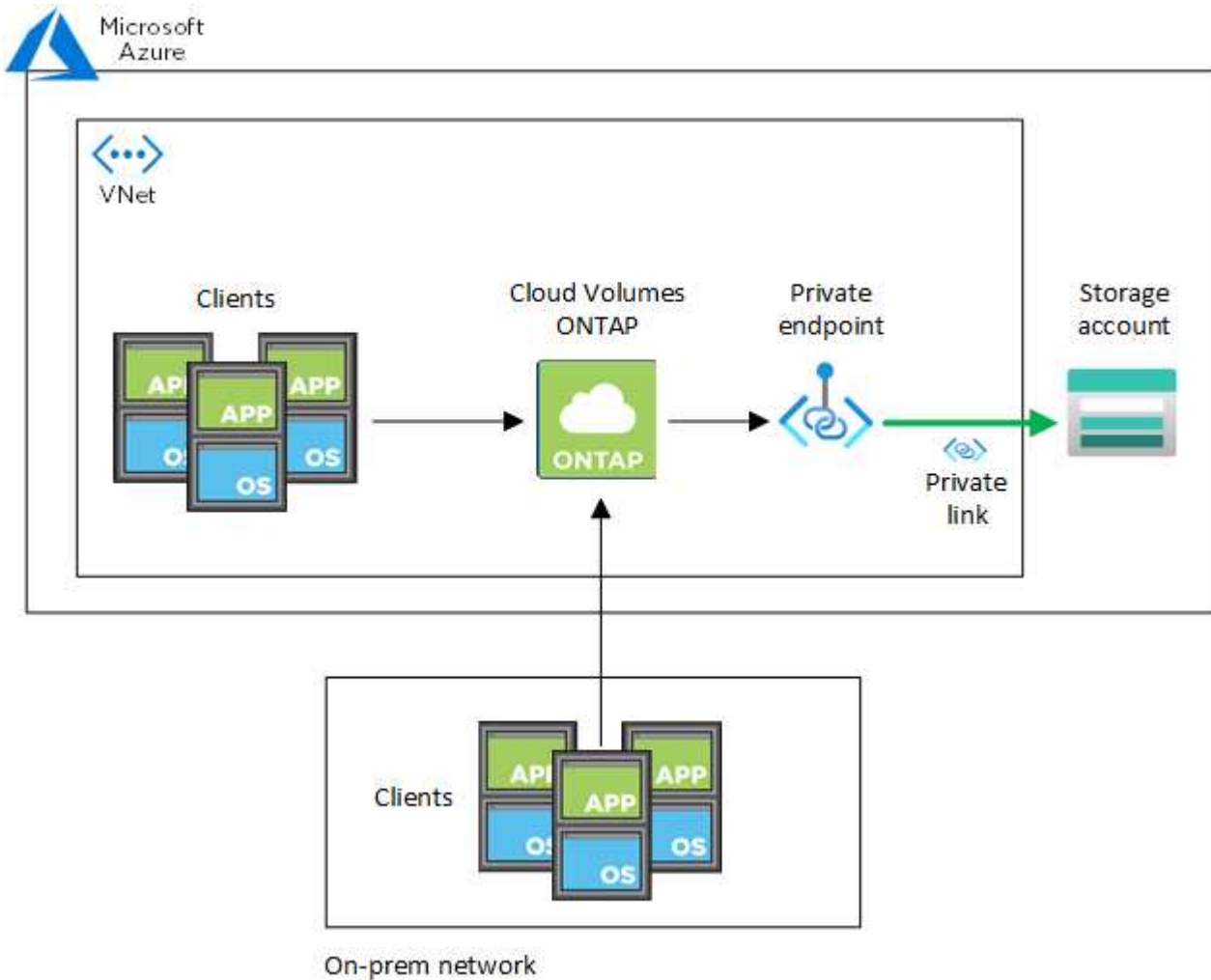
Wenn Sie optional mit benutzerdefinierten DNS arbeiten, müssen Sie von Ihren benutzerdefinierten DNS-Servern aus einen bedingten Forwarder zur Azure Private DNS Zone erstellen. Weitere Informationen finden Sie unter ["Die Dokumentation von Azure über einen DNS-Forwarder"](#).

Funktionsweise von Private Link-Verbindungen

Wenn BlueXP Cloud Volumes ONTAP in Azure implementiert, wird damit ein privater Endpunkt in der Ressourcengruppe erstellt. Der private Endpunkt ist mit Storage-Konten für Cloud Volumes ONTAP verknüpft. Dadurch wird der Zugriff auf Cloud Volumes ONTAP Storage über das Microsoft Backbone-Netzwerk übertragen.

Der Client-Zugriff erfolgt über den privaten Link, wenn sich Clients innerhalb desselben vnet wie Cloud Volumes ONTAP, innerhalb von Peered VNets oder in Ihrem lokalen Netzwerk befinden, wenn sie ein privates VPN oder eine ExpressRoute Verbindung zum vnet verwenden.

Das Beispiel zeigt den Client-Zugriff über einen privaten Link innerhalb desselben Netzwerks und von einem Netzwerk vor Ort, das entweder über ein privates VPN oder eine ExpressRoute Verbindung verfügt.



Wenn die Connector- und Cloud Volumes ONTAP-Systeme in verschiedenen VNets bereitgestellt werden, müssen Sie vnet Peering zwischen dem vnet einrichten, in dem der Connector bereitgestellt wird, und dem vnet, in dem die Cloud Volumes ONTAP-Systeme bereitgestellt werden.

Stellen Sie BlueXP Einzelheiten zu Ihrem Azure Private DNS zur Verfügung

Wenn Sie verwenden "Azure Private DNS", Dann müssen Sie eine Konfigurationsdatei auf jedem Connector ändern. Andernfalls kann BlueXP die private Link-Verbindung zu Azure zwischen Cloud Volumes ONTAP und den zugehörigen Speicherkonten nicht aktivieren.

Beachten Sie, dass der DNS-Name mit den Benennungsanforderungen für Azure DNS übereinstimmen muss "[Wie in der Azure-Dokumentation zu sehen ist](#)".

Schritte

1. SSH auf dem Connector-Host und melden Sie sich an.
2. Navigieren Sie zum folgenden Verzeichnis: /Opt/Application/netapp/cloudmanager/docker_occm/Data
3. Bearbeiten Sie App.conf, indem Sie den Parameter „user-private-dns-zone-settings“ mit den folgenden Schlüsselwort-Wert-Paaren hinzufügen:

```
"user-private-dns-zone-settings" : {  
  "resource-group" : "<resource group name of the DNS zone>",  
  "subscription" : "<subscription ID>",  
  "use-existing" : true,  
  "create-private-dns-zone-link" : true  
}
```

Der Parameter sollte auf derselben Ebene wie die „System-id“ eingegeben werden, wie unten gezeigt:

```
"system-id" : "<system ID>",  
"user-private-dns-zone-settings" : {
```

Beachten Sie, dass das Abonnement-Schlüsselwort nur erforderlich ist, wenn die private DNS-Zone in einem anderen Abonnement als der Connector vorhanden ist.

4. Speichern Sie die Datei und melden Sie sich vom Connector ab.

Ein Neustart ist nicht erforderlich.

Rollback bei Ausfällen aktivieren

Wenn BlueXP einen Azure Private Link nicht im Rahmen bestimmter Aktionen erstellt, führt er die Aktion ohne die Azure Private Link-Verbindung durch. Dies kann bei der Erstellung einer neuen Arbeitsumgebung (einzeln Node oder HA-Paar) oder bei folgenden Aktionen auf einem HA-Paar passieren: Das Erstellen eines neuen Aggregats, das Hinzufügen von Festplatten zu einem vorhandenen Aggregat oder das Erstellen eines neuen Storage-Kontos bei über 32 tib Anforderungen.

Sie können dieses Standardverhalten ändern, indem Sie Rollback aktivieren, wenn BlueXP den Azure Private Link nicht erstellt. Auf diese Weise können Sie sicherstellen, dass Sie die Sicherheitsvorschriften Ihres Unternehmens vollständig erfüllen.

Wenn Sie Rollback aktivieren, stoppt BlueXP die Aktion und führt alle Ressourcen zurück, die im Rahmen der Aktion erstellt wurden.

Sie können Rollback über die API oder durch Aktualisierung der Datei App.conf aktivieren.

Rollback über die API aktivieren

Schritt

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

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


Rollback durch Aktualisierung von App.conf aktivieren

Schritte

1. SSH auf dem Connector-Host und melden Sie sich an.
2. Navigieren Sie zum folgenden Verzeichnis: /Opt/Application/netapp/cloudmanager/docker_occm/Data
3. Bearbeiten Sie App.conf, indem Sie den folgenden Parameter und Wert hinzufügen:

```
"rollback-on-private-link-failure": true  
. Speichern Sie die Datei und melden Sie sich vom Connector ab.
```

Ein Neustart ist nicht erforderlich.

Verschieben von Ressourcengruppen

Cloud Volumes ONTAP unterstützt Azure Ressourcengruppen. Der Workflow wird jedoch nur in der Azure Konsole ausgeführt.

Sie können eine Arbeitsumgebung innerhalb eines Azure-Abonnements von einer Ressourcengruppe auf eine andere Ressourcengruppe in Azure verschieben. Das Verschieben von Ressourcengruppen zwischen verschiedenen Azure-Abonnements wird nicht unterstützt.

Schritte

1. Entfernen Sie die Arbeitsumgebung aus **Canvas**.

Informationen zum Entfernen einer Arbeitsumgebung finden Sie unter "[Entfernen von Cloud Volumes ONTAP Arbeitsumgebungen](#)".

2. Führen Sie die Verschiebung der Ressourcengruppe in der Azure-Konsole aus.

Informationen zum Abschließen des Verzuwöllig finden Sie unter "[Verschieben Sie Ressourcen in eine neue Ressourcengruppe oder ein Abonnement in der Microsoft Azure-Dokumentation](#)".

3. Entdecken Sie in **Canvas** die Arbeitsumgebung.
4. Suchen Sie in den Informationen für die Arbeitsumgebung nach der neuen Ressourcengruppe.

Ergebnis

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

Trennen Sie SnapMirror Traffic in Azure

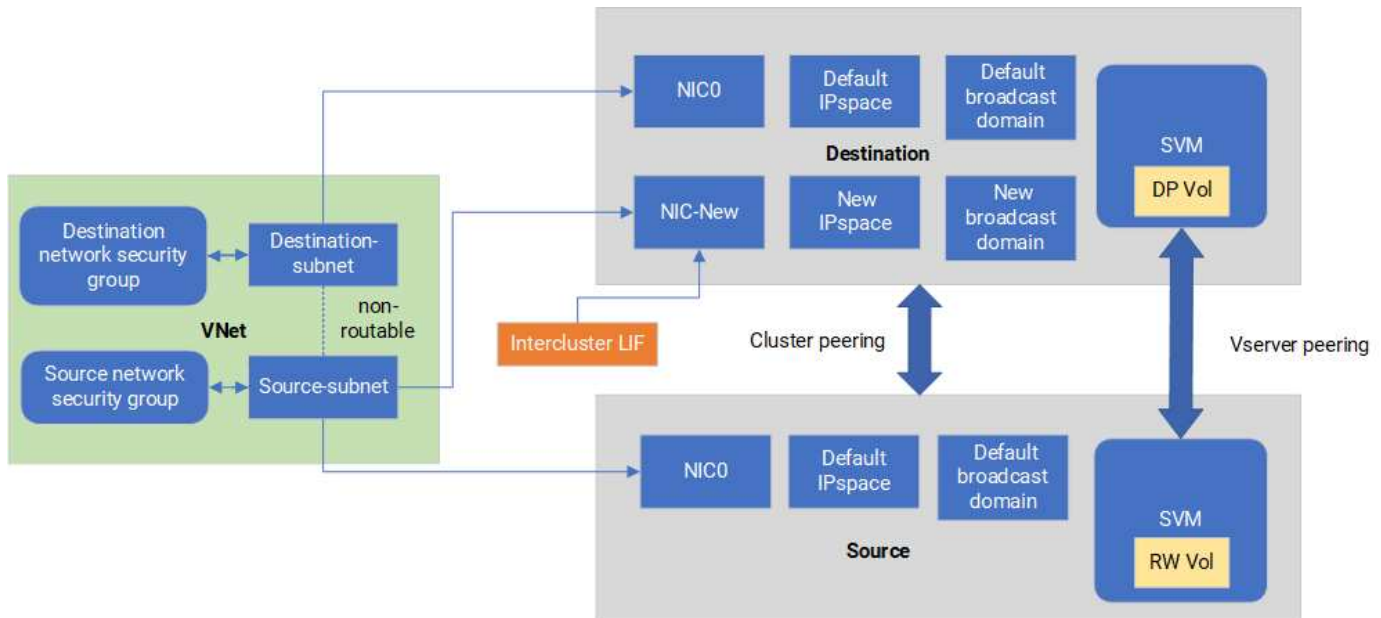
Mit Cloud Volumes ONTAP in Azure können Sie den SnapMirror Replizierungsverkehr von Daten- und Managementverkehr trennen. Um den SnapMirror Replizierungsverkehr von Ihrem Datenverkehr zu trennen, fügen Sie eine neue Netzwerkschnittstellenkarte (NIC), eine zugeordnete Intercluster LIF und ein nicht routingfähiges Subnetz hinzu.

Allgemeines zur Trennung von SnapMirror Datenverkehr in Azure

Standardmäßig konfiguriert BlueXP alle NICs und LIFs in einer Cloud Volumes ONTAP-Implementierung im selben Subnetz. In solchen Konfigurationen wird der Datenverkehr der SnapMirror Replizierung sowie der Daten- und Managementverkehr im gleichen Subnetz verarbeitet. Die Trennung von SnapMirror Traffic nutzt ein zusätzliches Subnetz, das nicht zu dem für Daten- und Managementdatenverkehr verwendeten Subnetz geleitet werden kann.

Abbildung 1

Die folgenden Diagramme zeigen die Trennung des SnapMirror Replizierungsdatenverkehrs zwischen einer zusätzlichen NIC, einer zugeordneten Intercluster LIF und einem nicht routingfähigen Subnetz in einer Implementierung mit einem einzelnen Node. Eine HA-Paar-Implementierung unterscheidet sich geringfügig.



Bevor Sie beginnen

Gehen Sie die folgenden Überlegungen durch:

- Es kann nur eine einzelne NIC zu einem einzelnen Cloud Volumes ONTAP-Knoten oder HA-Paar-Implementierung (VM-Instanz) für die SnapMirror-Traffic-Trennung hinzugefügt werden.
- Um einen neuen NIC hinzuzufügen, muss der zu implementierende VM-Instanztyp über eine nicht verwendete NIC verfügen.
- Die Quell- und Ziel-Cluster sollten Zugriff auf dasselbe virtuelle Netzwerk (vnet) haben. Ziel-Cluster ist ein Cloud Volumes ONTAP System in Azure. Beim Quell-Cluster kann es sich um ein Cloud Volumes ONTAP System in Azure oder um ein ONTAP System handeln.

Schritt: Erstellen Sie eine zusätzliche NIC und verbinden Sie sie mit der Ziel-VM

Dieser Abschnitt enthält Anweisungen zum Erstellen einer zusätzlichen NIC und zum Anhängen an die Ziel-VM. Die Ziel-VM ist das Single Node- oder HA-Paar-System in Cloud Volumes ONTAP in Azure, wo Sie Ihre zusätzliche NIC einrichten möchten.

Schritte

1. Beenden Sie den Node in der ONTAP CLI.

```
dest::> halt -node <dest_node-vm>
```

- Überprüfen Sie im Azure-Portal, ob der Status der VM (Node) angehalten lautet.

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>  
--query instanceView.statuses[1].displayStatus
```

- Beenden Sie den Node mithilfe der Bash-Umgebung in Azure Cloud Shell.

- Stoppen Sie den Node.

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

- Zuordnung des Knotens aufheben.

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-  
vm>
```

- Konfigurieren Sie Regeln für Netzwerksicherheitsgruppen, damit die beiden Subnetze (Subnetz des Quell-Clusters und Subnetz des Zielclusteres) nicht routungsfähig sind.

- Erstellen Sie die neue NIC auf der Ziel-VM.
- Suchen Sie nach der Subnetz-ID für das Subnetz des Quell-Clusters.

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet  
-name <vnet> --query id
```

- Erstellen Sie die neue NIC auf der Ziel-VM mit der Subnetz-ID für das Quell-Cluster-Subnetz. Hier geben Sie den Namen für die neue NIC ein.

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new>  
--subnet <id_from_prev_command> --accelerated-networking true
```

- Speichern Sie die private IP-Adresse. Diese IP-Adresse, <new_added_nic_primary_addr>, wird verwendet, um eine Intercluster LIF in zu erstellen [Broadcast-Domäne, Intercluster LIF für die neue NIC](#).

- Verbinden Sie die neue NIC mit der VM.

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics  
<dest_node-vm-nic-new>
```

6. Starten Sie die VM (Knoten).

```
az vm start --resource-group <dest_node-rg> --name <dest_node-vm>
```

7. Gehen Sie im Azure-Portal zu **Networking** und bestätigen Sie, dass die neue NIC, z.B. nic-New, existiert und beschleunigte Vernetzung aktiviert ist.

```
az network nic list --resource-group azure-59806175-60147103-azure-rg  
--query "[].{NIC: name, VM: virtualMachine.id}"
```

Wiederholen Sie bei HA-Paar-Implementierungen die Schritte für den Partner-Node.

Schritt 2: Erstellen Sie einen neuen IPspace, Broadcast-Domain und Intercluster LIF für die neue NIC

Durch einen separaten IPspace für Intercluster-LIFs wird die logische Trennung zwischen den Netzwerkfunktionen für die Replizierung zwischen Clustern ermöglicht.

Verwenden Sie die ONTAP-CLI für die folgenden Schritte.

Schritte

1. Erstellen Sie den neuen IPspace (New_ipspace).

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. Erstellen Sie eine Broadcast-Domain auf dem neuen IPspace (New_ipspace) und fügen Sie den nic-New-Port hinzu.

```
dest::> network port show
```

3. Für Systeme mit einem einzigen Node lautet der neu hinzugefügte Port *e0b*. Für HA-Paar-Implementierungen mit verwalteten Datenträgern lautet der neu hinzugefügte Port *e0d*. Für HA-Paar-Implementierungen mit Page Blobs ist der neu hinzugefügte Port *e0e*. Verwenden Sie den Node-Namen und nicht den VM-Namen. Suchen Sie den Node-Namen, indem Sie ausführen `node show`.

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500  
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. Erstellen Sie eine Intercluster LIF auf der neuen Broadcast-Domain (New_bd) und auf der neuen NIC (nic-New).

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. Überprüfung der Erstellung der neuen Intercluster LIF

```
dest::> net int show
```

Wiederholen Sie bei HA-Paar-Implementierungen die Schritte für den Partner-Node.

Schritt 3: Überprüfen Sie Cluster-Peering zwischen den Quell- und Zielsystemen

Dieser Abschnitt enthält Anweisungen zur Überprüfung von Peering zwischen Quell- und Zielsystemen.

Verwenden Sie die ONTAP-CLI für die folgenden Schritte.

Schritte

1. Vergewissern Sie sich, dass die Intercluster LIF des Ziel-Clusters die Intercluster LIF des Quell-Clusters anpingen kann. Da der Ziel-Cluster diesen Befehl ausführt, ist die Ziel-IP-Adresse die Intercluster LIF IP-Adresse auf der Quelle.

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. Vergewissern Sie sich, dass die Intercluster LIF des Quell-Clusters die Intercluster LIF des Ziel-Clusters anpingen kann. Das Ziel ist die IP-Adresse der neuen NIC, die auf dem Ziel erstellt wurde.

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

Wiederholen Sie bei HA-Paar-Implementierungen die Schritte für den Partner-Node.

Schritt 4: SVM-Peering zwischen Quell- und Zielsystem erstellen

Dieser Abschnitt enthält Anweisungen zum Erstellen von SVM-Peering zwischen dem Quell- und Zielsystem.

Verwenden Sie die ONTAP-CLI für die folgenden Schritte.

Schritte

1. Erstellen Sie Cluster-Peering auf dem Ziel mithilfe der Intercluster-Quell-IP-Adresse des `-peer-addr`. Bei HA-Paaren sollten Sie die LIF-IP-Quelladresse für beide Nodes als auflisten `-peer-addr`.

```
dest::> cluster peer create -peer-addr <10.161.189.6> -ip-space <new_ipspace>
```

2. Geben Sie die Passphrase ein und bestätigen Sie sie.
3. Erstellen Sie Cluster-Peering auf der Quelle mithilfe der LIF-IP-Adresse des Ziel-Clusters als `peer-addr`. Bei HA-Paaren müssen die Ziel-Intercluster-LIF-IP-Adresse für beide Nodes als auflisten `-peer-addr`.

```
src::> cluster peer create -peer-addr <10.161.189.18>
```

4. Geben Sie die Passphrase ein und bestätigen Sie sie.
5. Prüfen Sie, ob das Cluster Peering ist.

```
src::> cluster peer show
```

Erfolgreiches Peering zeigt **verfügbar** im Verfügbarkeitsfeld an.

6. SVM-Peering auf dem Ziel erstellen. Quell- und Ziel-SVMs sollten Daten-SVMs sein.

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm> -peer-cluster <src_cluster> -applications snapmirror``
```

7. SVM-Peering akzeptieren.

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. Prüfen Sie, ob die SVM einen Spitzeneinschlag hat.

```
dest::> vserver peer show
```

Peer-Status wird angezeigt **peered** Und Peering Anwendungen zeigt **snapmirror**.

Schritt 5: Erstellen einer SnapMirror Replizierungsbeziehung zwischen dem Quell- und Zielsystem

Dieser Abschnitt enthält Anweisungen zum Erstellen einer SnapMirror Replizierungsbeziehung zwischen dem Quell- und Zielsystem.

Um eine vorhandene SnapMirror Replizierungsbeziehung zu verschieben, müssen Sie zuerst die bestehende SnapMirror Replizierungsbeziehung trennen, bevor Sie eine neue SnapMirror Replizierungsbeziehung erstellen.

Verwenden Sie die ONTAP-CLI für die folgenden Schritte.

Schritte

1. Erstellung eines geschützten Volumes auf der Ziel-SVM

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP  
-size <10GB> -aggregate <aggr1>
```

2. Erstellen Sie die SnapMirror Replizierungsbeziehung auf dem Ziel, das die SnapMirror Richtlinie und einen Zeitplan für die Replizierung umfasst.

```
dest::> snapmirror create -source-path src_svm:src_vol -destination  
-path dest_svm:new_dest_vol -vserver dest_svm -policy  
MirrorAllSnapshots -schedule 5min
```

3. Initialisieren Sie die SnapMirror Replizierungsbeziehung auf dem Ziel.

```
dest::> snapmirror initialize -destination-path <dest_svm:new_dest_vol>
```

4. Überprüfen Sie in der ONTAP CLI den SnapMirror Beziehungsstatus, indem Sie den folgenden Befehl ausführen:

```
dest::> snapmirror show
```

Der Beziehungsstatus lautet `Snapmirrored` Und die Gesundheit der Beziehung ist `true`.

5. Optional: Führen Sie in der ONTAP-CLI den folgenden Befehl aus, um den Aktionsverlauf für die SnapMirror Beziehung anzuzeigen.

```
dest::> snapmirror show-history
```

Optional können Sie die Quell- und Ziel-Volumes mounten, eine Datei auf die Quelle schreiben und überprüfen, ob das Volume auf das Ziel repliziert wird.

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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