Azure-Verwaltung

Cloud Volumes ONTAP

NetApp
February 13, 2026

Inhalt

Azure-Verwaltung

Ändern des Azure-VM-Typs für Cloud Volumes ONTAP

Sie können aus mehreren VM-Typen wählen, wenn Sie Cloud Volumes ONTAP in Microsoft Azure starten. Sie können den VM-Typ jederzeit ändern, wenn Sie feststellen, dass er für Ihre Anforderungen zu klein oder zu groß ist.

Informationen zu diesem Vorgang

- Die automatische Rückgabe muss für ein Cloud Volumes ONTAP HA-Paar aktiviert sein (dies ist die Standardeinstellung). Wenn dies nicht der Fall ist, schlägt der Vorgang fehl.

  "ONTAP 9-Dokumentation: Befehle zum Konfigurieren der automatischen Rückgabe"

- Das Ändern des VM-Typs kann sich auf die Servicegebühren von Microsoft Azure auswirken.
- Der Vorgang startet Cloud Volumes ONTAP.

  Bei Single-Node-Systemen wird die I/O unterbrochen.

  Bei HA-Paaren erfolgt die Änderung ohne Unterbrechung. HA-Paare stellen weiterhin Daten bereit.

Die NetApp Console ändert jeweils einen Knoten, indem sie die Übernahme einleitet und auf die Rückgabe wartet. Das Qualitätssicherungsteam von NetApp hat während dieses Vorgangs sowohl das Schreiben als auch das Lesen von Dateien getestet und konnte auf der Clientseite keine Probleme feststellen. Beim Ändern der Verbindungen wurden auf der E/A-Ebene einige Wiederholungsversuche beobachtet, die Anwendungsschicht konnte die Neuverdrahtung der NFS/CIFS-Verbindungen jedoch bewältigen.

Schritte

1. Wählen Sie auf der Seite **Systeme** das System aus.
2. Klicken Sie auf der Registerkarte „Übersicht“ auf den Bereich „Funktionen“ und dann auf das Stiftsymbol neben „VM-Typ“.

   Wenn Sie eine knotenbasierte Pay-as-you-go-Lizenz (PAYGO) verwenden, können Sie optional eine andere Lizenz und einen anderen VM-Typ auswählen, indem Sie auf das Stiftsymbol 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.

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

Der Organisations- oder Kontoadministrator kann in der NetApp Console eine Einstellung aktivieren, die Probleme mit der Rückgabe von Cloud Volumes ONTAP -Speicher

während Azure-Wartungsereignissen verhindert. Wenn Sie diese Einstellung aktivieren, blockiert Cloud Volumes ONTAP CIFS-Sperren und setzt aktive CIFS-Sitzungen zurück.

Informationen zu diesem Vorgang

Microsoft Azure plant regelmäßige Wartungsereignisse auf seinen virtuellen Maschinen. Wenn bei einem Cloud Volumes ONTAP HA-Paar ein Wartungsereignis auftritt, leitet das HA-Paar die Speicherübernahme ein. Wenn während dieses Wartungsereignisses aktive CIFS-Sitzungen vorhanden sind, können die Sperren der CIFS-Dateien die Speicherrückgabe verhindern.

Wenn Sie diese Einstellung aktivieren, wird Cloud Volumes ONTAP die Sperren blockieren und die aktiven CIFS-Sitzungen zurücksetzen. Dadurch kann das HA-Paar während dieser Wartungsereignisse die Speicherrückgabe abschließen.

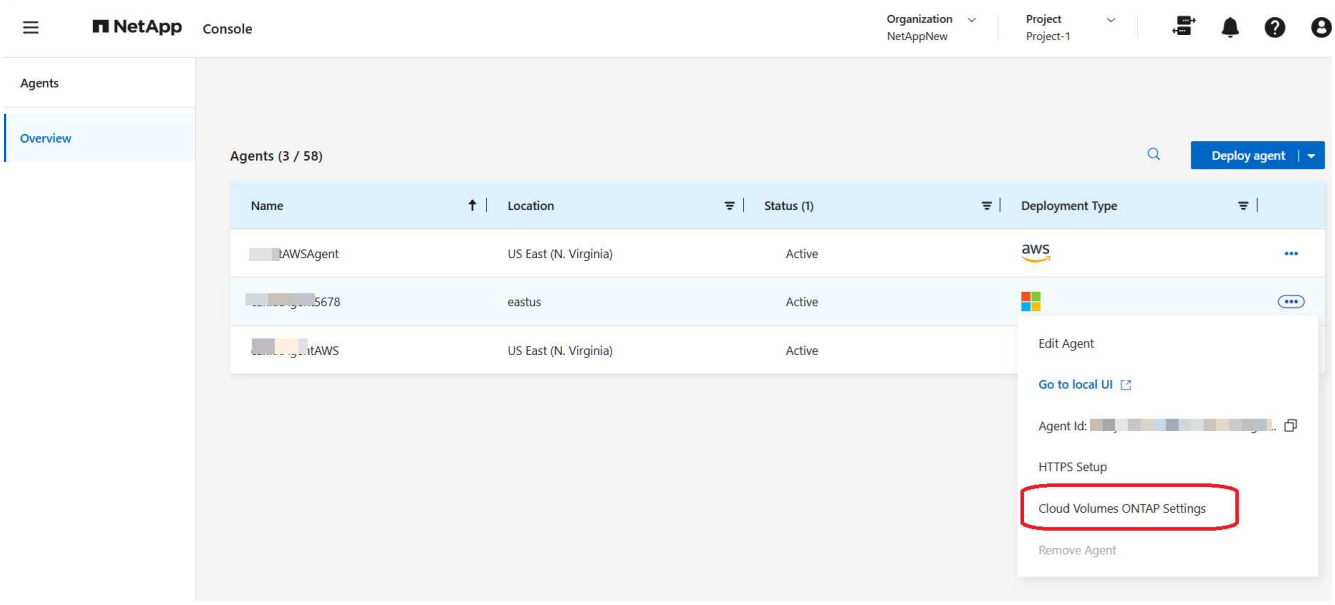
> Dieser Vorgang kann für CIFS-Clients störend sein. Daten, die nicht von CIFS-Clients festgeschrieben werden, können verloren gehen.

Bevor Sie beginnen

Sie müssen einen Konsolenagenten erstellen, bevor Sie die Konsoleneinstellungen ändern können. "Erfahren Sie mehr" .

Schritte

1. Gehen Sie im linken Navigationsbereich zu **Administration > Agenten**.
2. Klicken Sie auf das ••• Symbol für den Konsolenagenten, der Ihr Cloud Volumes ONTAP -System verwaltet.
3. Wählen Sie * Cloud Volumes ONTAP -Einstellungen*.



4. Klicken Sie unter **Azure** auf **Azure CIFS-Sperren für Azure HA-Systeme**.
5. Klicken Sie auf das Kontrollkästchen, um die Funktion zu aktivieren, und klicken Sie dann auf **Speichern**.

Verwenden Sie einen Azure Private Link oder Service-Endpunkte für Cloud Volumes ONTAP Systeme

Cloud Volumes ONTAP verwendet einen Azure Private Link für Verbindungen zu den zugehörigen Speicherkonten. Bei Bedarf können Sie Azure Private Links deaktivieren und stattdessen Dienstendpunkte verwenden.

Überblick

Standardmäßig aktiviert die NetApp Console einen Azure Private Link für Verbindungen zwischen Cloud Volumes ONTAP und den zugehörigen Speicherkonten. Ein Azure Private Link sichert Verbindungen zwischen Endpunkten in Azure und bietet Leistungsvorteile.

Bei Bedarf können Sie Cloud Volumes ONTAP so konfigurieren, dass anstelle eines Azure Private Link Dienstendpunkte verwendet werden.

Bei beiden Konfigurationen beschränkt die Konsole immer den Netzwerkzugriff für Verbindungen zwischen Cloud Volumes ONTAP und Speicherkonten. Der Netzwerkzugriff ist auf das VNet beschränkt, in dem Cloud Volumes ONTAP bereitgestellt wird, und das VNet, in dem der Konsolenagent bereitgestellt wird.

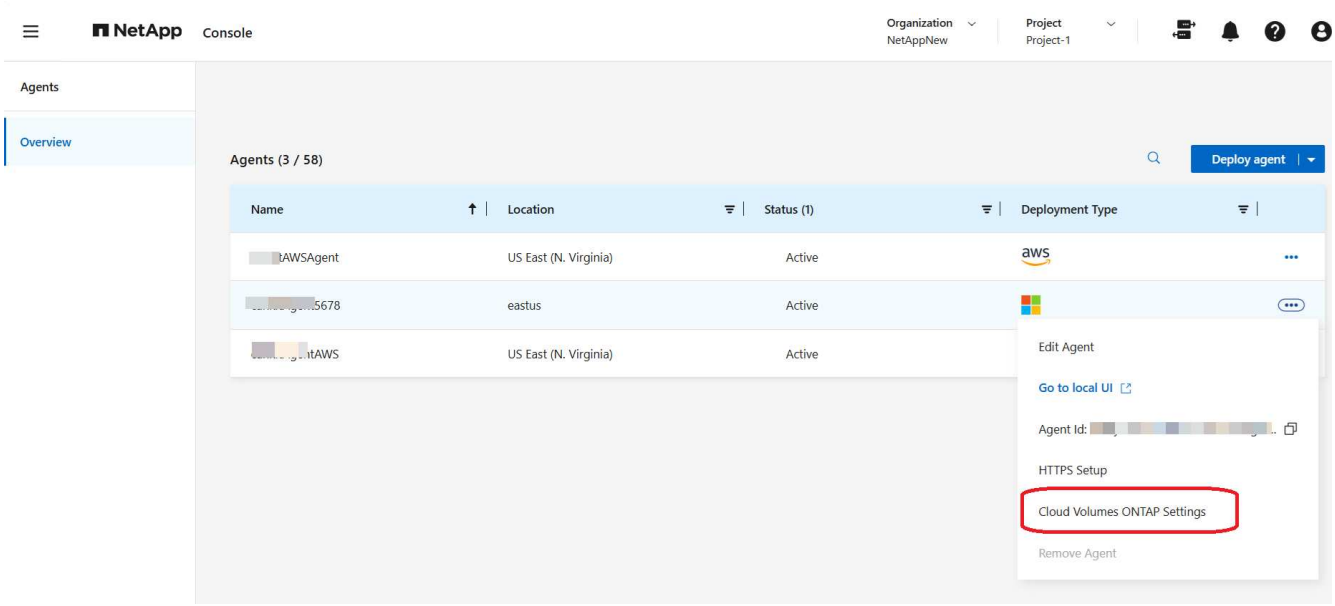
Deaktivieren Sie Azure Private Links und verwenden Sie stattdessen Dienstendpunkte

Falls Ihr Unternehmen dies erfordert, können Sie eine Einstellung in der Konsole ändern, sodass Cloud Volumes ONTAP so konfiguriert wird, dass Service-Endpunkte anstelle eines Azure Private Link verwendet werden. Das Ändern dieser Einstellung gilt für neue Cloud Volumes ONTAP -Systeme, die Sie erstellen. Service-Endpunkte werden nur unterstützt in"Azure-Regionspaare" zwischen dem Konsolenagenten und Cloud Volumes ONTAP VNets.

Der Konsolenagent sollte in derselben Azure-Region wie die von ihm verwalteten Cloud Volumes ONTAP -Systeme oder in der "Azure-Regionenpaar" für die Cloud Volumes ONTAP -Systeme.

Schritte

1. Gehen Sie im linken Navigationsbereich zu **Administration > Agenten**.
2. Klicken Sie auf das ••• Symbol für den Konsolenagenten, der Ihr Cloud Volumes ONTAP -System verwaltet.
3. Wählen Sie * Cloud Volumes ONTAP -Einstellungen*.



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

Nach Abschluss

Wenn Sie Azure Private Links deaktiviert haben und der Konsolen-Agent einen Proxyserver verwendet, müssen Sie den direkten API-Verkehr aktivieren.

"Erfahren Sie, wie Sie den direkten API-Verkehr auf dem Konsolenagenten aktivieren"

Arbeiten mit Azure Private Links

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

Voraussetzung für benutzerdefiniertes DNS

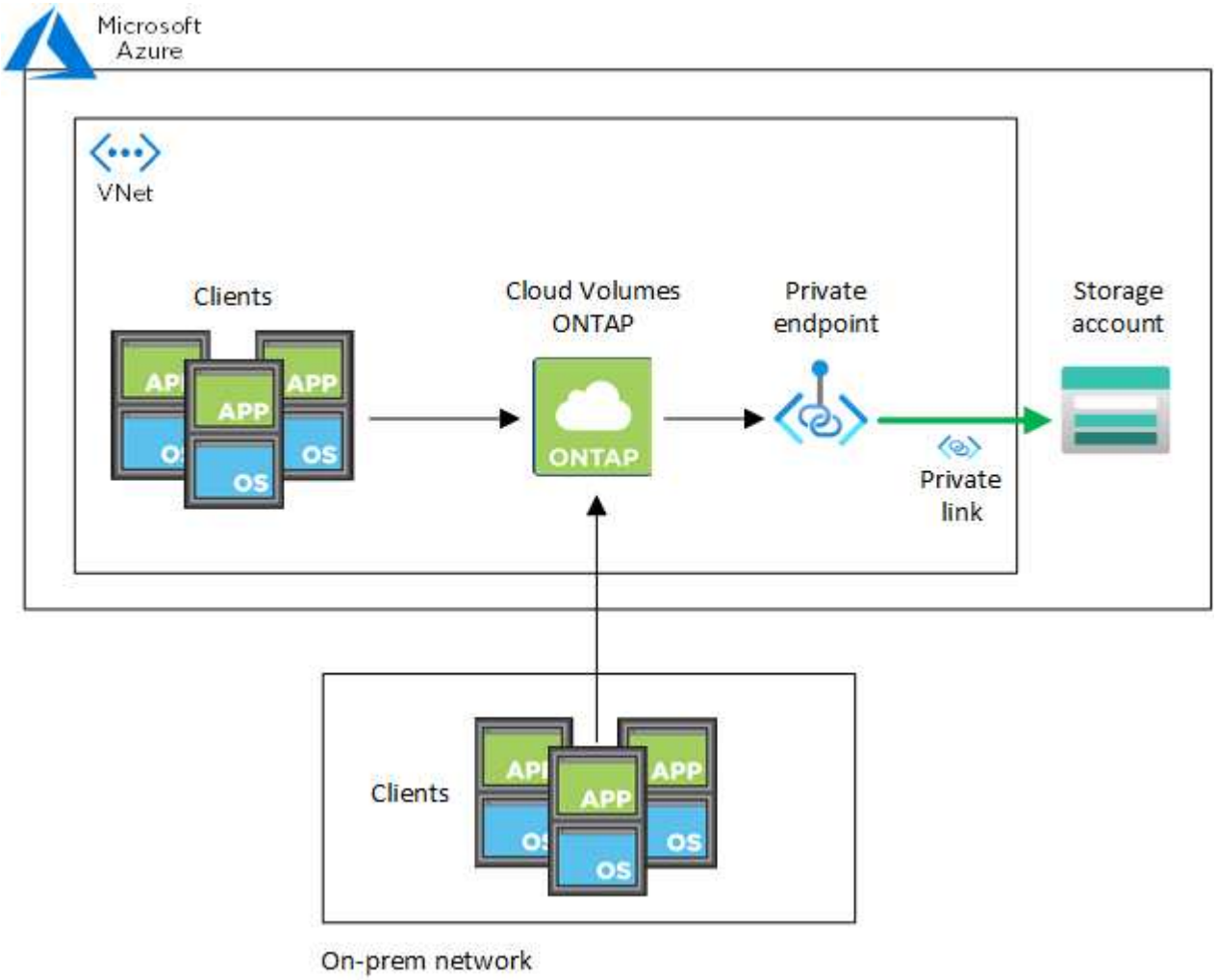
Wenn Sie mit benutzerdefiniertem DNS arbeiten, müssen Sie optional von Ihren benutzerdefinierten DNS-Servern eine bedingte Weiterleitung zur privaten Azure-DNS-Zone erstellen. Weitere Informationen finden Sie unter"Azure-Dokumentation zur Verwendung einer DNS-Weiterleitung" .

Funktionsweise von Private Link-Verbindungen

Wenn die Konsole Cloud Volumes ONTAP in Azure bereitstellt, erstellt sie einen privaten Endpunkt in der Ressourcengruppe. Der private Endpunkt ist mit Speicherkonten für Cloud Volumes ONTAP verknüpft. Daher erfolgt der Zugriff auf den Cloud Volumes ONTAP -Speicher über das Microsoft-Backbone-Netzwerk.

Der Clientzugriff erfolgt über die private Verbindung, wenn sich Clients im selben VNet wie Cloud Volumes ONTAP, in Peering-VNets oder in Ihrem lokalen Netzwerk befinden, wenn eine private VPN- oder ExpressRoute-Verbindung zum VNet verwendet wird.

Hier ist ein Beispiel, das den Clientzugriff über eine private Verbindung innerhalb desselben VNet und von einem lokalen Netzwerk aus zeigt, das entweder über eine private VPN- oder ExpressRoute-Verbindung verfügt.



Wenn der Konsolenagent und die Cloud Volumes ONTAP -Systeme in unterschiedlichen VNets bereitgestellt werden, müssen Sie VNet-Peering zwischen dem VNet einrichten, in dem der Konsolenagent bereitgestellt wird, und dem VNet, in dem die Cloud Volumes ONTAP -Systeme bereitgestellt werden.

Geben Sie Details zu Ihrem Azure Private DNS an

Wenn Sie "Privates Azure-DNS" , dann müssen Sie auf jedem Konsolenagenten eine Konfigurationsdatei ändern. Andernfalls kann die Konsole die Azure Private Link-Verbindung zwischen Cloud Volumes ONTAP und den zugehörigen Speicherkonten nicht herstellen.

Beachten Sie, dass der DNS-Name den Azure DNS-Benennungsanforderungen entsprechen muss. "wie in der Azure-Dokumentation gezeigt" .

Schritte

1. Stellen Sie per SSH eine Verbindung zum Konsolenagent-Host her und melden Sie sich an.
2. Navigieren Sie zum `/opt/application/netapp/cloudmanager/docker_occm/data` Verzeichnis.
3. Bearbeiten `app.conf` durch Hinzufügen der `user-private-dns-zone-settings` Parameter mit den folgenden Schlüsselwort-Wert-Paaren:

```
"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 `subscription` Das Schlüsselwort ist nur erforderlich, wenn sich die private DNS-Zone in einem anderen Abonnement befindet als das des Konsolenagenten.

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

   Ein Neustart ist nicht erforderlich.

Rollback bei Fehlern aktivieren

Wenn die Konsole im Rahmen bestimmter Aktionen keinen Azure Private Link erstellen kann, führt sie die Aktion ohne die Azure Private Link-Verbindung aus. Dies kann beim Erstellen eines neuen Systems (einzelner Knoten oder HA-Paar) passieren oder wenn die folgenden Aktionen auf einem HA-Paar stattfinden: Erstellen eines neuen Aggregats, Hinzufügen von Datenträgern zu einem vorhandenen Aggregat oder Erstellen eines neuen Speicherkontos beim Überschreiten von 32 TiB.

Sie können dieses Standardverhalten ändern, indem Sie das Rollback aktivieren, wenn die Konsole den Azure Private Link nicht erstellen kann. Auf diese Weise können Sie sicherstellen, dass Sie die Sicherheitsvorschriften Ihres Unternehmens vollständig einhalten.

Wenn Sie das Rollback aktivieren, stoppt die Konsole die Aktion und führt ein Rollback aller Ressourcen durch, die im Rahmen der Aktion erstellt wurden.

Sie können das Rollback über die API oder durch Aktualisieren der Datei app.conf aktivieren.

Rollback über die API aktivieren

Schritt

1. Verwenden Sie die `PUT /occm/config` API-Aufruf mit folgendem Anforderungstext:

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

Rollback durch Aktualisieren von app.conf aktivieren

Schritte

1. Stellen Sie per SSH eine Verbindung zum Host des Konsolenagenten her 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 Konsolenagenten ab.
```

Ein Neustart ist nicht erforderlich.

Verschieben einer Azure-Ressourcengruppe für Cloud Volumes ONTAP in der Azure-Konsole

Cloud Volumes ONTAP unterstützt das Verschieben von Azure-Ressourcengruppen, der Workflow erfolgt jedoch nur in der Azure-Konsole.

Sie können ein Cloud Volumes ONTAP -System innerhalb desselben Azure-Abonnements von einer Ressourcengruppe in eine andere Ressourcengruppe in Azure verschieben. Das Verschieben von Ressourcengruppen zwischen verschiedenen Azure-Abonnements wird nicht unterstützt.

Schritte

1. Entfernen Sie das Cloud Volumes ONTAP -System. Weitere Informationen finden Sie unter "Entfernen von Cloud Volumes ONTAP -Systemen" .
2. Führen Sie die Ressourcengruppenverschiebung in der Azure-Konsole aus.

   Um den Umzug abzuschließen, lesen Sie"Verschieben von Ressourcen in eine neue Ressourcengruppe oder ein neues Abonnement in der Dokumentation von Microsoft Azure" .
3. Suchen Sie auf der Seite **Systeme** nach dem System.
4. Suchen Sie in den Informationen zum System nach der neuen Ressourcengruppe.

Ergebnis

Das System und seine Ressourcen (VMs, Datenträger, Speicherkonten, Netzwerkschnittstellen, Snapshots) befinden sich in der neuen Ressourcengruppe.

Trennen Sie den SnapMirror -Datenverkehr in Azure

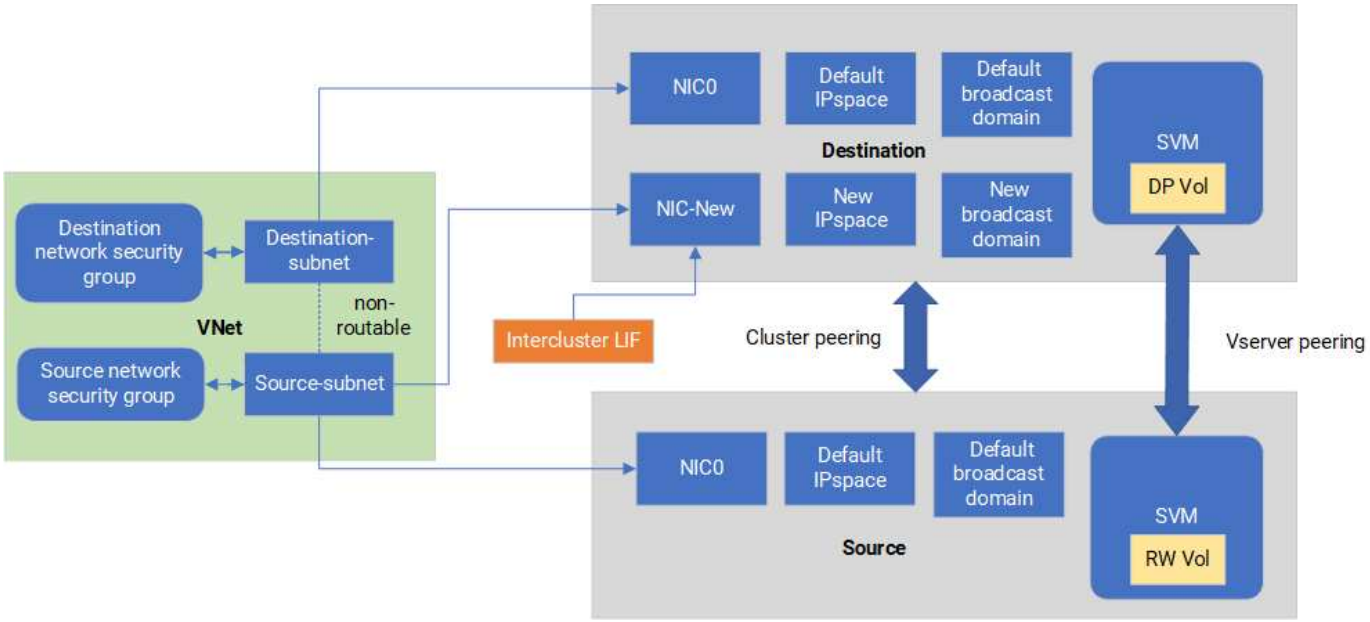
Mit Cloud Volumes ONTAP in Azure können Sie den SnapMirror Replikationsdatenverkehr vom Daten- und Verwaltungsdatenverkehr trennen. Um den SnapMirror -Replikationsverkehr von Ihrem Datenverkehr zu trennen, fügen Sie eine neue Netzwerkschnittstellenkarte (NIC), ein zugehöriges Intercluster-LIF und ein nicht routbares Subnetz hinzu.

Informationen zur SnapMirror -Verkehrstrennung in Azure

Standardmäßig konfiguriert die NetApp Console alle NICs und LIFs in einer Cloud Volumes ONTAP Bereitstellung im selben Subnetz. In solchen Konfigurationen verwenden der SnapMirror Replikationsverkehr sowie der Daten- und Verwaltungsverkehr dasselbe Subnetz. Durch die Trennung des SnapMirror -Verkehrs wird ein zusätzliches Subnetz genutzt, das nicht an das vorhandene Subnetz weitergeleitet werden kann, das für den Daten- und Verwaltungsverkehr verwendet wird.

Abbildung 1

Die folgenden Diagramme zeigen die Trennung des SnapMirror -Replikationsdatenverkehrs mit einer zusätzlichen Netzwerkkarte, einem zugehörigen Intercluster-LIF und einem nicht routingfähigen Subnetz in einer Einzelknotenbereitstellung. Eine HA-Paarbereitstellung unterscheidet sich geringfügig.



Bevor Sie beginnen

Beachten Sie die folgenden Überlegungen:

- Sie können einem Cloud Volumes ONTAP Einzelknoten oder einer HA-Paar-Bereitstellung (VM-Instanz) zur SnapMirror Verkehrstrennung nur eine einzelne Netzwerkkarte hinzufügen.
- Um eine neue Netzwerkkarte hinzuzufügen, muss der von Ihnen bereitgestellte VM-Instanztyp über eine ungenutzte Netzwerkkarte verfügen.
- Die Quell- und Zielcluster sollten Zugriff auf dasselbe virtuelle Netzwerk (VNet) haben. Der Zielcluster ist ein Cloud Volumes ONTAP -System in Azure. Der Quellcluster kann ein Cloud Volumes ONTAP -System in Azure oder ein ONTAP System sein.

Schritt 1: Erstellen Sie eine zusätzliche Netzwerkkarte und verbinden Sie sie mit der Ziel-VM

Dieser Abschnitt enthält Anweisungen zum Erstellen einer zusätzlichen Netzwerkkarte und zum Anschließen an die Ziel-VM. Die Ziel-VM ist das Einzelknoten- oder HA-Paarsystem in Cloud Volumes ONTAP in Azure, in dem Sie Ihre zusätzliche Netzwerkkarte einrichten möchten.

Schritte

1. Stoppen Sie den Knoten in der ONTAP CLI.

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

2. Überprüfen Sie im Azure-Portal, ob der Status der VM (Knoten) „Beendet“ lautet.

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

3. Verwenden Sie die Bash-Umgebung in Azure Cloud Shell, um den Knoten zu stoppen.
   a. Stoppen Sie den Knoten.

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

   b. Heben Sie die Zuordnung des Knotens auf.

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

4. Konfigurieren Sie Netzwerksicherheitsgruppenregeln, um die beiden Subnetze (Quellcluster-Subnetz und Zielcluster-Subnetz) untereinander nicht routbar zu machen.
   a. Erstellen Sie die neue Netzwerkkarte auf der Ziel-VM.
   b. Suchen Sie die Subnetz-ID für das Subnetz des Quellclusters.

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

   c. Erstellen Sie die neue Netzwerkkarte auf der Ziel-VM mit der Subnetz-ID für das Subnetz des Quellclusters. Hier geben Sie den Namen für die neue Netzwerkkarte ein.

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

   d. Speichern Sie die private IP-Adresse. Diese IP-Adresse, <new_added_nic_primary_addr>, wird verwendet, um ein Intercluster-LIF inBroadcast-Domäne, Intercluster-LIF für die neue NIC .
5. Schließen Sie die neue Netzwerkkarte an die VM an.

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

6. Starten Sie die VM (den Knoten).

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

7. Gehen Sie im Azure-Portal zu **Netzwerk** und bestätigen Sie, dass die neue Netzwerkkarte, z. B. nic-new,

vorhanden ist und der beschleunigte Netzwerkbetrieb aktiviert ist.

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

Wiederholen Sie bei HA-Paar-Bereitstellungen die Schritte für den Partnerknoten.

Schritt 2: Erstellen Sie einen neuen IPspace, eine neue Broadcast-Domäne und ein Intercluster-LIF für die neue Netzwerkkarte

Ein separater IP-Bereich für LIFs zwischen Clustern bietet eine logische Trennung zwischen Netzwerkfunktionen für die Replikation zwischen Clustern.

Verwenden Sie für die folgenden Schritte die ONTAP CLI.

Schritte

1. Erstellen Sie den neuen IPspace (new_ipspace).

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

2. Erstellen Sie eine Broadcast-Domäne im neuen IPspace (new_ipspace) und fügen Sie den nic-new-Port hinzu.

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

3. Bei Einzelknotensystemen ist der neu hinzugefügte Port *e0b*. Bei HA-Paar-Bereitstellungen mit verwalteten Datenträgern ist der neu hinzugefügte Port *e0d*. Bei HA-Paar-Bereitstellungen mit Seitenblobs ist der neu hinzugefügte Port *e0e*. Verwenden Sie den Node-Name, nicht den VM-Name. Finden Sie den Node-Name, indem Sie `node show` ausführen.

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

4. Erstellen Sie ein Intercluster-LIF auf der neuen Broadcast-Domäne (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. Überprüfen Sie die Erstellung des neuen Intercluster-LIF.

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

Wiederholen Sie bei HA-Paar-Bereitstellungen die Schritte für den Partnerknoten.

Schritt 3: Überprüfen des Cluster-Peerings zwischen Quell- und Zielsystemen

Dieser Abschnitt enthält Anweisungen zum Überprüfen des Peerings zwischen den Quell- und Zielsystemen.

Verwenden Sie für die folgenden Schritte die ONTAP CLI.

Schritte

1. Überprüfen Sie, ob das Intercluster-LIF des Zielclusters das Intercluster-LIF des Quellclusters anpingen kann. Da der Zielcluster diesen Befehl ausführt, ist die Ziel-IP-Adresse die LIF-IP-Adresse zwischen den Clustern auf der Quelle.

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

2. Überprüfen Sie, ob das Intercluster-LIF des Quellclusters das Intercluster-LIF des Zielclusters anpingen kann. Das Ziel ist die IP-Adresse der neuen Netzwerkkarte, die am Ziel erstellt wurde.

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

Wiederholen Sie bei HA-Paar-Bereitstellungen die Schritte für den Partnerknoten.

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

Dieser Abschnitt enthält Anweisungen zum Erstellen eines SVM-Peerings zwischen dem Quell- und dem Zielsystem.

Verwenden Sie für die folgenden Schritte die ONTAP CLI.

Schritte

1. Erstellen Sie Cluster-Peering auf dem Ziel unter Verwendung der Quell-Intercluster-LIF-IP-Adresse als `-peer-addrs` . Listen Sie für HA-Paare die Quell-Intercluster-LIF-IP-Adresse für beide Knoten als `-peer -addrs` .

```
dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace
<new_ipspace>
```

2. Geben Sie die Passphrase ein und bestätigen Sie sie.
3. Erstellen Sie Cluster-Peering auf der Quelle unter Verwendung der LIF-IP-Adresse des Zielclusters als `peer-addrs` . Listen Sie für HA-Paare die Ziel-Intercluster-LIF-IP-Adresse für beide Knoten als `-peer`

`-addrs .`

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

4. Geben Sie die Passphrase ein und bestätigen Sie sie.
5. Überprüfen Sie, ob der Cluster gepeert wurde.

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

Bei erfolgreichem Peering wird im Verfügbarkeitsfeld **Verfügbar** angezeigt.

6. Erstellen Sie SVM-Peering auf dem Ziel. Sowohl Quell- als auch Ziel-SVMs sollten Daten-SVMs sein.

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

7. Akzeptieren Sie SVM-Peering.

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

8. Überprüfen Sie, ob die SVM gepeert wurde.

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

Peer-Status zeigt*`peered` * und Peering-Anwendungen zeigt*`snapmirror` *.

Schritt 5: Erstellen Sie eine SnapMirror -Replikationsbeziehung zwischen dem Quell- und Zielsystem

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

Um eine vorhandene SnapMirror -Replikationsbeziehung zu verschieben, müssen Sie zuerst die vorhandene SnapMirror -Replikationsbeziehung auflösen, bevor Sie eine neue SnapMirror -Replikationsbeziehung erstellen.

Verwenden Sie für die folgenden Schritte die ONTAP CLI.

Schritte

1. Erstellen Sie ein datengeschütztes Volume 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 Replikationsbeziehung auf dem Ziel, die die SnapMirror -Richtlinie und den Zeitplan für die Replikation enthält.

```
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 Replikationsbeziehung 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 ist `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 Zielvolumes mounten, eine Datei auf die Quelle schreiben und überprüfen, ob das Volume auf das Ziel repliziert wird.