Azure-Administration

Cloud Volumes ONTAP

NetApp
June 27, 2024

Inhalt

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.

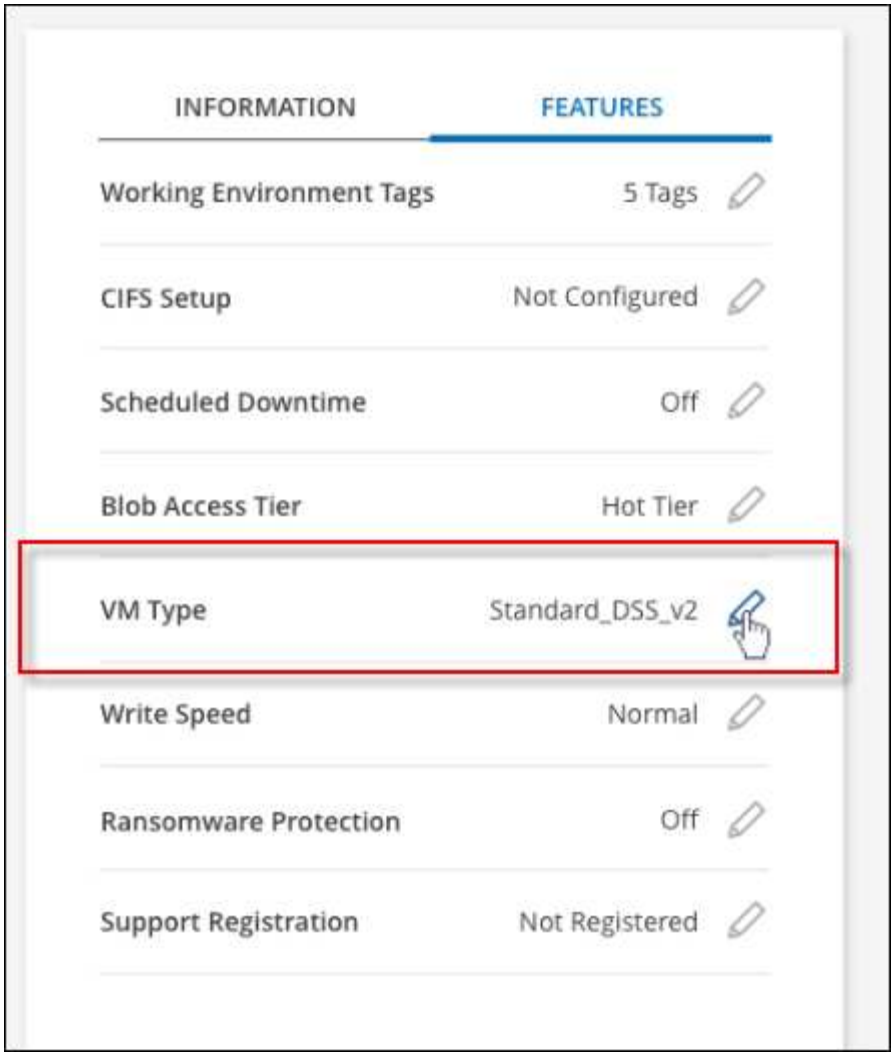
  Bei Systemen mit einem Node wird die I/O unterbrochen.

  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.

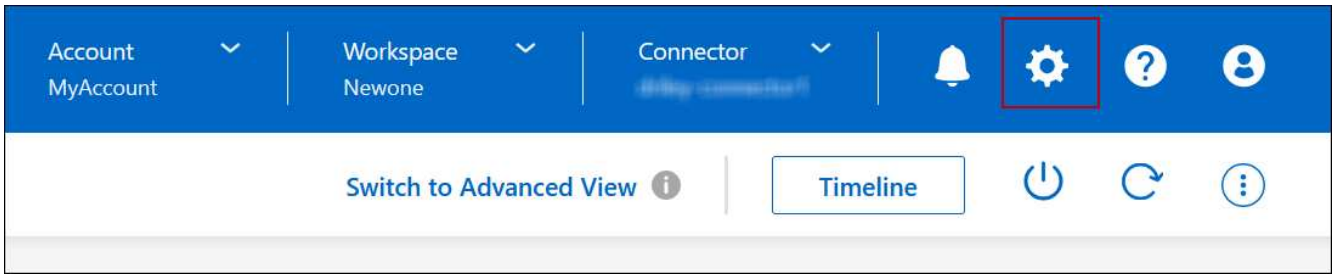
Dieser Prozess kann CIFS-Clients stören. Daten, die nicht von CIFS-Clients übertragen werden, können verloren gehen.

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 **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.

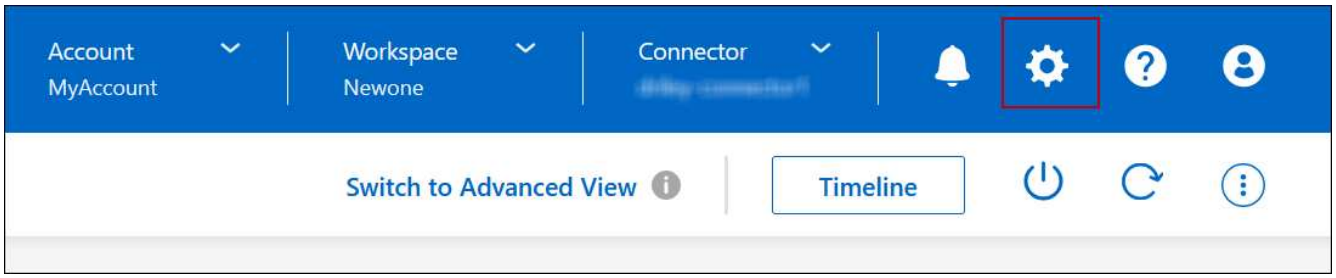
Deaktivieren Sie Azure Private Links, und verwenden Sie stattdessen Service-Endpunkte

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. Service-Endpunkte werden nur in unterstützt "Azure Region-Paare" Zwischen Stecker und Cloud Volumes ONTAP VNets.

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

Schritte

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

Nachdem Sie fertig sind

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

"Erfahren Sie, wie Sie direkten API-Datenverkehr auf dem Connector aktivieren"

Arbeiten Sie mit Azure Private Links

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

Anforderung für benutzerdefiniertes DNS

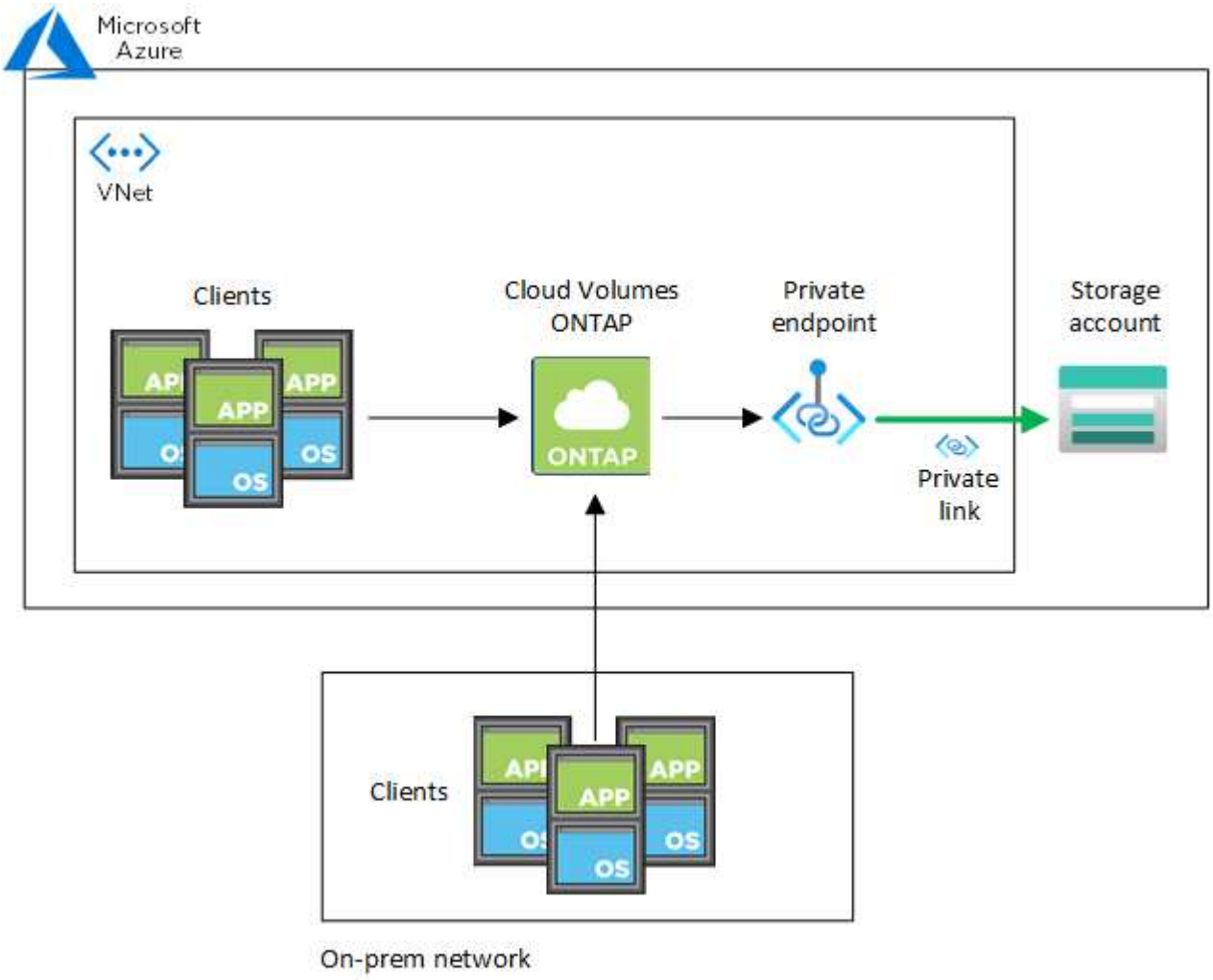
Wenn Sie optional mit benutzerdefinierten DNS arbeiten, müssen Sie von Ihren benutzerdefinierten DNS-Servern aus einen bedingten Forwarder zur Azure Private DNS Zone erstellen. Weitere Informationen finden Sie unter "Die Dokumentation von Azure über einen DNS-Forwarder".

Funktionsweise von Private Link-Verbindungen

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

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

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



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

Stellen Sie BlueXP Einzelheiten zu Ihrem Azure Private DNS zur Verfügung

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

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

Schritte

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

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

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

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

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

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

   Ein Neustart ist nicht erforderlich.

Rollback bei Ausfällen aktivieren

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

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

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

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

Rollback über die API aktivieren

Schritt

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

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

Rollback durch Aktualisierung von App.conf aktivieren

Schritte

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

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

   Ein Neustart ist nicht erforderlich.

Verschieben von Ressourcengruppen

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

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

Schritte

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

   Informationen zum Entfernen einer Arbeitsumgebung finden Sie unter "Entfernen von Cloud Volumes ONTAP Arbeitsumgebungen".

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

   Informationen zum Abschließen des Verzuvöllig finden Sie unter "Verschieben Sie Ressourcen in eine neue Ressourcengruppe oder ein Abonnement in der Microsoft Azure-Dokumentation".

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

Ergebnis

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