Erste Schritte in Azure

Cloud Manager 3.8

NetApp
March 25, 2024

Inhalt

Erste Schritte in Azure

Erste Schritte mit Cloud Volumes ONTAP für Azure

Erste Schritte mit Cloud Volumes ONTAP für Azure

Einen Konnektor erstellen

Wenn Sie keine haben "Stecker" Dennoch muss ein Kontoadministrator einen erstellen. "Erfahren Sie, wie Sie in Azure einen Connector erstellen".

Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von Cloud Manager aufgefordert, einen Connector bereitzustellen, wenn Sie noch keinen haben.

Planen Sie Ihre Konfiguration

Cloud Manager bietet vorkonfigurierte Pakete, die Ihren Workload-Anforderungen entsprechen, oder Sie können eine eigene Konfiguration erstellen. Wenn Sie sich für eine eigene Konfiguration entscheiden, sollten Sie sich mit den verfügbaren Optionen vertraut machen. "Weitere Informationen .".

Richten Sie Ihr Netzwerk ein

1. Stellen Sie sicher, dass Ihre vnet und Subnetze Verbindungen zwischen dem Connector und Cloud Volumes ONTAP unterstützen.
2. Aktivieren Sie den ausgehenden Internetzugriff über das Ziel-vnet, damit der Konnektor und der Cloud Volumes ONTAP mehrere Endpunkte kontaktieren können.

   Dieser Schritt ist wichtig, da der Connector Cloud Volumes ONTAP nicht ohne Outbound-Internetzugang verwalten kann. Wenn Sie die ausgehende Verbindung begrenzen müssen, lesen Sie die Liste der Endpunkte für "Anschluss und Cloud Volumes ONTAP".

"Erfahren Sie mehr über Netzwerkanforderungen".

Starten Sie Cloud Volumes ONTAP mit Cloud Manager

Klicken Sie auf **Arbeitsumgebung hinzufügen**, wählen Sie den Systemtyp aus, den Sie bereitstellen möchten, und führen Sie die Schritte im Assistenten aus. "Lesen Sie Schritt-für-Schritt-Anleitungen".

Weiterführende Links

- "Bewertung"
- "Erstellen eines Connectors über Cloud Manager"
- "Erstellen eines Connectors über den Azure Marketplace"
- "Installieren der Connector-Software auf einem Linux-Host"

- "Was Cloud Manager mit Azure-Berechtigungen tut"

Planen Ihrer Cloud Volumes ONTAP-Konfiguration in Azure

Wenn Sie Cloud Volumes ONTAP in Azure implementieren, können Sie entweder ein vorkonfiguriertes System wählen, das Ihren Workload-Anforderungen entspricht, oder Sie erstellen Ihre eigene Konfiguration. Wenn Sie sich für eine eigene Konfiguration entscheiden, sollten Sie sich mit den verfügbaren Optionen vertraut machen.

Auswahl eines Lizenztyps

Cloud Volumes ONTAP ist in zwei Preisoptionen erhältlich: Nutzungsbasiert und als BYOL-Modell (Bring-Your-Own-License). Für Pay-as-you-go können Sie zwischen drei Lizenzen wählen: Explore, Standard oder Premium. Jede Lizenz bietet verschiedene Kapazitäts- und Computing-Optionen.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP 9.7 in Azure"

Storage-Grenzen kennen

Die Rohkapazitätsgrenze für ein Cloud Volumes ONTAP System ist an die Lizenz gebunden. Zusätzliche Beschränkungen wirken sich auf die Größe von Aggregaten und Volumes aus. Sie sollten sich dieser Grenzen bei der Planung Ihrer Konfiguration bewusst sein.

"Storage-Höchstwerte für Cloud Volumes ONTAP 9.7 in Azure"

Dimensionierung Ihres Systems in Azure

Mit der Dimensionierung Ihres Cloud Volumes ONTAP Systems können Sie die Anforderungen an Performance und Kapazität erfüllen. Bei der Auswahl von VM-Typ, Festplattentyp und Festplattengröße sind einige wichtige Punkte zu beachten:

Typ der virtuellen Maschine

Sehen Sie sich die unterstützten Typen von Virtual Machines in an "Versionshinweise zu Cloud Volumes ONTAP" Und überprüfen Sie anschließend Details zu jedem unterstützten VM-Typ. Beachten Sie, dass jeder VM-Typ eine bestimmte Anzahl an Datenfestplatten unterstützt.

- "Azure-Dokumentation: Allgemeine Größe virtueller Maschinen"
- "Azure-Dokumentation: Für den Speicher optimierte Größen virtueller Maschinen"

Azure-Festplattentyp

Wenn Sie Volumes für Cloud Volumes ONTAP erstellen, müssen Sie den zugrunde liegenden Cloud-Storage auswählen, den Cloud Volumes ONTAP als Festplatte verwendet.

HA-Systeme verwenden Premium-Blobs auf Seite. In der Zwischenzeit können Systeme mit einem Node zwei Typen von Azure Managed Disks nutzen:

- *Premium SSD Managed Disks* bieten hohe Performance für I/O-intensive Workloads zu höheren Kosten.
- *Standard SSD Managed Disks* bieten konsistente Performance für Workloads, die niedrige IOPS erfordern.

- *Standard HDD Managed Disks* sind eine gute Wahl, wenn Sie keine hohen IOPS benötigen und Ihre Kosten senken möchten.

  Weitere Details zu den Anwendungsfällen für diese Festplatten finden Sie unter "Microsoft Azure-Dokumentation: Welche Festplattentypen sind in Azure verfügbar?".

Festplattengröße Azure

Wenn Sie Cloud Volumes ONTAP Instanzen starten, müssen Sie die standardmäßige Festplattengröße für Aggregate auswählen. Cloud Manager verwendet diese Festplattengröße für das anfängliche Aggregat und für alle zusätzlichen Aggregate, die es erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Sie können Aggregate erstellen, die eine Festplattengröße verwenden, die sich von der Standardgröße unterscheidet "Verwenden der erweiterten Zuweisungsoption".

Alle Festplatten in einem Aggregat müssen dieselbe Größe haben.

Bei der Auswahl der Festplattengröße sollten Sie mehrere Faktoren berücksichtigen. Die Festplattengröße wirkt sich darauf aus, wie viel Sie für Storage zahlen, wie viele Volumes Sie in einem Aggregat erstellen können, wie viel Kapazität insgesamt für Cloud Volumes ONTAP zur Verfügung steht und wie hoch die Storage-Performance ist.

Die Performance von Azure Premium Storage ist an die Festplattengröße gebunden. Größere Festplatten bieten höhere IOPS und einen höheren Durchsatz. Beispielsweise kann die Auswahl von 1-TB-Festplatten eine bessere Performance bieten als 500-GB-Festplatten zu höheren Kosten.

Es gibt keine Performance-Unterschiede zwischen den Festplattengrößen für Standard-Storage. Sie sollten die Festplattengröße basierend auf der benötigten Kapazität auswählen.

Unter Azure finden Sie IOPS und Durchsatz nach Festplattengröße:

- "Microsoft Azure: Preisgestaltung für Managed Disks"
- "Microsoft Azure: Page Blobs Pricing"

Auswahl einer Konfiguration, die Flash Cache unterstützt

Eine Cloud Volumes ONTAP-Konfiguration in Azure umfasst lokalen NVMe-Storage, den Cloud Volumes ONTAP zur Steigerung der Performance als *Flash Cache* verwendet. "Weitere Informationen zu Flash Cache".

Azure Network Information Worksheet

Wenn Sie Cloud Volumes ONTAP in Azure implementieren, müssen Sie Details zu Ihrem virtuellen Netzwerk angeben. Sie können ein Arbeitsblatt verwenden, um die Informationen von Ihrem Administrator zu sammeln.

Azure Informationen	Ihr Wert
Region	
Virtuelles Netzwerk (VNet)	
Subnetz	
Netzwerksicherheitsgruppe (wenn Sie Ihre eigene verwenden)	

Auswählen einer Schreibgeschwindigkeit

Mit Cloud Manager können Sie eine Einstellung für die Schreibgeschwindigkeit für Cloud Volumes ONTAP Systeme mit einem Node wählen. Bevor Sie sich für eine Schreibgeschwindigkeit entscheiden, sollten Sie die Unterschiede zwischen den normalen und hohen Einstellungen sowie Risiken und Empfehlungen verstehen, wenn Sie eine hohe Schreibgeschwindigkeit verwenden.

Unterschied zwischen normaler Schreibgeschwindigkeit und hoher Schreibgeschwindigkeit

Wenn Sie sich für eine normale Schreibgeschwindigkeit entscheiden, werden die Daten direkt auf die Festplatte geschrieben, wodurch die Wahrscheinlichkeit eines Datenverlusts bei einem ungeplanten Systemausfall verringert wird.

Wenn Sie hohe Schreibgeschwindigkeit wählen, werden die Daten vor dem Schreiben auf die Festplatte im Speicher gepuffert, was eine schnellere Schreibleistung ermöglicht. Aufgrund dieses Cachings besteht die Gefahr eines Datenverlusts, wenn ein ungeplanter Systemausfall auftritt.

Die Datenmenge, die bei einem ungeplanten Systemausfall verloren gehen kann, entspricht der Spanne der letzten beiden Konsistenzpunkte. Ein Konsistenzpunkt ist das Schreiben gepufferter Daten auf die Festplatte. Ein Konsistenzpunkt tritt auf, wenn das Schreibprotokoll voll ist oder nach 10 Sekunden (je nachdem, was zuerst eintritt). Die Performance des AWS EBS-Volumes kann sich jedoch auf die Verarbeitungszeit des Konsistenzpunkts auswirken.

Wann wird hohe Schreibgeschwindigkeit verwendet

Hohe Schreibgeschwindigkeit ist eine gute Wahl, wenn für Ihre Workload eine schnelle Schreibleistung erforderlich ist und Sie das Risiko eines Datenverlusts bei einem ungeplanten Systemausfall überstehen können.

Empfehlungen bei hoher Schreibgeschwindigkeit

Wenn Sie die hohe Schreibgeschwindigkeit aktivieren, sollten Sie den Schreibschutz auf der Anwendungsebene sicherstellen.

Auswählen eines Volume-Nutzungsprofils

ONTAP umfasst mehrere Storage-Effizienzfunktionen, mit denen Sie die benötigte Storage-Gesamtmenge reduzieren können. Wenn Sie ein Volume in Cloud Manager erstellen, können Sie ein Profil auswählen, das diese Funktionen aktiviert, oder ein Profil, das sie deaktiviert. Sie sollten mehr über diese Funktionen erfahren, um zu entscheiden, welches Profil Sie verwenden möchten.

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.

Netzwerkanforderungen für die Implementierung und das Management von Cloud Volumes ONTAP in Azure

Richten Sie Ihr Azure Netzwerk ein, um Cloud Volumes ONTAP Systeme ordnungsgemäß funktionieren zu können. Dazu gehört auch die Vernetzung von Connector und Cloud Volumes ONTAP.

Anforderungen für Cloud Volumes ONTAP

Die folgenden Netzwerkanforderungen müssen in Azure erfüllt werden.

Outbound-Internetzugang für Cloud Volumes ONTAP

Cloud Volumes ONTAP erfordert ausgehenden Internetzugang, um Nachrichten an NetApp AutoSupport zu senden, der proaktiv den Zustand Ihres Storage überwacht.

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

"Erfahren Sie, wie AutoSupport konfiguriert wird".

Sicherheitsgruppen

Sie müssen keine Sicherheitsgruppen erstellen, da Cloud Manager dies für Sie tut. Wenn Sie Ihre eigene Verwendung benötigen, lesen Sie die unten aufgeführten Sicherheitsgruppenregeln.

Anzahl der IP-Adressen

Cloud Manager weist Cloud Volumes ONTAP in Azure die folgende Anzahl von IP-Adressen zu:

- Single Node: 5 IP-Adressen
- HA-Paar: 16 IP-Adressen

  Cloud Manager erstellt eine SVM-Management-LIF auf HA-Paare, jedoch nicht auf Systemen mit einem einzelnen Node in Azure.

Ein LIF ist eine IP-Adresse, die einem physischen Port zugewiesen ist. Für Managementtools wie SnapCenter ist eine SVM-Management-LIF erforderlich.

Verbindung von Cloud Volumes ONTAP zu Azure Blob Storage für Data Tiering

Wenn Sie „kalte“ Daten für den Azure Blob Storage Tiering möchten, müssen Sie keine Verbindung zwischen der Performance-Tier und der Kapazitäts-Tier einrichten, solange Cloud Manager über die erforderlichen Berechtigungen verfügt. Cloud Manager unterstützt ein vnet-Service-Endpunkt für Sie, wenn die Cloud Manager-Richtlinie über die folgenden Berechtigungen verfügt:

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Diese Berechtigungen sind in der neuesten enthalten "Cloud Manager-Richtlinie".

Weitere Informationen zum Einrichten von Daten-Tiering finden Sie unter "Tiering von kalten Daten auf kostengünstigen Objekt-Storage".

Verbindungen zu ONTAP Systemen in anderen Netzwerken

Um Daten zwischen einem Cloud Volumes ONTAP System in Azure und ONTAP Systemen in anderen Netzwerken zu replizieren, müssen Sie über eine VPN-Verbindung zwischen Azure VNet und dem anderen Netzwerk verfügen, z. B. einem AWS VPC oder Ihrem Unternehmensnetzwerk.

Anweisungen finden Sie unter "Microsoft Azure Dokumentation: Erstellen Sie eine Site-to-Site-Verbindung im Azure-Portal".

Anforderungen an den Steckverbinder

Richten Sie Ihr Netzwerk ein, damit der Connector Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen kann. Der wichtigste Schritt besteht darin, ausgehenden Internetzugriff auf verschiedene Endpunkte zu gewährleisten.

Wenn Ihr Netzwerk für die gesamte Kommunikation mit dem Internet einen Proxyserver verwendet, können Sie den Proxyserver über die Seite Einstellungen angeben. Siehe "Konfigurieren des Connectors für die Verwendung eines Proxy-Servers".

Verbindungen zu Zielnetzwerken

Für einen Connector ist eine Netzwerkverbindung zu den VPCs und VNets erforderlich, in denen Cloud Volumes ONTAP bereitgestellt werden soll.

Wenn Sie beispielsweise einen Connector in Ihrem Unternehmensnetzwerk installieren, müssen Sie eine VPN-Verbindung zur VPC oder vnet einrichten, in der Sie Cloud Volumes ONTAP starten.

Outbound-Internetzugang

Für den Connector ist ein abgehender Internetzugang erforderlich, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung zu managen. Ein Connector kontaktiert folgende Endpunkte beim Managen von Ressourcen in Azure:

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den meisten Azure Regionen.
https://management.microsoftazure.de https://login.microsoftonline.de	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den Azure Germany Regionen.

Endpunkte	Zweck
https://management.usgovcloudapi.net https://login.microsoftonline.com	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den Azure US Gov Regionen.
https://api.services.cloud.netapp.com:443	API-Anfragen an NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://repo.cloud.support.netapp.com	Wird zum Herunterladen der Abhängigkeiten von Cloud Manager verwendet.
http://repo.mysql.com/	Zum Herunterladen von MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Cloud Manager kann Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images abrufen und herunterladen.
https://cloudmanagerinfraprod.azurecr.io	Zugriff auf Software-Images von Container-Komponenten für eine Infrastruktur, die Docker ausführt und eine Lösung für die Service-Integration mit Cloud Manager bietet.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cloudmanager.cloud.netapp.com	Kommunikation mit dem Cloud Manager-Service, der Cloud Central-Konten einschließt
https://netapp-cloud-account.auth0.com	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
https://mysupport.netapp.com	Kommunikation mit NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Kommunikation mit NetApp bei Systemlizenzrechten und Support-Registrierung
https://ipa-signer.cloudmanager.netapp.com	Ermöglicht Cloud Manager die Generierung von Lizenzen (beispielsweise eine FlexCache Lizenz für Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Erforderlich, um Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster zu verbinden Mit den Endpunkten ist die Installation von NetApp Trident möglich.
*.blob.core.windows.net	Bei Verwendung eines Proxy erforderlich für HA-Paare

Endpunkte	Zweck
Verschiedene Standorte von Drittanbietern, z. B.: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org An Standorten von Drittanbietern können Änderungen vorgenommen werden.	Während Upgrades lädt Cloud Manager die neuesten Pakete für Abhängigkeiten von Drittanbietern herunter.

Während Sie fast alle Aufgaben über die SaaS-Benutzeroberfläche ausführen sollten, steht auf dem Connector weiterhin eine lokale Benutzeroberfläche zur Verfügung. Die Maschine, auf der der Webbrowser ausgeführt wird, muss über Verbindungen zu den folgenden Endpunkten verfügen:

Endpunkte	Zweck
Der Connector-Host	Sie müssen die IP-Adresse des Hosts aus einem Webbrowser eingeben, um die Cloud Manager-Konsole zu laden. Je nach Ihrer Verbindung mit Ihrem Cloud-Provider können Sie die private IP oder eine dem Host zugewiesene öffentliche IP verwenden: • Eine private IP funktioniert, wenn Sie über ein VPN verfügen und direkten Zugriff auf Ihr virtuelles Netzwerk haben • Eine öffentliche IP funktioniert in jedem Netzwerkszenario In jedem Fall sollten Sie den Netzwerkzugriff sichern, indem Sie sicherstellen, dass die Sicherheitsgruppenregeln den Zugriff nur von autorisierten IPs oder Subnetzen ermöglichen.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Ihr Webbrowser stellt über NetApp Cloud Central eine Verbindung zu diesen Endpunkten her, um eine zentralisierte Benutzerauthentifizierung zu ermöglichen.
https://widget.intercom.io	Für Ihren Produkt-Chat, der Ihnen das Gespräch mit NetApp Cloud-Experten ermöglicht.

Regeln für Sicherheitsgruppen für Cloud Volumes ONTAP

Cloud Manager erstellt Azure-Sicherheitsgruppen mit den ein- und ausgehenden Regeln, die für den erfolgreichen Betrieb von Cloud Volumes ONTAP erforderlich sind. Sie können die Ports zu Testzwecken oder zur Verwendung eigener Sicherheitsgruppen verwenden.

Die Sicherheitsgruppe für Cloud Volumes ONTAP erfordert sowohl eingehende als auch ausgehende Regeln.

Eingehende Regeln für Single-Node-Systeme

Die unten aufgeführten Regeln erlauben den Datenverkehr, es sei denn, die Beschreibung stellt fest, dass bestimmte eingehende Daten blockiert werden.

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
1000 Inbound_SSH	22 TCP	Beliebige Art	SSH-Zugriff auf die IP-Adresse der Cluster Management LIF oder einer Node Management LIF
1001 Inbound_http	80 TCP	Beliebige Art	HTTP-Zugriff auf die System Manager Webkonsole mit der IP-Adresse der Cluster-Management-LIF
1002 Inbound_111_tcp	111 TCP	Beliebige Art	Remote-Prozeduraufruf für NFS
1003 Inbound_111_udp	111 UDP	Beliebige Art	Remote-Prozeduraufruf für NFS
1004 eingehend_139	139 TCP	Beliebige Art	NetBIOS-Servicesitzung für CIFS
1005 Inbound_161-162 _tcp	161-162 TCP	Beliebige Art	Einfaches Netzwerkverwaltungsprotokoll
1006 Inbound_161-162 _udp	161-162 UDP	Beliebige Art	Einfaches Netzwerkverwaltungsprotokoll
1007 eingehend_443	443 TCP	Beliebige Art	HTTPS-Zugriff auf die System Manager-Webkonsole unter Verwendung der IP-Adresse der Cluster-Management-LIF
1008 eingehend_445	445 TCP	Beliebige Art	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
1009 Inbound_635_tcp	635 TCP	Beliebige Art	NFS-Mount
1010 Inbound_635_udp	635 UDP	Beliebige Art	NFS-Mount
1011 eingehend_749	749 TCP	Beliebige Art	Kerberos
1012 Inbound_2049_tcp	2049 TCP	Beliebige Art	NFS-Server-Daemon
1013 Inbound_2049_udp	2049 UDP	Beliebige Art	NFS-Server-Daemon
1014 eingehend_3260	3260 TCP	Beliebige Art	ISCSI-Zugriff über die iSCSI-Daten-LIF

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
1015 Inbound_4045-4046_tcp	4045-4046 TCP	Beliebige Art	NFS Lock Daemon und Network Status Monitor
1016 Inbound_4045-4046_udp	4045-4046 UDP	Beliebige Art	NFS Lock Daemon und Network Status Monitor
1017 eingehend_10000	10000 TCP	Beliebige Art	Backup mit NDMP
1018 eingehend_11104-11105	11104-11105 TCP	Beliebige Art	SnapMirror Datenübertragung
3000 Inbound_Deny_all_tcp	Alle TCP-Ports	Beliebige Art	Blockieren Sie den gesamten anderen TCP-eingehenden Datenverkehr
3001 Inbound_Deny_all_udp	Alle Ports UDP	Beliebige Art	Alle anderen UDP-eingehenden Datenverkehr blockieren
65000 AllowVnetInBound	Alle Ports und Protokolle	VirtualNetwork zu VirtualNetwork	Eingehender Verkehr aus dem vnet
65001 AllowAzureLoad BalancerInBound	Alle Ports und Protokolle	AzureLoadBalancer zu jedem	Datenverkehr vom Azure Standard Load Balancer
65500 DenyAllInBound	Alle Ports und Protokolle	Beliebige Art	Alle anderen eingehenden Datenverkehr blockieren

Eingehende Regeln für HA-Systeme

Die unten aufgeführten Regeln erlauben den Datenverkehr, es sei denn, die Beschreibung stellt fest, dass bestimmte eingehende Daten blockiert werden.

HA-Systeme weisen weniger eingehende Regeln als Systeme mit einzelnen Nodes auf, da eingehender Datenverkehr durch den Azure Standard Load Balancer geleitet wird. Aus diesem Grund sollte der Verkehr aus dem Load Balancer geöffnet sein, wie in der Regel "AllowAzureLoadBalancerInBound" gezeigt.

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
100 eingehend_443	443 beliebiges Protokoll	Beliebige Art	HTTPS-Zugriff auf die System Manager-Webkonsole unter Verwendung der IP-Adresse der Cluster-Management-LIF
101 Inbound_111_tcp	111 beliebiges Protokoll	Beliebige Art	Remote-Prozeduraufruf für NFS
102 Inbound_2049_tcp	2049 beliebiges Protokoll	Beliebige Art	NFS-Server-Daemon

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
111 Inbound_SSH	22 beliebiges Protokoll	Beliebige Art	SSH-Zugriff auf die IP-Adresse der Cluster Management LIF oder einer Node Management LIF
121 eingehend_53	53 beliebiges Protokoll	Beliebige Art	DNS und CIFS
65000 AllowVnetInBound	Alle Ports und Protokolle	VirtualNetwork zu VirtualNetwork	Eingehender Verkehr aus dem vnet
65001 AllowAzureLoad BalancerInBound	Alle Ports und Protokolle	AzureLoadBalancer zu jedem	Datenverkehr vom Azure Standard Load Balancer
65500 DenyAllInBound	Alle Ports und Protokolle	Beliebige Art	Alle anderen eingehenden Datenverkehr blockieren

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP enthält die folgenden ausgehenden Regeln.

Port	Protokoll	Zweck
Alle	Alle TCP	Gesamter abgehender Datenverkehr
Alle	Alle UDP-Protokolle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie strenge Regeln für ausgehenden Datenverkehr benötigen, können Sie mit den folgenden Informationen nur die Ports öffnen, die für die ausgehende Kommunikation durch Cloud Volumes ONTAP erforderlich sind.

Die Quelle ist die Schnittstelle (IP-Adresse) auf dem Cloud Volumes ONTAP System.

Service	Port	Protokoll	Quelle	Ziel	Zweck
Active Directory	88	TCP	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	137	UDP	Node Management-LIF	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	138	UDP	Node Management-LIF	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	139	TCP	Node Management-LIF	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	389	TCP UND UDP	Node Management-LIF	Active Directory-Gesamtstruktur	LDAP
	445	TCP	Node Management-LIF	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	464	TCP	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	464	UDP	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	749	TCP	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	88	TCP	Daten-LIF (NFS, CIFS, iSCSI)	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	137	UDP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	138	UDP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	139	TCP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	389	TCP UND UDP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	LDAP
	445	TCP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	464	TCP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	464	UDP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	749	TCP	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V - Passwort ändern und festlegen (RPCSEC_GSS)
DHCP	68	UDP	Node Management-LIF	DHCP	DHCP-Client für die erstmalige Einrichtung

Service	Port	Protokoll	Quelle	Ziel	Zweck
DHCPS	67	UDP	Node Management-LIF	DHCP	DHCP-Server
DNS	53	UDP	Node Management LIF und Daten LIF (NFS, CIFS)	DNS	DNS
NDMP	18600-18699	TCP	Node Management-LIF	Zielserver	NDMP-Kopie
SMTP	25	TCP	Node Management-LIF	Mailserver	SMTP-Warnungen können für AutoSupport verwendet werden
SNMP	161	TCP	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	161	UDP	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	162	TCP	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	162	UDP	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
SnapMirror	11104	TCP	Intercluster-LIF	ONTAP Intercluster-LIFs	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
	11105	TCP	Intercluster-LIF	ONTAP Intercluster-LIFs	SnapMirror Datenübertragung
Syslog	514	UDP	Node Management-LIF	Syslog-Server	Syslog-Weiterleitungsmeldungen

Sicherheitsgruppenregeln für den Konnektor

Die Sicherheitsgruppe für den Konnektor erfordert sowohl ein- als auch ausgehende Regeln.

Regeln für eingehende Anrufe

Die Quelle für eingehende Regeln in der vordefinierten Sicherheitsgruppe ist 0.0.0.0/0.

Port	Protokoll	Zweck
22	SSH	Bietet SSH-Zugriff auf den Connector-Host
80	HTTP	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
443	HTTPS	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Konnektor öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Connector enthält die folgenden ausgehenden Regeln.

Port	Protokoll	Zweck
Alle	Alle TCP	Gesamter abgehender Datenverkehr
Alle	Alle UDP-Protokolle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.

Die Quell-IP-Adresse ist der Connector-Host.

Service	Port	Protokoll	Ziel	Zweck
Active Directory	88	TCP	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	139	TCP	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	389	TCP	Active Directory-Gesamtstruktur	LDAP
	445	TCP	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	464	TCP	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	749	TCP	Active Directory-Gesamtstruktur	Active Directory Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	137	UDP	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	138	UDP	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	464	UDP	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
API-Aufrufe und AutoSupport	443	HTTPS	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe an AWS und ONTAP und Senden von AutoSupport Nachrichten an NetApp
API-Aufrufe	3000	TCP	ONTAP Cluster Management LIF	API-Aufrufe für ONTAP
DNS	53	UDP	DNS	Wird für die DNS-Auflösung durch Cloud Manager verwendet

Starten von Cloud Volumes ONTAP in Azure

Sie können ein Single-Node-System oder ein HA-Paar in Azure starten, indem Sie eine Cloud Volumes ONTAP-Arbeitsumgebung in Cloud Manager erstellen.

Bevor Sie beginnen

- Sie sollten ein haben "Anschluss, der Ihrem Arbeitsbereich zugeordnet ist".

Sie müssen ein Kontoadministrator sein, um einen Konnektor zu erstellen. Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, fordert Cloud Manager Sie auf, einen Connector zu erstellen, wenn Sie noch keinen haben.

- "Sie sollten darauf vorbereitet sein, den Konnektor jederzeit in Betrieb zu nehmen".
- Sie sollten eine Konfiguration auswählen und Azure Netzwerkinformationen von Ihrem Administrator erhalten haben. Weitere Informationen finden Sie unter "Planung Ihrer Cloud Volumes ONTAP Konfiguration".
- Für die Implementierung eines BYOL-Systems benötigen Sie für jeden Node die 20-stellige Seriennummer (Lizenzschlüssel).

Über diese Aufgabe

Wenn Cloud Manager ein Cloud Volumes ONTAP-System in Azure erstellt, werden mehrere Azure-Objekte wie eine Ressourcengruppe, Netzwerkschnittstellen und Storage-Konten erstellt. Sie können eine Zusammenfassung der Ressourcen am Ende des Assistenten überprüfen.

Risiko von Datenverlusten

Aufgrund des Risikos eines Datenverlusts wird die Bereitstellung von Cloud Volumes ONTAP in einer vorhandenen, gemeinsam genutzten Ressourcengruppe nicht empfohlen. Das Rollback ist derzeit standardmäßig deaktiviert, wenn die API zur Bereitstellung in einer vorhandenen Ressourcengruppe verwendet wird. Durch Löschen von Cloud Volumes ONTAP werden möglicherweise weitere Ressourcen aus dieser freigegebenen Gruppe gelöscht.

Als Best Practice empfiehlt es sich, eine neue, dedizierte Ressourcengruppe für Cloud Volumes ONTAP zu verwenden. Dies ist die Standard- und einzige empfohlene Option, wenn Sie Cloud Volumes ONTAP in Azure über Cloud Manager implementieren.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.
2. **Wählen Sie einen Standort**: Wählen Sie **Microsoft Azure** und **Cloud Volumes ONTAP Single Node** oder **Cloud Volumes ONTAP High Availability**.
3. **Details und Anmeldeinformationen**: Optional können Sie die Azure-Anmeldeinformationen und das Abonnement ändern, einen Cluster-Namen und einen Ressourcengruppennamen angeben, bei Bedarf Tags hinzufügen und dann Anmeldeinformationen angeben.

   In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Name der Arbeitsumgebung	Cloud Manager verwendet den Namen der Arbeitsumgebung, um sowohl das Cloud Volumes ONTAP System als auch die virtuelle Azure Maschine zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.

Feld	Beschreibung
Name der Ressourcengruppe	Behalten Sie den Standardnamen für die neue Ressourcengruppe bei, oder deaktivieren Sie **Standard verwenden** und geben Sie Ihren eigenen Namen für die neue Ressourcengruppe ein. Als Best Practice empfiehlt es sich, eine neue, dedizierte Ressourcengruppe für Cloud Volumes ONTAP zu verwenden. Es ist zwar möglich, Cloud Volumes ONTAP in einer vorhandenen, gemeinsam genutzten Ressourcengruppe mit Hilfe der API zu implementieren, es wird jedoch aufgrund des Risikos von Datenverlust nicht empfohlen. Weitere Informationen finden Sie in der oben stehenden Warnung.
Tags	Tags sind Metadaten für Ihre Azure Ressourcen. Wenn Sie in diesem Feld Tags eingeben, werden sie von Cloud Manager der Ressourcengruppe hinzugefügt, die dem Cloud Volumes ONTAP System zugeordnet ist. Sie können bis zu vier Tags aus der Benutzeroberfläche hinzufügen, wenn Sie eine Arbeitsumgebung erstellen. Nach der Erstellung können Sie weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen einer Arbeitsumgebung nicht auf vier Tags beschränkt. Informationen zu Tags finden Sie unter "Microsoft Azure-Dokumentation: Verwenden von Tags zur Organisation Ihrer Azure-Ressourcen".
Benutzername und Passwort	Dies sind die Anmeldedaten für das Cloud Volumes ONTAP Cluster-Administratorkonto. Sie können diese Anmeldedaten verwenden, um über OnCommand System Manager oder seine CLI eine Verbindung zu Cloud Volumes ONTAP herzustellen.
Anmeldeinformationen bearbeiten	Sie können verschiedene Azure Zugangsdaten und ein anderes Azure Abonnement für dieses Cloud Volumes ONTAP System wählen. Sie müssen ein Azure Marketplace Abonnement mit dem ausgewählten Azure Abonnement verknüpfen, um ein Pay-as-you-go Cloud Volumes ONTAP System zu implementieren. "Hier erfahren Sie, wie Sie Anmeldedaten hinzufügen".

Im folgenden Video wird gezeigt, wie Sie ein Marketplace-Abonnement zu einem Azure-Abonnement verknüpfen:

► https://docs.netapp.com/de-de/occm38//media/video_subscribing_azure.mp4 *(video)*

4. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie nicht mit Cloud Volumes ONTAP verwenden möchten.
   - "Erfahren Sie mehr über Cloud Compliance".
   - "Weitere Informationen zu Backup in der Cloud".
5. **Standort & Konnektivität**: Wählen Sie einen Standort und eine Sicherheitsgruppe aus und aktivieren Sie das Kontrollkästchen, um die Netzwerkverbindung zwischen Cloud Manager und dem Zielspeicherort zu bestätigen.
6. **Lizenz- und Support-Site-Konto**: Geben Sie an, ob Sie Pay-as-you-go oder BYOL verwenden möchten, und legen Sie dann ein NetApp Support Site Konto fest.

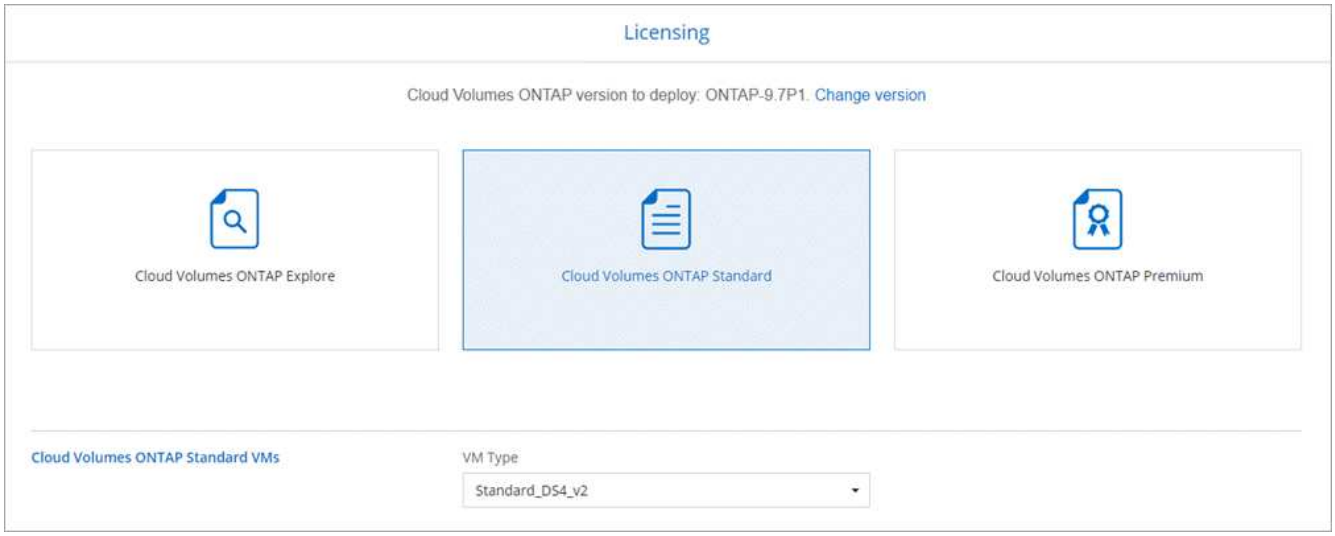
   Informationen zur Funktionsweise von Lizenzen finden Sie unter "Lizenzierung".

   Ein NetApp Support Site Konto ist optional für „Pay-as-you-go“-Systeme erhältlich, wird aber für BYOL-Systeme benötigt. "Erfahren Sie, wie Sie Konten der NetApp Support Site hinzufügen".

7. **Vorkonfigurierte Pakete**: Ein Paket zur schnellen Bereitstellung eines Cloud Volumes ONTAP-Systems einrichten oder auf **eigene Konfiguration erstellen** klicken.

Wenn Sie eines der Pakete auswählen, müssen Sie nur ein Volume angeben und dann die Konfiguration prüfen und genehmigen.

8. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP-Version nach Bedarf, wählen Sie eine Lizenz und wählen Sie einen virtuellen Maschinentyp.



Wenn sich Ihre Anforderungen nach dem Start des Systems ändern, können Sie die Lizenz oder den Typ der virtuellen Maschine später ändern.

> Wenn für die ausgewählte Version ein neuer Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert Cloud Manager das System beim Erstellen der Arbeitsumgebung auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.6 RC1 und 9.6 GA auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.6 bis 9.7.

9. **Vom Azure Marketplace abonnieren**: Folgen Sie den Schritten, wenn Cloud Manager programmatische Bereitstellungen von Cloud Volumes ONTAP nicht aktivieren könnte.
10. **Zugrunde liegende Storage-Ressourcen**: Wählen Sie die Einstellungen für das anfängliche Aggregat: Einen Festplattentyp, eine Größe für jede Festplatte und ob Daten-Tiering zu Blob-Storage aktiviert werden soll.

    Beachten Sie Folgendes:

    - Der Festplattentyp ist für das anfängliche Volume. Sie können einen anderen Festplattentyp für nachfolgende Volumes auswählen.
    - Die Festplattengröße gilt für alle Festplatten im ursprünglichen Aggregat und für alle zusätzlichen Aggregate, die Cloud Manager erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuweisungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

      Hilfe bei der Auswahl von Festplattentyp und -Größe finden Sie unter "Dimensionierung Ihres Systems in Azure".

    - Sie können eine bestimmte Volume-Tiering-Richtlinie auswählen, wenn Sie ein Volume erstellen oder bearbeiten.
    - Wenn Sie das Daten-Tiering deaktivieren, können Sie es bei nachfolgenden Aggregaten aktivieren.

"Weitere Informationen zum Daten-Tiering".

11. **Schreibgeschwindigkeit & WURM** (nur Systeme mit einem Knoten): Wählen Sie **normale** oder **hohe** Schreibgeschwindigkeit und aktivieren Sie ggf. den WORM-Speicher (Write Once, Read Many).

    Auswahl einer Schreibgeschwindigkeit wird nur bei Single-Node-Systemen unterstützt.

    "Erfahren Sie mehr über Schreibgeschwindigkeit".

    WORM kann nicht aktiviert werden, wenn Daten-Tiering aktiviert wurde.

    "Erfahren Sie mehr über WORM Storage".

12. **Secure Communication to Storage & WORM** (nur HA): Wählen Sie, ob eine HTTPS-Verbindung zu Azure-Speicherkonten aktiviert und ggf. WORM-Speicher (Write Once, Read Many) aktiviert werden soll.

    Die HTTPS-Verbindung besteht aus einem Cloud Volumes ONTAP 9.7 HA-Paar zu Azure Storage-Konten. Beachten Sie, dass die Aktivierung dieser Option sich auf die Schreib-Performance auswirken kann. Sie können die Einstellung nicht ändern, nachdem Sie die Arbeitsumgebung erstellt haben.

    "Erfahren Sie mehr über WORM Storage".

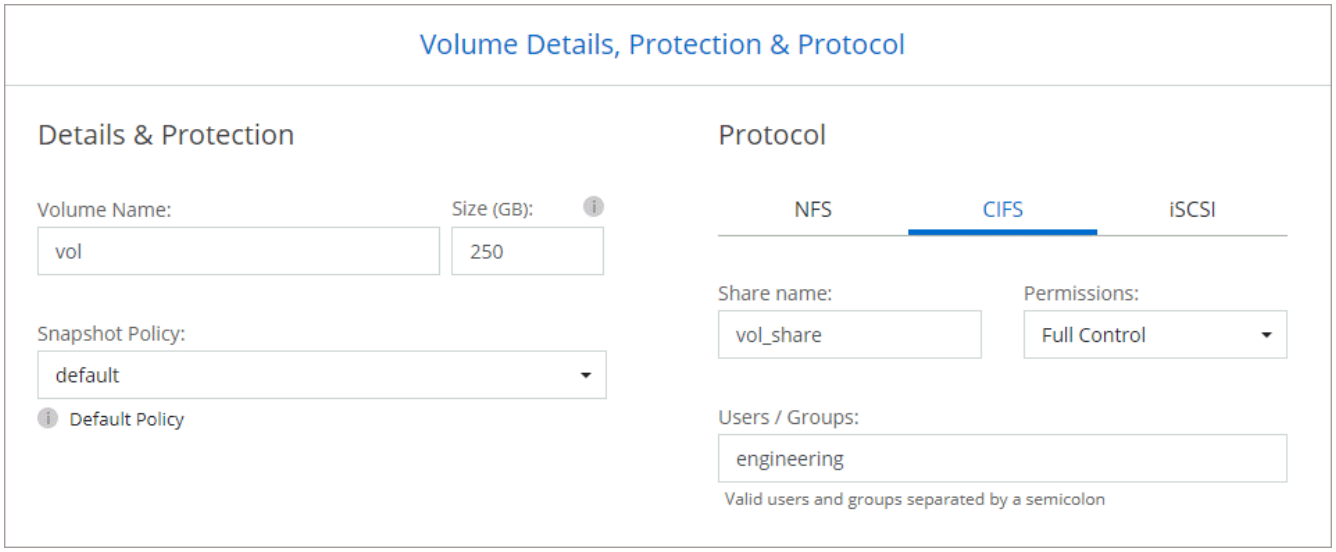
13. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

    Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
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.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt Cloud Manager einen Wert ein, der Zugriff auf alle Instanzen im Subnetz ermöglicht.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch Zugriffssteuerungslisten oder ACLs genannt). Sie können lokale oder domänenbasierte Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Domain-Windows-Benutzernamen angeben, müssen Sie die Domäne des Benutzers mit dem Format Domain\Benutzername einschließen.
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.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume: Entweder NFSv3 oder NFSv4.

Feld	Beschreibung
Initiatorgruppe und IQN (nur für iSCSI)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. 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. Wenn Sie ein iSCSI-Volume erstellen, erstellt Cloud Manager automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Nachdem Sie das Volume erstellt haben, "Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen".

Die folgende Abbildung zeigt die für das CIFS-Protokoll ausgefüllte Volume-Seite:



14. **CIFS Setup**: Wenn Sie das CIFS-Protokoll wählen, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
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.
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.

Feld	Beschreibung
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. Um Azure AD-Domänendienste als AD-Server für Cloud Volumes ONTAP zu konfigurieren, müssen Sie in diesem Feld **OU=AADDC-Computer** oder **OU=AADDC-Benutzer** eingeben.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"^]
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 "Cloud Manager API-Entwicklerleitfaden" Entsprechende Details.

15. **Nutzungsprofil, Festplattentyp und Tiering-Richtlinie**: Wählen Sie aus, ob Sie Funktionen für die Storage-Effizienz aktivieren und gegebenenfalls die Volume Tiering-Richtlinie ändern möchten.

    Weitere Informationen finden Sie unter "Allgemeines zu Volume-Nutzungsprofilen" Und "Data Tiering - Übersicht".

16. **Überprüfen & Genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um Details zum Support und zu den von Cloud Manager erworbenen Azure Ressourcen anzuzeigen.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie Auf **Go**.

Ergebnis

Cloud Manager implementiert das Cloud Volumes ONTAP System. Sie können den Fortschritt in der Timeline verfolgen.

Wenn Sie Probleme bei der Implementierung des Cloud Volumes ONTAP Systems haben, lesen Sie die Fehlermeldung. Sie können auch die Arbeitsumgebung auswählen und auf **Umgebung neu erstellen** klicken.

Weitere Hilfe finden Sie unter "NetApp Cloud Volumes ONTAP Support".

Nachdem Sie fertig sind

- 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, verwenden Sie System Manager oder die CLI.

  Mithilfe von Quotas können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder qtree verwendeten Dateien einschränken oder nachverfolgen.